ASA FirePOWER 模块用户指南

5.4.1 版
2015 年 1 月 22 日

思科系统公司
www.cisco.com
思科在全球设有 200 多个办事处。
有关地址、电话号码和传真号码信息，
可查阅思科网站：
www.cisco.com/go/offices。

本手册中有关产品的规格和信息如有更改，恕不另行通知。我们相信本手册中的所有声明、信息和建议均准确可靠，但不提供任何明示或暗示的担保。用户应承担使用产品的全部责任。

随产品一起提供的信息包含有产品配套的软件许可和有限担保，且构成本文的一部分。如果您找不到软件许可或有限担保，请与思科代表联系以索取副本。

思科所采用的 TCP 报头压缩是加州大学伯克莱分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。版权所有。© 1981，加利福尼亚州大学董事会。

无论在该手册中是否作出了其他担保，来自这些供应商的所有文档文件和软件都按“原样”提供且仍有可能存在缺陷。思科和上述供应商不承诺所有明示或暗示的担保，包括（但不限于）对特定用途的适销性、适用性、非侵权性以及因交易、使用或商业惯例所衍生的担保。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

思科和思科徽标是思科和/或其附属公司在美国 和其他国家/地区的商标或注册商标。要查看思科商标的列表，请访问以下 URL：www.cisco.com/go/trademarks。文中提及的第三方商标均归属各所有者。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。 (1110R)

本文档中使用的任何互联网协议 (IP) 地址和电话号码并不代表实际地址和电话号码。本文档中包括的任何示例、命令显示输出、网络拓扑图和其他图形仅用于说明目的。在图示内容中使用的 IP 地址或电话号码纯属虚构，如有雷同，纯属巧合。

© 2015 年 思科系统公司。版权所有。

目 录

思科 ASA FirePOWER 模块介绍

思科 ASA FirePOWER 模块® 是可以在思科 ASA5506-X 设备上部署的模块。此模块旨在帮助您在遵守贵组织的安全策略 （保护网络的准则）的情况下处理网络流量。安全策略可能还包括可接受的使用策略 (AUP)，该策略向员工提供他们可以如何使用贵组织的系统的准则。

本指南提供有关 ASA FirePOWER 模块特性和功能的 onbox 配置的信息，可通过 ASDM 访问。每章的说明文本、图形和操作步骤都提供了详细信息，帮助您浏览用户界面，最大限度地提高系统性能，并提供疑难解答。

注 如果在托管 ASA FirePOWER 模块的 ASA 上启用命令授权，您必须使用具有权限级别 15 的用户名登录，以查看 ASA FirePOWER 的主页、配置页面和监控页面。不支持对 ASA FirePOWER 页面的只读或仅监控访问，状态页除外。

以下主题将介绍 ASA FirePOWER 模块，描述其主要组件，并帮助您了解如何使用本指南：

ASA FirePOWER 模块介绍

在网段上安装的 ASA 设备上运行的 ASA FirePOWER 模块监控流量以进行分析。

内联部署的系统可以使用*访问控制*影响流量的传输，允许您以精细方式指定如何处理传入、传出和穿越网络的流量。您收集的有关网络流量的数据以及从中获取的所有信息都可用来基于以下条件过滤和控制该流量：

- 简单、易于确定的传输层和网络层特征：源和目的、端口和协议等
- 流量的最新的上下文信息，包括诸如信誉、风险、业务相关性、使用的应用或访问的 URL 等特征
- 贵组织中的 Microsoft Active Directory LDAP 用户

每种类型的流量检查和控制都以提供最大灵活性和性能的方式进行。例如，基于信誉的黑名单，因为它使用简单的源和目标数据，可以在进程中较早阻止禁止的流量，同时检测和阻止入侵和攻击是最后一道防线。

ASA FirePOWER 模块组件

以下主题介绍 的一些确保贵组织安全的重要功能、可接受的使用策略和流量管理战略：

访问控制

*访问控制*是一项基于策略的功能，可用于指定、检查和记录可以流经网络的流量。*访问控制策*决定系统如何处理网络上的流量。

最简单的访问控制策略使用其*默认操作*处理所有流量。 您可以将此默认操作设置为阻止或信任所有流量，而无需进一步检查，或者检查流量以获取是否存在入侵。

更复杂的访问控制策略可以根据安全情报数据将流量列入黑名单，以及使用*访问控制规则*对网络流量记录和处理进行精细控制。这些规则可以简单或复杂，使用多个条件匹配和检查流量；您可以通过安全区域、网络或地理位置、端口、应用、请求的 URL 和用户来控制流量。高级访问控制选项包括预处理和性能。

每个访问控制规则还具有一个*操作*，用于确定是否监控、信任、阻止或允许匹配的流量。当您允许流量时，可以指定在流量到达您的资产或退出您的网络之前，系统首先利用入侵或文件策略对其进行检查以阻止任何漏洞攻击、恶意软件或禁止的文件。

入侵检测和防御

入侵检测和防御是系统在允许流量到达目的地之前的最后一道防线。*入侵策略*是访问控制策略调用的几组已定义的入侵检测和防御配置。使用*入侵规则*和其他设置，这些策略检查流量是否存在安全违规，以及在内联部署中可以阻止或修改恶意流量。

如果系统提供的策略不能完全满足贵组织的安全需求，那么自定义策略可以改进环境中的系统性能，并且可以提供网络中发生的恶意流量和策略违规的集中视图。通过创建和调整自定义策略，您可以非常精细地配置系统如何处理和检查网络中流量的入侵情况。

高级恶意软件防护和文件控制

为了帮助识别和减轻恶意软件的影响， ASA FirePOWER 模块的文件控制和高级恶意软件防护组件可以检测、跟踪、捕获、分析和阻止 （可选）网络流量中的文件传输 （包括恶意软件文件和档案文件中的嵌套文件）。

文件控制

*文件控制*允许设备检测并阻止用户通过特定应用协议上传 （发送）或下载 （接收）特定类型的文件。可以配置文件控制，作为全局访问控制配置的一部分；与访问控制规则关联的文件策略可以检查符合规则条件的网络流量。

基于网络的高级恶意软件防护 (AMP)

基于网络的*高级恶意软件防护* (AMP) 允许系统检查几种类型的文件中的网络流量是否存在恶意软件。

无论是否存储检测到的文件，都可以将其提交给综合安全情报云，使用文件的 SHA-256 哈希值进行简单的已知性质搜索。使用此上下文信息，可以配置系统来阻止或允许特定的文件。

可以配置恶意软件防护，作为全局访问控制配置的一部分；与访问控制规则关联的文件策略可以检查符合规则条件的网络流量。

可为网络服务、协调和服务管理功能体现出网络价值的

有几种方法可以使用应用程序编程接口 (API) 来与系统交互。有关详细信息，可以从以下任一支持站点下载更多文档：

- **Sourcefire**：(https://support.sourcefire.com/)
- **思科**：(http://www.cisco.com/cisco/web/support/index.html)

许可证约定

各个章节开头的许可证声明指出了使用本节所述功能所要求使用的许可证，详情如下：

保护

保护许可证允许设备进行入侵检测和防御、文件控制以及安全情报过滤。

可控性

可控性许可证允许设备执行用户和应用控制。可控性许可证要求具备保护许可证。

URL 过滤

URL 过滤许可证允许设备基于受监控主机请求的 URL，使用定期更新的云计算型的类别和信誉数据确定哪些流量可以流经网络。 URL 过滤许可证要求具备保护许可证。

恶意软件

恶意软件许可证允许设备执行基于网络的高级恶意软件防护 (AMP)，也就是说，检测、捕获并阻止通过网络传输的文件中的恶意软件。它还允许查看其轨迹，跟踪通过网络传输的文件。恶意软件许可证要求具备保护许可证。

由于许可的功能通常是累加的，此文档仅提供每项功能的最高要求许可证。例如，如果功能需要保护可控性许可证，则只列出可控性。但是，如果功能要求的不是附加的许可证，文档列出它们时会带有加号 (+)。

许可证声明中“或”语句表明要使用本部分描述的功能需要使用特定的许可证，但是附加许可证可以增加功能。例如，在文件策略内，有些文件规则操作要求使用保护许可证，而其他的则要求使用恶意软件许可证。因此，文件规则文档的许可证声明会列出保护或恶意软件。

IP 地址约定

可以使用 IPv4 无类域间路由选择 (CIDR) 表示法和类似的 IPv6 前缀长度表示法定义 ASA FirePOWER 模块很多位置的地址块。

CIDR 表示法使用网络 IP 地址结合位掩码来定义指定地址块中的 IP 地址。例如，下表列出了 CIDR 表示法中的 IPv4 地址空间。

表 1-1　CIDR 表示法语法示例

CIDR 块	CIDR 块中的 IP 地址	子网掩码	IP 地址数量
10.0.0.0/8	10.0.0.0 - 10.255.255.255	255.0.0.0	16,777,216
172.16.0.0/12	172.16.0.0 - 172.31.255.255	255.240.0.0	1,048,576
192.168.0.0/16	192.168.0.0 - 192.168.255.255	255.255.0.0	65,536

同样， IPv6 使用网络 IP 地址结合前缀长度来定义指定块中的 IP 地址。例如， 2001:db8::/32 指定的 IPv6 地址在 2001:db8:: 网络中，前缀长度为 32 位，即 2001:db8:: 至 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff。

使用 CIDR 或前缀长度表示法指定 IP 地址块时， ASA FirePOWER 模块只使用前缀长度指定的网络 IP 地址部分。例如，如果键入 10.1.2.3/8，则 ASA FirePOWER 模块使用 10.0.0.0/8。

换句话说，虽然思科建议使用 CIDR 或前缀长度表示法时采用使用标准网络 IP 地址的标准方法，但是 ASA FirePOWER 模块并不要求必须这么做。

管理可重用对象

为提高灵活性以及易用性， ASA FirePOWER 模块允许创建命名*对象*；命名对象是将名称与值相关联的可重复使用的配置，以便在要使用该值时，可以改用此命名对象。

可建以下类型的对象：

- 表示 IP 地址和网络、端口/协议对、安全区域以及源/目标国家/地区 （地理定位）的基于网络的对象。
- 帮助处理流量的对象，包括安全情报源和列表、应用过滤器、 URL、文件列表和入侵策略变量集

可以在 ASA FirePOWER 模块的不同位置使用这些对象，包括访问控制策略、网络分析策略、入侵策略和规则、报告、控制面板等等。

将对象分组使得可以引用带有单个配置的多个对象。可以将网络、端口、 URL 对象分组。

注 在大多数情况下，编辑策略中使用的对象要求重新应用策略以使更改生效。编辑安全区域后也需要重新应用相应的设备配置。

有关详细信息，请参阅以下各节：

使用对象管理器

许可证：任何环境

使用对象管理器 (**Configuration > ASA FirePOWER Configuration > Object Management**) 创建和管理对象，包括应用过滤器、变量集和安全区域。可以将网络、端口、 URL 对象 对象分组；还可以排序、过滤和浏览对象及对象组的列表。

有关详情，请参阅：

- 第 2-2 页上的将对象分组
- 第 2-3 页上的浏览、排序和过滤对象

将对象分组

许可证：任何环境

可以将网络、端口、和 URL 对象分组。系统允许互用对象和对象组。例如，在任何要使用端口对象的地方，也可以使用端口对象组。相同类型的对象和对象组不能具有相同的名称。

编辑策略中使用的对象组 （例如，访问控制策略中使用的网络对象组）时，必须重新应用该策略以使更改生效。

删除组不会删除组中的对象，只会删除对象之间的相关性。此外，也无法删除正在使用的组。例如，无法删除在已保存访问控制策略中的 URL 条件内使用的 URL 组。

要将可重用对象分组，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在要分组的 **Network**、 **Port**或 **URL** 对象类型下，选择 **Object Groups**。

系统显示要分组的对象类型的页面。

步骤 3　点击要分组的对象对应的 **Add** 按钮。

显示一个弹出窗口，可以在其中创建组。

步骤 4　在 **Name** 字段中为创建的组键入名称。可以使用除花括号 ({}) 以外的所有可打印标准 ASCII 字符。

步骤 5　选择一个或多个对象，然后点击 **Add**。

- 使用 Shift 和 Ctrl 键可选择多个对象，或者右键单击并选择 **Select All**。
- 使用过滤器字段 ( ) 可搜索要包括的现有对象，在您键入时，该字段会更新以显示匹配的项目。点击搜索字段上方的重新加载图标 ( )，或点击搜索字段中的清除图标 ( ) 可清除搜索字符串。
- 如果现有对象不符合您的需要，可点击添加图标 ( ) 快速创建对象。

步骤 6　点击 **Store ASA FirePOWER Changes**。

组创建成功。

浏览、排序和过滤对象

许可证：任何环境

对象管理器每页显示 20 个对象或对象组。如果有超过 20 个任何类型的对象或对象组，请使用位于页面底部的导航链接查看其他页面。还可以转到特定页或点击刷新图标 ( ) 刷新视图。

默认情况下，页面会按名称的字母顺序列示对象和对象组。然而，也可以按显示的任何列对每种类型的对象或对象组进行排序。列标题旁边的向上 (▲) 或向下 (▼) 箭头表示页面按该列升序或降序排序。还可以按名称或值对页面上的对象进行过滤。

要排序对象或对象组：

步骤 1　点击列标题。要按相反方向排序，请再次点击标题。

要过滤对象或对象组：

步骤 1　在 **Filter** 字段中键入搜索条件。

页面会在您键入内容时进行更新，以显示匹配的项目。字段接受一个或多个星号 (*) 作为通配符。

使用网络对象

许可证：任何环境

网络对象代表可单独指定或作为地址块指定的一个或多个 IP 地址。可以在 ASA FirePOWER 模块中的不同位置使用网络对象和对象组（请参阅第 2-2 页上的将对象分组），包括访问控制策略、网络变量、入侵规则、报告等等。

无法删除正在使用的网络对象。此外，在编辑访问控制策略、策略或入侵策略中使用的网络对象后，必须重新应用策略以使更改生效。

要创建网络对象：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **Network** 下，选择 **Individual Objects**。

步骤 3　点击 **Add Network**。

系统将显示 Network Objects 弹出窗口。

步骤 4　在 **Name** 字段中为网络对象键入名称。可以使用除花括号 ({}) 以外的所有可打印标准 ASCII 字符。

步骤 5　对于要添加到网络对象的每个 IP 地址或地址块，键入其值，然后点击 **Add**。

步骤 6　点击 **Store ASA FirePOWER Changes**。

网络对象添加成功。

使用安全情报列表和源

许可证：保护

安全情报功能允许根据源或目标 IP 地址对每个访问控制策略指定可以流经网络的流量。如果要将特定 IP 地址加入黑名单（即，在访问控制规则对流向和来自该 IP 地址的流量进行分析之前拒绝这些流量），这尤其有用。同样，可将 IP 地址添加到白名单，从而强制系统使用访问控制来处理这些 IP 地址的连接。

如果不确定是否要将特定 IP 地址添加到黑名单，可以使用“仅监控”设置，这样，系统可以使用访问控制来处理连接，但也会记录连接与黑名单的匹配情况。

默认情况下，每个访问控制策略中都包括*全局白名单*和*全局黑名单*，它们适用于所有区域。此外，在每个访问控制策略中，可以使用网络对象和对象组的组合，以及安全情报列表和源（这些都可使用安全区域进行限制）来建立独立的白名单和黑名单。

比较源和列表

安全情报*源*是系统按配置的间隔从 HTTP 或 HTTPS 服务器下载的 IP 地址的动态集合。由于源会定期更新，因此，系统可使用最新信息来过滤网络流量。为帮助构建黑名单， ASA FirePOWER 模块提供*情报源*；情报源表示 VRT 确定的信誉不佳的 IP 地址。

尽管源更新可能需要几分钟才会生效，但是在创建或修改源后或在计划的源更新后不必重新应用访问控制策略。

注　如果要对系统从互联网下载源的时间进行严格控制，可以禁用该源的自动更新。但是，思科建议您允许自动更新。虽然可以手动执行按需更新，但是允许系统定期下载源可获得最新、最相关的数据。

与源相比，安全情报*列表*是手动上传到系统的 IP 地址的简单静态列表。可使用自定义列表对源以及全局白名单和黑名单进行扩充和微调。请注意，编辑自定义列表（以及编辑网络对象和从全局白名单或黑名单删除 IP 地址）后，需要重新应用访问控制策略，才能使更改生效。

格式化和已损坏源数据

源和列表源文件必须是大小不超过 500MB 的简单文本文件，每个 IP 地址或地址块占一行。注释行必须以 `#` 字符开头。列表源文件必须使用 `.txt` 扩展名。

如果系统下载损坏的源或具有无法识别的 IP 地址的源，则系统会继续使用旧源数据（除非是第一次下载）。但是，如果系统可以识别即便源中的一个 IP 地址，也会使用其可识别的地址更新。

互联网访问和高可用性

系统使用 443/HTTPS 端口下载情报源，使用 443/HTTP 或 80/HTTP 端口下载自定义源或第三方源。要更新源，必须打开设备上的相应端口（入站和出站）。如果系统无法直接访问源站点，可以使用代理服务器。

注　在下载自定义源时，系统不执行对等 SSL 证书验证，系统也不支持使用证书捆绑包或自签证书来验证远程对等设备。

管理源和列表

可以使用对象管理器的 Security Intelligence 页面创建和管理安全情报列表和源（统称为安全情报对象）。（有关创建和管理网络对象和对象组的信息，请参阅第 2-3 页上的使用网络对象。）

请注意，无法删除当前正用于已保存或已应用的访问控制策略的自定义列表或源。也不能删除全局列表，但可以移除单个 IP 地址。同样，虽然不能删除情报源，但对情报源进行编辑可以禁用或更改其更新频率。

安全情报对象快速参考

下表提供了可用于执行安全情报过滤的对象的快速参考。

表 2-1　安全情报对象功能

容量	全局白名单或黑名单	情报源	自定义源	自定义列表	网络对象
使用方法	默认情况下在访问控制策略中	在所有访问控制策略中作为白名单或黑名单对象			
是否可以通过安全区域进行限制？	no	是	是	是	是
是否可以删除？	no	no	是，除非当前正用于已保存或已应用的访问控制策略		
对象管理器编辑功能	仅删除 IP 地址	禁用或更改更新频率	完全修改	仅上传已修改列表	完全修改
修改后是否需要重新应用访问控制策略？	删除后需要重新应用（添加 IP 地址后不需要重新应用）	no	no	是	是

有关创建管理和使用安全情报列表和源的详细信息，请参阅：

- 第 2-5 页上的使用全局白名单和黑名单
- 第 2-6 页上的使用情报源
- 第 2-7 页上的使用自定义安全情报源
- 第 2-7 页上的手动更新安全情报源
- 第 2-8 页上的使用自定义安全情报列表
- 第 5-1 页上的使用安全情报 IP 地址声誉设置黑名单

使用全局白名单和黑名单

许可证：保护

默认情况下，每个访问控制策略中都包含系统的全局白名单和全局黑名单，它们应用于所有区域。可以为每个策略选择是否使用这些全局列表。

向全局列表中添加 IP 地址后，不必重新应用访问控制策略。相反，从全局白名单或黑名单删除 IP 地址后，必须应用访问控制策略，更改才会生效。

请注意，尽管可以将子网掩码为 /0 的网络对象添加到白名单或黑名单，但这些对象中使用 `/0` 子网掩码的地址块将被忽略，并且不会基于这些地址进行白名单和黑名单过滤。安全情报源中子网掩码为 `/0` 的地址块将被忽略。如果希望监控或阻止策略所针对的所有流量，请分别使用具有 **Monitor** 或 **Block** 规则操作的访问控制规则，并使用 **Source Networks** 和 **Destination Networks** 的默认值 **any**，而不使用安全情报过滤。

从全局白名单或黑名单移除 IP 地址：

步骤 1　在对象管理器的 Security Intelligence 页面上，点击全局白名单或黑名单旁边的编辑图标 ( )。

系统将显示 Global Whitelist 或 Global Blacklist 弹出窗口。

步骤 2　点击列表中要移除的 IP 地址旁边的删除图标 ( )。

要一次删除多个 IP 地址，请使用 Shift 和 Ctrl 键选择要删除的 IP 地址，然后右键单击并选择 **Delete**。

步骤 3　点击 **Store ASA FirePOWER Changes**。

更改保存成功，但必须应用访问控制策略以使其生效。

使用情报源

许可证：保护

为帮助构建黑名单，ASA FirePOWER 模块提供情报源（包括 VRT 确定为信誉不佳的 IP 地址的多个定期更新列表）。源中的每个列表代表一个特定类别：开放中继、已知攻击者、伪造 IP 地址（虚假）等。在访问控制策略中，可以将任何或所有类别加入到黑名单。

由于情报源会定期更新，因此系统可以使用最新信息来过滤网络流量。恶意 IP 地址是指诸如恶意软件、垃圾邮件、僵尸网络以及网络钓鱼的安全威胁，它们的出现和消失速度要快于更新和应用新策略的速度。

虽然不能删除情报源，但对情报源进行编辑可以更改其更新频率。默认情况下，源每两小时更新一次。

要修改情报源的更新频率：

步骤 1　在对象管理器的 Security Intelligence 页面上，点击 Intelligence Feed 旁边的编辑图标 ( )。

系统将显示 Security Intelligence 弹出窗口。

步骤 2　编辑 **Update Frequency**。

可选择从两小时到一周不等的时间间隔。也可以禁用源更新。

步骤 3　点击 **Store ASA FirePOWER Changes**。

已保存您的更改。

使用自定义安全情报源

许可证：保护

自定义或第三方安全情报源允许您使用互联网上其他定期更新且信誉良好的白名单和黑名单来扩充情报源。您也可以设置内部源；。

配置源时，可使用 URL 指定位置；但 URL 不能使用 Punycode 编码。默认情况下，系统按配置的间隔下载整个源。

或者，可以将系统配置为使用 md5 校验和来确定是否下载更新的源。如果校验和自上次模块下载源以来没有更改，则系统无需重新下载该源。您可能希望将 md5 校验和用于内部源，尤其是那些很大的内部源。 md5 校验和必须存储在仅带有该校验和的简单文本文件中。不支持注释。

要配置安全情报源：

步骤 1　在对象管理器的 Security Intelligence 页面上，点击 **Add Security Intelligence**。

系统将显示 Security Intelligence 弹出窗口。

步骤 2　在 **Name** 字段中为源键入名称。可以使用除花括号 ({}) 以外的所有可打印标准 ASCII 字符。

步骤 3　从 **Type** 下拉列表中指定要配置 **Feed**。

弹出窗口将会更新以显示新的选项。

步骤 4　指定**源 URL**，或者，还可以指定 **MD5 URL**。

步骤 5　从 **Update Frequency** 选择更新频率。

可选择从两小时到一周不等的时间间隔。也可以禁用源更新。

步骤 6　点击 **Store ASA FirePOWER Changes**。

安全情报源对象创建成功。除非已禁用源更新，否则系统会尝试下载并验证源。现在，您可以在访问控制策略中使用该源对象。

手动更新安全情报源

许可证：保护

手动更新安全情报源会更新所有源（包括情报源）。

要更新所有安全情报源：

步骤 1　在对象管理器的 Security Intelligence 页面上，点击 **Update Feeds**。

步骤 2　确认要更新所有源。

系统显示确认对话框，警告您更新可能需要几分钟才能生效。

步骤 3　点击 **OK**。

系统下载并验证源更新后，开始使用已更新的源过滤流量。

使用自定义安全情报列表

许可证：保护

安全情报列表是手动上传的 IP 地址和地址块的简单静态列表。如果要增加和微调的源或其中一个全局列表，则自定义列表很有用。

请注意，地址块的子网掩码可以是 0 到 32 之间的任意整数或 0 到 128 之间的任意整数（分别适用于 IPv4 和 IPv6）。

例如，如果信誉良好的源错误地阻止了对重要资源的访问，但整体来说该源对您的组织很有用，您可以创建仅包括分类不当的 IP 地址的自定义白名单，而不从访问控制策略的黑名单中移除该安全情报源对象。

请注意，要修改安全情报列表，必须更改源文件并上传新副本。有关详细信息，请参阅第 2-8 页上的更新安全情报列表。

要将新的安全情报列表上传，请执行以下操作：

步骤 1　在对象管理器的 Security Intelligence 页面上，点击 **Add Security Intelligence**。

系统将显示 Security Intelligence 弹出窗口。

步骤 2　在 **Name** 字段中为列表键入名称。可以使用除花括号 ({}) 以外的所有可打印标准 ASCII 字符。

步骤 3　从 **Type** 下拉列表中指定要上传 **List**。

弹出窗口将会更新以显示新的选项。

步骤 4　点击 **Browse** 浏览至列表 .txt 文件，然后点击 **Upload**。

列表上传成功。弹出窗口将显示系统在列表中查找到的 IP 地址和地址块的总数。

如果显示的数字不是您期望的值，请检查文件格式并重试。

步骤 5　点击 **Store ASA FirePOWER Changes**。

安全情报列表对象保存成功。现在，您可以在访问控制策略中使用该列表对象。

更新安全情报列表

许可证：保护

要编辑安全情报列表，必须更改源文件并上传新副本。不能使用 ASDM 修改文件的内容。如果您无权访问源文件，则可以使用 ASDM 界面下载副本。

要修改安全情报列表：

步骤 1　在对象管理器的 Security Intelligence 页面上，点击要更新的列表旁边的编辑图标 ( )。

系统将显示 Security Intelligence 弹出窗口。

步骤 2　如果需要列表副本进行编辑，请点击 **Download**，然后按照提示将列表另存为文本文件。

步骤 3　根据需要对列表进行更改。

步骤 4　在 Security Intelligence 弹出窗口中，点击 **Browse** 浏览到修改后的列表，然后点击 **Upload**。

列表上传成功。

步骤 5　点击 **Store ASA FirePOWER Changes**。

已保存您的更改。如果列表正由活动访问控制策略使用，则必须应用策略，更改才会生效。

使用端口对象

许可证：任何环境

端口对象以略有不同的方式代表不同协议：

- 对于 TCP 和 UDP，端口对象代表传输层协议（协议号括在括号内，加上一个可选的相关端口或端口范围）。例如：`TCP(6)/22`。
- 对于 ICMP 和 ICMPv6 (IPv6-ICMP)，端口对象代表互联网层协议以及可选类型和代码。例如：`ICMP(1):3:3`。
- 端口对象还可以代表不使用端口的其他协议。

请注意，系统提供已知端口的默认端口对象。可以修改或删除这些对象，但思科建议您创建自定义端口对象。

可以在 ASA FirePOWER 模块中的不同位置使用端口对象和对象组（请参阅第 2-2 页上的将对象分组），包括访问控制策略、端口变量和事件搜索。

不能删除正在使用的网络端口。此外，在编辑访问控制策略中使用的端口对象后，必须重新应用策略以使更改生效。

请注意，不能为访问控制规则中的源端口条件添加除 TCP 或 UDP 以外的任何协议。此外，在规则中设置源端口条件和目标端口条件时，不能混用传输协议。

如果向源端口条件中使用的端口对象组添加不受支持的协议，则使用了该协议的规则在应用策略时不会应用。此外，如果创建同时包含 TCP 和 UDP 端口的端口对象，然后将其添加为规则的源端口条件，则不能添加目标端口，反之亦然。

要创建端口对象：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **Port** 下，选择 **Individual Objects**。

步骤 3　点击 **Add Port**。

系统将显示 Port Objects 弹出窗口。

步骤 4　在 **Name** 字段中为端口对象键入名称。可以使用除花括号 ({}) 以外的所有可打印标准 ASCII 字符。

步骤 5　选择 **Protocol**。

可以快速选择 **TCP**、**UDP**、**IP**、**ICMP** 或 **IPv6-ICMP**，或者使用 **Other** 下拉列表选择其他协议或选择 **All**。

步骤 6　或者，使用 **Port** 或端口范围限制 TCP 或 UDP 端口对象。

可以指定 1 到 65535 之间的任何端口，或者指定 `any` 以匹配所有端口。使用连字符可指定端口范围。

步骤 7　或者，使用 **Type** 和相关 **Code**（如果适当）限制 ICMP 或 IPV6-ICMP 端口对象。

创建 ICMP 或 IPv6 ICMP 对象时，可以指定类型和代码（如适用）。有关 ICMP 类型和代码的详细信息，请参阅 http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml 和 http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml。可以将类型设置为 any 以匹配任意类型，或者将代码设置为 any 以匹配指定类型的任意代码。

步骤 8　或者，选择 **Other** 并从下拉列表中选择协议。如果选择 **All**，请在 **Port** 字段中键入端口号。

步骤 9　点击 **Store ASA FirePOWER Changes**。

端口对象添加成功。

使用 URL 对象

许可证：任何环境

配置的每个 URL 对象代表单个 URL 或 IP 地址。可以在使用 URL 对象和对象组（请参阅第 2-2 页上的将对象分组），包括访问控制策略。例如，可以编写阻止特定 URL 的访问控制规则。

请注意，要阻止 HTTPS 流量，可以输入从流量的安全套接字层 (SSL) 证书中获取的 URL。输入从证书获取的 URL 时，请输入域名并忽略子域信息。（例如，键入 `example.com` 而不是 `www.example.com`。）如果基于证书 URL 阻止流量，会同时阻止流向该网站的 HTTP 和 HTTPS 流量。

不能删除正在使用的 URL 对象。此外，在编辑用于访问控制策略的 URL 对象后，必须重新应用策略，才能使更改生效。

要添加 URL记对象：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Object Management**。

系统将显示 Object Management 页面。

步骤 2　在 **URL** 下，选择 **Individual Objects**。

步骤 3　点击 **Add URL**。

系统将显示 URL Objects 弹出窗口。

步骤 4　在 **Name** 字段中为 URL 对象键入名称。可以使用除花括号 ({}) 以外的所有可打印标准 ASCII 字符。

步骤 5　键入 URL 对象的 **URL** 或 IP 地址。

步骤 6　点击 **Store ASA FirePOWER Changes**。

URL 对象添加成功。

使用应用过滤器

许可证：任何环境

ASA FirePOWER 模块分析 IP 流量时，会尝试识别网络上常用的应用。应用感知是执行基于应用的访问控制的关键。系统随附适用于许多应用的检测器，而且思科经常通过系统和漏洞数据库 (VDB) 更新和添加更多检测器。

应用过滤器根据与应用的风险、业务相关性、类型、类别和标记关联的条件对应用进行分组。使用应用过滤器可以快速为访问控制规则创建应用条件，因为无需逐个搜索和添加应用；有关详细信息，请参阅第 8-3 页上的将流量与应用过滤器相匹配。

使用应用过滤器的另一个好处是，修改或添加新应用时，无需更新使用过滤器的访问控制规则。例如，如果配置访问控制策略阻止所有社交网络应用，并且 VDB 更新包括新的社交网络应用检测器，更新该 VDB 时就会更新该策略。虽然必须先重新应用策略，系统才可以阻止新应用，但无需更新阻止该应用的访问控制规则。

如果思科提供的应用过滤器未根据您的需求对应用分组，您可以创建自己的过滤器。用户定义的过滤器可以对ASA FirePOWER 模块提供的过滤器进行分组和组合。例如，您可以创建可阻止所有非常高风险、低业务相关性应用的过滤器。您还可以通过手动指定单个应用来创建过滤器，但请谨记，当更新模块软件或 VDB 时，这些过滤器不会自动更新。

可以在访问控制规则中使用用户定义的应用过滤器，就像使用ASA FirePOWER 模块提供的应用过滤器一样。

使用对象管理器 (**Configuration > ASA FirePOWER Configuration > Object Management**) 创建和管理应用过滤器。请注意，还可以在向访问控制规则添加应用条件时快速创建应用过滤器。

Application Filters 列表包括ASA FirePOWER 模块提供的应用过滤器，您可以选择它们来构建自己的过滤器。可以使用搜索字符串来限制显示的过滤器；这对类别和标记尤其有用。

Available Applications 列表包含所选过滤器中的各个应用。还可以使用搜索字符串来限制显示的应用。

系统将同一类型的多个过滤器与 OR 操作关联。假设一个中等风险过滤器包含 100 个应用，一个高风险过滤器包含 50 个应用。如果同时选择两个过滤器，系统将显示 150 个可用的应用。

系统将不同类型的过滤器与 AND 操作关联。例如，如果选择中等风险和高风险过滤器，以及中等业务相关性和高业务相关性过滤器，系统将显示具有中等或高风险的应用，以及具有中等或高业务相关性的应用。

提示 点击信息图标 ( ) 可获得相关应用的详细信息。要显示其他信息，请点击弹出窗口中的任意互联网搜索链接。

在确定要添加到过滤器的应用后，可以逐个添加这些应用，或者，如果选择了应用过滤器，可选择 **All apps matching the filter**。可以添加多个过滤器和多个应用的任意组合，只要 Selected Applications and Filters 列表中的总项数不超过 50。

创建的应用过滤器会在对象管理器的 Application Filters 页面上列出。该页面显示组成每个过滤器的条件总数。

有关对显示的应用过滤器进行排序和过滤的信息，请参阅第 2-2 页上的使用对象管理器。请注意，不能删除正在使用的应用过滤器。此外，在编辑用于访问控制策略的应用过滤器后，必须重新应用策略，才能使更改生效。

要创建应用过滤器：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Object Management**。

系统将显示 Object Management 页面。

步骤 2　点击 **Application Filters**。

系统将显示 Application Filters 部分。

步骤 3　点击 **Add Application Filter**。

系统将显示 Application Filters 弹出窗口。

步骤 4　在 **Name** 字段中为过滤器提供名称。可以使用除花括号 ({}) 以外的所有可打印标准 ASCII 字符。

步骤 5　或者，在 **Application Filters** 列表中使用ASA FirePOWER 模块提供的过滤器，以减少要添加到过滤器的应用列表中的应用数量：

- 点击每种过滤器类型旁边的箭头可展开和折叠列表。
- 右键单击某种过滤器类型并点击 **Check All** 或 **Uncheck All**。请注意，列表会指示已选择的每种类型的过滤器数目。
- 要减少显示的过滤器，请在 **Search by name** 字段中键入搜索字符串；这对类别和标记尤其有用。要清除搜索，请点击清除图标 ( )。
- 要刷新过滤器列表并清除所有选定的过滤器，请点击重新加载图标 ( )。
- 要清除所有过滤器和搜索字段，请点击 **Clear All Filters**。

与所选过滤器匹配的应用将会显示在 Available Applications 列表中。该列表每次显示 100 个应用。

步骤 6　从 **Available Applications** 列表中选择要添加到过滤器的应用：

- 选择 **All apps matching the filter** 可添加满足在上一步骤中指定的限制条件的所有应用。
- 要减少显示的应用，请在 **Search by name** 字段中键入搜索字符串。要清除搜索，请点击清除图标 ( )。
- 使用位于列表底部的页码图标可浏览可用应用的列表。
- 使用 Shift 和 Ctrl 键可选择多个应用。右键单击并选择 **Select All** 可全部选择当前显示的应用。
- 要刷新应用列表并清除所有选定的应用，请点击重新加载图标 ( )。

不能同时选择单个应用和 **All apps matching the filter**。

步骤 7　将所选应用添加到过滤器。可以点击并拖动，也可以点击 **Add to Rule**。

结果是以下项的组合：

- 所选的应用过滤器
- 所选的各个可用应用，或者 **All apps matching the filter**

最多可以将 50 个应用和过滤器添加到过滤器。要从所选应用中删除应用或过滤器，请点击相应的删除图标 ( )。还可以选择一个或多个应用和过滤器，或右键单击并选择 **Select All**，然后右键单击并选择 **Delete Selected**。

步骤 8　点击 **Store ASA FirePOWER Changes**。

应用过滤器保存成功。

使用变量集

许可证：保护

变量代表通常在入侵规则中用来识别源 IP 地址、目标 IP 地址、源端口和目标端口的值。还可以在入侵策略中使用变量表示规则抑制、自适应配置文件和动态规则状态中的 IP 地址。

提示　无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。

可以使用变量集对变量进行管理、自定义和分组。可以使用 ASA FirePOWER 模块提供的默认变量集，也可以创建您自己的自定义变量集。可以在任何变量集中修改预定义默认变量，以及添加和修改用户定义的变量。

ASA FirePOWER 模块提供的大多数共享对象规则和标准文本规则都使用预定义的默认变量来定义网络和端口号。例如，大部分规则使用变量 `$HOME_NET` 指定受保护网络，使用变量 `$EXTERNAL_NET` 指定未受保护（或外部）网络。此外，专用规则通常会使用其他预定义的变量。例如，检测针对网络服务器的漏洞攻击的规则使用 `$HTTP_SERVERS` 和 `$HTTP_PORTS` 变量。

当变量更准确地反映网络环境时，规则更加有效。至少应修改默认变量集中的的默认变量，如第 2-13 页上的优化预定义默认变量中所述。通过确保变量 （例如 `$HOME_NET`）正确地定义网络且 `$HTTP_SERVERS` 包括网络上的所有网络服务器，从而优化处理和监控所有相关系统的可疑活动。

要使用变量，请将变量集链接到与访问控制规则相关的入侵策略或访问控制策略的默认操作。默认情况下，默认设置集链接到访问控制策略使用的所有入侵策略。

有关详细信息，请参阅：

- 第 2-13 页上的优化预定义默认变量
- 第 2-15 页上的了解变量集
- 第 2-17 页上的管理变量集
- 第 2-18 页上的管理变量
- 第 2-19 页上的添加和编辑变量
- 第 2-24 页上的重置变量
- 第 2-25 页上的将变量集链接到入侵策略
- 第 2-25 页上的了解高级变量

优化预定义默认变量

许可证：保护

默认情况下， ASA FirePOWER 模块提供一个默认变量集，它包含预定义默认变量。漏洞研究团队 (VRT) 使用规则更新来提供新的和已更新的入侵规则及其他入侵策略元素，包括默认变量。有关详细信息，请参阅第 35-8 页上的导入规则更新和本地规则文件。

由于 ASA FirePOWER 模块提供的许多入侵规则使用预定义默认变量，因此应为这些变量设置适当的值。可以在任何或所有变量集中修改这些默认变量的值，具体取决于如何使用变量集识别网络流量。有关详细信息，请参阅第 2-19 页上的添加和编辑变量。

注意事项　导入访问控制策略或入侵策略会以导入的默认变量覆盖默认变量集中的现有默认变量。如果现有默认变量集包含不属于导入默认变量集的自定义变量，则会保留该唯一的变量。有关详细信息，请参阅第 B-3 页上的导入配置。

下表介绍 ASA FirePOWER 模块提供的变量并指示通常会修改哪些变量。要获得为网络定制自定义变量方面的帮助，请联系专业服务或支持部门。

表 2-2　ASA FirePower 模块提供的变量

变量名	说明	是否需要修改？
$AIM_SERVERS	定义已知的 AOL Instant Messenger (AIM) 服务器，并用于基于聊天的规则和查找 AIM 漏洞攻击的规则。	不需要。
$DNS_SERVERS	定义域名服务 (DNS) 服务器。如果创建专门影响 DNS 服务器的规则，可以使用 $DNS_SERVERS 变量作为目标或源 IP 地址。	在当前规则集中不需要。
$EXTERNAL_NET	定义 ASA FirePOWER 模块视为未受保护的网络，并在许多规则中用于定义外部网络。	需要；应该充分定义 $HOME_NET，然后避免将 $HOME_NET 作为 $EXTERNAL_NET 的值。
$FILE_DATA_PORTS	定义非加密端口，用于检测网络数据流中的文件的入侵规则。	不需要。
$FTP_PORTS	定义网络上 FTP 服务器的端口，用于 FTP 服务器漏洞攻击规则。	如果 FTP 服务器使用除默认端口以外的端口，需要修改（可以在模块界面中查看默认端口）。
$GTP_PORTS	定义数据包解码器用于提取 GTP（通用分组无线业务 [GPRS] 隧道协议）PDU 中的负载的数据信道端口。	不需要。
$HOME_NET	定义相关入侵策略监控的网络，用于许多定义内部网络的规则。	需要，以便包括内部网络的 IP 地址。
$HTTP_PORTS	定义网络上 FTP 服务器的端口，用于网络服务器漏洞攻击规则。	如果网络服务器使用除默认端口以外的端口，需要修改（可以在模块界面中查看默认端口）。
$HTTP_SERVERS	定义网络上的网络服务器。用于网络服务器漏洞攻击规则。	如果运行 HTTP 服务器，需要修改。
$ORACLE_PORTS	定义网络上的 Oracle 数据库服务器端口，用于扫描针对 Oracle 数据库的攻击的规则。	如果运行 Oracle 服务器，需要修改。
$SHELLCODE_PORTS	定义希望系统对其扫描外壳代码漏洞的端口，用于检测使用外壳代码的漏洞的规则。	不需要。
$SIP_PORTS	定义网络上 SIP 服务器的端口，用于 SIP 漏洞攻击规则。	不需要。
$SIP_SERVERS	定义网络上的 SIP 服务器，用于针对 SIP 的漏洞攻击的规则。	需要；如果运行 SIP 服务器，应该充分定义 $HOME_NET，然后包括 $HOME_NET 作为 $SIP_SERVERS 的值。
$SMTP_SERVERS	定义网络上的 SMTP 服务器，用于解决针对邮件服务器的漏洞的规则。	如果运行 SMTP 服务器，需要修改。
$SNMP_SERVERS	定义网络上的 SNMP 服务器，用于扫描针对 SNMP 服务器的攻击的规则。	如果运行 SNMP 服务器，需要修改。
$SNORT_BPF	代表一个旧版的高级变量，仅当该变量存在于安装了 V5.3.0 之前的 ASA FirePOWER 模块软件的系统，随后软件升级到 V5.3.0 或更高版本的情况下，才会显示该变量。请参阅第 2-25 页上的了解高级变量。	不需要，只能查看或删除此变量。删除此变量后不能对其进行编辑或恢复。

表 2-2　ASA FirePower 模块提供的变量（续）

变量名	说明	是否需要修改？
$SQL_SERVERS	定义网络上的数据库服务器，用于解决针对数据库的漏洞的规则。	如果运行 SQL 服务器，需要修改。
$SSH_PORTS	定义网络上 SSH 服务器的端口，用于 SSH 服务器漏洞规则。	如果 SSH 服务器使用除默认端口以外的端口，需要修改（可以在模块界面中查看默认端口）。
$SSH_SERVERS	定义网络上的 SSH 服务器，用于解决针对 SSH 的漏洞的规则。	需要修改；如果运行 SSH 服务器，应该充分定义 $HOME_NET，然后包括 $HOME_NET 作为 $SSH_SERVERS 的值。
$TELNET_SERVERS	定义网络上的已知 Telnet 服务器，用于解决针对 Telnet 的漏洞的规则。	如果运行 Telnet 服务器，需要修改。
$USER_CONF	提供一个通用工具，使您能够配置无法通过模块界面以其他方式提供的一个或多个功能。请参阅第 2-25 页上的了解高级变量。 ⚠ **注意事项** 存在冲突或重复的 $USER_CONF 配置会导致系统停止。请参阅第 2-25 页上的了解高级变量。	不需要，除非功能描述中有指示或在支持人员的指导下进行。

了解变量集

许可证：保护

将一个变量添加到任意变量集会将其添加到所有变量集；也就是说，每个变量集都是系统中当前配置的所有变量的集合。在任何变量集中，都可以添加用户定义的变量以及自定义任何变量的值。

最初， ASA FirePOWER 模块提供由预定义默认值组成的单个默认变量集。默认变量集中的每个变量最初设置为其默认值，对于预定义变量，该默认值是由 VRT 设置并在规则更新中提供的值。

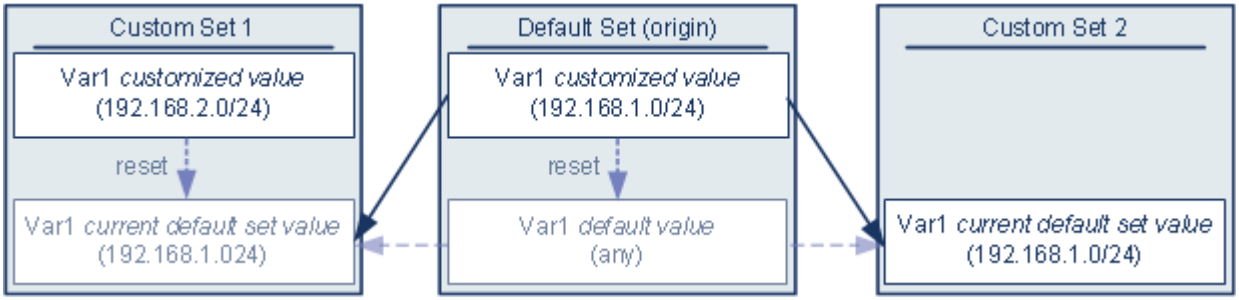
虽然可以将预定义默认变量保留为所配置的默认值，但思科建议您修改预定义变量的子集，如第 2-13 页上的优化预定义默认变量中所述。

可以仅使用默认变量集中的变量，但在许多情况下，执行以下操作可得到最大益处：添加一个或多个自定义变量集；在不同变量集中配置不同的变量值；甚至添加新变量。

使用多个变量集时务必谨记，默认变量集中任何变量的*当前值*决定所有其他变量集中该变量的*默认值*。

示例：将用户定义的变量添加到默认变量集

下图说明了将用户定义的变量 Var1 （其值为 192.168.1.0/24）添加到默认变量集时发生的变量集交互。



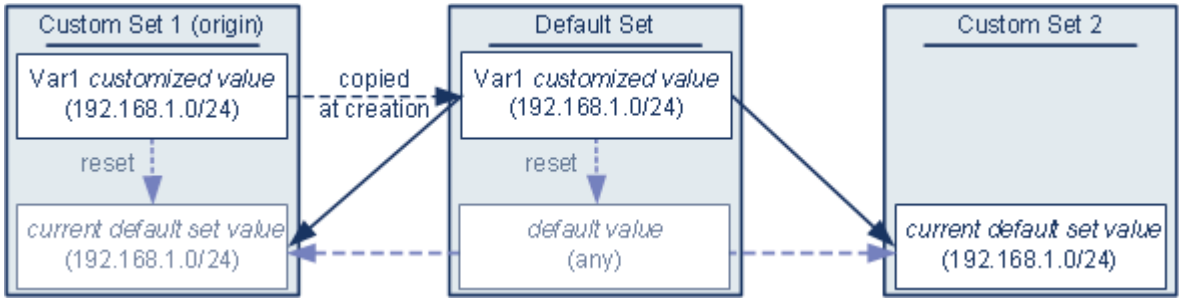
或者，可以在任何变量集中自定义 Var1 的值。在未自定义 Var1 的自定义变量集 2 中，此变量的值是 192.168.1.0/24。在自定义变量集 1 中，Var1 的自定义值 192.168.2.0/24 覆盖了默认值。重置默认变量集中某个用户定义的变量会将所有变量集中该变量的默认值重置为 any。

须注意的一点是，在本示例中，如果不更新自定义变量集 2 中的 Var1，进一步自定义或重置默认变量集中的 Var1 会导致更新自定义变量集 2 中 Var1 的默认值，从而影响与变量集相关联的所有入侵策略。

虽然在本示例中未显示，但请注意，用户定义的变量和默认变量的变量集之间的交互相同，不同之处在于重置默认变量集中的默认变量会在当前规则更新中将其值重置为由系统配置的值。

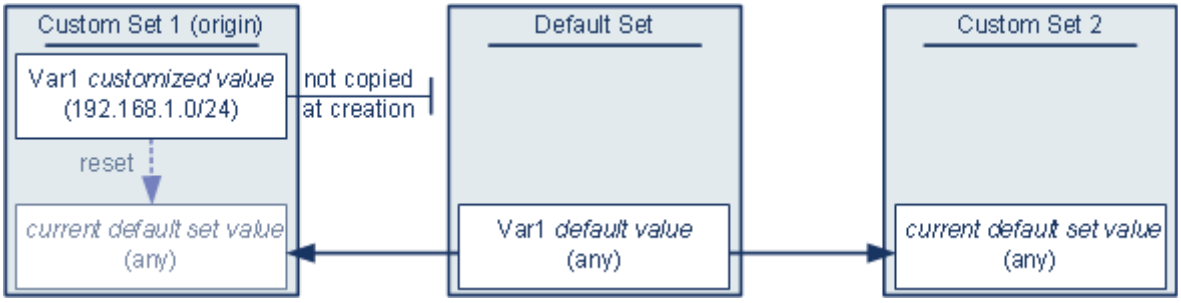
示例：将用户定义的变量到添加到自定义变量集

以下两个示例说明了将用户定义的变量添加到自定义变量集时变量集之间的交互。保存新变量时，系统会提示您选择是否将配置值用作其他变量集的默认值。在以下示例中，您选择**使用**配置值。



请注意，除了 Var1 来自自定义变量集 1 以外，本示例与以上将 Var1 添加到默认变量集的示例完全相同。将 Var1 的自定义值 192.168.1.0/24 添加到自定义变量集 1 会将该值复制到默认变量集，以作为默认值为 any 的自定义值。之后，Var1 值和交互就像之前将 Var1 添加到默认变量集一样。请记住，与前一个示例一样，进一步自定义或重置默认变量集中的 Var1 会导致更新自定义变量集 2 中 Var1 的默认值，从而影响与变量集相关联的所有入侵策略。

在下一个示例中，像前一个示例一样，将 Var1（其值为 192.168.1.0/24）添加到自定义变量集 1，但选择**不使用** Var1 的配置值作为其他变量集中的默认值。



此方法会将 Var1（其默认值为 any）添加到所有变量集。添加 Var1 后，可以在任何变量集中自定义它的值。此方法的优点是，通过最初不在默认变量集中自定义 Var1，可以降低这样的风险：在默认变量集中自定义此变量的值时，无意中更改了尚未自定义 Var1 的变量集（例如，自定义变量集 2）中的当前值。

管理变量集

许可证：保护

如果选择 Object Manager 页面 (**Configuration > ASA FirePOWER Configuration > Object Management**) 上的 **Variable Sets**，则对象管理器会列出默认变量集以及您创建的任何自定义变量集。

在全新安装的系统上，默认变量集仅由 ASA FirePOWER 模块预定义的默认变量组成。

每个变量集都包括思科提供的默认变量以及从任何变量集添加的所有自定义变量。请注意，可以编辑默认变量集，但不能重命名或删除默认变量集。

下表总结了可用于管理变量集的操作。

表 2-3　　变量集管理操作

要.....	您可以.....
显示变量集	选择 **Configuration > ASA FirePOWER Configuration > Object Management**，然后选择 **Variable Set**。
按名称过滤变量集	键入名称；当您键入时，页面会刷新以显示匹配的名称。
清除名称过滤	点击过滤器字段中的清除图标 (✖)。
添加自定义变量集	点击 **Add Variable Set**。 为方便使用，新变量集包括所有当前定义的默认和自定义变量。
编辑变量集	点击要编辑的变量集旁边的编辑图标 ( )。 **提示**　可以在变量集的行中右键单击，然后选择 **Edit**。
删除自定义变量集	点击变量集旁边的删除图标 ( )，然后点击 **Yes**。不能删除默认变量集。请注意，在删除的变量集中创建的变量不会被删除，这些变量在其他变量集中也不会受到影响。 **提示**　可以在变量集的行中右键单击，选择 **Delete**，然后点击 **Yes**。使用 Ctrl 和 Shift 键可选择多个变量集。

在配置变量集后，可以将其链接到入侵策略。

要创建或编辑变量集：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Object Management**。

系统将显示 Object Management 页面。

步骤 2　选择 **Variable Set**。

步骤 3　添加变量集或编辑现有变量集：

- 要添加变量集，请点击 **Add Variable Set**。
- 要编辑变量集，请点击变量集旁边的编辑图标 ( )。

系统显示新建或编辑变量集页面。有关添加或编辑变量集中的变量的信息，请参阅第 2-19 页上的添加和编辑变量。

管理变量

许可证：保护

可通过新建或编辑变量页面管理变量集中的变量。所有变量集的变量页面都将变量划分到 Customized Variables 和 Default Variables 页面区域。

*默认变量*是 ASA FirePOWER 模块提供的变量。可以自定义默认变量的值。不能重命名或删除默认变量，也不能更改其默认值。

自定义*变量*是以下其中一种变量：

- 自定义的默认变量

  编辑默认变量的值时，系统会将该变量从 Default Variables 区域转移到 Customized Variables 区域。由于默认变量集中的变量值决定自定义变量集中变量的默认值，因此，自定义默认变量集中的默认变量会修改所有其他变量集中该变量的默认值。

- 用户定义的变量

  您可以添加和删除自己的变量，在不同变量集中自定义这些变量的值，以及将自定义变量重置为默认值。重置用户定义的变量时，该变量保留在 Customized Variables 区域。

下表总结了可用于创建或编辑变量的操作。

表 2-4　　变量管理操作

要.....	您可以.....
显示变量页面	在变量集页面上，点击 **Add Variable Set** 创建新变量集，或者点击要编辑的变量集旁边的编辑图标 ( )。
对变量集进行命名或者描述	在 **Name** 和 **Description** 字段中输入字母数字字符串（可包含空格和特殊字符）。
添加变量	点击 **Add**。 有关详细信息，请参阅第 2-19 页上的添加和编辑变量。
编辑变量	点击要编辑的变量旁边的编辑图标 ( )。 有关详细信息，请参阅第 2-19 页上的添加和编辑变量。
将已修改变量重置为默认值	**提示**　点击已修改变量旁边的重置图标 ( )。如果重置图标呈灰色显示，表示当前值已经是默认值。

表 2-4　　变量管理操作 （续）

要.....	您可以.....
删除用户定义的自定义变量	点击变量集旁边的删除图标 ( )；如果在添加该变量后已保存变量集，点击 **Yes** 确认要删除变量。 不能删除默认变量，也不能删除入侵规则或其他变量使用的用户定义的变量。
保存对变量集的更改	点击 **Store ASA FirePOWER Changes**，然后，如果访问控制策略正在使用该变量集，请点击 **Yes** 确认要保存更改。 由于默认变量集中的当前值决定所有其他变量集中的默认值，因此，修改或重置默认变量集中的变量会更改未对该变量默认值进行自定义的那些变量集中的该变量当前值。

要查看变量集中的变量，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Object Management**。

系统将显示 Object Management 页面。

步骤 2　选择 **Variable Set**。

步骤 3　添加变量集或编辑现有变量集：

- 要添加变量集，请点击 **Add Variable Set**。
- 要编辑变量集，请点击变量集旁边的编辑图标 ( )。

系统显示新建或编辑变量集页面。

步骤 4　要添加变量或编辑现有变量：

- 要添加变量，点击 **Add**。
- 要编辑变量，点击变量旁边的编辑图标 ( )。

系统显示新建或编辑变量页面。

有关添加或编辑变量集中的变量的信息，请参阅第 2-19 页上的添加和编辑变量。

添加和编辑变量

许可证：保护

可以修改任何自定义变量集中的变量。

如果您创建自定义标准文本规则，您可能还希望添加自己的用户定义的变量，以便更准确地反映您的流量或作为快捷方式简化规则创建过程。例如，如果创建只检查“隔离区”(DMZ) 中流量的规则，可以创建名为 `$DMZ` 的变量，其值列出已暴露的服务器 IP 地址。这样，在所有为该区域编写的所有规则中都可以使用 `$DMZ` 变量。

将变量添加到变量集会将其添加到所有其他变量集。除了下述一种例外情况，变量将被添加到其他变量集作为默认值，然后可以对默认值进行自定义。

添加自定义变量集中的变量时，必须选择是否使用配置值作为默认变量集中的定制值：

- 如果**使用**配置的值（例如，192.168.0.0/16），变量添加到默认变量集时，将会使用配置值作为自定义值，且默认值为 `any`。由于默认变量集中的当前值决定在其他变量集中的默认值，因此，其他自定义变量集中的初始默认值为配置值（在本示例中为 192.168.0.0/16）。

- 如果**不使用**配置值，变量添加到默认变量集时，只会使用默认值 any，因此，其他自定义变量集中的初始默认值为 any。

有关详细信息，请参阅第 2-15 页上的了解变量集。

可在 New Variable 页面上向变量集添加变量，在 Edit Variable 页面上编辑现有变量。这两个页面的使用方法相同，唯一不同之处在于，编辑现有变量时不能更改变量名称或变量类型。

这两个页面均主要包括三个窗口：

- 可用项目，包括现有网络或端口变量、对象和网络对象组
- 要包括在变量定义中的网络或端口
- 要从变量定义中排除的网络或端口

可以创建或编辑两种类型的变量：

- *网络*变量指定网络流量中的主机的 IP 地址。请参阅第 2-22 页上的使用网络变量。
- *端口*变量指定网络流量中的 TCP 或 UDP 端口，包括这两种端口类型的值 any。请参阅第 2-23 页上的使用端口变量。

指定是否要添加网络或端口变量类型时，页面会刷新以列出可用项目。在列表上方的搜索字段可用于对列表施加约束，该列表在您键入时会更新。

可以选择并拖动项目列表中的可用项目，以包括或排除这些项目。还可以选择项目并点击 **Include** 或 **Exclude** 按钮。使用 Ctrl 和 Shift 键可选择多个项目。可以使用包含或排除项目列表下方的配置字段为网络变量指定文本 IP 地址和地址块，并为端口变量指定端口和端口范围。

要包含或排除的项目列表可以包括原义字符串和现有变量、对象和网络对象组（对于网络变量）的任意组合。

下表总结了可用于创建或编辑变量的操作。

表 2-5　　变量编辑操作

要.....	您可以.....
显示变量页面	在变量集页面上，点击 **Add** 添加新变量，或者点击现有变量旁边的编辑图标 ( )。
为变量命名	在 **Name** 字段中，键入一个唯一的字母数字字符串 （区分大小写，不能包含除下划线字符 (_) 以外的特殊字符）。 请注意，变量名称区分大小写；例如， var 和 Var 是不同的。
指定网络或端口变量	从 **Type** 下拉列表中选择 **Network** 或 **Port**。 有关可以如何使用和配置网络和端口变量的详细信息，请参阅第 2-22 页上的使用网络变量和第 2-23 页上的使用端口变量。
添加单个网络对象以供随后在可用网络列表中选择	从 **Type** 下拉列表中选择 **Network**，然后点击添加图标 ( )。有关使用对象管理器添加网络对象的信息，请参阅第 2-3 页上的使用网络对象。
添加单个端口对象以供随后在可用端口列表中选择	从 **Type** 下拉列表中选择 **Port**，然后点击添加图标 ( )。 虽然可以添加任何端口类型，但只有 TCP 和 UDP 端口（包括这两种端口类型的值 any）是有效变量值，可用端口列表仅显示使用这些值类型的变量。有关使用对象管理器添加端口对象的信息，请参阅第 2-9 页上的使用端口对象。
按名称搜索可用端口或网络项目	在可用项目列表上方的搜索字段中键入名称；当您键入时，页面会刷新以显示匹配的名称。
清除名称搜索	点击搜索字段上方的重新加载图标 ( ) 或搜索字段中的清除图标 ( )。

表 2-5　　变量编辑操作 （续）

要.....	您可以.....
区分可用项目	查找变量图标 ( )、网络对象图标 ( )、端口图标 ( ) 和对象组图标 ( ) 旁边的项目。 请注意，仅网络组可用，端口组不可用。
选择在变量定义中要包括或排除的对象	点击可用网络或端口列表中的对象；使用 Ctrl 和 Shift 键可选择多个对象。
将选定项目添加到包含或排除的网络或端口列表	拖放选定项目 或者，点击 **Include** 或 **Exclude**。 可以从可用项目列表添加网络变量、端口变量、网络对象和端口对象。还可以添加网络对象组。
将文字网络或端口添加到要包括或排除的网络或端口列表	点击以从 **Network** 或 **Port** 文字字段中移除提示符，键入网络变量的文字 IP 地址或地址块，或者键入端口变量的端口或端口范围，然后点击 **Add**。 请注意，不能输入域名或列表；要添加多个项目，请逐个添加。
添加具有值 any 的变量	对变量进行命名并选择变量类型，然后点击 **Store ASA FirePOWER Changes** 而不配置值。
从包含或排除列表删除变量或对象	点击变量旁边的删除图标 ( )。
保存新的或修改后的变量	点击 **Store ASA FirePOWER Changes**；然后，如果添加的是自定义变量集中的变量，请点击 **Yes** 以使用配置值作为其他变量集中的默认值，或者点击 **No** 以使用默认值 any。

有关详细信息，请参阅：

- 第 2-22 页上的使用网络变量
- 第 2-23 页上的使用端口变量

要添加或编辑变量，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Object Management**。

系统将显示 Object Management 页面。

步骤 2　选择 **Variable Set**。

步骤 3　添加变量集或编辑现有变量集：

- 要添加变量集，请点击 **Add Variable Set**。
- 要编辑现有变量集，请点击变量集旁边的编辑图标 ( )。

系统显示新建或编辑变量集页面。

步骤 4　要添加新变量或编辑现有变量：

- 要添加新变量，请点击 **Add**。
- 要编辑现有变量，请点击变量旁边的编辑图标 ( )。

系统显示新建或编辑变量页面。

步骤 5　如果是添加新变量：

- 在 **Name** 字段中为变量输入一个唯一名称。

  可以使用字母数字字符和下划线 (_) 字符。
- 从 **Type** 下拉列表中选择 **Network** 或 **Port** 变量类型。

步骤 6　或者，将项目从可用网络或端口列表移至包含或排除项目列表。

可以选择一个或多个项目然后执行拖放操作，或者点击 **Include** 或 **Exclude**。使用 Ctrl 和 Shift 键可选择多个项目。

提示　如果网络或端口变量的包含变量列表和排除变量列表中的地址或端口重叠，排除的地址或端口优先。

步骤 7　或者，输入一个文字值，然后点击 **Add**。

对于网络变量，可以输入单个 IP 地址或地址块。对于端口变量，可以添加单个端口或端口范围，用连字符 (-) 隔开上限和下限值。

如有需要，可重复此步骤输入多个文字值。

步骤 8　点击 **Store ASA FirePOWER Changes** 以保存变量。如果是添加自定义变量集中的新变量，有以下选项可供选择：

- 点击 **Yes** 添加使用配置值作为默认变量集中的自定义值（进而也是其他自定义变量集中的默认值）的变量。
- 点击 **No** 将变量添加为默认变量集中的默认值 `any`（进而在其他自定义变量集中也使用此默认值）。

步骤 9　完成更改后，点击 **Store ASA FirePOWER Changes** 以保存变量集，然后点击 **Yes**。

更改保存成功，与该变量集链接的所有访问控制策略均显示为过期状态。要使更改生效，必须将与该变量集链接的访问控制策略应用于入侵策略；请参阅第 4-10 页上的应用访问控制策略。

使用网络变量

许可证：保护

网络变量代表可用于已在入侵策略、入侵策略规则抑制、动态规则状态和自适应配置文件中启用的入侵规则中的 IP 地址。网络变量与网络对象和网络对象组的不同在于，网络变量特定于入侵策略和入侵规则，而网络对象和对象组则可用于在 ASA FirePOWER 模块中的不同位置（包括访问控制策略、网络变量、入侵规则、和报告等）表示 IP 地址。有关详细信息，请参阅第 2-3 页上的使用网络对象。

可在以下配置中使用网络变量来指定网络上主机的 IP 地址：

- 入侵规则

  入侵规则 **Source IPs** 和 **Destination IPs** 报头字段可用于限制仅检查来自或发往特定 IP 地址的数据包。请参阅第 23-5 页上的在入侵规则中指定 IP 地址。

- 抑制

  在特定 IP 地址或 IP 地址范围触发入侵规则或预处理器时，源或目标入侵规则抑制中的 **Network** 字段让您能够抑制入侵事件通知。请参阅第 20-23 页上的按入侵策略配置抑制。

- 动态规则状态

  源或目标动态规则状态中的 **Network** 字段让您能够检测在给定时间段内发生过多入侵规则或预处理器规则匹配的情况。请参阅第 20-25 页上的添加动态规则状态。

- 自适应配置文件

  自适应配置文件 **Networks** 字段识别网络（您希望在其中改进被动部署中的数据包分段和 TCP 流的重组）中的主机。请参阅第 18-1 页上的在被动部署中调整预处理。

在本节中所述字段中使用变量时，链接至入侵策略的变量集决定使用该入侵策略的访问控制策略处理的网络流量中的变量值。

可以将以下网络配置的任意组合添加到变量：

- 从可用网络列表中选择的网络变量、网络对象和网络对象组的任意组合

  有关使用对象管理器创建单个网络对象和成组网络对象的信息，请参阅第 2-3 页上的使用网络对象。

- 从 New Variable 或 Edit Variable 页面添加的单个网络对象（这些对象随后可添加到变量以及其他现有和将来的变量）

- 文字的、单个 IP 地址或地址块

  可以通过逐个添加来列出多个文字 IP 地址和地址块。可以单独列出 IPv4 和 IPv6 地址以及地址块，或者列出它们的任意组合。指定 IPv6 地址时，可使用 RFC 4291 中定义的任意寻址约定。

在任何变量中添加的包含网络的默认值是单词 `any`，它表示任意 IPv4 或 IPv6 地址。排除网络的默认值为 none，它表示无网络。还可以使用文字值指定地址 `::`，以指示包含网络列表中的任何 IPv6 地址，或排除列表中没有 IPv6 地址。

将网络添加到排除列表会使指定的地址和地址块无效。也就是说，可以匹配除了被排除的 IP 地址或地址块以外的所有 IP 地址。

例如，排除文字地址 `192.168.1.1` 会指定除 192.168.1.1 以外的所有 IP 地址，排除 `2001:db8:ca2e::fa4c` 会指定除 2001:db8:ca2e::fa4c 以外的所有 IP 地址。

使用文字网络或可用网络可以排除任意的网络组合。例如，排除文字值 `192.168.1.1` 和 `192.168.1.5` 会*包含*除 192.168.1.1 或 192.168.1.5 以外的所有 IP 地址。也就是说，系统将此解释为“**既不是** 192.168.1.1 **也不是** 192.168.1.5”，这就会匹配除括号中列出的 IP 地址以外的所有 IP 地址。

添加或编辑网络变量时，请注意以下几点：

- 在逻辑上，不能排除值 `any`，如果排除该值，将表示无地址。例如，不能将具有值 `any` 的变量添加到排除网络列表。
- 网络变量为指定的入侵规则和入侵策略功能识别流量。请注意，无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。
- 排除值必须解析为包含值的子集。例如，不能包含地址块 192.168.5.0/24 并排除 192.168.6.0/24。如果这样做，系统将会显示警告错误消息并标识出违规的变量，而且，当您排除包含值范围之外的值时，将无法保存变量集。

有关添加和编辑网络变量的信息，请参阅第 2-19 页上的添加和编辑变量。

使用端口变量

许可证：保护

端口变量代表可在入侵策略中启用的入侵规则的 **Source Port** 和 **Destination Port** 报头字段中使用的 TCP 和 UDP 端口。端口变量与端口对象和端口对象组的不同之处在于，端口变量特定于入侵规则。可以为除 TCP 和 UDP 以外的其他协议创建端口对象，还可以使用端口对象，包括端口变量访问控制策略、。有关详细信息，请参阅第 2-9 页上的使用端口对象。

可以在入侵规则 **Source Port** 和 **Destination Port** 报头字段中使用端口变量来限制仅检查来自或发往特定 TCP 或 UDP 端口的数据包。

在这些字段中使用变量时，链接到与访问控制规则或策略相关的入侵策略的变量集决定应用访问控制策略的网络流量中这些变量的值。

可以将以下端口配置的任意组合添加到变量：

- 从可用端口列表中选择的端口变量和端口对象的任意组合

  请注意，可用端口列表不显示端口对象组，而且不能将这些对象组添加到变量。有关使用对象管理器创建端口对象的信息，请参阅第 2-9 页上的使用端口对象。

- 从 New Variable 或 Edit Variable 页面添加的单个端口对象（这些对象随后可添加到变量以及其他现有和将来的变量）

  仅 TCP 和 UDP 端口（包括两种端口类型的值 any）是有效的变量值。如果使用新建或编辑变量页面添加不是有效变量值的有效端口对象，对象将被添加到系统，但不会显示在可用对象列表中。使用对象管理器编辑用于变量的端口对象时，只能将其值更改为有效的变量值。

- 单个文本端口值和端口范围

  必须使用破折号 (-) 隔开端口范围。带有冒号 (:) 的端口范围表示具有向后兼容性，但不能在创建的端口变量中使用冒号。

  可以通过逐个添加来列出多个文本端口值的任意组合。

添加或编辑端口变量时，请注意以下几点：

- 在任何变量中添加的包含端口的默认值是单词 any，它表示任意端口或端口范围。排除端口的默认值为 none，它表示无端口。

提示　要创建一个值为 any 的变量，请在不添加具体值的情况下命名并保存该变量。

- 在逻辑上，不能排除值 any，如果排除该值，将表示无端口。例如，将具有值 any 的变量添加到排除端口列表时，无法保存变量集。
- 将端口添加到排除列表会使指定端口和端口范围失效。也就是说，可以匹配除了被排除的端口或端口范围以外的所有端口。
- 排除值必须解析为包含值的子集。例如，不能包含端口范围 10-50 并排除端口 60。如果这样做，系统将会显示警告错误消息并标识出违规的变量，而且，当您排除包含值范围之外的值时，将无法保存变量集。

有关添加和编辑端口变量的信息，请参阅第 2-19 页上的添加和编辑变量。

重置变量

许可证：保护

在变量集新建或编辑变量页面上，可以将变量重置为默认值。下表总结了重置变量的基本原则。

表 2-6　　变量重置值

要重置的变量类型	所属变量集类型	重置后的值
default	default	规则更新值
用户定义的变量	default	any
默认变量或用户定义的变量	custom	当前默认变量集值 （已修改或未修改）

重置自定义变量集中的变量会将其重置为该变量在默认变量集中的当前值。

相反，重置或修改默认变量集中某个变量的值总是会更新所有自定义变量集中该变量的默认值。如果重置图标呈灰色显示，表示不能重置变量，这意味着该变量在该变量集中没有自定义值。除非自定义了自定义变量集中某个变量的值，否则对默认变量集中该变量的更改会更新与该变量集链接的任何入侵策略中使用的值。

注　理想做法是修改默认变量集中的某个变量，以评估这些更改如何影响使用链接自定义变量集中的该变量的任何入侵策略，尤其是在尚未定制自定义变量集中的变量值时。

当自定义值和重置值相同时，这表示以下其中一种情况属实：

- 您在自定义或默认变量集中，而且在其中添加了值为 `any` 的变量
- 您在自定义变量集中，在其中添加了具有显式值的变量，并且选择了使用配置值作为默认值

将变量集链接到入侵策略

许可证：可控性

默认情况下，ASA FirePOWER 模块会将默认变量集链接到访问控制策略中使用的所有入侵策略。应用使用入侵策略的访问控制策略时，在入侵策略中已启用的入侵规则使用链接的变量集中的变量值。

修改访问控制策略中的入侵策略使用的自定义变量集时，系统会反映该策略的状态，在 Access Control 页面上将其状态显示为过时。必须重新应用该访问控制策略，才能使变量集的更改生效。修改默认变量集时，系统会将使用入侵策略的所有访问控制策略的状态显示为过时，因此，必须重新应用所有访问控制策略才能使更改生效。

有关信息，请参阅以下各节：

- 要将除默认变量集外的其他变量集链接到访问控制规则，请参阅第 10-4 页上的配置访问控制规则以执行入侵防御中所述的步骤。
- 要将除默认变量集外的其他变量集链接到访问控制策略的默认操作，请参阅第 4-4 页上的为网络流量设置默认的处理和检查。
- 要应用访问控制策略（包括将变量集链接到入侵策略的策略），请参阅第 4-10 页上的应用访问控制策略。

了解高级变量

许可证：保护

通过高级变量，可以配置无法通过模块界面以其他方式配置的功能。 ASA FirePOWER 模块目前仅提供两个高级变量，因此您只能编辑 USER_CONF 高级变量。

USER_CONF

USER_CONF 提供一个通用工具，使您能够配置无法通过模块界面以其他方式提供的一个或多个功能。

注意事项　请**勿**使用高级变量 USER_CONF 来配置入侵策略功能，除非功能描述或支持人员指示您这样做。存在冲突或重复的配置会导致系统停止。

编辑 USER_CONF 时，可以在单行中最多输入总共 4096 个字符；达到该限制后，行会自动换行。可以包含任意数量的有效说明或行，直至达到变量的最大字符长度限制（8192 个字符）或物理限制（例如磁盘空间）。在命令指令中，可以在任何完整参数之后使用反斜杠 (\) 续行符。

重置 USER_CONF 会将其清空。

使用文件列表

许可证：恶意软件

如果使用基于网络的高级恶意软件防护 (AMP)，而且综合安全情报云错误地识别某个文件的性质，则可以使用 SHA-256 哈希值将该文件添加到*文件列表*，以便将来能够更好地检测该文件。根据文件列表的类型，可以执行以下操作：

- 要好像云已为文件分配了安全性质一样对其进行处理，请将文件添加到*白名单*。
- 要好像云已为文件分配了恶意软件性质一样对其进行处理，请将文件添加到*自定义检测列表*。

由于您手动指定这些文件的阻止行为，因此，系统将不会执行恶意软件云查找，即使这些文件被云识别为恶意软件。请注意，必须为文件策略中的某个规则配置 **Malware Cloud Lookup** 或 **Block Malware** 操作和匹配的文件类型，以计算文件的 SHA 值。有关详细信息，请参阅第 24-9 页上的使用文件规则。

默认情况下，每个文件策略中都包含系统的白名单和自定义检测列表。可以为每个策略选择不使用这两个列表中的任何一个或者都不使用。

注意事项　请**勿**在白名单中包含实际上是恶意软件的文件。系统不会阻止它们，即使云已为这些文件分配了恶意软件性质，或者已将它们添加到自定义检测列表。

每个文件列表最多可以包含 10000 个唯一的 SHA-256 值。要将文件添加到文件列表，可执行以下操作：

- 上传文件，以便系统计算并添加文件的 SHA-256 值。
- 直接输入文件的 SHA-256 值。
- 创建并上传包含多个 SHA-256 值的逗号分隔值 (CSV) 源文件。所有非重复的 SHA-256 值都将被添加到文件列表。

将文件添加到文件列表，编辑文件列表中的 SHA-256 值或删除文件列表中的 SHA-256 值时，必须重新应用使用该列表的所有访问控制策略，更改才会生效。

有关使用文件列表的详细信息，请参阅：

- 第 2-27 页上的将多个 SHA-256 值上传到文件列表
- 第 2-28 页上的将单个文件上传到文件列表
- 第 2-28 页上的将 SHA-256 值添加到文件列表
- 第 2-29 页上的修改文件列表中的文件
- 第 2-29 页上的从文件列表下载源文件

将多个 SHA-256 值上传到文件列表

许可证：恶意软件

可通过上传包含 SHA-256 值和描述的列表的逗号分隔值 (CSV) 源文件将多个 SHA-256 值添加到文件列表。系统验证内容并使用有效的 SHA-256 值填充文件列表。

源文件必须为具有 .csv 文件扩展名的简单文本文件。所有标题必须以井号 (#) 开头；标题将被视为注释，不会上传。每个条目应包含一个 SHA-256 值，后接一段描述（最多包含 256 个字母数字或特殊字符），并以 LF 或 CR+LF 换行字符结尾。系统将会忽略条目中的任何其他信息。

请注意：

- 从文件列表删除源文件也会从该文件列表删除所有相关的 SHA-256 哈希值。
- 如果成功上传源文件导致文件列表包含超过 10000 个不同的 SHA-256 值，则不能将多个文件上传到该文件列表。
- 上传时，系统会截去描述中超过 256 个字符的字符，仅保留前 256 个字符。如果描述包括逗号，必须使用转义字符 (\,)。如果未包含描述，将会改为使用源文件名。
- 如果文件列表包含 SHA-256 值，并且上传了包括该值的源文件，新上传的值不会修改现有 SHA-256 值。查看与 SHA-256 值相关的捕获的文件、文件事件或恶意软件事件时，所有威胁名称或描述都来源于单个 SHA-256 值。
- 系统不会在源文件中上传无效的 SHA-256 值。
- 如果多个上传的源文件包括相同 SHA-256 值的条目，系统将使用最新的值。
- 如果源文件包括相同 SHA-256 值的多个条目，系统将使用最后一个。
- 不能在对象管理器中直接编辑源文件。要进行更改，必须首先直接修改源文件，删除系统中的副本，然后上传修改后的源文件。有关详细信息，请参阅第 2-29 页上的从文件列表下载源文件。

要将源文件上传到文件列表，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Object Management**。

系统将显示 Object Management 页面。

步骤 2　点击 **File List**。

系统将显示 File List 部分。

步骤 3　点击要从源文件向其添加值的文件列表旁边的编辑图标 ( )。

系统将显示 File List 弹出窗口。

步骤 4　从 **Add by** 字段选择 `List of SHAs`。

弹出窗口将会更新以包括新字段。

步骤 5　或者，在 **Description** 字段中输入源文件的描述。

如果不输入描述，系统将会使用文件名。

步骤 6　点击 **Browse** 浏览到源文件，然后点击 **Upload and Add List** 添加列表。

源文件即被添加到文件列表。 SHA-256 列显示文件包含多少个 SHA-256 值。

步骤 7　点击 **Store ASA FirePOWER Changes**。

步骤 8　重新应用具有使用此文件列表的文件策略的所有访问控制策略。

应用策略后，系统不再对文件列表中的文件执行恶意软件云查找。

将单个文件上传到文件列表

许可证：恶意软件

如果想要将文件副本添加到文件列表，可以将文件上传到系统进行分析；系统计算文件的 SHA-256 值并将该文件添加到列表。系统不对用于 SHA-256 计算的文件大小强制实施任何限制。

要通过使用系统计算文件的 SHA-256 值来添加文件，请执行以下操作：

步骤 1　在对象管理器的 File List 页面上，点击要添加文件的白名单或自定义检测列表旁边的编辑图标 ( )。

系统将显示 File List 弹出窗口。

步骤 2　从 **Add by** 字段选择 **Calculate SHA**。

弹出窗口将会更新以包括新字段。

步骤 3　或者，在 **Description** 字段中输入文件的描述。

如果不输入描述，在上传时文件名将被用作描述。

步骤 4　点击 **Browse** 浏览到源文件，然后点击 **Calculate and Add SHA** 添加列表。

文件即被添加到文件列表。

步骤 5　点击 **Store ASA FirePOWER Changes**。

步骤 6　重新应用具有使用此文件列表的文件策略的所有访问控制策略。

应用策略后，系统不再对文件列表中的文件执行恶意软件云查找。

将 SHA-256 值添加到文件列表

许可证：恶意软件

可以提交文件的 SHA-256 值以将其添加到文件列表。不能添加重复的 SHA-256 值。

要通过手动输入文件的 SHA-256 值来添加文件，请执行以下操作：

步骤 1　在对象管理器的 File List 页面上，点击要添加文件的白名单或自定义检测列表旁边的编辑图标 ( )。

系统将显示 File List 弹出窗口。

步骤 2　从 **Add by** 字段选择 `Enter SHA Value`。

弹出窗口将会更新以包括新字段。

步骤 3　在 **Description** 字段中输入源文件的描述。

步骤 4　键入或粘贴文件的完整 **SHA-256** 值。系统不支持匹配部分值。

步骤 5　点击 **Add** 添加文件。

文件即被添加到文件列表。

步骤 6　点击 **Store ASA FirePOWER Changes**。

步骤 7　重新应用具有使用此文件列表的文件策略的所有访问控制策略。

应用策略后，系统不再对文件列表中的文件执行恶意软件云查找。

修改文件列表中的文件

许可证：恶意软件

可以编辑或删除文件列表中的各个 SHA-256 值。请注意，不能在对象管理器中直接编辑源文件。要进行更改，必须首先直接修改源文件，删除系统中的副本，然后上传修改后的源文件。有关详细信息，请参阅第 2-29 页上的从文件列表下载源文件。要编辑文件列表中的文件，请执行以下操作：

步骤 1　在对象管理器的 File List 页面上，点击要修改文件的白名单或自定义检测列表旁边的修改图标 ( )。

系统将显示 File List 弹出窗口。

步骤 2　点击要编辑的 SHA-256 值旁边的编辑图标 ( )。

系统将显示 Edit SHA-256 弹出窗口。

提示　也可以从列表中删除文件。点击要移除的文件旁边的删除图标 ( )。

步骤 3　更新 **SHA-256** 值或 **Description**。

步骤 4　点击**保存 (Save)**。

系统将显示 File List 弹出窗口。系统更新列表中的文件条目。

步骤 5　点击 **Store ASA FirePOWER Changes**。

步骤 6　重新应用具有使用此文件列表的文件策略的所有访问控制策略。

应用策略后，系统不再对文件列表中的文件执行恶意软件云查找。

从文件列表下载源文件

许可证：恶意软件

可以查看、下载或删除文件列表中的现有源文件条目。请注意，不能编辑已上传的源文件。必须首先删除文件列表中的源文件，再上传更新后的文件。有关上传源文件的详细信息，请参阅第 2-27 页上的将多个 SHA-256 值上传到文件列表。

与源文件相关的条目数是指不同的 SHA-256 值的数量。如果从文件列表删除某个源文件，文件列表包含的 SHA-256 条目总数将会减少等于该源文件中有效条目的数量。

要下载源文件，请执行以下操作：

步骤 1　在对象管理器的 File List 页面上，点击要下载源文件的白名单或自定义检测列表旁边的修改图标 ( )。

系统将显示 File List 弹出窗口。

步骤 2　点击要下载的源文件旁边的视图图标 ( )。

系统将显示 View SHA-256's in list 弹出窗口。

步骤 3　点击 **Download SHA List** 并按照提示保存源文件。

步骤 4　点击**关闭**。

系统将显示 File List 弹出窗口。

使用安全区域

许可证：任何环境

支持的设备：任何环境

*安全区域*是对一个或多个 ASA 接口的分组，可用于在各种策略和配置中对流量进行管理和分类。您可以在一台设备上配置多个区域。这使得能够将网络划分为可以应用各种策略的网段。您必须向安全区域分配至少一个接口，以根据该安全区域来匹配流量，并且每个接口可以仅属于一个区域。

除使用安全区域对接口进行分组以外，还可以在 ASA FirePOWER 模块 （包括访问控制策略）使用区域。例如，可以编写仅适用于特定源或目标区域的访问控制规则。

对象管理器的 Security Zones 页面列出在上配置的区域ASA FirePOWER 模块。

不能删除正在使用的安全区域。在区域中添加或移除接口后，必须将设备配置重新应用于。您还必须重新应用使用该区域的访问控制策略。

要添加安全区域，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Object Management**。

系统将显示 Object Management 页面。

步骤 2　选择 **Security Zones**。

步骤 3　点击 **Add Security Zone**。

系统将显示 Security Zones 弹出窗口。

步骤 4　在 **Name** 字段中为区域键入名称。可以使用除花括号 ({}) 和井号 (#) 以外的所有可打印标准 ASCII 字符。

步骤 5　从 **Type** 选择区域的接口类型。

创建安全区域后，不能更改其类型。

步骤 6　选择一个或多个接口。

使用 Shift 和 Ctrl 键可选择多个对象。如果尚未配置接口，可以创建空区域并在以后向其添加接口；请跳至步骤 9。

步骤 7　点击 **Add**。

所选的接口即被添加到区域，并按设备分组。

步骤 8　重复步骤 6 至 8，将其他设备上的接口添加到该区域。

步骤 9　点击 **Store ASA FirePOWER Changes**。

安全区域添加成功。

使用地理定位对象

许可证：任何环境

配置的每个地理定位对象代表系统识别为受监控网络上流量的源或目标的一个或多个国家/地区或大洲。可以使用地理定位对象，包括访问控制策略、。例如，可编写阻止流向或来自某些国家/地区的流量的访问控制规则。有关按地理位置过滤流量的信息，请参阅第 7-3 页上的按网络或地理位置控制流量。

要确保使用最新信息来过滤网络流量，思科强烈建议您定期更新地理定位数据库 (GeoDB)。有关下载和安装 GeoDB 更新的信息，请参阅第 35-17 页上的更新地理定位数据库。

不能删除正在使用的地理定位对象。此外，编辑访问控制策略中使用的地理定位对象后，必须重新应用访问控制策略以使更改生效。

要添加地理定位对象，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Object Management**。

系统将显示 Object Management 页面。

步骤 2　选择 **Geolocation**。

系统将显示 Geolocation Objects 页面。

步骤 3　点击 **Add Geolocation**。

系统将显示 Geolocation Object 弹出窗口。

步骤 4　在 **Name** 字段中为地理定位对象键入名称。可以使用除花括号 ({}) 以外的所有可打印标准 ASCII 字符。

步骤 5　选择要包括到地理定位对象中的国家/地区和大洲的相应复选框。

选择大洲会选择该大洲的所有国家/地区，以及 GeoDB 更新将来可能添加到该大洲下的所有国家/地区。取消选择大洲下的所有国家/地区会取消选择该大洲。可以选择国家/地区和大洲的任意组合。

步骤 6　点击 **Store ASA FirePOWER Changes**。

地理定位对象添加成功。

管理设备配置

在 Device Management 页面中，您可以管理 ASA FirePOWER 模块的设备和接口配置。

注意事项 如果在故障转移对中配置了 ASA， ASA FirePOWER 配置不会与辅助设备的 ASA FirePOWER 模块自动同步。在每次更改后，您必须手动将 ASA FirePOWER 配置从主设备中导出并导入至辅助设备。故障转移时，模块还会丢失无法进行故障转移的设备上的所有配置。

有关详细信息，请参阅：

- 第 3-1 页上的编辑设备配置
- 第 3-4 页上的管理 ASA FirePOWER 模块接口
- 第 3-4 页上的将更改应用于设备配置
- 第 3-5 页上的配置远程管理
- 第 3-7 页上的配置 eStreamer （在 eStreamer 服务器上）

编辑设备配置

当 Device Management 页面的 Device 选项卡适用于 ASA FirePOWER 模块时，其显示详细的设备配置和信息。它允许您对部分设备配置进行更改，例如，更改显示的模块名称修改管理设置。

有关详细信息，请参阅：

- 第 3-2 页上的编辑常规设备配置
- 第 3-2 页上的查看设备系统设置
- 第 3-3 页上的了解高级设备设置

编辑常规设备配置

许可证：任何环境

Device 选项卡的 General 部分显示模块名称，您可以更改该名称。在这里，您还可以指定设备能否将数据包传输到 ASA FirePOWER 模块。

要编辑常规设备配置，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Device Management > Device**。

系统将显示 Device 页面。

步骤 2　在 **General** 部分旁边，点击编辑图标 ( )。

系统将显示 General 弹出窗口。

步骤 3　在 **Name** 字段中，键入模块的新分配名称。除以下无效字符外，可以输入字母数字字符和特殊字符：+、（、）、{、}、#、&、\、<、>、?、‘ 和 “。

步骤 4　选择 **Transfer Packets** 复选框以允许数据包数据随事件存储在 ASA FirePOWER 模块上。清除该复选框以防止设备随事件发送数据包数据。

步骤 5　点击 **Save**。

系统保存更改。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 3-4 页上的将更改应用于设备配置。

查看设备系统设置

许可证：任何环境

Device 选项卡的 System 部分显示只读系统信息表，如下表中所述。

表 3-1　System 部分表字段

字段	说明
型号	设备的型号名称和编号。
串行	设备的机箱的序列号。
时间	设备的当前系统时间。
版本	ASA FirePOWER 模块上当前安装的软件版本。
策略	指向当前应用到 ASA FirePOWER 模块的系统策略的链接。

了解高级设备设置

Device 选项卡上的 Advanced 部分显示高级配置设置，如下表所述。

表 3-2　　Advanced 部分表字段

字段	说明
Application Bypass	模块上自动应用旁路的状态。
Bypass Threshold	自动应用旁路阈值 （以毫秒为单位）。

可以使用 Advanced 部分编辑其中任何设置。有关详细信息，请参阅：

- 第 3-3 页上的自动应用旁路
- 第 3-3 页上的编辑高级设备设置

自动应用旁路

许可证：任何环境

自动应用旁路 (AAB) 功能限制通过接口处理数据包所允许的时间，并在超过时间的情况下允许数据包绕开检测。该功能适用于任何部署；但在内联部署中最有价值。

通过网络的数据包延迟容限来平衡数据包处理时延。如果 Snort 中出现故障或设备配置不当导致流量处理时间超过指定阈值，则 AAB 会导致 Snort 在发生故障后的 10 分钟内重新启动，并生成故障排除数据，您可以分析这些数据以调查处理时间过长的原因。

如果选择该选项，则可以更改旁路阈值。默认设置为 3000 毫秒 (ms)。有效范围为 250 ms 到 60,000 ms。

注　只有在花费过量时间处理单个数据包时，才会激活 AAB。如果使用 AAB，则系统会终止所有 Snort 进程。

有关启用自动应用旁路和设置旁路阈值的详细信息，请参阅第 3-3 页上的编辑高级设备设置。

编辑高级设备设置

可以使用 Devices 选项卡的 Advanced 部分修改自动应用旁路。

要修改高级设备设置，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Device Management > Device**。

系统将显示 Device 页面。

步骤 2　在 **Advanced** 部分旁边，点击编辑图标 ( )。

系统将显示 Advanced 弹出窗口。

步骤 3　或者，如果网络对延迟敏感，请选择 **Automatic Application Bypass**。自动应用旁路在内联部署中最有用。有关详细信息，请参阅第 3-3 页上的自动应用旁路。

步骤 4　如果 Automatic Application Bypass 选项，可以在 **Bypass Threshold** 中键入旁路阈值（以毫秒 (ms) 为单位）。默认设置为 3000 ms，并且有效范围为从 250 ms 到 60,000 ms。

步骤 5　点击 **Save**。

已保存您的更改。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 3-4 页上的将更改应用于设备配置。

管理 ASA FirePOWER 模块接口

许可证：可控性、防护

编辑 ASA FirePOWER 接口时，从 ASA FirePOWER 模块只能配置接口的安全区域。有关详情，请参见第 2-30 页上的使用安全区域。

您使用 ASDM 和 CLI 配置接口。

要编辑 ASA FirePOWER 接口，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Device Management > Interfaces**。

系统将显示 Interfaces 页面。

步骤 2　在要编辑的接口旁边，点击编辑图标 ( )。

系统将显示 Edit Interface 弹出窗口。

步骤 3　从 **Security Zone** 下拉列表中，选择现有安全区域或选择 **New** 以添加新的安全区域。

步骤 4　点击 **Store ASA FirePOWER Changes**。

系统配置安全区域。请注意，应用设备配置后，更改才会生效；有关详细信息，请参阅第 3-4 页上的将更改应用于设备配置。

将更改应用于设备配置

许可证：任何环境

在对设备、的 ASA FirePOWER 配置进行更改后，必须应用更改，然后更改才会在整个模块中生效。请注意，设备必须有未应用的更改，否则此选项保持禁用。

请注意，如果您编辑接口并重新应用设备策略， Snort 重启设备上的所有接口实例，而不仅仅重启您编辑的那些实例。

要将更改应用到设备，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Device Management > Device** or **Configuration > ASA FirePOWER Configuration > Device Management > Interfaces**。

系统将显示 Device Management 页面。

步骤 2　点击 **Apply ASA FirePOWER Changes**。

步骤 3　出现提示时，点击 **Apply**。

系统将应用设备更改。

提示　或者，从 Apply Device Changes 对话框中，点击 **View Changes**。在新窗口中显示 Device Management Revision Comparison Report 页面。有关详细信息，请参阅第 3-5 页上的使用设备管理修订比较报告。

步骤 4　点击 **OK**。

将返回到 Device Management 页面。

使用设备管理修订比较报告

许可证：任何环境

通过设备管理比较报告，可以先查看已对设备进行的更改，然后再应用这些更改。报告显示当前设备配置和建议设备配置之间的全部差异。可借此机会发现任何潜在的配置错误。

要在应用设备更改之前对其进行比较，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Device Management > Device** or **Configuration > ASA FirePOWER Configuration > Device Management > Interfaces**。

系统将显示 Device Management 页面。

步骤 2　点击 **Apply Changes**。

系统将显示 Apply Device Changes 弹出窗口。请注意，设备必须有未应用的更改，否则 Apply Changes 图标保持禁用状态。

步骤 3　点击 **View Changes**。

在新窗口中显示 Device Management Revision Comparison Report 页面。

步骤 4　点击 **Previous** 和 **Next** 以滚动浏览当前设备配置和建议设备配置之间的差异。

步骤 5　或者，点击 **Comparison Report** 以生成报告的 PDF 版本。

配置远程管理

许可证：任何环境

必须先在两个 FireSIGHT 系统设备之间设置双向、 SSL 加密的通信信道，然后才能对两台设备进行相互管理。设备使用信道共享配置和事件信息。高可用性对等体也使用该信道，默认情况下，该信道在端口 8305/tcp 上。

必须在将受管理的设备上（即在要使用防御中心管理的设备上）配置远程管理。配置远程管理后，可以使用管理设备的网络界面将受管设备添加到部署中。

注　在建立远程管理并向防御中心注册 具备 FirePOWER 服务的 Cisco ASA 防火墙之后，必须从防御中心而不是 ASDM 管理 ASA FirePOWER 模块。

要启用两台设备之间的通信，必须提供设备相互识别的方法。 FireSIGHT 系统在允许通信时使用三个条件：

- 尝试建立通信时所使用的设备的主机名或 IP 地址

  在 NAT 环境中，即使另一设备没有可路由地址，在配置远程管理或添加受管设备时也必须提供主机名或 IP 地址。

- 长度多达 37 个字符的用于识别连接的自生成字母数字注册密钥
- 可帮助 FireSIGHT 系统在 NAT 环境中建立通信的可选唯一字母数字 NAT ID

  该 NAT ID **必须**在用于注册受管设备的所有 NAT ID 中唯一。

将受管设备注册到防御中心时，选择的访问控制策略即应用到该设备。但是，如果不对您选择的访问控制策略中使用的功能所需的设备启用许可证，访问控制策略应用会失败。

要配置本地设备的远程管理，请执行以下操作：

访问： 管理员

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > Configuration > Registration**。

系统将显示 Remote Management 页面。

步骤 2　点击 **Add Manager**。

系统将显示 Add Remote Management 页面。

步骤 3　在 **Management Host** 字段中，键入要用于管理此设备的设备的 IP 地址或主机名。

主机名是完全限定域名或通过本地 DNS 解析为有效 IP 地址的名称。

在 NAT 环境中，如果计划在添加受管设备时指定 IP 地址或主机名，则无需在此处进行指定。在这种情况下，FireSIGHT 系统使用后来将提供的 NAT ID 识别受管 ASA FirePOWER 模块界面上的远程管理器。

注意事项　如果网络使用 DHCP 来分配 IP 地址，请使用主机名而不是 IP 地址。

步骤 4　在 **Registration Key** 字段中，键入要用于设置设备之间的通信的注册密钥。

步骤 5　对于 NAT 环境，请在 **Unique NAT ID** 字段中，键入要用于设置设备之间的通信的**唯一**字母数字 NAT ID。

步骤 6　点击 **Save**。

在设备确认其是否可以相互通信后，会显示 Pending Registration 状态。

步骤 7　使用管理设备的网络用户界面将此设备添加到部署中。

注　启用设备的远程管理时，在使用 NAT 的一些高可用性部署中，可能还需要以管理员身份添加辅助防御中心。有关详细信息，请与技术支持部门联系。

编辑远程管理

许可证：任何环境

使用以下过程编辑管理设备的主机名或 IP 地址。也可以更改管理设备的显示名称，该名称仅在 FireSIGHT 系统环境的上下文内使用。尽管可以使用主机名作为设备的显示名称，但是输入其他显示名称不会更改主机名。

要编辑远程管理，请执行以下操作：

访问： 管理员

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > Configuration > Registration**。

系统将显示 Remote Management 页面。

步骤 2　点击要为其编辑远程管理设置的管理器旁边的编辑图标 ( )。

系统将显示 Edit Remote Management 页面。

步骤 3　在 **Name** 字段中，更改管理设备的显示名称。

步骤 4　在 **Host** 字段中，更改管理设备的 IP 地址或主机名。

主机名是完全限定域名或通过本地 DNS 解析为有效 IP 地址的名称。

步骤 5　点击 **Save**。

已保存您的更改。

配置 eStreamer （在 eStreamer 服务器上）

许可证：FireSIGHT + 保护

在您想要用作 eStreamer 服务器的设备可以开始以流的形式向外部客户端发送 eStreamer 事件之前，必须配置用于向客户端发送事件的 eStreamer 服务器，提供关于客户端的信息，并要在生成建立通信时使用的身份验证凭据集。

配置 eStreamer 事件类型

可以控制 eStreamer 服务器能够向客户端传输其所请求的事件类型。

受管设备或防御中心上的可用事件类型有：

- 入侵事件
- 入侵事件数据包数据
- 入侵事件额外数据

要配置 eStreamer 传输的事件类型，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > Configuration > Registration**。

系统将显示 Registration 页面。

步骤 2　选择 **eStreamer** 选项卡。

系统将显示 eStreamer 页面。

步骤 3　在 **eStreamer Event Configuration** 下，选择想要 eStreamer 转发至请求客户端的事件类型旁的复选框。

在受管设备或防御中心上，可选择以下任何或全部事件：

- **Intrusion Events**，以传输入侵事件。
- **Intrusion Event Packet Data**，以传输与入侵事件关联的数据包。
- **Intrusion Event Extra Data**，以传输与入侵事件关联的额外数据，如通过 HTTP 代理或负载平衡器连接至网络服务器的客户端的源 IP 地址。

注　请注意，这可控制 eStreamer 服务器可传输的事件。您的客户端仍必须在发送至 eStreamer 服务器的请求消息中，特别请求您想要其接收的事件类型。有关详细信息，请参阅《*FireSIGHT 系统* eStreamer *集成指南*》。

步骤 4　点击 **Save**。

您的设置将得以保存，收到请求时，您选择的事件将转发至 eStreamer 客户端。

为 eStreamer 客户端添加身份验证

只有先从 eStreamer 页面将客户端添加至 eStreamer 服务器的对等数据库，然后 eStreamer 才能向客户端发送 eStreamer 事件。还必须将 eStreamer 服务器生成的身份验证证书复制至客户端。

要添加 eStreamer 客户端，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > Configuration > Registration**。

系统将显示 Registration 页面。

步骤 2　选择 **eStreamer** 选项卡。

系统将显示 eStreamer 页面。

步骤 3　点击 **Create Client**。

系统将显示 Create Client 页面。

步骤 4　在 **Hostname** 字段中，输入运行 eStreamer 客户端的主机的主机名称或 IP 地址。

注　如果使用主机名称，eStreamer 服务器**必须**能够将主机名称解析为 IP 地址。如果尚未配置 DNS 解析，应先配置解析或使用 IP 地址。

步骤 5　如果想要对证书文件进行加密，请在 **Password** 字段中输入密码。

步骤 6　点击 **Save**。

eStreamer 服务器现在会允许主机访问 eStreamer 服务器上的 8302 端口，并将创建在客户端-服务器身份验证过程中使用的身份验证证书。系统再次显示 eStreamer 页面，新的客户端将在 **Hostname** 下列出。

步骤 7　点击客户端主机名称旁的下载图标 ( )，以下载证书文件。

步骤 8　将证书文件保存至客户端用于 SSL 身份验证的适当目录。

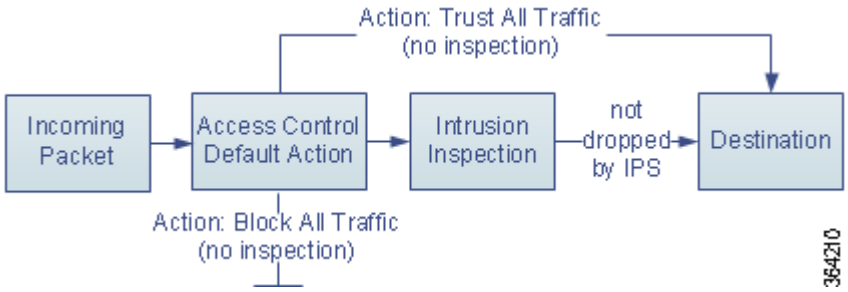
客户端现在可以连接至 eStreamer 服务器。无需重新启动 eStreamer 服务。

提示 要撤消客户端的访问权限，请点击想要移除的主机旁的删除图标 ( )。请注意，不需要重新启动 eStreamer 服务，访问权限将立即撤消。

开始使用访问控制策略

*访问控制策略*确定系统如何处理网络上的流量。每台 ASA FirePOWER 模块都可能有一条当前应用的策略。

最简单的访问控制策略使用其*默认操作*处理所有流量。您可以将此默认操作设置为阻止或信任所有流量，而无需进一步检查，也可以将其设置为检查流量是否存在入侵。



请注意，只有内联部署的 ASA FirePOWER 模块才能影响流量的流动。如将配置为阻止或修改流量的访问控制策略应用于被动部署的设备，可能会产生意外的结果。在某些情况下，系统会阻止您将内联配置应用于被动部署的 ASA FirePOWER 模块。

本章说明如何创建和应用简单的访问控制策略。它还包含有与管理访问控制策略有关的基本信息：编辑、更新、比较等。有关详细信息，请参阅：

更复杂的访问控制策略可以基于安全情报数据将流量列入黑名单，以及使用*访问控制规则*来对网络流量日志记录和处理进行精细控制。这些规则可能很简单，也可能很复杂，使用多个条件匹配和检查流量。高级访问控制策略选项控制预处理、性能和其他通用首选项。

在您创建基本的访问控制策略后，请参阅以下章节了解有关根据您的部署对其进行定制的详细信息：

- 第 5-1 页上的使用安全情报 IP 地址声誉设置黑名单说明了如何根据最新声誉情报立即将连接列入黑名单（加以阻止）。
- 第 11-1 页上的了解网络分析和入侵策略说明了作为系统的入侵检测与防御功能的一部分，网络分析和入侵策略如何预处理和检查数据包。
- 第 6-1 页上的使用访问控制规则调整流量说明了访问控制规则如何提供跨多台 ASA FirePOWER 模块处理网络流量的精细方法。
- 第 10-1 页上的使用入侵和文件策略控制流量说明了入侵和文件策略如何通过检测和选择性阻止入侵、受禁文件和恶意软件，在允许流量流向其目标之前提供最后一道防线。

访问控制的许可证和角色要求

虽然不管您的 ASA FirePOWER 模块上的许可证如何，您均可创建访问控制策略，但许多功能要求您在应用策略之前，先启用适当的许可证。

有关详细信息，请参阅第 4-2 页上的访问控制和型号要求。

访问控制和型号要求

虽然不管您的 ASA FirePOWER 模块上的许可证如何，您均可创建访问控制策略，但访问控制的某些方面要求您在应用策略之前，先启用特定许可功能。

警告图标和确认对话框会指出您的部署不支持的功能。有关详细信息，参阅第 4-12 页上的对访问控制策略和规则进行故障排除。

下表说明了应用访问控制策略的许可证要求。

表 4-1　　访问控证和型号要求

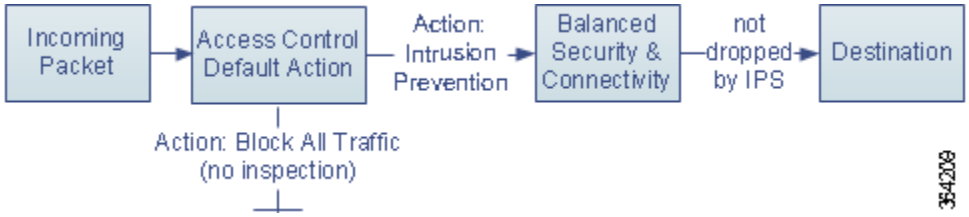
要应用以下访问控制策略...	许可证
基于区域、网络或端口执行访问控制 使用文本 URL 和 URL 对象执行 URL 过滤	任何
使用地理位置数据执行访问控制 （源或目标国家/地区或大陆）	任何
执行入侵检测与防御、文件控制或者安全情报过滤	保护
执行高级恶意软件防护，即基于网络的恶意软件检测与阻止	恶意软件
执行用户或应用程序控制	可控性
使用类别和信誉数据执行 URL 过滤	URL 过滤

创建基本的访问控制策略

许可证：任何

创建新的访问控制策略时，您必须为其提供唯一名称，并指定默认操作。此时，默认操作确定 ASA FirePOWER 模块如何处理所有流量；您稍后将会添加影响流量的其他配置。

当您创建新的策略时，您可以将默认操作设置为阻止所有流量而无需进一步检查，或检查流量是否存在入侵，如下图所示。



提示　当您首次创建访问控制策略时，无法选择信任流量作为默认操作。如果您想要默认信任所有流量，请在创建策略后更改默认操作。

使用 Access Control Policy 页面 (**Policies > Access Control**) 创建新的访问控制策略并管理现有访问控制策略。

或者，您可以使用和修改系统提供的名为 Default Trust All Traffic 的初始策略。

要创建访问控制策略，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

提示　您还可以从此 ASA FirePOWER 模块复制现有策略，或从另一 ASA FirePOWER 模块导入策略。要复制策略，请点击复制图标 ( )。要导入策略，请参阅第 B-1 页上的导入和导出配置。

步骤 2　点击 **New Policy**。

系统将显示 New Access Control Policy 弹出窗口。

步骤 3　在 **Name** 和 **Description** 中为策略提供唯一名称和描述（后者为可选项）。

可以使用所有的可打印字符，包括空格和特殊字符，井号 (#)、分号 (;) 或大括号 ({}) 除外。名称必须包含至少一个非空格字符。

步骤 4　指定初始**默认操作**：

- **Block all traffic** 通过 **Access Control: Block All Traffic** 默认操作创建策略。
- **Intrusion Prevention** 通过 **Intrusion Prevention: Balanced Security and Connectivity** 默认操作创建策略。

有关如何选择初始默认操作以及稍后如何对其进行更改的指导，请参阅第 4-4 页上的为网络流量设置默认的处理和检查。

步骤 5　点击 **Store ASA FirePOWER Changes**。

系统将显示访问控制策略编辑器。有关如何配置新策略的信息，请参阅第 4-7 页上的编辑访问控制策略。请注意，策略在应用后才会生效；请参阅第 4-10 页上的应用访问控制策略。

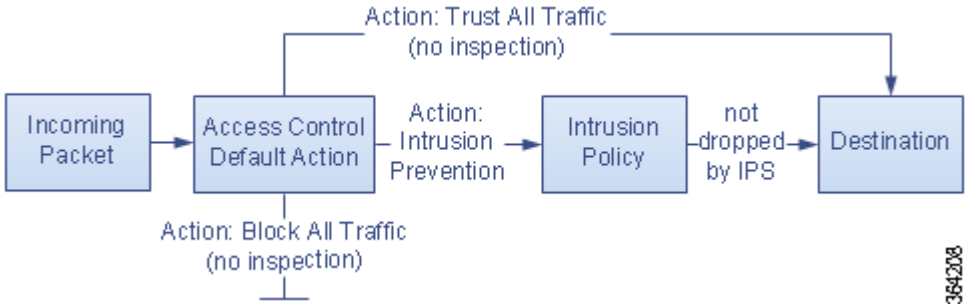
为网络流量设置默认的处理和检查

许可证：任何

当您创建访问控制策略时，必须选择默认操作。访问控制策略的默认操作确定系统如何处理以下流量：

- 未被安全情报列入黑名单
- 与策略中的所有规则均不匹配（“监控”规则除外，这些规则会匹配和记录流量，但不处理或检查流量）。

因此，当您应用不包含任何访问控制规则或安全情报配置的访问控制策略时，默认操作确定如何处理您网络上的*所有*流量。您可以阻止或信任所有流量，而无需进一步检查，或检查流量是否存在入侵。您拥有的选项如下图所示。

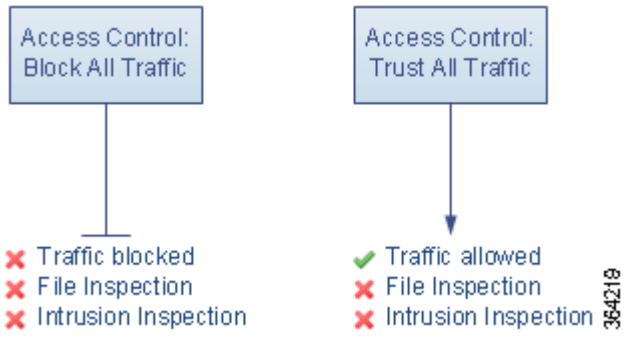


下表描述了不同的默认操作如何处理流量，并列出了您可以对每个默认操作处理的流量执行的检查类型。请注意，您**不能**对默认操作处理的流量执行文件或恶意软件检查。有关详细信息，请参阅第 10-1 页上的使用入侵和文件策略控制流量。

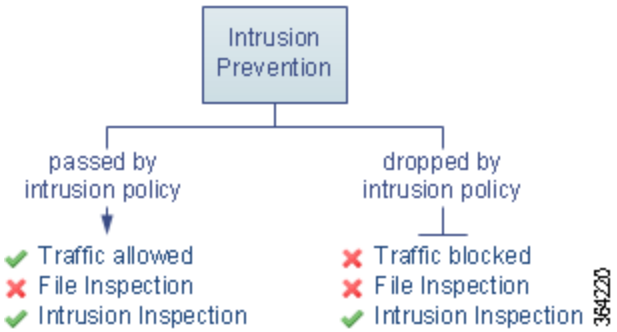
表 4-2　　访问控制策略的默认操作

默认操作	对流量的影响	检查类型和策略
访问控制：阻止所有流量	阻止，无需进一步检查	无
访问控制：信任所有流量	信任（允许流向其最终目标，而无需进一步检查）	无
入侵防御	允许，前提是其由指定的入侵策略传递（需要保护许可证）	入侵，使用指定入侵策略和关联变量集

下图说明了 **Block All Traffic** 和 **Trust All Traffic** 的默认操作。



下图说明了 **Intrusion Prevention** 默认操作。



当您首次创建访问控制策略时，默认操作处理的日志记录连接会被默认禁用。如果您选择执行入侵检查的默认操作，系统会自动将默认入侵变量集与您选择的入侵策略相关联。创建该策略后，您可以更改这些选项中的任一选项，也可以更改默认操作本身。

要更改访问控制策略的默认操作和相关选项，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要配置的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Default Action**。

- 要阻止所有流量，请选择 **Access Control: Block All Traffic**。
- 要信任所有流量，请选择 **Access Control: Trust All Traffic**。
- 要同时使用入侵策略检查所有流量，请选择全部以标签 **Intrusion Prevention** 开头的入侵策略。记住，入侵策略可以阻止流量。

注意事项　请勿使用 `Experimental Policy 1`，除非思科代表指示这样做。思科使用该策略进行测试。

步骤 4　如果您选择 **Intrusion Prevention** 默认操作，请点击变量图标 ( )，以更改与您选择的入侵策略相关联的变量集。

在显示的弹出窗口中，选择新变量集，并点击 **OK**。通过点击编辑图标 ( ) 也可在新窗口中编辑选定的变量集。如果您未更改变量集，系统会使用默认的变量集。有关详细信息，请参阅第 2-13 页上的使用变量集。

步骤 5　点击日志记录图标 ( )，以更改默认操作处理的连接的日志记录选项。

您可以在匹配连接和结束时，对其进行记录。请注意，系统无法记录受阻流量的结束。您可以将连接记录至 ASA FirePOWER 模块事件查看器、外部系统日志 (syslog) 或 SNMP 陷阱服务器。有关详细信息，请参阅第 25-10 页上的记录访问控制默认操作处理的连接。

管理访问控制策略

许可证：任何

在 Access Control Policy 页面上 (**Configuration > ASA FirePOWER Configuration > Policies > Access Control**)，您可以查看自己的当前自定义访问控制策略，以及有关是否应用策略的信息。

除了您创建的自定义策略，系统会提供您可以编辑和使用的自定义策略 Default Allow All Traffic。

Access Control Policy 页面上的选项可供您采取下表中的操作。

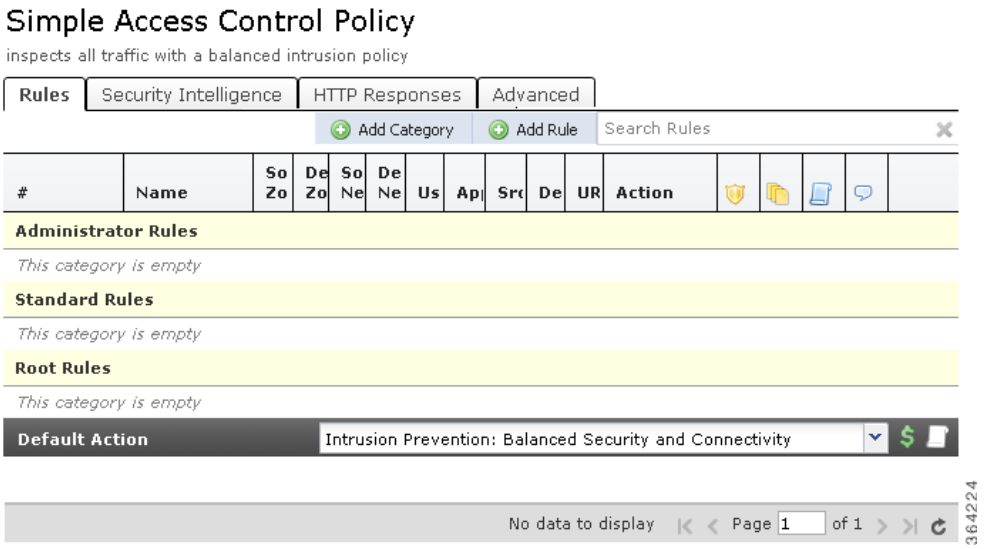
表 4-3　　访问控制策略管理操作

要.....	您可以.....	请参阅.....
创建新的访问控制策略	点击 **New Policy**。	第 4-3 页上的创建基本的访问控制策略
编辑现有访问控制策略	点击编辑图标 ( )。	第 4-7 页上的编辑访问控制策略
将访问控制策略重新应用	点击应用图标 ( )。	第 4-10 页上的应用访问控制策略
导出访问控制策略，以便在另一 ASA FirePOWER 模块上导入	点击导出图标 ( )	第 B-1 页上的导出配置
查看列出访问控制策略中的当前配置设置的 PDF 报告	点击报告图标 ( )。	第 4-15 页上的生成当前访问控制设置的报告
比较访问控制策略	点击 **Compare Policies**。	第 4-16 页上的比较访问控制策略
删除访问控制策略	点击删除图标 ( )，然后确认您想要删除策略。您无法删除已应用的访问控制策略，或目前正在应用的策略。	

编辑访问控制策略

许可证：任何

当您首次创建新的访问控制策略时，系统将显示访问控制策略编辑器，显示的焦点是 Rules 选项卡。下图展示新创建的策略。由于新策略尚无规则或其他配置，因此，默认操作可以处理*所有*流量。在这种情况下，默认操作会在允许流量流向其最终目标之前，先使用系统提供的平衡式安全性和连接性入侵策略检查流量。



使用访问控制策略编辑器添加与组织规则等。以下列表提供了有关您可以更改的策略配置的信息。

名称和描述

要更改策略的名称和描述，请点击适当的字段，并键入新名称或描述。

安全情报

安全情报是抵御恶意互联网内容的第一道防线。该功能可供您根据最新声誉情报立即将连接列入黑名单（加以阻止）。要确保对重要资源的持续访问，您可以使用自定义白名单覆盖黑名单。此流量过滤发生在任何基于策略的任何其他检查、分析或流量处理**之前**，包括规则和默认操作。有关详细信息，请参阅第 5-1 页上的使用安全情报 IP 地址声誉设置黑名单。

规则

规则提供了一种精细的网络流量处理方法。系统已对访问控制策略中的规则进行编号，从 1 开始。系统会用升序规则编号按从上到下顺序将流量与访问控制规则相匹配。

在大多数情况下，系统会按照其*所有*条件均与流量相匹配的*第一条*访问控制规则处理网络流量。这些条件包括安全区域、网络或地理位置、端口、应用、请求的 URL 或用户。条件可能很简单，也可能很复杂；它们的使用通常取决于某些许可证。

使用 Rules 选项卡可以添加、启用、禁用、过滤和管理规则以及对规则进行分类。有关详细信息，请参阅第 6-1 页上的使用访问控制规则调整流量。

默认操作

默认操作确定系统如何处理未被安全情报列入黑名单且与任何访问控制规则均不匹配的流量。通过使用默认操作，您可以阻止或信任所有流量，而无需对其进一步检查，或检查流量是否存入侵。您还可以启用或禁用默认操作处理的连接的记录。

有关详细信息，请参阅第 4-4 页上的为网络流量设置默认的处理和检查和第 25-8 页上的根据访问控制处理记录连接。

HTTP 响应

您可以指定系统阻止用户的网站请求时用户在浏览器中看到的内容 - 显示系统提供的一般响应页面，或输入自定义 HTML。您还可以显示一个页面，该页面会警告用户，但允许他们点击按钮来继续，或者刷新页面来加载原来请求的站点。有关详细信息，请参阅第 8-12 页上的显示受阻 URL 的自定义网页。

高级访问控制选项

高级访问控制策略设置通常只需要进行很小的修改或不需要修改。默认设置适用于大多数的部署。您可以修改的高级设置包括：

- 对于您的用户请求的每个 URL，您在 ASA FirePOWER 模块数据库中存储的字符数量；请参阅第 25-11 页上的记录在连接中检测到的 URL
- 用户绕过初始阻止后，您重新阻止网站前的时长；请参阅第 8-11 页上的为受阻网站设置用户绕过超时
- 允许您根据网络区域定制许多预处理选项并设置默认入侵检查行为的网络分析和入侵策略设置；请参阅第 13-1 页上的自定义流量预处理
- 可全局性应用于您在其中应用访问控制策略的所有网络区域和高级传输和网络预处理器设置；请参阅第 17-1 页上的配置高级传输/网络设置
- 自适应配置文件，用于根据您网络的主机操作系统在被动部署中提升数据包分片和 TCP 流的重组；请参阅第 18-1 页上的在被动部署中调整预处理
- 入侵检查、文件控制、文件存储和高级恶意软件防护的性能选项；请参阅第 10-5 页上的调整入侵防御性能和第 10-15 页上的调整文件和恶意软件检测性能和存储

当您编辑访问控制策略时，会有一条消息指明您有未保存的更改。要保留更改，您必须在退出策略编辑器前保存策略。如果您未保存更改就尝试退出策略编辑器，系统会提醒您有未保存的更改；您可以放弃更改并退出策略，或者返回策略编辑器。

为保护您会话的隐私，在策略编辑器上不执行操作过 60 分钟后，系统将丢弃对您策略做出的更改，您将返回 Access Control Policy 页面。无活动时间的前 30 分钟过后，屏幕上将会显示一条消息，并会定期更新以提供更改被放弃前的剩余分钟数。在页面上进行任何操作都会取消定时器。

要编辑访问控制策略：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要配置的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　编辑您的策略。采取以上概述的任何操作。

步骤 4　保存或丢弃您的配置：

- 要保存您的更改并继续编辑，请点击 **Store ASA FirePOWER Changes**。
- 要保存您的更改并应用您的策略，请点击 **Apply ASA FirePOWER Changes**。请参阅第 4-10 页上的应用访问控制策略。
- 要放弃更改，请点击 **Cancel**；如果出现提示，点击 **OK**。

了解过期策略警告

许可证：任何

在 Access Control Policy 页面上 (**Configuration > ASA FirePOWER Configuration > Policies > Access Control**)，过期策略以红色状态文本标记

在几乎所有的情况下，每当更改访问控制策略时，均必须重新应用该策略，才能使更改生效。如果访问控制策略调用其他策略或依赖其他配置，对那些策略或配置进行更改也需要您重新应用访问控制策略（或者，对于入侵策略更改，您可以只重新应用入侵策略）。

需要重新应用策略的配置更改包括：

- 修改访问控制策略本身：对访问控制规则、默认操作、安全情报过滤、包括 NAP 规则在内的高级选项等等做出的任何更改。
- 更改访问控制策略调用的任何入侵和文件策略：网络分析策略、入侵策略以及文件策略。
- 更改访问控制策略或其调用的策略中使用的任何可重复使用的对象或配置：网络、端口、URL 和地理位置对象；安全情报列表和源；应用过滤器或检测器；入侵策略变量集；文件列表；安全区域等。
- 更新系统软件、入侵规则或漏洞数据库 (VDB)。

切记，您可以在 ASA FirePOWER 模块接口中的多个位置更改这些配置中的某些配置。例如，您可以使用对象管理器修改安全区域 (**Configuration > ASA FirePOWER Configuration > Object Management**)。

请注意，以下更新不需要重新应用策略：

- 对 URL 过滤数据的自动更新
- 计划的地理位置数据库 (GeoDB) 更新

要确定访问控制或入侵策略为何过期，请使用比较查看器。

要确定访问控制策略为何过期：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。过期策略以红色状态文本标记，指明 ASA FirePOWER 模块需要策略更新。

步骤 2　点击过期策略的策略状态。

系统将显示包含详细信息的 Apply Access Control Policy 弹出窗口。

步骤 3　点击您感兴趣的已更改部分旁的 **Out-of-date**。

策略比较报告将会在新的窗口中显示。有关详细信息，请参阅第 4-16 页上的比较访问控制策略和第 19-8 页上的比较两个入侵策略或版本。

步骤 4　或者，重新应用策略。

请参阅下一节，应用访问控制策略。

应用访问控制策略

许可证：任何

更改访问控制策略后，您必须将策略应用，以便在 ASA FirePOWER 模块监控的网络上实施更改。虽然您可以应用访问控制策略及其关联入侵策略的任何组合，但应用访问控制策略会自动应用所有关联的、网络分析文件策略。您无法独立应用这些策略。

注意事项　在特殊情况下，应用访问控制策略可能会导致流量和处理的短暂暂停，而且还可能会导致一些数据包在未经检查的情况下通过。应用应用访问控制策略可能最多需要五分钟时间。为最大限度地减少不变之处，请在更改窗口内应用访问控制策略。

当 Snort® 进程重新启动时，会出现流量中断，例如，在以下情况下，进程将重新启动：在 ASA FirePOWER 模块升级后您将包含新版本 Snort，在包含共享对象规则的规则导入后首次应用策略时，以及在某些情况下，在您安装 VDB 更新时。

请注意，只有内联部署的设备才能影响流量的流动。如将配置为阻止或修改流量的访问控制策略应用于被动部署，则可能会产生意外的结果。例如，因为受阻连接在被动部署中实际上不会被阻止，系统可能为每条受阻连接报告多个连接开始事件。

应用访问控制策略时，另请记住以下要点：

- 部分功能需要特定许可证系统的最低版本。有关详细信息，请参阅第 4-2 页上的访问控制和型号要求，以及您正在运行的系统版本的版本说明。如果访问控制策略需要许可证通过最近应用的设备配置启用，系统会将访问控制策略应用排入队列，直到设备配置完成应用。
- 当您应用访问控制策略时，系统会一起评估所有规则，并创建扩展的条件集，供于评估网络流量。可能出现一个弹出窗口，警告您已超过。您在整个访问控制策略内只能选择三个入侵策略。有关详细信息，请参阅第 4-13 页上的简化规则以便提高性能。
- 导入入侵规则更新时，您可以在导入完成后自动重新应用访问控制和入侵策略。这样，您就可使用最新入侵规则与高级设置，以及预处理器规则与预处理器设置。如果您允许规则更新修改系统提供的基本策略，此功能特别有用。请注意，规则更新还可以修改您的访问控制策略中的高级预处理和性能选项的默认值。有关详细信息，请参阅第 35-8 页上的导入规则更新和本地规则文件。

有关详细信息，请参阅以下各节：

- 第 4-10 页上的应用完整的策略说明了如何使用快速应用选项应用访问控制策略以及所有关联的网络分析、入侵文件策略。
- 第 4-11 页上的应用选定的策略配置说明了如何应用特定访问控制策略配置，包括个别入侵策略。

应用完整的策略

许可证：任何

您可以随时将访问控制策略应用。应用访问控制策略也会应用不同于目前运行策略的任何关联策略：

- 网络分析策略
- 入侵策略
- 文件策略

弹出窗口将会允许您以单一的快速应用操作的形式同时应用所有的策略。使用快速应用选项时，将不应用未更改的策略。

要快速应用完整的访问控制策略：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要应用的策略旁的应用图标 ( )。

系统将显示 Apply Access Control Policy 弹出窗口。

或者，在编辑策略时，您可以点击 **Apply ASA FirePOWER Changes**；请参阅第 4-7 页上的编辑访问控制策略。

步骤 3　点击 **Apply All**。

策略应用任务将会排入队列。点击 **OK** 返回 Access Control Policy 页面。您可以在 Task Status 页面 (**Monitoring > ASA FirePOWER Monitoring > Task Status**) 上监控策略应用任务的进度。

应用选定的策略配置

许可证：任何

可以使用详细的策略应用页面将更改应用于访问控制策略和任何关联的入侵策略。此详细页面，用一列列出了关联入侵策略。您均可指定是逐一还是组合向访问控制策略和/或关联的入侵策略应用更改。

在以下的任一情况下，必须同时应用访问控制策略和关联的入侵策略：

- 首次将访问控制策略应用时
- 当入侵策略是新添加至访问控制策略时

在这两种情况下，访问控制策略和入侵策略的状态都会链接，即必须同时应用或同时不应用。

请注意，无论您应用的入侵策略如何，应用访问控制策略均会自动应用所有关联的网络分析和文件策略，这些策略不同于。您无法独立应用这些策略。

访问控制策略列

Access Control Policy 列提供了指示是否应用访问控制策略的复选框。

提示　尽管可以在应用任务仍处于任务队列，即应用任务尚未完成时重新应用策略，但是这样做没有任何的好处。

状态消息会指示策略目前是最新的，还是已过期。当策略已过期时，您可以在方便地显示该策略与当前运行策略的比较。比较不会包含访问控制策略关联的入侵策略的差异。

入侵策略列

Intrusion Policies 列提供的一个或多个复选框用于指明是否将与访问控制策略关联的入侵策略应用。单个灰色的复选框指示所有关联的入侵策略与当前运行的策略一致，在这种情况下，复选框会被清除且无法选取。无法应用未改变的入侵策略，仅发生改变的入侵策略会被列出，这些策略可以单独选择。当同一个入侵策略与策略中的多个规则关联时，入侵策略仅列出一次。

入侵策略的复选框会被选取，当访问控制策略和入侵策略必须同时应用时，如上所述，在以下的任一情况下，复选框会变灰且无法更改：

- 首次将访问控制策略应用时
- 当入侵策略是新添加至访问控制策略时

状态消息会指示入侵策略目前是最新的，还是已过期。如果某个入侵策略与设备上当前运行的入侵策略不同，则该入侵策略即为过期。设备上的一致入侵策略是最新的。当策略已过期时，您可以方便地显示该策略与当前运行策略的比较。

要应用选定的访问控制策略配置：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要应用的策略旁的应用图标 ( )。

系统将显示 Apply Access Control Policy 弹出窗口。

或者，在编辑策略时，您可以点击 **Apply ASA FirePOWER Changes**；请参阅第 4-7 页上的编辑访问控制策略。

步骤 3　点击 **Details**。

系统将显示包含详细信息的 Apply Access Control Policy 弹出窗口。请注意，您还可从 Access Control Policy 页面 (**Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**) 打开弹出窗口，只需点击策略 **Status** 列中的过期消息。

步骤 4　选择或清除访问控制策略复选框，指定是否将访问控制策略应用。

步骤 5　选择或清除入侵策略复选框，指定是否将入侵策略应用。

步骤 6　点击 **Apply Selected Configurations**。

策略应用任务将会排入队列。点击 **OK** 返回 Access Control Policy 页面。

请注意，可能会出现一个弹出窗口，警告您已超过支持的最大入侵策略数量。您必须重新评估访问控制策略，并整合入侵策略。您无法应用访问控制策略，直到关联的入侵策略（包括默认操作）的数量降至最大数量之内。

您可以在 Task Status 页面 (**Monitoring > ASA FirePOWER Monitoring > Task Status**) 上监控策略应用任务的进度。

对访问控制策略和规则进行故障排除

许可证：任何

正确地配置访问控制策略，尤其是创建访问控制规则并对其排序，是一项非常复杂的任务。然而，此任务对于构建有效的部署至关重要。如果您尚未缜密地计划您的策略，有些规则可能会取代其他规则，或者包含无效的配置。规则和其他策略设置均可能需要额外的许可证。

要帮助确保系统如预期处理流量，访问控制策略接口需要有强健的反馈系统。访问控制策略和规则编辑器中的图标可以标记警告和错误，如访问控制错误图标表中所述。

提示　在访问控制策略编辑器中，点击 **Show Warnings** 可显示一个弹出窗口，其中列出该策略所有警告。

此外，在应用时，系统就可能影响流量分析和流动的任何问题向您发出警告。

表 4-4　访问控制错误图标

图标	描述	详细信息
	错误	如果规则或配置存在错误，则更正错误之前无法应用策略，即便禁用任何受影响的规则也是如此。
	警告	您可以应用显示规则或其他警告的访问控制策略。然而，标记有警告的不当配置将不起作用。 例如，您可以应用这样的策略：包含被取代的规则，或者因为配置不当（使用空对象组的条件、在没有启用云通信的情况下配置 URL 条件等）而无法匹配流量的规则。这些规则不评估流量。如果禁用存在警告的规则，警告图标将会消失。如果在没有纠正潜在问题的情况下启用规则，警告图标将会再次显示。 又例如，许多功能需要特定许可证。访问控制策略仅可以成功应用。
	信息	信息图标传达有关可能影响流量流动的配置的有用信息。这些问题不会阻止您应用策略。 例如，如果您在执行应用控制或 URL 过滤，系统可能会根据一些访问控制规则跳过与连接的头几个数据包相匹配，直到系统在该连接中识别应用或网络流量。这样，就可建立连接，以便识别应用和 HTTP 请求。有关详细信息，请参阅第 8-5 页上的对应用控制的限制和第 8-10 页上的对 URL 检测和阻止的限制。

正确地配置访问控制策略和规则还可以减少处理网络流量所需的资源。创建复杂规则、调用许多不同的入侵策略以及对规则进行错误排序均可能影响性能。

有关详细信息，请参阅：

- 第 4-2 页上的访问控制的许可证和角色要求
- 第 4-13 页上的简化规则以便提高性能
- 第 4-14 页上的了解规则取代和无效配置警告
- 第 4-14 页上的对规则排序以便提高性能和避免取代

简化规则以便提高性能

复杂的访问控制策略和规则可能会消耗大量的资源。当您应用访问控制策略时，系统会一起评估所有规则，并创建 ASA FirePOWER 模块评估网络流量。可能出现一个弹出窗口，警告您已超过支持的访问控制规则或入侵策略的最大数量。

简化访问控制规则

以下准则可以帮助您简化访问控制规则和提高性能：

- 构建规则时，在您的条件中使用尽可能少的单独的元素。例如，在网络条件中，使用 IP 地址块，而不是单独的 IP 地址。在端口条件中，使用端口范围。使用应用过滤器及 URL 类别和声誉来执行应用控制和 URL 过滤，使用 LDAP 用户组来执行用户控制。

  请注意，将各元素组合到然后用于访问控制规则条件的对象并不能提高性能。例如，使用包含 50 个 IP 地址的网络对象，与逐一将这些 IP 地址纳入条件中相比，只能给您带来组织优势，而不是性能优势。
- 尽可能按安全区域限制规则。如果设备的接口不处于限制区域的规则中的某个区域，则该规则不会影响该设备的性能。
- 不要过度配置规则。如果一个条件足以匹配您想要处理的流量，请不要使用两个条件。

避免入侵策略和变量集激增

您可以在访问控制策略中用于检查流量的唯一入侵策略的数量取决于您策略的复杂性：您可以将一个入侵策略与每条“允许和交互式阻止”规则以及默认操作相关联。每个唯一的入侵策略和变量集**对均**视为一个策略。您在整个访问控制策略内只能选择三个入侵策略。

如果您超过了支持的入侵策略数量，请重新评估您的访问控制策略。您可能想要整合入侵策略或变量集。

在您的访问控制策略中的每个以下位置，检查弄清您选择的策略数量，以及这些策略使用的变量集的数量：高级访问控制策略设置中的 **Intrusion Policy used before Access Control rule is determined** 选项、访问控制策略的默认操作，以及该策略中的任何访问控制规则的检查设置。

了解规则取代和无效配置警告

许可证：任何

正确配置访问控制规则（以及高级部署中的网络分析规则）并对其排序，对于构建有效的部署至关重要。在访问控制策略中，访问控制规则可以取代其他规则或包含无效的配置。与此相似，您使用访问控制策略的高级设置配置的网络分析规则，也可能存在相同的问题。系统会使用警告和错误图标标记这些问题。

了解规则取代警告

访问控制规则的条件会取代匹配流量的后续规则。例如：

```
规则 1：允许管理员用户
规则 2：阻止管理员用户
```

以上的第二个规则永远不会阻止流量，因为第一个规则已允许流量。

请注意：

- 任何类型的规则条件均可以取代后续规则。
- 规则还会取代所有已配置条件均相同的一致后续规则。
- 如有任何条件不同，则后续规则不会被取代。

了解无效的配置警告

因为访问控制策略所依赖的外部设置可能会变化，有效的访问控制策略可能会变得无效。请考虑以下示例：

- 如果您将端口组添加至某条规则中的源端口，然后将端口组更改为包含 ICMP 端口，则该规则会变得无效，其旁边将出现一个警告图标。您仍然可以应用策略，但该规则将不会对网络流量产生影响。
- 如果您将用户添加至规则，然后将 LDAP 用户感知设置更改为排除该用户，该规则将不再起作用，因为用户已不再是访问受控用户。

对规则排序以便提高性能和避免取代

许可证：任何

系统已对访问控制策略中的规则进行编号，从 1 开始。系统会用升序规则编号按从上到下顺序将流量与规则相匹配。除监控规则外，流量匹配的第一条规则是处理该流量的规则。

正确的访问控制规则顺序可以减少处理网络流量所需的资源，防止规则取代。尽管您创建的规则对于每一个组织和部署都是唯一的，但在对规则排序时，仍有一些需要遵循的通用准则，这些准则不但能满足您的需求，而且能优化性能。

按关键性从高到低对规则排序

首先，您必须根据贵组织的需求对规则进行排序。将必须应用于所有流量的优先规则靠近策略的顶部放置。例如，如果您想要检查单个用户的流量是否存在入侵（使用允许规则），但又信任部门中的所有其他用户（使用信任规则），请按该顺序放置两个访问控制规则。

从具体到一般对规则进行排序

您可以将具体的规则，即更严格地定义其处理的流量的规则，靠前放置，从而提高性能。这一点很重要的另一原因是，有着广泛条件的规则可能与许多不同类型的流量相匹配，并且可以取代较为靠后、更为具体的规则。

请考虑以下情景：您想要阻止大多数的社交网络站点，但允许访问一些其他站点。例如，您可能想要图形设计师能够访问 Creative Commons Flickr 和 deviantART 的内容，但不能访问诸如 Facebook 或 Google+ 之类的其他站点。您应按以下方式对规则进行排序：

```
规则 1：对于“Design”LDAP 用户组，允许 Flickr、deviantART
规则 2：阻止社交网络
```

如果您颠倒规则顺序：

```
规则 1：阻止社交网络
规则 2：对于“Design”用户组，允许 Flickr、deviantART
```

第一条规则会阻止所有的社交网络流量，包括 Flickr 和 deviantART。因为没有流量将与第二条规则相匹配，所以，您的设计师将无法访问您想要提供的内容。

将检查流量的规则靠后放置

因为入侵、文件和恶意软件检查需要处理资源，将不检查流量的规则（信任、阻止）放置在检查流量的规则（允许、交互式阻止）之前，可以提高性能。这是因为“信任”和“阻止”规则可以转移系统可能早已检查过的流量。在所有其他因素均平等的前提下，也就是说，假设有一组规则，其中的任一条规则都不比其他规则更为关键，且取代不是问题，请考虑按以下顺序排列这些规则：

- 记录匹配连接但不对流量采取任何其他操作的“监控”规则
- 处理流量而无需进一步检查的“信任和阻止”规则
- 不对流量进行进一步检查的“允许和交互式阻止”规则
- 可选择性检查流量是否存恶意软件和/或入侵的“允许和交互式阻止”规则

生成当前访问控制设置的报告

许可证：任何

访问控制策略报告是特定时间点的策略和规则配置的记录。您可以使用该报告（其中包含以下信息）来进行审核或检查当前配置。

表 4-5　　访问控制策略报告的各部分

部分	描述
策略信息	提供策略的名称和描述、上次修改策略的用户的名称以及策略上次修改的日期和时间
HTTP 阻止响应 HTTP 交互式阻止响应	提供您使用策略阻止网站时，向用户显示的页面的相关详细信息。
安全情报	提供策略的安全情报白名单和黑名单的相关详细信息。
默认操作	列出默认操作和关联的变量集（如果有）。

表 4-5　访问控制策略报告的各部分 （续）

部分	描述
规则	列出策略中的每条访问控制规则，并提供其配置的相关详细信息。
高级设置	有关策略的高级设置的详细信息，包括： • 用于为访问控制策略预处理流量的网络分析策略，以及全局预处理选项 • 用于被动部署的自适应配置文件设置 • 用于检测文件、恶意软件和入侵的性能设置 • 其他策略范围的设置
引用对象	提供访问控制策略引用的可重用对象的相关详细信息，包括入侵策略变量集。

还可以生成访问控制比较报告，该报告将一个策略与当前应用的策略或另一策略进行比较。有关详细信息，请参阅第 4-16 页上的比较访问控制策略。

要查看访问控制策略报告：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要生成报告的策略旁的报告图标 ( )。在生成访问控制策略报告前，切记保存所有更改，只有已保存的更改会在报告中显示。

系统将会生成报告。您将报告保存至您的计算机。

比较访问控制策略

许可证：任何

如要审阅策略更改以便符合组织的标准或提高系统性能，可以检查两个访问控制策略之间的差异。可以比较任何两个策略，也可以将当前应用的策略与另一策略进行比较。在进行比较后，或者生成 PDF 报告来记录两个策略之间的差异。

有两个可以用来比较策略的工具：

- 比较视图仅会以并排格式显示两个策略之间的差异。每个策略的名称将会显示在比较视图左侧和右侧的标题栏中，当选择 **Running Configuration** 时除外，在这种情况下，空白栏代表当前的活动策略。

  您可以使用此工具来在模块界面中查看和导航两个策略（在其差异已突出显示）。

- 比较报告会以类似策略报告的格式（但采用 PDF 格式）创建仅有两个策略之间的差异的记录。

  可以使用此工具来保存、复制、打印和共享策略比较，供未来检查使用。

如需了解和使用策略比较工具的更多相关信息，请参阅：

- 第 4-17 页上的使用访问控制策略比较视图
- 第 4-17 页上的使用访问控制策略比较报告

使用访问控制策略比较视图

许可证：任何

比较视图会以并排格式显示两个策略，每个策略由比较视图左侧和右侧标题栏中的名称确定。比较运行配置之外的两个策略时，最后修改的时间和最后修改的用户将会随策略名称显示。

两个策略之间的差异将会突出显示：

- 蓝色指示突出显示的设置在两个策略中不同，不同之处以红色文本标注。
- 绿色指示突出显示的设置在一个策略中存在，但在另一个策略中不存在。

您可以执行下表中的任何操作。

表 4-6　访问控制策略比较视图操作

要.....	您可以.....
逐一浏览更改	点击标题栏上方的 **Previous** 或 **Next**。 在左右两侧之间以双箭头图标 (⇹) 为中心移动， **Difference** 数字调整为识别您正在查看哪个差异。
生成新的策略比较视图	点击 **New Comparison**。 系统将显示 **Select Comparison** 窗口。有关详细信息，请参阅第 4-17 页上的使用访问控制策略比较报告。
生成策略比较报告	点击 **Comparison Report**。 策略比较报告将会创建仅列出两个策略之间的差异的 PDF 文档。

使用访问控制策略比较报告

许可证：任何

访问控制策略比较报告是策略比较视图确定的两个访问控制策略或者一个策略和当前应用的策略之间的所有差异的记录，以 PDF 格式提供。可以使用此报告来进一步检查两个策略配置之间差异，以及保存和分发比较结果。

对于可以访问的所有策略，都可以通过比较视图生成访问控制策略比较报告。在生成策略报告前，切记保存所有更改，只有已保存的更改会在报告中显示。

策略比较报告的格式与策略报告相同，有一处例外：策略报告包含策略中的所有配置，而策略比较报告仅列出策略之间的那些不同配置。访问控制策略比较报告包含第 4-15 页上的表 4-5 中所述的各部分。

提示　您可以使用类似的操作步骤来比较网络分析、入侵、文件或系统策略。

要比较两个访问控制策略：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击 **Compare Policies**。

系统将显示 Select Comparison 窗口。

步骤 3　从 **Compare Against** 下拉列表中选择要进行比较的类型：

- 要比较两个不同的策略，请选择 **Other Policy**。
  页面将会刷新，并显示 Policy A 和 Policy B 下拉列表。
- 要将另一策略与当前活动的策略进行比较，请选择 **Running Configuration**。
  页面将会刷新，并会显示 Target/Running Configuration A 和 Policy B 下拉列表。

步骤 4　根据您选择的比较类型，有以下选项可供选择：

- 如果您比较两个不同的策略，请从 Policy A 和 Policy B 下拉列表中选择要比较的策略。
- 如果您将正运行的配置与另一策略进行比较，请从 Policy B 下拉列表中选择第二个策略。

步骤 5　点击 **OK** 显示策略比较视图。
系统将显示比较视图。

步骤 6　或者点击 **Comparison Report** 生成访问控制策略比较报告。
屏幕上将会显示访问控制策略比较报告。您将报告保存至您的计算机。

使用安全情报 IP 地址声誉设置黑名单

作为防御恶意互联网内容的第一道防线，ASA FirePOWER 模块包括安全情报功能，可供您根据最新声誉情报立即将连接列出黑入单（阻止），再也无需资源更密集型深入分析。安全情报过滤需要保护许可证 外的所有受管设备上均受支持。

安全情报通过阻止具有已知不良声誉的 IP 地址的往返流量而发挥作用。此流量过滤发生在任何其他策略型检测、分析或流量处理**之前**。

请注意，您可以通过 IP 地址手动限制流量来创建可执行与安全情报过滤类似的功能的访问控制规则。但是，访问控制规则范围更广泛，配置更为复杂，并且无法使用动态源自动更新。

被安全情报列入黑名单的流量会被立即阻止，因此其将不接受任何进一步检测 — 既不检查其是否存在入侵、漏洞、恶意软件等。或者，在被动部署中建议选择使用安全情报过滤的仅监控设置。这使系统能够分析本应被列入黑名单的连接，但也将匹配项记录至黑名单并生成连接结束安全情报事件。

为了您的方便，思科提供*情报源*（有时称为 *Sourcefire 情报源*），它包括由 VRT 确定具有不良声誉且定期更新的多个 IP 地址集合组成。情报源可跟踪开放中继、已知攻击者、伪造 IP 地址 (bogon) 等等。您还可自定义功能以满足贵组织的独特需求，例如：

- **第三方源** — 使用第三方声誉源补充情报源，系统可以像更新思科源一样自动更新第三方声誉源
- **自定义黑名单** — 系统允许您以多种方式根据自己的需求将特定 IP 地址手动列入黑名单
- **按安全区域实施黑名单** — 为提高性能，您可能想要锁定实施目标，例如将垃圾邮件黑名单限定于处理邮件流量的区域
- **监控，而不是列入黑名单** — 在被动部署中及对于其实施之前的源测试尤为有用；只监控违规会话，而不阻止它们，从而生成连接结束事件
- **列入白名单以消除误报** — 当黑名单范围太大或不正确阻止想要允许的流量 （例如，重要资源）时，可使用自定义白名单覆盖黑名单

有关配置可执行安全情报的访问控制策略以执行安全情报过滤和查看此过滤生成的事件数据的详细信息，请参阅：

- 第 5-2 页上的选择安全情报战略
- 第 5-3 页上的建立安全情报白名单和黑名单
- 第 25-7 页上的记录安全情报 （列入黑名单）决策

选择安全情报战略

许可证：保护

构建黑名单的最简易方式是使用情报源，它可跟踪已知为开放中继、已知攻击者、伪造 IP 地址 (bogon) 等的 IP 地址。因为情报源定期更新，使用它可确保系统使用最新信息来过滤网络流量。恶意 IP 地址是指诸如恶意软件、垃圾邮件、僵尸网络以及网络钓鱼的安全威胁，它们的出现和消失速度要快于更新和应用新策略的速度。

为扩大情报源，可以使用自定义或第三方 IP 地址列表和源执行安全情报过滤，其中：

- *列表*是 IP 地址的静态列表，可以将其上传至 ASA FirePOWER 模块
- *源*是 ASA FirePOWER 模块定期从互联网下载的 IP 地址的动态列表；情报源是一种特殊的源。

有关如何配置安全情报列表和源（包括互联网访问要求）的详细信息，请参阅第 2-4 页上的使用安全情报列表和源。

使用安全情报全局黑名单

在分析过程中，可以构建*全局黑名单*。例如，如果注意到入侵事件中有一组可路由 IP 地址与漏洞攻击相关联，则可将这些 IP 地址列入黑名单。在所有访问控制策略中，ASA FirePOWER 模块使用此全局黑名单（和相关的*全局白名单*）来执行安全情报过滤。如需管理这些全局列表的相关信息，请参阅第 2-5 页上的使用全局白名单和黑名单。

注　尽管全局黑名单（或全局白名单；请见下文）的源更新和增添会在整个部署中自动实施更改，但对安全情报对象做出的任何其他更改均需要重新应用访问控制策略。有关详细信息，请参阅第 2-5 页上的表 2-1。

使用网络对象

最后，构建黑名单的一种简便方式为使用代表 IP 地址、 IP 地址块或 IP 地址集合的*网络对象或网络对象组*。如需创建和修改网络对象的相关信息，请参阅第 2-3 页上的使用网络对象。

使用安全情报白名单

除了黑名单，每个访问控制策略还有关联的白名单，也可以使用安全情报对象来进行填充。策略的白名单可以覆盖其黑名单。即系统使用访问控制规则评估已列入白名单的源或目标 IP 地址的流量，即便 IP 地址也被列入黑名单。通常，如果黑名单仍然有用，但范围又太过广泛，错误地阻止您想要检查的流量，则可以使用白名单。

例如，如果可信源不当地阻止了对重要资源的访问，但其整体而言对您的组织有用，可以仅将不当分类的 IP 地址列入白名单，而不是从黑名单移除整个源。

通过安全区域实施安全情报过滤

为提高精细度，可以根据连接中的源或目标 IP 地址是否位于特定安全区域来实施安全情报过滤。

要扩展以上的白名单示例，可以将不当分类的 IP 地址列入白名单，但随后使用组织中需要访问 IP 地址的人员所使用的安全区域限制白名单对象。这样，只有有业务需要的人员才可以访问列入白名单的 IP 地址。再如，您可以使用第三方垃圾邮件源将邮件服务器安全区域上的流量列入黑名单。

监控连接而非将其列入黑名单

如果您不确定是否想要将特殊 IP 地址或地址集列入黑名单，则可使用“仅监控”设置，该设置允许系统将匹配连接传递给访问控制规则，但也将匹配项记录到黑名单并生成连接结束安全情报事件。请注意，无法将全局黑名单设置为仅监控。

考虑一下这样的情况，在使用第三方源实施阻止之前，想要先对该源进行测试。当将源设置为仅监控时，系统允许已被阻止的连接，以便系统能对其进行进一步的分析，但是也会记录这些连接中的每一个连接，以供进行评估。

在被动部署中，为提高性能，思科 建议始终采用仅监控的设置。被动部署无法影响流量；与将系统配置为阻止流量相比，没有任何优势。此外，因为阻止的连接实际上在被动部署中并未被阻止，因此，系统可能针对每条已阻止连接报告多个连接开始事件。

建立安全情报白名单和黑名单

许可证：保护

要构架白名单和黑名单，可用网络对象和组的任何组合以及安全情报源和列表填充它们，您可按安全区域对所有这些进行限制。

默认情况下，访问控制策略使用应用至任意区域的 ASA FirePOWER 模块 的全局白名单和黑名单。这些列表由分析师填充。可以为每个策略选择是否使用这些全局列表。

注　您不能使用已填充全局白名单或黑名单的访问控制策略应用。如果您向任一全局列表添加了 IP 地址，则**必须**先从策略的安全情报配置中移除非空列表，然后才能应用该策略。有关详细信息，请参阅第 2-5 页上的使用全局白名单和黑名单。

在建立白名单和黑名单后，可以记录列入黑名单的连接。也可以将个别列入黑名单的对象（包括源和列表）设置为仅监控。这使得系统可以使用访问控制处理涉及列入黑名单的 IP 地址的连接，但也将连接的匹配项记录至黑名单。

可以使用访问控制策略中的 Security Intelligence 选项卡来配置白名单、黑名单和日志记录选项。该页面列出了可以在白名单或黑名单中使用的可用对象以及可以用于限制列入白名单和黑名单的对象的可用区域。每种类型的对象或区域用不同的图标区分。标有思科图标 (思科) 的对象代表情报源中的不同类别。思科

在黑名单中，设置为阻止的对象标有阻止图标 ( )，而仅监控的对象标有监控图标 ( )。因为白名单会覆盖黑名单，如果您向两个列表添加相同的对象，系统会显示带删除线的已列入黑名单对象。

最多可以向白名单和黑名单添加总计 255 个对象。即白名单中的对象数量加上黑名单中的对象数量不能超过 255。

请注意，尽管可以将网络掩码为 /0 的网络对象添加到白名单或黑名单，但这些对象中使用 /0 网络掩码的地址块将被忽略，并且不会基于这些地址进行白名单和黑名单过滤。安全情报源中网络掩码为 /0 的地址块也将被忽略。如果想要监控或阻止策略已锁定为目标的所有流量，请分别使用包含 **Monitor** 或 **Block** 规则操作的访问控制规则，并使用 **Source Networks** 和 **Destination Networks** 的默认值 **any**，而不使用安全情报过滤。

要建立访问控制策略的安全情报白名单和黑名单，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要配置的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Security Intelligence** 选项卡。

屏幕上将会显示访问控制策略的安全情报设置。

步骤 4　或者点击日志记录图标 ( ) 来记录已列入黑名单的连接。

必须先启用日志记录，才可以将已列入黑名单的对象设置为仅监控。有关详细信息，请参阅第 25-7 页上的记录安全情报（列入黑名单）决策。

步骤 5　通过选择一个或多个**可用对象**开始构建白名单和黑名单。

使用 Shift 和 Ctrl 键可选择多个对象，或者右键单击并选择 **Select All**。

提示　可以搜索需要包含的现有对象，如果没有现有对象符合组织的需求，也可以动态创建对象。有关详细信息，请参阅第 5-4 页上的搜索添加至白名单或黑名单的对象。

步骤 6　或者通过选择一个**可用区域**，按区域限制选定对象。

默认情况下，对象不会受到限制，即它们拥有取值为 `Any` 的区域。请注意，可以用仅一个区域进行限制，而不是使用 **Any**。如要在多个区域上实施对象的安全情报过滤，对于每个区域，都必须将对象分别添加至白名单或黑名单。此外，全局白名单或黑名单无法通过区域进行限制。

步骤 7　点击 **Add to Whitelist** 或 **Add to Blacklist**。

还可以点击并拖动选定对象至任一列表。

您选择的对象已添加到白名单或黑名单。

提示　要移除列表中的一个对象，请点击其删除图标 ( )。可以使用 Shift 和 Ctrl 键来选择多个对象，或者右键单击并 **Select All**，然后右键单击并选择 **Delete Selected**。如果您在删除全局列表，则必须确认您的选择。请注意，从白名单或黑名单移除一个对象不会将其从 ASA FirePOWER 模块中删除。

步骤 8　重复步骤 5 至 7，直到完成至白名单和黑名单的对象添加。

步骤 9　或者，右键单击 **Blacklist** 下的对象，然后选择 **Monitor-only (do not block)**，将列入黑名单的对象设置为仅监控。

在被动部署中，思科建议将所有已列入黑名单的对象设置为仅监控。然而，请注意，无法将全局黑名单设置为仅监控。

步骤 10　点击 **Store ASA FirePOWER Changes**。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

搜索添加至白名单或黑名单的对象

许可证：保护

如果有多个网络对象、组、源和列表，可以使用搜索功能来限制要添加至黑名单或白名单的对象。

要搜索添加至白名单或黑名单的对象，请执行以下操作：

步骤 1　在 **Search by name or value** 字段中键入您的查询。

在键入字符串时， Available Objects 列表将会更新，从而显示匹配项。要清除搜索字符串，请点击搜索字段上方的重新加载图标 ( ) 或点击搜索字段中的清除图标 ( )。

可以搜索为这些对象配置的网络对象名称以及值。例如，如果有一个名为 Texas Office 的网络对象，该对象配置了 192.168.3.0/24 这个值，且该对象包含在组对象 US Offices 中，则可以键入部分或完整的搜索字符串（例如 Tex）或者键入某个值（例如 3）来显示这两个对象。

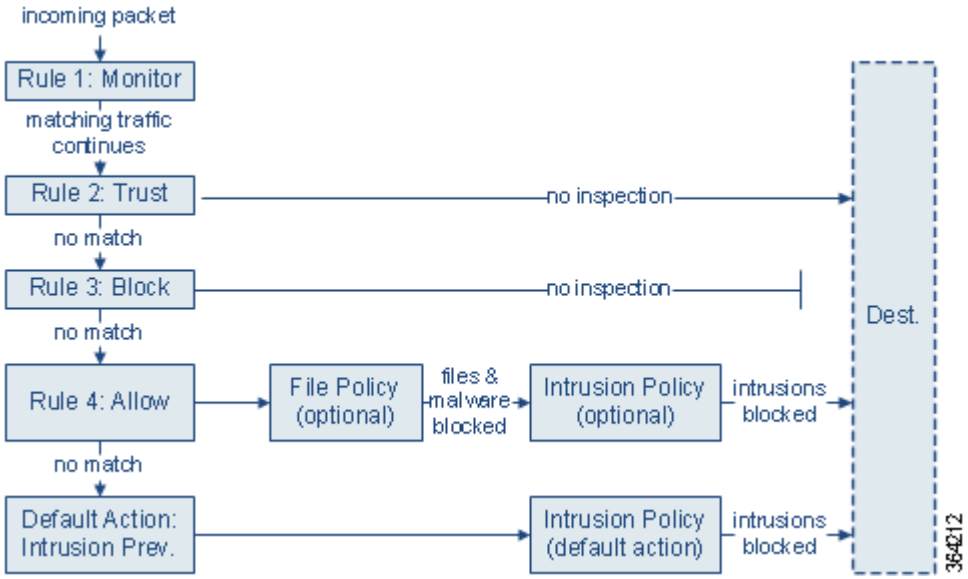
使用访问控制规则调整流量

在访问控制策略中，*访问控制规则*提供处理网络流量的精细方法。

基于安全情报的流量过滤以及一些解码和预处理发生在访问控制规则评估网络流量**之前**。系统按您指定的顺序将流量与访问控制规则相匹配。在大多数情况下，系统根据*所有*规则条件匹配流量的*第一个*访问控制规则处理网络流量。条件可以简单，也可以复杂；可通过安全区域、网络或地理位置、端口、应用、请求的 URL 和用户控制流量。

每个规则也有*操作*，确定是否监控、信任、阻止或允许匹配的流量。当允许流量时，指定系统使用入侵或文件策略先检测流量以在漏洞、恶意软件或禁止的文件到达您的资产或退出网络之前予以阻止。但是，在系统信任或阻止流量之后，**不**执行进一步检测。

以下场景汇总了内联入侵防御部署中访问控制规则评估流量的方式。



在这种情况中，流量评估如下：

- **规则 1：Monitor** 第一次评估流量。 Monitor 规则跟踪和记录网络流量，但不影响流量。系统继续根据其他规则匹配流量，以确定允许其通过，还是拒绝。
- **规则 2：Trust** 继续评估流量。允许匹配的流量传至目标，无需进一步检测。不匹配的流量继续根据下一规则进行评估。
- **规则 3：Block** 第三次评估流量。匹配的流量被阻止，无需进一步检测。不匹配的流量继续根据最终规则进行评估。

- **规则 4：Allow** 是最终规则。对于此规则，允许匹配的流量；但检测和阻止流量内禁止的文件、恶意软件、入侵和漏洞。允许其他非禁止、非恶意流量到达目标。请注意，您可能有其他只执行文件检测、只执行入侵检测或者两类检测都不执行的 Allow 规则。
- **Default Action** 处理不匹配任何规则的所有流量。在此情况下，默认操作在允许非恶意流量通过之前执行入侵防御。在不同的部署中，您可能有默认操作可以信任或阻止所有流量，而无需进一步检测。（您不能对默认操作处理的流量执行文件或恶意软件检测。）

有关访问控制规则的详细信息，请参阅：

- 第 6-2 页上的创建和编辑访问控制规则
- 第 6-9 页上的管理策略中的访问控制规则
- 第 4-12 页上的对访问控制策略和规则进行故障排除

创建和编辑访问控制规则

许可证：任何环境

在访问控制策略中，访问控制规则提供处理网络流量的精细方法。除唯一名称之外，每个访问控制规则都具有以下基本组件：

State

默认情况下，规则处于启用状态。如果您禁用某规则，系统将不用它来评估网络流量并停止为该规则生成警告和错误。

Position

系统已对访问控制策略中的规则进行编号，从 1 开始。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。除 Monitor 规则之外，流量匹配的第一个规则是处理该流量的规则。

Conditions

条件指定规则处理的特定流量。条件可以依据安全区域、网络或地理位置、端口、应用、请求的 URL 或用户匹配流量。条件可以简单，也可以复杂；条件的使用通常取决于许可证。

Action

规则操作确定系统如何处理匹配的流量。您可以监控、信任、阻止或允许（执行或无需执行进一步检测）匹配的流量。请注意，系统不对受信任或被阻止的流量进行检测。

Inspection

访问控制规则的检测选项管理系统如何检测和阻止您意外允许的恶意流量。通过规则允许流量时，可以指定系统先使用入侵或文件策略检测流量以在漏洞、恶意软件或禁止的文件到达您的资产或退出网络之前予以阻止。

Logging

规则的日志记录设置管理系统保存其处理流量的记录。您可以对匹配规则的流量保存记录。一般而言，您可以记录连接开始和结束的会话。您可以将连接记录到 ASA FirePOWER 模块，以及系统日志 (syslog) 或 SNMP 陷阱服务器。

Comments

每次保存对访问控制规则所做的更改时，您都可以添加一个注释。

使用访问控制规则编辑器添加和编辑访问控制规则；从访问控制策略编辑器的 Rules 选项卡访问规则编辑器。在规则编辑器中，您可以：

- 在编辑器的上部配置基本属性，如规则的名称、状态、位置和操作。
- 使用编辑器下部左侧的选项卡添加条件。
- 使用下部右侧的选项卡配置检测和日志记录选项，还可以向规则添加注释。为了方便，无论您在查看哪个选项卡，编辑器都列出规则的检测和日志记录选项。

注　正确创建和排序访问控制规则是一项复杂的任务，但重要的是构建有效部署。如果不认真规划您的策略，这些规则会抢占其他规则，需要额外的许可证或包含无效配置。为帮助确保系统按预期处理流量，访问控制策略接口具有规则的强大警告和错误反馈系统。有关详细信息，请参阅第 4-12 页上的对访问控制策略和规则进行故障排除。

要创建或修改访问控制规则，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要添加规则的访问控制策略旁边的编辑图标 ( )。

系统将显示策略页面，重点显示 Rules 选项卡。

步骤 3　您有以下选项：

- 要添加新规则，请点击 **Add Rule**。
- 要编辑现有规则，请点击要编辑的规则旁边的编辑图标 ( )。

系统将显示访问控制规则编辑器。

步骤 4　为规则键入**名称**。

每个规则必须有唯一名称。最多可以使用 30 个可打印字符，包括空格和特殊字符，但 (:) 除外。

步骤 5　配置规则组件，如上汇总。可以配置以下内容或接受默认设置：

- 指定规则是否为 **Enabled**。
- 指定规则位置；请参阅第 6-4 页上的指定规则的评估顺序。
- 在 **Action** 中选择规则操作；请参阅第 6-6 页上的使用规则操作确定流量处理和检测。
- 配置规则的条件；请参阅第 6-4 页上的使用 Conditions 指定规则处理的流量。
- 对于 Allow 和 Interactive Block 规则，配置规则的 **Inspection** 选项；请参阅第 10-1 页上的使用入侵和文件策略控制流量。
- 指定 **Logging** 选项；请参阅第 25-1 页上的记录网络流量中的连接。
- 添加 **Comments**；请参阅第 6-9 页上的向规则添加注释。

步骤 6　点击 **Store FirePOWER Changes** 保存规则。

您的规则已保存。您可以点击删除图标 ( ) 删除规则。您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

指定规则的评估顺序

许可证：任何环境

首次创建访问控制规则时，使用规则编辑器中的 **Insert** 下拉列表指定该规则的位置。系统已对访问控制策略中的规则进行编号，从 1 开始。系统会用升序的规则号码以从上到下的顺序将流量匹配到访问控制规则中。

在大多数情况下，系统根据*所有*规则条件匹配流量的*第一个*访问控制规则处理网络流量。除了 Monitor 规则（记录流量，但不影响流量）之外，系统在流量匹配一个规则后，**不再**继续根据其他低优先级规则评估流量。

提示 适当的访问控制规则顺序可减少处理网络流量所需的资源并防止规则抢占。尽管您创建的规则对于每个组织和部署来说都是唯一的，但是排序规则时需要遵循几个基本原则，才可优化性能，同时满足您的需求。有关详细信息，请参阅第 4-14 页上的对规则排序以便提高性能和避免取代。

除了按照编号排序规则之外，还可按类别对规则进行分组。默认情况下，系统提供三个类别：管理员、标准和根。您可以添加自定义类别，但不可删除思科提供的类别或更改其顺序。有关更改现有规则的位置或类别的信息，请参阅第 6-11 页上的更改规则的位置或类别。

要在编辑或创建规则时将规则添加到类别，请执行以下操作：

步骤 1 在访问控制规则编辑器中，从 **Insert** 下拉列表中选择 **Into Category**，然后选择要使用的类别。

保存规则时，系统将其置于该类别的最后位置。

要在编辑或创建规则时按编号定位规则，请执行以下操作：

步骤 1 在访问控制规则编辑器中，从 **Insert** 下拉列表中选择 **above rule** 或 **below rule**，然后键入合适的规则编号。

保存规则时，系统将其置于您指定的位置。

使用 Conditions 指定规则处理的流量

许可证：因功能而异

访问控制规则的条件标识规则处理的流量类型。条件可以简单，也可以复杂；可通过安全区域、网络或地理位置、端口、应用、请求的 URL 和用户控制流量。

向访问控制规则添加条件时，请记住以下要点：

- 您可以为每个规则配置多个条件。为使规则应用于流量，流量必须匹配规则中的**所有**条件。例如，您可以使用单一规则对特定主机（区域或网络条件）执行 URL 过滤（URL 条件）。
- 可以为规则中的每个条件最多可以添加 50 个标准。匹配**所有**条件的标准的流量满足该条件。例如，您可以使用单一规则为最多 50 个用户和组执行用户控制。

请注意，最多可以使用 50 个源标准和 50 个目标标准按源和目标限制区域和网络条件。如果将源和目标标准添加到区域或网络条件，匹配的流量必须源自指定源区域/网络之一**并**通过目标区域/网络之一流出。换句话说，系统使用 OR 运算连接同类型的多个条件标准，使用 AND 运算连接多个条件类型。例如，如果规则条件如下：

```
Source Networks: 10.0.0.0/8, 192.168.0.0/16
Application Category: peer to peer
```

规则将匹配来自其中一个私有 IPv4 网络的一台主机的 P2P 应用流量 - 数据包必须源自一个 **OR** 其他源网络， **AND** 表示点对点应用流量。以下两个连接同时触发规则：

```
10.42.0.105 to anywhere, using LimeWire
192.168.42.105 to anywhere, using Kazaa
```

如果不为规则配置特定条件，系统将不基于此标准匹配流量。例如，无论会话中使用的应用如何，具有网络条件但不具有应用条件的规则根据流量源或目标评估流量。

注　应用访问控制策略时，系统评估其所有规则并创建一个扩展标准集，ASA FirePOWER 模块使用该扩展标准集评估网络流量。复杂的访问控制策略和规则可控制重要资源。有关简化访问控制规则的提示和提高性能的其他方式，请参阅第 4-12 页上的对访问控制策略和规则进行故障排除。

添加或编辑访问控制规则时，可使用规则编辑器下部左侧的选项卡添加和编辑规则条件。下表概述可添加的条件类型。

表 6-1　访问控制规则条件类型

这些条件.....	匹配流量.....	详细信息
区域	通过特定安全区域中的一个接口进入或离开设备	安全区域是根据部署和安全策略划分的一个或多个接口的逻辑分组。要构建区域条件，请参阅第 7-1 页上的按安全区域控制流量。
网络	按照其源或目标 IP 地址、国家/地区或大洲	您可以明确指定 IP 地址或地址块。利用地理定位功能还可以根据源或目标国家/地区或大洲控制流量。要构建网络条件，请参阅第 7-3 页上的按网络或地理位置控制流量。
端口	按照其源端口或目标端口	对于 TCP 和 UDP，可以根据传输层协议控制流量。对于 ICMP 和 ICMPv6 (IPv6-ICMP)，可以根据互联网层协议及可选类型和代码控制流量。使用端口条件，还可以使用不用端口的其他协议控制流量。要构建端口条件，请参阅第 7-4 页上的按端口和 ICMP 代码控制流量。
应用	按照会话中检测的应用	您可以控制对单个应用的访问，或根据基本特征：键入、风险、业务相关性、类别和标记 过滤访问。要构建应用条件，请参阅第 8-2 页上的控制应用流量。
URL	按照会话中请求的 URL	您可以分别限制或根据 URL 的一般分类和风险级别限制网络中的用户可访问的网站。要构建 URL 条件，请参阅第 8-6 页上的阻止 URL。
用户	按照参与会话的用户	根据登录受监控会话所涉及的主机的 LDAP 用户，可以控制流量。可以根据从 Microsoft Active Directory 服务器检索的单个用户或组控制流量。要构建用户条件，请参阅第 9-1 页上的根据用户控制流量。

请注意，虽然可使用任意许可证创建访问控制规则，但某些规则条件需要您先启用特定许可功能，然后才可以应用策略。有关详细信息，请参阅第 4-2 页上的访问控制和型号要求。

使用规则操作确定流量处理和检测

许可证：任何环境

每个访问控制规则都有确定匹配流量的以下过程的*操作*：

- 处理 - 首先，规则操作管理系统是否将监控、信任、阻止或允许匹配规则条件的流量
- 检测 - 利用某些规则操作，可以在正确许可的条件下通过进一步检测匹配的流量，然后才允许流量通过
- 日志记录 - 该规则操作确定何时以及如何记录有关匹配的流量的详细信息

访问控制策略的*默认操作*处理不满足任何非“监控”访问控制规则条件的流量；请参阅第 4-4 页上的为网络流量设置默认的处理和检查。

请记住，只有内联部署的设备才可以阻止或修改流量。被动部署设备可以分析和记录，但是不影响流量。有关规则操作的详细信息以及规则操作如何影响流量处理、检测和日志记录，请参阅：

- 第 6-6 页上的Monitor 操作：延迟操作并确保日志记录
- 第 6-6 页上的Trust 操作：无检测通过流量
- 第 6-7 页上的Blocking 操作：无检测阻止流量
- 第 6-7 页上的Interactive Blocking 操作：允许用户绕过网站拦截
- 第 6-8 页上的Allow 操作：允许和检测流量
- 第 10-1 页上的使用入侵和文件策略控制流量
- 第 25-8 页上的根据访问控制处理记录连接

Monitor 操作：延迟操作并确保日志记录

许可证：任何环境

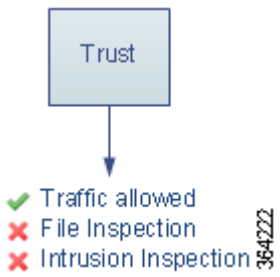
Monitor 操作不影响流量；匹配的流量既不会被立即允许，也不会被立即拒绝。更确切地是，根据其他规则匹配流量以确定允许还是拒绝该流量。所匹配的第一个非 Monitor 规则确定流量和任何进一步的检测。如果没有其他匹配的规则，系统使用默认操作。

由于 Monitor 规则的主要目的是跟踪网络流量，因此系统会自动记录监控流量的连接结束事件。即，即使流量不匹配其他规则，且您不对默认操作进行日志记录，系统也会记录连接。有关详细信息，请参阅第 25-4 页上的了解受监控连接的日志记录。

Trust 操作：无检测通过流量

许可证：任何环境

Trust 操作允许流量通过，无需任何类型的进一步检测。

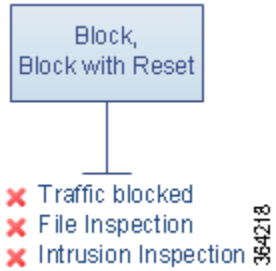


您可以在连接开始和结束时记录受信任的网络流量。有关详细信息，请参阅第 25-5 页上的了解受信任连接的日志记录。

Blocking 操作：无检测阻止流量

许可证：任何环境

Block 和 **Block with reset** 操作拒绝流量，无需任何类型的进一步检测。 Block with reset 规则也会重置连接。



对于 HTTP 流量，当系统阻止网络请求时，您可以使用解释连接被拒绝的自定义页面覆盖默认的浏览器或服务器页面。系统将此自定义页面称为 *HTTP 响应页面*；请参阅第 8-12 页上的显示受阻 URL 的自定义网页。

您可以仅记录连接开始时被阻止的网络流量。请注意，仅内联部署的设备才可以阻止流量。因为阻止的连接实际上在被动部署中并未被阻止，所以系统可能针对每个被阻止的连接报告多个连接开始事件。有关详细信息，请参阅第 25-5 页上的了解受阻和交互式受阻连接的记录。

注意事项　在拒绝服务 (DoS) 攻击期间记录被阻止的 TCP 连接会影响系统性能并因多个相似事件。对 Block 规则启用日志记录之前，考虑此规则是否监控面向互联网的接口或其他易受 DoS 攻击的接口的流量。

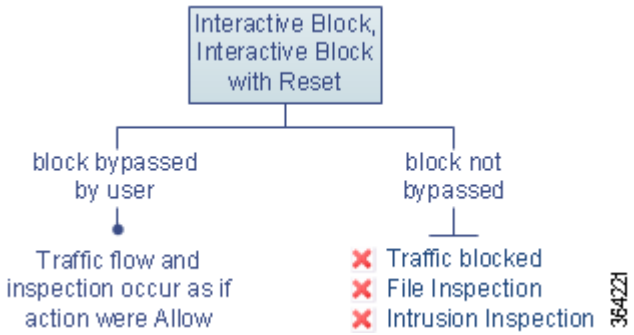
Interactive Blocking 操作：允许用户绕过网站拦截

许可证：任何环境

对于 HTTP 流量，**Interactive Block** 和 **Interactive Block with reset** 操作使用户有机会通过点击可定制的警告页面（称为 *HTTP 响应页面*）绕过网站拦截。Interactive Block with reset 规则也可以重置连接。

对于所有交互式阻止的流量，系统的处理、检测和日志记录取决于用户是否绕过拦截：

- 如果用户不（或无法）绕过拦截，该规则模拟 Block 规则。匹配的流量不经进一步检测即被拒绝，并且您可以只记录连接的开始。这些连接开始事件有 `Interactive Block` 或 `Interactive Block with Reset` 操作。
- 如果用户绕过拦截，该规则模拟 Allow 规则。因此，您可以将任一类型的 Interactive Block 规则与文件和入侵策略关联，以检测此用户允许的流量。系统也可以记录连接开始和结束事件。这些连接事件都有 `Allow` 操作。



Allow 操作：允许和检测流量

许可证：任何环境

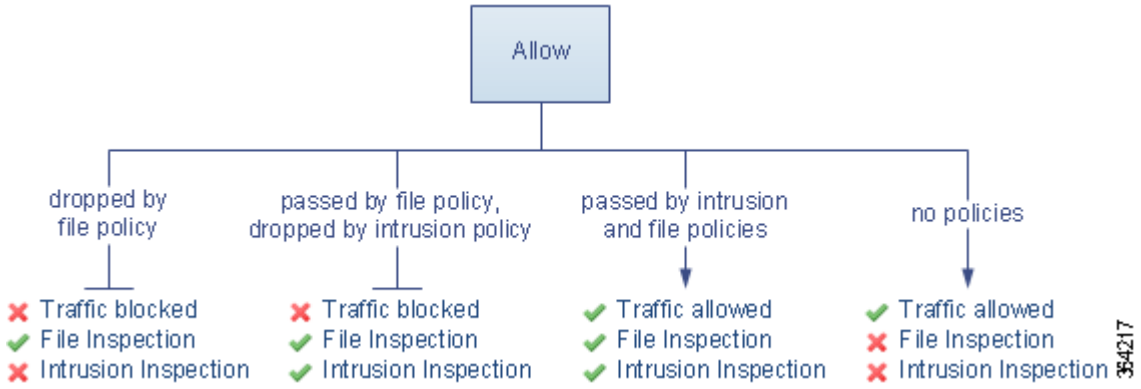
Allow 操作允许匹配的流量通过。当您允许流量时，可以使用关联的入侵或文件策略（或两者）进一步检测和阻止网络流量：

- 借助保护许可证，您可以使用入侵策略根据入侵检测和防御配置分析网络流量，或者丢弃恶意数据包。
- 借助保护许可证，还可以使用文件策略执行文件控制。借助文件控制，可以检测和阻止用户通过特定应用协议上传（发送）或下载（接收）特定类型的文件。
- 借助恶意软件许可证，您还可以使用文件策略执行基于网络的高级恶意软件防护 (AMP)。基于网络的 AMP 可以检测文件中的恶意软件，或者阻止检测到的恶意软件。

有关如何将入侵或文件策略与访问控制规则相关联的指导，请参阅第 10-1 页上的使用入侵和文件策略控制流量。

下图说明在满足 Allow 规则（或用户忽略的 Interactive Block 规则；请参阅第 6-7 页上的Interactive Blocking 操作：允许用户绕过网站拦截）条件的流量中进行的检测类型。请注意，文件检测会在入侵检测之前发生；被阻止文件不会进行入侵相关漏洞检测。

为简单起见，该图显示入侵和文件策略均与访问控制规则相匹配（或都不匹配）的情况下的流量。但是，可以单独配置其中一个策略。如果没有文件策略，流量将由入侵策略确定；如果没有入侵策略，流量将由文件策略确定。



您可以在连接开始和结束时记录允许的网络流量。

向规则添加注释

许可证：任何环境

创建或编辑访问控制规则时，可以添加注释。例如，您可为其他用户汇总整体配置，或者当您变更规则和更改的原因时进行记录。您可以显示规则的所有注释列表，以及添加每条注释的用户以及添加注释的日期。

保存规则时，自上次保存所做的所有注释都将变为只读。

要将注释添加到规则，请执行以下操作：

步骤 1　在访问控制规则编辑器中，选择 **Comments** 选项卡。

系统将显示 Comments 页面。

步骤 2　点击 **New Comment**。

系统将显示 New Comment 弹出窗口。

步骤 3　键入您的注释，然后点击 **OK**。

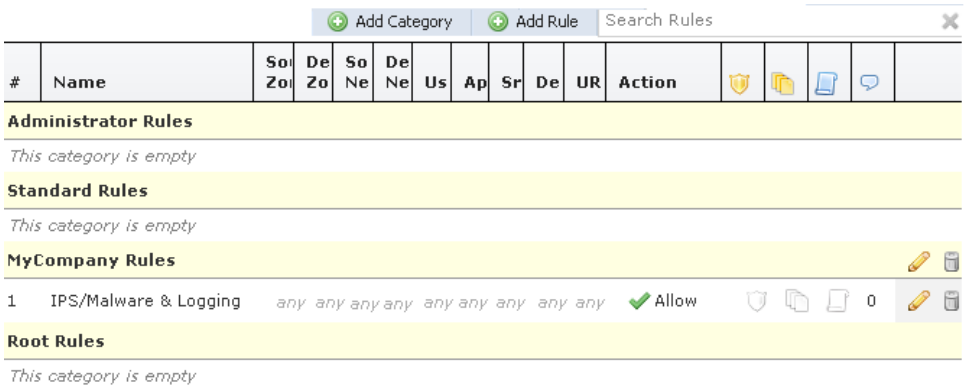
您的注释已保存。您可以在保存规则之前编辑或删除此注释。

步骤 4　保存或继续编辑规则。

管理策略中的访问控制规则

许可证：任何环境

如下图所示，访问控制策略编辑器的 Rules 选项卡允许您添加、编辑、搜索、移动、启用、禁用、删除和以其他方式管理策略中的访问控制规则。



对于每个规则，策略编辑器显示其名称、条件概述、规则操作以及传达规则检测和日志记录选项的图标。其他图标表示注释、警告、错误和其他重要信息，如下表所述。被禁用的规则在规则名称下方呈灰色显示并带有相应的标记 (`disabled`)。

表 6-2　了解访问控制策略编辑器

图标	说明	您可以.....
	入侵检测	点击活动（黄色）检测图标编辑规则的检测选项；请参阅第 10-1 页上的使用入侵和文件策略控制流量。如果图标为非活动状态（白色），则没有为该规则选择此类型的策略。
	文件和恶意软件检测	
	日志记录	点击活动（蓝色）日志记录图标编辑规则的日志记录选项；请参阅第 25-8 页上的根据访问控制处理记录连接。如果图标为非活动状态（白色），则已为该规则禁用连接日志记录。
	注释	点击注释栏中的编号可向规则添加注释；请参阅第 6-9 页上的向规则添加注释。编号指示规则已包含的注释数。
	警告	在访问控制策略编辑器中，点击 **Show Warnings** 显示为策略列出所有警告的弹出窗口；请参阅第 4-12 页上的对访问控制策略和规则进行故障排除。
	错误	
	信息	

有关管理访问控制规则的信息，请参阅：

- 第 6-2 页上的创建和编辑访问控制规则
- 第 6-10 页上的搜索访问控制规则
- 第 6-11 页上的启用和禁用规则
- 第 6-11 页上的更改规则的位置或类别

搜索访问控制规则

许可证：任何环境

可以使用字母数字字符串（包括空格和可打印的特殊字符）在访问控制规则列表中搜索匹配值。搜索会检测规则名称和已添加至规则的任意规则条件。对于规则条件，搜索会匹配可以为每个条件类型（区域、网络、应用程序等）添加的任意名称或值。这包括各个对象名称或值、组对象名称、组内的各个对象名称或值以及文本值。

可以使用部分或完整的搜索字符串。对于每个匹配规则，匹配值列将会突出显示。例如，如果在所有或部分规则上搜索字符串 `100Bao`，已添加 100Bao 应用程序的每个规则的 Applications 列都会突出显示。如果有名为 100Bao 的规则，则 Name 和 Applications 列都会突出显示。

可以导航至每个上一个或下一个匹配规则。状态消息会显示当前的匹配项以及匹配项的总数量。

匹配可能会出现在多页规则列表的任意页面上。当第一个匹配项不在第一个页面上时，屏幕上将会显示第一个匹配项所在的页面。当您处于最后一个匹配项时，选择下一匹配项会使您到达第一个匹配项，当处于第一个匹配项时，选择上一匹配项会到达最后一个匹配项。

要搜索规则，请执行以下操作：

步骤 1　在想要搜索的策略的访问控制策略编辑器中，点击 **Search Rules** 提示信息，键入搜索字符串，然后按 Enter 键。还可以使用 Tab 键或点击空白页面区域来发起搜索。

带有匹配值的规则列会被突出显示，其突出显示方式与指示的 （第一个）匹配项不同。

步骤 2　查找感兴趣的规则：

- 要在匹配规则之间导航，可以点击下一匹配项 (▼) 或上一匹配项 (▲) 图标。
- 要刷新页面并清除搜索字符串和所有突出显示的内容，请点击清除图标 (✖)。

启用和禁用规则

许可证：任何环境

创建访问控制规则时，默认情况下启用规则。如果您禁用某规则，系统将不用该规则来评估网络流量并停止为该规则生成警告和错误。在查看访问控制策略中的规则列表时，禁用的规则会呈灰色显示，不过，您仍然可以修改它们。请注意，也可以使用规则编辑器启用或禁用访问控制规则；请参阅第 6-2 页上的创建和编辑访问控制规则。

要更改访问控制规则的状态，请执行以下操作：

步骤 1　在包含您要启用或禁用规则的策略的访问控制策略编辑器中，右键单击规则并选择规则状态：

- 要启用非活动规则，请选择 **State > Enable**。
- 要禁用活动规则，请选择 **State > Disable**。

步骤 2　点击 **Store FirePOWER Changes** 保存策略。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

更改规则的位置或类别

许可证：任何环境

为帮助您组织访问控制规则，每个访问控制策略都有三个系统提供的规则类别：管理员规则、标准规则和根规则。您不能移动、删除或重命名这些类别，但可以创建自定义类别。

有关详情，请参阅：

- 第 6-12 页上的移动规则
- 第 6-12 页上的添加新规则类别

移动规则

许可证：任何环境

适当的访问控制规则顺序可减少处理网络流量所需的资源并防止规则抢占。

以下步骤说明如何使用访问控制策略编辑器一次移动一个或多个规则。还可使用规则编辑器移动单个访问控制规则；请参阅第 6-2 页上的创建和编辑访问控制规则。

要移动规则，请执行以下操作：

步骤 1　在包含想要移动规则的策略的访问控制策略编辑器中，通过点击每个规则的空白区域选择规则。使用 Ctrl 和 Shift 键选择多个规则。

突出显示您选择的规则。

步骤 2　移动规则。可以剪切、粘贴或拖放规则。

要将规则剪切和粘贴到新位置，请右键单击选定规则并选择 **Cut**。然后，在想要粘贴所剪切规则的位置旁，右键单击规则的空白区域并选择 **Paste above** 或 **Paste below**。请注意，您不能在两个不同访问控制策略之间拷贝和粘贴访问控制规则。

步骤 3　点击 **Store FirePOWER Changes** 保存策略。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

添加新规则类别

许可证：任何环境

为帮助您组织访问控制规则，每个访问控制策略都有三个系统提供的规则类别：管理员规则、标准规则和根规则。尽管在标准规则和根规则之间创建自定义类，但是不能移动、删除或重命名这些类别。

添加自定义类别允许进一步组织规则，而无需创建额外的策略。可以重命名和删除添加的类别。不能移动这些类别，但可以将规则移入其中以及从中移出。

要添加新的类别，请执行以下操作：

步骤 1　在要添加规则类别的策略的访问控制策略编辑器中，点击 Add Category。

提示　如果您的策略已经包含规则，则可以点击现有规则在该行的空白区域，先设置新类别的位置，然后才能添加。还可以右键单击现有规则并选择 **Insert new category**。

屏幕上将会显示 Add Category 弹出窗口。

步骤 2　键入唯一的类别**名称**。

可以输入字母数字名称，包括空格和特殊的可打印字符，最多可有 30 个字符。

步骤 3　有以下选项可供选择：

- 要将新类别定位至紧靠现有类别上方的位置，从第一个 **Insert** 下拉列表中选择 **above Category**，然后从第二个下拉列表选择您想要在其上定位规则的类别。
- 如要将新的类别规则定位至现有规则之下，从下拉列表选择 **below rule**，然后输入现有规则编号。仅当策略中存在至少一个规则时，该选项才有效。

- 如要将规则定位至现有规则之上，从下拉列表选择 **above rule**，然后输入现有规则编号。仅当策略中存在至少一个规则时，该选项才有效。

步骤 4　点击**确定**。

您的类别已添加。可以点击自定义类别旁边的编辑图标 () 编辑其名称，或者点击删除图标 () 删除该类别。删除的类别中的规则将会添加至以上类别。

步骤 5　点击 **Store FirePOWER Changes** 保存策略。

使用基于网络的规则控制流量

*访问控制策略*内的*访问控制规则*可以对网络流量记录和处理进行精细的控制。基于网络的条件可供您使用以下一个或多个条件管理哪些流量可以穿越您的网络：

- 源和目标安全区域
- 源和目标 IP 地址或地理位置
- 源端口和目标端口，还包括传输层协议和 ICMP 代码选项

您可以相互整合基于网络的条件，或将其与其他类型的条件整合，以便创建访问控制规则。这些访问控制规则可能很简单，也可能很复杂，它使用多个条件来匹配和检查流量。有关访问控制规则的详细信息，请参阅第 6-1 页上的使用访问控制规则调整流量。

注 基于安全情报的流量过滤以及一些解码和预处理在访问控制规则评估网络流量**之前**发生。

表 7-1 基于网络的访问控制规则的许可证要求

要求	地理位置控制	所有其他基于网络的控制
许可证	任何	任何

有关构建基于网络的访问控制规则的信息，请参阅：

- 第 7-1 页上的按安全区域控制流量
- 第 7-3 页上的按网络或地理位置控制流量
- 第 7-4 页上的按端口和 ICMP 代码控制流量

按安全区域控制流量

许可证：任何

访问控制规则中的区域条件可供您，按流量的源和目标安全区域控制流量。*安全区域*是一个或多个接口的分组。

作为简单示例，可以创建两个区域：内部和外部，设备上的第一个接口对分配至这些区域。在内侧连接至网络的主机代表您的受保护资产。

要扩展此情景，您可以另行部署以相同方式配置的设备 以便保护多个不同位置中的类似资源。每台这些设备均会保护其内部安全区域中的资产。

提示　您不需要将所有内部（或外部）接口分组至单个区域。选择对您的部署和安全策略有意义的分组。有关创建区域的详细信息，请参阅第 2-30 页上的使用安全区域。

在此部署中，您可能决定，尽管想要这些主机无限制地访问互联网，但是，您想要通过检查入站流量是否存在入侵和恶意软件来保护它们。

要运用访问控制实现这一目标，请配置带有区域条件的访问控制规则，其中 **Destination Zone** 设置为 **Internal**。此简单访问控制规则匹配从内部区域中的任何接口离开设备的流量。

要确保系统检查匹配流量是否存在入侵和恶意软件，请选择规则操作 **Allow**，然后将该规则与入侵和文件策略相关联。有关详细信息，请参阅第 6-6 页上的使用规则操作确定流量处理和检测和第 10-1 页上的使用入侵和文件策略控制流量。

如果您想要构建更为复杂的规则，可以在单个区域条件中向每个 **Source Zones** 和 **Destination Zones** 添加最多 50 个区域：

- 要匹配从区域中的接口*离开*设备的流量，请将该区域添加至 **Destination Zones**。

  因为被动部署的设备不会传输流量，所以，您不能在 **Destination Zone** 条件中使用包含被动接口的区域。
- 要匹配从区域中的接口*进入*设备的流量，请将该区域添加至 **Source Zones**。
- 如果同时向一条规则添加源区域和目标区域条件，则匹配流量必须源自其中一个指定源区域**并**通过其中一个目标区域流出。

构建区域条件时，警告图标指明无效的配置。有关详细信息，第 4-12 页上的对访问控制策略和规则进行故障排除。

要按区域控制流量：

步骤 1　在将您的访问控制策略中，新建访问控制规则或编辑现有规则。

有关详细说明，请参阅第 6-2 页上的创建和编辑访问控制规则。

步骤 2　在规则编辑器中，选择 Zones 选项卡。

系统将显示 Zones 选项卡。

步骤 3　从 **Available Zones** 中查找并选择您想要添加的区域。

要搜索需要添加的区域，请点击 **Available Zones** 列表上方的 **Search by name** 提示，然后键入区域名称。该列表会在您键入内容时进行更新，以显示匹配的区域。

点击以选择区域。要选择多个区域，请使用 Shift 和 Ctrl 键，或者右键单击，然后选择 **Select All**。

步骤 4　点击 **Add to Source** 或 **Add to Destination**，以便将选定区域添加至适当列表。

您也可以拖放选定区域。

步骤 5　保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

按网络或地理位置控制流量

许可证：因功能而异

访问控制规则中的网络条件可供您按流量的源和目标 IP 地址控制流量。您可以：

- 显式指定想要控制的流量的源和目标 IP 地址，或者
- 使用地理位置功能，该功能将 IP 地址与地理位置关联，以便根据流量的源或目标国家/地区或大陆控制流量

当您构建基于网络的访问控制规则条件时，可以手动指定 IP 地址和地理位置。另外，您可以使用网络和地理位置*对象*配置网络条件，这些对象可重复使用，可以将名称与一个或多个 IP 地址、地址块、国家/地区、大陆等相关联。

提示 创建网络或地理位置对象后，您不仅可将其用于构建访问控制规则，还可以在系统的模块接口中的各种其他位置将其用于代表 IP 地址。您可以使用对象管理器来创建这些对象；您也可以在配置访问控制规则时动态创建网络对象。有关详细信息，请参阅第 2-1 页上的管理可重用对象。

请注意，如果您想要按地理位置编写规则来控制流量，以便确保您正在使用最新的地理位置数据来过滤流量，思科**强烈**建议您定期更新您的 ASA FirePOWER 模块上的地理位置数据库 (GeoDB)；请参阅第 35-17 页上的更新地理定位数据库。

表 7-2　网络条件要求

要求	地理位置控制	IP 地址控制
许可证	任何	任何

在单一网络条件中，您可以向每个 **Source Networks** 和 **Destination Networks** 最多添加 50 项，而且可以混用基于网络和基于地理位置的配置。

- 要匹配*来自* IP 地址或地理位置的流量，请配置 **Source Networks**。
- 要匹配*流向* IP 地址或地理位置的流量，请配置 **Destination Networks**。

如果同时向一条规则添加源网络条件和目标网络条件，则匹配流量必须源自其中一个指定 IP 地址**并**流向其中一个目标 IP 地址。

构建网络条件时，警告图标指明无效的配置。有关详细信息，第 4-12 页上的对访问控制策略和规则进行故障排除。

要按网络或地理位置控制流量：

步骤 1　在将您的访问控制策略中，新建访问控制规则或编辑现有规则。

有关详细说明，请参阅第 6-2 页上的创建和编辑访问控制规则。

步骤 2　在规则编辑器中，选择 Networks 选项卡。

系统将显示 Networks 选项卡。

步骤 3　从 **Available Networks** 中查找并选择您想要添加的网络，如下所示：

- 点击 Networks 选项卡，以显示要添加的网络对象和组；点击 Geolocation 选项卡，以显示地理位置对象。
- 要动态添加您随后可以添加至条件的网络对象，请点击 **Available Networks** 列表上方的添加图标 ()；请参阅。第 2-3 页上的使用网络对象

- 要搜索需要添加的网络或地理位置对象，请选择适当的选项卡，点击 **Available Networks** 列表上方的 **Search by name or value** 提示，然后键入对象名称或对象的其中一个组件的值。该列表会在您键入内容时进行更新，以显示匹配的对象。

要选择对象，请点击该对象。要选择多个对象，请使用 Shift 和 Ctrl 键，或者右键单击，然后选择 **Select All**。

步骤 4　点击 **Add to Source** 或 **Add to Destination**，以将选定对象添加至适当列表。

您也可以拖放选定对象。

步骤 5　添加您想要手动指定的任何源或者目标 IP 地址或地址块。

点击 **Source Networks** 或 **Destination Networks** 列表下方的 **Enter an IP address** 提示，然后键入 IP 地址或地址块，并点击 **Add**。

步骤 6　保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

按端口和 ICMP 代码控制流量

许可证：任何

访问控制规则中的网络条件可供您按流量的源和目标端口控制流量。在此情景下，“端口”是指以下其中一项：

- 对于 TCP 和 UDP，您可以根据传输层协议控制流量。系统使用括号内的协议号，以及可选的关联端口或端口范围来表示此配置。例如：TCP(6)/22。
- 对于 ICMP 和 ICMPv6 (IPv6-ICMP)，您可以根据其互联网层协议以及可选的类型和代码控制流量。例如：ICMP(1):3:3。
- 您可以借助于未使用端口的其他协议控制流量。

当您构建基于端口的访问控制规则条件时，您可以手动指定端口。此外，您可以使用端口*对象*配置端口条件，这些对象可重复使用，可将名称与一个或多个端口相关联。

提示　创建端口对象后，您不仅可将其用于构建访问控制规则，还可以在系统的模块接口中的各个其他位置将其用于代表端口。您可以使用对象管理器创建端口对象，也可以在配置访问控制规则时动态创建端口对象。有关详细信息，请参阅第 2-9 页上的使用端口对象。

在单一网络条件中，您可以向每个 **Selected Source Ports** 和 **Selected Destination Ports** 列表最多添加 50 项：

- 要匹配*来自*端口的流量，请配置 **Selected Source Ports**。

  如果仅将源端口添加至条件，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为源端口条件。

- 要匹配*流向*端口的流量，请配置 **Selected Destination Ports**。

  如果仅将目标端口添加至条件，则可以添加使用不同传输协议的端口。

- 要匹配即源自特定 **Selected Source Ports** *又*流向特定 **Selected Destination Ports** 的流量，请同时配置二者。

  如果同时将源和目标端口添加至条件，则只能添加共享单一传输协议 （TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

构建端口条件时，切记以下几点：

- 当您添加类型设置为 0 的目标 ICMP 端口或类型设置为 129 的目标 ICMPv6 端口时，访问控制规则仅与主动提供的回应回复相匹配。为应答 ICMP 回应请求而发送的 ICMP 回应回复被忽略。为使某个规则匹配任何 ICMP 回应，请使用 ICMP 类型 8 或 ICMPv6 类型 128。
- 当您将 GRE (47) 协议用作目标端口条件时，只能将基于网络的其他条件添加至访问控制规则，即区域和网络条件。如果您添加基于声誉或用户的条件，则无法保存规则。

构建端口条件时，警告图标指明无效的配置。例如，您可以使用对象管理器来编辑正在使用的端口对象，以使使用这些对象组的规则变得无效。有关详细信息，第 4-12 页上的对访问控制策略和规则进行故障排除。

要按端口控制流量：

步骤 1　在将您的访问控制策略中，新建访问控制规则或编辑现有规则。

有关详细说明，请参阅第 6-2 页上的创建和编辑访问控制规则。

步骤 2　在规则编辑器中，选择 Ports 选项卡。

系统将显示 Ports 选项卡。

步骤 3　从 **Available Ports** 中查找并选择您想要添加的端口，如下所示：

- 要动态添加您随后可以添加至条件的端口对象，请点击 Available Ports 列表上方的添加图标 ()；请参阅  。第 2-9 页上的使用端口对象
- 要搜索需要添加的端口对象和组，请点击 **Available Ports** 列表上方的 **Search by name or value** 提示，然后键入对象名称或对象中某一端口的值。该列表会在您键入内容时进行更新，以显示匹配的对象。例如，如果您键入 80， ASA FirePOWER 模块会显示思科提供的 HTTP 端口对象。

  要选择对象，请点击该对象。要选择多个对象，请使用 Shift 和 Ctrl 键，或者右键单击，然后选择 **Select All**。

步骤 4　点击 **Add to Source** 或 **Add to Destination**，以将选定对象添加至适当列表。

您也可以拖放选定对象。

步骤 5　添加您想要手动指定的任何源或目标端口。

- 对于源端口，请从 **Selected Source Ports** 列表下方的 **Protocol** 下拉列表选择 **TCP** 或 **UDP**。然后，键入 **Port**。您可以为单个端口指定从 0 到 65535 之间的一个值。
- 对于目标端口，请从 **Selected Destination Ports** 列表下方的 **Protocol** 下拉列表选择协议 （包括代表所有协议的 **All**）。您还可以键入未在列表中出现的未分配协议的编号。

  如果您选择 **ICMP** 或 **IPv6-ICMP**，则出现一个弹出窗口，您可以在其中选择类型和相关代码。有关 ICMP 类型和代码的详细信息，请参阅 http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml 和 http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml。

  如果您不想指定协议，或者如果您指定 TCP 或 UDP，请输入 **Port**。您可以为单个端口指定从 0 到 65535 之间的一个值。

点击 **Add**。请注意， ASA FirePOWER 模块不会将会导致无效配置的端口添加至规则条件。

步骤 6　保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

使用基于信誉的规则控制流量

*访问控制策略*中的*访问控制规则*对网络流量日志记录和处理进行精细控制。访问控制规则中的基于信誉的条件可用于确定网络流量的情景，并根据情况实施流量限制，从而帮助您控制可以穿越网络的流量。访问控制规则监管以下类型的基于信誉的控制：

- 应用条件可供您执行*应用控制*，此控制方法根据各个应用以及应用的基本特性（类型、风险、业务关联性、类别和标记）来控制应用流量。
- URL 条件可供您执行 *URL 过滤*，此控制方法根据各个网站以及系统对网站分配的类别和信誉来控制网络流量。

基于信誉的条件可以相互组合或与其他类型的条件组合，以创建访问控制规则。这些访问控制规则可能很简单，也可能很复杂，使用多个条件匹配和检查流量。有关访问控制规则的详细信息，请参阅第 6-1 页上的使用访问控制规则调整流量。

基于安全情报的流量过滤以及一些解码和预处理在访问控制规则评估网络流量**之前**发生。基于信誉的访问控制需要以下许可证

表 8-1　　基于信誉的访问控制规则的许可证要求

要求	应用控制	URL 过滤（类别 和信誉）	URL 过滤（手动）
许可证	可控性	URL 过滤	任意

有关向访问控制规则添加基于信誉的条件的信息，请参阅：

- 第 8-2 页上的控制应用流量
- 第 8-6 页上的阻止 URL

ASA FirePOWER 模块可以执行其他类型的基于信誉的控制，但是您无法使用访问控制规则配置这些控制类型。有关详细信息，请参阅：

- 第 5-1 页上的使用安全情报 IP 地址声誉设置黑名单说明如何根据连接的源或目标的信誉限制流量，来作为第一道防线。
- 第 10-5 页上的调整入侵防御性能说明如何检测、跟踪、存储、分析和阻止恶意软件及其他类型的受禁文件的传输。

控制应用流量

许可证：可控性

ASA FirePOWER 模块在分析 IP 流量时，可以识别网络上的常用应用并将其分类。

了解应用控制

访问控制规则中的应用条件可供您执行此*应用控制*。在单一访问控制规则中，有多种方法可以指定要接受流量控制的应用：

- 可以选择个别应用，包括自定义应用。
- 可以使用系统提供的*应用过滤器*，它们是根据应用的基本特性（类型、风险、业务关联性、类别和标记）组织的命名应用集。
- 可以创建和使用自定义应用过滤器，以您选择的任何方式对应用（包括自定义应用）进行分组。

应用过滤器可供您快速创建访问控制规则的应用条件。这些过滤器可简化策略创建和管理，并且保证系统将按预期控制网络流量。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务关联性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

此外，思科还通过系统和漏洞数据库 (VDB) 更新频繁更新和添加其他检测器。通过根据应用特性使用过滤器，可以确保系统使用最新的检测器来监控应用流量。

构建应用条件

在使用应用条件的情况下，流量要与访问控制规则相匹配，则必须与添加到 **Selected Applications and Filters** 列表的其中一个过滤器或应用相匹配。

在单一应用条件中，您最多可以向 **Selected Applications and Filters** 列表中添加 50 个项目。下列每项均视为一个项目：

- **Application Filters** 列表中的一个或多个过滤器（单独或自定义组合）。此项表示应用集（按特性分组）。
- 通过在 **Available Applications** 列表中保存应用搜索创建的过滤器。此项表示应用集 （按子字符串匹配分组）。
- **Available Applications** 列表中的每项应用。

在模块界面中，添加到条件中的过滤器会在独立添加的应用上方单独列出。

请注意，当应用访问控制策略时，对于包含应用条件的每条规则，系统均会生成要匹配的唯一应用的列表。换句话说，可以使用重叠过滤器和逐一指定的应用确保完整覆盖。

注　对于加密流量，系统可以仅使用标记有 **SSL 协议** 的应用识别和过滤流量。系统只会在流量中检测不带此标记的应用。

有关详细信息，请参阅：

- 第 8-3 页上的将流量与应用过滤器相匹配
- 第 8-3 页上的匹配来自个别应用的流量
- 第 8-4 页上的向访问控制规则中添加应用条件
- 第 8-5 页上的对应用控制的限制

将流量与应用过滤器相匹配

许可证：可控性

在访问控制规则中构建应用条件时，请使用 **Application Filters** 列表创建要匹配其流量的应用集（按特性分组）。

请注意，用于在访问控制规则中过滤应用的机制与用于通过对象管理器来创建可重复使用的自定义应用过滤器的机制相同；请参阅第 2-11 页上的使用应用过滤器。您还可以将在访问控制规则中动态创建的多个过滤器另存为新的可重复使用的过滤器。如果您的过滤器中包括其他用户创建的过滤器，则该过滤器无法保存，因为系统不允许嵌套用户创建的过滤器。

了解过滤器组合方式

选择过滤器时（单一或组合），**Available Applications** 列表会更新为仅显示符合条件的应用。可以选择系统提供的组合形式的过滤器，但不能选择自定义过滤器。

系统将同一类型的多个过滤器与 OR 操作关联。例如，如果您在 Risks 类型下选择 Medium 和 High 过滤器，则产生的过滤器为：

Risk: Medium OR High

如果 Medium 过滤器包含 110 个应用，High 过滤器包含 82 个应用，系统会在 **Available Applications** 列表中显示全部 192 个应用。

系统将不同类型的过滤器与 AND 操作关联。例如，如果您选择 Risks 类型下的 Medium 和 High 过滤器，以及 Business Relevance 类型下的 Medium 和 High 过滤器，则所生成的过滤器为：

Risk: Medium OR High
和
Business Relevance: Medium OR High

在此情况下，系统仅显示 Medium 或 High Risk 类型和 Medium 或 High Business Relevance 类型中均包含的应用。

查找和选择过滤器

要选择过滤器，请点击过滤器类型旁边的箭头以展开该类型，然后选择或清除要显示或隐藏其应用的每个过滤器旁边的复选框。您也可以右键单击系统提供的过滤器类型（**Risks**、**Business Relevance**、**Types**、**Categories** 或 **Tags**），然后选择 **Check All** 或 **Uncheck All**。

要搜索过滤器，请点击 **Available Filters** 列表上方的 **Search by name** 提示，然后键入名称。列表会在您键入内容时进行更新，以显示匹配的过滤器。

过滤器选择完毕，请使用 **Available Applications** 列表将这些过滤器添加到规则中；请参阅第 8-3 页上的匹配来自个别应用的流量。

匹配来自个别应用的流量

许可证：可控性

在访问控制规则中构建应用条件时，请使用 **Available Applications** 列表选择要进行流量匹配的应用。

浏览应用列表

首次开始构建条件时，该列表不受限制，并且显示系统检测的每个应用（一次 100 个）：

- 要翻页浏览应用，请点击列表下方的箭头。
- 要打开弹出窗口，显示有关应用特性的摘要信息以及可点选的互联网搜索链接，请点击应用旁边的信息图标 ( )。

查找要匹配的应用

为帮助查找要匹配的应用，您可以通过以下方式限制 **Available Applications** 列表：

- 要搜索应用，请点击列表上方的 **Search by name** 提示，然后键入名称。列表会在您键入内容时进行更新，以显示匹配的应用。
- 要通过应用过滤器来限制应用，请使用 **Application Filters** 列表（请参阅第 8-3 页上的将流量与应用过滤器相匹配）。**Available Applications** 列表在您应用过滤器时进行更新。

进行限制后，在 **Available Applications** 列表顶部会出现 **All apps matching the filter** 选项。通过此选项，可以将受限制列表中的所有应用一次性全部添加到 **Selected Applications and Filters** 列表。

注　如果您在 Application Filters 列表中选择一个或多个过滤器，并在这种状态下搜索 **Available Applications** 列表，系统会使用 AND 运算将您的选择与搜索过滤出的 **Available Applications** 列表进行组合。也就是说，**All apps matching the filter** 条件包括 **Available Applications** 列表中当前显示的所有个别条件以及在 **Available Applications** 列表上方输入的搜索字符串。

在条件中选择要匹配的单个应用

找到要匹配的应用，然后点击将其选定。要选择多个应用，请使用 Shift 和 Ctrl 键，或者右键单击并选择 **Select All** 以选择当前受限制视图中的所有应用。

在单个应用条件中，可以通过逐个选择应用来匹配最多 50 个应用；要添加 50 个以上的应用，必须创建多个访问控制规则或者使用过滤器将应用分组。

为条件选择与某个过滤器匹配的所有应用

通过搜索或使用 **Application Filters** 列表中的过滤器进行限制后，在 **Available Applications** 列表的顶部会出现 **All apps matching the filter** 选项。

通过此选项，可以将受限制 **Available Applications** 列表中的整个应用集一次性添加到 **Selected Applications and Filters** 列表。与单独添加应用的不同之处在于，无论应用集由多少个单独的应用构成，应用集都仅作为一项添加（按照最多 50 项计算）。

以此方式构建应用条件时，您添加到 **Selected Applications and Filters** 列表的过滤器名称会显示为一个串联字符串，其中包括该过滤器中代表的过滤器类型，每种类型后会最多显示三个过滤器名称。若同一类型的过滤器超过三个，则会显示省略号 (...)。例如，以下过滤器名称包括 Risks 类型下的两个过滤器，包括 Business Relevance 类型下的四个过滤器：

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

使用 **All apps matching the filter** 添加的过滤器中未代表的过滤器类型，将不会包含在所添加的过滤器名称中。这些过滤器类型设置为 *any*；也就是说，这些过滤器类型不限制过滤器，因此允许对这些过滤器使用任何值。

可以向应用条件中添加 **All apps matching the filter** 的多个实例，其中每个实例计为 **Selected Applications and Filters** 列表中的单独项。例如，可以将所有高风险应用添加为一项，然后清除选择，再将所有低业务关联性应用添加为另一项。此应用条件会匹配风险高或业务关联性低的应用。

向访问控制规则中添加应用条件

许可证：可控性

在使用应用条件的情况下，流量要与访问控制规则相匹配，则必须与添加到 **Selected Applications and Filters** 列表的其中一个过滤器或应用相匹配。

每个条件最多可以添加 50 项，并且添加到条件中的过滤器列出在上方并与逐个添加的应用分隔开来。构建应用条件时，无效的配置会以警告图标加以指示。有关详细信息，请参阅第 4-12 页上的对访问控制策略和规则进行故障排除。

要控制应用流量，请执行以下操作：

步骤 1　在确定您的访问控制策略中，创建新的访问控制规则或编辑现有规则。

有关详细说明，请参阅第 6-2 页上的创建和编辑访问控制规则。

步骤 2　在规则编辑器中，选择 Applications 选项卡。

系统将显示 Applications 选项卡。

步骤 3　作为可选操作，您可以使用过滤器限制 **Available Applications** 列表中显示的应用列表。

选择 **Application Filters** 列表中的一个或多个过滤器。有关详细信息，请参阅第 8-3 页上的将流量与应用过滤器相匹配。

步骤 4　从 **Available Applications** 列表查找并选择要添加的应用。

可以搜索并选择个别应用，或者在列表受限制时，选择 **All apps matching the filter**。有关详细信息，请参阅第 8-3 页上的匹配来自个别应用的流量。

步骤 5　点击 **Add to Rule** 以将所选应用添加到 **Selected Applications and Filters** 列表。

您也可以拖放所选应用和过滤器。过滤器会显示在标题 *Filters* 下，应用显示在标题 *Applications* 下。

提示　在将其他过滤器添加到此应用条件中之前，请点击 **Clear All Filters** 以清除现有选择。

步骤 6　或者，点击 **Selected Applications and Filters** 列表上方的添加图标 ( ) 以保存由列表中当前包含的所有个别应用和过滤器组成的自定义过滤器。

使用对象管理器管理此动态创建的过滤器；请参阅第 2-11 页上的使用应用过滤器。请注意，无法保存包括另一用户创建的过滤器的过滤器，因为不能嵌套用户创建的过滤器。

步骤 7　保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

对应用控制的限制

许可证：可控性

执行应用控制时，请谨记以下要点。

应用识别的速度

在满足以下条件之前，系统无法执行应用控制：

- 客户端和服务器之间建立受监控连接，并且
- 系统识别会话中的应用

此识别应在 3 到 5 个数据包内发生。如果第一批数据包中的其中之一与包含应用条件的访问控制规则中的所有其他条件相匹配，但是识别未完成，则访问控制策略允许数据包通过。此行为允许建立连接，以便可以识别应用。为便于识别，受影响的规则会以信息图标 ( ) 标记。

允许的数据包通过访问控制策略的*默认*入侵策略（既不是*默认操作*入侵策略也不是近乎匹配规则的入侵策略）进行检查。有关详细信息，请参阅第 13-1 页上的为访问控制设置默认入侵策略。

在系统完成其识别后，系统会将访问控制规则操作以及任何关联入侵策略与文件策略应用于与其应用条件相匹配的剩余会话流量。

处理加密流量

系统可以识别和过滤通过使用 StartTLS（如 SMTPS、POPS、FTPS、TelnetS 和 IMAPS）进行加密的未加密应用流量。此外，系统还可以根据 TLS 客户端问询消息中的服务器名称指示或服务器证书主题专有名称值来识别某些加密应用。

这些应用标记为 **SSL 协议**。系统只会在的流量中检测不带此标记的应用。

处理无负载的应用流量数据包

对于在用于应用识别的连接中没有负载的数据包，系统会应用默认策略操作。

处理推荐流量

要创建用于处理网络服务器所推荐的流量（如广告流量）的规则，请为被推荐应用（而非推荐应用）添加条件。

控制使用多个协议的应用流量 (Skype)

系统可以检测多个类型的 Skype 应用流量。构建用于控制 Skype 流量的应用条件时，请从 **Application Filters** 列表中选择 **Skype** 标记，而非选择个别应用。这确保系统可以相同方式检测和控制所有 Skype 流量。有关详细信息，请参阅第 8-3 页上的将流量与应用过滤器相匹配。

阻止 URL

许可证：因功能而异

访问控制规则中的 URL 条件可供您限制网络上用户能够访问的网站。此功能称为 *URL 过滤*。使用访问控制指定要阻止（或者允许）的 URL 有两种方法：

- 通过任何许可证，可以手动指定个别 URL 或 URL 组来实现对网络流量的精细、自定义控制。
- 通过 URL 过滤许可证，还可以根据 URL 的一般分类或*类别*以及风险级别或*信誉*控制对网站的访问。系统在连接日志、入侵事件和应用详细信息中显示此类别和信誉数据。

注　要查看事件中的 URL 类别和信誉信息，必须至少创建一条具有 URL 条件的访问控制规则。

当阻止网站时，可以允许用户浏览器的默认行为，也可以显示系统提供的通用页面或自定义页面。您还可以让用户能够通过点击忽略警告页面来绕过对网站的阻止。

表 8-2　URL 过滤的许可证要求

要求	基于类别和信誉	手动
许可证	URL 过滤	任何

有关详细信息，请参阅：

- 第 8-7 页上的执行基于信誉的 URL 阻止
- 第 8-8 页上的执行手动 URL 阻止
- 第 8-10 页上的对 URL 检测和阻止的限制
- 第 8-10 页上的允许用户绕过 URL 阻止
- 第 8-12 页上的显示受阻 URL 的自定义网页

执行基于信誉的 URL 阻止

许可证：URL 过滤

通过 URL 过滤许可证，可以根据所请求的 URL 类别和信誉（ASA FirePOWER 模块从思科云获取）控制用户对网站的访问：

- URL *类别*是 URL 一般分类。例如， ebay.com 属于 **Auctions** 类别，而 monster.com 属于 **Job Search** 类别。 URL 可以属于多个类别。
- URL *信誉*表示 URL 会被用于可能违反组织安全策略之用途的可能性。 URL 的风险范围可从 **High Risk** （第 1 级）到 **Well known** （第 5 级）。

注 要使具有基于类别和信誉的 URL 条件的访问控制规则生效，**必须**先启用与思科云的通信。这样，ASA FirePOWER 模块才能检索 URL 数据。有关详细信息，请参阅第 33-6 页上的启用云通信。

基于信誉的 URL 阻止的优点

URL 类别和信誉可供您快速创建访问控制规则的 URL 条件。例如，可以创建用于识别和阻止 **Abused Drugs** 类别中所有 **High Risk** URL 的访问控制规则。如果用户尝试浏览至任何包含该类别和信誉组合的 URL，会话将被阻止。

使用思科云中的类别和信誉数据还会简化策略创建和管理。此方法可保证系统将按预期控制网络流量。最后，由于云会不断更新有关新 URL 以及现有 URL 的新类别和新风险的信息，因此可以确保系统使用最新信息来过滤所请求的 URL。代表安全威胁 （如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的恶意站点出现和消失的速度可能比您更新和应用新策略的速度要快。

一些示例包括：

- 如果规则阻止所有游戏站点，则在新的域注册并分类为 **Gaming** 时，系统可以自动阻止这些站点。
- 如果规则阻止所有恶意软件站点，当某个博客页面受到恶意软件感染时，云可以将该 URL 从 **Blog** 重新分类为 **Malware**，以便系统可以阻止该站点。
- 如果规则阻止高风险的社交网站，并且某人在其包含指向恶意负载的链接的简档页面发布链接，则云可以将该页面的信誉从 **Benign sites** 更改为 **High Risk**，这样系统即可阻止该网站。

请注意，如果云不知道 URL 的类别或信誉，或者，如果 ASA FirePOWER 模块无法联系云，则该 URL **不会**触发具有基于类别和信誉的 URL 条件的访问控制规则。您无法手动向 URL 分配类别或信誉。

构建 URL 条件

在一个 URL 条件中，您最多可以向 **Selected URLs** 中添加 50 个要匹配的项。每个 URL 类别（或者按信誉进行限定）计为一项。请注意，也可以在 URL 条件中使用文本 URL 和 URL 对象，但是不能使用信誉来限定这些项。有关详细信息，请参阅第 8-8 页上的执行手动 URL 阻止。

请注意，不能使用信誉来限定文本 URL 或 URL 对象。

构建 URL 条件时，警告图标指明无效的配置。有关详细信息，参阅第 4-12 页上的对访问控制策略和规则进行故障排除。

要使用类别和信誉数据控制所请求的 URL 的流量，请执行以下操作：

步骤 1　在确定您的访问控制策略中，创建新的访问控制规则或编辑现有规则。

有关详细说明，请参阅第 6-2 页上的创建和编辑访问控制规则。

步骤 2　在规则编辑器中，选择 URLs 选项卡。

系统将显示 URLs 选项卡。

步骤 3　从 **Categories and URLs** 列表查找并选择要添加的 URL 的类别。要不区分类别匹配网络流量，请选择 **Any** 类别。

要搜索需要添加的类别，请点击 **Categories and URLs** 列表上方的 **Search by name or value** 提示，然后键入类别名称。列表会在您键入内容时进行更新，以显示匹配的类别。

要选择类别，请点击该类别。要选择多个类别，请使用 Shift 和 Ctrl 键。

提示　虽然可以右键单击并**选择所有**类别，但是以此方式添加所有类别会超过访问控制规则的最大项数限制（50 项）。请改用 **Any**。

步骤 4　作为可选操作，您可以点击 **Reputations** 列表中的信誉级别来限定类别选择。如果不指定信誉级别，则系统默认为 **Any**（表示所有级别）。

只能选择一个信誉级别。选择信誉级别时，访问控制规则的行为会根据其目的而有所不同：

- 如果规则阻止或监控网络访问（规则操作为 **Block**、**Block with reset**、**Interactive Block**、**Interactive Block with reset** 或 **Monitor**），则选择信誉级别还会选择严重性超过该级别的所有信誉。例如，如果将规则配置为阻止或监控 **Suspicious sites**（第 2 级），则其还会自动阻止或监控 **High risk**（第 1 级）站点。
- 如果规则允许网络访问，则无论是信任网络访问还是对网络访问进一步执行检查（规则操作为 **Allow** 或 **Trust**），选择信誉级别还会选择严重性低于该级别的所有信誉。例如，如果您将规则配置为允许 **Benign sites**（第 4 级），系统还会自动允许 **Well known**（第 5 级）站点。

如果更改规则的规则操作，系统根据上述几点自动更改 URL 条件中的信誉级别。

步骤 5　点击 **Add to Rule** 或拖放选定项以将其添加到 **Selected URLs** 列表。

步骤 6　保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

执行手动 URL 阻止

许可证：任意

要按类别和信誉补充或选择性覆盖 URL 过滤，可以通过手动指定个别 URL 或 URL 组来控制网络流量。借此可以实现对允许和阻止的网络流量的精细、自定义控制。您也可以在没有特殊许可证的情况下执行此类型的 URL 过滤。

要手动指定将在访问控制规则中允许或阻止的 URL，可以键入单个文本 URL。或者，可以使用 URL 对象配置 URL 条件，这些条件可重复使用并将名称与 URL 或 IP 地址相关联。

提示　创建 URL 对象后，不仅可以将其用于构建访问控制规则，还可以在系统的模块接口中的各种其他位置表示 URL。可以使用对象管理器创建这些对象，也可以在配置访问控制规则时动态创建 URL 对象。有关详细信息，请参阅第 2-10 页上的使用 URL 对象。

在 URL 条件中手动指定 URL

虽然手动输入可以对允许或阻止的网络流量进行精确控制，但是不能使用信誉来限定手动指定的 URL。此外，还必须确保规则不会产生意外后果。要确定网络流量是否与 URL 条件相匹配，系统执行简单的子字符串匹配。如果 URL 对象或手动键入的 URL 的值与受监控主机所请求的 URL 的任何部分相匹配，系统将认为满足访问控制规则的 URL 条件。

因此，当在 URL 条件中（包括在 URL 对象中）手动指定 URL 时，请仔细考虑可能受影响的其他流量。例如，如果您允许到 example.com 的所有流量，用户可以浏览的 URL 将包括：

- http://example.com/
- http://example.com/newexample
- http://www.example.com/

再例如，请考虑要明确阻止 ign.com（游戏站点）的情景。但是，子字符串匹配意味着阻止 *ign.com* 也会阻止 veris*ign.com*，这可能并非您的意愿。

手动阻止加密的网络流量

访问控制规则中的 URL 条件：

- 忽略网络流量的加密协议（HTTP 与 HTTPS）

  例如，访问控制规则会对访问 http://example.com/ 的流量和访问 https://example.com/ 的流量采用相同的处理方式。要配置仅与 HTTP 或 HTTPS 流量匹配的访问控制规则，请向该规则添加应用条件。有关详细信息，请参阅第 8-6 页上的阻止 URL。

- 根据用于加密流量的公钥证书中的主题公用名来匹配 HTTPS 流量，并且忽略主题公用名中的子域

  手动过滤 HTTPS 流量时，请勿包含子域信息。

构建 URL 条件时，警告图标指明无效的配置。有关详细信息，请参阅第 4-12 页上的对访问控制策略和规则进行故障排除。

要通过手动指定需要允许或阻止的 URL 来控制网络流量，请执行以下操作：

步骤 1　在确定您的访问控制策略中，创建新的访问控制规则或编辑现有规则。

有关详细说明，请参阅第 6-2 页上的创建和编辑访问控制规则。

步骤 2　在规则编辑器中，选择 URLs 选项卡。

系统将显示 URLs 选项卡。

步骤 3　从 **Categories and URLs** 列表查找并选择要添加的 URL 对象和组：

- 要动态添加 URL 对象（之后可以添加到条件中），请点击 **Categories and URLs** 列表上方的添加图标 ( )；请参阅第 2-10 页上的使用 URL 对象。
- 要搜索需要添加的 URL 对象和组，请点击 **Categories and URLs** 列表上方的 **Search by name or value** 提示，然后键入对象的名称或者对象中 URL 或 IP 地址的值。列表会在您键入内容时进行更新，以显示匹配的对象。

要选择对象，请点击该对象。要选择多个对象，请使用 Shift 和 Ctrl 键。虽然可以右键单击并**选择所有** URL 对象和类别，但是以此方式添加 URL 会超过访问控制规则的最大值 （50 项）。

步骤 4　点击 **Add to Rule** 以将选定项添加到 **Selected URLs** 列表中。

您也可以拖放选定项。

步骤 5　添加要手动指定的任何文本 URL。**不能**在此字段中使用通配符 (*)。

点击 **Selected URLs** 列表下方的 **Enter URL** 提示；然后键入 URL 或 IP 地址并点击 **Add**。

步骤 6　保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

对 URL 检测和阻止的限制

许可证：任何环境

执行 URL 检测和阻止时，请谨记以下要点。

URL 识别的速度

在满足以下情况之前，系统无法过滤 URL：

- 客户端与服务器之间建立受监控连接
- 系统识别会话中的 HTTP 或 HTTPS 应用
- 系统识别所请求的 URL（对于加密会话，则为客户端问询消息或服务器证书中的 URL）

此识别应在 3 到 5 个数据包内发生。如果第一批数据包中的其中之一与包含 URL 条件的访问控制规则中的所有其他条件匹配，但是识别未完成，则访问控制策略允许该数据包通过。此行为允许建立连接，以便可以识别 URL。为便于识别，受影响的规则会以信息图标 ( ) 标记。

允许的数据包通过访问控制策略的*默认*入侵策略（既不是*默认操作*入侵策略也不是近乎匹配规则的入侵策略）进行检查。有关详细信息，请参阅第 13-1 页上的为访问控制设置默认入侵策略。

在系统完成其识别后，系统会将访问控制规则操作以及任何关联的入侵策略与文件策略应用于与其 URL 条件匹配的剩余会话流量。

处理加密的网络流量

在使用具有 URL 条件的访问控制规则评估加密的网络流量时，系统会遵循以下原则：

- 忽略加密协议；如果访问控制规则具有 URL 条件但不具有指定该协议的应用条件，则该规则将采用同样的方式处理 HTTPS 和 HTTP 流量
- 根据用于加密流量的公钥证书中的主题公用名与 HTTPS 流量相匹配，并且忽略主题公用名中的子域
- 不显示 HTTP 响应页面，即使已配置该页面也如此

在 URL 中搜索查询参数

系统不使用 URL 中的搜索查询参数来匹配 URL 条件。例如，考虑这样一个场景：您阻止所有购物流量。在这种情况下，系统不会阻止使用网络搜索来搜索 amazon.com，但会阻止浏览至 amazon.com。

允许用户绕过 URL 阻止

许可证：任何环境

使用访问控制规则阻止用户的 HTTP Web 请求时，将规则操作设置为 **Interactive Block** 或 **Interactive Block with reset**，即可允许用户通过点击忽略带有警告的 *HTTP 响应页面*来绕过阻止操作。可以显示系统提供的通用响应页面，也可以输入自定义 HTML。

默认情况下，系统允许用户绕过阻止 10 分钟（600 秒），而不会针对用户的后续访问操作显示警告页面。可以将持续时间设置为长达一年，也可以强制用户每次都绕过阻止。

如果用户不绕过阻止，系统会拒绝匹配流量而不执行进一步检查。此外，您也可以重置连接。另一方面，如果用户绕过阻止，则系统允许流量。允许此流量意味着可以继续检查未加密负载（确定是否存在入侵、恶意和被禁止的文件）。请注意，用户在绕过阻止后可能必须刷新才能加载未加载的页面元素。

请注意，将交互式 HTTP 响应页面与为“阻止”规则配置的响应页面分开进行配置。例如，可以向在无交互情况下其会话被阻止的用户显示系统提供的页面，但是向可以点击以继续操作的用户显示自定义页面。有关详细信息，请参阅第 8-12 页上的显示受阻 URL 的自定义网页。

提示　要在访问控制策略中快速禁用对所有规则的交互式阻止，则既不要显示系统提供的页面，也不要显示自定义页面。这样一来，系统就会在不提供交互机会的情况下阻止与“交互式阻止”规则匹配的所有连接。

要允许用户绕过网站阻止，请执行以下操作：

步骤 1　创建将网络流量与 URL 条件相匹配的访问控制规则。

请参阅第 8-7 页上的执行基于信誉的 URL 阻止和第 8-8 页上的执行手动 URL 阻止。

步骤 2　确保访问控制规则操作为 **Interactive Block** 或 **Interactive Block with reset**。

请参阅第 6-6 页上的使用规则操作确定流量处理和检测。

步骤 3　假设用户将绕过阻止并相应地选择规则的检查和日志记录选项。与 Allow 规则一样：

- 可以将任一类型的“交互式阻止”规则与文件和入侵策略相关联。有关详细信息，请参阅第 10-1 页上的使用入侵和文件策略控制流量。
- 以交互方式阻止的流量的日志记录选项与允许的流量的日志记录选项相同，但请记住，如果用户不绕过交互式阻止，则系统只能记录连接开始事件。

  请注意，在系统最初警告用户时，它会使用重置操作以 Interactive Block 或 Interactive Block 标记任何已记录的连接开始事件。如果用户绕过阻止，则为会话记录的其他连接事件具有 Allow 操作。有关详细信息，请参阅第 25-8 页上的根据访问控制处理记录连接。

步骤 4　或者，设置用户绕过阻止后且系统再次显示警告页面前所耗用的时间量。

请参阅第 8-11 页上的为受阻网站设置用户绕过超时。

步骤 5　或者，创建并使用要显示的自定义页面来允许用户绕过阻止。

请参阅第 8-12 页上的显示受阻 URL 的自定义网页。

为受阻网站设置用户绕过超时

许可证：任何环境

默认情况下，系统允许用户绕过交互式阻止 10 分钟 （600 秒），而在后续访问时不显示警告页面。可以将持续时间设置为长达一年，或者设置为零以强制用户每次都绕过阻止。此设置适用于策略中的每条“交互式阻止”规则。不能对每条规则都设置限制。

要自定义用户绕过到期之前的时间长度，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要配置的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略的高级设置。

步骤 4　点击 General Settings 旁边的编辑图标 ( )。

系统将显示 General Settings 弹出窗口。

步骤 5　在 **Allow an Interactive Block to bypass blocking for (seconds)** 字段中，键入用户绕过到期之前必须经过的秒数。

可以指定从零到 31536000 （一年）的任何秒数。指定零会强制用户每次都绕过阻止。

步骤 6　点击**确定**。

系统将显示访问控制策略的高级设置。

步骤 7　点击 **Store ASA FirePOWER Changes**。

只有应用访问控制策略才能使更改生效。有关详细信息，请参阅第 4-10 页上的应用访问控制策略。

显示受阻 URL 的自定义网页

许可证：任何环境

当系统阻止用户的 HTTP Web请求时，该用户在浏览器中看到的内容取决于如何使用访问控制规则的操作来阻止会话。您应该选择：

- **Block** 或 **Block with reset** 以拒绝连接。被阻止的会话将会超时；系统重置 Block with reset 连接。但是，对于两种阻止操作，均可使用说明连接已被拒绝的自定义页面来覆盖默认浏览器或服务器页面。系统将此自定义页面称为 *HTTP 响应页面*。
- **Interactive Block** 或 **Interactive Block with reset**（如果要显示 *交互式 HTTP 响应页面*来警告页面，但又允许其点击按钮以继续操作或者刷新页面以加载最初请求的站点）。用户在绕过响应页面后可能必须刷新才能加载未加载的页面元素。

可以显示系统提供的通用响应页面，也可以输入自定义 HTML。当输入自定义文本时，计数器将会显示已使用的字符的数量。

在每个访问控制策略中，您将交互式 HTTP 响应页面与用于在无交互情况下阻止流量（也就是说，使用“阻止”规则）的响应页面分开配置。例如，可以向在无交互情况下其会话被阻止的用户显示系统提供的页面，但是向可以点击以继续操作的用户显示自定义页面。

HTTP 响应页面向用户的可靠显示取决于页面的网络配置、流量负载和大小。如果构建自定义响应页面，请记住，较小的页面更可能成功显示。

要配置 HTTP 响应页面，请执行以下操作：

步骤 1　编辑的访问控制策略。

有关详细信息，请参阅第 4-7 页上的编辑访问控制策略。

步骤 2　选择 HTTP Responses 选项卡。

系统将显示访问控制策略的 HTTP 响应页面设置。

步骤 3　对于 **Block Response Page** 和 **Interactive Block Response Page**，从下拉列表选择响应。对于每个页面，有以下选项可供选择：

- 要使用通用响应，请选择 **System-provided**。可以点击查看图标 () 以查看此页面的 HTML 代码。
- 要创建自定义响应，请选择 **Custom**。

  系统将显示一个弹出窗口，其中预先填充有系统提供的可以替换或修改的代码。完成时，保存更改。请注意，可以通过点击编辑图标 () 来编辑自定义页面。
- 要防止系统显示 HTTP 响应页面，请选择 **None**。请注意，为以交互方式阻止的会话选择此选项可防止用户点击以继续操作；会话将在无交互的情况下被阻止。

步骤 4　点击 **Store ASA FirePOWER Changes**。

只有应用访问控制策略才能使更改生效。有关详细信息，请参阅第 4-10 页上的应用访问控制策略。

根据用户控制流量

*访问控制策略*中的*访问控制规则*对网络通信记录和处理进行精细控制。访问控制规则的用户条件可供您执行*用户控制* - 通过根据登录主机的 LDAP 用户限制流量来管理哪些流量可以穿越网络。

用户控制通过将*访问受控的用户*与 IP 地址相关联来实现。系统监控指定用户登录和注销主机或因其他原因对 Active Directory 凭证进行身份验证。例如，贵组织可能s使用依赖于 Active Directory 进行集中身份验证的服务或应用。

要使流量与具有用户条件的访问控制规则相匹配，必须将受监控会话中的源或目标主机的 IP 地址与登录的访问受控的用户相关联。您可以根据单个用户或这些用户所属的组来控制流量。

您可以将用户条件相互组合或与其他类型的条件组合来创建访问控制规则。这些访问控制规则可能是简单或复杂的，使用多个条件匹配和检查流量。有关访问控制规则的详细信息，请参阅第 6-1 页上的使用访问控制规则调整流量。

注 在访问控制规则对网络流量进行评估**之前**，会出现基于安全智能的流量过滤及一些解码和预处理。

用户控制需要可控性许可证并且仅受 LDAP 用户和组（访问受控用户）支持。

用户感知功能可使所有部署类型确定“谁”在执行“什么操作”。例如，您可以确定：

- 谁正在尝试未授权访问具有高主机重要性的服务器
- 谁正在耗用异常大量的带宽
- 谁尚未应用关键操作系统更新
- 谁正在使用即时消息软件或 P2P 文件共享应用，而这样做是违反公司的 IT 策略的
- 谁拥有作为入侵事件的目标的主机
- 谁发起了内部攻击或端口扫描（需要保护）

借助这些信息，可以采用有针对性的方法降低风险，以及采取措施防止中断他人的活动。用户控制增强了阻止 LDAP 用户和用户活动的能力。用户感知功能和控制功能共同显著改进了审计控制并增强了合规性。

下表列出了对用户感知和控制的要求

表 9-1 用户感知和控制要求

要求	用户感知	用户控制
许可证一致	任何环境	可控性
用于用户元数据检索的 LDAP 服务器	Windows Server 2003 和 Windows Server 2008 上的 Microsoft Active Directory （用户控制所必需的）	

有关详情，请参阅：

- 第 9-2 页上的向访问控制规则添加用户条件
- 第 9-3 页上的检索访问受控用户和 LDAP 用户元数据

向访问控制规则添加用户条件

许可证： 可控性

ASA FirePOWER 模块的用户控制功能通过将访问受控的用户与主机 IP 地址相关联来发挥作用。要使流量与具有用户条件的访问控制规则相匹配，必须将受监控会话中的源或目标主机的 IP 地址与登录的访问受控的用户相关联。

您必须配置 ASA FirePOWER 模块与 Microsoft Active Directory 服务器之间的连接，然后才能执行用户控制；请参阅第 9-3 页上的检索访问受控用户和 LDAP 用户元数据。

注意事项 如果您配置大量要监控的用户组，或者，如果您有非常多的用户映射到网络中的主机，由于内存限制，系统可能会丢弃基于用户组的用户映射。因此，基于用户组的访问控制规则可能无法如预期那样触发。

最多只能将 50 个用户和组添加到单个用户条件中的 **Selected Users**。带有用户组的条件与该组任何成员（包括任何子组的成员，个别排除的用户和排除的子组的成员除外）的往返流量相匹配。

注 系统必须在该组中检测到至少一个用户的活动，然后您才能使用组条件执行用户控制。此初始连接不由其匹配的访问控制规则处理，而是由其匹配的下一个规则或访问控制策略默认操作处理。

构建用户条件时，警告图标表示无效配置。有关详细信息，请参阅第 4-12 页上的对访问控制策略和规则进行故障排除。

要控制用户流量，请执行以下步骤：

步骤 1 在访问控制策略中，新建访问控制规则或编辑现有规则。

有关详细说明，请参阅第 6-2 页上的创建和编辑访问控制规则。

步骤 2 在规则编辑器中，选择 Users 选项卡。

系统将显示 Users 选项卡。

步骤 3 从 **Available Users** 列表查找并选择要添加的用户和组。

用户和组标记有不同的图标。要搜索要添加的用户和组，点击 **Available Users** 列表上方的 **Search by name or value** 提示，然后键入用户或组的名称。列表会在您键入内容时进行更新，以显示匹配的项目。

要选择一个项目，请点击该项目。要选择多个项目，请使用 Shift 和 Ctrl 键，或点击右键并选择 **Select All**。

步骤 4 点击 **Select All** 可将选定的用户和组添加到 **Selected Users** 列表。

也可以拖放选定的用户和组。

步骤 5 保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

检索访问受控用户和 LDAP 用户元数据

功能而异

如果要执行用户控制（即，编写包含用户条件的访问控制规则），必须配置 ASA FirePOWER 模块与贵组织的至少一个 Microsoft Active Directory 服务器之间的连接。ASA FirePOWER 模块定期和自动查询 LDAP 服务器以更新访问受控用户的元数据，访问受控用户指以及您在限制流量时可以用作条件的用户和组。

有关详情，请参阅：

- 第 9-3 页上的连接到用于用户感知和控制的 LDAP 服务器
- 第 9-6 页上的按需更新用户控制参数
- 第 9-6 页上的暂停与 LDAP 服务器的通信
- 第 9-7 页上的使用用户代理报告 Active Directory 登录

连接到用于用户感知和控制的 LDAP 服务器

许可证： FireSIGHT或可控性

ASA FirePOWER 模块与贵组织的 LDAP 服务器之间的连接可以：

- 指定您在使用访问控制规则限制流量时可用作条件的访问受控用户和组。
- 可供您查询服务器上有关访问受控用户和一些非访问受控用户的元数据

这些连接或*用户感知对象*，指定 LDAP 服务器的连接设置和身份验证过滤器设置 。

要执行用户控制，您**必须**连接到一个 Microsoft Active Directory LDAP 服务器。如果只希望检索 LDAP 用户元数据，系统支持与其他类型的 LDAP 服务器的连接；请参阅第 9-1 页上的表 9-1。

当系统检测到用户活动时，它可以将该用户的记录添加到 ASA FirePOWER 模块用户。 ASA FirePOWER 模块定期查询 LDAP 服务器，以获取自上次查询以来检测到其活动的新的和已更新用户的元数据。对于已存在于用户数据库中的用户，如果其元数据在过去 12 小时里没有更新，将会为其更新元数据。系统检测到新用户登录后， ASA FirePOWER 模块更新用户元数据可能需要几分钟时间。

注　即使您从 LDAP 服务器移除系统检测到的用户， ASA FirePOWER 模块也**不会**移除该用户；您必须手动删除。但是，在ASA FirePOWER 模块下一次更新访问受控用户列表时， LDAP 更改**会**反映在访问控制规则中。

下表列出了可与受监控用户相关联的 LDAP 元数据。请注意，要成功从 LDAP 服务器检索用户元数据，服务器**必须**使用此表中列出的 LDAP 字段名称。如果在 LDAP 服务器上重命名该字段，ASA FirePOWER 模块将无法使用该字段中的信息来填充其用户列表。

表 9-2　　将 LDAP 字段映射到思科字段

元数据	ASA FirePOWER 模块	Active Directory
LDAP 用户名	用户名	samaccountname
first name	名字	givenname
last name	姓氏	sn

表 9-2　　将 LDAP 字段映射到思科字段 （续）

元数据	ASA FirePOWER 模块	Active Directory
email address	电子邮件	邮件 userprincipalname （如果 mail 没有值）
department	部门	department distinguishedname （如果 department 没有值）
电话号码	电话	telephonenumber

与您的 LDAP 管理员密切协作，确保正确配置 LDAP 服务器，您可以连接到这些服务器并获取在创建 LDAP 连接时必须提供的信息。

服务器类型、 IP 地址和端口

必须为主要（或者备用）LDAP 服务器指定、IP 地址或主机名和端口。您**必须**使用 Microsoft Active Directory LDAP 服务器。

LDAP 特定参数

在 ASA FirePOWER 模块搜索 LDAP 服务器以检索身份验证服务器上的用户信息时，它需要该搜索的起点。可以通过提供基本识别名称（或*基础 DN*）来指定要搜索的*命名空间*或目录树。通常，基础 DN 具有指示公司领域和运营单位的基础结构。例如，Example 公司的 Security 部门的基础 DN 可能为 `ou=security,dc=example,dc=com`。请注意，识别主服务器之后，可以从该服务器自动检索可用基础 DN 列表并选择相应的基础 DN。

必须为对于您要检索的用户信息具有适当权限的用户提供用户凭证。请记住，您指定的用户识别名称对于目录服务器的目录信息树必须是唯一的。

还可以为 LDAP 连接指定加密方法。请注意，如果使用证书进行身份验证，证书中 LDAP 服务器的名称**必须**与在 ASA FirePOWER 模块界面中指定的主机名相匹配。例如，如果在配置 LDAP 连接时使用 `10.10.10.250`，而不是证书中的 `computer1.example.com`，连接将会失败。

最后，必须指定超时持续时间，超过该时间后，尝试联系无响应 LDAP 服务器的行为将会回滚为备份连接。

用户和组访问控制参数

要执行用户控制，请指定要在访问控制规则中用作条件的组。

包含某个组即会自动包含该组的所有成员（包括任何子组的成员）。但是，如果要在访问控制规则中使用子组，必须明确包含要使用的子组。还可排除组和单个用户。排除某个组将会排除该组的所有成员，即使用户是包含的组的成员。

如果访问控制参数范围太宽泛， ASA FirePOWER 模块会尽可能获取有关更多用户的信息，并报告无法在任务队列中检索的用户数。

注　如果没有指定要包含的任何组，系统将会检索与您提供的 LDAP 参数匹配的所有组的用户数据。出于性能方面的考虑，思科建议您仅明确包含代表要在访问控制中使用的用户的组。请注意，**不能**包含用户或域用户组。

还必须指定ASA FirePOWER 模块查询 LDAP 服务器以获取要在访问控制中使用的新用户的频率。

在创建 LDAP 连接后，点击删除图标 ( ) 并确认选择，即可将其删除。要修改 LDAP 连接，请点击编辑图标 ( )。启用连接后，保存的更改将在 ASA FirePOWER 模块下一次查询 LDAP 服务器时生效。

要为用户感知和用户控制创建 LDAP 连接，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Users**。

系统将显示 Users Policy 页面。

步骤 2　点击 **Add LDAP Connection**。

系统将显示 Create User Awareness Authentication Object 页面。

步骤 3　在 **Name** 和 **Description** 字段中为对象键入名称和描述。

步骤 4　您**必须**使用 Microsoft Active Directory LDAP **服务器类型**。

步骤 5　**IP Address** 或 **Host Name** 中为主 LDAP 服务器指定 IP 地址或主机名（如有需要，也可以为备份 LDAP 服务器指定这两项）。

步骤 6　在 **Port** 中指定 LDAP 服务器用于身份验证流量的端口。

步骤 7　在 **Base DN** 中为要访问的 LDAP 目录指定基础 DN。

例如，要对示例公司的安全组织中的名称进行身份验证，请键入 `ou=security,dc=example,dc=com`。

提示　要获取完整的可用域列表，请点击 **Fetch DNs**，并从下拉列表中选择相应的基本识别名称。

步骤 8　在 **User Name** 和 **Password** 字段中指定要用于验证 LDAP 目录的访问权限的识别用户名和密码。确认密码。

步骤 9　在 **Encryption** 中选择加密方法。如在使用加密，则可添加 **SSL Certificate**。

证书中的主机名**必须**与在第 4 步中指定的 LDAP 服务器的主机名匹配。

步骤 10　在 **Timeout** 中指定超时持续时间（以秒为单位），超过该时间后，尝试联系无响应 LDAP 服务器的行为将会回滚为备份连接。

步骤 11　或者，在指定对象的用户感知设置之前，点击 **Test** 测试连接。

步骤 12　或者，启用 **User/Group Access Control Parameters** 以指定要在访问控制中使用的用户。

步骤 13　点击 **Fetch Groups**，以使用提供的 LDAP 参数填充可用组列表。

步骤 14　通过使用左箭头和右箭头按钮包含和排除组，从而指定要在访问控制中使用的用户。

包含某个组即会自动包含该组的所有成员（包括任何子组的成员）。但是，如果要在访问控制规则中使用子组，必须明确包含要使用的子组。排除某个组将会排除该组的所有成员，即使用户是包含的组的成员。

步骤 15　在 **User Exclusions** 中指定任何特定用户排除。

排除用户可防止您将用户作为条件编写访问控制规则。使用逗号分隔多个用户。还可以在此字段中使用星号 (*) 作为通配符。

步骤 16　指定想要查询 LDAP 服务器以获取新用户和组信息的频率。

默认情况下， ASA FirePOWER 模块每天午夜查询一次服务器：

- 使用 **Start At** 下拉列表指定希望查询发生的时间。 **0** 代表午夜， **1** 代表凌晨 1 点，等等。
- 使用 **Update Interval** 下拉列表指定查询服务器的频率（以小时为单位）。

步骤 17　点击 **Save**。

如果添加或更改了用户和组访问控制参数，请确认是否要应用所做的更改。系统将保存对象，并再次显示 Users Policy 页面。

步骤 18　点击您刚创建的连接旁边的滑块启用该连接。

如果要启用连接并且连接具有用户和组访问控制参数，请选择是否希望立即查询 LDAP 服务器以获取用户和组信息。请注意，如不立即查询 LDAP 服务器，查询将会在预定时间进行。可以在任务队列中监控任何查询的进度 (**Monitoring > ASA FirePOWER Monitoring > Task Status**)。

按需更新用户控制参数

许可证： 可控性

如果更改 LDAP 连接中的用户和组访问控制参数，或者如果更改 LDAP 服务器上的用户或组且您想要更改立即可用于用户控制，则可强制 ASA FirePOWER 模块从 Active Directory 服务器执行按需用户数据检索。

如果 LDAP 连接中的访问控制参数范围太宽泛， ASA FirePOWER 模块会尽可能获取有关更多用户的信息，并报告无法在任务队列中检索的用户数。

要执行按需用户数据检索，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Users**。

系统将显示 Users Policy 页面。

步骤 2　在要用于查询 LDAP 服务器的 LDAP 连接旁边，点击下载图标 ( )。

查询开始。可以在任务队列中监控其进度 (**Monitoring > ASA FirePOWER Monitoring > Task Status**)。

暂停与 LDAP 服务器的通信

功能而异

只有已启用的 LDAP 连接才能使 ASA FirePOWER 模块查询 LDAP 服务器。要停止查询，可以暂时禁用 LDAP 连接，而无需删除这些连接。

当您重新启用用于访问控制的 LDAP 连接时，可以强制 ASA FirePOWER 模块立即查询服务器获取更新的用户和组信息，或者也可以等到预定的首次查询出现。

要禁用或重新启用 LDAP 连接，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Users**。

系统将显示 Users Policy 页面。

步骤 2　点击您刚创建的连接旁边的滑块，可暂停或重新启用该连接。

如在重新启用连接并且连接具有用户和组访问控制参数，请选择是否想要立即查询 LDAP 服务器以获取用户和组信息。如不立即查询 LDAP 服务器，查询将会在预定时间进行。可以在任务队列中监控任何查询的进度 (**Monitoring > ASA FirePOWER Monitoring > Task Status**)。

使用用户代理报告 Active Directory 登录

许可证： 可控性

在 Microsoft Windows 计算机上部署的用户代理可以监控 Microsoft Active Directory 服务器，然后在贵组织中的 LDAP 用户登录和注销主机，或由于其他原因使用 Active Directory 凭证进行身份验证时通知 ASA FirePOWER 模块。例如，贵组织可能使用依赖于 Active Directory 进行集中身份验证的服务或应用。

此代理报告的信息将作为用户控制的基础。要使流量与具有用户条件的访问控制规则相匹配，必须将受监控会话中的源或目标主机的 IP 地址与登录的访问受控的用户相关联。您可以根据单个用户或这些用户所属的组来控制流量。

注 如要执行用户控制，**必须**安装并使用用户代理。但是，用户代理仅报告与 Active Directory 身份验证相关的用户活动。用户感知功能可供您查看所有代理报告的用户活动，以及在允许的网络流量中检测到的其他活动。

要通过用户代理为用户感知或控制检索 LDAP 用户身份验证，首先请将每个 ASA FirePOWER 模块配置为允许来自代理的连接。在高可用性部署中，应同时在主要 ASA FirePOWER 模块和辅助 ASA FirePOWER 模块上启用代理通信。在 ASA FirePOWER 模块上启用用户代理通信之后，可以在 Windows 计算机上安装代理。

最后，将用户代理配置为接受来自 Microsoft Active Directory 服务器的数据并将该信息报告给 ASA FirePOWER 模块。您也可以将代理配置为从报告中排除特定用户名和 IP 地址，并记录状态消息到本地事件日志或 Windows 应用程序日志。

要将 ASA FirePOWER 模块配置为连接到用户代理，请执行以下操作：

步骤 1 选择 **Configuration > ASA FirePOWER Configuration > Policies > Users**。

系统将显示 Users Policy 页面。

步骤 2 点击 **Add User Agent**。

系统将显示 Add User Agent 弹出窗口。

步骤 3 键入代理的**名称**。

步骤 4 键入计划要安装代理的计算机的**主机名或地址**。**必须**使用 IPv4 地址；不能将 ASA FirePOWER 模块配置为使用 IPv6 地址连接到用户代理。

步骤 5 点击 **Add User Agent**。

ASA FirePOWER 模块现可连接到所指定计算机上的用户代理。要删除连接，请点击删除图标 ( ) 并确认删除。

步骤 6 在指定的计算机上安装用户代理。将其配置为接受来自 Microsoft Active Directory 服务器的数据并将该信息报告给 ASA FirePOWER 模块。

有关最新详细信息，请参阅《*用户代理配置指南*》。请注意，在配置用户代理时，ASA FirePOWER 模块具有与防御中心相同的角色。因此，例如，当您配置到 ASA FirePOWER 模块的连接时，只需创建到防御中心的连接并提供 ASA FirePOWER 模块的信息，就如果它是防御中心。

使用入侵和文件策略控制流量

入侵策略和文件策略在 FireSIGHT 系统共同发挥作用，作为允许流量到达其目的地之前的最后一道防线。

- **入侵策略**监管系统的入侵防御功能；请参阅第 11-1 页上的了解网络分析和入侵策略。
- **文件策略**监管系统的基于网络的文件控制和高级恶意软件防护 (AMP) 功能；请参阅第 24-4 页上的了解和创建文件策略。

基于安全情报的流量过滤（黑名单）、以及流量解码和预处理均发生在检测网络流量是否存在入侵、受禁文件和恶意软件**之前**。访问控制规则和访问控制默认操作决定哪些流量由入侵和文件策略检测。

通过将入侵策略或文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略和/或文件策略检测流量。

入侵防御和 AMP 要求您启用特定许可功能，如下表所述。

表 10-1　　入侵和文件检测的许可证要求

特性	说明	许可证
入侵预防	检测和选择性阻止入侵和漏洞	保护
文件控制	检测和选择性阻止文件类型传输	保护
高级恶意软件防护 (AMP)	检测、跟踪和选择性阻止恶意软件传输	恶意软件

有关检测流量中是否存在入侵、受禁文件和恶意软件的详细信息，请参阅：

- 第 10-2 页上的检测允许流量是否存在入侵和恶意软件
- 第 10-5 页上的调整入侵防御性能
- 第 10-15 页上的调整文件和恶意软件检测性能和存储

检测允许流量是否存在入侵和恶意软件

许可证：保护或恶意软件

入侵和文件策略监管系统的入侵防御、文件控制和 AMP 功能，是允许流量到达其目的地之前的最后一道防线。基于安全情报的流量过滤、解码和预处理以及访问控制规则选择均发生在入侵和文件检测**之前**。

通过将入侵策略或文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略和/或文件策略检测流量。访问控制规则条件可能很简单，也可能很复杂；您可以通过安全区域、网络或地理位置、端口、应用、请求的 URL 和用户控制流量。

系统按您指定的顺序将流量与访问控制规则相匹配。在大多数情况下，系统根据其*所有*条件均与流量匹配的*第一条*访问控制规则处理网络流量。访问控制规则的*操作*决定系统如何处理匹配流量。您可以（不一定需要进一步检测）监控、信任、阻止或允许匹配流量；请参阅第 6-6 页上的使用规则操作确定流量处理和检测。

请注意，Interactive Block 规则与 Allow 规则有相同的检测选项。因此，您可以在用户通过点击警告页面绕过已阻止网页时检测流量是否存在恶意内容。有关详细信息，请参阅第 6-7 页上的 Interactive Blocking 操作：允许用户绕过网站拦截。

不符合中任何非监控访问控制规则的流量将通过默认操作来处理。请注意，系统可能检测默认操作允许的流量是否存在入侵，而不是检测其是否存在受禁文件或恶意软件。您**无法**将文件策略与访问控制默认操作相关联。

注　有时，当访问控制策略分析某条连接时，系统必须处理该连接中的头几个数据包，**从而让其通过**，然后才能确定哪个访问控制规则（如有）将处理流量。因此，这些数据包不会未经检测就到达其目的地，您可以使用称为默认入侵策略的入侵策略对其进行检测并生成入侵事件。有关详细信息，请参阅第 13-1 页上的为访问控制设置默认入侵策略。

有关上述情景的更多信息以及如何将文件和入侵策略与访问控制规则和访问控制默认操作相关联的说明，请参阅：

- 第 10-2 页上的了解文件和入侵检测顺序
- 第 10-3 页上的配置访问控制规则以执行 AMP 或文件控制
- 第 10-4 页上的配置访问控制规则以执行入侵防御
- 第 4-4 页上的为网络流量设置默认的处理和检查

了解文件和入侵检测顺序

许可证：保护或恶意软件

注　可检测入侵防御或默认操作允许的流量是否存在入侵，但不能检测其是否存在受禁文件或恶意软件。您**无法**将文件策略与访问控制默认操作相关联。

您不必在同一规则中同时执行文件和入侵检测。对于符合 Allow 或 Interactive Block 规则的连接：

- 没有文件策略，数据流取决于入侵策略
- 没有入侵策略，数据流取决于文件策略

提示　系统不会对受信任的流量执行任何种类的检测。

对由访问控制规则处理的任何单条连接，文件检测均发生在入侵检测之前。也就是说，系统不检测文件策略所阻止的文件是否存在入侵。在文件检测中，基于类型的简单阻止优先于恶意软件检测和阻止。

注　文件在会话中得以检测和阻止之前，来自该会话的数据包均可能接受入侵检测。

例如，请考虑按照访问控制规则中所定义通常要允许特定网络流量的情况。但是，作为预防措施，您希望阻止下载可执行文件，检测恶意软件的已下载的 PDF 并阻止找到的所有实例，然后对流量执行入侵检测。

您可以使用与自己想要暂时允许通过的流量的特征相匹配的规则创建访问控制策略，然后将其与入侵策略和文件策略相关联。文件策略阻止所有可执行文件的下载，也可检测和阻止包含恶意软件的 PDF：

- 首先，系统根据文件策略中指定的简单类型匹配阻止所有可执行文件的下载。由于这些文件会被立即阻止，因此，其既不接受恶意软件云查找也不接受入侵检测。
- 接着，系统对下载到网络主机的 PDF 执行恶意软件云查找。具有恶意软件文件性质的任何 PDF 均被阻止，且不接受入侵检测。
- 最后，系统使用与访问控制规则关联的入侵策略检测任何剩余流量，包括文件策略未阻止的文件。

配置访问控制规则以执行 AMP 或文件控制

许可证：保护或恶意软件

访问控制策略可能有多个与文件策略相关联的访问控制规则。您可以为任何 Allow 或 Interactive Block 访问控制规则配置文件检测，这样，您就可在网络中不同类型的流量到达其最终目的地之前，将不同的文件和恶意软件检测配置文件与其匹配。

当系统根据文件策略中的设置检测到受禁文件（包括恶意软件）时，会自动将事件记录。如果您不想记录文件或恶意软件事件，则可按每条访问控制规则禁用此日志记录功能。将文件策略与访问控制规则相关联之后，清除访问控制规则编辑器 Logging 选项卡上的 **Log Files** 复选框。有关详细信息，请参阅第 25-6 页上的为允许的连接禁用文件和恶意软件事件日志记录。

无论调用访问控制规则的日志记录配置如何，系统均会将关联连接的末端记录；请参阅第 25-2 页上的与文件和恶意软件事件关联的连接（自动）。

要将文件策略与访问控制规则相关联，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要使用访问控制规则配置 AMP 或文件控制所在的访问控制策略旁的编辑图标 ( )。

步骤 3　新建一条规则或编辑现有规则；请参阅第 6-2 页上的创建和编辑访问控制规则。

系统将显示访问控制规则编辑器。

步骤 4　确保规则操作设置为 **Allow**、 **Interactive Block** 或 **Interactive Block with reset**。

步骤 5　选择 Inspection 选项卡。

系统将显示 Inspection 选项卡。

步骤 6　选择 **File Policy** 检测与访问控制规则相匹配的流量，或选择 **None** 禁用匹配流量的文件检测。

可以点击显示的编辑图标 ( )，在编辑策略；请参阅第 24-8 页上的创建文件策略。

步骤 7　点击 **Add** 保存规则。

您的规则保存成功。只有保存和应用访问控制策略才能使更改生效；请参阅第 4-10 页上的应用访问控制策略。

配置访问控制规则以执行入侵防御

许可证：保护

访问控制策略可能有多个与入侵策略相关联的访问控制规则。您可以为任何 Allow 或 Interactive Block 访问控制规则配置文件检测，这样，您就可在网络中不同类型的流量到达最终目的地之前，使不同的入侵检测配置文件与其匹配。

每当系统使用入侵策略评估流量，它均可使用关联的*变量集*。变量集中的变量代表通常在入侵规则中用来识别源 IP 地址、目标 IP 地址、源端口和目标端口的值。您还可以使用入侵策略中的变量表示规则抑制和动态规则状态中的 IP 地址。

提示　即使您使用系统提供的入侵策略，思科**仍强烈**建议您配置系统的入侵变量以准确反映您的网络环境。至少，修改默认变量集中的默认变量；请参阅第 2-13 页上的优化预定义默认变量。

虽然您可以将不同的入侵策略-变量集对与每条 Allow 和 Interactive Block（以及默认操作）相关联，但是，如果目标设备没有足够的资源可按照配置执行检测，则无法应用访问控制策略。有关详细信息，请参阅第 4-13 页上的简化规则以便提高性能。

了解系统提供的入侵策略和自定义入侵策略

思科提供带有 ASA FirePOWER 模块的多种入侵策略。通过使用系统提供的入侵策略，您可以借鉴思科漏洞研究团队 (VRT) 的经验。对于这些策略，VRT 设置入侵和预处理程序规则状态，并提供高级设置的初始配置。您可以按原样使用系统提供的策略，也可以将其作为基础构建自定义策略。构建自定义策略可以提高系统在您的环境中的性能，并提供网络上发生的恶意流量和策略违规行为的集中视图。

除了您创建的自定义策略之外，系统还提供两种自定义策略：初始内联策略和初始被动策略。这两种入侵策略使用“平衡安全性和连接”入侵策略作为其基础。两者之间的唯一区别在于其 **Drop When Inline** 设置，该设置在内联策略中启用删除行为，在被动策略中禁用删除行为。有关详细信息，请参阅第 11-6 页上的比较系统提供的策略与自定义策略。

连接和入侵事件日志记录

在访问控制规则调用的入侵策略检测到入侵时，它会入侵事件。不管访问控制规则的日志记录配置如何，系统还可将入侵发生所在连接的末端记录；请参阅第 25-2 页上的与入侵关联的连接（自动）。

要将入侵策略与访问控制规则相关联，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要使用访问控制规则配置入侵检测所在的访问控制策略旁的编辑图标 ( )。

步骤 3　新建一条规则或编辑现有规则；请参阅第 6-2 页上的创建和编辑访问控制规则。

系统将显示访问控制规则编辑器。

步骤 4　确保规则操作设置为 **Allow**、 **Interactive Block** 或 **Interactive Block with reset**。

步骤 5　选择 Inspection 选项卡。

系统将显示 Inspection 选项卡。

步骤 6　选择系统提供的入侵策略或自定义**入侵策略**，或选择 **None** 禁用对与访问控制规则相匹配的流量进行的入侵检测。

如果选择自定义入侵策略，则可点击显示的编辑图标 ( )，在编辑该策略；请参阅第 19-4 页上的编辑入侵策略。

注意事项　请勿选择 `Experimental Policy 1`，除非思科代表指示这样做。思科使用该策略进行测试。

步骤 7　或者，更改与入侵策略相关联的**变量集**。

可以点击显示的编辑图标 ( )，在编辑变量集；请参阅第 2-13 页上的使用变量集。

步骤 8　点击 **Save** 保存规则。

您的规则保存成功。只有保存和应用访问控制策略才能使更改生效；请参阅第 4-10 页上的应用访问控制策略。

调整入侵防御性能

许可证：保护

思科提供了多项功能，用于提高系统在分析流量中入侵企图时的性能。可以基于每个访问控制策略配置这些性能设置，他们可应用于该父访问控制策略调用的所有入侵策略。

有关详情，请参阅：

- 第 10-6 页上的限制入侵的模式匹配介绍如何指定事件队列中允许的数据包数量，以及如何针对将重新构造为较大数据流的数据包启用或禁用检测。
- 第 10-6 页上的覆盖入侵规则的正则表达式限制介绍如何覆盖 Perl 兼容正则表达式 (PCRE) 的默认匹配和递归限制。
- 第 10-7 页上的限制每个数据包生成的入侵事件介绍如何配置规则处理事件队列的设置。
- 第 10-8 页上的配置数据包和入侵规则延迟阈值介绍在需要通过数据包和规则延迟阈值将设备延迟保持在可接受水平时如何平衡安全性。
- 第 10-14 页上的配置入侵性能统计数据日志记录介绍如何配置基本性能监控和报告参数。

限制入侵的模式匹配

许可证：保护

您可以指定事件队列中允许的数据包数量。您还可以在数据流重组前后，启用或禁用对将重建到更大数据流中的数据包进行的检测。

要配置事件队列设置，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Performance Settings** 旁的编辑图标 ( )，然后在出现的弹出窗口中选择 **Pattern Matching Limits** 选项卡。

步骤 5　可修改以下选项：

- 在 **Maximum Pattern States to Analyze Per Packet** 字段中键入要排队的最多事件数量的值。
- 要对在数据流重组前后将重建到更大数据流中的数据包执行检测，请选择 **Disable Content Checks on Traffic Subject to Future Reassembly**。重组前后的检测需要更多的处理开销，可能会导致性能下降。
- 要禁用对在数据流重组前后将重建到更大数据流中的数据包执行的检测，请清除 **Disable Content Checks on Traffic Subject to Future Reassembly**。禁用检测会减少数据流插件检测的处理开销，并可提高性能。

步骤 6　点击**确定**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 4-10 页上的应用访问控制策略。

覆盖入侵规则的正则表达式限制

许可证：保护

可以覆盖入侵规则中使用的 PCRE 默认匹配和递归限制以检测数据包负载内容。有关在入侵规则中使用 `pcre` 关键字的详细信息，请参阅第 23-32 页上的使用 PCRE 搜索内容。默认限制可确保最低水平的性能。覆盖这些限制可能会提高安全性，但也会因允许根据低效的正则表达式对数据包进行评估而严重影响性能。

注意事项　除非在撰写入侵规则方面很有经验，并且了解衰减模式的影响，否则，不要覆盖默认的 PCRE 限制。

下表介绍在覆盖默认限制时可配置的选项。

表 10-2　正则表达式约束选项

选项	说明
Match Limit State	指定是否覆盖 **Match Limit**。您有以下选项： • 选择 **Default**，以使用为 **Match Limit** 配置的值 • 选择 **Unlimited**，以允许不限次数的尝试 • 选择 **Custom**，为 **Match Limit** 指定 1 或更大的值，或指定 0 以彻底禁用 PCRE 匹配评估
Match Limit	指定在与 PCRE 正则表达式中定义的模式进行匹配时的尝试次数。
Match Recursion Limit State	指定是否覆盖 **Match Recursion Limit**。您有以下选项： • 选择 **Default**，以使用为 **Match Recursion Limit** 配置的值 • 选择 **Unlimited**，以允许进行次数不限的递归 • 选择 **Custom**，为 **Match Recursion Limit** 指定 1 或更大的值，或指定 0 以彻底禁用 PCRE 递归 注意：为使 **Match Recursion Limit** 具有意义，其值必须小于 **Match Limit**。
Match Recursion Limit	指定在根据数据包静载荷对 PCRE 正则表达式进行评估时的递归次数。

要配置 PCRE 覆盖，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Performance Settings** 旁的编辑图标 ( )，然后在出现的弹出窗口中选择 Regular Expression Limits 选项卡。

步骤 5　可以修改正则表达式约束选项表中的任一选项。

步骤 6　点击**确定**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 4-10 页上的应用访问控制策略。

限制每个数据包生成的入侵事件

许可证：保护

当规则引擎根据规则评估流量时，它会将针对给定的数据包或数据包流生成的事件放在事件队列中，然后将队列顶部的事件报告至用户界面。可选择使规则引擎在生成多个事件时为每个数据包或数据包流记录多个事件。记录这些事件之后，就可收集除已报告事件之外的相关信息。配置此选项时，可指定队列中可放置的事件数量及要记录的事件的数量，并可选择队列中事件顺序的确定条件。

下表介绍在确定为每个数据包或数据流记录的事件数量时可配置的选项。

表 10-3　入侵事件日志记录限制选项

选项	说明
Maximum Events Stored Per Packet	为给定数据包或数据包流可存储的最多事件数量。
Maximum Events Logged Per Packet	为给定数据包或数据包流记录的事件数量。这不能超过 **Maximum Events Stored Per Packet** 的值。
Prioritize Event Logging By	该值用于确定事件队列中事件排序方法。排序最高的事件通过用户界面进行报告。有以下选项可供选择： • `priority`，按事件的优先级对队列中的事件进行排序。 • `content_length`，按识别出的最长匹配内容对事件进行排序。当事件按内容长度排序时，规则事件始终优先于解码器和预处理程序事件。

要配置为每个数据包或数据包流记录的事件数量，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Performance Settings** 旁的编辑图标 ( )，然后在出现的弹出窗口中选择 **Intrusion Event Logging Limits** 选项卡。

步骤 5　可以修改入侵事件日志记录限制选项表中的任一选项。

步骤 6　点击**确定**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 4-10 页上的应用访问控制策略。

配置数据包和入侵规则延迟阈值

许可证：保护

可以在需要通过数据包和规则延迟阈值将设备延迟保持在可接受水平时平衡安全性。有关详情，请参阅：

了解数据包延迟阈值

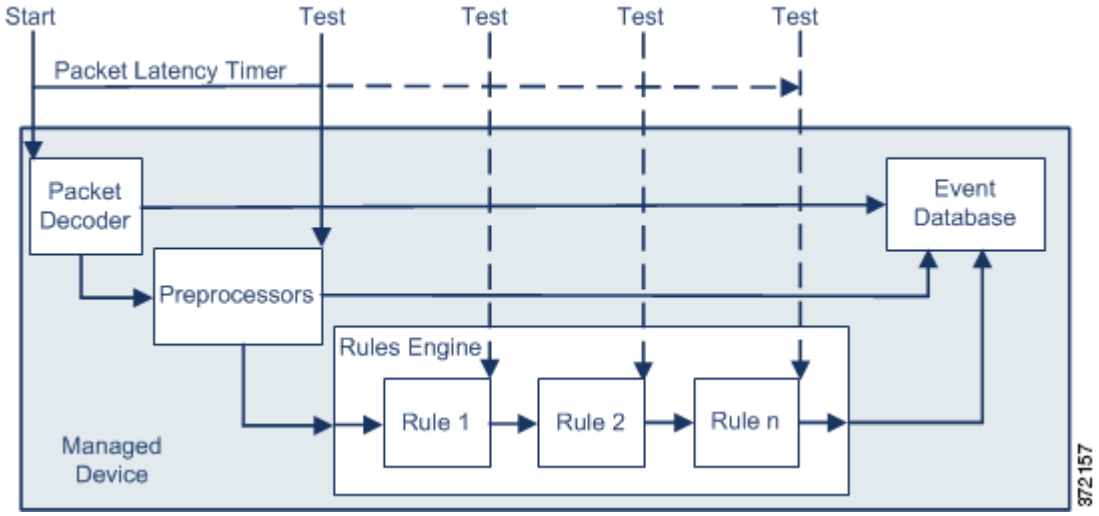
许可证：保护

可在需要将设备延迟保持在可接受水平时平衡安全性，只需启用数据包延迟阈值。数据包延迟阈值用于度量适用的解码器、预处理程序和规则在处理数据包时所需的总时间，并在处理时间超过可配置阈值时停止对数据包的检测。

数据包延迟阈值度量所需时间，而不仅是处理时间，目的是为了更准确地反映规则在处理数据包时实际所需的时间。然而，延迟阈值功能是基于软件实现的延迟管理功能，并不能实施严格的定时功能。

延迟阈值的得失分别为：实现性能和延迟优势的同时，也会导致未经检测的数据包可能包含攻击。但是，数据包延迟阈值提供的工具可用于平衡安全性与连接性。

解码器处理开始时，每个数据包的计时器开始计时。计时器会持续计时，直到数据包的所有处理工作结束或处理时间在计时测试点超过阈值。



如上图所示，数据包延迟计时在以下测试点测试：

- 在所有解码器和预处理程序的处理完成之后且在规则处理开始之前
- 在每条规则的处理之后

如果处理时间在任何测试点超出阈值，数据包检测将停止。

提示　总的数据包处理时间不包括常规的 TCP 数据流或 IP 分片重组时间。

对于由处理数据包的解码器、预处理程序或规则所触发的事件，数据包延迟阈值不会对其产生影响。只有当数据包已完全处理完毕，或当数据包处理因超过了延迟阈值而终止时（以先出现者为准），任何适用的解码器、预处理程序或规则才会触发事件。如果丢弃规则在内联部署中检测到入侵，则丢弃规则将触发事件并将数据包丢弃。

注　只有当数据包的处理因超出数据包延迟阈值而停止后，才会根据规则评估数据包。本可触发事件的规则无法触发该事件，同时，丢弃规则无法丢弃该数据包。

有关丢弃规则的详细信息，请参阅第 20-17 页上的设置规则状态。

数据包延迟阈值功能对被动式部署和内嵌式部署的性能均有提升作用，并且可以停止检测需要大量处理时间的数据包，从而降低延迟。例如，这些性能优势可以在以下情形中发挥出来：

- 对于被动和内联式部署，多个规则依序检测一个数据包需要过长的时间
- 对于内联式部署，网络性能不佳（例如，当有人下载超大文件时）期间，数据包处理变慢。

在被动式部署中，停止数据包的处理可能无助于恢复网络性能，这是因为，只不过转至处理下一数据包而已。

配置数据包延迟阈值

许可证：保护

下表介绍了在配置数据包延迟阈值时可设置的选项。

表 10-4　　数据包延迟阈值 选项

选项	说明
Threshold (microseconds)	指定数据包检测停止的时间，以微秒为单位。有关所建议的最小阈值设置，请参阅最小数据包延迟阈值设置表。

可启用规则 134:3，这样，当系统因超过数据包延迟阈值而停止检测数据包时可生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

很多因素影响系统性能和数据包延迟，如 CPU 速度、数据速率、数据包大小和协议类型。因此，思科建议您使用下表中的阈值设置，直到您计算出了适合自己的网络环境的设置。

表 10-5　　最小数据包延迟阈值设置

针对此数据速率...	将阈值（微秒）设置为至少...
1 Gbps	100
100 Mbps	250
5 Mbps	1000

计算设置时请确定：

- 每秒的平均数据包数
- 每个数据包所需的平均微秒数

将网络中每个数据包所需的平均微秒数乘以一个较大的安全因子，以确保不必要地中止数据包检测。

例如，最小数据包延迟阈值设置表建议 1 G 环境中的最小数据包延迟阈值应为 100 微秒。此建议的最小阈值所依据的测试数据为每秒平均 250,000 个数据包，即每微秒 0.25 个数据包，或每个数据包用时 4 微秒。乘以因子 25 即得出建议的最小阈值 100 微秒。

要配置数据包延迟阈值，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Latency-Based Performance Settings** 旁的编辑图标 ( )，然后在出现的弹出窗口中选择 Packet Handling 选项卡。

步骤 5　有关所建议的最小**阈值**设置，请参阅最小数据包延迟阈值设置表。

步骤 6　点击**确定**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 4-10 页上的应用访问控制策略。

了解规则延迟阈值

许可证：保护

可在需要将设备延迟保持在可接受水平时平衡安全性，只需启用规则延迟阈值。规则延迟阈值功能可以衡量每个规则处理各个数据包所花费的时间、将超过阈值的规则及一系列相关规则暂停指定的时间（如果处理时间连续超过规则延迟阈值一定次数 [可配置]），以及在暂停到期后恢复规则。

规则延迟阈值度量所需时间，而不仅是处理时间，目的是为了更准确地反映规则在处理数据包时实际所需的时间。然而，延迟阈值功能是基于软件实现的延迟管理功能，并不能实施严格的定时功能。

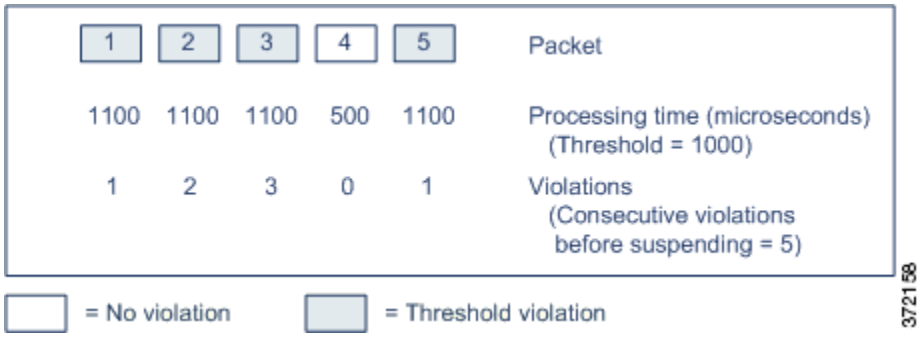
延迟阈值的得失分别为：实现性能和延迟优势的同时，也会导致未经检测的数据包可能包含攻击。但是，规则延迟阈值提供的工具可用于平衡安全性与连接性。

计时器测量每次根据一组规则处理数据包所用的处理时间。任何时候，只要规则处理时间超出指定的规则延迟阈值，系统就会递增计数器的计数。如果连续超出阈值的次数达到了指定的数值，系统就会执行下列操作：

- 按指定的期限暂停规则
- 触发事件以指明规则已暂停
- 暂停时间到期时重新启用规则
- 触发事件以指明规则已重新启用

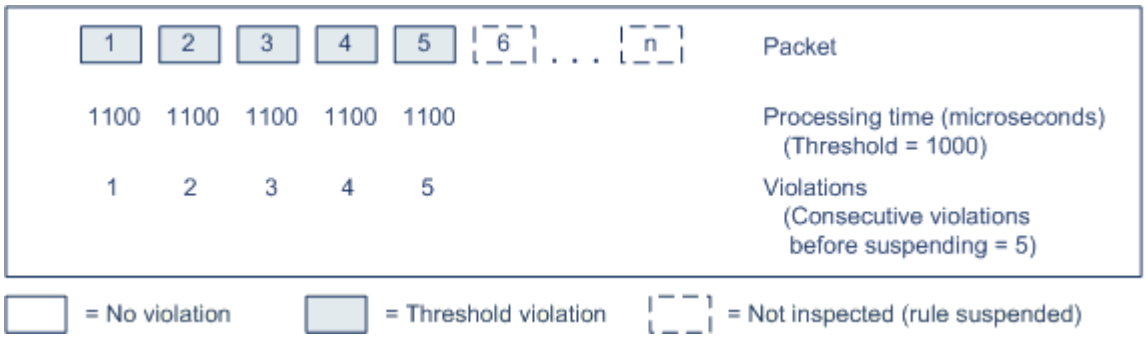
当该组规则已暂停时，或当规则违规次数非连续时，系统会将计数器清零。如在暂停规则前允许一定次数的连续违规，则将忽略对性能的影响无足轻重的偶发性违规，转而专注于反复超出规则延迟阈值的规则所造成的更大影响。

以下示例显示了未导致规则暂停的 5 次连续规则处理时间。



在以上示例中，处理前三个数据包中各个数据包的所需时间超出 1000 微秒的规则延迟阈值，每次违规时违规计数器均将递增 1 次计数。第四个数据包的处理时间未超出阈值，因此违规计数器重置为 0。第五个数据包的处理时间超出阈值，因此违规计数器从 1 开始重新计数。

以下示例显示了导致规则暂停的 5 次连续规则处理时间。



在第二个示例中，处理五个数据包中每个数据包所需的时间均超出 1000 微秒的规则延迟阈值。由于每个数据包的规则处理时间是 1100 微秒，超出 1000 微秒阈值的次数到达指定的连续 5 次，因此该组规则被暂停。在暂停时间到期前，任何后续的数据包（在图中表示为数据包 6 至 n）均不会根据暂停的规则得以检测。如果重新启用规则后收到了更多的数据包，违规计数器从 0 开始重新计数。

规则延迟阈值对数据包处理规则所触发的入侵事件无影响。无论规则处理时间是否超出阈值，规则都会因数据包中检测到的任何入侵而触发事件。如果检测到入侵的规则是内联部署中的丢弃规则，则将丢弃数据包。当丢弃规则检测到数据包中存在将导致暂停规则的入侵时，丢弃规则将触发入侵事件，数据包将被丢弃，该规则和所有相关规则均被暂停。有关丢弃规则的详细信息，请参阅第 20-17 页上的设置规则状态。

注　系统不会根据已暂停的规则对数据包进行评估。本可触发事件的已暂停规则无法触发该事件，同时，丢弃规则无法丢弃该数据包。

通过暂停在处理数据包时耗时最长的规则，规则延迟阈值可提高被动和内联部署模式下的系统性能，并缩短内联部署中的延迟。在可配置的时间到期之前，系统不会根据被暂停的规则对数据包再次进行评估，从而留出时间让过载设备进行恢复。例如，这些性能优势可以在以下情形中发挥出来：

- 匆忙写就、大量未经测试的规则需要过长的处理时间
- 网络性能不佳期间（例如，当有人下载超大文件时），数据包检测变慢。

配置规则延迟阈值

许可证：保护

可修改规则延迟阈值、已暂停规则的暂停时间以及暂停规则前必须连续超出阈值的次数。

如果规则处理数据包时所用时间超过 **Consecutive Threshold Violations Before Suspending Rule** 所指定的连续次数的**阈值**，则规则延迟阈值就会按 **Suspension Time** 指定的时间暂停规则。

可启用规则 134:1，当规则已暂停时生成事件；并启用规则 134:2，在启用已暂停规则时生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

下表进一步介绍在配置规则延迟阈值时可设置的选项。

表 10-6　规则延迟阈值选项

选项	说明
阈值	指定规则在检测数据包时不应超出的时间，单位为微秒。有关所建议的最小阈值设置，请参阅最小规则延迟阈值设置表。
暂停规则前连续超出阈值的次数	指定在暂停规则之前，规则可按超过为 **Threshold** 设置的时间检测数据包的连续次数。
Suspension Time	指定暂停一组规则前需经过的秒数。

许多因素影响系统性能，如 CPU 速度、数据速率、数据包大小和协议类型。因此，思科建议您使用下表中的阈值设置，直到您计算出了适合自己的网络环境的设置。

表 10-7　最小规则延迟阈值设置

针对此数据速率...	将阈值（微秒）设置为至少...
1 Gbps	500
100 Mbps	1250
5 Mbps	5000 年

计算设置时请确定：

- 每秒的平均数据包数
- 每个数据包所需的平均微秒数

将网络中每个数据包所需的平均微秒数乘以一个较大的安全因子，以确保不必要地中断规则检测。

要配置规则延迟阈值，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Latency-Based Performance Settings** 旁的编辑图标 ( )，然后在出现的弹出窗口中选择 Rule Handling 选项卡。

步骤 5　可以配置规则延迟阈值选项表中的任一选项。

有关所建议的最小**阈值**设置，请参阅最小规则延迟阈值设置表。

步骤 6　点击**确定**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 4-10 页上的应用访问控制策略。

配置入侵性能统计数据日志记录

许可证：保护

可配置指定设备如何监控和报告其自身性能的基本参数。这样，就可通过配置以下选项，指定系统更新设备上的性能统计数据的时间间隔：

Sample time (seconds) and Minimum number of packets

当过了所指定的性能统计数据更新之间的秒数时，系统验证其已分析的数据包是否到达指定数量。如果到达，则系统更新性能统计数据。否则，系统等待，直到其分析的数据包到达指定的数量。

Troubleshooting Options: Log Session/Protocol Distribution

支持部门可能要求您在故障排除调用期间记录协议分布、数据包长度和端口统计信息。

注意事项 更改此故障排除选项的设置将会影响性能，只能在支持部门的指导下完成该更改。

Troubleshooting Options: Summary

支持部门可能要求您在故障排除调用期间将系统配置为仅在 Snort® 进程关闭或重新启动时计算性能统计数据。要启用此选项，也必须启用 **Log Session/Protocol Distribution** 故障排除选项。

注意事项 更改此故障排除选项的设置将会影响性能，只能在支持部门的指导下完成该更改。

要配置基本的性能统计数据参数，请执行以下操作：

步骤 1 选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2 点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3 选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4 点击 **Performance Settings** 旁的编辑图标 ( )，然后在出现的弹出窗口中选择 Performance Statistics 选项卡。

步骤 5 如上所述修改 **Sample time** 或 **Minimum number of packets**。

步骤 6 或者，展开 **Troubleshoot Options** 部分并修改这些选项（仅当支持部门要求这样做时）

步骤 7 点击 **OK**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 4-10 页上的应用访问控制策略。

调整文件和恶意软件检测性能和存储

许可证：保护或恶意软件

如果使用文件策略执行文件控制或者恶意软件检测或拦截，则可以设置下表中列出的选项。记住，提高文件大小会影响系统的性能。

表 10-8　高级访问控制文件和恶意软件检测选项

字段	说明	默认值	范围	备注
Limit the number of bytes inspected when doing file type detection	指定执行文件类型检测时检测的字节的数量。	1460 字节，或者 TCP 数据包的最大分段大小	0 - 4294967295 (4GB)	设置为 0 可移除限制。 在大多数情况下，系统可以使用第一个数据包确定常见的文件类型。
Do not calculate SHA-256 hash values for files larger than (in bytes)	禁止系统存储大于特定大小的文件，对文件进行查阅综合安全情报云或阻止文件（如果已添加至自定义检测列表）。	10485760 (10MB)	0 - 4294967295 (4GB)	设置为 0 可移除限制。
Allow file if cloud lookup for Block Malware takes longer than (seconds)	指定进行恶意软件云查找时，没有缓存的处置，系统将会保持匹配**阻止恶意软件**规则的文件的最后一个字节的时长。如果该时间过去，系统没有获得处置，文件将会通过。不可用的处置不会被缓存。	2 秒	0 - 30 秒	尽管该选项接受最长 30 秒的值，思科 建议使用默认值，以避免因为连接故障而阻止流量。如未联系支持部门，**请勿**将此选项设置为 0。

要配置文件和恶意软件检测性能和存储，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Files and Malware Settings** 旁的编辑图标 ( )。

系统将显示文件和恶意软件设置弹出窗口。

步骤 5　可以设置高级访问控制文件和恶意软件检测选项表中的任一选项。

步骤 6　点击 **OK**。

只有保存和应用访问控制策略才能使更改生效；请参阅第 4-10 页上的应用访问控制策略。

了解网络分析和入侵策略

网络分析和入侵策略作为 ASA FirePOWER 模块入侵检测和防御功能的一部分，共同发挥作用。术语*入侵检测*通常指被动分析网络流量以寻找潜在入侵，并存储攻击数据用于安全分析的过程。术语*入侵防御*包括入侵检测的概念，但是增加了在恶意流量流经网络时对其进行拦截或更改的能力。

在入侵防御部署中，当系统检测数据包时：

- **网络分析策略**监管流量如何*解码*和*预处理*，以便可以进一步对其进行评估，尤其对于可能指示入侵尝试的异常流量更加如此。
- **入侵策略**使用*入侵和预处理程序规则*（有时统称为*入侵规则*）根据模式检测已解码数据包是否存在攻击。入侵策略与*变量集*配对，这使您能够使用指定值准确反映网络环境。

网络分析和入侵策略均由父访问控制策略调用，但是在不同时间调用。在系统分析流量时，网络分析（解码和预处理）阶段发生在入侵防御（其他预处理和入侵规则）阶段之前并与其分隔开来。网络分析和入侵策略共同提供广泛且深入的数据包检测。它们可以帮助您检测、提醒和防范可能威胁主机及其数据的可用性、完整性和保密性的网络流量。

ASA FirePOWER 模块随附若干以类似方式命名的网络分析和入侵策略（例如，Balanced Security and Connectivity），这些策略是相辅相成的。通过使用系统提供的策略，您可以利用思科漏洞研究团队 (VRT) 的经验。对于这些策略，VRT 会设置入侵和预处理程序规则状态，以及提供预处理程序和其他高级设置的初始配置。

您还可以创建自定义网络分析和入侵策略。您可以调整自定义策略中的设置，以对您最重要的方式检测流量。您使用类似的策略编辑器，创建、编辑、保存及管理网络分析和入侵策略。编辑任一类型的策略时，在 用户界面的左侧会出现导航面板；右侧显示各种配置页面。

本章简要概述网络分析和入侵策略监管的配置类型，说明策略如何协作以检测流量和生成策略违例记录，以及提供有关对策略编辑器进行导航的基本信息。本章还说明使用自定义策略与系统提供的策略的优点和局限性。有关详细信息，请参阅：

- 第 11-2 页上的了解策略如何检测入侵的流量
- 第 11-6 页上的比较系统提供的策略与自定义策略
- 第 11-11 页上的使用导航面板
- 第 11-12 页上的解决冲突和提交策略更改

要自定义入侵部署，请参阅以下内容来获取后续步骤：

- 第 2-13 页上的使用变量集说明如何配置系统的入侵变量以准确反映网络环境。即使不使用自定义策略，思科也**强烈**建议修改默认变量集中的默认变量。高级用户可以创建并使用自定义变量集与一个或多个自定义入侵策略配对。
- 第 19-1 页上的入侵策略使用入门说明如何创建和编辑简单的自定义入侵策略。

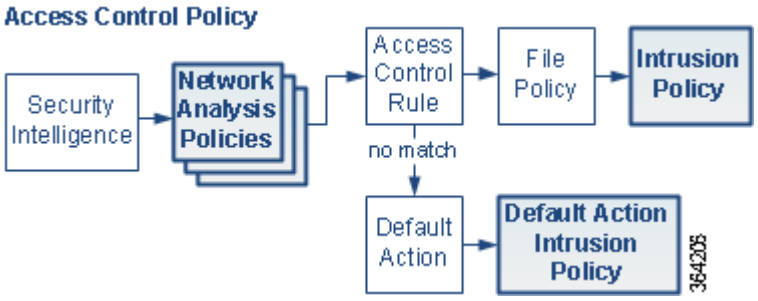
- 第 10-1 页上的使用入侵和文件策略控制流量说明如何配置系统，以通过将入侵策略与父访问控制策略关联来使用入侵策略仅检测您感兴趣的流量。它还说明如何配置高级入侵策略性能选项。
- 第 17-1 页上的配置高级传输/网络设置说明如何配置全局适用于的所有流量的高级传输和网络预处理程序设置。您在访问控制策略中而不是在网络分析或入侵策略中配置这些高级设置。
- 第 14-1 页上的网络分析策略使用入门说明如何创建和编辑简单的自定义网络分析策略。
- 第 13-2 页上的利用网络分析策略自定义预处理说明如何更改默认网络分析策略。对于高级用户，本节还说明如何通过分配自定义网络分析策略以预处理匹配流量来根据特定安全区域网络 定制预处理。
- 第 12-1 页上的在网络分析或入侵策略中使用层说明在较大的组织或复杂部署中如何使用构建块（称为策略*层*）更高效地管理多个网络分析或入侵策略。

了解策略如何检测入侵的流量

许可证：保护

当系统在访问控制部署过程中分析流量时，网络分析（解码和预处理）阶段发生在入侵防御（入侵规则和高级设置）阶段之前并与其分隔开来。

下图以简化方式显示内联的入侵防御和高级恶意软件防护 (AMP) 部署中流量分析的顺序。它说明访问控制策略如何调用其他策略来检测流量，以及这些策略的调用顺序。网络分析和入侵策略选择阶段突出显示。



在内联部署中，系统可以阻止流量，而不在图示过程中的几乎任何步骤进一步检测。安全智能、网络分析策略、文件策略和入侵策略均可以丢弃或修改流量。

类似地，在该过程的每个步骤中，数据包都可能会导致系统生成事件。入侵和预处理程序事件（有时统称为*入侵事件*）指示数据包或其内容可能表示安全风险。

请注意，对于单个连接而言，虽然系统在访问控制规则之前选择网络分析策略（如图所示），但是一些预处理（特别是应用层预处理）发生在访问控制规则选择之后。这不影响您在自定义网络分析策略中配置预处理的方式。

有关详细信息，请参阅：

- 第 11-3 页上的解码、规范化和预处理：网络分析策略
- 第 11-4 页上的访问控制规则：入侵策略选择
- 第 11-4 页上的入侵检测：入侵策略、规则和变量集
- 第 11-5 页上的入侵事件生成

解码、规范化和预处理：网络分析策略

许可证：保护

如果没有解码和预处理，则系统无法适当评估流量是否存在入侵，因为协议差异使得无法进行模式匹配。如第 11-2 页上的了解策略如何检测入侵的流量中的图中所示，网络分析策略监管以下流量处理任务：

- 在流量由安全智能过滤**之后**
- 在流量可由文件或入侵策略检测**之前**

网络分析策略分阶段监管数据包处理。首先，系统通过前三个 TCP/IP 层将数据包解码，然后继续规范化、预处理和检测协议异常。

- 数据包解码器将数据包报头和负载转换为可由预处理程序并在以后由入侵规则轻松使用的格式。 TCP/IP 堆栈的各层从数据链路层开始并持续到网络层和传输层依次解码。数据包解码器还会检测数据包报头中的各种异常行为。有关详细信息，请参阅第 17-14 页上的了解数据包解码。
- 在内联部署中，内联规范化预处理程序重新格式化（规范化）流量，以尽量降低攻击者逃避检测的可能性。它会准备数据包以供其他预处理程序和入侵规则进行检测，并且帮助确保系统处理的数据包与网络上主机接收的数据包相同。有关详细信息，请参阅第 17-5 页上的规范化内联流量。
- 各种网络层和传输层预处理程序检测利用 IP 分段的攻击，执行校验和验证，以及执行 TCP 和 UDP 会话预处理；请参阅第 17-1 页上的配置传输层和网络层预处理。

  请注意，一些高级传输和网络预处理程序设置全局适用于由访问控制策略的处理的所有流量。您在访问控制策略中而不是在网络分析策略中配置这些高级设置；请参阅第 17-1 页上的配置高级传输/网络设置。
- 各种应用层协议解码器将特定类型的数据包数据规范化为入侵规则引擎可以分析的格式。通过规范化应用层协议编码，系统可以将相同的内容相关的入侵规则有效地应用于以不同方式表示其数据的数据包，并且获取有意义的结果。有关详细信息，请参阅第 15-1 页上的使用应用层预处理器。
- Modbus 和 DNP3 SCADA 预处理程序检测异常流量并向入侵规则提供数据。监控与数据采集 (SCADA) 协议可监视和控制工业、基础设施以及工厂流程（例如制造、生产、水处理、配电、机场和运输系统等）并从中获取数据。有关详细信息，请参阅第 16-1 页上的配置 SCADA 预处理。
- 通过若干预处理程序，可以检测特定威胁，如 Back Orifice、端口扫描、 SYN 泛洪和其他基于速率的攻击；请参阅第 21-1 页上的检测特定威胁。

  请注意，您配置敏感数据预处理程序，它会检测入侵策略中的敏感数据，如 ASCII 文本形式的信用卡号与社会保障号；请参阅第 21-17 页上的检测敏感数据。

在新建的访问控制策略中，一个默认网络分析策略监管对同一父访问控制策略调用的*所有*入侵策略的*所有*流量的预处理。最初，系统使用 Balanced Security and Connectivity 网络分析策略作为默认值，但是，可以将其更改为另一个系统提供的网络分析策略或自定义网络分析策略。在更复杂的部署中，高级用户可以通过分配不同的自定义网络分析策略以预处理匹配流量来根据特定安全区域网络定制流量预处理选项。有关详细信息，请参阅第 11-6 页上的比较系统提供的策略与自定义策略。

访问控制规则：入侵策略选择

许可证：保护

在初始预处理后，访问控制规则（如果存在）会评估流量。在大多数情况下，数据包匹配的第一条访问控制规则处理该流量；您可以监控、信任、阻止或允许匹配流量。

当使用访问控制规则允许流量时，系统可能按该顺序检测流量是否存在恶意软件、受禁文件和入侵。不与任何访问控制规则匹配的流量由访问控制策略的默认操作进行处理，该操作还检测是否存在入侵。

注　所有数据包（**无论**哪个网络分析策略对其进行预处理）均与配置的访问控制规则相匹配，因此可能会由上而下受到入侵策略的检测。有关详细信息，请参阅第 11-9 页上的自定义策略的限制。

第 11-2 页上的了解策略如何检测入侵的流量中的图显示流经内联的入侵防御和 AMP 部署中的设备的流量，如下所示：

- 访问控制规则允许匹配流量继续。然后，检测流量是否存在受禁文件和恶意软件，再检测流量是否存在入侵。
- 在此情景中，访问控制策略的默认操作允许匹配流量。然后，依次由入侵策略检测流量。将入侵策略与访问控制规则或默认操作相关联时，可以（但不必）使用其他入侵策略。

图中的示例不包括任何阻止或信任规则，因为系统不检测已阻止或信任的流量。有关详细信息，请参阅第 6-6 页上的使用规则操作确定流量处理和检测和第 4-4 页上的为网络流量设置默认的处理和检查。

入侵检测：入侵策略、规则和变量集

许可证：保护

在允许流量继续到达其目标之前，可以使用入侵防御作为系统的最后一道防线。入侵策略监管系统如何检测流量是否存在安全违规，并且在内联部署中可以阻止或修改恶意流量。入侵策略的主要功能是管理启用哪些入侵和预处理程序规则及其如何配置。

入侵和预处理程序规则

入侵规则是一组指定的关键字和参数，用于检测企图利用网络漏洞的行为；系统使用入侵规则来分析网络流量，以检测其是否与规则中的条件匹配。系统将数据包与每条规则中指定的条件进行比较，如果数据包数据与规则中指定的所有条件都匹配，则触发此规则。

系统包含 VRT 创建的以下类型的规则：

- *共享对象入侵规则*，已编译且无法修改（规则标题信息除外，如源和目标端口及 IP 地址）
- *标准文本入侵规则*，可以保存并修改为规则的新自定义实例。
- *预处理程序规则*，是指与网络分析策略中的预处理程序和数据包解码器检测选项关联的规则。不能复制或编辑预处理程序规则。默认情况下，大多数预处理程序规则均已禁用；您必须将其启用才能使用预处理程序生成事件，并在内联部署中丢弃有问题的数据包。

当系统根据入侵策略处理数据包时，首先，规则优化器会根据传输层、应用协议、受保护网络的方向等条件对子集中所有已激活的规则进行分类。然后，入侵规则引擎选择要应用于每个数据包的相应规则子集。最后，多规则搜索引擎执行三种不同类型的搜索以确定流量是否与规则匹配：

- 协议字段搜索在应用协议的特定字段中查找匹配项。
- 一般内容搜索在数据包负载中查找 ASCII 或二进制字节匹配项。

- 数据包异常搜索查找没有包含特定内容而是违反既定协议的数据包报头和负载。

在自定义入侵策略中，您可以通过启用和禁用规则以及通过编写和添加自己的标准文本规则来调整检测。

变量集

只要系统使用入侵策略来评估流量，它便会使用关联的*变量集*。变量集中的大多数变量表示入侵规则中常用于识别源和目标 IP 地址及端口的值。您还可以在入侵策略中使用变量表示规则禁止和动态规则状态中的 IP 地址。

系统提供单个由预定义默认变量组成的默认变量集。系统提供的大多数共享对象规则和标准文本规则均使用这些预定义默认变量来定义网络和端口号。例如，大部分规则使用变量 `$HOME_NET` 指定受保护网络，使用变量 `$EXTERNAL_NET` 指定未受保护（或外部）网络。此外，专用规则通常会使用其他预定义的变量。例如，检测针对网络服务器的漏洞攻击的规则使用 `$HTTP_SERVERS` 和 `$HTTP_PORTS` 变量。

提示 即使您使用系统提供的入侵策略，思科也**强烈**建议修改默认变量集中的关键默认变量。当使用准确反映网络环境的变量时，处理会得以优化，并且系统可以监控相关系统是否存在可疑活动。高级用户可以创建并使用自定义变量集与一个或多个自定义入侵策略配对。有关详细信息，请参阅第 2-13 页上的优化预定义默认变量。

入侵事件生成

许可证：保护

当系统识别可能的入侵时，它会生成*入侵*或*预处理程序事件*（有时统称为*入侵事件*）。您可以查看数据更好地了解对网络资产的攻击。在内联部署中，-系统还可以丢弃或替换明知有危害的数据包。

的每个入侵事件均包括事件报头并包含有关事件名称和分类的信息；源和目标 IP 地址；端口；生成事件的进程；事件的日期和时间，以及有关攻击源及其目标的情景信息。对于基于数据包的事件，系统还会记录一个或多个已触发事件的数据包的已解码数据包报头和负载的副本。

数据包解码器、预处理程序和入侵规则引擎均会导致系统生成事件。例如：

- 如果数据包解码器（在网络分析策略中配置）接收少于 20 字节（没有任何选项或负载的 IP 数据报的大小）的 IP 数据包，解码器将此解释为异常流量。如果之后启用了用于检测数据包的入侵策略中的配套解码器规则，则系统会生成预处理程序事件。
- 如果 IP 分片重组预处理程序遇到一系列重叠的 IP 片段，则预处理程序会将此解释为可能的攻击，当启用了配套预处理程序规则时，系统会生成预处理程序事件。
- 在入侵规则引擎内，会编写大多数标准文本规则和共享对象规则，以便其在由数据包触发时生成入侵事件。

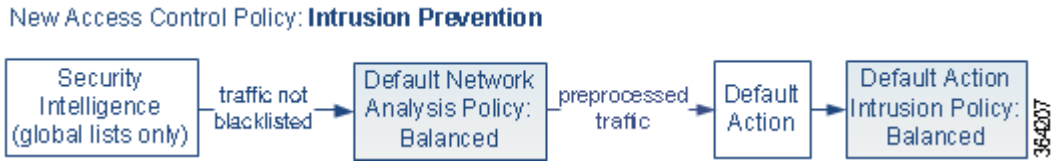
随着设备累积的入侵事件越来越多，您可以开始分析潜在攻击。系统为您提供复审入侵事件和评估其在网络环境与安全策略情境中是否重要所需的工具。

比较系统提供的策略与自定义策略

许可证：保护

创建新的访问控制策略是使用 ASA FirePOWER 模块管理流量过程中的头几个步骤之一。默认情况下，新创建的访问控制策略调用系统提供的网络分析和入侵策略来检测流量。

下图显示内联的入侵防御部署中新创建的访问控制策略最初如何处理流量。预处理和入侵防御阶段突出显示。



请注意以下各种操作的方式：

- 默认网络分析策略监管由访问控制策略处理的*所有*流量的预处理。最初，系统提供的 *Balanced Security and Connectivity 网络分析策略*是默认策略。
- 访问控制策略的默认操作允许由系统提供的 *Balanced Security and Connectivity 入侵策略*确定的所有非恶意流量。
- 策略使用默认安全智能选项（仅全局白名单和黑名单），并且不使用访问控制规则对网络流量执行特殊处理和检测。

可以采取用于调整入侵防御部署的一个简单步骤是使用系统提供的一组不同的网络分析和入侵策略为作为默认值。思科通过 ASA FirePOWER 模块提供若干对这些策略。

或者，您可以通过创建和使用自定义策略来定制入侵防御部署。您可能会发现这些策略中配置的预处理程序选项、入侵规则和其他高级设置无法满足网络的安全需求。通过调整网络分析和入侵策略，可以非常精细地配置系统如何处理网络流量并检测其是否存在入侵。

有关详细信息，请参阅：

- 第 11-6 页上的了解系统提供的策略
- 第 11-7 页上的自定义策略的优势
- 第 11-9 页上的自定义策略的限制

了解系统提供的策略

许可证：保护

思科通过 ASA FirePOWER 模块提供若干对网络分析和入侵策略。通过使用系统提供的网络分析和入侵策略，您可以利用思科漏洞研究团队 (VRT) 的经验。对于这些策略，VRT 会设置入侵和预处理程序规则状态，以及提供预处理程序和其他高级设置的初始配置。可以按现状使用系统提供的策略，也可以将其用作自定义策略的基础。

提示 即使您使用系统提供的网络分析和入侵策略，也应该配置系统的入侵变量，以准确反映网络环境。至少，要修改默认变量集中的关键默认变量；请参阅第 2-13 页上的优化预定义默认变量。

随着新的漏洞被发现， VRT 会发布入侵规则更新。这些规则更新可以修改系统提供的任何网络分析或入侵策略，并且可以提供新的和已更新的入侵规则及预处理程序规则、现有规则的已修改状态，以及已修改的默认策略设置。规则更新还可以从系统提供的策略中删除规则，并且提供新规则类别，以及修改默认变量集。

如果规则更新影响部署，则系统会将受影响的入侵和网络分析策略标记为过期，以及标记其父访问控制策略。您必须重新应用已更新的策略以使其更改生效。

为方便起见，可以将规则更新配置为自动重新应用受影响的入侵策略（单独或与受影响的访问控制策略组合）。这使您能够轻松、自动保持部署为最新，以防范最近发现的漏洞和入侵。

要确保最新的预处理设置，**必须**重新应用访问控制策略，这还会重新应用与当前运行的网络分析和文件策略不同的任何关联 SSL、网络分析和文件策略，并还可以更新高级预处理和性能选项的默认值。有关详细信息，请参阅第 35-8 页上的导入规则更新和本地规则文件。

思科通过 ASA FirePOWER 模块提供以下网络分析和入侵策略：

Balanced Security and Connectivity 网络分析和入侵策略

这些策略专为速度和检测而构建。共同使用时，这些策略充当大多数组织的良好起点。系统在大多数情况下均使用 Balanced Security and Connectivity 策略和设置作为默认值。

Connectivity Over Security 网络分析和入侵策略

这些策略专为连接性（能够获取所有资源）优先于网络基础设施安全性的组织而构建。此入侵策略启用的规则远远少于 Security over Connectivity 策略中启用的规则。仅会启用阻止流量的最重要规则。

Security Over Connectivity 网络分析和入侵策略

这些策略专为网络基础设施安全性优先于用户便利性的组织而构建。此入侵策略启用可能会提醒或丢弃合法流量的许多网络异常入侵规则。

No Rules Active 入侵策略

在 No Rules Active 入侵策略中，所有入侵规则和高级设置均已禁用。如果您要创建自己的入侵策略而不是将其基于系统提供的其他策略之一中的已启用规则，可以尝试使用此策略。

注意事项　思科使用另一个策略 Experimental Policy 1 来进行测试。请勿使用此策略，除非思科代表指示这样做。

自定义策略的优势

许可证：保护

您可能会发现系统提供的网络分析和入侵策略中配置的预处理程序选项、入侵规则和其他高级设置不完全满足贵组织的安全需要。

构建自定义策略可以提高环境中系统的性能，并且可以密切关注网络上发生的恶意流量和策略违例。通过创建和调整自定义策略，可以非常精细地配置系统如何处理和检查网络流量是否存在入侵。

所有自定义策略都具有基本策略（也称为基层），用于为策略中所有配置定义默认设置。层是可用于高效管理多个网络分析或入侵策略的构建块；请参阅第 12-1 页上的在网络分析或入侵策略中使用层。

在大多数情况下，自定义策略基于系统提供的策略，但是可以使用其他自定义策略。不过，所有自定义策略在策略链中都以系统提供的策略作为最终基础。由于规则更新可能会修改系统提供的策略，因此导入规则更新可能会对您产生影响，即使使用自定义策略作为基础也如此。如果规则更新影响策略，模块接口会将受影响策略标记为过期。有关详细信息，请参阅第 12-4 页上的允许规则更新修改系统提供的基本策略。

有关详细信息，请参阅：

- 第 11-8 页上的自定义网络分析策略的优势
- 第 11-8 页上的自定义入侵策略的优势

自定义网络分析策略的优势

许可证：保护

默认情况下，一个网络分析策略预处理由访问控制策略处理的所有流量。这意味着所有数据包都根据相同设置进行解码和预处理，无论后来使用哪种入侵策略（和因此使用的入侵规则集）对其进行检测。

最初，系统提供的 Balanced Security and Connectivity 网络分析策略是默认策略。调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值；请参阅第 13-3 页上的为访问控制设置默认网络分析策略。

可用的调整选项因预处理程序而异，但是可以调整预处理程序和解码器的一些方法包括：

- 可以禁用不适用于正在监控的流量的预处理程序。例如， HTTP Inspect 预处理程序规范化 HTTP 流量。如果确信网络中没有任何使用 Microsoft 互联网信息服务 (IIS) 的 Web 服务器，则可以禁用查找特定于 IIS 的流量的预处理程序选项，从而减少系统处理开销。

  注　如果在自定义网络分析策略中禁用预处理程序，但是系统需要使用该预处理程序在今后根据已启用的入侵或预处理程序规则评估数据包，则系统会自动启用并使用该预处理程序，尽管预处理程序在网络分析策略用户界面中保持禁用。

- 指定端口（如果适用）以关注某些预处理程序的活动。例如，可以确定要对 DNS 服务器响应

对于复杂部署的高级用户，可以创建多个网络分析策略，每个策略定制为以不同方式预处理流量。然后，可以将系统配置为使用这些策略通过不同的安全区域网络监管流量的预处理。

注　使用自定义网络分析策略（尤其是多个网络分析策略）定制预处理是一个高级任务。由于预处理和入侵检测密切相关，因此，您**必须**注意，要确保允许检测单个数据包的网络分析和入侵策略能够互补。有关详细信息，请参阅第 11-9 页上的自定义策略的限制。

自定义入侵策略的优势

许可证：保护

在新建的初始配置为执行入侵防御的访问控制策略中，默认操作允许所有流量，但是首先会使用系统提供的 Balanced Security and Connectivity 入侵策略对流量进行检测。除非添加访问控制规则或更改默认操作，否则所有流量都由该入侵策略进行检测；请参阅第 11-6 页上的比较系统提供的策略与自定义策略中的图。

要自定义入侵防御部署，可以创建多个入侵策略，每个策略定制为以不同方式检测流量。然后，使用指定哪个策略检测哪个流量的规则来配置访问控制策略。访问控制规则可能很简单，也可能很复杂，使用多个条件来匹配和检测流量，包括安全区域、网络或地理位置、端口、应用、请求的 URL 或用户。第 11-2 页上的了解策略如何检测入侵的流量中的情景显示由两个入侵策略之一检测流量的部署。

入侵策略的主要功能是管理启用哪些入侵和预处理程序规则及其如何配置，如下所示：

- 在每个入侵策略中，应该验证所有适用于环境的规则是否已启用，并且通过禁用不适用于环境的规则来提高性能。在内联部署中，可以指定哪些规则应该丢弃或修改恶意数据包。有关详细信息，请参阅第 20-17 页上的设置规则状态。
- 可以修改现有规则并根据需要编写新标准文本规则，以捕获新的漏洞或强制实施安全策略；请参阅第 23-1 页上的了解和编写入侵规则。

您可能对入侵策略进行的其他自定义包括：

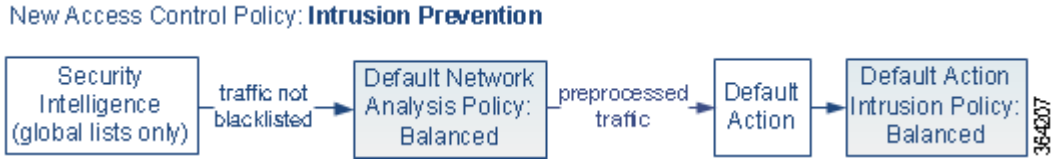
- 敏感数据预处理器检测敏感信息，例如 ASCII 文本格式的信用卡号和社会保障号。请注意，在网络分析策略中配置了用于检测特定威胁（back orifice 攻击、多种端口扫描类型以及尝试以过多流量淹没网络的基于速率的攻击）的其他预处理程序。有关详细信息，请参阅第 21-1 页上的检测特定威胁。
- 全局阈值导致系统根据与入侵规则匹配的流量在指定时间段内源自或流向特定地址或地址范围的次数来生成事件。这有助于防止系统被大量事件淹没。有关详细信息，请参阅第 22-1 页上的全局限制入侵事件记录。
- 禁止入侵事件通知和设置个别规则或全体入侵策略的阈值也可以防止系统被大量事件淹没。有关详细信息，请参阅第 20-19 页上的按策略过滤入侵事件通知。
- 除 入侵事件外，您还可以启用对系统日志工具的日志记录或者将事件数据发送到 SNMP 陷阱服务器。根据策略，可以指定入侵事件通知限制，设置发送到外部日志记录工具的入侵事件通知，以及配置对入侵事件的外部响应。有关详细信息，请参阅第 28-1 页上的配置入侵规则的外部警报。

自定义策略的限制

许可证：保护

由于预处理和入侵检测如此密切相关，因此，您**必须**小心确保自己的配置允许网络网络分析和入侵策略处理和检测单个数据包，以实现互补。

默认情况下，系统使用一个网络分析策略预处理的所有流量。下图显示内联的入侵防御部署中新创建的访问控制策略最初如何处理流量。预处理和入侵防御阶段突出显示。



请注意默认网络分析策略如何监管由访问控制策略处理的所有流量的预处理。最初，系统提供的 Balanced Security and Connectivity 网络分析策略是默认策略。

调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值，如第 11-8 页上的自定义网络分析策略的优势中所概括。但是，如果在自定义网络分析策略中禁用预处理程序，但是系统需要根据已启用的入侵或预处理程序规则评估预处理的数据包，则系统自动启用并使用该预处理程序，尽管它在网络分析策略用户界面中保持禁用。

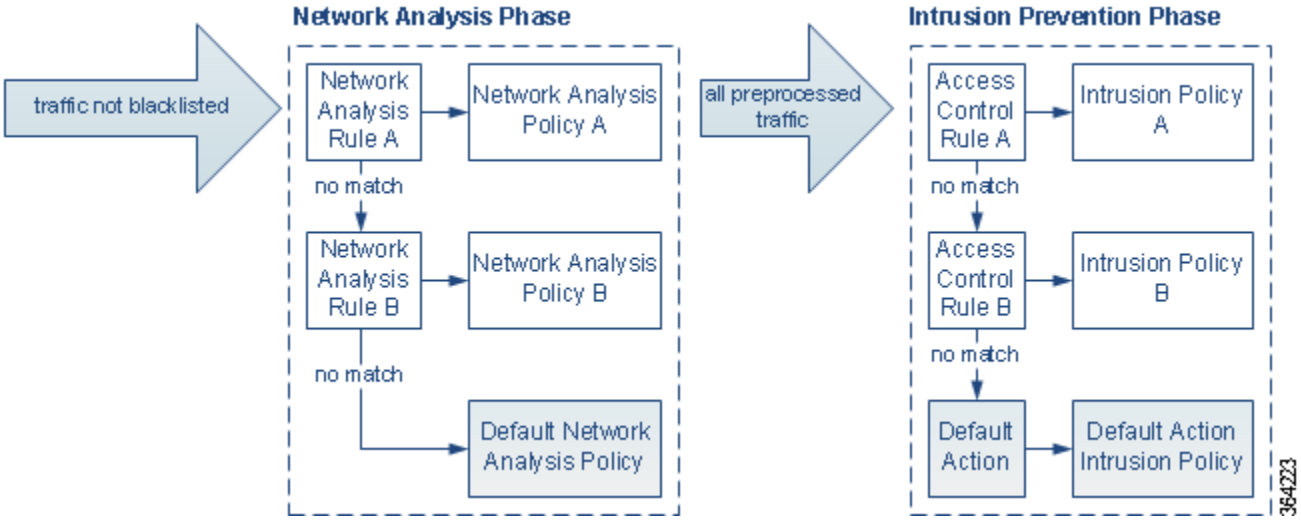
注　要获取禁用预处理程序的性能优势，您**必须**确保自己的入侵策略均未启用需要该预处理程序的规则。

如果使用多个自定义网络分析策略，则会引起其他问题。对于复杂部署的高级用户，可以通过分配自定义网络分析策略以预处理匹配流量来根据特定安全区域-网络定制预处理。为此，可以向访问控制策略中添加自定义*网络分析规则*。每条规则均具有关联的网络分析策略，用于监管与该规则匹配的流量的预处理。

提示　可以将网络分析规则配置为访问控制策略中的高级设置。与 ASA FirePOWER 模块中其他类型的规则不同，网络分析规则调用网络分析策略，而不是被其包含。

系统按规则号由上而下将数据包与任何已配置的网络分析规则相匹配。不与任何网络分析规则相匹配的流量由默认网络分析策略预处理。虽然这使您在预处理流量时具有极大灵活性，但请记住，所有数据包**无论**由哪个网络分析策略进行了预处理，后来都会在各自的进程中与访问控制规则匹配，从而可能会接受入侵策略的检查。换句话说，使用特定网络分析策略预处理数据包**不**保证将通过任何特殊入侵策略检测该数据包。您**必须**仔细配置访问控制策略，以使其调用正确的网络分析和入侵策略来评估特殊数据包。

下图集中细解了网络分析策略（预处理）选择阶段如何在入侵防御（规则）阶段之前发生并与其分隔开来。为简单起见，该图消除文件/恶意软件检测阶段。它还突出显示默认网络分析和默认操作入侵策略。



在此情景中，访问控制策略配置有两条网络分析规则和一个默认网络分析策略：

- 网络分析规则 A 使用网络分析策略 A 预处理匹配流量。之后，您希望此流量由入侵策略 A 进行检测。
- 网络分析规则 B 使用网络分析策略 B 预处理匹配流量。之后，您希望此流量由入侵策略 B 进行检测。
- 所有剩余流量都使用默认网络分析策略进行预处理。之后，您希望此流量由与访问控制策略的默认操作关联的入侵策略进行检测。

系统在预处理流量之后，可以检测流量是否存在入侵。该图显示具有两条访问控制规则和一个默认操作的访问控制策略：

- 访问控制规则 A 允许匹配流量。然后，流量由入侵策略 A 进行检测。
- 访问控制规则 B 允许匹配流量。然后，流量由入侵策略 B 进行检测。
- 访问控制策略的默认操作允许匹配流量。然后，流量由默认操作的入侵策略进行检测。

每个数据包的处理均由网络分析策略和入侵策略对进行监管，但系统**不**为您协调该对。请考虑以下情景：访问控制策略配置错误，以致网络分析规则 A 和访问控制规则 A 不处理相同流量。例如，您可能希望配对的策略监管特殊安全区域上流量的处理，但是在两条规则的条件中错误地使用不同的区域。这可能会导致错误地预处理流量。因此，使用网络分析规则和自定义策略定制预处理是一项**高级**任务。

请注意，对于单个连接而言，虽然系统在访问控制规则之前选择网络分析策略，但是一些预处理（特别是应用层预处理）发生在访问控制规则选择之后。这**不**影响您在自定义网络分析策略中配置预处理的方式。

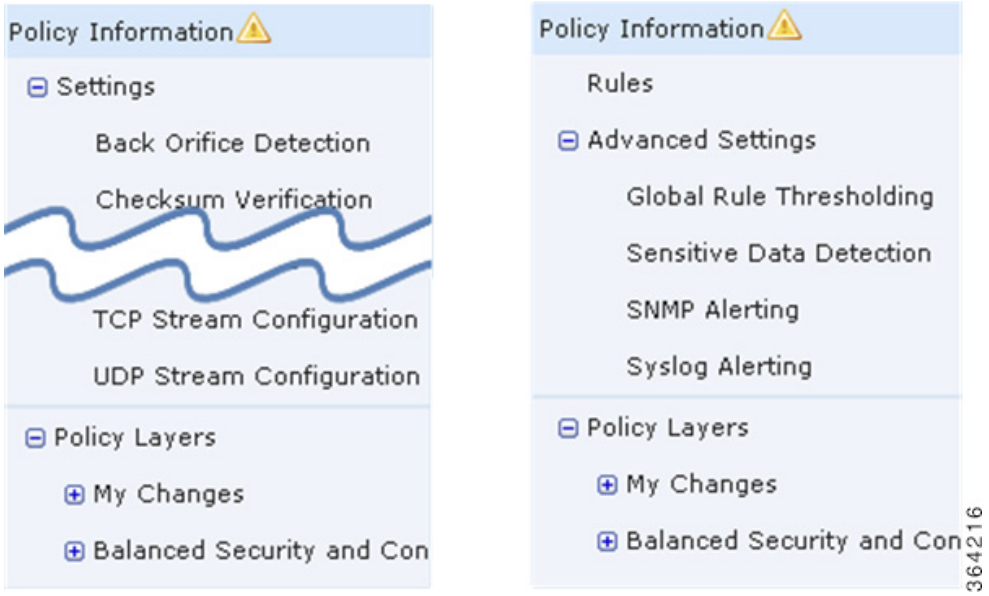
使用导航面板

许可证：保护

网络分析和入侵策略使用类似的用户界面编辑和保存对其配置做出的更改；请参阅：

- 第 14-4 页上的编辑网络分析策略
- 第 19-4 页上的编辑入侵策略

编辑任一类型的入侵策略时，用户界面的左侧会出现导航面板。下图显示网络分析策略（左）和入侵策略（右）的导航面板。



分隔线将导航面板分隔成指向策略设置的链接，可以通过（下方）或不通过（上方）与策略层的直接交互来配置这些设置。要导航到任何设置页面，请在导航面板中点击其名称。某项在导航面板中的浓阴影突出显示当前设置页面。例如，在上方的插图中，Policy Information 页面会显示到导航面板的右侧。

Policy Information

Policy Information 页面提供常用设置的配置选项。如以上网络分析策略面板的插图所示，当策略包含未保存的更改时，在导航面板中的 **Policy Information** 旁边会显示策略更改图标 (⚠)。保存更改后，该图标消失。

Rules （仅入侵策略）

入侵策略中的 Rules 页面可供您配置共享对象规则、标准文本规则和预处理程序规则的规则状态及其他设置。有关详细信息，请参阅第 20-1 页上的使用规则调整入侵策略。

Settings （网络分析策略）和 Advanced Settings （入侵策略）

网络分析策略中的 Settings 页面可供您启用或禁用预处理程序以及访问预处理程序配置页面。展开 **Settings** 链接会显示指向策略中所有已启用预处理程序的个别配置页面的子链接。有关详细信息，请参阅第 14-6 页上的在网络分析策略中配置预处理器。

入侵策略中的 Advanced Settings 页面可供您启用或禁用高级设置以及访问这些高级设置的配置页面。展开 **Advanced Settings** 链接会显示指向策略中所有已启用高级设置的个别配置页面的子链接。有关详细信息，请参阅第 19-6 页上的在入侵策略中配置高级设置。

Policy Layers

Policy Layers 页面显示构成网络分析或入侵策略的各层的摘要。展开 Policy Layers 链接会显示指向策略中的各层的摘要页面的子链接。展开各层子链接会显示指向层中已启用的所有规则、预处理程序或高级设置的配置页面的进一步子链接。有关详细信息，请参阅第 12-1 页上的在网络分析或入侵策略中使用层。

解决冲突和提交策略更改

许可证：保护

编辑网络分析或入侵策略时，您必须在系统识别更改之前将其保存（或*提交*）。

注 保存后，必须应用网络分析或入侵策略以使更改生效。如果应用策略而不保存，则系统会使用最新保存的配置。虽然可以独立重新应用入侵策略，但是网络分析策略与其父访问控制策略一起应用。

解决编辑冲突

Network Analysis Policy 页面和 Intrusion Policy 页面 显示每个策略是否有未保存的更改请参阅第 14-4 页上的编辑网络分析策略和第 19-4 页上的编辑入侵策略。

思科建议每次仅一个人员编辑策略。如果您是以同一用户身份通过多个用户界面实例编辑相同的网络分析或入侵策略，并且保存一个实例的更改，则无法保存另一个实例的更改。

解析配置依赖关系

为了执行特殊分析，许多预处理程序和入侵规则均要求流量首先以某种方式得以解码或预处理，或者具有其他依存关系。保存网络分析或入侵策略时，系统会自动启用必需的设置，或者警告您已禁用的设置不会影响流量，如下所示：

- 如果已添加 SNMP 规则警报，但未配置 SNMP 告警，则无法保存入侵策略。必须配置 SNMP 告警或禁用规则警报，然后再次保存。
- 如果入侵策略包含已启用的敏感数据规则，但是您尚未启用敏感数据预处理程序，则无法保存该入侵策略。必须允许系统启用预处理程序并保存策略，或者禁用规则并再次保存。

- 如果在网络分析策略中禁用必需的预处理程序，则仍然可以保存该策略。但是，系统会自动将已禁用的预处理程序与其当前设置配合使用，即使预处理程序在用户界面中保持禁用也如此。有关详细信息，请参阅第 11-9 页上的自定义策略的限制。
- 如果在网络分析策略中禁用内联模式，但是启用内联规范化预处理程序，则仍然可以保存该策略。不过，系统会警告您将忽略规范化设置。禁用内联模式还会导致系统忽略允许预处理程序修改或阻止流量的其他设置，包括校验和验证和基于速率的攻击防御。有关详细信息，请参阅第 14-5 页上的允许预处理器影响内联部署中的流量和第 17-5 页上的规范化内联流量。

提交、丢弃和缓存策略更改

在编辑网络分析或入侵策略时，如果退出策略编辑器而不保存更改，则系统会缓存这些更改。即使注销系统或系统崩溃，仍然会缓存更改。系统缓存可以按照一个网络分析和一个入侵策略来存储未保存的更改；编辑同一类型的另一个策略之前，必须提交或丢弃更改。编辑另一个策略而不保存对第一个策略的更改时，或者导入入侵规则更新时，系统会丢弃缓存的更改。

可以在网络分析或入侵策略编辑器的 Policy Information 页面上提交或丢弃策略更改；请参阅第 14-4 页上的编辑网络分析策略和第 19-4 页上的编辑入侵策略。

下表总结如何保存或丢弃对网络分析或入侵策略做出的更改。

表 11-1　提交对网络分析或入侵策略做出的更改

要.....	在 Policy Information 页面上，可以...
保存对策略的更改	点击 **Commit Changes**。 或者，输入备注；点击 **OK** 继续提交。
丢弃所有未保存的更改	点击 **Discard Changes**，然后点击 **OK** 丢弃更改并转至 Intrusion Policy 页面。如果不希望丢弃更改，请点击 **Cancel** 返回到 Policy Information 页面。
退出策略，但是缓存更改	选择任何菜单或选择指向另一个页面的其他路径。请在提示时点击 **Leave page** 退出，或者点击 **Stay on page** 停留在高级编辑器中。

在网络分析或入侵策略中使用层

拥有众多 ASA FirePOWER 模块的大型组织可能具有许多入侵策略和网络分析策略来支持不同部门或业务单位（某些情况下还包括不同公司）的独特需求。两种策略类型中的配置均包含在构建块（称为*层*）中，可用于高效管理多个策略。

入侵和网络分析策略中的层基本以相同方式工作。您可以创建和编辑任一策略类型，而无需刻意使用层。您也可以修改策略配置；如果您没有向策略中添加用户层，系统会自动将您的更改纳入单个可配置的层（初始名称为 *My Changes*）。作为可选操作，您可以添加最多 200 个层，在其中配置任意组合的设置。可以复制、合并、移动和删除用户层，并且最重要的是，可与同一类型的其他策略共享个别用户层。

有关详细信息，请参阅：

- 第 12-1 页上的了解层堆栈描述构成基本策略的用户可配置层和内置层。
- 第 12-5 页上的管理层说明如何在策略中使用层。

了解层堆栈

许可证：保护

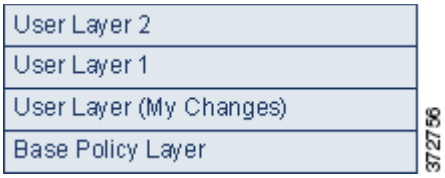
在未添加层的网络分析或入侵策略中，会包括只读格式的内置基本策略层，以及一个初始名称为 My Changes 的用户可配置层。可以复制、合并、移动或删除任何用户可配置层，并将任何用户可配置层设置为由同一类型的其他策略共享。

每个策略层均包含网络分析策略中所有预处理程序或入侵策略中所有入侵规则和高级设置的完整配置。最低基本策略层包含创建策略时选择的基本策略中的所有设置。较高层中的设置优先于较低层中的相同设置。在某一层中未明确设置的功能从对其进行了明确设置的下一最高层*继承*其设置。

系统会将层*平展*，也就是说，它在处理网络流量时，仅应用所有设置的累积效果。

提示 可以仅根据基本策略中的默认设置创建入侵或网络分析策略。

下图显示一个示例层堆栈，除基本策略层和初始 My Changes 层以外，还包括其他两个用户可配置层 *User Layer 1* 和 *User Layer 2*。请注意，图中添加的每个用户可配置层初始定位为堆栈中的最高层；因此，图中的 User Layer 2 最后添加并位于堆栈中的最高层。



使用多层时，请注意以下要点：

- 当策略中的最高层为只读层或如第 12-8 页上的在策略之间共享层中所述的共享层时，如果执行以下任一操作，则系统会自动将用户可配置层添加为入侵策略中的最高层：
  - 在入侵策略 Rules 页面上修改规则操作 （即规则状态、事件过滤，动态状态或警报）。有关详细信息，请参阅第 20-1 页上的使用规则调整入侵策略。
  - 启用、禁用或修改任何预处理程序、入侵规则或高级设置。

  除了会导致产生新层的更改外，系统添加层中的所有设置都会被继承。
- 当最高层为共享层时，系统会在您执行以下任一操作时添加一层：
  - 与其他策略共享最高层
  - 向策略中添加共享层
- 无论是否允许规则更新修改策略，规则更新中的更改都绝不会覆盖您在层中所做的更改。这是因为规则更新中的更改是在基本策略中做出，基本策略会确定基本策略层中的默认设置；您的更改始终在更高层中做出，因此其会覆盖规则更新对基本策略所做出的任何更改。有关详细信息，请参阅第 35-8 页上的导入规则更新和本地规则文件。

有关详细信息，请参阅第 12-2 页上的了解基本层。

了解基本层

许可证：保护

入侵或网络分析策略的基本层（也称为基本策略）定义策略中所有配置的默认设置，并且是策略中的最低层。在不添加新层的情况下创建新策略以及更改设置，更改会存储在 My Changes 层中，并会覆盖（但不会更改）基本策略中的设置。

有关详细信息，请参阅：

- 第 12-3 页上的了解系统提供的基本策略
- 第 12-3 页上的了解自定义基本策略
- 第 12-3 页上的更改基本策略
- 第 12-4 页上的允许规则更新修改系统提供的基本策略

了解系统提供的基本策略

许可证：保护

思科通过 ASA FirePOWER 模块提供若干对网络分析和入侵策略。通过使用系统提供的网络分析和入侵策略，您可以受益于思科漏洞研究团队 (VRT) 的经验。对于这些策略， VRT 会设置入侵和预处理程序规则状态，以及提供预处理程序和其他高级设置的初始配置。可以按原样使用系统提供的这些策略，也可以将其用作自定义策略的基础。

如果使用系统提供的策略为基础，则导入规则更新可能会修改基本策略中的设置。但是，可将自定义策略配置为不对系统提供的基本策略自动执行这些更改。这样一来，您可以独立于规则更新导入计划，手动更新系统提供的基本策略。在任一情况下，规则更新对基本策略所做出的更改不会更改或覆盖 My Changes 或任何其他层中的设置。有关详细信息，请参阅第 12-4 页上的允许规则更新修改系统提供的基本策略。

系统提供的入侵和网络分析策略以类似方式命名，但是包含不同的配置。例如， Balanced Security and Connectivity 网络分析策略和 Balanced Security and Connectivity 入侵策略可协同工作，并一同在入侵规则更新中进行更新。有关详细信息，请参阅第 11-6 页上的了解系统提供的策略。

了解自定义基本策略

许可证：保护

如果您不希望使用系统提供的策略作为网络分析或入侵策略中的基本策略，则可以使用自定义策略作为基础。您可以调整自定义策略中的设置，以对您最重要的方式检查流量，从而能够提高性能以及您有效响应其生成的事件的能力。

可以链接最多五个自定义策略，这五个策略中有四个使用其余四个之一以前创建的策略作为其基本策略；第五个策略必须使用系统提供的策略作为其基础。

如果更改被其他策略用作基础的自定义策略，所做的更改会自动作为使用该基础的策略的默认设置。此外，由于在策略链中所有策略都以系统提供的策略作为最终基础，因此，导入规则更新可能会影响您的策略，即使您使用自定义基本策略亦如此。如果链中的第一个自定义策略（即使用系统提供的策略作为其基础的策略）允许规则更新修改其基本策略，则您的策略可能会受影响。有关更改此设置的信息，请参阅第 12-4 页上的允许规则更新修改系统提供的基本策略。

无论如何进行更改，对基本策略的更改（由规则更新或在修改用作基本策略的自定义策略时所做出）都不会更改或覆盖 My Changes 或任何其他层中的设置。

更改基本策略

许可证：保护

您可以为网络分析或入侵策略选择其他基本策略，或者允许规则更新修改系统提供的基本策略，而不影响较高层中的更改。

要更改基本策略，请执行以下操作：

步骤 1　编辑策略时，点击导航面板中的 **Policy Information**。

系统将显示 Policy Information 页面。

步骤 2　从 **Base Policy** 下拉列表中选择基本策略。

步骤 3　或者，如果选择系统提供的基本策略，则点击 **Manage Base Policy** 指定入侵规则更新是否可以自动修改基本策略。

有关详细信息，请参阅第 12-4 页上的允许规则更新修改系统提供的基本策略。

步骤 4　保存策略、继续编辑、丢弃更改、恢复为基本策略中的默认配置设置，或退出并在系统缓存中保留更改。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

允许规则更新修改系统提供的基本策略

许可证：保护

您导入的规则更新会为系统提供的策略提供已修改的网络分析预处理程序设置、已修改的入侵策略高级设置、新的和已更新的入侵规则，以及已修改的现有规则状态。规则更新还可以删除规则并提供新规则类别和默认变量。有关详细信息，请参阅第 35-8 页上的导入规则更新和本地规则文件。

规则更新始终通过对预处理程序、高级设置和规则的任何更改来修改系统提供的策略。对默认变量和规则类别的更改在系统级别处理。有关详细信息，请参阅第 12-3 页上的了解系统提供的基本策略。

当使用系统提供的策略作为基本策略时，您可以允许规则更新修改基本策略，在此情况下，基本策略是系统提供的策略的副本。如果允许规则更新更新基本策略，则新规则更新在基本策略中所做的更改与其对用作基本策略的系统提供的策略所做出的更改相同。如果您未曾对相应的设置进行过修改，则基本策略中的设置会决定策略中的设置。但是，规则更新不会覆盖您在策略中所做出的更改。

如果不允许规则更新更新基本策略，则可以在导入一个或多个规则更新后手动更新基本策略。

无论入侵策略中的规则状态如何或者是否允许规则更新更新基本入侵策略，规则更新始终会删除 VRT 删除的入侵规则。在将更改重新应用于网络流量之前，当前应用的入侵策略中的规则行为如下：

- 已禁用的规则保持禁用。
- 设置为 Generate Events 的规则在触发时继续生成事件。
- 设置为 Drop and Generate Events 的规则在触发时继续生成事件并丢弃有问题的数据包。

除非同时满足以下两个条件，否则规则更新不会修改自定义基本策略：

- 允许规则更新修改父策略（即用于创建自定义基本策略的策略）的系统提供的基本策略。
- 未曾在父策略中做出将覆盖父策略的基本策略中相应设置的更改。

如果同时满足两个条件，则在保存父策略时，规则更新中的更改会传递到子策略（即，使用自定义基本策略的策略）。

例如，如果规则更新启用以前禁用的入侵规则，并且您未曾修改该规则在父入侵策略中的状态，则在保存父策略时，已修改的规则状态会传递到基本策略。

同样，如果规则更新修改默认预处理程序设置，并且您未曾修改父网络分析策略中的设置，则在保存父策略时，已修改的设置会传递到基本策略。

有关详细信息，请参阅第 12-3 页上的更改基本策略。

要允许规则更新修改系统提供的基本策略，请执行以下操作：

步骤 1　编辑使用系统提供的策略作为其基本策略的策略时，点击导航面板中的 **Policy Information**。

系统将显示 Policy Information 页面。

步骤 2　点击 **Manage Base Policy**。

系统将显示 Base Policy 摘要页面。

步骤 3　选择或清除 **Update when a new Rule Update is installed** 复选框。

在清除此复选框的情况下保存策略然后导入规则更新时， Base Policy 摘要页面上会显示 **Update Now** 按钮，并且该页面上的状态消息会更新，通知此策略已过期。或者，可以点击 **Update Now**，使用最新导入的规则更新中的更改更新基本策略。

步骤 4　保存策略、继续编辑、丢弃更改、恢复为基本策略中的默认配置设置，或退出并在系统缓存中保留更改。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

管理层

许可证：保护

Policy Layers 页面提供网络分析或入侵策略的完整层堆栈的单页摘要。在此页面上，可以添加共享和非共享层，复制、合并、移动和删除层，访问每层的摘要页面，以及访问每层中已启用、禁用和覆盖的配置的配置页面。

对于每层，您均可查看以下信息：

- 层是内置层、共享用户层还是非共享用户层
- 哪些层包含最高（即最有效）预处理程序或高级设置配置（按功能名称）
- 在入侵策略中，在该层中设置了其状态的入侵规则的数量，以及设置为每个规则状态的规则的数量。

每层的摘要中的功能名称指明在该层中已启用、禁用、覆盖或继承哪些配置，如下所示：

当功能...	功能名称...
在层中已启用	以纯文本编写
在层中已禁用	删除
被更高层中的配置覆盖	以斜体文本编写
从更低层继承	不存在

此页面还提供所有已启用预处理程序（网络分析）或高级设置（入侵）的实际效果的摘要，以及入侵策略和入侵规则的摘要。

下表列出 Policy Layers 页面上可执行的操作。

表 12-1　网络分析和入侵策略层配置操作

要...	您可以...
显示 Policy Information 页面	点击 **Policy Summary**。 有关可以在 Policy Information 页面上采取的操作的信息，请参阅第 20-1 页上的使用规则调整入侵策略、第 14-1 页上的网络分析策略使用入门和第 19-1 页上的入侵策略使用入门。
显示某个层摘要页面	点击该层对应的行中的层名称，或者点击用户层旁边的编辑图标 ( )。您也可以点击查看图标 ( ) 来访问共享层的只读摘要页面。 有关可以在层的摘要页面上采取的操作的信息，请参阅第 12-8 页上的在策略之间共享层、第 12-12 页上的在层中配置预处理程序和高级设置和第 12-10 页上的配置层中的入侵规则。
访问层级别预处理程序或高级设置配置页面	点击该层对应的行中的功能名称。请注意，配置页面在基本策略和共享层中为只读。有关详细信息，请参阅第 12-12 页上的在层中配置预处理程序和高级设置。

表 12-1　网络分析和入侵策略层配置操作 （续）

要...	您可以...
访问按规则状态类型过滤的层级别规则配置页面	点击该层的摘要中的丢弃并生成事件图标 ( )、生成事件图标 ( ) 或已禁用图标 ( )。如果该层不包含设置为所选规则状态的规则，则不会显示任何规则。
向策略中添加层	请参阅第 12-6 页上的添加层。
从另一策略添加共享层	请参阅第 12-8 页上的在策略之间共享层。
更改层的名称或描述	请参阅第 12-7 页上的更改层名称和描述。
移动、复制或删除层	请参阅第 12-7 页上的移动、复制和删除层。
将层合并到其下方的下一层中	请参阅第 12-8 页上的合并层。

要使用 Policy Layers 页面，请执行以下操作：

步骤 1　编辑策略时，点击导航面板中的 **Policy Layers**。

系统将显示 Policy Layers 摘要页面。

步骤 2　可以采取网络分析和入侵策略层配置操作表中的任何操作。

步骤 3　保存策略、继续编辑、丢弃更改、恢复为基本策略中的默认配置设置，或退出并在系统缓存中保留更改。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

添加层

许可证：保护

您最多可以向网络分析或入侵策略中添加 200 层。添加的层显示为策略中的最高层。初始状态对于所有功能都为 Inherit，并且在入侵策略中，未设置事件过滤、动态状态或警报规则操作。

要向网络分析或入侵策略中添加层，请执行以下操作：

步骤 1　编辑策略时，点击导航面板中的 **Policy Layers**。

系统将显示 Policy Layers 页面。

步骤 2　点击 User Layers 旁边的添加层图标 ( )。

系统将显示 Add Layer 弹出窗口。

步骤 3　键入唯一层**名称**，然后点击 **OK**。

新层显示为 User Layers 下最上方的层。

步骤 4　保存策略、继续编辑、丢弃更改、恢复为基本策略中的默认配置设置，或退出并在系统缓存中保留更改。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

更改层名称和描述

许可证：保护

您可以在网络分析或入侵策略中更改用户可配置层的名称，或者添加或修改在编辑该层时可视的描述。

要更改层的名称并添加或修改其描述，请执行以下操作：

步骤 1　编辑策略时，点击导航面板中的 **Policy Layers**。

系统将显示 Policy Layers 页面。

步骤 2　点击要编辑的用户层旁边的编辑图标 ( )。

系统将显示该层的摘要页面。

步骤 3　可以采取以下操作：

- 修改层**名称**。
- 添加或修改层**描述**。

步骤 4　保存策略、继续编辑、丢弃更改、恢复为基本策略中的默认配置设置，或退出并在系统缓存中保留更改。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

移动、复制和删除层

许可证：保护

您可以在网络分析或入侵策略中复制、移动或删除用户层，包括初始 My Changes 层。请注意以下考虑事项：

- 在复制层时，副本显示为最高层。
- 复制共享层会创建可选择在以后与其他策略共享的未共享副本。
- 不能删除共享层；已启用共享但未曾与其他策略共享的层不是共享层。

要复制、移动或删除层，请执行以下操作：

步骤 1　编辑策略时，点击导航面板中的 **Policy Layers**。

系统将显示 Policy Layers 页面。

步骤 2　可以采取以下操作：

- 要复制层，请点击要复制的层的复制图标 ( )。

  页面将刷新，并且该层的副本显示为最高层。
- 要在 User Layers 页面区域内将层上移或下移，请点击层摘要中的任何开放区域并将其拖动，直至位置箭头 ( ) 指向层上方或下方要将该层移到的行。

  屏幕将刷新，并且层显示在新位置中。
- 要删除层，请点击要删除的层的删除图标 ( )，然后点击 **OK**。

  页面将刷新，并且该层删除成功。

步骤 3　保存策略、继续编辑、丢弃更改、恢复为基本策略中的默认配置设置，或退出并在系统缓存中保留更改。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

合并层

许可证：保护

您可以将网络分析或入侵策略中的用户可配置层与其下方的下一用户层合并。合并层保留任一层特有的所有设置，并且如果两层均包含同一预处理程序、入侵规则或高级设置的设置，则会接受更高层中的设置。合并层保留更低层的名称。

如果在策略中创建的共享层会添加到其他策略，则可以将该共享层正上方的非共享层与该共享层合并，但是不能将该共享层与其下方的非共享层合并。

如果在一个策略中添加的共享层在其他策略中已创建，则可以将该共享层合并到其正下方的非共享层中，所生成的层不再共享；不能将非共享层合并到其下方的共享层中。

要将用户层与其下方的用户层合并，请执行以下操作：

步骤 1　编辑策略时，点击导航面板中的 **Policy Layers**。

系统将显示 Policy Layers 页面。

步骤 2　点击两层的上层中的合并图标 ( )，然后点击 **OK**。

页面将刷新，该层与其下方的层合并成功。

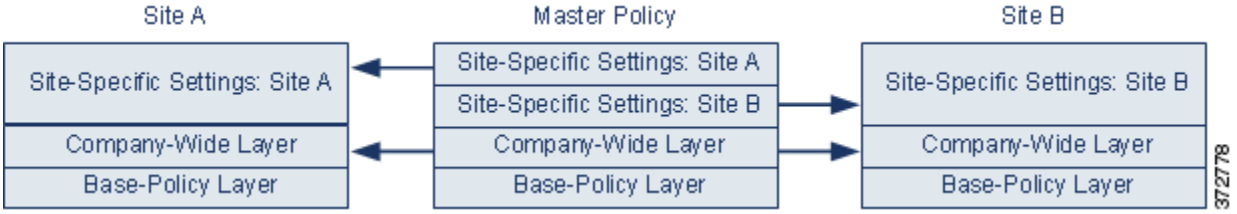
步骤 3　保存策略、继续编辑、丢弃更改、恢复为基本策略中的默认配置设置，或退出并在系统缓存中保留更改。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

在策略之间共享层

许可证：保护

您可以将用户可配置层与同一类型（入侵或网络分析）的其他策略共享。在共享层中修改配置后提交更改时，系统会更新使用该共享层的所有策略，并为您提供所有受影响策略的列表。只能在已创建该层的策略中修改共享层功能配置。

下图显示充当站点特定策略的源的示例主策略。



图中的主策略包括具有适用于位于 Site A 和 Site B 的策略的设置的公司范围层。它还包括每个策略的站点特定层。例如，如果使用网络分析策略，则 Site A 在受监控网络上可能没有 Web 服务器，并且不需要 HTTP Inspect 预处理程序的保护或处理开销，但两个站点均可能需要 TCP 数据流预处理。可在与两个站点共享的公司范围层启用 TCP 数据流处理，在与 Site A 共享的站点特定层

禁用 HTTP Inspect 预处理程序，在与 Site B 共享的站点特定层启用 HTTP Inspect 预处理程序。如果编辑站点特定策略中更高层中的配置，还可进一步调整每个站点的策略，必要时可借助任何配置调整。

示例主策略中的扁平化网络设置不大可能对流量监控有用，但配置和更新站点特定策略所节省的时间使得它成为策略层的一种有用应用。

也可使用许多其他层配置。例如，您可以按公司、部门、网络来定义策略层。如果使用入侵策略，则还可以在一层中包含高级设置，在另一层中包含规则设置。

提示　当基本策略是在其中已创建要共享的层的自定义策略时，不能向策略中添加共享层。当尝试保存更改时，将出现一条错误消息，指明策略包含循环依赖。有关详细信息，请参阅第 12-3 页上的了解自定义基本策略。

要与其他策略共享某个层，必须执行以下操作：

- 在要共享的层的层摘要页面上启用共享。
- 在要共享的策略的 Policy Layers 页面上添加共享层。

不能对正在由另一个策略使用的层禁用共享；必须先从另一个策略中删除该层，或者删除另一个策略。

要启用或禁用与其他策略共享层，请执行以下操作：

步骤 1　编辑策略时，点击导航面板中的 **Policy Layers**。

系统将显示 Policy Layers 页面。

步骤 2　点击要与其他策略共享的层旁边的编辑图标 ( )。

系统将显示该层的摘要页面。

步骤 3　选择（启用）或清除（禁用）**Sharing** 复选框。

步骤 4　保存策略、继续编辑、丢弃更改、恢复为基本策略中的默认配置设置，或退出并在系统缓存中保留更改。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

要向策略中添加共享层，请执行以下操作：

步骤 1　编辑策略时，点击导航面板中的 **Policy Layers**。

系统将显示 Policy Layers 页面。

步骤 2　点击 User Layers 旁边的添加共享层图标 ( )。

系统将显示 Add Shared Layer 弹出窗口。

步骤 3　从 Add Shared Layer 下拉列表中选择要添加的共享层，然后点击 **OK**。

系统将显示 Policy Layers 摘要页面，并且所选共享层显示为策略中的最高层。

如果任何其他策略中没有共享层，则不会显示下拉列表；在弹出窗口中点击 **OK** 或 **Cancel** 返回到 Policy Layers 摘要页面。

步骤 4　保存策略、继续编辑、丢弃更改、恢复为基本策略中的默认配置设置，或退出并在系统缓存中保留更改。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

配置层中的入侵规则

许可证：保护

在入侵策略中，可以为任何用户可配置层中的规则设置规则状态、事件过滤、动态状态、警报和规则注释。访问要进行更改的层之后，可以按照在入侵策略 Rules 页面上所用的相同方法在该层的 Rules 页面上添加设置；请参阅第 20-1 页上的使用规则调整入侵策略。

可以在该层的 Rules 页面上查看个别层设置，也可以在 Rules 页面的策略视图中查看所有设置的实际效果。在 Rules 页面的策略视图中修改规则设置时，修改的是策略中的最高用户可配置层。可以在任何 Rules 页面上使用层下拉列表切换到另一层。

下表描述在多个层中配置相同类型设置的效果。

表 12-2　　层规则设置

您可以设置...	此设置类型...	以...
一个	规则状态	覆盖为更低层中的规则设置的规则状态，并忽略在更低层中为该规则配置的所有阈值、抑制、基于速率的规则状态和警报。有关详细信息，请参阅第 20-17 页上的设置规则状态。 如果希望规则从基本策略或更低层继承其状态，请将规则状态设置为 Inherit。请注意，当在入侵策略 Rules 页面上操作时，不能将规则状态设置为 Inherit。 另请注意，当在特定层的 Rules 页面上查看规则状态设置时，规则状态设置会进行颜色编码：其有效状态设置在更低层中的规则以黄色突出显示；其有效状态设置在更高层中的规则以红色突出显示；其有效状态设置在当前层中的规则不突出显示。由于入侵策略 Rules 页面是所有规则设置的实际效果的综合视图，因此规则状态在此页面上未进行颜色编码。
一个	阈值 SNMP 警报	覆盖更低层中规则的相同类型设置。请注意，设置阈值会覆盖该层中规则的任何现有阈值。有关详细信息，请参阅第 20-19 页上的配置事件阈值和第 20-28 页上的添加 SNMP 警报。
一个或多个	抑制 基于速率的规则状态	将每个所选规则的相同类型设置向下累积合并至为该规则设定规则状态所在的第一层。系统会忽略设定规则状态所在层下方的设置。有关详细信息，请参阅第 20-23 页上的按入侵策略配置抑制和第 20-25 页上的添加动态规则状态。
一个或多个	注释	向规则中添加注释。注释因规则而异，而非因策略或层而异。可以向任何层中的规则添加一条或多条注释。有关详细信息，请参阅第 20-8 页上的为规则添加规则注释。

例如，如果在一层中将规则状态设置为 Drop and Generate Events，在更高层中设置为 Disabled，则入侵策略 Rules 页面显示该规则已禁用。

又例如，如果在一层中将规则的基于源的抑制设置为 192.168.1.1，并且还在另一层中将该规则的基于目标的抑制设置为 192.168.1.2，则 Rules 页面显示累积效果是抑制源地址 192.168.1.1 和目标地址 192.168.1.2 的事件。请注意，抑制和基于速率的规则状态设置会将每个所选规则的相同类型设置累积合并至为该规则设定规则状态所在的第一层。系统会忽略设定规则状态所在层下方的设置。

要在层中修改规则，请执行以下操作：

步骤 1　编辑入侵策略时，展开导航面板中的 **Policy Layers** 并展开要修改的策略层。

步骤 2　点击要修改的策略层正下方的 **Rules**。

系统将显示该层的 Rules 页面。

可以修改层规则设置表中的任何设置。有关配置入侵规则的详细信息，请参阅第 20-1 页上的使用规则调整入侵策略。

要从可编辑层删除单项设置，请双击该层 Ruels 页面上的规则消息，以显示规则详细信息。点击要删除的设置旁边的 **Delete**，然后双击 **OK**。

步骤 3　保存策略、继续编辑、丢弃更改、恢复为基本策略中的默认配置设置，或退出并在系统缓存中保留更改。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

移除多层规则设置

许可证：保护

您可以在入侵规则 Rules 页面上选择一条或多条规则，然后从入侵策略中的多个层同时移除特定类型的事件过滤器、动态状态或警报。

系统将向下移除每层中设置的设置类型，直至移除所有设置或遇到为规则设置了规则状态的层。如果遇到设置了规则状态的层，则系统会从该层中移除设置并停止移除设置类型。

当系统在共享层或在基本策略中遇到该设置类型时，如果策略中的最高层可以编辑，则系统会将该规则的剩余设置和规则状态复制到该可编辑层。否则，如果策略中的最高层是共享层，系统会在该共享层上方创建新的可编辑层，并将该规则的剩余设置和规则状态复制到该可编辑层。

注　移除从共享层或基本策略派生的规则设置会导致忽略从更低层或基本策略中对该规则做出的任何更改。要停止忽略从更低层或基本策略做出的更改，请在最高层的摘要页面上将规则状态设置为 **Inherit**。有关详细信息，请参阅第 20-17 页上的设置规则状态。

要移除多层中的规则集，请执行以下操作：

步骤 1　编辑入侵策略时，点击导航面板中 Policy Information 正下方的 **Rules**。

提示　您也可以从任何层的 Rules 页面上的层下拉列表中选择 **Policy**，或者选择 Policy Information 页面上的 **Manage Rules**。

系统将显示入侵策略 Rules 页面。

步骤 2　选择要从中移除多个设置的规则。您有以下选项：

- 要选择特定规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

有关查找规则的信息，请参阅第 20-9 页上的了解入侵策略中的规则过滤和第 20-16 页上的在入侵策略中设置规则过滤器。

步骤 3　您有以下选项：

- 要移除规则的所有阈值，请选择 **Event Filtering > Remove Thresholds**。
- 要移除规则的所有抑制，请选择 **Event Filtering > Remove Suppressions**。
- 要移除规则的所有基于速率的规则状态，请选择 **Dynamic State > Remove Rate-Based Rule States**。
- 要移除规则的所有 SNMP 警报设置，请选择 **Alerting > Remove SNMP Alerts**。

系统将显示一个确认弹出窗口。

注　移除从共享层或基本策略派生的规则设置会导致忽略从更低层或基本策略中对该规则做出的任何更改。要停止忽略从更低层或基本策略做出的更改，请在最高层的摘要页面上将规则状态设置为 **Inherit**。有关详细信息，请参阅第 20-17 页上的设置规则状态。

步骤 4　点击 **OK**。

系统移除所选设置并将规则的剩余设置复制到策略中的最高可编辑层。请参阅此操作步骤的简介，以了解如何影响系统复制剩余设置的条件。

步骤 5　保存策略、继续编辑、丢弃更改、恢复为基本策略中的默认配置设置，或退出并在系统缓存中保留更改。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

接受来自自定义基本策略的规则更改

许可证：保护

当未曾添加层的自定义网络分析或入侵策略使用另一个自定义策略作为其基本策略时，在以下情况下，必须将规则设置为继承其规则状态：

- 删除为基本策略中的规则设置的事件过滤器、动态状态或 SNMP 警报，以及
- 您希望规则接受在用作基本策略的另一个自定义策略中对其做出的后续更改

以下操作步骤说明如何完成此任务。要在已添加层的策略中接受这些规则的设置，请参阅第 12-11 页上的移除多层规则设置。

要在未曾添加层的策略中接受规则更改，请执行以下操作：

步骤 1　编辑入侵策略时，展开导航面板中的 **Policy Layers** 链接，然后展开 **My Changes** 链接。

步骤 2　点击 My Changes 正下方的 **Rules** 链接。

系统将显示 My Changes 层的 Rules 页面。

步骤 3　选择要接受其设置的规则。您有以下选项：

- 要选择特定规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

有关查找规则的信息，请参阅第 20-9 页上的了解入侵策略中的规则过滤和第 20-16 页上的在入侵策略中设置规则过滤器。

步骤 4　从 **Rule State** 下拉列表中选择 **Inherit**。

步骤 5　保存策略、继续编辑、丢弃更改、恢复为基本策略中的默认配置设置，或退出并在系统缓存中保留更改。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

在层中配置预处理程序和高级设置

许可证：保护

您使用类似的机制在网络分析策略中配置预处理程序和在入侵策略中配置高级设置。您可以启用和禁用预处理程序（在网络分析 Settings 页面上）和入侵策略高级设置（在入侵策略 Advanced Settings 页面上）。这些页面还提供所有相关功能的有效状态的摘要。例如，如果网络分析 SSL 预处理程序在一层中已禁用但在更高层中已启用，则 Settings 页面将其显示为已启用。在这些页面上做出的更改显示在策略的顶层中。

您也可以在用户可配置层的摘要页面上启用或禁用预处理程序或高级设置并访问其配置页面。在此页面上，可以修改层名称和描述，并配置是否将该层与同一类型的其他策略共享；有关详细信息，请参阅第 12-8 页上的在策略之间共享层。可以通过选择导航面板中 **Policy Layers** 下方的层名称来切换到另一层的摘要页面。

启用预处理程序或高级设置时，在导航面板中的层名称下方会显示指向该功能的配置页面的子链接，并且在层的摘要页面上的功能旁边会显示编辑图标 ( )；在层中禁用该功能或将其设置为 Inherit 时，这些图标会消失。

设置预处理程序或高级设置的状态（已启用或已禁用）会覆盖更低层中该功能的状态和配置设置。如果希望预处理程序或高级设置从基本策略或更低层继承其状态和配置，请将其设置为 **Inherit**。请注意，当在 Settings 或 Advanced Settings 页面上操作时，无法选择 Inherit。

每层摘要页面上的颜色编码按如下指明有效配置位于更高层、更低层还是当前层中：

- 红色 - 有效配置位于更高层
- 黄色 - 有效配置位于更低层
- 无光度 - 有效配置位于当前层

由于 Settings 和 Advanced Settings 页面是所有相关设置的综合视图，因此，这些页面不使用颜色编码指明有效配置的位置。

系统使用已启用该功能的最高层中的配置。除非明确修改配置，否则系统使用默认配置。例如，如果在一层中启用并修改网络分析 DCE/RPC 预处理程序，并且还在更高层中将其启用但不修改，则系统使用更高层中的默认配置。

下表描述用户可配置层的摘要页面上可执行的操作。

表 12-3　　层摘要页面操作

要...	您可以...
修改层名称或描述	为 **Name** 或 **Description** 键入新值。
与其他入侵策略共享层	选择 **Allow this layer to be used by other policies**。 有关详细信息，请参阅第 12-8 页上的在策略之间共享层。
在当前层中启用或禁用预处理程序/高级设置	点击功能旁边的 **Enabled** 或 **Disabled**。 启用时，在导航面板中的层名称下方会显示指向配置页面的子链接，并且在功能旁边的摘要页面上会显示编辑图标 ( )。 禁用会移除子链接和编辑图标。
从当前层下方最高层中的设置继承预处理程序/高级设置状态和配置	点击 **Inherit**。 页面将刷新，如果功能已启用，则不再显示导航面板中的功能子链接和编辑图标。
访问已启用的预处理程序/高级设置的配置页面	点击编辑图标 ( ) 或功能子链接以修改当前配置。 请注意， Back Orifice 预处理程序没有用户可配置选项。

要在用户层中修改预处理程序/高级设置，请执行以下操作：

步骤 1　编辑策略时，请展开导航面板中的 **Policy Layers**，然后点击要修改的层的名称。

系统将显示该层的摘要页面。

步骤 2　可以采取层摘要页面操作表中的任何操作。

步骤 3　保存策略、继续编辑、丢弃更改、恢复为基本策略中的默认配置设置，或退出并在系统缓存中保留更改。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

自定义流量预处理

访问控制策略中的多项高级设置可监管需要特定专门技术才能做出的入侵检测和防御配置。高级设置通常只需要很少的修改或者不需要修改，不通用于各个部署。

本章介绍如何设置以下首选项：

- 第 13-1 页上的为访问控制设置默认入侵策略说明如何更改访问控制策略的默认入侵策略，用于在系统准确确定如何检测流量之前初始检测流量。
- 第 13-2 页上的利用网络分析策略自定义预处理说明如何通过分配自定义网络分析策略预处理匹配流量，根据特定安全区域、网络定制某些流量预处理选项。

其他章节介绍访问控制策略的策略预处理和性能选项。有关详情，请参阅：

- 第 17-1 页上的配置高级传输/网络设置
- 第 18-1 页上的在被动部署中调整预处理
- 第 10-5 页上的调整入侵防御性能
- 第 10-15 页上的调整文件和恶意软件检测性能和存储

为访问控制设置默认入侵策略

许可证：任何环境

每个访问控制策略使用其*默认入侵策略*初始检测流量，然后系统才能准确确定如何检测该流量。之所以这样做，是因为有时系统必须处理连接中的前几个数据包，**允许其通过**，然后它才能确定哪条访问控制规则（如有）将处理流量。因此，这些数据包不会未经检测就到达其目的地，然而，您可以使用称为默认入侵策略的入侵策略对其进行检测并生成入侵事件。

默认入侵策略在执行应用控制和 URL 过滤时尤为有用，因为系统无法在客户端与服务器之间完全建立连接之前识别应用或过滤 URL。例如，如果一个数据包与具有应用或 URL 条件的访问控制规则中的所有其他条件相匹配，则将允许该数据包及其后续数据包通过，直到建立连接且完成应用或 URL 识别，通常为 3 到 5 个数据包。

系统使用默认入侵策略检测允许的这些数据包，他们可以生成事件，内联时还可阻止恶意流量。系统识别应处理连接的访问控制规则或默认操作后，相应地处理和检测连接中剩余的数据包。

在创建访问控制策略时，其默认入侵策略取决于您**首先**选择的默认操作。用于访问控制的初始默认入侵策略如下：

- Balanced Security and Connectivity（系统提供的策略）是在您首先选择 **Intrusion Prevention** 默认操作时访问控制策略的默认入侵策略。
- No Rules Active 是在您首先选择 **Block all traffic** 默认操作时访问控制策略的默认入侵策略。尽管选择此选项会禁用对上述已允许数据包的入侵检测，但是，如果您对入侵数据不感兴趣，它可提高性能。

注　如未执行入侵检测，则保持 No Rules Active 策略作为为默认入侵策略。有关详细信息，请参阅第 4-12 页上的对访问控制策略和规则进行故障排除。

请注意，如果您在创建访问控制策略后更改默认操作，则默认入侵策略不会自动更改。要手动更改，请使用访问控制策略的高级选项。

要更改访问控制策略的默认入侵策略，请执行以下操作：

步骤 1　在想要更改其默认入侵策略的访问控制策略中，选择 **Advanced** 选项卡，然后点击 Network Analysis and Intrusion Policies 分区旁的编辑图标 ( )。

系统将显示 Network and Analysis Policies 对话框。

步骤 2　从 **Intrusion Policy used before Access Control rule is determined** 下拉列表中，选择一条默认入侵策略。您可以选择系统或用户创建的策略。

请注意，如果选择用户创建的策略，可点击编辑图标 ( ) 在新窗口中编辑该策略。无法编辑系统提供的策略。

注意事项　请勿使用 `Experimental Policy 1`，除非思科代表指示这样做。思科使用该策略进行测试。

步骤 3　点击 **OK**，保存更改。

必须应用访问控制策略，使更改生效。

利用网络分析策略自定义预处理

许可证：任何环境

*网络分析策略*监管如何解码和预处理流量，以便进一步对其进行评估，特别适用于可能表明入侵尝试的异常流量。此流量预处理发生在安全情报黑名单之后，但是在入侵策略详细检测数据包之前。默认情况下，系统提供的 Balanced Security and Connectivity 网络分析策略应用于访问控制策略处理的*所有*流量。

提示　系统提供的 Balanced Security and Connectivity 网络分析策略和 Balanced Security and Connectivity 入侵策略共同发挥作用，均可在入侵规则更新中更新。但是，网络分析策略主要监管预处理选项，而入侵策略主要监管入侵规则。

调整预处理的一个简单方法是创建和使用自定义网络分析策略作为默认值；请参阅第 14-2 页上的创建自定义网络分析策略。可用的调整选项因预处理程序而异。

对于复杂部署的高级用户，您可以创建多个网络分析策略，每个策略经过定制可采用不同方式预处理流量。然后，可以将系统配置为使用这些策略通过不同的安全区域、或监管流量预处理。

为此，请向访问控制策略中添加自定义*网络分析规则*。每条规则均有：

- 一组规则条件，用于识别想要预处理的特定流量
- 一条关联的网络分析策略，想要用来预处理符合所有规则条件的流量

在系统预处理流量时，其将数据包按照规则编号自上而下的顺序与网络分析规则相匹配。不与任何网络分析规则匹配的流量由默认网络分析策略预处理。

注　如果禁用预处理程序，但系统需要根据已启用的入侵或预处理程序规则评估预处理的数据包，系统将自动启用和使用预处理程序，尽管它在网络分析策略中保持禁用。定制预处理，特别是使用多个自定义网络分析策略，是一项**高级**任务。由于预处理和入侵检测如此密切相关，因此，请**务必**小心确保允许网络和入侵策略检测每个数据包，以实现互补。有关详细信息，请参阅第 11-9 页上的自定义策略的限制。

有关详细信息，请参阅：

- 第 13-3 页上的为访问控制设置默认网络分析策略
- 第 13-4 页上的使用网络分析规则指定要预处理的流量
- 第 13-7 页上的管理网络分析规则

为访问控制设置默认网络分析策略

许可证：任何环境

默认情况下，系统提供的 Balanced Security and Connectivity 网络分析策略应用于访问控制策略处理的所有流量。如果您添加网络分析规则来定制流量预处理选项，默认网络分析策略预处理这些规则未处理的所有流量。

访问控制策略的高级设置可供您更改此默认策略。

要更改访问控制策略的默认网络分析策略，请执行以下操作：

步骤 1　在想要更改默认网络分析策略的访问控制策略中，选择 **Advanced** 选项卡，然后点击 Network Analysis and Intrusion Policies 分区旁的编辑图标 ( )。

系统将显示 Network and Analysis Policies 对话框。

步骤 2　从 **Default Network Analysis Policy** 下拉列表中，选择一条默认网络分析策略。您可以选择系统或用户创建的策略。

请注意，如果选择用户创建的策略，可点击编辑图标 ( ) 在新窗口中编辑该策略。无法编辑系统提供的策略。

注意事项　请**勿**使用 `Experimental Policy 1`，除非思科代表指示这样做。思科使用该策略进行测试。

步骤 3　点击 **OK** 保存您的更改。

必须应用访问控制策略，使更改生效。

使用网络分析规则指定要预处理的流量

许可证：任何环境

在访问控制策略的高级设置中，您可以使用网络分析规则定制网络流量的预处理配置。与访问控制规则相似，网络分析规则从 1 开始编号。

在系统预处理流量时，它将数据包按照升序规则编号自上而下的顺序与网络分析规则相匹配，然后根据所有条件都匹配的第一个规则预处理流量。下表描述可添加到规则的条件。

表 13-1　网络分析规则条件类型

此条件...	匹配流量...	详细信息
区域	在特定安全区域中通过一个接口进入或离开设备	安全区域是根据您的部署和安全策略划分的一个或多个接口的逻辑分组。要构建区域条件，请参阅第 13-5 页上的按区域预处理流量。
网络	通过其源 IP 地址或目标 IP 地址	您可以明确指定 IP 地址。要构建网络条件，请参阅第 13-6 页上的按网络预处理流量。

如果不为规则配置特殊条件，则系统将不根据该条件匹配流量。例如，一条包含网络条件但不含区域条件的规则根据其源 IP 地址或目标 IP 地址评估流量，不管其进出接口如何。不与任何网络分析规则匹配的流量由默认网络分析策略预处理。

要添加自定义网络分析规则，请执行以下操作：

步骤 1　在想要创建自定义预处理配置的访问控制策略中，选择 **Advanced** 选项卡，然后点击 Intrusion and Network Analysis Policies 分区旁的编辑图标 ( )。

系统将显示 Network and Analysis Policies 对话框。如果您尚未添加任何自定义网络分析规则，模块接口指明您拥有 **No Custom Rules**，否则显示您已配置的规则数量。

提示　点击 **Network Analysis Policy List** 以在新窗口中显示 Network Analysis Policy 页面。使用此页面查看和编辑自定义网络分析策略；请参阅第 14-3 页上的管理网络分析策略

步骤 2　在 **Network Analysis Rules** 旁，点击指明您所拥有的自定义规则数量的语句。

系统将展开对话框以显示自定义规则（如有）。

步骤 3　点击 **Add Rule**。

系统将显示网络分析规则编辑器。

步骤 4　构建您的规则条件。您可以使用以下标准限制 NAP 预处理：

- 第 13-5 页上的按区域预处理流量
- 第 13-6 页上的按网络预处理流量

步骤 5　点击 **Network Analysis** 选项卡，然后从 **Network Analysis Policy** 下拉列表中选择一条策略，以便将网络分析策略与规则相关联。

系统使用您选择的网络分析策略预处理符合规则的所有条件的流量。请注意，如果选择用户创建的策略，可点击编辑图标 ( ) 在新窗口中编辑该策略。无法编辑系统提供的策略。

注意事项　请**勿**使用 `Experimental Policy 1`，除非思科代表指示这样做。思科使用该策略进行测试。

步骤 6　点击**添加**。

该规则添加在任何其他规则之后。要更改规则的评估顺序，请参阅第 13-7 页上的管理网络分析规则。

按区域预处理流量

许可证：任何环境

网络分析规则中的区域条件可供您根据其源和目标安全区域预处理流量。安全区域是一个或多个接口的分组。有关创建区域的详细信息，请参阅第 2-30 页上的使用安全区域。

在单一区域条件中最多可向每个 **Source Zones** 和 **Destination Zones** 添加 50 个区域：

- 要匹配从该区域的一个接口*离开*设备的流量，请将该区域添加到 **Destination Zones**。请注意，由于被动部署的设备不传输流量，您无法在 **Destination Zones** 条件中使用包含被动接口的区域。
- 要匹配从该区域的一个接口*进入*设备的流量，请将该区域添加到 **Source Zones**。

如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

警告图标 (⚠) 指明无效配置，如不包含接口的区域。有关详细信息，请参阅第 4-12 页上的对访问控制策略和规则进行故障排除。

要按区域预处理流量，请执行以下操作：

步骤 1　在想要按区域预处理流量的访问控制策略中，新建一条网络分析规则或编辑现有规则。

有关详细说明，请参阅第 13-4 页上的使用网络分析规则指定要预处理的流量。

步骤 2　在网络分析规则编辑器中，选择 **Zones** 选项卡。

系统将显示 Zones 选项卡。

步骤 3　查找并选择要从 **Available Zones** 添加的区域。

要搜索想要添加的区域，请点击 **Available Zones** 列表上方的 **Search by name** 提示，然后键入区域名称。列表随键入内容进行更新以显示匹配区域。

点击选择一个区域。要选择多个区域，请使用 **Shift** 和 **Ctrl** 键；或者右键单击，然后选择 **Select All**。

步骤 4　点击 **Add to Source** 或 **Add to Destination** 可将选定区域添加到适当的列表。

您也可以拖放选定区域。

步骤 5　保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

按网络预处理流量

许可证：任何环境

网络分析规则中的网络条件可供您按照源 IP 地址和目标 IP 地址预处理流量。您可以手动为想要预处理的流量指定源 IP 地址和目标 IP 地址，也可以用网络对象配置网络条件，这些网络对象可重用并将名称与一个或多个 IP 地址和地址块相关联。

提示 创建网络对象后，您不仅可以使用它构建网络分析规则，还可用来表示系统模块接口中各种其他位置的 IP 地址。您可以使用对象管理器创建这些对象；也可在配置网络分析规则时即时创建网络对象。有关详细信息，请参阅第 2-3 页上的使用网络对象。

在单一网络条件中最多可向每个 **Source Networks** 和 **Destination Networks** 添加 50 个项目：

- 要从 IP 地址匹配流量，请配置 **Source Networks**。
- 要将流量与 IP 地址相匹配，请配置 **Destination Networks**。

如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

在构建网络条件时，警告图标 ( ) ）指明无效配置。有关详细信息，参阅第 4-12 页上的对访问控制策略和规则进行故障排除。

要按网络预处理流量，请执行以下操作：

步骤 1 在想要按网络预处理流量的访问控制策略中，新建一条网络分析规则或编辑现有规则。

有关详细说明，请参阅第 13-4 页上的使用网络分析规则指定要预处理的流量。

步骤 2 在网络分析规则编辑器中，选择 **Networks** 选项卡。

系统将显示 Networks 选项卡。

步骤 3 查找并选择要从 **Available Networks** 添加的网络，如下所示：

- 要即时添加网络对象，然后可将其添加到该条件，请点击 **Available Networks** 列表上方的添加图标 ( )；请参阅第 2-3 页上的使用网络对象。
- 要搜索想要添加的网络，请点击 **Available Networks** 列表上方的 **Search by name or value** 提示，然后键入对象名称或其中一个对象组件的值。列表随键入内容进行更新以显示匹配对象。

要选择一个对象，请点击它。要选择多个对象，请使用 Shift 和 Ctrl 键；或者右键单击，然后选择 **Select All**。

步骤 4 点击 **Add to Source** 或 **Add to Destination** 可将选定对象添加到适当的列表。

您也可以拖放选定对象。

步骤 5 添加要手动指定的任何源或目标 IP 地址或地址块。

点击 **Source Networks** 或 **Destination Networks** 列表下方的 **Enter an IP address** 提示；然后键入一个 IP 地址或地址块并点击 **Add**。

步骤 6 保存或继续编辑规则。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

管理网络分析规则

许可证：任何环境

网络分析规则只是指定如何预处理与这些限制条件匹配的流量的一组配置和条件。可在现有访问控制策略的高级选项中创建和编辑网络分析规则。每条规则只属于一个策略。

要编辑自定义网络分析规则，请执行以下操作：

步骤 1　在想要更改自定义预处理配置的访问控制策略中，选择 **Advanced** 选项卡，然后点击 Intrusion and Network Analysis Policies 分区旁的编辑图标 ( )。

系统将显示 Network and Analysis Policies 对话框。如果您尚未添加任何自定义网络分析规则，则模块接口指明您扔有 **No Custom Rules**，否则显示您已配置的规则数量。

步骤 2　在 **Network Analysis Rules** 旁，点击指明您所拥有的自定义规则数量的语句。

系统将展开对话框以显示自定义规则（如有）。

步骤 3　编辑您的自定义规则。您有以下选项：

- 要编辑某条规则的条件或更改该规则调用的网络分析策略，请点击该规则旁的编辑图标 ( )。
- 要更改某条规则的评估顺序，请点击该规则并将其拖至正确的位置。要选择多条规则，请使用 Shift 和 Ctrl 键。
- 要删除某条规则，请点击该规则旁的删除图标 ( )。

步骤 4　点击 **OK**，保存更改。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

网络分析策略使用入门

*网络分析策略*管理许多流量预处理选项，并供访问控制策略中的高级设置调用。网络分析相关预处理在安全情报黑名单之后进行，但在访问控制规则详细检查数据包之前，以及所有入侵或文件检查开始之前进行。

默认情况下，系统使用*平衡的安全性和连接性*网络分析策略预处理由访问控制策略处理的所有流量。但是，您可以选择不同的默认网络分析策略执行此预处理。为方便您使用，系统提供若干不可更改的网络分析策略选择，这些策略由漏洞研究团队 (VRT) 针对安全性和连接性的特定平衡专门进行调整。您也可以用具有自定义预处理设置的自定义网络分析策略替换此默认策略。

提示 系统提供的入侵和网络分析策略具有类似的名称，但包含不同的配置。例如，平衡安全性和连接网络分析策略和平衡安全性和连接入侵策略配合工作并可以在入侵规则更新中同时更新。但是，网络分析策略管理的主要是预处理选项，而入侵策略管理的主要是入侵规则。第 11-1 页上的了解网络分析和入侵策略概述网络分析和入侵策略如何协同工作检查流量，以及使用导航面板、解决冲突和确认更改的基本信息。

您也可以为特定安全区域、网络定制流量预处理选项，方式是：创建多个自定义网络分析策略，然后分配这些策略以预处理不同的流量。

注 定制预处理（特别是使用多个自定义网络分析策略）是一项**高级**任务。由于预处理和入侵检查密切相关，检查每个数据包的网络分析和入侵策略**必须**相互补充。系统**不会**为您协调策略，在误配置时将使用默认选项。有关详细信息，请参阅第 11-9 页上的自定义策略的限制。

本章介绍如何创建简单的自定义网络分析策略。本章还包含有关管理网络分析策略的基本信息：编辑和比较等。有关详情，请参阅：

创建自定义网络分析策略

许可证：任何环境

当创建新的网络分析策略时，必须为其提供唯一的名称，指定基本策略并选择*内联模式*。

基本策略定义网络分析策略的默认设置。修改新策略中的设置会覆盖（但不会更改）基本策略中的该设置。您可以使用系统提供的策略或自定义策略作为您的基本策略。有关详细信息，请参阅第 12-2 页上的了解基本层。

网络分析策略的内联模式允许预处理器修改（标准化）和丢弃流量，从而使攻击者避开检测的可能性最小化。请注意，在被动部署中，无论内联模式如何设置，系统都无法影响流量传输。有关详细信息，请参阅第 14-5 页上的允许预处理器影响内联部署中的流量。

要创建网络分析策略，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击 **Create Policy**。

如果在另一策略中有未保存的更改，当系统提示您返回 Network Analysis Policy 页面时，请点击 **Cancel**。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Create Network Analysis Policy 弹出窗口。

步骤 7　在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

步骤 8　指定初始**基本策略**。

您可以将系统提供的策略或自定义策略用作基本策略。

注意事项　请**勿**使用 `Experimental Policy 1`，除非思科代表指示这样做。思科使用该策略进行测试。

步骤 9　指定是否允许预处理器影响内联部署中的流量：

- 要允许预处理器影响流量，请启用 **Inline Mode**。
- 要阻止预处理器影响流量，请禁用 **Inline Mode**。

步骤 10　创建策略：

- 点击 **Create Policy** 创建新策略并返回到 Network Analysis Policy 页面。新策略的设置与其基本策略相同。
- 点击 **Create and Edit Policy** 创建策略并在高级网络分析策略编辑器中对其进行编辑；请参阅第 14-4 页上的编辑网络分析策略。

管理网络分析策略

许可证：任何环境

在 Network Analysis Policy 页面上，可以查看当前的自定义网络分析策略以及以下信息：

- 最近一次修改策略的时间和日期（采用当地时间）以及执行此修改的用户。
- 是否已启用 **Inline Mode** 设置，该设置允许预处理器影响流量
- 哪些访问控制策略使用网络分析策略来预处理流量
- 策略是否有未保存的更改，以及有关何人（如果有任何人）当前正在编辑该策略的信息

Network Analysis Policy 页面上的选项允许您采取下表中的措施。

表 14-1　网络分析策略管理操作

要.....	您可以.....	请参阅.....
创建新的网络分析策略	点击 **Create Policy**。	第 14-2 页上的创建自定义网络分析策略
编辑现有网络分析策略	点击编辑图标 ( )。	第 14-4 页上的编辑网络分析策略
查看列出网络分析策略中当前配置设置的 PDF 报告	点击报告图标 ( )。	第 14-8 页上的生成当前网络分析设置的报告
比较两个网络分析策略或同一策略两个版本的设置	点击 **Compare Policies**。	第 14-9 页上的比较两个网络分析策略或版本
删除网络分析策略	请点击删除图标 ( ) 并确认要删除策略。如果网络分析策略被访问控制策略引用，则无法删除该网络分析策略。	

编辑网络分析策略

许可证：任何环境

当您创建新的网络分析策略时，它具有与其基本策略相同的设置。下表列出了根据您的需求定制新策略时可执行的最常见的操作：

表 14-2　　网络分析策略编辑操作

要.....	您可以.....	请参阅.....
允许预处理器修改或丢弃流量	选择 Policy Information 页面上的 **Inline Mode** 复选框。	第 14-5 页上的允许预处理器影响内联部署中的流量
更改基本策略	从 Policy Information 页面上的 **Base Policy** 下拉列表中选择基本策略。	第 12-3 页上的更改基本策略
查看基本策略中的设置	在 Policy Information 页面上点击 **Manage Base Policy**。	第 12-2 页上的了解基本层
启用、禁用或编辑预处理器的设置	在导航面板中点击 **Settings**。	第 14-6 页上的在网络分析策略中配置预处理器
管理策略层	在导航面板中点击 **Policy Layers**。	第 12-1 页上的在网络分析或入侵策略中使用层

当您定制网络分析策略时，特别是在禁用预处理器时，请记住某些预处理器和入侵规则要求首先以某种方式对流量进行解码或预处理。如果您禁用一个必要的预处理器，系统会自动使用其当前设置，但是，预处理器在网络分析策略模块界面中将保持禁用状态。

注　由于预处理和入侵检查密切相关，检查每个数据包的网络分析和入侵策略**必须**相互补充。定制预处理（特别是使用多个自定义网络分析策略）是一项**高级**任务。有关详细信息，请参阅第 11-9 页上的自定义策略的限制。

系统为每个用户缓存一条网络分析策略。在编辑网络分析策略时，如果您选择任何菜单或指向另一页的其他路径，即使您离开此页，更改也会保留在系统缓存中。除了可执行上表中的操作，第 11-1 页上的了解网络分析和入侵策略还提供有关使用导航面板、解决冲突和确认更改的信息。

要编辑网络分析策略，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击想要配置的网络分析策略旁的编辑图标 ( )。

系统将显示网络分析策略编辑器，焦点位于 Policy Information 页面上，并且左侧带导航面板。

步骤 7　编辑您的策略。采取上面总结的任何操作。

步骤 8　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

允许预处理器影响内联部署中的流量

许可证：任何环境

在内联部署中，某些预处理器可以修改和阻止流量。例如：

- 内联规范化预处理器将数据包标准化为准备这些数据包，以便由其他预处理器和入侵规则引擎进行分析。您还可以使用预处理器的 **Block Unrecoverable TCP Header Anomalies** 和 **Allow These TCP Options** 选项阻止某些数据包。有关详细信息，请参阅第 17-5 页上的规范化内联流量。
- 系统可以丢弃具有无效校验和的数据包；请参阅第 17-4 页上的验证校验和。
- 系统可以丢弃匹配基于速率的攻击防护设置的数据包；请参阅第 21-8 页上的防御基于速率的攻击。

要使网络分析策略中配置的预处理器影响流量，还必须启用并正确配置该预处理器，并正确部署设备内联。最后，您必须启用网络分析策略的 **Inline Mode** 设置。

如果要评估配置如何在内联部署中起作用，而不会实际修改流量，您可以禁用内联模式。请注意，在轻触模式下的被动部署，无论内联模式如何设置，系统都无法影响流量传输。

提示　在内联部署中，思科建议您启用内联模式并配置已启用 **Normalize TCP Payload** 选项的内联规范化预处理器。在被动部署中，思科建议您配置自适应配置文件。

要允许预处理器影响内联部署中的流量，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

系统将显示 Policy Information 页面。

步骤 7　指定是否允许预处理器影响流量：

- 要允许预处理器影响流量，请启用 **Inline Mode**。
- 要阻止预处理器影响流量，请禁用 **Inline Mode**。

步骤 8　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

在网络分析策略中配置预处理器

许可证：任何环境

*预处理器*通过规范化流量和标识协议异常，准备要进行进一步检查的流量。在数据包触发您配置的预处理器选项时，预处理器生成预处理器事件。网络分析策略的基本策略决定了默认情况下启用哪些预处理器及各自的默认配置。

当您在网络分析策略的导航面板中选择 **Settings** 时，策略将按类型列出其预处理器。在 Settings 页面中，您可以启用或禁用网络分析策略中的预处理器，以及访问预处理器配置页面。

必须启用预处理器，这样您才能对其进行配置。当启用预处理器时，该预处理器配置页面的子链接显示在导航面板中 **Settings** 链接下，并且到配置页的 **Edit** 链接显示在 Settings 页面上的预处理器旁边。

提示　要将预处理器的配置恢复为基本策略中的设置，请点击预处理器配置页面上的 **Revert to Defaults**。出现提示时，请确认您要恢复。

当禁用预处理器时，子链接和 **Edit** 链接将不显示，但会保留您的配置。请注意，为了执行其特定分析，许多预处理器和入侵规则要求首先以某种方式对流量进行解码或预处理。如果您禁用一个必要的预处理器，系统会自动使用其当前设置，但是，预处理器在网络分析策略模块界面中将保持禁用状态。

注　在大多数情况下，配置预处理器要求特定专业知识，并且通常很少需要修改或不需要任何修改。定制预处理（特别是使用多个自定义网络分析策略）是一项**高级**任务。由于预处理和入侵检查密切相关，检查每个数据包的网络分析和入侵策略**必须**相互补充。有关详细信息，请参阅第 11-9 页上的自定义策略的限制。

修改预处理器配置要求了解配置及其对网络的潜在影响。以下各节提供指向每个预处理器的具体配置详细信息的链接。

应用层预处理器

应用层协议解码器将特定类型的数据包数据标准化为入侵规则引擎可以分析的格式。

表 14-3　应用层预处理器设置

想了解以下内容.....	请参阅.....
DCE/RPC 配置	第 15-2 页上的解码 DCE/RPC 流量
DNS 配置	第 15-12 页上的检测 DNS 域称服务器响应中的漏洞
FTP 和 Telnet 配置	第 15-16 页上的解码 FTP 和 Telnet 流量
HTTP 配置	第 15-27 页上的解码 HTTP 流量
Sun RPC 配置	第 15-40 页上的使用 Sun RPC 预处理器
SIP 配置	第 15-42 页上的解码会话发起协议
GTP 命令信道配置	第 15-45 页上的配置 GTP 命令通道
IMAP 配置	第 15-47 页上的解码 IMAP 流量
POP 配置	第 15-49 页上的解码 POP 流量
SMTP 配置	第 15-52 页上的解码 SMTP 流量
SSH 配置	第 15-59 页上的使用 SSH 预处理器检测攻击
SSL 配置	第 15-63 页上的使用 SSL 预处理器

SCADA 预处理器

Modbus 和 DNP3 预处理器检测流量异常并为入侵规则引擎提供数据，以供检查。

表 14-4　SCADA 预处理器设置

想了解以下内容.....	请参阅.....
Modbus 配置	第 16-1 页上的配置 Modbus 预处理器
DNP3 配置	第 16-3 页上的配置 DNP3 预处理器

传输层/网络层预处理器

网络层和传输层预处理器检测网络层和传输层的漏洞。数据包发送到预处理器之前，数据包解码器将数据包报头和负载转换为便于预处理器和入侵规则引擎使用的格式；它还检测数据包报头中的各种异常行为。

表 14-5　传输层和网络层预处理器设置

想了解以下内容.....	请参阅.....
校验和验证	第 17-4 页上的验证校验和
内联规范化	第 17-5 页上的规范化内联流量
IP 分片重组	第 17-10 页上的对 IP 数据包进行分片重组
数据包解码	第 17-14 页上的了解数据包解码
TCP 数据流配置	第 17-18 页上的使用 TCP 数据流预处理
UDP 数据流配置	第 17-28 页上的使用 UDP 数据流预处理

请注意，某些高级传输和网络预处理器设置全局应用于您应用访问控制策略的所有网络、区域中。您在一个访问控制策略而非网络分析策略中配置这些高级设置；请参阅第 17-1 页上的配置高级传输/网络设置。

具体威胁检测

Back Orifice 预处理器分析 Back Orifice 神奇 cookie 的 UDP 流量。可以配置端口扫描检测器来报告扫描活动。基于速率的攻击防御有助于保护您的网络免受 SYN 泛洪和旨在击溃网络的海量并发连接。

表 14-6　具体威胁检测设置

想了解以下内容.....	请参阅.....
Back Orifice 检测	第 21-1 页上的检测 Back Orifice
端口扫描检测	第 21-2 页上的检测端口扫描
基于速率的攻击防御	第 21-8 页上的防御基于速率的攻击

请注意，您在入侵策略中配置敏感数据预处理器，该预处理器用于检测敏感数据（例如，ASCII 文本中的信用卡号和社会安全保障号）。有关详细信息，请参阅第 21-17 页上的检测敏感数据。

生成当前网络分析设置的报告

许可证：任何环境

网络分析策略报告是在特定时间点的策略配置记录。该系统将基本策略中的设置与策略层的设置组合，不区分源自基本策略或策略层的设置。

您可以将包括以下信息的报告用于审计目的或检查当前配置。

表 14-7　网络分析策略报告部分

部分	说明
策略信息	提供策略的名称和说明、上次修改策略的用户的名称以及策略上次修改的日期和时间。还指明是否可以启用内联规范化，当前规则更新版本，以及基本策略是否锁定为当前规则更新。
设置	列出所有已启用的预处理器设置及其配置。

还可以生成比较两个网络分析策略或同一策略的两个版本的比较报告。有关详细信息，请参阅第 14-9 页上的比较两个网络分析策略或版本。

要查看网络分析策略报告，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要生成报告的策略旁的报告图标 ( )。请记住，应先确认所有更改，再生成网络分析策略报告；只有确认的更改才会显示在报告中。

系统将会生成报告。系统将提示您保存报告到您的计算机。

比较两个网络分析策略或版本

许可证：任何环境

要查看策略更改以便符合组织的标准或优化系统性能，可以检查两个网络分析策略之间的差异。可以比较任何两个网络分析策略或同一网络分析策略的两个版本。比较之后，可以生成 PDF 报告，记录两个策略或两个版本的策略之间的区别。

您可以使用两个工具来比较网络分析策略或策略版本：

- 此比较视图只并排显示两个网络分析策略或网络分析策略版本之间的差异；比较视图左右两侧标题栏中将显示每个策略的名称或策略版本。

  您可以使用该工具在模块界面上查看和浏览两个策略版本，其中突出显示其差异。

- 比较报告创建仅有两个网络分析策略或网络分析策略版本之间差异的记录，其格式类似于网络分析策略报告的格式，但是采用 PDF 格式。

  可以将其用于保存、复制、打印和共享策略比较，以备进一步检查。

如需了解和使用策略比较工具的更多相关信息，请参阅：

- 第 14-9 页上的使用网络分析策略比较视图
- 第 14-10 页上的使用网络分析策略比较报告

使用网络分析策略比较视图

许可证：任何环境

此比较视图并排显示两个策略或策略版本，比较视图的左右两侧标题栏中将按照名称标识每个策略或策略版本。上次修改时间和最近一次做出修改的用户会与策略名称一起显示。

两个策略之间的差异将会突出显示：

- 蓝色指示突出显示的设置在两个策略中不同，不同之处以红色文本标注。
- 绿色指示突出显示的设置在一个策略中存在，但在另一个策略中不存在。

您可以执行下表中的任何操作。

表 14-8　网络分析策略比较视图操作

要.....	您可以.....
逐一浏览更改	点击标题栏上方的 **Previous** 或 **Next**。 在左右两侧之间以双箭头图标 (⇔) 为中心移动，**Difference** 数字调整为识别您正在查看哪个差异。
生成新的策略比较视图	点击 **New Comparison**。 系统将显示 **Select Comparison** 窗口。有关详情，请参见第 14-10 页上的使用网络分析策略比较报告。
生成策略比较报告	点击 **Comparison Report**。 策略比较报告会创建仅列出两个策略或策略版本之间差异的 PDF 文档。

使用网络分析策略比较报告

许可证：任何环境

网络分析策略比较报告是两个网络分析策略或同一网络分析策略的两个版本之间所有差异的记录，通过网络分析策略比较视图识别，以 PDF 格式显示。可以使用此报告来进一步检查两个网络分析策略配置之间的差异，以及保存和发布您的发现。

对于您能够访问的任何策略，都可以通过比较视图生成网络分析策略比较报告。在生成策略报告前，切记保存所有更改，只有已保存的更改会在报告中显示。

策略比较报告的格式与策略报告相同，有一处例外：策略报告包含策略中的所有配置，而策略比较报告仅列出策略之间的那些不同配置。网络分析策略比较报告包含第 14-8 页上的表 14-7 中描述的部分。

提示　您可以使用类似的步骤比较 访问控制、入侵或文件运行状况策略。

要比较两个网络分析策略或策略版本，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击 **Compare Policies**。

系统将显示 Select Comparison 窗口。

步骤 7　从 **Compare Against** 下拉列表中选择要进行比较的类型：

- 要比较两个不同的策略，请选择 **Other Policy**。

  页面将会刷新，并显示 Policy A 和 Policy B 下拉列表。
- 要比较同一策略的两个修订版，请选择 **Other Revision**。

  此页面刷新，系统将显示 Policy、 Revision A 和 Revision B 下拉列表。

步骤 8　根据您选择的比较类型，有以下选项可供选择：

- 如果您比较两个不同的策略，请从 Policy A 和 Policy B 下拉列表中选择要比较的策略。
- 如果比较同一策略的两个版本，请选择 Policy，然后从 Revision A 和 Revision B 下拉列表中选择要比较的有时间戳的版本。

步骤 9　点击 **OK** 显示策略比较视图。

系统将显示比较视图。

步骤 10　或者，点击 **Comparison Report** 生成网络分析策略比较报告。

系统将显示网络分析策略比较报告。系统将提示您保存报告到您的计算机。

使用应用层预处理器

您在网络分析策略中配置应用层预处理程序，从而为使用在入侵策略中启用的规则进行检测准备流量。有关详情，请参见第 11-1 页上的了解网络分析和入侵策略。

应用层协议可以多种方式呈现相同的数据。思科提供应用层协议解码器，这些解码器可将特定类型的数据包数据规范化为入侵规则引擎可以分析的格式。规范化应用层协议编码使得规则引擎可以有效地将相同的内容相关规则应用于其数据以不同方式呈现的数据包，并获得有意义的结果。

请注意，大多数情况下，除非在入侵策略中启用随附预处理器规则，否则预处理器不会生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

有关详细信息，请参阅：

- 第 15-2 页上的解码 DCE/RPC 流量介绍 DCE/RPC 预处理器，并解释如何对其进行配置以防止检测躲避行为并检测 DCE/RPC 流量异常。
- 第 15-12 页上的检测 DNS 域称服务器响应中的漏洞介绍 DNS 预处理器，并解释如何对其进行配置以检测 DNS 域名服务器响应中三种特定漏洞的任何一种。
- 第 15-16 页上的解码 FTP 和 Telnet 流量介绍 FTP/Telnet 解码器，并解释如何对其进行配置以规范化和解码 FTP 与 Telnet 流量。
- 第 15-27 页上的解码 HTTP 流量介绍 HTTP 解码器，并解释如何对其进行配置以规范化 HTTP 流量。
- 第 15-40 页上的使用 Sun RPC 预处理器介绍 HTTP 解码器，并解释如何对其进行配置以规范化 RPC 流量。
- 第 15-42 页上的解码会话发起协议解释如何使用 SIP 预处理器来解码和检测 SIP 流量异常。
- 第 15-45 页上的配置 GTP 命令通道解释如何使用 GTP 预处理器向规则引擎提供数据包解码器提取的 GTP 命令通道消息。
- 第 15-47 页上的解码 IMAP 流量解释如何使用 IMAP 预处理器来解码和检测 IMAP 流量异常。
- 第 15-49 页上的解码 POP 流量解释如何使用 POP 预处理器来解码和检测 POP 流量异常。
- 第 15-52 页上的解码 SMTP 流量介绍 SMTP 解码器，并解释如何对其进行配置以解码和规范化 SMTP 流量。
- 第 15-59 页上的使用 SSH 预处理器检测攻击解释如何识别和处理 SSH 加密流量中的漏洞。
- 第 15-63 页上的使用 SSL 预处理器解释如何使用 SSL 预处理器识别加密流量，以及如何通过停止流量检查来消除误报。
- 第 16-1 页上的配置 SCADA 预处理解释如何使用 Modbus 和 DNP3 预处理器检测对应流量中的异常，以及如何向规则引擎提供数据以检查某些协议字段。

解码 DCE/RPC 流量

许可证：保护

DCE/RPC 协议使不同网络主机上的进程可以像在同一主机上一样进行通信。这些进程间通信一般通过 TCP 和 UDP 在主机之间传输。在 TCP 传输中， DCE/RPC 也可以进一步封装在 Windows 服务器消息块 (SMB) 协议或 Samba 中；Samba 是一种在由 Windows 和类似 UNIX 或类似 Linux 操作系统组成的混合环境中用于进程间通信的开源 SMB 实现。此外，网络上的 Windows IIS网络服务器可能使用 IIS RPC over HTTP，后者通过防火墙向代理 TCP 传输 DCE/RPC 流量提供分布式通信。

请注意，对 DCE/RPC 预处理器选项和功能的说明包括 DCE/RPC 的 Microsoft 实现（又称为 MSRPC）；对 SMB 选项和功能的说明涉及 SMB 和 Samba。

虽然大多数 DCE/RPC 漏洞出现在针对 DCE/RPC 服务器（实际上可能是网络上任何主机）的 DCE/RPC 客户端请求中，但在服务器响应中也可能出现漏洞。DCE/RPC 预处理器检测封装在 TCP、UDP 和 SMB 传输（包括使用版本 1 RPC over HTTP 的 TCP 传输 DCE/RPC）中的 DCE/RPC 请求和响应。此预处理器分析 DCE/RPC 数据流并检测 DCE/RPC 流量中的异常行为和逃避技术。它还分析 SMB 数据流并检测异常 SMB 行为和逃避技术。

除 IP 分片重组预处理器提供的 IP 分片重组和 TCP 数据流预处理器无缝提供的 TCP 数据流以外，DCE/RPC 预处理器还会将 SMB 分段重组并将 DCE/RPC 分片重组。请参阅第 17-18 页上的使用 TCP 数据流预处理和第 17-10 页上的对 IP 数据包进行分片重组。

最后， DCE/RPC 预处理器会规范化 DCE/RPC 流量，以便规则引擎进行处理。有关使用特定 DCE/RPC 规则关键字检测 DCE/RPC 服务、操作和存根数据的详细信息，请参阅第 23-54 页上的 DCE/RPC 关键字。

要配置 DCE/RPC 预处理器，可以修改控制预处理器工作方式的全局选项，并指定一个或多个基于目标的服务器策略，从而通过 IP 地址和运行的 Windows 或 Samba 版本识别网络上的 DCE/RPC 服务器：

必须启用生成器 ID (GID) 为 132 或 133 的 DCE/RPC 预处理器规则才可生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

有关详细信息，请参阅：

- 第 15-2 页上的选择全局 DCE/RPC 选项
- 第 15-3 页上的了解基于目标的 DCE/RPC 服务器策略
- 第 15-4 页上的了解 DCE/RPC 传输
- 第 15-7 页上的选择 DCE/RPC 基于目标的策略选项
- 第 15-10 页上的配置 DCE/RPC 预处理器

选择全局 DCE/RPC 选项

许可证：保护

DCE/RPC 预处理器全局选项控制预处理器的工作方式。修改这些选项可能会对性能或检测能力造成负面影响，但 **Memory Cap Reached** 选项除外。除非您已充分理解此预处理器及其与已启用的 DCE/RPC 规则之间的交互，否则请勿修改这些选项。尤其是，必须确保 **Maximum Fragment Size** 选项和 **Reassembly Threshold** 选项大于或等于规则需要检测的深度。有关详细信息，请参阅第 23-16 页上的限制内容匹配和第 23-28 页上的使用 Byte_Jump 和 Byte_Test。

如果在以下描述中未提及预处理器规则，表明选项未与预处理器规则关联。

Maximum Fragment Size

如果选择了 **Enable Defragmentation**，可指定介于 1514 到 65535 字节之间的最大 DCE/RPC 分片长度。预处理器会在分片重组前将较大分片截断成为指定的尺寸以便进行处理，但不会改变实际数据包。空白字段将禁用此选项。

Reassembly Threshold

如果选择了 **Enable Defragmentation**，0 将禁用该选项，而 1 到 65535 字节将指定在向规则引擎发送重组数据包前要排队的分片 DCE/RPC 最小字节数和 （如适用）分段 SMB 最小字节数量。值越小，实现早期检测的可能性越高，但可能会对性能造成负面影响。如果启用此选项，应当测试性能所受影响。

Enable Defragmentation

指定是否对 DCE/RPC 流量进行分片整理。当此选项处于禁用状态时，预处理器仍会检测异常并向规则引擎发送 DCE/RPC 数据，但可能会检测不出分片 DCE/RPC 数据中的漏洞。

尽管通过此选项可灵活选择是否对 DCE/RPC 流量进行分片重组，但大多数 DCE/RPC 漏洞都会尝试利用分片隐藏自己。禁用此选项将会忽略大多数已知漏洞，从而造成大量漏报。

Memory Cap Reached

检测达到或超过分配给预处理器的最大内存限制的时间。当达到或超过最大内存上限时，预处理器会释放与造成内存上限事件的会话相关的所有待处理数据并忽略该会话的剩余部分。

可以启用规则 133:1 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Auto-Detect Policy on SMB Session

检测在 SMB `Session Setup And` 请求和响应中识别出的 Windows 或 Samba 版本。如果检测到的版本不同于为 **Policy** 配置选项配置的 Windows 或 Samba 版本，检测到的版本将会仅覆盖为该会话配置的版本。有关详情，请参见第 15-3 页上的了解基于目标的 DCE/RPC 服务器策略。

例如，如果将 **Policy** 设置为 Windows XP，而预处理器检测到 Windows Vista，预处理器将对该会话使用 Windows Vista 策略。其他设置仍然有效。

如果 DCE/RPC 传输不是 SMB （即，传输协议为 TCP 或 UDP），将无法检测到版本，且策略不能实现自动配置。

要启用此选项，请从下拉列表中选择以下其中一项：

- 选择 **Client**，检查该策略类型的服务器到客户端流量。
- 选择 **Server**，检查该策略类型的客户端到服务器流量。
- 选择 **Both**，检查该策略类型的服务器到客户端流量和客户端到服务器流量。

了解基于目标的 DCE/RPC 服务器策略

许可证：保护

可以创建一个或多个基于目标的服务器策略，并使用这些策略将 DCE/RPC 预处理器配置为像指定类型的服务器一样检查 DCE/RPC 流量。基于目标的策略配置包括识别在网络上识别出的主机上运行的 Windows 或 Samba 版本，启用传输协议并指定将 DCE/RPC 流量传输到这些主机的端口，以及设置其他特定于服务器的选项。

Windows 和 Samba DCE/RPC 的实现有很大不同。例如，在对 DCE/RPC 流量进行分片重组时，所有 Windows 版本都在第一个分片中使用 DCE/RPC 上下文 ID，而所有 Samba 版本都在最后一个分片中使用上下文 ID。再如， Windows Vista 在第一个分片中使用操作编号报头字段来识别特定函数调用，而 Samba 及其他所有 Windows 版本都在最后一个分片中使用操作编号字段。

Windows 和 Samba SMB 的实现也有很大不同。例如，Windows 在与命名管道配合使用时可识别 SMB OPEN 和 READ 命令，而 Samba 不能识别这些命令。

启用 DCE/RPC 预处理器会自动启用默认基于目标的策略。或者，可以添加针对运行不同 Windows 或 Samba 版本的其他主机的基于目标的策略，方法是从 **Policy** 下拉列表选择所需的版本。默认基于目标的策略适用于未包含在其他基于目标的策略的任何主机。

在每个基于目标的策略中，可以启用一个或多个传输并为每个传输指定*检测端口*。还可以启用和指定*自动检测端口*。有关详情，请参见第 15-4 页上的了解 DCE/RPC 传输。

还可以配置基于目标的策略的其他选项。可以设置预处理器，使它检测试图连接一个或多个识别出的共享 SMB 资源的情况。可以将预处理器配置为会检测 SMB 流量中的文件，以及会检查检测出的文件中的指定字节数。还可以修改原本只能由具备 SMB 协议专业知识的用户修改的高级选项；通过该选项，可以将预处理器设置为会检测链式 SMB AndX 命令数量超过指定最小数量的情况。

在每个基于目标的策略中，可以：

- 启用一个或多个传输并为每个传输指定*检测端口*。
- 启用和指定*自动检测端口*。有关详情，请参见第 15-4 页上的了解 DCE/RPC 传输。
- 设置预处理器，使它检测试图连接一个或多个识别出的共享 SMB 资源的情况。
- 将预处理器配置为会检测 SMB 流量中的文件，以及会检查检测出的文件中的指定字节数。
- 修改原本只能由具备 SMB 协议专业知识的用户修改的高级选项；通过该选项，可以将预处理器设置为会检测链式 SMB AndX 命令数量超过指定最小数量的情况。

请注意，可以启用 **Auto-Detect Policy on SMB Session** 全局选项，以便在 DCE/RPC 传输是 SMB 时自动覆盖为每个会话的目标策略配置的策略类型。请参阅第 15-3 页上的Auto-Detect Policy on SMB Session。

除在 DCE/RPC 预处理器中启用 SMB 流量文件检测以外，还可以配置文件策略以便选择性地捕获和阻止这些文件。有关详细信息，请参阅第 24-8 页上的创建文件策略和第 24-9 页上的使用文件规则。

了解 DCE/RPC 传输

许可证：保护

在每个基于目标的策略中，都可以启用一个或多个 TCP、UDP、SMB 和 RPC over HTTP 传输。启用传输时，还必须指定一个或多个*检测端口*（即，已知用于传输 DCE/RPC 流量的端口）。或者，也可以启用和指定*自动检测端口*；预处理器会首先对这些端口进行测试，以确定它们是否传输 DCE/RPC 流量，仅在检测到 DCE/RPC 流量的情况下，预处理器才会继续进行处理。

思科建议您使用默认检测端口（可以是已知端口，也可以是各协议的常用端口）。在非默认端口检测到 DCE/RPC 流量的情况下才可以添加端口。

启用自动检测端口时，请确保将端口范围设置为 1024 到 65535，以便覆盖整个临时端口范围。请注意，很少会为 RPC over HTTP Proxy Auto-Detect Ports 选项和 SMB Auto-Detect Ports 选项启用或指定自动检测端口，因为这两者出现流量的可能性很低甚至不可能出现，除非是在指定的默认检测端口上。另请注意，传输检测端口未识别出的端口才会出现自动检测。有关为每个传输启用或禁用自动检测端口的建议，请参阅第 15-7 页上的选择 DCE/RPC 基于目标的策略选项。

可以在 Windows 基于目标的策略中为一个或多个传输指定任意组合的端口，以便与网络流量匹配，但是，在 Samba 基于目标的策略中只能为 SMB 传输指定端口。

请注意，在默认基于目标的策略中必须至少启用一个 DCE/RPC 传输，除非已经添加至少已启用一个传输的 DCE/RPC 基于目标的策略。例如，您可能想为所有 DCE/RPC 实现指定主机，但没有适用于未指定主机的默认基于目标的策略，在这种情况下，您不会为默认基于目标的策略启用传输。

有关详细信息，请参阅：

- 第 15-5 页上的了解无连接和面向连接 DCE/RPC 流量
- 第 15-6 页上的了解 RPC over HTTP 传输

了解无连接和面向连接 DCE/RPC 流量

许可证：保护

DCE/RPC 消息符合两种不同的 DCE/RPC 协议数据单元 （PDU）之一：

- 面向连接 DCE/RPC PDU 协议

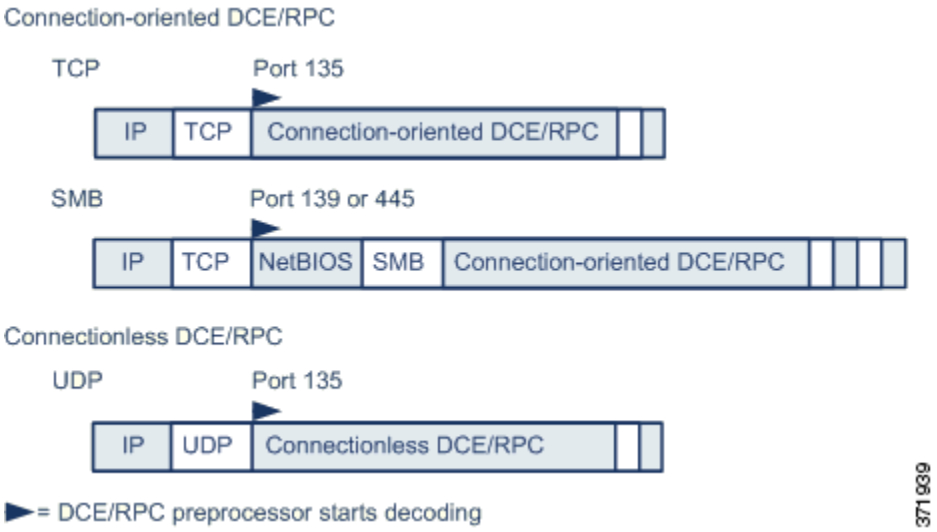
  DCE/RPC 预处理器在 TCP、 SMB 和 RPC over HTTP 传输中检测面向连接 DCE/RPC。

- 无连接 DCE/RPC PDU 协议

  DCE/RPC 预处理器在 UDP 传输中检测无连接 DCE/RPC。

这两种 DCE/RPC PDU 协议都有独特的报头和数据特性。例如，面向连接的 DCE/RPC 的报头长度通常为 24 字节，而无连接 DCE/RPC 的报头长度固定为 80 字节。此外，分片无连接 DCE/RPC 的正确分片顺序不能通过无连接传输处理，而必须通过无连接 DCE/RPC 报头值提供保证；相比之下，传输协议可确保面向连接 DCE/RPC 的分片顺序正确。 DCE/RPC 预处理器使用这些特性及其他特定协议特性监控这两种协议是否存在异常和其他躲避技术，对流量进行解码和分片重组，然后再将流量传送到规则引擎。

下图说明了 DCE/RPC 预处理器开始为不同传输处理 DCE/RPC 流量的点。



对于上图，请注意以下几点：

- 已知 TCP 或 UDP 端口 135 识别 TCP 和 UDP 传输中的 DCE/RPC 流量。
- 图中未包含 RPC over HTTP。

  对于 RPC over HTTP，面向连接 DCE/RPC 在完成 HTTP 初始设置序列后直接通过 TCP 传输（如图所示）。有关详情，请参见第 15-6 页上的了解 RPC over HTTP 传输。

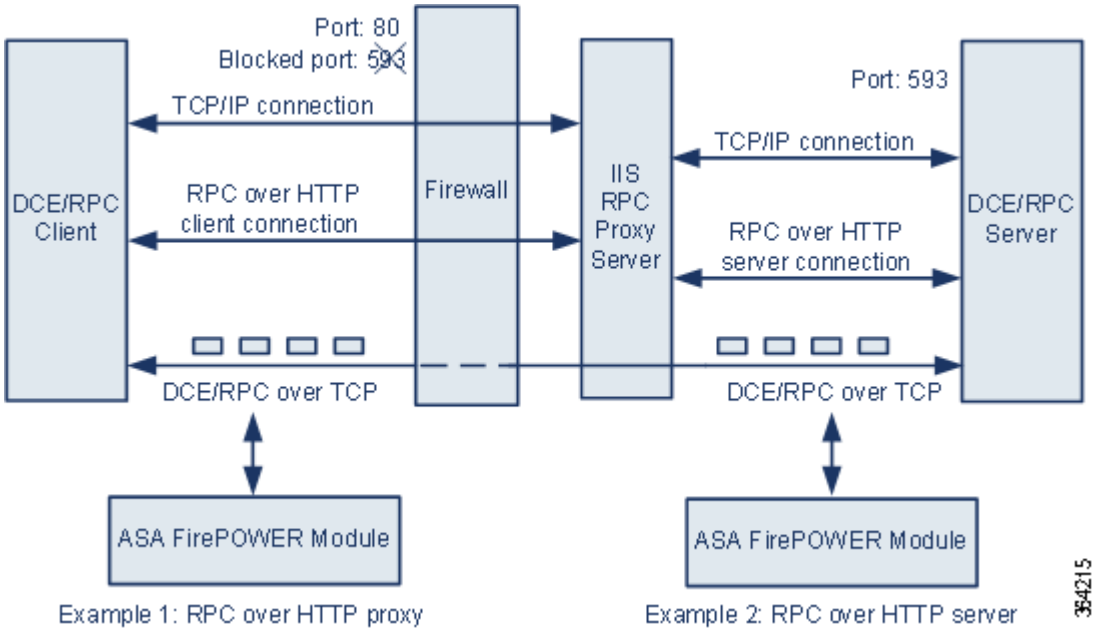
- DCE/RPC 预处理器通常接收适用于 NetBIOS 会话服务的已知 TCP 端口 139 或以类似方式实现的已知 Windows 端口 445 上的 SMB 流量。

  由于 SMB 具有除传输 DCE/RPC 以外的许多功能，因此，预处理器会首先测试 SMB 流量是否正在传输 DCE/RPC 流量，如果不是，预处理器会停止处理，如果是，则继续进行处理。
- IP 封装所有 DCE/RPC 传输。
- TCP 传输所有面向连接 DCE/RPC。
- UDP 传输无连接 DCE/RPC。

了解 RPC over HTTP 传输

许可证：保护

借助 Microsoft RPC over HTTP，可以引导 DCE/RPC 流量穿过防火墙，如下图所示。DCE/RPC 预处理器检测版本 1 Microsoft RPC over HTTP。



Microsoft IIS 代理服务器和 DCE/RPC 服务器可以位于同一主机上，也可以位于不同的主机上。对于这两种情况，都提供独立的代理和服务器选项。对于上图，请注意以下几点：

- DCE/RPC 服务器监控端口 593 的 DCE/RPC 客户端流量，但防火墙阻止该端口。

  默认情况下，防火墙通常会阻止端口 593。
- RPC over HTTP 使用已知 HTTP 端口 80（防火墙通常允许此端口）通过 HTTP 传输 DCE/RPC。
- 示例 1 显示将会选择 **RPC over HTTP proxy** 选项来监控 DCE/RPC 客户端和 MicroSoft IIS RPC 代理服务器之间的流量。
- 示例 2 显示当 MicroSoft IIS RPC 代理服务器和 DCE/RPC 服务器位于不同的主机且设备监控这两个服务器之间的流量时，将会选择 **RPC over HTTP server** 选项。
- RPC over HTTP 完成 DCE/RPC 客户端和服务器代理设置后，流量仅包含通过 TCP 传输的面向连接 DCE/RPC。

选择 DCE/RPC 基于目标的策略选项

许可证：保护

每个基于目标的策略都允许指定以下各个选项。请注意，除 **Memory Cap Reached** 和 **Auto-Detect Policy on SMB Session** 这两个选项外，修改这些选项可能会对性能或检测能力造成负面影响。除非您已充分理解此预处理器及其与已启用的 DCE/RPC 规则之间的交互，否则请勿修改这些选项。

如果在以下描述中未提及预处理器规则，表明选项未与预处理器规则关联。

网络

需要应用 DCE/RPC 基于目标的服务器策略的主机 IP 地址。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。总共最多可以指定 255 个配置文件（包括默认策略）。有关在 ASA FirePOWER 模块中指定 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-3 页上的IP 地址约定。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如， 0.0.0.0/0 或 ::/0）。

另请注意，为使基于目标的策略处理流量，您识别的网络必须与由网络分析策略 （其中已配置该基于目标的策略）处理的网络、区域匹配或者是其子集。有关详情，请参见第 13-2 页上的利用网络分析策略自定义预处理。

策略

目标主机或受监控网段上主机使用的 Windows 或 Samba DCE/RPC 实现。有关这些策略的详细信息，请参阅第 15-3 页上的了解基于目标的 DCE/RPC 服务器策略。

请注意，可以启用 **Auto-Detect Policy on SMB Session** 全局选项，以便在 DCE/RPC 传输是 SMB 时自动覆盖每个会话的此选项的设置。请参阅第 15-3 页上的Auto-Detect Policy on SMB Session。

SMB Invalid Shares

用于识别一个或多个 SMB 共享资源的字母数字文本字符串，不区分大小写；预处理器将会检测是否有程序试图连接您指定的共享资源。您可以在逗号分隔列表中指定多个共享，或者可以将共享用引号引起来（旧版软件要求这样做，但现在不再有此要求），例如：

```
"C$", D$, "admin", private
```

当 SMB 端口和 SMB 流量检测功能都处于启用状态时，预处理器会检测 SMB 流量中的无效共享。

请注意，大多数情况下，对于被识别为无效共享的 Windows 命名的驱动器，应该在其后面附上一个美元符号。例如，将驱动器 C 标识为 C$ 或 "C$"。

可以启用规则 133:26 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

SMB Maximum AndX Chain

允许的的链式 SMB AndX 命令最大数量，介于 0 到 255 之间。通常，超过若干链式 AndX 命令即表示存在异常行为，可能代表有躲避行为。指定 1 表示不允许链式命令，指定 0 将会禁止检测链式命令数量。

请注意，预处理器会首先计算链式命令数量，如果随附的 SMB 预处理器规则已启用，并且链式命令数量等于或超过配置的值，预处理器将会生成事件。然后会继续进行处理。

注　只有 SMB 协议专业人员才可以修改此选项的默认设置。

可以启用规则 133:20 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

RPC proxy traffic only

当 **RPC over HTTP Proxy Ports** 处于启用状态时，此选项指明检测到的客户端 RPC over HTTP 流量是仅包含代理流量还是可能包含其他网络服务器流量。例如，端口 80 可能传输代理流量和其他网络服务器流量。

此选项处于禁用状态时，将会同时传输代理流量和其他网络服务器流量。例如，如果服务器是专用代理服务器，请启用此选项。启用此选项后，预处理器会测试流量以确定其是否传输 DCE/RPC，如果不是，预处理器将会忽略该流量，如果是，则继续进行处理。请注意，仅在已选择 **RPC over HTTP Proxy Ports** 复选框的情况下，此选项才有用。

RPC over HTTP Proxy Ports

当设备位于 DCE/RPC 客户端和 MicroSoft IIS RPC 代理服务器之间，对每个指定端口上通过 RPC over HTTP 传输的 DCE/RPC 流量启用检测。请参阅第 15-6 页上的了解 RPC over HTTP 传输。

启用此选项后，可以添加任意发现 DCE/RPC 流量的端口，但是这项操作一般并不必要，因为网络服务器通常使用默认端口传输 DCE/RPC 和其他流量。启用此选项后，不可以启用 **RPC over HTTP Proxy Auto-Detect Ports**，但如果检测到的客户端 RPC over HTTP 流量仅包含代理流量而不包含其他网络服务器流量，可以启用 **RPC Proxy Traffic Only**。

RPC over HTTP Server Ports

当 MicroSoft IIS RPC 代理服务器和 DCE/RPC 服务器位于不同的主机且设备监控这两个服务器之间流量时，对每个指定端口上通过 RPC over HTTP 传输的 DCE/RPC 流量启用检测。请参阅第 15-6 页上的了解 RPC over HTTP 传输。

启用此选项后，通常还应启用 **RPC over HTTP Server Auto-Detect Ports**（端口范围介于 1025 到 65535 之间），即使不知道网络上是否存在任何代理网络服务器。请注意，RPC over HTTP 服务器端口有时会重新配置，在这种情况下，应该为此选项将重新配置的服务器端口添加到端口列表。

TCP Ports

对每个指定端口上 TCP 中的 DCE/RPC 流量启用检测。

合法 DCE/RPC 流量和漏洞可能使用多种端口，高于端口 1024 的其他端口很常用。启用此选项后，通常还应启用 **TCP Auto-Detect Ports**（端口范围介于 1025 到 65535 之间）。

UDP Ports

对每个指定端口上 UDP 中的 DCE/RPC 流量启用检测。

合法 DCE/RPC 流量和漏洞可能使用多种端口，高于端口 1024 的其他端口很常用。启用此选项后，通常还应启用 **UDP Auto-Detect Ports**（端口范围介于 1025 到 65535 之间）。

SMB Ports

对每个指定端口上 SMB 中的 DCE/RPC 流量启用检测。

可能会出现使用默认检测端口的 SMB 流量。其他端口很少见。通常使用默认设置。

RPC over HTTP Proxy Auto-Detect Ports

当设备位于 DCE/RPC 客户端和 MicroSoft IIS RPC 代理服务器之间时，对指定端口上通过 RPC over HTTP 传输的 DCE/RPC 流量启用自动检测。请参阅第 15-6 页上的了解 RPC over HTTP 传输。

启用此选项后，通常需要指定介于 1025 到 65535 之间的端口范围，以覆盖整个临时端口范围。

RPC over HTTP Server Auto-Detect Ports

当 MicroSoft IIS RPC 代理服务器和 DCE/RPC 服务器位于不同的主机且设备监控这两个服务器之间流量时，对指定端口上通过 RPC over HTTP 传输的 DCE/RPC 启用自动检测。请参阅第 15-6 页上的了解 RPC over HTTP 传输。

TCP Auto-Detect Ports

对指定端口上 TCP 中的 DCE/RPC 流量启用自动检测。

UDP Auto-Detect Ports

对指定端口上 UDP 中的 DCE/RPC 流量启用自动检测。

SMB Auto-Detect Ports

对 SMB 中的 DCE/RPC 流量启用自动检测。

SMB File Inspection

启用 SMB 流量检查以检测文件。您有以下选项：

- 选择 **Off** 禁用文件检查。
- 选择 **Only**，检查文件数据但不检查 SMB 中的 DCE/RPC 流量。选择此选项可以提高文件和 DCE/RPC 流量检查性能。
- 选择 **On**，检查 SMB 中的文件和 DCE/RPC 流量。选择此选项可能会影响性能。

以下各项不支持 SMB 流量检查：

- 在 SMB 2.x 和 SMB 3.x 中传输的文件
- 在启用此选项和应用政策之前在建立的 TCP 或 SMB 会话中传输的文件
- 单一 TCP 或 SMB 会话同时传输的文件
- 在多个 TCP 或 SMB 会话之间传输的文件
- 与非连续数据一起传输的文件（例如，协商了消息签名时）
- 与具有相同偏移量的不同数据一起传输的文件（与数据重叠）
- 在远程客户端打开用于编辑并由客户端保存到文件服务器的文件

SMB File Inspection Depth

如果 **SMB File Inspection** 设置为 **Only** 或 **On**，此选项表示在 SMB 流量中检测到文件时检查的字节数。指定以下各项之一：

- `1` 到 `2147483647`（约 2GB）之间的任意整数
- `0` 以检查整个文件
- `-1` 以禁用文件检查

在此字段中输入的值应等于或小于在访问控制策略中指定的值。如果为此选项设置的值大于为 **Limit the number of bytes inspected when doing file type detection** 定义的值，系统会将访问控制策略设置用作有效的最大值。有关详细信息，请参阅第 10-15 页上的调整文件和恶意软件检测性能和存储。

如果 **SMB File Inspection** 设置为 **Off**，此字段将被禁用。

配置 DCE/RPC 预处理器

许可证：保护

可以配置 DCE/RPC 预处理器全局选项以及一个或多个基于目标的服务器策略。

除非启用带有生成器 ID (GID) 133 的规则，否则预处理器不会生成事件。有关与特定检测选项相关的规则，请参阅第 15-2 页上的选择全局 DCE/RPC 选项和第 15-7 页上的选择 DCE/RPC 基于目标的策略选项；另请参阅第 20-17 页上的设置规则状态。

此外，大多数 DCE/RPC 预处理器规则都会针对 SMB、面向连接 DCE/RPC 或无连接 DCE/RPC 流量中检测到的异常和躲避技术生成事件。下表列出了可为各类流量启用的规则。

表 15-1　　流量相关 DCE/RPC 规则

流量	预处理器规则 GID:SID
中小企业 (SMB)	133:2 到 133:26，以及 133:48 到 133:57
面向连接 DCE/RPC	133:27 到 133:39
检测无连接 DCE/RPC	133:40 到 133:43

要配置 DCE/RPC 预处理器，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **DCE/RPC Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 DCE/RPC Configuration 页面。页面底部的消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　可以修改第 15-2 页上的选择全局 DCE/RPC 选项中所述的任何选项。

步骤 10　此时您有两种选择：

- 添加新的基于目标的策略。点击页面左侧 **Servers** 旁边的添加图标 ( )。系统将显示 Add Target 弹出窗口。在 **Server Address** 字段中指定一个或多个 IP 地址，然后点击 **OK**。

  可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。有关在 ASA FirePOWER 模块中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-3 页上的IP 地址约定。

  总共最多可以配置 255 个策略（包括默认策略）。

  请注意，为使基于目标的策略处理流量，您识别的网络必须与由网络分析策略（其中已配置该基于目标的策略）处理的网络、区域 匹配或者是其子集。有关详情，请参见第 13-2 页上的利用网络分析策略自定义预处理。

  新条目将出现在页面左侧的服务器列表中，突出显示以表明其已被选定；Configuration 部分会进行更新，以反映所添加的策略的当前配置。

- 修改现有基于目标的策略的设置。点击在页面左侧 **Servers** 中添加的策略的配置地址，或者点击 **default**。

  所选项目将会突出显示，并且 Configuration 部分会进行更新以显示所选策略的当前配置。要删除现有策略，请点击要删除的策略旁边的删除图标 ( )。

步骤 11　可以修改以下基于目标的策略选项：

- 要指定要对其应用 DCE/RPC 基于目标的服务器策略的主机，请在 **Networks** 字段中输入单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。

  总共最多可以指定 255 个配置文件（包括默认策略）。请注意，不能修改默认策略中的 **Networks** 设置。默认策略适用于网络上未在其他策略中识别出的所有服务器。

- 要指定要应用于网段上指定主机的策略类型，请从 **Policy** 下拉列表选择 Windows 或 Samba 策略类型之一。

  请注意，可以启用 **Auto-Detect Policy on SMB Session** 全局选项，以便在 DCE/RPC 传输是 SMB 时自动覆盖每个会话的此选项的设置。请参阅第 15-3 页上的Auto-Detect Policy on SMB Session。

- 要将预处理器设置为会检测是否有企图连接到特定 SMB 共享资源的情况，请在 **SMB Invalid Shares** 字段中输入用以识别共享资源的单一字符串或字符串的逗号分隔列表（字符串不区分大小写）。或者，用引号将单个字符串引起来（旧版软件要求这样做，但现在不再有此要求）

  例如，要检测名为 C$、 D$、 admin 和 private 的共享资源，可以输入：

  ```
  "C$", D$, "admin", private
  ```

  请注意，要检测 SMB 无效共享，还必须启用 **SMB Ports** 或 **SMB Auto-Detect Ports** 和 **SMB Traffics** 全局选项。

  另请注意，大多数情况下，对于被识别为无效共享的 Windows 命名的驱动器，应该在其后面附上一个美元符号。例如，可输入 `c$` 或 `"c$"` 来标识驱动器 C。

- 要检查在 SMB 中的 DCE/RPC 流量中检测到的文件而不分析 DCE/RPC 流量，请从 **SMB File Inspection** 下拉列表选择 **Only**。要检查在 SMB 中的 DCE/RPC 流量中检测到的文件和 DCE/RPC 流量，请从 **SMB File Inspection** 下拉列表选择 **On**。在 **SMB File Inspection Depth** 字段输入要在检测到的文件中检查的字节数。输入 `0` 将会检查整个检测到的文件。

- 要指定允许的链式 SMB AndX 命令最大数量，请在 **SMB Maximum AndX Chains** 字段中输入 0 到 255 之间的值。指定 `1` 表示不允许任何链式命令。指定 `0` 或将此选项留空将会禁用此功能。

  注　只有 SMB 协议专业人员可以修改 **SMB Maximum AndX Chains** 选项的设置。

- 要为 Windows 策略传输对已知用于传输 DCE/RPC 流量的端口上的 DCE/RPC 流量启用处理，请选择或清除检测传输旁边的复选框，或者添加或删除用于该传输的端口。

为 Windows 策略选择 **RPC over HTTP Proxy Ports**、**RPC over HTTP Server Ports**、**TCP Ports** 或 **UDP Ports** 或者它们的任意组合。如果 **RPC over HTTP proxy** 已启用，且检测到的客户端 RPC over HTTP 流量仅包含代理流量（也就是说，不包含其他网络服务器流量），可选择 **RPC Proxy Traffic Only**。

为 Samba 策略选择 **SMB Ports**。

大多数情况下使用默认设置。有关详细信息，请参阅第 15-4 页上的了解 DCE/RPC 传输、第 15-6 页上的了解 RPC over HTTP 传输和第 15-7 页上的选择 DCE/RPC 基于目标的策略选项。

可以输入单一端口、用破折线 (-) 分隔的一系列端口编号或者用逗号分隔的端口编号和端口范围列表。

- 要测试指定端口是否传输 DCE/RPC 流量并在指定端口是传输 DCE/RPC 流量的情况下继续进行处理，请选择或清除自动检测传输旁边的复选框，或者添加或删除用于该传输的端口。

  为 Windows 策略选择 **RPC over HTTP Server Auto-Detect Ports**、**TCP Auto-Detect Ports** 或 **UDP Auto-Detect Ports** 或者它们的任意组合。

  请注意，极少情况下需要甚至无需选择 **RPC over HTTP Proxy Auto-Detect Ports** 或 **SMB Auto-Detect Ports**。

  通常应该为自动检测端口指定 1025 到 65535 之间的端口范围，以涵盖整个临时端口范围。有关详细信息，请参阅第 15-4 页上的了解 DCE/RPC 传输、第 15-6 页上的了解 RPC over HTTP 传输和第 15-7 页上的选择 DCE/RPC 基于目标的策略选项。

有关详情，请参见第 15-7 页上的选择 DCE/RPC 基于目标的策略选项。

步骤 12 保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

检测 DNS 域称服务器响应中的漏洞

许可证：保护

DNS 预处理器会检查 DNS 域称服务器响应中是否存在以下具体漏洞：

- RData 文本字段中的溢出尝试
- 过时的 DNS 资源记录类型
- 试验性 DNS 资源记录类型

有关详细信息，请参阅：

- 第 15-13 页上的了解 DNS 预处理器资源记录检查
- 第 15-14 页上的检测 RData 文本字段中的溢出尝试
- 第 15-14 页上的检测过时的 DNS 资源记录类型
- 第 15-14 页上的检测试验性 DNS 资源记录类型
- 第 15-15 页上的配置 DNS 预处理器

了解 DNS 预处理器资源记录检查

许可证：保护

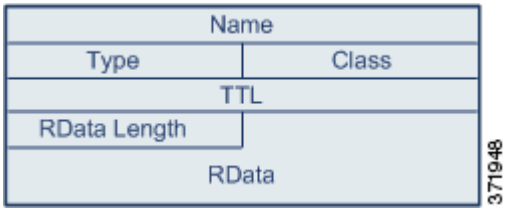
最常见的 DNS 域称服务器响应类型提供与促成响应的查询中域名对应的一个或多个 IP 地址。其他服务器响应类型提供邮件消息目的地或者可提供从最初查询的服务器无法获得的信息的域名服务器位置，等等。

DNS 响应包括一个消息头、一个包含一个或多个请求的 Question 部分以及响应 Question 部分中请求的三个部分 （Answer、 Authority 和 Additional Information）。这三个部分中的响应反映域名服务器内保留的*资源记录* (RR)。下表将介绍这三个部分。

表 15-2　　DNS 域称服务器 RR 响应

部分	包含的内容	示例
回答	（可选）为查询提供明确答复的一个或多个资源记录	对应于域名的 IP 地址
职权	（可选）指向授权域名服务器的一个或多个资源记录	用于响应的授权域名服务器的名称
更多信息	（可选）提供与 Answer 部分相关的其他信息的一个或多个资源记录	要查询的另一个服务器的 IP 地址

有许多类型的资源记录，全部遵循以下结构：



理论上，任何类型的资源记录均可用于域名服务器响应消息的 Answer、 Authority 或 Additional Information 部分。 DNS 预处理器会检查这三个响应部分中的资源记录是否存在其会检测的漏洞。

Type 和 RData 资源记录字段对于 DNS 预处理器特别重要。 Type 字段识别资源记录类型。 RData（资源数据）字段提供响应内容。 RData 字段的大小和内容因资源记录类型而异。

DNS 消息通常使用 UDP 传输协议，但如果消息类型需要可靠传输或者消息大小超过 UDP 能力，DNS 消息也会使用 TCP。 DNS 预处理器会检查 UDP 和 TCP 流量中的 DNS 服务器响应。

DNS 预处理器不会检查在中途恢复的 TCP 会话，如果会话因丢包而丧失状态， DNS 预处理器将会停止检查。

为 DNS 预处理器配置的典型端口为已知端口 53， DNS 域名服务器对在 UDP 和 TCP 中传输的 DNS 消息使用该端口。

检测 RData 文本字段中的溢出尝试

许可证：保护

当资源记录类型为 TXT （文本）时， RData 字段为长度可变的 ASCII 文本字段。

如果选择 DNS 预处理器的 **Detect Overflow attempts on RData Text fields** 选项，将会检测条目 CVE-2006-3441 在 MITRE 的通用漏洞字典数据库中识别出的具体漏洞。这是 Microsoft Windows 2000 Service Pack 4、Windows XP Service Pack 1、Windows XP Service Pack 2 和 Windows Server 2003 Service Pack 1 中的已知漏洞。攻击者可以利用该漏洞发送或者导致主机接收恶意域名服务器响应，导致 RData 文本字段长度计算错误，造成缓冲区溢出，最终全面控制主机。

如果网络上可能有主机运行尚未升级纠正该漏洞的操作系统，应该启用此功能。

可以启用规则 131:3 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

检测过时的 DNS 资源记录类型

许可证：保护

RFC 1035 将多种资源记录类型识别为过时类型。由于这些是过时记录类型，因此，某些系统未对其进行说明，可能容易产生漏洞。在正常 DNS 响应中不会遇到这些记录类型，除非故意将网络配置为包含这些记录类型。

可以将系统配置为会检测过时的资源记录类型。下表列出并说明这些记录类型。

表 15-3　过时的 DNS 资源记录类型

RR 类型	代码	说明
3	MD	邮件目的地
4	MF	邮件转发器

可以启用规则 131:1 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

检测试验性 DNS 资源记录类型

许可证：保护

RFC 1035 将多种资源记录类型识别为试验性类型。由于这些是试验性记录类型，因此，某些系统未对其进行说明，可能容易产生漏洞。在正常 DNS 响应中不会遇到这些记录类型，除非故意将网络配置为包含这些记录类型。

可以将系统配置为会检测试验性资源记录类型。下表列出并说明这些记录类型。

表 15-4　试验性 DNS 资源记录类型

RR 类型	代码	说明
7	MB	邮箱域名
8	MG	邮件组成员
9	MR	邮件重命名域名
10	NUL	空资源记录

可以启用规则 131:2 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

配置 DNS 预处理器

许可证：保护

可按照以下步骤配置 DNS 预处理器。有关配置本页中所述选项的详细信息，请参阅第 15-14 页上的检测 RData 文本字段中的溢出尝试、第 15-14 页上的检测过时的 DNS 资源记录类型和第 15-14 页上的检测试验性 DNS 资源记录类型。

要配置 DNS 预处理器，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **DNS Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 DNS Configuration 页面。页面底部的消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　或者，可以修改 Settings 区域中的以下任何内容：

- 在 **Ports** 字段中指定 DNS 预处理器应为 DNS 服务器响应监控的源端口。使用逗号分隔多个端口。
- 选择 **Detect Overflow Attempts on RData Text fields** 复选框将会检测 RData 文本字段缓冲区溢出尝试。
- 选择 **Detect Obsolete DNS RR Types** 复选框将会检测过时资源记录类型。
- 选择 **Detect Experimental DNS RR Types** 复选框将会检测试验性资源记录类型。

步骤 10　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

解码 FTP 和 Telnet 流量

许可证：保护

FTP/Telnet 解码器会分析 FTP 和 Telnet 数据流，对 FTP 和 Telnet 命令进行规范化，再由规则引擎处理这些命令。

必须启用生成器 ID (GID) 分别为 125 和 126 的 FTP 和 Telnet 预处理器规则才可生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

有关详细信息，请参阅：

了解 FTP 和 Telnet 全局选项

许可证：保护

可以设置全局选项以确定 FTP/Telnet 解码器是否对数据包执行状态检查或无状态检查，是否检测加密 FTP 或 Telnet 会话，以及是否在遇到加密数据后继续检查数据流。

如果在以下描述中未提及预处理器规则，表明选项未与预处理器规则关联。

状态性检查

如果选择此选项， FTP/Telnet 解码器将会保存状态，提供各个数据包的会话上下文，并且仅检查重组的会话。如果清除此选项，将会在没有会话上下文的情况下分析每个数据包。

要检查 FTP 数据传输，必须选择此选项。

Detect Encrypted Traffic

检测加密 Telnet 和 FTP 会话。

可以启用规则 125:7 和 126:2 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Continue to Inspect Encrypted Data

指示预处理器在数据流加密后持续检查数据流，以寻找最终解密数据。

配置 FTP/Telnet 全局选项

许可证：保护

需要配置 FTP/Telnet 解码器的全局选项，以控制是否执行无状态或有状态检查，是否检测加密流量，以及解码器是否应继续在其确定为已加密的数据流中查找解密数据。有关全局设置的详细信息，请参阅第 15-16 页上的了解 FTP 和 Telnet 全局选项。

要配置全局选项，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

系统将显示 Advanced Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **FTP and Telnet Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 FTP and Telnet Configuration 页面。

页面底部的消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

提示　有关配置本页中所述其他选项的详细信息，请参阅第 15-18 页上的配置 Telnet 选项、第 15-22 页上的配置服务器级别 FTP 选项和第 15-25 页上的配置客户端级别 FTP 选项。

步骤 9　或者，可以修改 Global Settings 页面区域中的以下任何内容：

- 选择 **Stateful Inspection** 将会检查包含 FTP 数据包的重组 TCP 数据流。清除 **Stateful Inspection** 将只会检查非重组数据包。
- 选择 **Detect Encrypted Traffic** 将会检测加密流量。清除 **Detect Encrypted Traffic** 将会忽略加密流量。

- 如有需要，可选择 **Continue to Inspect Encrypted Data**，以便在数据流加密后继续检查数据流，以及如果数据流再次解码，可以对其进行处理。

步骤 10　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

了解 Telnet 选项

许可证：保护

可以通过 FTP/Telnet 解码器启用或禁用 Telnet 命令规范化，启用或禁用特定异常情况，以及设置允许的 Are You There (AYT) 攻击阈值。

如果在以下描述中未提及预处理器规则，表明选项未与预处理器规则关联。

端口

指明要实现 Telnet 流量规范化的端口。可在此界面列出多个端口，端口之间用逗号分隔。

Normalize

对流向指定端口的 Telnet 流量进行规范化。

Detect Anomalies

检测没有对应 SE （下级协商终点）的 Telnet SB （下级协商起点）。

Telnet 支持以 SB（下级协商起点）开始并且必须以 SE 结束（下级协商终点）的下级协商。但是，Telnet 服务器的某些实现将忽略无对应 SE 的 SB。这是异常行为，可能意味着存在躲避行为。由于 FTP 在控制接口使用 Telnet 协议，因此也容易受此行为影响。

如果在 Telnet 流量中检测到这种异常，可以启用规则 126:3 生成事件；如果在 FTP 命令通道中检测到这种异常，可以启用规则 125:9 生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Are You There Attack Threshold Number

检测超过指定阈值的连续 AYT 命令数量。思科建议您将 AYT 阈值设置为不超过 20 的数值。

可以启用规则 126:1 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

配置 Telnet 选项

许可证：保护

可以启用或禁用规范化，启用或禁用特定异常情况，以及控制允许的 Are You There (AYT) 攻击阈值。有关 Telnet 选项的更多信息，请参阅第 15-18 页上的了解 Telnet 选项。

要配置 Telnet 选项，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **FTP and Telnet Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 FTP and Telnet Configuration 页面。

页面底部的消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

提示　有关配置本页中所述其他选项的详细信息，请参阅第 15-17 页上的配置 FTP/Telnet 全局选项、第 15-22 页上的配置服务器级别 FTP 选项和第 15-25 页上的配置客户端级别 FTP 选项。

步骤 9　或者，可以修改 Telnet Settings 页面区域中的以下任何内容：

- 在 **Ports** 字段中指定应解码 Telnet 流量的端口。Telnet 通常连接到 TCP 端口 23。使用逗号分隔多个端口。

注意事项　由于加密流量 (SSL) 无法解码，因此，添加端口 22 (SSH) 可能会产生意外结果。

- 选择或清除 **Normalize** Telnet Protocol Options 复选框，以启用或禁用 Telnet 规范化。
- 选择或清除 **Detect Anomalies** Telnet Protocol 复选框，以启用或禁用异常检测功能。
- 使用 **Are You There Attack Threshold Number** 指定允许的连续 AYT 命令阈值。

提示　思科建议将 AYT 阈值设置为不超过默认值的数值。

步骤 10　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

了解服务器级别 FTP 选项

许可证：保护

可以在多个 FTP 服务器上设置解码选项。创建的每个服务器配置文件都包含服务器 IP 地址以及应监控其流量的服务器端口。可以为特定服务器指定需要验证和可忽略的 FTP 命令，以及设置最大命令参数长度。还可以设置解码器应针对特定命令验证的具体命令语法，以及设置替代最大命令参数长度。

如果在以下描述中未提及预处理器规则，表明选项未与预处理器规则关联。

网络

使用此选项可指定 FTP 服务器的一个或多个 IP 地址。

可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。最多可配置 1024 个字符，最多可指定 255 个配置文件（包括默认配置文件）。有关在 ASA FirePOWER 模块中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-3 页上的IP 地址约定。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或地址块，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如， 0.0.0.0/0 或 ::/0）。

另请注意，为使基于目标的策略处理流量，您识别的网络必须与由网络分析策略 （其中已配置该基于目标的策略）处理的网络、区域 匹配或者是其子集。有关详情，请参见第 13-2 页上的利用网络分析策略自定义预处理。

端口

使用此选项可指定设备应监控流量的 FTP 服务器上的端口。可在此界面列出多个端口，端口之间用逗号分隔。

File Get Commands

使用此选项可定义用于从服务器向客户端传输文件的 FTP 命令。请勿改变此选项的值，除非支持人员要求这样做。

File Put Commands

使用此选项可定义用于从客户端向服务器传输文件的 FTP 命令。请勿改变此选项的值，除非支持人员要求这样做。

Additional FTP Commands

使用此行可指定解码器应检测的其他命令。使用空格隔开其他命令。

Default Max Parameter Length

在未设置替代最大参数长度的情况下，使用此选项可检测命令的最大参数长度。

可以启用规则 125:3 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Alternate Max Parameter Length

使用此选项可指定要为其检测其他最大参数长度的命令，并指定这些命令的最大参数长度。点击 **Add** 可添加行，在添加的行中可指定其他最大参数长度，以便检测特定命令。

Check Commands for String Format Attacks

使用此选项可检查指定命令的字符串格式攻击。

可以启用规则 125:5 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Command Validity

使用此选项可为特定命令输入有效格式。有关创建 FTP 命令参数验证语句来验证作为 FTP 通信一部分接收的参数的语法的详细信息，请参阅第 15-21 页上的创建 FTP 命令参数验证语句。点击 **Add** 可添加命令验证行。

可以启用规则 125:2 和 125:4 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Ignore FTP Transfers

使用此选项可禁用除数据传输通道状态检查之外的所有检查，从而提高 FTP 数据传输的性能。

Detect Telnet Escape Codes within FTP Commands

使用此选项可检测何时在 FTP 命令通道上使用 Telnet 命令。

可以启用规则 125:1 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Ignore Erase Commands during Normalization

如果选择了 **Detect Telnet Escape Codes within FTP Commands**，使用此选项可在 FTP 流量规范化过程中忽略 Telnet 字符和行擦除命令。此选项的设置应与 FTP 服务器处理 Telnet 擦除命令的方式相匹配。请注意，新 FTP 服务器通常会忽略 Telnet 擦除命令，而旧服务器通常会进行处理。

Troubleshooting Options: Log FTP Command Validation Configuration

支持人员可能要求您在故障排除呼叫期间配置系统，以打印为服务器列出的每个 FTP 命令的配置信息。

注意事项　更改此故障排除选项的设置会影响性能，应当仅在支持人员的指导下进行操作。

创建 FTP 命令参数验证语句

许可证：保护

为 FTP 命令创建验证语句时，可以通过使用空格隔开参数来指定一组替代参数。还可以在两个参数之间建立二进制 OR 关系，方法是使用竖线 (`|`) 隔开这两个参数。用方括号 (`[]`) 引起来的参数是可选参数。用花括号 (`{}`) 引起来的参数是必要参数。

可以创建 FTP 命令参数验证语句，以验证作为 FTP 通信一部分接收的参数的语法。有关详情，请参见第 15-20 页上的了解服务器级别 FTP 选项。

下表中列出的任何参数均可用于 FTP 命令参数验证语句中。

表 15-5　　FTP 命令参数

使用的参数	出现的验证
`int`	所代表的参数必须是整数。
`number`	所代表的参数必须是 1 到 255 之间的整数。
`char` *_chars*	所代表的参数必须是单个字符，并且必须是 *_chars* 参数中指定的字符之一。 例如，定义带有验证语句 `char` ***SBC*** 的 `MODE` 的命令有效性可检查如下内容：`MODE` 命令的参数是否包含字符 `S`（代表数据流模式）、字符 `B`（代表数据块模式），或字符 `C`（代表压缩模式）。

表 15-5　FTP 命令参数 （续）

使用的参数	出现的验证
date *_datefmt*	如果 *_datefmt* 包含 #，所代表的参数必须是数字。 如果 *_datefmt* 包含 c，所代表的参数必须是字符。 如果 *_datefmt* 包含文字字符串，所代表的参数必须与文字字符串相匹配。
字符串	所代表的参数必须是字符串。
host_port	所代表的参数必须是有效的主机端口说明符（如网络工作组发布的 RFC959《文件传输协议规范》中所规定）。

可以根据需要结合使用上表中的语法来创建参数验证语句，以便在需要验证流量时能够正确验证每个 FTP 命令。

注　如果要在 TYPE 命令中包含复杂的表达式，应将表达式放在空格之间。此外，应将每个操作数放在空格之间。例如，键入字符 `char A | B` ，而非 `char A|B`。

配置服务器级别 FTP 选项

许可证：保护

可以配置多个服务器级别的选项。对于添加的每个 FTP 服务器，可以指定要监控的端口、要验证的命令、命令的默认最大参数长度、特定命令的替代参数长度，以及特定命令的验证语法。还可以选择是否在 FTP 通道上检查字符串格式攻击和 Telnet 命令，以及是否打印每个命令的配置信息。有关服务器级别 FTP 选项的更多信息，请参阅第 15-20 页上的了解服务器级别 FTP 选项。

要配置服务器级别 FTP 选项，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **FTP and Telnet Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 FTP and Telnet Configuration 页面。

页面底部的消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

提示　有关配置本页中所述其他选项的详细信息，请参阅第 15-17 页上的配置 FTP/Telnet 全局选项、第 15-18 页上的配置 Telnet 选项和第 15-25 页上的配置客户端级别 FTP 选项。

步骤 9　此时您有两种选择：

- 添加新的服务器配置文件。点击页面左侧 **FTP Server** 旁边的添加图标 ( )。系统将显示 Add Target 弹出窗口。在 **Server Address** 字段中为客户端指定一个或多个 IP 地址，然后点击 **OK**。

  可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可指定 1024 个字符，最多可配置 255 个策略（包括默认策略）。有关在 ASA FirePOWER 模块中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-3 页上的IP 地址约定。

  请注意，为使基于目标的策略处理流量，您识别的网络必须与由网络分析策略（其中已配置该基于目标的策略）处理的网络、区域 匹配或者是其子集。有关详情，请参见第 13-2 页上的利用网络分析策略自定义预处理。

  新条目将出现在页面左侧的 FTP 服务器列表中，突出显示以表明其已被选定；Configuration 部分会进行更新，以反映所添加的策略的当前配置。

- 修改现有服务器配置文件的设置。点击在页面左侧 **FTP Server** 中添加的配置文件的配置地址，或者点击 **default**。

  所选项目将会突出显示，并且 Configuration 部分会进行更新以显示所选配置文件的当前配置。要删除现有配置文件，请点击要删除的配置文件旁边的删除图标 ( )。

步骤 10　或者，可以修改 Configuration 页面区域中的以下任何内容：

- 修改 **Networks** 字段中列出的地址，并点击页面的任何其他区域。

  突出显示的地址在页面左侧进行更新。

  请注意，不能修改默认配置文件中的 **Network** 设置。默认配置文件适用于网络上未在其他策略中识别出的所有服务器。

- 在 **Ports** 中指定任何应进行 FTP 流量监控的任何端口。端口 21 是已知的 FTP 流量端口。
- 在 **File Get Commands** 字段中更新用于从服务器向客户端传输文件的 FTP 命令。
- 在 **File Put Commands** 字段中更新用于从客户端向服务器传输文件的 FTP 命令。

注　请勿修改 **File Get Commands** 和 **File Put Commands** 字段中的值，除非支持人员要求这样做。

- 要检测除 FTP/Telnet 预处理器在默认情况下检查的命令以外的其他 FTP 命令，请在 **Additional FTP Commands** 中键入命令，命令之间用空格隔开。

  可以根据需要添加尽可能多的其他 FTP 命令。

注　可能需要添加的其他命令包括 XPWD、 XCWD、 XCUP、 XMKD 和 XRMD。有关这些命令的详细信息，请参阅网络工作组发布的 RFC775 《面向目录的 FTP 命令规范》。

- 在 **Default Max Parameter Length** 字段中指定命令参数的默认最大字节数。
- 要为特定命令检测其他最大参数长度，请点击 **Alternate Max Parameter Length** 旁边的 **Add**。在出现的行的第一个文本框中，指定最大参数长度。在第二个文本框中指定命令，命令之间用空格隔开，在这种情况下，应适用替代最大参数长度。

  可以根据需要添加尽可能多的替代最大参数长度。
- 要检查特定命令的字符串格式攻击，请在 **Check Commands for String Format Attacks** 文本框中指定命令，命令之间用空格隔开。
- 要指定命令的有效格式，请点击 **Command Validity** 旁边的 **Add**。指定要验证的命令，然后键入命令参数的验证语句。有关验证语句语法的详细信息，请参阅第 15-20 页上的了解服务器级别 FTP 选项。
- 要禁用除数据传输通道状态检查之外的所有检查，从而提高 FTP 数据传输的性能，请启用 **Ignore FTP Transfers**。

注　要检查数据传输，必须选择 FTP/Telnet **Stateful Inspection** 全局选项。有关设置全局选项的详细信息，请参阅第 15-16 页上的了解 FTP 和 Telnet 全局选项。

- 要检测何时在 FTP 命令通道上使用 Telnet 命令，请选择 **Detect Telnet Escape Codes within FTP Commands**。
- 在 FTP 流量规范化过程中忽略 Telnet 字符和行擦除命令，请启用 **Ignore Erase Commands during Normalization**。

步骤 11　或者，修改相关的故障排除选项（但应仅在支持人员要求的情况下才这样做）；点击 **Troubleshooting Options** 旁边的 **+** 号可展开故障排除选项部分。

步骤 12　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

了解客户端级别 FTP 选项

许可证：保护

可以为 FTP 客户端创建配置文件。在每个配置文件中，可以指定来自客户端的 FTP 响应的最大响应长度。还可以配置解码器是否检测反弹攻击，以及为特定客户端在 FTP 命令通道上使用 Telnet 命令。

如果在以下描述中未提及预处理器规则，表明选项未与预处理器规则关联。

网络

使用此选项可指定 FTP 客户端的一个或多个 IP 地址。

可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。最多可指定 1024 个字符，最多可指定 255 个配置文件（包括默认配置文件）。有关在 ASA FirePOWER 模块中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-3 页上的IP 地址约定。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或地址块，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如， 0.0.0.0/0 或 ::/0）。

另请注意，为使基于目标的策略处理流量，您识别的网络必须与由网络分析策略（其中已配置该基于目标的策略）处理的网络、区域 匹配或者是其子集。有关详情，请参见第 13-2 页上的利用网络分析策略自定义预处理。

Max Response Length

使用此选项可指定来自 FTP 客户端的响应字符串的最大长度。

可以启用规则 125:6 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Detect FTP Bounce Attempts

使用此选项可检测 FTP 反弹攻击。

可以启用规则 125:8 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Allow FTP Bounce to

使用此选项可配置包含附加主机以及这些主机上端口的列表，在这些主机上， FTP PORT 命令不应被视为 FTP 反弹攻击。

Detect Telnet Escape Codes within FTP Commands

使用此选项可检测何时在 FTP 命令通道上使用 Telnet 命令。

可以启用规则 125:1 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Ignore Erase Commands During Normalization

如果选择了 **Detect Telnet Escape Codes within FTP Commands**，使用此选项可在 FTP 流量规范化过程中忽略 Telnet 字符和行擦除命令。此选项的设置应与 FTP 客户端处理 Telnet 擦除命令的方式相匹配。请注意，新 FTP 客户端通常会忽略 Telnet 擦除命令，而旧客户端通常会进行处理。

配置客户端级别 FTP 选项

许可证：保护

可以为 FTP 客户端配置客户端配置文件，以监控来自客户端的 FTP 流量。有关可设置用于监控客户端的选项的更多信息，请参阅第 15-24 页上的了解客户端级别 FTP 选项。有关 Telnet 选项的详细信息，请参阅第 15-18 页上的了解 Telnet 选项。有关其他 FTP 选项的详细信息，请参阅第 15-20 页上的了解服务器级别 FTP 选项和第 15-16 页上的了解 FTP 和 Telnet 全局选项。

要配置客户端级别 FTP 选项，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **FTP and Telnet Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 FTP and Telnet Configuration 页面。

步骤 9　此时您有两种选择：

- 添加新的客户端配置文件。点击页面左侧 **FTP Client** 旁边的添加图标( )。系统将显示 Add Target 弹出窗口。在 **Client Address** 字段中为客户端指定一个或多个 IP 地址，然后点击 **OK**。

  可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可指定 1024 个字符，最多可配置 255 个策略（包括默认策略）。有关在 ASA FirePOWER 模块中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-3 页上的IP 地址约定。

  请注意，为使基于目标的策略处理流量，您识别的网络必须与由网络分析策略（其中已配置该基于目标的策略）处理的网络、区域 匹配或者是其子集。有关详情，请参见第 13-2 页上的利用网络分析策略自定义预处理。

  新条目将出现在页面左侧的 FTP 客户端列表中，突出显示以表明其已被选定；Configuration 部分会进行更新，以反映所添加的策略的当前配置。

- 修改现有客户端配置文件的设置。点击在页面左侧 **FTP Client** 中添加的配置文件的配置地址，或者点击 **default**。

  所选项目将会突出显示，并且 Configuration 部分会进行更新以显示所选配置文件的当前配置。要删除现有配置文件，请点击要删除的配置文件旁边的删除图标 ( )。

步骤 10　或者，可以修改 Configuration 页面区域中的以下任何内容：

- 或者，修改 **Networks** 字段中列出的地址，并点击页面的任何其他区域。

  突出显示的地址在页面左侧进行更新。

  请注意，不能修改默认配置文件中的 **Network** 设置。默认配置文件适用于网络上未在其他策略中识别出的所有客户端主机。

- 在 **Max Response Length** 字段中指定来自 FTP 客户端的响应的最大长度（以字节为单位）。
- 要检测 FTP 反弹攻击，请选择 **Detect FTP Bounce attempts**。

  FTP/Telnet 解码器检测何时发出 FTP PORT 命令以及指定主机与客户端的指定主机不匹配这种情况。

- 要配置包含附加主机和端口的列表（FTP PORT 命令在这些主机和端口上不应被视为 FTP 反弹攻击），请在 **Allow FTP Bounce to** 字段中指定每个主机（或 CIDR 格式的网络），后跟一个冒号 (:) 和端口或端口范围。要为主机输入端口范围，请使用破折号 (-) 隔开范围内的开始端口和最终端口。可以通过用逗号隔开主机条目来输入多个主机。

例如，要允许指向端口 21 处的主机 192.168.1.1 的 FTP PORT 命令，以及指向 22 到 1024 之间任一端口处的主机 192.168.1.2 的命令，请键入：

```
192.168.1.1:21, 192.168.1.2:22-1024
```

有关在 ASA FirePOWER 模块中使用 CIDR 表示法和前缀长度的信息，请参阅第 1-3 页上的IP 地址约定。

注　要为主机指定多个单独端口，必须为每个端口定义重复主机 IP 地址。例如，要指定 192.168.1.1 上的端口 22 和 25，请键入 `192.168.1.1:22, 192.168.1.1:25`。

- 要检测何时在 FTP 命令通道上使用 Telnet 命令，请选择 **Detect Telnet Escape Codes within FTP Commands**。
- 在 FTP 流量规范化过程中忽略 Telnet 字符和行擦除命令，请选择 **Ignore Erase Commands During Normalization**。

步骤 11　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

解码 HTTP 流量

许可证：保护

HTTP 检查预处理器负责以下工作：

- 解码和规范化发送到网络上网络服务器的 HTTP 请求以及来自该服务器的 HTTP 响应
- 将发送到网络服务器的消息分成 URI、非 cookie 报头、 cookie 报头、方法和消息正文等组成部分，以提高与 HTTP 相关的入侵规则的性能
- 将从网络服务器接收到的消息分成状态代码、状态消息、非 set-cookie 报头、cookie 报头和响应正文等组成部分，以提高与 HTTP 相关的入侵规则的性能
- 检测可能的 URI 编码攻击
- 使规范化数据可用于附加规则处理

HTTP 流量可以各种格式进行编码，因此规则很难适当地进行检查。 HTTP 检查可解码 14 种编码，从而确保 HTTP 流量获得可能的最佳检查。

可以在一个服务器上或者对服务器列表全局配置 HTTP 检查选项。

使用 HTTP 检查预处理器时，请注意以下几点：

- 预处理器引擎*无状态地*执行 HTTP 规范化。也就是说，它会逐个数据包进行 HTTP 字符串规范化，并且只能处理已由 TCP 数据流预处理器重组的 HTTP 字符串。
- 必须启用生成器 ID (GID) 为 119 的 HTTP 预处理器规则才可生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

有关详细信息，请参阅：

- 第 15-28 页上的选择全局 HTTP 规范化选项
- 第 15-28 页上的配置全局 HTTP 配置选项
- 第 15-29 页上的选择服务器级别 HTTP 规范化选项
- 第 15-36 页上的选择服务器级别的 HTTP 规范化编码选项
- 第 15-38 页上的配置 HTTP 服务器选项

- 第 15-39 页上的启用其他 HTTP 检查预处理器规则

选择全局 HTTP 规范化选项

许可证：保护

为 HTTP 检查预处理器的全局 HTTP 选项用于控制预处理器的工作方式。如果由未指定为网络服务器的端口接收 HTTP 流量，可使用这些选项启用或禁用 HTTP 规范化。

请注意：

- 如果启用 **Unlimited Decompression**，提交修改时，**Maximum Compressed Data Depth** 和 **Maximum Decompressed Data Depth** 选项将会自动设置为 65535。有关详情，请参见第 15-29 页上的选择服务器级别 HTTP 规范化选项。
- 如果在与访问控制策略的默认操作相关的入侵策略以及与访问控制规则相关的入侵策略中，**Maximum Compressed Data Depth** 和 **Maximum Decompressed Data Depth** 选项的值不同，将会使用最大值。

如果在以下描述中未提及预处理器规则，表明选项未与预处理器规则关联。

Detect Anomalous HTTP Servers

检测发送到未指定为网络服务器的端口或由其接收的 HTTP 流量。

注　如果启用该选项，请确保在 HTTP Configuration 页面上的服务器配置文件中列出会接收 HTTP 流量的所有端口。如果不这样做，并且启用此选项以及随附的预处理器规则，则与该服务器之间的正常流量会生成事件。默认的服务器配置文件包含所有通常用于 HTTP 流量的端口，但如果修改了该配置文件，可能需要将这些端口添加到另一个配置文件中，以防止生成事件。

可以启用规则 120:1 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Detect HTTP Proxy Servers

检测使用未由 **Allow HTTP Proxy Use** 选项定义的代理服务器的 HTTP 流量。

可以启用规则 119:17 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Maximum Compressed Data Depth

启用 **Inspect Compressed Data**（或者 **Decompress SWF File (LZMA)**、**Decompress SWF File (Deflate)** 或 **Decompress PDF File (Deflate)**）后，设置要解压缩的压缩数据的最大大小。可指定 1 到 65535 字节。

Maximum Decompressed Data Depth

启用 **Inspect Compressed Data**（或者 **Decompress SWF File (LZMA)**、**Decompress SWF File (Deflate)** 或 **Decompress PDF File (Deflate)**）后，设置规范化解压缩数据的最大大小。可指定 1 到 65535 字节。

配置全局 HTTP 配置选项

许可证：保护

可以配置对流向非标准端口的 HTTP 流量以及使用代理服务器的 HTTP 流量的检测。有关全局 HTTP 配置选项的详细信息，请参阅第 15-28 页上的选择全局 HTTP 规范化选项。

要配置全局 HTTP 配置选项，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **HTTP Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 HTTP Configuration 页面。

步骤 9　可以修改第 15-28 页上的选择全局 HTTP 规范化选项中所述的任何全局选项。

步骤 10　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

选择服务器级别 HTTP 规范化选项

许可证：保护

可以为监控的每个服务器、全局地为所有服务器或者为服务器列表设置服务器级别选项。此外，可以根据环境需求，使用预定义的服务器配置文件来设置这些选项，或者单独设置这些选项。可以使用这些选项或设置这些选项的其中一个默认配置文件来指定要规范化其流量的 HTTP 服务器端口、要规范化的服务器响应负载以及要规范化的编码的类型。

如果在以下描述中未提及预处理器规则，表明选项未与预处理器规则关联。

网络

使用此选项可指定一个或多个服务器的 IP 地址。可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。

除总共最多 255 个配置文件（包括默认配置文件）的限制以外，还可以在 HTTP 服务器列表中包含最多 496 个字符（或大约 26 个条目），并为所有服务器配置文件指定总共最多 256 个地址条目。有关在 ASA FirePOWER 模块中使用 IPv4 CIDR 记法和 IPv6 前缀长度的详细信息，请参阅第 1-3 页上的IP 地址约定。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如， 0.0.0.0/0 或 ::/0）。

另请注意，为使基于目标的策略处理流量，您识别的网络必须与由网络分析策略（其中已配置该基于目标的策略）处理的网络、区域 匹配或者是其子集。有关详情，请参见第 13-2 页上的利用网络分析策略自定义预处理。

端口

预处理器引擎会对其 HTTP 流量进行规范化的端口。使用逗号分隔多个端口号。

Oversize Dir Length

检测长度超过指定值的 URL 目录。

可以启用规则 119:15 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Client Flow Depth

为要在 **Ports** 中定义的客户端 HTTP 流量中的原始 HTTP 数据包（包括报头和负载数据）中检查的规则指定字节数。如果规则中的 HTTP 内容规则选项检查请求消息的特定部分，客户端流量深度不适用。有关详情，请参见第 23-21 页上的 HTTP 内容选项。

可指定 -1 到 1460 之间的值。思科建议将客户端流量深度设置为最大值。可指定以下任意值：

- 1 到 1460，检查第一个数据包中的指定字节数。如果第一个数据包包含的字节数小于指定值，将会检查整个数据包。请注意，指定值适用于分段和重组的数据包。

  另请注意，值 300 通常表示许多客户端请求报头末尾出现的大尺寸 HTTP Cookie 无需检查。

- 0 将会检查所有客户端流量，包括会话中的多个数据包，在必要时可超出 1460 字节这个限制。请注意，此值可能会影响性能。

- -1 将会忽略所有客户端流量。

Server Flow Depth

为要在 **Ports** 中指定的服务器端 HTTP 流量中的原始 HTTP 数据包中检查的规则指定字节数。**Inspect HTTP Responses** 处于禁用状态时，会检查原始报头和负载；**Inspect HTTP Response** 处于启用状态时，仅检查原始响应正文。

Server Flow Depth 为要在 **Ports** 中定义的服务器端 HTTP 流量中检查的规则指定会话中原始服务器响应数据的字节数。可以使用此选项来平衡 HTTP 服务器响应数据的性能和检查水平。如果规则中的 HTTP 内容规则选项检查响应消息的特定部分，服务器流量深度不适用。有关详情，请参见第 23-21 页上的 HTTP 内容选项。

不同于客户端流量深度，服务器流量深度为要检查的规则指定每个 HTTP 响应而非每个 HTTP 请求数据包的字节数。

可指定 -1 到 65535 之间的值。思科建议将服务器流量深度设置为最大值。可以指定以下任何内容：

- 1 到 65535：

  当 **Inspect HTTP Responses** 处于**启用**状态时，仅检查原始 HTTP 响应正文，不会检查非原始 HTTP 报头；当 **Inspect Compressed Data** 处于启用状态时，还会同时检查解压缩数据。

当 **Inspect HTTP Responses** 处于**禁用**状态时，会检查原始数据包报头和负载。

如果会话包含的响应字节小于指定值，规则将会根据需要在多个数据包中彻底检查给定会话中的所有响应数据包。如果会话包含的响应字节大于指定值，规则将会根据需要在多个数据包中仅检查该会话中的指定字节数。

请注意，流量深度值小可能会导致针对 **Ports** 中定义的服务器端流量的规则出现漏报。大多数这些规则针对的是，可能处于非报头数据的大约前 100 字节中的 HTTP 报头或内容。报头长度通常少于 300 字节，但报头大小可以不同。

另请注意，指定值适用于分段和重组的数据包。

– 0 将会为 **Ports** 中定义的所有 HTTP 服务器端流量检查整个数据包（包括超过 65535 字节的会话中的响应数据）。

  请注意，此值可能会影响性能。

– -1：

  当 **Inspect HTTP Responses** 处于**启用**状态时，仅检查原始 HTTP 响应正文，不会检查原始 HTTP 响应正文。

  当 **Inspect HTTP Responses** 处于**禁用**状态时，会忽略在 **Ports** 中定义的所有服务器端流量。

Maximum Header Length

检测 HTTP 请求中长度超过指定最大字节数的报头字段；如果启用了 **Inspect HTTP Responses**，还会对 HTTP 响应执行此项检查。值 0 将会禁用此选项。指定 1 到 65535 之间的任何值将会启用此选项。

可以启用规则 119:19 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Maximum Number of Headers

检测 HTTP 请求中的报头数量超过此设置的情况。指定 1 到 1024 之间的任何值将会启用此选项。

可以启用规则 119:20 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Maximum Number of Spaces

当 HTTP 请求中折线中的空格数量等于或超过此设置时，进行检测。值 0 将会禁用此选项。指定 1 到 65535 之间的任何值将会启用此选项。

可以启用规则 119:26 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

HTTP Client Body Extraction Depth

指定从 HTTP 客户端请求的消息正文提取的字节数。通过选择 `content` 或 `protected_content` 关键字 **HTTP Client Body** 选项，可以使用入侵规则检查提取的数据。有关详情，请参见第 23-21 页上的 HTTP 内容选项。

可指定 -1 到 65495 之间的值。指定 -1 将会忽略客户端正文。指定 0 将会提取整个客户端正文。请注意，指定特定字节数进行提取可提高系统性能。另请注意，要使 **HTTP Client Body** 选项在入侵规则中起作用，必须为此选项指定一个 0 到 65495 之间的值。

Small Chunk Size

指定被认为是小数据块的数据块可包含的最大字节数。可指定 1 到 255 之间的值。值 0 将会禁用对异常连续小片段的检测。有关详细信息，请参阅 **Consecutive Small Chunks** 选项。

Consecutive Small Chunks

指定在使用分块传输编码的客户端流量或服务器流量中，代表异常大数量的连续小数据块的数量。 **Small Chunk Size** 选项指定小数据块的最大大小。

例如，将 **Small Chunk Size** 设置为 10 并将 **Consecutive Small Chunks** 设置为 5，可检测包含 10 个或更少字节的 5 个连续数据块。

对于客户端流量和服务器流量，可分别启用预处理器规则 119:27 和 120:7 针对过多小数据块这种情况触发事件。如果 **Small Chunk Size** 已启用且此选项设置为 0 或 1，启用这些规则将会对每个指定大小或更小的数据块触发事件。有关详情，请参见第 20-17 页上的设置规则状态。

HTTP Methods

指定除系统预期会在流量中遇到的 GET 和 POST 以外的 HTTP 请求方法。使用逗号隔开多个值。

入侵规则将 `content` 或 `protected_content` 关键字与 **HTTP Method** 参数配合使用来搜索 HTTP 方法中的内容。请参阅第 23-21 页上的HTTP 内容选项。如果在流量中遇到 GET、POST 或为此选项配置的方法以外的方法，可以启用规则 119:31 生成事件。

No Alerts

当随附的预处理器规则处于启用状态时禁用入侵事件。

注　此选项**不**会禁用 HTTP 标准文本规则和共享对象规则。

Normalize HTTP Headers

当 **Inspect HTTP Responses** 处于启用状态时，启用请求和响应报头中非 cookie 数据的规范化。如果**未**启用 **Inspect HTTP Responses**，启用请求和响应报头中 HTTP 报头（包括 cookie）的规范化。

Inspect HTTP Cookies

允许从 HTTP 请求提取 cookie。如果 **Inspect HTTP Responses** 已启用，还允许从响应报头提取 set-cookie 数据。当不需要提取 cookie 时，禁用此选项可提高性能。

请注意，`Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。

Normalize Cookies in HTTP headers

启用 HTTP 请求报头中 cookie 的规范化。当 **Inspect HTTP Responses** 处于启用状态时，还会启用响应报头中 set-cookie 数据的规范化。选择了 **Inspect HTTP Cookies** 之后才能选择此选项。

Allow HTTP Proxy Use

允许将受监控的网络服务器用作 HTTP 代理。此选项仅用于检查 HTTP 请求。

Inspect URI Only

仅检查规范化 HTTP 请求数据包的 URI 部分。

Inspect HTTP Responses

启用对 HTTP 响应的延展检查，从而使预处理器不仅会对 HTTP 请求消息进行解码和规范化，还会提取响应字段以供规则引擎进行检查。启用此选项后，系统会提取响应报头、正文、状态代码等；如果还启用了 **Inspect HTTP Cookies**，系统还会提取 set-cookie 数据。有关详细信息，请参阅第 23-21 页上的HTTP 内容选项、第 23-87 页上的生成关于 HTTP 编码类型和位置的事件和第 23-90 页上的指向特定负载类型。

可以启用规则 120:2 和 120:3 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Normalize UTF Encodings to UTF-8

如果启用了 **Inspect HTTP Responses**，此选项检测 HTTP 响应中的 UTF-16LE、 UTF-16BE、UTF-32LE 和 UTF32-BE 编码，并将其规范化为 UTF-8。

可以启用规则 120:4 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Inspect Compressed Data

当 **Inspect HTTP Responses** 已启用时，此选项启用 HTTP 响应正文中的 gzip 和兼容 deflate 的压缩数据的解压，以及对规范化解压缩数据的检查。系统将检查分块和非分块 HTTP 响应数据。系统会根据需要逐一检查多个数据包中的解压缩数据；也就是说，系统不会将来自不同数据包的解压缩数据合并来进行检查。当达到 **Maximum Compressed Data Depth**、 **Maximum Decompressed Data Depth** 或压缩数据末尾时，解压缩结束。当达到 **Server Flow Depth** 中指定的值时，对解压缩数据的检查将会结束，除非还选择了 **Unlimited Decompression**。可以使用 `file_data` 规则关键字检查解压缩数据；有关详细信息，请参阅第 23-90 页上的指向特定负载类型。

Unlimited Decompression

启用 **Inspect Compressed Data** （或者 **Decompress SWF File (LZMA)**、 **Decompress SWF File (Deflate)** 或 **Decompress PDF File (Deflate)**）后，跨多个数据包覆盖 **Maximum Decompressed Data Depth**；也就是说，此选项支持跨多个数据包无限解压缩。请注意，启用此选项不会影响单个数据包中的 **Maximum Compressed Data Depth** 或 **Maximum Decompressed Data Depth**。另请注意，如果启用此选项，提交修改时 **Maximum Compressed Data Depth** 和 **Maximum Decompressed Data Depth** 将会设置为 65535。请参阅第 15-28 页上的选择全局 HTTP 规范化选项。

Normalize Javascript

当 **Inspect HTTP Responses** 已启用时，此选项启用对 HTTP 响应正文中 Javascript 的检测和规范化。预处理器会对模糊 JavaScript 数据（例如，unescape 函数、decodeURI 函数和 String.fromCharCode 方法）进行规范化。预处理器会对 unescape、decodeURI 和 decodeURIComponent 函数中的以下编码进行规范化：

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

预处理器检测连续空格，并将其规范化为一个空格。此选项处于启用状态时，配置字段允许您指定模糊 Javascript 数据中允许的最大连续空格数量。可输入 1 到 65535 之间的值。值 0 将会禁止生成事件，不管与该字段相关的预处理器规则 (120:10) 是否启用。

预处理器还会对 Javascript 加号 (+) 运算符进行规范化，并使用该运算符连接字符串。

可以使用 `file_data` 关键字使入侵规则指向规范化的 Javascript 数据。有关详情，请参见第 23-90 页上的指向特定负载类型。

可以启用规则 120:9、 120:10 和 120:11 为此选项生成事件，如下所示：

表 15-6　规范化 Javascript 选项规则

规则	会触发事件的情况
120:9	预处理器内的模糊级别大于或等于 2。
120:10	Javascript 模糊数据中的连续空格数量大于或等于为允许的最大连续空格数量配置的值。
120:11	经转义或编码的数据包含多于一种类型的编码。

有关详情，请参见第 20-17 页上的设置规则状态。

Decompress SWF File (LZMA) and Decompress SWF File (Deflate)

启用 **HTTP Inspect Responses** 后，这些选项解压缩位于 HTTP 请求的 HTTP 响应主体中文件的压缩部分。

注　您只能解压缩在 HTTP GET 响应中找到的文件的压缩部分。

- **Decompress SWF File (LZMA)** 解压缩 Adobe ShockWave Flash (`.swf`) 文件的 LZMA 兼容压缩部分。
- **Decompress SWF File (Deflate)** 解压缩 Adobe ShockWave Flash (`.swf`) 文件的 deflate 兼容压缩部分。

当达到 **Maximum Compressed Data Depth** 或 **Maximum Decompressed Data Depth** 中指定的值，或者达到压缩数据末尾时，解压缩将会结束。当达到 **Server Flow Depth** 中指定的值时，对解压缩数据的检查将会结束，除非还选择了 **Unlimited Decompression**。可以使用 `file_data` 规则关键字检查解压缩数据；有关详细信息，请参阅第 23-90 页上的指向特定负载类型。

可以启用规则 120:12 和 120:13 来为此选项生成事件，如下所示：

表 15-7　解压缩 SWF 文件选项规则

规则	会触发事件的情况
120:12	deflate 文件解压缩失败。
120:13	LZMA 文件解压缩失败。

Decompress PDF File (Deflate)

启用 **HTTP Inspect Responses** 后，**Decompress PDF File (Deflate)** 解压缩位于 HTTP 请求的 HTTP 响应主体中可移植文档格式 (`.pdf`) 文件的 deflate 兼容压缩部分。系统只能使用 `/FlateDecode` 数据流过滤器解压缩 PDF 文件。不支持其他数据流过滤器（包括 `/FlateDecode /FlateDecode`）。

注　您只能解压缩在 HTTP GET 响应中找到的文件的压缩部分。

当达到 **Maximum Compressed Data Depth** 或 **Maximum Decompressed Data Depth** 中指定的值，或者达到压缩数据末尾时，解压缩将会结束。当达到 **Server Flow Depth** 中指定的值时，对解压缩数据的检查将会结束，除非还选择了 **Unlimited Decompression**。可以使用 `file_data` 规则关键字检查解压缩数据；有关详细信息，请参阅第 23-90 页上的指向特定负载类型。

您可以启用规则 120:14、 120:15、 120:16 和 120:17 来为此选项生成事件，如下所示：

表 15-8　解压缩 PDF 文件 (Deflate) 选项规则

规则	会触发事件的情况
120:14	文件解压缩失败。
120:15	由于压缩类型不受支持，文件解压缩失败。
120:16	由于 PDF 数据流过滤器不受支持，文件解压缩失败。
120:17	文件解析失败。

Extract Original Client IP Address

允许从 X-Forwarded-For (XFF)、 True-Client-IP 或自定义的 HTTP 报头提取原始客户端 IP 地址。可以在入侵事件视图中显示提取的原始客户端 IP 地址。有关详情，请参见第 26-1 页上的查看事件。

可以启用规则 119:23、 119:29 和 119:30 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

XFF Header Priority

启用 **Extract Original Client IP Address** 后，指定系统处理原始客户端 IP HTTP 报头的顺序。如果在受监控网络上预计会遇到除 X-Forwarded-For (XFF) 或 True-Client-IP 以外的客户端 IP 地址，则可以点击 **Add** 向优先级列表中添加其他报头名称。然后，可以使用每种报头类型旁边的向上和向下箭头图标调整其优先级。请注意，如果在 HTTP 请求中显示多个 XFF 报头，则系统仅处理优先级最高的报头。

Log URI

允许从 HTTP 请求数据包提取原始 URI （如果有），并将该 URI 与为会话生成的所有入侵事件相关联。

启用此选项后，可以在入侵事件表视图的 HTTP URI 列中显示提取的 URI 的前 50 个字符。可以在数据包视图中显示完整的 URI （最多 2048 字节）。有关详情，请参见第 26-1 页上的查看事件。

Log Hostname

允许从 HTTP 请求主机报头中提取主机名（如果有），并将该主机名与为会话生成的所有入侵事件相关联。如果存在多个主机报头，将会从第一个报头提取主机名。

启用此选项后，可以在入侵事件表视图的 HTTP Hostname 列中显示提取的主机名的前 50 个字符。可以在数据包视图中显示完整的主机名（最多 256 字节）。有关详情，请参见第 26-1 页上的查看事件。

可以启用规则 119:25 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

请注意，在启用了预处理器和规则 119:24 的情况下，如果在 HTTP 请求中检测到多个主机报头，预处理器将会生成入侵事件，不管此选项的设置如何。有关详情，请参见第 15-39 页上的启用其他 HTTP 检查预处理器规则。

简档

指定为 HTTP 流量规范化的编码的类型。系统提供了一个适用于大多数服务器的默认配置文件、适用于 Apache 服务器和 IIS 服务器的若干默认配置文件以及自定义默认设置，您可以对这些设置进行自定义，以满足受监控流量的需求。有关详情，请参见第 15-36 页上的选择服务器级别的 HTTP 规范化编码选项。

选择服务器级别的 HTTP 规范化编码选项

许可证：保护

可以选择服务器级别的 HTTP 规范化选项来指定为 HTTP 流量进行规范化的编码类型，并使系统针对包含指定类型编码的流量生成事件。

如果在以下描述中未提及预处理器规则，表明选项未与预处理器规则关联。

ASCII Encoding

对编码的 ASCII 字符进行解码，并指定规则引擎是否生成关于 ASCII 编码 URI 的事件。

可以启用规则 119:1 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

UTF-8 Encoding

对 URI 中的标准 UTF-8 Unicode 序列进行解码。

可以启用规则 119:6 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Microsoft %U Encoding

对 IIS %u 编码方案进行解码，该编码方案使用 %u，后跟四个字符；其中这四个字符是与 IIS Unicode 代码点相关的十六进制编码值。

提示 合法的客户端很少使用 %u 编码，因此，思科建议对使用 %u 编码的 HTTP 流量进行解码。

可以启用规则 119:3 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Bare Byte UTF-8 Encoding

对裸字节编码进行解码（这种解码方法使用非 ASCII 字符作为解码 UTF-8 值时的有效值）。

提示 裸字节编码允许用户模拟 IIS 服务器和正确解释非编码标准。思科建议启用此选项，因为合法的客户端不以这种方式编码 UTF-8。

可以启用规则 119:4 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Microsoft IIS Encoding

使用 Unicode 代码点映射进行解码。

提示 思科建议启用此选项，因为它主要出现在攻击和躲避尝试中。

可以启用规则 119:7 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Double Encoding

通过在每个进行解码的请求 URI 中形成两条通道，解码 IIS 双编码流量。思科建议启用此选项，因为它通常只存在于攻击情况中。

可以启用规则 119:2 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Multi-Slash Obfuscation

将连续的多个斜杠规范化为一个斜杠。

可以启用规则 119:8 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

IIS Backslash Obfuscation

将反斜杠规范化为正斜杠。

可以启用规则 119:9 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Directory Traversal

对目录遍历和自引用目录进行规范化。如果启用随附的预处理器规则来生成关于此类型流量的事件，可能会产生误报，因为有些网站使用目录遍历来引用文件。

可以启用规则 119:10 和 119:11 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Tab Obfuscation

规范化有关对空格分隔符使用制表符的非 RFC 标准。Apache 及其他非 IIS网络服务器在 URL 中使用制表符 (0x09) 作为分隔符。

注　无论此选项的配置如何，如果制表符前有空格字符 (0x20)， HTTP 检查预处理器都将制表符看作空格。

可以启用规则 119:12 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Invalid RFC Delimiter

规范化 URI 数据中的换行符 (\n)。

可以启用规则 119:13 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Webroot Directory Traversal

检测穿过 URL 中初始目录的目录遍历。

可以启用规则 119:18 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Tab URI Delimiter

将制表符 (0x09) 用作 URI 的分隔符。 Apache、新版本的 IIS 以及其他一些网络服务器使用制表符作为 URL 的分隔符。

注　无论此选项的配置如何，如果制表符前有空格字符 (0x20)， HTTP 检查预处理器都将制表符看作空格。

Non-RFC characters

检测在相应字段中添加的并出现在传入或传出 URI 数据中的非 RFC 字符列表。修改该字段时，请使用表示字节字符的十六进制格式。如果要配置此选项，请谨慎设置它的值。使用极常见的字符可能会生成大量事件。

可以启用规则 119:14 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Max Chunk Encoding Size

检测 URI 数据中异常大的数据块的大小。

可以启用规则 119:16 和 119:22 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Disable Pipeline Decoding

禁止对管道化请求进行 HTTP 解码。禁用此选项可提高性能，因为不会对管道中等待的 HTTP 请求进行解码和分析，且只会使用通用模式匹配对这些请求进行检查。

Non-Strict URI Parsing

允许非严格的 URI 解析。应仅在接受 "GET /index.html abc xo qr \n" 格式的非标准 URI 的服务器上使用此选项。此选项处于启用状态时，解码器会假设 URI 在第一和第二空格之间，即使第二个空格后没有有效的 HTTP 标识符。

Extended ASCII Encoding

允许对 HTTP 请求 URI 中的扩展 ASCII 字符进行解析。请注意，此选项仅适用于自定义的服务器配置文件，不适用于为 Apache、 IIS 或所有服务器提供的默认配置文件。

配置 HTTP 服务器选项

许可证：保护

可按照以下步骤配置 HTTP 服务器选项。有关 HTTP 服务器选项的详细信息，请参阅第 15-29 页上的选择服务器级别 HTTP 规范化选项和第 15-36 页上的选择服务器级别的 HTTP 规范化编码选项。

要配置服务器级别的 HTTP 配置选项，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **HTTP Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 HTTP Configuration 页面。页面底部的消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　此时您有两种选择：

- 添加新的服务器配置文件。点击页面左侧 **Servers** 旁边的添加图标 ( )。系统将显示 Add Target 弹出窗口。在 **Server Address** 字段中为客户端指定一个或多个 IP 地址，然后点击 **OK**。

  可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可在列表中包含 496 个字符，为所有服务器配置文件总共最多可指定 256 个地址条目，总共最多可创建 255 个配置文件（包括默认配置文件）。有关在 ASA FirePOWER 模块中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-3 页上的IP 地址约定。

  请注意，为使基于目标的策略处理流量，您识别的网络必须与由网络分析策略（其中已配置该基于目标的策略）处理的网络、区域 匹配或者是其子集。有关详情，请参见第 13-2 页上的利用网络分析策略自定义预处理。

  新条目将出现在页面左侧的服务器列表中，突出显示以表明其已被选定；Configuration 部分会进行更新，以反映所添加的策略的当前配置。

- 修改现有配置文件的设置。点击在页面左侧 **Servers** 中添加的配置文件的配置地址，或者点击 **default**。

  所选项目将会突出显示，并且 Configuration 部分会进行更新以显示所选配置文件的当前配置。要删除现有配置文件，请点击要删除的配置文件旁边的删除图标 ( )。

步骤 10　或者，修改 **Networks** 字段中列出的地址，并点击页面的任何其他区域。

突出显示的地址在页面左侧进行更新。

请注意，不能修改默认配置文件中 **Networks** 的设置。默认配置文件适用于网络上未在其他策略中识别出的所有服务器。

步骤 11　在 **Ports** 字段中，列出要使用 HTTP 检查对其进行流量检查的端口。使用逗号分隔多个端口。

步骤 12　可以修改第 15-29 页上的选择服务器级别 HTTP 规范化选项中所述的任何其他选项。

步骤 13　如下所述选择服务器配置文件：

- 选择 **Custom** 将会创建自己的服务器配置文件（有关详细信息，请参阅第 15-36 页上的选择服务器级别的 HTTP 规范化编码选项）。
- 选择 **All** 将会使用适用于所有服务器的标准默认配置文件。
- 选择 **IIS** 将会使用默认的 IIS 配置文件。
- 选择 **Apache** 将会使用默认的 Apache 配置文件。

步骤 14　如果选择 **Custom**，将出现自定义选项。

步骤 15　在配置文件中对要使用的 HTTP 解码选项进行配置。

有关可用规范化选项的详细消息，请参阅第 15-29 页上的选择服务器级别 HTTP 规范化选项。

步骤 16　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

启用其他 HTTP 检查预处理器规则

许可证：保护

可以启用下表的 **Preprocessor Rule GID:SID** 列中的规则，为与特定配置选项无关的 HTTP 检查预处理器规则生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

表 15-9　其他 HTTP 检查预处理器规则

预处理器规则 GID:SID	说明
120:5	如果在 HTTP 响应流量中遇到 UTF-7 编码，将会生成事件；UTF-7 应仅在需要 7 位奇偶校验的情况下出现，例如， SMTP 流量。
119:21	如果 HTTP 请求报头包含多于一个 `content-length` 字段，将会生成事件。
119:24	如果 HTTP 请求包含多于一个主机报头，将会生成事件。
119:28 120:8	如果启用，这些规则不生成事件。
119:32	如果在流量中遇到 HTTP 0.9，将会生成事件。请注意，还必须启用 TCP Stream Configuration。请参阅第 17-18 页上的使用 TCP 数据流预处理。
119:33	如果 HTTP URI 包含非转义空格，将会生成事件。
119:34	如果 TCP 连接包含 24 个或更多管道化 HTTP 请求，将会生成事件。

使用 Sun RPC 预处理器

许可证：保护

RPC（远程过程调用）规范化采用分片 RPC 记录，并将这些记录规范化为单个记录，以便规则引擎可以检查完整的记录。例如，攻击者可能会试图发现 RPC `admind` 运行所在的端口。某些 UNIX 主机使用 RPC `admind` 执行远程分布式系统任务。如果主机执行弱身份验证，恶意用户可能会控制远程管理。Snort ID (SID) 为 575 的标准文本规则（生成器 ID：1）会搜索特定位置中的内容，并识别不适当的 `portmap GETPORT` 请求，以此来检测这种攻击。

端口

指定要规范化其流量的端口。可在此界面列出多个端口，端口之间用逗号分隔。典型的 RPC 端口为 111 和 32771。如果网络将 RPC 流量发送到其他端口，可考虑添加这些端口。

Detect fragmented RPC records

检测 RPC 分片记录。

可以启用规则 106:1 和 106:5 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Detect multiple records in one packet

在每个数据包（或重组数据包）中检测多于一个 RPC 请求。

可以启用规则 106:2 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Detect fragmented record sums which exceed one fragment

检测超过当前数据包长度的重组分片记录长度。

可以启用规则 106:3 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Detect single fragment records which exceed the size of one packet

检测部分记录

可以启用规则 106:4 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

配置 Sun RPC 预处理器

许可证：保护

可以按照以下步骤配置 Sun RPC 预处理器。有关 Sun RPC 预处理器的配置选项的详细消息，请参阅第 15-40 页上的使用 Sun RPC 预处理器。

要配置 Sun RPC 预处理器，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **Sun RPC Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Sun RPC Configuration 页面。页面底部的消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　在 **Ports** 字段中，键入要解码其 RPC 流量的端口号。使用逗号分隔多个端口。

步骤 10　可以在 Sun RPC 配置页面上选择或清除以下任何检测选项：

- **Detect fragmented RPC records**
- **Detect multiple records in one packet**
- **Detect fragmented record sums which exceed one packet**
- **Detect single fragment records which exceed the size of one packet**

步骤 11　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

解码会话发起协议

许可证：保护

会话初始协议 (SIP) 为客户端应用（例如网络电话、多媒体会议、即时消息、网络游戏和文件传输）的一个或多个用户提供一个或多个会话的呼叫建立、修改和取消。每个 SIP 请求中的 *method* 字段识别请求的目的，请求 URI 则指定发送请求的目的地。每个 SIP 响应中的状态代码指明请求操作的结果。

使用 SIP 建立呼叫后，实时传输协议 (RTP) 负责随后的音频和视频通信；会话的此部分有时又称为呼叫通道、数据通道或音频/视频数据通道。对于数据通道参数协商、会话公告和会话邀请，RTP 在 SIP 消息正文中使用会话描述协议 (SDP)。

SIP 预处理器负责：

- 解码和分析 SIP 2.0 流量
- 提取包括 SDP 数据（如果有）在内的 SIP 报头和消息正文，并将提取的数据传递给规则引擎，以进行进一步检查
- 在检测到以下条件并且相应的预处理器规则已启用的情况下，将会生成事件：SIP 数据包中存在异常和已知漏洞；调用序列乱序和无效。
- 或者，忽略呼叫通道

预处理器会根据在 SDP 消息中识别出的端口来识别 RTP 通道（该消息嵌入在 SIP 消息正文中），但预处理器不提供 RTP 协议检查。

使用 SIP 预处理器时，请注意以下几点：

- UDP 通常传输 SIP 支持的媒体会话。 UDP 数据流预处理为 SIP 预处理器提供 SIP 会话跟踪。
- SIP 规则关键字允许您指向 SIP 数据包报头或消息正文，并限制为对特定 SIP 方法或状态代码进行数据包检测。有关详细信息，请参阅第 23-56 页上的SIP 关键字。
- 如果启用了预处理器，在向规则引擎发送提取的数据之前，预处理器不会生成事件，除非还启用了随附的带有生成器 ID (GID) 140 的规则。有关详情，请参见第 20-17 页上的设置规则状态。

有关详细信息，请参阅：

- 第 15-42 页上的选择 SIP 预处理器选项
- 第 15-44 页上的配置 SIP 预处理器
- 第 15-45 页上的启用其他 SIP 预处理器规则

选择 SIP 预处理器选项

许可证：保护

以下列表说明可修改的 SIP 预处理器选项。

对于 **Maximum Request URI Length**、**Maximum Call ID Length**、**Maximum Request Name Length**、**Maximum From Length**、 **Maximum To Length**、 **Maximum Via Length**、 **Maximum Contact Length** 和 **Maximum Content Length** 选项，可指定 1 到 65535 字节，或者指定 0 以禁止生成事件，不管相关规则是否已启用。

如果在以下描述中未提及预处理器规则，表明选项未与预处理器规则关联。

端口

指定用于检查 SIP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

Methods to Check

指定 SIP 检测方法。可以指定以下当前定义的任何 SIP 方法：

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

方法不区分大小写。方法名称可以包含字母字符、数字和下划线字符。不得使用其他特殊字符。使用逗号隔开多种方法。

由于将来可能会定义新的 SIP 方法，因此，配置可以包含当前未定义的字母串。系统最多支持 32 种方法，包括 21 种当前定义的方法和 11 种其他方法。系统将忽略您可能配置的任何未定义的方法。

请注意，除了为此选项指定的方法外，总共 32 种方法中包括入侵规则中使用 `sip_method` 关键字的指定方法。有关详情，请参见第 23-57 页上的 sip_method。

Maximum Dialogs within a Session

指定数据流会话中允许的最大对话数量。如果创建了多于此数量的对话，将会丢弃最早的对话，直至对话数量不超过指定的最大数量；如果启用了规则 140:27，还将触发事件。

可指定 1 到 4194303 之间的整数。

Maximum Request URI Length

指定 Request-URI 报头字段中允许的最大字节数。如果启用了规则 140:3，长度大于此设置的 URI 将会触发事件。请求 URI 字段指明请求的目标路径或目标页面。

Maximum Call ID Length

指定请求或响应 Call-ID 报头字段中允许的最大字节数。如果启用了规则 140:5，长度大于此设置的 Call-ID 字段将会触发事件。 Call-ID 字段唯一地识别请求和响应中的 SIP 会话。

Maximum Request Name Length

指定请求名称中允许的最大字节数（该名称是 CSeq 事务标识符中指定的方法的名称）。如果启用了规则 140:7，长度大于此设置的请求名称将会触发事件。

Maximum From Length

指定请求或响应 From 报头字段中允许的最大字节数。如果启用了规则 140:9，长度大于此设置的 From 字段将会触发事件。 From 字段识别消息发起方。

Maximum To Length

指定请求或响应 To 报头字段中允许的最大字节数。如果启用了规则 140:11，长度大于此设置的 To 字段将会触发事件。 To 字段识别消息收件人。

Maximum Via Length

指定请求或响应 Via 报头字段中允许的最大字节数。如果启用了规则 140:13，长度大于此设置的 Via 字段将会触发事件。 Via 字段提供请求的路径，并在响应中提供回执信息。

Maximum Contact Length

指定请求或响应 Contact 报头字段中允许的最大字节数。如果启用了规则 140:15，长度大于此设置的 Contact 字段将会触发事件。 Contact 字段提供用以指定与后续消息进行联系的位置的 URI。

Maximum Content Length

指定在请求或响应消息正文的内容中允许的最大字节数。如果启用了规则 140:16，长度大于此设置的内容将会触发事件。

Ignore Audio/Video Data Channel

启用和禁用数据通道流量检查。请注意，如果启用了此选项，预处理器会继续检查其他非数据通道 SIP 流量。

配置 SIP 预处理器

许可证：保护

可按照以下步骤配置 SIP 预处理器。

要配置 SIP 预处理器，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **SIP Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 SIP Configuration 页面。页面底部的消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　可以修改第 15-42 页上的选择 SIP 预处理器选项中所述的任何选项。

步骤 10　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

启用其他 SIP 预处理器规则

许可证：保护

下表中的 SIP 预处理器规则与特定配置选项无关。与其他 SIP 预处理器规则一样，如果要使这些规则生成事件，必须启用它们。有关启用规则的详细信息，请参阅第 20-17 页上的设置规则状态。

表 15-10　其他 SIP 预处理器规则

预处理器规则 GID:SID	说明
140:1	如果预处理器正在监控系统允许的最大 SIP 会话数量，将会生成事件。
140:2	如果必填的 Request_URI 字段在 SIP 请求中为空，将会生成事件。
140:4	如果 Call-ID 报头字段在 SIP 请求或响应中为空，将会生成事件。
140:6	如果 SIP 请求或响应 CSeq 字段中的序列号值不是小于 231 的 32 位无符号整数，将会生成事件。
140:8	如果 From 报头字段在 SIP 请求或响应中为空，将会生成事件。
140:10	如果 To 报头字段在 SIP 请求或响应中为空，将会生成事件。
140:12	如果 Via 报头字段在 SIP 请求或响应中为空，将会生成事件。
140:14	如果必填的 Contact 报头字段在 SIP 请求或响应中为空，将会生成事件。
140:17	如果 UDP 流量中的单个 SIP 请求或响应数据包包含多条消息，将会生成事件。请注意，旧版本 SIP 支持多条消息，但 SIP 2.0 仅在每个数据包中支持一条消息。
140:18	如果 UDP 流量中的 SIP 请求或响应中消息正文的实际长度与 SIP 请求或响应中的 Content-Length 报头字段中指定的值不匹配时，将会生成事件。
140:19	如果预处理器无法识别 SIP 响应的 CSeq 字段中的方法名称，将会生成事件。
140:20	如果 SIP 服务器不质询经过身份验证的邀请消息，将会生成事件。请注意，当有 InviteReplay 计费攻击时，会出现这种情况。
140:21	如果会话信息在建立呼叫前发生变化，将会生成事件。请注意，当有 FakeBusy 计费攻击时，会出现这种情况。
140:22	如果响应状态代码不是一个三位数字，将会生成事件。
140:23	如果 Content-Type 报头字段未指定内容类型且消息正文包含数据，将会生成事件。
140:24	如果 SIP 版本不是 1、 1.1 或 2.0，将会生成事件。
140:25	如果 CSeq 报头字段中指定的方法与 SIP 请求中的 method 字段不匹配，将会生成事件。
140:26	如果预处理器无法识别在 SIP 请求方法字段中命名的方法，将会生成事件。

配置 GTP 命令通道

许可证：保护

通用分组无线业务 (GPRS) 隧道协议 (GTP) 实现通过 GTP 核心网络进行通信。GTP 预处理器检测 GTP 流量中的异常，并将命令通道信令消息转发到规则引擎以进行检查。可以使用 `gtp_version`、`gtp_type` 和 `gtp_info` 规则关键字检查 GTP 命令通道流量中是否存在漏洞。

单一配置选项允许为预处理器进行 GTP 命令通道消息检查的端口修改默认设置。

如果要下表中所列的 GTP 预处理器规则生成事件，必须启用它们。有关启用规则的详细信息，请参阅第 20-17 页上的设置规则状态。

表 15-11　GTP 预处理器规则

预处理器规则 GID:SID	说明
143:1	如果预处理器检测到无效的消息长度，将会生成事件。
143:2	如果预处理器检测到无效的信息元素长度，将会生成事件。
143:3	如果预处理器检测到无序的信息元素，将会生成事件。

可以按照以下步骤修改 GTP 预处理器为其监控 GTP 命令消息的端口。

要配置 GTP 命令通道，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **GTP Command Channel Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 GTP Command Channel Configuration 页面。

步骤 9　或者，修改预处理器进行 GTP 命令消息检查的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口。

步骤 10　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

解码 IMAP 流量

许可证：保护

互联网邮件应用协议 (IMAP) 用于从远程 IMAP 服务器检索邮件。IMAP 预处理器检查服务器到客户端的 IMAP4 流量，如果相关的预处理器规则已启用，还会生成关于异常流量的事件。此预处理器还可以提取和解码客户端到服务器 IMAP4 流量中的邮件附件，并将附件数据发送到规则引擎。可以在入侵规则中使用 `file_data` 关键字以指向附件数据。有关详情，请参见第 23-90 页上的指向特定负载类型。

提取和解码涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

如果要 IMAP 预处理器规则生成事件，必须启用这些规则。 IMAP 预处理器规则的生成器 ID (GID) 为 141。有关详细信息，请参阅第 20-17 页上的设置规则状态。

有关详细信息，请参阅：

- 第 15-47 页上的选择 IMAP 预处理器选项
- 第 15-48 页上的配置 IMAP 预处理器
- 第 15-49 页上的启用其他 IMAP 预处理器规则

选择 IMAP 预处理器选项

许可证：保护

以下列表说明可修改的 IMAP 预处理器选项。

请注意，解码（或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

另请注意，当 **Base64 Decoding Depth**、 **7-Bit/8-Bit/Binary Decoding Depth**、 **Quoted-Printable Decoding Depth** 或 **Unix-to-Unix Decoding Depth** 选项的值在以下设置中不同时，将会使用最高值：

- 默认网络分析策略
- 由同一访问控制策略中的网络分析规则调用的任何其他自定义网络分析策略

有关详细信息，请参阅第 13-3 页上的为访问控制设置默认网络分析策略和第 13-4 页上的使用网络分析规则指定要预处理的流量。

如果在以下描述中未提及预处理器规则，表明选项未与预处理器规则关联。

端口

指定用于检查 IMAP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

Base64 Decoding Depth

指定要从每个 Base64 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、 65534、 65535 除外，因为它们将向下舍入为 65532。

如果启用了 Base64 解码，可以启用规则 141:4，以在解码失败时生成事件；导致解码失败的原因包括，编码不正确或数据损坏，等等。

7-Bit/8-Bit/Binary Decoding Depth

指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括 7 位、8 位、二进制以及各种多部分内容类型（例如，纯文本、jpeg 图像、mp3 文件等）。可指定 1 到 65535 字节，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。

Quoted-Printable Decoding Depth

指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。

如果启用了 Quoted-Printable 解码，可以启用规则 141:6，以在解码失败时生成事件；导致解码失败的原因包括，编码不正确或数据损坏，等等。

Unix-to-Unix Decoding Depth

指定要从每个 Unix-to-Unix 编码（UuEncode 编码）的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。

如果启用了 Unix-to-Unix 解码，可以启用规则 141:7，以在解码失败时生成事件；导致解码失败的原因包括，编码不正确或数据损坏，等等。

配置 IMAP 预处理器

许可证：保护

可按照以下步骤配置 IMAP 预处理器。有关 IMAP 预处理器配置选项的更多信息，请参阅第 15-47 页上的选择 IMAP 预处理器选项。

要配置 IMAP 预处理器，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **IMAP Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 IMAP Configuration 页面。页面底部的消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　在 **Ports** 中指定应解码其 IMAP 流量的端口。使用逗号分隔多个端口号。

步骤 10　指定要从以下邮件附件类型的任意组合中提取和解码数据的最大字节数：

- **Base64 Decoding Depth**
- **7-Bit/8-Bit/Binary Decoding Depth**（包括各种多部分内容类型，例如纯文本格式、jpeg 图像、mp3 文件等）
- **Quoted-Printable Decoding Depth**
- **Unix-to-Unix Decoding Depth**

对于每种类型，可指定 1 到 65535 字节；或者指定 0 以提取和（如有必要）解码数据包中的所有数据。指定 -1 将会忽略附件类型的数据。

可以在入侵规则中使用 `file_data` 规则关键字来检查附件数据。有关详情，请参见第 23-90 页上的指向特定负载类型。

步骤 11　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

启用其他 IMAP 预处理器规则

许可证：保护

下表中的 IMAP 预处理器规则与特定配置选项无关。与其他 IMAP 预处理器规则一样，如果要使这些规则生成事件，必须启用它们。有关启用规则的详细信息，请参阅第 20-17 页上的设置规则状态。

表 15-12　其他 IMAP 预处理器规则

预处理器规则 GID:SID	说明
141:1	如果预处理器检测到未在 RFC 3501 中定义的客户端命令，将会生成事件。
141:2	如果预处理器检测到未在 RFC 3501 中定义的服务器响应，将会生成事件。
141:3	如果预处理器正在使用系统允许的最大内存量，将会生成事件。在这种情况下，预处理将会停止解码，直至内存可用。

解码 POP 流量

许可证：保护

邮局协议 (POP) 用于从远程 POP 邮件服务器检索邮件。 POP 预处理器检查服务器到客户端的 POP3 流量，如果相关的预处理器规则已启用，还会生成关于异常流量的事件。此预处理器还可以提取和解码客户端到服务器 POP3 流量中的邮件附件，并将附件数据发送到规则引擎。可以在入侵规则中使用 `file_data` 关键字以指向附件数据。有关详情，请参见第 23-90 页上的指向特定负载类型。

提取和解码涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

如果要 POP 预处理器规则生成事件，必须启用这些规则。 POP 预处理器规则的生成器 ID (GID) 为 142。有关详情，请参见第 20-17 页上的设置规则状态。

有关详细信息，请参阅：

- 第 15-50 页上的选择 POP 预处理器选项
- 第 15-51 页上的配置 POP 预处理器
- 第 15-52 页上的启用其他 POP 预处理器规则

选择 POP 预处理器选项

许可证：保护

以下列表说明可修改的 POP 预处理器选项。

请注意，解码（或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

另请注意，如果在与访问控制策略的默认操作相关的入侵策略以及与访问控制规则相关的入侵策略中， **Base64 Decoding Depth**、 **7-Bit/8-Bit/Binary Decoding Depth**、 **Quoted-Printable Decoding Depth** 或 **Unix-to-Unix Decoding Depth** 选项的值不同，将会使用最大值。

如果在以下描述中未提及预处理器规则，表明选项未与预处理器规则关联。

端口

指定用于检查 POP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

Base64 Decoding Depth

指定要从每个 Base64 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、 65534、 65535 除外，因为它们将向下舍入为 65532。

如果启用了 Base64 解码，可以启用规则 142:4，以在解码失败时生成事件；导致解码失败的原因包括，编码不正确或数据损坏，等等。有关详情，请参见第 20-17 页上的设置规则状态。

7-Bit/8-Bit/Binary Decoding Depth

指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括 7 位、8 位、二进制以及各种多部分内容类型（例如，纯文本、jpeg 图像、mp3 文件等）。可指定 1 到 65535 字节，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。

Quoted-Printable Decoding Depth

指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。

当启用可打印字符引用编码时，您可以启用规则 142:6，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。有关详情，请参见第 20-17 页上的设置规则状态。

Unix-to-Unix Decoding Depth

指定要从每个 Unix-to-Unix 编码（UuEncode 编码）的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。

当启用 Unix-to-Unix 解码时，您可以启用规则 142:7，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。有关详情，请参见第 20-17 页上的设置规则状态。

配置 POP 预处理器

许可证：保护

可按照以下步骤配置 POP 预处理器。有关 POP 预处理器配置选项的更多信息，请参阅第 15-50 页上的选择 POP 预处理器选项。

要配置 POP 预处理器，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **POP Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 POP Configuration 页面。页面底部的消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　在 **Ports** 中指定应解码其 IMAP 流量的端口。使用逗号分隔多个端口号。

步骤 10　指定要从以下邮件附件类型的任意组合中提取和解码数据的最大字节数：

- **Base64 Decoding Depth**
- **7-Bit/8-Bit/Binary Decoding Depth**（包括各种多部分内容类型，例如纯文本格式、jpeg 图像、mp3 文件等）
- **Quoted-Printable Decoding Depth**
- **Unix-to-Unix Decoding Depth**

对于每种类型，可指定 1 到 65535 字节；或者指定 0 以提取和（如有必要）解码数据包中的所有数据。指定 -1 将会忽略附件类型的数据。

可以在入侵规则中使用 `file_data` 规则关键字来检查附件数据。有关详情，请参见第 23-90 页上的指向特定负载类型。

步骤 11　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

启用其他 POP 预处理器规则

许可证：保护

下表中的 POP 预处理器规则与特定配置选项无关。与其他 POP 预处理器规则一样，如果要使这些规则生成事件，必须启用它们。有关启用规则的详细信息，请参阅第 20-17 页上的设置规则状态。

表 15-13　其他 POP 预处理器规则

预处理器规则 GID:SID	说明
142:1	如果预处理器检测到未在 RFC 1939 中定义的客户端命令，将会生成事件。
142:2	如果预处理器检测到未在 RFC 1939 中定义的服务器响应，将会生成事件。
142:3	如果预处理器正在使用系统允许的最大内存量，将会生成事件。在这种情况下，预处理将会停止解码，直至内存可用。

解码 SMTP 流量

许可证：保护

SMTP 预处理器指示规则引擎对 SMTP 命令进行规范化。预处理器还可以提取和解码客户端到服务器流量中的邮件附件，并根据不同的软件版本，提取邮件的文件名、地址和报头数据，以在显示 SMTP 流量触发的入侵事件时提供上下文。

使用 SMTP 预处理器时，请注意以下几点：

- 必须启用生成器 ID (GID) 为 124 的 SMTP 预处理器规则才可生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

有关详细信息，请参阅：

- 第 15-53 页上的了解 SMTP 解码
- 第 15-56 页上的配置 SMTP 解码
- 第 15-59 页上的启用 SMTP 最大解码内存警报

了解 SMTP 解码

许可证：保护

可以启用或禁用规范化，还可以对选项进行配置以控制 SMTP 解码器检测的异常流量类型。

请注意，解码（或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

另请注意，如果在与访问控制策略的默认操作相关的入侵策略以及与访问控制规则相关的入侵策略中，**Base64 Decoding Depth**、**7-Bit/8-Bit/Binary Decoding Depth**、**Quoted-Printable Decoding Depth** 或 **Unix-to-Unix Decoding Depth** 选项的值不同，将会使用最大值。

如果在以下描述中未提及预处理器规则，表明选项未与预处理器规则关联。

端口

指定要实现 SMTP 流量规范化的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口。

状态性检查

如果选择此选项，SMTP 解码器将会保存状态，提供各个数据包的会话上下文，并且仅检查重组的会话。如果清除此选项，将会在没有会话上下文的情况下分析每个数据包。

Normalize

如果设置为 All，将会规范化所有命令。会检查命令后是否有多个空格字符。

如果设置为 None，不会对命令进行规范化。

如果设置为 Cmds，将会规范化 **Custom Commands** 中列出的命令。

Custom Commands

如果 **Normalize** 设置为 Cmds，此选项会规范化列出的命令。

可在文本框中指定应进行规范化的命令。会检查命令后是否有多个空格字符。

空格 (ASCII 0x20) 和制表符 (ASCII 0x09) 字符被视为是用于规范化目的的空格字符。

Ignore Data

不处理邮件数据；仅处理 MIME 邮件报头数据。

Ignore TLS Data

不处理根据传输层安全协议加密的数据。

No Alerts

当随附的预处理器规则处于启用状态时禁用入侵事件。

Detect Unknown Commands

检测 SMTP 流量中的未知命令。

可以启用规则 124:5 和 124:6 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Max Command Line Len

检测 SMTP 命令行的长度何时大于此值。指定 0 将不会检测命令行长度。

RFC2821 （网络工作组制定的关于简单邮件传输协议的规范）建议将最大命令行长度设置为 512。

可以启用规则 124:1 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Max Header Line Len

检测 SMTP 数据报头行的长度何时大于此值。指定 0 将不会检测数据报头行长度。

可以启用规则 124:2 和 124:7 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Max Response Line Len

检测 SMTP 响应行的长度何时大于此值。指定 0 将不会检测响应行长度。

RFC 2821 建议将最大响应行长度设置为 512。

可以启用规则 124:3 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Alt Max Command Line Len

检测任何指定命令的 SMTP 命令行的长度何时大于此值。指定 0 将不会检测指定命令的命令行长度。为众多命令设置了不同的默认行长度。

此设置将覆盖指定命令的 Max Command Line Len 设置。

可以启用规则 124:3 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Invalid Commands

检测命令是否是从客户端发出的。

可以启用规则 124:5 和 124:6 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Valid Commands

允许此列表中的命令。

即使此列表为空，预处理器仍允许下列有效命令：ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR

注　RCPT TO 和 MAIL FROM 是 SMTP 命令。对这两个命令，预处理器配置分别使用命令名 RCPT 和 MAIL。在代码中，预处理器会将 RCPT 和 MAIL 映射到正确的命令名。

可以启用规则 124:4 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Data Commands

列出以与 SMTP DATA 命令按照 RFC5321 的要求发送数据相同的方法发起数据发送的命令。使用空格分隔多个命令。

Binary Data Commands

列出以与 BDAT 命令按照 RFC 3030 的要求发送数据类似的方法发起数据发送的命令。使用空格分隔多个命令。

Authentication Commands

列出发起客户端和服务器之间的身份认证交换的命令。使用空格分隔多个命令。

Detect xlink2state

检测作为 X-Link2State Microsoft Exchange 缓冲区数据溢出攻击的一部分的数据包。在内联部署中，系统还可以丢弃这些数据包。

可以启用规则 124:8 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Base64 Decoding Depth

在 **Ignore Data** 已禁用的情况下，指定要从每个 Base64 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。如果选择了 **Ignore Data**，预处理器将不会对数据进行解码。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、65534、65535 除外，因为它们将向下舍入为 65532。

如果启用了 Base64 解码，可以启用规则 124:10，以在解码失败时生成事件；导致解码失败的原因包括，编码不正确或数据损坏，等等。有关详情，请参见第 20-17 页上的设置规则状态。

请注意，此选项取代已被弃用的 **Enable MIME Decoding** 和 **Maximum MIME Decoding Depth** 选项，后两个选项由于具有向后兼容性，因此在现有入侵策略中仍受到支持。

7-Bit/8-Bit/Binary Decoding Depth

在 **Ignore Data** 已禁用的情况下，指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括 7 位、8 位、二进制以及各种多部分内容类型（例如，纯文本、jpeg 图像、mp3 文件等）。可指定 1 到 65535 字节，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。如果选择了 **Ignore Data**，预处理器将不会提取数据。

Quoted-Printable Decoding Depth

在 **Ignore Data** 已禁用的情况下，指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。

可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。如果选择了 **Ignore Data**，预处理器将不会对数据进行解码。

当启用可打印字符引用编码时，您可以启用规则 124:11，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。有关详情，请参见第 20-17 页上的设置规则状态。

Unix-to-Unix Decoding Depth

在 **Ignore Data** 已禁用的情况下，指定要从每个 Unix-to-Unix 编码（UuEncode 编码）的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。如果选择了 **Ignore Data**，预处理器将不会对数据进行解码。

当启用 Unix-to-Unix 解码时，您可以启用规则 124:13，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。有关详情，请参见第 20-17 页上的设置规则状态。

Log MIME Attachment Names

允许从 MIME Content-Disposition 报头提取 MIME 附件文件名，并将提取的文件名与为会话生成的所有入侵事件相关联。支持多个文件名。

启用此选项后，可以在入侵事件表视图的 Email Attachment 列中查看与事件相关的文件名。有关详情，请参见第 26-1 页上的查看事件。

Log To Addresses

允许从 SMTP RCPT TO 命令提取收件人邮件地址，并将提取的收件人地址与为会话生成的所有入侵事件相关联。支持多个收件人。

启用此选项后，可以在入侵事件表视图的 Email Recipient 列中查看与事件相关的收件人。有关详情，请参见第 26-1 页上的查看事件。

Log From Addresses

允许从 SMTP MAIL FROM 命令提取发件人邮件地址，并将提取的发件人地址与为会话生成的所有入侵事件相关联。支持多个发件人地址。

启用此选项后，可以在入侵事件表视图的 Email Sender 列中查看与事件相关的收件人。有关详情，请参见第 26-1 页上的查看事件。

Log Headers

允许提取邮件报头。要提取的字节数取决于 **Header Log Depth** 中指定的值。

可以使用 `content` 或 `protected_content` 关键字来编写将邮件报头数据用作模式的入侵规则。还可以在入侵事件数据包视图中查看提取的邮件报头。有关详情，请参见第 26-1 页上的查看事件。

Header Log Depth

指定在 **Log Headers** 已启用的情况下要提取的邮件报头的字节数。可指定 0 到 20480 字节。值 0 将会禁用 **Log Headers**。

配置 SMTP 解码

许可证：保护

可以使用入侵策略的 SMTP Configuration 页面来配置 SMTP 规范化。有关 SMTP 预处理器配置选项的详细信息，请参阅第 15-53 页上的了解 SMTP 解码。

要配置 SMTP 解码选项，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **SMTP Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 SMTP Configuration 页面。页面底部的消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　在 **Ports** 中指定应解码其 SMTP 流量的端口，端口之间用逗号分隔。

步骤 10　选择 **Stateful Inspection** 将会检查包含 SMTP 数据包的重组 TCP 数据流。清除 **Stateful Inspection** 将只会检查非重组数据包

步骤 11　配置规范化选项：

- 要对所有命令进行规范化，请选择 **All**。
- 要只对 **Custom Commands** 中指定的命令进行规范化，请选择 **Cmds** 并指定要规范化的命令。使用空格分隔各个命令。
- 如果不想对任何命令进行规范化，请选择 **None**。
- 要忽略除 MIME 邮件报头数据以外的邮件数据，请选择 **Ignore Data**。
- 要忽略根据传输层安全协议加密的数据，请选择 **Ignore TLS Data**。
- 要禁止在随附的预处理器规则已启用的情况下生成事件，请选择 **No Alerts**。
- 要检测 SMTP 数据中的未知命令，请选择 **Detect Unknown Commands**。

步骤 12　在 **Max Command Line Len** 字段中指定最大命令行长度。

步骤 13　在 **Max Header Line Len** 字段中指定最大数据报头行长度。

步骤 14　在 **Max Response Line Len** 字段中指定最大响应行长度。

注　RCPT TO 和 MAIL FROM 是 SMTP 命令。对这两个命令，预处理器配置分别使用命令名 RCPT 和 MAIL。在代码中，预处理器会将 RCPT 和 MAIL 映射到正确的命令名。

步骤 15　如有需要，点击 **Alt Max Command Line Len** 旁边的 **Add**，添加要为其指定替代最大命令行长度的命令，然后指定行长度以及要对其应用该指定长度的命令（命令之间用空格隔开）。

步骤 16　在 **Invalid Commands** 字段中指定要将其看作无效命令并进行检测的任何命令。使用空格分隔各个命令。

步骤 17　在 **Valid Commands** 字段中指定要将其看作有效命令的任何命令。使用空格分隔各个命令。

注　即使 **Valid Commands** 列表为空，预处理器仍会将下列命令看作有效命令：ATRN、 AUTH、BDAT、 DATA、 DEBUG、 EHLO、 EMAL、 ESAM、 ESND、 ESOM、 ETRN、 EVFY、EXPN、 HELO、 HELP、 IDENT、 MAIL、 NOOP、 QUIT、 RCPT、 RSET、 SAML、SOML、 SEND、 ONEX、 QUEU、 STARTTLS、 TICK、 TIME、 TURN、 TURNME、VERB、 VRFY、 X-EXPS、 X-LINK2STATE、 XADR、 XAUTH、 XCIR、 XEXCH50、XGEN、 XLICENSE、 XQUE、 XSTA、 XTRN 或 XUSR。

步骤 18　在 **Data Commands** 字段中指定您希望以与 SMTP DATA 命令按照 RFC5321 的要求发送数据相同的方法发起数据发送的任何命令。使用空格分隔各个命令。

步骤 19　在 **Binary Data Commands** 字段中指定您希望以与 BDAT 命令按照 RFC 3030 的要求发送数据类似的方法发起数据发送的任何命令。使用空格分隔各个命令。

步骤 20　在 **Authentication Commands** 字段中指定发起客户端和服务器之间的身份验证交换的任何命令。使用空格分隔各个命令。

步骤 21　检测作为 X-Link2State Microsoft Exchange 缓冲区数据溢出攻击的一部分的数据包，请选择 **Detect xlink2state**。

步骤 22　要为不同类型的邮件附件指定要提取和解码的数据的最大字节数，请为以下任何类型的附件指定一个值：

- **Base64 Decoding Depth**
- **7-Bit/8-Bit/Binary Decoding Depth**（包括各种多部分内容类型，例如纯文本格式、jpeg 图像、mp3 文件等）
- **Quoted-Printable Decoding Depth**
- **Unix-to-Unix Decoding Depth**

可指定 1 到 65535 字节，或者指定 0 以提取和（必要时）解码该类型数据包中的所有数据。指定 -1 将会忽略附件类型的数据。

可以在入侵规则中使用 `file_data` 规则关键字来检查提取的数据。有关详情，请参见第 23-90 页上的指向特定负载类型。

要提取和解码跨数据包数据或跨越多个 TCP 分段的数据，还必须选择 SMTP **Stateful Inspection** 选项。

步骤 23　配置用于将上下文信息与 SMTP 流量触发的入侵事件相关联的选项：

- 要允许提取 MIME 附件文件名以便与入侵事件相关联，请选择 **Log MIME Attachment Names**。
- 要允许提取收件人邮件地址，请选择 **Log To Addresses**。
- 要允许提取发件人邮件地址以便与入侵事件相关联，请选择 **Log From Addresses**。
- 要提取邮件报头以便与入侵事件相关联并编写用于检查邮件报头的规则，请选择 **Log Headers**。

  请注意，报头信息显示在入侵事件数据包视图中。另请注意，还可以编写使用 `content` 或 `protected_content` 关键字并以邮件报头数据作为模式的入侵规则。有关详情，请参见第 26-1 页上的查看事件。

  或者，可以在 **Header Log Depth** 中指定 0 到 20480 字节之间的邮件标头，便于进行提取。值 0 将会禁用 **Log Headers**。

步骤 24　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

启用 SMTP 最大解码内存警报

许可证：保护

可以启用 SMTP 预处理器规则 124:9，以便当启用的预处理器使用系统允许用于解码以下类型编码数据的最大内存量时生成事件：

- Base64
- 7 位/8 位/二进制
- Quoted-printable
- Unix-to-Unix

如果超过最大解码内存，预处理器将停止解码这些类型的编码数据，直至内存可用。这个预处理器规则与单个特定配置选项不相关。有关启用规则的详细信息，请参阅第 20-17 页上的设置规则状态。

使用 SSH 预处理器检测攻击

许可证：保护

SSH 预处理器可检测质询-响应缓冲区溢出攻击、CRC-32 攻击、SecureCRT SSH 客户端缓冲区溢出攻击、协议不匹配攻击以及错误的 SSH 消息传输方向。预处理器还可以检测任何版本字符串（版本 1 和 2 除外）。

密钥交换后，会发生质询-响应缓冲区溢出攻击和 CRC-32 攻击，并会因此进行加密。这两种攻击在身份验证质询之后立即向服务器发送超过 20 KB 的反常态大量负载。 CRC-32 攻击仅适用于 SSH 版本 1；质询-响应缓冲区溢出攻击仅适用于 SSH 版本 2。会话开始时可读取版本字符串。除了版本字符串中存在差异外，这两种攻击都可以同样的方式加以处理。

在密钥交换之前尝试进行连接时，会发生 SecureCRT SSH 攻击和协议不匹配攻击。 SecureCRT 漏洞会向客户端发送超长协议标识符字符串，从而导致缓冲区溢出。如果非 SSH 客户端应用试图连接到安全 SSH 服务器或者服务器和客户端的版本号不匹配，会出现协议不匹配攻击。

可以将预处理器配置为会检查指定端口或端口列表的流量，或者会自动检测 SSH 流量。预处理器将会继续检查 SSH 流量，直至传递了未超过指定字节数的指定数量的加密数据包，或者直至超过指定数量的数据包中指定的最大字节数。如果超过最大字节数，系统将会假设出现了 CRC-32（SSH 版本 1）攻击或质询-响应缓冲区溢出（SSH 版本 2）攻击。此外，还可以检测 SecureCRT 攻击、协议不匹配攻击及错误的消息传输方向。请注意，预处理器检测时无需配置任何版本字符串值（版本 1 和 2 除外）。

使用 SSH 预处理器时，请注意：

- 必须启用生成器 ID (GID) 为 128 的 SSH 预处理器规则才可生成事件。有关详情，请参见第 20-17 页上的设置规则状态。
- SSH 预处理器不处理蛮力攻击。有关蛮力攻击的详细信息，请参阅第 20-25 页上的添加动态规则状态。

有关详细信息，请参阅：

- 第 15-60 页上的选择 SSH 预处理器选项
- 第 15-62 页上的配置 SSH 预处理器

选择 SSH 预处理器选项

许可证：保护

本节介绍了可用于配置 SSH 预处理器的选项。

如果发生以下任何一种情况，预处理器将停止检查会话流量：

- 对于某个数量的加密数据包，服务器与客户端之间发生有效交换；连接继续保持。
- 在达到在 **Number of Bytes Sent Without Server Response** 中设置的值之前，达到要检查的加密数据包数量；假设发生了攻击。

在 **Number of Encrypted Packets to Inspect** 中设置的数量内的每个有效服务器响应会重置 **Number of Bytes Sent Without Server Response**，且数据包计数继续进行。

可考虑以下 SSH 预处理器配置示例：

- **Server Ports**：22
- **Autodetect Ports**：off
- **Maximum Length of Protocol Version String**：80
- **Number of Encrypted Packets to Inspect**：25
- **Number of Bytes Sent Without Server Response**：19,600
- 所有检测选项均启用。

在本示例中，预处理器仅检查端口 22 的流量。也就是说，自动检测被禁用，因此只检查指定的端口。

此外，如果发生以下任何一种情况，本示例中的预处理器会停止检查流量：

- 客户端发送 25 个加密数据包，这些数据包总共不超过 19,600 字节。假设没有发生攻击。
- 客户端发送 25 个加密数据包，这些数据包总共不超过 19,600 字节。在这种情况下，预处理器可将发生的攻击视为质询-响应缓冲区溢出攻击，因为本示例中的会话为 SSH 版本 2 会话。

本示例中的预处理器还将检测处理流量过程中发生的以下任何情况：

- 服务器溢出，由大于 80 字节的版本字符串触发，表明为 SecureCRT 攻击
- 协议不匹配
- 数据包的传输方向错误

最后，预处理器将自动检测任何版本字符串（版本 1 和 2 除外）。

如果在以下描述中未提及预处理器规则，表明选项未与预处理器规则关联。

服务器端口

指定 SSH 预处理器应检查其流量的端口。

可以配置单个端口或端口的逗号分隔列表。

Autodetect Ports

将预处理器设置为会自动检测 SSH 流量。

如果选择此选项，预处理器会检查某个 SSH 版本号的所有流量。如果客户端和服务器数据包均没有包含版本号，预处理器将会停止处理。如果禁用此选项，预处理器只检查在 **Server Ports** 选项中确定的流量。

Number of Encrypted Packets to Inspect

指定每个会话待检查的加密数据包的数量。

将此选项设置为 0 将允许所有流量通过。

减少待检查的加密数据包的数量可能会导致一些攻击避开检测。增加待检查的加密数据包的数量可能会对性能造成负面影响。

Number of Bytes Sent Without Server Response

指定在假设存在质询-响应缓冲区溢出或 CRC-32 攻击之前， SSH 客户端在未获得响应的情况下可以向服务器发送的最大字节数。

如果预处理器对于质询-响应缓冲区溢出或 CRC-32 攻击生成误报，请增加此选项的值。

Maximum Length of Protocol Version String

指定在假设存在 SecureCRT 攻击之前，服务器版本字符串中允许的最大字节数。

Detect Challenge-Response Buffer Overflow Attack

启用或禁用质询-响应缓冲区溢出攻击检测。

可以启用规则 128:1 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Detect SSH1 CRC-32 Attack

启用或禁用 CRC-32 攻击检测。

可以启用规则 128:2 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Detect Server Overflow

启用或禁用 SecureCRT SSH 客户端缓冲区溢出攻击检测。

可以启用规则 128:3 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Detect Protocol Mismatch

启用或禁用协议不匹配检测。

可以启用规则 128:4 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Detect Bad Message Direction

允许或禁止检测流量传输方向错误这种情况（即，如果假定的服务器生成客户端流量，或者客户端生成服务器流量）。

可以启用规则 128:5 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Detect Payload Size Incorrect for the Given Payload

允许或禁止检测负载大小不正确的数据包，例如，SSH 数据包中指定的长度与 IP 报头中指定的总长度不一致，或者消息被截断（即，无足够的数据用于整个 SSH 报头）。

可以启用规则 128:6 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

Detect Bad Version String

请注意，启用预处理器后，它在检测时无需配置任何版本字符串（版本 1 和 2 除外）。

可以启用规则 128:7 为此选项生成事件。有关详情，请参见第 20-17 页上的设置规则状态。

配置 SSH 预处理器

许可证：保护

本节说明如何配置 SSH 预处理器。

要配置 SSH 预处理器，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **SSH Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 SSH Configuration 页面。页面底部的消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　可以修改 SSH Configuration 预处理器页面上的任何选项。有关详情，请参见第 15-60 页上的选择 SSH 预处理器选项。

步骤 10　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

使用 SSL 预处理器

许可证：保护

虽然系统无法分析加密流量的内容，但可以设置 SSL 预处理器选项，以继续尝试检查不时会产生误报以及浪费检测资源的流量。但是，通过使用 SSL 预处理器，系统可以分析 SSL 会话开始时所交换的握手和密钥交换消息的内容，以便确定会话加密的时间。当 SSL 预处理处于活动状态时，可促使系统在会话变为加密状态时立即暂停检查会话。要使用 SSL 预处理器，必须确保 TCP 数据流预处理选项已启用。

有关详细信息，请参阅：

- 第 15-63 页上的了解 SSL 预处理
- 第 15-63 页上的启用 SSL 预处理器规则
- 第 15-64 页上的配置 SSL 预处理器

了解 SSL 预处理

许可证：保护

SSL 预处理器停止检查加密数据，这有助于消除误报。SSL 预处理器在检查 SSL 握手时会维护状态信息，跟踪该会话的状态和 SSL 版本。如果预处理器检测到会话状态已被加密，系统会将该会话的流量标记为“加密”。建立加密后，可以将系统配置为停止处理加密会话中的所有数据包。

对于每个数据包， SSL 预处理器都会验证流量是否包含 IP 报头、TCP 报头和 TCP 负载，以及流量发生在指定适用于 SSL 预处理的端口上。对于符合条件的流量，可根据以下情况确定流量是否已加密：

- 系统检测会话中的所有数据包，未启用 **Server side data is trusted**，会话中包含来服务器和客户端的 Finished 消息和至少一个来自服务器和客户端的数据包 （包含应用记录但不包含警报记录）
- 系统漏检了一些流量，未启用 **Server side data is trusted**，而且会话中至少包含来自服务器和客户端的一个数据包（包含应用记录但不包含警报记录）
- 系统检测会话中的所有数据包，未启用 **Server side data is trusted**，会话中包含来客户端的 Finished 消息和至少一个来自客户端的数据包（包含应用记录但不包含警报记录）
- 系统漏检了一些流量，未启用 **Server side data is trusted**，而且会话中至少包含来自客户端的一个数据包（包含应用记录但不包含警报记录）

如果选择停止处理加密流量，系统会在将该会话标记为“加密”后忽略其中的后续数据包。

注　可向某规则添加 `ssl_state` 和 `ssl_version` 关键字，以便在该规则中使用 SSL 状态或版本信息。有关详细信息，请参阅第 23-49 页上的从会话提取 SSL 信息。

启用 SSL 预处理器规则

许可证：保护

启用 SSL 预处理器后，它会检查 SSL 会话开始时交换的握手和密钥交换消息的内容。

请注意，如果您希望 SSL 预处理器规则生成事件，则必须启用这些规则，其生成器 ID (GID) 为 137。有关详情，请参见第 20-17 页上的设置规则状态。

下表说明了可启用的 SSL 预处理器规则。

表 15-14　SSL 预处理器规则

预处理器规则 GID:SID	说明
137:1	在服务器问候消息之后检测到客户端问候消息，后者是无效的，被视为异常行为。
137:2	在 **Server side data is trusted** 禁用的情况下检测到服务器问候消息（但没有检测到客户端问候消息），该问候消息是无效状态，被视为异常行为。有关详情，请参见第 15-64 页上的配置 SSL 预处理器。

配置 SSL 预处理器

许可证：保护

在默认情况下，系统将尝试检查加密的流量。如果启用了 SSL 预处理器，它会检测会话加密的时间。启用 SSL 预处理器后，规则引擎可以调用预处理器来获得 SSL 状态和版本信息。如果在某个入侵策略中启用使用 `ssl_state` 和 `ssl_version` 关键字的规则，则还应在该策略中启用 SSL 预处理器。

此外，可以启用 **Stop inspecting encrypted traffic** 选项来禁止检查和重组加密的会话。SSL 预处理器会维护会话状态，因此，它可以禁止对会话中所有流量的检查。如果启用了 SSL 预处理**并**选择了 **Stop inspecting encrypted traffic** 选项，则系统只停止检查加密会话中的流量。

要仅以服务器流量为依据标别加密流量，可以启用 **Server side data is trusted** 选项；也就是说，可信赖服务器端数据来指明流量是否已加密。 SSL 预处理器通常会检查客户端流量以及服务器对该流量的响应，从而确定会话是否已加密。但是，如果系统无法检测会话的两端，就可能不会将会话标记为“加密”，因此，可依赖于 SSL 服务器来确定会话是否已加密。请注意，如果启用 **Server side data is trusted** 选项，还必须启用 **Stop inspecting encrypted traffic** 选项，这样系统就不会继续检查加密会话中的流量。

可以指定预处理器监控加密会话流量的端口。

注　如果 SSL 预处理器检测到指定用于 SSL 监控的端口上有非 SSL 流量，它会尝试将该流量作为 SSL 流量进行解码，然后将其标记为“损坏”。

要配置 SSL 预处理器，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Application Layer Preprocessors 下的 **SSL Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 SSL Configuration 页面。页面底部的消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　输入 SSL 预处理器应监控加密会话流量的端口（用逗号隔开）。只会检查包含在 **Ports** 字段中的端口的加密流量。

步骤 10　点击 **Stop inspecting encrypted traffic** 复选框，以允许或禁止在会话被标记为“加密”后检查会话中的流量。

步骤 11　点击 **Server side data is trusted** 复选框，以允许或禁止仅以客户端流量为依据标别加密流量。

步骤 12　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

配置 SCADA 预处理

您在网络分析策略中配置监控与数据采集 （SCADA）预处理器，该预处理器准备流量，以便使用在入侵策略中启用的规则进行检查。有关详情，请参见第 11-1 页上的了解网络分析和入侵策略。

SCADA 协议可监控和控制工业、基础设施以及工厂流程（例如制造、生产、水处理、配电、机场和运输系统等）并从中获取数据。ASA FirePOWER 模块为您可在网络分析策略中配置的 Modbus 和 DNP3 SCADA 协议提供预处理器。

如果在相应的入侵策略中启用了包含 Modbus 或 DNP3 关键字的规则，系统将自动分别使用带有当前设置的 Modbus 或 DNP3 预处理器，尽管该预处理器在网络分析策略模块接口中保持禁用状态。有关详细信息，请参阅第 23-68 页上的 Modbus 关键字和第 23-70 页上的 DNP3 关键字。

有关详细信息，请参阅：

配置 Modbus 预处理器

许可证：保护

Modbus 协议由 Modicon 于 1979 年首次发布，是一种广泛使用的 SCADA 协议。Modbus 预处理器可检测 Modbus 流量中的异常，解码 Modbus 协议以供规则引擎进行处理（规则引擎使用 Modbus 关键字来访问某些协议字段）。有关详情，请参见第 23-68 页上的 Modbus 关键字。

单一配置选项允许为预处理器进行 Modbus 流量检查的端口修改默认设置。

如果要下表中所列的 Modbus 预处理器规则生成事件，必须启用这些规则。有关启用规则的详细信息，请参阅第 20-17 页上的设置规则状态。

表 16-1 Modbus 预处理器规则

预处理器规则 GID:SID	说明
144:1	如果 Modbus 报头中的长度与 Modbus 函数代码所要求的长度不匹配，将会生成事件。 每个 Modbus 函数都有预期的请求和响应格式。如果消息长度与预期格式不匹配，将会生成此事件。

表 16-1　Modbus 预处理器规则（续）

预处理器规则 GID:SID	说明
144:2	如果 Modbus 协议 ID 未非零值，将会生成事件。协议 ID 字段用于将其他协议与 Modbus 协议复用。由于预处理器并不处理此类其他协议，因此会生成此事件。
144:3	如果预处理器检测到保留的 Modbus 函数代码，将会生成事件。

请注意，关于 Modbus 预处理器的使用，如果网络不包含任何启用了 Modbus 的设备，您不应该在应用于流量的网络分析策略中启用此预处理器。

可以按照以下步骤修改 Modbus 预处理器监控的端口。

要配置 Modbus 预处理器，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 **SCADA Preprocessors** 下的 **Modbus Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Modbus Configuration 页面。页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　或者，在 **Ports** 中修改预处理器要检查其 Modbus 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口。

步骤 10　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

配置 DNP3 预处理器

许可证：保护

分布式网络协议 (DNP3) 是一种 SCADA 协议，最初开发用于为电站之间提供一致的通信。DNP3 还广泛应用于供水、废物处置、运输及其他行业。

DNP3 预处理器可检测 DNP3 流量中的异常，解码 DNP3 协议以供规则引擎进行处理（规则引擎使用 DNP3 关键字来访问某些协议字段）。有关详情，请参见第 23-70 页上的 DNP3 关键字。

如果要下表中所列的 DNP3 预处理器规则生成事件，必须启用这些规则。有关启用规则的详细信息，请参阅第 20-17 页上的设置规则状态。

表 16-2　　DNP3 预处理器规则

预处理器规则 GID:SID	说明
145:1	在 **Log bad CRC** 已启用的情况下，如果预处理器检测到具有无效校验和的链路层帧，将会生成事件。
145:2	如果预处理器检测到具有无效长度的 DNP3 链路层帧，将会生成事件并阻止该数据包。
145:3	如果预处理器检测到具有无效序列号的传输层分段，将会生成事件并在重组期间阻止数据包。
145:4	如果需要清除 DNP3 重组缓冲区后才能重组完整的片段，将会生成事件。如果在其他分片已加入队列后出现带有 FIR 标志的分片，将会发生这种情况。
145:5	如果预处理器检测到使用保留地址的 DNP3 链路层帧，将会生成事件。
145:6	如果预处理器检测到使用保留函数代码的 DNP3 请求或响应，将会生成事件。

请注意，关于 DNP3 预处理器的使用，如果网络不包含任何启用了 DNP3 的设备，您不应该在应用于流量的网络分析策略中启用此预处理器。有关详情，请参见第 17-26 页上的配置 TCP 数据流预处理。

以下列表说明可配置的 DNP3 预处理器选项。

端口

启用对每个指定端口的 DNP3 流量检查。可以指定单个端口或端口的逗号分隔列表。可以为每个端口指定一个 0 到 65535 之间的值。

Log bad CRCs

如果启用此选项，将会验证包含在 DNP3 链路层帧中的校验和。具有无效校验和的帧将被忽略。

可以启用规则 145:1，以便在检测到无效校验和时生成事件。

要配置 DNP3 预处理器，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 **SCADA Preprocessors** 下的 **DNP3 Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 DNP3 Configuration 页面。页面底部消息会识别包含配置的网络分析策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　或者，在 **Ports** 中修改预处理器要检查其 DNP3 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口。

步骤 10　或者，选择或清除 **Log bad CRCs** 复选框，以便指定是否验证包含在 DNP3 链路层帧中的校验和并忽略具有无效校验和的帧。

步骤 11　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅网络分析策略编辑操作表。

配置传输层和网络层预处理

您在网络分析策略中的网络层预处理器上配置大多数传输，从而使用在入侵策略中启用的规则准备流量进行检查。有关详细信息，请参阅第 11-1 页上的了解网络分析和入侵策略。

网络层和传输层预处理器检测对 IP 分片、校验和验证及 TCP 和 UDP 会话预处理加以利用的攻击。在将数据包发送到预处理器之前，数据包解码器将数据包报头和负载转换为便于预处理器和入侵规则引擎使用的格式，并检测数据包报头的各种异常行为。在数据包解码后到将数据包发送到其他预处理器之前这段期间，内联规范化预处理器会对流量进行规范化以便进行内联部署。

可以按 区域或网络定制在网络分析策略中配置的传输层和网络层预处理器设置。某些传输层和网络层设置全局应用于所有流量，并且可在访问控制策略中配置这些设置。

配置高级传输/网络设置

许可证：保护

高级传输和网络预处理器设置全局应用于所有应用访问控制策略的网络、区域。可以在访问控制策略中而非网络分析策略中配置这些高级设置。

以下各节介绍这些设置：

使用入侵丢弃规则启动活动响应

许可证：保护

丢弃规则是指规则状态设置为 Drop and Generate Events 的入侵规则或预处理器规则。在内联部署中，系统通过丢弃触发数据包并阻止数据包起始的会话来对 TCP 或 UDP 丢弃规则作出响应。在被动部署中，系统无法丢弃数据包，并且除使用活动响应的情况以外，不会阻止会话。

提示 由于在*会话*方面通常未考虑 UDP 数据流，因此，请参阅第 17-28 页上的使用 UDP 数据流预处理，以进一步了解数据流预处理器如何使用封装 IP 数据报报头中的源和目标 IP 地址字段及 UDP 报头中的端口字段来确定流动方向并识别 UDP 会话。

您可以配置 **Maximum Active Responses** 选项来启动一个或多个*活动响应*，从而在有问题的数据包触发 TCP 或 UDP 丢弃规则时，更精确具体地关闭 TCP 连接或 UDP 会话。

在内联部署中启用活动响应后，系统通过丢弃触发数据包并在客户端和服务器流量中均插入 TCP 重置 (RST) 数据包来对 TCP 丢弃规则作出响应。系统在被动部署中无法丢弃数据包；在被动部署中启用活动响应时，系统通过向 TCP 连接的客户端和服务器端均发送 TCP 重置来对 TCP 丢弃规则作出响应。在内联部署或被动部署中启用活动响应后，系统通过向会话的两端发送 ICMP 不可达数据包来关闭 UDP 会话。活动响应在内联部署中最有效，因为重置更有可能及时到达以影响连接或会话。

根据 **Maximum Active Responses** 选项的配置，如果系统看到连接或会话的任一端有其他流量，也可以启动其他活动响应。自从先前响应以来经过指定的秒数后，系统最多会启动数量为指定最大值的每个其他活动响应。

有关有关设置最大活动响应数的信息，请参阅第 17-19 页上的选择 TCP 全局选项。

请注意，无论 **Maximum Active Responses** 的配置如何，已触发的 **resp** 或 **react** 规则也会启动活动响应；但是， **Maximum Active Responses** 控制系统是否以与其控制丢弃规则的最大活动响应数相同的方式来启动 **resp** 和 **react** 规则的其他活动响应。有关详细信息，请参阅第 23-77 页上的使用规则关键字发起活动响应。

您还可以使用 `config response` 命令配置要使用的活动响应接口以及要在被动部署中尝试的 TCP 重置次数。有关详细信息，请参阅第 23-80 页上的设置活动响应重置尝试次数和界面。

预处理器规则不与以下选项关联。

Maximum Active Responses

指定每次 TCP 连接的最大活动响应数 （1 至 25）。如果已启动活动响应的连接上出现其他流量，并且在先前活动响应后流量出现超过**最小响应秒数**，系统会发送其他活动响应，除非已达到指定的最大数量。设置为 0 会禁用丢弃规则触发的活动响应，并禁用 **resp** 或 **react** 规则触发的其他活动响应。有关详细信息，请参阅第 17-2 页上的使用入侵丢弃规则启动活动响应和第 23-77 页上的使用规则关键字发起活动响应。

Minimum Response Seconds

指定等待 1 到 300 秒，直至出现**最大活动响应数**，然后在系统已启动活动响应的连接上的任何其他流量都会产生后续活动响应。

要使用丢弃规则发起活动响应，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 7　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 8　点击 **Transport/Network Layer Preprocessor Settings** 旁边的编辑图标 ( )。

系统将显示 Transport/Network Layer Preprocessor Settings 弹出窗口。

步骤 9　您有以下选项：

- 为每个 TCP 连接的 **Maximum Active Responses** 指定 1 到 25 之间的值。设置为 0 会禁用丢弃规则触发的活动响应，并禁用 **resp** 或 **react** 规则触发的其他活动响应。
- 为 **Minimum Response Seconds** 指定 1 到 300 之间的值，等待直至发生 **Maximum Active Responses** 为止，或者在系统已发起活动响应的连接上的任何其他流量产生后续活动响应为止。

步骤 10　点击 **OK**。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

故障排除：记录会话终止消息

许可证：保护

支持人员可能会在故障排除呼叫期间要求您配置系统，以在单个连接超过指定阈值时记录消息。更改此选项的设置会影响性能，应仅在支持人员的指导下进行操作。

要记录会话终止消息，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 7　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 8　点击 **Transport/Network Layer Preprocessor Settings** 旁边的编辑图标 ( )。

系统将显示 Transport/Network Layer Preprocessor Settings 弹出窗口。

步骤 9　展开 **Troubleshooting Options**。

步骤 10　为 **Session Termination Logging Threshold** 指定字节数，当会话终止并超过该指定数字时，将会记录消息。

1GB 的上限还受到设备上分配用于数据流处理的内存容量的限制。

步骤 11　点击 **OK**。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

验证校验和

许可证：保护

系统可验证所有协议级校验和，以确保接收完整的 IP、TCP、UDP 和 ICMP 传输，且基本级别的数据包在传输过程中未被篡改或意外修改。校验和使用算法来验证数据包中协议的完整性。如果系统计算所得的值与终端主机在数据包中写入的值相同，则数据包将被视为未更改。

禁用校验和验证可能使网络容易受到插入攻击。请注意，系统不生成校验和验证事件。在内联部署中，您可以将系统配置为会丢弃校验和无效的数据包。

要配置校验和，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Edit Policy 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 Transport/Network Layer Preprocessors 中的 **Checksum Verification**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Checksum Verification 页面。页面底部的消息标识包含配置的策略层。有关详细信息，请参阅第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　在被动或内联部署中，可以将 Checksum Verification 部分中的任何选项设置为 **Enabled** 或 **Disabled**；在内联部署中，可以设置为 **Drop**：

- **ICMP 校验和**
- **IP 校验和**
- **TCP 校验和**
- **UDP 校验和**

请注意，要丢弃恶意数据包，除将选项设置为 **Drop** 以外，还必须在关联网络分析策略中启用 **Inline Mode**。有关详细信息，请参阅第 14-5 页上的允许预处理器影响内联部署中的流量。另请注意，在被动部署中将这些选项设置为 **Drop** 与将其设置为 **Enabled** 相同。

步骤 10　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

规范化内联流量

许可证：保护

内联规范化预处理器会将流量规范化，从而尽可能降低攻击者在内联部署中得以避开检测的可能性。如果在网络分析策略中启用内联规范化预处理器，则系统会测试以下两个条件来确保使用的是内联部署：

- 在策略中已启用 **Inline Mode**。请参阅第 14-5 页上的允许预处理器影响内联部署中的流量。
- 已启用内联规范化的访问控制策略应用于以内联方式部署的设备。

仅当两个条件均得到满足时，预处理器才会对指定流量进行规范化。

您可以指定 IPv4、IPv6、ICMPv4、ICMPv6 和 TCP 流量的任意组合的规范化。大多数规范化由内联规范化预处理器逐个数据包执行。但是， TCP 数据流预处理器处理大多数状态相关的数据包和数据流规范化，包括 TCP 负载规范化。

在数据包解码器进行解码后会立即执行内联规范化，直至其他预处理器进行处理。规范化从内数据包层继续执行到外数据包层。

内联规范化预处理器不会生成事件；它准备数据包以供内联部署中的其他预处理器和规则引擎使用。预处理器还有助于确保系统处理的数据包与网络中主机接收的数据包相同。

提示 在内联部署中，思科建议在已启用 **Normalize TCP Payload** 选项的情况下配置内联规范化预处理器。在被动部署中，思科建议配置自适应配置文件。有关详细信息，请参阅第 18-1 页上的在被动部署中调整预处理。

Minimum TTL

当 **Reset TTL** 大于或等于为此选项设置的值（1 至 255）时，请指定以下设置：

- 启用 **Normalize IPv4** 后系统允许 IPv4 Time to Live (TTL) 字段使用的最小值；较小的值会导致将 TTL 的数据包值规范化为针对 **Reset TTL** 设置的值
- 启用 **Normalize IPv6** 后系统允许 IPv6 Hop Limit 字段使用的最小值；较小的值会导致将 TTL 的数据包值规范化为针对 **Reset TTL** 设置的值

此字段为空时，系统假设值为 1。

请注意，可以启用解码器规则类别中的以下规则来生成此选项的事件：

- 您可以启用规则 116:428，以在系统检测到 TTL 小于指定最小值的 IPv4 数据包时生成事件。
- 您可以启用规则 116:270，以在系统检测到跳数限制小于指定最小值的 IPv6 数据包时生成事件。

有关详细信息，请参阅第 17-17 页上的配置数据包解码中的 **Detect Protocol Header Anomalies** 选项。

Reset TTL

如果设置为大于或等于 **Minimum TTL** 的值（1 到 255），请规范化以下字段：

- IPv4 TTL 字段（如果启用了 **Normalize IPv4**）
- IPv6 Hop Limit 字段（如果启用了 **Normalize IPv6**）

当数据包值小于 **Minimum TTL** 时，系统会通过将其 TTL 或 Hop Limit 值更改为针对此选项设置的值来规范化数据包。将此选项设置为值 0 或任何小于 **Minimum TTL** 的值会禁用此选项。此字段为空时，系统假设值为 0。

Normalize IPv4

启用 IPv4 流量规范化。此选项处于启用状态并且为 **Reset TTL** 设置的值会启用 TTL 规范化时，系统还会根据需要规范化 TTL 字段。启用此选项后，还可以启用 **Normalize Don't Fragment Bits** 和 **Normalize Reserved Bits**。

启用此选项时，系统执行以下基本 IPv4 规范化：

- 将具有多余负载的数据包截断至 IP 报头中指定的数据报长度
- 清除 Differentiated Services (DS) 字段（以前称为 Type of Service (TOS) 字段）
- 将所有选项八位元设置为 1 (No Operation)

Normalize Don't Fragment Bit

清除 IPv4 Flags 报头字段的 1 位 Don't Fragment 子字段。通过启用此选项，下游路由器可在必要时对数据包进行分片而不是将其丢弃；启用此选项还可以根据要丢弃的构造数据包来防止躲避检测。必须启用 **Normalize IPv4** 后才可以选择此选项。

Normalize Reserved Bit

清除 IPv4 Flags 报头字段的 1 位 Reserved 子字段。通常会启用此选项。必须启用 **Normalize IPv4** 后才可以选择此选项。

Normalize TOS Bit

清除一个字节的 Differentiated Services 字段（以前称为 Type of Service）。必须启用 **Normalize IPv4** 后才可以选择此选项。

Normalize Excess Payload

将具有多余负载的数据包截断至 IP 报头中指定的数据报长度加上第 2 层 （例如以太网）报头，但是不截断为小于最小帧长度。必须启用 **Normalize IPv4** 后才可以选择此选项。

Normalize IPv6

将 Hop-by-Hop Options 和 Destination Options 扩展报头中的所有 Option Type 字段设置为 00（跳过并继续处理）。此选项处于启用状态并且为 **Reset TTL** 设置的值会启用跳数限制规范化时，系统还会根据需要规范化 Hop Limit 字段。

Normalize ICMPv4

清除 ICMPv4 流量中 Echo (Request) 和 Echo Reply 消息内的 8 位 Code 字段。

Normalize ICMPv6

清除 ICMPv6 流量中 Echo (Request) 和 Echo Reply 消息内的 8 位 Code 字段。

Normalize/Clear Reserved Bits

清除 TCP 报头中的保留位。

Normalize/Clear Option Padding Bytes

清除任何 TCP 选项填充字节。

Clear Urgent Pointer if URG=0

如果未设置紧急 (URG) 控制位，则清除 16 位 TCP 报头 Urgent Pointer 字段。

Clear Urgent Pointer/URG on Empty Payload

如果没有负载，则清除 TCP 报头 Urgent Pointer 字段和 URG 控制位。

Clear URG if Urgent Pointer is Not Set

如果未设置紧急指针，则清除 TCP 报头 URG 控制位。

Normalize Urgent Pointer

如果指针大于负载长度，则将两字节的 TCP 报头 Urgent Pointer 字段设置为负载长度。

Normalize TCP Payload

启用 TCP Data 字段的规范化以确保重传数据的一致性。无法正确重组的所有数据段都会被丢弃。

Remove Data on SYN

如果 TCP 操作系统策略**不是** Mac OS，则移除同步 (SYN) 数据包中的数据。

此选项还对规则 129:2 禁用事件生成。

Remove Data on RST

从 TCP 重置 (RST) 数据包中移除所有数据。

Trim Data to Window

将 TCP Data 字段修剪为在 Window 字段中指定的大小。

Trim Data to MSS

如果负载长度大于 MSS，则将 TCP Data 字段修剪为 Maximum Segment Size (MSS)

Block Unrecoverable TCP Header Anomalies

启用此选项时，系统阻止异常 TCP 数据包，这些数据包在规范化的情况下会无效，并可能受到接收主机的阻止。例如，系统阻止后续传输到已建立的会话上的任何 SYN 数据包。

无论是否启用规则，系统都会丢弃与以下任何 TCP 数据流预处理器规则匹配的任何数据包：

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 至 129:19

Total Blocked Packets 性能图跟踪内联部署中阻止的数据包的数量，并且，在被动部署，跟踪在内联部署中已阻止的数量。

显式堵塞通知

对显式堵塞通知 (ECN) 标志启用逐个数据包或逐条数据流规范化，如下所示：

- 选择 **Packet** 以逐个数据包清除 ECN 标志（无论协商与否）
- 选择 **Stream** 以逐条数据流清除 ECN 标志（如果未协商 ECN 的使用）

如果选择 **Stream**，您还必须确保启用 TCP 数据流预处理器的 **Require TCP 3-Way Handshake** 选项以进行此规范化；有关详细信息，请参阅第 17-20 页上的选择 TCP 策略选项。

允许这些 TCP 选项

禁用您在流量中允许的特定 TCP 选项的规范化。

系统不对您明确允许的选项进行规范化。系统会通过将您未明确允许的选项设置为 No Operation （TCP 选项 1）来规范化这些选项。

系统始终允许 Maximum Segment Size (MSS)、 Window Scale 和 Time Stamp TCP 选项，因为这些选项常用于实现最佳 TCP 性能。无论 **Allow These TCP Options** 的配置如何，系统都会规范化这些常用选项。系统不会自动允许其他不太常用的选项。

您可以通过配置选项关键字和/或选项编号的逗号分隔列表来允许特定选项，如下例所示：

```
sack, echo, 19
```

指定选项关键字等同于指定与该关键字相关的一个或多个 TCP 选项的编号。例如，指定 `sack` 等同于指定 TCP 选项 4 (Selective Acknowledgment Permitted) 和选项 5 (Selective Acknowledgment)。选项关键字不区分大小写。

您还可以指定 `any`，这样将会允许所有 TCP 选项并有效地禁用所有 TCP 选项的规范化。

下表总结了如何指定要允许的 TCP 选项。如果将字段留空，则系统仅允许 MSS、 Window Scale 和 Time Stamp 选项。

可指定的内容	以允许.....
sack	TCP 选项 4 (Selective Acknowledgment Permitted) 和选项 5 (Selective Acknowledgment)
echo	TCP 选项 6 (Echo Request) 和选项 7 (Echo Reply)
partial_order	TCP 选项 9 (Partial Order Connection Permitted) 和选项 10 (Partial Order Service Profile)
conn_count	TCP 连接计数选项 11 (CC)、选项 12 (CC.New) 和选项 13 (CC.Echo)
alt_checksum	TCP 选项 14 (Alternate Checksum Request) 和选项 15 (Alternate Checksum)
md5	TCP 选项 19 (MD5 Signature)
选项编号 （2 至 255）	特定选项，包括没有关键字的选项
any	所有 TCP 选项；此设置会有效地禁用 TCP 选项规范化

如果没有为此选项指定 `any`，则规范化会包含以下内容：

- 除 MSS、 Window Scale、 Time Stamp 及任何明确允许的选项以外，所有选项字节都设置为 No Operation （TCP 选项 1）
- 如果时间戳存在但无效，或者有效但未协商，则将时间戳八位元设置为 No Operation
- 如果 Time Stamp 已协商但不存在，则阻止数据包
- 如果未设置 Acknowledgment (ACK) 控制位，则清除 Time Stamp Echo Reply (TSecr) 选项字段
- 如果未设置 SYN 控制位，则将 MSS 和 Window Scale 选项设置为 No Operation (TCP Option 1)

要配置内联规范化预处理器，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Edit Policy 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　根据在 Transport/Network Layer Preprocessors 下是否已启用 **Inline Normalization**，有两个选项：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Inline Normalization 页面。页面底部的消息标识包含配置的策略层。有关详细信息，请参阅第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　您可以设置第 17-5 页上的规范化内联流量中所述的任何选项。

步骤 10　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

对 IP 数据包进行分片重组

许可证：保护

由于 IP 数据报大于最大传输单位 (MTU) 而将其分为两个或多个更小的 IP 数据报，这个过程即为数据报 *分片*。单个 IP 数据报片段可能未包含足够的信息来识别隐藏攻击。攻击者可能尝试通过将攻击数据传输到分片数据包中来躲避检测。在规则引擎对分片的 IP 数据报执行规则之前， IP 分片重组预处理器会重组这些数据报，以便规则可以更适当地识别这些数据包中的攻击。如果分片的数据报无法重组，则不对其执行规则。

请注意，如果您希望 IP 分片重组预处理器规则生成事件，则必须启用这些规则，其生成器 ID (GID) 为 123。有关详细信息，请参阅第 20-17 页上的设置规则状态。

有关详细信息，请参阅：

- 第 17-10 页上的了解 IP 分片漏洞
- 第 17-11 页上的基于目标的分片重组策略
- 第 17-12 页上的选择分片重组选项
- 第 17-13 页上的配置 IP 分片重组

了解 IP 分片漏洞

许可证：保护

启用 IP 分片重组可以帮助您检测针对网络上主机的攻击（例如泪滴 [teardrop] 攻击）和针对系统本身的资源消耗攻击（例如 Jolt2 攻击）。

泪滴攻击利用某些操作系统中在尝试重组重叠 IP 片段时会导致这些操作系统崩溃的漏洞。IP 分片重组预处理器在被启用并配置为识别重叠片段之后，会执行此操作。IP 分片重组预处理器会检测重叠片段攻击（例如泪滴攻击）中的第一批数据包，但对于同一攻击不会检测后续数据包。

Jolt2 攻击会发送同一分片的 IP 数据包的大量副本，以尝试过度使用 IP 分片重组器并导致拒绝服务攻击。内存使用上限会中断此攻击以及 IP 分片重组预处理器中的类似攻击，并在全面检查基础上注重系统自我保护。这样，系统不会因攻击而崩溃，可保持运行，并继续检查网络流量。

不同的操作系统以不同方式重组分片数据包。可以确定主机运行的操作系统的攻击者还可以对恶意数据包进行分片，以便目标主机以特定方式对这些数据包进行重组。由于系统不知道受监控网络上的主机运行的操作系统，因此预处理器可能会不正确地重组和检查数据包，致使漏洞成功躲过检测。要缓解这种攻击，您可以配置分片重组预处理器，使其会针对网络中的每个主机使用适当方法对数据包进行分片重组。有关详细信息，请参阅第 17-11 页上的基于目标的分片重组策略。

请注意，您也可以使用自适应配置文件，通过数据包中目标主机的主机操作系统信息来为 IP 分片重组预处理器动态选择基于目标的策略。有关详细信息，请参阅第 18-1 页上的在被动部署中调整预处理。

基于目标的分片重组策略

许可证：保护

主机的操作系统使用三个条件来确定重组数据包时支持哪些数据包片段：操作系统接收片段的顺序；片段的偏移量（片段的距离，以字节为单位，从数据包开头起算）；以及片段相对于重叠片段的开始和结束位置。虽然每个操作系统都使用这些条件，但是不同的操作系统在重组分片数据包时支持不同的片段。因此，网络中具有不同操作系统的两个主机可能会以完全不同的方式重组同一组重叠片段。

攻击者（了解其中一个主机的操作系统）可能会尝试通过发送隐藏在重叠数据包片段中的恶意内容来逃避检测并利用该主机。该数据包经过重组和检查后看似无害，但是由目标主机进行重组后则会包含恶意的漏洞。但是，如果将 IP 分片重组预处理器配置为可感知受监控网段上运行的操作系统，则它会以与目标主机相同的方式重组分片，从而识别攻击。

根据目标主机的操作系统，可以将 IP 分片重组预处理器配置为使用七个分片重组策略之一。下表列出了这七个策略以及使用每个策略的操作系统。First 和 Last 这两个策略名称反映这些策略是否支持原始或后续重叠数据包。

表 17-1　　基于目标的分片重组策略

策略	操作系统
BSD	AIX
	FreeBSD
	IRIX
	VAX/VMS
BSD-right	HP JetDirect
首页	Mac OS
	HP-UX
Linux	Linux
	OpenBSD
Last	Cisco IOS
Solaris	SunOS
Windows	Windows

选择分片重组选项

许可证：保护

您可以选择简单启用或禁用 IP 分片重组；但是，思科建议您以更精细的级别指定已启用的 IP 分片重组预处理器的行为。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

您可以配置全局 **Preallocated Fragments** 选项：

Preallocated Fragments

预处理器一次可以处理的最大单个片段数量。指定要预分配的片段节点的数量会启用静态内存分配。

注意事项

处理单个片段会使用大约 1550 字节的内存。如果预处理器处理单个片段所需的内存超过设备的预定允许的内存限制，则设备的内存限制优先。

您可以为每个 IP 分片重组策略配置以下选项：

Networks

要对其应用分片重组策略的一个或多个主机的 IP 地址。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。您可以指定总共最多 255 个配置文件（包括默认策略）。有关在 ASA FirePOWER 模块中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-3 页上的IP 地址约定。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址表示法来表示 `any`（例如， 0.0.0.0/0 或 ::/0）。

另请注意，为使基于目标的策略可以处理流量，您识别的网络必须与由网络分析策略 （其中已配置该基于目标的策略）处理的网络、区域 匹配或者是其子集。有关详细信息，请参阅第 13-2 页上的利用网络分析策略自定义预处理。

Policy

要为受监控网段上的主机组使用的分片重组策略。有七个策略可供选择：BSD、 BSD-Right、First、 Linux、 Last、 Solaris 和 Windows。有关这些策略的详细信息，请参阅第 17-11 页上的基于目标的分片重组策略。

Timeout

指定预处理器引擎在重组分片数据包时可用的最长时间（以秒为单位）。如果在指定的时间段内无法重组数据包，则预处理器引擎会停止尝试重组数据包并丢弃接收到的片段。

Minimum TTL

指定数据包可具有的可接受最小 TTL 值。此选项检测基于 TTL 的插入攻击。

您可以启用规则 123:1 来生成此选项的事件。有关详细信息，请参阅第 20-17 页上的设置规则状态。

Detect Anomalies

确定分片问题，例如重叠片段。

您可以启用以下规则来生成此选项的事件：

- 123:1 至 123:4
- 123:5（BSD 策略）
- 123:6 至 123:8

Overlap Limit

指定在检测到某会话中存在所配置数量（介于 0 [无限制] 和 255 之间）的重叠片段时，针对该会话的分片重组将会停止。必须启用 **Detect Anomalies** 后才可以配置此选项。不指定值将会禁用此选项。

您可以启用规则 123:12 来生成此选项的事件。有关详细信息，请参阅第 20-17 页上的设置规则状态。

Minimum Fragment Size

指定在检测到小于配置数量 （介于 0 [无限制] 和 255 字节之间）的非最后一个片段时，数据包将被视为恶意数据包。必须启用 **Detect Anomalies** 后才可以配置此选项。不指定值将会禁用此选项。

您可以启用规则 123:13 来生成此选项的事件。有关详细信息，请参阅第 20-17 页上的设置规则状态。

配置 IP 分片重组

许可证：保护

您可以使用以下步骤配置 IP 分片重组预处理器。有关 IP 分片重组预处理器配置选项的详细信息，请参阅第 17-12 页上的选择分片重组选项。

要配置 IP 分片重组，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Edit Policy 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　根据是否已启用 Transport/Network Layer Preprocessors 下的 **IP Defragmentation**，有两个选项：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 IP Defragmentation 页面。页面底部的消息标识包含配置的策略层。有关详细信息，请参阅第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　或者，可以在 Global Settings 页面区域中修改 **Preallocated Fragments** 的设置。

步骤 10　此时您有两种选择：

- 添加新的基于目标的策略。点击页面左侧 **Servers** 旁边的添加图标 ( )。系统将显示 Add Target 弹出窗口。在 **Host Address** 字段中指定一个或多个 IP 地址，然后点击 **OK**。

  可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。您可以创建总共 255 个基于目标的策略 （包括默认策略）。有关在 ASA FirePOWER 模块中使用 IP 地址块的信息，请参阅第 1-3 页上的IP 地址约定。

  请注意，为使基于目标的策略处理流量，您识别的网络必须与由网络分析策略 （其中已配置该基于目标的策略）处理的网络、区域 匹配或者是其子集。有关详细信息，请参阅第 13-2 页上的利用网络分析策略自定义预处理。

  新条目将出现在页面左侧的目标列表中，突出显示以表明其已被选定；Configuration 部分会进行更新，以反映所添加的策略的当前配置。

- 修改现有基于目标的策略的设置。点击您在页面左侧 **Hosts** 中添加的策略的配置地址，或者点击 **default**。

  所选项目将会突出显示，并且 Configuration 部分会进行更新以显示所选策略的当前配置。要删除现有的基于目标的策略，请点击要删除的策略旁边的删除图标 ( )。

步骤 11　或者，可以修改 Configuration 页面区域中的任何选项。

步骤 12　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

了解数据包解码

许可证：保护

在将捕获的数据包发送到预处理器之前，系统首先会将数据包发送到数据包解码器。数据包解码器将数据包报头和负载转换为便于预处理器和规则引擎使用的格式。每个堆栈层依次进行解码，从数据链路层开始并继续直至网络层和传输层。

请注意，如果您希望数据包解码器规则生成事件，则必须启用这些规则，其生成器 ID (GID) 为 116。有关详细信息，请参阅第 20-17 页上的设置规则状态。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

解码 GTP 数据信道

解码封装的 GTP （通用分组无线业务 [GPRS] 隧道协议）数据信道。默认情况下，解码器会解码端口 3386 上的版本 0 数据和端口 2152 上的版本 1 数据。您可以使用 `GTP_PORTS` 默认变量修改用于识别封装的 GTP 流量的端口。有关详细信息，请参阅第 2-13 页上的优化预定义默认变量。

您可以启用规则 116:297 和 116:298 来生成此选项的事件。

检测非标准端口上的 Terado

检查除端口 3544 以外的其他 UDP 端口上识别的 IPv6 流量的 Teredo 隧道。

系统始终检查存在的 IPv6 流量。默认情况下，IPv6 检查包括 4in6、6in4、6to4 和 6in6 隧道方案，如果 UDP 报头指定端口 3544，还包括 Teredo 隧道。

在 IPv4 网络中，IPv4 主机可以使用 Teredo 协议通过 IPv4 网络地址转换 (NAT) 设备传输 IPv6 流量。 Teredo 将 IPv6 数据包封装在 IPv4 UDP 数据报中，以允许在 IPv4 NAT 设备后面进行 IPv6 连接。系统通常使用 UDP 端口 3544 识别 Teredo 流量。但是，攻击者可能会使用非标准端口来尝试避开检测。您可以启用 **Detect Teredo on Non-Standard Ports** 来促使系统检查 Teredo 隧道的所有 UDP 负载。

Teredo 解码仅发生在第一个 UDP 报头上，并且仅当 IPv4 用于外部网络层时才会发生。如果由于 IPv6 数据中封装的 UDP 数据而在 Teredo IPv6 层之后出现第二个 UDP 层，则规则引擎会使用 UDP 入侵规则对内部和外部 UDP 层均进行分析。

请注意，**policy-other** 规则类别中的入侵规则 12065、12066、12067 和 12068 会检测 Teredo 流量，但不对这些流量进行解码。您可以根据需要在内联部署中使用这些规则丢弃 Teredo 流量；但是，启用 **Detect Teredo on Non-Standard Ports** 时，应确保这些规则处于禁用状态或者设置为生成事件而不丢弃流量。有关详细信息，请参阅第 20-9 页上的过滤入侵策略中的规则和第 20-17 页上的设置规则状态。

检测过大长度值

在数据包报头指定的数据包长度大于实际数据包长度时进行检测。

您可以启用规则 116:6、 116:47、 116:97 和 116:275 来生成此选项的事件。

检测无效 IP 选项

检测无效 IP 报头选项以识别使用无效 IP 选项的漏洞。例如，存在针对防火墙的拒绝服务攻击，该攻击导致系统冻结。防火墙尝试解析无效的 Timestamp 和 Security IP 选项且未能检查到零长度，导致无法恢复的无限循环。规则引擎会识别零长度选项并提供可用于缓解对防火墙的攻击的信息。

您可以启用规则 116:4 和 116:5 来生成此选项的事件。有关详细信息，请参阅第 20-17 页上的设置规则状态。

检测试验性 TCP 选项

检测具有试验性 TCP 选项的 TCP 报头。下表介绍了这些选项。

TCP 选项	说明
9	允许的偏序连接
10	偏序服务配置文件
14	替代校验和请求
15	替代校验和数据
18	尾部校验和
20	空间通信协议标准 (SCPS)
21	选择性否定确认 (SCPS)
22	记录边界 (SCPS)

TCP 选项	说明
23	损坏 (SPCS)
24	SNAP
26	TCP 压缩过滤器

由于这些是试验性选项，因此，某些系统未对其进行说明，可能容易产生漏洞。

注　除上表中列出的试验性选项外，系统还将选项编号大于 26 的任何 TCP 选项视为试验性选项。

您可以启用规则 116:58 来生成此选项的事件。有关详细信息，请参阅第 20-17 页上的设置规则状态。

检测过时 TCP 选项

检测具有过时 TCP 选项的 TCP 报头。由于这些是过时选项，因此，某些系统未对其进行说明，可能容易产生漏洞。下表介绍了这些选项。

TCP 选项	说明
6	回显
7	回显回复
16	Skeeter
17	Bubba
19	MD5 签名
25	未分配

您可以启用规则 116:57 来生成此选项的事件。有关详细信息，请参阅第 20-17 页上的设置规则状态。

检测 T/TCP

检测带有 CC.ECHO 选项的 TCP 报头。CC.ECHO 选项确认使用的是事务 TCP (T/TCP)。由于 T/TCP 报头选项未广泛使用，因此，某些系统未对其进行说明，可能容易产生漏洞。

您可以启用规则 116:56 来生成此选项的事件。有关详细信息，请参阅第 20-17 页上的设置规则状态。

检测其他 TCP 选项

检测具有其他 TCP 解码事件选项未检测到的无效 TCP 选项的 TCP 报头。例如，此选项检测长度不正确或者选项数据长度超过 TCP 报头范围的 TCP 选项。

您可以启用规则 116:54、 116:55 和 116:59 来生成此选项的事件。有关详细信息，请参阅第 20-17 页上的设置规则状态。

检测协议报头异常

检测更具体的 IP 和 TCP 解码器选项未检测到的其他解码错误。例如，解码器可能会检测到格式错误的数据链路协议报头。

要生成此选项的事件，可以启用除了与其他数据包解码器选项专门相关的规则以外的任何数据包解码器规则。有关详细信息，请参阅第 20-17 页上的设置规则状态

请注意，以下规则生成异常 IPv6 流量触发的事件：116:270 至 116:274、116:275 至 116:283、116:291、116:292、116:295、116:296、116:406、116:458、116:460、116:461。

另请注意与内联规范化预处理器的 **Minimum TTL** 选项相关的以下规则：

- 您可以启用规则 116:428，以在系统检测到 TTL 小于指定最小值的 IPv4 数据包时生成事件。
- 您可以启用规则 116:270，以在系统检测到跳数限制小于指定最小值的 IPv6 数据包时生成事件。

有关详细信息，请参阅第 17-5 页上的规范化内联流量中的内联规范化 **Minimum TTL** 选项。

配置数据包解码

许可证：保护

您可以在 Packet Decoding 配置页面上配置数据包解码。有关数据包解码配置选项的详细信息，请参阅第 17-14 页上的了解数据包解码。

要配置数据包解码，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Edit Policy 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否已启用 Transport/Network Layer Preprocessors 中的 **Packet Decoding**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Packet Decoding 页面。页面底部的消息标识包含配置的策略层。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改

步骤 9　可以启用或禁用 Packet Decoding 页面上的任何检测选项。有关详细信息，请参阅第 17-14 页上的了解数据包解码。

步骤 10　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

使用 TCP 数据流预处理

许可证：保护

TCP 协议定义连接可以处于的各种状态。每个 TCP 连接通过源 IP 地址和目标 IP 地址以及源端口和目标端口进行识别。 TCP 一次仅允许存在一个具有相同连接参数值的连接。

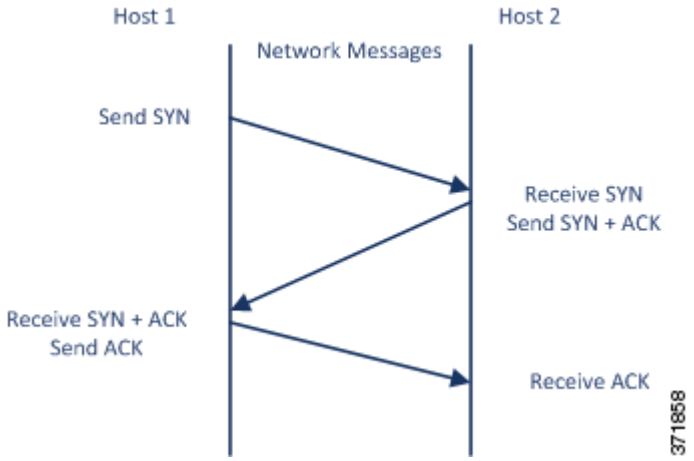
请注意，如果您希望 TCP 数据流预处理器规则生成事件，则必须启用这些规则，其生成器 ID (GID) 为 129。有关详细信息，请参阅第 20-17 页上的设置规则状态。

有关详细信息，请参阅：

了解与状态相关的 TCP 漏洞

许可证：保护

如果向入侵规则添加带有 `established` 参数的 `flow` 关键字，则入侵规则引擎会在有状态模式下检查与规则和流指令匹配的数据包。状态模式仅评估通过客户端与服务器之间的合法三次握手建立的 TCP 会话所包含的流量。下图说明三次握手。



您可以配置系统，以便预处理器对无法识别为已建立的 TCP 会话的一部分的任何 TCP 流量进行检测；但是，对于典型使用不建议此操作，因为事件会使系统迅速过载且不会提供有意义的数据。

stick 和 snot 之类的攻击使用系统的广泛的规则集和数据包检测自身。这些工具根据基于 Snort 的入侵规则生成数据包，并通过网络发送这些数据包。如果您的规则不包括用于为状态检查配置规则的 `flow` 或 `flowbits` 关键字，则每个数据包将触发规则，进而导致系统过载。您可以通过状态检查来忽略这些数据包，因为它们不是已建立的 TCP 会话的一部分，而且不提供有意义的信息。执行状态检查时，规则引擎仅检测属于已建立的 TCP 会话的一部分的那些攻击，从而使分析人员关注这些攻击而不是由 stick 或 snot 攻击导致的事件量。

选择 TCP 全局选项

许可证：保护

TCP 数据流预处理器具有一个全局选项，用于控制 TCP 数据流预处理器的功能。

预处理器规则未与此选项关联。

Packet Type Performance Boost

支持忽略已启用规则中未指定的所有端口和应用协议的 TCP 流量，但在源端口和目标端口均设置为 `any` 的 TCP 规则具有 `flow` 或 `flowbits` 选项时除外。这种性能改进可能会导致未能检测出某些攻击。

了解基于目标的 TCP 策略

许可证：保护

不同操作系统以不同方法实施 TCP。例如， Windows 和其他一些操作系统需要 TCP 重置段以具有精确的 TCP 序列号来重置会话，而 Linux 和其他操作系统则允许使用一系列序列号。在本示例中，数据流预处理器必须明确了解目标主机会如何根据序列号对重置作出响应。仅当目标主机认为重置有效时，数据流预处理器才会停止跟踪会话，因此，攻击在预处理器停止检查数据流后无法通过发送数据包来躲避检测。在 TCP 实施中的其他变化包括操作系统是否采用 TCP 时间戳选项，并且在采用时如何处理时时间戳，以及操作系统接受还是忽略 SYN 数据包中的数据等等方面。

不同操作系统也以不同方式重组重叠的 TCP 数据段。重叠的 TCP 数据段可能会反映未确认的 TCP 流量的正常重传。它们也可能表示攻击者（了解其中一个主机的操作系统）尝试通过发送隐藏在重叠数据段中的恶意内容来躲避检测并利用该主机。但是，您可以将数据流预处理器配置为可感知受监控网段上运行的操作系统，使其以与目标主机相同的方式重组数据段，从而识别攻击。

您可以创建一个或多个 TCP 策略，以根据受监控网段上的不同操作系统定制 TCP 数据流检查和重组。对于每个策略，可识别 13 个操作系统策略之一。您根据需要使用尽可能多的 TCP 策略将每个 TCP 策略绑定到特定 IP 地址或地址块，以识别使用其他操作系统的任意或所有主机。默认 TCP 策略适用于在任何其他 TCP 策略中未识别的受监控网络上的任何主机，因此无需为默认 TCP 策略指定 IP 地址、 CIDR 块或前缀长度。

请注意，您也可以使用自适应配置文件，通过数据包中目标主机的主机操作系统信息来为 TCP 数据流预处理器动态选择基于目标的策略。有关详细信息，请参阅第 18-1 页上的在被动部署中调整预处理。

下表列出了操作系统策略以及使用每个策略的主机操作系统。

表 17-2　TCP 操作系统策略

策略	操作系统
首页	未知 OS
Last	Cisco IOS
BSD	AIX FreeBSD OpenBSD
Linux	Linux 2.4 内核 Linux 2.6 内核
旧 Linux	Linux 2.2 及更低版本的内核
Windows	Windows 98 Windows NT Windows 2000 Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista
Solaris	Solaris OS SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 及更高版本
HPUX 10	HP-UX 10.2 及更低版本
Mac OS	Mac OS 10 (Mac OS X)

提示　当您不知道主机操作系统时， First 操作系统策略可以提供一些保护。但是，它可能会导致未能检测出某些攻击。如果您知道操作系统，则应该编辑策略以指定正确的操作系统。

选择 TCP 策略选项

许可证：保护

以下列表介绍可设置以识别和控制 TCP 数据流预处理器检查的 TCP 流量的选项。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

Network

指定要对其应用 TCP 数据流重组策略的主机 IP 地址。

可以指定单个 IP 地址或地址块。总共最多可以指定 255 个配置文件（包括默认策略）。有关在 ASA FirePOWER 模块中使用 IPv4 和 IPv6 地址块的详细信息，请参阅第 1-3 页上的IP 地址约定。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址表示法来表示 `any`（例如， 0.0.0.0/0 或 ::/0）。

另请注意，为使基于目标的策略可以处理流量，您识别的网络必须与由网络分析策略（其中已配置该基于目标的策略）处理的网络、区域匹配或者是其子集。有关详细信息，请参阅第 13-2 页上的利用网络分析策略自定义预处理。

Policy

识别一个或多个目标主机的 TCP 策略操作系统。如果选择除 **Mac OS** 以外的其他策略，则系统会从同步 (SYN) 数据包中删除数据并禁用规则 129:2 的事件生成。

有关详细信息，请参阅第 17-19 页上的了解基于目标的 TCP 策略。

Timeout

规则引擎在状态表中保持数据流处于非活动状态的秒数（介于 1 和 86400 之间）。如果数据流在指定时间内未重组，则入侵规则引擎会将其从状态表中删除。

注　如果设备部署在网络流量可能达到设备的带宽限制的网段上，则应考虑将该值设置为较大值（例如 600 秒），以降低处理开销量。

Maximum TCP Window

指定由接收主机指定的所允许的最大 TCP 窗口大小（1 至 1073725440 字节）。值设置为 0 会禁用检查 TCP 窗口大小。

注意事项　上限是 RFC 允许的最大窗口大小，旨在防止攻击者躲避检测；但是，设置明显过大的最大窗口大小可能导致自愿接受的拒绝服务。

您可以启用规则 129:6 来生成此选项的事件。有关详细信息，请参阅第 20-17 页上的设置规则状态。

Overlap Limit

指定在检测到某会话中存在所配置数量（介于 0 [无限制] 和 255 之间）的重叠分段时，针对该会话的分段重组将会停止，并且，如果 **Stateful Inspection Anomalies** 以及随附的预处理器规则均处于启用状态，将会生成事件。

您可以启用规则 129:7 来生成此选项的事件。有关详细信息，请参阅第 20-17 页上的设置规则状态。

Flush Factor

在内联部署中，指定在经过所配置数量（介于 1 和 2048 之间）的大小未减小的分段后检测到大小减小的分段时，系统会刷新为进行检测而累积的分段数据。值设置为 0 会禁用此分段模式的检测（这可能意味着请求或响应结束）。请注意，必须启用 Inline Normalization **Normalize TCP Payload** 选项才会使此选项生效。有关详细信息，请参阅第 17-5 页上的规范化内联流量。

Stateful Inspection Anomalies

检测 TCP 堆栈中的异常行为。启用随附的预处理器规则后，如果 TCP/IP 堆栈编写得不好，可能会生成许多事件。

您可以启用以下规则来生成此选项的事件：

– 129:1 至 129:5

- 129:6（仅适用于 Mac OS）
- 129:8 至 129:11
- 129:13 至 129:19

有关详细信息，请参阅第 20-17 页上的设置规则状态。

TCP Session Hijacking

通过针对会话上接收到的后续数据包验证三次握手期间从 TCP 连接两端检测到的硬件 (MAC) 地址来检测 TCP 会话劫持。当一端或另一端的 MAC 地址不匹配时，如果启用了 **Stateful Inspection Anomalies** 以及两个对应的预处理器规则之一，系统会生成事件。

您可以启用规则 129:9 和 129:10 来生成此选项的事件。有关详细信息，请参阅第 20-17 页上的设置规则状态。

Consecutive Small Segments

启用 **Stateful Inspection Anomalies** 后，可指定允许的连续 TCP 小分段的最大数量（1 至 2048）。值设置为 0 会禁止连续小分段。

此选项必须与 **Small Segment Size** 选项一起进行设置；您可以同时禁用这两个选项或者将它们都设置为非零值。请注意，在无干预确认的情况下接收多达 2000 个连续分段，即使每个分段长度为 1 字节，分段数量也会远远超出您通常的预期。

您可以启用规则 129:12 来生成此选项的事件。有关详细信息，请参阅第 20-17 页上的设置规则状态。

Small Segment Size

启用 **Stateful Inspection Anomalies** 后，可指定被视为小分段的 TCP 分段大小（1 至 2048 字节）。值设置为 0 会禁止指定小分段的大小。

此选项必须与 **Consecutive Small Segments** 选项一起进行设置；您可以同时禁用这两个选项或者将它们都设置为非零值。请注意，一个 2048 字节的 TCP 分段大于普通的 1500 字节的以太网帧。

Ports Ignoring Small Segments

启用 **Stateful Inspection Anomalies**、**Consecutive Small Segments** 和 **Small Segment Size** 后，您或者可以指定一个或多个会忽略小 TCP 分段检测的端口的逗号分隔列表。将此选项留空表示未忽略任何端口。

您可以向列表中添加任何端口，但是列表仅影响 TCP 策略中的某个 **Perform Stream Reassembly on port** 列表中指定的端口。

Require TCP 3-Way Handshake

指定仅在 TCP 三次握手完成时，会话才被视为已建立的会话。禁用此选项可提高性能，防御 SYN 泛洪攻击，并允许在部分异步环境中操作。启用此选项可避免尝试通过发送不属于已建立的 TCP 会话的信息来生成误报的攻击。

您可以启用规则 129:20 来生成此选项的事件。有关详细信息，请参阅第 20-17 页上的设置规则状态。

3-Way Handshake Timeout

指定启用 **Require TCP 3-Way Handshake** 后必须允许用于完成握手的时间（0 [无限制] 至 86400 秒 [24 小时]）。必须启用 **Require TCP 3-Way Handshake** 后才能修改此选项的值。

Packet Size Performance Boost

将预处理器设置为在重组缓冲区中不对大数据包进行排队。这种性能改进可能会导致未能检测出某些攻击。禁用此选项可防止使用 1 到 20 字节的小数据包尝试躲避检测。当您肯定所有流量都由超大数据包组成并因此无此类攻击时，可启用此选项。

Legacy Reassembly

重组数据包时，将数据流预处理器设置为模拟废弃的数据流 4 预处理器，借此可以将该数据流预处理器重组的事件与基于数据流 4 预处理器重组的相同数据流的事件相比较。

Asynchronous Network

指定受监控网络是否为异步网络，即，系统只能看到一半流量的网络。启用此选项后，系统不重组 TCP 数据流来提高性能。

Perform Stream Reassembly on Client Ports, Server Ports, Both Ports

为客户端端口和/或服务器端口指定用于识别要重组的数据流预处理器流量的端口的逗号分隔列表。请参阅第 17-24 页上的选择数据流重组选项。

Perform Stream Reassembly on Client Services, Server Services, Both Services

为客户端服务和/或服务器服务指定用于识别要重组的数据流预处理器流量的服务。请参阅第 17-24 页上的选择数据流重组选项。

Troubleshooting Options: Maximum Queued Bytes

支持人员可能会在故障排除呼叫期间要求您指定可以在 TCP 连接的一端排队的数据量。值 0 表示无限字节数。

注意事项 更改此故障排除选项的设置会影响性能，应仅在支持人员的指导下进行操作。

Troubleshooting Options: Maximum Queued Segments

支持人员可能会在故障排除呼叫期间要求您指定可以在 TCP 连接的一端排队的数据段的最大字节数。值 0 表示无限的数据段字节数。

注意事项 更改此故障排除选项的设置会影响性能，应仅在支持人员的指导下进行操作。

重组 TCP 数据流

许可证：保护

数据流预处理器收集和重组属于 TCP 会话的服务器到客户端通信数据流和/或客户端到服务器通信数据流的一部分的所有数据包。这允许规则引擎将数据流作为单个已重组实体进行检查，而不是仅检查属于指定数据流的一部分的个别数据包。

有关详细信息，请参阅：

- 第 17-24 页上的了解基于数据流的攻击
- 第 17-24 页上的选择数据流重组选项

了解基于数据流的攻击

许可证：保护

数据流重组允许规则引擎识别基于数据流的攻击，在检查个别数据包时它可能无法检测此类攻击。您可以根据网络需要指定规则引擎重组哪些通信数据流。例如，在监控网络服务器上的流量时，您可能只希望检查客户端流量，因为您不太可能从自己的网络服务器接收到恶意流量。

选择数据流重组选项

许可证：保护

在每个 TCP 策略中，您可以指定用于识别要重组的数据流预处理器流量的端口的逗号分隔列表。启用自适应配置文件后，您还可以列出用于识别要重组的流量的服务（以替代端口或端口组合的形式）。有关启用和使用自适应配置文件的详细信息，请参阅第 18-1 页上的在被动部署中调整预处理。

您可以指定端口和/或服务。您可以为客户端端口和/或服务器端口的任意组合指定单独的端口列表。您还可以为客户端服务和/或服务器服务指定单独的服务列表。例如，假设您要重组以下内容：

- 来自客户端的 SMTP（端口 25）流量
- FTP 服务器响应（端口 21）
- 两个方向的 telnet（端口 23）流量

您可以配置以下内容：

- 对于客户端端口，指定 `23 和 25`
- 对于服务器端口，指定 `21 和 23`

或者，您可以配置以下内容：

- 对于客户端端口，指定 `25`
- 对于服务器端口，指定 `21`
- 对于客户端端口和服务器端口，指定 `23`

此外，请参考以下示例，该示例将端口和服务进行组合，并在启用自适应配置文件后有效：

- 对于客户端端口，指定 `23`
- 对于客户端服务，指定 `smtp`
- 对于服务器端口，指定 `21`
- 对于服务器服务，指定 `telnet`

虽然您也可以指定 `all` 作为参数来为所有端口提供重组，但是思科**不**建议将端口设置为 `all`，因为这样做可能会不必要地增加此预处理器检查的流量并降低性能。

TCP 重组自动透明地包括添加到其他预处理器的端口。但是，如果明确向已添加到其他预处理器配置的 TCP 重组列表中添加端口，则会正常处理这些附加端口。这包括下列预处理器的端口列表：

- FTP/Telnet （服务器级 FTP）
- DCE/RPC
- HTTP Inspect
- SMTP
- 会话初始协议
- POP

- IMAP
- SSL

对端口求反（例如，!77）可通过防止 TCP 数据流预处理器处理该端口的流量来提高性能。

请注意，重组其他流量类型 （客户端和/或服务器）会增加资源需求。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

对客户端端口执行数据流重组

根据连接的客户端的端口启用数据流重组。换句话说，它对目标为网络服务器、邮件服务器或通常由 $HOME_NET 中指定的 IP 地址定义的其他 IP 地址的数据流进行重组。如果您预计客户端会发出恶意流量，请使用此选项。

对客户端服务执行数据流重组

根据连接的客户端的服务启用数据流重组。如果您预计客户端会发出恶意流量，请使用此选项。

此功能需要保护和可控性许可证。

对服务器端口执行数据流重组

根据连接的服务器端的端口启用数据流重组。换句话说，它对从网络服务器、邮件服务器或通常由 $EXTERNAL_NET 中指定的 IP 地址定义的其他 IP 地址发出的数据流进行重组。当您要监控服务器端攻击时，请使用此选项。您可以通过不指定端口来禁用此选项。

对服务器服务执行数据流重组

根据连接的服务器端的服务启用数据流重组。当您要监控服务器端攻击时，请使用此选项。您可以通过不指定服务来禁用此选项。

此功能需要保护和可控性许可证。

对客户端端口和服务器端口执行数据流重组

根据连接的客户端和服务器端的端口启用数据流重组。如果您预计相同端口的恶意流量在客户端和服务器之间可能以任一方向传播，请使用此选项。您可以通过不指定端口来禁用此选项。

对客户端服务和服务器服务执行数据流重组

根据连接的客户端和服务器端的服务启用数据流重组。如果您预计相同服务的恶意流量在客户端和服务器之间可能以任一方向传播，请使用此选项。可以通过不指定服务来禁用此选项。

此功能需要保护和可控性许可证。

配置 TCP 数据流预处理

许可证：保护

您可以配置 TCP 数据流预处理（包括 TCP 策略）。有关 TCP 数据流预处理器配置选项的详细信息，请参阅第 17-20 页上的选择 TCP 策略选项。

要配置数据流预处理器以跟踪 TCP 会话，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Edit Policy 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否已启用 Transport/Network Layer Preprocessors 中的 **TCP Stream Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 TCP Stream Configuration 页面。页面底部的消息标识包含配置的策略层。有关详细信息，请参阅第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　或者，修改 Global Settings 下的 **Packet Type Performance Boost**。有关详细信息，请参阅第 17-19 页上的选择 TCP 全局选项。

步骤 10　此时您有两种选择：

- 添加新的基于目标的策略。点击页面左侧 **Hosts** 旁边的添加图标 ( )。系统将显示 Add Target 弹出窗口。在 **Host Address** 字段中指定一个或多个 IP 地址，然后点击 **OK**。

  可以指定单个 IP 地址或地址块。您可以创建总共 255 个基于目标的策略 （包括默认策略）。有关在 ASA FirePOWER 模块中使用 IP 地址块的信息，请参阅第 1-3 页上的IP 地址约定。

  请注意，为使基于目标的策略处理流量，您识别的网络必须与由网络分析策略 （其中已配置该基于目标的策略）处理的网络、区域 匹配或者是其子集。有关详细信息，请参阅第 13-2 页上的利用网络分析策略自定义预处理。

  新条目将出现在页面左侧的目标列表中，突出显示以表明其已被选定；Configuration 部分会进行更新，以反映所添加的策略的当前配置。

- 修改现有基于目标的策略的设置。点击您在页面左侧 **Hosts** 中添加的策略的配置地址，或者点击 **default**。

  所选项目将会突出显示，并且 Configuration 部分会进行更新以显示所选策略的当前配置。要删除现有的基于目标的策略，请点击要删除的策略旁边的删除图标 ( )。

步骤 11　或者，修改 Configuration 中的任何 TCP 策略选项。

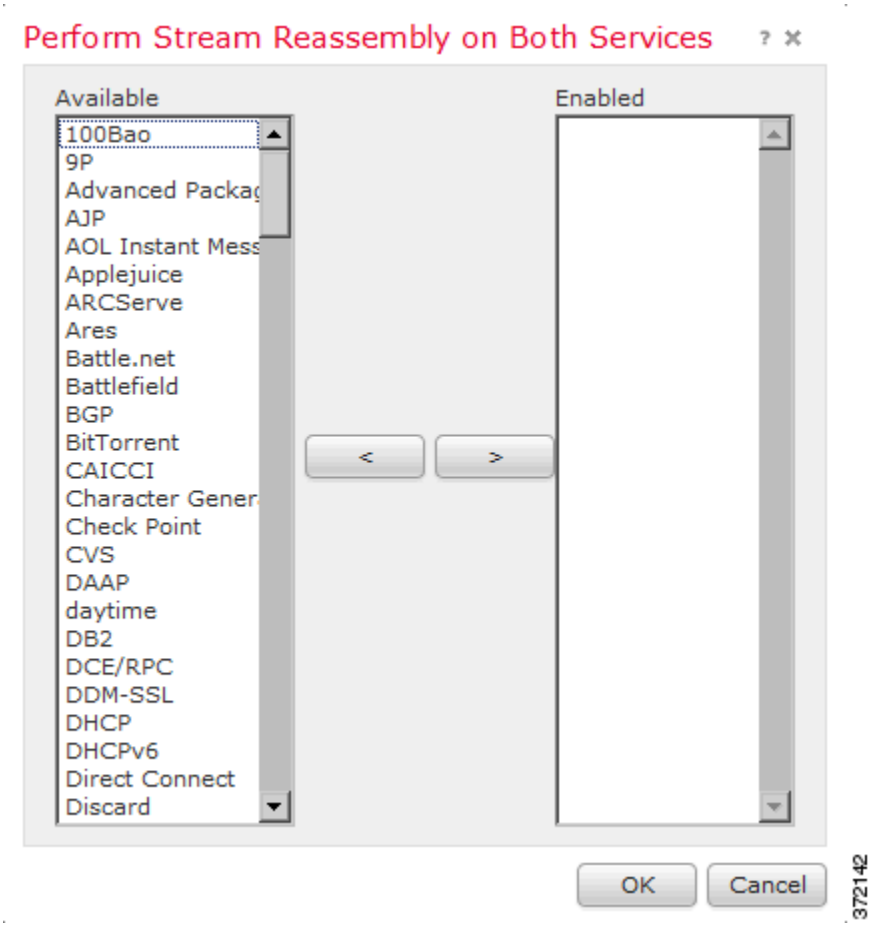
有关根据客户端服务和/或服务器服务修改数据流重组的设置的特定说明，请转至步骤 12；否则，转至步骤 15。

有关详细信息，请参阅第 17-20 页上的选择 TCP 策略选项和第 17-24 页上的选择数据流重组选项。

步骤 12　要根据客户端服务和/或服务器服务修改数据流重组的设置，请在要修改的字段内点击，或者点击要修改的该字段旁边的 **Edit**。

将会出现所选字段的弹出窗口。

例如，下图显示 Perform Stream Reassembly on Both Services 弹出窗口。



请注意，您可以启用自适应配置文件，以根据在网络上发现的服务监控要重组的数据流预处理器的流量。有关详细信息，请参阅第 18-1 页上的在被动部署中调整预处理。

步骤 13　您有两种选择：

- 要添加要监控的服务，请从左侧的 **Available** 列表中选择一个或多个服务，然后点击右箭头 (**>**) 按钮。
- 要删除服务，请从右侧的 **Enabled** 列表中选择要删除的服务，然后点击左箭头 (**<**) 按钮。

按住 Ctrl 或 Shift 键的同时点击可选择多个服务检测器。您也可以点击并拖动以选择多个相邻服务检测器。

步骤 14　点击 **OK** 以添加所选的项目。

系统将显示 TCP Stream Configuration 页面并更新服务。

步骤 15　或者，展开 **Troubleshooting Options** 并仅在支持人员要求的情况下才修改任一 TCP 数据流预处理策略设置。有关详细信息，请参阅第 17-20 页上的选择 TCP 策略选项。

步骤 16　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

使用 UDP 数据流预处理

许可证：保护

当规则引擎使用以下任何参数根据包含 `flow` 关键字（请参阅第 23-46 页上的将规则应用于 TCP 或 UDP 客户端或服务器流量）的 UDP 规则处理数据包时，会发生 UDP 数据流预处理：

- 成熟市场
- `To Client`
- `From Client`
- `To Server`
- `From Server`

UDP 是一个无连接协议，并不提供在两个终端之间建立通信信道、交换数据和关闭该信道的方法。在*会话*方面通常未考虑 UDP 数据流。但是，数据流预处理器使用封装 IP 数据报报头中的源和目标 IP 地址字段及 UDP 报头中的端口字段来确定流动方向并识别会话。当出现下列情况时，会话将会结束：超过可配置的计时器时；或者，任一终端收到表明另一个终端不可达或所请求的服务不可用。

请注意，系统不生成与 UDP 数据流预处理相关的事件；但是，您可以启用相关数据包解码器规则来检测 UDP 协议报头异常。有关数据包解码器生成的事件的信息，请参阅第 17-14 页上的了解数据包解码。

配置 UDP 数据流预处理

许可证：保护

您可以配置 UDP 数据流预处理。

要配置数据流预处理器以跟踪 UDP 会话，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要编辑的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Edit Policy 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否已启用 Transport/Network Layer Preprocessors 中的 **UDP Stream Configuration**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 UDP Stream Configuration 页面。页面底部的消息标识包含配置的策略层。有关详细信息，请参阅第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　或者，配置**超时**值以指定预处理器在状态表中保留非活动数据流的秒数 （1 至 86400）。如果在指定时间内看不到其他数据报，预处理器会从状态表中删除数据流。

步骤 10　或者，选择 **Packet Type Performance Boost** 以忽略已启用的规则中未指定的所有端口和应用协议的 UDP 流量，但在源端口和目标端口均设置为 `any` 的 UDP 规则具有 `flow` 或 `flowbits` 选项时除外。这种性能改进可能会导致未能检测出某些攻击。

步骤 11　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

在被动部署中调整预处理

通常，系统使用网络分析策略中的静态设置预处理和分析流量。然而，通过自适应配置文件功能，系统可适应网络流量，只需将流量与主机信息相关联，相应地处理流量。

当主机接收流量时，主机上运行的操作系统重组 IP 片段。重组所用顺序取决于操作系统。与之类似，每个操作系统都可能以不同方式执行 TCP，因此 TCP 数据流重组方式也有不同。如果预处理器重组数据时所用格式与目标主机操作系统所用格式不同，该系统在接受主机端重组数据时有可能错过可能是恶意的内容。

提示 在被动部署中，思科建议您配置自适应配置文件。在内联部署中，思科建议您在启用 **Normalize TCP Payload** 选项的情况下配置内联规范化预处理程序。有关详细信息，请参阅第 17-5 页上的规范化内联流量。

有关使用自适应配置文件改善数据包片段和 TCP 数据流重组的详细信息，请参阅：

了解自适应配置文件

许可证：保护

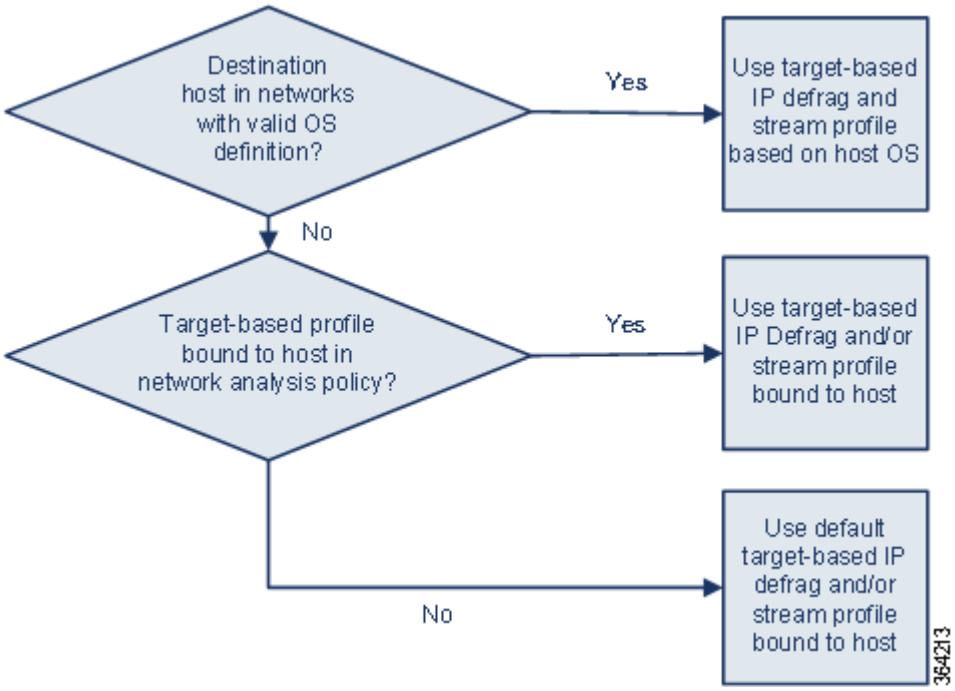
借助于自适应配置文件，可启用最适合 IP 分片重组和 TCP 数据流预处理的操作系统配置文件。有关网络分析策略中受自适应配置文件这影响的各方面的详细信息，请参阅第 17-10 页上的对 IP 数据包进行分片重组和第 17-18 页上的使用 TCP 数据流预处理。

通过预处理器使用自适应配置文件

许可证：保护

自适应配置文件有助于以与目标主机上操作系统相同的方式对 IP 数据包进行分片重组并重组数据流。然后入侵规则引擎使用与目标主机所用的相同格式分析数据。

自适应配置文件可根据目标主机的主机配置文件中的操作系统切换到适当的操作系统配置文件，如下图所示。



例如，您为 10.6.0.0/16 子网配置自适应配置文件，并将默认 IP 分片重组基于目标的策略设置为 Linux。配置该设置的 ASA FirePOWER 模块有一个包括 10.6.0.0/16 子网的。

当设备检测到来自主机 A （未连至 10.6.0.0/16 子网）的流量时，它使用基于 Linux 目标的策略重组 IP 片段。然而，当它检测到来自主机 B （在 10.6.0.0/16 子网中）的流量时，将检索主机 B 的操作系统数据，在网络映射中，主机 B 运行 Microsoft Windows XP Professional。该系统使用基于 Windows 目标的配置文件对指定给主机 B 的流量进行 IP 分片重组。

有关 IP 分片重组预处理器的信息，请参阅第 17-10 页上的对 IP 数据包进行分片重组。有关流量预处理器的信息，请参阅第 17-18 页上的使用 TCP 数据流预处理。

配置自适应配置文件

许可证：保护

要使用主机信息来确定哪些基于目标的配置文件可用于 IP 分片重组和 TCP 数据流预处理，您可配置自适应配置文件。

在配置自适应配置文件时，您需要将自适应配置文件设置绑定到一个特定网络或多个网络。要成功使用自适应配置文件，该网络必须处于设备监测的区段中。

您可以指明在网络中的哪些主机上应使用自适应配置文件处理流量，只需用与访问控制策略的默认入侵策略相链接的变量集中配置的所需值指定 IP 地址、地址块或网络变量。有关详情，请参见第 13-1 页上的为访问控制设置默认入侵策略。

您可以单独或以任意组合方式使用此类寻址方法，作为 IP 地址、地址块或由逗号分隔的变量列表，如下列实例所示：

```
192.168.1.101, 192.168.4.0/24, $ HOME_NET
```

有关指定地址块的详细信息，请参阅第 1-3 页上的 IP 地址约定。

提示 通过使用带有任意值的变量或指定 `0.0.0.0/0` 作为网络值，您可以将自适应配置文件应用于网络中的所有主机。

要配置自适应配置文件，请执行以下操作：

步骤 1 选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2 点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3 选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4 点击 **Detection Enhancement Settings** 旁的编辑图标 ( )。

系统将显示 Detection Enhancement Settings 弹出窗口。

步骤 5 选择 **Adaptive Profiles - Enabled** 启用自适应配置文件。

步骤 6 或者，在 **Adaptive Profiles - Attribute Update Interval** 字段中，键入同步数据持续的分钟数。

注 增大此选项的值可提升大型网络的性能。

步骤 7 在 **Adaptive Profiles - Networks** 字段中，键入特定 IP 地址、地址块、变量或者包括由逗号隔开的任何此类寻址方法的列表，以标识网络中您要使用自适应配置文件的任何主机。

有关配置变量的信息，请参阅第 2-13 页上的使用变量集。

步骤 8 点击 **OK** 保留设置。

入侵策略使用入门

*入侵策略*是已定义的几组入侵检测和防护配置，用于检查流量是否存在安全违规，以及在内联部署中阻止或修改恶意流量。入侵策略供访问控制策略调用，是系统在允许流量到达目标之前的最后一道防线。

思科通过 ASA FirePOWER 模块提供多种入侵策略。使用系统提供的策略，您可以利用思科漏洞研究团队 (VRT) 的经验。对于这些策略，VRT 设置入侵和预处理器规则状态（启用或禁用），并提供其他高级设置的初始配置。启用的规则导致系统为匹配规则的流量生成入侵事件（或阻止该流量）。禁用规则将停止该规则的处理。

提示 系统提供的入侵和网络分析策略具有类似的名称，但包含不同的配置。例如，平衡安全性和连接网络分析策略和平衡安全性和连接入侵策略配合工作并可以在入侵规则更新中同时更新。但是，网络分析策略管理的主要是预处理选项，而入侵策略管理的主要是入侵规则。第 11-1 页上的了解网络分析和入侵策略概述网络分析和入侵策略如何协同工作检查流量，以及使用导航面板、解决冲突和确认更改的基本信息。

如果创建自定义入侵策略，您可以：

- 通过启用和禁用规则，以及撰写和添加您自己的规则来调整检测。
- 配置各种高级设置，例如，外部警告，敏感数据预处理和全局规则阈值。
- 使用分层作为构建块，以有效地管理多个入侵策略。

当定制入侵策略时，特别是在启用和添加规则时，请记住一些入侵规则要求首先以某种方式对流量进行解码或预处理。在入侵策略检查数据包之前，数据包根据网络分析策略中配置对其进行预处理。如果您禁用必需的预处理器，尽管预处理器在网络分析策略用户界面中保持禁用状态，系统还会自动使用其当前设置。

注 由于预处理和入侵检查密切相关，检查每个数据包的网络分析和入侵策略**必须**相互补充。定制预处理（特别是使用多个自定义网络分析策略）是一项**高级**任务。有关详细信息，请参阅第 11-9 页上的自定义策略的限制。

在配置自定义入侵策略后，可以在访问控制配置过程中通过以下方式使用该策略：将入侵策略与一个或多个访问控制规则或访问控制策略的默认操作相关联。这会强制系统在某个允许的流量到达最终目的地之前使用入侵策略检查该流量。与入侵策略共同使用的变量集，用于准确地反映您的家庭和外部网络以及网络上的服务器（如果适当）。有关详细信息，请参阅第 10-1 页上的使用入侵和文件策略控制流量。

本章介绍如何创建简单的自定义入侵策略。本章还包含有关管理入侵策略的基本信息：编辑和比较等。有关详情，请参阅：

创建自定义入侵策略

许可证：保护

当您创建新的入侵策略时，必须为其提供唯一的名称，指定基本策略并指定丢弃行为。

基本策略定义入侵策略的默认设置。修改新策略中的设置会覆盖（但不会更改）基本策略中的该设置。您可以使用系统提供的策略或自定义策略作为您的基本策略。有关详细信息，请参阅第 12-2 页上的了解基本层。

入侵策略的丢包行为或 **Drop when Inline** 设置确定系统如何处理丢弃规则（规则状态设置为 Drop and Generate Events 的入侵或预处理器规则）和影响流量的其他入侵策略配置。当想要放弃或替换恶意数据包时，应该在内联部署中启用丢弃行为。请注意，在被动部署中，系统无法影响流量传输，无论丢包行为如何设置。有关详细信息，请参阅第 19-5 页上的设置内联部署中的丢弃行为。

要创建入侵策略，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

提示　您也可以从另一个 ASA FirePOWER 模块导出策略；请参阅第 B-1 页上的导入和导出配置。

步骤 2　点击 **Create Policy**。

如果您在另一策略中有未保存的更改，当系统提示您返回 Intrusion Policy 页面时请点击 **Cancel**。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Create Intrusion Policy 弹出窗口。

步骤 3　在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

步骤 4　指定初始**基本策略**。

您可以使用系统提供的策略或自定义策略作为您的基本策略。

注意事项　请**勿**使用 `Experimental Policy 1`，除非思科代表指示这样做。思科使用该策略进行测试。

步骤 5　设置内联部署中的系统丢弃行为：

- 要允许入侵策略影响流量并生成事件，请启用 **Drop when Inline**。
- 要阻止入侵策略影响流量但允许生成事件，请禁用 **Drop when Inline**。

步骤 6　创建策略：

- 点击 **Create Policy** 创建新策略并返回到 Intrusion Policy 页面。新策略的设置与其基本策略相同。
- 点击 **Create and Edit Policy** 创建策略并在高级入侵策略编辑器中打开该策略进行编辑；请参阅第 19-4 页上的编辑入侵策略。

管理入侵策略

许可证：保护

在 Intrusion Policy 页面 (**Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**) 上，可以查看当前自定义入侵策略以及以下信息：

- 最近一次修改策略的时间和日期（采用当地时间）以及。
- 是否已启用 **Drop when Inline** 设置，该设置允许您在内联部署中丢弃和修改流量
- 哪些访问控制策略使用入侵策略来检查流量
- 策略是否有未保存的更改

Intrusion Policy 页面上的选项允许您采取下表中的措施。

表 19-1　　入侵策略管理操作

要.....	您可以.....	请参阅.....
创建新的入侵策略	点击 **Create Policy**。	第 19-2 页上的创建自定义入侵策略
编辑现有入侵策略	点击编辑图标 ( )。	第 19-4 页上的编辑入侵策略
重新应用入侵策略	点击应用图标 ( )。	第 19-7 页上的应用入侵策略
导出入侵策略以便导入到另一个 ASA FirePOWER 模块	点击导出图标 ( )。	第 B-1 页上的导出配置
查看在入侵策略中列出当前配置设置的 PDF 报告	点击报告图标 ( )。	第 19-7 页上的生成当前入侵设置的报告
比较两个入侵策略或同一策略两个版本的设置	点击 **Compare Policies**。	第 19-8 页上的比较两个入侵策略或版本
删除入侵策略	请点击删除图标 ( ) 并确认要删除策略。如果访问控制策略引用了某条入侵策略，则无法删除该入侵策略。	

编辑入侵策略

许可证：保护

当创建新的入侵策略时，它具有与其基本策略相同的入侵规则和高级设置。下表说明了编辑入侵策略时最常见的操作：

表 19-2　入侵策略编辑操作

要.....	您可以.....	请参阅.....
指定内联部署中的丢弃行为	选择或清除 Policy Information 页面上的 **Drop when Inline** 复选框。	第 19-5 页上的设置内联部署中的丢弃行为
更改基本策略	从 Policy Information 页面上的 **Base Policy** 下拉列表中选择基本策略。	第 12-3 页上的更改基本策略
查看基本策略中的设置	在 Policy Information 页面上点击 **Manage Base Policy**。	第 12-2 页上的了解基本层
显示或配置入侵规则	在 Policy Information 页面上点击 **Manage Rules**。	第 20-2 页上的查看入侵策略中的规则
按当前规则状态显示经过滤的入侵规则视图，或者，配置这些规则	在 Policy Information 页面上，点击 **Manage Rules** 下方设置成 Generate Events 或 Drop and Generate Events 的规则数量旁边的 **View**。	第 20-9 页上的过滤入侵策略中的规则
启用、禁用或编辑高级设置	在导航面板中点击 **Advanced Settings**	第 19-6 页上的在入侵策略中配置高级设置
管理策略层	在导航面板中点击 **Policy Layers**。	第 12-1 页上的在网络分析或入侵策略中使用层

当定制入侵策略时，特别是在启用和添加规则时，请记住某些入侵规则要求首先以某种方式对流量进行解码或预处理。在入侵策略检查数据包之前，数据包根据网络分析策略中配置对其进行预处理。如果您禁用必需的预处理器，尽管预处理器在网络分析策略用户界面中保持禁用状态，系统还会自动使用其当前设置。

注　由于预处理和入侵检查密切相关，检查每个数据包的网络分析和入侵策略**必须**相互补充。定制预处理（特别是使用多个自定义网络分析策略）是一项**高级**任务。有关详细信息，请参阅第 11-9 页上的自定义策略的限制。

系统为每个用户缓存。在编辑入侵策略时，如果您选择任何菜单或指向另一页的其他路径，即使您离开此页，更改也会保留在系统缓存中。除了可执行上表中的操作，第 11-1 页上的了解网络分析和入侵策略还提供了有关解决冲突确认更改的信息

要编辑入侵策略，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击想要配置的入侵策略旁边的编辑图标 ( )。

系统将显示入侵策略编辑器，焦点位于 Policy Information 页面上，并且左侧带导航面板。

步骤 3　编辑您的策略。采取上面总结的任何操作。

步骤 4　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

设置内联部署中的丢弃行为

许可证：保护

在内联部署中，入侵策略可以阻止和修改流量：

- *丢弃规则*可以丢弃匹配的数据包和生成入侵事件。要配置入侵或预处理器丢弃规则，请将其状态设置为 Drop and Generate Events；请参阅第 20-17 页上的设置规则状态。
- 入侵规则可使用 `replace` 关键字来替换恶意内容；请参阅第 23-27 页上的替换内联部署中的内容。

要使入侵规则影响流量，必须正确配置丢弃规则和替换内容的规则，并正确部署系统内联。最后，必须启用入侵策略的*丢弃行为*或 **Drop when Inline** 设置。

注　要阻止恶意软件文件通过 FTP 传输，不仅必须正确配置基于网络的高级恶意软件防护 (AMP)，还必须在访问控制策略的默认入侵策略中启用 **Drop when Inline**。要确定或更改默认入侵策略，请参阅第 13-1 页上的为访问控制设置默认入侵策略。

如果想要评估配置如何在内联部署中起作用，而实际上不会影响流量，则可以禁用丢弃行为。在这种情况下，系统生成入侵事件，但不会丢弃触发丢弃规则的数据包。当对结果满意时，可以启用丢弃行为。

请注意，在轻触模式下的被动部署，无论丢包行为如何设置，系统都无法影响流量传输。换句话说，在被动部署中，设置为 Drop and Generate Events 的规则与设置为 Generate Events 的规则行为相同 - 系统生成入侵事件，但不会丢弃数据包。

当您查看入侵事件时，工作流可以包括*内联结果*，以指示流量是否确实已丢弃，或者它是否仅仅应该已丢失。当数据包匹配丢弃规则时，内联结果如下：

- `Dropped`，适用于已启用丢弃行为的正确配置的内联部署所丢弃的数据包
- `Would have dropped`，适用于因设备以被动方式部署或因禁用丢弃行为而未被丢弃的数据包。 请注意，系统修剪时，无论如何部署，对于检测到的数据包，内联结果始终为 `Would have dropped`。

要设置内联部署中的入侵策略的丢弃行为：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

系统将显示 Policy Information 页面。

步骤 3　设置策略的丢弃行为：

- 要允许入侵规则影响流量并生成事件，请启用 **Drop when Inline**。
- 要阻止入侵规则影响流量但仍旧生成事件，请禁用 **Drop when Inline**。

步骤 4　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

在入侵策略中配置高级设置

许可证：保护

配置入侵策略的*高级设置*需要特定专业知识。入侵策略的基本策略决定了默认情况下启用哪些高级设置及各自的默认配置。

当在入侵策略的导航面板中选择 **Advanced Settings** 时，策略将按类型列出其高级设置。在 Advanced Settings 页面中，您可以启用或禁用入侵策略中的高级设置，以及访问高级设置配置页面。

高级设置必须在启用后才能配置。当您启用高级设置后，导航面板中 **Advanced Settings** 链接下方将会显示指向高级设置配置页面的子链接， Advanced Settings 页面高级设置旁边将会出现指向配置页面的 **Edit** 链接。

提示 要将高级设置的配置恢复为基本策略中的设置，请点击该高级设置配置页面上的 **Revert to Defaults**。出现提示时，请确认您要恢复。

当禁用高级设置时，子链接和 **Edit** 链接将不显示，但会保留您的配置。请注意，某些入侵策略配置（敏感数据规则、入侵规则的 SNMP 警报）需要启用和正确配置高级设置。您无法保存通过这种方式误配置的入侵策略；请参阅第 11-12 页上的解决冲突和提交策略更改。

修改高级设置的配置要求了解正在进行的修改及其对网络的潜在影响。以下部分提供指向每项高级设置具体配置详细信息的链接。

具体威胁检测

敏感数据预处理器检测敏感信息，例如 ASCII 文本格式的信用卡号和社会保障号。有关配置此预处理器的信息，请参阅第 21-17 页上的检测敏感数据。

请注意，在网络分析策略中配置用于检测具体威胁（后洞攻击、若干端口扫描类型和尝试通过大量流量淹没网络的基于速率的攻击）的其他预处理器。有关详细信息，请参阅第 21-1 页上的检测特定威胁。

入侵规则阈值

全局规则阈值允许使用阈值来限制系统记录和显示的入侵事件数量，从而可以防止您的系统由于无法应付大量事件而崩溃。有关详细信息，请参阅第 22-1 页上的全局限制入侵事件记录。

外部响应

除了用户界面中的各种入侵事件视图之外，您还可以启用将日志记录到系统日志工具或者将事件数据发送到 SNMP 陷阱服务器。根据策略，您可以指定入侵事件通知限制，设置发送到外部日志记录工具的入侵事件通知，以及配置对入侵事件的外部响应。有关详情，请参阅：

- 第 28-3 页上的配置 SNMP 响应
- 第 28-5 页上的配置系统日志响应

应用入侵策略

许可证：保护

向使用访问控制 （请参阅第 4-10 页上的应用访问控制策略）的应用入侵策略后，可以随时重新应用此入侵策略。这样就可以在监控下的网络上实施入侵策略更改，而无需重新应用访问控制策略。重新应用时，还可以查看比较报告，检查自从最后一次应用此入侵策略之后所做的更改。

重新应用入侵策略时,请注意以下事项：

- 可以安排定期重复执行入侵策略重新应用任务；请参阅第 31-4 页上的自动应用入侵策略。
- 导入规则更新时，可以在导入完成后自动应用入侵策略。如果不启用此选项，就必须手动重新应用被规则更新更改的策略。有关详情，请参见第 35-8 页上的导入规则更新和本地规则文件。

要重新应用入侵策略，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的应用图标 ( )。

系统将显示 Reapply Intrusion Policy 窗口。

步骤 3　点击 **Reapply**。

策略重新应用成功。可以使用任务队列监控应用的状态 (**Monitoring > ASA FirePOWER Monitoring > Task Status**)。有关详情，请参见第 C-1 页上的查看任务队列。

生成当前入侵设置的报告

许可证：保护

入侵策略报告是在特定时间点对策略配置的记录。该系统将基本策略中的设置与策略层的设置组合，不区分源自基本策略或策略层的设置。

您可以将包括以下信息的报告用于审计目的或检查当前配置。

表 19-3　　入侵策略报告部分

部分	说明
策略信息	提供入侵策略的名称和说明、上次修改策略的用户的名称以及上次修改策略的日期和时间。还指明在内联部署中丢弃数据是处于启用还是禁用状态，当前规则更新版本，以及基本策略是否锁定为当前规则更新。
高级设置	列出所有已启用入侵策略高级设置及其配置。
规则	提供所有已启用规则及其操作的列表。

还可以生成比较两个入侵策略或同一策略的两个版本的比较报告。有关详细信息，请参阅第 19-8 页上的比较两个入侵策略或版本。

要查看入侵策略报告，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击您想要生成报告的入侵策略旁边的报告图标 ( )。请记住，应先确认任何潜在更改再生成入侵策略报告；只有确认的报告才会显示在报告中。

系统生成入侵策略报告。系统会提示您将报告保存到计算机上。

比较两个入侵策略或版本

许可证：保护

如要查看策略更改是否符合贵组织的标准或优化系统性能，可以检查这两个入侵策略之间的区别。对于可以访问的安全策略，可以比较任意两个入侵策略或同一个入侵策略的两个版本。比较之后，可以生成 PDF 报告，记录两个策略或两个版本的策略之间的区别。

有两个可以用来比较入侵策略的工具：

- 此比较视图只并排显示两个入侵策略或入侵策略版本之间的差异；比较视图左右两侧标题栏中显示每个策略的名称。

  您可以使用该工具在用户界面上查看和浏览两个策略版本，其中突出显示其差异。

- 比较报告只以类似于入侵策略报告的形式创建关于两个入侵策略或两个版本之间区别的记录，但采用的是 PDF 格式。

  可以将其用于保存、复制、打印和共享策略比较，以备进一步检查。

如需了解和使用入侵策略比较工具的更多信息，请参阅：

- 第 19-8 页上的使用入侵策略比较视图
- 第 19-9 页上的使用入侵策略比较报告

使用入侵策略比较视图

许可证：保护

此比较视图并排显示两个入侵策略或其两个版本，比较视图左右两侧标题栏中将按照名称标识每个策略或每个版本。最近一次修改的时间和执行最后一次修改的用户显示在策略名称右侧。请注意，Intrusion Policy 页面用本地时间显示最后一次修改策略的时间，但是入侵策略报告则用 UTC 时间列出此修改时间。两个入侵策略或两个版本之间的区别会突出显示出来：

- 蓝色表示两个策略或两个版本中此突出显示的设置不同。并且用红色文本注明其不同之处。
- 绿色表示此突出显示的设置在一个策略或一个版本中出现了，而在另一个策略或版本中却没有出现。

可以执行下表中的任何操作。

表 19-4　入侵策略比较视图操作

要.....	您可以.....
逐一浏览更改	点击标题栏上方的 **Previous** 或 **Next**。 在左右两侧之间以双箭头图标 (⇔) 为中心移动，**Difference** 数字调整为识别您正在查看哪个差异。
生成新的入侵策略比较视图	点击 **New Comparison**。 系统将显示 **Select Comparison** 窗口。有关详情，请参见使用入侵策略比较报告。
生成入侵策略比较报告	点击 **Comparison Report**。 策略比较报告创建仅列出两个策略或策略修订版之间的差异的 PDF 文档。

使用入侵策略比较报告

许可证：保护

入侵策略比较报告是关于入侵策略比较视图标识的两个入侵策略或同一入侵策略两个版本之间全部区别的一个 PDF 格式记录。可以使用此报告进一步检查两个入侵策略配置之间的区别以及保存和分发其比较结果。

对于可以访问的任何入侵策略，都可以从此比较视图生成入侵策略比较报告。请记住，应先确认任何潜在更改再生成入侵策略报告；只有确认的报告才会显示在报告中。

入侵策略比较报告的格式与入侵策略报告相同，但有一个区别：入侵策略报告包含入侵策略中的所有设置，而入侵策略比较报告则只包含策略之间存在区别的那些设置。

根据配置，入侵策略报告可能包含表入侵策略报告部分所述的一个或多个分区。

提示　您可以使用类似的步骤比较 访问控制、网络分析、文件或系统策略。

要比较两个入侵策略或同一策略的两个版本，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击 **Compare Policies**。

系统将显示 Select Comparison 窗口。

步骤 3　从 **Compare Against** 下拉列表中选择要进行比较的类型：

- 要比较两个不同的策略，请选择 **Other Policy**。
- 要比较同一策略的两个修订版，请选择 **Other Revision**。

请记住，应先确认所有更改，再生成入侵策略报告；只有确认的报告才会显示在报告中。

步骤 4　根据您选择的比较类型，有以下选项可供选择：

- 如果您比较两个不同的策略，请从 **Policy A** 和 **Policy B** 下拉列表中选择要比较的策略。
- 如果您比较同一策略的两个修订版，请从 **Policy** 下拉列表中选择该策略，然后从 **Revision A** 和 **Revision B** 下拉列表中选择要比较的修订版。

步骤 5　点击 **OK** 显示入侵策略比较视图。

系统将显示比较视图。

步骤 6　点击 **Comparison Report**，生成入侵策略比较报告。

步骤 7　系统将显示入侵策略报告。系统会提示您将报告保存到计算机上。

使用规则调整入侵策略

可以使用入侵策略中的 Rules 页面为共享对象规则、标准文本规则和预处理器规则配置规则状态和其他设置。

将规则的状态设置为 Generate Events 或 Drop and Generate Events 即可启用该规则。启用规则后，系统将对与该规则匹配的流量生成事件。禁用规则将停止该规则的处理。或者，可以设置入侵策略，以便在内联部署中设置为 Drop and Generate Events 的规则对匹配的流量生成事件并丢弃该流量。有关详情，请参见第 19-5 页上的设置内联部署中的丢弃行为。在被动部署中，设置为 Drop and Generate Events 的规则仅对匹配的流量生成事件。

您可以对规则进行过滤来显示规则的一个子集，这样就能选择要更改其规则状态或规则设置的确切规则集。

当入侵规则或规则参数要求预处理器处于禁用状态时，系统会自动在其当前配置下使用该预处理器，即使其在网络分析策略的 用户界面中保持禁用也如此。有关详细信息，请参阅第 11-9 页上的自定义策略的限制。

有关详细信息，请参阅：

- 第 20-2 页上的了解入侵防御规则类型说明可在入侵策略中查看和配置的入侵规则和预处理器规则。
- 第 20-2 页上的查看入侵策略中的规则说明如何在 Rules 页面中更改规则的顺序，解释该页面中的图标，并着重介绍规则详细信息。
- 第 20-9 页上的过滤入侵策略中的规则说明如何使用规则过滤器来查找要对其应用规则设置的规则。
- 第 20-17 页上的设置规则状态说明如何从 Rules 页面启用和禁用规则。
- 第 20-19 页上的按策略过滤入侵事件通知介绍如何为特定规则设置事件过滤阈值以及如何对特定规则设置抑制。
- 第 20-25 页上的添加动态规则状态介绍在匹配的流量中检测到速率异常时如何设置动态触发的规则状态。
- 第 20-28 页上的添加 SNMP 警报说明如何将 SNMP 警报与特定规则相关联。
- 第 20-29 页上的添加规则注释说明如何向入侵策略中的规则添加注释。

了解入侵防御规则类型

许可证：保护

入侵策略包含两种类型的规则：入侵规则和预处理器规则。

入侵规则是一组指定的关键字和参数，用于检测企图利用网络漏洞的行为；入侵规则通过分析网络流量来检查其是否符合规则中的条件。系统将数据包与每条规则中指定的条件进行比较，如果数据包数据符合规则中指定的所有条件，则触发此规则。系统包含两种由思科漏洞研究团队 (VRT) 创建的入侵规则：其一为共享对象规则，已编写好且不能修改（源端口、目标端口和 IP 地址等规则头信息除外）；其二为标准文本规则，可以修改并另存为新的自定义规则实例。

系统中还包含预处理器规则，即与预处理器和数据包解码器检测选项相关联的规则。预处理器规则不能复制或编辑。大多数预处理器规则默认禁用，如果需要系统为预处理器规则生成事件并在内联部署中丢弃违规的数据包，必须启用这些规则（即设置为 Generate Events 或 Drop and Generate Events）。

VRT 为系统随附的每个默认入侵策略确定思科共享对象规则、标准文本规则和预处理器规则的默认规则状态。

下表描述 ASA FirePOWER 模块随附的各类型的规则。

表 20-1　规则类型

类型	说明
共享对象规则	思科漏洞研究团队 (VRT) 创建的入侵规则，以 C 源代码编译的二进制模块方式提供。您可以使用共享对象规则，以标准文本规则无法采取的方式来检测攻击。不能修改共享对象规则中的规则关键字和参数；限制修改规则中使用的变量，限制修改源端口、目标端口和 IP 地址等方面的信息，也限制将新的规则实例另存为自定义共享对象规则。共享对象规则的 GID （生成器 ID）为 3。有关详情，请参见第 23-95 页上的修改现有规则。
标准文本规则	由 VRT 创建、复制并另存为新的自定义规则的入侵规则、使用规则编辑器创建的入侵规则或导入为本地规则（在本地设备上创建和导入）的入侵规则。不能修改 VRT 创建的标准规则中的规则关键字和参数；限制修改规则中使用的变量，限制修改源端口、目标端口和 IP 地址等方面的信息，也限制将新的规则实例另存为自定义标准文本规则。有关详细信息，请参阅第 23-95 页上的修改现有规则、第 23-1 页上的了解和编写入侵规则和第 35-12 页上的导入本地规则文件。VRT 创建的标准文本规则的 GID（生成器 ID）为 1。使用规则编辑器创建的或导入为本地规则的自定义标准文本规则，其 SID（签名 ID）为 1000000 或更大值。
预处理器规则	与数据包解码器的检测选项关联或与 ASA FirePOWER 模块随附的预处理器之一关联的规则。 .如果需要预处理器规则生成事件，必须启用这些规则。这些规则的 GID （生成器 ID）为解码器或预处理器专用的 GID。

查看入侵策略中的规则

许可证：保护

您可以调整规则在入侵策略中的显示方式，并且可按多个条件将规则排序。也可以显示特定规则的详细信息，以便查看规则设置、规则文档和其他规则详情。

Rules 页面有四个主要的功能区域：

- 过滤功能 - 有关详细信息，请参阅第 20-9 页上的过滤入侵策略中的规则
- 规则属性菜单 - 有关详细信息，请参阅第 20-17 页上的设置规则状态、第 20-19 页上的按策略过滤入侵事件通知、第 20-25 页上的添加动态规则状态、第 20-28 页上的添加 SNMP 警报和第 20-29 页上的添加规则注释

- 规则列表 - 有关详细信息，请参阅Rules 页面列表。
- 规则详细信息 - 有关详细信息，请参阅第 20-4 页上的查看规则详细信息

此外，还可以按不同的条件对规则排序；有关详细信息，请参阅第 20-4 页上的对规则的显示排序。

请注意，用作列标题的图标与用于访问这些配置项的菜单栏中的菜单相对应。例如， Rule State 菜单使用与 Rule State 列相同的图标 ( ) 标记。

下表介绍 Rules 页面中的各列。

表 20-2　　Rules 页面列

标题	说明	有关详细信息，请参阅...
GID	该整数表示规则的生成器 ID (GID)。	第 26-1 页上的查看事件
SID	该整数表示充当规则唯一标识符的 Snort ID (SID)。	第 26-1 页上的查看事件
Message	此规则生成的事件中包含的消息，亦充当该规则的名称。	第 23-11 页上的定义事件消息
	该规则的规则状态，可以是以下三种状态之一： • drop and generate events ( ) • generate events ( ) • disable ( ) 请注意，点击某条规则的规则状态图标即可访问该规则的 Set rule state 对话框。	第 20-17 页上的设置规则状态
	事件过滤器，包括应用于该规则的事件阈值和事件抑制。	第 20-19 页上的按策略过滤入侵事件通知
	该规则的动态规则状态，如果发生指定的速率异常则会生效。	第 20-25 页上的添加动态规则状态
	为规则配置的警报 （当前仅限 SNMP 警报）。	第 20-28 页上的添加 SNMP 警报
	向规则添加的注释。	第 20-29 页上的添加规则注释

也可以使用层下拉列表切换到策略中其他层的 Rules 页面。请注意，除非向策略中添加层，否则下拉列表中列出的唯一可编辑视图是策略的 Rules 页面和最初命名为 `My Changes` 的策略层的 Rules 页面；另请注意，在这些视图其中之一进行更改与在其他视图中进行更改相同。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。该下拉列表中还会列出只读基本策略的 Rules 页面。有关基本策略的详细信息，请参阅第 12-2 页上的了解基本层。

要查看入侵策略中的规则，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在其他策略中有未保存的更改，请点击 **OK** 废弃这些更改并继续操作。有关保存其他策略中未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 Policy Information 页面中的 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

请注意，选择导航面板中的分隔线上方的 **Rules** 会转到相同的规则列表。在此视图中可查看和设置策略中的所有规则属性。

对规则的显示排序

许可证：保护

点击标题或图标可按 Rules 页面中的任意列对规则排序。

请注意，标题或图标上的向上 (▲) 或向下 (▼) 箭头表示目前是按该列的该方向排序。

要对入侵策略中的规则排序，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在其他策略中有未保存的更改，请点击 **OK** 废弃这些更改并继续操作。有关保存其他策略中未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　点击要按其排序的列顶部的标题或图标。

此时将按列标题上显示的箭头所指示的方向依据该列对规则排序。要按相反方向排序，请再次点击标题。排序顺序和箭头都将颠倒过来。

查看规则详细信息

许可证：保护

您可以从 Rule Detail 视图查看规则文档和规则开销。还可以查看和添加特定于规则的功能。

请注意，除非将本地规则映射到漏洞，否则其没有任何开销。

表 20-3　　规则详细信息

项目	说明	有关详细信息，请参阅...
Summary	规则摘要。对基于规则的事件，此行将在规则文档包含摘要信息时显示。	第 26-1 页上的查看事件
Rule State	规则的当前规则状态。也表示已设置规则状态的层。	第 20-17 页上的设置规则状态；第 12-1 页上的在网络分析或入侵策略中使用层

表 20-3　规则详细信息（续）

项目	说明	有关详细信息，请参阅...
Thresholds	当前为此规则设置的阈值，以及用于为该规则添加阈值的工具。	第 20-6 页上的为规则设置阈值
Suppressions	当前为此规则设置的抑制设置，以及用于为该规则添加抑制的工具。	第 20-6 页上的为规则设置抑制
Dynamic State	当前为此规则设置的基于速率的规则状态，以及用于为该规则添加动态规则状态的工具。	第 20-7 页上的为规则设置动态规则状态
Alerts	当前为此规则设置的警报，以及用于为该规则添加警报的工具。当前，仅支持 SNMP 警报。	第 20-8 页上的为规则设置 SNMP 警报
Comments	向此规则添加的注释，以及用于为该规则添加注释的工具。	第 20-8 页上的为规则添加规则注释
Documentation	当前规则的规则文档，由思科漏洞研究团队 (VRT) 提供。	第 26-1 页上的查看事件

要查看规则详细信息，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在其他策略中有未保存的更改，请点击 **OK** 废弃这些更改并继续操作。有关保存其他策略中未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　突出显示要查看其规则详细信息的规则。

步骤 5　点击 **Show details**。

系统将显示 Rule Detail 视图。要重新隐藏详细信息，请点击 **Hide details**。

提示　双击 Rules 视图中的规则也可打开 Rule Detail。

为规则设置阈值

许可证：保护

您可以从 Rule Detail 页面为规则设置单个阈值。添加阈值将覆盖该规则的任何现有阈值。有关阈值的详细信息，请参阅第 20-19 页上的配置事件阈值。

请注意，当键入的值无效时，字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

要在规则详细信息中设置阈值，请执行以下操作：

步骤 1　点击 **Thresholds** 旁边的 **Add**。

系统将显示 Set Threshold 对话框。

步骤 2　从 **Type** 下拉列表中，选择要设置的阈值的类型。

- 选择 **Limit** 以限制为在每个时间段内向指定数量的事件实例发送通知。
- 选择 **Threshold** 以在每个时间段内为指定数量的各事件实例提供通知。
- 选择 **Both** 则在每个时间段内事件实例数达到指定数量后提供一次通知。

步骤 3　从 **Track By** 下拉列表中，选择 **Source**或 **Destination** 以指示希望按源 IP 地址还是目标 IP 地址跟踪事件实例。

步骤 4　在 **Count** 字段中，键入要用作阈值的事件实例数。

步骤 5　在 **Seconds** 字段中，键入一个 0 和 2147483647 之间的数字（以秒为单位）来指定跟踪事件实例的时间段。

步骤 6　点击 **OK**。

系统将添加阈值并在 Event Filtering 列中该规则旁边显示事件过滤器图标 ( )。如果向规则中添加多个事件过滤器，系统将在图标上注明事件过滤器的数量。

为规则设置抑制

许可证：保护

您可以从 Rule Detail 页面为规则设置一个或多个抑制。有关抑制的详细信息，请参阅第 20-23 页上的按入侵策略配置抑制。

请注意，当键入的值无效时，字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

要在规则详细信息中设置抑制，请执行以下操作：

步骤 1　点击 **Suppressions** 旁边的 **Add**。

系统将显示 Add Suppression 对话框。

步骤 2　从 **Suppression Type** 下拉列表中，选择下列选项之一。

- 选择 **Rule** 将完全抑制所选规则的事件。
- 选择 **Source** 将抑制由指定源 IP 地址发出的数据包生成的事件。
- 选择 **Destination** 将抑制由发往指定目标 IP 地址的数据包生成的事件。

步骤 3　如果选定 **Source** 或 **Destination** 作为抑制类型，则会显示 Network 字段。在 **Network** 字段中，输入 IP 地址、地址块或由这些内容组成的任意组合的逗号分隔列表。如果入侵策略与某个访问控制策略的默认操作相关联，则还可以在默认操作变量集中指定或列出网络变量。

有关使用 IPv4 CIDR 和 IPv6 前缀长度地址块的详细信息，请参阅第 1-3 页上的IP 地址约定。

步骤 4　点击 **OK**。

系统将添加抑制条件并在 Event Filtering 列中被抑制的该规则旁边显示事件过滤器图标 ( )。如果向规则中添加多个事件过滤器，图标上的数字表示过滤器的数量。

为规则设置动态规则状态

许可证：保护

您可以从 Rule Detail 页面为规则设置一个或多个动态规则状态。列出的第一个动态规则状态具有最高优先级。请注意，当两个动态规则状态相冲突时，将执行第一个状态的操作。有关动态规则状态的详细信息，请参阅第 20-25 页上的了解动态规则状态。

请注意，当键入的值无效时，字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

要在规则详细信息中设置动态规则状态，请执行以下操作：

步骤 1　点击 **Dynamic State** 旁边的 **Add**。

系统将显示 Add Rate-Based Rule State 对话框。

步骤 2　从 **Track By** 下拉列表中，选择用于指示希望如何跟踪匹配规则的选项。

- 选择 **Source** 将跟踪由特定的一个或一组源地址发出的该规则匹配项的数量。
- 选择 **Destination** 将跟踪发往特定的一个或一组目标地址的该规则匹配项的数量。
- 选择 **Rule** 将跟踪该规则的所有匹配项。

步骤 3　或者，如果将 **Track By** 设置为 **Source** 或 **Destination**，请在 **Network** 字段中输入要跟踪的每台主机的 IP 地址。

有关使用 IPv4 CIDR 和 IPv6 前缀长度表示法的详细信息，请参阅第 1-3 页上的IP 地址约定。

步骤 4　在 **Rate** 旁边，指示每个时间段的规则匹配项数，以设置攻击速率：

- 在 **Count** 字段中，使用 0 到 2147483647 之间的整数指定要用作阈值的规则匹配项数。
- 在 **Seconds** 字段中，使用 0 到 2147483647 之间的整数指定构成会跟踪攻击的时间段的秒数。

步骤 5　从 **New State** 状态下拉列表中，选择满足条件时要采取的新操作。

- 选择 **Generate Events** 将生成事件。
- 选择 **Drop and Generate Events** 将在内联部署中生成事件并丢弃触发该事件的数据包，或在被动部署中生成事件。
- 选择 **Disabled** 将不执行任何操作。

步骤 6　在 **Timeout** 字段中，使用 1 到 2147483647（约为 68 年）之间的整数，键入希望新操作保持有效的秒数。在超时后，规则将恢复到其原始状态。指定 0 可防止新操作超时。

步骤 7　点击 **OK**。

系统将添加动态规则状态并在 Dynamic State 列中该规则旁边显示动态状态图标 ( )。如果向规则中添加多个动态规则状态过滤器，图标上的数字表示过滤器的数量。

如果任何必填字段为空白，您将收到错误消息，指示必须填写哪些字段。

为规则设置 SNMP 警报

许可证：保护

您可以从 Rule Detail 页面为规则设置 SNMP 警报。有关 SNMP 警报的详细信息，请参阅第 20-28 页上的添加 SNMP 警报。

要在规则详细信息中添加 SNMP 警报，请执行以下操作：

步骤 1　点击 **Alerts** 旁边的 **Add SNMP Alert**。

系统将添加警报并在 Alerting 列中该规则旁边显示警报图标 ( )。如果向规则中添加多个警报，则系统将在图标上指示警报的数量。

为规则添加规则注释

许可证：保护

您可以从 Rule Detail 页面为规则添加规则注释。有关规则注释的详细信息，请参阅第 20-29 页上的添加规则注释。

要在规则详细信息中添加注释，请执行以下操作：

步骤 1　点击 **Comments** 旁边的 **Add**。

系统将显示 Add Comment 对话框。

步骤 2　在 **Comment** 字段中，键入规则注释。

步骤 3　点击 **OK**。

系统将添加注释并在 Comments 列中该规则旁边显示注释图标 ( )。如果向规则中添加多个注释，图标上的数字表示注释的数量。

提示　要删除规则注释，请点击规则注释部分中的 **Delete**。请注意，仅当缓存的注释具有未提交的入侵策略更改时，才能删除该注释。提交入侵策略更改之后，规则注释即是永久性的。

过滤入侵策略中的规则

许可证：保护

可以按单一条件或按一个或多个条件的组合来过滤 Rules 页面中显示的规则。

您所构造的过滤器显示在 Filter 文本框中。点击过滤器面板中的关键字和关键字参数可以构造过滤器。当选择多个关键字时，系统会使用 AND 逻辑将其组合，以创建复合搜索过滤器。例如，如果选择 **Category** 下的 **preprocessor**，然后选择 **Rule Content > GID** 并输入 `116`，则会得到过滤器 `Category: “preprocessor” GID:”116”`，该过滤器检索属于预处理器规则**并且** GID 为 116 的所有规则。

通过 Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific、Preprocessor 和 Priority 过滤器组，可以为一个关键字提交多个参数（以逗号分隔）。例如，可以按 Shift 键，然后从 **Category** 中选择 **os-linux** 和 **os-windows** 以产生过滤器 `Category:"os-windows,os-linux"`，该过滤器检索 `os-linux` 类别中或 `os-windows` 类别中的任意规则。

要显示过滤器面板，请点击显示图标 ( )。

要隐藏过滤器面板，请点击隐藏图标 ( )。

有关详细信息，请参阅以下主题：

- 第 20-9 页上的了解入侵策略中的规则过滤
- 第 20-16 页上的在入侵策略中设置规则过滤器

了解入侵策略中的规则过滤

许可证：保护

规则过滤器关键字可帮助您找到要对其应用规则状态或事件过滤器等规则设置的规则。您可以按关键字进行过滤，同时从 Rules 页面的过滤器面板选择所需参数作为关键字的参数。

有关详细信息，请参阅：

- 第 20-9 页上的构造入侵策略规则过滤器的指导原则
- 第 20-11 页上的了解规则配置过滤器
- 第 20-13 页上的了解规则内容过滤器
- 第 20-15 页上的了解规则类别
- 第 20-15 页上的直接编辑规则过滤器

构造入侵策略规则过滤器的指导原则

许可证：保护

在大多数情况下，构建过滤器时可以在入侵策略中使用 Rules 页面左侧的过滤器面板来选择要使用的关键字/参数。

规则过滤器在过滤器面板中分为不同的规则过滤器组。许多规则过滤器组包含子条件，因此可以更轻松地找到所需的特定规则。有些规则过滤器有多个级别，可展开以向下钻取到各个规则。

过滤器面板中的项有时表示过滤器类型组，有时表示关键字，还有时表示关键字的参数。以下经验法则可以帮助您构建过滤器：

- 当选择不是关键字的过滤器类型组标题（Rule Configuration、Rule Content、Platform Specific 和 Priority）时，该标题会展开列出可用的关键字。

点击条件列表中的节点来选择关键字时，将显示一个弹出窗口，供您提供要作为过滤条件的参数。

如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

- 当选择属于关键字的过滤器类型组标题（Category、Classifications、Microsoft Vulnerabilities、Microsoft Worms、Priority 和 Rule Update）时，该标题会列出可用参数。

  从此类型的组中选择项时，该参数及其应用到的关键字将立即添加到过滤器中。如果该关键字已经在过滤器中，它将替换与该组对应的关键字的现有参数。

  例如，如果点击过滤器面板中 **Category** 下的 **os-linux**，则会将 `Category:"os-linux"` 添加到过滤器文本框中。如果随后点击 **Category** 下的 **os-windows**，过滤器将更改为 `Category:"os-windows"`。

- Rule Content 下的 Reference 是关键字，其下方列出的特定引用 ID 类型同样如此。选择任何引用关键字时，会显示一个弹出窗口，供您提供要添加到现有过滤器的参数和关键字。如果过滤器中已在使用该关键字，则提供的新参数将替换现有参数。

  例如，如果点击过滤器面板中的 **Rule Content > Reference > CVE ID**，系统将显示弹出窗口，提示您提供 CVE ID。如果输入 `2007`，则会将 `CVE:"2007"` 添加到过滤器文本框中。又例如，如果点击过滤器面板中的 **Rule Content > Reference**，系统将显示弹出窗口，提示您提供该引用。如果输入 `2007`，则会将 `Reference:"2007"` 添加到过滤器文本框中。

- 当从不同的组中选择规则过滤器关键字时，会将每个过滤器关键字都添加到过滤器中并保留所有现有关键字（除非被同一关键字的新值覆盖）。

  例如，如果点击过滤器面板中 **Category** 下的 **os-linux**，则会将 `Category:"os-linux"` 添加到过滤器文本框中。如果随后点击 **Microsoft Vulnerabilities** 下的 **MS00-006**，过滤器将更改为 `Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`。

- 当选择多个关键字时，系统会使用 AND 逻辑将其组合，以创建复合搜索过滤器。例如，如果选择 **Category** 下的 **preprocessor**，然后选择 **Rule Content > GID** 并输入 `116`，则会得到过滤器 `Category: "preprocessor" GID:"116"`，该过滤器检索属于预处理器规则**并且** GID 为 116 的所有规则。

- Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific 和 Priority 过滤器组可以为一个关键字提交多个参数（以逗号分隔）。例如，按住 Shift 键，然后从 **Category** 中选择 **os-linux** 和 **os-windows** 以产生过滤器 `Category:"os-windows,os-linux"`，该过滤器检索 `os-linux` 类别中或 `os-windows` 类别中的任意规则。

同一规则可以按多个过滤器关键字/参数对进行检索。例如，如果按类别 **dos** 来过滤规则，系统将显示 DOS Cisco 尝试规则 (SID 1545)，按优先级 **High** 进行过滤亦如此。

注　思科 VRT 可能会使用规则更新机制来添加和移除规则过滤器。

请注意，Rules 页面中的规则可以是共享对象规则（生成器 ID 为 3），也可以是标准文本规则（生成器 ID 为 1）。下表介绍不同的规则过滤器。

表 20-4　规则过滤器组

过滤器组	说明	是否支持多个参数？	标题为...	列表中的项为...
Rule Configuration	根据规则的配置查找规则。请参阅第 20-11 页上的了解规则配置过滤器。	否	组	关键词
Rule Content	根据规则的内容查找规则。请参阅第 20-13 页上的了解规则内容过滤器。	否	组	关键词

表 20-4　规则过滤器组（续）

过滤器组	说明	是否支持多个参数？	标题为...	列表中的项为...
Category	根据规则编辑器使用的规则类别来查找规则。请注意，本地规则显示于本地子组中。请参阅第 20-15 页上的了解规则类别。	是	关键字	参数
Classifications	根据规则生成的事件的数据包显示中所显示的攻击分类来查找规则。请参阅第 23-11 页上的定义入侵事件分类。	否	关键字	参数
Microsoft Vulnerabilities	根据 Microsoft 公告号查找规则。	是	关键字	参数
Microsoft Worms	根据影响 Microsoft Windows 主机的特定蠕虫查找规则。	是	关键字	参数
Platform Specific	根据规则与特定操作系统版本的相关性来查找规则。 请注意，规则可能会影响多个操作系统或某个操作系统的多个版本。例如，启用 SID 2260 会影响多个版本的 Mac OS X、 IBM AIX 以及其他操作系统。	是	关键字	参数 请注意，如果从子列表中选择其中一项，则会向参数添加修饰符。
Preprocessors	查找各个预处理器的规则。 请注意，在预处理器已启用时，必须启用与预处理器选项相关联的预处理器规则才能生成该选项的事件。	是	组	子组
Priority	根据高、中和低优先级查找规则。 分配给规则的分类将确定该规则的优先级。这些组进一步分为不同的规则类别。请注意，本地规则 （即您创建的规则）不会显示在优先级组中。	是	关键字	参数 请注意，如果从子列表中选择其中一项，则会向参数添加修饰符。
Rule Update	查找通过特定规则更新添加或修改的规则。对于每个规则更新，可以查看更新中的所有规则、仅查看更新中导入的新规则或仅查看更新所更改的现有规则。	否	关键字	参数

了解规则配置过滤器

许可证：保护

您可以按多个规则配置设置来过滤 Rules 页面中列出的规则。

点击条件列表中的节点来选择关键字时，将显示一个弹出窗口，供您提供要作为过滤条件的参数。

如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

有关可用于过滤的规则配置设置的详细信息，请参阅以下操作步骤。

要使用 Rule State 过滤器，请执行以下操作：

步骤 1　在 **Rule Configuration** 下，点击 **Rule State**。

步骤 2　从 **Rule State** 下拉列表中，选择要按其过滤的规则状态：

- 要查找只生成事件的规则，请选择 **Generate Events**，然后点击 **OK**。

- 要查找设置为生成事件并丢弃匹配数据包的规则，请选择 **Drop and Generate Events**，然后点击 **OK**。
- 要查找已禁用的规则，请选择 **Disabled**，然后点击 **OK**。

Rules 页面将更新，以根据当前规则状态显示规则。

要使用 Threshold 过滤器，请执行以下操作：

步骤 1　在 **Rule Configuration** 下，点击 Threshold。

步骤 2　从 **Threshold** 下拉列表中，选择要按其过滤的阈值设置。

- 要查找阈值类型为 `limit` 的规则，请选择 **Limit**，然后点击 **OK**。
- 要查找阈值类型为 `threshold` 的规则，请选择 **Threshold**，然后点击 **OK**。
- 要查找阈值类型为 `both` 的规则，请选择 **Both**，然后点击 **OK**。
- 要查找按 `source` 跟踪阈值的规则，请选择 **Source**，然后点击 **OK**。
- 要查找按 `destination` 跟踪阈值的规则，请选择 **Destination**，然后点击 **OK**。
- 要查找设置了阈值的所有规则，请选择 **All**，然后点击 **OK**。

Rules 页面将更新，以显示已应用过滤器中指示的阈值类型的规则。

要使用 Suppression 过滤器，请执行以下操作：

步骤 1　在 **Rule Configuration** 下，点击 **Suppression**。

步骤 2　从 **Threshold** 下拉列表中，选择要按其过滤的抑制设置。

- 要查找针对该规则所检测的数据包抑制事件的规则，请选择 **By Rule**，然后点击 **OK**。
- 要查找根据流量的源抑制事件的规则，请选择 **By Source**，然后点击 **OK**。
- 要查找根据流量的目标抑制事件的规则，请选择 **By Destination**，然后点击 **OK**。
- 要查找设置了抑制的所有规则，请选择 **All**，然后点击 **OK**。

Rules 页面将更新，以显示已应用过滤器中指示的抑制类型的规则。

要使用 Dynamic State 过滤器，请执行以下操作：

步骤 1　在 **Rule Configuration** 下，点击 **Dynamic State**。

步骤 2　从 **Dynamic State** 下拉列表中，选择要按其过滤的抑制设置。

- 要查找为该规则所检测的数据包配置动态状态的规则，请选择 **By Rule**，然后点击 **OK**。
- 要查找根据流量的源为数据包配置动态状态的规则，请选择 **By ource**，然后点击 **OK**。
- 要查找根据流量的目标配置动态状态的规则，请选择 **By Destination**，然后点击 **OK**。
- 要查找配置了动态状态 `Generate Events` 的规则，请选择 **Generate Events**，然后点击 **OK**。
- 要查找配置了动态状态 `Drop and Generate Events` 的规则，请选择 **Drop and Generate Events**，然后点击 **OK**。

- 要查找配置了动态状态 `Disabled` 的规则，请选择 **Disabled**，然后点击 **OK**。
- 要查找设置了抑制的所有规则，请选择 **All**，然后点击 **OK**。

Rules 页面将更新，以显示已应用过滤器中指示的动态规则状态的规则。

要使用 Alert 过滤器，请执行以下操作：

步骤 1　在 **Rule Configuration** 下，点击 **Alert**。

步骤 2　从 **Alert** 下拉列表中，选择要按其过滤的警报：**SNMP**。

步骤 3　点击 **OK**。

Rules 页面将更新，以显示已应用警报过滤器的规则。

要使用 Comment 过滤器，请执行以下操作：

步骤 1　在 **Rule Configuration** 下，点击 **Comment**。

步骤 2　在 **Comment** 字段中，键入要按其过滤的注释文本字符串，然后点击 **OK**。

Rules 规则页面将更新，以显示对规则应用的注释包含过滤器中指示的字符串的规则。

了解规则内容过滤器

许可证：保护

您可以按多个规则内容项来过滤 Rules 页面中列出的规则。例如，通过搜索规则的 SID 可以快速检索该规则。也可以查找用于检测发往特定目标端口的流量的所有规则。

点击条件列表中的节点来选择关键字时，将显示一个弹出窗口，供您提供要作为过滤条件的参数。

如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

例如，如果点击过滤器面板中 **Rule Content** 下的 **SID**，系统将显示弹出窗口，提示您提供 SID。如果键入 `1045`，则会将 `SID:"1045"` 添加到过滤器文本框中。如果随即再次点击 **SID** 并将 SID 过滤器更改为 `1044`，过滤器将更改为 `SID:"1044"`。

有关可用于过滤的规则内容的详细信息，请参阅下表。

表 20-5　Rule Content 过滤器

要使用此过滤器，请点击 ...	然后...	结果
Message	键入要按其过滤的消息字符串，然后点击 **OK**。	查找在消息字段中包含所提供字符串的规则。
SID	键入要按其过滤的 SID 编号，然后点击 **OK**。	查找具有指定 SID 的规则。
GID	键入要按其过滤的 GID 编号，然后点击 **OK**。	查找具有指定 GID 的规则。

表 20-5　Rule Content 过滤器（续）

要使用此过滤器，请点击 ...	然后...	结果
Reference	键入要按其过滤的引用字符串，然后点击 **OK**。 要输入希望按其过滤的特定类型的引用的字符串，请选择 **CVE ID**、 **URL**、 **Bugtraq ID**、 **Nessus ID**、 **Arachnids ID** 或 **Mcafee ID**，然后键入字符串并点击 **OK**。	查找在引用字段中包含所提供字符串的规则。
Action	选择要按其过滤的操作： • 要查找警报规则，请选择 **Alert** 并点击 **OK**。 • 要查找通过规则，请选择 **Pass** 并点击 **OK**。	查找以 `alert` 或 `pass` 开头的规则。
Protocol	选择要按其过滤的协议：**ICMP**、 **IP**、 **TCP** 或 **UDP**；然后单击 **OK**。	查找包含所选协议的规则。
Direction	选择要按其过滤的方向设置： • 要查找用于检测按特定方向移动的流量的规则，请选择 **Directional**，然后点击 **OK**。 • 要查找用于检测在源与目标之间按任一方向移动的流量的规则，请选择 **Bidirectional**，然后点击 **OK**。	根据规则是否包含指示的方向设置来查找规则。
Source IP	键入要按其过滤的源 IP 地址，然后点击 **OK**。 请注意，您可以根据有效 IP 地址、CIDR 块/前缀长度或者使用 `$HOME_NET` 或 `$EXTERNAL_NET` 等变量进行过滤。	查找使用指定的地址或变量作为规则中的源 IP 地址标识的规则。
Destination IP	键入要按其过滤的目标 IP 地址，然后点击 **OK**。 请注意，您可以根据有效 IP 地址、CIDR 块/前缀长度或者使用 `$HOME_NET` 或 `$EXTERNAL_NET` 等变量进行过滤。	查找使用指定的地址或变量作为规则中的源 IP 地址标识的规则。
Source port	键入要按其过滤的源端口，然后点击 **OK**。 端口值必须为 1 到 65535 之间的整数或端口变量。	查找包含指定源端口的规则。
Destination port	键入要按其过滤的目标端口，然后点击 **OK**。 端口值必须为 1 到 65535 之间的整数或端口变量。	查找包含指定目标端口的规则。

表 20-5　Rule Content 过滤器（续）

要使用此过滤器，请点击 ...	然后...	结果
Rule Overhead	选择要按其过滤的规则开销量：**Low**、**Medium**、**High** 或 **Very High**；然后点击 **OK**。	查找具有所选规则开销的规则。
Metadata	键入要按其过滤的元数据键/值对（以空格分隔），然后点击 **OK**。 例如，键入 `metadata:"service http"` 可查找元数据与 HTTP 应用协议相关的规则。	查找元数据包含匹配的键值对的规则。

了解规则类别

许可证：保护

ASA FirePOWER 模块根据规则检测的流量类型对规则分类。在 Rules 页面中，可以按规则类别过滤，从而可为某个类别中的所有规则设置规则属性。例如，如果网络中没有 Linux 主机，则可以按 **os-linux** 类别过滤，然后禁用表明将禁用整个 **os-linux** 类别的所有规则。

注　思科 VRT 可能会使用规则更新机制来添加和删除规则类别。

直接编辑规则过滤器

许可证：保护

您可以编辑过滤器来修改在点击过滤器面板中的过滤器时所提供的特殊关键字及其参数。 Rules 页面中的自定义过滤器的功能与规则编辑器中使用的过滤器类似，但也可以使用在 Rules 页面过滤器中提供的任何关键字，方法是使用在通过过滤器面板选择过滤器时显示的语法。要确定供今后使用的关键字，请点击右侧过滤器面板中的相应参数。过滤器关键字和参数语法显示在过滤器文本框中。

要查看仅支持特定值的关键字参数列表，请参阅第 20-11 页上的了解规则配置过滤器、第 20-13 页上的了解规则内容过滤器和第 20-15 页上的了解规则类别。请记住，仅对 Category 和 Priority 过滤器类型支持关键字的多个以逗号分隔的参数。

您可以使用关键字和参数、字符串及带引号的文本字符串（以空格分隔多个过滤条件）。过滤器不能包含正则表达式、通配符或任何特殊运算符，例如取反字符 (!)、大于号 (>) 和小于号 (<) 等。当键入的搜索条件没有关键字、关键字的首字母没有大写或者没有用引号将参数引起来时，该搜索将被视为字符串搜索，并搜索类别、消息和 SID 字段中有无指定条件。

所有关键字、关键字参数和字符串都不区分大小写。除关键字 `gid` 和 `sid` 之外，所有参数和字符串都被视为部分字符串。`gid` 和 `sid` 的参数只会返回完全匹配项。

每个规则过滤器都可以包含一个或多个关键字，其格式如下：

`Keyword:"argument"`

其中，*`keyword`* 是规则类型表中所述过滤器组中的关键字之一，而 *`argument`* 则是要在与该关键字相关的一个或多个特定字段中搜索的单个字母数字字符串，需用双引号引起来且不区分大小写。请注意，键入的关键字应该首字母大写。

除 gid 和 sid 之外的所有关键字的参数都会被视为部分字符串。例如，参数 123 将返回 "12345"、"41235"、"45123"，依此类推。gid 和 sid 的参数只会返回完全匹配项；例如，sid:3080 只会返回结果 SID 3080。

每个规则过滤器还可以包含一个或多个字母数字字符串。字符串将搜索规则的 Message 字段、Signature ID 和 Generator ID。例如，字符串 123 会返回规则消息中的 "Lotus123"、"123mania" 等字符串，也会返回 SID 6123、SID 12375 等。有关规则的 Message 字段的详细信息，请参阅第 23-11 页上的定义事件消息。使用一个或多个字符串来进行过滤可以搜索部分 SID。

所有字符串都不区分大小写并被视为部分字符串。例如，字符串 ADMIN、admin 或 Admin 中的任何字符串都会返回 "admin"、"CFADMIN"、"Administrator" 等。

用引号将字符串引起来可以返回完全匹配项。例如，用引号引起来的文本字符串 "overflow attempt" 只会返回完全匹配的该字符串，而由 overflow 和 attempt 这两个字符串组成的未加引号的过滤器则会返回 "overflow attempt"、"overflow multipacket attempt"、"overflow with evasion attempt" 等。

通过输入关键字和/或字符串的任意组合（以空格分隔）可以缩小过滤结果的范围。结果包括符合所有过滤条件的任意规则。

可以按照任意顺序输入多个过滤条件。例如，以下每个过滤器返回的规则相同：

- url:at login attempt cve:200
- login attempt cve:200 url:at
- login cve:200 attempt url:at

在入侵策略中设置规则过滤器

许可证：保护

您可以对 Rules 页面中的规则进行过滤来显示其中一组规则。然后，您可以使用任何页面功能。例如，当您需要为某个特定类别中的所有规则设置阈值时，此功能会非常有用。您可以对已过滤或未过滤列表中的规则使用相同的功能。例如，您可以将新的规则状态应用到已过滤或未过滤列表中的规则。

可以从入侵策略中 Rules 页面左侧的过滤器面板中选择预定义的过滤器关键字。选择过滤器时，该页面会显示所有匹配的规则，或者指出没有匹配的规则。

有关可以使用的所有关键字和参数以及如何在过滤器面板中构造过滤器的详细信息，请参阅第 20-9 页上的了解入侵策略中的规则过滤。

您可以对过滤器添加关键字来进一步对其进行限制。输入的任何过滤器都会搜索整个规则数据库并返回所有匹配的规则。当您在页面仍显示上一过滤器的结果时输入过滤条件，页面将清空，转而返回新过滤器的结果。

您也可以使用在选择过滤器时提供的相同关键字和参数语法来键入过滤条件，或者在选择过滤器后修改其中的参数值。当键入的搜索条件没有关键字、关键字的首字母没有大写或者没有用引号将参数引起来时，该搜索将被视为字符串搜索，并搜索类别、消息和 SID 字段中有无指定条件。

要过滤入侵策略中的特定规则，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在其他策略中有未保存的更改，请点击 **OK** 废弃这些更改并继续操作。有关保存其他策略中未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　点击左侧过滤器面板中的关键字或参数构造过滤器。请注意，如果点击过滤器中已存在的关键字的参数，则该参数将替换现有的参数。有关详情，请参阅：

- 第 20-9 页上的构造入侵策略规则过滤器的指导原则
- 第 20-11 页上的了解规则配置过滤器
- 第 20-13 页上的了解规则内容过滤器
- 第 20-15 页上的了解规则类别
- 第 20-15 页上的直接编辑规则过滤器

页面将刷新，显示所有匹配的规则，而与该过滤器匹配的规则数量将显示于过滤器文本框的上方。

步骤 5　选择要在其中应用新设置的一条或多条规则。您有以下选项：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　或者，对规则作出通常会在该页面上作出的任何更改。有关详细信息，请参阅以下各节：

- 有关在 Rules 页面中启用和禁用规则的信息，请参阅第 20-17 页上的设置规则状态。
- 有关向规则添加阈值和抑制的信息，请参阅第 20-19 页上的按策略过滤入侵事件通知。
- 有关如何设置在匹配的流量中发生速率异常时触发的动态规则状态的信息，请参阅第 20-25 页上的添加动态规则状态。
- 有关向具体规则添加 SNMP 警报的信息，请参阅第 20-28 页上的添加 SNMP 警报。
- 有关向规则添加规则注释的信息，请参阅第 20-29 页上的添加规则注释。

步骤 7　保存策略，继续编辑，废弃更改，或者退出并在系统缓存中保留更改。

有关详细信息，请参阅第 19-3 页上的管理入侵策略和第 19-4 页上的编辑入侵策略。

设置规则状态

许可证：保护

思科漏洞研究团队 (VRT) 为每个默认策略中的每条入侵规则和预处理器规则设置了默认状态。例如，一条规则可能会在 Security over Connectivity 默认策略中启用而在 Connectivity over Security 默认策略中禁用。您创建的入侵策略规则将继承用于创建该策略的默认策略中相应规则的默认状态。

您可以将规则逐一设置为 Generate Events、Drop and Generate Events 或 Disable，也可以按各种因素过滤规则以选择要修改其状态的规则。在内联部署中，可以在内联入侵部署中使用 Drop and Generate Events 规则状态来丢弃恶意数据包。请注意，在被动部署中，规则状态为 Drop and Generate Events 的规则会生成事件但不丢弃数据包.。将规则设置为 Generate Events 或 Drop and Generate Events 可启用该规则；将规则设置为 Disable 将禁用该规则。

我们以两种情况为例。在第一种情况下，特定规则的规则状态被设置为 Generate Events。当恶意数据包通过网络并触发该规则时，数据包被发送到其目标，系统生成入侵事件。在第二种情况下，假设同一规则的规则状态在内联部署中被设置为 Drop and Generate Events。在此情况下，当恶意数据包通过网络时，系统会丢弃恶意数据包并生成入侵事件。该数据包永远不会到达其目标。

在入侵策略中，可将规则的状态设置为下列之一：

- 如果需要系统检测特定的入侵企图并在发现匹配的流量时生成入侵事件，可将规则状态设置为 **Generate Events**。
- 如果需要系统检测特定的入侵企图，然后在内联部署中发现匹配流量时丢弃包含攻击的数据包并生成入侵事件，或者在被动部署中发现匹配流量时生成入侵事件，可将规则状态设置为 **Drop and Generate Events**。

  请注意，为使系统丢弃数据包，在内联部署中必须将入侵策略设置为丢弃规则；有关详细信息，请参阅第 19-5 页上的设置内联部署中的丢弃行为。
- 如果不希望系统评估匹配流量，请将规则状态设置为 **Disable**。

要使用丢弃规则，必须执行以下操作：

- 在入侵策略中启用 **Drop when Inline** 选项。
- 对于所有应该丢弃与其匹配的数据包的规则，将规则状态设置为 **Drop and Generate Events**。
- 将包含与入侵策略关联的访问控制规则的访问控制策略应用于在内联部署中。

在 Rules 页面中过滤规则可帮助您查找要设置为丢弃规则的规则。有关详细信息，请参阅第 20-9 页上的过滤入侵策略中的规则。

有关规则剖析、规则关键字及其选项和规则编写语法的详细信息，请参阅第 23-1 页上的了解和编写入侵规则。

VRT 有时会使用规则更新来更改默认策略中一条或多条规则的默认状态。如果允许规则更新对基本策略进行更新，则意味着当用于创建策略的默认策略中的默认状态发生更改时，也允许规则更新更改策略中的规则默认状态。但请注意，如果您已经更改了规则状态，规则更新不会覆盖您的更改。

要更改一条或多条规则的规则状态，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在其他策略中有未保存的更改，请点击 **OK** 废弃这些更改并继续操作。有关保存其他策略中未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

请注意，此页面指示已启用规则的总数、设置为 Generate Events 的已启用规则总数以及设置为 Drop and Generate Events 的总数。另请注意，在被动部署中，设置为 Drop and Generate Events 的规则仅生成事件。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　查找要在其中设置规则状态的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅以下主题：第 20-9 页上的了解入侵策略中的规则过滤和第 20-16 页上的在入侵策略中设置规则过滤器。

  页面将刷新，显示所有匹配的规则。

步骤 5　选择要在其中设置规则状态的一条或多条规则。您有以下选项：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　您有以下选项：

- 要在流量与所选规则匹配时生成事件，请选择 **Rule State > Generate Events**。
- 要在流量与所选规则匹配时在内联部署中生成事件并丢弃流量，请选择 **Rule State > Drop and Generate Events**。
- 如果要不检查与所选规则匹配的流量，请选择 **Rule State > Disable**。

注　思科**强烈**建议**不要**启用入侵策略中的所有入侵规则。如果启用所有规则，则设备的性能可能会下降。相反，应调整规则集，使之与网络环境尽可能匹配。

步骤 7　保存策略，继续编辑，废弃更改，或者退出并在系统缓存中保留更改。有关详细信息，请参阅第 19-3 页上的管理入侵策略和第 19-4 页上的编辑入侵策略。

按策略过滤入侵事件通知

许可证：保护

入侵事件的重要性可根据发生频率或者源或目标 IP 地址而定。在某些情况下，直至事件发生一定次数后您可能才会在意。例如，如果有人企图登录服务器，在其失败达到一定次数之前，您可能不会担心。但在其他情况下，也许只需要发生几次，就能让您知道存在普遍性问题。例如，如果有人对网络服务器发动 DoS 攻击，可能只需要发生区区数次入侵事件，您就会明白需要解决这种情况。发生数百次相同事件只会让系统不堪重负。

有关详细信息，请参阅以下各节：

- 第 20-19 页上的配置事件阈值说明如何根据发生次数设置指示事件显示频率的阈值。您可以逐个事件和逐个策略配置阈值。
- 第 20-23 页上的按入侵策略配置抑制说明如何逐个源或目标 IP 地址和逐个策略抑制指定事件的通知。

配置事件阈值

许可证：保护

您可以逐个入侵策略为各条规则设置阈值，根据事件在指定时间段内生成的次数来限制系统记录和显示入侵事件的次数。这可以防止因相同事件数量过多而使系统不堪重负。您可以按每条共享对象规则、标准文本规则或预处理器规则设置阈值。

有关详细信息，请参阅：

- 第 20-19 页上的了解事件阈值
- 第 20-21 页上的添加和修改入侵事件阈值
- 第 20-22 页上的查看和删除入侵事件阈值
- 第 20-6 页上的为规则设置阈值

了解事件阈值

许可证：保护

首先，必须指定阈值类型。可以选择的选项如下表所述。

表 20-6　阈值选项

选项	说明
Limit	为指定时间段内触发规则的指定数量的数据包（由 Count 参数指定）记录并显示事件。例如，如果将类型设置为 **Limit**，将 **Count** 设置为 10，并将 **Seconds** 设置为 60，而同一分钟内有 14 个数据包触发规则，则系统在显示发生的前 10 个违反该规则的事件后将停止记录违反该规则的事件。
Threshold	在指定时间段内，当指定数量的数据包（由 Count 参数指定）触发规则时，记录并显示一个事件。请注意，达到事件阈值计数且系统记录该事件之后，时间计数器将重新开始计数。例如，将类型设置为 **Threshold**，将 **Count** 设置为 10，并将 **Seconds** 设置为 60 时，如果到 33 秒时规则触发 10 次，则系统将生成一个事件，然后将 Seconds 和 Count 计数器重置为 0。其后，该规则在接下来 25 秒内又触发 10 次。由于计数器在第 33 秒时已重置为 0，因此系统此时会再记录一个事件。
Both	每个指定时间段在指定数量（计数）的数据包触发规则后记录并显示一次事件。例如，如果将类型设置为 **Both**，将 **Count** 设置为 2，并将 **Seconds** 设置为 10，则事件计数结果如下： • 如果 10 秒内触发规则一次，系统不会生成任何事件（未达到阈值） • 如果 10 秒内触发规则两次，系统将生成一个事件（第二次触发规则时达到阈值） • 如果 10 秒内触发规则四次，系统将生成一个事件（第二次触发规则时达到阈值，忽略其后的事件）

接下来，必须指定跟踪，从而确定事件阈值是按源 IP 地址计算还是按目标 IP 地址计算。从下表中选择一个选项来指定系统如何跟踪事件实例。

表 20-7　阈值 IP 选项

选项	说明
Source	按源 IP 地址计算事件实例计数。
Destination	按目标 IP 地址计算事件实例计数。

最后，必须指定用于定义阈值的实例数和时间段。

表 20-8　阈值实例/时间选项

选项	说明
Count	每个跟踪 IP 地址在每个指定时间段内达到阈值所需的事件实例数量。
Seconds	计数重置之前经过的秒数。如果将阈值类型设置为 **limit**，将跟踪设置为 **Source IP**，将 **count** 设置为 10，并将 **seconds** 设置为 10，则系统将记录并显示 10 秒钟内发生的来自指定源端口的前 10 个事件。如果前 10 秒内只发生了 7 个事件，系统将记录并显示这些事件，而如果前 10 秒内发生了 40 个事件，系统将记录并显示 10 个事件，然后在 10 秒过后重新开始计数。

请注意，入侵事件阈值可单独使用，也可与基于速率的攻击防御、`detection_filter` 关键字和入侵事件抑制的任意组合配合使用。有关详细信息，请参阅第 20-25 页上的添加动态规则状态、第 23-80 页上的过滤事件和第 20-23 页上的按入侵策略配置抑制。

有关详细信息，请参阅：

- 第 20-21 页上的添加和修改入侵事件阈值

- 第 20-6 页上的为规则设置阈值
- 第 20-22 页上的查看和删除入侵事件阈值

添加和修改入侵事件阈值

许可证：保护

您可以为一条或多条特定规则设置阈值。也可以单独或同时修改现有阈值设置。可以为每条规则设置一个阈值。添加阈值将覆盖该规则的任何现有阈值。

有关查看和删除阈值配置的详细信息，请参阅第 20-22 页上的查看和删除入侵事件阈值。

您还可以修改默认应用到所有规则和预处理器生成的事件的全局阈值。有关详细信息，请参阅第 22-1 页上的全局限制入侵事件记录。

请注意，当键入的值无效时，字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

要添加或修改事件阈值，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在其他策略中有未保存的更改，请点击 **OK** 废弃这些更改并继续操作。有关保存其他策略中未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　查找要在其中设置阈值的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅以下主题：第 20-9 页上的了解入侵策略中的规则过滤和第 20-16 页上的在入侵策略中设置规则过滤器。

页面将刷新，显示所有匹配的规则。

步骤 5　选择要在其中设置阈值的一条或多条规则。您有以下选项：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　选择 **Event Filtering > Threshold**。

系统将显示阈值弹出窗口。

步骤 7　从 **Type** 下拉列表中，选择要设置的阈值的类型。

- 选择 **Limit** 以限制为在每个时间段内向指定数量的事件实例发送通知。
- 选择 **Threshold** 以在每个时间段内为指定数量的各事件实例提供通知。
- 选择 **Both** 则在每个时间段内事件实例数达到指定数量后提供一次通知。

步骤 8　从 **Track By** 下拉列表中，选择要按 **Source** 还是 **Destination** IP 地址跟踪事件实例。

步骤 9　在 **Count** 字段中，指定要用作阈值的事件实例数。

步骤 10　在 **Seconds** 字段中指定时间段的秒数，系统将跟踪该时间段内的事件实例。

步骤 11　点击 **OK**。

系统将添加阈值并在 Event Filtering 列中该规则旁边显示事件过滤器图标 ( )。如果向规则中添加多个事件过滤器，图标上的数字表示事件过滤器的数量。

步骤 12　保存策略，继续编辑，废弃更改，或者退出并在系统缓存中保留更改。

有关详细信息，请参阅第 19-3 页上的管理入侵策略和第 19-4 页上的编辑入侵策略。

查看和删除入侵事件阈值

许可证：保护

您可能需要查看或删除现有阈值设置。可以使用 Rules Details 视图显示为阈值配置的设置，看其是否适合系统。如果不适合，可以添加新的阈值来覆盖现有值。

请注意，您也可以修改默认应用到所有规则和预处理器生成的事件的全局阈值。有关详情，请参见第 22-1 页上的全局限制入侵事件记录。

要查看或删除阈值，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在其他策略中有未保存的更改，请点击 **OK** 废弃这些更改并继续操作。有关保存其他策略中未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　查找配置了要查看或删除的阈值的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅以下主题：第 20-9 页上的了解入侵策略中的规则过滤和第 20-16 页上的在入侵策略中设置规则过滤器。

  页面将刷新，显示所有匹配的规则。

步骤 5　选择配置了要查看或删除的阈值的一条或多条规则。您有以下选项：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　要删除每条所选规则的阈值，请选择 **Event Filtering > Remove Thresholds** 。在随即显示的确认弹出窗口中点击 **OK**。

提示　要删除特定阈值，还可以突出显示该规则，然后点击 **Show details**。展开阈值设置，然后点击要移除的阈值设置旁边的 **Delete**。点击 **OK** 确认要删除该配置。

页面将刷新，该阈值被删除。

步骤 7　保存策略，继续编辑，废弃更改，或者退出并在系统缓存中保留更改。有关详细信息，请参阅第 19-3 页上的管理入侵策略和第 19-4 页上的编辑入侵策略。

按入侵策略配置抑制

许可证：保护

您可以在特定 IP 地址或 IP 地址范围触发特定规则或预处理器时抑制入侵事件通知。这对杜绝误报十分有用。例如，如果邮件服务器传输的数据包看起来像某种特定的漏洞，则可能会在邮件服务器触发该事件时抑制对其发出的事件通知。所有数据包都会触发该规则，但您只会看到真正的攻击事件。

请注意，入侵事件抑制可单独使用，也可与基于速率的攻击防御、`detection_filter` 关键字和入侵事件阈值的任意组合配合使用。有关详细信息，请参阅第 20-25 页上的添加动态规则状态、第 23-80 页上的过滤事件和第 20-19 页上的配置事件阈值。

有关详细信息，请参阅：

- 第 20-23 页上的抑制入侵事件
- 第 20-24 页上的查看和删除抑制条件

抑制入侵事件

许可证：保护

您可以抑制一条或多条规则的入侵事件通知。当某条规则的通知被抑制时，规则会触发，但不会生成事件。您可以为规则设置一个或多个抑制。列出的第一个抑制的优先级最高。请注意，当两个抑制相冲突时，将执行第一个抑制的操作。

请注意，当键入的值无效时，字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

要抑制事件显示，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在其他策略中有未保存的更改，请点击 **OK** 废弃这些更改并继续操作。有关保存其他策略中未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　查找要在其中设置抑制的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅以下主题：第 20-9 页上的了解入侵策略中的规则过滤和第 20-16 页上的在入侵策略中设置规则过滤器。

  页面将刷新，显示所有匹配的规则。

步骤 5　选择要为其配置抑制条件的一条或多条规则。您有以下选项：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　选择 **Event Filtering > Suppression**。

系统将显示抑制弹出窗口。

步骤 7　选择下列 **Suppression Type** 选项之一：

- 选择 **Rule** 将完全抑制所选规则的事件。
- 选择 **Source** 将抑制由指定源 IP 地址发出的数据包生成的事件。
- 选择 **Destination** 将抑制由发往指定目标 IP 地址的数据包生成的事件。

步骤 8　如果为抑制类型选择 **Source** 或 **Destination**，则在 **Network** 字段中输入要指定为源或目标 IP 地址的 IP 地址、地址块或变量，或者输入由这些值的任意组合组成并以逗号分隔的列表。

有关在 中使用 IPv4 CIDR 和 IPv6 前缀长度地址块的详细信息，请参阅第 1-3 页上的IP 地址约定。

步骤 9　点击 **OK**。

系统将添加抑制条件并在 Event Filtering 列中被抑制的该规则旁边显示事件过滤器图标 ( )。如果向规则中添加多个事件过滤器，图标上的数字表示事件过滤器的数量。

步骤 10　保存策略，继续编辑，废弃更改，或者退出并在系统缓存中保留更改。

有关详细信息，请参阅第 19-3 页上的管理入侵策略和第 19-4 页上的编辑入侵策略。

查看和删除抑制条件

许可证：保护

您可能需要查看或删除现有抑制条件。例如，由于某个邮件服务器通常会传输看起来像漏洞的数据包，因此可以抑制由该邮件服务器 IP 地址发出的数据包的事件通知。如果以后停用该邮件服务器并将此 IP 地址重新分配给其他主机，应删除对该源 IP 地址的抑制条件。

要查看或删除定义的抑制条件，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在其他策略中有未保存的更改，请点击 **OK** 废弃这些更改并继续操作。有关保存其他策略中未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。默认情况下，页面按消息的字母顺序列出规则。

步骤 4　查找要在其中查看或删除抑制的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅以下主题：第 20-9 页上的了解入侵策略中的规则过滤和第 20-16 页上的在入侵策略中设置规则过滤器。

  页面将刷新，显示所有匹配的规则。

步骤 5　选择要查看或删除其抑制设置的一条或多条规则。您有以下选项：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　此时您有两种选择：

- 要删除某条规则的所有抑制，请选择 **Event Filtering > Remove Suppressions** 。在随即显示的确认弹出窗口中点击 **OK**。
- 要删除特定的抑制设置，请突出显示该规则，然后点击 **Show details**。展开抑制设置，然后点击要删除的抑制设置旁边的 **Delete**。点击 **OK** 确认要删除所选设置。

页面将刷新，该抑制设置被删除。

步骤 7　保存策略，继续编辑，废弃更改，或者退出并在系统缓存中保留更改。有关详细信息，请参阅第 19-3 页上的管理入侵策略和第 19-4 页上的编辑入侵策略。

添加动态规则状态

许可证：保护

基于速率的攻击通过向网络或主机发送过大的流量，企图让网络或主机不堪重负，导致其速度下降或拒绝合法请求。为了应对特定规则出现过多规则匹配项的情况，可以使用基于速率的防御来更改规则的操作。

有关详细信息，请参阅：

- 第 20-25 页上的了解动态规则状态
- 第 20-26 页上的设置动态规则状态

了解动态规则状态

许可证：保护

您可以配置入侵策略，使其包含基于速率的过滤器，在指定时间段内出现某条规则的太多匹配项时进行检测。可以（以内联方式部署的设备）使用此功能在指定时间内拦截基于速率的攻击，然后恢复为规则匹配项仅生成事件而不丢弃流量的规则状态。

基于速率的攻击防御可确定异常流量模式，并可将这些流量对合法请求的影响降至最低。您可以识别出发往一个或多个特定目标 IP 地址或者由一个或多个特定源 IP 地址发出的流量中存在的过多规则匹配项。也可以对检测的所有流量中符合特定规则的过多匹配项作出反应。

在入侵策略中，可以为任何入侵规则或预处理器规则配置基于速率的过滤器。基于速率的过滤器包含三个组成部分：

- 规则的匹配速率，配置为特定秒数内的规则匹配项数量
- 超过速率时要执行的新操作，可用的操作有三项：Generate Events、Drop and Generate Events 和 Disable
- 操作的持续时间，配置为超时值

请注意，新操作自开始之后，在到达超时时间之前会一直执行，即使速率在这段时间内降到配置的速率以下亦不会停止。达到超时后，如果速率低于阈值，则规则的操作会恢复到为该规则最初配置的操作。

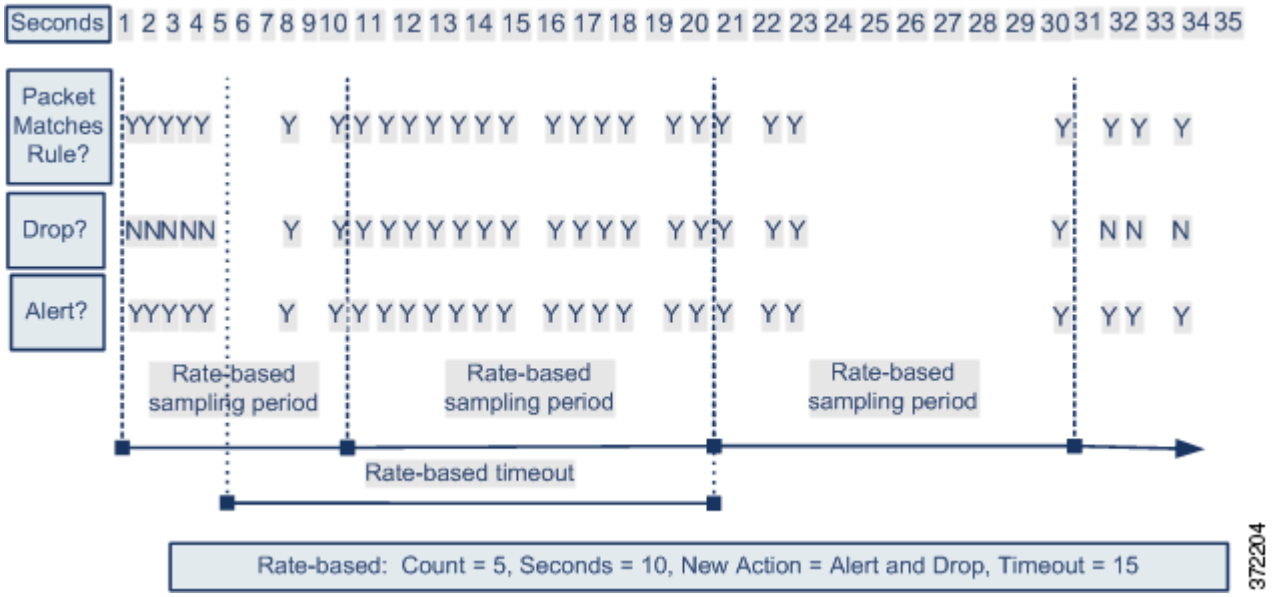
在内联部署中，可以将基于速率的攻击防御临时或永久配置为拦截攻击。如果没有基于速率的配置，设置为 Generate Events 的规则确实会生成事件，但系统不会丢弃这些规则的数据包。但是，如果攻击流量所匹配的规则配置了基于速率的条件，则基于速率的操作可能会导致系统在该操作处于活动状态的时间内丢弃数据包，即便这些规则最初并未设置为 Drop and Generate Events。

注　基于速率的操作无法启用禁用的规则，也无法丢弃与禁用的规则匹配的流量。

可以对同一规则定义多个基于速率的过滤器。入侵策略中列出的第一个过滤器优先级最高。请注意，当两个基于速率的过滤器的操作相冲突时，将执行第一个基于速率的过滤器的操作。

下图显示的例子中，攻击者正在尝试访问主机。反复尝试查找密码触发了配置有基于速率的攻击防御的规则。当在 10 秒的时间跨度内发生五次规则匹配之后，基于速率的设置会将规则属性更改为 Drop and Generate Events。新的规则属性在 15 秒之后超时。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样速率高于当前或前一个采样周期的阈值，新操作将继续。只有在采样周期完毕而采样速率低于阈值速率之后，新操作才会恢复为 Generate Events。



设置动态规则状态

许可证：保护

在某些情况下，您可能不希望将某规则设置为 Drop and Generate Events 状态，因为您不想丢弃与该规则匹配的每个数据包，但同时您又确实希望在指定事件内出现特定频率的匹配项时丢弃与该规则匹配的数据包。动态规则状态可用于配置应该触发规则操作更改的速率、达到该速率时应该改而执行的操作以及新操作应该持续的时间。

您可以通过指定计数来设置该规则的命中数，并设置以秒数为单位的时间段，在该时间段内应达到该命中数才会触发操作更改。此外，您还可以设置超时，让该操作在超时时间到期后恢复为该规则以前的状态。

可以为同一规则定义多个动态规则状态过滤器。入侵策略的规则详细信息中列出的第一个过滤器优先级最高。请注意，当两个基于速率的过滤器的操作相冲突时，将执行第一个基于速率的过滤器的操作。

请注意，当键入的值无效时，字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

注　动态规则状态无法启用禁用的规则，也无法丢弃与禁用的规则匹配的流量。

要添加动态规则状态，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在其他策略中有未保存的更改，请点击 **OK** 废弃这些更改并继续操作。有关保存其他策略中未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。

步骤 4　查找要在其中添加动态规则状态的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅：第 20-9 页上的了解入侵策略中的规则过滤和第 20-16 页上的在入侵策略中设置规则过滤器。

  页面将刷新，显示所有匹配的规则。

步骤 5　选择要在其中添加动态规则状态的一条或多条规则。您有以下选项：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　选择 **Dynamic State > Add Rate-Based Rule State**。

系统将显示 Add Rate-Based Rule State 对话框。

步骤 7　从 **Track By** 下拉列表中，选择要如何跟踪规则匹配项。

- 选择 **Source** 将跟踪由特定的一个或一组源地址发出的该规则匹配项的数量。
- 选择 **Destination** 将跟踪发往特定的一个或一组目标地址的该规则匹配项的数量。
- 选择 **Rule** 将跟踪该规则的所有匹配项。

步骤 8　如果将 **Track By** 设置为 **Source** 或 **Destination** 时，请在 **Network** 字段中输入要跟踪的每台主机的地址。

可以指定单个 IP 地址、地址块、变量或由这些值的任意组合组成并以逗号分隔的列表。有关在中使用 IPv4 CIDR 和 IPv6 前缀长度地址块的详细信息，请参阅第 1-3 页上的IP 地址约定。

步骤 9　在 **Rate** 旁边，指示每个时间段的规则匹配项数，以设置攻击速率：

- 在 **Count** 字段中，使用 1 到 2147483647 之间的整数指定要用作阈值的规则匹配项数量。
- 在 **Count** 字段中，使用 1 到 2147483647 之间的整数指定时间段的秒数，系统将跟踪该时间段内的攻击。

步骤 10　从 **New State** 下拉列表中，选择满足条件时要采取的新操作。

- 选择 **Generate Events** 将生成事件。
- 选择 **Drop and Generate Events** 将在内联部署中生成事件并丢弃触发该事件的数据包，或在被动部署中生成事件。
- 选择 **Disabled** 将不执行任何操作。

步骤 11　在 **Timeout** 字段中，键入希望新操作保持有效的秒数。在超时后，规则将恢复到其原始状态。指定 0 或将 **Timeout** 字段留空可防止新操作超时。

步骤 12　点击 **OK**。

系统将添加动态规则状态并在 Dynamic State 列中该规则旁边显示动态状态图标 ( )。如果向规则中添加多个动态规则状态过滤器，图标上的数字表示过滤器的数量。

如果任何必填字段为空白，您将收到错误消息，指示必须填写哪些字段。

提示　要删除一组规则的所有动态规则设置，请在 Rules 页面中选择这些规则，然后选择 **Dynamic State > Remove Rate-Based States**。也可以从规则的规则详细信息中删除单独的基于速率的规则状态过滤器，方法是选择该规则后点击 **Show details**，然后点击要删除的基于速率的过滤器旁边的 **Delete**。

步骤 13　保存策略，继续编辑，废弃更改，或者退出并在系统缓存中保留更改。

有关详细信息，请参阅第 19-3 页上的管理入侵策略和第 19-4 页上的编辑入侵策略。

添加 SNMP 警报

许可证：保护

如果为 ASA FirePOWER 模块配置 SNMP 警报，则可以配置特定规则，以在规则生成事件时提供 SNMP 警报。有关详细信息，请参阅第 28-1 页上的使用 SNMP 响应。

要设置 SNMP 警报，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在其他策略中有未保存的更改，请点击 **OK** 废弃这些更改并继续操作。有关保存其他策略中未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。

步骤 4　查找要在其中设置 SNMP 警报的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅以下主题：第 20-9 页上的了解入侵策略中的规则过滤和第 20-16 页上的在入侵策略中设置规则过滤器。

  页面将刷新，显示所有匹配的规则。

步骤 5　选择要在其中设置 SNMP 警报的一条或多条规则：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　选择 **Alerting > Add SNMP Alert**。

系统将添加警报并在 Alerting 列中该规则旁边显示警报图标 ( )。如果向规则中添加多个警报类型，图标上的数字表示警报类型的数量。

提示　要从规则中移除 SNMP 警报，请点击规则旁边的复选框并选择 **Alerting > Remove SNMP Alerts**，然后点击 **OK** 以确认删除。

步骤 7　保存策略，继续编辑，废弃更改，或者退出并在系统缓存中保留更改。有关详细信息，请参阅第 19-3 页上的管理入侵策略和第 19-4 页上的编辑入侵策略。

添加规则注释

许可证：保护

您可以向规则添加注释。添加的任何注释都将显示于 Rules 页面的 Rule Details 视图中。

提交包含注释的入侵策略更改后，点击该规则 Edit 页面中的 **Rule Comment** 也可查看该注释。有关编辑规则的详细信息，请参阅第 23-95 页上的修改现有规则。

要将注释添加到规则，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在其他策略中有未保存的更改，请点击 **OK** 废弃这些更改并继续操作。有关保存其他策略中未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击 **Rules**。

系统将显示 Rules 页面。

步骤 4　查找要在其中向规则添加注释的一条或多条规则。您有以下选项：

- 要对当前显示排序，请点击列标题或图标。要反向排序，请再次点击。
- 点击左侧过滤器面板中的关键字或参数构造过滤器。有关详细信息，请参阅以下主题：第 20-9 页上的了解入侵策略中的规则过滤和第 20-16 页上的在入侵策略中设置规则过滤器。

  页面将刷新，显示所有匹配的规则。

步骤 5　选择要在其中添加注释的一条或多条规则：

- 要选择具体规则，请选择该规则旁边的复选框。
- 要选择当前列表中的所有规则，请选择列顶部的复选框。

步骤 6　选择 **Comments > Add Rule Comment**。

系统将显示 Add Comment 对话框。

步骤 7　在 **Comment** 字段中，键入规则注释。

步骤 8　点击 **OK**。

系统将添加注释并在 Comments 列中该规则旁边显示注释图标 ( )。如果向规则中添加多个注释，图标上的数字表示注释的数量。

提示　要删除规则注释，请突出显示该规则并点击 **Show Details**，然后点击 **Comment** 部分中的 **Delete**。请注意，仅当缓存的注释具有未提交的入侵策略更改时，才能删除该注释。提交入侵策略更改之后，规则注释即是永久性的。

步骤 9　保存策略，继续编辑，废弃更改，或者退出并在系统缓存中保留更改。

有关详细信息，请参阅第 19-3 页上的管理入侵策略和第 19-4 页上的编辑入侵策略。

检测特定威胁

您可以在网络分析策略中使用若干预处理器检测对受监控网络的具体威胁（例如，后洞攻击、若干端口扫描类型和尝试通过大量流量淹没网络的基于速率的攻击）。请注意，当入侵规则或规则参数要求禁用的预处理器时，尽管预处理器在网络分析策略用户界面中保持禁用状态，系统还会自动使用其当前设置。有关详细信息，请参阅第 11-9 页上的自定义策略的限制。

您还可以使用在入侵规则中配置的敏感数据检测来检测以非安全方式传输的敏感数字数据。

有关检测具体威胁的详细信息，请参阅：

- 第 21-1 页上的检测 Back Orifice 说明了 Back Orifice 攻击检测。
- 第 21-2 页上的检测端口扫描介绍不同类型的端口扫描并说明如何在威胁发展成攻击之前使用端口扫描检测来识别网络威胁。
- 第 21-8 页上的防御基于速率的攻击说明如何限制拒绝服务 (DoS) 和 SYN 泛洪攻击。
- 第 21-17 页上的检测敏感数据说明如何在 ASCII 文本中检测和生成关于敏感数据 （例如，信用卡号和社会保障号码）的事件。

检测 Back Orifice

许可证：保护

ASA FirePOWER 模块提供了一种检测是否存在 Back Orifice 程序的预处理器。此程序可用于获取对 Windows 主机的管理员访问权限。Back Orifice 预处理器为 Back Orifice 神奇 cookie "`*!*QWTY?`"（位于数据包的前八个字节且使用 XOR 加密）分析 UDP 流量。

Back Orifice 预处理器具有配置页面，但没有配置选项。如果启用此预处理器，还必须为其启用下表中的预处理器规则，以生成相应的事件。有关详情，请参见第 20-17 页上的设置规则状态。

表 21-1 Back Orifice GID:SIDs

预处理器规则 GID:SID	说明
105:1	检测到 Back Orifice 流量
105:2	检测到 Back Orifice 客户端流量
105:3	检测到 Back Orifice 服务器流量
105:4	检测到 Back Orifice snort 缓冲区攻击

要查看 Back Orifice Detection 页面，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 **Specific Threat Detection** 下的 **Back Orifice Detection**：

- 如果已启用预处理器，请点击 **Edit**。
- 如果已禁用预处理器，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Back Orifice Detection 页面。页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

检测端口扫描

许可证：保护

端口扫描是一种通常被攻击者用作攻击前奏的网络侦察形式。在端口扫描中，攻击者将特制的数据包发送到目标主机。通过检查主机响应时所用的数据包，攻击者通常可以直接或通过推理确定主机上的哪些端口是开放的，以及哪种应用协议正在这些端口上运行。

请注意，当启用端口扫描检测时，必须在入侵策略 Rules 页面上为启用的端口扫描类型启用生成器 ID (GID) 为 122 的规则，以便端口扫描检测器可以生成端口扫描事件。有关详细信息，请参阅第 20-17 页上的设置规则状态和第 21-7 页上的表 21-5。

端口扫描本身不算是攻击。事实上，攻击者使用的一些端口扫描技术也可能会被网络上的合法用户使用。思科的端口扫描检测器旨在通过检测活动模式来帮助确定哪些端口扫描可能是恶意的。

攻击者可能会使用多种方法来探测网络。他们通常使用不同的协议从目标主机获取不同的响应，以期即使某一种协议被阻止，也可以使用另一种。下表介绍了可在端口扫描检测器中激活的协议。

表 21-2　协议类型

协议	说明
TCP	检测 TCP 探针，例如 SYN 扫描、 ACK 扫描、 TCP connect() 扫描和带异常标志组合（如 Xmas tree、 FIN 和 NULL）的扫描
UDP	检测 UDP 探针，如零字节 UDP 数据包
ICMP	检测 ICMP 回应请求 (ping)
IP	检测 IP 协议扫描。这些扫描与 TCP 和 UDP 扫描不同，因为攻击者不是查找开放端口，而是尝试去发现目标主机支持哪些 IP 协议。

注 对于端口扫描连接检测器生成的事件，协议号设置为 255。由于默认情况下端口扫描没有特定协议与之关联，因此，互联网编号分配机构 (IANA) 未将协议号分配给它。IANA 指定 255 作为保留号码，因此，该号码用于端口扫描事件中以指明事件没有关联的协议。

根据目标主机的数量、扫描主机的数量和扫描的端口数量，端口扫描通常分为四种类型。下表介绍了可检测的端口扫描活动的类型。

表 21-3　端口扫描类型

类型	说明
端口扫描检测	一对一端口扫描，在这种扫描中，攻击者使用一个或几个主机扫描单个目标主机上的多个端口。 一对一端口扫描具有如下特征： • 扫描主机的数量少 • 扫描单个主机 • 扫描的端口数量多 此选项检测 TCP、 UDP 和 IP 端口扫描。
端口清扫	一对多端口清扫，在这种扫描中，攻击者使用一个或几个主机扫描多个目标主机上的单个端口。 端口清扫具有如下特征： • 扫描主机的数量少 • 扫描的主机数量多 • 扫描的唯一端口数量少 此选项检测 TCP、 UDP、 ICMP 和 IP 端口清扫。

表 21-3　端口扫描类型（续）

类型	说明
诱骗端口扫描	一对一端口扫描，在这种攻击中，攻击者将伪造的源 IP 地址与真实的扫描 IP 地址混合在一起。 诱骗端口扫描具有如下特征： • 扫描主机的数量多 • 一次扫描的端口数量少 • 扫描的主机为一个（或数量少） 诱骗端口扫描选项检测 TCP、 UDP 和 IP 协议端口扫描。
分布式端口扫描	多对一端口扫描，在这种攻击中，多个主机查询单个主机是否有开放端口。 分布式端口扫描具有如下特征： • 扫描主机的数量多 • 一次扫描的端口数量多 • 扫描的主机为一个（或数量少） 分布式端口扫描选项检测 TCP、 UDP 和 IP 协议端口扫描。

端口扫描检测器所了解的关于探针的信息主要是基于查看探测主机的否定响应。例如，当网络客户端尝试连接到网络服务器时，客户端会使用端口 80/tcp 且可以依靠服务器将该端口打开。但是，当攻击者探测服务器时，攻击者事先并不知道该服务器是否提供网络 服务。当端口扫描检测器得到否定响应（即，无法访问 ICMP 或 TCP RST 数据包）时，它会将响应记录为潜在的端口扫描。当目标主机位于设备（例如，过滤否定响应的防火墙或路由器）的另一端，这个过程更难以执行。在这种情况下，端口扫描检测器可以根据选择的灵敏度级别生成*已过滤*端口扫描事件。

下表介绍了可选择的三种不同的灵敏度级别。

表 21-4　灵敏度级别

功率水平	说明
低	只检测目标主机的否定响应。选择此级别的灵敏度可抑制误报，但请记住，这样可能会遗漏某些类型的端口扫描（慢速扫描、过滤扫描）。 此级别使用最短的时间周期进行端口扫描检测。
中	根据主机的连接数量检测端口扫描，这意味着，可以检测过滤的端口扫描。但是，非常活跃的主机（例如网络地址转换器和代理）可能会生成误报。 请注意，可以将这些活跃主机的 IP 地址添加到 **Ignore Scanned** 字段以减少此类误报。 此级别使用较长的时间周期进行端口扫描检测。
高	根据时间周期侦测端口扫描，这意味着，可以检测基于时间的端口扫描。但是，如果使用此选项，应通过在 **Ignore Scanned** 和 **Ignore Scanner** 字段中指定 IP 地址，随时间小心地调整检测器。 此级别使用更长的时间周期进行端口扫描检测。

有关详细信息，请参阅：

- 第 21-5 页上的配置端口扫描检测
- 第 21-7 页上的了解端口扫描事件

配置端口扫描检测

许可证：保护

端口扫描检测配置选项可用于精细调整端口扫描检测器如何报告扫描活动。

请注意，当启用端口扫描检测时，必须在 Rules 页面上为启用的端口扫描类型启用生成器 ID (GID) 为 122 的规则，以便端口扫描检测器生成端口扫描事件。有关详细信息，请参阅第 20-17 页上的设置规则状态和端口扫描检测 SID (GID:122)表。

要配置端口扫描检测，请执行以下操作：

管理员/入侵管理员

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存在另一策略中未保存的信息，请参见[曾是“确认入侵策略更改”；更新 xref]。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 **Specific Threat Detection** 下的 **Portscan Detection**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

  系统将显示 Portscan Detection 页面。页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　在 **Protocol** 字段中，指定要启用以下哪些协议：

- TCP
- UDP
- ICMP
- IP

按住 Ctrl 或 Shift 键的同时点击可选择多个协议或清除单个协议。有关详细信息，请参阅协议类型表。

请注意，必须确保已启用 TCP 数据流处理以在 TCP 上检测扫描，并且确保已启用 UDP 流处理以在 UDP 上检测扫描。

步骤 10　在 **Scan Type** 字段中，指定要检测以下哪些端口扫描：

- 端口扫描检测
- 端口清扫
- 诱骗端口扫描
- 分布式端口扫描

按住 Ctrl 或 Shift 键的同时点击可选择或取消选择多个协议。有关详细信息，请参阅端口扫描类型表。

步骤 11　在 **Sensitivity Level** 列表中，选择要使用的级别：低、中或高。

有关详细信息，请参阅灵敏度级别表。

步骤 12　或者，在 **Watch IP** 字段中，指定要监视哪个主机的端口扫描活动标志，或者将字段留空以监视所有网络流量。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。有关使用 IPv4 和 IPv6 地址块的信息，请参阅第 1-3 页上的 IP 地址约定。

步骤 13　或者，在 **Ignore Scanners** 字段中，指定要作为扫描器而忽略的主机。可使用此字段指示在网络上特别活跃的主机。可能需要随时间修改此主机列表。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。有关使用 IPv4 和 IPv6 地址块的信息，请参阅第 1-3 页上的 IP 地址约定。

步骤 14　或者，在 **Ignore Scanned** 字段中，指定要作为扫描目标而忽略的主机。可使用此字段指示在网络上特别活跃的主机。可能需要随时间修改此主机列表。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。有关使用 IPv4 和 IPv6 地址块的信息，请参阅第 1-3 页上的 IP 地址约定。

步骤 15　或者，清除 **Detect Ack Scans** 复选框以停止监视在中途恢复的会话。

注　检测中途会话有助于识别 ACK 扫描，但可能会导致错误事件，特别是在含大流量和丢弃数据包的网络中。

步骤 16　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

了解端口扫描事件

许可证：保护

当启用端口扫描检测时，必须启用生成器 ID (GID) 为 122 且 Snort® ID (SID) 为 1 至 27 的规则，从而为每种启用的端口扫描类型生成事件。有关详情，请参见第 20-17 页上的设置规则状态。下表中的 **Preprocessor Rule SID** 列列出了必须为每种端口扫描类型启用的预处理器规则的 SID。

表 21-5　　端口扫描检测 SID (GID:122)

端口扫描类型	协议:	灵敏度级别	预处理器规则 SID
端口扫描检测	TCP	低	1
		中或高	5
	UDP	低	17
		中或高	21
	ICMP	低	不生成事件。
		中或高	不生成事件。
	IP	低	9
		中或高	13
端口清扫	TCP	低	3, 27
		中或高	7
	UDP	低	19
		中或高	23
	ICMP	低	25
		中或高	26
	IP	低	11
		中或高	15
诱骗端口扫描	TCP	低	2
		中或高	6
	UDP	低	18
		中或高	22
	ICMP	低	不生成事件。
		中或高	不生成事件。
	IP	低	10
		中或高	14
分布式端口扫描	TCP	低	4
		中或高	8
	UDP	低	20
		中或高	24
	ICMP	低	不生成事件。
		中或高	不生成事件。
	IP	低	12
		中或高	16

启用随附的预处理器规则后，端口扫描检测器会生成入侵事件，可以像任何其他事件一样进行查看。但是，数据包视图上显示的信息不同于其他类型的入侵事件。本节介绍了端口扫描事件的数据包视图上显示的字段，以及如何使用这些信息来了解网络中发生的探测的类型。

首先使用入侵事件视图钻取到端口扫描事件的数据包视图。

请注意，不能下载端口扫描数据包，因为单个端口扫描事件是基于多个数据包；但是，端口扫描数据包视图提供了所有可用的数据包信息。

注　对于端口扫描连接检测器生成的事件，协议号设置为 255。由于默认情况下端口扫描没有特定协议与之关联，因此，互联网编号分配机构 (IANA) 未将协议号分配给它。IANA 指定 255 作为保留号码，因此，该号码用于端口扫描事件中以指明事件没有关联的协议。

下表介绍了端口扫描事件的数据包视图中提供的信息。

表 21-6　端口扫描数据包视图

信息	说明
设备	检测事件的设备。
时间	事件发生的时间。
通信	预处理器生成的事件消息。
源 IP：	扫描主机的 IP 地址。
目标 IP：	被扫描主机的 IP 地址。
Priority Count	被扫描主机发出的否定响应（例如，TCP RST 和 ICMP unreachable）的数量。否定响应的数量越多，优先级计数就越高。
Connection Count	主机上的活动连接数量。此值对于基于连接的扫描（例如 TCP 和 IP）而言更准确。
IP Count	与被扫描主机联系的 IP 地址变化的次数。例如，如果第一个 IP 地址是 10.1.1.1，第二个 IP 是 10.1.1.2，第三 IP 是 10.1.1.1，那么 IP 计数为 3。 此数字对于活跃的主机（例如代理和 DNS 服务器）而言不太准确。
Scanner/Scanned IP Range	被扫描主机或扫描主机的 IP 地址范围，具体取决于扫描类型。对于端口清扫，此字段显示被扫描主机的 IP 范围。对于端口扫描，此字段显示扫描主机的 IP 范围。
Port/Proto Count	对于 TCP 和 UDP 端口扫描，是指正被扫描的端口变化的次数。例如，如果扫描的第一个端口是 80，扫描的第二个端口是 8080，扫描的第三个端口又是 80，那么端口计数为 3。 对于 IP 协议端口扫描，是指正用于连接至被扫描主机的协议变化的次数。
Port/Proto Range	对于 TCP 和 UDP 端口扫描，是指被扫描端口的范围。 对于 IP 协议端口扫描，是指已用于尝试连接至扫描的主机的 IP 协议号的范围。
Open Ports	在被扫描主机上打开的 TCP 端口。此字段仅在端口扫描检测到一个或多个开放端口时显示。

防御基于速率的攻击

许可证：保护

基于速率的攻击是取决于连接频率或攻击实施重复次数的攻击。可以使用基于速率的检测标准检测发生的基于速率的攻击，采取应对措施，在攻击停止后返回到常规检测设置。有关配置基于速率的检测的详细信息，请参阅：

- 第 21-9 页上的了解基于速率的攻击防御
- 第 21-11 页上的基于速率的攻击防御及其他过滤器
- 第 21-15 页上的配置基于速率的攻击防御

- 第 20-25 页上的了解动态规则状态
- 第 20-26 页上的设置动态规则状态

了解基于速率的攻击防御

许可证：保护

可以将网络分析策略配置为包括基于速率的过滤器，这种过滤器可检测针对网络中主机的过多活动。可以在内联模式下部署的设备上使用此功能，以在指定时间内阻止基于速率的攻击，然后恢复为仅生成事件且不丢弃流量。

基于速率的攻击防御可确定异常流量模式，并可将这些流量对合法请求的影响降至最低。基于速率的攻击通常具有以下其中一种特征：

- 任何包含与网络主机之间过多不完整连接的流量，表示 SYN 泛洪攻击

  要配置 SYN 攻击检测，请参阅第 21-10 页上的防御 SYN 攻击。
- 任何包含与网络主机之间过多完整连接的流量，表示 TCP/IP 泛洪攻击

  要配置并发连接检测，请参阅第 21-11 页上的控制同步连接。
- 在流向特定目标 IP 地址或来自特定源 IP 地址的流量中规则匹配过多。

  要配置基于源或目标的动态规则状态，请参阅第 20-26 页上的设置动态规则状态。
- 所有流量中某个特定规则的匹配过多。

  要配置基于规则的动态规则状态，请参阅第 20-26 页上的设置动态规则状态。

在网络分析策略中，您可以为整个策略配置 SYN 泛洪或 TCP/IP 连接泛洪检测；在入侵策略中，您可以为单独的入侵或预处理器规则设置基于速率的过滤器。请注意，手动向规则 135:1 和 135:2 添加基于速率的过滤器是无效的。 GID:135 的规则使用客户端作为源值，使用服务器作为目标值。有关详细信息，请参阅第 21-10 页上的防御 SYN 攻击和第 21-11 页上的控制同步连接。

每个基于速率的过滤器都包含下列几个组成部分：

- 网络地址名称（适用于整个策略或基于规则的源或目标设置）
- 规则的匹配速率，配置为特定秒数内的规则匹配项数量
- 超过该速率时要执行的新操作

  为整个策略设定基于速率的设置时，系统会在其检测到基于速率的攻击时生成事件，或者也可以在内联部署中丢弃流量。为具体规则设置基于速率的操作时，有三个可用的操作：Generate Events、 Drop and Generate Event 和 Disable。
- 操作的持续时间，配置为超时值

请注意，新操作自开始之后，在到达超时时间之前会一直执行，即使速率在这段时间内降到配置的速率以下亦不会停止。当超时周期结束后，如果速率低于阈值，则规则的操作会恢复到最初为该规则配置的操作。对于整个策略的设置，操作会恢复到流量匹配的每个规则的操作；如果不匹配任何规则，操作会停止。

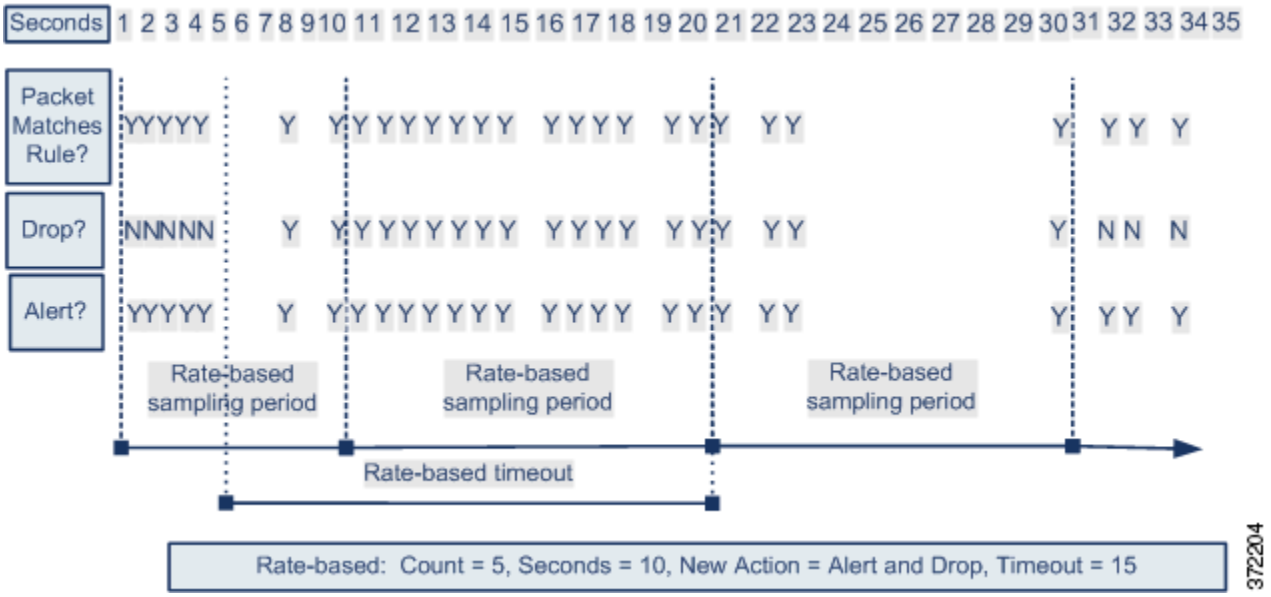
在内联部署中，可以将基于速率的攻击防御临时或永久配置为拦截攻击。在没有基于速率的配置的情况下，设置为 Generate Events 的规则会创建事件，但系统不会丢弃这些规则的数据包。但是，如果攻击流量所匹配的规则配置了基于速率的条件，则基于速率的操作可能会导致系统在该操作处于活动状态的时间内丢弃数据包，即便这些规则最初并未设置为 Drop and Generate Events。

注　基于速率的操作无法启用禁用的规则，也无法丢弃与禁用的规则匹配的流量。但是，如果在策略级别设置基于速率的过滤器，则可以在指定时段内生成事件或生成事件并丢弃包含过多 SYN 数据包或 SYN/ACK 交互的流量。

可以对同一规则定义多个基于速率的过滤器。入侵策略中列出的第一个过滤器优先级最高。请注意，当两个基于速率的过滤器操作相冲突时，系统会实施第一个基于速率的过滤器的操作。同样，如果对整个策略设置的基于速率的过滤器与对具体规则设置的基于速率的过滤器相冲突，前者优先。

下图显示的例子中，攻击者正在尝试访问主机。反复尝试查找密码触发了配置有基于速率的攻击防御的规则。当在 10 秒的时间跨度内发生五次规则匹配之后，基于速率的设置会将规则属性更改为 Drop and Generate Events。新的规则属性在 15 秒之后超时。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样速率高于当前或前一个采样周期的阈值，新操作将继续。只有在采样周期完毕而采样速率低于阈值速率之后，新操作才会恢复为生成事件。



防御 SYN 攻击

许可证：保护

SYN 攻击防御选项有助于保护网络主机免受 SYN 泛洪攻击。可以根据在一段时间内看到的数据包数量保护单个主机或整个网络。如果设备采用被动部署，可以生成事件。如果设备采用内联部署，还可以丢弃恶意数据包。超时周期结束后，如果速率条件已停止，将会停止事件生成和数据包丢弃。

例如，可以配置一项设置以允许任一 IP 地址发出最多 10 个 SYN 数据包，并连续 60 秒阻止来自该 IP 地址的进一步连接。

启用此选项还会激活规则 135:1。手动激活此规则是无效的。规则状态始终显示为 Disabled，不会改变。如果此选项已启用且超过定义的速率条件，规则会生成事件。

控制同步连接

许可证：保护

可以限制与网路上主机之间的 TCP/IP 连接，以防止拒绝服务 (DoS) 攻击或用户进行过多活动。当系统检测到与指定 IP 地址成功连接的配置数量或地址范围时，它会对额外连接生成事件。基于速率的事件生成继续进行，直到超时周期结束且未发生速率条件。在内联部署中，可以选择丢弃数据包，直到速率条件超时。

例如，可以配置一项设置以允许任一 IP 地址发出最多 10 个成功的同步连接，并连续 60 秒阻止来自该 IP 地址的进一步连接。

启用此选项还会激活规则 135:2。手动激活此规则是无效的。规则状态始终显示为 Disabled，不会改变。如果此选项已启用且超过定义的速率条件，规则会生成事件。

基于速率的攻击防御及其他过滤器

许可证：保护

关键字 `detection_filter`、阈值和抑制功能提供了其他方式来过滤流量或系统生成的事件。可以单独使用基于速率的攻击防御，也可以将其与阈值、抑制功能或 `detection_filter` 关键字随意组合使用。

有关详细信息，请参阅：

- 第 21-11 页上的基于速率的攻击防御和检测过滤
- 第 21-12 页上的动态规则状态和阈值或抑制
- 第 21-13 页上的整个策略基于速率的检测和阈值或抑制
- 第 21-14 页上的使用多种过滤方法进行基于速率的检测

基于速率的攻击防御和检测过滤

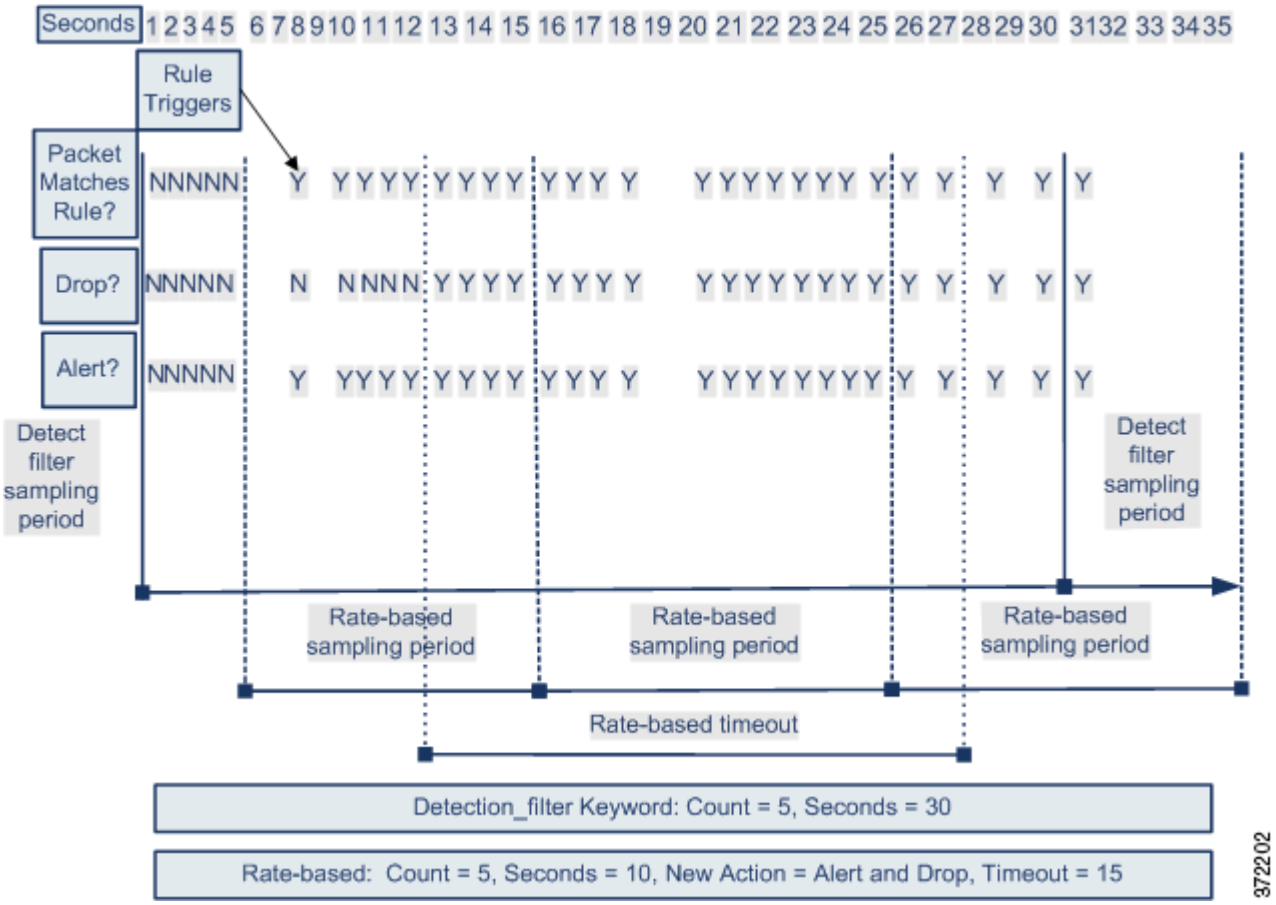
许可证：保护

关键字 `detection_filter` 可防止触发规则，直到指定时间内出现规则匹配的阈值次数。当规则包含 `detection_filter` 关键字时，系统会在每个超时周期跟踪传入数据包与规则中的模式相匹配的次数。系统可以从特定的源或目标 IP 地址计算该规则的匹配次数。速率超过规则中的速率后，会开始针对该规则的事件通知。

以下示例显示了尝试强行登录的攻击者。重复尝试查找密码会触发还包含 `detection_filter` 关键字且计数设置为 5 的规则。此规则已配置基于速率的攻击防御。如果在 10 秒内出现五次规则匹配，基于速率的设置会将规则属性更改为 Drop and Generate Events 并保持 20 秒。

如图所示，与规则匹配的前五个数据包不会生成事件，因为在速率超过 `detection_filter` 关键字所指示的速率之前规则不会触发。规则触发后，事件通知开始，但基于速率的标准在再通过五个数据包之前不会触发新操作 Drop and Generate Events。

如果符合基于速率的标准，将会生成事件并会丢弃数据包，直到基于速率的超时周期结束且速率低于阈值。 20 秒之后，基于速率的操作超时。请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。由于采样的速率高于之前采样周期的阈值速率，因此发生超时时，基于速率的操作会继续。



请注意，虽然示例未进行描述，但可以将 Drop and Generate Events 规则状态与 `detection_filter` 关键字结合使用，以在规则的匹配速率达到指定速率时开始丢弃流量。确定是否为规则配置基于速率的设置时，请考虑将规则设置为 Drop and Generate Events 和包含 `detection_filter` 关键字是否会获得相同的结果，或者是否要在入侵策略中管理速率和超时设置。有关详细信息，请参阅第 20-17 页上的设置规则状态。

动态规则状态和阈值或抑制

许可证：保护

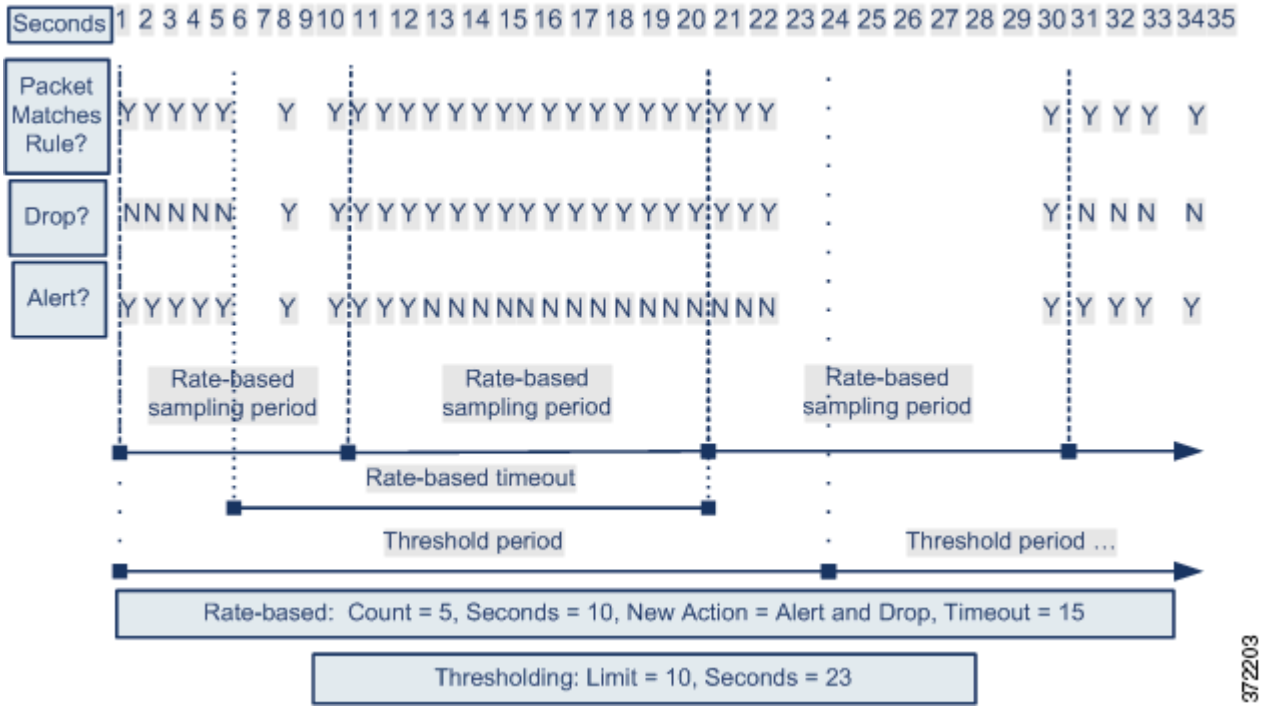
可以使用阈值和抑制功能来减少过多的事件，具体做法是，限制某一规则的事件通知数量或抑制该规则的所有通知。有关阈值和抑制功能的可用选项的详细信息，请参阅第 20-19 页上的配置事件阈值和第 20-23 页上的按入侵策略配置抑制。

如果将抑制功能应用于某一规则，系统会为所有适用的 IP 地址抑制该规则的事件通知，即使基于速率的操作发生变化。但是，阈值与基于速率的标准之间的交互更加复杂。

以下示例显示了尝试强行登录的攻击者。重复尝试查找密码会触发已配置基于速率的攻击防御的规则。如果在 10 秒内出现五次规则攻击，基于速率的设置会将规则属性更改为 Drop and Generate Events 并保持 15 秒。此外，极限阈值会在 23 秒内将规则可生成的事件数量限制为 10。

如图所示，规则为前五个匹配数据包生成事件。五个数据包之后，基于速率的标准会触发新操作 Drop and Generate Events，对于接下来的五个数据包，规则会生成事件且系统会丢弃数据包。第十个数据包之后，已达到极限阈值，因此，对于剩余的数据包，系统不会生成事件，但会丢弃数据包。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样的速率高于当前或之前采样周期的阈值速率，新操作将会继续。新操作只会在采样周期结束后恢复生成事件，在此情况下采样的速率低于阈值速率。



请注意，虽然本例中未显示，但如果在达到阈值*后*因基于速率的标准而触发新操作，系统会生成一个事件以指示操作变化。因此，例如，对于第 14 个数据包，如果达到极限阈值 10，系统停止生成事件且操作从 Generate Events 更改为 Drop and Generate Events，系统会生成第十一个事件以指示操作变化。

整个策略基于速率的检测和阈值或抑制

许可证：保护

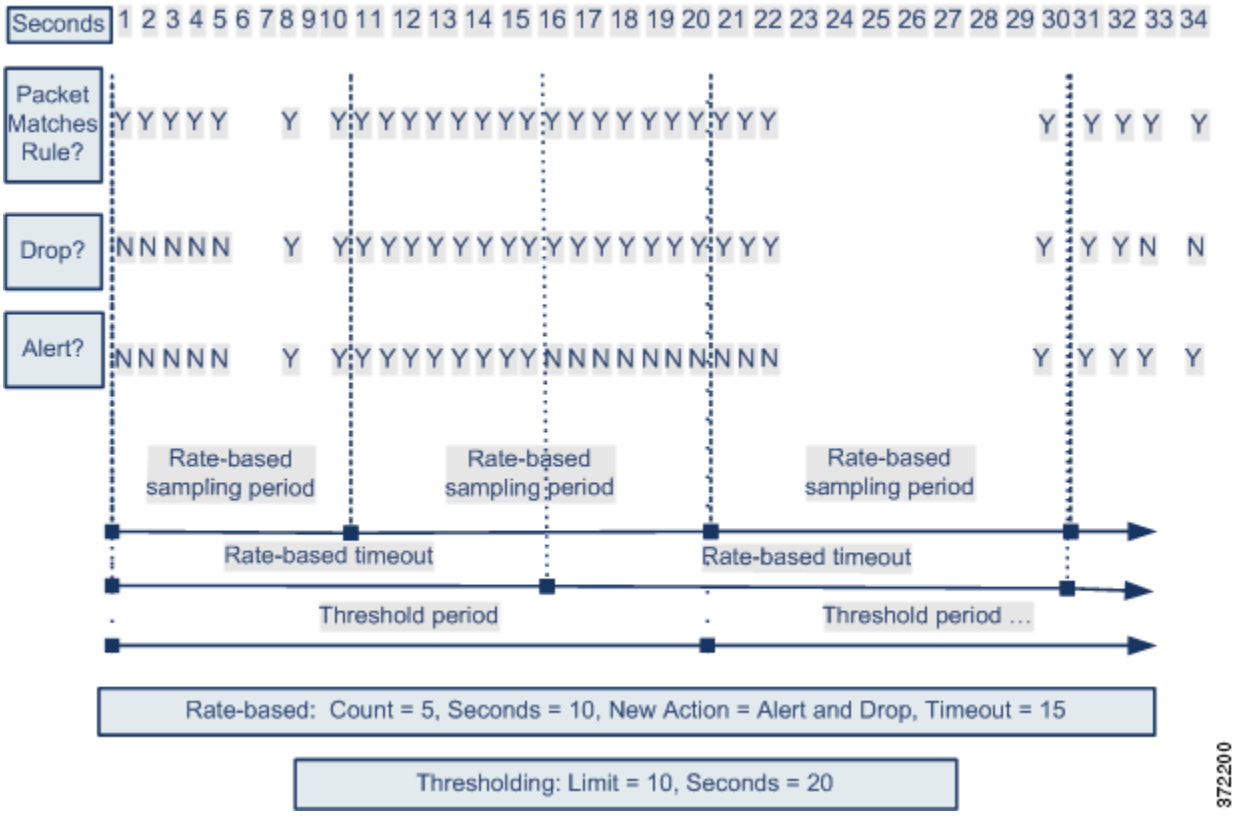
通过，可以使用阈值和抑制功能来减少过多的事件，具体做法是，限制源或目标的事件通知数量或者抑制该规则的所有通知。有关阈值和抑制功能的可用选项的详细信息，请参阅第 22-3 页上的配置全局阈值、第 20-19 页上的配置事件阈值和第 20-23 页上的按入侵策略配置抑制。

如果抑制功能应用于某一规则，系统会为所有适用的 IP 地址抑制该规则的事件通知，即使因整个策略或规则特定基于速率的设置而发生速率操作变化。但是，阈值与基于速率的标准之间的交互更加复杂。

以下示例显示了尝试对网络中的主机进行拒绝服务 (DoS) 攻击的攻击者。许多来自相同源的同步主机连接会触发整个策略的 Control Simultaneous Connections 设置。如果在 10 秒内一个源有五个连接，设置会生成事件并丢弃恶意流量。此外，全局极限阈值会在 20 秒内将所有规则或设置可生成的事件数量限制为 10。

如图所示，整个策略的设置会为前十个匹配数据包生成事件并丢弃流量。第十个数据包之后，已达到极限阈值，因此，对于剩余的数据包，不会生成事件，但会丢弃数据包。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样的速率高于当前或之前采样周期的阈值速率，生成事件和丢弃流量这两种基于速率的操作将会继续。基于速率的操作只在采样周期结束后停止，在此情况下采样的速率低于阈值速率。



请注意，虽然本例中未显示，但如果在达到阈值*后*因基于速率的标准而触发新操作，系统会生成一个事件以指示操作变化。因此，例如，对于第 14 个数据包，如果达到极限阈值 10，系统停止生成事件且操作更改为 Drop and Generate Events，系统会生成第十一个事件以指示操作变化。

使用多种过滤方法进行基于速率的检测

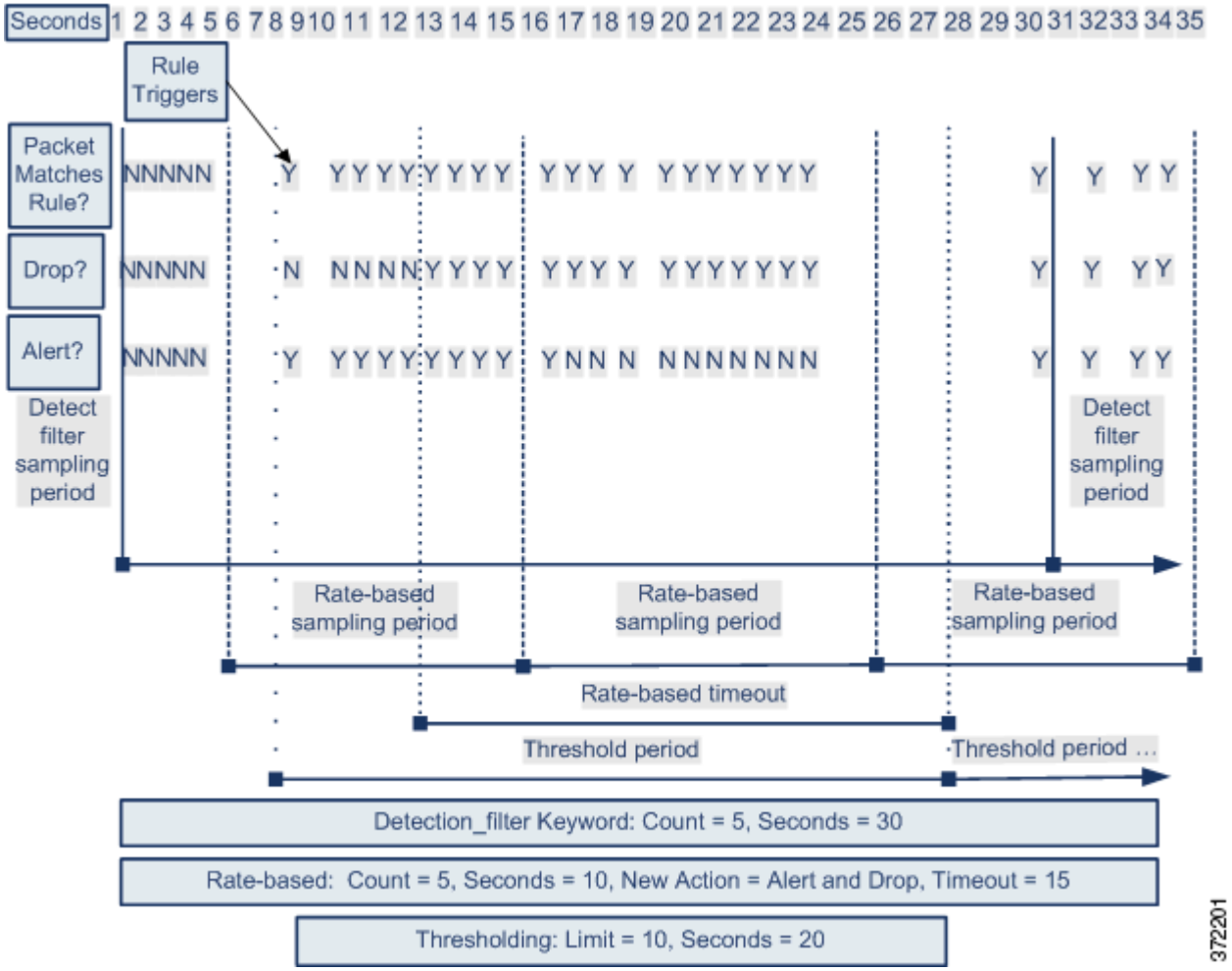
许可证：保护

可能会出现 `detection_filter` 关键字、阈值或抑制功能和基于速率的标准都适用于同一流量这种情况。为规则启用抑制功能后，系统会为指定 IP 地址抑制事件，即使发生基于速率的变化。

以下示例显示了尝试强行登录的攻击者，并描述了 `detection_filter` 关键字、基于速率的过滤和阈值功能交互的情况。重复尝试查找密码会触发包括 `detection_filter` 关键字且计数设置为 5 的规则。此规则还具有基于速率的攻击防御设置，如果在 15 秒内出现五次规则匹配，该设置会将规则属性更改为 Drop and Generate Events 并保持 30 秒。此外，极限阈值会在 30 秒内将规则限为 10 个事件。

如图所示，与规则匹配的前五个数据包不会产生事件通知，因为在速率超过 `detection_filter` 关键字所指示的速率之前规则不会触发。规则触发后，事件通知开始，但基于速率的标准在再通过五个数据包之前不会触发新操作 Drop and Generate Events。如果符合基于速率的标准，系统会为数据包 11 至 15 生成事件并丢弃数据包。第十五个数据包之后，已达到极限阈值，因此，对于剩余的数据包，系统不会生成事件，但会丢弃数据包。

请注意，基于速率的超时后，数据包仍会在随后的基于速率的采样周期内丢弃。因为采样的速率高于之前采样周期的阈值速率，新操作将会继续。



配置基于速率的攻击防御

许可证：保护

可以在策略级别配置基于速率的攻击防御以阻止 SYN 泛洪攻击，也可以阻止来自特定源或到达特定目标的过多连接。

要配置基于速率的攻击防御，请执行以下操作：

管理员/入侵管理员

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要编辑的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 **Advanced** 选项卡。

系统将显示访问控制策略高级设置页面。

步骤 4　点击 **Network Analysis and Intrusion Policies** 旁边的编辑图标 ( )。

系统将显示 Network Analysis and Intrusion Policies 弹出窗口。

步骤 5　点击 **Network Analysis Policy List**。

系统将显示 Network Analysis Policy List 弹出窗口。

步骤 6　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 7　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 8　您有两种选择，具体取决于是否启用了 **Specific Threat Detection** 下的 **Rate-Based Attack Prevention**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Rate-Based Attack Prevention 页面。页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 9　此时您有两种选择：

- 要防止旨在对主机发起泛洪攻击的不完整连接，请点击 **SYN Attack Prevention** 下的 **Add**。

  系统将显示 SYN Attack Prevention 对话框。
- 要防止过多连接，请点击 **Control Simultaneous Connections** 下的 **Add**。

  系统将显示 Control Simultaneous Connections 对话框。

步骤 10　选择要跟踪流量的方式：

- 要跟踪来自特定源或一系列源的所有流量，请从 **Track By** 下拉列表选择 **Source**，然后在 **Network** 字段中输入单个 IP 地址或地址块。
- 要跟踪到达特定目标或一系列目标的所有流量，请从 **Track By** 下拉列表选择 **Destination**，然后在 **Network** 字段中输入单个 IP 地址或地址块。

请注意，系统会单独跟踪 Network 字段中包含的每个 IP 地址的流量。来自超过所配置速率的 IP 地址的流量会带来仅为该 IP 地址生成的事件。例如，进行网络设置时，可将源 CIDR 块设置为 `10.1.0.0/16` 并将系统配置为在有十个同步连接打开时生成事件。如果 10.1.4.21 有八个连接打开，10.1.5.10 有六个连接打开，则系统不会生成事件，因为这两个源地址的打开连接均未达到触发数量。但是，如果 10.1.4.21 有十一个同步连接打开，系统只会为来自 10.1.4.21 的连接生成事件。

有关使用 CIDR 表示法和前缀长度的信息，请参阅第 1-3 页上的 IP 地址约定。

步骤 11　指示速率跟踪设置的触发速率：

- 对于 SYN 攻击配置，在 **Rate** 字段中指明每个秒数的 SYN 数据包数量。
- 对于并发连接配置，在 **Count** 字段中指示连接数量。

步骤 12　要丢弃与基于速率的攻击防御设置匹配的数据包，请选择 **Drop**。

步骤 13　在 **Timeout** 字段中指定时间段，在该时间段结束后将会停止生成事件和丢弃流量（如适用，针对具有 SYN 的匹配模式或同步连接的流量）。

注意事项　超时值可以是 1 至 1,000,000 之间的任意整数。但是，设置较高的超时值可能会完全阻止连接至内联部署中的某个主机。

步骤 14　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

检测敏感数据

许可证：保护

敏感数据（如社会保障号码、信用卡号码、驾驶证号码等）可能会被有意或无意地在互联网上泄露。系统提供的敏感数据预处理程序能够检测 ASCII 文本中的敏感数据并为之生成事件，此功能对于检测意外数据泄露特别有用。

系统不会检测经过加密的或模糊的敏感数据，也不会检测压缩或编码格式（例如 Base64 编码邮件附件）的敏感数据。例如，系统会检测电话号码 (555)123-4567，但不会检测该号码经过模糊处理的版本（即，每个数字用空格分开，例如 (5 5 5) 1 2 3 - 4 5 6 7，或者通过 HTML 代码介入，例如 (555)-123-4567）。但是，系统会检测采用 HTML 代码的号码 (555)-123-4567，在该号码中，没有介入代码中断编号模式。

提示　敏感数据预处理器可以检测使用 FTP 或 HTTP 上传和下载的未加密 Microsoft Word 文件中的敏感数据；之所以可以这样，大概是因为 Word 文件单独分组 ASCII 文本和格式命令的方式。

系统通过将各个数据类型与流量进行比对来检测每个 TCP 会话中的敏感数据。可以为每种数据类型和适用于入侵策略中所有数据类型的全局选项修改默认设置。思科提供了常用的预定义数据类型。您也可以创建自定义数据类型。

敏感数据预处理程序规则与每种数据类型相关联。可通过为数据类型启用相应的预处理器，为每种数据类型启用敏感数据检测和事件生成。配置页面上的链接会将您指向 Rules 页面上的敏感数据规则的过滤视图，可以在其中启用和禁用规则以及配置其他规则属性。

保存对入侵策略所做的更改时，如果与数据类型关联的规则已启用且敏感数据检测已禁用，可以选择自动启用敏感数据预处理器。

有关详细信息，请参阅：

- 第 21-18 页上的部署敏感数据检测
- 第 21-18 页上的选择全局敏感数据检测选项
- 第 21-19 页上的选择具体数据类型选项
- 第 21-20 页上的使用预定义数据类型
- 第 21-20 页上的配置敏感数据检测
- 第 21-22 页上的选择要监控的应用协议
- 第 21-23 页上的特殊情况：检测 FTP 流量中的敏感数据
- 第 21-23 页上的使用自定义数据类型

部署敏感数据检测

许可证：保护

由于敏感数据检测对 系统的性能具有较大影响，思科建议您遵循以下准则：

- 选择 No Rules Active 默认策略作为基本入侵策略；有关详细信息，请参阅第 12-3 页上的了解系统提供的基本策略。
- 确保在相应的网络分析策略中已启用以下设置：
  - **Application Layer Preprocessors** 下的 **FTP and Telnet Configuration**
  - **Transport/Network Layer Preprocessors** 下的 **IP Defragmentation** 和 **TCP Stream Configuration**。
- 将包括含敏感数据配置的入侵策略的访问控制策略应用于为敏感数据检测保留的设备；有关详细信息，请参阅第 4-10 页上的应用访问控制策略。

选择全局敏感数据检测选项

许可证：保护

全局敏感数据检测选项用于控制预处理器的工作方式。可以修改指定以下内容的全局选项：

- 预处理器是否在触发数据包中替换信用卡号或社会保障号的最后四位数
- 网络上的哪些目标主机监控敏感数据
- 单个会话中所有数据类型总共出现多少次会产生事件

请注意，全局敏感数据选项是特定于策略的并适用于所有数据类型。

您可以配置以下全局敏感数据检测选项。

掩码

在触发数据包中用 X 替换信用卡号或社会保障号的最后四位数。掩码数字显示在用户界面中的入侵事件数据包视图中和下载的数据包中。

网络

指定监控敏感数据的目标主机。可以指定单个 IP 地址，地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。系统会将空白字段解读为 `any`，意指任何目标 IP 地址。有关使用 IPv4 和 IPv6 地址块的信息，请参阅第 1-3 页上的IP 地址约定。

Global Threshold

指定在生成全局阈值事件之前预处理器必须在任何组合中检测的单个会话中所有数据类型出现的总次数。可以指定 1 至 65535 之间的任意数字。

思科建议将此选项的值设置为大于在策略中启用的任何单个数据类型的最高阈值。有关详情，请参见第 21-19 页上的选择具体数据类型选项。

关于全局阈值，请注意：

- 必须启用预处理器规则 139:1 才能检测和生成关于数据类型出现次数的事件。有关在入侵策略中启用规则的详细信息，请参阅第 20-17 页上的设置规则状态。
- 在每个会话中，预处理器最多生成一个全局阈值事件。
- 全局阈值事件与具体数据类型事件无关；也就是说，预处理器会在达到全局阈值时生成事件，而不管任何具体数据类型的事件阈值是否达到，反之亦然。

选择具体数据类型选项

许可证：保护

具体数据类型确定了在指定目标网络流量中可以针对其进行检测并生成事件的敏感数据。可以为指定以下内容的数据类型选项修改默认设置：

- 某种检测到的数据类型必须达到才能生成单个会话事件的阈值
- 每种数据类型要监控的目标端口
- 每种数据类型要监控的应用协议

每种数据类型至少必须指定一个事件阈值和至少一个要监控的端口或应用协议。

由思科提供的每种预定义数据类型使用一种其他方法无法访问的 `sd_pattern` 关键字来定义用于在流量中进行检测的内置数据模式。有关预定义数据类型的列表，请参阅第 21-20 页上的表 21-8。您还可以创建自定义数据类型，然后可以使用简单的正则表达式为这些数据类型指定自己的数据模式。有关详情，请参见第 21-23 页上的使用自定义数据类型。

请注意，数据类型名称和模式适用于整个系统；所有其他数据类型选项适用于策略。

下表介绍了可配置的数据类型选项。

表 21-7　　具体数据类型选项

选项	说明
数据类型	显示数据类型的唯一名称。
阈值	指定系统生成事件时数据类型出现的次数。如果没有为启用的数据类型设置阈值，在保存策略时会收到一条错误消息。可以指定 1 至 255 之间的数字。 请注意，在每个会话中，预处理器为检测到的数据类型生成一个事件。另请注意，全局阈值事件与具体数据类型事件无关；也就是说，预处理器会在达到数据类型事件阈值时生成事件，而不管全局事件阈值是否达到，反之亦然。
目标端口	为数据类型指定要监控的目标端口。可以指定单个端口、端口的逗号分隔列表或 `any`（表示任何目标端口）。如果在没有为某种数据类型设置至少一个端口或应用协议的情况下为该数据类型启用了规则，在保存策略时会收到一条错误消息。
应用协议 请注意，此功能需要可控性许可证。	最多可以为数据类型指定八个要监控的应用协议。如果在没有为某种数据类型设置至少一个端口或应用协议的情况下为该数据类型启用了规则，在保存策略时会收到一条错误消息。 有关为数据类型选择应用协议的详细说明，请参阅第 21-22 页上的选择要监控的应用协议。
Pattern	对于自定义数据类型，这是指定的检测模式（思科提供的数据类型的数据模式已预先定义）。有关详情，请参见第 21-23 页上的使用自定义数据类型。用户界面不显示预定义数据类型的内置模式。 请注意，自定义和预定义的数据模式是针对整个系统的。

使用预定义数据类型

许可证：保护

每个入侵策略包括用于检测常用数据模式的预定义数据类型（如信用卡号、电子邮件地址、美国电话号码以及带或不带连字符的美国 社会安全保障号）。每种预定义数据类型都与一个生成器 ID (GID) 为 138 的敏感数据预处理器规则相关。必须启用入侵策略中的关联敏感数据规则才能为要用于策略中的每种数据类型启用检测和事件生成。有关在入侵策略中启用规则的详细信息，请参阅第 20-17 页上的设置规则状态。

为了帮助启用敏感数据规则，配置页面上的链接会将您指向 Rules 页面的过滤视图，其中显示所有预定义和自定义的敏感数据规则。您还可以在 Rules 页面上选择敏感数据规则过滤类别，从而只显示预定义的敏感数据规则。有关详情，请参见第 20-9 页上的过滤入侵策略中的规则。预定义的敏感数据规则还列于 Rule Editor 页面 (**Policies > Intrusion > Rule Editor**)，可在其中的敏感数据规则类别下查看这些规则，但不能进行编辑。

下表介绍了每种数据类型，并列出了必须启用才能为数据类型启用检测和事件生成的对应预处理器规则。

表 21-8　　敏感数据类型

数据类型	说明	预处理器规则 GID:SID
信用卡号	匹配 15 位和 16 位数字的 Visa®、 MasterCard®、 Discover® 和 American Express® 信用卡号 （无论是否带正常分隔破折号或空格）； 也可以使用 Luhn 算法来验证信用卡校验位。	138:2
邮件地址	匹配邮件地址。	138:5
美国 电话号码	匹配 符合 `(\d{3}) ?\d{3}-\d{4}` 模式的美国电话号码。	138:6
不带连字符的美国 社会安全保障号	匹配 具有有效的 3 位数区域号码、有效的 2 位数群组号码且不带连字符的 9 位数美国社会保障号。	138:4
带连字符的美国 社会安全保障号	匹配 具有有效的 3 位数区域号码、有效的 2 位数群组号码且带连字符的 9 位数美国社会保障号。	138:3
自定义	匹配指定流量中的用户定义数据模式。有关详情，请参见第 21-23 页上的使用自定义数据类型。	138:>999999

为了减少对社会保障号以外的 9 位数号码的误报，预处理器使用一种算法来验证 3 位数区域号码和 2 位数群组号码；在每个社会保障号中，这两组号码位于 4 位数序列号的前面。预处理器可验证 2009 年 11 月之前的社会保障号中的群组号码。

配置敏感数据检测

许可证：保护

可以修改默认全局设置和具体数据类型的设置。还必须为要检测的每种数据类型启用预处理器规则。

如果在策略中启用敏感数据预处理器规则而未启用敏感数据检测，在保存策略更改时，系统会提示启用敏感数据检测。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

下表介绍了可在 Sensitive Data Detection 页面采取的操作。

表 21-9　敏感数据配置操作

要.....	您可以.....
修改全局设置	有关可修改的全局设置的信息，请参阅第 21-8 页上的表 21-6。
修改数据类型选项	点击 Targets 页面区域中的数据类型名称。 Configuration 页面区域会进行更新以显示数据类型的当前设置。有关可修改的选项的详细信息，请参阅具体数据类型选项表。
为数据类型添加或删除要监控的应用协议 请注意，此功能需要可控性许可证。	在 **Application Protocols** 字段中点击，或点击字段旁边的 **Edit**。系统将显示 Application Protocols 弹出窗口： • 要添加要监控的应用协议（最多八个），请从左侧的 **Available** 列表中选择一个或多个应用协议，然后点击右箭头 (**>**) 按钮。 • 要删除应用协议，请从右侧的 **Enabled** 列表中选择，然后点击左箭头 (**<**) 按钮。 点击的同时使用 Ctrl 或 Shift 选择多个应用协议。您也可以点击并拖动鼠标，以选择多个相邻的应用协议。 **注**　要检测 FTP 流量中的敏感数据，必须添加 `Ftp 数据`应用协议。有关详情，请参见第 21-23 页上的特殊情况：检测 FTP 流量中的敏感数据。
创建自定义数据类型	在页面左侧点击 **Data Types** 旁边的 **+** 符号。系统将显示 Add Data Type 弹出窗口。 指定唯一的数据类型名称和要使用该数据类型检测的模式，然后点击 **OK**，或者点击 **Cancel** 放弃编辑。有关详情，请参见第 21-23 页上的使用自定义数据类型。
显示敏感数据预处理器规则	点击 Global Settings 页面区域上方的 **Configure Rules for Sensitive Data Detection** 链接。所有敏感数据预处理器规则的列表显示在 Rules 页面的过滤视图中。 或者，可以启用或禁用任何列出的规则。请注意，必须为要用于入侵策略中的每种数据类型启用敏感数据预处理器规则。有关详情，请参见第 20-17 页上的设置规则状态。 还可以为 Rules 页面上可用的任何其他操作（例如规则抑制、基于速率的攻击防御，等等）配置敏感数据规则；有关详细信息，请参阅第 20-1 页上的使用规则调整入侵策略。 点击 **Back** 返回到 Sensitive Data Detection 页面。

要配置敏感数据检测，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Advanced Settings**。

系统将显示 Advanced Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 **Specific Threat Detection** 下的 **Sensitive Data Detection**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Sensitive Data Detection 页面。页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 5　可以采取敏感数据配置操作表中所述的任何操作。

步骤 6　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

选择要监控的应用协议

许可证：可控性

最多可以为每种数据类型指定八个应用协议进行监控。

必须为每种数据类型至少指定一个要监控的应用协议或端口。但是，除了要检测 FTP 流量中的敏感数据的情况之外，思科建议在指定应用协议时指定相应的端口，以便实现最全面覆盖。例如，如果指定 HTTP，还可以配置通用的 HTTP 端口 80。如果网络上的新主机执行 HTTP，系统会在它发现新 HTTP 应用协议的时间间隔内监控端口 80。

在想要检测 FTP 流量中的敏感数据的情况下，您必须指定 FTP 数据应用协议；指定端口号没有好处。有关详情，请参见第 21-23 页上的特殊情况：检测 FTP 流量中的敏感数据。

要修改检测敏感数据的应用协议，请执行以下操作：

管理员/入侵管理员

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Advanced Settings**。

系统将显示 Advanced Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 **Specific Threat Detection** 下的 **Sensitive Data Detection**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Sensitive Data Detection 页面。

页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 5　点击 **Data Types** 下的数据类型名称并选择要修改的数据类型。

Configuration 页面会进行更新以显示选定数据类型的当前设置。

步骤 6　在 **Application Protocols** 字段中点击，或点击字段旁边的 **Edit**。

系统将显示 Application Protocols 弹出窗口。

步骤 7　您有两种选择：

- 要添加要监控的应用协议（最多八个），请从左侧的 **Available** 列表中选择一个或多个应用协议，然后点击右箭头 (**>**) 按钮。
- 要删除应用协议，请从右侧的 **Enabled** 列表中选择，然后点击左箭头 (**<**) 按钮。

点击的同时使用 Ctrl 或 Shift 选择多个应用协议。您也可以点击并拖动鼠标，以选择多个相邻的应用协议。

注　要检测 FTP 流量中的敏感数据，必须添加 FTP 数据应用协议。有关详情，请参见第 21-23 页上的特殊情况：检测 FTP 流量中的敏感数据。

步骤 8　点击 **OK** 以添加应用协议。

系统将显示 Sensitive Data Detection 页面且应用协议会进行更新。

特殊情况：检测 FTP 流量中的敏感数据

许可证：可控性

通常，可通过指定要监控的端口或在部署中指定应用协议来确定要监控敏感数据的流量。但是，对于检测 FTP 流量中的敏感数据来说，指定端口或应用协议并不足够。在 FTP 应用协议的流量中找到 FTP 流量中的敏感数据，这种情况间歇出现并使用临时端口号，因此难以检测。要检测 FTP 流量中的敏感数据，**必须**在配置中包括以下几项：

- 指定 FTP data 应用协议。

  指定 FTP data 应用协议可检测 FTP 流量中的敏感数据。有关详情，请参见第 21-22 页上的选择要监控的应用协议。

  对于检测 FTP 流量中的敏感数据这种特殊情况，指定 FTP data 应用协议不会调用检测功能；而是会调用 FTP/Telnet 预处理器的快速处理功能来检测 FTP 流量中的敏感数据。有关详情，请参见第 15-16 页上的解码 FTP 和 Telnet 流量。

- 确保配置包括至少一个要监控敏感数据的端口。

  请注意，不需要指定 FTP 端口 （只要检测 FTP 流量中的敏感数据这种罕见情况除外）。大多数敏感数据配置将包括其他端口 （例如 HTTP 或邮件端口）。如果只要指定一个 FTP 端口进行监控，思科建议指定 FTP 命令端口 23。有关详细信息，请参阅第 21-20 页上的配置敏感数据检测。

使用自定义数据类型

许可证：保护

可以创建和修改自定义数据类型以检测指定的数据模式。例如，医院可以创建一种数据类型来保护患者编号；再如，大学可以创建一种数据类型来检测具有唯一编号模式的学号。

创建的每种自定义数据类型还会创建一个敏感数据预处理器规则，该规则的生成器 ID (GID) 为 138，Snort ID 为大于或等于 1000000（也就是本地规则的 SID）。必须启用关联的敏感数据规则才能为要用于策略中的每种自定义数据类型启用检测和事件生成。有关在入侵策略中启用规则的详细信息，请参阅第 20-17 页上的设置规则状态。

为了帮助启用敏感数据规则，配置页面上的链接会将您指向 Rules 页面的过滤视图，其中显示所有预定义和自定义的敏感数据规则。您还可以通过在 Rules 页面上选择本地规则过滤类别，使自定义敏感数据规则与任何本地自定义规则一起显示。有关详情，请参见第 20-9 页上的过滤入侵策略中的规则。请注意，自定义敏感数据规则不会列于 Rule Editor 页面。

创建的自定义数据类型已添加到所有入侵策略。必须在要使用的任何策略中启用关联敏感数据规则，才能检测和生成特定自定义数据类型的事件。

请注意，必须使用 Sensitive Data Detection 配置页面才能创建数据类型及其关联的规则。不能使用规则编辑器创建敏感数据规则。

有关详细信息，请参阅：

- 第 21-24 页上的定义自定义数据类型的数据模式
- 第 21-25 页上的配置自定义数据类型
- 第 21-27 页上的编辑自定义数据类型名称和检测模式

定义自定义数据类型的数据模式

许可证：保护

可使用一组由以下部分组成的正则表达式来定义自定义数据类型的数据模式：

- 三个元字符
- 允许将元字符用作原义字符的转义字符
- 六个字符类

元字符是在正则表达式中具有特殊含义的原义字符。下表介绍了可在定义自定义数据模式时使用的元字符。

表 21-10　敏感数据模式元字符

元字符	说明	示例
?	匹配前面的字符或转义序列零次或一次；也就是说，前面的字符或转义序列是可选的。	colou?r 匹配 color 或 colour
{*n*}	匹配前面的字符或转义序列 *n* 次。	例如， \d{2} 匹配 55、 12 等； \l{3} 匹配 AbC、 www 等； \w{3} 匹配 a1B、 25C 等； x{5} 匹配 xxxxx
\	元字符可用作实际字符，还可用于指定预定义的字符类。有关可在敏感数据模式下使用的字符类的说明，请参阅第 21-25 页上的表 21-12。	\?匹配问号； \\ 匹配反斜杠； \d 匹配数字字符；等等

必须将反斜杠用于转义下表中的字符，这样敏感数据预处理器才能将它们正确解释为原义字符。

表 21-11　转义敏感数据模式字符

使用的转义字符	代表的原义字符
\?	?
\{	{
\}	}
\\	\

下表介绍了可在定义自定义数据模式时使用的字符类。

表 21-12　敏感数据模式字符类

字符类	说明	字符类定义
\d	匹配任何 ASCII 数字字符 0-9	0-9
\D	匹配任何不是 ASCII 数字字符的字节	不是 0-9
\l （小写“ell”）	匹配任何 ASCII 字母	a-zA-Z
\L	匹配任何不是 ASCII 字母的字节	不是 a-zA-Z
\w	匹配任何 ASCII 字母数字字符 请注意，与 PCRE 正则表达式不同，这不包括下划线 (_)。	a-zA-Z0-9
\W	匹配任何不是 ASCII 字母数字字符的字节	不是 a-zA-Z0-9

预处理器将直接输入 （而不是作为正则表达式的一部分输入）的字符视为原义字符。例如，数据模式 1234 匹配 `1234`。

以下数据模式示例 （用于预定义的敏感数据规则 138:4）使用转义的数字字符类、乘数和选项说明符元字符、文字连字符 (-) 和左右括号 () 字符来检测美国 电话号码：

```
(\d{3}) ?\d{3}-\d{4}
```

创建自定义数据模式时务必谨慎。考虑将下列备用数据模式用于检测电话号码，尽管使用的是有效语法，但可能会导致许多误报：

```
(?\d{3})??\d{3}-?\d{4}
```

由于第二个示例结合了可选括号、可选空格和可选破折号，它会在下列所需模式中检测电话号码及其他方面：

- `(555)123-4567`
- `555123-4567`
- `5551234567`

但是，第二个示例模式也会检测以下可能无效的模式及其他方面，从而造成误报：

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

最后举一个极端的例子（仅作说明用途）：创建一种数据模式，用以在小型企业网络上的所有目标流量中使用一个低事件阈值来检测小写字母 `a`。这种数据模式能够在短短几分钟内生成数百万的事件，从而可能令系统不胜负荷。

配置自定义数据类型

许可证：保护

实质上，是为针对预定义的数据类型所配置的自定义数据类型配置相同的数据类型选项。有关设置所有数据类型通用的选项，请参阅第 21-19 页上的选择具体数据类型选项。此外，还必须为自定义数据类型指定名称和数据模式。

请注意，创建自定义数据类型还会创建关联的自定义敏感数据预处理规则，必须在要使用该数据类型的每个策略中启用该规则。有关在入侵策略中启用规则的详细信息，请参阅第 20-17 页上的设置规则状态。

要创建或修改自定义数据类型，请执行以下操作：

管理员/入侵管理员

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Advanced Settings**。

系统将显示 Advanced Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 **Specific Threat Detection** 下的 **Sensitive Data Detection**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Sensitive Data Detection 页面。

页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 5　您有以下选项：

- 要创建自定义数据类型，请在页面左侧点击 **Data Types** 旁边的 **+** 符号。系统将显示 Add Data Type 弹出窗口。

  指定唯一的数据类型名称和要使用该数据类型检测的模式，然后点击 **OK**，或者点击 **Cancel** 放弃编辑。有关详情，请参见第 21-27 页上的编辑自定义数据类型名称和检测模式。

  系统将显示 Sensitive Data Detection 页面。如果点击 **OK**，页面会进行更新以显示更改。

- 要修改任何预定义和自定义数据类型通用的选项，请点击 **Targets** 页面区域中的数据类型名称。

  Configuration 页面区域会进行更新以显示数据类型的当前设置。有关详情，请参见第 21-20 页上的配置敏感数据检测。

- 要为自定义数据类型编辑系统范围的名称和数据模式，请参阅第 21-27 页上的编辑自定义数据类型名称和检测模式。

- 要删除自定义数据类型，请点击要删除的数据类型旁边的删除图标 ( )，然后点击 **OK**，或者点击 **Cancel** 放弃删除数据类型。

  请注意，如果任何入侵策略中启用了某个数据类型的敏感数据类型规则，不能删除该数据类型。删除某个自定义数据类型会导致从所有入侵策略中删除该数据类型。

编辑自定义数据类型名称和检测模式

许可证：保护

可以为自定义敏感数据规则修改系统范围的名称和检测模式。请注意，更改这些设置会导致系统上所有其他策略中的设置也随之更改。另请注意，如果必须已应用的访问控制策略包含使用修改的自定义数据类型的入侵策略，必须重新应用这些策略。

除自定义数据类型名称和数据模式之外，所有数据类型选项都是特定于策略的，适用于自定义和预定义的数据类型。有关修改自定义数据类型名称和数据模式以外选项的详细信息，请参阅第 21-19 页上的选择具体数据类型选项。

要编辑自定义数据类型名称和数据模式，请执行以下操作：

管理员/入侵管理员

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Advanced Settings**。

系统将显示 Advanced Settings 页面。

步骤 4　您有两种选择，具体取决于是否启用了 **Specific Threat Detection** 下的 **Sensitive Data Detection**：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Sensitive Data Detection 页面。

页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 5　在 **Targets** 页面区域，点击要修改的自定义数据类型的名称。

页面会进行更新以显示数据类型的当前设置，并且 **Edit Data Type Name and Pattern** 链接显示在 Configuration 页面区域的右上方。

步骤 6　点击 **Edit Data Type Name and Pattern** 链接。

系统将显示 Edit Data Type 弹出窗口。

步骤 7　修改数据类型名称和/或模式，然后点击 **OK**，或者点击 **Cancel** 放弃所做的编辑。有关指定数据模式的详细信息，请参阅第 21-24 页上的定义自定义数据类型的数据模式。

系统将显示 Sensitive Data Detection 页面。如果点击 **OK**，页面将会显示更改。

全局限制入侵事件记录

阈值可用于限制系统记录和显示入侵事件的次数。阈值，作为入侵策略的一部分而配置，导致系统根据与某条规则匹配的流量在指定时间段内源自或被引导至特定地址或地址范围的次数生成事件。这可以防止事件数量过多。此功能需要保护许可证。

设置事件通知阈值有两种方式：

- 可以跨所有流量设置全局阈值，用于限制每个指定时间段记录和显示来自特定源地址或目标地址的事件的频率。有关详细信息，请参阅第 22-1 页上的了解阈值和第 22-3 页上的配置全局阈值。
- 可以按照入侵策略配置中的每条共享对象规则、标准文本规则或预处理器规则设置阈值，如第 20-19 页上的配置事件阈值中所述。

了解阈值

许可证：保护

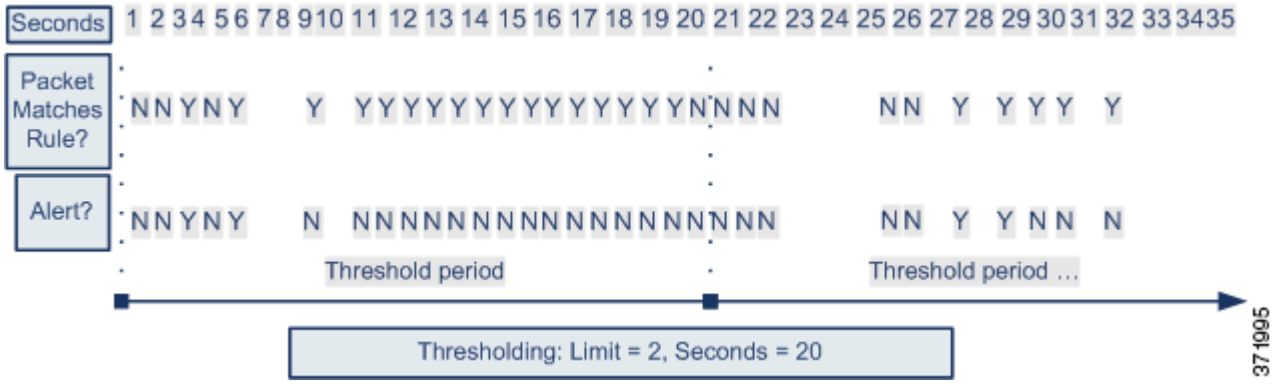
默认情况下，每个入侵策略都包含全局规则阈值。默认阈值将每条规则的事件生成频率限制为对发往同一个目标地址的流量每 60 秒生成一个事件。此全局阈值默认应用于所有入侵规则和预处理器规则。请注意，可以在入侵策略的 Advanced Settings 页面中禁用此阈值。

也可以对特定的规则设置单独的阈值，从而覆盖此阈值。例如，可将全局限值阈值设置为每 60 秒生成五个事件，然后为 SID 1315 设置每 60 秒生成十个事件的特定阈值。所有其他规则每 60 秒生成的事件不超过五个，但是系统每 60 秒可为 SID 1315 生成多达十个事件。

有关设置基于规则的阈值的详细信息，请参阅第 20-19 页上的配置事件阈值。

下图显示的例子中，系统正在受到违反特定规则的攻击。全局限值阈值将每条规则的事件生成频率限制为每 20 秒生成两个事件。

请注意，该时间段在 1 秒时开始，在 21 秒时结束。该时间段结束后，请注意时间周期重新开始，接下来两次规则匹配生成了事件，随后系统在这一时间段内不再生成事件。



了解阈值选项

许可证：保护

可以通过阈值来限制入侵事件的生成，只在某个时间段内生成特定数量的事件，或者只为一组事件生成一个事件。配置全局阈值时，首先应指定阈值类型，如下表所述。

表 22-1　　阈值选项

选项	说明
限制	为指定时间段内触发规则的指定数量的数据包（由计数参数指定）记录并显示事件。例如，如果将类型设置为 **Limit**，将 **Count** 设置为 10，并将 **Seconds** 设置为 60，而同一分钟内有 14 个数据包触发规则，则系统在显示发生的前 10 个违反该规则的事件后将停止记录违反该规则的事件。
阈值	在指定时间段内，当指定数量的数据包（由计数参数指定）触发规则时，记录并显示一个事件。请注意，达到事件阈值计数且系统记录该事件之后，时间计数器将重新开始计数。例如，将类型设置为 **Threshold**，将 **Count** 设置为 10，并将 **Seconds** 设置为 60 时，如果到 33 秒时规则触发 10 次，系统将生成一个事件，然后将 Seconds 和 Count 计数器重置为 0。其后，该规则在接下来 25 秒内又触发 10 次。由于计数器在第 33 秒时已重置为 0，因此，系统此时会记录另一个事件。
共通活动	每个指定时间段在指定数量（计数）的数据包触发规则后记录并显示一次事件。例如，如将类型设置为 **Both**，将 **Count** 设置为 2，将 **Seconds** 设置为 10，则事件计数结果如下： • 如果 10 秒内触发规则一次，系统不会生成任何事件（未达到阈值） • 如果 10 秒内触发规则两次，系统将生成一个事件（第二次触发规则时达到阈值） • 如果 10 秒内触发规则四次，系统将生成一个事件（第二次触发规则时达到阈值，忽略其后的事件）

接下来指定跟踪，确定事件实例计数是按源 IP 地址计算还是按目标 IP 地址计算。最后，指定用于定义阈值的实例数和时间段。

表 22-2　　阈值实例/时间选项

选项	说明
计数	每个跟踪 IP 地址或地址范围在每个指定时间段内达到阈值所需的事件实例数。
数秒	计数重置之前经过的秒数。如果将阈值类型设置为 **Limit**，将跟踪设置为 **Source**，将 **Count** 设置为 10，并将 **Seconds** 设置为 10，则系统将记录并显示 10 秒钟内发生的来自指定源端口的前 10 个事件。如果前 10 秒内只发生了七个事件，系统将记录并显示这些事件，而如果前 10 秒内发生了 40 个事件，系统将记录并显示 10 个事件，然后在为期 10 秒的时间段过后重新开始计数。

配置全局阈值

许可证：保护

可以设置全局阈值来管理每个规则在一段时间内生成的事件数。设置全局阈值后，该阈值将应用于没有特定阈值可覆盖该阈值的每条规则。有关配置阈值的详细信息，请参阅第 22-1 页上的了解阈值。

默认情况下，在您的系统上已配置全局阈值。默认值如下所示：

- **Type** - Limit
- **Track By** - Destination
- **Count** - 1
- **Seconds** - 60

要配置全局阈值，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Advanced Settings**。

系统将显示 Advanced Settings 页面。

步骤 4　此时有两种选择，取决于 **Intrusion Rule Thresholds** 下的 **Global Rule Thresholding** 是否启用：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Global Rule Thresholding 页面。页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 5　从 **Type** 单选按钮中，选择在秒数参数指定的时间内将应用的阈值的类型。有关详细信息，请参阅阈值选项表：

- 选择 **Limit** 则记录并显示触发规则的每个数据包的事件，直到超过计数参数指定的限值为止。
- 选择 **Threshold** 则为触发该规则并且代表与计数参数设置的阈值相匹配的实例或者是阈值倍数的每个数据包记录并显示一个事件。
- 选择 **Both** 则在触发规则的数据包达到计数参数指定的数量之后记录并显示一个事件。

步骤 6　从 **Track By** 单选按钮中选择跟踪方法：

- 选择 **Source** 则在来自一个或多个特定源 IP 地址的流量中查找规则匹配项。
- 选择 **Destination** 则在发往特定目标 IP 地址的流量中查找规则匹配项。

步骤 7　在 **Count** 字段中：

- 对于 **Limit** 阈值，请指定每个跟踪 IP 地址在每个指定时间段内达到阈值所需的事件实例数。
- 对于 **Threshold** 阈值，请指定要用作阈值的规则匹配项的数量。

步骤 8　在 **Seconds** 字段中：

- 对于 **Limit** 阈值，请指定组成跟踪攻击的时间段的秒数。
- 对于 **Threshold** 阈值，请指定计数重置之前经过的秒数。请注意，如果在指示的秒数过完之前规则匹配项数量即达到 **Count** 字段指示的数量，计数将重置。

步骤 9　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

禁用全局阈值

许可证：保护

默认情况下，全局限值阈值将发往目标地址的流量的事件数限制为每 60 秒一个事件。如果要为特定规则的事件设置阈值但不将阈值默认应用于每条规则，可以在最高策略层禁用全局阈值。

要禁用全局阈值，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Settings**。

系统将显示 Settings 页面。

步骤 4　在 **Intrusion Rule Thresholds** 下，请禁用 **Global Rule Thresholding**。

步骤 5　保存策略，继续编辑，放弃所做的更改，或者在系统缓存中保留更改的同时退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

了解和编写入侵规则

*入侵规则*是一组指定的关键字和参数，通过分析网络流量来检查其是否符合规则中的条件，从而检测试图利用网络漏洞的行为。系统将数据包与每条规则中指定的条件进行比较，如果数据包数据符合规则中指定的所有条件，则触发此规则。如果规则是*警报规则*，将生成入侵事件。如果是*通过规则*，将忽略流量。可以通过 ASA FirePOWER 模块界面查看和评估入侵事件。

注意事项 将编写的入侵规则用于生产环境之前，请务必使用受控网络环境测试这些规则。编写错误的入侵规则可能会严重影响系统性能。

请注意：

- 对于内联部署中的*丢弃*规则，系统将丢弃数据包并生成事件。有关丢弃规则的详细信息，请参阅第 20-17 页上的设置规则状态。
- 思科提供两种类型的入侵规则：共享对象规则和标准文本规则。思科漏洞研究工作组 (VRT) 可以使用共享对象规则来检测传统标准文本规则无法检测的漏洞攻击。不能创建共享对象规则。在自行编写入侵规则时，可以创建标准文本规则。

可以编写自定义标准文本规则，以调整可能出现的事件类型。请注意，虽然本文档有时讨论以检测特定漏洞为目标的规则，但最成功的规则是以检测可能试图利用已知漏洞的流量为目标，而不是以检测特定已知漏洞为目标。通过编写规则和指定规则的事件消息，可以更轻松地识别可能存在攻击和策略逃避行为的流量。有关评估事件的详细信息，请参阅第 26-1 页上的查看事件。

当在自定义入侵策略中启用自定义标准文本规则时，请记住，某些规则关键字和参数要求首先以特定方式对流量进行解码或预处理。本章说明在用于管理预处理的网络分析策略中必须配置的选项。请注意，如果禁用所需的预处理器，系统会自动采用其当前设置使用该预处理器，尽管该预处理器在网络分析策略用户界面中保持禁用状态。

注 由于预处理和入侵检查密切相关，因此用于检查单个数据包的网络分析和入侵策略**必须**相互补充。定制预处理（特别是使用多个自定义网络分析策略）是一个**高级**任务。有关详细信息，请参阅第 11-9 页上的自定义策略的限制。

有关详细信息，请参阅：

- 第 23-2 页上的了解规则结构介绍构成有效标准文本规则的组成部分，包括规则报头和规则选项。
- 第 23-3 页上的了解规则报头详细介绍规则报头的各个部分。
- 第 23-9 页上的了解规则中的关键字和参数说明 ASA FirePOWER 模块中可用的入侵规则关键字的用法和语法。

- 第 23-93 页上的构建规则解释如何使用规则编辑器构建新规则。
- 第 23-97 页上的过滤 Rule Editor 页面上的规则解释如何显示规则子集以帮助查找特定规则。

了解规则结构

许可证：保护

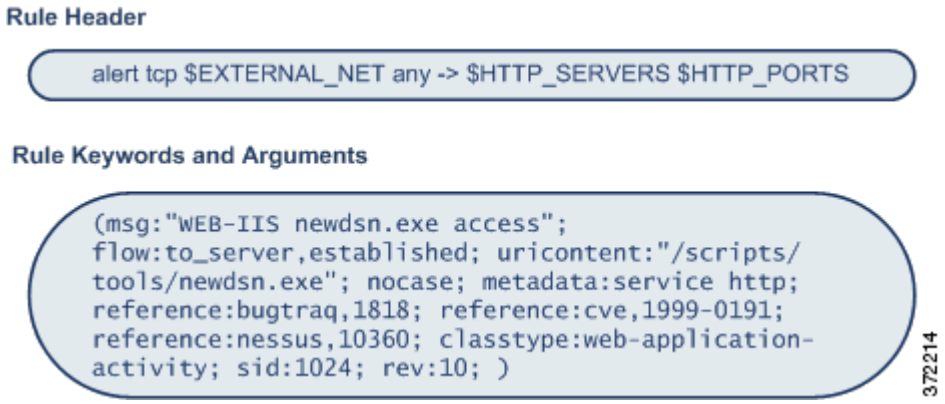
所有标准文本规则均包含两个逻辑部分：规则报头和规则选项。规则报头包含：

- 规则的操作或类型
- 协议
- 源 IP 地址、目标 IP 地址和子网掩码
- 方向指示符（显示从源到目标的流量流动方向）
- 源端口和目标端口

规则选项部分包含：

- 事件消息
- 关键字及其参数
- 模式（数据包负载必须与之匹配才能触发规则）
- 规范（规定规则引擎应检查数据包的哪些部分）

下图说明规则的组成部分：

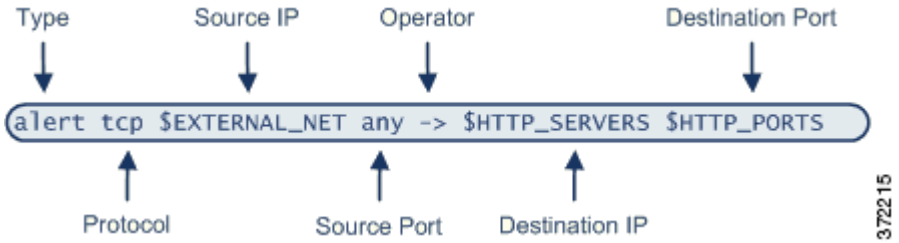


请注意，括号里的是规则选项部分。规则编辑器提供了一个易于使用的界面来帮助构建标准文本规则。

了解规则报头

许可证：保护

每个标准文本规则和共享对象规则都有一个包含参数的规则报头。下面说明规则报头的组成部分：



下表介绍了规则报头的上述各个部分。

表 23-1　　规则报头值

规则报头组成部分	示例值	示例值的作用
操作	警报	如果触发，将会生成事件。
协议	tcp	仅测试 TCP 流量。
源 IP 地址	$EXTERNAL_NET	测试来自不在内部网络上的任何主机的流量。
源端口	any	测试来自发起主机上任何端口的流量。
运算符	->	测试外部流量（流向网络上的网络服务器）。
目标 IP 地址:	$HTTP_SERVERS	测试将要传送到内部网络上被指定为网络服务器的任何主机的流量
目标端口	$HTTP_PORTS	测试传送到内部网络上 HTTP 端口的流量。

注　与大多数入侵规则一样，以上示例使用默认变量。有关变量、变量的含义以及如何配置变量的详细信息，请参阅第 2-13 页上的使用变量集。

有关规则报头参数的详细信息，请参阅：

- 第 23-4 页上的指定规则操作介绍规则类型，并解释如何指定触发规则时发生的操作。
- 第 23-4 页上的指定协议解释如何为规则应测试的流量定义流量协议。
- 第 23-5 页上的在入侵规则中指定 IP 地址解释如何在规则报头中定义单个 IP 地址和 IP 地址块。
- 第 23-8 页上的在入侵规则中定义端口解释如何在规则报头中定义单个端口和端口范围。
- 第 23-9 页上的指定方向介绍可用的运算符，并解释应如何指定流量的流动方向才能使规则对流量进行测试。

指定规则操作

许可证：保护

每个规则报头都包含一个用于指定数据包触发规则时系统应采取的操作的参数。操作设置为 *alert* 的规则将会针对触发规则的数据包生成入侵事件并记录该数据包的详细信息。操作设置为 *pass* 的规则不会针对触发规则的数据包生成入侵事件，也不会记录该数据包的详细信息。

注 在内联部署中，规则状态设置为 *Drop and Generate Events* 的规则会针对触发规则的数据包生成入侵事件。此外，如果在被动部署中应用丢弃规则，该规则将会充当警报规则。有关丢弃规则的详细信息，请参阅第 20-17 页上的设置规则状态。

默认情况下，通过规则会覆盖警报规则。可以创建通过规则来防止符合通过规则中定义的条件的数据包在特定情况下触发警报规则，而无需禁用预警报则。例如，您可能希望使检测尝试作为“匿名”用户登录 FTP 服务器这种情况的规则保持活动状态。但是，如果网络有一个或多个合法的匿名 FTP 服务器，您可以编写并激活一个通过规则，在其中指明匿名用户不会对那些特定服务器触发原始规则。

在规则编辑器中，可以从 **Action** 列表中选择规则类型。有关使用规则编辑器构建规则报头的步骤的详细信息，请参阅第 23-93 页上的构建规则。

指定协议

许可证：保护

在每个规则报头中，必须指定规则检查的流量的协议。可以指定以下网络协议用于分析：

- ICMP （互联网控制消息协议）
- IP （互联网协议）

注 如果协议设置为 `ip`，系统将忽略入侵规则报头中的端口定义。有关详细信息，请参阅第 23-8 页上的在入侵规则中定义端口。

- TCP （传输控制协议）
- UDP （用户数据报协议）

如果使用 **IP** 作为协议类型，将会检查 IANA 分配的所有协议（包括 TCP、UDP、ICMP、IGMP 等等）。有关 IANA 分配的协议的完整列表，请参阅 http://www.iana.org/assignments/protocol-numbers。

注 目前不能编写与 IP 负载中下一个报头（例如 TCP 报头）模式匹配的规则。相反，内容匹配从上一个解码的协议开始。要解决这个问题，可以使用规则选项来匹配 TCP 报头中的模式。

在规则编辑器中，可以从 **Protocol** 列表中选择协议类型。有关使用规则编辑器构建规则报头的步骤的详细信息，请参阅第 23-93 页上的构建规则。

在入侵规则中指定 IP 地址

许可证：保护

通过将数据包检查限制为仅针对来自或发往特定 IP 地址的数据包，可以减少系统必须执行的数据包检查工作量。这样做还可以令规则更加具体，并消除规则针对源和目标 IP 地址未指示可疑行为的数据包进行触发的可能性，从而减少误报。

提示　系统只能识别 IP 地址，不接受源或目标 IP 地址的主机名。

在规则编辑器中，可以在 **Source IPs** 和 **Destination IPs** 字段中指定源 IP 地址和目标 IP 地址。有关使用规则编辑器构建规则报头的步骤的详细信息，请参阅第 23-93 页上的构建规则。

编写标准文本规则时，可以根据自身需求以多种方法指定 IPv4 和 IPv6 地址。可以指定单个 IP 地址、`any`、IP 地址列表、CIDR 表示法、前缀长度、网络变量、网络对象或网络对象组。此外，还可以指明要排除的特定 IP 地址或 IP 地址集。指定 IPv6 地址时，可使用 RFC 4291 中定义的任意寻址约定。

下表总结了可用于指定源 IP 地址和目标 IP 地址的各种方法。

表 23-2　源/目标 IP 地址语法

要指定.....	使用.....	示例
任何 IP 地址	`any`	`any`
特定 IP 地址	IP 地址 请注意，不能在同一规则中混合使用 IPv4 和 IPv6 源地址和目标地址。	`192.168.1.1` `2001:db8::abcd`
IP 地址列表	使用方括号 (`[]`) 将地址括起来，并使用逗号分隔各个 IP 地址	`[192.168.1.1,192.168.1.15]` `[2001:db8::b3ff, 2001:db8::0202]`
IP 地址块	IPv4 CIDR 块或 IPv6 地址前缀表示法	`192.168.1.0/24` `2001:db8::/32`
除特定 IP 地址或地址集以外的任何项	在要否定的端口、端口列表或端口范围前面加上 `!`字符	`!192.168.1.15` `!2001:db8::0202:b3ff:fe1e`
IP 地址块中除一个或多个特定 IP 地址以外的任何 IP 地址	在地址块后加上被否定地址或地址块的列表	`[10.0.0/8, !10.2.3.4, !10.1.0.0/16]` `[2001:db8::/32, !2001:db8::8329, !2001:db8::0202]`
网络变量定义的 IP 地址	前面带有 `$` 的大写字母形式的变量名称 请注意，无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。有关详细信息，请参阅第 2-13 页上的使用变量集。	`$HOME_NET`
除 IP 地址变量定义的地址以外的所有 IP 地址	前面带有 `!$` 的大写字母形式的变量名称 有关详细信息，请参阅第 23-7 页上的在入侵规则中排除 IP 地址。	`!$HOME_NET`

表 23-2　源/目标 IP 地址语法（续）

要指定.....	使用.....	示例
网络对象或网络对象组定义的 IP 地址	采用 `!{object_name}` 这种格式的对象或对象组名称。 有关详细信息，请参阅第 2-3 页上的使用网络对象。	`${192.168sub16}`
除网络对象或网络对象组定义的地址以外的所有 IP 地址	对象或对象组名称用花括号 ({}) 括起来，前面带有 `!$`。 有关详细信息，请参阅第 2-3 页上的使用网络对象。	`!${192.168sub16}`

有关可用于指定源和目标 IP 地址的语法的更多详细信息，以及有关使用变量指定 IP 地址的信息，请参阅：

- 第 1-3 页上的IP 地址约定.
- 第 2-13 页上的使用变量集
- 第 23-6 页上的指定 IP 地址
- 第 23-6 页上的指定多个 IP 地址
- 第 23-7 页上的指定网络对象
- 第 23-7 页上的在入侵规则中排除 IP 地址

指定 IP 地址

许可证：保护

可以指定 `any` 这个词作为规则的源或目标 IP 地址，以指示 IPv4 或 IPv6 地址。

例如，以下规则在 **Source IPs** 和 **Destination IPs** 字段中使用参数 **`any`** 来评估具有 IPv4 或 IPv6 源地址或目标地址的数据包：

```
alert tcp any any -> any any
```

还可以指定 `::` 以指示 IPv6 地址。

指定多个 IP 地址

许可证：保护

可以列出多个 IP 地址，地址之间用逗号分隔，如有需要，还可以用方括号将非否定地址列表括起来，如以下示例所示：

```
[192.168.1.100,192.168.1.103,192.168.1.105]
```

可以单独或以任意组合列出 IPv4 和 IPv6 地址，如以下示例所示：

```
[192.168.1.100,2001:db8::1234,192.168.1.105]
```

请注意，现在不再要求用方括号将 IP 地址列表括起来（旧版软件要求这样做）。另请注意，输入列表时，可以在每个逗号前后添加一个空格。

注　必须用方括号将否定列表括起来。有关详细信息，请参阅第 23-7 页上的在入侵规则中排除 IP 地址。

也可以使用 IPv4 无类域间路由选择 (CIDR) 表示法或 IPv6 前缀长度来指定地址块。例如：

- 192.168.1.0/24 指定子网掩码为 255.255.255.0 的 192.168.1.0 网络中的 IPv4 地址，即，192.168.1.0 至 192.168.1.255。有关详细信息，请参阅第 1-3 页上的IP 地址约定。

- 2001:db8::/32 指定前缀长度为 32 位的 2001:db8:: 网络中的 IPv6 地址，即， 2001:db8:: 至 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff。

提示 如果需要指定 IP 地址块，但仅以 CIDR 或前缀长度表示法无法表示出该地址块，可以在 IP 地址列表中使用 CIDR 块和前缀长度。

指定网络对象

许可证：保护

可以使用以下语法指定网络对象或网络对象组：

```
${object_name | group_name}
```

其中：

- *object_name* 是网络对象的名称
- *group_name* 是网络对象组的名称

有关创建网络对象和网络对象组的信息，请参阅第 2-3 页上的使用网络对象。

假设已创建一个名为 `192.168sub16` 的网络对象和一个名为 `all_subnets` 的网络对象组，那么，可以指定以下语法以识别使用该网络对象的 IP 地址：

```
${192.168sub16}
```

并且可以指定以下语法以使用该网络对象组：

```
${all_subnets}
```

还可以对网络对象和网络对象组进行否定。例如：

```
!${192.168sub16}
```

有关详细信息，请参阅第 23-7 页上的在入侵规则中排除 IP 地址。

在入侵规则中排除 IP 地址

许可证：保护

可以使用感叹号 (`!`) 否定指定 IP 地址。也就是说，可以匹配除指定 IP 地址以外的所有 IP 地址。例如， `!192.168.1.1` 指定除 192.168.1.1 以外的任何 IP 地址， `!2001:db8:ca2e::fa4c` 指定除 2001:db8:ca2e::fa4c 以外的任何 IP 地址。

要否定某个 IP 地址列表，请用方括号将该 IP 地址列表括起来，并在其前面加上 `!`。例如，`![192.168.1.1,192.168.1.5]` 将定义除 192.168.1.1 和 192.168.1.5 以外的任何 IP 地址。

注 要否定 IP 地址列表，必须使用方括号。

对 IP 地址列表使用否定字符时务必要小心。例如，如果使用 `[!192.168.1.1,!192.168.1.5]` 匹配不是 192.168.1.1 和 192.168.1.5 的任何地址，系统会将此语法解释为“非 192.168.1.1 的任何地址，**或**非 192.168.1.5 的任何地址”。

由于 192.168.1.5 不是 192.168.1.1，且 192.168.1.1 不是 192.168.1.5，因此，这两个 IP 地址都与 `[!192.168.1.1,!192.168.1.5]` 的 IP 地址值匹配；此语法实质上与使用“`any`”相同。

应该使用 `![192.168.1.1,192.168.1.5]`。系统会将此语法为“**非** 192.168.1.1 **且非** 192.168.1.5”，这意味着，与方括号中所列地址以外的任何 IP 地址匹配。

请注意，从逻辑上讲，不能对 `any` 进行否定（如果它被否定，将表示无地址）。

在入侵规则中定义端口

许可证：保护

在规则编辑器中，可以在 **Source Port** 和 **Destination Port** 字段中指定源端口和目标端口。有关使用规则编辑器构建规则报头的步骤的详细信息，请参阅第 23-93 页上的构建规则。

ASA FirePOWER 模块使用特定类型的语法来定义规则报头中使用的端口号。

注　如果协议设置为 `ip`，系统将忽略入侵规则报头中的端口定义。有关详细信息，请参阅第 23-4 页上的指定协议。

可以列出多个端口，端口之间用逗号分隔，如以下示例所示：

```
80, 8080, 8138, 8600-9000, !8650-8675
```

或者，可以用方括号将端口列表括起来（旧版软件要求这样做，但现在不再有此要求），如以下示例所示：

```
[80, 8080, 8138, 8600-9000, !8650-8675]
```

请注意，**必须**用方括号将否定端口列表括起来，如以下示例所示：

```
![20, 22, 23]
```

另请注意，入侵规则的源或目标端口列表最多可包含 64 个字符。

下表总结了可使用的语法：

表 23-3　　源/目标端口语法

要指定.....	使用	示例
任意端口	`any`	`any`
特定端口	端口号	`80`
端口范围	范围内第一个和最后一个端口号之间使用破折号	`80-443`
所有小于或等于指定端口号的端口	在端口号前面加上破折号	`-21`
所有大于或等于指定端口号的端口	在端口号后面加上破折号	`80-`
除特定端口或端口范围以外的所有端口	在要否定的端口、端口列表或端口范围前面加上 `!` 字符 请注意，从逻辑上讲，可以否定除 *any*（如果它被否定，将表示*无端口*）以外的所有端口名称。	`!20`
端口变量定义的所有端口	前面带有 `$` 的大写字母形式的变量名称 有关详细信息，请参阅第 2-23 页上的使用端口变量。	`$HTTP_PORTS`
除端口变量定义的端口以外的所有端口	前面带有 `!$` 的大写字母形式的变量名称	`!$HTTP_PORTS`

指定方向

许可证：保护

在规则报头中，可以指定数据包接受规则检查必须流经的方向。下表介绍了这些选项。

表 23-4　规则报头中的方向选项

使用.....	以测试.....
Directional	仅测试从指定源 IP 地址流向指定目标 IP 地址的流量
双向	测试指定的源 IP 地址和目标 IP 地址之间的所有流量

有关使用规则编辑器构建规则报头的步骤的详细信息，请参阅第 23-93 页上的构建规则。

了解规则中的关键字和参数

许可证：保护

借助规则语言，可以通过组合关键字来指定规则行为。关键字及其相关值（称为*参数*）规定系统如何评估规则引擎测试的数据包和数据包相关值。ASA FirePOWER 模块当前支持可以执行检查功能（例如内容匹配、协议特定模式匹配和状态特定匹配）的关键字。在每个关键字中最多可以定义 100 个参数，还可以组合任意数量的兼容关键字来创建非常具体的规则。这有助于降低出现误报和漏报的可能性，使您可以重点关注接收到的入侵信息。

请注意，也可以使用自适应配置文件，以根据规则元数据和主机信息动态调整规则对特定数据包的当前处理方式。有关详细信息，请参阅第 18-1 页上的在被动部署中调整预处理。

有关详细信息，请参阅以下各节：

- 第 23-10 页上的定义入侵事件详细信息介绍可用于定义事件消息、优先级信息以及关于规则检测的漏洞的外部信息参考的关键字的语法及使用。
- 第 23-14 页上的搜索内容匹配介绍如何使用 `content` 或 `protected_content` 关键字测试数据包负载的内容。
- 第 23-16 页上的限制内容匹配介绍如何对 `content` 或 `protected_content` 关键字使用修饰关键字。
- 第 23-27 页上的替换内联部署中的内容介绍如何在内联部署中使用 `replace` 关键字替换同等长度的指定内容。
- 第 23-28 页上的使用 Byte_Jump 和 Byte_Test介绍如何使用 `byte_jump` 和 `byte_test` 关键字计算规则引擎应在数据包中的哪个位置开始测试内容匹配以及应评估哪些字节。
- 第 23-32 页上的使用 PCRE 搜索内容介绍如何使用 `pcre` 关键字在规则中使用兼容 Perl 的正则表达式。
- 第 23-38 页上的向规则添加元数据介绍如何使用 `metadata` 关键字向规则添加信息。
- 第 23-41 页上的检查 IP 报头值介绍用于测试数据包 IP 报头中值的关键字的语法及使用。
- 第 23-43 页上的检查 ICMP 报头值介绍用于测试数据包 ICMP 报头中值的关键字的语法及使用。
- 第 23-45 页上的检查 TCP 报头值和数据流大小介绍用于测试数据包 TCP 报头中值的关键字的语法及使用。
- 第 23-49 页上的启用和禁用 TCP 数据流重组介绍在连接上检测到的流量与规则条件匹配的情况下，如何启用和禁用数据流重组。

- 第 23-49 页上的从会话提取 SSL 信息介绍用于从加密流量中提取版本和状态信息的关键字的使用及语法。
- 第 23-75 页上的将数据包数据读取到关键字参数中介绍如何将数据包中的值读入到某个变量，以便日后在同一规则中使用该变量来指定某些其他关键字中参数的值。
- 第 23-51 页上的检查应用层协议值介绍用于测试应用层协议属性的关键字的使用及语法。
- 第 23-73 页上的检查数据包特征介绍 `dsize`、`sameIP`、`isdataat`、`fragoffset` 和 `cvs` 关键字的使用及语法。
- 第 23-77 页上的使用规则关键字发起活动响应解释如何使用 `resp` 关键字主动关闭 TCP 连接或 UDP 会话，如何使用 `react` 关键字发送 HTML 页面并主动关闭 TCP 连接，以及如何使用 `config response` 命令指定活动响应接口和被动部署中的 TCP 重置尝试次数。
- 第 23-80 页上的过滤事件介绍如何防止规则触发事件（除非指定数量的数据包在规定时间内满足规则检测条件）。
- 第 23-81 页上的评估攻击后流量介绍如何记录主机或会话的额外流量。
- 第 23-82 页上的检测跨越多个数据包的攻击介绍如何向来自在一个会话中涉及多个数据包的攻击的数据包分配状态名称，然后根据其状态对数据包进行分析和发出警报。
- 第 23-87 页上的生成关于 HTTP 编码类型和位置的事件介绍如何在规范化之前生成有关 HTTP 请求或响应 URI、报头或 cookie （包括 set-cookie）中编码类型的事件。
- 第 23-88 页上的检测文件类型和版本介绍如何使用 `file_type` 或 `file_group` 关键字指向特定文件类型或文件版本。
- 第 23-90 页上的指向特定负载类型介绍如何指向 HTTP 响应实体正文、SMTP 负载或编码邮件附件的开头。
- 第 23-91 页上的指向数据包负载的开头介绍如何指向数据包负载的开头。
- 第 23-91 页上的解码和检查 Base64 数据介绍如何使用 `base64_decode` 和 `base64_data` 关键字解码和检查 Base64 数据（尤其是在 HTTP 请求中）。

定义入侵事件详细信息

许可证：保护

构建标准文本规则，可以在其中纳入描述规则检测到且容易被利用的漏洞的上下文信息。也可以在其中纳入对漏洞数据库的外部参考，以及定义入侵事件在贵公司中具有的优先级。这样，如果分析师发现入侵事件，他们可随时获取有关优先级、漏洞和已知缓解措施的信息。

有关事件相关关键字的详细信息，请参阅：

- 第 23-11 页上的定义事件消息
- 第 23-11 页上的定义事件优先级
- 第 23-11 页上的定义入侵事件分类
- 第 23-13 页上的定义事件参考

定义事件消息

许可证：保护

可以指定规则触发时以消息形式显示的有意义的文本。这类消息使您可以即时了解规则检测的漏洞的性质。可以使用除花括号 ({}) 以外的所有可打印标准 ASCII 字符。系统将移除将消息完全引起来的引号。

提示 必须指定规则消息。此外，消息不能只包含空白字符、一个或多个引号、一个或多个撇号或者仅由空白字符、引号或撇号组成的任意组合。

要在规则编辑器中定义事件消息，请在 **Message** 字段中输入事件消息。有关使用规则编辑器构建规则的详细信息，请参阅第 23-93 页上的构建规则。

定义事件优先级

许可证：保护

默认情况下，规则的优先级来源于其事件分类。但是，可以通过向规则添加 `priority` 关键字覆盖分类优先级。

要使用规则编辑器指定优先级，请从 **Detection Options** 列表中选择 **priority**，然后从下拉列表中选择 **high**、 **medium** 或 **low**。例如，要为检测网络应用攻击的规则分配 **high** 优先级，请向该规则添加 `priority` 关键字，并选择 **high** 作为优先级。有关使用规则编辑器构建规则的详细信息，请参阅第 23-93 页上的构建规则。

定义入侵事件分类

许可证：保护

对于每个规则，可以指定事件数据包显示中出现的攻击分类。下表列出了每种分类的名称和编号。

表 23-5　　规则分类

编号	分类名称	说明
1	not-suspicious	非可疑流量
2	unknown	未知流量
3	bad-unknown	潜在不良流量
4	attempted-recon	尝试信息泄露
5	successful-recon-limited	信息泄露
6	successful-recon-largescale	大规模信息泄露
7	attempted-dos	尝试拒绝服务
8	successful-dos	拒绝服务攻击
9	attempted-user	尝试获取用户权限
10	unsuccessful-user	未成功获取用户权限
11	successful-user	成功获取用户权限
12	attempted-admin	尝试获取管理员权限
13	successful-admin	成功获取管理员权限

表 23-5　规则分类（续）

编号	分类名称	说明
14	rpc-portmap-decode	解码 RPC 查询
15	shellcode-detect	检测到可执行代码
16	string-detect	检测到可疑字符串
17	suspicious-filename-detect	检测到可疑文件名
18	suspicious-login	检测到尝试使用可疑用户名的登录
19	system-call-detect	检测到系统调用
20	tcp-connection	检测到 TCP 连接
21	trojan-activity	检测到网络木马
22	unusual-client-port-connection	客户端使用异常端口
23	network-scan	检测网络扫描
24	denial-of-service	检测拒绝服务攻击
25	non-standard-protocol	检测非标准协议或事件
26	protocol-command-decode	通用协议命令解码
27	web-application-activity	访问可能易受攻击的网络应用
28	web-application-attack	网络应用攻击
29	misc-activity	其他活动
30	misc-attack	其他攻击
31	icmp-event	一般 ICMP 事件
32	inappropriate-content	检测到不当内容
33	policy-violation	可能违反公司隐私策略
34	default-login-attempt	尝试使用默认用户名和密码登录
35	sdf	敏感数据
36	malware-cnc	已知恶意软件命令和控制流量
37	client-side-exploit	已知客户端攻击尝试
38	file-format	已知的恶意文件或基于文件的攻击

要在规则编辑器中指定分类，请从 **Classification** 列表中选择分类。有关规则编辑器的详细信息，请参阅第 23-93 页上的编写新规则。

添加自定义分类

许可证：保护

如果想将更多自定义内容用于对所定义的规则生成的事件的数据包显示描述中，可创建自定义分类。

要向 Classification 列表添加分类，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy > Rule Editor**。

系统将显示 Rule Editor 页面。

步骤 2　点击 **Create Rule**。

系统将显示 Create Rule 页面。

步骤 3　在 **Classification** 下拉列表中点击 **Edit Classifications**。

系统将显示一个弹出窗口。

步骤 4　在 **Classification Name** 字段中键入分类的名称。

最多可以使用 255 个字母数字字符，但如果使用的字符超过 40 个，页面将难以阅读。不支持以下字符：`<>()\'"&$;` 以及空格字符。

步骤 5　在 **Classification Description** 字段中键入对分类的描述。

最多可以使用 255 个字母数字字符和空格。不支持以下字符：`<>()\'"&$;`

步骤 6　从 **Priority** 列表中选择优先级。

可以选择 **high**、 **medium** 或 **low**。

步骤 7　点击 **Add**。

新类别将被添加到列表并可在规则编辑器中使用。

步骤 8　点击**完成 (Done)**。

定义事件参考

许可证：保护

可以使用 `reference` 关键字添加对外部网站以及对关于事件的其他信息的参考。添加参考使分析师可以随时获得所需的资源，从而帮助他们确定数据包触发规则的原因。下表列出了一些可提供关于已知漏洞和攻击的数据的外部系统。

表 23-6　　外部攻击识别系统

系统 ID	说明	示例 ID
`bugtraq`	Bugtraq 页面	`8550`
`cve`	通用漏洞与风险页面	`CAN-2003-0702`
`mcafee`	McAfee 页面	`98574`
`url`	网站参考	`www.example.com?exploit=14`
`msb`	Microsoft 安全公告	`MS11-082`
`nessus`	Nessus 页面	`10039`
`secure-url`	安全网站参考 (https://...)	`intranet/exploits/exploit=14` 请注意，可以对任何安全网站使用 `secure-url`。

要使用规则编辑器指定参考，请从 **Detection Options** 列表中选择 **reference**，并在相应字段中输入一个值，如下所示：

`id_system,id`

其中，*id_system* 是用作前缀的系统，*id* 是 Bugtraq ID、CVE 编号、Arachnids ID 或 URL（不包含 http://）。

例如，要指定 Microsoft Commerce Server 2002 服务器存在的、Bugtraq ID 为 17134 的身份验证绕过漏洞，请在 **reference** 字段中输入以下内容：

```
bugtraq,17134
```

向规则添加参考时应注意以下几点：

- 逗号后不能有空格。
- 系统 ID 不能是大写字母。

有关使用规则编辑器构建规则的详细信息，请参阅第 23-93 页上的构建规则。

搜索内容匹配

许可证：保护

使用 content 关键字或 protected_content 关键字可以指定要在数据包中检测的内容。有关详细信息，请参阅：

- 第 23-14 页上的使用 content 关键字
- 第 23-14 页上的使用 protected_content 关键字
- 第 23-15 页上的配置内容匹配

使用 content 关键字

当使用 content 关键字时，规则引擎在数据包负载或数据流中搜索该字符串。例如，如果输入 /bin/sh 作为其中一个 content 关键字的值，则规则引擎会在数据包负载中搜索字符串 /bin/sh。

可以使用 ASCII 字符串、十六进制内容（二进制字节代码）或这两者的组合来匹配内容。可以在关键字值中将十六进制内容放在两条竖线 (|) 之间。例如，可以混合使用十六进制内容和 ASCII 内容，例如，|90C8 C0FF FFFF|/bin/sh。

可以在一个规则中指定多项内容匹配。要这样做，请使用 content 关键字的其他实例。对于各项内容匹配，可以指明必须在数据包负载或数据流中发现内容匹配才可触发规则。

使用 protected_content 关键字

protected_content 关键字使您可以在配置规则参数前对搜索内容字符串进行编码。原始规则作者在配置关键字前使用哈希函数（SHA-512、SHA-256 或 MD5）对字符串进行编码。

如果使用 protected_content 关键字而不使用 content 关键字，规则引擎在数据包负载或数据流中搜索字符串的方式并不会改变，且大多数关键字选项将起到预期作用。下表总结了 protected_content 关键字选项与 content 关键字选项存在差异的例外情况。

表 23-7　　protected_content 选项例外

选项	说明
Hash Type	protected_content 规则关键字的新增选项。有关详细信息，请参阅第 23-17 页上的 Hash Type。
Case Insensitive	不支持
Within	不支持

表 23-7　protected_content 选项例外（续）

选项	说明
深度	不支持
长度	protected_content 规则关键字的新增选项。有关详细信息，请参阅第 23-20 页上的长度。
Use Fast Pattern Matcher	不支持
Fast Pattern Matcher Only	不支持
Fast Pattern Matcher Offset and Length	不支持

思科建议在包含 protected_content 关键字的规则中至少包含一个 content 关键字，以确保规则引擎使用快速模式匹配程序，从而加快处理速度和提高性能。在规则中， content 关键字应置于 protected_content 关键字之前。请注意，如果规则包含至少一个 content 关键字，无论您是否启用 content 关键字的 Use Fast Pattern Matcher 参数，规则引擎都会使用快速模式匹配程序。

配置内容匹配

大多数情况下，应始终在 content 或 protected_content 关键字后面加上修饰符，指示对内容进行搜索的位置、搜索是否区分大小写及其他选项。有关 content 和 protected_content 关键字的修饰符的详细信息，请参阅限制内容匹配。

请注意，要使规则触发事件，所有内容匹配必须为真，也就是说，每项内容匹配与其他匹配之间都存在 AND 关系。

另请注意，在内联部署中，可以将规则设置为匹配恶意内容并将其更换为您自定义的等长文本字符串。有关详细信息，请参阅第 23-27 页上的替换内联部署中的内容。

要输入待匹配的内容，请执行以下操作：

步骤 1　在 content 字段中输入要查找的内容（例如，|90C8 C0FF FFFF|/bin/sh）。

如果要搜索**不是**指定内容的任何内容，请选择 **Not** 复选框。

注意事项　如果创建的规则只包含一个 content 关键字，但没有为该关键字选择 **Not** 选项，可能会使入侵策略无效。有关详细信息，请参阅第 23-18 页上的非。

步骤 2　如有需要，可以添加用于修饰 content 关键字的其他关键字，或者为该关键字添加限制条件。

有关其他关键字的详细信息，请参阅第 23-9 页上的了解规则中的关键字和参数。有关限制 content 关键字的详细信息，请参阅第 23-16 页上的限制内容匹配。

步骤 3　继续创建或编辑规则。

有关详细信息，请参阅第 23-93 页上的编写新规则或第 23-95 页上的修改现有规则。

要输入待匹配的受保护内容，请执行以下操作：

步骤 1　可使用 SHA-512、SHA-256 或 MD5 哈希生成器对要查找的内容进行编码（例如，通过 SHA-512 哈希生成器运行字符串 `Sample1`）。

生成器将为该字符串生成哈希。

步骤 2　在 `protected_content` 字段中，键入在第 1 步中生成的哈希 （例如，`B20AABAF59605118593404BD42FE69BD8D6506EE7F1A71CE6BB470B1DF848C814BC5DBEC2081999F15691A71FAECA5FBA4A3F8B8AB56B7F04585DA6D73E5DD15`）。

如果要搜索**不是**指定内容的任何内容，请选择 **Not** 复选框。

注意事项　如果创建的规则只包含一个 `protected_content` 关键字，但没有为该关键字选择 **Not** 选项，可能会使入侵策略无效。有关详细信息，请参阅第 23-18 页上的非。

步骤 3　从 **Hash Type** 下拉列表中选择在第 1 步中使用的哈希函数（例如 **SHA-512**）。请注意，在第 2 步中输入的哈希的位数**必须**与散列类型匹配，否则系统不会保存规则。有关详细信息，请参阅第 23-17 页上的 Hash Type。

提示　如果选择思科设置的**默认值**，系统将假设 SHA-512 为哈希函数。

步骤 4　在必填的 **Length** 字段中键入一个值。该值**必须**与要查找的原始非哈希字符串的长度（例如，步骤 2 中的字符串 `Sample1` 的长度为 `7`）一致。

有关详细信息，请参阅第 23-20 页上的长度。

步骤 5　在 **Offset** 或 **Distance** 字段中键入一个值。不能在单个关键字配置中同时使用 **Offset** 和 **Distance** 选项。

有关详细信息，请参阅第 23-21 页上的在 protected_content 关键字中使用搜索位置选项。

步骤 6　或者，可添加其他限制选项来修饰 `protected_content` 关键字。

有关详细信息，请参阅第 23-16 页上的限制内容匹配。

步骤 7　或者，可添加其他关键字来修饰 `protected_content` 关键字。

有关详细信息，请参阅第 23-9 页上的了解规则中的关键字和参数。

步骤 8　继续创建或编辑规则。

有关详细信息，请参阅第 23-93 页上的编写新规则或第 23-95 页上的修改现有规则。

限制内容匹配

许可证：保护

可以通过修饰 `content` 或 `protected_content` 关键字的参数来限制内容搜索的位置以及大小写。配置用于修饰 `content` 或 `protected_content` 关键字的选项可以指定要搜索的内容。

有关详细信息，请参阅：

- 第 23-17 页上的 Case Insensitive
- 第 23-17 页上的 Hash Type
- 第 23-18 页上的 Raw Data

- 第 23-18 页上的非
- 第 23-19 页上的搜索位置选项
- 第 23-21 页上的 HTTP 内容选项
- 第 23-25 页上的 Use Fast Pattern Matcher

Case Insensitive

许可证：保护

注 配置 protected_content 关键字时不支持此选项。有关详细信息，请参阅第 23-14 页上的使用 protected_content 关键字。

可以指示规则引擎在搜索 ASCII 字符串内容匹配时忽略大小写。要使搜索不区分大小写，请在指定内容搜索时选择 **Case Insensitive**。

要在进行内容搜索时指定不区分大小写，请执行以下操作：

步骤 1 为添加的 content 关键字选择 **Case Insensitive**。

步骤 2 继续创建或编辑规则。

有关详细信息，请参阅限制内容匹配、第 23-14 页上的搜索内容匹配、第 23-93 页上的编写新规则或第 23-95 页上的修改现有规则。

Hash Type

许可证：保护

注 此选项仅对于 protected_content 关键字可配置。有关详细信息，请参阅第 23-14 页上的使用 protected_content 关键字。

使用 **Hash Type** 下拉列表确定用于编码搜索字符串的哈希函数。系统支持对 protected_content 搜索字符串进行 SHA-512、 SHA-256 和 MD5 哈希处理。如果哈希内容的长度与所选的哈希类型不匹配，系统将不会保存规则。

系统将自动选择思科设置的默认值。如果选择了 **Default**，将不会向规则写入特定哈希函数，且系统将假设 SHA-512 为哈希函数。

要在搜索受保护内容时指定哈希函数，请执行以下操作：

步骤 1 从 **Hash Type** 下拉列表中，选择 **Default**、**SHA-512**、**SHA-256** 或 **MD5** 作为添加的 protected_content 关键字的哈希。

提示 如果选择思科设置的**默认值**，系统将假设 SHA-512 为哈希函数。有关详细信息，请参阅第 23-17 页上的 Hash Type。

步骤 2　继续创建或编辑规则。有关详细信息，请参阅限制内容匹配、第 23-14 页上的搜索内容匹配、第 23-93 页上的编写新规则或第 23-95 页上的修改现有规则。

Raw Data

许可证：保护

Raw Data 选项指示规则引擎在分析规范化负载数据（由网络分析策略解码）之前分析原始数据包负载，并且此选项不使用参数值。进行规范化之前，可以在分析 telnet 流量时使用此关键字在负载中检查 telnet 协商选项。

不能在同一个 `content` 或 `protected_content` 关键字中同时使用 **Raw Data** 选项和任何 HTTP 内容选项。有关详细信息，请参阅第 23-21 页上的 HTTP 内容选项。

提示　可以配置 HTTP 检查预处理器 **Client Flow Depth** 和 **Server Flow Depth** 选项，以确定是否在 HTTP 流量中检查原始数据以及检查的原始数据量。有关详细信息，请参阅第 15-29 页上的选择服务器级别 HTTP 规范化选项。

要分析原始数据，请执行以下操作：

步骤 1　为添加的 `content` 或 `protected_content` 关键字选择 **Raw Data** 复选框。

步骤 2　继续创建或编辑规则。有关详细信息，请参阅限制内容匹配、第 23-14 页上的搜索内容匹配、第 23-93 页上的编写新规则或第 23-95 页上的修改现有规则。

非

许可证：保护

选择 **Not** 选项可搜索与指定内容不匹配的内容。如果创建包含已选择 **Not** 选项的 `content` 或 `protected_content` 关键字的规则，则必须在该规则中至少包含另一个未选择 **Not** 选项的 `content` 或 `protected_content` 关键字。

注意事项　请勿创建仅包含一个已选择 **Not** 选项的 `content` 或 `protected_content` 关键字的规则。否则，可能会使入侵策略无效。

例如， SMTP 规则 1:2541:9 包含三个 `content` 关键字，其中一个选择了 **Not** 选项。如果移除除选择了 **Not** 选项的关键字以外的其他 `content` 关键字，基于该规则的自定义规则将无效。将该规则添加到入侵策略将导致策略失效。

要搜索与指定内容不匹配的内容，请执行以下操作：

步骤 1　为添加的 `content` 或 `protected_content` 关键字选择 **Not** 复选框。

提示　不能对同一个 `content` 关键字同时选择 **Not** 复选框和 **Use Fast Pattern Matcher** 复选框。

步骤 2　在规则中至少包含另一个未选择 **Not** 选项的 `content` 或 `protected_content` 关键字。

步骤 3　继续创建或编辑规则。有关详细信息，请参阅限制内容匹配、第 23-14 页上的搜索内容匹配、第 23-93 页上的编写新规则或第 23-95 页上的修改现有规则。

搜索位置选项

许可证：保护

可以使用搜索位置选项指定开始搜索指定内容的位置以及继续搜索的深度。有关每个这些选项的详细信息，请参阅：

- 第 23-19 页上的深度
- 第 23-19 页上的距离
- 第 23-20 页上的长度
- 第 23-20 页上的偏移
- 第 23-20 页上的 Within

关于如何在 `content` 或 `protected_content` 关键字中使用搜索位置选项的信息，请参阅：

- 第 23-20 页上的在 content 关键字中使用搜索位置选项
- 第 23-21 页上的在 protected_content 关键字中使用搜索位置选项

深度

注　此选项**仅**在配置 `content` 关键字时可用。有关详细信息，请参阅第 23-14 页上的使用 content 关键字。

指定最大内容搜索深度（以字节为单位），从偏移量值起点开始计算，如果没有配置偏移量，则从数据包负载起点开始计算。

例如，如果规则的内容值为 `cgi-bin/phf`，`offset` 值为 `3`，`depth` 值为 `22`，规则将从字节 3 开始搜索 `cgi-bin/phf` 字符串内容匹配，并在处理完符合规则报头指定参数的数据包中的 22 个字节（字节 25）后停止。

必须指定一个大于或等于指定内容长度的数值，最多 65535 字节。不能指定值 0。

默认深度是搜索至数据包终点。

距离

指示规则引擎识别在上一次成功内容匹配后出现指定数量字节的后续内容匹配。

由于偏移量计数器从字节 0 开始计算，因此，应指定比所需字节数小 1 的值，以便从上一次成功内容匹配开始继续搜索。例如，如果指定 4，搜索将从第五个字节开始。

可指定 -65535 到 65535 字节之间的值。如果在 `Distance` 中指定负值，开始搜索的字节可能位于数据包开头以外。所有计算都会将数据包以外的字节考虑在内，尽管搜索实际上从数据包的第一个字节开始。例如，如果数据包当前位置是第五个字节，下一个内容规则选项指定 `Distance` 值为 -10，`Within` 值为20，搜索将从负载起点开始，且 `Within` 选项将调整为 15。

默认距离是 0，表示继上一次内容匹配之后数据包中的当前位置。

长度

注 此选项**仅**在配置 protected_content 关键字时可用。有关详细信息，请参阅第 23-14 页上的使用 protected_content 关键字。

Length protected_content 关键字选项表示非哈希搜索字符串的长度 （以字节为单位）。

例如，如果使用了内容 Sample1 生成安全哈希，请将 **Length** 值设置为 7。**必须**在该字段中输入一个值。

偏移

指定数据包负载中开始内容搜索的位置与数据包负载起点之间的距离 （以字节为单位）。可指定 -65535 到 65535 字节之间的值。

由于偏移量计数器从字节 0 开始计算，因此，应指定比所需字节数小 1 的值，以便从数据包负载起点开始继续搜索。例如，如果指定 7，搜索将从第八个字节开始。

默认偏移量是 0，表示数据包起点。

Within

注 此选项**仅**在配置 content 关键字时可用。有关详细信息，请参阅第 23-14 页上的使用 content 关键字。

Within 选项指明，要触发规则，下一次内容匹配必须发生在上一次成功内容匹配结束之后指定数量的字节内。例如，如果将 **Within** 值指定为 8，下一次内容匹配必须出现在数据包负载中接下来的八个字节之内，否则将无法满足触发规则的条件。

可以指定一个大于或等于指定内容长度的数值，最多 65535 字节。

Within 的默认设置是搜索至数据包终点。

在 content 关键字中使用搜索位置选项

可以使用两个 content 位置对指定开始搜索指定内容的位置以及继续搜索的深度，如下所述：

- 同时使用 **Offset** 和 **Depth** 选项可相对于数据包负载起点进行搜索。
- 同时使用 **Distance** 和 **Within** 可相对于当前搜索位置进行搜索。

如果仅指定选项对中的其中一个选项，系统将会假设另一个选项使用默认值。

不能将 **Offset** 和 **Depth** 选项与 **Distance** 和 **Within** 选项混合使用。例如，不能将 **Offset** 和 **Within** 这两个选项配对。可以在规则中使用任意数量的位置选项。

如果未指定位置，系统将假设 **Offset** 和 **Depth** 选项为默认值；也就是说，将从数据包负载起点开始进行内容搜索，直至数据包终点。

还可以使用现有 byte_extract 变量指定位置选项的值。有关详细信息，请参阅第 23-75 页上的将数据包数据读取到关键字参数中。

要在 content 关键字中指定搜索位置值，请执行以下操作：

步骤 1 在字段中为添加的 content 关键字键入一个值。有以下选项可供选择：

- **Offset**
- **深度**

- **距离**
- **Within**

可以在规则中使用任意数量的位置选项。

步骤 2　继续创建或编辑规则。有关详细信息，请参阅第 23-16 页上的限制内容匹配、第 23-14 页上的搜索内容匹配、第 23-93 页上的编写新规则或第 23-95 页上的修改现有规则。

在 protected_content 关键字中使用搜索位置选项

将必填的 **Length** `protected_content` 选项与 **Offset** 或 **Distance** 位置选项结合使用，可指定开始搜索指定内容的位置以及继续搜索的深度，如下所示：

- 同时使用 **Length** 和 **Offset** 选项可相对于数据包负载起点搜索受保护字符串。
- 同时使用 **Length** 和 **Distance** 选项可相对于当前搜索位置搜索受保护字符串。

提示　不能在单个关键字配置中同时使用 **Offset** 和 **Distance** 选项，但可以在规则内使用任意数量的位置选项。

如果未指定位置，系统将假设使用默认值；也就是说，将从数据包负载起点开始进行内容搜索，直至数据包终点。

还可以使用现有 `byte_extract` 变量指定位置选项的值。有关详细信息，请参阅第 23-75 页上的将数据包数据读取到关键字参数中。

要在 protected_content 关键字中指定搜索位置值，请执行以下操作：

步骤 1　在字段中为添加的 `protected_content` 关键字键入一个值。有以下选项可供选择：

- **Length**（必填）
- **Offset**
- **距离**

不能在单个 `protected_content` 关键字配置中同时使用 **Offset** 和 **Distance** 选项，但可以在规则内使用任意数量的位置选项。

步骤 2　继续创建或编辑规则。有关详细信息，请参阅第 23-16 页上的限制内容匹配、第 23-14 页上的搜索内容匹配、第 23-93 页上的编写新规则或第 23-95 页上的修改现有规则。

HTTP 内容选项

许可证：保护

通过 HTTP `content` 或 `protected_content` 关键字选项，可以在 HTTP 检查预处理器解码的 HTTP 消息中指定搜索内容匹配项的位置。

以下两个选项搜索 HTTP 响应中的状态字段：

- **HTTP Status Code**
- **HTTP Status Message**

请注意，尽管规则引擎搜索未规范化的原始状态字段，但这里分别列出这些选项，以方便在下文解释将其他原始 HTTP 字段与规范化 HTTP 字段结合使用时应考虑的限制。

以下五个选项搜索 HTTP 请求和/或 HTTP 响应（视情况而定）中的规范化字段（有关详细信息，请参阅第 23-21 页上的 HTTP 内容选项）：

- **HTTP URI**
- **HTTP Method**
- **HTTP Header**
- **HTTP Cookie**
- **HTTP Client Body**

以下三个选项搜索 HTTP 请求和/或 HTTP 响应（视情况而定）中的（未规范化）原始非状态字段（有关详细信息，请参阅第 23-21 页上的 HTTP 内容选项）：

- **HTTP Raw URI**
- **HTTP Raw Header**
- **HTTP Raw Cookie**

选择 HTTP `content` 选项时，请遵循以下准则：

- HTTP `content` 选项仅适用于 TCP 流量。
- 为避免对性能造成负面影响，应只选择消息中那些可能出现指定内容的部分。

  例如，如果流量可能包含大型 cookie （例如，购物车消息中的 cookie），可以在 HTTP 报头中搜索指定内容，而不是在 HTTP cookie 中搜索。
- 为利用 HTTP 检查预处理器规范化以及提高性能，所创建的任何 HTTP 相关规则应包含至少一个已选择 **HTTP URI**、 **HTTP Method**、 **HTTP Header** 或 **HTTP Client Body** 选项的 `content` 或 `protected_content` 关键字。
- 不能将 `replace` 关键字与 HTTP `content` 或 `protected_content` 关键字选项配合使用。

可以指定单个规范化 HTTP 选项或状态字段，或者使用规范化 HTTP 选项与状态字段的任意组合，以指向要匹配的内容区域。但在使用 HTTP 字段选项时，请注意以下限制：

- 不能在同一个 `content` 或 `protected_content` 关键字中同时使用 **Raw Data** 选项和任何 HTTP 选项。
- 不能在同一个 `content` 或 `protected_content` 关键字中同时使用原始 HTTP 字段选项（**HTTP Raw URI**、**HTTP Raw Header** 或 **HTTP Raw Cookie**）及其对应的规范化选项（分别是 **HTTP URI**、**HTTP Header** 或 **HTTP Cookie**）。
- 不同同时选择 **Use Fast Pattern Matcher** 和以下一个或多个 HTTP 字段选项：

  HTTP Raw URI、**HTTP Raw Header**、**HTTP Raw Cookie**、**HTTP Cookie**、**HTTP Method**、**HTTP Status Message** 或 **HTTP Status Code**

  但是，可以在也使用快速模式匹配程序搜索以下其中一个规范化字段的 `content` 或 `protected_content` 关键字中包含上述选项：

  HTTP URI、 **HTTP Header** 或 **HTTP Client Body**

  例如，如果选择 **HTTP Cookie**、 **HTTP Header** 和 **Use Fast Pattern Matcher**，规则引擎将会在 HTTP cookie 和 HTTP 报头中搜索内容，但快速模式匹配程序仅适用于 HTTP 报头，而不适用于 HTTP cookie。
- 如果将受限选项和不受限选项结合使用，快速模式匹配程序将仅搜索您指定的不受限字段，以测试是否要将规则传递到规则编辑器以完成评估（包括受限字段的评估）。有关详细信息，请参阅第 23-25 页上的 Use Fast Pattern Matcher。

上述限制反映在以下列表内用于描述 HTTP `content` 和 `protected_content` 关键字选项的各选项描述中。

HTTP URI

选择此选项将会在规范化的请求 URI 字段中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP URI (U) 选项结合使用来搜索相同的内容。有关详细信息，请参阅特定于 Snort 的后正则表达式修饰符表。

注 管道化 HTTP 请求数据包包含多个 URI。如果选择了 **HTTP URI**，且规则引擎检测到管道化 HTTP 请求数据包，规则引擎将会搜索数据包中的所有 URI 以进行内容匹配。

HTTP Raw URI

选择此选项将会在规范化的请求 URI 字段中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP URI (U) 选项结合使用来搜索相同的内容。有关详细信息，请参阅特定于 Snort 的后正则表达式修饰符表。

注 管道化 HTTP 请求数据包包含多个 URI。如果选择了 **HTTP URI**，且规则引擎检测到管道化 HTTP 请求数据包，规则引擎将会搜索数据包中的所有 URI 以进行内容匹配。

HTTP Method

选择此选项将会在请求方法字段中搜索内容匹配，该字段确定要对 URI 中识别出的资源执行的操作（例如 GET 和 POST）。

HTTP Header

选择此选项将会在 HTTP 请求内的规范化报头字段（cookie 除外）中搜索内容匹配；如果 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项已启用，还会在响应中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP 报头 (H) 选项结合使用来搜索相同的内容。有关详细信息，请参阅特定于 Snort 的后正则表达式修饰符表。

HTTP Raw Header

选择此选项将会在 HTTP 请求内的原始报头字段（cookie 除外）中搜索内容匹配；如果 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项已启用，还会在响应中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP 原始报头 (D) 选项结合使用来搜索相同的内容。有关详细信息，请参阅特定于 Snort 的后正则表达式修饰符表。

HTTP Cookie

选择此选项将会在规范化 HTTP 客户端请求报头内识别出的任何 cookie 中搜索内容匹配；如果 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项已启用，还会在响应 set-cookie 数据中搜索内容匹配。请注意，系统将消息正文中包含的 cookie 看作正文内容。

若要仅对 cookie 进行内容匹配搜索，必须启用 HTTP 检查预处理器的 **Inspect HTTP Cookies** 选项；否则，规则引擎将搜索包括 cookie 在内的整个报头。有关详细信息，请参阅第 15-29 页上的选择服务器级别 HTTP 规范化选项。

请注意：

- 不能将此选项与 `pcre` 关键字 HTTP cookie (C) 选项结合使用来搜索相同的内容。有关详细信息，请参阅特定于 Snort 的后正则表达式修饰符表。
- `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。

HTTP Raw Cookie

选择此选项将会在原始 HTTP 客户端请求报头内识别出的任何 cookie 中搜索内容匹配；如果 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项已启用，还会在响应 set-cookie 数据中搜索内容匹配；请注意，系统将消息正文中包含的 cookie 看作正文内容。

若要仅对 cookie 进行内容匹配搜索，必须启用 HTTP 检查预处理器的 **Inspect HTTP Cookies** 选项；否则，规则引擎将搜索包括 cookie 在内的整个报头。有关详细信息，请参阅第 15-29 页上的选择服务器级别 HTTP 规范化选项。

请注意：

- 不能将此选项与 `pcre` 关键字 HTTP 原始 cookie (K) 选项结合使用来搜索相同的内容。有关详细信息，请参阅特定于 Snort 的后正则表达式修饰符表。
- `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。

HTTP Client Body

选择此选项将会在 HTTP 客户端请求消息正文中搜索内容匹配。

请注意，要使此选项起作用，必须为 HTTP 检查预处理器的 **HTTP Client Body Extraction Depth** 选项指定一个 0 到 65535 之间的值。有关详细信息，请参阅第 15-29 页上的选择服务器级别 HTTP 规范化选项。

HTTP Status Code

选择此选项将会在 HTTP 响应的三位数状态代码中搜索内容匹配。

要使此选项能够返回匹配，必须启用 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项。有关详细信息，请参阅第 15-29 页上的选择服务器级别 HTTP 规范化选项。

HTTP Status Message

选择此选项将会在 HTTP 响应中状态代码随附的文字描述中搜索内容匹配。

要使此选项能够返回匹配，必须启用 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项。有关详细信息，请参阅第 15-29 页上的选择服务器级别 HTTP 规范化选项。

要在进行 TCP 流量内容搜索时指定 HTTP 选项，请执行以下操作：

步骤 1　或者，要利用 HTTP 检查预处理器规范化以及提高性能，请选择：

- 为添加的 `content` 或 `protected_content` 关键字至少选择 **HTTP URI**、 **HTTP Raw URI**、 **HTTP Method**、 **HTTP Header**、 **HTTP Raw Header** 或 **HTTP Client Body** 选项之一
- **HTTP Cookie** 或 **HTTP Raw Cookie** 选项

步骤 2　继续创建或编辑规则。有关详细信息，请参阅第 23-16 页上的限制内容匹配、第 23-14 页上的搜索内容匹配、第 23-93 页上的编写新规则或第 23-95 页上的修改现有规则。

Use Fast Pattern Matcher

许可证：保护

注　配置 protected_content 关键字时，这些选项**不**可用。有关详细信息，请参阅第 23-14 页上的使用 protected_content 关键字。

快速模式匹配程序快速确定在将数据包传递到规则引擎之前要对哪些规则进行评估。这项初步工作可大大减少用于数据包评估的规则数量，从而提高性能。

默认情况下，快速模式匹配程序会在数据包内搜索规则中指定的最长内容；这样可最大程度地消除不必要的规则评估。以如下规则片段为例：

```
alert tcp any any -> any 80 (msg:"Exploit"; content:"GET";
http_method; nocase; content:"/exploit.cgi"; http_uri;
nocase;)
```

几乎所有 HTTP 客户端请求都包含内容 GET，但很少会包含 /exploit.cgi。使用 GET 作为快速模式内容将会导致规则引擎在大多数情况下评估此规则，但极少会产生匹配。但是，对于大多数客户端 GET 请求，将不会使用 /exploit.cgi 对其进行评估，从而提高性能。

规则引擎仅在快速模式匹配程序检测到指定内容时根据规则评估数据包。例如，如果某个规则中的三个 content 关键字分别指定内容 short、 longer 和 longest，快速模式匹配程序将使用内容 longest，并且仅在规则引擎在负载中找到 longest 的情况下对该规则进行评估。

可以使用 **Use Fast Pattern Matcher** 选项为快速模式匹配程序指定较短的搜索模式。理想情况下，指定的模式在数据包中被找到的可能性低于最长模式，因此，因此能够更具体地识别所针对的漏洞。

在同一个 content 关键字中选择 **Use Fast Pattern Matcher** 和其他选项时，请注意以下限制：

- 只能为每个规则指定一次 **Use Fast Pattern Matcher**。
- 如果同时选择 **Use Fast Pattern Matcher** 和 **Not**，将不能使用 **Distance**、 **Within**、 **Offset** 和 **Depth**。
- 不同同时选择 Use Fast Pattern Matcher 和以下任何 HTTP 字段选项：

  HTTP Raw URI、**HTTP Raw Header**、**HTTP Raw Cookie**、**HTTP Cookie**、**HTTP Method**、**HTTP Status Message** 或 **HTTP Status Code**

  但是，可以在也使用快速模式匹配程序搜索以下其中一个规范化字段的 content 关键字中包含上述选项：

  HTTP URI、 **HTTP Header** 或 **HTTP Client Body**

  例如，如果选择 **HTTP Cookie**、 **HTTP Header** 和 **Use Fast Pattern Matcher**，规则引擎将会在 HTTP cookie 和 HTTP 报头中搜索内容，但快速模式匹配程序仅适用于 HTTP 报头，而不适用于 HTTP cookie。

  请注意，不能在同一个 content 关键字中同时使用原始 HTTP 字段选项（**HTTP Raw URI**、**HTTP Raw Header** 或 **HTTP Raw Cookie**）和对应的规范化选项（分别是 **HTTP URI**、**HTTP Header** 或 **HTTP Cookie**）。有关详细信息，请参阅第 23-21 页上的HTTP 内容选项。

  如果将受限选项和不受限选项结合使用，快速模式匹配程序将仅搜索您指定的不受限字段，以测试是否要将数据包传递到规则引擎以完成评估（包括受限字段的评估）。
- 或者，如果选择 **Use Fast Pattern Matcher**，还可以选择 **Fast Pattern Matcher Only** 或 **Fast Pattern Matcher Offset and Length** 选项，但不能同时选择这两个选项。
- 检查 Base64 数据时，不能使用快速模式匹配程序；有关详细信息，请参阅第 23-91 页上的解码和检查 Base64 数据。

仅使用快速模式匹配程序

通过 **Fast Pattern Matcher Only**，可以仅将 `content` 关键字作为快速模式匹配程序选项，而不作为规则选项。如果无需规则引擎评估指定的内容，可以使用此选项来节省资源。例如，假设规则仅要求内容 `12345` 位于负载中的任何位置。如果快速模式匹配程序检测到该模式，可根据规则中的其他关键字对数据包进行评估。规则引擎无需重新评估数据包来确定其是否包含模式 `12345`。

如果规则包含其他与指定内容相关的状况，无需使用此选项。例如，如果另一个规则条件尝试确定 `abcd` 是否出现在 `1234` 之前，将无需使用此项选项搜索内容 `1234`。在这种情况下，规则引擎无法确定相对位置，因为选择 **Fast Pattern Matcher Only** 将会指示规则引擎不搜索指定内容。

使用此选项时请注意：

- 指定的内容与位置无关，也就是说，该内容可出现在负载中的任何位置；因此，不能使用位置选项（**Distance**、**Within**、**Offset**、**Depth** 或 **Fast Pattern Matcher Offset and Length**）。
- 不能将此选项与 **Not** 结合使用。
- 不能将此选项与 **Fast Pattern Matcher Offset and Length** 结合使用。
- 指定的内容将被视为不区分大小写，因为所有模式均以不区分大小写的方式插入到快速模式匹配程序中；系统会自动处理这种情况，因此您无需在选择此选项时选择 **Case Insensitive**。
- 不可在使用 **Fast Pattern Matcher Only** 选项的 `content` 关键字后紧接着使用以下关键字（这些关键字设置相对于当前搜索位置的搜索位置）：
- `isdataat`
- `pcre`
- `content`（在选择了 **Distance** 或 **Within** 的情况下）
- `content`（在选择了 **HTTP URI** 的情况下）
- `asn1`
- `byte_jump`
- `byte_test`
- `byte_extract`
- `base64_decode`

指定快速模式匹配程序偏移量和长度

使用 **Fast Pattern Matcher Offset and Length** 选项可指定要搜索的部分内容。如果模式很长，且只需模式的一部分即足以识别出可能是匹配的规则，使用此选项可减少内存消耗。如果快速模式匹配程序选择了某个规则，将会根据该规则评估整个模式。

可以确定快速模式匹配程序要使用的部分，方法是，使用以下语法以字节为单位指定搜索的开始位置（偏移量）以及搜索内容的深入度（长度）：

`offset,length`

例如，对于以下内容：

```
1234567
```

如果如下指定偏移量和长度字节数：

```
1,5
```

快速模式匹配器将仅搜索内容 `23456`。

请注意，不能将此选项与 **Fast Pattern Matcher Only** 结合使用。

要指定快速模式匹配程序要搜索的内容，请执行以下操作：

步骤 1　为添加的 `content` 关键字选择 **Use Fast Pattern Matcher**。

步骤 2　或者，选择 **Fast Pattern Matcher Only**，以确定在无规则引擎评估的情况下数据包中是否存在指定模式。

仅在快速模式匹配程序检测到指定内容的情况下，才会继续评估。

步骤 3　或者，使用以下语法在 **Fast Pattern Matcher Offset and Length** 选项中指定要在其中搜索内容的部分模式：

```
offset,length
```

其中，*`offset`* 指定从内容开头到搜索开始位置之间的字节数，*`length`* 指定继续搜索的字节数。

步骤 4　继续创建或编辑规则。有关详细信息，请参阅第 23-16 页上的限制内容匹配、第 23-32 页上的使用 PCRE 搜索内容、第 23-93 页上的编写新规则或第 23-95 页上的修改现有规则。

替换内联部署中的内容

许可证：保护

可以在内嵌部署中使用 `replace` 关键字替换指定内容。

要使用 `replace` 关键字，请构建一个使用 `content` 关键字来查找特定字符串的自定义标准文本规则。然后使用 `replace` 关键字指定一个字符串，以替换该内容。替代值和内容值必须是相同长度的字符串。

注　**不能**使用 `replace` 关键字替换 `protected_content` 关键字中的哈希内容。有关详细信息，请参阅第 23-14 页上的使用 protected_content 关键字。

或者，可以用引号将替代字符串引起来，以便向后兼容以前的 ASA FirePOWER 模块软件版本。如果不加引号，替代字符串将被自动添加到规则，以使规则在语法上正确。要将前引号或后引号纳入为替代文本的一部分，必须使用反斜杠对引号进行转义，如以下示例所示：

```
"replacement text plus \"quotation\" marks""
```

每个规则可包含多个 `replace` 关键字，但只能包含一个 `content` 关键字。只会替换规则找到的内容中的第一个实例。

下面介绍 `replace` 关键字的使用示例：

- 如果系统检测到传入数据包包含漏洞，您可以使用一个无害字符串来替换该恶意字符串。有时，这种方法比单纯地丢弃违规数据包更有效。在某些攻击场景中，攻击者只需重新发送被丢弃的数据包，直至该数据包绕过网络防御或对网络造成泛洪攻击。通过将一个字符串替换为另一个字符串（而非丢弃数据包），可以令攻击者相信其攻击的目标并非易受攻击。
- 如果您担心侦察攻击，这类攻击试图了解是您否正在运行易受攻击版本的设备（例如，网络服务器），则您可以检测传出数据包，并将横幅替换为自己的文本。

注　请确保在要其中使用替换规则的内联入侵规则中将规则状态设置为 Generate Events；如果将规则设置为 Drop and Generate events，将会导致数据包被丢弃，进而造成无法替换内容。

在字符串替换过程中，该系统会自动更新数据包校验和，以使目标主机可以毫无差错地接收数据包。

请注意，不能将 replace 关键字与 HTTP 请求消息的 content 关键字选项结合使用。有关详细信息，请参阅第 23-14 页上的搜索内容匹配和第 23-21 页上的 HTTP 内容选项。

要在内联部署中替换内容，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **content** 并点击 **Add Option**。

系统将显示 content 关键字。

步骤 2　在 **content** 字段中指定要检测的内容，如有需要，还可以选择任何适用参数。请注意，不能将 HTTP 请求消息的 content 关键字选项与 replace 关键字结合使用。

步骤 3　从下拉列表中选择 **replace** 并点击 **Add Option**。

replace 关键字将显示在 content 关键字下方。

步骤 4　在 **replace:** 字段中为指定内容指定替代字符串。

使用 Byte_Jump 和 Byte_Test

许可证：保护

可以使用 byte_jump 和 byte_test 来计算规则引擎应在数据包中的哪个位置开始测试数据匹配以及应评估哪些字节。

还可以使用 byte_jump 和 byte_test **DCE/RPC** 参数来定制 DCE/RPC 预处理器处理的流量的关键字。如果使用 **DCE/RPC** 参数时，还可以将 byte_jump 和 byte_test 与其他特定 DCE/RPC 关键字一起使用。有关详细信息，请参阅第 15-2 页上的解码 DCE/RPC 流量和第 23-54 页上的 DCE/RPC 关键字。

有关详细信息，请参阅：

- 第 23-28 页上的 byte_jump
- 第 23-30 页上的 byte_test

byte_jump

许可证：保护

byte_jump 关键字首先计算指定字节段中定义的字节数，然后在数据包中跳过该数量的字节 - 可以从指定字节段的末尾向前跳，也可以从数据包负载起点向前跳，具体取决于指定的选项。这对于具有如下特点的数据包很有用：数据包中的特定字节段描述数据包所包含的变量数据。

下表介绍了 byte_jump 关键字所需的参数。

表 23-8　所需的 byte_jump 参数

参数	说明
字节	从数据包进行计算的字节数。
Offset	从负载开头到开始进行处理之间的字节数。偏移量计数器从字节 0 开始计数，因此，应该如下计算 offset 值：用从数据包负载起点或上一次成功内容匹配起向前跳所需的字节数减去 1。 还可以使用现有 byte_extract 变量指定此参数的值。有关详细信息，请参阅第 23-75 页上的将数据包数据读取到关键字参数中。

下表介绍了可用于定义系统如何解释您为必需参数指定的值的选项。

表 23-9　其他可选 byte_jump 参数

参数	说明
Relative	使偏移量相对于上一次成功内容匹配中找到的上一个模式。
调整	将转换的字节数四舍五入为下一个 32 位边界。
倍数	指明规则引擎应将其与从数据包获取的 `byte_jump` 值相乘的值，以获得最终的 `byte_jump` 值。 也就是说，规则引擎跳过一个与您通过 Multiplier 参数指定的整数相乘的字节数，而不是跳过指定字节段中定义的字节数。
Post Jump Offset	应用其他 `byte_jump` 参数后要向前跳或向后跳的字节数（-63535 到 63535）。选择正值将会向前跳，选择负值将会向后跳。将此字段留空或输入 `0` 将会禁用此字段。 有关选择 **DCE/RPC** 参数后不适用的 `byte_jump` 参数，请参阅字节顺序参数表中的 **DCE/RPC** 参数。
From Beginning	指明规则引擎应从数据包负载起点跳过负载中指定的字节数，而不是从指定要跳过的字节数的字节段末尾跳过。

只能指定 **DCE/RPC**、 **Endian** 或 **Number Type**。

如果要定义 `byte_jump` 关键字如何计算字节，可以从下表所述的参数中进行选择（如果没有指定参数，将使用网络字节顺序）。

表 23-10　字节顺序参数

参数	说明
Big Endian	按大端字节顺序处理数据（大端字节顺序是默认的网络字节顺序）。
Little Endian	按小端字节顺序处理数据
DCE/RPC	指定 DCE/RPC 预处理器处理的流量的 `byte_jump` 关键字。有关详细信息，请参阅第 15-2 页上的解码 DCE/RPC 流量。 由 DCE/RPC 预处理器确定大端字节顺序或小端字节顺序， **Number Type**、**Endian** 和 **From Beginning** 参数不适用。 如果启用此参数，还可以将 `byte_jump` 与其他特定 DCE/RPC 关键字结合使用。有关详细信息，请参阅第 23-54 页上的 DCE/RPC 关键字。

使用下表所列的其中一个参数来定义系统如何查看数据包中的字符串。

表 23-11　数字类型参数

参数	说明
Hexadecimal String	使用十六进制格式表示转换的字符串数据。
Decimal String	使用十进制格式表示转换的字符串数据。
Octal String	使用八进制格式表示转换的字符串数据。

例如，如果如下设置 byte_jump 的值：

- Bytes = 4
- Offset = 12
- Relative 已启用
- Align 已启用

规则引擎将会计算自上一次成功内容匹配后显示的 13 个字节当中 4 个字节中描述的数量，并向前跳过数据包中该数量的字节。例如，如果特定数据包中计算出的 4 个字节是 00 00 00 1F，规则引擎会将它转换为 31。由于指定了 align （指示引擎移到下一个 32 位边界），因此，规则引擎将在数据包中向前跳过 32 个字节。

或者，如果如下设置 byte_jump 的值：

- Bytes = 4
- Offset = 12
- From Beginning 已启用
- Multiplier = 2

规则引擎将会计算在数据包起点后显示的 13 个字节当中 4 个字节中描述的数值。然后，引擎会将该数值乘以 2，以获得将要跳过的字节总数。例如，如果特定数据包中计算出的 4 个字节是 00 00 00 1F，规则引擎会将它转换为 31，然后再乘以 2 以得到 62。由于启用了 From Beginning，因此，规则引擎会跳过数据包中的前 63 个字节。

要使用 byte_jump，请执行以下操作：

步骤 1　从下拉列表中选择 byte_jump 并点击 **Add Option**。

byte_jump 部分将显示在上次选择的关键字下方。

byte_test

许可证：保护

byte_test 关键字会计算指定字节段中的字节数，并将计算出的字节数与您指定的运算符和值作比较。

下表介绍了 byte_test 关键字所需的参数。

表 23-12　所需的 byte_test 参数

参数	说明
字节	从数据包进行计算的字节数。可指定 1 到 10 字节。
Operator and Value	将指定值与 <、 >、 =,、 !、 &、 ^、 !>、 !<、 !=、 !& 或 !^ 作比较。 例如，如果指定 !1024，byte_test 将会转换该指定数字，且如果该数字不等于 1024，则会生成事件（如果其他所有关键字参数都匹配）。 请注意，! 和 != 是等效的。 还可以使用现有 byte_extract 变量指定此参数的值。有关详细信息，请参阅第 23-75 页上的将数据包数据读取到关键字参数中。

表 23-12　所需的 byte_test 参数 （续）

参数	说明
Offset	从负载开头到开始进行处理之间的字节数。偏移量计数器从字节 0 开始计数，因此，应该如下计算 `offset` 值：用从数据包负载起点或上一次成功内容匹配起向前计算所需的字节数减去 1。 还可以使用现有 `byte_extract` 变量指定此参数的值。有关详细信息，请参阅第 23-75 页上的将数据包数据读取到关键字参数中。

可以用下表中所述的参数进一步定义系统如何使用 `byte_test` 参数。

表 23-13　其他可选 byte_test 参数

参数	说明
Relative	使偏移量相对于上一次成功模式匹配。
调整	将转换的字节数四舍五入为下一个 32 位边界。

只能指定 **DCE/RPC**、 **Endian** 或 **Number Type**。

要定义 `byte_test` 关键字如何计算其测试的字节，请从下表中选择参数。如果未指定参数，将使用网络字节顺序。

表 23-14　字节顺序 byte_test 参数

参数	说明
Big Endian	按大端字节顺序处理数据（大端字节顺序是默认的网络字节顺序）。
Little Endian	按小端字节顺序处理数据
DCE/RPC	指定 DCE/RPC 预处理器处理的流量的 `byte_test` 关键字。有关详细信息，请参阅第 15-2 页上的解码 DCE/RPC 流量。 由 DCE/RPC 预处理器确定大端字节顺序或小端字节顺序， **Number Type** 和 **Endian** 参数不适用。 如果启用此参数，还可以将 `byte_test` 与其他特定 DCE/RPC 关键字结合使用。有关详细信息，请参阅第 23-54 页上的 DCE/RPC 关键字。

可以使用下表所列的其中一个参数来定义系统如何在数据包中查看字符串。

表 23-15　数字类型 byte-test 参数

参数	说明
Hexadecimal String	使用十六进制格式表示转换的字符串数据。
Decimal String	使用十进制格式表示转换的字符串数据。
Octal String	使用八进制格式表示转换的字符串数据。

例如，如果如下指定 `byte_test` 的值：

- Bytes = 4
- Operator and Value > 128

- Offset = 8
- Relative 已启用

规则引擎会计算自（相对于）上一次成功内容匹配后显示的 9 个字节当中 4 个字节中描述的数值，如果计算出的数值大于 128 字节，将触发规则。

要使用 byte_test，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 `byte_test` 并点击 **Add Option**。

`byte_test` 部分将显示在上次选择的关键字下方。

使用 PCRE 搜索内容

许可证：保护

`pcre` 关键字使您可以使用兼容 Perl 的正则表达式 (PCRE) 为指定的内容检查数据包负载。使用 PCRE 可避免编写以匹配相同内容的细微变化为目的的多个规则。

搜索可以多种方式显示的内容时，正则表达式很有用。内容可能有不同的属性；在尝试从数据包负载中查找内容时，您会需要考虑其属性。

请注意，入侵规则使用的正则表达式语法是完整正则表达式库的一个子集，并该库中所用命令的语法在某些方面存在不同之处。使用规则编辑器添加 `pcre` 关键字时，请按以下格式输入完整的值：

```
!/pcre/ ismxAEGRBUIPHDMCKSY
```

其中：

- !是可选的否定式（如果想匹配**不**匹配的正则表达式的模式，请使用此否定式）。
- */pcre/*是一个兼容 Perl 的正则表达式。
- `ismxAEGRBUIPHDMCKSY` 是修饰符选项的任意组合。

另请注意，在 PCRE 中使用下表所列字符在数据包负载中搜索特定内容时，必须对这些字符进行转义，以使规则引擎能正确地解释这些字符。

表 23-16　　转义 PCRE 字符

必须转义的字符.....	使用反斜杠.....	或使用十六进制代码.....
# （哈希标记）	\#	\x23
; （分号）	\;	\x3B
| （竖线）	\\|	\x7C
: （冒号）	\:	\x3A

提示　或者，可以用引号将兼容 Perl 的正则表达式引起来，例如，*pcre_expression* 或 “*pcre_expression*”。这一做法适合习惯使用旧版本的有经验的用户（旧版本要求必须用引号将正则表达式引起来）。规则在保存后再显示时，规则编辑器不会显示引号。

还可以使用 m?regex?，其中，?是除 / 以外的分隔符。如果需要在正则表达式中匹配一个正斜杠，但不想用一个反斜杠来进行转义，可能需要使用此分隔符。例如，可以使用 m?*regex*?ismxAEGRBUIPHDMCKSY，其中 *regex* 是兼容 Perl 的正则表达式，ismxAEGRBUIPHDMCKSY 是修饰符选项的任意组合。有关正则表达式语法的详细信息，请参阅第 23-33 页上的有关兼容 Perl 的正则表达式的基础知识。

以下各节提供了有关为 pcre 关键字构建有效值的详细信息：

- 第 23-33 页上的有关兼容 Perl 的正则表达式的基础知识介绍用于兼容 Perl 的正则表达式中的常见语法。
- 第 23-34 页上的PCRE 修饰符选项介绍可用于修改正则表达式的选项。
- 第 23-37 页上的PCRE 关键字值示例提供了 pcre 关键字在规则中的使用示例。

有关兼容 Perl 的正则表达式的基础知识

许可证：保护

pcre 关键字接受兼容 Perl 的正则表达式 (PCRE) 标准语法。以下各节介绍这种语法。

提示 尽管本节介绍可用于 PCRE 的基本语法，但您可能想要参阅专门关于 Perl 和 PCRE 的网上参考资料或书籍，以获取更多高级信息。

元字符

许可证：保护

元字符是在正则表达式中具有特殊含义的原义字符。在正则表达式中使用元字符时，必须通过在元字符前添加一个反斜杠来对其进行“转义”。

下表举例说明可用于 PCRE 的元字符。

表 23-17　PCRE 元字符

元字符	说明	示例
.	匹配除换行符以外的任何字符。如果将 s 用作修饰选项，还将匹配换行符。	abc.匹配 abcd、 abc1、 abc# 等等。
*	匹配字符或表达式的零次或多次出现次数。	abc* 匹配 abc、 abcc、 abccc、 abccccc 等等。
?	匹配字符或表达式的零次或一次出现次数。	abc?匹配 abc。
+	匹配字符或表达式的一次或多次出现次数。	abc+ 匹配 abc、 abcc、 abccc、 abccccc 等等。
()	组表达。	(abc)+ 匹配 abc、 abcabc、 abcabcabc 等等。
{}	为字符或表达式指定匹配项数限制。如果要设置下限和上限，请用逗号将下限和上限隔开。	a{4,6} 匹配 aaaa、 aaaaa 或 aaaaaa。 (ab){2} 匹配 abab。
[]	允许定义字符类，并匹配字符集中包含的任意字符或字符组合。	[abc123] 匹配 a、 b 或 c 等等。
^	匹配字符串开头的内容。如果在字符类中使用，也可用于否定。	^in 匹配 info 中的“in”，但不匹配 bin 中的“in”。 [^a] 匹配不包含 a 的任何内容。
??	匹配字符串结尾的内容。	ce$ 匹配 announce 中的“ce”，但不匹配 cent 中的“ce”。

表 23-17　PCRE 元字符（续）

元字符	说明	示例
|	指示 OR 表达式。	(MAILTO|HELP) 匹配 MAILTO 或 HELP。
\	元字符可用作实际字符，还可用于指定预定义的字符类。	\. 匹配句号，* 匹配星号，\\ 匹配反斜线，依此类推。\d 匹配数字字符，\w 匹配字母数字字符，依此类推。有关 PCRE 中使用的字符类的详细信息，请参阅第 23-34 页上的字符类。

字符类

许可证：保护

字符类包括字母字符、数字字符、字母数字字符和空白字符。可以用方括号（参阅第 23-33 页上的元字符）创建自己的字符类，也可以使用预定义类作为不同字符类型的快捷方式。如果不与其他限定符配合使用，一个字符类通常匹配一个数字或字符。

下表举例说明 PCRE 接受的预定义字符类。

表 23-18　PCRE 字符类

字符类	说明	字符类定义
\d	匹配数字字符（“数字”）。	[0-9]
\D	对应不是数字字符的任何字符。	[^0-9]
\w	匹配字母数字字符（“单词”）。	[a-zA-Z0-9_]
\W	匹配不是字母数字字符的任何字符。	[^a-zA-Z0-9_]
\s	匹配空白字符，包括空格、回车符、制表符、换行符和换页符。	[\r\t\n\f]
\S	匹配不是空白字符的任何字符。	[^ \r\t\n\f]

PCRE 修饰符选项

许可证：保护

指定 pcre 关键字值中的正则表达式语法后，可以使用修饰选项。这些修饰符执行特定于 Perl、PCRE 和Snort 的处理功能。修饰符始终按以下格式显示在 PCRE 值的末尾：

/*pcre*/ismxAEGRBUIPHDMCKSY

其中，ismxAEGRBUPHMC 可以包括下表中的任何修饰选项。

提示　或者，可以用引号将正则表达式和任何修饰选项引起来，例如，“/pcre/ismxAEGRBUIPHDMCKSY”。这一做法适合习惯使用旧版本的有经验的用户（旧版本要求必须用引号将正则表达式引起来）。规则在保存后再显示时，规则编辑器不会显示引号。

下表介绍了可用于执行 Perl 处理功能的选项。

表 23-19　Perl 相关的后正则表达式选项

选项	说明
i	使正则表达式不区分大小写。
s	点字符 (.) 匹配除换行符和 \n 字符以外的所有字符。可使用 "s" 选项覆盖此选项，这样，点字符将匹配所有字符（包括换行符）。
m	默认情况下，一个字符串被视为单行字符，^ 和 $ 分别匹配特定字符串的开头和结尾。如果使用 "m" 代替选项，^ 和 $ 将匹配紧接在缓冲区内所有换行符之前或之后的内容，以及位于缓冲区开头或结尾的内容。
x	忽略可能在这一模式中出现的空白数据字符，除非其为转义字符（前面加有反斜杠）或包含在字符类中。

下表介绍了可用于正则表达式后的 PCRE 修饰符。

表 23-20　PCRE 相关的后正则表达式选项

选项	说明
A	模式必须在字符串开头进行匹配（与在正则表达式中使用 ^ 具有相同的效果）。
E	将 $ 设置为只在目标字符串结尾进行匹配。（如果最后一个字符是换行符，即使没有E， $ 也会匹配紧接在该字符之前的内容，但不会匹配任何其他换行符之前的内容）。
G	默认情况下， * + 和 ?是“贪婪”的，这意味着，如果找到两个或更多匹配项，将会选择最长的匹配项。使用 G 字符可使这些字符在后面无问号字符 (?)的情况下总是选择第一个匹配项。例如，在使用 G 修饰符的构造中， *?+?和 ?? 将是贪婪字符，*、 + 或 ? 在不附带问号的情况下将是 非贪婪字符。

下表介绍了可用于正则表达式后的 Snort 特定修饰符。

表 23-21　特定于 Snort 的后正则表达式修饰符

选项	说明
R	相对于规则引擎上一次找到的匹配项的结尾搜索匹配的内容。
B	在未被预处理器解码的数据中搜索内容（此选项类似于使用带有 content 或 protected_content 关键字的 Raw Data 参数）。
你	在已由 HTTP 检查预处理器解码的规范化 HTTP 请求消息的 URI 中搜索内容。请注意，不能将此选项与 content 或 protected_content 关键字的 **HTTP URI** 选项结合使用来搜索相同的内容。有关详细信息，请参阅第 23-21 页上的 HTTP 内容选项。 **注**　管道化 HTTP 请求数据包包含多个 URI。包含 U 选项的 PCRE 表达式使规则引擎仅在管道化 HTTP 请求数据包的第一个 URI 中搜索内容匹配。要搜索数据包中的所有 URI，请使用已选择 **HTTP URI** 的 content 或 protected_content 关键字（可随附或不随附使用 U 选项的 PCRE 表达式）。
I	在已由 HTTP 检查预处理器解码的原始 HTTP 请求消息的 URI 中搜索内容。请注意，不能将此选项与 content 或 protected_content 关键字 **HTTP Raw URI** 选项结合使用来搜索相同的内容。有关详细信息，请参阅第 23-21 页上的 HTTP 内容选项。
P	在已由 HTTP 检查预处理器解码的规范化 HTTP 请求消息的正文中搜索内容。有关详细信息，请参阅第 23-21 页上的 HTTP 内容选项中的 content 和 protected_content 关键字 **HTTP Client Body** 选项。

表 23-21　特定于 Snort 的后正则表达式修饰符（续）

选项	说明
H	在已由 HTTP 检查预处理器解码的 HTTP 请求或响应消息的报头（不包括 cookie）中搜索内容。请注意，不能将此选项与 `content` 或 `protected_content` 关键字 **HTTP Header** 选项结合使用来搜索相同的内容。有关详细信息，请参阅第 23-21 页上的 HTTP 内容选项。
D	在已由 HTTP 检查预处理器解码的原始 HTTP 请求或响应消息的报头（不包括 cookie）中搜索内容。请注意，不能将此选项与 `content` 或 `protected_content` 关键字 **HTTP Raw Header** 选项结合使用来搜索相同的内容。有关详细信息，请参阅第 23-21 页上的 HTTP 内容选项。
M	在已由 HTTP 检查预处理器解码的规范化 HTTP 请求消息的方法字段中搜索内容；该方法字段确定要对 URI 中识别出的资源执行的操作（例如，GET、PUT、CONNECT 等）。有关详细信息，请参阅第 23-21 页上的 HTTP 内容选项中的 `content` 和 `protected_content` 关键字 **HTTP Method** 选项。
C	如果 HTTP 检查预处理器的 **Inspect HTTP Cookies** 选项已启用，将会在 HTTP 请求报头的任何 cookie 中搜索规范化内容；如果该预处理器的 **Inspect HTTP Responses** 选项已启用，还会在 HTTP 响应报头的任何 set-cookie 中搜索规范化内容。如果未启用 **Inspect HTTP Cookies** 选项，将会搜索包括 cookie 或 set-cookie 数据在内的整个报头。 请注意： • 消息正文中包含的 cookie 将被视为正文内容。 • 不能将此选项与 `content` 或 `protected_content` 关键字 **HTTP Cookie** 选项结合使用来搜索相同的内容。有关详细信息，请参阅第 23-21 页上的 HTTP 内容选项。 • `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。
K	如果 HTTP 检查预处理器的 **Inspect HTTP Cookies** 选项已启用，将会在 HTTP 请求报头的任何 cookie 中搜索原始内容；如果该预处理器的 **Inspect HTTP Responses** 选项已启用，还会在 HTTP 响应报头的任何 set-cookie 中搜索原始内容。如果未启用 **Inspect HTTP Cookies** 选项，将会搜索包括 cookie 或 set-cookie 数据在内的整个报头。 请注意： • 消息正文中包含的 cookie 将被视为正文内容。 • 不能将此选项与 `content` 或 `protected_content` 关键字 **HTTP Raw Cookie** 选项结合使用来搜索相同的内容。有关详细信息，请参阅第 23-21 页上的 HTTP 内容选项。 • `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。
S	搜索 HTTP 响应中的三位数状态代码。有关详细信息，请参阅第 23-21 页上的 HTTP 内容选项中的 `content` 和 `protected_content` 关键字 **HTTP Status Code** 选项。
有	搜索 HTTP 响应中状态代码随附的文字描述。有关详细信息，请参阅第 23-21 页上的 HTTP 内容选项中的 `content` 和 `protected_content` 关键字 **HTTP Status Message** 选项。

注　请勿将 U 选项与 R 选项结合使用，否则可能会导致性能问题。此外，请勿将 U 选项与任何其他 HTTP 内容选项（I、P、H、D、M、C、K、S 或 Y）结合使用。

PCRE 关键字值示例

许可证：保护

以下示例显示可为 pcre 输入的值，并说明每个示例将会匹配的内容。

- **/feedback[(\d{0,1})]?\.cgi/U**

  此示例搜索 feedback 的数据包负载， feedback 后面紧跟着零个或一个数字字符，再紧跟着 .cgi，且仅在 URI 数据中进行搜索。

  此示例将匹配：

- feedback.cgi
- feedback1.cgi
- feedback2.cgi
- feedback3.cgi

  此示例不匹配：

- feedbacka.cgi
- feedback11.cgi
- feedback21.cgi
- feedbackzb.cgi
- **/^ez(\w{3,5})\.cgi/iU**

  此示例在字符串开头搜索 ez 的数据包负载，ez 后面跟有一个包含 3 到 5 个字母的单词，该单词后面跟着 .cgi。此搜索不区分大小写，且仅搜索 URI 数据。

  此示例将匹配：

- EZBoard.cgi
- ezman.cgi
- ezadmin.cgi
- EZAdmin.cgi

  此示例不匹配：

- ezez.cgi
- fez.cgi
- abcezboard.cgi
- ezboardman.cgi
- **/mail(file|seek)\.cgi/U**

  此示例在 URI 数据中搜索后面跟有 file 或 seek 的 mail 的数据包负载。

  此示例将匹配：

- mailfile.cgi
- mailseek.cgi

  此示例不匹配：

- MailFile.cgi
- mailfilefile.cgi
- **m?http\\x3a\x2f\x2f.*(\n|\t)+?U**

  此示例跟在任意数量字符后面的 HTTP 请求中为制表符或换行符搜索 URI 内容的数据包负载。此示例使用 m?*regex*?来避免在表达式中使用 http\:\/\/。请注意，冒号前面有一个反斜杠。

  此示例将匹配：

- http://www.example.com?scriptvar=x&othervar=\n\..\..

- `http://www.example.com?scriptvar=\t`

  此示例不匹配：

- `ftp://ftp.example.com?scriptvar=&othervar=\n\..\..`
- `http://www.example.com?scriptvar=|/bin/sh -i|`
- **`m?http\\x3a\x2f\x2f.*=\|.*\|+?sU`**

  此示例为带有任意数量字符（包括换行符）的 URL 搜索数据包负载，后面跟有一个等号以及包含任意数量字符或空白字符的竖线。此示例使用 `m?`*`regex`*`?`来避免在表达式中使用 `http\:\/\/`。

  此示例将匹配：

- `http://www.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?input=|cat /etc/passwd|`

  此示例不匹配：

- `ftp://ftp.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?value=x&input?|cat /etc/passwd|`
- **`/[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}/i`**

  此示例为任何 MAC 地址搜索数据包负载。请注意，此示例使用反斜杠对冒号进行转义。

向规则添加元数据

许可证：保护

可以使用 `metadata` 关键字向规则添加描述性信息。可以根据自身需求使用添加的信息来整理或识别规则以及搜索规则。

系统按以下格式验证元数据：

`key value`

其中，*`key`* 和 *`value`* 提供以空格分隔的组合描述。这是思科 VRT 用于向思科提供的规则添加元数据的格式。

也可以使用其他格式：

`key=value`

例如，借助 *`key value`* 格式，可以使用一个类别和子类别按作者和日期识别规则，如下所示：

```
author SnortGuru_20050406
```

可以在一个规则中使用多个 `metadata` 关键字。还可以使用逗号在一个 `metadata` 关键字中隔开多个 *`key value`* 语句，如以下示例所示：

```
author SnortGuru_20050406, revised_by SnortUser1_20050707,
revised_by SnortUser2_20061003, revised_by
SnortUser1_20070123
```

并非只能使用 *`key value`* 或 *`key=value`* 格式；但是，应了解根据这两种格式进行验证引起的局限性。

避免受限字符

许可证：保护

请注意以下字符限制：

- 请勿在 `metadata` 关键字中使用分号 (;) 和冒号 (:)。
- 请注意，如果使用逗号，系统会将逗号视为多个 *`key value`* 或 *`key=value`* 语句的分隔符。例如：

  `key value, key value, key value`

- 请注意，如果使用等号 (=) 字符或空格字符，系会将这些字符视为 *key* 和 *value* 之间的分隔符。例如：

```
key value
key=value
```

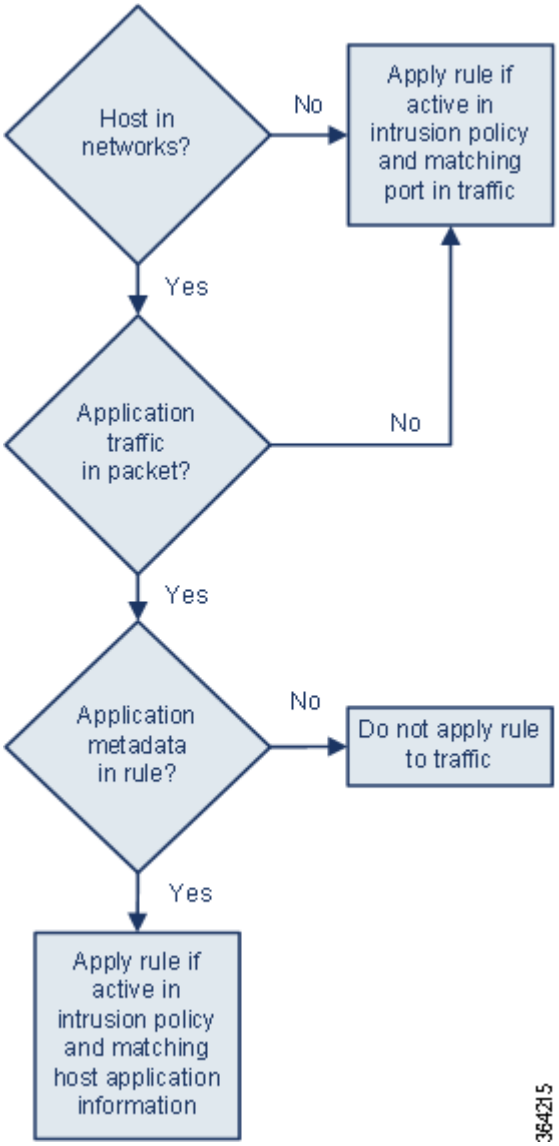
允许使用所有其他字。

添加 service 元数据

许可证：保护

规则引擎应用具有与数据包中用于主机的应用协议信息匹配的 `service` 元数据的活动规则来分析和处理流量。如果不匹配，系统不会将规则应用于流量 如果主机没有应用协议信息，或者规则没有 `service` 元数据，系统会对照规则中的端口检查流量中的端口，以确定是否将规则应用于流量。

下图说明根据应用信息来匹配规则和流量：



要将规则与确定的应用协议进行匹配，必须定义 metadata 关键字和 *key value* 语句，在其中，service 应作为 *key*，并指定 *value* 的应用。例如， metadata 关键字中的以下 *key value* 语句将规则与 HTTP 流量关联：

```
service http
```

下表介绍了最常用的应用值。

注　如需有关定义表中未列出的应用方面的帮助，请联系支持部门。

表 23-22　服务值

价值	说明
dcerpc	分布式计算环境/远程过程调用系统
dns	域名系统
finger	Finger 用户信息协议
ftp	文件传输协议
ftp-data	文件传输协议（数据信道）
http	超文本传输协议
imap	互联网消息访问协议
isakmp	互联网安全关联和密钥管理协议
netbios-dgm	NetBIOS 数据报服务
NetBIOS-ns	NetBIOS 名称服务
NetBIOS-ssn	NetBIOS 会话服务
nntp	网络新闻传输协议
oracle	Oracle 网络服务
pop2	邮局协议第 2 版
POP3	邮局协议第 3 版
smtp	简单邮件传输协议
ssh	安全外壳网络协议
telnet	Telnet 网络协议
tftp	简单文件传输协议
x11	X Window 系统

避免使用保留的元数据

许可证：保护

应避免在 metadata 关键字使用以下词语，无论是作为单个参数还是作为 *key value* 语句中的关键字；这些词语被保留供 VRT 使用：

```
应用
引擎
impact_flag
操作系统
策略
rule-type
```

```
rule-flushing
soid
```

注　如需有关将受限元数据添加到可能不具有预期作用的本地规则方面的帮助，请联系支持部门。有关详细信息，请参阅第 35-12 页上的导入本地规则文件。

检查 IP 报头值

许可证：保护

可以使用关键字来识别数据包 IP 报头中可能存在的攻击或安全策略违规。有关详细信息，请参阅：

- 第 23-41 页上的检查分片和保留位
- 第 23-42 页上的检查 IP 报头标别值
- 第 23-42 页上的识别指定的 IP 选项
- 第 23-42 页上的识别指定的 IP 协议号
- 第 23-43 页上的检查数据包的服务类型
- 第 23-43 页上的检查数据包的生存时间值

检查分片和保留位

许可证：保护

`fragbits` 关键字检查 IP 报头中的分片和保留位。可以检查每个数据包的 Reserved 位、 More Fragments位和 Don't Fragment 位的任意组合。

表 23-23　Fragbits 参数值

参数	说明
R	Reserved 位
M	More Fragments 位
D	Don’t Fragment 位

为进一步改进使用 `fragbits` 关键字的规则，可以在规则的参数值后指定下表中所述的任何运算符。

表 23-24　Fragbit 运算符

运算符	说明
加号 (+)	数据包必须匹配所有指定的位。
星号 (*)	数据包可以匹配任何指定的位。
感叹号 (!)	如果未设置任何指定的位，数据包将符合条件。

例如，要生成有关设置了 Reserved 位（还可能设置了任何其他位）的数据包的事件，请使用 `R+` 作为 `fragbits` 值。

检查 IP 报头标别值

许可证：保护

id 关键字根据您在此关键字的参数中指定的值测试 IP 报头分片标别字段。某些拒绝服务工具和扫描仪将此字段设置为容易检测的特定数字。例如，在 SID 630 （检测 Synscan 端口扫描）中，id 设置为 39426，这是在扫描仪传输的数据包中用作 ID 号的静态值。

注　id 参数值必须为数字。

识别指定的 IP 选项

许可证：保护

使用 IPopts 关键字可在数据包中搜索指定的 IP 报头选项。下表列出了可用的参数值。

表 23-25　IPoption 参数

参数	说明
rr	记录路由
eol	列表结束
nop	无操作
ts	时间戳
秒	IP 安全选项
lsrr	松散源路由
ssrr	严格源路由
satid	数据流标识符

分析师最经常监视严格和松散源路由，因为这两个选项可能指出欺骗性源 IP 地址。

识别指定的 IP 协议号

许可证：保护

使用 ip_proto 关键字可识别使用指定为关键字值的 IP 协议的数据包。可以为 IP 协议指定 0 到 255 之间的数字。有关完整的协议号列表，请访问 http://www.iana.org/assignments/protocol-numbers。可以将这些协议号与以下运算符结合使用：<、> 或 !。例如，要检查使用非 ICMP 的任何协议的流量，请使用 !1 作为 ip_proto 关键字的值。也可以在一个规则中多次使用 ip_proto 关键字；但请注意，规则引擎会将此关键字的多个实例解释为具有布尔 AND 关系。例如，如果创建一个包含 ip_proto:!3; ip_proto:!6 的规则，该规则将忽略使用 GGP 协议和 TCP 协议的流量。

检查数据包的服务类型

许可证：保护

有些网络使用服务类型 (ToS) 值设置在网络上传输的数据包的优先级。使用 `tos` 关键字可根据指定为该关键字的参数的值测试数据包的 IP 报头 ToS 值。对于其 ToS 已设置为指定值且符合规则中规定的其他条件的数据包，使用 `tos` 关键字的规则将会触发。

注　`tos` 参数值必须为数字。

ToS 字段已在 IP 报头协议中弃用，取而代之的是 Differentiated Services Code Point (DSCP) 字段。

检查数据包的生存时间值

许可证：保护

数据包的生存时间 (ttl) 值指明数据包在被丢弃之前可以跳多少次。可以使用 `ttl` 关键字根据指定为关键字参数的值或值范围测试数据包的 IP 报头 ttl 值。将 `ttl` 关键字参数设置为较小的值 （例如 0 或 1）可能会有帮助，因为小的生存时间值有时表示跟踪路由或入侵逃避行为。（但请注意，此关键字的适当值取决于设备放置和网络拓扑。）按如下方式使用语法：

- 将 TTL 值设置为 0 到 255 之间的整数。也可以该值前面加上一个等号 (=)（例如，可以指定 `5` 或 `=5`）。
- 使用连字符 (-) 指定 TTL 值的范围（例如，`0-2` 指定 0 到 2 之间的所有值，`-5` 指定 0 到 5 之间的所有值，`5-` 指定 5 到 255 之间的所有值）。
- 使用大于号 (>)指定 TTL 值大于一个特定值（例如，`>3` 指定大于 3 的所有值）。
- 使用大于或等于号 (>=) 指定 TTL 值大于或等于一个特定值（例如，`>=3` 指定大于或等于 3 的所有值）。
- 使用小于号 (<)指定 TTL 值小于一个特定值（例如，`<3` 指定小于 3 的所有值）。
- 使用小于或等于号 (<=) 指定 TTL 值小于或等于一个特定值（例如，`<=3` 指定小于或等于 3 的所有值）。

检查 ICMP 报头值

许可证：保护

ASA FirePOWER 模块支持可用于识别 ICMP 数据包报头中的攻击和安全策略违规的关键字。但请注意，存在的预定义规则检测大多数 ICMP 类型和代码。可考虑启用现有规则或者根据现有规则创建本地规则；如果您从头开始构建 ICMP 规则，可能会更快找到符合您需求的规则。

有关 ICMP 特定关键字的详细信息，请参阅：

- 第 23-44 页上的识别静态 ICMP ID 和序列值
- 第 23-44 页上的检查 ICMP 消息类型
- 第 23-44 页上的检查 ICMP 消息代码

识别静态 ICMP ID 和序列值

许可证：保护

ICMP 标别号和序列号有助于将 ICMP 响应与 ICMP 请求关联起来。在正常流量中，这些值动态地分配给数据包。有些隐蔽通道和分布式拒绝服务 (DDoS) 程序使用静态 ICMP ID 和序列值。使用以下关键字可识别具有静态值的 ICMP 数据包。

icmp_id

`icmp_id` 关键字检查 ICMP 回应请求或应答数据包的 ICMP ID 号。应使用对应于 ICMP ID 号的数值作为 `icmp_id` 关键字的参数。

icmp_seq

`icmp_seq` 关键字检查 ICMP 回应请求或应答数据包的 ICMP 序列。应使用对应于 ICMP 序列号的数值作为 `icmp_seq` 关键字的参数。

检查 ICMP 消息类型

许可证：保护

使用 `itype` 关键字可查找具有特定 ICMP 消息类型值的数据包。可以指定有效的 ICMP 类型值（有关 ICMP 类型编号的完整列表，请访问 http://www.iana.org/assignments/icmp-parameters 或 http://www.faqs.org/rfcs/rfc792.html）或无效的 ICMP 类型值来测试不同类型的流量。例如，攻击者可以将 ICMP 类型值设置为超出范围，从而导致拒绝服务和泛洪攻击。

可以使用小于号 (<) 和大于号 (>) 指定 `itype` 参数值的范围。

例如：

- <35
- >36
- 3<>55

提示　有关 ICMP 类型编号的完整列表，请访问 http://www.iana.org/assignments/icmp-parameters 或 http://www.faqs.org/rfcs/rfc792.html。

检查 ICMP 消息代码

许可证：保护

ICMP 消息有时包含代码值，用于在目标不可达的情况下提供有关详细信息。（有关与消息类型（可对其使用消息代码）相关的 ICMP 消息代码的完整列表，请参阅 http://www.iana.org/assignments/icmp-parameters 中的第二节。）

使用 `icode` 关键字可识别具有特定 ICMP 代码值的数据包。可以指定有效的 ICMP 代码值或无效的 ICMP 代码值来测试不同类型的流量。

可以使用小于号 (<) 和大于号 (>) 指定 `icode` 参数值的范围。

例如：

- 要查找小于 35 的值，请指定 `<35`。
- 要查找大于 36 的值，请指定 `>36`。
- 要查找 3 到 55 之间的值，请指定 `3<>55`。

提示　可以同时使用 `icode` 和 `itype` 关键字来识别与这两者都匹配的流量。例如，要识别包含 ICMP Destination Unreachable 代码类型和 ICMP Port Unreachable 代码类型的 ICMP 流量，请指定 3 作为 `itype` 关键字的值（用于 Destination Unreachable 类型），并指定 3 作为 `icode` 关键字的值（用于 Port Unreachable 类型）。

检查 TCP 报头值和数据流大小

许可证：保护

ASA FirePOWER 模块支持专门用于使用数据包 TCP 报头和 TCP 数据流大小来识别尝试的攻击的关键字。有关 TCP 特定关键字的详细信息，请参阅：

- 第 23-45 页上的检查 TCP 确认值
- 第 23-45 页上的检查 TCP 标志组合
- 第 23-46 页上的将规则应用于 TCP 或 UDP 客户端或服务器流量
- 第 23-47 页上的识别静态 TCP 序列号
- 第 23-48 页上的识别给定大小的 TCP 窗口
- 第 23-48 页上的识别给定大小的 TCP 数据流

检查 TCP 确认值

许可证：保护

可以使用 `ack` 关键字将某个值与数据包的 TCP 确认号进行比较。如果数据包的 TCP 确认号与为 `ack` 关键字指定的值相匹配，则会触发规则。

`ack` 参数值必须为数字。

检查 TCP 标志组合

许可证：保护

可以使用 `flags` 关键字指定 TCP 标志的任意组合，如果在已检查的数据包中设置此关键字，将导致规则触发。

注　在使用 `A+` 作为 `flags` 的值的一般情况下，应转为使用具有 `established` 值的 `flow` 关键字。通常，如果使用标志以确保标志的所有组合均已检测到，应使用具有 `stateless` 值的 `flow` 关键字。关于 `flow` 关键字的详细信息，请参阅第 23-46 页上的将规则应用于 TCP 或 UDP 客户端或服务器流量。

可以检查或忽略下表中所述的 `flag` 关键字的值。

表 23-26　flag 参数

参数	TCP 标志
Ack	确认数据。
Psh	数据应该在此数据包中发送。
Syn	新的连接。

表 23-26　flag 参数 （续）

参数	TCP 标志
Urg	包含紧急数据的数据包。
Fin	关闭的连接。
Rst	中止的连接。
CWR	ECN 堵塞窗口已减少。这以前是 R1 参数，仍支持向后兼容。
ECE	ECN 响应。这以前是 R2 参数，仍支持向后兼容。

提示　有关显式拥塞通知 (ECN) 的详细信息，请参阅以下网址提供的信息：http://www.faqs.org/rfcs/rfc3168.html。

使用 `flags` 关键字时，可以使用运算符来指示系统如何匹配多个标志。下表介绍了这些运算符。

表 23-27　与 flags 配合使用的运算符

运算符	说明	示例
全部	数据包必须包含所有指定的标志。	选择 `Urg` 和 `all` 可规定数据包必须包含紧急标志，且可以包含任何其他标志。
any	数据包可包含任何指定的标志。	选择 `Ack`、 `Psh` 和 `any` 可规定必须设置 `Ack` 和/或 `Psh` 标志才能触发规则，且也可以对数据包设置其他标志。
不会	数据包**不得**包含指定的标志集。	选择 `Urg` 和 `not` 可规定**不**对会触发此规则的数据包进行设置紧急标志。

将规则应用于 TCP 或 UDP 客户端或服务器流量

许可证：保护

可以使用 `flow` 关键字选择由规则根据会话特征进行的检查的数据包。 `flow` 关键字允许您指定规则应用的流量的方向，从而将规则应用于客户端流量或服务器流量。要指定 `flow` 关键字如何检查数据包，可以设置要分析的流量的方向、已检查的数据包的状态以及这些数据包是否是重建数据流的一部分。

数据包状态检测发生在规则处理之后。如果要使某个 TCP 规则忽略无状态流量（尚未建立会话上下文的流量），必须将 `flow` 关键字添加到该规则，并为该关键字选择 **Established** 参数。如果要使某个 UDP 规则忽略无状态流量，必须将 `flow` 关键字添加到该规则，并选择 **Established** 参数和/或方向参数。这样，TCP 或 UDP 规则就会执行数据包状态检查。

如果添加方向参数，规则引擎将只检查具有已建立状态且流向与指定方向匹配的数据包。例如，如果将具有 `established` 参数和 `From Client` 参数的 `flow` 关键字添加到某个规则，且该规则会在检测到 TCP 或 UDP 连接的情况下触发，那么规则引擎将只检查从特定客户端发送的数据包。

提示　为了获得最佳性能，应始终在 TCP 规则或 UDP 会话规则中包含 `flow` 关键字。

要指定流量，请从 Create Rule 页面上的 **Detection Options** 列表中选择 `flow` 关键字，并点击 **Add Option**。然后，为每个字段从列表中选择参数。

下表介绍了可为 `flow` 关键字指定的数据流相关参数：

表 23-28　状态相关 flow 参数

参数	说明
成熟市场	在已建立连接的情况下触发。
无状态	无论数据流处理器的状态如何，都会触发。

下表介绍了可为 `flow` 关键字指定的方向选项：

表 23-29　flow 方向参数

参数	说明
To Client	服务器响应时触发。
To Server	客户端响应时触发。
From Client	客户端响应时触发。
From Server	服务器响应时触发。

请注意，`From Server` 和 `To Client` 执行相同的功能，`To Server` 和 `From Client` 执行相同的功能。这些选项是为了是规则具有上下文和可读性。例如，如果要创建用于检测从服务器向客户端发起的木马攻击的规则，应使用 `From Server`。但是，如果要创建用于检测从客户端向服务器发出的木马攻击的规则，应使用 `From Client`。

下表介绍了可为 `flow` 关键字指定的数据流相关参数：

表 23-30　数据流相关的 flow 参数

参数	说明
Ignore Stream Traffic	重建流数据包时不触发。
Only Stream Traffic	仅在重建流数据包时触发。

例如，可以使用 `To Server, Established, Only Stream Traffic` 作为 `flow` 关键字的值，这样将会检测在建立的会话中从客户端流向服务器并且由数据流预处理器重组的流量。

识别静态 TCP 序列号

许可证：保护

使用 `seq` 关键字可指定静态序列号值。序列号与指定参数相匹配的数据包将会触发包含此关键字的规则。虽然此关键字很少使用，但它有助于识别使用生成的具有静态序列号的数据包的攻击和网络扫描。

识别给定大小的 TCP 窗口

许可证：保护

可以使用 `window` 关键字指定想要的 TCP 窗口大小。包含此关键字的规则每当遇到具有指定 TCP 窗口大小的数据包时，都会触发。虽然此关键字很少使用，但它有助于识别使用生成的具有静态 TCP 窗口大小的数据包的攻击和网络扫描。

识别给定大小的 TCP 数据流

许可证：保护

可以将 `stream_size` 关键字与数据流预处理器配合使用，以确定 TCP 数据流的大小（以字节为单位），具体格式如下：

`direction,operator,bytes`

其中，*`bytes`* 是字节数。必须以逗号 (,) 分隔参数中的每个选项。

下表介绍了可为 `stream_size` 关键字指定的不区分大小写的方向选项：

表 23-31　stream_size 关键字定向参数

参数	说明
客户端	当来自客户端的数据流与指定数据流大小相匹配时触发。
服务器	当来自服务器的数据流与指定数据流大小相匹配时触发。
both	当来自客户端和服务器的流量都与指定数据流大小相匹配时触发。 例如，如果来自客户端的流量大于 200 字节，且来自服务器的流量也大于 200 字节，参数 `both, >, 200` 将会触发。
either	当来自客户端或服务器流量与指定数据流大小相匹配时触发（无论哪一种情况先发生）。 例如，如果来自客户端的流量大于 200 字节，或来自服务器的流量大于 200 字节，参数 `either, >, 200` 将会触发。

下表介绍了可与 `stream_size` 关键字配合使用的运算符：

表 23-32　stream_size 关键字参数运算符

运算符	说明
=	等于
!=	不等于
>	大于
<	小于
>=	大于或等于
<=	小于或等于

例如，可以使用 `client, >=, 5001216` 作为 `stream_size` 关键字的参数，以检测从客户端发往服务器的且大于或等于 5001216 字节的 TCP 数据流。

启用和禁用 TCP 数据流重组

许可证：保护

如果对连接检查的流量与规则条件相匹配，可以使用 `stream_reassemble` 关键字为单一连接启用或禁用 TCP 数据流重组。或者，可以在规则中多次使用此关键字。

可使用以下语法启用或禁用数据流重组：

```
enable|disable, server|client|both, option, option
```

下表介绍了可与 `stream_reassemble` 关键字配合使用的可选参数。

表 23-33　stream_reassemble 可选参数

参数	说明
noalert	无论规则中是否指定任何其他检测选项，都不生成事件。
fastpath	当有匹配时，忽略连接流量的其余部分。

例如，以下示例禁用 TCP 客户端数据流重组，而且不针对在 HTTP 响应中检测到 200 OK 状态代码的连接生成事件：

```
alert tcp any 80 -> any any (flow:to_client, established; content: “200 OK”;
stream_reassemble:disable, client, noalert
```

要使用 stream_reassemble，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 `stream_reassemble` 并点击 **Add Option**。

系统将显示 `stream_reassemble` 部分。

从会话提取 SSL 信息

许可证：保护

可以使用 SSL 规则关键字调用安全套接字层 (SSL) 预处理器，并从加密会话中的数据包提取有关 SSL 版本和会话状态的信息。

客户机和服务器进行通信以使用 SSL 或安全传输层 (TLS) 建立加密会话时，它们之间会交换握手消息。虽然在会话中传输的数据是加密的，但握手消息没有加密。

SSL 预处理器从特定握手字段提取状态和版本信息。握手中的两个字段分别指明用于加密会话的 SSL 或 TLS 版本以及握手的阶段。

有关详细信息，请参阅：

- 第 23-50 页上的 ssl_state
- 第 23-50 页上的 ssl_version

ssl_state

许可证：保护

ssl_state 关键字可用于匹配加密会话的状态信息。要同时检查所用的两个或更多 SSL 版本，请在规则中使用多个 ssl_version 关键字。

如果规则使用 ssl_state 关键字，规则引擎将调用 SSL 预处理器来检查流量的 SSL 状态信息。

例如，要检测是否有攻击者试图通过发送具有超长长度和过量数据的 ClientHello 消息来造成服务器缓冲区溢出，可以使用带有 client_hello 参数的 ssl_state 关键字，然后检查异常大的数据包。

可使用逗号分隔列表为 SSL 状态指定多个参数。如果列出多个参数，系统将使用 OR 运算符对这些参数进行评估。例如，如果指定 client_hello 和 server_hello 作为参数，系统将会根据带有 client_hello 或 server_hello 的流量对规则进行评估。

还可以否定任何参数；例如：

```
!client_hello, !unknown
```

为确保连接已达到状态集中的每种状态，应使用具有 ssl_state 规则选项的多个规则。 ssl_state 关键字将以下标识符作为参数：

表 23-34　ssl_state 参数

参数	目的
client_hello	当客户端请求加密会话时，匹配消息类型为 ClientHello 的握手消息。
server_hello	当服务器响应客户端的加密会话请求时，匹配消息类型为 ServerHello 的握手消息。
client_keyx	当客户端向服务器发出密钥以确认收到来自服务器的密钥时，匹配消息类型为 ClientKeyExchange 的握手消息。
server_keyx	当客户端向服务器发出密钥以确认收到来自服务器的密钥时，匹配消息类型为 ServerKeyExchange 的握手消息。
unknown	匹配任何握手消息类型。

ssl_version

许可证：保护

ssl_version 关键字可用于匹配加密会话的版本信息。如果规则使用 ssl_version 关键字，规则引擎将调用 SSL 预处理器来检查流量的 SSL 版本信息。

例如，如果知道 SSL 2 版本中存在缓冲区溢出漏洞，可以使用带有 sslv2 参数的 ssl_version 关键字来识别使用该 SSL 版本的流量。

可使用逗号分隔列表为 SSL 版本指定多个参数。如果列出多个参数，系统将使用 OR 运算符对这些参数进行评估。例如，如果要识别任何未使用 SSLv2 的加密流量，可以向规则添加 ssl_version:ssl_v3,tls1.0,tls1.1,tls1.2。这样，规则将会评估任何使用 SSL 3 版本、TLS 1.0 版本、 TLS 1.1 版本或 TLS 1.2 版本的流量。

ssl_version 关键字将以下 SSL/TLS 版本标识符作为参数：

表 23-35　ssl_version 参数

参数	目的
sslv2	匹配使用安全套接字层 (SSL) 2 版本编码的流量。
sslv3	匹配使用安全套接字层 (SSL) 3 版本编码的流量。
tls1.0	匹配使用传输层安全 (TLS) 1.0 版本编码的流量。
tls1.1	匹配使用传输层安全 (TLS) 1.1 版本编码的流量。
tls1.2	匹配使用传输层安全 (TLS) 1.2 版本编码的流量。

检查应用层协议值

许可证：保护

虽然预处理器执行对于应用层协议值的大部分检查和规范化工作，但您仍可以使用以下各节中所述的关键字对应用层值进行检查。

- 第 23-51 页上的 RPC
- 第 23-52 页上的 ASN.1
- 第 23-53 页上的 urilen
- 第 23-54 页上的 DCE/RPC 关键字
- 第 23-56 页上的 SIP 关键字
- 第 23-58 页上的 GTP 关键字
- 第 23-68 页上的 Modbus 关键字
- 第 23-70 页上的 DNP3 关键字

RPC

许可证：保护

rpc关键字在 TCP 或 UDP 数据包中识别开放网络计算远程过程调用 (ONC RPC) 服务。这使您可以检测尝试识别主机上 RPC 程序的行为。入侵者可以使用 RPC 端口映射程序来确定网络上是否运行着可以利用的任何 RPC 服务。他们还可能尝试访问不使用端口映射程序运行 RPC 的其他端口。下表列出了 rpc 关键字接受的参数。

表 23-36　rpc 关键字参数

参数	说明
应用	RPC 应用编号
procedure	调用的 RPC 程序
version	RPC 版本

要为 rpc 关键字指定参数，请使用以下语法：

application,procedure,version

其中， *application* 是 RPC 应用编号， *procedure* 是 RPC 程序编号， *version* 是 RPC 版本号。必须为 rpc 关键字指定所有参数 - 如果不能够指定某一参数，应以星号 (*) 代替。

例如，要搜索具有任意程序或版本的 RPC 端口映射程序（以数字 100000 表示的 RPC 应用），可使用 100000,*,* 作为参数。

ASN.1

许可证：保护

asn1 关键字使您可以解码整个或部分数据包，以查找各种恶意编码。

下表介绍了 asn1 关键字的参数。

表 23-37　　asn.1 关键字参数

参数	说明
Bitstring Overflow	检测可远程攻击的无效位串编码。
Double Overflow	检测大于标准缓冲区的双 ASCII 编码。这是 Microsoft Windows 中的一个已知漏洞，但目前不知道哪些服务可能会被利用。
Oversize Length	检测长度大于提供的参数的 ASN.1 类型。例如，如果将 Oversize Length 设置为 500，任何大于 500 的 ASN.1 类型都会触发规则。
Absolute Offset	设置从数据包负载起点算起的绝对偏移量。（请记住，偏移量计数器从字节 0 开始计算。）例如，如果要解码 SNMP 数据包，请将 Absolute Offset 设置为 0，但不设置 Relative Offset。 Absolute Offset 可以是正数或负数。
Relative Offset	从上一次成功内容匹配、pcre 或 byte_jump 算起的相对偏移量。要解码紧接在内容“foo”后的 ASN.1 序列，请将 Relative Offset 设置为 0，但不设置 Absolute Offset。 Relative Offset 可以是正数或负数。（请记住，偏移量计数器从字节 0 开始计算。）

例如，Microsoft ASN.1 库中存在一个会造成缓冲区溢出的已知漏洞，使得攻击者能够利用包含特制的身份验证数据包的条件。当系统解码 ASN.1 数据时，数据包中的攻击代码可以在具有系统级别权限的主机上执行，或可能导致 DoS 条件。以下规则使用 asn1 关键字检测试图利用此漏洞的行为：

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445
(flow:to_server, established; content:"|FF|SMB|73|"; nocase;
offset:4; depth:5;
asn1:bitstring_overflow,double_overflow,oversize_length
100,relative_offset 54;)
```

当有 TCP 流量从 $EXTERNAL_NET 变量中定义的使用任何端口的任何 IP 地址流向 $HOME_NET 变量中定义的使用端口 445 的任何 IP 地址，上述规则将会生成事件。此外，它仅对与服务器之间建立的 TCP 连接执行规则。然后，该规则在特定位置对特定内容进行测试。最后，该规则使用 asn1 关键字检测位串编码和双 ASCII 编码，以及确定自上一次成功内容匹配结束以来从 55 字节起算超过 100 字节的 asn.1 类型长度。（请记住，偏移量计数器从字节 0 开始计算。）

urilen

许可证：保护

可以将 urilen 关键字和 HTTP 检查预处理器结合使用，以检查 HTTP 流量中特定长度、小于最大长度、大于最小长度或在指定范围内的 URI。

在 HTTP 检查预处理器对数据包进行规范化和检查后，规则引擎将根据规则评估数据包，并确定 URI 是否与 urilen 关键字指定的长度条件相匹配。可以使用此关键字来检测试图利用 URI 长度漏洞的攻击，例如，创建缓冲区溢出，以使攻击者可以在具有系统级别权限的主机上形成 DoS 条件或执行代码。

在规则中使用 urilen 关键字时，请注意：

- 实际上， urilen 关键字总是与 flow:established 关键字以及一个或多个其他关键字结合使用。
- 规则协议始终是 TCP。有关详细信息，请参阅第 23-4 页上的指定协议。
- 目标端口始终是 HTTP 端口。有关详细信息，请参阅第 23-8 页上的在入侵规则中定义端口和第 2-13 页上的优化预定义默认变量。

可以使用十进制字节数、小于号 (<) 和大于号 (>) 指定 URI 长度。

例如：

- 指定 5 将会检测长度为 5 字节的 URI。
- 指定 < 5（用一个空格字符隔开）将会检测长度小于 5 字节的 URI。
- 指定 > 5（用一个空格字符隔开）将会检测长度大于 5 字节的 URI。
- 指定 3 <> 5（<> 前后各有一个空格字符）将会检测长度为 3 到 5 字节的 URI。

例如， Novell 服务器的监控和诊断实用程序 iMonitor 2.4 版中存在一个已知漏洞，该漏洞来自 eDirectory 8.8 版。包含过长 URI 的一个数据包造成缓冲区溢出，使得攻击者者能够利用包含特制数据包的条件，该数据包可以在具有系统级别权限的主机上执行或可能导致 DoS 条件。以下规则使用 urilen 关键字检测试图利用此漏洞的行为：

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"EXPLOIT eDirectory 8.8 Long URI iMonitor buffer
overflow attempt";flow:to_server,established;
urilen:> 8192; uricontent:"/nds/"; nocase;
classtype:attempted-admin; sid:x; rev:1;)
```

当有 TCP 流量从 $EXTERNAL_NET 变量中定义的使用任何端口的任何 IP 地址流向 $HOME_NET 变量中定义的使用 $HTTP_PORTS 变量中定义的端口的任何 IP 地址，上述规则将会生成事件。此外，仅针对与服务器之间建立的 TCP 连接根据该规则评估数据包。该规则使用 urilen 关键字检测长度超过 8192 字节的任何 URI。最后，该规则在 URI 中搜索不区分大小写的特定内容 /nds/。

DCE/RPC 关键字

许可证：保护

下表中所述的三个 DCE/RPC 关键字可用于监控 DCE/RPC 会话流量的漏洞。当系统处理带有这些关键字的规则时，会调用 DCE/RPC 预处理器。有关详细信息，请参阅第 15-2 页上的解码 DCE/RPC 流量。

表 23-38　　DCE/RPC 关键字

使用.....	使用方式	要检测的内容
dce_iface	独立	识别特定 DCE/RPC 服务的数据包
dce_opnum	在前面加上 dce_iface	识别特定 DCE/RPC 服务操作的数据包
dce_stub_data	在前面加上 dce_iface 和 dce_opnum	定义特定操作请求或响应的存根数据

请注意，在上表中，应始终在 dce_iface 前面加上 dce_iface，在 dce_stub_data 前面加上 dce_iface 和 dce_opnum。

也可以将这些 DCE/RPC 关键字与其他规则关键字结合连用。请注意，对于 DCE/RPC 规则，应使用选择了 **DCE/RPC** 参数的 byte_jump、byte_test 和 byte_extract 关键字。有关详细信息，请参阅第 23-28 页上的使用 Byte_Jump 和 Byte_Test和第 23-75 页上的将数据包数据读取到关键字参数中。

思科建议在包含 DCE/RPC 关键字的规则中至少包含一个 content 关键字，以确保规则引擎使用快速模式匹配程序，从而加快处理速度和提高性能。请注意，如果规则包含至少一个 content 关键字，无论您是否启用 content 关键字的 **Use Fast Pattern Matcher** 参数，规则引擎都会使用快速模式匹配程序。有关详细信息，请参阅第 23-14 页上的搜索内容匹配和第 23-25 页上的 Use Fast Pattern Matcher。

在以下情况下，可以将 DCE/RPC 版本及相邻报头信息用作匹配的内容：

- 规则不包括其他 content 关键字
- 规则包含另一个 content 关键字，但 DCE/RPC 版本及相邻信息代表比其他内容更独特的模式

  例如， DCE/RPC 版本及相邻信息更有可能比内容的单个字节更加独特。

应使用以下其中一个版本及相邻信息内容匹配来终止限定规则：

- 对于面向连接的 DCE/RPC 规则，使用内容 |05 00 00|（用于 05 主要版本、00 次要版本和请求 PDU [协议数据单元]类型 00）。
- 对于无连接的 DCE/RPC 规则，使用内容 |04 00|（用于 04 版本和请求 PDU 类型 00）。

在这两种情况下，都应将版本及相邻信息的 content 关键字放在规则末尾，以调用快速模式匹配程序而不重复 DCE/RPC 预处理器已完成的处理。请注意：将 content 关键字放在规则末尾这种做法适用于被用作调用快速模式匹配程序的手段的版本内容，对于规则中的其他内容匹配无需这样做。

有关详细信息，请参阅：

- 第 23-55 页上的 dce_iface
- 第 23-56 页上的 dce_opnum
- 第 23-56 页上的 dce_stub_data

dce_iface

许可证：保护

可以使用 dce_iface 关键字识别特定 DCE/RPC 服务。

或者，还可以将 dce_iface 与 dce_opnum 和 dce_stub_data 关键字结合使用，以进一步限制要检查的 DCE/RPC 流量。有关详细信息，请参阅第 23-56 页上的 dce_opnum和第 23-56 页上的 dce_stub_data。

固定的 16 字节通用唯一标识符 (UUID) 用于识别分配给每个 DCE/RPC 服务的应用接口。例如，UUID 4b324fc8-670-01d3-1278-5a47bf6ee188 识别 DCE/RPC lanmanserver 服务（又称为 srvsvc 服务），该服务提供大量用于共享对等网络打印机、文件和 SMB 命名管道的管理功能。DCE/RPC 预处理器使用 UUID 及相关报头值来跟踪 DCE/RPC 会话。

接口 UUID 是由 5 个十六进制字符串（字符串之间用连字符分隔）组成：

```
<4hexbytes>-<2hexbytes>-<2hexbytes>-<2hexbytes>-<6hexbytes>
```

可以通过输入整个 UUID （包括连字符）来指定接口，如以下用于 netlogon 接口的 UUID 中所示：

```
12345678-1234-abcd-ef00-01234567cffb
```

请注意，必须以大端字节顺序指定 UUID 中的前三个字符串。尽管发布的接口列表和协议分析工具通常以正确的字节顺序显示 UUID，但您可能需要在输入前重新排列 UUID 字节顺序。考虑以下所示的信使服务 UUID，在原始 ASCII 文本中，该 UUID 的前三个字符串有时可能会以小端字节顺序显示：

```
f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc
```

可以为 dce_iface 关键字指定这个 UUID，方法是，插入连字符，并以大端字节顺序放置前三个字符串，如下所示：

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

尽管一个 DCE/RPC 会话可能包含发向多个接口的请求，但在一个规则中只能包含一个 dce_iface 关键字。可创建其他规则来检测其他接口。

DCE/RPC 应用接口也有接口版本号。或者，可以指定带有运算符的接口版本，用该操作符指明版本是等于、不等于、小于还是大于指定值。

除了 TCP 分段或 IP 分片外，还可以对面向连接和无连接的 DCE/RPC 进行分片。通常，将任何 DCE/RPC 分片（第一个除外）与指定接口相关联没有任何作用，而且这样做可能导致大量误报。但是，为了提高灵活性，可以根据指定接口对所有分片进行评估。

下表总结了 dce_iface 关键字参数。

表 23-39　dce_iface 参数

参数	说明
Interface UUID	UUID （包括连字符），用于识别要在 DCE/RPC 流量中检测的特定服务的应用接口。与指定接口相关的任何请求将匹配接口 UUID。
版本	或者，可以选择应用接口版本号 0 到 65535 和一个操作符，以指明是否检测大于 (>)、小于 (<)、等于 (=) 或不等于 (!) 指定值的版本。
All Fragments	或者，可以选择匹配与 DCE/RPC 分片相关的所有接口和（如有指定）接口版本。默认情况下，此参数被禁用，表示关键字仅在第一个分片或整个未分片数据包与指定接口相关时才进行匹配。请注意，启用此参数可能会导致误报。

dce_opnum

许可证：保护

可以将 dce_opnum 关键字和 DCE/RPC 预处理器结合使用，以检测识别 DCE/RPC 服务提供的一个或多个特定操作的数据包。

客户端功能调用请求特定服务函数（这些函数在 DCE/RPC 规范中称为*操作*）。操作编号 (opnum) 用于识别 DCE/RPC 报头中的特定操作。漏洞可能会针对特定操作。

例如， UUID 12345678-1234-abcd-ef00-01234567cffb 识别用于 netlogon 服务的接口；该服务提供几十个不同的操作，其中之一是操作 6， NetrServerPasswordSet 操作。

应该在 dce_opnum 关键字前面加上 dce_iface 关键字，以识别操作的服务。有关详细信息，请参阅第 23-55 页上的dce_iface。

可以为特定操作指定一个 0 到 65535 之间的十进制值，可以指定一系列由连字符分隔的操作，或者指定逗号分隔的操作和范围列表，其中的操作和范围可按任何顺序排列。

以下任何示例都将指定有效的 netlogon 操作编号：

```
15
15-18
15, 18-20
15, 20-22, 17
15, 18-20, 22, 24-26
```

dce_stub_data

许可证：保护

可以将 dce_stub_data 关键字和 DCE/RPC 预处理器结合使用，以指定无论任何其他规则选项如何，规则引擎都应从存根数据的开头开始检查。紧跟在 dce_stub_data 关键字后面的数据包负载规则选项相对于存根数据缓冲区适用。

DCE/RPC 存根数据提供客户端程序调用和 DCE/RPC 运行时系统之间的接口，这种机制可提供对于 DCE/RPC 至关重要的例程和服务。 DCE/RPC 漏洞在 DCE/RPC 数据包的存根数据部分中识别出。由于存根数据与特定的操作或函数调用相关，因此，应始终在 dce_stub_data 前面加上 dce_iface 和 dce_opnum，以识别相关的服务和操作。

dce_stub_data 关键字没有参数。有关详细信息，请参阅第 23-55 页上的 dce_iface和第 23-56 页上的 dce_opnum。

SIP 关键字

许可证：保护

有四个 SIP 关键字可用于监控 SIP 会话流量的漏洞。

请注意， SIP 协议容易受到拒绝服务 (DoS) 攻击。基于速率的攻击防御可能对解决这类攻击的规则有利。有关详细信息，请参阅第 20-25 页上的添加动态规则状态和第 21-8 页上的防御基于速率的攻击。

有关详细信息，请参阅：

- 第 23-57 页上的 sip_header
- 第 23-57 页上的 sip_body
- 第 23-57 页上的 sip_method
- 第 23-58 页上的 sip_stat_code

sip_header

许可证：保护

可以使用 sip_header 关键字从提取的 SIP 请求或响应报头开头开始检查，并将检查限制为仅针对报头字段。

sip_header 关键字没有参数。有关详细信息，请参阅第 23-57 页上的 sip_method和第 23-58 页上的 sip_stat_code。

以下示例规则分片指向 SIP 报头并匹配 CSeq 报头字段：

```
alert udp any any -> any 5060 ( sip_header; content:"CSeq"; )
```

sip_body

许可证：保护

可以使用 sip_body 关键字在提取的 SIP 请求或响应消息正文开头开始检查，并将检查限制为仅针对消息正文。

sip_body 关键字没有参数。

以下示例规则分片指向 SIP 消息正文，并匹配所提取 SDP 数据的 c（连接信息）字段中的特定 IP 地址：

```
alert udp any any -> any 5060 ( sip_body; content:"c=IN 192.168.12.14"; )
```

请注意，规则不仅限于搜索 SDP 内容。 SIP 预处理器将提取整个消息正文并使其可供规则引擎使用。

sip_method

许可证：保护

每个 SIP 请求中的 *method* 字段用于识别请求的目的。可以使用 sip_method 关键字测试特定方法的 SIP 请求。使用逗号隔开多种方法。

可以指定以下当前定义的任何 SIP 方法：

```
Ack、benotify、bye、cancel、do、info、invite、join、message、notify、options、prack、
publish、quath、refer、register、service、sprack、subscribe、unsubscribe、update
```

方法不区分大小写。可以使用逗号分隔多种方法。

由于可能在将来定义新的 SIP 方法，因此也可以指定自定义方法（即，当前未定义的方法）。RFC 2616 中定义了接受的字段值，该规范允许除控制字符和分隔符（例如 =、(和 }）以外的所有字符。有关被排除分隔符的完整列表，请参阅 RFC 2616。如果系统在流量中遇到指定的自定义方法，它将检查数据包报头，但不检查消息。

系统最多支持 32 种方法，包括 21 种当前定义的方法和 11 种其他方法。系统将忽略您可能配置的任何未定义的方法。请注意，总共有 32 种方法，包括使用 **Methods to Check** SIP 预处理器选项指定的方法。有关详细信息，请参阅第 15-42 页上的选择 SIP 预处理器选项。

如果使用否定形式，只能指定一种方法。例如：

```
!invite
```

但请注意，一个规则中的多个 sip_method 关键字与 **AND** 运算相关联。例如，要测试除 invite 和 cancel 以外的所有提取的方法，可以使用两个否定形式的 sip_method 关键字：

```
sip_method: !invite
sip_method: !cancel
```

思科建议在包含 sip_method 关键字的规则中至少包含一个 content 关键字，以确保规则引擎使用快速模式匹配程序，从而加快处理速度和提高性能。请注意，如果规则包含至少一个 content 关键字，无论您是否启用 content 关键字的 **Use Fast Pattern Matcher** 参数，规则引擎都会使用快速模式匹配程序。有关详细信息，请参阅第 23-14 页上的搜索内容匹配和第 23-25 页上的 Use Fast

Pattern Matcher。

sip_stat_code

许可证：保护

每个 SIP 响应中的三位数状态代码指明请求操作的结果。可以使用 `sip_stat_code` 关键字测试 SIP 响应的特定状态代码。

可以指定一个一位响应型数字（1 到 9）、一个特定的三位数（100 到 999）或者包含这两项的任意组合的逗号分隔列表。如果列表中的任何一个数字与 SIP 响应中的代码相匹配，则列表匹配。

下表介绍了可指定的 SIP 状态代码值。

表 23-40　　sip_stat_code 值

要检测的内容	可指定的内容	示例	会检测的内容
特定状态代码	三位数状态代码	189	189
任何以指定一位数开始的三位数代码	一位数	1	1xx；即， 100、101、 102 等
值列表	以逗号分隔的特定代码与一位数的组合	222, 3	222 以及 300、301、 302 等

另请注意，规则引擎不使用快速模式匹配程序搜索用 `sip_stat_code` 关键字指定的值，无论规则是否包含 `content` 关键字。

GTP 关键字

许可证：保护

有三个 GSRP 隧道协议 (GTP) 关键字可用于检查 GTP 命令通道的 GTP 版本、消息类型和信息元素。GTP 关键字不可与其他入侵规则关键字（例如 `content` 或 `byte_jump` 关键字）结合使用。如果规则使用了 `gtp_info` 或 `gtp_type` 关键字，还必须使用 `gtp_version` 关键字。

有关详细信息，请参阅：

- 第 23-58 页上的 gtp_version
- 第 23-59 页上的 gtp_type
- 第 23-63 页上的 gtp_info

gtp_version

可以使用 `gtp_version` 关键字检查 GTP 控制信息以确定 GTP 版本为 0、 1 还是 2。

由于不同的 GTP 版本定义不同的信息类型和信息元素，因此，使用 `gtp_type` 或 `gtp_info` 关键字时必须同时使用此关键字。可以将值指定为 0、 1 或 2。

要指定 GTP 版本，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **gtp_version** 并点击 **Add Option**。

系统将显示 `gtp_version` 关键字。

步骤 2　将值指定为 `0`、`1` 或 `2` 以识别 GTP 版本。

gtp_type

每条 GTP 消息由一种消息类型标识，消息类型由一个数值和一个字符串组成。可以将 `gtp_type` 与 `gtp_version` 关键字结合使用，以检查流量中的特定 GTP 消息类型。

可以为消息类型指定定义的十进制值，可以指定定义的字符串，或者指定包含这两项的任意组合的逗号分隔列表，如以下示例所示：

```
10, 11, echo_request
```

系统使用 OR 操作来匹配列出的每个值或字符串。值和字符串的列出顺序并不重要。列表中的任何一个值或字符串均与此关键字匹配。如果尝试保存包含无法识别的字符串或超出范围的值的规则，将会出现错误消息。

请注意，下表中不同的 GTP 版本有时会对同一种消息类型使用不同的值。例如，`sgsn_context_request` 这一消息类型在 GTPv0 和 GTPv1 中值是 50，但在 GTPv2 中值是 130。

`gtp_type` 关键字匹配不同的值，具体取决于数据包中的版本号。在上述示例中，在 GTPv0 或 GTPv1 数据包中，此关键字匹配消息类型值 50，在 GTPv2 数据包中，则匹配值 130。如果数据包中的消息类型值不是在数据包中指定的版本的已知值，此关键字不会匹配数据包。

如果为消息类型指定一个整数，则当关键字中的消息类型与 GTP 数据包中的该值匹配时，关键字将会匹配，无论数据包中指定的版本如何。

下表列出了系统识别出的为每种 GTP 消息类型定义的值和字符串。

表 23-41　　GTP 消息类型

价值	0 版本	版本 1	版本 2
1	echo_request	echo_request	echo_request
2	echo_response	echo_response	echo_response
3	version_not_supported	version_not_supported	version_not_supported
4	node_alive_request	node_alive_request	不适用
5	node_alive_response	node_alive_response	不适用
6	redirection_request	redirection_request	不适用
7	redirection_response	redirection_response	不适用
16	create_pdp_context_request	create_pdp_context_request	不适用
17	create_pdp_context_response	create_pdp_context_response	不适用
18	update_pdp_context_request	update_pdp_context_request	不适用
19	update_pdp_context_response	update_pdp_context_response	不适用
20	delete_pdp_context_request	delete_pdp_context_request	不适用
21	delete_pdp_context_response	delete_pdp_context_response	不适用
22	create_aa_pdp_context_request	init_pdp_context_activation_request	不适用
23	create_aa_pdp_context_response	init_pdp_context_activation_respons e	不适用
24	delete_aa_pdp_context_request	不适用	不适用
25	delete_aa_pdp_context_response	不适用	不适用

表 23-41　GTP 消息类型（续）

价值	0 版本	版本 1	版本 2
26	error_indication	error_indication	不适用
27	pdu_notification_request	pdu_notification_request	不适用
28	pdu_notification_response	pdu_notification_response	不适用
29	pdu_notification_reject_request	pdu_notification_reject_request	不适用
30	pdu_notification_reject_response	pdu_notification_reject_response	不适用
31	不适用	supported_ext_header_notification	不适用
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response
36	note_ms_present_request	note_ms_present_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	不适用	不适用	change_notification_request
全球 39	不适用	不适用	change_notification_response
48	identification_request	identification_request	不适用
49	identification_response	identification_response	不适用
50	sgsn_context_request	sgsn_context_request	不适用
51	sgsn_context_response	sgsn_context_response	不适用
52	sgsn_context_ack	sgsn_context_ack	不适用
53	不适用	forward_relocation_request	不适用
54	不适用	forward_relocation_response	不适用
55	不适用	forward_relocation_complete	不适用
56	不适用	relocation_cancel_request	不适用
57	不适用	relocation_cancel_response	不适用
58	不适用	forward_srns_contex	不适用
59	不适用	forward_relocation_complete_ack	不适用
60	不适用	forward_srns_contex_ack	不适用
64	不适用	不适用	modify_bearer_command
65	不适用	不适用	modify_bearer_failure_indication
66	不适用	不适用	delete_bearer_command
67	不适用	不适用	delete_bearer_failure_indication
68	不适用	不适用	bearer_resource_command
69	不适用	不适用	bearer_resource_failure_indication
70	不适用	ran_info_relay	downlink_failure_indication
71	不适用	不适用	trace_session_activation

表 23-41　GTP 消息类型（续）

价值	0 版本	版本 1	版本 2
72	不适用	不适用	trace_session_deactivation
73	不适用	不适用	stop_paging_indication
95	不适用	不适用	create_bearer_request
96	不适用	mbms_notification_request	create_bearer_response
97	不适用	mbms_notification_response	update_bearer_request
98	不适用	mbms_notification_reject_request	update_bearer_response
99	不适用	mbms_notification_reject_response	delete_bearer_request
100	不适用	create_mbms_context_request	delete_bearer_response
101	不适用	create_mbms_context_response	delete_pdn_request
102	不适用	update_mbms_context_request	delete_pdn_response
103	不适用	update_mbms_context_response	不适用
104	不适用	delete_mbms_context_request	不适用
105	不适用	delete_mbms_context_response	不适用
112	不适用	mbms_register_request	不适用
113	不适用	mbms_register_response	不适用
114	不适用	mbms_deregister_request	不适用
115	不适用	mbms_deregister_response	不适用
116	不适用	mbms_session_start_request	不适用
117	不适用	mbms_session_start_response	不适用
118	不适用	mbms_session_stop_request	不适用
119	不适用	mbms_session_stop_response	不适用
120	不适用	mbms_session_update_request	不适用
121	不适用	mbms_session_update_response	不适用
128	不适用	ms_info_change_request	identification_request
129	不适用	ms_info_change_response	identification_response
130	不适用	不适用	sgsn_context_request
131	不适用	不适用	sgsn_context_response
132	不适用	不适用	sgsn_context_ack
133	不适用	不适用	forward_relocation_request
134	不适用	不适用	forward_relocation_response
135	不适用	不适用	forward_relocation_complete
136	不适用	不适用	forward_relocation_complete_ack
137	不适用	不适用	forward_access
138	不适用	不适用	forward_access_ack
139	不适用	不适用	relocation_cancel_request
140	不适用	不适用	relocation_cancel_response

表 23-41　GTP 消息类型（续）

价值	0 版本	版本 1	版本 2
141	不适用	不适用	configuration_transfer_tunnel
149	不适用	不适用	detach
150	不适用	不适用	detach_ack
151	不适用	不适用	cs_paging
152	不适用	不适用	ran_info_relay
153	不适用	不适用	alert_mme
154	不适用	不适用	alert_mme_ack
155	不适用	不适用	ue_activity
156	不适用	不适用	ue_activity_ack
160	不适用	不适用	create_forward_tunnel_request
161	不适用	不适用	create_forward_tunnel_response
162	不适用	不适用	suspend
163	不适用	不适用	suspend_ack
164	不适用	不适用	在如图所示的
165	不适用	不适用	resume_ack
166	不适用	不适用	create_indirect_forward_tunnel_request
167	不适用	不适用	create_indirect_forward_tunnel_response
168	不适用	不适用	delete_indirect_forward_tunnel_request
169	不适用	不适用	delete_indirect_forward_tunnel_response
170	不适用	不适用	release_access_bearer_request
171	不适用	不适用	release_access_bearer_response
176	不适用	不适用	downlink_data
177	不适用	不适用	downlink_data_ack
179	不适用	不适用	pgw_restart
180	不适用	不适用	pgw_restart_ack
200	不适用	不适用	update_pdn_request
201	不适用	不适用	update_pdn_response
211	不适用	不适用	modify_access_bearer_request
212	不适用	不适用	modify_access_bearer_response
231	不适用	不适用	mbms_session_start_request
232	不适用	不适用	mbms_session_start_response
233	不适用	不适用	mbms_session_update_request
234	不适用	不适用	mbms_session_update_response
235	不适用	不适用	mbms_session_stop_request
236	不适用	不适用	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	不适用

表 23-41　GTP 消息类型（续）

价值	0 版本	版本 1	版本 2
241	data_record_transfer_response	data_record_transfer_response	不适用
254	不适用	end_marker	不适用
255	pdu	pdu	不适用

要指定 GTP 消息类型，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **gtp_type** 并点击 **Add Option**。

系统将显示 `gtp_type` 关键字。

步骤 2　为消息类型指定一个定义的十进制值（0 到 255）、定义的字符串或包含这两项的任意组合的逗号分隔列表。有关系统识别出的值和字符串，请参阅 GTP 消息类型表。

gtp_info

一条 GTP 消息可以包含多个信息元素，其中的每一个元素均由已定义的一个数值和一个字符串来识别。可以将 `gtp_info` 与 `gtp_version` 关键字结合使用，以在特定信息元素开头开始检查，并将检查限制为仅针对该信息元素。

可以为信息元素指定已定义的十进制值或字符串。可以指定一个值或字符串，也可以在一个规则中使用多个 `gtp_info` 关键字来检查多个信息元素。

如果一条消息包含相同类型的多个信息元素，将会全部检查这些元素来进行匹配。如果信息元素按无效顺序出现，将仅检查最后一个实例。

请注意，不同的 GTP 版本有时对同一个信息元素使用不同的值。例如，`cause` 这个信息元素在 GTPv0 和 GTPv1 中值是 1，但在 GTPv2 中值是 2。

`gtp_info` 关键字匹配不同的值，具体取决于数据包中的版本号。在上述示例中，在 GTPv0 或 GTPv1 数据包中，此关键字匹配信息元素值 1，在 GTPv2 数据包中，则匹配值 2。如果数据包中的信息元素值不是在数据包中指定的版本的已知值，此关键字不会匹配数据包。

如果为信息元素指定一个整数，则当关键字中的消息类型与 GTP 数据包中的该值匹配时，关键字将会匹配，无论数据包中指定的版本如何。

下表列出了系统识别出的每个 GTP 信息元素的值和字符串。

表 23-42　GTP 信息元素

价值	0 版本	版本 1	版本 2
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	恢复
4	tlli	tlli	不适用
5	p_tmsi	p_tmsi	不适用
6	qos	不适用	不适用
8	recording_required	recording_required	不适用
9	身份验证	身份验证	不适用

表 23-42　GTP 信息元素（续）

价值	0 版本	版本 1	版本 2
11	map_cause	map_cause	不适用
12	p_tmsi_sig	p_tmsi_sig	不适用
13	ms_validated	ms_validated	不适用
14	恢复	恢复	不适用
15	selection_mode	selection_mode	不适用
16	flow_label_data_1	teid_1	不适用
17	flow_label_signalling	teid_control	不适用
18	flow_label_data_2	teid_2	不适用
19	ms_unreachable	teardown_ind	不适用
20	不适用	nsapi	不适用
21	不适用	ranap	不适用
22	不适用	rab_context	不适用
23	不适用	radio_priority_sms	不适用
24	不适用	radio_priority	不适用
25	不适用	packet_flow_id	不适用
26	不适用	charging_char	不适用
27	不适用	trace_ref	不适用
28	不适用	trace_type	不适用
29	不适用	ms_unreachable	不适用
71	不适用	不适用	apn
72	不适用	不适用	ambr
73	不适用	不适用	ebi
74	不适用	不适用	ip_addr
75	不适用	不适用	mei
76	不适用	不适用	msisdn
77	不适用	不适用	indication
78	不适用	不适用	pco
79	不适用	不适用	paa
80	不适用	不适用	bearer_qos
80	不适用	不适用	flow_qos
82	不适用	不适用	rat_type
83	不适用	不适用	serving_network
84	不适用	不适用	bearer_tft
85	不适用	不适用	tad
86	不适用	不适用	uli
87	不适用	不适用	f_teid

表 23-42　　GTP 信息元素（续）

价值	0 版本	版本 1	版本 2
88	不适用	不适用	tmsi
89	不适用	不适用	cn_id
90	不适用	不适用	s103pdf
91	不适用	不适用	s1udf
92	不适用	不适用	delay_value
93	不适用	不适用	bearer_context
94	不适用	不适用	charging_id
95	不适用	不适用	charging_char
96	不适用	不适用	trace_info
97	不适用	不适用	bearer_flag
99	不适用	不适用	pdn_type
100	不适用	不适用	pti
101	不适用	不适用	drx_parameter
103	不适用	不适用	gsm_key_tri
104	不适用	不适用	umts_key_cipher_quin
105	不适用	不适用	gsm_key_cipher_quin
106	不适用	不适用	umts_key_quin
107	不适用	不适用	eps_quad
108	不适用	不适用	umts_key_quad_quin
109	不适用	不适用	pdn_connection
110	不适用	不适用	pdn_number
111	不适用	不适用	p_tmsi
112	不适用	不适用	p_tmsi_sig
113	不适用	不适用	hop_counter
114	不适用	不适用	ue_time_zone
115	不适用	不适用	trace_ref
116	不适用	不适用	complete_request_msg
117	不适用	不适用	guti
118	不适用	不适用	f_container
119	不适用	不适用	f_cause
120	不适用	不适用	plmn_id
121	不适用	不适用	target_id
123	不适用	不适用	packet_flow_id
124	不适用	不适用	rab_contex
125	不适用	不适用	src_rnc_pdcp
126	不适用	不适用	udp_src_port

表 23-42　GTP 信息元素（续）

价值	0 版本	版本 1	版本 2
127	charge_id	charge_id	apn_restriction
128	end_user_address	end_user_address	selection_mode
129	mm_context	mm_context	src_id
130	pdp_context	pdp_context	不适用
131	apn	apn	change_report_action
132	protocol_config	protocol_config	fq_csid
133	gsn	gsn	channel
134	msisdn	msisdn	emlpp_pri
135	不适用	qos	node_type
136	不适用	authentication_qu	fqdn
137	不适用	tft	ti
138	不适用	target_id	mbms_session_duration
139	不适用	utran_trans	mbms_service_area
140	不适用	rab_setup	mbms_session_id
141	不适用	ext_header	mbms_flow_id
142	不适用	trigger_id	mbms_ip_multicast
143	不适用	omc_id	mbms_distribution_ack
144	不适用	ran_trans	rfsp_index
145	不适用	pdp_context_pri	uci
146	不适用	addi_rab_setup	csg_info
147	不适用	sgsn_number	csg_id
148	不适用	common_flag	cmi
149	不适用	apn_restriction	service_indicator
150	不适用	radio_priority_lcs	detach_type
151	不适用	rat_type	ldn
152	不适用	user_loc_info	node_feature
153	不适用	ms_time_zone	mbms_time_to_transfer
154	不适用	imei_sv	throttling
155	不适用	camel	ARP
156	不适用	mbms_ue_context	epc_timer
157	不适用	tmp_mobile_group_id	signalling_priority_indication
158	不适用	rim_routing_addr	tmgi
159	不适用	mbms_config	mm_srvcc
160	不适用	mbms_service_area	flags_srvcc
161	不适用	src_rnc_pdcp	nmbr
162	不适用	addi_trace_info	不适用

表 23-42　　GTP 信息元素（续）

价值	0 版本	版本 1	版本 2
163	不适用	hop_counter	不适用
164	不适用	plmn_id	不适用
165	不适用	mbms_session_id	不适用
166	不适用	mbms_2g3g_indicator	不适用
167	不适用	enhanced_nsapi	不适用
168	不适用	mbms_session_duration	不适用
169	不适用	addi_mbms_trace_info	不适用
170	不适用	mbms_session_repetition_num	不适用
171	不适用	mbms_time_to_data	不适用
173	不适用	bss	不适用
174	不适用	cell_id	不适用
175	不适用	pdu_num	不适用
177	不适用	mbms_bearer_capab	不适用
178	不适用	rim_routing_disc	不适用
179	不适用	list_pfc	不适用
180	不适用	ps_xid	不适用
181	不适用	ms_info_change_report	不适用
182	不适用	direct_tunnel_flags	不适用
183	不适用	correlation_id	不适用
184	不适用	bearer_control_mode	不适用
185	不适用	mbms_flow_id	不适用
186	不适用	mbms_ip_multicast	不适用
187	不适用	mbms_distribution_ack	不适用
188	不适用	reliable_inter_rat_handover	不适用
189	不适用	rfsp_index	不适用
190	不适用	fqdn	不适用
191	不适用	evolved_allocation1	不适用
192	不适用	evolved_allocation2	不适用
193	不适用	extended_flags	不适用
194	不适用	uci	不适用
195	不适用	csg_info	不适用
196	不适用	csg_id	不适用
197	不适用	cmi	不适用
198	不适用	apn_ambr	不适用
199	不适用	ue_network	不适用
200	不适用	ue_ambr	不适用

表 23-42　GTP 信息元素（续）

价值	0 版本	版本 1	版本 2
201	不适用	apn_ambr_nsapi	不适用
202	不适用	ggsn_backoff_timer	不适用
203	不适用	signalling_priority_indication	不适用
204	不适用	signalling_priority_indication_nsapi	不适用
205	不适用	high_bitrate	不适用
206	不适用	max_mbr	不适用
251	charging_gateway_addr	charging_gateway_addr	不适用
255	private_extension	private_extension	private_extension

可以按照以下步骤指定 GTP 信息元素。

要指定 GTP 信息元素，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **gtp_info** 并点击 **Add Option**。

系统将显示 `gtp_info` 关键字。

步骤 2　为信息元素指定一个已定义的十进制值（0 到 255）或者一个已定义的字符串。有关系统识别出的值和字符串，请参阅 GTP 信息元素表。

Modbus 关键字

许可证：保护

可以使用 Modbus 关键字指向 Modbus 请求或响应中 Data 字段的开头，以匹配 Modbus 函数代码和 Modbus 单元 ID。可以单独使用 Modbus 关键字，也可以将它与其他关键字（例如 `content` 和 `byte_jump` 关键字）结合使用。

有关详细信息，请参阅：

- 第 23-69 页上的 modbus_data
- 第 23-69 页上的 modbus_func
- 第 23-70 页上的 modbus_unit

modbus_data

可以使用 `modbus_data` 关键字指向 Modbus 请求或响应中 Data 字段的开头。

要指向 Modbus Data 字段的开头，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **modbus_data** 并点击 **Add Option**。

系统将显示 `modbus_data` 关键字。

`modbus_data` 关键字没有参数。

modbus_func

可以使用 modbus_func 关键字来匹配 Modbus 应用层请求或响应报头中的 Function Code 字段。可以为 Modbus 函数代码指定一个已定义的十进制值或一个已定义的字符串。

下表列出了系统识别出的为 Modbus 函数代码定义的值和字符串。

表 23-43　Modbus 函数代码

价值	字符串
1	read_coils
2	read_discrete_inputs
3	read_holding_registers
4	read_input_registers
5	write_single_coil
6	write_single_register
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
17	report_slave_id
20	read_file_record
21	write_file_record
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue
43	encapsulated_interface_transport

要指定 Modbus 函数代码，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **modbus_func** 并点击 **Add Option**。

系统将显示 modbus_func 关键字。

步骤 2　为函数代码指定一个已定义的十进制值（0 到 255）或者一个已定义的字符串。有关系统识别出的值和字符串，请参阅 Modbus 函数代码表。

modbus_unit

可以使用 modbus_unit 关键字来匹配 Modbus 请求或响应报头中的 Unit ID 字段。

要指定 Modbus 单元 ID，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **modbus_unit** 并点击 **Add Option**。

系统将显示 `modbus_unit` 关键字。

步骤 2　指定一个 0 到 255 之间的十进制值。

DNP3 关键字

许可证：保护

DNP3 关键字可用于以下目的：指向应用层分片的开头；匹配 DNP3 响应和请求中的 DNP3 函数代码和函数对象；以及匹配 DNP3 响应中的内部指示标志。可以单独使用 DNP3 关键字，也可以将它与其他关键字（例如 `content` 和 `byte_jump` 关键字）结合使用。

有关详细信息，请参阅：

- 第 23-70 页上的 dnp3_data
- 第 23-71 页上的 dnp3_func
- 第 23-72 页上的 dnp3_ind
- 第 23-73 页上的 dnp3_obj

dnp3_data

可以使用 `dnp3_data` 关键字指向重组 DNP3 应用层分片的开头。

DNP3 预处理器将链路层帧重组到应用层分片中。`dnp3_data` 关键字指向每个应用层分片的开头；其他规则选项可匹配分片中的重组数据，而无需每 16 个字节分隔数据并添加校验和。

要指向重组 DNP3 分片的开头，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **modbus_data** 并点击 **Add Option**。

系统将显示 `dnp3_data` 关键字。

`dnp3_data` 关键字没有参数。

dnp3_func

可以使用 `dnp3_func` 关键字来匹配 DNP3 应用层请求或响应报头中的 Function Code 字段。可以为 DNP3 函数代码指定一个已定义的十进制值或一个已定义的字符串。

下表列出了系统识别出的为 DNP3 函数代码定义的值和字符串。

表 23-44　　DNP3 函数代码

价值	字符串
0	confirm
1	read
2	write

表 23-44　DNP3 函数代码（续）

价值	字符串
3	选择
4	operate
5	direct_operate
6	direct_operate_nr
7	immed_freeze
8	immed_freeze_nr
9	freeze_clear
10	freeze_clear_nr
11	freeze_at_time
12	freeze_at_time_nr
13	cold_restart
14	warm_restart
15	initialize_data
16	initialize_appl
17	start_appl
18	stop_appl
19	save_config
20	enable_unsolicited
21	disable_unsolicited
22	assign_class
23	delay_measure
24	record_current_time
25	open_file
26	close_file
27	delete_file
28	get_file_info
29	authenticate_file
30	abort_file
31	activate_config
32	authenticate_req
33	authenticate_err
129	效率低下
130	unsolicited_response
131	authenticate_resp

要指定 DNP3 函数代码，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **dnp3_func** 并点击 **Add Option**。

系统将显示 dnp3_func 关键字。

步骤 2　为函数代码指定一个已定义的十进制值（0 到 255）或者一个已定义的字符串。有关系统识别出的值和字符串，请参阅 DNP3 函数代码表。

dnp3_ind

可以使用 dnp3_ind 关键字来匹配 DNP3 应用层响应报头中 Internal Indications 字段中的标志。

可以为一个已知标志指定一个字符串，也可以指定以逗号分隔的标志列表，如以下示例所示：

```
class_1_events, class_2_events
```

如果指定多个标志，此关键字将会匹配列表中的任何标志。要检测标志组合，可在一个规则中多次使用 dnp3_ind 关键字。

以下列表提供了系统识别出的用于已定义的 DNP3 内部指示标志的字符串语法。

```
class_1_events
class_2_events
class_3_events
need_time
local_control
device_trouble
device_restart
no_func_code_support
object_unknown
parameter_error
event_buffer_overflow
already_executing
config_corrupt
reserved_2
reserved_1
```

要指定 DNP3 内部指示标志，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **dnp3_ind** 并点击 **Add Option**。

系统将显示 dnp3_ind 关键字。

步骤 2　可以为一个已知标志指定一个字符串，也可以指定以逗号分隔的标志列表。

dnp3_obj

可以使用 dnp3_obj 关键字来匹配请求或响应中的 DNP3 对象报头。

DNP3 数据由一系列不同类型的 DNP3 对象组成，例如模拟输入、二进制输入，等等。每种类型均以*组*进行识别，例如模拟输入组、二进制输入组等，每个组均可由一个十进制值进行识别。每个组中的对象均以*对象变体*进一步识别，例如 16 位整数、 32 位整数、短浮点等，每个这些变体均指定对象的数据格式。每种类型的对象变体也可以十进制值进行识别。

可以通过为对象报头组和类型和对象变体类型分别指定一个十进制数值来识别对象报头。这两种类型的组合可定义特定类型的 DNP3 对象。

要指定 DNP3 对象的指定，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **dnp3_obj** 并点击 **Add Option**。

系统将显示 `dnp3_obj` 关键字。

步骤 2　指定一个 0 到 255 之间的十进制值来识别已知对象组，并指定另一个 0 到 255 之间的十进制值来识别已知对象变体类型。

检查数据包特征

许可证：保护

可以编写只针对具有特定特征的数据包生成事件的规则。ASA FirePOWER 模块提供以下关键字来评估数据包特征：

- 第 23-73 页上的 dsize
- 第 23-74 页上的 isdataat
- 第 23-74 页上的 sameip
- 第 23-74 页上的 fragoffset
- 第 23-75 页上的 cvs

dsize

许可证：保护

`dsize` 关键字测试数据包负载的大小。使用此关键字时，可以用大于号和小于号 （`<` 和 `>`）指定值的范围。可以使用以下语法来指定范围：

`>number_of_bytes`
`<number_of_bytes`
`number_of_bytes<>number_of_bytes`

例如，要表示大于 400 字节的数据包大小，请使用 `>400` 作为 `dtype` 值。要表示小于 500 字节的数据包大小，请使用 `<500`。要规定规则应对介于 400 到 500 字节（包含 400 和 500 字节）的任何数据包触发，请使用 `400<>500`。

注意事项　`dsize` 关键字测试未经任何预处理器解码的数据包。

isdataat

许可证：保护

`isdataat` 关键字指示规则引擎验证数据是否驻留在负载中的特定位置。

下表列出了可与 `isdataat` 关键字配合使用的参数。

表 23-45　isdataat 参数

参数	类型	说明
Offset	必填	负载中的特定位置。例如，要测试显示在数据包中字节 50 处的数据，需要指定 50 作为偏移量值。A !修饰符否定 isdataat 测试的结果；如果负载中不存在一定数量的数据，此修饰符将会发出警报。 还可以使用现有 byte_extract 变量指定此参数的值。有关详细信息，请参阅第 23-75 页上的将数据包数据读取到关键字参数中。
Relative	可选	使位置相对于上一次成功内容匹配。指定相对位置时请注意，计数器从字节 0 开始计算，因此，应该如下计算相对位置：用从上一次成功内容匹配起向前计算所需的字节数减去 1。例如，要指定数据必须显示在上一次成功内容匹配后的第九个字节处，需要将相对偏移量指定为 8。
Raw Data	可选	指定数据在由任何 ASA FirePOWER 模块预处理器进行解码或应用层规范化之前位于原始数据包负载中。如果上一次内容匹配出现在原始数据包数据中，可以将此参数与 **Relative** 结合使用。

例如，在查找内容 foo 的规则搜索中，如果如下指定 isdataat 的值：

- Offset = !10
- Relative 已启用

那么，如果规则引擎在负载结束前未能在 foo 之后检测到 10 字节，系统将会发出警报。

要使用 isdataat，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 isdataat 并点击 **Add Option**。

系统将显示 isdataat 部分。

sameip

许可证：保护

sameip 关键字测试数据包的源 IP 地址和目标 IP 地址是否相同。此关键字没有参数。

fragoffset

许可证：保护

fragoffset 关键字测试分片数据包的偏移量。由于某些漏洞（例如，WinNuke 拒绝服务攻击）使用手动生成的具有特定偏移量的数据包分片，因此，此关键字很有用。

例如，要测试分片数据包的偏移量是否为 31337 字节，应指定 31337 作为 fragoffset 的值。

为 fragoffset 关键字指定参数时，可以使用以下运算符。

表 23-46　fragoffset 关键字参数运算符

运算符	说明
!	不会
>	大于
<	小于

请注意，不能将 not (!) 运算符与 < 或 > 结合使用。

cvs

许可证：保护

cvs 关键字测试并发版本系统 (CVS) 流量中是否存在格式不正确的 CVS 条目。攻击者可以使用格式不正确的条目来强制堆溢出，并且在 CVS 服务器上执行恶意代码。此关键字可用于识别针对两种已知 CVS 漏洞的攻击：CVE-2004-0396 （CVS1.11.x 至 1.11.15，以及 CVS1.12.x 至 1.12.7）和 CVS-2004-0414 （CVS1.12.x 至 1.12.8，以及 CVS1.11.x 至 1.11.16）。cvs 关键字检查格式正确的记录，如果检测到格式不正确的条目，将会发出警报。

规则应包含 CVS 运行所在的端口。此外，应将任何可能出现流量的端口添加到 TCP 策略的数据流重组端口列表，以便为 CVS 会话维护状态。 TCP 端口 2401 (pserver) 和 514 (rsh) 包含在出现数据流重组的客户端端口列表中。但请注意，如果服务器作为 xinetd 服务器 （即， pserver）运行，它可以在任何 TCP 端口上运行。应将任何非标准端口添加到数据流重组 **Client Ports** 列表中。有关详细信息，请参阅第 17-24 页上的选择数据流重组选项。

要检测格式不正确的 CVS 条目，请执行以下操作：

步骤 1　将 cvs 选项作为关键字参数添加到规则和类型 invalid-entry。

将数据包数据读取到关键字参数中

许可证：保护

可以使用 byte_extract 将数据包中指定数量的字节读取到某个变量中。然后，可以在同一规则中使用该变量作为某些其他检测关键字中特定参数的值。

此参数很有用，例如，可用于从其中的特定字节段描述数据包数据所包含的字节数的数据包提取数据大小。例如，特定字节段可能指出后续数据是由 4 个字节组成；您可以提取 4 个字节的数据大小来作为变量值。

可以使用 byte_extract 在规则中最多同时创建两个独立的变量。可以任意多次地重新定义 byte_extract 变量；如果输入变量名称相同但变量定义不同的新的 byte_extract 关键字，将会覆盖该变量的上一个定义。

下表介绍了 byte_extract 关键字所需的参数。

表 23-47　所需的 byte_extract 参数

参数	说明
Bytes to Extract	要从数据包提取的字节数。可以指定 1、 2、 3 或 4 字节。
Offset	从负载开头到开始提取数据之间的字节数。可指定 -65534 到 65535 字节。偏移量计数器从字节 0 开始计数，因此，计算偏移量值时，应该用向前计算所需的字节数减去 1。例如，指定 7 将会从 8 字节开始向前计算。规则引擎会从数据包负载起点开始向前计算；如果还指定了 **Relative**，规则引擎会从上一次成功内容匹配起向前计算。请注意，如果还指定了 **Relative**，只能指定负数；有关详细信息，请参阅其他可选的 byte_extract 参数表。
Variable Name	用于其他检测关键字的参数中的变量名称。可以指定以字母开头的字母数字字符串。

要进一步定义系统如何查找要提取的数据，可以使用下表中所述的参数。

表 23-48　其他可选的 byte_extract 参数

参数	说明
倍数	从数据包提取的值的乘数。可指定 0 到 65535 之间的任意数字。如果未指定乘数，将会默认设置为 1。
调整	将提取的数值四舍五入为最接近的 2 字节或 4 字节边界。如果选择了 **Multiplier**，系统会在进行舍入之前应用该乘数。
Relative	使**偏移量**相对于上一次成功内容匹配的结尾而不是负载起点。有关详细信息，请参阅所需的 byte_extract 参数表。

只能指定 **DCE/RPC**、 **Endian** 或 **Number Type**。

要定义 `byte_extract` 关键字如何计算其测试的字节，可以从下表中选择参数。如果未选择任何参数，规则引擎将采用大端字节顺序。

表 23-49　字节顺序 byte_extract 参数

参数	说明
Big Endian	按大端字节顺序处理数据（大端字节顺序是默认的网络字节顺序）。
Little Endian	按小端字节顺序处理数据
DCE/RPC	指定 DCE/RPC 预处理器处理的流量的 `byte_extract` 关键字。有关详细信息，请参阅第 15-2 页上的解码 DCE/RPC 流量。 由 DCE/RPC 预处理器确定大端字节顺序或小端字节顺序， **Number Type** 和 **Endian** 参数不适用。 如果启用此参数，还可以将 `byte_extract` 与其他特定 DCE/RPC 关键字结合使用。有关详细信息，请参阅第 23-54 页上的 DCE/RPC 关键字。

可以指定数字类型来将数据读取为 ASCII 字符串。要定义系统如何在数据包中查看字符串，可选择下表中所述的其中一个参数。

表 23-50　数字类型 byte_extract 参数

参数	说明
Hexadecimal String	以十六进制格式读取提取的字符串数据。
Decimal String	以十进制格式读取提取的字符串数据。
Octal String	以八进制格式读取提取的字符串数据。

例如，如果如下指定 `byte_extract` 的值：

- Bytes to Extract = 4
- Variable Name = var
- Offset = 8
- Relative 已启用

那么，规则引擎将会距离（相对于）上一次成功内容匹配 9 字节的四个字节中描述的数字读取到名为 `var` 的变量中（然后，您可以将该数字指定为某些关键字参数的值）。

下表列出了可以在其中指定 `byte_extract` 关键字中定义的变量的关键字参数。

表 23-51　接受 byte_extract 变量的参数

关键字	参数	有关详细信息，请参阅.....
content	Depth、 Offset、 Distance、 Within	第 23-16 页上的限制内容匹配
byte_jump	Offset	第 23-28 页上的 byte_jump
byte_test	Offset、 Value	第 23-30 页上的 byte_test
isdataat	Offset	第 23-74 页上的 isdataat

要使用 byte_extract，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 `byte_extract` 并点击 **Add Option**。

`byte_extract` 部分将显示在上次选择的关键字下方。

使用规则关键字发起活动响应

许可证：保护

系统可以发起活动响应，以在响应触发的 TCP 规则时关闭 TCP连接，或者在响应触发的 UDP 规则时关闭 UDP 会话。有两个关键字提供了两种不同的活动响应发起方法。如果数据包触发包含这两个关键字当中的任何一个，系统将发起单一活动响应。您还可以使用 `config response` 命令配置要使用的活动响应接口以及要在被动部署中尝试的 TCP 重置次数。

活动响应在内联部署中最有效，因为重置更有可能及时到达以影响连接或会话。例如，在内联部署中对 `react` 关键字作出响应时，系统会为连接的两端将 TCP 重置 (RST) 数据包直接插入到流量中（正常情况下，这样应该会关闭连接）。

出于一些原因，活动响应并不用于取代防火墙；这些原因包括：系统不能在被动部署中插入数据包；攻击者可能已选择忽略或绕过活动响应。

由于活动响应可以回送，因此，系统不允许 TCP 重置发起 TCP 重置；这样可防止活动响应出现无穷尽的顺序。此外，为了符合标准做法，系统也不允许 ICMP 不可达数据包发起 ICMP 不可达数据包。

可以配置 TCP 数据流预处理器，使它在入侵规则触发了活动响应后检测连接或会话的其他流量。如果预处理器检测到其他流量，它会将指定最大数量的其他活动响应发送到连接或会话的两端。有关详细信息，请参阅第 17-2 页上的使用入侵丢弃规则启动活动响应。

有关可用于发起活动响应的关键字的信息，请参阅：

- 第 23-78 页上的按类型和方向发起主动响应
- 第 23-79 页上的在 TCP 重置之前发送 HTML 页面
- 第 23-80 页上的设置活动响应重置尝试次数和界面

按类型和方向发起主动响应

许可证：保护

可以使用 `resp` 关键字来主动响应 TCP 连接或 UDP 会话，具体取决于在规则报头中指定的是 TCP 还是 UDP 协议。有关详细信息，请参阅第 23-4 页上的指定协议。

使用关键字参数可指定数据包方向，以及指定是使用 TCP 重置 (RST) 数据包还是 ICMP 不可达数据包作为活动响应。

可以使用任何 TCP 重置或 ICMP 不可达参数来关闭 TCP 连接。只能使用 ICMP 不可达参数来关闭 UDP 会话。

此外，不同的 TCP 重置参数使得可以将数据包源和/或目标作为活动响应的目标。所有 ICMP 不可达参数都将数据包源作为目标，并且允许指定是使用 ICMP 网络、主机还是端口的不可达数据包，还是同时使用这三者的不可达数据包。

下表列出可与 `resp` 关键字配合使用以指定在规则触发时希望 ASA FirePOWER 模块执行此操作的参数。

表 23-52　　resp 参数

参数	说明
reset_source	将 TCP 重置数据包引至发送触发规则的数据包的终端。此外，可以指定 `rst_snd`（为了获得向后兼容性，仍支持使用此参数）。
reset_dest	将 TCP 重置数据包引至触发规则的数据包的预期目标终端。此外，可以指定 `rst_rcv`（为了获得向后兼容性，仍支持使用此参数）。
reset_both	将 TCP 重置数据包引至发送终端和接收终端。此外，可以指定 `rst_all`（为了获得向后兼容性，仍支持使用此参数）。
icmp_net	将 ICMP 网络不可达消息引至发送方。
icmp_host	将 ICMP 主机不可达消息引至发送方。
icmp_port	将 ICMP 端口不可达消息引至发送方。此参数用于终止 UDP 流量。
icmp_all	将以下 ICMP 消息引至发送方： • 网络不可达消息 • 主机不可达消息 • 端口不可达消息

例如，要将规则配置为会在规则触发时重置连接的两端，可使用 reset_both 作为 resp 关键字的值。

可以使用逗号分隔列表指定多个参数，如下所示：

argument,*argument*,*argument*

关于使用 config response 命令配置用以使用的主动响应界面和试图在被动部署中进行的 TCP 重新设定数的详细信息，请参阅第 23-80 页上的设置活动响应重置尝试次数和界面。

要指定活动响应，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **resp** 并点击 **Add Option**。

系统将显示 resp 关键字。

步骤 2　在 **resp** 字段中指定 resp 参数表中所述的任意参数；使用逗号分隔列表可指定多个参数。

在 TCP 重置之前发送 HTML 页面

许可证：保护

如果数据包触发规则，您可以使用 react 关键字将默认 HTML 页面发送到 TCP 连接客户端；发送 HTML 页面后，系统将使用 TCP 重置数据包来发起对连接两端的活动响应 react 关键字不会对 UDP 流量触发活动响应。

或者，可以指定以下参数：

msg

如果数据包触发使用 msg 参数的 react 规则， HTML 页面将包含规则事件消息。关于事件消息字段的说明，请参阅第 23-2 页上的了解规则结构。

如果未指定 msg 参数， HTML 页面将包含以下消息：

```
You are attempting to access a forbidden site.
Consult your system administrator for details.
```

注　由于活动响应可以回送，因此，请确保 HTML 响应页面不会触发 react 规则；否则，可能会导致活动响应出现无穷尽的顺序。思科建议您将 react 规则用于生产环境之前，先广泛测试这些规则。

关于使用 config response 命令配置用以使用的主动响应界面和试图在被动部署中进行的 TCP 重新设定数的详细信息，请参阅第 23-80 页上的设置活动响应重置尝试次数和界面。

要在发起活动响应之前发送 HTML 页面，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **react** 并点击 **Add Option**。

系统将显示 react 关键字。

步骤 2　您有两种选择：

- 要在关闭连接之前将包含为规则配置的事件消息的 HTML 页面发送到客户端，请在 **react** 字段中键入 msg。
- 要在关闭连接之前将包含以下默认消息的 HTML 页面发送到客户端，请将 **react** 字段留空：

```
You are attempting to access a forbidden site.
Consult your system administrator for details
```

设置活动响应重置尝试次数和界面

许可证：保护

可以使用 **config response** 命令进一步配置由 `resp` 和 `react` 规则发起的 TCP 重置的行为。此命令还会影响丢弃规则发起的活动响应的行为；有关详细信息，请参阅第 17-2 页上的使用入侵丢弃规则启动活动响应。

要使用 **config response** 命令，可以在 USER_CONF 高级变量中的单独一行插入此命令。有关使用 USER_CONF 变量的详细信息，请参阅第 2-25 页上的了解高级变量。

注意事项 请**勿**使用高级变量 `USER_CONF` 来配置入侵策略功能，除非功能描述或支持人员指示您这样做。存在冲突或重复的配置会导致系统停止。

要指定活动响应重置尝试次数和/或活动响应界面，请执行以下操作：

步骤 1 在 USER_CONF 高级变量中的单独一行插入 `config response` 命令的一种形式，具体取决于您是要仅指定活动响应重置尝试次数、仅指定活动响应界面还是要同时指定这两者。有以下选项可供选择：

- 要仅指定活动响应重置尝试次数，请插入以下命令：
  `config response: attempts att`
  例如：`config response: attempts 10`
- 要仅指定活动响应界面，请插入以下命令：
  `config response: device dev`
  例如：`config response: device eth0`
- 要指定活动响应重置尝试次数和活动响应界面，请插入以下命令：
  `config response: attempts att, device dev`
  例如：`config response: attempts 10, device eth0`

  其中：

  att 是尝试次数（1 到 20），每个 TCP 重置数据包在达到指定的尝试次数后，就会停留在当前连接窗口，以使接收主机接受该数据包。这种*扫射式*序列仅对被动部署有用；在内联部署中，系统会将重置数据包直接插入到数据流中，而不是触发数据包。系统只发送 1 个 ICMP 可达活动响应。

  dev 备用接口，您希望系统在被动部署中使用该接口发送活动响应，或者在内联部署中在该接口处插入活动响应。

过滤事件

许可证：保护

可以使用 `detection_filter` 关键字来防止某个规则生成事件，除非在指定时间内有指定数量的数据包触发该规则。这样可防止规则过早生成事件。例如，在几秒钟内登录失败两三次可能是预期行为，但在同一时间内出现大量登录尝试可能表示存在蛮力攻击。

`detection_filter` 关键字需要使用参数来定义系统是否跟踪源或目标 IP 地址、满足检测条件多少次后才会触发事件以及持续计数多长时间。

可使用以下语法延迟事件触发：

```
track by_src/by_dst, count count, seconds number_of_seconds
```

track 参数指定在计算符合规则检测条件的数据包数量时，是否使用数据包的源或目标 IP 地址。可选择下表中所述的参数值来指定系统如何跟踪事件实例。

表 23-53　detection_filter 跟踪参数

参数	说明
by_src	按源 IP 地址计算检测条件。
by_dst	按目标 IP 地址计算检测条件。

count 参数指定要使某个规则生成事件，在指定时间内必须有多少数据包为指定 IP 地址触发该规则。

seconds 参数指定要使某个规则生成事件，必须在多少秒内有指定数量的数据包触发该规则。

假设某个规则在数据包中搜索内容 foo，并将以下参数与 detection_filter 关键字配合使用：

```
track by_src, count 10, seconds 20
```

在此示例中，规则在 20 秒内从来自给定 IP 地址的 10 个数据包中检测到 foo 后才会生成事件。如果系统在头 20 秒内仅检测到有 7 个数据包包含 foo，将不会生成事件。但是，如果在头 20 秒内 foo 出现 40 次，规则将会生成 30 个事件，并在 20 秒后再次进行计数。

比较 threshold 和 detection_filter 关键字

detection_filter 关键字取代已被弃用的 threshold 关键字。但是，为了获得向后兼容性，仍支持使用 threshold 关键字，其作用与您在入侵策略中设置的阈值相同。

detection_filter 关键字是一种检测功能，适合在数据包触发规则前使用。在达到指定的数据包数量之前，规则不会针对触发检测到的数据包生成事件；在内联部署中，如果规则设置为丢弃数据包，在达到指定的数据包数量之前，规则不会丢弃数据包。相反，规则会针对会触发规则且在达到指定数据包数量后出现的数据包生成事件；在内联部署中，如果规则设置为丢弃数据包，规则将会丢弃数据包。

阈值是一种事件通知功能，不会造成检测操作。此功能适合在数据包触发事件后使用。在内联部署中，被设置为丢弃数据包的规则将会丢弃触发其本身的所有数据包，无论规则阈值如何。

请注意，可以在入侵策略中使用使用 detection_filter 关键字与入侵事件阈值、入侵事件抑制和基于速率的攻击防御等功能的任意组合。另请注意，如果启用某个导入的本地规则，而该规则将弃用的 threshold 关键字与某个入侵策略中的入侵事件阈值功能结合起来使用，策略验证将会失败。有关详细信息，请参阅第 20-19 页上的配置事件阈值、第 20-23 页上的按入侵策略配置抑制、第 20-26 页上的设置动态规则状态和第 35-12 页上的导入本地规则文件。

评估攻击后流量

许可证：保护

使用 tag 关键字可指示系统记录主机或会话的其他流量。使用 tag 关键字指定要捕获的流量的类型和数量时，可使用以下语法：

```
tagging_type, count, metric, optional_direction
```

以下三个表介绍了其他可用参数。

有两种标记类型可供选择。下表介绍了这两种标记类型。请注意，如果您在入侵规则中仅配置规则报头选项，会话标记参数类型会使系统像记录来自不同会话的数据包一样来记录来自同一个会话的数据包。要对自同一个会话的数据包进行分组，请在同一入侵规则中配置一个或多个规则选项（例如，flag 关键字或 content 关键字）。

表 23-54　标记参数

参数	说明
会话	记录触发规则的会话中的数据包。
主机	记录来自发送触发规则的数据包的主机的数据包。可以添加方向修饰符，以仅记录来自主机 (src) 或发送到主机 (dst) 的流量。

要指明想要记录的流量数量，请使用以下参数：

表 23-55　计数参数

参数	说明
count	您想在规则触发后记录的数据包数量或秒数。 此度量单位用指标参数指定 （该参数跟在计数参数后面）。

选择下表中所述的其中一个指标，以指明是要按时间还是流量数量进行记录。

注意事项　高带宽网络可以每秒查看成千上万个数据包，而且对大量数据包进行标记可能会严重影响性能，因此，请务必根据网络环境调整设置。

表 23-56　记录指标参数

参数	说明
数据包	在规则触发后记录计数指定的数量的数据包。
秒	在规则触发后在计数指定的秒数内记录流量。

例如，如果带有以下 tag 关键字值的规则触发：

```
host, 30, seconds, dst
```

将会记录在接下来的 30 秒内从客户端传输到主机的所有数据包。

检测跨越多个数据包的攻击

许可证：保护

可以使用 flowbits 关键字为会话分配状态名称。通过根据之前命名的状态分析会话中的后续数据包，系统可以检测在一个会话中跨越多个数据包的攻击，并发出有关警报。

flowbits 状态名称是用户定义的标签，将被分配给会话特定部分中的数据包。可以根据数据包内容给数据包分配状态名称标签，以帮助将恶意数据包和那些您不想对其发出警报的数据包区分开。最多可以为定义 1024 个状态名称。例如，如果要对您知道仅在成功登录后才会出现的恶意数据包发出警报，可以使用 flowbits 关键字过滤掉构成初始登录尝试的数据包，这样就能够重点关注恶意数据包。要这样做，首先要创建一个会给具有状态为 logged_in 的已建立登录的会话中的所有数据包分配标签的规则，然后创建另一个包含 flowbits 的规则，用以检查具有您在第一个规则中设置的状态的数据包，并且只对这些数据包采取操作。有关使用 flowbits 来确定用户是否已登录的示例，请参阅第 23-84 页上的使用 state_name 的 flowbits 示例。

可选的*组名称*用于向状态组添加状态名称。一个状态名称可以属于若干个组。未与组关联的状态并不相互排斥，因此，触发和设置未与组关联的状态的规则不会影响其他同时设置的状态。有关在组中包含状态名称可如何防止误报的示例（通过取消设置同一个组中的另一个状态），请参阅第 23-85 页上的导致误报的 flowbits 示例。

下表介绍了可用于 `flowbits` 关键字的运算符、状态和组的各种组合。请注意，状态名称可以包含字母数字字符、句号 (.)、下划线 (_) 和破折号 (-)。

表 23-57　flowbits 选项

运算符	状态选项	组	说明
set	state_name	可选	为数据包设置某个指定状态。如果定义了某个组，则在该指定的组中设置该状态。
	state_name&state_name	可选	为数据包设置多个指定状态。如果定义了某个组，则在该指定的组中设置这些状态。
setx	state_name	必需	为数据包在指定组中设置某个指定状态，并取消设置该组中的所有其他状态。
	state_name&state_name	必需	为数据包在指定组中设置多个指定状态，并取消设置该组中的所有其他状态。
unset	state_name	没有组	为数据包取消设置某个指定状态。
	state_name&state_name	没有组	为数据包取消设置多个指定状态。
	全部	必需	取消设置指定组中的所有状态。
toggle	state_name	没有组	取消设置某个指定状态（如果已设置），以及设置某个指定状态（如果未设置）。
	state_name&state_name	没有组	取消设置多个指定状态（如果已设置），以及设置多个指定状态（如果未设置）。
	全部	必需	取消设置指定组中已设置的所有状态，以及设置指定组中未设置的所有状态。
isset	state_name	没有组	确定是否已在数据包中设置了某个指定状态。
	state_name&state_name	没有组	确定是否已在数据包中设置了多个指定状态。
	state_name|state_name	没有组	确定是否已在数据包中设置了任何指定状态。
	any	必需	确定是否已在指定组中设置了任何状态。
	全部	必需	确定是否已在指定组中设置了所有状态。
isnotset	state_name	没有组	确定是否未在数据包中设置某个指定状态。
	state_name&state_name	没有组	确定是否未在数据包中设置多个指定状态。
	state_name|state_name	没有组	确定是否未在数据包中设置任何指定状态。
	any	必需	确定是否未在数据包中设置任何状态。
	全部	必需	确定是否未在数据包中设置所有状态。
重置	（无状态）	可选	为所有数据包取消设置所有状态。取消设置某个组中的所有状态（如果已指定该组）。
noalert	（无状态）	没有组	可将此运算符与任何其他运算符结合使用，以抑制事件生成。

使用 flowbits 关键字时，请注意：

- 使用 setx 运算符时，指定的状态只能属于指定的组，而不能属于任何其他组。
- 可以多次定义 setx 操作符，每次用一个实例指定不同的状态和同一个组。
- 如果使用 setx 运算符并指定了某个组，则不能对该指定的组使用 set、 toggle 或 unset 运算符。
- isset 和 isnotset 运算符会对指定状态进行评定，无论该状态是否在组中。
- 保存入侵策略、重新应用入侵策略以及应用访问控制策略时（不管访问控制策略是引用一个入侵策略还是多个入侵策略），如果您启用包含**未**指定组的 isset 或 isnotset 运算符的一个规则，而且您不会为对应的状态名称和协议启用至少一个会影响 flowbits 分配的规则（set、setx、set、toggle），那么，将会启用会影响对应状态名称的 flowbits 分配的所有规则。
- 保存入侵策略、重新应用入侵策略以及应用访问控制策略时（不管访问控制策略是引用一个入侵策略还是多个入侵策略），如果您启用包含**已**指定组的 isset 或 isnotset 运算符的一个规则，系统还将会启用会影响 flowbits 分配（set、setx、unset、toggle）且定义对应组名称的所有规则。

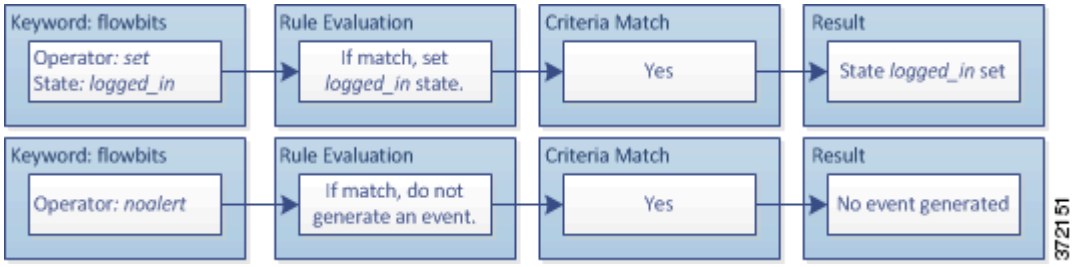
使用 state_name 的 flowbits 示例

以 Bugtraq ID #1110 中所述的 IMAP 漏洞为例。该漏洞存在于 IMAP 的实现中，尤其是在 LIST、LSUB、 RENAME、 FIND 和 COPY 命令中。但是，要想利用该漏洞，攻击者必须登录到 IMAP 服务器。由于来自 IMAP 服务器的登录确认及紧随着而来的漏洞必定存在于不同的数据包中，因此，难以构建非基于流量的规则来捕获该漏洞。使用 flowbits 关键字可以构建一系列规则来追踪用户是否登录到 IMAP 服务器；如果是，将会在检测到其中一项攻击时生成事件。如果用户未登录，则攻击不能利用该漏洞，且不会生成事件。

以下两个规则分片说明了此示例。第一个规则分片查找来自 IMAP 服务器的 IMAP 登录确认：

```
alert tcp any 143 -> any any (msg:"IMAP login"; content:"OK
LOGIN"; flowbits:set,logged_in; flowbits:noalert;)
```

下图说明了上述规则分片中 flowbits 关键字的影响：

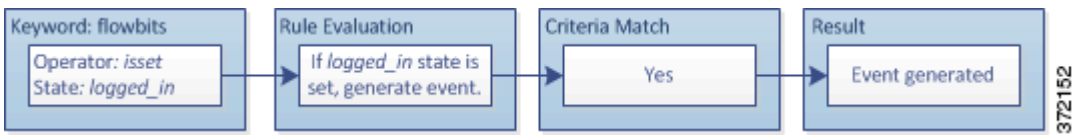


请注意， flowbits:set 设置 logged_in 状态， flowbits:noalert 则抑制警报，因为 IMAP 服务器上可能会出现许多无恶意的登录会话。

以下规则分片查找 LIST 字符串，但不生成事件，除非由于会话中某个之前的数据包而设置了 logged_in 状态：

```
alert tcp any any -> any 143 (msg:"IMAP LIST";
content:"LIST"; flowbits:isset,logged_in;)
```

下图说明了上述规则分片中 flowbits 关键字的影响：



在这种情况下，如果之前的数据包已促使包含第一个分片的规则触发，则包含第二个分片的规则将会触发并生成事件。

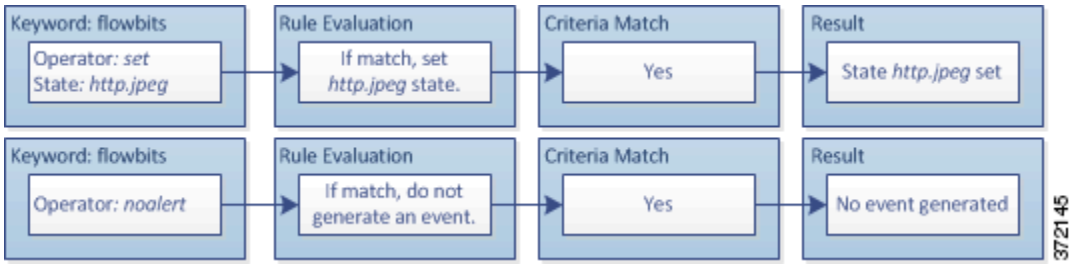
导致误报的 flowbits 示例

在一个组中包含在不同规则中设置的不同状态名称可防止误报事件；如果后续数据包中的内容与状态不再有效的规则相匹配，就会出现误报事件。以下示例说明不在一个组中包含多个状态名称如何会导致误报。

假设以下三个规则分片在一个会话中按所示的顺序触发：

```
(msg:"JPEG transfer"; content:"image/";pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
flowbits:set,http.jpeg; flowbits:noalert;)
```

下图说明了上述规则分片中 `flowbits` 关键字的影响：

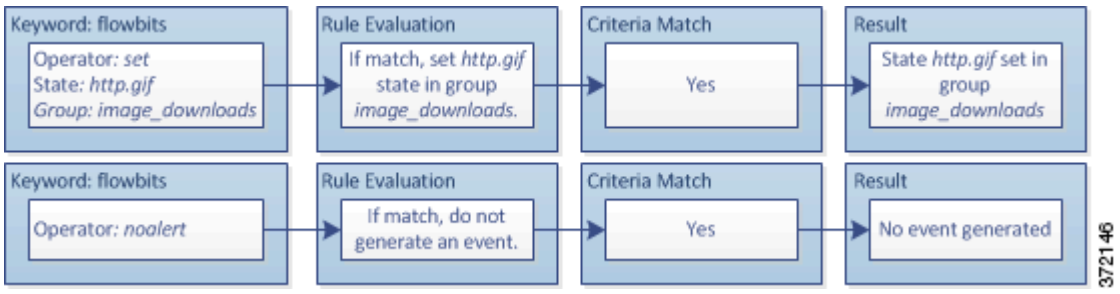


第一个规则分片中的 `content` 和 `pcre` 关键字与 JPEG 文件下载相匹配，`flowbits:set,http.jpeg` 设置 `http.jpeg flowbits` 状态，`flowbits:noalert` 使规则停止生成事件。将不会生成事件，因为该规则的目的是检测文件下载并设置 `flowbits` 状态；为此，一个或多个伴随规则可以测试状态名称和恶意内容，如果检测到恶意内容，将会生成事件。

以下规则分片检测在上述 JPEG 文件下载之后发生的 GIF 文件下载：

```
(msg:"GIF transfer"; content:"image/"; pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
flowbits:set,http.tif,image_downloads; flowbits:noalert;)
```

下图说明了上述规则分片中 `flowbits` 关键字的影响：

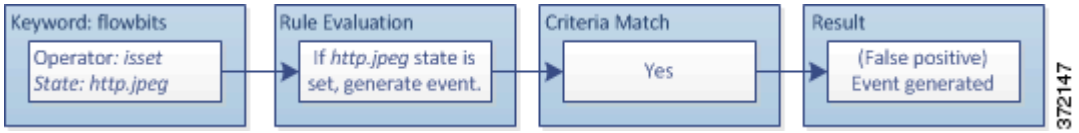


第二个规则中的 `content` 和 `pcre` 关键字与 GIF 文件下载相匹配，`flowbits:set,http.gif` 设置 `http.gif` 流位状态，`flowbits:noalert` 阻止规则生成事件。请注意，仍会设置由第一个规则分片设置的 `http.jpeg` 状态，即使不再需要使用它；这是因为如果检测到后续 GIF 下载，JPEG 下载必须终止。

第三个规则分片伴随第一个规则分片出现：

```
(msg:"JPEG exploit";
flowbits:isset,http.jpeg;content:"|FF|"; pcre:"
/\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

下图说明了上述规则分片中 `flowbits` 关键字的影响：



在第三个规则分片中，`flowbits:isset,http.jpeg` 确定是否已设置现在不相关的 `http.jpeg` 状态，`content` 和 `pcre` 则匹配在 JPEG 文件中是恶意的但在 GIF 文件中并非恶意的内容。第三个规则分片会针对 JPEG 文件中不存在漏洞生成误报事件。

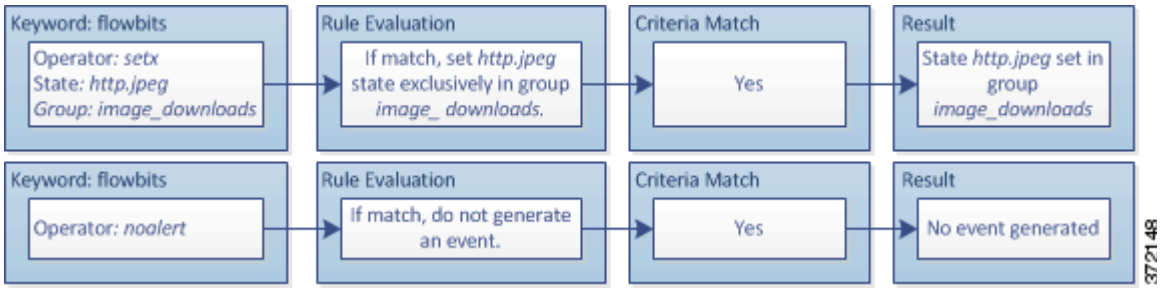
防止误报的 flowbits 示例

以下示例说明在一个组中包含多个状态名称并使用 `setx` 运算符如何能防止误报。

以下规则分片与上一个规则分片示例大致相同，不同之处是，以下示例的前两个规则将两个不同的状态名称包含在同一个状态组中。

```
(msg:"JPEG transfer"; content:"image/";pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
flowbits:setx,http.jpeg,image_downloads; flowbits:noalert;)
```

下图说明了上述规则分片中 `flowbits` 关键字的影响：

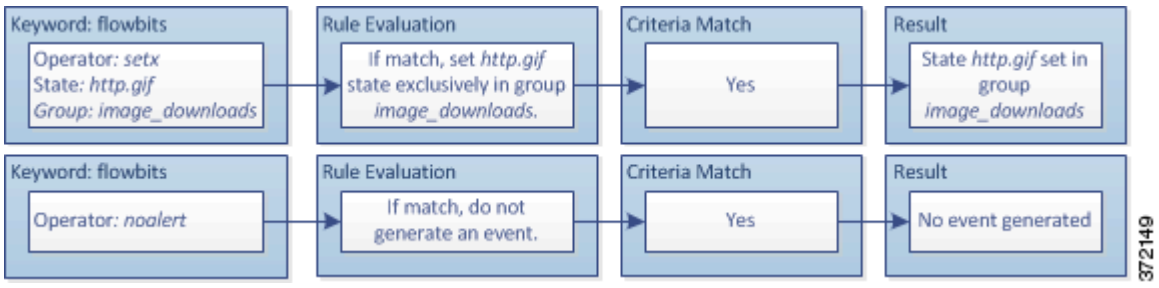


如果第一个规则分片检测到 JPEG 文件下载，`flowbits:setx,http.jpeg,image_downloads` 关键字会将 `flowbits` 状态设置为 `http.jpeg`，并将该状态包含在 `image_downloads` 组中。

然后，下一个规则会后续 GIF 文件下载：

```
(msg:"GIF transfer"; content:"image/"; pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
flowbits:setx,http.tif,image_downloads; flowbits:noalert;)
```

下图说明了上述规则分片中 `flowbits` 关键字的影响：

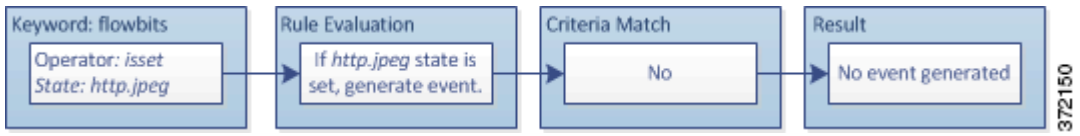


如果第二个规则片段与 GIF 下载相匹配，`flowbits:setx,http.gif,image_downloads` 关键字将会设置 `http.gif flowbits` 状态，并取消设置组中的另一个状态 `http.jpeg`。

第三个规则分片不会导致误报：

```
(msg:"JPEG exploit";
flowbits:isset,http.jpeg;content:"|FF|"; pcre:"/
\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

下图说明了上述规则分片中 `flowbits` 关键字的影响：



由于 `flowbits:isset,http.jpeg` 为假，因此，规则引擎会停止处理规则，且不会生成事件，从而避免误报 （即使 GIF 文件中的内容与 JPEG 文件的漏洞内容相匹配）。

生成关于 HTTP 编码类型和位置的事件

许可证：保护

可以使用 `http_encode` 关键字在未经规范化的 HTTP 请求或响应中生成关于编码类型的事件 - 可以是在 HTTP URI 中，在 HTTP 报头的非 cookie 数据中，在 HTTP 请求报头的 cookie 中，或者在 HTTP 响应的 set-cookie 数据。

必须配置 HTTP 检查预处理器以检查 HTTP 响应和 HTTP cookie，从而使用 `http_encode` 关键字返回规则的匹配项。有关详细信息，请参阅第 15-27 页上的解码 HTTP 流量和第 15-29 页上的选择服务器级别 HTTP 规范化选项。

此外，要使入侵规则中的 `http_encode` 关键字针对特定编码类型触发事件，必须在 HTTP 检查预处理器配置中为该编码类型启用解码和警报选项。有关详细信息，请参阅第 15-36 页上的选择服务器级别的 HTTP 规范化编码选项。

请注意， base36 编码类型已被弃用。为了实现向后兼容性，允许在现有规则中使用 base36 参数，但它不会使规则引擎检查 base36 流量。

下表介绍了此选项可在 HTTP URI、报头、 cookie 和 set-cookie 中为其生成事件的编码类型。

表 23-58　　HTTP_encode 编码类型

编码类型	说明
utf8	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测 UTF-8 编码。
double_encode	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测双编码。
non_ascii	当检测到非 ASCII 字符但未启用检测到的编码类型时，在指定位置检测非 ASCII 字符。
uencode	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测 Microsoft %u 编码。
bare_byte	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测裸字节编码。

要在入侵规则中识别 HTTP 编码类型和位置，请执行以下操作：

步骤 1　向规则添加 `http_encode` 关键字。

步骤 2　从 **Encoding Location** 下拉列表中，选择是要在 HTTP URI、报头还是 cookie （包括 set-cookie）中搜索指定的编码类型。

步骤 3　使用以下其中一种格式指定一个或多个编码类型：

```
encode_type
encode_type|encode_type|encode_type...
!encode_type
```

其中， *encode_type* 是以下其中一项：

```
utf8, double_encode, non_ascii, uencode, bare_byte
```

请注意，不能同时使用否定 (!) 和 OR (|) 运算符。

步骤 4　或者，将多个 `http_encode` 关键字添加到同一个规则，并为每个关键字添加条件。例如，按照以下条件输入两个关键字：

第一个 `http_encode` 关键字：

- **Encoding Location**：`HTTP URI`
- **Encoding Type**：`utf8`

另一个 `http_encode` 关键字：

- **Encoding Location**：`HTTP URI`
- **Encoding Type**：`uencode`

此示例配置将在 HTTP URI 中搜索 UTF-8 和 Microsoft IIS %u 编码。

检测文件类型和版本

许可证：保护

`file_type` 和 `file_group` 关键字允许根据文件的类型和版本检测通过 FTP、 HTTP、 SMTP、 IMAP、 POP3 和 NetBIOS-ssn (SMB) 传输的文件。请**勿**在单个入侵规则中使用多个 `file_type` 或 `file_group` 关键字。

提示　更新漏洞数据库 (VDB) 可以使规则编辑器获得最新的文件类型、版本和组。有关详细信息，请参阅第 35-7 页上的更新漏洞数据库。

必须启用特定预处理器，以便为与 `file_type` 或 `file_group` 关键字匹配的流量生成入侵事件。

表 23-59　file_type 和 file_group 入侵事件生成

传输协议	所需的预处理器或预处理器选项
FTP	FTP/Telnet 预处理器和 **Normalize TCP Payload** 内联规范化预处理器选项；请参阅第 15-16 页上的解码 FTP 和 Telnet 流量和第 17-5 页上的规范化内联流量。
HTTP	HTTP 检查预处理器；请参阅第 15-27 页上的解码 HTTP 流量。
SMTP	SMTP 预处理器；请参阅第 15-52 页上的解码 SMTP 流量。
IMAP	IMAP 预处理器；请参阅第 15-47 页上的解码 IMAP 流量。

表 23-59　file_type 和 file_group 入侵事件生成

传输协议	所需的预处理器或预处理器选项
POP3	POP 预处理器；请参阅第 15-49 页上的解码 POP 流量。
NetBIOS-ssn (SMB)	**SMB File Inspection** DCE/RPC 预处理器选项；请参阅第 15-2 页上的解码 DCE/RPC 流量。

有关详细信息，请参阅：

- 第 23-89 页上的 file_type
- 第 23-89 页上的 file_group

file_type

使用 `file_type` 关键字可指定在流量中检测到的文件的类型和版本。文件类型参数 （例如 **JPEG** 和 **PDF**）用于识别要在流量中查找的文件格式。

注　请**勿**在同一入侵规则中将 `file_type` 关键字与另一个 `file_type` 或 `file_group` 关键字配合使用。

系统默认选择 **Any Version**，但某些文件类型允许选择版本选项（例如 PDF 版本 **1.7**）来确定要在流量中查找的特定文件类型版本。

要查看和配置最新的文件类型和版本，请更新 VDB。有关详细信息，请参阅第 35-7 页上的更新漏洞数据库。

要在入侵规则中选择文件类型和版本，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **file_type** 并点击 **Add Option**。

系统将显示 `file_type` 关键字。

步骤 2　从下拉列表中选择一个或多个文件类型。选择文件类型会自动将相应的参数添加到规则。

要从规则中移除文件类型参数，请点击要移除的文件类型旁边的删除 ( ) 图标。

步骤 3　或者，可以为每种文件类型自定义目标版本。系统默认选择 **Any Version**，但某些文件类型允许选择单个目标版本。

注　更新 VDB 可以使规则编辑器获得最新的文件类型和版本。如果选择 **Any Version**，系统将会配置规则，以包含在以后的 VDB 更新中添加的新版本。

file_group

使用 `file_group` 关键字可选择思科定义的、包含在流量中找到的类似文件类型 （例如**多媒体**或**音频**）的组。文件组还包含思科为组中的每种文件类型定义的版本。

注　请**勿**在同一入侵规则中将 `file_group` 关键字与另一个 `file_group` 或 `file_type` 关键字配合使用。

要查看和配置最新的文件组，请更新 VDB。有关详细信息，请参阅第 35-7 页上的更新漏洞数据库。

要在入侵规则中选择文件组，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **file_group** 并点击 **Add Option**。

系统将显示 `file_group` 关键字。

步骤 2　选择要添加到规则的文件组。

指向特定负载类型

许可证：保护

`file_data` 关键字提供一个指针，该指针作为可用于其他关键字（例如 `content`、`byte_jump`、`byte_test` 和 `pcre`）的位置参数参考。检测到的流量确定 `file_data` 关键字指向的数据类型。可以使用 `file_data` 关键字指向以下负载类型的开头：

- HTTP 响应正文

  要检查 HTTP 响应数据包，必须启用 HTTP 检查预处理器，还必须将该预处理器配置为会检查 HTTP 响应。有关详细信息，请参阅第 15-27 页上的解码 HTTP 流量和第 15-29 页上的选择服务器级别 HTTP 规范化选项中的 **Inspect HTTP Responses**。如果 HTTP 检查预处理器检测到 HTTP 响应正文数据，`file_data` 关键字将会进行匹配。

- 未压缩的 gzip 文件数据

  要检查 HTTP 响应正文中未压缩的 gzip 文件，必须启用 HTTP 检查预处理器，还必须将该预处理器配置为会检查 HTTP 响应以及会解压缩 HTTP 响应正文中的 gzip 压缩文件。有关详细信息，请参阅第 15-27 页上的解码 HTTP 流量以及第 15-29 页上的选择服务器级别 HTTP 规范化选项中的 **Inspect HTTP Responses** 和 **Inspect Compressed Data** 选项。如果 HTTP 检查预处理器在 HTTP 响应正文中检测到未压缩的 gzip 数据，`file_data` 关键字将会进行匹配。

- 规范化的 JavaScript

  要检查规范化的 JavaScript 数据，必须启用 HTTP 检查预处理器，还必须将该预处理器配置为检查 HTTP 响应。有关详细信息，请参阅第 15-27 页上的解码 HTTP 流量和第 15-29 页上的选择服务器级别 HTTP 规范化选项中的 **Inspect HTTP Responses**。如果 HTTP 检查预处理器在响应主体数据中检测到 JavaScript，`file_data` 关键字将会进行匹配。

- SMTP 负载

  要检查 SMTP 负载，必须启用 SMTP 预处理器。有关详细信息，请参阅第 15-56 页上的配置 SMTP 解码。如果 SMTP 预处理器检测到 SMTP 数据，`file_data` 关键字将会进行匹配。

- SMTP、 POP 或 IMAP 流量中的编码邮件附件

  要检查 SMTP、 POP 或 IMAP 流量中的邮件附件，必须分别启用 SMTP、 POP 或 IMAP 预处理器或者启用它们的任意组合。然后，必须确保将已启用的每个预处理器配置为会对您想要解码的每种附件编码类型进行解码。可以为每个预处理器配置的附件解码选项是：**Base64 Decoding Depth**、 **7-Bit/8-Bit/Binary Decoding Depth**、 **Quoted-Printable Decoding Depth** 和 **Unix-to-Unix Decoding Depth**。有关详细信息，请参阅第 15-47 页上的解码 IMAP 流量、第 15-49 页上的解码 POP 流量和第 15-52 页上的解码 SMTP 流量。

  可以在一个规则中使用多个 `file_data` 关键字。

要指向特定负载类型的开头，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **file_data** 并点击 **Add Option**。

系统将显示 `file_data` 关键字。

`file_data` 关键字没有参数。

指向数据包负载的开头

许可证：保护

`pkt_data` 关键字提供一个指针，该指针作为可用于其他关键字（例如 `content`、`byte_jump`、`byte_test` 和 `pcre`）的位置参数参考。

如果检测到规范化的 FTP、 telnet 或 SMTP 流量， `pkt_data` 关键字将指向规范化数据包负载的开头。如果检测到其他流量， `pkt_data` 关键字将指向原始 TCP 或 UDP 负载的开头。

必须启用以下规范化选项，系统才会对相应流量进行规范化以供入侵规则进行检测：

- 要规范化 FTP 流量以供检测，必须启用 FTP 和 Telnet 预处理器的 **Detect Telnet Escape codes within FTP commands** 选项；请参阅第 15-22 页上的配置服务器级别 FTP 选项。
- 要规范化 telnet 流量以供检测，必须启用 FTP 和 Telnet 预处理器的 **Normalize** telnet 选项；请参阅第 15-18 页上的了解 Telnet 选项。
- 要规范化 SMTP 流量以供检测，必须启用 SMTP 预处理器的 **Normalize** 选项；请参阅第 15-53 页上的了解 SMTP 解码。

可以在一个规则中使用多个 `pkt_data` 关键字。

要指向数据包负载的开头，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **pkt_data** 并点击 **Add Option**。

系统将显示 `pkt_data` 关键字。

`pkt_data` 关键字没有参数。

解码和检查 Base64 数据

许可证：保护

可以结合使用 `base64_decode` 和 `base64_data` 关键字，以指示规则引擎将指定数据作为 Base64 数据进行解码和检查。这可能很有用，例如，对于检查 Base64 编码 HTTP 身份验证请求报头，以及对于检查 HTTP PUT 和 POST 请求中的 Base64 编码数据。

这两个关键字对于编码和检查 HTTP 请求中的 Base64 数据尤其有用。但是，也可以将这两个关键字与像 HTTP 一样使用空格和制表符的任何协议（例如 SMTP）结合使用，以将长的报头行展开为跨越多行。如果协议中不存在这样的行展开（即为“折叠”），检查将在后面不跟有空格或制表符的任何回车符或换行符处结束。

有关详细信息，请参阅：

- 第 23-92 页上的base64_decode

- 第 23-92 页上的base64_data

base64_decode

许可证：保护

base64_decode 关键字指示规则引擎将数据包数据解码为 Base64 数据。使用可选参数可指定要解码的字节数量以及在数据中的哪个位置开始解码。

可以在一个规则中使用 base64_decode 关键字一次；此关键字必须位于至少一个 base64_data 关键字实例前面。有关详细信息，请参阅第 23-92 页上的 base64_data。

解码 Base64 数据之前，规则引擎会将跨越多行的已折叠的长报头展开。当规则引擎遇到以下任何情况时，解码将会结束：

- 报头行结尾
- 要解码的指定字节数
- 数据包结尾

下表介绍了可与 base64_decode 关键字配合使用的参数。

表 23-60　　可选的 base64_decode 参数

参数	说明
字节	指定要解码的字节数。如果未指定，解码将持续到报头行结尾或数据包负载结尾（以先到者为准）。可以指定非零的正值。
Offset	确定相对于数据包负载开头的偏移量，如果还指定了 **Relative**，则确定相对于当前检查位置的偏移量。可以指定非零的正值。
Relative	指定相对于当前检查位置的检查。

要解码 Base64 数据，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **base64_decode** 并点击 **Add Option**。

系统将显示 base64_decode 关键字。

步骤 2　或者，选择可选的 base64_decode 参数表中所述的任意参数。

base64_data

许可证：保护

base64_data 关键字提供用于检查使用 base64_decode 关键字进行解码的 Base64 数据的参考。base64_data 关键字将检查设置在解码的 Base64 数据开头开始。或者，可以随后使用可用于其他关键字的位置参数（例如 content 或 byte_test）进一步指定要检查的位置。

使用 base64_decode 关键字后，必须至少使用一次 base64_data 关键字至少一次；可以多次使用 base64_data 以返回到解码的 Base64 数据的开头。

检查 Base64 数据时，请注意：

- 不能使用快速模式匹配程序；有关详细信息，请参阅第 23-25 页上的 Use Fast Pattern Matcher。

- 如果在某个规则中以干预性 HTTP 内容参数中断 Base64 检查，必须在该规则中插入另一个 `base64_data` 关键字后再进一步检查 Base64 数据；有关详细信息，请参阅第 23-21 页上的 HTTP 内容选项。

要检查解码的 Base64数据，请执行以下操作：

步骤 1　在 Create Rule 页面上，从下拉列表中选择 **base64_data** 并点击 **Add Option**。

系统将显示 `base64_data` 关键字。

构建规则

许可证：保护

就像创建自定义标准文本规则一样，您也可以修改现有的由思科提供的标准文本规则和共享对象规则，并将所做的更改保存为新规则。请注意，对于思科提供的共享对象规则，您只能修改规则报头信息，例如，源端口、目标端口、源 IP 地址和目标 IP 地址。不能修改共享对象规则中的规则关键字和规则参数。

有关详细信息，请参阅：

- 第 23-93 页上的编写新规则
- 第 23-95 页上的修改现有规则
- 第 23-96 页上的向规则添加注释
- 第 23-96 页上的删除自定义规则

编写新规则

许可证：保护

您可以创建自己的标准文本规则。

在自定义标准文本规则中，可以设置规则报头设置、规则关键字和规则参数。或者，可以通过规则报头设置将规则设置为仅针对使用特定协议以及发往或来自特定 IP 地址或端口的流量。

创建新规则后，可以使用规则编号（其格式为 `GID:SID:Rev`）再次迅速找到该规则。所有标准文本规则的规则编号均以 1 开头。规则编号的第二部分（Snort ID (SID) 号）指明规则是本地规则还是由思科提供的规则。当您创建新规则时，系统会向新规则分配下一个可用于本地规则的 Snort ID 号，并将该规则保存在本地规则类别中。本地规则的 Snort ID 号从 1,000,000 开始，每个本地新规则的 SID 号按 1 递增。规则编号的最后一部分是修订号。对于新规则，修订号为 1。每修改一次自定义规则，修订号就增加 1。

注　系统会向您导入的入侵策略中的任何自定义规则分配一个新的 SID。有关详细信息，请参阅第 B-1 页上的导入和导出配置。

要使用规则编辑器编写自定义标准文本规则，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy > Rule Editor**。

系统将显示 Rule Editor 页面。

步骤 2　点击 **Create Rule**。

系统将显示 Create Rule 页面。

步骤 3　在 **Message** 字段中，输入要与事件一起显示的消息。

有关事件消息的详细信息，请参阅第 23-11 页上的定义事件消息。

提示　必须指定规则消息。此外，消息不能只包含空白字符、一个或多个引号、一个或多个撇号或者仅由空白字符、引号或撇号组成的任意组合。

步骤 4　从 **Classification** 列表中选择用以描述事件类型的分类。

有关有效分类的详细信息，请参阅第 23-11 页上的定义入侵事件分类。

步骤 5　从 **Action** 列表中选择要创建的规则的类型。可以使用以下其中一个选项：

- 选择 **alert**，将会创建在被流量触发时会生成事件的规则。
- 选择 **pass**，将会创建忽略触发自身的流量的规则。

步骤 6　从 **Protocol** 列表中选择您希望规则检查的数据包的流量协议（**tcp**、**udp**、**icmp** 或 **ip**）。

有关选择协议类型的详细信息，请参阅第 23-4 页上的指定协议。

步骤 7　在 **Source IPs** 字段中，为应触发规则的流量输入源 IP 地址或地址块。在 **Destination IPs** 字段中，为应触发规则的流量输入目标 IP 地址或地址块。

有关规则编辑器接受的 IP 地址语法的更多详细信息，请参阅第 23-5 页上的在入侵规则中指定 IP 地址。

步骤 8　在 **Source Port** 字段中，为应触发规则的流量输入发起端口号。在 **Destination Port** 字段中，为应触发规则的流量输入接收端口号。

注　如果协议设置为 `ip`，系统将忽略入侵规则报头中的端口定义。

有关规则编辑器接受的端口语法的更多详细信息，请参阅第 23-8 页上的在入侵规则中定义端口。

步骤 9　从 **Direction** 列表中，选择指示您希望触发规则的流量方向的运算符。可以使用以下其中一个选项：

- **Directional** 匹配从源 IP 地址流向目标 IP 地址的流量
- **Bidirectional** 从源 IP 地址流向目标 IP 地址或从目标 IP 地址流向源 IP 地址的流量

步骤 10　从 **Detection Options** 列表中选择要使用的关键字。

步骤 11　点击 **Add Option**。

步骤 12　输入要用于指定所添加的关键字的任何参数。有关规则关键字及其使用方式的详细信息，请参阅第 23-9 页上的了解规则中的关键字和参数。

添加关键字和参数时，还可以执行以下操作：

- 要对添加的关键字进行重新排序，请点击要移动的关键字旁边的向上或向下箭头。
- 要删除关键字，点击要删除的关键字旁边的 **X**。

对要添加的每个关键字选项重复第12 至第 10 步。

步骤 13　点击 **Save As New** 保存规则。

系统会向新创建的规则分配规则编号序列中下一个可用于本地规则的 Snort ID (SID) 号，并将该规则保存在本地规则类别中。

系统不会根据新的或更改后的规则来评估流量，直至您在适当的入侵策略中启用这些规则，并将该入侵策略作为访问控制策略的一部分进行应用。有关详细信息，请参阅第 4-10 页上的应用访问控制策略。

修改现有规则

许可证：保护

您可以修改自定义标准文本规则。您还可以修改思科提供的标准文本规则或共享对象规则，并通过保存规则来创建一个或多个规则实例。

创建规则或修改思科规则会将新规则或修订复制到本地规则类别中，并会向该规则分配下一个大于 100000 的可用 Snort ID (SID)。

对于共享对象规则，只能修改报头信息。不能修改共享对象规则或其参数中使用的规则关键字。修改共享对象规则的报头信息并保存更改将会为该规则创建生成器 ID (GID) 为 3 的新实例，并会为自定义规则创建下一个可用 SID。Rule Editor 将共享对象规则的新实例链接到保留的 `soid` 关键字，该关键字将创建的规则映射到 VRT 所创建的规则。您可以删除自行创建的共享对象规则实例，但是不能删除由思科提供的共享对象规则。有关详细信息，请参阅第 23-3 页上的了解规则报头和第 23-96 页上的删除自定义规则。

注　请勿修改共享对象规则的协议；否则，将会致使规则无效。

要修改规则，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy > Rule Editor**。

系统将显示 Rule Editor 页面。

步骤 2　找到要修改的规则。您有以下选项：

- 要通过浏览规则类别查找规则，请浏览文件夹以找到所需的规则，然后点击该规则旁边的编辑图标 ( )。
- 要通过过滤页面上显示的规则来查找规则，请在规则列表左上方带有过滤器图标 ( ) 的文本框中输入一个规则过滤器。导航到所需的规则并点击该规则旁边的编辑图标 ( )。有关详细信息，请参阅第 23-97 页上的过滤 Rule Editor 页面上的规则。

规则编辑器将会打开，其中显示所选的规则。

请注意，如果您选择共享对象规则，规则编辑器将仅显示规则报头信息。在 Rule Editor 页面上，可以通过以数字 3 (GID) 开头的列表来识别共享对象规则，例如 3:1000004。

步骤 3　修改规则 （有关规则选项的详细信息，请参阅第 23-93 页上的编写新规则），然后点击 **Save As New**。

规则将保存到本地规则类别中。

提示　如果您想使用规则的本地修而不使用系统规则，可按照第 20-17 页上的设置规则状态中所述的步骤禁用系统，并且激活本地规则。

步骤 4　如第 4-10 页上的应用访问控制策略中所述将入侵策略作为访问控制策略的一部分进行应用来激活入侵规则，以使所做的更改生效。

向规则添加注释

许可证：保护

可以向任何入侵规则添加注释。这样做可以提供有关规则以及其识别出的漏洞或策略违规的额外上下文和信息。

要将注释添加到规则，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy > Rule Editor**。

系统将显示 Rule Editor 页面。

步骤 2　找到要添加注释的规则。您有以下选项：

- 要通过浏览规则类别查找规则，请浏览文件夹以找到所需的规则，然后点击该规则旁边的编辑图标 ( )。
- 要通过过滤页面上显示的规则来查找规则，请在规则列表左上方带有过滤器图标 ( ) 的文本框中输入一个规则过滤器。导航到所需的规则并点击该规则旁边的编辑图标 ( )。有关详细信息，请参阅第 23-97 页上的过滤 Rule Editor 页面上的规则。

系统将显示规则编辑器。

步骤 3　点击 **Rule Comment**。

系统将显示 Rule Comment 页面。

步骤 4　在文本框中输入注释，然后点击 **Add Comment**。

输入的注释将保存在注释文本框中。

删除自定义规则

许可证：保护

您可以删除当前未在入侵策略中启用的自定义规则。您不能删除思科提供的标准文本规则或共享对象规则规则。

系统将删除的规则存储在删除的类别中，您可以使用删除的规则作为新规则的依据。有关编辑规则的信息，请参阅第 23-95 页上的修改现有规则。

入侵策略中的 Rules 页面不显示删除的类别，因此您不能启用删除的自定义规则。

请注意，您还可以删除 Rule Updates 页面上的所有本地规则。有关示例，请参阅第 35-9 页上的使用一次性规则更新。

有关详细信息，请参阅以下各节：

- 有关创建自定义规则的信息，请参阅第 23-93 页上的编写新规则。
- 有关导入本地规则的信息，请参阅第 35-8 页上的导入规则更新和本地规则文件。
- 有关设置规则状态的信息，请参阅第 20-17 页上的设置规则状态。

要删除自定义规则，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy > Rule Editor**。

系统将显示 Rule Editor 页面。

步骤 2　您有两种选择：

- 点击 **Delete Local Rules**，然后点击 **OK**。

  入侵规则中当前未启用且对其的更改已保存的所有规则将从本地规则类别中删除，并移至删除的类别中。

- 浏览文件夹以找到本地规则类别；点击本地规则类别以展开它，然后点击要删除的规则旁边的删除图标 ( )。

  该规则从本地规则类别中删除，并移至删除的类别中。

  请注意，自定义标准文本规则的生成器 ID (GID) 为 1（例如，1:1000012），自定义共享对象规则的 GID 为 3（例如，3:1000005）。

提示　系统还会将您连同修改后的报头信息一起保存的共享对象规则存储在本地规则类别中，并以 3 作为 GID 将它们列出来。您可以删除您修改后的共享对象规则版本，但不能删除原始共享对象规则。

过滤 Rule Editor 页面上的规则

许可证：保护

您可以对 Rule Editor 页面中的规则进行过滤来显示其中一组规则。例如，如果想要修改某个规则或更改其状态，但是难以在成千上万个可用规则中找到该规则，这个过滤功能可能很有用。

当您输入过滤器时，页面将显示至少包含一条匹配规则或消息 （如果没有匹配规则）的文件夹。过滤器可以包含特殊关键字及其参数、字符串和用引号引起来的文字字符串，多个过滤器条件之间用空格隔开。过滤器不能包含正则表达式、通配符或任何特殊运算符，例如取反字符 (!)、大于号 (>) 和小于号 (<) 等。

所有关键字、关键字参数和字符串都不区分大小写。除关键字 `gid` 和 `sid` 之外，所有参数和字符串都被视为部分字符串。`gid` 和 `sid` 的参数只会返回完全匹配项。

或者，可以在未经过滤的原始页面上展开某个文件夹，如果后续过滤器返回该文件夹中的匹配项，该文件夹将会保持展开。这对于在包含大量规则的文件夹中搜索规则可能有用。

不能使用后续过滤器限制任何过滤器。输入的任何过滤器都会搜索整个规则数据库并返回所有匹配的规则。当您在页面仍显示上一过滤器的结果时输入过滤条件，页面将清空，转而返回新过滤器的结果。

您可以对已过滤或未过滤列表中的规则使用相同的功能。例如，您可以编辑 Rule Editor 页面上经过过滤或未经过滤的列表中的规则。

有关详细信息，请参阅以下各节：

- 第 23-98 页上的在规则过滤器中使用关键字
- 第 23-99 页上的在规则过滤器中使用字符串
- 第 23-99 页上的在规则过滤器中结合使用关键字和字符串
- 第 23-99 页上的过滤规则

在规则过滤器中使用关键字

许可证：保护

每个规则过滤器都可以包含一个或多个关键字，其格式如下：

keyword:*argument*

其中，*keyword* 是规则过滤器关键字表中的其中一个关键字，*argument* 是要在与该关键字相关的一个或多个指定字段中搜索的一个字母数字字符串，不区分大小写。

除 gid 和 sid 之外的所有关键字的参数都会被视为部分字符串。例如，参数 123 将返回 "12345"、"41235"、"45123" 等结果。gid 和 sid 的参数只会返回完全匹配项；例如，sid:3080 只会返回结果 SID 3080。

提示 使用一个或多个字符串来进行过滤可以搜索部分 SID。有关详细信息，请参阅第 23-99 页上的在规则过滤器中使用字符串。

下表介绍了可以用于过滤规则的特定过滤关键字和参数。

表 23-61　规则过滤器关键字

关键字	说明	示例
arachnids	根据规则引用中的完整或部分 Arachnids ID 返回一个或多个规则。有关详细信息，请参阅第 23-13 页上的定义事件参考。	arachnids:181
bugtraq	根据规则引用中的完整或部分 Bugtraq ID 返回一个或多个规则。有关详细信息，请参阅第 23-13 页上的定义事件参考。	bugtraq:2120
cve	根据规则引用中的完整或部分 CVE 编号返回一个或多个规则。有关详细信息，请参阅第 23-13 页上的定义事件参考。	cve:2003-0109
gid	参数 1 将返回标准文本规则。参数 3 将返回共享对象规则。有关详细信息，请参阅第 20-2 页上的表 20-1。	gid:3
mcafee	根据规则引用中的完整或部分 McAfee ID 返回一个或多个规则。有关详细信息，请参阅第 23-13 页上的定义事件参考。	mcafee:10566
msg	根据规则的完整或部分 Message 字段（又称为事件消息）返回一个或多个规则。有关详细信息，请参阅第 23-11 页上的定义事件消息。	msg:chat
nessus	根据规则引用中的完整或部分 Nessus ID 返回一个或多个规则。有关详细信息，请参阅第 23-13 页上的定义事件参考。	nessus:10737
ref	根据规则引用或规则 Message 字段中一个完整的字母数字字符串或其一部分返回一个或多个规则。有关详细信息，请参阅第 23-13 页上的定义事件参考和第 23-11 页上的定义事件消息。	ref:MS03-039
sid	返回带有完全匹配的 Signature ID 的规则。	sid:235
url	根据规则引用中的完整或部分 URL 返回一个或多个规则。有关详细信息，请参阅第 23-13 页上的定义事件参考。	url:faqs.org

在规则过滤器中使用字符串

许可证：保护

每个规则过滤器可以包含一个或多个字母数字字符串。字符串将搜索规则的 **Message** 字段、Signature ID 和 Generator ID。例如，字符串 `123` 会返回规则消息中的 `"Lotus123"`、`"123mania"` 等字符串，也会返回 SID 6123、 SID 12375 等。有关规则的 **Message** 字段的详细信息，请参阅第 23-11 页上的定义事件消息。

所有字符串都不区分大小写并被视为部分字符串。例如， `ADMIN`、 `admin` 或 `Admin` 等字符串中任意一个字符串都会返回 `"admin"`、 `"CFADMIN"`、 `"Administrator"` 等结果。

用引号将字符串引起来可以返回完全匹配项。例如，用引号引起来的原义字符串 `"overflow attempt"` 只会返回完全匹配的该字符串，而由 `overflow` 和 `attempt` 这两个字符串组成的未加引号的过滤器则会返回 `"overflow attempt"`、 `"overflow multipacket attempt"`、 `"overflow with evasion attempt"` 等结果。

在规则过滤器中结合使用关键字和字符串

许可证：保护

输入关键字、文字字符串或这二者的任意组合并以空格分隔可以缩小过滤结果的范围。结果包括符合所有过滤条件的任意规则。

可以按照任意顺序输入多个过滤条件。例如，以下每个过滤器返回的规则相同：

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

过滤规则

许可证：保护

可以对 Rule Editor 页面上的规则进行过滤以显示规则子集，以便更容易找到特定规则。然后，可以使用任何页面功能。

要过滤特定规则，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy > Rule Editor**。

系统将显示 Rule Editor 页面。

如果要查找要进行编辑的规则， Rule Editor 页面上的规则过滤功能可能特别有用。有关详细信息，请参阅第 23-95 页上的修改现有规则。

步骤 2　或者，从 Group Rules By 列表中选择其他分组方法。

提示　如果所有子组中的总规则数量很大，过滤所需的时间可能大大增加，因为规则显示在多个类别中，即使唯一规则的总数少很多也是如此。

步骤 3　或者，点击要展开的任何组旁边的文件夹。

文件夹将会展开以显示该组中的规则。请注意，一些规则组包含也可以展开的子组。

另请注意，如果您预期规则可能在某个组中，在未经过滤的原始页面上展开该组可能有用。如果后续过滤器返回该文件夹中的匹配项，当您点击过滤器清除图标 (✖) 返回到未经过滤的原始页面时，该组将会保持展开。

步骤 4　要激活过滤器文本框，请点击规则列表左上方的文本框中的过滤器图标 ( )。

步骤 5　键入过滤器限制条件并按 Enter。

过滤器可以包含关键字、变量和字符串（可以用引号引起来），多个条件之间用空格隔开。有关详细信息，请参阅第 23-97 页上的过滤 Rule Editor 页面上的规则。

页面将会刷新以显示至少包含一个匹配规则的任何组。

步骤 6　或者，打开尚未打开的文件夹以显示匹配规则。您有以下过滤选择：

- 要输入新的过滤器，请将光标放在过滤器文本框中，并点击以激活它；键入过滤器并按 Enter。
- 要清除当前已过滤列表并返回到原始未过滤页面，请点击过滤器清除图标 (✖)。

步骤 7　或者，对规则作出通常会在该页面上作出的任何更改。请参阅第 23-95 页上的修改现有规则。

要使所做的更改生效，请按照第 4-10 页上的应用访问控制策略中所述将入侵策略作为访问控制策略的一部分进行应用。

阻止恶意软件和禁止的文件

*恶意软件*可以通过多种途径进入企业网络。为了帮助您识别和减轻恶意软件的影响， ASA FirePOWER 模块的文件控制、和高级恶意软件防护组件可以检测、跟踪、存储、分析并 （可选）阻止恶意软件及其他类型的文件在网络流量中的传输。

您可以配置系统执行恶意软件防护和文件控制，将其作为整体访问控制配置的一部分。您创建并与访问控制规则关联的*文件策略*会处理与规则匹配的网络流量。

虽然您可以使用任何许可证创建文件策略，但是恶意软件防护和文件控制的某些方面要求在 ASA FirePOWER 模块上启用特定获许可功能，如下表所述。

表 24-1　　入侵和文件检查的许可证和设备要求

特性	说明	添加该许可证...
入侵预防	检测和（可选）阻止入侵和漏洞	保护
文件控制	检测和（可选）阻止文件类型传输	保护
高级恶意软件防护 (AMP)	检测、跟踪和 （可选）阻止恶意软件传输	恶意软件

有关详情，请参阅：

- 第 24-1 页上的了解恶意软件防护和文件控制
- 第 24-4 页上的了解和创建文件策略

了解恶意软件防护和文件控制

许可证：保护、恶意软件或任何

通过使用*高级恶意软件防护*功能，您可以将 ASA FirePOWER 模块配置为检测、跟踪、分析并选择性地阻止网络上传输的恶意软件文件。

系统可以检测并或者阻止多种类型的文件（包括 PDF、Microsoft Office 文档及其他）中的恶意软件。ASA FirePOWER 模块监控这些文件类型传输的基于应用协议的特定网络流量。当 ASA FirePOWER 模块检测到合格的文件时，ASA FirePOWER 模块使用文件的 SHA - 256 哈希值执行*恶意软件云查找*。根据这些结果，思科云将文件性质返回到ASA FirePOWER 模块。

如果文件在云中具有据您所知是不正确的处理，则可向文件列表中添加该文件的 SHA-256 值。

- 要好像云已为文件分配了安全性质一样对其进行处理，请将文件添加到*白名单*。
- 要好像云已为文件分配了恶意软件性质一样对其进行处理，请将文件添加到*自定义检测列表*。

如果系统在文件列表中检测到文件的 SHA-256 值，会采取适当措施而不执行恶意软件查找或检查文件性质。请注意，必须为文件策略中的某个规则配置 **Malware Cloud Lookup** 或 **Block Malware** 操作和匹配的文件类型，以计算文件的 SHA 值。可以按文件策略启用白名单或自定义检测列表。

要检查或阻止文件，您必须在 ASA FirePOWER 模块上启用保护许可证。要将文件添加到文件列表，您必须启用恶意软件许可证。

了解文件性质

系统根据思科云返回的性质来确定文件性质。由于向文件列表中进行添加或由于威胁评分，文件可具有思科云返回的以下文件性质之一：

- `Malware` 表明云将文件归类为恶意软件。
- `Clean` 表示云将文件归类为安全，或用户将文件添加到安全列表。
- `Unknown` 表示在云分配性质之前发生的恶意软件云查找。云尚未将文件分类。
- `Custom Detection` 表示用户将文件添加到自定义检测列表。
- `Unavailable` 表示ASA FirePOWER 模块无法执行恶意软件云查找。您可能看到小部分事件有此性质；这是预期行为。

提示 如果在很短时间内连续看到多个 `Unavailable` 恶意软件活动，请检查您的云连接和端口配置。有关详细信息，请参阅第 D-1 页上的安全、互联网接入和通信端口。

根据文件性质， ASA FirePOWER 模块文件或者止文件的上传或下载。为了提高性能，如果系统根据文件的 SHA-256 值已经知道文件的性质您的设备会使用缓存的性质而不是查询思科云。

请注意，文件性质可以更改。例如，云可以确定先前被视为安全的文件现在被识别为恶意软件，或者正好相反，以前被识别为恶意软件的文件实际上是安全的。如果上一周对其执行了恶意软件查找的文件的性质发生变化，云会通知 ASA FirePOWER 模块，因此系统在下次检测到该文件进行传输时可以采取适当措施。已更改的文件性质称为*追溯性*性质。

从恶意软件云查找返回的文件性质都具有生存时间 (TTL) 值。在 TTL 值中指定的持续时间内保持某种文件性质而无更新后，系统会清除缓存的信息。性质具有以下 TTL 值：

- Clean - 4 小时
- Unknown - 1 小时
- Malware - 1 小时

如果缓存的恶意软件云查找识别出已超时的缓存性质，系统会执行新查找以确定文件性质。

了解文件控制

如果贵组织不仅要阻止恶意软件文件的传输，还要阻止所有特定类型的文件的传输（无论文件是否包含恶意软件），则可通过*文件控制*功能来做到这一点。与恶意软件防护一样，ASA FirePOWER 模块也会监控特定文件类型传输的网络流量，然后阻止或允许文件。

系统可以检测恶意软件的所有文件类型以及许多其他文件类型都支持文件控制。这些文件类型分为三类：基本类别，包括多媒体（swf 和 mp3）；可执行文件（exe 和 torrent）；以及 PDF。请注意，与恶意软件防护不同，文件控制不需要思科云的查询。

配置恶意软件防护和文件控制

许可证：保护或恶意软件

通过将文件策略与访问控制规则相关联，可以将恶意软件防护和文件控制配置为整体访问控制配置的一部分。这种关联保证系统在传递流量中与访问控制规则的条件匹配的文件之前，首先检查该文件。

文件策略（例如父项访问控制策略）包含的规则用于确定系统如何处理与每个规则的条件相符的文件。可以配置单独的文件规则，以对不同的文件类型、应用协议或传输方向采取不同操作。

当文件与规则匹配时，规则可以：

- 根据简单文件类型匹配允许或阻止文件
- 根据恶意软件文件性质阻止文件
- 此外，文件策略还可以 根据白名单或自定义检测列表中的条目自动将文件视为安全文件或恶意软件

举一个简单的例子，您可以实施会阻止用户下载可执行文件的文件策略。有关文件策略以及将其与访问控制规则相关联的详细信息，请参阅第 24-4 页上的了解和创建文件策略。

根据恶意软件防护和文件控制记录事件

许可证：保护或恶意软件

ASA FirePOWER 模块将系统文件检查和处理的记录作为捕获文件、文件事件和恶意软件事件进行记录：

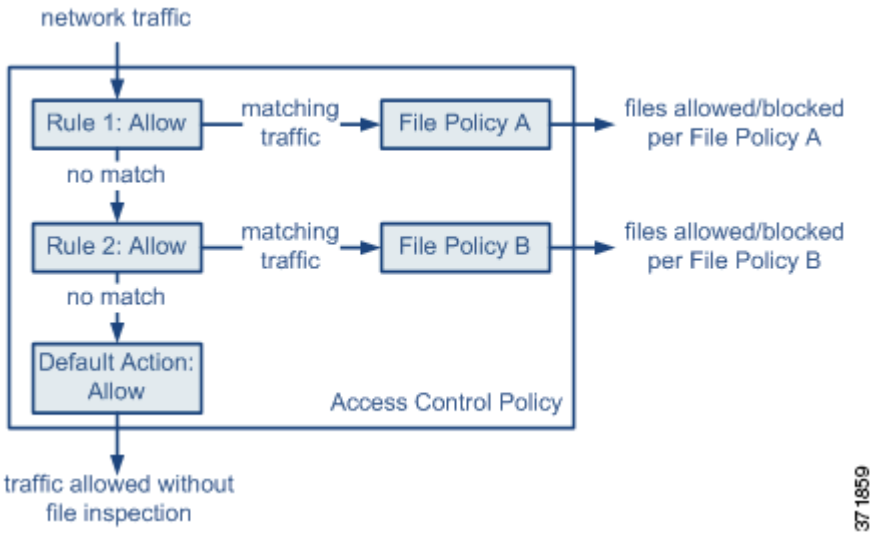
- *文件事件*表示系统在网络流量中检测到并或者被阻止的文件。
- *恶意软件事件*表示系统在网络流量中检测到并或者被阻止的恶意软件文件。
- *追溯性恶意软件事件*表示恶意软件文件的性质已更改的文件。

当系统根据对网络流量中恶意软件的检测或阻止情况生成恶意软件事件时，它还会生成文件事件，因为要在文件中检测恶意软件，系统必须先检测该文件本身。

了解和创建文件策略

许可证：保护或恶意软件

文件策略是作为整体访问控制配置的一部分供系统用于执行高级恶意软件防护和文件控制的一组配置。



策略有两个访问控制规则，两者都使用 Allow 操作并与文件策略关联。策略的默认操作也是允许流量，但不执行文件策略检查。在本示例中，流量处理如下：

- 与 `Rule 1` 匹配的流量根据 `File Policy A` 进行检查。
- 与 `Rule 1` 不匹配的流量根据 `Rule 2` 进行评估。与 `Rule 2` 匹配的流量根据 `File Policy B` 进行检查。
- 允许与任一规则不匹配的流量；不能将文件策略与默认操作关联。

文件策略（例如父项访问控制策略）包含的规则用于确定系统如何处理与每个规则的条件相符的文件。可以配置单独的文件规则，以对不同的文件类型、应用协议或传输方向采取不同操作。

文件与某个规则匹配后，规则可以：

- 根据简单文件类型匹配允许或阻止文件
- 根据恶意软件文件性质阻止文件
- 此外，文件策略还可以 根据白名单或自定义检测列表中的条目自动将文件视为安全文件或恶意软件

可以将单个文件策略与其操作为 **Allow**、**Interactive Block** 或 **Interactive Block with reset** 的访问控制规则关联。这样，系统将会使用该文件策略检查符合访问控制规则条件的网络流量。通过将不同文件策略与不同访问控制规则相关联，可以精细控制如何识别并阻止网络上传输的文件。但请注意，您**不能**使用文件策略检查由访问控制默认操作处理的流量。有关详细信息，请参阅第 10-2 页上的检测允许流量是否存在入侵和恶意软件。

文件规则

可使用文件规则来填充文件策略。下表介绍文件规则的组成部分。

表 24-2　　文件规则组件

文件规则组件	说明
应用协议	系统可以检测和检查通过 FTP、 HTTP、 SMTP、 IMAP、 POP3 和 NetBIOS-ssn (SMB) 传输的文件。为了提高性能，可以逐个文件规则将文件检测仅限于其中一种应用协议。
传输方向	对于已下载的文件，可以检查通过 FTP、 HTTP、 IMAP、 POP3 和 NetBIOS-ssn (SMB) 传入的流量；对于已上传的文件，可以检查通过 FTP、 HTTP、 SMTP 和 NetBIOS-ssn (SMB) 传出的流量。
文件类别和类型	系统检测各种类型的文件。这些文件类型分为三类：基本类别，包括多媒体（swf 和 mp3）；可执行文件（exe 和 torrent）；以及 PDF。可以配置用于检测个别文件类型或整个类别的文件类型的规则。 例如，可以阻止所有多媒体文件，或者仅阻止 ShockWave Flash (swf) 文件。或者，可以将系统配置为会在用户下载 BitTorrent (torrent) 文件时向您发出警报。 **注意事项**　频繁触发的文件规则可能会影响系统性能。例如，检测 HTTP 流量（例如 YouTube，用于传输重要的 Flash 内容）中的多媒体文件可能会产生可能生成数量巨大的事件。
文件规则操作	文件规则操作用于确定系统如何处理与规则条件相符的流量。 **注**　文件规则是以规则操作顺序而非数字顺序进行评估。有关详细信息，请参阅下一节，文件规则操作和评估顺序。

文件规则操作和评估顺序

每个文件规则都有用于确定系统如何处理与规则条件匹配的流量的关联操作。可以在文件策略中设置单独的规则，以对不同的文件类型、应用协议或传输方向采取不同操作。规则操作如下 （按规则操作顺序列出）：

- *Block Files* 规则允许阻止特定文件类型。
- *Block Malware* 规则允许计算特定文件类型的 SHA-256 哈希值，然后使用云查找过程先确定通过网络传输的文件是否包含恶意软件，再阻止表示威胁的文件。
- *Malware Cloud Lookup* 规则允许根据云查找记录通过网络传输的恶意软件性质的文件，同时仍允许其传输。
- *Detect Files* 规则可供您将特定文件类型的检测记录，同时仍允许其传输。

对于每次文件规则操作，您可以配置选项在阻止文件传输时重置连接并将已捕获的文件存储到 ASA FirePOWER 模块。下表详细说明可用于每次文件操作的选项。

表 24-3　　文件规则操作

操作	重置连接？
Block Files	是（推荐）
Block Malware	是（推荐）
Detect Files	no
Malware Cloud Lookup	no

文件和恶意软件检测、捕获以及阻止附注与限制

请注意有关文件和恶意软件检测、捕获以及阻止行为的以下详细信息和限制：

- 在会话中检测到并阻止文件之前，会话中的数据包可能受到入侵检查。
- 无论使用何种传输协议，如果未检测到文件的文件结尾标记，**Block Malware** 规则或自定义检测列表不会阻止该文件。系统会等待接收整个文件后再阻止文件（如文件结尾标记所指示），并在检测到该标记后阻止文件。
- 如果 FTP 文件传输的文件结尾标记单独从最后一个数据段进行传输，则会阻止该标记，并且 FTP 客户端会指明文件传输已失败，但是文件实际上会完整传输到磁盘。
- FTP 通过不同信道传输命令和数据。在被动中， FTP 数据会话及其控制会话中的流量可能不会被负载均衡到同一个 Snort。
- 如果文件与带有应用协议条件的规则相匹配，在系统成功确定该文件的应用协议之后，会生成文件事件。无法识别的文件不生成文件事件。
- 对于使用适合于 FTP 的具有 **Block Malware** 规则的访问控制策略，如果将默认操作设置为已禁用 **Drop when Inline** 的入侵策略，则系统会为检测到的与规则匹配的文件或恶意软件生成事件，但不丢弃文件。要阻止 FTP 文件传输并使用入侵策略作为在其中选择文件策略的访问控制策略的默认操作，必须选择已启用 **Drop when Inline** 的入侵策略。
- 具有 **Block Files** 和 **Block Malware** 操作的文件规则会阻止通过 HTTP 自动恢复文件下载，方法是在进行初始文件传输尝试后检测到相同的文件、URL、服务器和客户端应用达到 24 小时的情况下阻止新会话。
- 在极少数情况下，如果来自 HTTP 上传会话的流量有故障，则系统无法正确重组流量，并因此不会阻止该会话或生成文件事件。
- 如果通过 NetBios-ssn 传输使用 **Block Files** 规则阻止的文件（例如 SMB 文件传输），则目标主机上可能会显示文件。但是，该文件不可用，原因是在下载启动后阻止了该文件，导致文件传输未完成。
- 如果创建文件规则以检测或阻止通过 NetBios-ssn 传输的文件（例如 SMB 文件传输），则系统不检查在应用调用文件策略的访问控制策略前启动的已建立的 TCP 或 SMB 会话中传输的文件，因此不会检测或阻止这些文件。
- 配置为在被动部署中阻止文件的规则不会阻止匹配的文件。由于连接继续传输文件，因此如果配置规则以记录连接的开始，则您可能会看到为此连接记录的多个事件。
- 如果 POP3、POP、SMTP 或 IMAP 会话中文件的所有文件名的总字节数超过 1024，则会话中的文件事件可能无法反映文件名缓冲区填充后检测到的文件的正确文件名。
- 当通过 SMTP 传输基于文本的文件时，某些邮件客户端会将换行符转换为 CRLF 换行符标准。由于基于 MAC 的主机使用回车 (CR) 字符，并且基于 Unix/Linux 的主机使用换行 (LF) 字符，因此，邮件客户端进行的换行可能修改文件的大小。注意某些邮件客户端在处理无法识别的文件类型时默认进行换行。
- 思科建议启用 **Reset Connection**（适用于 **Block Files** 和 **Block Malware** 操作）以防止受阻应用会话保持打开，直到 TCP 连接重置为止。如果不重置连接，则客户端会话仍保持打开，直到 TCP 连接自我重置为止。
- 如果文件规则配置有 **Malware Cloud Lookup** 或 **Block Malware** 操作，并且ASA FirePOWER 模块无法与云建立连接，则系统无法执行任何已配置的规则操作选项，直到恢复云连接为止。

文件规则评估示例

与访问控制策略中不同（规则按数字顺序进行评估），文件策略如第 24-5 页上的文件规则操作和评估顺序中所述处理文件。也就是说，简单阻止优先于恶意软件检测和阻止，后者优先于简单检测和日志记录。例如，可考虑使用在单个文件策略中处理 PDF 文件的四种规则。无论这些规则在模块界面中的显示顺序如何，它们都按以下顺序进行评估：

表 24-4　文件规则评估顺序示例

应用 协议	方向	操作	操作选项	结果
SMTP	上传	Block Files	重置连接	阻止用户通过邮件发送 PDF 文件并重置连接。
FTP	下载	Block Malware	重置连接	阻止通过文件传输下载恶意软件 PDF 文件，并重置连接。
POP3 IMAP	下载	Malware Cloud Lookup		检查通过邮件收到的 PDF 文件是否含有恶意软件。
任何环境	任何环境	Detect Files	无	检测和记录，但是当用户在网络上（即，通过 HTTP）查看 PDF 文件时允许流量。

ASA FirePOWER 模块使用警告图标 ( ) 来指出有冲突的文件规则。

请注意，不能对系统检测到的所有文件类型都执行恶意软件分析。从 **Application Protocol**、**Direction of Transfer** 和 **Action** 下拉列表中选择值之后，系统会对文件类型的列表进行约束。

记录文件事件、恶意软件事件和警报

将文件策略与访问控制规则关联时，系统自动为匹配的流量启用文件和恶意软件事件日志记录。系统在检查文件时，可以生成以下类型的事件：

- *文件事件*，表示检测到的文件或受阻文件，以及检测到的恶意软件文件
- *恶意软件事件*，表示检测到的恶意软件文件
- *追溯性恶意软件事件*，在先前检测到的文件的 Malware 文件性质发生变化时生成

在文件策略生成文件事件或恶意软件事件或者捕获文件时，无论调用访问控制规则的日志记录配置如何，系统都会自动将关联的连接端记录。

注　检查 NetBIOS-ssn (SMB) 流量所生成的文件事件不会立即生成连接事件，因为客户端和服务器构建一个持久连接。系统在客户端或服务器结束会话之后生成连接事件。

对于每个这些连接事件：

- **File** 字段包含表示连接中检测到的文件（包括恶意软件文件）的数量的图标 ( )；点击该图标会显示这些文件的列表，并且对于恶意软件文件还会显示其文件性质。
- **Reason** 字段表示记录连接事件的原因，具体取决于文件规则操作：
  - `File Monitor` （适用于 Detect Files 和 Malware Cloud Lookup 文件规则以及白名单中的文件）
  - `File Block` （适用于 Block Files 或 Block Malware 文件规则）
  - `File Custom Detection` （如果系统在自定义检测列表中遇到文件）
  - `File Resume Allow`（如果 Block Files 或 Block Malware 文件规则最初阻止文件传输）。应用允许文件的新访问控制策略后，会自动恢复 HTTP 会话。
  - `File Resume Block`（如果 Detect Files 或 Malware Cloud Lookup 文件规则最初允许文件传输）。应用阻止文件的新访问控制策略后，会自动停止 HTTP 会话。
- 对于已阻止文件或恶意软件的连接，**Action** 为 `Block`。

与 ASA FirePOWER 模块生成的任何类型的事件相同，您可以查看、和分析文件事件及恶意软件事件。您还可以使用恶意软件事件来，或者通过SNMP 系统日志向自己发出警报。

互联网访问

系统使用端口 443 对基于网络的 AMP 执行恶意软件云查找。必须在ASA FirePOWER 模块上打开该端口 （出站）。

管理文件策略

可以在 File Policies 页面 (**Policies > Files**) 上创建、编辑、修改和比较文件策略，该页面显示现有文件策略的列表及其上次修改日期。

点击文件策略的应用图标 ( ) 会显示一个对话框，该对话框指示哪些访问控制策略使用该文件策略，然后将您重定向到 Access Control Policy 页面。之所以出现此操作，是因为文件策略被视为其父访问控制策略的一部分，从而令您无法独立应用文件策略。要使用新文件策略，或者应用对现有文件策略进行的更改，必须应用或重新应用父访问控制策略。

请注意，删除已保存或已应用的访问控制策略中使用的文件策略。

有关管理文件策略的详细信息，请参阅：

- 第 24-8 页上的创建文件策略
- 第 24-9 页上的使用文件规则
- 第 24-11 页上的比较两个文件策略

创建文件策略

许可证：保护或恶意软件

创建文件策略并使用规则对其进行填充后，即可在访问控制策略中使用该文件策略。

提示　要复制现有文件策略，请点击复制图标 ( )，然后在出现的对话框中为新策略键入唯一名称。然后就可以修改副本。

要创建文件策略，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Files**。

系统将显示 File Policies 页面。

步骤 2　点击 **New File Policy**。

随即出现 File Policies 对话框。

对于新策略，模块界面会指明该策略未在使用。如在编辑使用中的文件策略，则模块界面会告知您使用该文件策略的访问控制策略的数量。在这两种情况下，都可以点击文本以跳至 Access Control Policies 页面；请参阅第 4-1 页上的开始使用访问控制策略。

步骤 3　在 **Name** 和 **Description** （可选）字段中为新策略输入名称和描述，然后点击 **Save**。

系统将显示 File Policy Rules 选项卡。

步骤 4　向文件策略添加一个或多个规则。

借助文件规则，可以精细控制要对其记录、阻止或扫描恶意软件的文件类型。有关添加文件规则的信息，请参阅第 24-9 页上的使用文件规则。

步骤 5　配置高级选项。有关详细信息，请参阅第 24-10 页上的配置高级文件策略常规选项。

步骤 6　点击 **Store ASA FirePOWER Changes**。

要使用新策略，必须向访问控制规则添加文件策略，然后应用该访问控制策略。如果编辑的是现有文件策略，必须重新应用任何使用该文件策略的访问控制策略。

使用文件规则

许可证：保护或恶意软件

文件策略必须包含一个或多个规则才能生效。可以在 File Policy Rules 页面上创建、编辑和删除规则，该页面在您创建新文件策略或编辑现有策略时出现。该页面列出策略中的所有规则以及每个规则的基本特征。

该页面还提供有关使用此文件策略的访问控制策略数量的通知。可以点击通知以显示父策略的列表，并或者转至 Access Control Policies 页面。

要创建文件规则，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Files**。

系统将显示 File Policies 页面。

步骤 2　您有以下选项：

- 要向新策略添加规则，请点击 **New File Policy** 创建新策略；请参阅第 24-8 页上的创建文件策略。
- 要向现有策略添加规则，请点击策略旁边的编辑图标 ( )。

步骤 3　在显示的 File Policy Rules 页面上，点击 **Add File Rule**。

系统将显示 Add File Rule 对话框。

步骤 4　从下拉列表中选择一个**应用协议**。

Any（默认值）检测 HTTP、 SMTP、 IMAP、 POP3、 FTP 和 NetBIOS-ssn (SMB) 流量中的文件。

步骤 5　从下拉列表中选择一个**传输方向**。

可以为下载的文件检查以下类型的传入流量：

- HTTP
- IMAP
- POP3
- FTP
- NetBIOS-ssn (SMB)

可以为上传的文件检查以下类型的传出流量：

- HTTP
- FTP
- SMTP
- NetBIOS-ssn (SMB)

无论用户是发送还是接收，使用 **Any** 都可通过多种应用协议检测文件。

步骤 6　选择文件规则 **Action**。有关详细信息，请参阅文件规则操作表。

选择 **Block Files** 或 **Block Malware** 时，**Reset Connection** 已默认启用。要在传输已阻止的文件时不重置连接，请清除 **Reset Connection** 复选框。

注　思科建议保持启用 **Reset Connection**，以防止受阻应用会话保持打开，直到 TCP 连接重置为止。

有关文件规则操作的详细信息，请参阅第 24-5 页上的文件规则操作和评估顺序。

步骤 7　选择一个或多个**文件类型**。使用 Shift 和 Ctrl 键以选择多个文件类型。可以通过以下方式过滤文件类型列表：

- 选择一个或多个**文件类型类别**。
- 按名称或描述搜索文件类型。例如，在 **Search name and description** 字段中键入 `Windows` 将会显示 Microsoft Windows 专用文件的列表。

可以在文件规则中使用的文件类型取决于您对 **Application Protocol**、**Direction of Transfer** 和 **Action** 所做的选择。

例如，为 **Direction of Transfer** 选择 **Download** 会删除 `GIF`、 `PNG`、 `JPEG`、 `TIFF` 和 `ICO` （从 **Graphics** 类别中）以防止文件事件过量。

步骤 8　将所选文件类型添加到 **Selected Files Categories and Types** 列表：

- 点击 **Add** 以将所选文件类型添加到规则。
- 将一个或多个文件类型拖放到 **Selected Files Categories and Types** 列表中。
- 在选定类别的情况下，点击 **All types in selected Categories**，然后点击 **Add** 或将该选择拖放到 **Selected Files Categories and Types** 列表。

步骤 9　点击 **Store ASA FirePOWER Changes**。

文件规则即被添加到策略。如果编辑的是现有文件策略，必须重新应用任何使用该文件策略的访问控制策略，所做的更改才能生效。

配置高级文件策略常规选项

许可证：恶意软件

在文件策略中，可以在 General 部分中设置以下高级选项。

表 24-5　高级文件策略常规选项

字段	说明	默认值
Enable Custom Detection List	选择此字段可在检测到自定义检测列表时阻止其中的文件。	enabled
Enable Clean List	选择此字段可在检测到白名单时允许其中的文件。	enabled

要配置高级文件策略常规选项，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Files**。

系统将显示 File Policies 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

系统将显示 File Policy Rule 页面。

步骤 3　选择 **Advanced** 选项卡。

系统将显示 Advanced 选项卡。

步骤 4　改选项，如高级文件策略常规选项表中所述。

步骤 5　点击 **Store ASA FirePOWER Changes**。

您必须重新应用任何使用已编辑的文件策略的访问控制策略。

比较两个文件策略

许可证：保护

要查看策略更改是否符合贵组织的标准或者要优化系统性能，您可以检查任意两个文件策略之间的差异或同一策略的两个修订版本。

文件策略*比较视图*并排显示两个文件策略或修订版本，其中上次修改时间和上次修改的用户显示在每个策略名称旁边。两个策略之间的差异将会突出显示：

- 蓝色指示突出显示的设置在两个策略中不同，不同之处以红色文本标注。
- 绿色指示突出显示的设置在一个策略中存在，但在另一个策略中不存在。

可以通过点击 **Previous** 和 **Next** 浏览差异。在左右两侧之间以双箭头图标 ( ) 为中心移动，**Difference** 数字调整为识别您正在查看哪个差异。或者，您可以生成文件策略*比较报告*，它是比较视图的 PDF 版本。

要比较两个文件策略，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Files**。

系统将显示 File Policies 页面。

步骤 2　点击 **Compare Policies**。

系统将显示 Select Comparison 对话框。

步骤 3　从 **Compare Against** 下拉列表中选择要进行比较的类型：

- 要比较两个不同策略，请选择 **Running Configuration** 或 **Other Policy**。两个选项之间的实际区别是，如果选择 **Running Configuration**，则系统会将您的比较选项之一限制为当前应用的文件策略集。
- 要比较同一策略的修订版本，请选择 **Other Revision**。

对话框将会刷新，显示比较选项。

步骤 4　根据您选择的比较类型，有以下选项可供选择：

- 如果比较的是两个不同策略，请选择您要比较的策略：**Policy A** 或 **Target/Running Configuration A** 和 **Policy B**。
- 如果比较的是同一策略的修订版本，请选择要使用的 **Policy**，然后选择两个修订版本：**Revision A** 和 **Revision B**。修订版本按日期和用户名进行列出。

步骤 5　点击 **OK**。

系统将显示比较视图。

或者，点击 **Comparison Report** 以生成文件策略比较报告。系统会提示您将报告保存到您的计算机上。

记录网络流量中的连接

当设备监控网络主机产生的流量时，它们可以生成其检测到的连接的记录。访问控制策略中的各种设置可供您精细地控制自己所记录的连接、连接记录时间以及数据存储位置。访问控制规则的特定日志记录配置还可以确定，您是否记录与该连接相关联的文件和恶意软件事件。

在大多数情况下，您可以在连接开始和终止时记录连接。当您记录连接时，系统会生成*连接事件*。无论何时基于的安全情报功能阻止连接或将其列入黑名单，您均可记录一种特殊类型的连接事件，称为*安全情报事件*。

连接事件包含关于检测到的会话的数据。

您应该根据贵组织的安全和合规性需求记录连接。

有关记录连接数据的详细信息，请参阅：

- 第 25-1 页上的决定要记录的连接
- 第 25-7 页上的记录安全情报（列入黑名单）决策
- 第 25-8 页上的根据访问控制处理记录连接
- 第 25-11 页上的记录在连接中检测到的 URL

决定要记录的连接

许可证：任何

通过使用访问控制策略中的各种设置，您可以记录您的 ASA FirePOWER 模块监控的任何的连接。在大多数情况下，您可以在连接开始和终止时记录连接。然而，由于被阻止的流量会不经进一步检测而遭直接拒绝，因此系统只能记录被阻止流量或列入黑名单流量的连接开始事件；而没有不同的连接终止事件可记录。

记录连接事件后，您可以在事件查看器中查看该事件。您还可以将连接数据发送至外部系统日志或 SNMP 陷阱服务器。

提示 要使用 ASA FirePOWER 模块对连接数据进行详细分析，思科建议您将关键连接的终止记录。

有关详细信息，请参阅：

- 第 25-2 页上的记录关键连接
- 第 25-3 页上的记录连接的开始和终止
- 第 25-4 页上的将连接记录至 ASA FirePOWER 模块或外部服务器

记录关键连接

许可证：任何

您应该根据贵组织的安全和合规性需求记录连接。如果您的目标是限制所生成事件的数量和提高性能，则只能启用对分析至关重要的连接的日志记录。然而，如果出于分析目的，您想要广泛了解网络流量，则可启用其他连接的日志记录。访问控制策略中的各种设置可供您精细地控制自己所记录的连接、连接记录时间以及数据存储位置。

注意事项　在拒绝服务 (DoS) 攻击期间，记录被阻止的 TCP 连接会多个类似事件会让系统不堪重负。在对阻止规则启用日志记录之前，请考虑该规则是监控面向互联网的接口上的流量，还是监控易遭受 DoS 攻击的其他接口上的流量。

除了您可以配置的日志记录，系统还会自动记录在其中检测到被阻止的文件、恶意软件或入侵尝试的大多数连接。系统均将这些连接终止事件，以供进一步分析。所有连接事件都会通过 Action 和 Reason

安全情报列入黑名单决策 （可选）

只要基于信誉的安全情报功能阻止连接或将其接列入黑名单，您就可以对该连接进行记录。或者，您可以像被动部署中建议的那样，使用仅监控设置进行安全情报过滤。这使得系统可以进一步分析本应列入黑名单的连接，并仍将匹配项记录至黑名单。

当您启用安全情报日志记录时，黑名单匹配项会生成安全情报事件以及连接事件。安全情报事件是您可以单独查看和分析的一类特殊连接事件，而且可以单独存储和删除。有关详细信息，请参阅第 25-7 页上的记录安全情报（列入黑名单）决策。

访问控制处理（可选）

您可以在访问控制规则或访问控制默认操作处理连接时记录该连接。您可以按每条访问控制规则配置此日志记录功能，以便仅记录关键连接。有关详细信息，请参阅第 25-8 页上的根据访问控制处理记录连接。

与入侵关联的连接（自动）

访问控制规则调用的入侵策略（请参阅第 6-1 页上的使用访问控制规则调整流量）检测到入侵并生成入侵事件时，系统会将发生入侵连接终止自动记录，而无论该规则的日志记录配置如何。

然而，与访问控制默认操作（请参阅第 4-4 页上的为网络流量设置默认的处理和检查）关联的入侵策略生成入侵事件时，系统**不会**自动记录关联连接的终止。相反，您必须明确启用默认操作连接日志记录。对于不想记录任何连接数据的仅入侵防御部署，这十分有用。

对于入侵受阻的连接，连接记录中的连接操作为 `Block`，原因为 `Intrusion Block`，即使执行入侵检测，也必须使用“允许”规则。

与文件和恶意软件事件关联的连接（自动）

访问控制规则调用的文件策略检测到受禁文件 （包括恶意软件）并生成文件或恶意软件事件时，系统会将检测到文件的连接终止自动记录，而无论该访问控制规则的日志记录配置如何。您**不能**禁用此日志记录。

注　检测 NetBIOS-ssn (SMB) 流量所生成的文件事件不会立即生成连接事件，因为客户端和服务器构建一个持久连接。系统在客户端或服务器终止会话之后生成连接事件。

对于文件受阻的连接，连接记录中的连接操作为 `Block`，即便要执行文件和恶意软件检测，也必须使用“允许”规则。连接原因是 `File Monitor`（检测到文件类型或恶意软件）或者是 `Malware Block` 或 `File Block`（文件受阻）。

记录连接的开始和终止

许可证：任何

当系统检测到连接时，在大多数情况下，您可以在其开始和终止时对其进行记录。

然而，因为受阻流量会被立即拒绝，无需进一步检测，在大多数情况下，您只能记录已阻止或列入黑名单的流量的连接开始事件；没有要记录的唯一连接终止。

注　对于单个未被阻止的连接，连接终止事件包含连接开始事件中的所有信息，以及在会话期间收集到的信息。

请注意，出于任何原因监控连接均会强制执行连接终止日志记录；请参阅第 25-4 页上的了解受监控连接的日志记录。

下表详细列出了连接开始和连接终止事件之间的差异，包括相比于记录每种事件的优势。

表 25-1　比较连接开始和终止事件

	连接开始事件	**连接终止事件**
生成时间...	当系统检测到连接开始（或者在头几个数据包之后，如果事件生成取决于应用或 URL 识别）	当系统： • 检测到连接关闭 • 在一段时间以后未检测到连接终止 • 由于内存限制，再也不能跟踪会话
记录对象...	安全情报或访问控制规则评估的所有连接	所有连接都是可配置的，尽管系统无法记录已受阻或列入黑名单的连接的终止
包含...	仅在第一个数据包中可以确定的信息（或者头几个数据包，如果事件生成取决于应用或 URL 识别）	连接开始事件中的所有信息，以及在会话期间通过检测流量确定的信息，例如，传输的总数据量或者连接中最后一个数据包的时间戳
十分有用...	如果您想要记录： • 受阻连接，包括安全情报列入黑名单决策	如果您想要： • 对会话期间收集的信息执行任何类型的详细分析 • 以图形格式查看连接数据

将连接记录至 ASA FirePOWER 模块或外部服务器

许可证：任何

您可以将连接事件记录至 ASA FirePOWER 模块以及外部系统日志或 SNMP 陷阱服务器。要将连接数据记录到外部服务器，必须先配置称为*警报响应*的外部服务器连接；请参阅第 27-2 页上的使用警报响应。

了解访问控制规则操作如何影响日志记录

许可证：因功能而异

每一条访问控制规则都有一个*操作*，该操作不仅可以确定系统如何检测和处理与该规则匹配的流量，而且可以确定您何时和如何记录关于匹配流量的详细信息。

有关详细信息，请参阅：

- 第 6-6 页上的使用规则操作确定流量处理和检测
- 第 25-4 页上的了解受监控连接的日志记录
- 第 25-5 页上的了解受信任连接的日志记录
- 第 25-5 页上的了解受阻和交互式受阻连接的记录
- 第 25-5 页上的了解允许连接的日志记录
- 第 25-6 页上的为允许的连接禁用文件和恶意软件事件日志记录

了解受监控连接的日志记录

许可证：因功能而异

系统始终会将后续连接的终止记录至 ASA FirePOWER 模块，而无论稍后处理该连接的规则或默认操作的日志记录配置如何：

- 与设定为监控的安全情报黑名单匹配的连接
- 与访问控制监控规则匹配的连接

换句话说，如果数据包匹配监控规则或安全情报监控的黑名单，即使该数据包不与其他规则匹配且您不对默认操作启用日志记录，系统也会始终记录该连接。每当系统由于安全情报过滤而记录连接事件时，它也会记录匹配的安全情报事件，这是一种您可以单独查看和分析的特殊类型连接事件；请参阅第 25-7 页上的记录安全情报（列入黑名单）决策。

由于受监控流量稍后始终会由另一规则或默认操作进行处理，因此，如果某个连接是因监控规则而被记录的，那么与其关联的操作就绝不可能是监控。相反，它会反映稍后处理该连接的规则关联操作或默认操作。

每次只有一个连接与 访问控制监控规则匹配时，系统均**不会**生成单独的事件。由于一个连接可能与多条监控规则相匹配，因此记录到 ASA FirePOWER 模块的每个连接事件均可能包含和显示关于该连接所匹配的前八条监控访问控制规则。

同样，如果您将连接事件发送至外部系统日志或 SNMP 陷阱服务器，则每当单一连接与监控规则相匹配时，系统均不会发送单独的警报。相反，系统在连接终止时发送的警报包含有关连接匹配的监控规则的信息。

了解受信任连接的日志记录

许可证：因功能而异

受信任连接是由信任访问控制规则或访问控制策略中的默认操作所处理的连接。您可以记录这些连接的开始和终止；然而，请记住，系统不会检测受信任连接是否存在入侵或受禁文件和恶意软件。因此，受信任连接的连接事件包含的信息有限。

了解受阻和交互式受阻连接的记录

许可证：因功能而异

对于阻止流量的访问控制规则和访问控制策略默认操作（包括交互式阻止规则），系统均会记录连接**开始**事件。匹配流量会被拒绝，无需进一步检测。

对于访问控制规则阻止的会话的连接事件，其操作为 `Block` 或 `Block with reset`。

在用户浏览到禁止访问的网站会令系统显示警告页面的交互式阻止访问控制规则，功能来记录连接终止事件。这是因为，如果用户点击浏览警告页面，该连接会被视为系统可以监控和记录并且允许访问的新连接；请参阅第 25-5 页上的了解允许连接的日志记录。

因此，对于与交互式阻止或包含重置规则的交互式阻止相匹配的数据包，系统可以生成以下连接事件：

- 用户的请求最初被阻止且显示警告页面时的连接开始事件；该事件的关联操作为 `Interactive Block` 或 `Interactive Block with reset`
- 当用户点击警告页面并加载最初请求的页面时生成的多个连接开始或连接终止事件；这些事件的关联操作为 `Allow`，原因为 `User Bypass`

请注意，只有内联部署的设备才能阻止流量。因为受阻连接在被动部署中实际上未被阻止，所以，系统可能会报告每条受阻连接的多个连接开始事件。

注意事项　在拒绝服务 (DoS) 攻击期间，记录被阻止的 TCP 连接会多个类似事件会让系统不堪重负。在对阻止规则启用日志记录之前，请考虑该规则是监控面向互联网的接口上的流量，还是监控易遭受 DoS 攻击的其他接口上的流量。

了解允许连接的日志记录

许可证：因功能而异

允许”访问控制规则允许匹配流量传递至下一阶段的检测和流量处理。

当您通过访问控制规则允许流量时，可以使用关联的入侵或文件策略（或同时使用两种策略），在流量到达其最终目标前，进一步检测流量并阻止入侵、禁止文件和恶意软件。

将按以下方式记录与“允许”访问控制规则匹配的流量的连接：

- 访问控制规则调用的入侵策略检测到入侵并生成入侵事件时，系统会将发生入侵连接终止自动记录至 ASA FirePOWER 模块，无论该规则的日志记录配置如何。
- 访问控制规则调用的文件策略检测到受禁文件（包括恶意软件）并生成文件或恶意软件事件时，系统会将检测到文件的连接终止自动记录至 ASA FirePOWER 模块，而无论该访问控制规则的日志记录配置如何。
- 或者，对于所有允许的流量，包括系统视作安全的流量或您未使用入侵或文件策略检测的流量，您可以启用连接开始和连接终止日志记录。

对于所有产生的连接事件， Action 和 Reason 字段均会反映事件记录原因。请注意：

- `Allow` 操作代表到达了最终目标，并且明确允许和用户绕过了交互式阻止的连接。
- `Block` 操作代表首先被访问控制规则允许，但在其中检测到入侵、受禁文件或恶意软件的连接。

为允许的连接禁用文件和恶意软件事件日志记录

许可证：保护或恶意软件

当您通过访问控制规则允许流量时，可以使用关联的文件策略检测传输的文件，在其可以到达其目标前，阻止受禁文件和恶意软件；请参阅第 10-5 页上的调整入侵防御性能。

当系统检测到受禁文件时，它会将以下事件类型之一自动记录至 ASA FirePOWER 模块：

- *文件事件*，代表检测到或阻止的文件，包括恶意软件文件
- *恶意软件事件*，仅代表检测到或阻止的恶意软件文件
- *可追溯的恶意软件事件*，其在之前检测到的文件的恶意软件性质变更时生成

如果您不希望记录文件或恶意软件事件，可以通过清除访问控制规则编辑器的 Logging 选项卡上的 **Log Files** 复选框，来针对每条访问控制规则禁用此日志记录。

注　思科建议您保持启用文件和恶意软件日志记录。

无论您是否保存文件和恶意软件事件，当网络流量违反文件策略时，系统均会自动将关联连接的终止记录至 ASA FirePOWER 模块，而无论调用访问控制规则的日志记录配置如何；请参阅第 25-2 页上的与文件和恶意软件事件关联的连接（自动）。

连接记和型号要求

许可证：因功能而异

因为您在访问控制策略中配置了连接日志记录，所以，您可以记录这些策略能够成功处理的任何连接。

虽然不管 ASA FirePOWER 模块上的许可证如何您均可创建访问控制策略，但访问控制的某些方面要求您先在上启用特定许可功能，然后才可能应用该策略。

下表说明了您必须拥有的许可证，以便能成功配置访问控制，从而记录访问控制策略处理的连接。

表 25-2　访问控制连接记录的许可证和型号要求

要记录连接…	许可证
对于使用网络、端口或文本 URL 条件处理的流量	任何
对于使用地理位置数据处理的流量	任何
关联于： • 信誉不良的 IP 地址（安全情报过滤） • 入侵或受禁文件	保护
恶意软件关联	恶意软件

表 25-2　访问控制连接记录的许可证和型号要求 （续）

要记录连接…	许可证
对于用户控制或应用控制处理的流量	可控性
对于系统使用 URL 类别和信誉数据进行过滤的流量，为受监控主机请求的 URL 显示 URL 类别和 URL 信誉信息	URL 过滤

记录安全情报 （列入黑名单）决策

许可证：保护

作为抵御恶意互联网内容的第一道防线，ASA FirePOWER 模块包含安全情报功能，该功能可供您根据最新信誉情报立即将连接列入黑名单（加以阻止），再也无需资源更密集的深入分析 。但是它会在基于策略的任何其他检测、分析或流量处理**之前**进行。

或者，您可以像被动部署中建议的那样，使用仅监控设置进行安全情报过滤。这使得系统可以进一步分析本应列入黑名单的连接，并仍将匹配项记录至黑名单。

启用安全情报日志记录将会记录访问控制策略处理的所有受阻和受监控的连接。然而，系统不会记录白名单匹配项；列入白名单的连接的记录取决于其最终的性质。

当系统由于安全情报过滤而记录连接事件时，它也会记录匹配的安全情报事件，这是一种您可以单独查看和分析的特殊类型连接事件。两种类型的事件均使用 **Action** 和 **Reason** 字段来反映黑名单匹配项。此外，您因此可以确定连接中列入黑名单的 IP 地址，列入黑名单和受监控的 IP 地址旁的主机图标在事件查看器中看上去稍有不同。

记录受阻且列入黑名单的连接

对于被阻止的连接，系统会记录连接开始安全情报和连接事件。因为列入黑名单的流量会被立即拒绝，无需进一步检测，所以，没有要记录的唯一连接终止。对于这些事件，操作为 `Block`，原因为 `IP Block`。

`IP 阻止`连接事件的每个唯一的发起方-响应方对都有 15 秒的阈值。换言之，一旦系统生成了其阻止连接的事件，在接下来的 15 秒内，无论端口或协议如何，对于这两个主机之间的额外的已阻止连接，系统不会生成另一连接事件。

记录受监控且列入黑名单的连接

对于安全情报功能监控而不是阻止的连接，系统会将连接终止安全情报和连接事件记录至 ASA FirePOWER 模块。无论访问控制规则或者访问控制默认操作稍后如何处理该连接，该记录都会发生。

对于这些连接事件，操作取决于连接的最终性质。**Reason** 字段包含 `IP 监控`以及连接可能已被记录的任何其他原因。

请注意，对于受监控的连接，系统还可能会生成连接开始事件，具体取决于稍后处理该连接的访问控制规则或默认操作中的日志记录设置。

要记录列入黑名单的连接：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要配置的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Security Intelligence 选项卡。

系统将显示该访问控制策略的安全情报设置。

步骤 4　点击日志记录图标 ( )。

系统将显示 Blacklist Options 弹出窗口。

步骤 5　选中 **Log Connections** 复选框。

步骤 6　指定要将连接和安全情报事件发送到何处。有以下选项可供选择：

- 要将事件发送至 ASA FirePOWER 模块，请选择 **Event Viewer**。
- 要将事件发送至外部系统日志服务器，请选择 **Syslog**，然后从下拉列表中选择系统日志警报响应。或者，您可以通过点击添加图标 ( ) 来添加系统日志警报响应；请参阅第 27-3 页上的创建系统日志警报响应。
- 要将连接事件发送至 SNMP 陷阱服务器，请选择 **SNMP Trap**，然后从下拉列表选择 SNMP 警报响应。或者，您可以通过点击添加图标 ( ) 来添加 SNMP 警报响应；请参阅第 27-2 页上的创建 SNMP 警报响应。

如果您想要将列入黑名单的对象设置为仅监控，或对安全情报过滤生成的连接事件执行任何其他基于 ASA FirePOWER 模块的分析，您**必须**将事件发送至 **事件查看器**。有关详细信息，请参阅第 25-4 页上的将连接记录至 ASA FirePOWER 模块或外部服务器。

步骤 7　点击 **OK** 设置日志记录选项。

Security Intelligence 选项卡将会再次显示。

步骤 8　点击 **Store ASA FirePOWER Changes**。

您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

根据访问控制处理记录连接

许可证：任何

在访问控制策略中，访问控制规则提供了处理网络流量的精细方法。因此您可以仅记录关键连接，针对每条访问控制规则启用连接记录，如果为规则启用连接记录，则系统会记录该规则处理的所有连接。

您还可以记录访问控制策略的默认操作处理的流量的连接。默认操作确定系统如何处理与策略中所有访问控制规则均不匹配的流量（“监控”规则除外，这些规则匹配和记录，但不处理或检测流量）。

请注意，即便您为所有访问控制规则和默认操作禁用了日志记录，连接终止事件仍可能会被记录至 ASA FirePOWER 模块，前提是该连接与访问控制规则相匹配且包含入侵尝试、受禁文件或恶意软件

取决于规则或默认策略操作以及您配置的关联检测选项，您的日志记录选项可能有所不同。有关详细信息，请参阅：

- 第 25-9 页上的记录与访问控制规则相匹配的连接
- 第 25-10 页上的记录访问控制默认操作处理的连接

记录与访问控制规则相匹配的连接

许可证：任何

要仅记录关键连接，您可以针对每条访问控制规则启用连接记录。如为某条规则启用日志记录，则系统会记录该规则处理的所有连接。

取决于规则操作及规则的入侵和文件检测配置，您的日志记录选项可能有所不同；请参阅第 25-4 页上的了解访问控制规则操作如何影响日志记录。另外，请注意，即便您为某条访问控制规则禁用日志记录，与该规则匹配的连接的连接终止事件仍可能被记录至 ASA FirePOWER 模块，前提是该连接：

- 包含入侵尝试、受禁文件或恶意软件
- 以前至少与一条访问控制监控规则相匹配

要将访问控制规则配置为记录连接、文件和恶意软件信息，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要修改的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器，重点显示 Rules 选项卡。

步骤 3　点击您想要在其中配置日志记录的规则旁的编辑图标 ( )。

系统将显示访问控制规则编辑器。

步骤 4　选择 Logging 选项卡。

系统将显示 Logging 选项卡。

步骤 5　指定您是想要选择 **Log at Beginning and End of Connection**、 **Log at End of Connection** 还是想要选择 **No Logging at Connection**。

对于单个未被阻止的连接，连接终止事件包含连接开始事件中的所有信息，以及在会话期间收集到的信息。因为受阻流量会被立即拒绝，无需进一步检测，所以，系统仅记录阻止规则的连接开始事件。为此，当您将规则操作设置为 **Block** 或 **Block with reset** 时，系统会提示您选择 **Log at Beginning of Connection**。

步骤 6　使用 **Log Files** 复选框指定系统是否应记录与连接相关联的任何文件和恶意软件事件。

当您将文件策略与该规则关联以便执行文件控制或 AMP 时，系统会自动启用该选项。思科建议让此选项保持启用状态；请参阅第 25-6 页上的为允许的连接禁用文件和恶意软件事件日志记录。

步骤 7　指定将连接事件发送至何处。有以下选项可供选择：

- 要将连接事件发送至 ASA FirePOWER 模块，请选择 Event Viewer。您无法针对监控规则禁用此选项。
- 要将事件发送至外部系统日志服务器，请选择 **Syslog**，然后从下拉列表中选择系统日志警报响应。或者，您可以通过点击添加图标 ( ) 来添加系统日志警报响应；请参阅第 27-3 页上的创建系统日志警报响应。
- 要将事件发送至 SNMP 陷阱服务器，请选择 **SNMP Trap**，然后从下拉列表选择 SNMP 警报响应。或者，您可以通过点击添加图标 ( ) 来添加 SNMP 警报响应；请参阅第 27-2 页上的创建 SNMP 警报响应。

如果您想要对连接事件执行基于 ASA FirePOWER 模块的分析，则您**必须**将事件发送至事件查看器。有关详细信息，请参阅第 25-4 页上的将连接记录至 ASA FirePOWER 模块或外部服务器。

步骤 8　点击 **Store ASA FirePOWER Changes**，以保存规则。

您的规则保存成功。您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

记录访问控制默认操作处理的连接

许可证：任何

您可以记录访问控制策略的默认操作处理的流量的连接。默认操作确定系统如何处理与策略中所有访问控制规则均不匹配的流量（“监控”规则除外，这些规则匹配和记录，但不处理或检测流量）；请参阅第 4-4 页上的为网络流量设置默认的处理和检查。

用于记录策略默认操作处理的连接的机制和选项与用于记录个别访问控制规则处理的连接的选项大致类似，如下表所述。也就是说，除了受阻流量，系统记录连接的开始和终止，而且您可以将连接事件发送至 ASA FirePOWER 模块或者外部系统日志或 SNMP 陷阱服务器。

表 25-3　访问控制默认操作日志记录选项

默认操作	比较	请参阅.....
访问控制：阻止所有流量	阻止规则	第 25-5 页上的了解受阻和交互式受阻连接的记录
访问控制：信任所有流量	信任规则	第 25-5 页上的了解受信任连接的日志记录
入侵防御	允许带有关联入侵策略的规则	第 25-5 页上的了解允许连接的日志记录

然而，记录访问控制规则处理的连接与记录默认操作处理的连接之间存在着一些差异：

- 默认操作没有文件日志记录选项。您无法使用默认操作执行文件控制或 AMP。
- 当与访问控制默认操作关联的入侵策略生成入侵事件时，系统**不会**自动记录相关连接终止事件。当您不想在入侵检测和仅限防御的部署中记录任何连接数据时，这很有帮助。

  如果您启用了默认操作的连接开始和终止日志记录，这一规则将不适用。在这种情况下，当关联的入侵策略触发时，除了记录连接开始事件外，系统还**会**日志记录连接终止事件。

请注意，即便您为默认操作禁用日志记录，与该规则匹配的连接的连接终止事件仍可能会被记录至 ASA FirePOWER 模块，前提是该连接以前至少与一条访问控制“监控”规则相匹配。

要记录由访问控制默认操作处理的流量中的连接，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击要修改的访问控制策略旁边的编辑图标 ( )。

系统将显示访问控制策略编辑器，重点显示 Rules 选项卡。

步骤 3　点击日志记录图标 ( )，该图标位于 **Default Action** 下拉列表旁。

系统将显示 Logging 弹出窗口。

步骤 4　指定您是想要选择 **Log at Beginning and End of ConnectionLog at End of Connection** 还是想要选择 **No Logging at Connection**。

对于单个未被阻止的连接，连接终止事件包含连接开始事件中的所有信息，以及在会话期间收集到的信息。因为受阻流量会被立即拒绝，无需进一步检测，系统仅记录“阻止所有流量”默认操作的连接开始事件。为此，当您将默认操作设置为 **Access Control: Block All Traffic** 时，系统会提示您选择 **Log at Beginning of Connection**。

步骤 5　指定将连接事件发送至何处。有以下选项可供选择：

- 要将连接事件发送至 ASA FirePOWER 模块，请选择 Event Viewer。您无法针对监控规则禁用此选项。
- 要将事件发送至外部系统日志服务器，请选择 **Syslog**，然后从下拉列表中选择系统日志警报响应。或者，您可以通过点击添加图标 ( ) 来添加系统日志警报响应；请参阅第 27-3 页上的创建系统日志警报响应。
- 要将事件发送至 SNMP 陷阱服务器，请选择 **SNMP Trap**，然后从下拉列表选择 SNMP 警报响应。或者，您可以通过点击添加图标 ( ) 来添加 SNMP 警报响应；请参阅第 27-2 页上的创建 SNMP 警报响应。

如果您要对连接事件执行基于 ASA FirePOWER 模块的分析，则**必须**将事件发送至事件查看器。有关详细信息，请参阅第 25-4 页上的将连接记录至 ASA FirePOWER 模块或外部服务器。

步骤 6　点击 **Store ASA FirePOWER Changes**，以保存策略。

您的策略保存成功。您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

记录在连接中检测到的 URL

许可证：任何

对于 HTTP 流量，当您将连接终止事件记录至 ASA FirePOWER 模块时，系统会记录在会话期间受监控主机请求的 URL。

默认情况下，系统会在连接日志中存储 URL 的前 1024 个字符。然而，您可以将系统配置为每个 URL 存储最多 4096 个字符，确保自己捕获受监控主机请求的完整 URL。或者，如果对访问的个别 URL 不感兴趣，可以通过存储 0 个字符来完全禁用 URL 存储。取决于网络流量，禁用 URL 字符存储或限制存储的 URL 字符的数量可以提高系统性能。

请注意，禁用 URL 日志记录并不影响 URL 过滤。访问控制规则会基于请求的 URL、其类别以及信誉来适当地过滤流量，即便系统不会记录这些规则处理的流量中请求的各个 URL。有关详细信息，请参阅第 8-6 页上的阻止 URL。

要自定义存储的 URL 字符的数量：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**。

系统将显示 Access Control Policy 页面。

步骤 2　点击想要配置的访问控制策略旁的编辑图标 ( )。

系统将显示访问控制策略编辑器。

步骤 3　选择 Advanced 选项卡。

系统将显示访问控制策略的高级设置。

步骤 4　点击 General Settings 旁的编辑图标 ( )。

系统将显示 General Settings 弹出窗口。

步骤 5　键入**要在连接事件中存储的最大 URL 字符数量**。

您可以指定从 0 至 4096 的任何数量。存储零个字符会禁用 URL 存储，而不会禁用 URL 过滤。

步骤 6　点击 **OK**。

系统将显示访问控制策略的高级设置。

步骤 7　点击 **Store ASA FirePOWER Changes** 以保存策略。

您的策略保存成功。您必须应用更改的访问控制策略以使更改生效；请参阅第 4-10 页上的应用访问控制策略。

查看事件

您可以查看针对 ASA FirePOWER 检查的流量记录的实时事件。

注 模块只在内存中缓存最近的 100 个事件。

有关详细信息，请参阅：

- 第 26-1 页上的访问 ASA FirePOWER 实时事件
- 第 26-2 页上的了解 ASA FirePOWER 事件类型
- 第 26-3 页上的 ASA FirePOWER 事件中的事件字段
- 第 26-10 页上的入侵规则分类

访问 ASA FirePOWER 实时事件

您可以在若干预定义的事件视图中查看 ASA FirePOWER 模块检测到的事件或创建自定义事件视图以查看您选择的事件字段。

注 模块只在内存中缓存最近的 100 个事件。

要查看 ASA FirePOWER 事件，请执行以下操作：

步骤 1 选择 **Monitoring > ASA FirePOWER Monitoring > Real-time Eventing**。

步骤 2 您有两种选择：

- 点击要查看的事件类型的现有选项卡：连接事件、安全情报事件、入侵事件、文件事件或恶意软件事件。
- 点击 + 图标创建自定义事件视图并选择您要包含在视图中的事件字段。

有关详细信息，请参阅第 26-2 页上的了解 ASA FirePOWER 事件类型和第 26-3 页上的 ASA FirePOWER 事件中的事件字段。

了解 ASA FirePOWER 事件类型

通过 ASA FirePOWER 模块可实时查看来自五种事件类型的事件字段的事件：连接事件、安全情报事件、入侵事件、文件事件和恶意软件事件。

Connection Events

连接日志，称为*连接事件*，包含有关检测到的会话的数据。任何单个连接事件的可用信息都取决于多种因素，但通常包括：

- 基本连接属性：时间戳、源和目标 IP 地址、入口和出口区域，处理连接的设备等
- 系统发现或推断的其他连接属性：应用、请求的 URL 或与连接关联的用户等
- 有关记录连接原因的元数据：哪个策略中的哪个访问控制规则（或其他配置）对流量进行处理，是否允许或阻止连接等等

访问控制中的各种设置使您可以精细控制记录哪些连接、何时记录以及在哪里存储数据。可以记录访问控制策略可以成功处理的任何连接。在以下情况下可以启用连接日志记录：

- 当连接由基于信誉的安全情报功能列入黑名单（阻止）或监控时
- 当连接由访问控制规则或访问控制默认操作处理时

除了您配置的日志记录外，系统会自动记录检测到被禁止的文件、恶意软件或入侵尝试的大多数连接。

Security Intelligence Events

当您启用安全情报日志记录时，黑名单匹配自动生成*安全情报事件*和连接事件。安全情报事件是您可以分别查看和分析的一种特殊类型的连接事件。有关配置连接日志记录的详细信息，包括安全情报黑名单决策，请参阅第 25-1 页上的记录网络流量中的连接。

提示 除非另行说明，否则有关连接事件的一般信息也与安全情报事件有关。有关安全情报的详细信息，请参阅第 5-1 页上的使用安全情报 IP 地址声誉设置黑名单。

Intrusion Events

系统检查网络上传输的数据包是否存在可能影响主机及其数据的可用性、完整性和机密性的恶意活动。如果系统识别出潜在的入侵，会生成*入侵事件*；入侵事件是有关攻击源和攻击目标的日期、时间、漏洞类型以及情境信息的记录。

File Events

*文件事件*表示系统在网络流量中检测到并或者被阻止的文件。

系统将按照当前适用文件策略记录当受管设备在网络流量中检测或阻止文件时生成的文件事件。

Malware Events

*恶意软件事件*表示系统在网络流量中检测到并或者被阻止的恶意软件文件。

在整体访问控制配置过程中， ASA FirePOWER 模块可以通过恶意软件许可证在网络流量内检测恶意软件；请参阅第 24-4 页上的了解和创建文件策略。

以下情形可产生恶意软件事件：

- 如果受管设备检测一组具体文件类型之一， ASA FirePOWER 模块执行恶意软件云查找，向 ASA FirePOWER 模块返回 `Malware`、 `Clean` 或 `Unknown` 文件性质。
- 如果 ASA FirePOWER 模块不能与云建立连接，或者云因其他原因不可用，文件性质为 `Unavailable`。您可以查看很少一部分事件发生此情况；这是预期行为。

- 如果受管设备检测到安全列表内文件，ASA FirePOWER 模块向该文件分配 Clean 文件性质。

ASA FirePOWER 模块将文件检测和性质记录以及其他情景数据作为恶意软件事件进行记录。

在网络流量中检测到并且被 ASA FirePOWER 模块确定为恶意软件的文件，会生成一个文件事件和一个恶意软件事件。这是由于要在文件中检测恶意软件，系统必须首先检测文件本身。

ASA FirePOWER 事件中的事件字段

Action

对于连接或安全情报事件，与记录连接的访问控制规则关联的操作或默认操作

- Allow 表示示确容许和用户忽略的被阻止连接。
- Trust 表示信任的连接。信任规则在第一个数据包上检测到的 TCP 连接仅生成连接结束事件。系统会在最终会话数据包之后一小时生成事件。
- Block 和 Block with reset 代表被阻止连接。系统还将 Block 操作与由安全情报列入黑名单的连接、入侵策略检测到存在漏洞的连接及文件被文件策略阻止的连接相关联。
- Interactive Block 和 Interactive Block with reset 标记开始连接事件，您可以在系统利用交互式规则最初阻止用户的 HTTP 请求时进行记录。如果用户点击阅读系统显示的警告页面，则您为会话记录的任何其他连接事件均具有 Allow 操作。
- Default Action 表示连接采用默认操作处理。
- 对于受安全情报监控的连接，该项操作即为由连接触发的第一个非监控访问控制规则的操作，或者为默认操作。同样地，因为匹配监控规则的流量始终由后续规则或通过默认操作进行处理，所以与因监控规则原因记录的连接相关联的操作不可能为 Monitor。

对于文件或恶意文件事件，与文件所匹配规则的规则操作相关联的文件规则操作，以及任何关联的文件规则操作选项。

Allowed Connection

系统是否允许事件的流量通过。

Application

在连接中检测到的应用。

Application Business Relevance

连接中检测到的应用流量的业务相关性：Very High、 High、 Medium、 Low 或 Very Low。连接中检测的各类应用都有相关业务相关性；该字段显示级别最低的业务相关性。

Application Categories

展示应用特征的类别，协助您了解应用功能。

Application Risk

连接中检测到的应用流量相关风险：Very High、 High、 Medium、 Low 或 Very Low。连接中检测的各类应用都有一个相关风险；该字段显示最高风险。

Application Tag

展示应用特征的标记，协助您了解应用功能。

Block Type

在访问控制规则中指定的与事件中的流量匹配的块类型：块或交互块。

Client

在连接中检测到的客户端应用。

如果系统无法识别连接中使用的具体客户端，则该字段将显示应用协议名称中追加的 `client`，以便提供通用名称，例如，`FTP client`。

Client Business Relevance

与连接中检测到的客户端流量相关的业务相关性：`Very High`、`High`、`Medium`、`Low` 或 `Very Low`。连接中检测的各类客户端都有相关的业务相关性；该字段显示级别最低（最不相关）的业务相关性。

Client Categories

展示在流量中检测到的客户端特征的类别，协助您了解客户端功能。

Client Risk

连接中检测到的客户端流量相关风险：`Very High`、`High`、`Medium`、`Low` 或 `Very Low`。连接中检测的各类客户端都有一个相关风险；该字段显示最高风险。

Client Tag

展示在流量中检测到的客户端特征的标记，协助您了解客户端功能。

Client Version

在连接中检测到的客户端的版本。

Connection

内部产生的流量的唯一 ID。

Connection Blocktype Indicator

在访问控制规则中指定的与事件中的流量匹配的块类型：块或交互块。

Connection Bytes

连接的总字节量。

Connection Time

连接的开始时间。

Connection Timestamp

检测到连接的时间。

Context

确定流量通过的安全情景的元数据。请注意，系统仅对多情景模式下的设备填充此字段。

Denied Connection

系统是否已拒绝事件的流量通过。

Destination Country and Continent

接收主机的国家/地区和大洲。

Destination IP

接收主机使用的 IP 地址。

Destination Port、 Destination Port Icode、 Destination Port/ICMP Code

会话响应方使用的目标端口或 ICMP 代码。

Direction

文件传输的方向。

Disposition

可以为下列文件性质之一：

- `Malware` 表示云将文件归类为恶意软件。
- `Clean` 表示云将文件归类为安全，或用户将文件添加到安全列表。
- `Unknown` 表示在云分配性质之前发生恶意软件云查找。文件未分类。
- `Custom Detection` 表示用户将文件添加到自定义检测列表。
- `Unavailable` 表示 ASA FirePOWER 模块无法执行恶意软件云查找。您可以查看很少一部分事件发生此情况；这是预期行为。
- `N/A` 表示 Detect Files 或 Block Files 规则处理了文件，ASA FirePOWER 模块不执行恶意软件云查找。

Egress Interface

与连接相关的出口接口。请注意，如果部署包括异步路由配置，入口和出口接口可能属于同一接口集。

Egress Security Zone

与连接相关的出口安全区。

Event

事件类型。

Event Microseconds

检测到事件的时间（毫秒）。

Event Seconds

检测到事件的时间（秒）。

Event Type

事件的类型。

File Category

一般类别文件类型，例如：`Office Documents`、 `Archive`、 `Multimedia`、 `Executables`、 `PDF files`、 `Encoded`、 `Graphics` 或 `System Files`。

File Event Timestamp

文件或恶意软件文件的创建时间和日期。

File Name

文件或恶意软件文件的名称。

File SHA256

文件的 SHA-256 哈希值。

File Size

文件或恶意软件文件的大小 (KB)

File Type

文件或恶意软件文件的文件类型，例如， `HTML` 或 `MSEXE`。

File/Malware Policy

与事件生成相关的文件策略。

Filelog Blocktype Indicator

在文件规则中指定的与事件中的流量匹配的块类型：块或交互块。

Firewall Policy Rules/SI Category

表示或包含连接中被列为黑名单的 IP 地址的黑名单对象名称。安全情报类别可以是网络对象或网络组、全局黑名单、自定义安全情报列表或源、或者情报源中一个类别的名称。请注意，只有在 **Reason** 是 `IP Block` 或 `IP Monitor` 时才填充该字段；安全情报事件视图中的条目始终显示原因。

Firewall Rule

处理连接的访问控制规则或默认操作，以及最多 8 条该连接匹配的监控规则。

First Packet

查看会话的第一个数据包的日期和时间。

HTTP Referrer

HTTP 来源地址，表示在连接中检测到的 HTTP 流量的请求 URL 来源地址（例如提供到另一个 URL 的链接或从其导入链接的网站）。

IDS Classification

生成事件的规则所属的分类。有关规则分类名称和编号，请参阅规则分类 表。

Impact

此字段中的影响级别指示入侵数据、网络发现数据和漏洞信息之间的相关性。

Impact Flag

参见 Impact。

Ingress Interface

与连接相关的入口接口。请注意，如果部署包括异步路由配置，入口和出口接口可能属于同一接口集。

Ingress Security Zone

与连接相关的入口安全区。

Initiator Bytes

会话发起方发送的总字节数。

Initiator Country and Continent

当检测到可路由的 IP 时，与启动会话的主机 IP 地址关联的国家/地区和大洲。

Initiator IP

发起会话响应方的主机 IP 地址（以及主机名，如果启用 DNS 解析）。

Initiator Packets

会话发起方发送的数据包总数。

Inline Result

以下之一：

- 一个黑色向下箭头，表明系统已丢弃触发规则的数据包
- 一个灰色向下箭头，表明如果已启用 **Drop when Inline** 入侵策略选项 （在内联部署中），或者在系统进行修剪时一个 Drop and Generate 规则生成了该事件，那么 IPS 应该已丢弃数据包
- 空白，表明触发规则未设置为 Drop and Generate Events
- 请注意，无论入侵策略的规则状态或内联丢弃行为如何，系统都不会丢弃被动部署中的数据包，当内联接口处于分路模式时也是如此。

IPS Blocktype Indicator

与事件中的流量匹配的入侵规则的操作。

Last Packet

查看会话的最后一个数据包的日期和时间。

MPLS Label

与触发此入侵事件的数据包相关的多协议标记交换标记。

Malware Blocktype Indicator

在文件规则中指定的与事件中的流量匹配的块类型：块或交互块。

Message

事件的说明文本。

对于基于规则的入侵事件，事件消息提取自规则。对于基于解码器和预处理器的事件，事件消息采用硬编码。

对于恶意软件事件而言，与恶意软件事件相关的所有其他信息。对于基于网络的恶意软件事件，该字段仅在文件性质发生变更的文件中填充。

Monitor Rules

该连接匹配的最多八个监控规则。

Netbios Domain

会话中使用的 NetBIOS 域。

Policy

与事件生成相关的访问控制、入侵或网络分析策略 (NAP) （如果有）。

Policy Revision

与事件生成相关的访问控制、文件、入侵或网络分析策略 (NAP) 的版本 （如果有）。

Priority

事件优先级由思科 VRT 确定。

Protocol

在连接中检测到的协议。

Reason

在以下几种情况，连接被记录的原因：

- `User Bypass` 表示系统最初阻止了用户的 HTTP 请求，但用户选择通过点击警告页面继续访问原先请求的站点。`User Bypass` 原因始终与 `Allow` 操作匹配。
- `IP Block` 表示基于安全情报数据，该系统未经检查就拒绝连接。`IP Block` 原因始终与 `Block` 操作匹配。
- `IP Monitor` 表示基于安全情报数据，该系统本可拒绝连接，但您将系统配置为监控连接，而不是拒绝连接。
- `File Monitor` 表示系统在连接中检测到特定类型的文件。
- `File Block` 表示连接中包含系统禁止传输的文件或恶意软件文件。`File Block` 原因始终与 `Block` 操作匹配。
- `File Custom Detection` 表示连接中包含自定义检测列表上的系统禁止传输的文件。
- `File Resume Allow` 表示文件传输最初被 Block Files 或 Block Malware 文件规则阻止。应用允许文件的新访问控制策略后，会自动恢复 HTTP 会话。请注意，此原因只出现在内联部署中。
- `File Resume Block` 表示件传输最初被 Detect Files 或 Malware Cloud Lookup 文件规则允许。应用阻止文件的新访问控制策略后，会自动停止 HTTP 会话。请注意，此原因只出现在内联部署中。
- `Intrusion Block` 表示系统阻止或本可阻止在连接中检测到的攻击程序（违反入侵策略）。`Intrusion Block` 原因与用于阻止攻击程序的 `Block` 操作和用于本可阻止的攻击程序的 `Allow` 操作相匹配。
- `Intrusion Monitor` 表示系统检测到但并未阻止连接中检测到的攻击程序。当触发的入侵规则状态设置为 **Generate Events** 时，会发生这种情况。

Receive Times

目标主机或响应方响应事件的时间。

Referenced Host

如果连接中的协议是 DNS、 HTTP 或 HTTPS，此字段显示各自协议使用的主机名。

Responder Bytes

会话响应方发送的总字节数。

Responder Country and Continent

当检测到可路由的 IP 时，与会话响应方的主机 IP 地址相关的国家/地区和大洲。

Responder Packets

会话响应方发送的数据包总数。

Responder IP

响应会话发起方的主机 IP 地址（以及主机名，如果启用 DNS 解析）。

Signature

与事件的流量匹配的入侵规则的签名 ID。

Source Country and Continent

发送主机的国家/地区和大洲。

Source IP

入侵事件中的发送主机使用的 IP 地址。

Source or Destination

发出或接收事件的连接的主机。

Source Port、 Source Port Type、 Source Port/ICMP Type

会话发起方使用的源端口或 ICMP 类型。

TCP Flags

在连接中检测到的 TCP 标志。

URL

在会话期间受监控主机所请求的 URL。

URL Category

在会话期间与受监控主机所请求的 URL 相关的类别（如果可用）。

URL Reputation

在会话期间与受监控主机所请求的 URL 相关的信誉（如果可用）。

URL Reputation Score

在会话期间与受监控主机所请求的 URL 相关的信誉得分（如果可用）。

User

发生事件的主机 (**Receiving IP**) 的用户。

User Agent

从连接中检测到的 HTTP 流量提取的用户代理应用信息。

VLAN

与触发事件的数据包相关的最内部的 VLAN ID。

Web App Business Relevance

与连接中检测到的网络应用流量相关的业务相关性：`Very High`、`High`、`Medium`、`Low` 或 `Very Low`。连接中检测的各类网络应用都有相关的业务相关性；该字段显示级别最低（最不相关）的业务相关性。

Web App Categories

展示在流量中检测到的网络应用特征的类别，协助您了解网络应用功能。

Web App Risk

连接中检测到的网络应用流量相关风险：`Very High`、`High`、`Medium`、`Low` 或 `Very Low`。连接中检测的各类网络应用都有一个相关风险；该字段显示最高风险。

Web App Tag

展示在流量中检测到的网络应用特征的标记，协助您了解网络应用功能。

Web Application

在流量中检测到的网络应用。

入侵规则分类

入侵规则包括攻击分类。下表列出每种分类的名称和编号

表 26-1　　规则分类

编号	分类名称	说明
1	not-suspicious	非可疑流量
2	unknown	未知流量
3	bad-unknown	潜在不良流量
4	attempted-recon	尝试信息泄露
5	successful-recon-limited	信息泄露
6	successful-recon-largescale	大规模信息泄露
7	attempted-dos	尝试拒绝服务
8	successful-dos	拒绝服务攻击
9	attempted-user	尝试获取用户权限
10	unsuccessful-user	未成功获取用户权限
11	successful-user	成功获取用户权限
12	attempted-admin	尝试获取管理员权限
13	successful-admin	成功获取管理员权限
14	rpc-portmap-decode	解码 RPC 查询
15	shellcode-detect	检测到可执行代码

表 26-1　规则分类（续）

编号	分类名称	说明
16	string-detect	检测到可疑字符串
17	suspicious-filename-detect	检测到可疑文件名
18	suspicious-login	检测到尝试使用可疑用户名的登录
19	system-call-detect	检测到系统调用
20	tcp-connection	检测到 TCP 连接
21	trojan-activity	检测到网络木马
22	unusual-client-port-connection	客户端使用异常端口
23	network-scan	检测网络扫描
24	denial-of-service	检测拒绝服务攻击
25	non-standard-protocol	检测非标准协议或事件
26	protocol-command-decode	通用协议命令解码
27	web-application-activity	访问可能易受攻击的网络应用
28	web-application-attack	网络应用攻击
29	misc-activity	其他活动
30	misc-attack	其他攻击
31	icmp-event	一般 ICMP 事件
32	inappropriate-content	检测到不当内容
33	policy-violation	可能违反公司隐私策略
34	default-login-attempt	尝试使用默认用户名和密码登录
35	sdf	敏感数据
36	malware-cnc	已知恶意软件命令和控制流量
37	client-side-exploit	已知客户端攻击尝试
38	file-format	已知的恶意文件或基于文件的攻击

配置外部警报

尽管 ASA FirePOWER 模块在模块界面中提供了各种事件视图，但您仍可能想要配置外部事件通知，以简化对关键系统的持续监控。可将模块配置为生成警报，在发生以下某一事件时通过邮件、 SNMP 陷阱或系统日志发送通知：

- 基于网络的恶意软件事件或回溯性恶意软件事件
- 由特定的访问控制规则触发的连接事件

要让ASA FirePOWER 模块发送这些警报，必须先创建一个*警报响应*，这是一组配置，允许模块与计划发送警报的外部系统进行交互。例如，这些配置可以指定、 SNMP 警报参数或系统日志设备和优先级。

创建警报响应之后，可将其与要用于触发警报的事件关联起来。请注意，在将警报响应与事件进行关联时，具体流程因事件类型而异：

- 可使用各类事件自己的配置页面，将警报响应与恶意软件事件关联起来。
- 通过使用访问控制规则和策略，可将 SNMP 和系统日志警报响应与已记录的连接关联起来。

还可在 ASA FirePOWER 模块中执行另外一种警报，即为单个的入侵事件配置、 SNMP 和系统日志入侵事件通知。可在入侵策略中配置这些通知；请参阅第 28-1 页上的配置入侵规则的外部警报和第 20-28 页上的添加 SNMP 警报。下表介绍了生成警报时必须拥有的许可证。

表 27-1　　生成警报时的许可证要求

要基于以下内容生成警报...	您需要该许可证.....
的入侵事件	保护
基于网络的恶意软件事件	恶意软件
连接事件	记录连接所需的许可证

有关详情，请参阅：

- 第 27-2 页上的使用警报响应
- 第 25-1 页上的记录网络流量中的连接

使用警报响应

许可证：任何环境

配置外部警报时，首先要创建一个警报响应，这是一组配置，允许 ASA FirePOWER 模块与计划发送警报的外部系统进行交互。可创建警报响应以通过邮件、简单网络管理协议 (SNMP) 陷阱或系统日志 (syslog) 发送警报。

在警报中收到的信息取决于触发警报的事件类型。

创建警报响应时，它将自动启用。只有已启用的警报响应才能生成警报。要阻止生成警报，可暂时禁用警报响应，而非删除配置。

您管理 Alerts 页面上的警报响应 (**ASA FirePOWER Configuration > Policies > Actions Alerts**)。每个警报响应旁的滑块指明该响应是否处于活动状态；只有已启用的警报响应才能生成警报。该页面也指明警报响应目前是否用于某一配置中，例如，在访问控制规则中记录连接。可点击名称、类型、使用状态和启用/禁用状态以按相应的列标题对警报响应排序；再次点击列标题可以反向排序。

有关详情，请参阅：

- 第 27-2 页上的创建 SNMP 警报响应
- 第 27-3 页上的创建系统日志警报响应
- 第 27-5 页上的修改警报响应
- 第 27-6 页上的删除警报响应
- 第 27-6 页上的启用和禁用警报响应

创建 SNMP 警报响应

许可证：任何环境

可使用 SNMPv1、 SNMPv2 或 SNMPv3 创建 SNMP 警报响应。

注　如果想要使用 SNMP 监控 64 位值，则必须使用 SNMPv2 或 SNMPv3。SNMPv1 不支持 64 位监控。

要创建 SNMP 警报响应，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Actions Alerts**。

系统将显示 Alerts 页面。

步骤 2　从 **Create Alert** 下拉菜单，选择 **Create SNMP Alert**。

系统将显示 Create SNMP Alert Configuration 弹出窗口。

步骤 3　在 **Name** 字段中，键入要用于标识 SNMP 响应的名称。

步骤 4　在 **Trap Server** 字段中，使用字母数字字符键入 SNMP 陷阱服务器的主机名或 IP 地址。

请注意，如在此字段中输入了无效的 IPv4 地址（例如 192.169.1.456），则系统**不会**发出警告。相反，无效地址会被视为主机名。

步骤 5　从 **Version** 下拉列表中，选择要使用的 SNMP 版本。

SNMP v3 是默认值。如果选择 SNMP v1 或 SNMP v2，系统会显示不同的选项。

步骤 6　您选择了哪个版本的 SNMP？

- 对于 SNMP v1 或 SNMP v2，在 **Community String** 字段中，使用字母数字字符或特殊符号 `*` 或 `$` 键入 SNMP 团体名称，然后跳至第 12 步。
- 对于 SNMP v3，在 **User Name** 字段中，键入要使用 SNMP 服务器对其进行身份验证的用户的名称并继续下一步。

步骤 7　从 **Authentication Protocol** 下拉列表中，选择要用于身份验证的协议。

步骤 8　在 **Authentication Password** 字段中，键入使用 SNMP 服务器进行身份验证所需的密码。

步骤 9　从 **Privacy Protocol** 列表中，选择 **None** 以不使用隐私协议或选择 **DES** 以使用 Data Encryption Standard 作为隐私协议。

步骤 10　在 **Privacy Password** 字段中，键入 SNMP 服务器要求的隐私密码。

步骤 11　在 **Engine ID** 字段中，使用偶数数字（十六进制形式）键入 SNMP 引擎的标识符。

使用 SNMPv3 时，系统使用引擎 ID 值对消息进行编码。 SNMP 服务器需要使用该值解码消息。

思科建议您使用 ASA FirePOWER 模块的 IP 地址的十六进制版本。例如，如果ASA FirePOWER 模块的 IP 地址是 `10.1.1.77`，请使用 `0a01014D0`。

步骤 12　单击 **Store ASA FirePOWER Changes**。

警报响应保存成功并自动启用。

创建系统日志警报响应

许可证：任何环境

配置系统警报响应时，可指定与系统日志消息相关联的严重性和设备，以确保它们得到系统日志服务器的正确处理。设备指明创建消息的子系统，严重性界定消息的严重性。设备和严重性不显示在系统日志中的实际消息中，而是告知接收系统日志消息的系统如何对消息进行归类。

提示　有关系统日志如何运行及如何对其进行配置的更多详细信息，请参阅系统文档。在 UNIX 系统上，`syslog` 和 `syslog.conf` 的 `man` 页面提供了概念信息和配置说明。

虽然在创建系统日志警报响应时可选择任一种设备，但您还是应该根据自己的系统日志服务器选择适合的一个；并非所有系统日志服务器都支持所有设备。对于 UNIX 系统日志服务器，`syslog.conf` 文件应指示哪些设备保存到了服务器的哪些日志文件上。

下表列出了可选择的系统日志设备。

表 27-2　　可选用的系统日志设施

设施	说明
ALERT	警报消息。
审计	审计子系统生成的消息。
AUTH	与安全和授权相关的消息。
AUTHPRIV	与安全和授权相关的访问限制消息。很多系统会将这些消息转发到一个安全的文件中。

表 27-2　可选用的系统日志设施 （续）

设施	说明
CLOCK	时钟后台守护程序生成的消息。 请注意，运行 Windows 操作系统的系统日志服务器将使用 CLOCK 设备。
CRON	时钟后台守护程序生成的消息。 请注意，运行 Linux 操作系统的系统日志服务器将使用 CRON 设备。
DAEMON	系统后台守护程序生成的消息。
FTP	FTP 后台守护程序生成的消息。
KERN	内核生成的消息。很多系统会在这些消息出现后将其传送至控制台打印。
LOCAL0-LOCAL7	内部进程生成的消息。
LPR	打印子系统生成的消息。
MAIL	邮件系统生成的消息。
新闻	网络新闻子系统生成的消息。
NTP	NTP 守护程序生成的消息。
SYSLOG	系统日志后台守护程序生成的消息。
用户	用户级进程生成的消息。
UUCP	UUCP 子系统生成的消息。

下表列出了可选择的标准系统日志严重性级别。

表 27-3　系统日志严重性级别

功率水平	说明
ALERT	应立即更正的状况。
CRIT	临界状况。
DEBUG	包含调试信息的消息。
EMERG	向所有用户广播的紧急状况。
ERR	错误状况。
INFO	信息性消息
请注意！	需要注意但非错误的状况。
警告	警告消息。

开始发送系统日志警报之前，请确保系统日志服务器可接受远程消息。

要创建系统日志警报，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Actions Alerts**。

系统将显示 Alerts 页面。从 **Create Alert** 下拉菜单中，选择 **Create Syslog Alert**。

系统将显示 Create Syslog Alert Configuration 弹出窗口。

步骤 2　在 **Name** 字段中，键入要用于标识已保存响应的名称。

步骤 3　在 **Host** 字段中，键入系统日志服务器的主机 或 IP 地址。

请注意，如在此字段中输入了无效的 IPv4 地址 （例如 192.168.1.456），则系统**将不**发出警告。相反，无效地址会被视为主机名。

步骤 4　在 **Port** 字段中，键入服务器用于系统日志消息的端口。

默认情况下，此值为 514。

步骤 5　从 **Facility** 列表中，选择设备。

请参阅可选用的系统日志设施表，了解可用设备列表。

步骤 6　从 **Severity** 列表中，选择严重性。

请参阅系统日志严重性级别表，了解可用严重性列表。

步骤 7　在 **Tag** 字段中，键入想要与系统日志消息一起显示的标记名称。

标记名称只能使用字母数字字符。**不能**使用空格或下划线。

例如，如果想在发送至系统日志的所有消息前加上 `FromDC`，请在该字段中键入 `FromDC`。

步骤 8　单击 **Store ASA FirePOWER Changes**。

警报响应保存成功并自动启用。

修改警报响应

许可证：任何环境

对于大多数类型的警报，如果某一警报响应已启用且在使用中，则对该警报响应做出的更改将立即生效。但对于访问控制规则中用于记录连接事件的警报响应而言，只有重新应用了访问控制策略，所做的更改才能生效。

要编辑警报响应，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Actions Alerts**。

系统将显示 Alerts 页面。

步骤 2　在要编辑的警报响应旁，点击编辑图标 ( )。

系统显示与该警报响应对应的配置弹出窗口。

步骤 3　根据需要进行更改。

步骤 4　单击 **Store ASA FirePOWER Changes**。

警报响应保存成功。

删除警报响应

许可证：任何环境

可删除未使用的任何警报响应。

要删除警报响应，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Actions Alerts**。

系统将显示 Alerts 页面。

步骤 2　在要删除的警报响应旁，点击删除图标 ( )。

步骤 3　确认要删除该警报响应。

警报响应删除成功。

启用和禁用警报响应

许可证：任何环境

只有已启用的警报响应才能生成警报。要阻止生成警报，可暂时禁用警报响应，而非删除配置。请注意，如在禁用某警报时该警报正在使用中，则该警报禁用后仍被视为在使用。

要启用或禁用警报响应，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies > Actions Alerts**。

系统将显示 Alerts 页面。

步骤 2　在要启用或禁用的警报响应旁，点击启用/禁用滑块。

如果警报响应已启用，则将其禁用。如果连接已禁用，点击该滑块将会启用连接。

配置入侵规则的外部警报

虽然 ASA FirePOWER 模块在用户界面内提供各种入侵事件视图，但一些企业更喜欢通过定义外部入侵事件通知对关键系统实施持续监控。可以记录日志到系统日志设施或将事件数据发送到 SNMP 陷阱服务器。

您可以为每个入侵策略指定入侵事件通知限制、设置发送到外部日志记录设施的入侵事件通知，也可以配置入侵事件的外部响应。

提示 一些分析师并不希望收到同一入侵事件的多个警报，但却希望控制收到特定入侵事件通知的频率。有关详情，请参见第 20-19 页上的按策略过滤入侵事件通知。

在 ASA FirePOWER 模块中，除了入侵策略，还可以执行另外一种警报。对于其他类型事件，可以配置SNMP 和系统日志警报响应活动。这些事件包括采用特定访问控制规则记录的连接事件。有关详细信息，请参阅第 27-1 页上的配置外部警报。

有关外部入侵事件通知的详细信息，请参阅以下章节。

- 第 28-1 页上的使用 SNMP 响应介绍用于将事件数据发送到指定 SNMP 陷阱服务器的配置选项，并提供指定 SNMP 警报选项的程序。
- 第 28-4 页上的使用系统日志响应介绍用于将事件数据发送到外部系统日志的配置选项，并提供指定系统日志警报选项的程序。

使用 SNMP 响应

许可证：保护

*SNMP 陷阱*是一种网络管理通知。将设备配置为以 SNMP 陷阱（又称为 *SNMP 警报*）的形式发送入侵事件通知。每个 SNMP 警报都包括以下内容:

- 生成陷阱的服务器的名称
- 检测到入侵事件的设备的 IP 地址
- 检测到入侵事件的设备的名称
- 事件数据

可以设置 SNMP 警报的多种参数。可设定的参数因所用的 SNMP 版本而有所不同。有关启用和禁用 SNMP 警报的详细信息，请参阅第 19-6 页上的在入侵策略中配置高级设置。

提示 如果网络管理系统要求使用管理信息库文件 (MIB)，您可以从ASA FirePOWER 模块中获取，具体位置为 `/etc/sf/DCEALERT.MIB`。

SNMP v2 选项

对于 SNMP v2，您可指定下表中介绍的选项。

表 28-1　SNMP v2 选项

选项	说明
Trap Type	警报中出现的 IP 地址所用到的陷阱类型。 如果网络管理系统正常显现 INET_IPV4 地址类型，则可以选择 **as Binary**。否则，应选择 **as String**。例如， HP Openview 就需要选择字符串类型。
Trap Server	收到 SNMP 陷阱通知的服务器。 可指定一个唯一的 IP 地址或主机名。
Community String	社区名称。

SNMP v3 选项

对于 SNMP v3，您可指定下表中介绍的选项。

注 当您使用 SNMP v3 时，设备会使用一个 Engine ID 值编码消息。SNMP 服务器需要使用该值解码消息。目前，该 Engine ID 值始终采用设备 IP 地址的十六进制形式，且该字符串的末尾为 `01`。例如，如果发送 SNMP 警报的设备有一个 IP 地址为 `172.16.1.50`，则 Engine ID 为 `0xAC10013201`，而如果设备有一个 IP 地址为 `10.1.1.77`，则 `0x0a01014D01` 就用作 Engine ID。

表 28-2　SNMP v3 选项

选项	说明
Trap Type	警报中出现的 IP 地址所用到的陷阱类型。 如果网络管理系统正常显现 INET_IPV4 地址类型，则可以选择 **as Binary**。否则，应选择 **as String**。例如， HP Openview 就需要选择字符串类型。
Trap Server	收到 SNMP 陷阱通知的服务器。 可指定一个唯一的 IP 地址或主机名。
Authentication Password	用于身份验证的密码。 SNMP v3 使用消息摘要 5 (MD5) 哈希函数或安全哈希算法 (SHA) 哈希函数进行密码加密，具体取决于配置。 一旦指定身份验证密码，身份验证即可启用。
Private Password	用于保护隐私的 SNMP 密钥。 SNMP v3 采用数据加密标准 (DES) 分组密码对密码进行加密。 一旦指定私有密码，隐私功能即可启用。指定私有密码后，还必须指定身份验证密码。
用户名	SNMP 用户名。

有关配置 SNMP 警报的信息，请参阅第 28-3 页上的配置 SNMP 响应。

配置 SNMP 响应

许可证：保护

您可以配置入侵策略中的 SNMP 警报。应用访问控制策略中的入侵策略后，一旦系统检测到任何入侵事件，就会通过 SNMP 陷阱发送通知。有关 SNMP 警报的详细信息，请参阅第 28-1 页上的使用 SNMP 响应。

要配置 SNMP 警报选项，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Advanced Settings**。

系统将显示 Advanced Settings 页面。

步骤 4　根据 External Responses 中 **SNMP Alerting** 的启用情况，您有两种选择：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 SNMP Alerting 页面。

页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 5　指定在警报中显示的 IP 地址所用的陷阱类型格式，可选择 **as Binary** 或 **as String**。

注　如果网络管理系统正常显现 INET_IPV4 地址类型，则可以使用 **as Binary** 选项。否则，应使用 **String** 选项。例如， HP OpenView 需要选择 **as String** 选项。

步骤 6　选择 SNMP v2 或 SNMP v3：

- 要配置 SNMP v2，请在相应字段中输入要使用的陷阱服务器的 IP 地址和社区名称。请参阅第 28-2 页上的 SNMP v2 选项。
- 要配置 SNMP v3，请在相应字段中输入要使用的陷阱服务器的 IP 地址、身份验证密码、私有密码和用户名。有关详情，请参见第 28-2 页上的 SNMP v3 选项。

注　必须选择 SNMP v2 **或** SNMP v3。

注　输入 SNMP v3 密码后，初始配置期间的密码会以明文显示，但以加密格式保存。

步骤 7　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

使用系统日志响应

许可证：保护

系统日志 (*syslog*) 是网络事件记录的标准记录机制。您可以将表示入侵事件通知的*系统日志警报*发动到设备的系统日志中。系统日志使您能够按照优先级和设施对信息进行分类。*优先级*反映的是警报的严重程度，*设施*显示的是生成警报的子系统。设施和优先级并不会在系统日志的实际消息内显示，而是用于规定系统对系统日志消息进行分类的方法。

系统日志警报包含以下信息：

- 生成警报的日期和时间
- 事件消息
- 事件数据
- 触发事件的生成器 ID
- 触发事件的 Snort ID
- 修订

您可以打开入侵策略中的系统日志警报、指定与系统日志中入侵事件通知有关的系统日志优先级和设施。应用了访问控制策略中的入侵策略后，如果检测到入侵事件，系统会发送系统日志警报给策略中指定的本地主机或日志记录主机上的系统日志设施。接收警报的主机会采用配置系统日志警报分类时设置的设施和优先级信息。

下表列出了在配置系统日志警报时可选择的设施。务必要根据所用远程系统日志服务器的配置情况来合理配置设施。远程系统中的 `syslog.conf` 文件（如果将系统日志消息记录到基于 UNIX 或 Linux 的系统）指示哪些设施保存在服务器的哪些日志文件中。

表 28-3　　可选用的系统日志设施

设施	说明
AUTH	与安全和授权相关的消息。
AUTHPRIV	与安全和授权相关的访问限制消息。很多系统会将这些消息转发到一个安全的文件中。
CRON	时钟后台守护程序生成的消息。
DAEMON	系统后台守护程序生成的消息。
FTP	FTP 后台守护程序生成的消息。
KERN	内核生成的消息。很多系统会在这些消息出现后将其传送至控制台打印。
LOCAL0-LOCAL7	内部进程生成的消息。
LPR	打印子系统生成的消息。
MAIL	邮件系统生成的消息。
新闻	网络新闻子系统生成的消息。
SYSLOG	系统日志后台守护程序生成的消息。
用户	用户级进程生成的消息。
UUCP	UUCP 子系统生成的消息。

选择以下标准系统日志优先级之一，显示在该警报生成的所有通知中：

表 28-4　　系统日志优先级

功率水平	说明
EMERG	紧急状况，向所有用户广播
ALERT	需要立即更正的状况
CRIT	严重的状况
ERR	错误状况
警告	警告消息
请注意！	并未出现错误，但需引起注意的状况
INFO	参考消息
DEBUG	包含调试信息的消息

有关系统日志工作方式和配置方法的详细信息，请参阅系统随附的文档。如果您在基于 UNIX 或 Linux 的系统日志中记录数据，`syslog.conf` man 文件（在命令行键入 `man syslog.con`）和系统日志 man 文件（在命令行键入 `man syslog`）提供有关系统日志工作方式和配置方法的信息。

配置系统日志响应

许可证：保护

您可以配置入侵策略中的系统日志警报。应用访问控制策略中的入侵策略后，一旦系统检测到任何入侵事件，就会通过系统日志发送通知。有关系统日志警报的详细信息，请参阅第 28-4 页上的使用系统日志响应。

要配置系统日志警报选项，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy**。

系统将显示 Intrusion Policy 页面。

步骤 2　点击要编辑的策略旁边的编辑图标 ( )。

如果在另一策略中的更改尚未保存，请点击 **OK** 放弃这些更改并继续操作。有关保存其他策略中尚未保存的更改的详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

系统将显示 Policy Information 页面。

步骤 3　点击左侧导航面板中的 **Advanced Settings**。

系统将显示 Advanced Settings 页面。

步骤 4　根据 External Responses 中 **Syslog Alerting** 的启用情况，您有两种选择：

- 如果该配置已启用，请点击 **Edit**。
- 如果该配置已禁用，请点击 **Enabled**，然后点击 **Edit**。

系统将显示 Syslog Alerting 页面。

页面底部消息会识别包含配置的入侵策略层。有关详情，请参见第 12-1 页上的在网络分析或入侵策略中使用层。

步骤 5　或者，在 **Logging Hosts** 字段中输入想要指定为日志记录主机的远程访问 IP 地址。用逗号分隔多个主机。

步骤 6　从下拉列表中选择设施和优先级。

有关设施和优先级选项的详细信息，请参阅第 28-4 页上的使用系统日志响应。

步骤 7　保存策略、继续编辑、放弃更改、恢复基本策略中的默认配置设置，或在系统缓存中保留变更后退出。有关详情，请参见第 11-12 页上的解决冲突和提交策略更改。

使用控制 ASA FirePOWER 面板控制面板

ASA FirePOWER 模块控制面板为您提供当前系统状态的概览。每个选项卡在三栏布局中显示构件。这些构件是较小的独立组件，可提供对 ASA FirePOWER 模块不同方面的洞察。您的系统附有多个预定义构件。例如， Appliance Information 构件为您提供设备名称、型号、以及当前运行的 ASA FirePOWER 模块软件版本。

该控制面板上有限制其构件的时间范围。您可以更改时间范围，以反映短至前一小时，或长至前一年的时间段里的信息。

每设备均附有默认控制面板，名为 Summary Dashboard。该控制面板可为临时用户提供常规 您的 ASA FirePOWER 模块部署的系统状态信息。

有关内容的详细信息，请参阅：

- 第 29-1 页上的了解控制面板构件
- 第 29-2 页上的了解预定义构件
- 第 29-5 页上的使用控制面板控制

了解控制面板构件

许可证： 任何环境

该控制板在三栏布局中显示多个构件。 ASA FirePOWER 模块附有多个预定义的控制板构件，每个构件均提供对 FireSIGHT 统不同方面的洞察。您可以将构件最小化和最大化，以及重新排列构件。

有关详情，请参阅：

- 第 29-2 页上的了解构件首选项
- 第 29-2 页上的了解预定义构件
- 第 29-5 页上的使用控制面板控制

了解构件首选项

许可证： 任何环境

每个构件都有一组可确定其行为的首选项。

构件首选项可以很简单。例如，您可设置 Current Interface Status 构件的首选项，该构件显示内部网络中所有已启用接口的当前状态。您只能配置此构件的更新频率。

要修改构件的首选项，请执行以下操作：

步骤 1 在您想要更改首选项的构件标题栏上，点击显示首选项图标 ( )。

系统将显示该构件的首选项部分。

步骤 2 根据需要进行更改。

更改会立即生效。有关可为各个构件指定的首选项的详细信息，请参阅第 29-2 页上的了解预定义构件。

步骤 3 在构件标题栏上，点击隐藏首选项图标 ( ) 隐藏首选项部分。

了解预定义构件

许可证： 任何环境

ASA FirePOWER 模块附有多个预定义构件，这些构件可为您提供当前系统状态的概览。

有关 构件的详细信息，请参阅：

了解 Appliance Information 构件

许可证： 任何环境

Appliance Information 构件提供：

- 设备名称、 IPv4 地址、 IPv6 地址和型号
- ASA FirePOWER 模块软件的版本、规则更新、以及。

通过修改构件首选项以显示简单或高级视图，您可以配置构件显示更多或更少信息；首选项还可控制构件的更新频率。有关详细信息，请参阅第 29-2 页上的了解构件首选项。

了解 Current interface Status 构件

许可证： 任何环境

Current Interface Status 构件显示设备上所有接口的状态，已启用或未使用。对于每个接口，该构件都会提供：

- 接口的名称
- 接口的链路状态
- 接口的链路模式（例如，100Mb 全双工或 10Mb 半双工）
- 接口类型，例如，铜或光纤
- 接口接收 (Rx) 和发送 (Tx) 的数据量

代表链路状态的球的颜色指明当前状态，如下所示：

- 绿色：链路正常并且全速运行
- 黄色：链路正常，但未全速运行
- 红色：链路不正常
- 灰色：链路通过管理方式禁用
- 蓝色：链路状态信息不可用（例如，ASA）

构件首选项可控制构件的更新频率。有关详细信息，请参阅第 29-2 页上的了解构件首选项。

了解 Disk Usage 构件

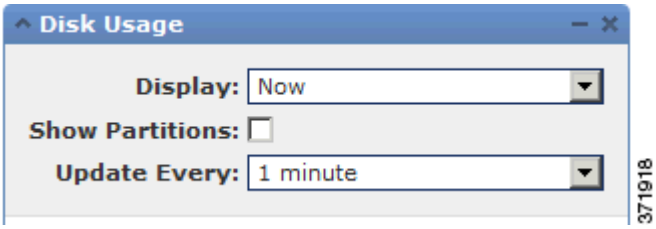
许可证： 任何环境

根据磁盘使用情况类别， Disk Usage 构件显示硬盘驱动器上已使用的空间。它还会显示设备硬盘驱动器每个分区已使用的空间和容量。By Category 堆积条形图显示每个磁盘使用情况类别在使用的总可用磁盘空间中的比例。下表列出了可用的类别。

表 29-1　　磁盘使用情况类别

磁盘使用情况类别	说明
活动	系统记录的所有事件
文件	系统存储的所有文件
备用	所有备份文件
更新	与更新相关的所有文件，例如规则更新和系统更新
其他	系统故障排除文件和其他文件
免费	设备上剩余的可用空间

如果您安装了恶意软件存储包，您可以通过修改构件首选项配置构件仅显示 By Category 堆积条形图和管理员 (`/`)、 `/Volume`、 `/boot`分区使用情况，以及`/var/storage`分区。



构件首选项还可以控制构件的更新频率，及其显示的是当前磁盘使用情况还是控制面板时间范围内收集的磁盘使用情况统计数据。有关详细信息，请参阅第 29-2 页上的了解构件首选项。

了解 Product Licensing 构件

许可证： 任何环境

Product Licensing 构件显示当前上的设备和功能许可证。它还可显示获得许可证的项目（例如，主机或用户）数量及允许保留许可证的项目数量。

构件的顶部显示上安装的所有设备和功能许可证，包括临时许可证，而 Expiring Licenses 部分仅显示临时且已到期的许可证。

构件背景中的长条显示正在使用的各种许可证的比例；您应该从右到左阅读这些长条。已到期许可证标标记有一条删除线。

您可以通过修改构件首选项配置构件显示所有当前许可的功能，或者您可许可的所有功能。首选项还可控制构件的更新频率。有关详细信息，请参阅第 29-2 页上的了解构件首选项。

您可以点击任何一种许可证类型发往本地配置的 License 页面并添加或删除功能许可证。有关详细信息，请参阅第 34-1 页上的许可 ASA FirePOWER 模块。

了解 Product Updates 构件

许可证： 任何环境

Product Updates 构件为您提供当前安装在设备上的软件 （ASA FirePOWER 模块软件和规则更新）的摘要以及有关您已经为该软件下载但未安装的可用更新的信息。

请注意，除非您已经配置定期下载、推送或安装软件更新的任务，否则构件会在软件最新版本一项显示 `Unknown`；该构件会使用定期任务确定最新版本。有关详细信息，请参阅第 31-1 页上的安排任务。

该构件还为您提供软件更新网页的链接

通过修改构件首选项，您可以配置构件以隐藏最新版本。首选项还可控制构件的更新频率。有关详细信息，请参阅第 29-2 页上的了解构件首选项。

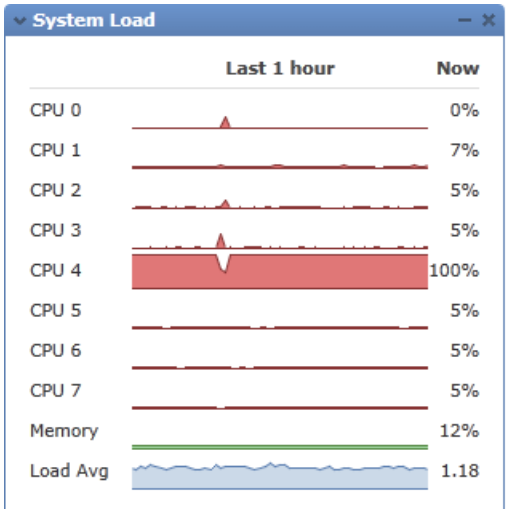
在 Product Updates 构件，您可以：

- 点击当前版本的 FireSIGHTASA FirePOWER 模块软件、规则更新、或地理定位更新，以手动更新设备：
- 要更新系统软件、或地理定位数据库，请参阅第 35-1 页上的更新 ASA FirePOWER 模块软件。
- 要导入最新的规则更新，请参阅第 35-8 页上的导入规则更新和本地规则文件。
- 点击，创建一个预定任务以下载最新版本的 ASA FirePOWER 模块软件 或规则更新；请参阅第 31-1 页上的安排任务。

了解 System Load 构件

许可证： 任何环境

System Load 构件可显示设备当前及控制面板时间范围内的（每个 CPU）CPU 使用率、内存 (RAM) 使用情况和系统负载（又称为平均负载，通过等待运行的进程数量衡量）。

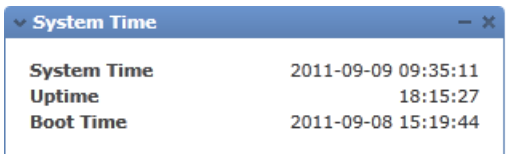


您可以通过修改构件首选项以配置构件显示或隐藏平均负载。首选项还可控制构件的更新频率。有关详细信息，请参阅第 29-2 页上的了解构件首选项。

了解 System Time 构件

许可证： 任何环境

System Time 构件可显示本地系统时间、正常运行时间和设备启动时间。



通过修改构件首选项，您可以配置构件以隐藏启动时间。首选项还会控制构件与设备的时钟同步的频率。有关详细信息，请参阅第 29-2 页上的了解构件首选项。

使用控制面板控制

许可证： 任何环境

您可以查看和修改显示在控制面板中的构件。

有关使用控制面板的详细信息，请参阅：

- 第 29-6 页上的查看控制面板
- 第 29-6 页上的修改控制面板
- 第 B-1 页上的导出配置

查看控制面板

许可证： 任何环境

在任何时，要查看您为 ASA FirePOWER 模块控制面板，请选择 **Home > ASA FirePOWER Dashboard**。

该控制面板上有限制其构件的时间范围。您可以更改时间范围以反映短至前一小时（默认），或长至前一年的时间周期信息。当您更改时间范围时，可按时间限制构件自动更新以反映新的时间范围。

请注意，并非所有的构件都可受时间限制。例如，控制面板时间范围对 Appliance Information 构件无影响，该构件可提供包括设备名称、型号和 当前版本的 ASA FirePOWER 模块软件 的信息。

要查控制面板，请执行以下操作：

步骤 1　选择 **Home > ASA FirePOWER Dashboard**。

系统将显示所选择的 ASA FirePOWER 控制面板

要更改控制面板时间范围，请执行以下操作：

步骤 1　从 **Show the Last** 下拉列表中，选择控制面板时间范围。

页面上的所有适当构件均将更新以反映新的时间范围。

修改控制面板

许可证： 任何环境

该控制面板在三栏布局中显示构件。您可以将构件最小化和最大化，，以及重新排列构件。

有关详细信息，请参阅：

- 第 29-6 页上的重新排列构件
- 第 29-6 页上的最小化和最大化构件

重新排列构件

许可证： 任何环境

您可以更改任何构件在选项卡上的位置

要移动构件，请执行以下操作：

步骤 1　点击您想要移动的标题栏，然后将其拖到新位置。

最小化和最大化构件

许可证： 任何环境

您可以将构件最小化以简化视图，然后在想再次看到时将其最大化。

要最小化构件，请执行以下操作：

步骤 1　在构件标题栏上点击最小化图标 (−)。

要最大化构件，请执行以下操作：

步骤 1　在最小化后的构件标题栏上点击最大化图标 (□)。

使用 ASA FirePOWER 报告

您可以通过查看多个时间段的报告来分析网络流量。报告汇总了您的网络流量的各个方面的信息。在大多数情况下，您可以从一般信息深入了解具体信息。例如，您可以查看一份有关所有用户的报告，然后查看有关特定用户的详细信息。

概述和详细信息报告包括多个报告组件（例如热门策略和网络分类）。这些报告显示您在查看的报告类型的最常见项目。例如，如果您查看特定用户的详细信息报告，则热门策略显示与该用户相关的命中率最高的策略。

有关详情，请参阅：

了解可用报告

许可证：任何环境

可用报告包括 ASA FirePOWER 模块中可用的主报告。可以从 ASA FirePOWER Reporting 菜单中查看这些报告。

一般来说，您可以单击许多项目，包括名称和 View More 链接，获得有关个别项目或整个受监控类别的详细信息。

Network Overview

此报告显示有关网络流量的摘要信息。使用此信息来帮助确定需要更深入分析的方面，或确认网络按一般预期正常运行。

Users

此报告显示您的网络的热门用户。使用此信息可帮助识别用户的异常活动。

提示 只有当用户身份信息与流量关联时，用户名才可用。如果要确保用户身份在报告中可用于大多数流量，访问控制策略应使用活动身份验证。

Applications

此报告显示应用，代表在流量中检测到的触发入侵事件的内容或 HTTP 流量的请求的 URL。请注意，如果模块检测到 HTTP 应用协议，但无法检测到特定网络应用，模块会在此处提供通用的网络浏览应用。

Web categories

此报告根据访问的网站分类显示网络中使用的网站分类，例如，赌博、广告、搜索引擎和门户网站。使用此信息可帮助识别用户访问的热门类别并确定您的访问控制策略是否能够充分阻止不需要的类别。

Policies

此报告显示您的访问控制策略如何应用于网络中的流量。使用此信息来帮助评估策略效果。

Ingress zones

此报告显示触发事件的数据包的入口安全区域。

Egress zones

此报告显示触发事件的数据包的出口安全区域。

Destinations

此报告根据对网络流量的分析显示在网络中使用的应用（如 Facebook）。使用此信息可帮助识别网络中使用的热门应用并确定是否需要其他访问控制策略以减少不需要的应用的使用。

Attackers

此报告显示触发事件的发送主机所用的源 IP 地址。

Targets

此报告显示触发事件的接收主机所用的目标 IP 地址。

Threats

此报告显示已分配给检测到的每个网络威胁的唯一标识号和说明文本。

Files logs

此报告显示检测到的文件的类型，例如， HTML 或 MSEXE。

报告基本知识

许可证：任何环境

以下各节说明了如何使用报告的基本知识。这些主题总体上适用于所有报告而非任何单份特定报告。

有关详情，请参阅：

- 第 30-3 页上的了解报告数据
- 第 30-3 页上的深入了解报告
- 第 30-3 页上的更改报告时间范围
- 第 30-4 页上的控制报告中显示的数据
- 第 30-4 页上的了解报告列

了解报告数据

许可证：任何环境

报告数据立即从设备收集，因此，报告中反映的数据与网络活动之间几乎无滞后时间。但是，在分析数据时请记住以下要点：

- 仅针对与应用于您的 ASA FirePOWER 模块的访问控制策略相匹配的流量收集数据。
- 数据聚合到 5 分钟时段，30 分钟和一小时的图形以 5 分钟增量显示数据点。在小时结束时，5 分钟时段聚合到一小时时段，一小时时段随后聚合到天和星期时段。 5 分钟时段保留 7 天，一小时时段保留 31 天，天时段最多可保留 365 天。越往前查找，数据聚合的时间范围就越长。当您查询旧数据时，如果您根据这些数据时段的可用性来调整查询，您将获得最佳结果。

注　如果数据点丢失，例如，因为设备无法访问超过 5 分钟，线状图中会出现间断。

深入了解报告

许可证：任何环境

报告包括许多链接来帮助您深入了解所需的信息。将鼠标光标悬停在项目上，即可查看哪条链接可引导您查看关于该项目的详细信息。

例如，在一个典型的报告项目中，您可以点击 View More 链接转至该项目的摘要报告。

您还可以查看特定项目的详细报告，只需在摘要报告中点击该项目。例如，点击应用摘要报告中的超文本传输协议 (HTTP) 即可转至 HTTP 的应用详细报告。

更改报告时间范围

许可证：任何环境

查看报告时，可使用 Time Range 列表更改定义要包括在报告中的信息的时间范围。时间范围列表显示在每份报告顶部，可供您选择预定义的时间范围，例如，上个小时或上个星期，或定义具有特定开始和结束时间的自定义时间范围。您选择的时间范围将用于您查看的所有其他报告，直到您更改选择。

报告每 10 分钟自动更新。

下表说明了时间范围选项。

表 30-1　报告的时间范围

时间范围	过多长时间才返加数据
上 30 分钟	完整的 30 分钟，以五分钟为间隔，外加最多五分钟额外时间。
上一小时	完整的 60 分钟，以五分钟为间隔，外加最多五分钟额外时间。
上 24 个小时	上 24 小时，以一小时为间隔，四舍五入到上个小时边界。例如，如果当前时间是 13:45，上 24 小时是从昨天 13:00 到今天 13:00。
过去 7 天	过去七天，以一小时为间隔，四舍五入到上个小时边界。
过去 30 天	过去 30 天，以一天为间隔，从上个午夜开始。
自定义范围	您定义的时间范围。系统显示开始日期、开始时间、截止日期和结束时间的编辑框；请点击每个框并选择所需的值。完成后，点击 **Apply** 更新报告。 在构建自定义时间范围时，您应根据数据时段的可用性调整您的时间范围。对于过去 7 - 31 天内的范围，请以小时为单位调整您的查询。对于更早的范围，请以天为单位调整查询数据范围；对于超过一年的范围，请以星期为单位调整查询数据范围。

控制报告中显示的数据

许可证：任何环境

概述和详细信息报告包括多个从属报告（例如热门策略和网络分类）。每个报告面板均包括可供您查看数据的不同方面的控件。您可以使用以下控件：

Transactions or Data Usage

点击这些链接查看基于事务数或事务中的数据量的图表。

All, Denied, Allowed

每份报告右上角的未标记的下拉列表均包括这些选项。使用这些选项来更改您是要查看仅已拒绝连接，仅已允许连接，还是包括拒绝或允许的所有连接。

View More

点击 View More 链接可转至您在查看的项目的报告。例如，点击 Destinations 报告的 Web Categories 图表中的 **View More**，即可转至 Web Categories 报告。如果您在查看详细报告中的报告，将转至您正在查看其详细信息的项目的详细 Web Categories 报告。

了解报告列

许可证：任何环境

除了以图形格式显示信息，报告通常还包含一个或多个用于展示信息的表。

- 许多列的含义根据包含它们的报告而进行修改。例如，事务列显示报告的项目类型的事务数量。还可以点击 **Values** 或 **Percentages** 来切换显示的原始值或报告项目的原始值总计的百分比。
- 点击列标题，即可更改各列的排序顺序。

下表说明了可在各种报告中找到的标准列。

表 30-2　报告列

列	说明
Transactions	报告的项目的事务总数。
Transactions allowed	允许用于已报告项目的事务数。
Transactions denied	被阻止（根据策略）用于已报告项目的事务数。
Total bytes	为已报告项目发送和接收的总字节数。
Bytes received	为已报告项目接收的字节数。
Total Bytes Sent	为已报告项目发送的字节数。

安排任务

可安排许多不同类型的管理任务在指定时间运行一次或反复运行。

注 有些任务 （例如，那些涉及自动化软件更新的任务，）可能会显著增加低带宽网络的负载。应安排此类任务在网络使用量较低的时段运行。

有关详细信息，请参阅：

- 第 31-1 页上的配置周期性任务解释如何设置预定任务，使其按固定时间间隔运行。
- 第 31-2 页上的自动运行备份作业提供备份作业的安排步骤。
- 第 31-3 页上的自动执行证书撤销列表下载提供设备证书撤销列表 (CRL) 的自动刷新步骤。
- 第 31-4 页上的自动应用入侵策略提供应用于的入侵策略的排队步骤。
- 第 31-5 页上的自动运行地理定位数据库更新提供地理定位数据库 (GeoDB) 自动更新的安排步骤。
- 第 31-6 页上的自动执行软件更新提供软件更新下载、推送和安装的安排步骤。
- 第 31-8 页上的自动更新 URL 过滤提供 URL 过滤数据的自动更新步骤。
- 第 31-9 页上的查看任务描述如何在安排任务之后进行查看和管理。
- 第 31-10 页上的编辑预定任务描述如何编辑现有任务。
- 第 31-11 页上的删除预定任务描述如何删除一次性任务和周期性任务的所有实例。

配置周期性任务

许可证：任何环境

使用相同流程为所有类型的任务设置周期性任务的频率。

请注意，用户界面上大多数页面中显示的时间为本地时间，由您在本地配置中指定的时区决定。此外，在适当时候， ASA FirePOWER 模块自动针对夏时令 (DST) 调整其本地时间显示。然而，跨越从 DST 到标准时间以及从标准时间到 DST 的过渡日期的周期性任务不因过渡而自行调整。也就是说，如果创建一个任务，预定在标准时间的凌晨 2:00 运行，则它将在 DST 期间的凌晨 3:00 运行。同样，如果创建一个任务，预定在 DST 期间的凌晨 2:00 运行，则它将在标准时间的凌晨 1:00 运行。

要配置周期性任务，请执行以下操作：

步骤 1　在 ASDM 中选择 **Configuration > ASA FirePOWER Configuration > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表中，选择想安排的任务类型。

可安排的每种任务类型均在其各自的部分有详细说明。

步骤 4　对于 **Schedule task to run** 选项，请选择 **Recurring**。

页面重新加载周期性任务选项。

步骤 5　在 **Start On** 字段中，指定想要开始周期性任务的日期。可使用下拉列表选择年、月、日。

步骤 6　在 **Repeat Every** 字段中，指定想要任务重复的频率。可指定小时数、天数、周数或月数。

提示　可键入数字，或者点击向上图标 (▲) 和向下图标 (▼) 指定时间间隔。例如，键入 2，选择 Days，让任务每两天运行一次。

步骤 7　在 **Run At** 字段中，指定想要开始周期性任务的时间。

步骤 8　如果已为 `Repeat Every` 选择 **Weeks**，则显示 **Repeat On** 字段。选择想要运行任务的一星期中天数旁边的复选框。

步骤 9　如果已为 `Repeat Every` 选择 **Months**，则显示 **Repeat On** 字段。使用下拉列表，选择想要运行任务的日期。

New Task 页面上的剩余选项取决于正在创建的任务。有关详细信息，请参阅：

- 第 31-2 页上的自动运行备份作业
- 第 31-3 页上的自动执行证书撤销列表下载
- 第 31-4 页上的自动应用入侵策略
- 第 31-6 页上的自动执行软件更新
- 第 31-8 页上的自动更新 URL 过滤

自动运行备份作业

可以使用调度程序自动化您的 ASA FirePOWER 模块的备份。必须先设计一个备份配置文件，然后才能将备份配置为预定任务。有关详细信息，请参阅第 37-3 页上的创建备份配置文件。

要自动运行备份任务，请执行以下操作：

步骤 1　在 ASDM 中选择 **Configuration > ASA FirePOWER Configuration > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表中，选择 **Backup**。

页面重新加载，显示备份选项。

步骤 4　指定您想如何安排备份， **Once** 或 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明设备上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 31-1 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　从 **Backup Profile** 列表中，选择相应的备份配置文件。

有关新建备份配置文件的详细信息，请参阅第 37-3 页上的创建备份配置文件。

步骤 7　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 8　或者，在 **Email Status To:** 字段中，键入要用于发送任务状态消息的邮件地址（或多个邮件地址，用逗号隔开）。

必须配置一台有效的邮件中继服务器以发送状态消息。有关配置中继主机的详细信息，请参阅第 32-6 页上的配置邮件中继主机和通知地址。

步骤 9　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动执行证书撤销列表下载

可使用调度程序，在启用用户证书的设备上，自动刷新设备网络服务器的证书撤销列表 (CRL)。在本地设备配置中启用 CRL 提取时自动创建 Download CRL 任务在，因此，此流程解释如何打开预定任务以设置频率。

提示　必须启用并配置用户证书，设置 CRL 下载 URL，然后才能安排任务。有关配置用户证书的信息，请参阅第 33-5 页上的要求用户证书。

要自动下载证书撤销列表，请执行以下操作：

步骤 1　在 ASDM 中选择 **Configuration > ASA FirePOWER Configuration > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　在 Task Details 中找到 **download CRL** 任务，点击编辑图标 ( )。

系统将显示 Edit Task 页面，其中显示了下载选项。

步骤 3　指定想要如何安排 CRL 下载， **Once** 或 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明设备上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 31-1 页上的配置周期性任务。

步骤 4　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 5　或者，在 **Email Status To:** 字段中，键入要用于发送任务状态消息的邮件地址（或多个邮件地址，用逗号隔开）。

必须在ASA FirePOWER 模块上配置一台有效的邮件中继服务器，以发送状态消息。有关配置中继主机的详细信息，请参阅第 32-6 页上的配置邮件中继主机和通知地址。

步骤 6　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动应用入侵策略

许可证：保护

可对应用于 ASA FirePOWER 模块的入侵策略进行排队。在任务运行时，如果引用入侵策略的访问控制策略应用于 ASA FirePOWER 模块，则此任务仅应用入侵策略。否则，任务未完成就会中止。

安排此任务之前，必须将入侵策略与访问控制策略相关联，并向设备应用访问控制策略；请参阅第 10-1 页上的使用入侵和文件策略控制流量。

要对的策略进行排队，请执行以下操作：

步骤 1　在 ASDM 中选择 **Configuration > ASA FirePOWER Configuration > Tools > Scheduling**。

系统将显示当前月份的安排日历页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表中，选择 **Queue Intrusion Policy Apply**。

系统将重新加载页面，显示用于对策略应用进行排队的选项。

步骤 4　指定想要如何安排任务， **Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明ASA FirePOWER 模块上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 31-1 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　在 **Intrusion Policy** 字段中，可进行以下选择：

- 选择要应用于 ASA FirePOWER 模块的一项入侵策略。
- 选择 **All intrusion policies**，将所有已应用的入侵策略应用于 字段 ASA FirePOWER 模块中选定的设备。

步骤 7　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段出现在安排日历页面底部的 Tasks Details 部分，因此，应限制注释的长短。

步骤 8　或者，在 **Email Status To:** 字段中，键入要用于发送任务状态消息的邮件地址（或多个邮件地址，用逗号隔开）。

必须配置有效的邮件中继服务器，才能发送状态消息。有关配置中继主机的详细信息，请参阅第 32-6 页上的配置邮件中继主机和通知地址。

步骤 9　点击 **Save**。

任务添加成功。在日历页面的 Task Details 部分，可查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

步骤 10　要编辑已保存的任务，请在任务出现在安排日历页面上的任何位置点击任务。

Task Details 部分出现在页面底部。要做出任何更改，请点击编辑图标 ( )。

自动运行地理定位数据库更新

许可证：任意环境

可使用调度程序，自动运行周期性地理定位数据库 (GeoDB) 更新。周期性 GeoDB 更新每 7 天（每周）运行一次；可配置每周更新运行时间。有关 GeoDB 更新的详细信息，请参阅第 35-17 页上的更新地理定位数据库。

要自动运行地理定位数据库更新，请执行以下操作：

步骤 1　在 ASDM 中，择 **Configuration > ASA FirePOWER Configuration > Updates**。

系统将显示 Product Updates 页面。

步骤 2　点击 **Geolocation Updates** 选项卡。

系统将显示 Geolocation Updates 页面。

步骤 3　在 **Recurring Geolocation Updates** 下方，选择 **Enable Recurring Weekly Updates** 复选框。

系统将显示 Update Start Time 字段。

步骤 4　在 **Update Start Time** 字段中，指定想要每周 GeoDB 更新运行的周日和时间。

步骤 5　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动执行软件更新

可自动下载大多数修补程序和主要版本，并将其应用到 ASA FirePOWER 模块。

注　在两种情况下，必须手动上传和安装更新。第一，无法安排 ASA FirePOWER 模块的主要更新。第二，无法为不能访问支持网站的设备安排更新，或者无法安排来自这些设备的推送。有关手动更新 ASA FirePOWER 模块的信息，请参阅第 35-1 页上的更新 ASA FirePOWER 模块软件。

如果想要加大对此过程的控制，可在得知更新已发布之后，在非高峰时段使用 **Once** 选项下载和安装更新。

有关详细信息，请参阅：

- 第 31-6 页上的自动下载软件
- 第 31-7 页上的自动安装软件

自动下载软件

可创建一个预定任务，自动从思科下载最新软件更新。可使用此任务安排下载计划手动安装的更新。

要自动下载软件更新，请执行以下操作：

步骤 1　在 ASDM 中选择 **Configuration > ASA FirePOWER Configuration > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表，选择 **Download Latest Update**。

系统重新加载 New Task 页面，显示更新选项。

步骤 4　指定想要如何安排任务， **Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明设备上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 31-1 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　在 **Update Items** 部分，选择 **Software**。

步骤 7　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 8　或者，在 **Email Status To:** 字段中，键入要用于发送任务状态消息的邮件地址（或多个邮件地址，用逗号隔开）。

必须配置有效的邮件中继服务器，才能发送状态消息。有关配置中继主机的详细信息，请参阅第 32-6 页上的配置邮件中继主机和通知地址。

步骤 9　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动安装软件

注意事项　视乎正在安装的更新，设备可能在安装软件之后重新启动。

要安排软件安装任务，请执行以下操作：

步骤 1　在 ASDM 中选择 **Configuration > ASA FirePOWER Configuration > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表，选择 **Install Latest Update**。

系统重新加载页面，显示用于安装更新的选项。

步骤 4　指定想要如何安排任务， **Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明设备上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 31-1 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 7　或者，在 **Email Status To:** 字段中，键入要用于发送任务状态消息的邮件地址（或多个邮件地址，用逗号隔开）。

必须配置有效的邮件中继服务器，才能发送状态消息。有关配置中继主机的详细信息，请参阅第 32-6 页上的配置邮件中继主机和通知地址。

步骤 8　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

自动更新 URL 过滤

许可证：URL 过滤

可使用调度程序，自动从综合安全情报云更新 URL 过滤数据。要成功完成 URL 过滤更新任务：

- ASA FirePOWER 模块必须能够访问互联网，否则无法连接云。
- 必须启用 URL 过滤，如第 33-6 页上的启用云通信中所述。

请注意，启用 URL 过滤时，也可启用自动更新。这会强制ASA FirePOWER 模块每 30 分钟连接一次云，获取 URL 过滤数据更新。如已启用自动更新，则不应创建预定任务以更新 URL 过滤数据。

虽然每日更新通常是小量更新，但是，如果距离上一次更新超过五天，新的 URL 过滤数据最多可能需要 20 分钟才能下载完（具体取决于带宽）。然后，执行更新也可能最多需要 30 分钟。

要自动运行 URL 过滤数据任务，请执行以下操作：

步骤 1　在 ASDM 中选择 **Configuration > ASA FirePOWER Configuration > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击 **Add Task**。

系统将显示 New Task 页面。

步骤 3　从 **Job Type** 列表，选择 **Update URL Filtering Database**。

页面重新加载，显示 URL 过滤更新选项。

步骤 4　指定想要如何安排更新， **Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。 **Current Time** 字段指明设备上的当前时间。
- 对于周期性任务，可使用多个选项设置任务实例之间的时间间隔。有关详细信息，请参阅第 31-1 页上的配置周期性任务。

步骤 5　在 **Job Name** 字段中，键入一个名称，最多不超过 255 个字母数字字符、空格或连接号。

步骤 6　或者，在 **Comment** 字段中，键入注释，最多不超过 255 个字母数字字符、空格或句号。

提示　Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 7　或者，在 **Email Status To** 字段中，键入要用于发送任务状态消息的邮件地址（或多个邮件地址，用逗号隔开）。

必须配置有效的邮件中继服务器，才能发送状态消息。有关配置中继主机的详细信息，请参阅第 32-6 页上的配置邮件中继主机和通知地址。

步骤 8　点击 **Save**。

任务添加成功。可在 Task Status 页面上查看正在运行的任务的状态；请参阅第 C-1 页上的查看长时间运行任务的状态。

查看任务

添加预定任务后，即可查看这些任务，评估它们的状态。在页面的 View Options 部分，查使用日历和预定任务列表查看预定任务。

有关详细信息，请参阅：

- 第 31-9 页上的使用日历
- 第 31-9 页上的使用任务列表

使用日历

Calendar 视图选项可用于查看哪些预定任务在哪天发生。

要使用日历查看预定任务，请执行以下操作：

步骤 1　在 ASDM 中选择 **Configuration > ASA FirePOWER Configuration > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　可使用日历视图执行以下任务：

- 点击左向双箭头图标 (<<)，向后移动一年：
- 点击左向单箭头图标 (<)，向后移动一个月。
- 点击右向单箭头图标 (>)，向前移动一个月。
- 点击右向双箭头图标 (>>)，向前移动一年。
- 点击 **Today**，返回当前月份和年份。
- 点击 **Add Task**，安排新任务。
- 点击一个日期，在日历下方的任务列表中查看所有预定任务的特定日期。
- 点击在某个日期发生的特定任务，在日历下方的任务列表中查看此任务。

注　有关使用任务列表的详细信息，请参阅使用任务列表。

使用任务列表

Task List 显示一列任务及其状态。打开日历时，任务列表出现在日历下方。此外，从日历中选择日期或任务，也可访问列任务列表。有关详情，请参见第 31-9 页上的使用日历。

表 31-1　　任务列表列

列	说明
字段名称	显示预定任务的名称及与其关联的注释。
类型	显示预定任务的类型。
开始时间	显示预定任务的开始日期和时间。

表 31-1　任务列表列（续）

列	说明
频率	显示任务的运行频率。
状态	描述预定任务的当前状态。 • 对号图标 ( ) 指明任务已成功运行。 • 问号图标 ( ) 指明任务处于未知状态。 • 感叹号图标 ( ) 指明任务已失败。
创建者	显示创建预定任务的用户的名称。
编辑	编辑预定任务。
删除	删除预定任务。

编辑预定任务

可编辑先前创建的预定任务。如果想要测试一次预定任务，确保参数正确，此功能特别有用。稍后，任务成功完成后，即可将其更改为周期性任务。

要编辑现有预定任务，请执行以下操作：

步骤 1　选择 **System > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击要编辑的任务，或者任务出现的日期。

系统将显示 Task Details 表，其中包含选定的一项或多项任务。

步骤 3　在表中找到要编辑的任务，点击编辑图标 ( )

系统将显示 Edit Task 页面，其中显示选定任务的详细信息。

步骤 4　根据自己的需求编辑任务，包括开始时间、作业名称、注释以及任务运行频率，一次或反复。不能更改作业类型。

剩余选项取决于正在编辑的任务。有关详细信息，请参阅：

- 第 31-2 页上的自动运行备份作业
- 第 31-3 页上的自动执行证书撤销列表下载
- 第 31-6 页上的自动执行软件更新
- 第 31-8 页上的自动更新 URL 过滤

步骤 5　点击 **Save**，保存编辑。

更改保存成功，再次显示 Scheduling 页面。

删除预定任务

可从 Schedule View 页面执行两类删除。可删除尚未运行的特定一次性任务，也可删除周期性任务的每个实例。如果删除周期性任务的一个实例，该任务的所有实例均将删除。如果删除预定运行一次的任务，则仅删除该任务。

以下各节描述如何删除任务：

- 要删除任务的所有实例，请参阅第 31-11 页上的删除周期性任务。
- 要删除任务的单个实例，请参阅第 31-11 页上的删除一次性任务。

删除周期性任务

删除周期性任务的一个实例时，将自动删除该任务的所有实例。

要删除周期性任务，请执行以下操作：

步骤 1　在 ASDM 中选择 **Configuration > ASA FirePOWER Configuration > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　在日历上，选择要删除的周期性任务的实例。

页面重新加载，在日历下方显示任务表。

步骤 3　在表中找到要删除的周期性任务的实例，点击删除图标 ( )。

该周期性任务的所有实例均将删除。

删除一次性任务

可使用任务列表删除预定的一次性任务，或删除以前运行过的预定任务的记录。

要删除单项任务，或者如果其已运行，请删除任务记录：

步骤 1　在 ASDM 中选择 **Configuration > ASA FirePOWER Configuration > Tools > Scheduling**。

系统将显示 Scheduling 页面。

步骤 2　点击要删除的任务或者任务出现的日期。

系统将显示一个表，其中包含选定的一项或多项任务。

步骤 3　在表中找到要删除的任务，点击删除图标 ( )。

选定任务的实例删除成功。

管理系统策略

系统策略可供您在自己的 ASA FirePOWER 模块上管理以下内容：

- 审核日志设置
- 邮件中继主机和通知地址
- SNMP 轮询设置
- STIG 合规性

有关详细信息，请参阅：

创建系统策略

许可证：任何环境

创建系统策略时，可以为其指定名称和说明。然后，可以配置策略的各个方面，每个方面都在其各自的部分中进行了描述。

不必创建新策略，只需从其他ASA FirePOWER 模块导出系统策略，再将该策略导入到您的ASA FirePOWER 模块。在应用导入的策略前，您可以进行编辑以满足需求。有关详细信息，请参阅第 B-1 页上的导入和导出配置。

要创建系统策略，请执行以下操作：

步骤 1 选择 **Configuration > ASA FirePOWER Configuration > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2 点击 **Create Policy**。

系统将显示 Create Policy 页面。

步骤 3 从下拉列表中，选择现有策略作为新系统策略的模板。

步骤 4 在 **New Policy Name** 字段中，输入新策略的名称。

步骤 5 在 **New Policy Description** 字段中，输入对新策略的描述。

步骤 6　点击**创建**。

即会保存系统策略并显示 Edit System Policy 页面。有关配置系统策略各方面的详细信息，请参阅：

- 第 32-5 页上的配置审核日志
- 第 32-6 页上的配置邮件中继主机和通知地址
- 第 32-7 页上的配置SNMP 轮询
- 第 32-8 页上的启用 STIG 合规性

编辑系统策略

许可证：任何环境

可以编辑现有的系统策略。如果编辑的系统策略当前已应用于某一ASA FirePOWER 模块，请在保存更改后重新应用该策略。有关详细信息，请参阅第 32-3 页上的应用系统策略。

要编辑现有的系统策略，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > System Policy**。

系统将显示 System Policy 页面，其中包含现有系统策略的列表。

步骤 2　点击要编辑的系统策略旁边的编辑图标 ( )。

系统将显示 Edit Policy 页面。可以更改策略名称和策略描述。有关配置系统策略各方面的详细信息，请参阅：

- 第 32-5 页上的配置审核日志
- 第 32-6 页上的配置邮件中继主机和通知地址
- 第 32-7 页上的配置SNMP 轮询
- 第 32-8 页上的启用 STIG 合规性

注　如在编辑的系统策略已应用于某一ASA FirePOWER 模块，请务必在完成编辑后重新应用更新后的策略。请参阅第 32-3 页上的应用系统策略。

步骤 3　点击 **Save Policy and Exit** 保存所做的更改。即会保存更改并显示 System Policy 页面。

应用系统策略

许可证：任何环境

可以将系统策略应用于ASA FirePOWER 模块。对于已应用的系统策略，您做的所有更改只有在重新应用该策略后才会生效。

要应用系统策略，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　点击要应用的系统策略旁边的应用图标 ( )。

步骤 3　点击**应用 (Apply)**。

系统将显示 System Policy 页面。系统会显示一条消息，以指明系统策略的应用状态。

删除系统策略

许可证：任何环境

即使系统策略正在使用中，您也可以将其删除。使用中的策略将会一直使用下去，直至应用新的策略。不能删除默认系统策略。

要删除系统策略，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　点击要删除的系统策略旁边的删除图标 ( )。要删除策略，请点击 **OK**。

系统将显示 System Policy 页面。系统会显示弹出消息，确认策略已删除。

配置系统策略

许可证：任何环境

可以配置多种系统策略设置。有关配置系统策略各方面的详细信息，请参阅：

- 第 32-4 页上的配置设备的访问列表
- 第 32-5 页上的配置审核日志
- 第 32-6 页上的配置邮件中继主机和通知地址
- 第 32-7 页上的配置SNMP 轮询
- 第 32-8 页上的启用 STIG 合规性

配置设备的访问列表

许可证：任何环境

Access List 页允许您控制哪些计算机可在特定端口上访问您的设备。默认情况下，用于访问网络接口的 443 端口（超文本传输安全协议或 HTTPS）和用于访问命令行的 22 端口（安全外壳或 SSH）面向所有 IP 地址启用。也可以添加 161 端口上的 SNMP 访问权限。请注意，对于您计划用于轮询 SNMP 信息的所有计算机，都必须为其添加 SNMP 访问权限。

注意事项　默认情况下，对设备的访问不受限制。要在更安全的环境中使用设备，请考虑为特定的 IP 地址添加对设备的访问权限，然后删除默认的 `any` 选项。

访问列表是系统策略的一部分。可以通过创建新的系统策略或编辑现有的系统策略来指定访问列表。无论采用何种方式，访问列表仅在您应用系统策略后才会生效。

请注意，访问列表不会同时控制外部数据库的访问权限。有关外部数据库访问列表的详细信息，请参阅第 33-6 页上的启用云通信。

要配置访问列表，请执行以下操作：

访问：管理

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的访问列表，请点击系统策略旁边的编辑图标 ( )。
- 要将访问列表配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 32-1 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

无论执行哪一种操作，系统都会显示 Access List 页面。

步骤 3　或者，要删除某一当前设置，请点击删除图标 ( )。

即会删除设置。

注意事项　对于您目前用来连接到设备接口的 IP 地址，如果您删除了它的访问权限，而且无“`IP=any port=443`”这一条目，那么当您应用该策略时，您将失去对系统的访问权限。

步骤 4　或者，要添加对一个或多个 IP 地址的访问权限，请点击 **Add Rules**。

系统将显示 Add IP Address 页面。

步骤 5　在 **IP Address** 字段中，可根据要添加的 IP 地址从以下选项中进行选择：

- 确切的 IP 地址（例如 192.168.1.101）
- 使用 CIDR 表示法的 IP 地址块（例如 192.168.1.1/24）

  有关在 FireSIGHT 系统中使用 CIDR 的信息，请参阅第 1-3 页上的IP 地址约定。
- `any`，指定任意 IP 地址

步骤 6　选择 **SSH**、**HTTPS**、**SNMP** 或它们的组合，以指定要为这些 IP 地址启用哪些端口。

步骤 7　点击**添加**。

系统再次显示 Access List 页面，其中反映出您所做的更改。

步骤 8　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详情，请参见第 32-3 页上的应用系统策略。

配置审核日志

许可证：任何环境

可以配置系统策略，以使ASA FirePOWER 模块将审核日志流化到外部主机。

注　必须确保外部主机可正常工作且可从ASA FirePOWER 模块进行访问，以发送审核日志。

发送主机的名称是发送的信息的一部分。可以使用工具、严重性级别和可选标记来进一步识别审核日志数据流。 ASA FirePOWER 模块会等到您应用系统策略之后才发送审核日志。

应用启用了此功能的策略且目标主机已配置为接收审核日志之后，系统日志才会发送出去。以下是输出结构的示例：

```
Date Time Host [Tag] Sender: [User_Name]@[User_IP], [Subsystem], [Action]
```

其中，本地日期、时间和主机名称位于括号内的可选标记之前，发送设备名称在审核日志消息之前。

例如：

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3000: admin@10.1.1.2, Operations > Monitoring, Page View
```

要配置审核日志设置，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的审核日志设置，请点击系统策略旁边的编辑图标 ( )。
- 要将审核日志设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 32-1 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

步骤 3　点击 **Audit Log Settings**。

系统将显示 Audit Log Settings 页面。

步骤 4　从 **Send Audit Log to Syslog** 下拉菜单中选择 **Enabled**。（默认设置为 **Disabled**。）

步骤 5　在 **Host** 字段中，使用 IP 地址或完全限定的主机名称指定审核信息的目标主机。默认端口 (514) 已被使用。

注意事项　对于您配置用于接收审核日志的计算机，如果未将其设置为可接收远程消息，主机将不会接受审核日志。

步骤 6　从 **Facility** 字段中选择系统日志工具。

步骤 7　从 **Severity** 字段中选择严重性级别。

步骤 8　或者，在 **Tag (optional)** 字段中插入参考标记。

步骤 9　要将常规审核日志发送到外部 HTTP 服务器，请从 **Send Audit Log to HTTP Server** 下拉列表中选择 **Enabled**。默认设置为 **Disabled**。

步骤 10　在 **URL to Post Audit** 字段中，指定要用于发送审核信息的 URL。必须输入与将会监听下列 HTTP POST 变量的监听程序相对应的 URL：

- `subsystem`
- `actor`
- `event_type`
- `讯息`
- `action_source_ip`
- `action_destination_ip`
- `result`
- `时间`
- `tag`（如果已如上所述进行了定义）

注意事项　要允许发送加密的信息，您必须使用 HTTPS URL。请注意，将审核信息发送到外部 URL 可能会影响系统性能。

步骤 11　点击 **Save Policy and Exit**。

系统策略更新成功。只有您将系统策略应用于防御中心，您的更改才会生效。有关详情，请参见第 32-3 页上的应用系统策略。

配置邮件中继主机和通知地址

许可证：任何环境

如果要执行以下操作，必须配置邮件主机：

- 通过邮件发送基于事件的报告
- 通过邮件发送有关已安排的任务的报告
- 通过邮件发送更改调节报告
- 通过邮件发送数据删除通知
- 通过邮件发送入侵事件警报

可以为设备和邮件中继主机之间的通信选择加密方法，并可根据需要为邮件服务器提供身份验证凭证。配置完设置后，可以测试设备与采用指定设置的邮件服务器之间的连接。

要配置邮件中继主机，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的邮件设置，请点击系统策略旁边的编辑图标 ( )。
- 要将邮件设置配置为新系统策略的一部分，请点击 **Create Policy**。

如第 32-1 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

步骤 3　点击 **Email Notification**。

系统将显示 Configure Email Notification 页面。

步骤 4　在 **Mail Relay Host** 字段中，键入要使用的邮件服务器的主机名或 IP 地址。

注　输入的邮件主机必须允许从设备进行访问。

步骤 5　在 **Port Number** 字段中，输入要在邮件服务器上使用的端口号。常用端口包括 25（未采用加密时使用）、465（采用 SSLv3 时使用）和 587（采用 TLS 时使用）。

步骤 6　要选择加密方法，有以下选项可供选择：

- 要对设备与使用传输层安全的邮件服务器之间的通信进行加密，请从 **Encryption Method** 下拉列表中选择 **TLS**。
- 要对设备与使用安全套接字层的邮件服务器之间的通信进行加密，请从 **Encryption Method** 下拉列表中选择 **SSLv3**。
- 要允许设备与邮件服务器之间进行未经加密的通信，请从 **Encryption Method** 下拉列表中选择 **None**。

请注意，设备和邮件服务器之间的加密通信不要求进行证书验证。

步骤 7　在 **From Address** 字段中，输入有效的邮件地址，以作为设备所发送的消息的源邮件地址。

步骤 8　或者，要在连接到邮件服务器时提供用户名和口令，请选择 **Use Authentication**。在 **Username** 字段中输入用户名。在 **Password** 字段中输入密码。

步骤 9　要使用已配置的邮件服务器发送测试邮件，请点击 **Test Mail Server Settings**。

系统会在按钮旁边显示一条消息，以指明测试是否成功。

步骤 10　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详情，请参见第 32-3 页上的应用系统策略。

配置SNMP 轮询

许可证：任何环境

对于使用此系统策略的设备，可以启用简单网络管理协议 (SNMP) 轮询功能。 SNMP 功能支持使用 SNMP 协议第 1 版、第 2 版和第 3 版。

请注意，启用系统策略 SNMP 功能不会导致设备发送 SNMP 陷阱；这样做只会使 MIB 中的信息可供网络管理系统轮询。

注　对于要用于轮询设备的任何计算机，都必须为其添加 SNMP 访问权限。有关详细信息，请参阅第 32-4 页上的配置设备的访问列表。请注意， SNMP MIB 包含可用于攻击设备的信息。思科建议您将 SNMP 访问权限的访问列表限制为将被用于轮询 MIB 的特定主机。思科还建议您针对网络管理访问权限使用 SNMPv3 和强密码。

要配置 SNMP 轮询：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的 SNMP 轮询设置，请点击系统策略旁边的编辑图标 ( )。
- 要将 SNMP 轮询设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 32-1 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Create**。

步骤 3　对于要用于轮询设备的各台计算机，如果还没有为其添加 SNMP 访问权限，请立即添加。有关详细信息，请参阅第 32-4 页上的配置设备的访问列表。

步骤 4　点击 **SNMP**。

系统将显示 SNMP 页面。

步骤 5　从 **SNMP** 下拉列表中，选择要使用的 SNMP 版本。

所选的版本显示在下拉列表中。

步骤 6　您有以下选项：

- 如果选择了 **Version1** 或 **Version 2**，请在 **Community String** 字段中键入 SNMP 团体名称。转至第 15 步。
- 如果选择了 **Version 3**，请点击 **Add User** 显示用户定义页面。

步骤 7　在 **Username** 字段中输入用户名。

步骤 8　从 **Authentication Protocol** 下拉列表中选择要用于身份验证的协议。

步骤 9　在 **Authentication Password** 字段中键入使用 SNMP 服务器进行身份验证时所需的密码。

步骤 10　在 **Verify Password** 字段（位于 **Authentication Password** 字段下方）中重新键入身份验证密码。

步骤 11　从 **Privacy Protocol** 列表中，选择要使用的隐私协议；或选择 **None** 以不使用隐私协议。

步骤 12　在 **Privacy Password** 字段中，输入 SNMP 服务器要求的 SNMP 隐私密钥。

步骤 13　在 **Verify Password** 字段（位于 **Privacy Password** 字段下方）中重新键入隐私密码。

步骤 14　点击 **Add**。

用户添加成功。可以重复步骤 613 以添加其他用户。点击删除图标 ( ) 可删除用户。

步骤 15　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详情，请参见第 32-3 页上的应用系统策略。

启用 STIG 合规性

许可证：任何环境

美国联邦政府内部的组织有时需要遵守《安全技术实施指南》(STIG) 中规定的一系列安全检查要求。STIG Compliance 选项会启用一些设置，这些设置旨在为遵守美国国防部规定的特定要求提供支持。

如果在部署中的任一 ASA FirePOWER 模块上启用了 STIG 合规性，则必须在所有 ASA FirePOWER 模块上均将其启用。

启用 STIG 合规性不能保证严格遵守所有适用的 STIG 规定。有关将此模式用于此版本产品时 FireSIGHT 系统ASA FirePOWER 模块STIG 合规性的详细信息，请与支持人员联系以获取5.4.1 版的 FireSIGHT 系统ASA FirePOWER 模块 STIG 版本说明。

启用 STIG 合规性时，本地外壳访问帐户的密码复杂性和保留规则会发生更改。有关这些设置的详细信息，请参阅5.4.1 版 的 STIG 版本说明。此外，在 STIG 合规性模式下，无法使用 SSH 远程存储。

请注意，应用启用了 STIG 合规性的系统策略会强制设备重新启动。如果某设备已启用了STIG，当您将启用了 STIG 的系统策略应用于该设备时，该设备不会重新启动。如果某设备已禁用了 STIG，当您将启用了 STIG 的系统策略应用于该设备时， STIG 将保持启用状态，且该设备不会重新启动。

注意事项　需在支持人员的协助下才能禁用此设置。此外，此设置可能会显著影响系统性能。思科除为了满足美国国防部的安全要求外，不建议启用 STIG 合规性。

要启用 STIG 合规性，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > System Policy**。

系统将显示 System Policy 页面。

步骤 2　您有以下选项：

- 要修改现有系统策略中的时间设置，请点击系统策略旁边的编辑图标 ( )。
- 要将时间设置配置为新系统策略的一部分，请点击 **Create Policy**。

  如第 32-1 页上的创建系统策略中所述为系统策略提供名称和描述，然后点击 **Save**。

步骤 3　点击 **STIG Compliance**。

系统将显示 STIG Compliance 页面。

步骤 4　如果要*永久地*在设备上启用 STIG 合规性，请选择 **Enable STIG Compliance**。

注意事项　在应用启用了 STIG 合规性的策略之后，将无法在设备上禁用 STIG 合规性。要禁用合规性，请与支持人员联系。

步骤 5　点击 **Save Policy and Exit**。

系统策略更新成功。所做的更改在应用系统策略后才会生效。有关详情，请参见第 32-3 页上的应用系统策略。

请注意，将启用 STIG 合规性的系统策略应用于某设备时，该设备会重新启动。另请注意，如果某设备已启用了STIG，当您将启用了 STIG 的系统策略应用于该设备时，该设备不会重新启动。

配置 ASA FirePOWER 模块设置

下表汇总了ASA FirePOWER 模块的本地配置。

表 33-1　　本地配置选项

选项	说明	有关详细信息，请参阅.....
信息	您可以查看有关设备的当前信息。您也可以更改设备名称。	第 33-1 页上的查看和修改设备信息
HTTPS 证书	在需要时，允许您从可信机构请求 HTTPS 服务器证书，然后将证书上传到您的设备。	第 33-2 页上的使用自定义 HTTPS 证书
云服务	允许您从综合安全情报云下载 URL 过滤数据，执行未归类 URL 查找，以及向思科发送有关检测到的文件的诊断信息。	第 33-6 页上的启用云通信

查看和修改设备信息

许可证：任何环境

Information 页面提供有关 ASA FirePOWER 模块的信息。信息包括只读信息，例如产品名称和型号、操作系统和版本以及当前系统策略。该页面还提供了更改设备名称的选项。

下表介绍了每个字段。

表 33-2　　设备信息

字段	说明
字段名称	您为设备指定的名称。请注意，此名称仅在 ASA FirePOWER 模块情景中使用。尽管您可以使用主机名作为设备的名称，但在此字段中输入其他名称不会更改主机名。
产品型号	设备的型号名称。
序列号	设备的机箱序列号。
软件版本	当前安装的软件版本。
操作系统	当前在设备上运行的操作系统。
Operating System Version	当前设备上运行的操作系统的版本。
IPv4 Address	设备默认 (`eth0`) 管理接口的 IPv4 地址。如果设备的 IPv4 管理处于禁用状态，此字段会予以指出。

表 33-2　　设备信息 （续）

字段	说明
IPv6 Address	设备默认 (eth0) 管理接口的 IPv6 地址。如果设备的 IPv6 管理处于禁用状态，此字段会予以指出。
Current Policies	当前应用的设备级策略。如果策略自上一次应用以来已更新，则策略的名称以斜体显示。
型号编号	设备的型号。此编号可能对于故障排除非常重要。

要修改设备信息，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　要更改设备名称，请在 **Name** 字段中键入新的名称。

名称**必须**是字母数字字符，并且不能仅包含数字字符。

步骤 3　要保存更改，请点击 **Save**。

页面刷新，您所做的更改被保存。

使用自定义 HTTPS 证书

许可证：任何环境

ASA FirePOWER 模块包括默认 SSL （安全套接字层）证书，您可以使用该证书在 ASDM与ASA FirePOWER 模块之间启动加密通信信道但是，因为默认证书并非由受到任何全球知名的证书颁发机构 (CA) 信任的 CA 生成，所以您可以用全球知名的或内部受信任的 CA 签署的自定义证书来代替默认证书。

可以通过 ASA FirePOWER 模块的本地配置管理证书。有关详情，请参阅：

- 第 33-3 页上的查看当前 HTTPS 服务器证书
- 第 33-3 页上的生成服务器证书签名请求
- 第 33-4 页上的上传服务器证书
- 第 33-5 页上的要求用户证书

查看当前 HTTPS 服务器证书

许可证：任何环境

可以查看设备当前使用的服务器证书的详细信息。该证书提供以下信息：

表 33-3　HTTPS 服务器证书信息

字段	说明
标的	对于安装证书的设备，提供 commonName、 countryName、organizationName 和 organizationalUnitName。
Issuer	对于签发证书的设备，提供 commonName、 countryName、organizationName 和 organizationalUnitName。
有效性	指明证书有效的时间段。
版本	指明证书版本。
序列号	指明证书序列号。
Signature Algorithm	指明用于签署证书的算法。

要查看证书详细信息，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **HTTPS Certificate**。

系统将显示 HTTPS Certificate 页面，其中提供ASA FirePOWER 模块当前证书的详细信息。

生成服务器证书签名请求

许可证：任何环境

可以根据设备信息和您提供的识别信息生成证书请求。可将生成的请求发送至证书颁发机构以请求服务器证书。如果安装有受浏览器信任的内部证书颁发机构 (CA)，那么还可以使用生成的请求对证书进行自签。生成的密钥采用 Base-64 编码 PEM 格式。

请注意，当通过本地配置 HTTPS Certificate 页面生成证书请求时，仅可为单一服务器生成证书。必须准确键入服务器的完全限定域名，因为它将出现在 **Common Name** 字段的证书中。如果公用名称与 DNS 主机名不匹配，那么当连接至设备时，您将接收到警告。同样，如果安装了并非由全球知名的或内部受信任的 CA 签署的证书，那么当连接至设备时，您将接收到安全警告。

要生成证书请求，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **HTTPS Certificate**。

系统将显示 HTTPS Certificate 页面。

步骤 3　点击 **Generate New CSR**。

将会弹出 Generate Certificate Signing Request 窗口。

步骤 4　在 **Country Name (two-letter code)** 字段中键入您所在国家/地区的双字母国家/地区代码（由两个字母组成的代码）。

步骤 5　在 **State or Province** 字段中键入您所在州或省的邮政缩写。

步骤 6　在 **Locality or City** 字段中键入您所在的地区或城市。

步骤 7　在 **Organization** 字段中键入您的组织名称。

步骤 8　在 **Organizational Unit (Department)** 字段中键入部门名称。

步骤 9　在 **Common Name** 字段中键入要为其申请证书的服务器的完全限定域名 （应与要在证书中显示的完全一致）。

步骤 10　点击 **Generate**。

将会弹出 Certificate Signing Request 窗口。

步骤 11　打开一个文本编辑器。

步骤 12　复制证书请求中的整个文本块（包括 `BEGIN CERTIFICATE REQUEST` 和 `END CERTIFICATE REQUEST` 行），然后将其粘贴到一个空白文本文件中。

步骤 13　将该文件另存为 *`servername`***`.csr`**，其中，*`servername`* 是您打算将证书用于其中的服务器的名称。

步骤 14　将该 CSR 文件上传至您想要向其请求证书的证书颁发机构，或者使用该 CSR 文件来创建自签证书。

上传服务器证书

许可证：任何环境

获得证书颁发机构 (CA) 的签名证书后，可以上传该证书。如果生成证书的签署机构要求您信任一个中间 CA，那么您还必须提供一个证书链（有时称为证书路径）。如果您需要用户证书，这些证书必须由其中间机构包括在证书链中的证书颁发机构生成。

要上传证书，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **HTTPS Certificate**。

系统将显示 HTTPS Certificate 页面。

步骤 3　点击 **Import HTTPS Certificate**。

将会弹出 Import HTTPS Certificate 窗口。

步骤 4　在文本编辑器中打开服务器证书，复制整个文本块（包括 `BEGIN CERTIFICATE` 和 `END CERTIFICATE` 行），然后将其粘贴到 **Server Certificate** 字段中。

步骤 5　或者，打开私有密钥文件，复制整个文本块（包括 `BEGIN RSA PRIVATE KEY` 和 `END RSA PRIVATE KEY` 行），然后将其粘贴到 **Private Key** 字段中。

步骤 6　打开您需要提供的每一个中间证书，复制整个文本块，然后将其复制到 **Certificate Chain** 字段中。

步骤 7　点击 **Save** 上传证书。

此时将会上传证书，并更新 HTTPS Certificate 页面以反映新证书。

要求用户证书

许可证：任何环境

可使用客户端浏览器证书检查功能来限制对ASA FirePOWER 模块界面的访问。启用用户证书时，网络服务器会检查用户的浏览器客户端是否选择了有效的用户证书。所选的用户证书必须由生成服务器证书的同一个可信证书颁发机构生成。如果用户在浏览器中选择的证书无效，或者并非由设备上证书链中的证书颁发机构生成，那么浏览器将无法加载模块界面。

您还可以加载服务器的证书撤销列表 (CRL)。CRL 列出证书颁发机构已撤销的所有证书，以便网络服务器能够验证客户端浏览器证书是否已被撤销。如果用户选择在 CRL 中列为已撤销证书的证书，浏览器将无法加载模块界面。设备支持上传采用可区别编码规则 (DER) 格式的 CRL。对一台服务器只能上传一个 CRL。

要确保撤销证书列表是最新的，您可以创建计划任务来更新 CRL。界面中会列出 CRL 的最新更新。

请确保使用的是用于服务器证书的同一证书颁发机构，并且已上传证书的中间证书。有关详细信息，请参阅第 33-4 页上的上传服务器证书。

注意事项　要启用用户证书，然后访问模块界面，浏览器中**必须**存在有效的用户证书（或者读卡器中已插入 CAC）。

要请求提供有效用户证书，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **HTTPS Certificate**。

系统将显示 HTTPS Certificate 页面。

步骤 3　选择 **Enable User Certificates**。如有提示，请从下拉列表中选择相应的证书。

系统将显示 Enable Fetching of CRL 选项。

步骤 4　或者，选择 **Enable Fetching of CRL**。

系统将显示其余的 CRL 配置选项。

步骤 5　键入现有 CRL 文件的有效 URL，然后点击 **Refresh CRL**。

所提供的 URL 的当前 CRL 会加载。

注　启用 CRL 获取功能会创建计划任务来定期更新 CRL。编辑任务以设置更新的频率。有关详细信息，请参阅第 31-3 页上的自动执行证书撤销列表下载。

步骤 6　验证您是否拥有由创建服务器证书的同一证书颁发机构生成的有效用户证书。

注意事项　当保存包含已启用用户证书的配置时，如果在您的浏览器证书存储中无有效用户证书，则会禁用对设备的所有网络服务器访问。请确保在保存设置之前已安装有效证书。

步骤 7　要应用用户证书配置，请点击 **Save**。

启用云通信

许可证：URL 过滤或恶意软件

ASA FirePOWER 模块联系思科综合安全情报云获得各种信息：

- 设备可以利用与访问控制规则相关的文件策略来检测在网络流量中传输的文件。 ASA FirePOWER 模块使用思科云中的数据来确定文件是否为恶意软件；请参阅第 24-4 页上的了解和创建文件策略。
- 启用 URL 过滤后，ASA FirePOWER 模块可检索许多通常被访问的 URL 的类别和信誉数据，还可对未分类 URL 执行查找。然后，可以迅速创建访问控制规则的 URL 条件；请参阅第 8-7 页上的执行基于信誉的 URL 阻止。

使用ASA FirePOWER 模块的本地配置指定以下选项：

启用 URL 过滤

必须启用此选项以执行类别和基于信誉的 URL 过滤。

未知 URL 的云查询

当监控网络上的某人尝试浏览不在本地数据集中的 URL 时，允许系统查询云。

如果云不知道 URL 的类别或信誉，或者，如果ASA FirePOWER 模块不能与云联系，那么 URL **不会**匹配关于基于类别或信誉的 URL 条件的访问控制规则。在这种情况下，您将无法手动对该 URL 指定类别或信誉。

如果您不想让思科云对未分类 URL 进行归类（例如，出于隐私原因），请禁用此选项。

启用自动更新

允许系统定期与云联系，以获取对设备本地数据集中 URL 数据的更新。尽管云通常每天更新一次数据，但是，启用自动更新会强制防御中心 ASA FirePOWER 模块每 30 分钟检查一次，以确保可以始终获得最新信息。

虽然每日更新通常是小量更新，但是，如果距离上一次更新超过五天，新的 URL 过滤数据最多可能需要 20 分钟才能下载完（具体取决于带宽）。然后，执行更新也可能最多需要 30 分钟。

如果希望严格控制系统联系云的时间，可以禁用自动更新而改为使用调度程序，如第 31-8 页上的自动更新 URL 过滤中所述。

注　思科建议启用自动更新或使用调度程序安排更新。虽然可以手动执行按需更新，但设置系统定期自动与云联系可为您提供最新、最相关的 URL 数据。

许可

执行基于类别和信誉的 URL 过滤和基于设备的恶意软件检测要求您在 ASA FirePOWER 模块上启用相应的许可证；请参阅第 34-1 页上的许可 ASA FirePOWER 模块。

如果您在 ASA FirePOWER 模块上不具有 URL 过滤许可证，那么您将**不能**配置云连接选项。，那么 Cloud Services 本地配置页面将仅显示您获得许可的选项。拥有已到期许可证的 ASA FirePOWER 模块不能与云联系。

请注意，除了导致 URL 过滤选项对话框出现，自动添加URL 过滤许可证到ASA FirePOWER 模块还会启用 **Enable URL Filtering** 和 **Enable Automatic Updates**。如有需要，可以手动禁用该选项。

互联网访问

系统使用端口 80/HTTP 和 443/HTTPS 与思科云通信。

以下步骤说明如何启用与思科云的通信以及执行 URL 数据的按需更新。请注意，如果有更新正在进行，则不能启动按需更新。

要启用与云的通信，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **Cloud Services**。

系统将显示 Cloud Services 页面。如果您有 URL 过滤许可证，该页面会显示上次更新 URL 数据的时间。

步骤 3　如上所述配置云连接选项。

必须先启用 **Enable URL Filtering**，然后才能启用 **Enable Automatic Updates** 或 **Query Cloud for Unknown URLs**。

步骤 4　点击 **Save**。

即会保存设置。如果已启用 URL 过滤（具体取决于上一次启用 URL 过滤经过的时间），或者首次启用 URL 过滤，防御中心ASA FirePOWER 模块会从云检索 URL 过滤数据。

要执行系统的 URL 数据按需更新，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Local > Configuration**。

系统将显示 Information 页面。

步骤 2　点击 **URL Filtering**。

系统将显示 URL Filtering 页面。

步骤 3　点击 **Update Now**。

ASA FirePOWER 模块联系云并更新其 URL 过滤数据 （如果有更新可用）。

许可 ASA FirePOWER 模块

您可许可各种功能，为贵公司创建最佳 ASA FirePOWER部署。

有关详情，请参阅：

了解许可

许可证：任何环境

您可许可各种功能，为贵公司创建最佳 ASA FirePOWER部署。

可供设备执行各种功能，包括：

- 入侵检测和阻止
- 安全情报过滤
- 文件控制和高级恶意软件防护
- 应用、用户和 URL 控制

有多种方式可能让您失去对 ASA FirePOWER 模块中许可功能的访问权。也可移除已许可的功能。此外，有些许可证可能过期。虽然有一些例外情况，但不能使用与已到期或删除的许可证关联的功能。

本节介绍 ASA FirePOWER 模块部署中可用的许可证类型。可在某设备上启用的许可证取决于已启用的其他许可证。

下表概述了 ASA FirePOWER 模块许可证。

表 34-1　　ASA FirePOWER 模块许可证

许可证	授予的功能	需要
保护	入侵检测和阻止 文件控制 安全情报过滤	无
可控性	用户和应用控制	保护

表 34-1　ASA FirePOWER 模块许可证（续）

许可证	授予的功能	需要
恶意软件	高级恶意软件防护（基于网络的恶意软件检测和拦截）	保护
URL 过滤	基于类别和信誉的 URL 过滤	保护

有关详情，请参阅：

- 第 34-2 页上的保护
- 第 34-2 页上的可控性
- 第 34-3 页上的恶意软件
- 第 34-3 页上的URL 过滤

保护

许可证：保护

保护许可证可用于执行入侵检测和阻止、文件控制和安全情报过滤：

- *入侵检测和阻止*可用于分析网络流量是否存在入侵和漏洞利用，或者丢弃攻击性数据包。
- *文件*控制可用于检测且或者阻止用户通过特定应用程序协议上传（发送）或下载（接收）特定类型的文件。借助于恶意软件许可证（请参阅第 34-3 页上的恶意软件），还可根据恶意软件布置检查并拦截这些文件类型的有限集。
- *安全情报过滤*可用于在流量将接受访问控制规则的分析之前，拉黑-拒绝源自和进入特定 IP 地址的流量。动态源可用于根据最新智能立即拉黑连接。或者，可将“仅监控”设置用于安全情报过滤。

虽然无需许可证即可配置访问控制策略以执行保护相关的检查，但不能应用该策略，直至首先将保护许可证添加至 ASA FirePOWER 模块。

如果从 ASA FirePOWER 模块删除保护许可证，保护， ASA FirePOWER 模块停止检测的入侵和文件事件。此外， ASA FirePOWER 模块将不会连接互联网获取思科提供的信息或第三方安全情报信息。重新启用保护之前，无法重新应用现有策略。

由于 URL 过滤、恶意软件和可控性许可证需要保护许可证，因此，删除或禁用保护许可证与删除或禁用 URL 过滤、恶意软件或可控性许可证有相同效果。

可控性

许可证：可控性

可控性许可证可用于实施用户和应用控制，只需将用户和应用条件添加至访问控制规则。要启用可控性，您还必须启用保护。

虽然无需可控性许可证即可向访问控制规则添加用户和应用条件，但不能应用策略，除非首先将可控性许可证添加至ASA FirePOWER 模块。

如果删除您的可控性许可证，并且现有的访问控制策略包含带用户或应用条件的规则，则无法重新应用这些策略。

URL 过滤

许可证：URL 过滤

URL 过滤可用于编写访问控制规则，以根据受监控主机请求的 URL 确定可横越网络且与这些 URL 的相关信息关联的流量，可通过思科从ASA FirePOWER 模块云获取该流量。要启用 URL 过滤，您还必须启用保护许可证。

提示　没有 URL 过滤许可证，可指定要许可或拦截的单一 URL 或 URL 组。这将对网络流量进行精细和自定义控制，但是，不允许使用 URL 类别和信誉数据来过滤网络流量。

URL 过滤需要基于订用的 URL 过滤许可证。虽然可添加基于类别和信誉的 URL 条件至访问控制规则，无需 URL 过滤许可证， ASA FirePOWER 模块将不会联系云获取 URL 信息。要应用访问控制策略，必须首先将 URL 过滤许可证添加至 ASA FirePOWER 模块，

如果从 ASA FirePOWER 模块删除许可证URL 过滤，则可能无法访问 URL 过滤。此外， URL 过滤许可证可能过期。如果许可证过期，或如果删除许可证，带 URL 条件的访问控制规则将立即停止过滤 URL， ASA FirePOWER 模块再也不能联系云。如果现有访问控制策略包括的规则带有基于类别和信誉的 URL 条件，则不能应用该等策略。

恶意软件

许可证：恶意软件

恶意软件许可证可用于执行高级恶意软件防护，也就是说，使用设备检测并拦截通过网络传输的文件中的恶意软件。要在设备上启用恶意软件，您还必须启用保护。

配置恶意软件检测作为文件策略的一部分，然后与一个或多个访问控制规则相关联。文件策略可以通过特定应用协议检测用户是否上传或下载特定类型的文件。恶意软件许可证可用于在这些文件类型受限集中检查恶意软件。恶意软件许可证还可用于将特定文件添加至文件列表，并在文件策略中启用文件列表，从而在检测时自动允许或拦截这些文件。

虽然可添加恶意软件检测文件策略至访问控制规则，而无需恶意软件许可证，在访问控制规则编辑器中，文件策略标有警告图标 ( )。在文件策略中，恶意软件云查找规则也标有警告图标。首先**必须**添加恶意软件许可证，，才能应用包括恶意软件检测文件策略的该策略。如果稍后删除该许可证，并且现有访问控制策略包括执行恶意软件检测的文件策略，则无法向这些设备重新应用现有访问控制策略。

如果删除恶意软件许可证或许可证全都过期，ASA FirePOWER 模块则停止执行恶意软件云查找，并停止确认从思科云发送的回顾性事件。如果现有访问控制策略包括执行恶意软件检测的文件策略，则将无法重新应用现有访问控制策略。请注意，在恶意软件许可证已过期或被删除后的极短时间内，系统可将缓存布置用于恶意软件云查找文件规则检测的文件。在时窗过期后，系统将向这些文件分配不可用的处置，而不是执行查找。

查看许可证

许可证：任何环境

使用 Licenses 页面查看 ASA FirePOWER 模块的许可证。

除了 Licenses 页面之外，还有其他一些方法可用于查看许可证数量和许可限制：

- Product Licensing 控制面板构件提供了许可证概览。
- Device 页面 (**Configuration > ASA FirePOWER Configuration > Device Management > Device**) 列出了许可证。

要查看许可证，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Licenses**。

系统将显示 Licenses 页面。

添加许可证至ASA FirePOWER 模块

许可证：任何环境

添加许可证至ASA FirePOWER 模块之前，确保拥有在购买许可证时思科提供的激活密钥。还**必须**添加许可证，才能使用许可的功能。

注　如果在备份完成后添加许可证，即使备份恢复，这些许可证不会删除也不会被覆盖。为防止恢复时出现冲突，请在恢复备份之前移除这些许可证，记住许可证使用位置，并在恢复备份之后添加和重新配置它们。如果发生冲突，请与技术支持部门联系。

要添加许可证，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Licenses**。

系统将显示 Licenses 页面。

步骤 2　点击 **Add New License**。

系统将显示 Add License 页面。

步骤 3　您是否收到带有许可证的邮件？

- 如果是，从邮件复制许可证，将其粘贴至 **License** 字段，然后点击 **Submit License**。

  如果许可证正确，则许可证添加成功。跳过该步骤的其他部分。
- 否则，点击 **Get License**。

  系统将显示 Licensing Center 网站。如果无法访问互联网，请切换至可访问 Internet 的计算机。请注意页面底部的许可证密钥并浏览至 https://keyserver.sourcefire.com/。

步骤 4　按照屏幕上的说明获取许可证，将通过邮件发送许可证。

提示　在登录支持网站后，还可在 **Licenses** 选项卡上申请许可证。

步骤 5　从邮件复制许可证，将其粘贴至 ASA FirePOWER 模块网络用户界面中的 **License** 字段，然后点击 **Submit License**。

如果许可证有效，则许可证添加成功。

删除许可证

许可证：任何环境

如果由于任何原因需要删除许可证，请执行以下步骤。谨记：因为思科根据每个ASA FirePOWER 模块的唯一许可证密钥生成许可证，因此，不能从一个ASA FirePOWER 模块删除许可证，然后在另一个ASA FirePOWER 模块上重用它。

在大多数情况下，删除许可证后，就无法使用该许可证启用的功能。有关详细信息，请参阅第 34-1 页上的了解许可。

要删除许可证，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Licenses**。

系统将显示 Licenses 页面。

步骤 2　在要删除的许可证旁边，点击删除图标 ( )。

步骤 3　确认要删除许可证。

许可证删除成功。

更新 ASA FirePOWER 模块软件

思科以电子形式分配多种不同类型的更新，其中包括 ASA FirePOWER 模块软件本身的主要和次要更新、规则更新、地理定位数据库 (GeoDB) 更新以及漏洞数据库 (VDB) 更新。

注意事项 本节包含有关更新 ASA FirePOWER 模块的一般信息。在更新 FireSIGHT 系统 （包括 VDB、GeoDB 或入侵规则）之前，**必须**阅读更新随附的版本说明或建议性文本。版本说明提供重要信息，包括先决条件、警告以及具体安装和卸载说明。

除非版本说明或建议性文本另有说明，否则，更新不会修改配置；设置将保持不变。

有关详细信息，请参阅：

了解更新类型

许可证：任何环境

思科以电子形式分配多种不同类型的更新，其中包括 ASA FirePOWER 模块软件本身的主要和次要更新、入侵规则更新和 VDB 更新。

下表介绍了思科提供的更新类型。对于大多数更新类型，可以安排下载和安装；请参阅第 31-1 页上的安排任务和第 35-11 页上的使用周期性规则更新。

表 35-1 ASA FirePOWER 模块更新类型

更新类型	说明	安排？	卸载？
	补丁包括数量有限的修复程序（通常更改版本号中的第四位数字；例如，5.4.0.1）。	是	是
FireSIGHT 系统	功能更新比补丁更全面，通常包括新功能（并且通常更改版本号中的第三位数字；例如，5.4.1）。	是	是

表 35-1　ASA FirePOWER 模块更新类型 （续）

更新类型	说明	安排？	卸载？
	主要更新（有时称为升级）包括新功能，并且可能需要进行大规模更改（通常改变版本号中的第一位或第二位数字；例如，5.3 或 5.4）。	否	否
VDB	VDB 更新影响主机可能易受攻击的已知漏洞的数据库。	是	否
入侵规则	入侵规则更新提供新的和更新后的入侵规则和预处理器规则、现有规则的修改后状态以及修改后的默认入侵策略设置。规则更新还可以删除规则，提供新规则类别和默认变量，以及修改默认变量值。	是	否
地理定位数据库 (GeoDB)	GeoDB 提供有关系统可通过可路由 IP 地址与之关联的物理位置、连接类型等等方面的更新信息。地理定位数据可用作访问控制规则中的条件。必须安装 GeoDB 才能查看地理定位详细信息。	是	否

请注意，可以卸载 FireSIGHT 系统补丁和其他次要更新，但不能卸载主要更新，也不能恢复到 VDB、GeoDB 或入侵规则的先前版本。如果已将更新为新的FireSIGHT 系统主要版本，但需要恢复为旧版本，请联系支持部门。

进行软件更新

许可证：任何环境

更新有一些基本步骤。首先，**必须**为更新做好准备，包括阅读版本说明以及完成必要的更新前任务。然后，开始更新。必须验证更新是否成功。最后，完成必要的更新后步骤。

有关详细信息，请参阅：

- 第 35-2 页上的制定更新计划
- 第 35-3 页上的了解更新过程
- 第 35-4 页上的更新 ASA FirePOWER 模块软件
- 第 35-5 页上的监控主要更新状态

制定更新计划

许可证：任何环境

开始更新之前，必须仔细阅读并理解版本说明（可从支持网站下载）。版本说明介绍、新特性和功能、已知问题、已解决的问题。版本说明还包含有关先决条件、警告以及具体安装和卸载说明的重要信息。

以下各节概述了制定更新计划时必须考虑的一些因素。

软件版本要求

必须确保运行的是正确的 FireSIGHT 系统软件版本。版本说明指明所需的版本。如果运行的是早期版本，可从支持网站获取更新。

时间和磁盘空间要求

确定有足够的可用磁盘空间并且更新时间足够。版本说明指明磁盘空间和时间方面的要求。

配置备份准则

开始主要更新之前，思科建议在将所有备份复制到外部位置后，删除 ASA FirePOWER 模块上驻留的所有备份。此外，不管更新类型如何，都应该将当前配置数据备份到外部位置。请参阅第 37-1 页上的使用备份和恢复。

何时进行更新

由于更新过程可能会影响流量检查流量，而且数据相关器在更新过程中处于禁用状态，因此，思科建议在维护窗口中或者中断对造成的影响最小时进行更新。

了解更新过程

许可证：任何环境

您使用 ASA FirePOWER 模块接口更新 ASA FirePOWER 模块。

Product Updates 页面 (**Configuration > ASA FirePOWER Configuration > Updates**) 显示每项更新的版本以及生成更新的日期和时间。该页面还指明更新过程中是否需要软件重新启动。将从支持部门获得的更新上传到时，这些更新显示在该页面中。该页面还显示补丁和功能更新的卸载程序；请参阅第 35-6 页上的卸载软件更新。该页面可能还列出了 VDB 更新。

提示　对于补丁和功能更新，可以利用自动更新功能；请参阅第 31-6 页上的自动执行软件更新。

流量和检查

安装或卸载更新时，以下功能可能会受到影响：

- 流量检查，包括应用和用户感知与控制、 URL 过滤、安全情报过滤、入侵检测与防御以及连接日志记录
- 流量

数据相关器在系统更新期间不运行。更新完成后，它会恢复正常运行。

网络流量中断的方式和持续时间取决于 ASA FirePOWER 模块的配置和部署方式，以及更新是否会重新启动 ASA FirePOWER 模块。有关特定更新如何和何时影响网络流量的详细信息，请参阅版本说明。

在更新期间使用 ASA FirePOWER 模块

不管更新类型如何，请**勿**使用正在更新的 ASA FirePOWER 模块执行除监控更新以外的其他任务。

为避免在主要更新期间使用 ASA FirePOWER 模块，并方便监控主要更新进度，系统简化了 ASA FirePOWER 模块界面。可以在任务队列中监控次要更新的进度 (**Monitoring > ASA FirePOWER Monitoring > Task Status**)。尽管在进行次要更新时并未禁止您使用ASA FirePOWER 模块，但思科并不建议执行此操作。

即使对于次要更新，更新过程中也可能无法使用 ASA FirePOWER 模块的网络界面。这是预期行为。如果出现这种情况，请等待，直到您可以再次访问 ASA FirePOWER 模块。如果仍在进行更新，**必须**避免使用 ASA FirePOWER 模块，直至更新完成。请注意，在更新过程中，ASA FirePOWER 模块可能会重新启动两次；这也是预期行为。

注意事项　如果更新出现问题（例如，更新失败；或者，手动刷新 Update Status 页面后不显示进度），请**勿**重新启动更新。在这种情况下，请联系支持部门。

更新后

必须完成版本说明中列出的所有更新后任务，以确保部署正常运行。

最重要的更新后任务是重新应用访问控制策略，请注意，应用访问控制策略可能会造成短暂停止流量和处理，还可能会导致遗漏检查一些数据包；请参阅第 4-10 页上的应用访问控制策略。

此外，还应：

- 确认更新是否成功。
- 如有必要，更新入侵规则、 VDB 和 GeoDB
- 根据版本说明中的信息更改任何必要的配置
- 进行版本说明中列出的任何其他更新后任务

更新 ASA FirePOWER 模块软件

许可证：任何环境

可使用以下两种方法之一来更新ASA FirePOWER 模块 软件，具体取决于更新类型以及 ASA FirePOWER 模块能否访问互联网：

- 如果 ASA FirePOWER 模块能访问互联网，可防御中心直接从支持网站获取更新。这种方法**不**适用于主要更新。
- 可手动从支持网站下载更新，然后将更新上传到 ASA FirePOWER 模块。如果 ASA FirePOWER 模块不能访问互联网或者要进行主要更新，可采用这种方法。

对于主要更新，更新 ASA FirePOWER 模块会删除之前更新的卸载程序。

要更新 ASA FirePOWER 模块软件，请执行以下操作：

步骤 1　阅读版本说明并完成必要的更新前任务。

更新前任务可能包括确保：ASA FirePOWER 模块运行的是正确的思科软件版本，有足够的可用磁盘空间进行更新，预留了足够时间来进行更新，已经备份配置数据，等等。

步骤 2　将更新上传。您有两种选择，具体取决于更新类型以及 ASA FirePOWER 模块能否访问互联网：

- 对于主要更新以外的所有其他更新，如果 ASA FirePOWER 模块能够访问互联网，请选择 **Configuration > ASA FirePOWER Configuration > Updates**, then click **Download Updates** 以检查以下任一支持站点上的最新更新：
  - **Sourcefire：**(https://support.sourcefire.com/)
  - **思科：**(http://www.cisco.com/cisco/web/support/index.html)
- 对于主要更新，如果 ASA FirePOWER 模块不能访问互联网，必须首先手动从以下任何一个支持网站下载更新：
  - **Sourcefire：**(https://support.sourcefire.com/)
  - **思科：**(http://www.cisco.com/cisco/web/support/index.html)
- 选择 **Configuration > ASA FirePOWER Configuration > Updates**，然后点击 **Upload Update**。点击 **Choose File** 浏览到并选择更新，然后点击 **Upload**。

注　可直接从支持网站下载更新（手动下载，或者点击 Product Updates 选项卡上的 **Download Updates** 进行下载）。如果通过邮件传输更新文件，可能会损坏更新文件。

更新成功上传。

步骤 3　选择 **Monitoring > ASA FirePOWER Monitoring > Task Status** 以查看任务队列，并确保所有工作未进行。

正在运行的任务会在更新开始时停止，不得恢复这些任务；必须在更新完成后手动将这些任务从任务队列删除。任务队列每 10 秒钟自动刷新一次。必须等到所有长时间运行的任务都完成后，才能开始更新。

步骤 4　选择 **Configuration > ASA FirePOWER Configuration > Updates**。

系统将显示 Product Updates 页面。

步骤 5　点击上传的更新旁边的安装图标。

更新过程开始。监控更新的方式取决于更新是主要更新还是次要更新。请参阅ASA FirePOWER 模块更新类型表和版本说明来确定更新类型：

- 对于次要更新，可以在任务队列中监控更新的进度（**Monitoring > ASA FirePOWER Monitoring > Task Status**）。
- 对于主要更新，可在任务队列中监控更新进度。但是，ASA FirePOWER 模块 完成其必要的更新前检查后，您将被锁定在模块界面之外。当您重新获得访问权限时，系统将显示 Upgrade Status 页面。有关详细信息，请参阅第 35-5 页上的监控主要更新状态。

注意事项　不管更新类型如何，请勿在更新完成前使用 ASA FirePOWER 模块执行除监控更新以外的其他任务；如有必要， ASA FirePOWER 模块会重新启动。有关详细信息，请参阅第 35-3 页上的在更新期间使用 ASA FirePOWER 模块。

步骤 6　在完成更新后，请访问 ASA FirePOWER 模块界面并刷新页面。否则，界面可能会出现意外行为。在完成主要更新后，如果是用户首次登录该界面，系统可能会显示用户软件授权协议 (EULA)。必须阅读并接受 EULA 才能继续。

步骤 7　如果支持网站上的可用规则更新比您的 ASA FirePOWER 模块的规则新，请导入最新的规则。

有关详细信息，请参阅第 35-8 页上的导入规则更新和本地规则文件。

步骤 8　重新应用访问控制策略。

应用访问控制策略可能会造成短暂停止流量和处理，还可能会导致遗漏检查一些数据包。有关详细信息，请参阅第 4-10 页上的应用访问控制策略。

步骤 9　如果支持网站上可用的 VDB 比防御中心 VDB 更加新，请安装最新的 VDB。

安装 VDB 更新会导致短暂停止流量和处理，还可能会导致遗漏检查一些数据包。有关详细信息，请参阅第 35-7 页上的更新漏洞数据库。

监控主要更新状态

许可证：任何环境

对于主要更新， ASA FirePOWER 模块提供简化的界面，以便轻松监控更新过程。简化的界面还防止您使用ASA FirePOWER 模块执行监控更新以外的任务。您可以开始在任务队列中监控更新的进度 (**Monitoring > ASA FirePOWER Monitoring > Task Status**)。但是，在ASA FirePOWER 模块完成必要的更新前检查后，系统会将您从用户界面锁定，直到简化的更新页面。

简化的界面显示从其进行更新的版本，更新后的版本以及自更新开始以来已过去的时间。此外，该页面还显示进度条并提供有关当前运行的脚本的详细信息。

提示　点击 **show log for current script** 可查看更新日志。点击 **hide log for current script** 可隐藏更新日志。

如果出于任何原因更新失败，页面会显示错误消息，其中指明失败的时间和日期、更新失败时正在运行的脚本，并提供有关如何联系支持部门的说明。请**勿**重新开始更新。

注意事项　如果更新出现任何其他问题（例如，手动刷新页面后很长时间都没有显示进度），请**勿**重新开始更新。在这种情况下，请联系支持部门。

更新完成后，ASA FirePOWER 模块显示成功消息并重新启动。ASA FirePOWER 模块重新启动完成后，完成所有必要的更新后步骤。

卸载软件更新

许可证：任何环境

应用补丁或功能更新时，更新过程中会创建卸载程序，移除更新。

卸载更新时，产生的思科软件版本取决于更新路径。例如，考虑这样一个场景：直接将从 5.0 版本更新为 5.0.0.2 版本。卸载 5.0.0.2 版本补丁可能会产生运行 5.0.0.1 版本，尽管您从未安装 5.0.0.1 版本更新。有关卸载更新时产生的思科软件版本的信息，请参阅版本说明。

注　对于主要更新，不支持卸载。如果已将更新为新主要版本，但需要恢复为旧版本，请联系支持部门。

流量和检查

卸载更新可能会影响流量检查以及流量。有关特定更新如何和何时影响网络流量的详细信息，请参阅版本说明。

卸载后

卸载更新后，卸载是否成功。有关每项更新的详细信息，请参阅版本说明。

要卸载补丁或功能更新，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Updates**。

系统将显示 Product Updates 页面。

步骤 2　点击要移除的更新的卸载程序旁边的安装图标。

如果出现提示，都需要确认是否要卸载更新并重新启动ASA FirePOWER 模块。

卸载过程开始。可以在任务队列中监控其进度 (**Monitoring > ASA FirePOWER Monitoring > Task Status**)。

注意事项　在卸载完成之前，请**勿**使用 ASA FirePOWER 模块界面执行任务；如有必要， ASA FirePOWER 模块会重新启动。有关详细信息，请参阅第 35-3 页上的在更新期间使用 ASA FirePOWER 模块。

步骤 3　刷新页面。否则，界面可能会出现意外行为。

更新漏洞数据库

许可证：任何环境

思科漏洞数据库 (VDB) 是可能影响主机的已知漏洞的数据库。思科漏洞研究团队 (VRT) 定期发布 VDB 更新。要更新 防御中心上的 Product Updates 页面。

注　安装包含检测更新的 VDB 更新可能导致流量传输和处理短时间暂停，还可能导致一些数据包未经检查就通过。您可能想要安排在低系统使用率时间进行更新，以便最大程度地降低系统停机时间的影响。

注　在完成 VDB 更新后，重新应用所有过时的访问控制策略。请记住，安装 VDB 或重新应用访问控制策略可能导致流量传输和处理短时间暂停，还可能导致一些数据包未经检查就通过。有关详细信息，请参阅第 4-10 页上的应用访问控制策略。

本节说明如何计划和执行手动 VDB 更新。

要更新漏洞数据库，请执行以下操作：

步骤 1　阅读适用于具体更新的 VDB 更新建议性文本。

建议性文本包括有关在更新过程中对 VDB 所做更改的信息。

步骤 2　选择 **Configuration > ASA FirePOWER Configuration > Updates**。

系统将显示 Product Updates 页面。

步骤 3　将更新上传：

- 如果 ASA FirePOWER 模块能够访问互联网，请点击 **Download Updates** 以检查以下任何一个支持网站上的最新更新：
  - **Sourcefire**：(https://support.sourcefire.com/)
  - **思科**：(http://www.cisco.com/cisco/web/support/index.html)
- 如果 ASA FirePOWER 模块不能访问互联网，请手动从以下任何一个支持网站下载更新，然后点击 **Upload Update**。点击 **Choose File** 浏览到并选择更新，然后点击 **Upload**：
  - **Sourcefire**：(https://support.sourcefire.com/)
  - **思科**：(http://www.cisco.com/cisco/web/support/index.html)

注　可直接从支持网站下载更新 （手动下载，或者点击 **Download Updates**）。如果通过邮件传输更新文件，可能会损坏更新文件。

更新成功上传。

步骤 4　点击 VDB 更新旁边的安装图标。

系统将显示 Install Update 页面。

步骤 5　点击**安装**。

注意事项 更新过程开始。可以在任务队列中监控更新的进度（**Monitoring > ASA FirePOWER Monitoring > Task Status**）。如果更新出现问题（例如，如果任务队列指出更新失败），**请勿**重新开始更新。在这种情况下，请联系支持部门。

必须重新应用所有过时的访问控制策略，才能使 VDB 更新生效；请参阅第 4-10 页上的应用访问控制策略。

导入规则更新和本地规则文件

许可证：任何环境

随着新的漏洞可知，思科漏洞研究团队 (VRT) 发布规则更新，您可以首先导入 ASA FirePOWER 模块，然后通过应用受影响的访问控制、网络分析和入侵策略来实施这些更新。

规则更新是累加性的，并且思科建议您始终导入最新的更新。不能导入与当前安装的规则的版本匹配或早于该版本的规则更新。

注 规则更新可能包含新的二进制文件，因此，请确保下载和安装规则更新的过程符合安全策略。此外，规则更新可能很大，因此，请确保在网络使用较少的时段导入规则。

规则更新可能提供以下内容：

- **新的和修改的规则和规则状态** - 规则更新提供新的和更新的入侵和预处理器规则。对于新的规则，每个系统提供的入侵规则中的规则状态可能不同。例如，一个新规则在 Security over Connectivity 入侵策略中可能是启用状态，在 Connectivity over Security 入侵策略中则可能是禁用状态。规则更新也可以更改现有规则的默认状态，或者完全删除现有规则。
- **新规则类别** - 规则更新可能包括始终添加的新规则类别。
- **修改的预处理程序和高级设置** - 规则更新可能更改系统提供的入侵策略中的高级设置以及系统提供的网络分析策略中的预处理器设置。它们也可以更新访问控制策略中的高级预处理和性能选项的默认值。
- **新的和修改的变量** - 规则更新可能修改现有默认变量的默认值，但不会覆盖您的更改。始终会添加新变量。

了解规则更新何时修改策略

规则更新可能影响系统提供和自定义网络分析策略，以及所有访问控制策略：

- **系统提供** - 对系统提供的网络分析和入侵策略的更改，以及对高级访问控制设置的所有更改，将在您更新后重新应用策略时自动生效。
- **自定义** - 因为每个自定义网络分析和入侵策略都使用系统提供的策略作为其基础，或作为策略链中的事件基础，所以规则更新可以影响自定义网络分析和入侵策略。但是，您可以阻止规则更新自动执行这些更改。这使您能够在独立于规则更新导入的计划中手动更新系统提供的基本策略。无论您的选择（在每个自定义策略基础上实施）如何，更新系统提供的策略**都不会**覆盖您定制的任何设置。有关详细信息，请参阅第 12-4 页上的允许规则更新修改系统提供的基本策略。

请注意，导入规则更新会丢弃对网络分析和入侵策略所做的所有已缓存更改。为方便起见， Rule Updates 页面列出包含已缓存更改的策略。有关详细信息，请参阅第 11-12 页上的解决冲突和提交策略更改。

重新应用策略

要使规则更新所做的更改生效，必须重新应用所有修改的策略。在导入规则更新时，您可以配置系统以自动重新应用入侵或访问控制策略。如果允许规则更新修改系统提供的基本策略，这种方法尤其有用。

- 重新应用访问控制策略也重新应用相关 网络分析和文件策略，但不重新应用入侵策略。还会更新所有修改的高级设置的默认值。由于您无法独立应用网络分析策略，因此如果要更新网络分析策略中的预处理器设置，必须重新应用访问控制策略。
- 重新应用入侵策略可以更新规则和其他更改的入侵策略设置。您可以同时重新应用入侵策略和访问控制策略，也可以仅应用入侵策略，从而更新入侵规则不更新任何其他访问控制配置。

当规则更新包括共享对象规则时，在导入规则后首次应用访问控制或入侵策略会导致流量和处理短时间暂停，还可能导致一些数据包未经检查就通过。有关应用访问控制和入侵策略的详细信息，包括要求、其他影响和建议，请参阅第 4-10 页上的应用访问控制策略。

有关导入规则更新的详细信息，请参阅：

- 第 35-9 页上的使用一次性规则更新说明如何从支持网站导入单个规则更新。
- 第 35-11 页上的使用周期性规则更新说明如何使用自动功能从支持网站下载和安装规则更新。
- 第 35-12 页上的导入本地规则文件说明如何导入在本地计算机上创建的标准文本规则文件的副本。
- 第 35-13 页上的查看规则更新日志说明规则更新日志。

使用一次性规则更新

许可证：任何环境

有两种方法可使用一次性规则更新：

- 第 35-9 页上的使用手动一次性规则更新说明如何将规则更新从支持网站手动下载，然后手动安装规则更新。
- 第 35-10 页上的使用自动一次性规则更新说明如何使用自动功能从支持网站搜索新的规则更新并进行上传。

使用手动一次性规则更新

许可证：任何环境

以下步骤说明如何手动导入新的规则更新。如果 ASA FirePOWER 模块不能访问互联网，此步骤尤其有用。

要手动导入规则更新，请执行以下操作：

步骤 1　从可访问互联网的计算机访问以下任何一个网站：

- **Sourcefire：**(https://support.sourcefire.com/)
- **思科：**(http://www.cisco.com/cisco/web/support/index.html)

步骤 2　点击 **Download**，然后点击 **Rules**。

步骤 3　浏览到最新的规则更新。

规则更新是累积的；您无法导入匹配或早于当前安装的规则版本的规则更新。

步骤 4　点击要下载的规则更新文件并保存到计算机。

步骤 5　选择 **Configuration > ASA FirePOWER Configuration > Updates**，然后选择 **Rule Updates** 选项卡。

系统将显示 Rule Updates 页面。

提示　也可以点击 Rule Editor 页面 (**Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Rule Editor)** 上的 **Import Rules**。

步骤 6　或者，点击 **Delete All Local Rules**，然后点击 **OK**，以将创建或导入的所有用户定义规则移到被删除的文件夹。有关详情，请参阅第 23-96 页上的删除自定义规则。

步骤 7　选择 **Rule Update or text rule file to upload and install**，然后点击 **Choose File** 以浏览并选择规则更新文件。

步骤 8　或者，在更新完成后，重新应用策略：

- 选择 **Reapply intrusion policies after the rule update import completes** 以自动重新应用入侵策略。仅选择此选项更新规则和其他已更改的入侵策略设置，无需更新您进行的所有其他访问控制配置。您**必须**选择此选项与访问控制策略一起重新应用入侵策略；重新应用访问控制策略在这种情况下不执行全面的应用。
- 选择 **Reapply access control policies after the rule update import completes** 以自动重新应用访问控制策略及其相关 、网络分析和文件策略，但不重新应用入侵策略。选择此选项也更新所有修改的访问控制高级设置的默认值。由于您无法独立于其父访问控制策略应用网络分析策略，因此如果要更新网络分析策略中的预处理器设置，**必须**重新应用访问控制策略。

步骤 9　点击 **Import**。

系统安装规则更新并显示 Rule Update Log 详细视图；请参阅第 35-16 页上的了解 Rule Update Import Log 详细视图。系统还应用在上一步中指定的策略；请参阅第 4-10 页上的应用访问控制策略和第 19-7 页上的应用入侵策略。

注　如果在安装规则更新时出现错误消息，请联系支持部门。

使用自动一次性规则更新

许可证：任何环境

以下步骤说明如何通过自动连接到支持网站导入新的规则更新。仅当ASA FirePOWER 模块可访问互联网时才能使用这些步骤。

要自动导入规则更新，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Updates**，然后选择 **Rule Updates** 选项卡。

系统将显示 Rule Updates 页面。

提示　也可以点击 Rule Editor 页面 (**Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Rule Editor)** 上的 **Import Rules**。

步骤 2　或者，点击 **Delete All Local Rules**，然后点击 **OK**，以将创建或导入的所有用户定义规则移到被删除的文件夹。有关详情，请参阅第 23-96 页上的删除自定义规则。

步骤 3　选择 **Download new Rule Update from the Support Site**。

步骤 4　或者，在更新完成后，重新对应用策略：

- 选择 **Reapply intrusion policies after the rule update import completes** 以自动重新应用入侵策略。仅选择此选项更新规则和其他已更改的入侵策略设置，无需更新您进行的所有其他访问控制配置。您**必须**选择此选项与访问控制策略一起重新应用入侵策略；重新应用访问控制策略在这种情况下不执行全面的应用。
- 选择 **Reapply access control policies after the rule update import completes** 以自动重新应用访问控制、网络分析和文件策略，但不重新应用入侵策略。选择此选项也更新所有修改的访问控制高级设置的默认值。由于您无法独立于其父访问控制策略应用网络分析策略，因此如果要更新网络分析策略中的预处理器设置，**必须**重新应用访问控制策略。

步骤 5　点击 **Import**。

系统安装规则更新并显示 Rule Update Log 详细视图；请参阅第 35-16 页上的了解 Rule Update Import Log 详细视图。系统还应用在上一步中指定的策略；请参阅第 4-10 页上的应用访问控制策略和第 19-7 页上的应用入侵策略。

注　如果在安装规则更新时出现错误消息，请联系支持部门。

使用周期性规则更新

许可证：任何环境

可以在 Rule Updates 页面上设置为按日、周或月导入规则更新。

规则更新导入中的适用子任务按如下出现：下载，安装，基本策略更新，策略重新应用。完成一个子任务后，才会开始下一个子任务。请注意，您仅能应用已配置周期性导入的 ASA FirePOWER 模块之前应用的策略。

要安排周期性规则更新，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Updates**，然后选择 **Rule Updates** 选项卡。

系统将显示 Rule Updates 页面。

提示　也可以点击 Rule Editor 页面 (**Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Rule Editor**) 上的 **Import Rules**。

步骤 2　或者，点击 **Delete All Local Rules**，然后点击 **OK**，以将创建或导入的所有用户定义规则移到被删除的文件夹。有关详情，请参阅第 23-96 页上的删除自定义规则。

步骤 3　选择 **Enable Recurring Rule Update Imports**。

页面展开，其中显示用于配置周期性导入的选项。导入状态消息显示在 **Recurring Rule Update Imports** 部分下方。保存设置即会启用周期性导入。

提示　要禁用周期性导入，请清除 **Enable Recurring Rule Update Imports** 复选框并点击 **Save**。

步骤 4　在 **Import Frequency** 字段中，从下拉列表选择 **Daily**、 **Weekly** 或 **Monthly**。

如果选择每周或每月导入频率，请使用显示的下拉列表选择您要在星期几或几号导入规则更新。通过一次或多次点击或键入选项的首字母或数字并按 Enter 键，可以从周期性任务下拉列表中选择一个选项。

步骤 5　在 **Import Frequency** 字段中，指定要开始周期性规则更新导入的时间。

步骤 6　或者，在更新完成后，重新应用策略：

- 选择 **Reapply intrusion policies after the rule update import completes** 以自动重新应用入侵策略。仅选择此选项更新规则和其他已更改的入侵策略设置，无需更新您进行的所有其他访问控制配置。您**必须**选择此选项与访问控制策略一起重新应用入侵策略；重新应用访问控制策略在这种情况下不执行全面的应用。
- 选择 **Reapply access control policies after the rule update import completes** 以自动重新应用访问控制策略及其网络和文件策略，但不重新应用入侵策略。选择此选项也更新所有修改的访问控制高级设置的默认值。由于您无法独立于其父访问控制策略应用网络分析策略，因此如果要更新网络分析策略中的预处理器设置，**必须**重新应用访问控制策略。

步骤 7　点击 **Save** 以按照设置启用周期性规则更新导入。

Recurring Rule Update Imports 部分下方的状态信息会发生变化，以指明尚未运行规则更新。在计划的时间，系统安装规则更新并应用在上一步中指定的策略；请参阅第 4-10 页上的应用访问控制策略和第 19-7 页上的应用入侵策略。

在导入之前或导入过程中，可注销或执行其他任务。在导入过程中访问时，Rule Update Log 显示红色状态图标 （ ），此外，您还可以在 Rule Update Log 详细视图中查看消息。根据规则更新大小和内容，可能几分钟之后才会显示状态消息。有关详细信息，请参阅第 35-13 页上的查看规则更新日志。

注　如果在安装规则更新时出现错误消息，请联系支持部门。

导入本地规则文件

许可证：任何环境

本地规则是一个自定义标准文本规则，即从本地计算机导入的采用 ASCII 或 UTF - 8 编码的一个明文文本文件。可按照 Snort 用户手册中的说明创建本地规则 （可在 http://www.snort.org 上获得该手册）。

导入本地规则时，请注意：

- 文本文件名称可包含字母数字字符和空格，不可包含除下划线 (_)、句号 (.) 和破折号 (-) 以外的其他特殊字符。
- 不一定要指定生成器 ID (GID)；如果要这样做，可以仅为标准文本规则指定 GID 1，为敏感数据规则指定 GID 138。
- 首次导入规则时，请**勿**指定 Snort ID (SID) 或版本号；这样做是为了避免与其他规则（包括已删除的规则）的 SID 发生冲突。

  系统会自动为规则分配下一个可用的自定义规则 SID （1000000 或更高）以及版本号 1。
- 导入之前已经导入的本地规则的更新版本时，**必须**包含系统分配的 SID 以及高于当前版本号的版本号。

  查看某个当前本地规则的版本号，请显示 Rule Editor 页面 ，点击本地规则类别以展开文件夹，然后点击该规则旁边的 **Edit**。

- 可以恢复已删除的本地规则，方法是，导入使用系统分配的 SID 且版本号高于当前版本号的规则。请注意，删除本地规则时，系统会自动增加版本号；这样方便恢复本地规则。

  要查看已删除的本地规则的版本号，请显示 Rule Editor 页面，点击已删除的规则类别以展开文件夹，然后点击该规则旁边的 **Edit**。
- 不能导入包含 SID 大于 2147483647 的规则的规则文件；这种导入将会失败。
- 如果导入包含长于 64 个字符的源端口列表或目标地主机列表，导入将会失效。
- 系统始终将导入的本地规则设置为禁用状态；必须手动设置本地规则的状态后，才能将它们用于入侵策略中。有关详情，请参阅第 20-17 页上的设置规则状态。
- 必须确保文件中的规则不包含任何转义字符。
- 规则导入程序要求以 ASCII 或 UTF-8 编码格式导入所有自定义规则。
- 所有导入的本地规则都会自动保存在本地规则类别中。
- 所有已删除的本地规则从会从本地规则类别转移到已删除规则类别。
- 系统会导入以一个井号 (#) 开头的本地规则。
- 系统会忽略以两个井号 (##) 开头的本地规则，也就是说，不导入这样的规则。
- 如果启用某个导入的本地规则，而该规则将弃用的 `threshold` 关键字与某个入侵策略中的入侵事件阈值功能结合起来使用，策略验证将会失败。有关详情，请参阅第 20-19 页上的配置事件阈值。

要导入本地规则文件，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Update**，然后选择 **Rule Updates** 选项卡。

系统将显示 Rule Updates 页面。

步骤 2　选择 **Rule Update or text rule file to upload and install**，然后点击 **Choose File** 以浏览规则文件。请注意，以这种方式上传的所有规则保存在本地规则类别中。

提示　您**仅可**导入采用 ASCII 或 UTF-8 编码的明文文本文件。

步骤 3　点击 **Import**。

规则文件成功导入。确保在入侵策略中启用适当的规则。下次应用受影响的策略时，导入的规则才会激活。

注　在应用您的入侵策略之前，系统**不**使用新的规则集进行检查。有关步骤，请参阅第 4-10 页上的应用访问控制策略。

查看规则更新日志

许可证：任何环境

ASA FirePOWER 模块会为导入的规则更新和本地规则文件生成记录。

每个记录都包含时间戳、导入文件的用户名称以及指明导入成功或失败的状态图标。可保留导入的所有规则更新和本地规则文件的列表，删除列表中的任何记录，以及访问有关所有导入的规则和规则更新组成部分的详细记录。下表说明您在 Rule Update Log 中可以采取的操作。

表 35-2　规则更新日志操作

要.....	您可以.....
了解有关表中各列的更多信息	在第 35-14 页上的了解规则更新日志表中获得详细信息。
删除导入日志中的导入文件记录 （包括有关文件中所有对象的详细记录）	点击导入文件名称旁边的删除图标 ( )。 **注**　删除日志中的文件并不会删除导入到导入文件中的任何对象，而只是删除导入日志记录。
查看导入到规则更新或本地规则文件中的每个对象的详细信息	点击导入文件名称旁边的视图图标 ( )。

有关详细信息，请参阅以下各节：

- 第 35-14 页上的了解规则更新日志表介绍导入的规则更新和本地规则文件的列表中的字段。
- 第 35-15 页上的查看规则更新导入日志详细信息介绍导入到规则更新或本地规则文件中的每个对象的详细记录。
- 第 35-16 页上的了解 Rule Update Import Log 详细视图介绍 Rule Update Log 详细视图中的每个字段。

要查看规则更新日志，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Updates**，然后选择 **Rule Updates** 选项卡。

系统将显示 Rule Updates 页面。

提示　也可以点击 Rule Editor 页面 (**Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Rule Editor**) 上的 **Import Rules**。

步骤 2　点击 **Rule Update Log**。

系统将显示 Rule Update Log 页面。该页面列出每个导入的规则更新和本地规则文件。

了解规则更新日志表

许可证：任何环境

下表介绍导入的规则更新和本地规则文件列表中的字段。

表 35-3　规则更新日志字段

字段	说明
Summary	导入文件的名称。如果导入失败，文件名称下方会显示有关导入失败原因的简要说明。
Time	导入开始的时间和日期。

表 35-3　规则更新日志字段 （续）

字段	说明
User ID	触发导入的用户的用户名。
Status	导入有以下状态： • 成功 ( ) • 失败或进行中 ( ) **提示**　导入过程中， Rule Update Log 页面上会显示红色状态图标，表示导入失败或未完成；成功完成导入后，该红色状态图标会变为绿色状态图标。

点击规则更新或文件名称旁边的视图图标 ( ) 可查看规则更新或本地规则文件的 Rule Update Log 详细视图，点击删除图标 ( ) 可删除文件记录以及与文件一起导入的所有详细对象记录。

提示　导入规则更新时，可查看详细导入信息。

查看规则更新导入日志详细信息

许可证：任何环境

Rule Update Import Log 详细视图列出导入到规则更新或本地规则文件中的每个对象的详细记录。此外，还可以根据列出的记录创建仅包含符合特定需求的信息的自定义工作流程或报告。

下表介绍可在 Rule Update Import Log 详细视图上执行的具体操作。

表 35-4　Rule Update Import Log 详细视图操作

要.....	您可以.....
了解有关表中各列的更多信息	在第 35-16 页上的了解 Rule Update Import Log 详细视图中获得详细信息。

要查看 Rule Update Import Log 详细视图，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Updates**，然后选择 **Rule Updates** 选项卡。

系统将显示 Rule Updates 页面。

提示　也可以点击 Rule Editor 页面 (**Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Rule Editor**) 上的 **Import Rules**。

步骤 2　点击 **Rule Update Log**。

系统将显示 Rule Update Log 页面。

步骤 3　点击要查看的详细记录的文件的旁边的视图图标 ( )。

系统将显示详细记录的表视图。

了解 Rule Update Import Log 详细视图

许可证：任何环境

可以查看导入到规则更新或本地规则文件中的每个对象的详细记录。下表介绍 Rule Update Log 详细视图中的字段。

表 35-5　Rule Update Import Log 详细视图字段

字段	说明
Time	导入开始的时间和日期。
Name	导入对象的名称（对于规则，对应的是规则 Message 字段；对于规则更新，对应的是组成部分名称）。
Type	导入对象的类型，可以是以下类型之一： • `rule update component` （已导入的组成部分，例如规则包或策略包） • `rule` （对于规则而言，是指新的或更新后的规则；请注意，在版本 5.0.1 中，此值替换为 `update` 值，后者已被弃用） • `policy apply` （为导入启用了 **Reapply intrusion policies after the Rule Update import completes** 选项）
Action	指明对对象类型执行了以下其中一项操作： • `new` （对于规则而言，是指第一次把规则存储在此 ASA FirePOWER 模块上） • `changed` （对于规则更新组成部分或规则而言，规则更新组成部分已被修改，或者规则的版本号更高且 GID 和 SID 相同） • `collision` （对于规则更新组成部分或规则而言，由于其版本与现有组成部分或规则相冲突，因此跳过导入） • `deleted` （对于规则而言，已从规则更新删除规则） • `enabled` （对于规则更新编辑而言，已在系统提供的策略中启用了预处理器、规则或其他功能） • `enabled` （对于规则而言，已在系统提供的策略中启用了规则） • `drop` （对于规则而言，已在系统提供的策略中将规则设置为 Drop and Generate Events） • `error` （对于规则更新或本地规则文件而言，导入失败） • `apply` （为导入启用了 **Reapply intrusion policies after the Rule Update import completes** 选项）
Default Action	规则更新定义的默认操作。当导入对象类型是 `rule` 时，默认操作是 `Pass`、 `Alert` 或 `Drop`。对于所有其他导入对象类型，没有默认操作。
GID	规则的生成器 ID。例如， `1` (标准文本规则) 或 `3` (共享对象规则)。
SID	规则的 SID。
Rev	规则的版本号。
Policy	对于导入的规则而言，此字段显示 `All`，表示导入的规则包含在所有系统提供的入侵策略中。对于其他导入对象类型，此字段为空白。
Details	组成部分或规则独有的字符串。对于规则、GID、SID 以及已更改规则的上一个版本号，此字段显示为 `previously (GID:SID:Rev)`。对于未更改的规则，此字段为空白。
Count	记录数 (`1`)。当表受限时， Count 字段显示在表视图中，而且在默认情况下， Rule Update Log 详细视图受限于规则更新记录。

更新地理定位数据库

许可证：任何环境

思科地理定位数据库 (GeoDB) 是包含地理数据的数据库。ASA FirePOWER 模块提供国家/地区和大洲。系统检测与已经检测到的 IP 地址匹配的 GeoDB 信息时，可查看与 IP 地址相关的地理定位信息。思科定期发布 GeoDB 更新。

要更新 GeoDB，请使用 Geolocation Updates 页面 (**Configuration > ASA FirePOWER Configuration > Updates > Geolocation Updates**)。上传 GeoDB 更新时，这些更新会显示在该页面中。

安装过程一般需要 30 到 40 分钟。虽然 GeoDB 更新不会中断任何其他系统功能（包括持续收集地理定位信息），但是，这个过程确实会耗用系统资源。制定更新计划时需要考虑这一点。

本节说明如何计划和执行手动 GeoDB 更新。还可以利用自动更新功能安排 GeoDB 更新；有关详细信息，请参阅第 31-5 页上的自动运行地理定位数据库更新。

要更新地理定位数据库，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Updates**。

系统将显示 Product Updates 页面。

步骤 2　点击 **Geolocation Updates** 选项卡。

系统将显示 Geolocation Updates 页面。

步骤 3　将更新上传。

- 如果ASA FirePOWER 模块访问互联网，请点击 **Download and install geolocation update from the Support Site** 以检查以下任何一个支持网站上的最新更新：
  - **Sourcefire：**(https://support.sourcefire.com/)
  - **思科：**(http://www.cisco.com/cisco/web/support/index.html)
- 如果ASA FirePOWER 模块不能访问互联网，请手动从以下任何一个支持网站下载更新，然后点击 **Upload and install geolocation update**。点击 **Choose File** 浏览并选择更新，然后点击 **Import**：
  - **Sourcefire：**(https://support.sourcefire.com/)
  - **思科：**(http://www.cisco.com/cisco/web/support/index.html)

注　可直接从支持网站下载更新（手动下载，或者点击 Geolocation Updates 页面上的 **Download and install geolocation update from the Support Site**）。如果通过邮件传输更新文件，可能会损坏更新文件。

更新过程开始。更新安装的平均持续时间是 30 到 40 分钟。可以在任务队列中监控更新的进度 (**Monitoring > ASA FirePOWER Monitoring > Task Status**)。

步骤 4　完成更新后，返回到 Geolocation Updates 页面，以确认 GeoDB 内部版本号与安装的更新相匹配。

GeoDB 更新将会覆盖之前的所有 GeoDB 版本并立即生效。尽管 GeoDB 需要几分钟时间方可在部署中生效，但完成更新后，无需重新应用访问控制策略。

监控系统

ASA FirePOWER 模块 ASA FirePOWER 模块提供许多有用的监控功能，帮助您在一个页面上对系统进行日常管理。例如，在 Host Statistics 页面中，您可以监控基本主机统计信息。以下各节提供有关该系统提供的监控功能的详细信息：

- 第 36-1 页上的查看主机统计信息描述如何查看主机信息，例如：
- 系统运行时间
- 磁盘和内存使用情况
- 系统进程
- 入侵事件信息
- 第 36-2 页上的监控系统状态和磁盘空间使用情况介绍如何查看基本事件和磁盘分区信息。
- 第 36-2 页上的查看系统进程状态介绍如何查看基本进程状态。
- 第 36-4 页上的了解运行的进程介绍设备上运行的基本系统进程。

查看主机统计信息

许可证：任何环境

Statistics 页面列出如下统计信息的当前状态：

- 一般主机统计信息；有关详细信息，请参阅主机统计信息表
- 入侵事件信息（需要保护）；有关详细信息，请参阅第 26-1 页上的查看事件

下表介绍了 Statistics 页面列出的主机统计信息。

表 36-1　　主机统计信息

类别	说明
时间	系统当前时间。
正常运行时间	系统上次启动后持续的天数（如果适用）、小时数和分钟数。
内存使用率	正使用的系统内存的百分比。
Load Average	过去 1 分钟、 5 分钟和 15 分钟内 CPU 队列的平均进程数。
磁盘使用情况	正使用的磁盘空间的百分比。点击箭头查看更详细的主机统计信息。有关详情，请参见第 36-2 页上的监控系统状态和磁盘空间使用情况。
流程	系统中运行的进程摘要。有关详情，请参见第 36-2 页上的查看系统进程状态。

要查看 Statistics 页面，请执行以下操作：

步骤 1　选择 **Monitoring > ASA FirePOWER Monitoring > Statistics**。

系统将显示 Statistics 页面。

监控系统状态和磁盘空间使用情况

许可证：任何环境

Statistics 页面的 Disk Usage 部分提供磁盘使用情况快览，可以按类别和分区状态进行查看。如果您在设备上安装了一个恶意软件存储包，您还可以查看分区状态。您可以随时监控此页面，确保系统进程和数据库有充足的磁盘空间可用。

要访问磁盘使用情况信息，请执行以下操作：

步骤 1　选择 **Monitoring > ASA FirePOWER Monitoring > Statistics**。

系统将显示 Statistics 页面。

有关磁盘使用类别的详细信息，请参阅第 29-3 页上的了解 Disk Usage 构件。

步骤 2　点击 **Total** 旁边的向下箭头将其展开。

Disk Usage 部分将展开，显示分区使用情况。如果您安装有一个恶意软件存储包，系统也会显示 `/var/storage` 分区使用情况。

查看系统进程状态

许可证：任何环境

在 Host Statistics 页面的 Processes 部分，您可以查看一台设备上正在运行的进程。它为每个运行的进程提供常规进程信息和特定信息。

下表介绍了进程列表中显示的各列。

表 36-2　进程状态

列	说明
Pid	进程 ID 编号
用户名	运行进程的用户或组的名称
Pri	进程优先级
Nice	*nice* 值是表示一个进程计划优先级的值。值范围为 -20（最高优先级）到 19（最低优先级）
规格	进程使用的内存大小（以千字节计，除非数值后是 m，即表示兆字节）
Res	内存中常驻页面文件的数量（以千字节计，除非数值后是 m，即表示兆字节）

表 36-2　　进程状态 （续）

列	说明
州	进程状态： • D - 进程处于不可中断休眠（通常 Input/Output） • N - 进程有一个正优先值 • R - 进程可运行（在运行队列中） • S - 进程处于休眠模式 • T - 进程被跟踪或停止 • W - 进程在分页 • X - 进程已废弃 • Z - 进程已失效 • < - 进程有一个负优先值
时间	进程运行的时间（格式为小时:分钟:秒）
Cpu	进程正在使用的 CPU 的百分比
命令	进程的可执行名称

要展开进程列表，请执行以下操作：

步骤 1　选择 **Monitoring > ASA FirePOWER Monitoring > Statistics**。

系统将显示 Statistics 页面。

步骤 2　点击 **Processes** 旁边的向下箭头。

进程列表将展开，列出常规进程状态信息，其中包括运行任务数量和类型、当前时间、当前系统正常运行时间、系统平均负载、 CPU、内存和交换信息，以及每个运行进程的特定信息。

Cpu(s) 列出以下 CPU 使用信息：

- 用户进程使用百分比
- 系统进程使用百分比
- 优先使用情况百分比（拥有负优先值进程的 CPU 使用情况，表示更高优先级）

  优先值是指系统进程的计划优先级，范围为 -20（最高优先级）到 19（最低优先级）。
- 空闲使用百分比

Mem 列出如下内存使用信息：

- 内存中千字节总数
- 内存中已使用千字节总数
- 内存中空闲的千字节总数
- 内存中缓存的千字节总数

Swap 列出如下交换使用信息：

- 交换空间中千字节总数
- 交换空间中已使用千字节总数

- 交换空间中空闲的千字节总数
- 交换空间中缓存的千字节总数

注　有关设备上运行进程类型的详细信息，请参阅第 36-4 页上的了解运行的进程。

要折叠进程列表，请执行以下操作：

步骤 1　点击 **Processes** 旁边的向上箭头。

进程列表将折叠。

了解运行的进程

许可证：任何环境

设备上运行有两个不同类型的进程：后台守护程序和可执行文件。后台守护程序始终运行，可执行文件在需要时运行。

有关详细信息，请参阅：

- 第 36-4 页上的了解系统后台守护程序
- 第 36-5 页上的了解可执行文件和系统实用程序

了解系统后台守护程序

许可证：任何环境

后台守护程序在设备上持续运行。他们确保服务可用，并在需要时产生进程。下表列出了 Process Status 页面可以看到的后台守护程序，并对其功能进行简要说明。

注　下表并非一台设备上可运行的所有进程的详尽列表。

表 36-3　系统后台守护程序

后台守护程序	说明
crond	管理计划命令的实施（cron 作业）
dhclient	管理动态主机 IP 地址
httpd	管理 HTTP （Apache 网络服务器）进程
httpsd	管理 HTTPS （使用 SSL 的 Apache 网络服务器）服务，检查正在运行的 SSL 和有效的证书身份验证；在后台运行，为设备提供安全的网络接入
keventd	管理 Linux 内核事件通知消息
klogd	管理 Linux 内核消息监听和记录

表 36-3　　系统后台守护程序 （续）

后台守护程序	说明
kswapd	管理 Linux 内核交换内存
kupdated	管理 Linux 内核更新进程，执行磁盘同步
mysqld	管理 ASA FirePOWER 模块数据库进程
ntpd	管理网络时间协议 (NTP) 进程
pm	管理所有思科进程，启动所需进程，重新启动所有意外发生故障的进程
reportd	管理报告
safe_mysqld	管理数据库安全模式操作；如果出现错误，重新启动数据库后台守护程序，并向文件中记录运行时间信息
sfmgr	使用到一台设备的 sftunnel 连接，为远程管理和配置该设备提供 RPC 服务
sftroughd	侦听进入套接字的连接，然后调用正确的可执行程序（通常是思科消息代理、sfmb）处理请求
sftunnel	为需要与远程设备通信的所有进程提供安全的通信通道
sshd	管理安全外壳 (SSH) 进程；在后台运行，为设备提供 SSH 接入
syslogd	管理系统日志 (syslog) 流程

了解可执行文件和系统实用程序

许可证：任何环境

系统会有许多可执行文件，它们在其他进程或用户操作执行时开始运行。下表介绍了在 Process Status 页面可能会看到的可执行程序。

表 36-4　　系统可执行程序和实用程序

可执行程序	说明
awk	执行用 `awk` 编程语言书写的程序的实用程序
bash	GNU Bourne-Again SHell
cat	读取文件并将内容写入标准输出的实用程序
chown	更改用户和组文件权限的实用程序
chsh	更改默认登录外壳的实用程序
cp	复制文件的实用程序
df	列出设备可用空间量的实用程序
echo	将内容写入标准输出的实用程序
egrep	按特定输入搜索文件和文件夹、支持标准 grep 不支持的正则表达式扩展集的实用程序
find	按特定输入循环搜索目录的实用程序
grep	按特定输入搜索文件和目录的实用程序
halt	停用服务器的实用程序
httpsdctl	处理安全 Apache 网络进程

表 36-4　　系统可执行程序和实用程序（续）

可执行程序	说明
hwclock	允许访问硬件时钟的实用程序
ifconfig	表示网络配置可执行程序。确保 MAC 地址保持不变
iptables	根据 Access Configuration 页面所做的更改处理访问限制。有关访问配置的详细信息，请参阅第 32-4 页上的配置设备的访问列表。
iptables-restore	处理 iptables 文件恢复
iptables-save	处理对 iptables 保存的更改
kill	可用来结束会话和进程的实用程序
killall	可用来结束所有会话和进程的实用程序
ksh	Korn Shell 的公共域版本
记录器	提供通过命令行访问系统日志后台守护程序方法的实用程序
md5sum	为指定文件打印校验和以及块数量的实用程序
mv	移动（重命名）文件的实用程序
myisamchk	指数据库表校验和修复
mysql	指数据库进程；可能出现多个实例
openssl	指创建身份验证证书
perl	指一个 perl 进程
ps	将进程信息写入标准输出的实用程序
sed	用来编辑一个或多个文本文件的实用程序
sh	Korn Shell 的公共域版本
shutdown	关闭设备的实用程序
sleep	在指定秒数内暂停进程的实用程序
smtpclient	启用邮件事件通知功能后，处理邮件传输的邮件客户端
snmptrap	将 SNMP 陷阱数据转发到启用 SNMP 通知功能后指定的 SNMP 陷阱服务器
snort （需要保护）	表示 Snort 正在运行
ssh	表示与设备连接的安全外壳 (SSH)
sudo	指 sudo 进程，其允许管理员以外的用户运行可执行程序
顶部	显示最大 CPU 进程信息的实用程序
touch	用来更改指定文件的访问和修改时间的实用程序
vim	用来编辑文本文件的实用程序
wc	执行指定文件行、字和字节计数的实用程序

使用备份和恢复

备份和恢复是所有系统维护计划的重要部分。当每个组织的备份计划极具个性化时， ASA FirePOWER 模块为归档数据提供一种机制，以便防御中心中的数据可在发生灾难的情况下恢复。

请注意有关备份和恢复的以下限制：

- 备份仅对您创建其时所使用的产品版本有效。
- 仅在以下情况下，您才可以将备份并且运行的 ASA FirePOWER 模块软件版本与用于创建该备份的该软件的版本完全相同。

注意事项 请勿使用备份和恢复进程来在 ASA FirePOWER 模块之间复制配置文件。配置文件包括 ASA FirePOWER 模块设备的唯一识别信息，并且不能共享。

注意事项 如果应用了任何入侵规则更新，不会备份这些更新。在恢复**之后**，需要应用最新的规则更新。

可以将备份文件保存到设备或本地计算机。

有关详细信息，请参阅以下各节：

- 有关创建备份文件的信息，请参阅第 37-1 页上的创建备份文件。
- 有关创建备份配置文件以便稍后可用作创建备份模板的信息，请参阅第 37-3 页上的创建备份配置文件。
- 有关从本地主机上传备份文件的信息，请参阅第 37-3 页上的从本地主机上传备份。
- 有关如何恢复设备的备份文件的信息，请参阅第 37-4 页上的从备份文档恢复设备。

创建备份文件

许可证：任何环境

您可以使用模块界面执行ASA FirePOWER 模块的备份。要查看和利用现有系统备份，请转到 Backup Management 页面。除事件数据外，还应定期保存包含恢复设备所需的所有配置文件的备份文件。在测试配置更改时也可能需要备份系统，以便可以根据需要还原已保存的配置。可以选择将备份文件保存到设备或本地计算机。

如果设备没有足够的磁盘空间，将无法创建备份文件；如果备份进程使用 90% 以上的可用磁盘空间，备份可能会失败。如果需要，请删除旧备份文件，将旧备份文件从设备转出。

此外，或者如果备份文件超过 4 GB，还可以通过 SCP 将其复制到远程主机。从本地计算机上传的备份文件不能超过 4 GB。

注意事项 如果为安全区域配置了任何接口关联，将不会备份这些关联。在恢复后，必须重新配置它们。有关详细信息，请参阅第 2-30 页上的使用安全区域。

要 ASA FirePOWER 模块创建该设备的备份文件，请执行以下操作：

步骤 1 选择 **Configuration > ASA FirePOWER Configuration > Tools > Backup/Restore**。

系统将显示 Backup Management 页面。

步骤 2 点击 **Device Backup**。

系统将显示 Create Backup 页面。

步骤 3 在 **Name** 字段中，键入一个备份文件名称。可以使用字母数字字符、标点符号和空格。

步骤 4 或者，为了在备份完成时收到通知，请选择 **Email** 复选框并在随附的文本框中键入邮件地址。

注 要接收邮件通知，您必须配置中继主机，如第 32-6 页上的配置邮件中继主机和通知地址中所述。

步骤 5 或者，要使用安全复制 (SCP) 将备份归档复制到不同的设备，请选择 **Copy when complete** 复选框，然后在随附的文本框中键入以下信息：

- 在 **Host** 字段中，键入要复制备份的机器的主机名或 IP 地址
- 在 **Path** 字段中，键入要复制备份目录路径
- 在 **User** 字段中，键入要用于登录 Telnet 远程机器的用户名
- 在 **Password** 字段中，键入该用户名的密码
  如果希望使用 SSH 公共密钥而不是密码来访问远程机器，则必须将 **SSH Public Key** 字段中的内容到该机器上指定用户的 `authorized_keys` 文件中。

在此选项处于清除状态时，系统在远程服务器上存储备份期间使用的临时文件；选择此选项时，不在远程服务器上存储临时文件。

提示 思科建议定期将备份保存到远程位置，这样才可以在系统故障时恢复设备。

步骤 6 您有以下选项：

- 要将备份文件保存到设备，请点击 **Start Backup**。

  备份文件会保存到 `/var/sf/backup` 目录中。

  当备份过程完成后，可以在 Restoration Database 页面查看文件。有关恢复备份文件的信息，请参阅第 37-4 页上的从备份文档恢复设备。
- 要将此配置保存为可供以后使用的备份配置文件，请点击 **Save As New**。

  您可以通过选择 **Configuration > ASA FirePOWER Configuration > Tools > Backup/Restore**，然后点击 **Backup Profiles** 来修改或删除备份配置文件。有关详情，请参见第 37-3 页上的创建备份配置文件。

创建备份配置文件

许可证：任何环境

可以使用 Backup Profiles 页面创建包含要用于不同类型备份的设置的备份配置文件。稍后可以在设备上备份文件时，选择这两个配置文件。

提示 当如所第 37-1 页上的创建备份文件述创建备份文件时，自动创建备份配置文件。

要创建配置文件，请执行以下操作：

步骤 1 选择 **Configuration > ASA FirePOWER Configuration > Tools > Backup/Restore**。

系统将显示 Backup Management 页面。

步骤 2 点击 the **Backup Profiles** 选项卡。

系统将显示 Backup Profiles 页面和现有备份配置文件列表。

提示 可以点击编辑图标 ( ) 来修改现有配置文件或点击删除图标 ( ) 从列表中删除配置文件。

步骤 3 点击 **Create Profile**。

系统将显示 Create Backup 页面。

步骤 4 键入一个备份配置文件名称。可以使用字母数字字符、标点符号和空格。

步骤 5 根据需要配置备份配置文件。

有关此页面中的选项的详细信息，请参阅第 37-1 页上的创建备份文件。

步骤 6 点击 **Save As New** 来保存备份配置文件。

系统将显示 Backup Profiles 页面，此时新配置文件显示在列表中。

从本地主机上传备份

许可证：任何环境

如果使用Backup Management表中描述的下载功能将备份文件下载到本地主机，可以将文件上传到 ASA FirePOWER 模块。

如果备份文件包含 PKI 对象，与内部 CA 和内部证书对象关联的私有密钥在上传时将通过随机生成的密钥来重新加密。

提示 无法从本地主机上传大于 4 GB 的备份。还可以使用 SCP 将备份复制到远程主机，然后从中检索。

要从本地主机上传备份，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Tools > Backup/Restore**。

系统将显示 Backup Management 页面。

步骤 2　点击 **Upload Backup**。

系统将显示 Upload Backup 页面。

步骤 3　点击 **Choose File** 并导航到要上传的备份文件。

在选择要上传的文件后，点击 **Upload Backup**。

步骤 4　点击 **Backup Management** 以返回 Backup Management 页面。

备份文件上传并在备份列表显示。在防御中心ASA FirePOWER 模块验证文件完整性之后，刷新 Backup Management 页面显示详细文件系统信息。

从备份文档恢复设备

许可证：任何环境

使用 Backup Management 页面，可以从备份文件恢复设备。要恢复备份，备份文件中的 VDB 版本必须与设备的当前 VDB 版本相符。完成恢复过程后，**必须**应用最新的思科规则更新。

如果使用本地存储，备份文件将保存到 `/var/sf/backup`，并与 `/var` 分区中的已用磁盘空间量一起列示在 Backup Management 页面底部。

注　如果在备份完成后添加许可证，即使备份恢复，这些许可证不会删除也不会被覆盖。为防止恢复时出现冲突，请在恢复备份之前移除这些许可证，记住许可证使用位置，并在恢复备份之后添加和重新配置它们。如果发生冲突，请与技术支持部门联系。

下表说明在 Backup Management 页面的各列和图标。

表 37-1　Backup Management

功能	说明
系统信息	原始设备名称、类型和版本。注意只能将备份恢复到同样的设备类型和版本。
创建日期	备份文件创建的日期和时间
文件名	备份文件的全名
VDB Version	备份时在设备上运行的漏洞数据库 (VDB) 版本。
位置	备份文件的位置
Size (MB)	备份文件的大小，以兆字节计算
View	点击备份文件的名称可查看压缩备份文件中的文件列表。
恢复	点击所选的备份文件可将其恢复其到设备。如果 VDB 版本与备份文件中的 VDB 版本不相符，将禁用此选项。
下载	点击所选的备份文件可将其保存到本地计算机。

表 37-1　Backup Management （续）

功能	说明
删除	点击所选的备份文件可将其删除。
升级	在防御中心中，当选择先前创建的本地备份时，点击可将备份发送到指定的远程备份位置。

要从备份文件恢复设备，请执行以下操作：

步骤 1　选择 **Configuration > ASA FirePOWER Configuration > Tools > Backup/Restore**。

系统将显示 Backup Management 页面。

步骤 2　要查看备份文件的内容，请点击该文件的名称。

系统将显示清单，列出每个文件名称、所有者和权限及其文件大小和日期。

步骤 3　点击 **Backup Management** 以返回 Backup Management 页面。

步骤 4　选择要恢复的备份文件并点击 **Restore**。

系统将显示 Restore Backup 页面。

请注意，如果备份中的 VDB 版本与设备当前安装的 VDB 版本不相符， **Restore** 按钮会变为灰色。

注意事项　此步骤会覆盖所有配置文件，会覆盖所有事件数据。

步骤 5　要恢复文件，请选择以下选项之一或两项均选择：

- **Replace Configuration Data**
- **Restore Event Data**

步骤 6　点击 **Restore** 开始恢复。

设备将使用指定的备份文件恢复。

步骤 7　重新启动设备。

步骤 8　将最新思科的规则更新重新应用到规则更新。

步骤 9　将任何访问控制、入侵和系统策略重新应用到恢复的系统。

生成故障排除文件

某些情况下，如果您的设备有问题，支持人员可能要求您生成故障排除文件以帮助诊断该问题。您可以选择下表中列出的任何选项以定制 ASA FirePOWER 模块报告的故障排除数据。

表 A-1 可选择的故障排除选项

该选项.....	报告.....
Snort Performance and Configuration	与设备上的 Snort 相关的数据和配置设置
Hardware Performance and Logs	与设备硬件性能相关的数据和日志
System Configuration, Policy, and Logs	与设备的当前系统配置相关的配置设置、数据和日志
Detection Configuration, Policy, and Logs	与对设备的检测相关的配置设置、数据和日志
Interface and Network Related Data	与设备的内联集和网络配置相关的配置设置、数据和日志
Discovery, Awareness, VDB Data, and Logs	与设备上的当前发现和感知配置相关的配置设置、数据和日志
Upgrade Data and Logs	与设备的前期升级相关的数据和日志
All Database Data	包含在故障排除报告中的所有数据库相关数据
All Log Data	设备数据库收集的所有日志
Network Map Information	当前网络拓扑数据

请注意，在所报告的数据方面，某些选项重叠，但是无论您选择什么选项，故障排除文件都不会包含冗余备份。

有关详细信息，请参阅：

- 第 A-1 页上的生成设备故障排除文件
- 第 A-2 页上的下载故障排除文件

生成设备故障排除文件

许可证：任何环境

使用以下步骤生成可以发送给支持人员的定制的故障排除文件。

要生成故障排除文件，请执行以下操作：

步骤 1 在 ASDM 中，选择**Configuration > ASA FirePOWER Configuration > Tools > Troubleshooting**。

步骤 2 点击 **Generate Troubleshooting Files**。

系统将显示 Troubleshooting Options 弹出窗口。

步骤 3　选择 **All Data** 以生成所有可能的故障排除数据或选择单个复选框来自定义报告。有关详细信息，请参阅可选择的故障排除选项表。

步骤 4　点击 **OK**。

ASA FirePOWER 模块生成故障排除文件。可以在任务队列中监控文件生成进程 (**Monitoring > ASA FirePOWER Monitoring > Task Status**)。

步骤 5　继续执行下一节下载故障排除文件中的操作步骤。

下载故障排除文件

许可证：任何环境

使用以下步骤下载所生成的故障排除文件的副本。

要下载故障排除文件，请执行以下操作：

步骤 1　在 ASDM 中，选择 **Monitoring > ASA FirePOWER Monitoring > Task Status**。

系统将显示 Task Status 页面。

步骤 2　找出对应所生成的故障排除文件的任务。

步骤 3　在设备生成故障排除文件并且任务状态变更为 `Completed` 之后，点击 **Click to retrieve generated files**。

步骤 4　按照浏览器的提示下载文件。

文件下载到单个 `.tar.gz` 文件中。

步骤 5　按照支持人员的指示将故障排除文件发送给思科。

导入和导出配置

您可使用 Import/Export 功能在同类设备之间复制多种类型的配置，包括策略。配置导入和导出不应作为备份工具，但可简化将新 ASA FirePOWER 模块的过程。

您可导入和导出下列配置：

- 访问控制策略及其相关网络和文件策略
- 入侵策略
- 系统策略
- 警报响应

要导入已导出的配置，两种必须ASA FirePOWER 模块运行相同软件版本。要导入一个导出的入侵或访问控制策略，两个设备的规则更新版本也必须匹配。

有关详细信息，请参阅：

- 第 B-1 页上的导出配置
- 第 B-3 页上的导入配置

导出配置

许可证：任何环境

您可导出单项配置，也可立即导出一组（相同类型或不同类型的）配置。当您稍后将软件包导入另一台设备时，您可选择要导入软件包中的哪些配置。

导出配置时，设备也导出该配置的版本信息。 FireSIGHT 系统 ASA FirePOWER 模块使用该信息确定能否将该配置导入另一台设备；无法导入设备上已存在的配置版本

此外，导出配置时，设备也导出该配置依存的系统配置，

提示 在 ASA FirePOWER 模块的许多列表页面中，列表项旁均包括导出图标 ( )。如果该图标存在，您可将其作为下列导出步骤的快速替代项。

您可导出以下配置：

- *警报响应* - 警报响应是一组配置，可供 ASA FirePOWER 模块与您计划发送警报所在的外部系统进行交互。
- *访问控制策略* - 可对访问控制策略包括的各个元素进行配置，以确定系统如何管理网络流量。这些组件包括访问控制规则；关联的入侵、文件和网络策略；以及规则和策略使用的对象，包括入侵变量集。导出访问控制策略也会导出该策略的所有设置和元素，但 URL 信誉和类别除外（如存在），这些 URL 信誉和类别在所有设备上均相同且用户无法更改。请注意，要导入访问控制策略，导出和导入 ASA FirePOWER 模块的规则更新版本必须匹配。

  如果导出的访问控制策略或其包含引用地理定位数据的规则，则将使用导入地理定位数据库 (GeoDB) 更新版本。
- *入侵策略* - 可配置入侵策略包括的各种元素，以检查网络流量是否存在入侵和政策违反之情况。这些组件是检测协议报头值、负载内容和某些数据包大小特征的入侵规则；和其他高级设置。

  导出入侵策略也会导出该策略的所有设置。例如，如果您选择设置事件生成规则，或为一条规则设置 SNMP 警报，或打开策略的敏感数据预处理程序，则这些设置仍然保留在已导出的策略中。自定义规则、自定义规则分类和用户定义的变量也会随策略一起导出。

  请注意，如果您导出的入侵策略与另一个入侵策略共享一个层，则该共享层将复制至正在导出的策略中，共享关系因而终止。当您将入侵策略导入另一台设备时，可根据自己的需求编辑已导入的策略，包括删除，添加和共享层。

  如果您将入侵策略从一个 ASA FirePOWER 模块导出到另一个时，如果第二个 ASA FirePOWER 模块 具有配置不同的默认变量，则已导入的策略可能有不同的表现。

注　不能使用 Import/Export 功能更新漏洞研究团队 (VRT) 创建的规则。相反，请下载并应用最新的规则更新版本；请参阅第 35-8 页上的导入规则更新和本地规则文件。

- *系统策略* - 系统策略控制一台 ASA FirePOWER 模块可能类似于部署过程中其他ASA FirePOWER 模块的各个方面，包括时间设置、和 SNMP 设置等。

注　导出过程可能需要几分钟，取决于正在导出的配置数量以及这些配置引用的对象数量。

要导出一项或多项配置，请执行以下操作：

步骤 1　确保导出配置的 ASA FirePOWER 模块和计划导入配置的 ASA FirePOWER 模块运行相同的版本。如果导出入侵或访问控制策略，请确保规则更新版本匹配。

如果 ASA FirePOWER 模块的版本（以及规则更新版本，如适用）不匹配，导入将失败。

步骤 2　选择 **Configuration > ASA FirePOWER Configuration > Tools > Import Export**。

系统将显示 Import/Export 页面，其中包括 ASA FirePOWER 模块上的配置列表。请注意，无配置需要导出的配置类别不显示在此列表中。

提示　点击配置类型旁的折叠文件夹图标 ( )，即可折叠配置列表。点击配置类型旁的展开文件夹图标 ( )，即可显示配置。

步骤 3　选择要导出的配置旁的复选框，并且点击 **Export**。

步骤 4　按照提示将已导出软件包保存至计算机。

导入配置

许可证：任何环境

可将从一台设备导出的配置导入另一台设备，只要设备支持此操作。

视乎正在导入的配置的类型，谨记以下要点：

- 确保导入配置的 ASA FirePOWER 模块与用来导出配置的 ASA FirePOWER 模块运行相同版本的软件。如果导入入侵或访问控制策略，两台设备上的规则更新版本也必须匹配。如果版本不匹配，导入将失败。
- 不支持 MDC 的控制面板如果导入根据区域评估流量的访问控制策略，则必须将已导入策略中的区域映射至导入 ASA FirePOWER 模块上的区域。映射区域时，其类型必须匹配。因此，只有先在导入ASA FirePOWER 模块上创建所需的任何区域类型，然后才能开始导入。有关安全区域的详细信息，请参阅第 2-30 页上的使用安全区域。
- 如果导入的访问控制策略包括名称与现有对象或对象组相同的对象或对象组，则您必须重命名该对象或对象组。
- 如果导入访问控制策略或入侵策略，导入进程将用已导入默认变量取代默认变量集中的现有默认变量。如果现有默认变量集包含不属于导入默认变量集的自定义变量，则会保留该唯一的变量。
- 如果导入的入侵策略与另一个入侵策略共享一个层，导出进程将终止此共享关系，之前的共享层将复制至软件包。换言之，已导入的入侵策略不包含共享层。

注　不能使用 Import/Export 功能更新漏洞研究团队 (VRT) 创建的规则。相反，请下载并应用最新的规则更新版本；请参阅第 35-8 页上的导入规则更新和本地规则文件。

ASA FirePOWER 模块由于可在单一软件包中导出多项配置，因此，导入软件包时必须选择将导入软件包中的哪些配置。

当尝试导入配置时， ASA FirePOWER 模块会判断该配置在设备中是否已存在。如果存在冲突，则可：

- 保留现有配置，
- 使用新配置替换现有配置，
- 保留最新配置，或
- 导入该配置作为新配置。

如在目标系统上对已导入的配置做出修改，然后重新导入该配置，则必须选择要保留该配置的何种版本。

视乎正在导入的配置数量以及这些配置所引用的对象数量，导入过程可能需要几分钟。

要导入一项或多项配置，请执行以下操作：

步骤 1　确保导出配置的 ASA FirePOWER 模块与计划导入配置的模块运行相同版本 FireSIGHT 系统。如果您要导入入侵或访问控制策略，还必须确保规则更新版本匹配。

如果 ASA FirePOWER 模块的版本（以及规则更新版本，如适用）不匹配，导入将失败。

步骤 2　导出要导入的配置；请参阅第 B-1 页上的导出配置。

步骤 3　在您想导入配置的设备上，选择 **Configuration > ASA FirePOWER Configuration > Tools > Import Export**。

系统将显示 Import Export 页面。

提示　点击配置类型旁的折叠文件夹图标 ( )，即可折叠配置列表。点击配置类型旁的展开文件夹图标 ( )，即可显示配置。

步骤 4　点击 **Upload Package**。

系统将显示 Upload Package 页面。

步骤 5　此时您有两种选择：

- 键入要上传的配置包的路径。
- 点击 **Upload File**，以查找软件包。

步骤 6　点击 **Upload**。

上传结果取决于软件包的内容。

- 如果软件包的配置与设备中现有版本完全匹配，将显示一条消息表明该版本已存在。设备的配置已为最新，无需导入。
- 如果您的设备与导出软件包的设备之间有 ASA FirePOWER 模块或（如适用）规则更新版本不匹配，系统将显示一条消息，表明无法导入软件包。更新 ASA FirePOWER 模块或规则更新版本并重试。
- 如果软件包包含的任何配置或规则版本在设备上不存在，系统将显示 Package Import 页面。继续执行下一步。

步骤 7　选择想要导入的配置并点击 **Import**。

导入进程开始解析，结果如下：

- 如果导入的配置在 ASA FirePOWER 模块上没有旧版本，导入将自动完成，并且系统将显示导入成功的消息。跳过该步骤的其他部分。
- 如果正在导入的访问控制策略包括安全区域，系统将显示 Access Control Import Resolution 页面。继续执行第 8 步。
- 如果导入的配置在设备上存在旧版本，系统将显示 Import Resolution 页面。继续执行第 9 步。

步骤 8　在每个导入安全区域旁，选择一个类型匹配的现有本地安全区域来进行映射，并点击 **Import**。

返回第 7 步。

步骤 9　展开每项配置并选择适当的选项。

- 要保留设备上的配置，请选择 **Keep existing**。
- 要用已导入的配置替换设备上的配置，请选择 **Replace existing**。
- 要保留最新配置，请选择 **Keep newest**。
- 要将已导入的配置另存为新配置，请选择 **Import as new**，或者，编辑配置名称。

  如果正在导入的访问控制策略包括启用了清空列表或自定义检测列表的文件策略，则 **Import as new** 选项不可用。
- 如果正在导入的访问控制策略或已保存搜索包括一个从属对象，既可接受建议的名称，也可重命名该对象。系统始终将这些从属对象作为新对象导入。无法选择保留或替换现有对象。请注意，对象和对象组在系统中的处理方式相同。

步骤 10　点击 **Import**。

配置导入成功。

查看长时间运行任务的状态

某些可在 ASA FirePOWER 模块上执行的任务不会立即完成，而是需要运行一段时间，例如应用策略或安装更新。可在任务队列中检查这些长时间运行任务的进度。任务队列还可以在任务解决成功或失败时报告。

有关详细信息，请参阅：

- 第 C-1 页上的查看任务队列
- 第 C-2 页上的管理任务队列

查看任务队列

许可证： 任何环境

执行长时间运行任务时，任务队列会报告这些任务状态，例如应用策略或安装更新。任务队列将提供有关复杂任务的信息并在任务完成时报告。

可在 Task Status 页面中查看任务队列，该页面每 10 秒钟自动刷新一次。

Job Summary 部分显示页面中列出的任务状态，如下表所述。

表 C-1　　任务队列任务类型

任务类型	说明
正在运行	当前正在进行的任务数。
正在等待	等待进行中任务完成后再运行的任务数。
已完成	成功完成的任务数。
正在重试	正在自动重试的任务数。请注意，并非所有的任务都可以重试。
已停止	由于系统更新而中断的任务数。已停止的任务不能恢复；必须手动将其从任务队列中删除。
失败	未成功完成的任务数。

Jobs 部分显示有关每项任务的信息，包括简要描述、任务启动时间、任务的当前状态，状态上一次发生变化的时间 相同类型的任务会一起显示在任务组中。

为确保 Task Status 页面快速载入， ASA FirePOWER 模块 从队列中移除时间超过一个月的所有已完成、已失败和已停止的任务，且从包含 1000 多个任务的任何任务组中移除最早的任务，每周一次。还可以从队列中手动移除任务；请参阅管理任务队列了解相关指示。

要查看任务队列，请执行以下操作：

步骤 1　此时您有两种选择：

- 如果手动启动任务，请在启动任务时显示的通知框中点击 **Task Status** 链接。

  系统在弹出窗口中显示 Task Status 页面。
- 如果已安排任务，或者，如果任务并非从正在查看的页面启动，请选择 **Monitoring > ASA FirePOWER Monitoring > Task Status**。

  系统将显示 Task Status 页面。

有关可在 Task Status 页面执行的操作的信息，请参阅管理任务队列。

管理任务队列

许可证： 任何环境

则在查看任务队列时可执行若干操作（请参阅第 C-1 页上的查看任务队列），如下表所述。

表 C-2　　任务队列操作

要.....	您可以.....
从任务队列中移除所有已完成的任务	点击 **Remove Completed Jobs**。
从任务队列中移除所有已失败的任务	点击 **Remove Failed Jobs**。
从任务队列中移除一个任务	点击要删除的任务旁的删除图标 ( )。 请注意，不能删除正在运行的任务。如果需要删除正在运行的任务（例如，如果该任务反复失败），请联系支持部门。
折叠任务组并隐藏任务	点击已展开任务组旁的已打开文件夹图标 ( )。
展开任务组并查看任务	点击已折叠任务组旁的已关闭文件夹图标 ( )。

安全、互联网接入和通信端口

为了保护ASA FirePOWER 模块，应将其安装在受保护的内部网络中。虽然 ASA FirePOWER 模块已配置为仅拥有必需的服务和可用端口，但必须确保无法从防火墙外部攻击它。

另请注意，ASA FirePOWER 模块的特定功能需要连接互联网。默认情况下，ASA FirePOWER 模块配置为直接连接至互联网。此外，系统还要求某些端口保持开放以实现安全的设备访问以便特定系统功能访问其正常运行本地或互联网资源。

有关详情，请参阅：

- 第 D-1 页上的互联网接入要求
- 第 D-2 页上的通信端口要求

互联网接入要求

默认情况下， FireSIGHT 系统是已配置为直接连接至互联网的 443/tcp (HTTPS) 和 80/tcp (HTTP) 端口的 ASA FirePOWER 模块，这些端口在上均默认打开；请参阅第 D-2 页上的通信端口要求。

下表介绍了 ASA FirePOWER 模块特定功能的互联网接入要求。

表 D-1　　ASA FirePOWER 模块功能互联网接入要求

特性	需要互联网接入以便...
入侵规则、 VDB 和 GeoDB 更新	将入侵规则、 GeoDB 或 VDB 更新直接下接至设备，或安排该等下载。
基于网络的 AMP	执行恶意软件云查找。
安全情报过滤	从外部来源下载安全情报源数据，包括情报源。
系统软件更新	将系统更新下载至设备或安排该等下载。
URL 过滤	下载基于云的 URL 类别和信誉数据以进行访问控制，并为未分类的 URL 执行查找。
whois	请求外部主机的 whois 信息。

通信端口要求

其他端口允许：

- 接入设备的 用户界面
- 与设备的安全远程连接
- 系统的某些功能访问其正常运行所需的本地或互联网资源

一般来说，功能相关端口会保持关闭，直至启用或配置关联的功能。

注意事项 在了解此操作对部署的影响之前，请**勿**关闭打开的端口。

例如，在受管设备上关闭出站端口 25/tcp (SMTP) 将阻止该设备发送个别入侵事件的邮件通知（请参阅第 28-1 页上的配置入侵规则的外部警报）。

下表列出了所需的开放端口，以便利用 ASA FirePOWER 模块功能。

表 D-2　用于 ASA FirePOWER 模块功能和操作的默认通 信端口

端口	说明	方向	支持...
22/tcp	SSH/SSL	双向	允计与设备进行安全远程连接。
25/tcp	SMTP	出站	从设备发送邮件通知和警报。
53/tcp	DNS	出站	使用 DNS。
67/udp 68/udp	DHCP	出站	使用 DHCP。 **注**　默认情况下，这些端口已**关闭**。
		双向	通过 HTTP 更新自定义和第三方安全情报源。 下载 URL 类别和信誉数据（还需要 443 端口）。
161/udp	SNMP	双向	允许通过 SNMP 轮询接入设备的 MIB。
162/udp	SNMP	出站	发送 SNMP 警报至远程陷阱服务器。
389/tcp 636/tcp	LDAP	出站	与一个 LDAP 服务器通信，以进行外部身份验证。
389/tcp 636/tcp	LDAP	出站	获取检测到的 LDAP 用户元数据。
443/tcp	HTTPS	入站接待	接入设备的用户界面。
443/tcp	HTTPS 云通信	双向	获取： • 软件、入侵规则、 VDB 和 GeoDB 更新 • URL 类别和信誉数据（还需要 80 端口） • 情报源和其他安全的安全情报源 • 网络流量中检测到的文件的恶意软件性质
			使用设备的用户界面下载软件更新。
514/udp	系统日志	出站	发送警报至远程系统日志服务器。
8305/tcp	设备通信	双向	在同一部署中的设备之间安全地进行通信。**Required**。
8307/tcp	主机输入客户端	双向	与主机输入客户端通信。