思科 ASA 系列 VPN ASDM 配置指南

软件版本 7.3
适用于 ASA 5506-X、ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、 ASA 5585-X、 ASA? 服务模块和自适应安全虚拟设备

发布日期：2014 年 7 月 24 日
更新日期：2014 年 12 月 18 日

Cisco Systems, Inc.
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。

文本部件号：不适用，仅在线提供

思科 ASA 系列 VPN ASDM 配置指南

关于本指南

文档目的

本指南旨在帮助您使用 ASDM 在自适应安全设备 (ASA) 上配置 VPN。本指南仅介绍最常见的一些配置场景，并未涵盖所有功能。

本指南适用于思科 ASA 系列。本指南中，术语“ASA”一般适用于所支持的型号，除非另有说明。

注 ASDM 支持许多 ASA 版本。ASDM 文档和在线帮助涵盖 ASA 支持的所有最新功能。如果您在运行较早版本的 ASA 软件，文档可能包含您版本中不支持的功能。同样，如果在较早主要版本或次要版本的维护版本中添加了一个功能，则 ASDM 文档包括该新功能，即使该功能在所有后续 ASA 版本中都不提供。请参阅每章的功能历史记录表确定功能的添加时间。有关每个 ASA 版本支持的 ASDM 的最低版本，请参阅 《*思科 ASA 系列兼容性*》。

相关文档

有关详细信息，请参阅 《*思科 ASA 系列文档导航*》，网址为：http://www.cisco.com/go/asadocs。

约定

本文档使用下列约定：

约定	说明
粗体	命令和关键字及用户输入的文本以**粗体**显示。
斜体	文档标题、新增或强调的术语以及要为其提供值的参数以*斜体*表示。
[ ]	方括号中的元素是可选项。
{x | y | z }	必需的备选关键字集中在大括号内，以竖线分隔。
[x | y | z]	可选的备选关键字集中在方括号内，以竖线分隔。
字符串	不加引号的字符集。请勿将字符串用引号引起来，否则会将字符串和引号视为一个整体。
`courier` **字体**	系统显示的终端会话和信息以 `courier` **字体**显示。
`courier` 粗体	命令和关键字及用户输入的文本以 **`courier` 粗体**显示。
`courier` 斜体	要提供值的参数以 *`courier` 斜体*显示。
< >	非打印字符 （如密码）括在尖括号中。
[ ]	系统提示的默认回复括在方括号中。
!， #	代码行开头的感叹号 (!) 或井号 (#) 表示注释行。

注 *表示读者需要注意的地方。*

提示 *表示以下信息有助于您解决问题。*

注意事项 *表示读者应当小心。*在这种情况下，操作可能会导致设备损坏或数据丢失。

获取文档和提交服务请求

有关获取文档、使用思科漏洞搜索工具 (BST)、提交服务请求和收集附加信息的详细信息，请参阅《*思科产品新特性文档*》，网址为：http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html。

通过 RSS 源的方式订阅*思科产品文档更新*（其中包括所有新的和修改过的思科技术文档），并将相关内容通过阅读器应用直接发送至您的桌面。 RSS 源是一种免费服务。

第 1 部分

站点到站点 VPN 和客户端 VPN

VPN 向导

发布日期：2014 年 7 月 24 日
更新日期：2014 年 12 月 18 日

VPN 概述

ASA 通过跨 TCP/IP 网络 （如互联网）创建被用户视为专用连接的安全连接来创建虚拟专用网络。它可以创建单一用户到 LAN 连接和 LAN 到 LAN 连接。

对于同时使用 IPv4 和 IPv6 寻址的 LAN 到 LAN 连接，如果两个对等体均为 ASA，并且如果二者在网络内部均有匹配的寻址方案（均为 IPv4 或均为 IPv6），则 ASA 支持 VPN 隧道。如果两个对等体在网络内部均为 IPv6 而网络外部为 IPv6，则此情况也成立。

安全连接被称为隧道，ASA 使用隧道协议来协商安全参数，创建并管理隧道，封装数据包，通过隧道传送或接收这些数据包以及将其解封。ASA 充当双向隧道终点：它可以接收明文数据包，将其封装，然后发送到会将其解封并发送到最终目标的隧道的另一端。它也可以接收已封装的数据包，将其解封，然后将其发送到其最终目标。

通过 VPN 向导，可以配置基本 LAN 到 LAN 连接和远程访问 VPN 连接，并为身份验证分配预先共享的密钥或数字证书。使用 ASDM 编辑和配置高级功能。

本节中描述的四个 VPN 向导如下：

- 第 1-2 页上的无客户端 SSL VPN 向导

  ASA 无客户端 SSL VPN 仅使用网络浏览器及其本机 SSL 加密从几乎任何支持互联网的位置提供安全套接字层 (SSL) 远程访问连接。通过此基于浏览器的 VPN，用户可以建立到自适应安全设备的安全、远程访问 VPN 隧道。在身份验证之后，用户将访问门户页，并且可以访问特定的受支持内部资源。网络管理员以组为基础按用户提供资源访问。用户无权直接访问内部网络上的资源。

- 第 1-3 页上的 AnyConnect VPN 向导

  Cisco AnyConnect VPN 客户端通过企业资源的全 VPN 隧道来为远程用户提供到 ASA 的安全 SSL 或 IPsec (IKEv2) 连接。在先前未安装客户端的情况下，远程用户在其浏览器中输入配置为接受无客户端 VPN 连接的接口的 IP 地址。ASA 下载与远程计算机的操作系统匹配的客户端。下载后，客户端会自行进行安装和配置，建立安全连接，并在连接终止时保留或自行卸载（视 ASA 配置而定）。如果先前已安装客户端，当用户进行身份验证时，ASA 将检查客户端的修订版本并在必要情况下升级客户端。

- 第 1-5 页上的 IPsec IKEv2 远程访问向导

  IKEv2 允许其他供应商的 VPN 客户端连接到 ASA。此支持可增强安全性并符合联邦和公共部门授权中定义的 IPsec 远程访问要求。

- 第 1-6 页上的 IPsec IKEv1 远程访问向导
- 第 1-9 页上的 IPsec 站点到站点 VPN 向导

无客户端 SSL VPN 向导

此向导通过门户页面为特定的受支持内部资源启用基于浏览器的无客户端连接。

SSL VPN 接口

提供连接配置文件以及 SSL VPN 用户连接到的接口。

- Connection Profile Name - 指定连接配置文件。
- SSL VPN Interface - 用户为 SSL VPN 连接访问的接口。
- Digital Certificate - 指定 ASA 发送到远程网络浏览器以对 ASA 进行身份验证的内容。
  - Certificate - 从下拉列表中进行选择。
- Accessing the Connection Profile
  - Connection Group Alias/URL - 可在登录期间从 Group 下拉列表中选择组别名。此 URL 会输入到网络浏览器中。
  - Display Group Alias list at the login page - 选中此选项，以在登录页面显示组别名列表。

User Authentication

在此窗格中指定身份验证信息。

- Authenticate using a AAA server group - 启用以使 ASA 能够联系远程 AAA 服务器组来对用户进行身份验证。
  - AAA Server Group Name - 从预先配置的组列表中选择 AAA 服务器组，或者点击 **New** 以创建新组。
- Authenticate using the local user database - 将新用户添加到存储在 ASA 上的本地数据库。
  - Username - 为用户创建用户名。
  - Password - 为用户创建密码。
  - Confirm Password - 重新键入同一密码以确认。
  - Add/Delete - 从本地数据库添加或删除用户。

Group Policy

组策略配置用户组的常见属性。请创建新的组策略或选择现有组策略以进行修改：

- Create new group policy - 支持创建新的组策略。请为新策略提供名称。
- Modify existing group policy - 选择现有组策略以进行修改。

Bookmark List

将门户页面中显示的组内部网网站列表配置为链接。一些示例包括 https://intranet.acme.com、rdp://10.120.1.2、 vnc://100.1.1.1 等。

- Bookmark List - 从下拉列表中进行选择。
- Manage - 点击以打开 Configure GUI Customization Object 对话框。

AnyConnect VPN 向导

使用此向导配置 ASA 以接受来自 AnyConnect VPN 客户端的 VPN 连接。此向导为完全网络访问配置 IPsec (IKEv2) 或 SSL VPN 协议。建立 VPN 连接后， ASA 将 AnyConnect VPN 客户端自动上载到最终用户的设备。

提醒用户运行该向导并不意味着 IKEv2 配置文件在预先部署场景自动适用。请提供成功预先部署 IKEv2 所必要的指导或步骤。

连接配置文件标识

连接配置文件标识用于向远程访问用户标识 ASA：

- Connection Profile Name - 提供远程访问用户将为 VPN 连接访问的名称。
- VPN Access Interface - 选择远程访问用户将为 VPN 连接访问的接口。

VPN 协议

指定为此连接配置文件允许的 VPN 协议。

AnyConnect 客户端默认为 SSL。如果启用 IPsec 作为连接配置文件的 VPN 隧道协议，还必须从 ASDM 使用配置文件编辑器创建并部署启用了 IPsec 的客户端配置文件，然后部署该配置文件。

如果预先部署而不是网络启动 AnyConnect 客户端，则第一个客户端连接将使用 SSL，并在会话期间从 ASA 接收客户端配置文件。对于后续连接，客户端使用配置文件中指定的协议（SSL 或 IPsec）。如果使用客户端预先部署指定了 IPsec 的配置文件，则第一个客户端连接将使用 IPsec。有关预先部署启用了 IPsec 的客户端配置文件的详细信息，请参阅 *AnyConnect 安全移动客户端管理员指南*。

- SSL
- IPsec (IKEv2)
- Device Certificate - 向远程访问客户端标识 ASA。一些 AnyConnect 功能 （如 “始终开启”和 IPsec/IKEv2）需要在 ASA 上具有有效的设备证书。
- Manage - 选择 **Manage** 将打开 Manage Identity Certificates 窗口。
  - Add - 选择 **Add** 以添加身份证书及其详细信息。
  - Show Details - 如果选择特定证书并点击 **Show Details**，则系统会显示 Certificate Details 窗口，其中提供将证书颁发给的人员和颁发者，以及指定其序列号、用途、关联信任点、有效时间范围等的有关信息。
  - Delete - 突出显示要移除的证书并点击 **Delete**。
  - Export - 突出显示证书并点击 **Export** 以将证书导出到具有或没有加密密码的文件。
  - Enroll ASA SSL VPN with Entrust - 通过来自 Entrust 的 SSL Advantage 数字证书使思科 ASA SSL VPN 设备快速启动并运行。

客户端映像

ASA 可以在访问企业网络时自动将最新的 AnyConnect 软件包上载到客户端设备。可以使用正则表达式将浏览器的用户代理与映像相匹配。您也可以通过将最常用的操作系统移至列表顶部来最小化连接设置时间。

身份验证方法

在此屏幕上指定身份验证信息。

- AAA server group - 启用以使 ASA 联系 AAA 服务器组来对用户进行身份验证。从预先配置的组列表中选择 AAA 服务器组，或者点击 **New** 以创建新组。
- Local User Database Details - 将新用户添加到存储在 ASA 上的本地数据库。
  - Username - 为用户创建用户名。
  - Password - 为用户创建密码。
  - Confirm Password - 重新键入同一密码以确认。
  - Add/Delete - 从本地数据库添加或删除用户。

Client Address Assignment

向远程 AnyConnect 用户提供一系列 IP 地址。

- IPv4 Address Pools - SSL VPN 客户端在连接到 ASA 时接收新 IP 地址。无客户端连接不需要新 IP 地址。 Address Pools 定义远程客户端可以接收的地址范围。请选择现有 IP 地址池，或者点击 **New** 以创建新池。

  如果选择 **New**，将必须提供开始和结束 IP 地址及子网掩码。
- IPv6 Address Poo - 选择现有 IP 地址池，或者点击 **New** 以创建新池。

注　无法为 IKEv2 连接配置文件创建 IPv6 地址池。

网络名解析服务器

指定在访问内部网络时为远程用户解析了哪些域名。

- DNS Servers - 输入 DNS 服务器的 IP 地址。
- WINS Servers - 输入 WINS 服务器的 IP 地址。
- Domain Name - 键入默认域名。

NAT 免除

如果在 ASA 上启用了网络转换，则必须免除 VPN 流量执行此转换。

AnyConnect 客户端部署

可以使用以下两种方法之一将 AnyConnect 客户端程序安装到客户端设备：

- Web launch - 使用网络浏览器访问 ASA 时， AnyConnect 客户端软件包自动进行安装。
- Pre-deployment - 手动安装 AnyConnect 客户端软件包。

Allow Web Launch 是一项全局设置，可影响所有连接。如果取消选中 （不允许），则 AnyConnect SSL 连接和无客户端 SSL 连接不工作。

对于预先部署，disk0:/test2_client_profile.xml 配置文件捆绑包含 .msi 文件，并且必须从 ASA 将此客户端配置文件包含在 AnyConnect 软件包中，以确保 IPsec 连接按预期工作。

IPsec IKEv2 远程访问向导

使用 IKEv2 远程访问向导为 VPN 客户端 （如移动用户）配置安全远程连接，以及标识连接到远程 IPsec 对等体的接口。

连接配置文件标识

输入 **Connection Profile Name** 并选择将用于 IPsec IKEv2 远程访问的 **VPN Access Interface**。

- Connection Profile Name - 键入一个名称以创建包含此 IPsec 连接的隧道连接策略的记录。连接策略可以指定身份验证、授权和记帐服务器、默认组策略及 IKE 属性。使用此 VPN 向导配置的连接策略会指定身份验证记录并使用 ASA Default Group Policy。
- VPN Access Interface - 选择用于与远程 IPsec 对等体建立安全隧道的接口。如果 ASA 有多个接口，则需要在运行此向导之前规划 VPN 配置，标识要用于每个计划与其建立安全连接的远程 IPsec 对等体的接口。

身份验证页面

IKE 对等身份验证 - 远程站点对等体通过预先共享的密钥或证书或者使用 EAP 的对等身份验证来进行身份验证。

- Pre-shared Key - 键入长度介于 1 到 128 个字符之间的字母数字字符串。

  使用预先共享的密钥是设置与有限数量的远程对等体和稳定网络的通信的一种快捷方法。它在大型网络中可能会导致可扩展性问题，因为每个 IPSec 对等体需要与其建立安全连接的每个对等体的配置信息。

  每对 IPSec 对等体必须交换预先共享的密钥以建立安全隧道。请使用安全方法与远程站点的管理员交换预先共享的密钥。
- Enable Certificate Authentication - 如果选中，则允许使用证书进行身份验证。
- Enable peer authentication using EAP - 如果选中，则允许使用 EAP 进行身份验证。如果选中此复选框，则必须使用证书进行本地身份验证。
- Send an EAP identity request to the client - 支持向远程访问 VPN 客户端发送 EAP 身份验证请求。

IKE 本地身份验证

- 启用本地身份验证，然后选择预先共享的密钥或证书
  - Preshared Key - 键入长度介于 1 到 128 个字符之间的字母数字字符串。
  - Certificate - 点击以使用证书在本地 ASA 和远程 IPsec 对等体之间进行身份验证。要完成此部分，必须先前已向 CA 注册并将一个或多个证书下载到 ASA。

    可以高效地管理用于与数字证书建立 IPSec 隧道的安全密钥。数字证书包含用于标识用户或设备的信息，如名称、序列号、公司、部门或 IP 地址。数字证书还包含公钥的副本。

    要使用数字证书，每个对等体需要向负责颁发数字证书的证书颁发机构 (CA) 注册。 CA 可以是受信任的供应商，或者是在组织内建立的私有 CA。

    当两个对等体要通信时，它们交换证书和数字签名数据以相互进行身份验证。向网络中添加新的对等体时，该对等体会向 CA 注册，并且其他任何对等体都不需要额外配置。

身份验证方法

IPsec IKEv2 远程访问仅支持 Radius 身份验证。

- AAA Server Group - 选择先前配置的 AAA 服务器组。
- New - 点击以配置新的 AAA 服务器组。
- AAA Server Group Details - 使用此区域修改 AAA 服务器组 （如果需要）。

客户端地址分配

屏幕上已有的内容比一切都更有用。

创建或选择 IPv4 和 IPv6 地址池。将为远程访问客户端分配来自 IPv4 或 IPv6 地址池中的地址。如果配置了两种地址，则 IPv4 地址优先。有关详细信息，请参阅*配置本地 IP 地址池*。

网络名解析服务器

指定在访问内部网络时如何为远程用户解析域名。

- DNS Servers - 键入 DNS 服务器的 IP 地址。
- WINS Servers - 键入 WINS 服务器的 IP 地址。
- Default Domain Name - 键入默认域名。

NAT 免除

- Exempt VPN traffic from Network Address Translation - 如果在 ASA 上启用了 NAT，则必须选中此项。

IPsec IKEv1 远程访问向导

注　思科 VPN 客户端已停产并终止支持。必须升级到 AnyConnect 安全移动客户端。

使用 IKEv1 远程访问向导为 VPN 客户端 （如移动用户）配置安全远程连接，以及标识连接到远程 IPsec 对等体的接口。

- VPN Tunnel Interface - 选择要用于远程访问客户端的接口。如果 ASA 有多个接口，请立即停止并配置 ASA 上的接口，然后再运行此向导。
- Enable inbound IPsec sessions to bypass interface access lists - 支持通过 ASA 始终允许 IPsec 身份验证的入站会话 （即，不检查接口访问列表语句）。请注意，入站会话只会绕过接口 ACL。配置的组策略、用户和下载的 ACL 仍然适用。

远程访问客户端

各种类型的远程访问用户可以打开到此 ASA 的 VPN 隧道。选择此隧道的 VPN 客户端类型。

- VPN 客户端类型
  - Easy VPN Remote 产品。
  - Microsoft Windows client using L2TP over IPsec - 指定 PPP 身份验证协议。选项包括 PAP、CHAP、 MS-CHAP-V1、 MS-CHAP-V2 和 EAP-PROXY：

    PAP - 在身份验证期间传递明文用户名和密码，并且不安全。

    CHAP - 为响应服务器质询，客户端使用明文用户名返回加密质询及密码。此协议比 PAP 更安全，但不加密数据。

    MS-CHAP, Version 1 - 与 CHAP 类似，但更安全，原因是服务器仅存储和比较加密密码，而不是像 CHAP 中存储和比较明文密码。

    MS-CHAP, Version 2 - 包含优于 MS-CHAP, Version 1 的安全增强功能。

    EAP-Proxy - 启用 EAP，它允许 ASA 代理面向外部 RADIUS 身份验证服务器的 PPP 身份验证过程。

    如果在远程客户端上未指定某协议，请勿指定该协议。
  - 指定客户端是否将以 username@tunnelgroup 形式发送隧道组名。

VPN 客户端身份验证方法及隧道组名称

使用 VPN Client Authentication Method and Name 窗格配置身份验证方法和创建连接策略（隧道组）。

- Authentication Method - 远程站点对等体通过预先共享的密钥或证书进行身份验证。
  - Pre-shared Key - 点击以使用预先共享的密钥在本地 ASA 和远程 IPsec 对等体之间进行身份验证。

    使用预先共享的密钥是设置与有限数量的远程对等体和稳定网络的通信的一种快捷方法。它在大型网络中可能会导致可扩展性问题，因为每个 IPSec 对等体需要与其建立安全连接的每个对等体的配置信息。

    每对 IPSec 对等体必须交换预先共享的密钥以建立安全隧道。请使用安全方法与远程站点的管理员交换预先共享的密钥。
  - Pre-shared Key - 键入长度介于 1 到 128 个字符之间的字母数字字符串。
  - Certificate - 点击以使用证书在本地 ASA 和远程 IPsec 对等体之间进行身份验证。要完成此部分，必须先前已向 CA 注册并将一个或多个证书下载到 ASA。

    可以高效地管理用于与数字证书建立 IPSec 隧道的安全密钥。数字证书包含用于标识用户或设备的信息，如名称、序列号、公司、部门或 IP 地址。数字证书还包含公钥的副本。

    要使用数字证书，每个对等体需要向负责颁发数字证书的证书颁发机构 (CA) 注册。 CA 可以是受信任的供应商，或者是在组织内建立的私有 CA。

    当两个对等体要通信时，它们交换证书和数字签名数据以相互进行身份验证。向网络中添加新的对等体时，该对等体会向 CA 注册，并且其他任何对等体都不需要额外配置。

    Certificate Signing Algorithm - 显示用于为数字证书签名的算法，rsa-sig 对应于 RSA。
  - Challenge/response authentication (CRACK) - 在客户端使用普遍方法（如 RADIUS）进行身份验证且服务器使用公钥身份验证时提供强大的相互身份验证。安全设备支持 CRACK 作为 IKE 选项，以便对诺基亚 92xx 通讯器系列设备上的诺基亚 VPN 客户端进行身份验证。
- Tunnel Group Name - 键入一个名称以创建包含此 IPsec 连接的隧道连接策略的记录。连接策略可以指定身份验证、授权和记帐服务器、默认组策略及 IKE 属性。使用此 VPN 向导配置的连接策略会指定身份验证记录并使用 ASA Default Group Policy。

客户端身份验证

使用 Client Authentication 窗格选择 ASA 对远程用户进行身份验证的方法。选择以下选项之一：

- Authenticate using the local user database - 点击以使用 ASA 内部身份验证。此方法用于用户数较少且稳定的环境。通过下一个窗格，可在 ASA 上为个人用户创建帐户。
- Authenticate using an AAA server group - 点击以使用内部服务器组进行远程用户身份验证。
  - AAA Server Group Name - 选择先前配置的 AAA 服务器组。
  - New... - 点击以配置新的 AAA 服务器组。

用户帐户

使用 User Accounts 窗格将新用户添加到 ASA 内部用户数据库以进行身份验证。

地址池

使用 Address Pool 窗格配置 ASA 分配给远程 VPN 客户端的本地 IP 地址池。

- Tunnel Group Name - 显示此地址池应用到的连接配置文件 （隧道组）的名称。可在 VPN Client and Authentication Method 窗格中设置此名称 （步骤 3）。
- Pool Name - 为地址池选择描述性标识符。
- New... - 点击以配置新地址池。

- Range Start Address - 键入地址池中的开始 IP 地址。
- Range End Address - 键入地址吃中的结束 IP 地址。
- Subnet Mask - （可选）选择这些 IP 地址的子网掩码。

推送至客户端的属性 （可选）

使用 Attributes Pushed to Client (Optional) 窗格使 ASA 将有关 DNS 和 WINS 服务器及默认域名的信息传递到远程访问客户端。

- Tunnel Group - 显示地址池应用到的连接策略的名称。可在 VPN Client Name and Authentication Method 窗格中设置此名称。
- Primary DNS Server - 键入主 DNS 服务器的 IP 地址。
- Secondary DNS Server - 键入辅助 DNS 服务器的 IP 地址。
- Primary WINS Server - 键入主 WINS 服务器的 IP 地址。
- Secondary WINS Server - 键入辅助 WINS 服务器的 IP 地址。
- Default Domain Name - 键入默认域名。

IKE 策略

IKE，也称为互联网安全关联和密钥管理协议 (ISAKMP)，是让两台主机商定如何构建 IPSec 安全关联的一种协商协议。每个 IKE 协商分为两个部分，分别称为第 1 阶段和第 2 阶段。第 1 阶段创建第一条隧道，用于保护后来的 IKE 协商消息。第 2 阶段创建用于保护数据的隧道。

使用 IKE Policy 窗格设置第 1 阶段 IKE 协商的条款，其中包括保护数据和确保隐私的加密方法、确保对等体身份的身份验证方法，以及用于建立加密密钥确定算法强度的 Diffie-Hellman 组。ASA 使用此算法派生加密密钥和哈希密钥。

- Encryption - 选择 ASA 用于建立保护第 2 阶段协商的第 1 阶段 SA 的对称加密算法。ASA 支持以下加密算法：

算法	说明
DES	数据加密标准。使用 56 位密钥。
3DES	三重 DES。使用 56 位密钥执行三次加密。
AES-128	高级加密标准。使用 128 位密钥。
AES-192	使用 192 位密钥的 AES。
AES-256	使用 256 位密钥的 AES。

  默认的 3DES 比 DES 更安全，但是需要对加密和解密进行更多处理。同样， AES 选项可提高安全性，但也需要增加处理。

- Authentication - 选择用于身份验证并确保数据完整性的哈希算法。默认值为 SHA。MD5 具有比 SHA 更小的摘要并被视为比其略微更快。已成功（但极其困难）演示过对 MD5 的攻击。不过，ASA 所使用的带密钥的哈希消息认证码 (HMAC) 版本可防止此类攻击。
- Diffie-Hellman Group - 选择 Diffie-Hellman 组标识符，供两个 IPsec 对等体用于派生共享密钥而不将其相互传输。默认的第 2 组 （1024 位 Diffie-Hellman）执行所需的 CPU 时间更少，但是不如第 5 组 （1536 位）安全。

注　VPN 3000 系列集中器的默认值为 MD5。 ASA 和 VPN 集中器之间的连接要求第 1 阶段和第 2 阶段 IKE 协商的身份验证方法在连接的两端均相同。

IPsec 设置 （可选）

使用 IPsec Settings (Optional) 窗格标识无需地址转换的本地主机/网络。默认情况下，ASA 通过使用动态或静态网络地址转换 (NAT) 对外部主机隐藏内部主机和网络的真实 IP 地址。NAT 可将不受信任的外部主机的攻击风险最小化，但是对于已由 VPN 进行身份验证和保护的主机可能不合适。

例如，使用动态 NAT 的内部主机通过将其 IP 地址与池中随机选择的地址相匹配来转换其 IP 地址。只有已转换的地址在外部才可见。除非配置 NAT 免除规则，否则尝试通过将数据发送到其真实 IP 地址来到达这些主机的远程 VPN 客户端无法连接到这些主机。

注　如果希望免除所有主机和网络执行 NAT，不要在此窗格上进行任何配置。如果有甚至是一个条目，则所有其他主机和网络都要执行 NAT。

- Interface - 选择用于连接到选定的主机或网络的接口的名称。
- Exempt Networks - 选择要从所选接口网络中免除的主机或网络的 IP 地址。
- Enable split tunneling - 选择以在未加密的情况下发送从远程访问客户端到公共互联网的流量。分割隧道会导致受保护网络的流量加密，而到未受保护网络的流量则未加密。启用分割隧道时，ASA 在身份验证后将 IP 地址列表推送到远程 VPN 客户端。远程 VPN 客户端会将到 ASA 后的 IP 地址的流量加密。所有其他流量都在未加密的情况下直接传播到互联网而不涉及 ASA。
- Enable Perfect Forwarding Secrecy (PFS) - 指定在生成第 2 阶段 IPsec 密钥时是否使用完全向前保密以及要使用的数量规模。 PFS 是一个加密概念，其中每个新密钥都与任何先前密钥无关。在 IPsec 协商中，除非启用 PFS，否则第 2 阶段密钥基于第 1 阶段密钥。PFS 使用 Diffie-Hellman 方法来生成密钥。

  PFS 确保在将来其中一个私钥被泄漏的情况下，从一组长期公钥和私钥派生的会话密钥不被泄漏。

  必须在连接的两端均启用 PFS。

  - Diffie-Hellman Group - 选择 Diffie-Hellman 组标识符，供两个 IPsec 对等体用于派生共享密钥而不将其相互传输。默认的第 2 组 （1024 位 Diffie-Hellman）执行所需的 CPU 时间更少，但是不如第 5 组 （1536 位）安全。

摘要

如果对配置满意，请点击 **Finish**。ASDM 保存 LAN 到 LAN 配置。点击 **Finish** 后，无法再使用 VPN 向导对此配置进行更改。使用 ASDM 编辑和配置高级功能。

IPsec 站点到站点 VPN 向导

两个 ASA 设备之间的隧道被称为站点到站点隧道，并且是双向的。站点到站点 VPN 隧道使用 IPsec 协议保护数据。

对等设备标识

- Peer IP Address - 配置另一个站点 （对等设备）的 IP 地址。
- VPN Access Interface - 选择要用于站点到站点隧道的接口。

保护流量

通过此步骤可标识本地网络和远程网络。这些网络使用 IPsec 加密来保护流量。

- Local Networks - 标识 IPsec 隧道中使用的主机。
- Remote Networks - 标识 IPsec 隧道中使用的网络。

安全

通过此步骤可配置使用对等设备进行身份验证的方法。可以选择简单配置并提供预先共享的密钥。或者，也可以选择 Customized Configuration 以获取更多高级选项，如下所示：

- IKE Version - 根据要使用的版本选中 IKEv1 或 IKEv2 复选框。
- IKE 第 1 版身份验证方法
  - Pre-shared Key - 使用预先共享的密钥是设置与有限数量的远程对等体和稳定网络的通信的一种快捷方法。它在大型网络中可能会导致可扩展性问题，因为每个 IPSec 对等体需要与其建立安全连接的每个对等体的配置信息。

    每对 IPSec 对等体必须交换预先共享的密钥以建立安全隧道。请使用安全方法与远程站点的管理员交换预先共享的密钥。
  - Device Certificate - 点击以使用证书在本地 ASA 和远程 IPsec 对等体之间进行身份验证。

    可以高效地管理用于与数字证书建立 IPSec 隧道的安全密钥。数字证书包含用于标识用户或设备的信息，如名称、序列号、公司、部门或 IP 地址。数字证书还包含公钥的副本。

    当两个对等体要通信时，它们交换证书和数字签名数据以相互进行身份验证。向网络中添加新的对等体时，该对等体会向 CA 注册，并且其他任何对等体都不需要额外配置。
- IKE 第 2 版身份验证方法
  - Local Pre-shared Key - 指定 IPsec IKEv2 身份验证方法和加密算法。
  - Local Device Certificate - 通过安全设备对 VPN 访问进行身份验证。
  - Remote Peer Pre-shared Key - 点击以使用预先共享的密钥在本地 ASA 和远程 IPsec 对等体之间进行身份验证。
  - Remote Peer Certificate Authentication - 如果选中，允许对等设备使用证书向此设备自行进行身份验证。
- Encryption Algorithms - 通过此选项卡可选择用于保护数据的加密算法的类型。
  - IKE Policy - 指定 IKEv1/IKEv2 认证算法。
  - IPsec Proposal - 指定 IPsec 加密算法。
- Perfect Forward Secrecy
  - Enable Perfect Forwarding Secrecy (PFS) - 指定在生成第 2 阶段 IPsec 密钥时是否使用完全向前保密以及要使用的数量规模。PFS 是一个加密概念，其中每个新密钥都与任何先前密钥无关。在 IPsec 协商中，除非启用 PFS，否则第 2 阶段密钥基于第 1 阶段密钥。 PFS 使用 Diffie-Hellman 方法来生成密钥。

    PFS 确保在将来其中一个私钥被泄漏的情况下，从一组长期公钥和私钥派生的会话密钥不被泄漏。

    必须在连接的两端均启用 PFS。
  - Diffie-Hellman Group - 选择 Diffie-Hellman 组标识符，供两个 IPsec 对等体用于派生共享密钥而不将其相互传输。默认的第 2 组 （1024 位 Diffie-Hellman）执行所需的 CPU 时间更少，但是不如第 5 组 （1536 位）安全。

NAT 免除

- Exempt ASA side host/network from address translation - 使用下拉列表选择要从地址转换中排除的主机或网络。

第 2 章

IKE、负载均衡和 NAC

IKE 也称为 ISAKMP，是允许两个主机商定如何建立 IPSec 安全关联的协商协议。要为虚拟专用网络配置 ASA，您可以设置在整个系统范围内应用的全局 IKE 参数，还可以创建对等体通过协商建立 VPN 连接的 IKE 策略。

负载均衡在 VPN 集群中的两个或更多 ASA 之间分配 VPN 流量。

网络访问控制 (NAC) 会执行终端合规性和漏洞检查，并以此作为网络生产访问的条件，从而防止企业网络遭受蠕虫、病毒和欺诈应用程序的入侵和感染。我们将这些检查称为*状态验证*。

在接口上启用 IKE

要使用 IKE，您必须在计划在其上使用 IKE 的接口上启用 IKE。

对于 VPN 连接

步骤 1 在 ASDM 中，选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**。

步骤 2 在 Access Interfaces 区域中，为您将将在其上使用 IKE 的接口选中 IPsec (IKEv2) Access 之下的 **Allow Access**。

对于站点对站点 VPN

步骤 1 在 ASDM 中，选择 **Configuration > Site-to-Site VPN > Connection Profiles**。

步骤 2 选择您想要在其上使用 IKEv1 和 IKEv2 的接口。

为站点对站点 VPN 设置 IKE 参数

IKE 参数

在 ASDM 中，选择 **Configuration > Site-to-Site VPN > Advanced > IKE Parameters**。

NAT 透明度

启用经由 NAT-T 的 IPsec

经由 NAT-T 的 IPsec 允许 IPSec 对等体通过 NAT 设备建立远程访问和 LAN 对 LAN 连接。其方法是使用端口 4500 将 IPsec 流量封装在 UDP 数据报中，从而为 NAT 设备提供端口信息。 NAT-T 会自动检测所有 NAT 设备，但只有在必要时封装 IPSec 流量。此功能默认为已启用。

- ASA 可同时支持标准 IPsec、经由 TCP 的 IPsec、 NAT-T 和经由 UDP 的 IPsec，具体取决于与其交换数据的客户端。
- 同时启用 NAT-T 和经由 UDP 的 IPsec 时，NAT-T 优先。
- 启用时，经由 TCP 的 IPsec 优先于所有其他连接方法。

NAT-T 的 ASA 实施支持单个 NAT/PAT 设备之后的 IPSec 对等体，如下所示：

- 一个 LAN 对 LAN 连接。
- LAN 对 LAN 连接或多个远程访问客户端，但不是二者的混合。

要使用 NAT-T，请执行以下操作：

- 为用于打开端口 4500 的接口创建 ACL (Configuration > Firewall > Access Rules)。
- 在此窗格中启用经由 NAT-T 的 IPsec。
- 在 Configuration > Site-to-Site VPN > Advanced > IPsec Prefragmentation Policies 窗格中的 Fragmentation Policy 参数上，编辑您将用于启用 IPsec 预分片的接口。配置该项后，可以仍然允许流量通过不支持 IP 分片的 NAT 设备；它们不会阻碍支持分片的 NAT 设备的操作。

启用经由 TCP 的 IPsec

对于标准 ESP 或 IKE 在其中无法工作，或者仅在修改现有防火墙规则的情况下才能工作的环境，经由 TCP 的 IPsec 使得 VPN 客户端可以在其中进行操作。经由 TCP 的 IPSec 将 IKE 和 IPSec 协议同时封装在 TCP 数据包内，并支持同时穿过 NAT 与 PAT 设备和防火墙的安全隧道。此功能默认为已禁用。

注　此功能不能与基于代理的防火墙配合使用。

经由 TCP 的 IPSec 可与远程访问客户端配合使用。它可在所有物理和 VLAN 接口上工作。它只是一个客户端到 ASA 功能。它不适用于 LAN 对 LAN 连接。

- ASA 可同时支持标准 IPsec、经由 TCP 的 IPsec、 NAT-Traversal 和经由 UDP 的 IPsec，具体取决于与其交换数据的客户端。
- 一次只支持一个隧道的 VPN 3002 硬件客户端，可使用标准 IPsec、经由 TCP 的 IPsec、NAT-Traversal 或经由 UDP 的 IPsec 进行连接。
- 启用时，经由 TCP 的 IPsec 优先于所有其他连接方法。

您可以同时在 ASA 及其连接的客户端上启用经由 TCP 的 IPsec。

您可以为您指定的最多 10 个端口启用经由 TCP 的 IPsec。如果您输入一个已知端口，例如端口 80 (HTTP) 或端口 443 (HTTPS)，系统会显示一条警告，指示与该端口关联的协议将不再工作。其结果是，您无法再使用浏览器通过启用 IKE 的接口管理 ASA。要解决此问题，请将 HTTP/HTTPS 管理重新配置到不同的端口。

您必须在客户端以及 ASA 上配置 TCP 端口。客户端配置必须包含至少一个您为 ASA 设置的端口。

发送至对等体的标识

选择对等体将在 IKE 协商期间用于标识自身的 **Identity**：

Address	使用交换 ISAKMP 标识信息的主机的 IP 地址。
Hostname	使用交换 ISAKMP 标识信息的主机的完全限定域名 （默认）。此名称包括主机名和域名。
Key ID	远端对等体使用您指定的 **Key Id String** 来查找预共享密钥。
Automatic	按连接类型确定 IKE 协商： • 预共享密钥的 IP 地址 • 证书身份验证的证书 DN。

会话控制

Disable Inbound Aggressive Mode Connections

第 1 阶段 IKE 协商可以使用主模式或攻击性模式。两者提供相同的服务，但是攻击性模式只需要对等体之间的两次交换，而不是三次。攻击性模式速度更快，但是不为通信方提供标识保护。因此在建立于其中加密信息的安全 SA 之前，需要它们交换标识信息。此功能默认为已禁用。

Alert Peers Before Disconnecting

客户端或 LAN 对 LAN 会话可能出于某些原因丢失，例如：ASA 关闭或重新启动、会话空闲超时、超过最长连接时间或管理员切断。

ASA 可以通知合格的对等体（在 LAN 对 LAN 配置中）、VPN 客户端和 VPN 3002 硬件客户端，会话即将断开，并向其传达原因。收到此警报的对等体或客户端会对该原因进行解码，并将其在事件日志或弹出窗格中显示。此功能默认为已禁用。

此窗格允许您启用该功能，以便 ASA 可以发送这些警报，并传达断开的原因。

合格客户端和对等体包括以下项：

- 已启用警报的安全设备。
- 运行 4.0 或更高版本软件的 VPN 客户端 （无需进行配置）。
- 运行 4.0 或更高版本软件，并且已启用警报的 VPN 3002 硬件客户端。
- 运行 4.0 或更高版本软件，并且已启用警报的 VPN 3000 集中器。

Wait for All Active Sessions to Voluntarily Terminate Before Rebooting

您可以安排 ASA 仅当所有活动会话都已自行终止后，才重新启动。此功能默认为已禁用。

Number of SAs Allowed in Negotiation for IKEv1

限制可以随时协商的 SA 的最大数量。

IKE v2 特定设置

IKE v2 可使用其他会话控制，限制打开的 SA 的数量。默认情况下，ASA 不限制打开的 SA 的数量。

- Cookie Challenge - 使得 ASA 可以响应 SA 发起数据包，向对等设备发送 Cookie 质询。
  - % threshold before incoming SAs are cookie challenged - ASA 允许协商的 SA 的总数量的百分比，超过该百分比后，对于任何未来的 SA 协商，都会触发 Cookie 质询。取值范围为 0 至 100%。默认值为 50%。
- Number of Allowed SAs in Negotiation - 限制可以随时协商的 SA 的最大数量。如果与 Cookie Challenge 配合使用，可以配置低于此限制的 Cookie 质询阈值，以便实现有效的交叉检查。
- Maximum Number of SAs Allowed - 限制 ASA 上允许的 IKEv2 连接的数量。默认情况下，限制是许可证指定的最大连接数。

使用 IKE v2 特定设置防止 DoS 攻击

您可以配置 Cookie Challenge（这会质询传入安全关联 (SA) 的标识），或者限制打开的 SA 的数量，从而防止对于 IPsec IKEv2 连接的拒绝服务 (DoS) 攻击。默认情况下，ASA 不会限制打开的 SA 的数量，也从不对 SA 进行 Cookie 质询。您还可以限制允许的 SA 的数量，这可以停止来自协商的更多连接，从而防御 Cookie 质询功能无法抵御的内存和/或 CPU 攻击，并且保护当前的连接。

对于 DoS 攻击，攻击者会在对等设备发送 SA 发起数据包，ASA 发送其响应，但对等设备没有进一步响应时发起攻击。如果对等设备不断如此操作， ASA 上所有允许的 SA 请求会被耗尽，直到其停止响应。

启用 Cookie 质询的阈值百分比可以限制打开的 SA 协商的数量。例如，使用默认设置 50%，当 50% 的允许 SA 处于协商 （打开）状态时， ASA 会对到达的任何其他 SA 发起数据包进行 Cookie 质询。对于有 10000 个允许的 IKEv2 SA 的思科 ASA 5585-X，在 5000 个 SA 变为打开状态后，任何更多的传入 SA 都需要接受 Cookie 质询。

如果与 ***Number of SAs Allowed in Negotiation*** 或 ***Maximum Number of SAs Allowed*** 配合使用，可以配置低于这些限制的 Cookie 质询阈值，以便实现有效的交叉检查。

您还可以通过选择 Configuration > Site-to-Site VPN > Advanced > System Options，在 IPsec 层次上限制所有 SA 的生存期。

创建 IKE 策略

关于 IKE

每个 IKE 协商分为两个部分，分别称为第 1 阶段和第 2 阶段。

第 1 阶段创建第一条隧道，用于保护后来的 IKE 协商消息。第 2 阶段创建用于保护数据的隧道。

要设置 IKE 协商条款，您可以创建一个或多个 IKE 策略，包括以下内容：

- 唯一优先级 （1 至 65543，其中 1 为最高优先级）。
- 身份验证方法，用于确保对等体的身份。
- 加密方法，用于保护数据并确保隐私。
- HMAC 方法，用于确保发送方身份，以及确保消息在传输过程中未被修改。
- Diffie-Hellman 群，用于确立 encryption-key-determination 算法的强度。 ASA 使用此算法派生加密密钥和哈希密钥。
- 在更换加密密钥前， ASA 可使用该加密密钥的时长限制。

对于 IKEv1，您只能为一个参数启用一个设置。对于 IKEv2，每个方案对于加密、 D-H 群、完整性哈希和 PRF 哈希可具有多个设置。

如果您未配置任何 IKE 策略，ASA 会使用默认策略，默认策略始终会被设为最低优先级，它包含有每个参数的默认值。如果您没有为特定参数指定值，则默认值生效。

当 IKE 协商开始时，发起协商的对等体将其所有策略发送到远程对等体，然后远程对等体按优先级顺序搜索其自己的策略的匹配项。

如果 IKE 策略具有相同的加密、哈希、身份验证和 Diffie-Hellman 值，而且 SA 生存期小于或等于发送的策略中的生存期，则它们之间存在匹配。如果生存期不同，则会应用较短的生存期（来自远程对等体）。如果不存在匹配， IKE 将拒绝协商，并且不会建立 IKE SA。

配置 IKE 策略

Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Policies

Configuration > Site-to-Site VPN > Advanced > IKE Policies

字段

- IKEv1 Policies - 显示每个配置的 IKE 策略的参数设置。
  - Priority # - 显示此策略的优先级。
  - Encryption - 显示加密方法。
  - Hash - 显示哈希算法。
  - D-H Group - 显示 Diffie-Hellman 群。
  - Authentication - 显示身份验证方法。
  - Lifetime (secs) - 显示以秒为单位的 SA 生存期。
- Add/Edit/Delete - 点击以便添加、编辑或删除 IKEv1 策略。
- IKEv2 Policies - 显示每个配置的 IKEv2 策略的参数设置。
  - Priority # - 显示此策略的优先级。
  - Encryption - 显示加密方法。
  - Integrity Hash - 显示哈希算法。
  - PRF Hash - 显示伪随机功能 (PRF) 哈希算法。
  - D-H Group - 显示 Diffie-Hellman 群。
  - Lifetime (secs) - 显示以秒为单位的 SA 生存期。
- Add/Edit/Delete - 点击以便添加、编辑或删除 IKEv2 策略。

添加 IKEv1 策略

Configuration > VPN > IKE > Policies > Add/Edit IKEv1 Policy

字段

Priority # - 键入一个数值，以便设置 IKE 策略的优先级。取值范围为 1 至 65535，其中 1 为最高优先级。

Encryption - 选择一个加密方法。这是保护在两个 IPSec 对等体之间传输的数据的对称加密方法。选项如下：

des	56 位 DES-CBC。安全性较低，但速度比备选方案快。默认值。
3des	168 位三重 DES。
aes	128 位 AES。
aes-192	192 位 AES。
aes-256	256 位 AES。

Hash - 选择确保数据完整性的哈希算法。它可以确保数据包来自您认为的发送方，并且在传输过程中未被修改。

sha	SHA-1	默认值为 SHA-1。 MD5 的摘要较小，被认为速度比 SHA-1 稍快。已发生过针对 MD5 的成功 （但非常困难）攻击；然而， IKE 使用的 HMAC 变体可防止此类攻击。
md5	MD5	

Authentication - 选择 ASA 用于建立每个 IPSec 对等体的标识的身份验证方法。对于增长型网络，预共享密钥不能很好地进行扩展，但是在小型网络中更容易设置。选项如下：

pre-share	预共享密钥。
rsa-sig	使用 RSA 签名算法生成的带密钥的数字证书。
crack	使用身份验证技术而非证书、启用 IPsec 的移动客户端的已验证加密密钥协议的 IKE 质询/响应。

D-H Group - 选择 Diffie-Hellman 群标识符，两个 IPsec 对等体会在不相互传输该标识符的情况下，使用该标识符来派生共享机密。

1	群 1 （768 位）	默认情况下，群 2（1024 位 Diffie - Hellman）执行所需的 CPU 时间较少，但安全性要低于群 1 或 5。
2	群 2 （1024 位）	
5	群 5 （1536 位）	

Lifetime (secs) - 为 SA 生存期选择 *Unlimited* 或输入一个整数。默认值为 86400 秒或 24 小时。在生存期更长的情况下， ASA 设置未来 IPsec 安全关联的速度会较慢。在不使用极短的重新生成密钥时间的情况下 （每隔几分钟的水平），加密强度足以确保安全性。我们建议您接受默认值。

Time Measure - 选择时间度量值。 ASA 接受以下值：

120 - 86400 秒

2 - 1440 分钟

1 - 24 小时

1 天

添加 IKEv2 策略

Configuration > VPN > IKE > Policies > Add/Edit IKEv2 Policy

字段

Priority # - 键入一个数值，以便设置 IKEv2 策略的优先级。取值范围为 1 至 65535，其中 1 为最高优先级。

Encryption - 选择一个加密方法。这是保护在两个 IPSec 对等体之间传输的数据的对称加密方法。选项如下：

des	为 ESP 指定 56 位 DES-CBC 加密。
3des	（默认）为 ESP 指定三重 DES 加密算法。
aes	为 ESP 指定使用 128 位密钥加密的 AES。
aes-192	为 ESP 指定使用 192 位密钥加密的 AES。
aes-256	为 ESP 指定使用 256 位密钥加密的 AES。
aes-gcm	指定 AES-GCM/GMAC 128 位支持，以确保对称加密和完整性。
aes-gcm-192	指定 AES-GCM/GMAC 192 位支持，以确保对称加密和完整性。
aes-gcm-256	指定 AES-GCM/GMAC 256 位支持，以确保对称加密和完整性。
NULL	表示不加密。

D-H Group - 选择 Diffie-Hellman 群标识符，两个 IPsec 对等体会在不相互传输该标识符的情况下，使用该标识符来派生共享机密。

1	群 1 （768 位）	默认情况下，群 2（1024 位 Diffie - Hellman）执行所需的 CPU 时间较少，但安全性要低于群 2 或 5。
2	群 2 （1024 位）	
5	群 5 （1536 位）	
14	群 14	
19	群 19	
20	群 20	
21	群 21	
24	群 24	

Integrity Hash - 选择确保 ESP 协议的数据完整性的哈希算法。它可以确保数据包来自您认为的发送方，并且在传输过程中未被修改。

sha **md5**	SHA 1 MD5	默认值为 SHA 1。 MD5 的摘要较小，被认为速度比 SHA-1 稍快。已发生过针对 MD5 的成功（但非常困难）攻击；然而，IKE 使用的 HMAC 变体可防止此类攻击。
sha256	SHA 2，256 位摘要	指定具有 256 位摘要的安全哈希算法 SHA 2。
sha384	**SHA 2，384 位摘要**	指定具有 384 位摘要的安全哈希算法 SHA 2。
sha512	**SHA 2，512 位摘要**	指定具有 512 位摘要的安全哈希算法 SHA 2。
null		表示将 AES-GCM 或 AES-GMAC 配置为加密算法。如果 AES-GCM 已被配置为加密算法，对于完整性算法您必须选择 null。

Pseudo-Random Function (PRF) - 对于在 SA 中使用的所有加密算法，指定用于构建密钥内容的 PRF。

sha **md5**	SHA-1 MD5	默认值为 SHA-1。 MD5 的摘要较小，被认为速度比 SHA-1 稍快。已发生过针对 MD5 的成功 （但非常困难）攻击；然而， IKE 使用的 HMAC 变体可防止此类攻击。
sha256	SHA 2，256 位摘要	指定具有 256 位摘要的安全哈希算法 SHA 2。
sha384	SHA 2，384 位摘要	指定具有 384 位摘要的安全哈希算法 SHA 2。
sha512	SHA 2，512 位摘要	指定具有 512 位摘要的安全哈希算法 SHA 2。

Lifetime (secs) - 为 SA 生存期选择 *Unlimited* 或输入一个整数。默认值为 86400 秒或 24 小时。在生存期更长的情况下， ASA 设置未来 IPsec 安全关联的速度会较快。在不使用极短的重新生成密钥时间的情况下 （每隔几分钟的水平），加密强度足以确保安全性。我们建议您接受默认值。

ASA 接受以下值：

120 - 86400 秒

2 - 1440 分钟

1 - 24 小时

1 天

分配策略

Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy

分配策略配置 IP 地址如何分配给远程访问客户端。

字段

- Use authentication server - 选择此项，以便按用户分配从身份验证服务器检索到的 IP 地址。如果您使用已配置 IP 地址的身份验证服务器（外部或内部），我们建议使用此方法。授权服务器在 Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups 窗格中配置。
- Use DHCP - 选择此项，以便从 DHCP 服务器获取 IP 地址。如果您使用 DHCP，请在 Configuration > Remote Access VPN > DHCP Serve 窗格中配置服务器。

- Use internal address pools - 选择此项，以便让 ASA 分配内部配置的地址池中的 IP 地址。内部配置的地址池是配置地址池分配的最简单方法。如果您使用此方法，请在 Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools 窗格中配置 IP 地址池。
  - Allow the reuse of an IP address __ minutes after it is released - 某个 IP 地址回到地址池后，重用此地址的延迟。添加延迟有助于在 IP 地址快速重新分配后防止防火墙可能遇到的问题。此选项默认为取消选中状态，表示 ASA 不会施加延迟。要添加延迟，请选择此复选框，并输入取值范围为 1 至 480 的分钟数，以便延迟 IP 地址重新分配。

配置 IPsec

ASA 会将 IPsec 用于 LAN 对 LAN VPN 连接，并提供有将 IPsec 用于客户端对 LAN VPN 连接的选项。在 IPsec 术语中，“对等体”是一个远程访问客户端或另一安全网关。

注　ASA 支持与思科对等体 （IPv4 或 IPv6），以及符合所有相关标准的第三方对等体的 LAN 对 LAN IPsec 连接。

在建立隧道的过程中，两个对等体会协商管理身份验证、加密、封装和密钥管理的安全关联。这些协商涉及两个阶段：第一个阶段，建立隧道 (IKE SA)；第二个阶段，管理该隧道内的流量 (IPsec SA)。

LAN 对 LAN VPN 可连接不同地理位置的网络。在 IPsec LAN 对 LAN 连接中， ASA 可充当发起方或响应方。在 IPsec 客户端对 LAN 连接中，ASA 只能充当响应方。发起方会提议 SA；响应方会接受、拒绝或提出相反提议，所有这一切都根据配置的 SA 参数进行。要建立连接，两个实体都必须同意 SA。

ASA 支持以下 IPSec 属性：

- 主模式用于使用数字证书进行身份验证时的协商第一阶段 ISAKMP 安全关联
- 攻击性模式用于使用预共享密钥进行身份验证时的协商第一阶段 ISAKMP 安全关联 (SA)
- 身份验证算法：
  - ESP-MD5-HMAC-128
  - ESP-SHA1-HMAC-160
- 身份验证模式：
  - 预共享密钥
  - X.509 数字证书
- Diffie-Hellman 群 1、 2 和 5。
- 加密算法：
  - AES-128、 -192 和 -256
  - 3DES-168
  - DES-56
  - ESP-NULL
- 扩展身份验证 (XAuth)
- 模式配置 （也称为 ISAKMP 配置方法）
- 隧道封装模式
- 使用 LZS 的 IP 压缩 (IPCOMP)

添加加密映射

Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps

此窗格显示当前配置的加密映射，该映射在 IPSec 规则中定义。您可以在此处添加、编辑、删除和上移、下移、剪切、复制和粘贴 IPsec 规则。

字段

注　您无法编辑、删除或复制隐式规则。使用动态隧道策略配置时，ASA 会隐式接受远程客户端的流量选择提议。您可以通过提供特定的流量选择来将其覆盖。

- Add - 点击以便启动 Create IPsec Rule 对话框，您可以在该对话框中为规则配置基本、高级和流量选择参数。
- Edit - 点击以便编辑现有规则。
- Delete - 点击以便删除表中突出显示的规则。
- Cut - 删除表中突出显示的规则，并在剪贴板中保留该规则，以供复制。
- Copy - 复制表中突出显示的规则。
- Find - 点击以便启用 Find 工具栏，您可以在其中指定想要查找的现有规则的参数。
  - Filter - 选择接口、源、目标、目标服务或规则查询，选择是或包含，并输入过滤参数，从而过滤查找结果。点击 ... 可以启动一个浏览对话框，该对话框会显示您可以选择的所有现有条目。
- Diagram - 显示描述突出显示的 IPSec 规则的图表。
- Type: Priority - 显示规则类型 （静态或动态）及其优先级。
- Traffic Selection
  - # - 指示规则编号。
  - Source - 指示流量发送至 Remote Side Host/Network 列中所列 IP 地址时，遵从此规则的 IP 地址。在详细信息模式 （请参阅 Show Detail 按钮）下，地址列可能包含带 any 一词的接口名称，如 inside:any。 any 表示内部接口上的任意主机都受此规则影响。
  - Destination - 列出当流量发自 Security Appliance Side Host/Network 列中所列 IP 地址时，遵从此规则的 IP 地址。在详细信息模式（请参阅 Show Detail 按钮）下，地址列可能包含带 any 一词的接口名称，如 outside:any。 any 表示外部接口上的任意主机都受此规则影响。同样也是在详细信息模式下，地址列可能包含用方括号括起来的 IP 地址，例如 [209.165.201.1-209.165.201.30]。这些地址都是转换后的地址。当内部主机连接至外部主机时，ASA 会将内部主机的地址映射至地址池中的地址。主机创建出站连接后，ASA 会保持该地址映射。此地址映射结构称为 xlate，会在内存中保留一段时间。
  - Service - 指定此规则指定的服务和协议 （TCP、 UDP、 ICMP 或 IP）。
  - Action - 指定 IPsec 规则类型 （保护或不保护）。
- Transform Set - 显示此规则的转换集。
- Peer - 标识 IPSec 对等体。
- PFS - 显示此规则的完全向前保密设置。
- NAT-T Enabled - 指示是否为此策略启用 NAT 遍历。
- Reverse Route Enabled - 指示是否为此策略启用反向路由注入。
- Connection Type -（仅对静态隧道策略有意义）将此策略的连接类型标识为双向、仅发出或仅应答。

- SA Lifetime - 显示该规则的 SA 生存期。
- CA Certificate - 显示该策略的 CA 证书。这仅适用于静态连接。
- IKE Negotiation Mode - 显示 IKE 协商是使用主模式还是攻击性模式。
- Description - （可选）指定此规则的简要描述。对于现有规则，这是您在添加该规则时键入的描述。隐式规则包括以下描述：“隐式规则”。要编辑除隐式规则之外的任意规则的描述，请右键单击此列，并选择 Edit Description 或双击此列。
- Enable Anti-replay window size - 设置抗重播窗口大小，该值为 64 的倍数，介于 64 至 1028 之间。在采用流量整形的分层 QoS 策略中，优先级排队的一个副作用 （请参阅 “Rule Actions > QoS Tab”）是数据包的重新排序。对于 IPSec 数据包，未处于抗重播窗口内的错序数据包，会生成警告系统日志消息。在进行优先级排队的情况下，这些警告会变成错误警报。配置抗重播窗口大小可以帮助您避免可能的错误警报。

创建 IPsec 规则/Tunnel Policy (Crypto Map) - Basic 选项卡

Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps - Edit IPsec Rule - Basic 选项卡

从 AAA Rules - Add Rule 部分提取字段。请使用此窗格为 IPsec 规则定义新的隧道策略。在您点击 **OK** 后，您在此处定义的值会显示在 IPsec Rules 表中。默认情况下，所有规则一旦显示在 IPsec Rules 表中，就会立即启用。

Tunnel Policy 窗格允许您定义用于协商 IPSec （第 2 阶段）安全关联 (SA) 的隧道策略。 ASDM 可捕获您的配置编辑，但不会将其保存至运行配置，直至您点击 **Apply**。

每个隧道策略都必须指定一个转换集，并确定其应用至的安全设备接口。转换集可标识执行 IPSec 加密和解密运算的加密和哈希算法。由于不是每个 IPSec 对等体都支持相同的算法，您可能想要指定一些策略，并为每个策略分配优先级。然后，安全设备会与远程 IPsec 对等体协商，以便商定两个对等体都支持的转换集。

隧道策略可以是 *static* 或 *dynamic*。静态隧道策略可以标识一个或多个，您的安全设备允许与其进行 IPsec 连接的 IPsec 对等体或子网。无论是您的安全设备发起连接，还是您的安全设备接收来自远程主机的连接请求，都可以使用静态策略。静态策略会要求您输入标识允许的主机或网络所需的信息。

对于被允许发起与安全设备的连接的远程主机，如果您无法或不想提供这些远程主机的相关信息，可以使用动态隧道策略。如果您仅将安全设备用作与远程 VPN 中央站点设备相关的 VPN 客户端，则不需要配置任何动态隧道策略。允许远程访问客户端，通过充当 VPN 中央站点设备的安全设备，发起与您的网络的连接时，动态隧道策略最为有用。远程访问客户端拥有动态分配的 IP 地址，或者您不想为大量的远程访问客户端配置单独的策略时，动态隧道策略非常有用。

字段

- Interface - 选择此策略应用至的接口的名称。
- Policy Type - 选择此隧道策略的类型 （静态或动态）。
- Priority - 输入此策略的优先级。
- IKE Proposals (Transform Sets) - 指定 IKEv1 和 IKEv2 IPsec 方案：
  - IKEv1 IPsec Proposal - 为策略选择方案 （转换集），然后点击 **Add** 将其移至活动转换集列表。点击 **Move Up** 或 **Move Down**，以便重新排列列表框中的方案。您最多可向加密映射条目或动态加密映射条目，添加 11 个方案。
  - IKEv2 IPsec Proposal - 为策略选择方案 （转换集），然后点击 **Add** 将其移至活动转换集列表。点击 **Move Up** 或 **Move Down**，以便重新排列列表框中的方案。您最多可向加密映射条目或动态加密映射条目，添加 11 个方案。
- Peer Settings - 对于动态加密映射条目可选 - 配置此策略的对等体设置。

  - Connection Type -（仅对静态隧道策略有意义）选择双向、仅发出或仅应答，以便指定此策略的连接类型。对于 LAN 对 LAN 连接，请选择双向或仅应答（而非仅发出）。对于 LAN 对 LAN 冗余，请选择仅应答。如果您选择仅发出，可以指定最多 10 个冗余对等体。对于单向，您可以指定仅发出或仅应答，二者均不会默认启用。
  - IP Address of Peer to Be Added - 输入您将要添加的 IPSec 对等体的 IP 地址。
- Enable Perfect Forwarding Secrecy - 选中此项，以便启用此策略的完全向前保密功能。PFS 是一个加密概念，其中每个新密钥都与任何先前密钥无关。在 IPsec 协商中，除非您指定完全向前保密，否则第 2 阶段的密钥会基于第 1 阶段的密钥。
- Diffie-Hellman 群 - 当您启用 PFS 时，还必须选择 ASA 用于生成会话密钥的 Diffie-Hellman 群。选项如下：
  - Group 1 (768-bits) = 使用完全向前保密功能，并且使用 Diffie-Hellman 群 1 来生成 IPsec 会话密钥，其中素数和生成元均为 768 位。此选项更加安全，但需要更多的处理开销。
  - Group 2 (1024-bits) = 使用完全向前保密功能，并且使用 Diffie-Hellman 群 2 来生成 IPsec 会话密钥，其中素数和生成元均为 1024 位。此选项比群 1 更加安全，但需要更多的处理开销。
  - Group 5 (1536-bits) = 使用完全向前保密功能，并且使用 Diffie-Hellman 群 5 来生成 IPsec 会话密钥，其中素数和生成元均为 1536 位。此选项比组 2 更加安全，但需要更多的处理开销。
  - Group 14 = 使用完全向前保密功能，并将 Diffie-Hellman 群 14 用于 IKEv2。
  - Group 19 = 使用完全向前保密功能，并将 Diffie-Hellman 群 19 用于 IKEv2，以便支持 ECDH。
  - Group 20 = 使用完全向前保密功能，并将 Diffie-Hellman 群 20 用于 IKEv2，以便支持 ECDH。
  - Group 21 = 使用完全向前保密功能，并将 Diffie-Hellman 群 21 用于 IKEv2，以便支持 ECDH。
  - Group 24 = 使用完全向前保密功能，并将 Diffie-Hellman 群 24 用于 IKEv2。

创建 IPsec 规则/Tunnel Policy (Crypto Map) - Advanced 选项卡

Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps - Edit IPsec Rule - Advanced 选项卡

字段

- Enable NAT-T - 启用此策略的 NAT 遍历 (NAT-T)。
- Enable Reverse Route Injection - 启用此策略的反向路由注入。
  如果您为远程 VPN 客户端或 LAN 对 LAN 会话运行 ASA 或路由信息协议 (RIP)，反向路由注入 (RRI) 会被用于填充运行动态路由协议（如开放最短路径优先 (OSPF) 或增强型内部网关路由协议 (EIGRP)）的内部路由器的路由表。
- Security Association Lifetime Settings - 配置安全关联 (SA) 的持续时间。此参数指定 IPsec SA 密钥生存期的度量方式，即 IPsec SA 过期并必须用新的密钥重新协商前，它可以持续的时长。
  - Time - 根据小时 (hh)、分钟 (mm) 和秒 (ss) 指定 SA 生存期。
  - Traffic Volume - 根据流量的千字节数定义 SA 生存期。输入负载数据的千字节数量，IPsec SA 在达到该数量后到期。最小值为 100 KB，默认值为 10000 KB，最大值为 2147483647 KB。
- Static Type Only Settings - 指定静态隧道策略的参数。
  - Device Certificate - 选择要使用的证书。如果您选择 None (Use Preshared Keys) 之外的选项，此设置为默认值。您选择 None 之外的选项时， Send CA certificate chain 复选框处于活动状态。
  - Send CA certificate chain - 启用整个信任点链的传输。

- IKE Negotiation Mode - 选择 IKE 协商模式、主模式或攻击性模式。此参数可以设置交换密钥信息和设置 SA 的模式。它设置该协商的发起方使用的模式；响应方会自动协商。攻击性模式速度较快，使用的数据包较少，交换次数较少，但是它不会保护通信方的身份。主模式速度较慢，使用的数据包较多，交换次数较多，但是它会保护通信方的身份。此模式更安全，并且是默认选择。如果选择 Aggressive，则 Diffie-Hellman Group 列表会激活。
- Diffie-Hellman Group - 选择要应用的 Diffie-Hellman 群。选择如下：群 1 （768 位）、群 2 （1024 位）或群 5 （1536 位）。

- ESP v3 - 指定是否为加密和动态加密映射验证传入 ICMP 错误消息，设置每安全关联策略，或者启用流量数据包：
  - Validate incoming ICMP error messages - 选择是否验证通过 IPsec 隧道接收，并发往专用网络上的内部主机的那些 ICMP 错误消息。
  - Enable Do Not Fragment (DF) policy - 定义 IPsec 子系统如何处理大型数据包，这些数据包在 IP 标头中设置了不分片 (DF) 位。选择以下任一选项：

    Clear DF bit - 忽略 DF 位。

    Copy DF bit - 保持 DF 位。

    Set DF bit - 设置并使用 DF 位。
  - Enable Traffic Flow Confidentiality (TFC) packets - 启用虚拟 TFC 数据包，这些数据包会通过隧道，用于屏蔽流量配置文件。

    注　在启用 TFC 之前，您必须先在 Tunnel Policy (Crypto Map) Basic 选项卡上设置 IKE v2 IPsec 方案。

    可以使用 Burst、 Payload Size 和 Timeout 参数生成穿过指定 SA 的随机长度的数据包。

创建 IPsec 规则/Traffic Selection 选项卡

Configuration > VPN > IPSec > IPSec Rules > Add/Edit Rule > Tunnel Policy (Crypto Map) - Traffic Selection 选项卡

此窗口允许您定义要保护 （允许）或不保护 （拒绝）哪些流量。

字段

- Action - 指定此规则要采取的操作。选项为保护和不保护。
- Source - 指定源主机或网络的 IP 地址、网络对象组或接口 IP 地址。规则不能将相同地址同时用作源和目标。点击 … 可启动包含以下字段的 Browse Source 对话框：
  - Add/Edit - 选择 IP 地址或网络对象组，以便添加更多源地址或组。
  - Delete - 点击此项可删除条目。
  - Filter - 输入 IP 地址，以便过滤显示的结果。
  - Name - 指示后面的参数指定源主机或网络的名称。
  - IP Address - 指示后面的参数指定源主机或网络的接口、 IP 地址和子网掩码。
  - Netmask - 选择应用于该 IP 地址的标准子网掩码。此参数在您选择 IP Address 选项按钮时显示。
  - Description - 输入描述。
  - Selected Source - 点击 **Source**，以便将选定条目作为源包含。

- Destination - 指定目标主机或网络的 IP 地址、网络对象组或接口 IP 地址。规则不能将相同地址同时用作源和目标。点击 … 可启动包含以下字段的 Browse Destination 对话框：
  - Add/Edit - 选择 IP 地址或网络对象组，以便添加更多目标地址或组。
  - Delete - 点击此项可删除条目。
  - Filter - 输入 IP 地址，以便过滤显示的结果。
  - Name - 指示后面的参数指定目标主机或网络的名称。
  - IP Address - 指示后面的参数指定目标主机或网络的接口、 IP 地址和子网掩码。
  - Netmask - 选择应用于该 IP 地址的标准子网掩码。此参数在您选择 IP Address 选项按钮时显示。
  - Description - 输入描述。
  - Selected Destination - 点击 **Destination**，以便将选定条目作为目标包含。
- Service - 输入一个服务，或者点击 ... 以便启动 Browse Service 对话框，在该对话框中，您可以从服务列表选择服务。
- Destination - 输入 Traffic Selection 条目的描述。
- More Options
  - Enable Rule - 点击此复选框可启用此规则。
  - Source Service - 输入一个服务或点击 **...** 以便启动 Browse Service 对话框，在该对话框中，您可以从服务列表选择服务。
  - Time Range - 定义此规则应用的时间范围。
  - Group - 表示后面的参数指定源主机或网络的接口和组名称。
  - Interface - 选择 IP 地址的接口名称。此参数在您选择 IP Address 选项按钮时显示。
  - IP Address - 指定此策略应用至的接口的 IP 地址。此参数在您选择 IP Address 选项按钮时显示。
  - Destination - 指定源或目标主机或网络的 IP 地址、网络对象组或接口 IP 地址。规则不能将相同地址同时用作源和目标。对于这些字段中的任一字段，点击 **...**，以便启动包含以下字段的 Browse 对话框：
  - Name - 选择用作源或目标主机或网络的接口名称。此参数在您选择 Name 选项按钮时显示。这是与此选项关联的唯一参数。
  - Interface - 选择 IP 地址的接口名称。此参数在您点击 Group 选项按钮时显示。
  - Group - 为源或目标主机或网络，选择指定接口上的组的名称。如果此列表中没有条目，您可以输入现有组的名称。此参数在您点击 Group 选项按钮时显示。
- **Protocol and Service** - 指定与此规则相关的协议和服务参数。

注　“Any - any”IPsec 规则不会被允许。此类规则会阻止设备及其对等体支持多个 LAN 对 LAN 隧道。

  - TCP - 指定此规则适用于 TCP 连接。此选项还会显示 Source Port and Destination Port 分组框。
  - UDP - 指定此规则适用于 UDP 连接。此选项还会显示 Source Port and Destination Port 分组框。
  - ICMP - 指定此规则适用于 ICMP 连接。此选项还会显示 ICMP Type 分组框。
  - IP - 指定此规则适用于 IP 连接。此选项还会显示 IP Protocol 分组框。
  - Manage Service Groups - 显示 Manage Service Groups 窗格，在此窗格上，您可以添加、编辑或删除一组 TCP/UDP 服务/端口。

  - Source Port and Destination Port - 包含 TCP 或 UDP 端口参数，具体取决于您在 Protocol and Service 分组框中选择的选项按钮。
  - Service - 指示您正为个别服务指定参数。指定应用过滤器时要使用的服务名称和布尔操作符。
  - Boolean operator (unlabeled) - 列出用于匹配服务框指定服务的布尔条件 （等于、不等于、大于、小于或范围）。
  - Service (unlabeled) - 标识要匹配的服务 （例如 https、 kerberos 或 any）。如果您指定了范围服务运算符，此参数会变成两个框，您可以在其中输入范围的起始值和结束值。
  - … - 显示一个服务列表，您可在其中选择要显示在 Service 框中的服务。
  - Service Group - 指示您要为源端口指定服务组的名称。
  - Service (unlabeled) - 选择要使用的服务组。
  - ICMP Type - 指定要使用的 ICMP 类型。默认值为 any。点击 **...** 按钮可显示可用类型列表。
- 选项
  - Time Range - 指定现有时间范围的名称，或者创建新的范围。
  - … - 显示 Add Time Range 窗格，您可以在该窗格上定义新的时间范围。
  - Please enter the description below (optional) - 为您提供空间，以便输入规则的简要描述。

Pre-Fragmentation

Configuration > VPN > IPSec > Pre-Fragmentation

使用此窗格可设置任意接口的 IPsec 预分片策略和不分片 (DF) 位策略。

当隧道流量通过公用接口时，IPsec 预分片策略指定如何处理超过最大传输单位 (MTU) 设置的数据包。此功能提供了一种处理 ASA 和客户端之间的路由器或 NAT 设备拒绝或丢弃 IP 分片的情况的方法。例如，假设客户端要从 ASA 后面的 FTP 服务器进行 FTP 获取。 FTP 服务器在公用接口上传输封装后会超过 ASA 的 MTU 大小的数据包。选定选项会决定 ASA 如何处理这些数据包。预分片策略适用于从 ASA 公用接口发出的所有流量。

ASA 会封装所有的隧道数据包。封装后， ASA 会先将超过 MTU 设置的数据包分片，然后通过公用接口传输它们。此为默认策略。此选项适用于允许分片数据包不受阻碍地通过隧道的情况。对于 FTP 示例，大型数据包会被封装，然后在 IP 层分片。中间设备可能会丢弃片段，或只是使片段错序。负载均衡设备可能会引入错序的片段。

当您启用预分片时， ASA 会先对超过 MTU 设置的隧道数据包进行分片，然后将其封装。如果这些数据包上的 DF 位已设置， ASA 会清除 DF 位，将数据包分片，然后将其封装。此操作会创建两个离开公用接口的独立未分片 IP 数据包，并且通过将片段转换为需要在对等体站点重组的完整数据包，将这些数据包成功传输至对等体站点。在我们的示例中， ASA 通过清除 DF 位覆盖 MTU 和允许分片。

注　在*任意*接口上更改 MTU 或预分片选项都会拆解*所有*现有连接 例如，如果 100 活动隧道在公用接口上终止，并且您在外部接口上更改 MTU 或预分片选项，则公用接口上的所有活动隧道都会被丢弃。

字段

- Pre-Fragmentation - 显示每个配置的接口的当前预分片配置。
  - Interface - 显示每个配置的接口的名称。
  - Pre-Fragmentation Enabled - 对于每个接口，显示是否已启用预分片。
  - DF Bit Policy - 显示每个接口的 DF 位策略。
- Edit - 显示 Edit IPsec Pre-Fragmentation Policy 对话框。

Edit IPsec Pre-Fragmentation Policy

Configuration > VPN > IPSec > Pre-Fragmentation > Edit IPSec Pre-Fragmentation Policy

使用该窗格可以为在父窗格上选定的接口，修改现有 IPsec 预分片策略和不分片 (DF) 位。

Configuration > VPN > IPsec > Pre-Fragmentation

字段

- Interface - 标识选定接口。您不能使用此对话框更改该参数。
- Enable IPsec pre-fragmentation - 启用或禁用 IPsec 预分片。ASA 会先对超过 MTU 设置的隧道数据包进行分片，然后将其封装。如果这些数据包上的 DF 位已设置， ASA 会清除 DF 位，将数据包分片，然后将其封装。此操作会创建两个离开公用接口的独立未分片 IP 数据包，并且通过将片段转换为需要在对等体站点重组的完整数据包，将这些数据包成功传输至对等体站点。
- DF Bit Setting Policy - 选择不分片位策略：Copy、 Clear 或 Set。

IPsec 转换集

Configuration > VPN > IPSec > Transform Sets

使用该窗格可查看、添加或编辑转换集。转换是一组在数据流上完成的操作，目的是提供数据身份验证、数据机密性和数据压缩。例如，采用 3DES 加密和 HMAC-MD5 身份验证算法 (ESP-3DES-MD5) 的 ESP 协议就是一种转换。

字段

- IKEv1 IPsec Proposals (Transform Sets) - 显示配置的转换集。
  - Name - 显示转换集的名称。
  - Mode - 显示转换集的模式，即隧道。此参数指定应用 ESP 加密和身份验证的模式；也就是说，将 ESP 应用至了原始 IP 数据包的哪一部分。隧道模式将 ESP 加密和身份验证应用至整个原始 IP 数据包 （IP 标头和数据），从而隐藏最终的源主机和目标地址。
  - ESP Encryption - 显示转换集的封装安全协议 (ESP) 加密算法。ESP 可提供数据隐私服务、可选的数据验证和抗重播服务。 ESP 会封装将要保护的数据。
  - ESP Authentication - 显示转换集的 ESP 身份验证算法。
- Add - 打开 Add Transform Set 对话框，您可以在其中添加新的转换集。
- Edit - 打开 Edit Transform Set 对话框，您可以在其中修改现有的转换集。
- Delete - 删除选定的转换集。无确认或撤消功能。
- IKEv2 IPsec Proposals - 显示配置的转换集。
  - Name - 显示 IPsec IKEv2 方案的名称。
  - Encryption - 显示 IKEv2 IPsec 方案的封装安全协议 (ESP) 加密算法。ESP 可提供数据隐私服务、可选的数据验证和抗重播服务。 ESP 会封装将要保护的数据。
  - Integrity Hash - 显示确保 ESP 协议的数据完整性的哈希算法。它可以确保数据包来自您认为的发送方，并且在传输过程中未被修改。它可以确保数据包来自您认为的发送方，并且在传输过程中未被修改。如果 AES-GCM/GMAC 已被配置为加密算法，对于完整性算法您必须选择 null。
- Add - 打开 Add IPsec Proposal 对话框，您可以在其中添加新的协议。
- Edit - 打开 Edit IPsec Proposal 对话框，您可以在其中修改现有的协议。
- Delete - 删除选定的方案。无确认或撤消功能。

Add/Edit IPsec Proposal (Transform Set)

Configuration > VPN > IPSec > Transform Sets > Add/Edit IPsec_Proposal_(Transform Set)

使用该窗格可添加或修改 IPsec IKEv1 转换集。转换是一组在数据流上完成的操作，目的是提供数据身份验证、数据机密性和数据压缩。例如，采用 3DES 加密和 HMAC-MD5 身份验证算法 (ESP-3DES-MD5) 的 ESP 协议就是一种转换。

字段

- Set Name - 指定此转换集的名称。
- Properties - 配置此转换集的属性。这些属性显示在 Transform Sets 表中。
  - Mode - 显示转换集的模式，即隧道。此字段显示应用 ESP 加密和身份验证的模式；也就是说，将 ESP 应用至了原始 IP 数据包的哪一部分。隧道模式将 ESP 加密和身份验证应用至整个原始 IP 数据包 （IP 标头和数据），从而隐藏最终的源主机和目标地址。
  - ESP Encryption - 选择转换集的封装安全协议 (ESP) 加密算法。ESP 可提供数据隐私服务、可选的数据验证和抗重播服务。 ESP 会封装将要保护的数据。
  - ESP Authentication - 选择转换集的 ESP 身份验证算法。

注 IPsec ESP （封装安全负载）协议同时提供加密和身份验证。数据包身份验证证明数据来自您认为的发送方；它通常被称为 “数据完整性”。

Add/Edit IPsec Proposal

Configuration > VPN > IPSec > Transform Sets > Add/Edit IPsec_Proposal

使用该窗格可添加或修改 IPsec IKEv2 方案。方案是一组在数据流上完成的操作，目的是提供数据身份验证、数据机密性和数据压缩。例如，采用 3DES 加密和 HMAC-MD5 身份验证算法 (ESP-3DES-MD5) 的 ESP 协议就是一种方案。

字段

- **Name - 指定此方案的名称。**
- **Encryption - 选择此方案的封装安全协议 (ESP) 加密算法。ESP 可提供数据隐私服务、可选的数据验证和抗重播服务。 ESP 会*封装*将要保护的数据。**
- **Integrity Hash - 选择此方案的 ESP 身份验证算法。哈希算法可确保 ESP 协议的数据完整性。它可以确保数据包来自您认为的发送方，并且在传输过程中未被修改。**

注　IPsec ESP（封装安全负载）协议同时提供加密和身份验证。数据包身份验证证明数据来自您认为的发送方；它通常被称为“数据完整性”。

配置负载均衡

如果您拥有一个远程客户端配置，在该配置中，您将使用连接至相同网络的两个或更多的 ASA 来处理远程会话，则可以将这些设备配置为共享其会话负载。此功能称为*负载均衡*。负载均衡会将会话流量定向至负载最低的设备，从而在所有设备之间分配负载。这样可以高效地利用系统资源，并提高性能极化可用性。

创建虚拟集群

要实施负载均衡，您可以将相同专用 LAN 对 LAN 网络上的两台或更多设备逻辑分组为*虚拟集群*。

虚拟集群中的所有设备都可以承载会话负载。虚拟集群中的一台设备，即*虚拟集群主用设备*，会将传入的连接请求定向至称为*备用设备*的其他设备。虚拟集群主用设备会监控集群中的所有设备、跟踪其忙碌程度，然后相应地分配会话负载。虚拟集群主用设备这一角色没有与某台物理设备绑定；它可以在设备之间切换。例如，如果当前的虚拟集群主用设备发生故障，该集群的一台备用设备会接管该角色，立即成为新的虚拟集群主用设备。

对于外部客户端，虚拟集群显示为单个*虚拟集群 IP 地址*。此 IP 地址不与特定物理设备绑定。它属于当前的虚拟集群主用设备；因此，它是虚拟的地址。VPN 客户端会尝试建立连接，先与此虚拟集群 IP 地址连接。随后，虚拟集群主用设备会将集群中负载最低的可用主机的公用 IP 地址，发送回客户端。在第二个事务（对用户透明）中，客户端会直接连接至该主机。这样，虚拟集群主用设备就能在资源之间均匀、高效地定向流量。

如果集群中的一台机器发生故障，终止的会话可以立即重新连接到虚拟集群 IP 地址。随后，虚拟集群主用设备会将这些连接，定向至集群中的另一活动设备。如果虚拟集群主用设备自身发生故障，该集群中的一台备用设备会作为新的虚拟会话主用设备，立即自动进行接管。即便该集群中的多台设备发生故障，只要该集群中的任一设备正常运行，并且可用，用户仍然可以继续与该集群连接。

负载均衡集群由受到以下限制的相同版本或混合版本的 ASA 组成：

- 包含两个相同版本 ASA 的负载均衡集群，可以为混合的 IPsec、 AnyConnect 和无客户端 SSL VPN 的客户端会话与无客户端会话进行负载均衡。
- 包括混合版本 ASA 或相同版本 ASA 的负载均衡集群仅可支持 IPsec 会话。然而，在这样的配置中， ASA 可能无法到达其全部的 IPsec 容量。第 19 页上的“比较负载均衡和故障转移”对该状况进行了说明。

从 7.1(1) 版本起，在确定集群中的每台设备所承载的负载方面， IPsec 和 SSL VPN 会话的数量和权重意义相当。这意味着与 ASA 7.0(x) 版本软件和 VPN 3000 集中器的负载均衡计算不同，也就是说，这些平台都使用加权算法，在某些平台上，会以不同于 IPsec 会话负载的方式计算 SSL VPN 会话。

该集群的虚拟主用设备会将会话请求分配至该集群的成员。ASA 会同等地对待所有会话（SSL VPN 或 IPSec 会话），并相应地分配它们。您可以配置允许的 IPsec 和 SSL VPN 会话的数量，可配置的数量最多为您的配置以及许可证允许的最大数量。

我们已测试过负载均衡集群中的最多十个节点。更大的集群可能能够正常工作，但是我们不正式支持此类拓扑。

地理负载均衡

在定期更改 DNS 解析的负载均衡环境中，必须谨慎考虑如何设置生存时间 (TTL) 值。要使 DNS 负载均衡配置与 AnyConnect 成功配合使用，从选定 ASA 到隧道完全建立，ASA 的名称到地址映射都必须保持相同。如果在输入凭据前，经过的时间过长，查找将会重新启动，不同的 IP 地址可能会成为解析后的地址。如果在输入凭据前， DNS 映射变更至不同的 ASA， VPN 隧道会失效。

VPN 的地理负载均衡通常使用 Cisco Global Site Selector (GSS)。GSS 使用 DNS 进行负载均衡，并且 DNS 解析的生存时间 (TTL) 值默认为 20 秒。如果您提高 GSS 上的 TTL 值，则可以显著降低连接发送故障的可能性。当用户输入凭据并建立隧道时，增加为更高的值可以为身份验证阶段提供充足的时间。

要增加输入凭证的时间，您还可以考虑禁用 Connect on Start Up。

比较负载均衡和故障转移

负载均衡和故障转移功能都是高可用性功能，但是它们的工作方式不同，并且具有不同的要求。在某些情况下，您可以同时使用负载均衡和故障转移。以下部分介绍这些功能之间的差异。

*负载均衡*是在虚拟集群中的设备之间，合理分配远程访问 VPN 流量的机制。它基于流量的简单分配，而不考虑吞吐量或其他因素。负载均衡集群由两台或更多的设备组成，其中之一是虚拟主用设备，其他设备为备用设备。这些设备不需要是完全相同的类型，也不需要具有相同的软件版本和配置。虚拟集群中的所有活动设备都可以承载会话负载。负载均衡会将流量定向至集群中负载最低的设备，从而在所有设备之间分配负载。这样可以高效地利用系统资源，提供更高的性能和高可用性。

*故障转移*配置需要两台一致的 ASA，并且它们通过专用故障转移链路或有状态故障转移链路相互连接。主用接口和设备的运行状况会受到监控，以便确定满足特定故障转移条件的时刻。如果这些条件得到满足，则会进行故障转移。故障转移同时支持 VPN 和防火墙配置。

ASA 支持两种故障转移配置：主用/主用故障转移和主用/备用故障转移。VPN 连接仅能在主用/备用配置、单一路由模式下运行。主用/主用故障转移需要多情景模式，所以不支持 VPN 连接。

使用主用/主用故障转移时，两台设备都可以传送网络流量。这不适用于负载均衡，尽管看似具有相同的效果。发生故障转移时，剩余的主用设备会根据配置的参数接管整合流量的传送。因此，配置主用/主用故障转移时，您必须确保两台设备的合并流量在每台设备的容量之内。

使用主用/备用故障转移时，只有一台设备会传送流量，而另一台设备会在备用状态下进行等待，不会传送流量。主用 / 备用故障转移允许您用第二台 ASA 来接管发生故障的设备的功能。当主用设备发生故障时，它将变为备用状态，而备用设备会变为主用状态。变为活动状态的设备会采用发生故障的设备的 IP 地址 （或者，对于透明防火墙，管理 IP 地址）和 MAC 地址，并开始传送流量。此时，处于备用状态的设备会接管主用设备的备用 IP 地址。如果主用设备发生故障，则由备用设备接管，而且不会给客户端 VPN 隧道带来任何干扰。

负载均衡许可要求

要使用 VPN 负载均衡，您必须具有带安全增强型许可证的 ASA 5512-X 型号设备，或者 ASA 5515-X 或更高型号的设备。VPN 负载均衡还需要一个活动的 3DES/AES 许可证。在启用负载均衡之前，安全设备将检查此加密许可证是否存在。如果没有检测到活动的 3DES 或 AES 许可证，安全设备会阻止启用负载均衡，也会阻止负载均衡系统进行 3DES 的内部配置，除非许可证允许此使用。

合格客户端

负载均衡仅在使用以下客户端发起的远程会话上有效：

- 思科 AnyConnect 安全移动客户端 （3.0 版本及更高版本）
- 思科 ASA 5505 安全设备 （充当 Easy VPN 客户端时）
- 支持 IKE 重定向的 IOS EZVPN 客户端设备 (IOS 831/871)
- 无客户端 SSL VPN （不是客户端）

负载均衡可与 IPSec 客户端和 SSL VPN 客户端与无客户端会话配合使用。所有其他 VPN 连接类型（L2TP、 PPTP、 L2TP/IPsec），包括 LAN 对 LAN，都可以连接至在其上启用了负载均衡的 ASA，但是它们不能参与负载均衡。

负载均衡先决条件

- 您必须在配置负载均衡之前，先配置 ASA 的公用和专用接口。为此，可选择 **Configuration > Device Setup > Interfaces**。
- 您必须事先配置虚拟集群 IP 地址所引用的接口。
- 加入集群的所有设备都必须共享同一个集群特定值：IP 地址、加密设置、加密密钥和端口。集群中的负载均衡设备上的所有外部和内部网络接口，都必须位于相同 IP 网络之上。

证书验证

使用 AnyConnect 为负载均衡执行证书验证，并且该连接通过某个 IP 地址重定向时，该客户端通过此 IP 地址进行其所有的名称检查。请确保重定向 IP 地址已在证书公用名或主题备用名称中列出。如果 IP 地址没有出现在这些字段中，则该证书会被视为不可信。

遵循 RFC 2818 中定义的准则，如果证书中包含有**主题备用名称**，我们会仅将**主题备用名称**用于名称检查，并忽略公用名。请确保已在证书的**主题备用名称**中，定义提供证书的服务器的 IP 地址。

对于独立 ASA， IP 地址为该 ASA 的 IP。在集群状况中，该地址取决于证书配置。如果该集群使用一个证书，则该地址会是该集群的 IP，而且该证书会包含带每个 ASA 的 IP 和 FQDN 的 Subject Alternative Name 扩展。如果该集群使用多个证书，则它还应是该 ASA 的 IP 地址。

使用高可用性和可扩展性向导配置 VPN 集群负载均衡

如果您拥有一个远程客户端配置，在该配置中，您将使用连接至相同网络的两个或更多的 ASA 来处理远程会话，则可以将这些设备配置为共享其会话负载。此功能称为负载均衡，它会将会话流量定向至负载最低的设备，从而在所有设备之间分配负载。负载均衡可以高效地利用系统资源，提供更高的性能和系统可用性。

使用 VPN Cluster Load Balancing Configuration 屏幕，可以为要参与负载均衡集群的设备，设置必需的参数。

启用负载均衡涉及以下操作：

- 建立集群的公用虚拟集群 IP 地址、UDP 端口（如需要）和 IPsec 共享机密，从而配置负载均衡集群。这些值对于集群中的每台设备均相同。
- 在设备上启用负载均衡，并定义设备特定属性，从而配置参与设备。这些值因设备而异。

先决条件

如果您将使用加密，则必须配置负载均衡内部接口。如果该接口未在负载均衡内部接口上启用，您尝试配置集群加密时会显示一条错误消息。

详细步骤

要实施负载均衡，可以执行以下步骤，从而将相同专用 LAN 对 LAN 网络上的两台或更多设备逻辑分组为一个虚拟集群：

步骤 1　选择 **Wizards > High Availability and Scalability**。

步骤 2　在 Configuration Type 屏幕中，点击 **Configure VPN Cluster Load Balancing**，然后点击 **Next**。

步骤 3　选择代表整个虚拟集群的单一 IP 地址。在公用子网地址范围内，指定由虚拟集群中的所有 ASA 共享的一个 IP 地址。

步骤 4　为此设备要参与的虚拟集群，指定 UDP 端口。默认值为 9023。如果另一应用正使用此端口，输入您想要用于负载均衡的 UDP 目标端口号。

步骤 5　要启用 IPSec 加密，并确保设备之间通信的所有负载均衡信息会被加密，请选中 **Enable IPSec Encryption** 复选框。您还必须指定并验证共享机密。虚拟集群中的 ASA 通过使用 IPsec 的 LAN 对 LAN 隧道进行通信。要禁用 IPSec 加密，请取消选中 **Enable IPSec Encryption** 复选框。

步骤 6　当您启用 IPsec 加密时，请指定 IPsec 对等体之间的共享机密。您输入的值会显示为连续的星号字符。

步骤 7　指定在集群内分配给此设备的优先级。取值范围为从 1 至 10。该优先级指示，此设备在启动或现有主用设备发生故障时，成为虚拟集群主用设备的可能性。设置的优先级越高（例如 10），此设备就越有可能将会成为虚拟集群主用设备。

注　如果虚拟集群中的设备在不同时间加电，第一台加电的设备会承担虚拟集群主用设备的角色。由于每个虚拟集群都需要一台主用设备，虚拟集群中的每台设备在其加电时都会进行检查，以确保该集群有一台虚拟主用设备。如果不存在主用设备，则该设备会承担此角色。后来加电并添加至该集群的设备，会成为备用设备。如果在虚拟集群中的所有设备同时加电，优先级设置最高的设备会成为虚拟集群主用设备。如果在虚拟集群中，两台或更多的设备同时加电，并且都拥有最高的优先级设置，则 IP 地址最小的设备会成为虚拟集群主用设备。

步骤 8　为该设备指定公用接口的名称或 IP 地址。

步骤 9　为该设备指定专用接口的名称或 IP 地址。

步骤 10　选中 **Send FQDN to client instead of an IP address when redirecting** 复选框，以便使 VPN 集群主用设备在将 VPN 客户端连接重定向至该集群设备时，发送使用集群设备的主机和域名的完全限定域名，而不是外部 IP 地址。

步骤 11　点击 **Next**。请在 Summary 屏幕中审阅您的配置。

步骤 12　点击 **Finish**。

VPN 集群负载均衡配置会被发送至 ASA。

配置负载均衡（不使用向导）

Load Balancing 窗格 (Configuration > Remote Access VPN > Load Balancing) 允许您在 ASA 上启用负载均衡。启用负载均衡涉及以下操作：

- 建立集群的公用虚拟集群 IP 地址、UDP 端口（如需要）和 IPsec 共享机密，从而配置负载均衡集群。这些值对于集群中的每台设备均相同。
- 在设备上启用负载均衡，并定义设备特定属性，从而配置参与设备。这些值因设备而异。

先决条件

- 对于使用 IPv6 地址的客户端，要成功连接至 ASA 的公开 IPv4 地址，网络中需要有可执行从 IPv6 至 IPv4 的网络地址转换的设备。
- 如果您将使用加密，则必须配置负载均衡内部接口。如果该接口未在负载均衡内部接口上启用，您尝试配置集群加密时会显示一条错误消息。

步骤 1　选择 **Configuration > Remote Access VPN > Load Balancing**。

步骤 2　选中 **Participate in Load Balancing**，以便指示此 ASA 是负载均衡集群的参与者。

您必须这样在参与负载均衡的每个 ASA 上，启用负载均衡。

步骤 3　在 **VPN Cluster Configuration** 区域中配置以下字段。对于整个虚拟集群，这些值都必须相同。该集群中的所有服务器都必须具有一致的集群配置。

- **Cluster IPv4 Address** - 指定代表整个 IPv4 虚拟集群的单一 IPv4 地址。在公用子网地址范围内，选择由虚拟集群中的所有 ASA 共享的一个 IP 地址。
  - **UDP Port** - 为此设备要参与的虚拟集群，指定 UDP 端口。默认值为 9023。如果另一应用正使用此端口，输入您想要用于负载均衡的 UDP 目标端口号。
- **Cluster IPv6 Address** - 指定代表整个 IPv6 虚拟集群的单一 IPv6 地址。在公用子网地址范围内，选择由虚拟集群中的所有 ASA 共享的一个 IP 地址。使用 IPv6 地址的客户端可以通过 ASA 集群的公开 IPv6 地址，或者通过 GSS 服务器，进行 AnyConnect 连接。同样地，使用 IPv4 地址的客户端可以通过 ASA 集群的公开 IPv4 地址，或者通过 GSS 服务器，进行 AnyConnect VPN 连接。任何一种连接类型都可以在 ASA 集群内进行负载均衡。

注　如果您具有一个至少配置有一个 DNS 服务器的 DNS 服务器组，且在一个 ASA 接口上启用了 DNS 查找，则也可以在 Cluster IPv4 Address 和 Cluster IPv6 Address 字段中指定虚拟集群的完全限定域名。

- **Enable IPsec Encryption** - 启用或禁用 IPsec 加密。如果您选中此复选框，则还必须指定并验证共享机密。虚拟集群中的 ASA 通过使用 IPsec 的 LAN 对 LAN 隧道进行通信。要确保设备之间通信的所有负载均衡信息会被加密，请选中此复选框。

- **IPsec Shared Secret** - 当您启用 IPsec 加密时，指定 IPsec 对等体之间的共享密钥。您在框中输入的值会显示为连续的星号字符。
- **Verify Secret** - 重新输入共享机密。确认在 IPsec Shared Secret 框中输入的共享机密。

步骤 4　在 **VPN Server Configuration** 区域中为特定 ASA 配置以下字段：

- **Public Interface** - 为该设备指定公用接口的名称或 IP 地址。
- **Private Interface** - 为该设备指定专用接口的名称或 IP 地址。
- **Priority** - 指定在集群内分配给此设备的优先级。取值范围为从 1 至 10。该优先级指示，此设备在启动或现有主用设备发生故障时，成为虚拟集群主用设备的可能性。设置的优先级越高 （例如 10），此设备就越有可能成为虚拟集群主用设备。

注　如果虚拟集群中的设备在不同时间加电，第一台加电的设备会承担虚拟集群主用设备的角色。由于每个虚拟集群都需要一台主用设备，虚拟集群中的每台设备在其加电时都会进行检查，以确保该集群有一台虚拟主用设备。如果不存在主用设备，则该设备会承担此角色。后来加电并添加至该集群的设备，会成为备用设备。如果在虚拟集群中的所有设备同时加电，优先级设置最高的设备会成为虚拟集群主用设备。如果在虚拟集群中，两台或更多的设备同时加电，并且都拥有最高的优先级设置，则 IP 地址最小的设备会成为虚拟集群主用设备。

- **NAT Assigned IPv4 Address** - 指定 NAT 将此设备的 IP 地址转换为的 IP 地址。如果 NAT 未被使用 （或者如果设备不在使用 NAT 的防火墙后面），将此字段留空。
- **NAT Assigned IPv6 Address** - 指定 NAT 将此设备的 IP 地址转换为的 IP 地址。如果 NAT 未被使用 （或者如果设备不在使用 NAT 的防火墙后面），将此字段留空。
- **Send FQDN to client** - 选中此复选框，以便使 VPN 集群主用设备在将 VPN 客户端连接重定向至该集群设备时，发送使用集群设备的主机和域名的完全限定域名，而不是外部 IP 地址。

  默认情况下， ASA 仅将负载均衡重定向中的 IP 地址发给客户端。如果使用的证书基于 DNS 名称，证书将在重定向到备用设备时变得无效。

  作为 VPN 集群主用设备，该 ASA 在将 VPN 客户端连接重定向至一个集群设备（集群中的另一 ASA）时，可以通过反向 DNS 查找，发送此集群设备的完全限定域名 (FQDN)，而不是其外部 IP 地址。

  集群中的负载均衡设备上的所有外部和内部网络接口，都必须位于相同 IP 网络之上。

注　使用 IPv6，并将 FQDNS 向下发送至客户端时，这些名称必须都能够由 ASA 通过 DNS 进行解析。

启用使用 FQDN 的无客户端 SSL VPN 负载均衡

步骤 1　通过选中 **Send FQDN to client instead of an IP address when redirecting** 复选框为负载均衡启用 FQDN。

步骤 2　如果这些条目不存在，为您的 ASA 的每个外部接口向 DNS 服务器添加一个条目。每个 ASA 外部 IP 地址都应具有一个与其关联的 DNS 条目，以供查找。对于反向查找，也必须启用这些 DNS 条目。

步骤 3　对于拥有通向 DNS 服务器的路由的接口， DNS 服务器路由的所有接口，在 **Configuration > Device Management > DNS > DNS Client** 对话框中启用 ASA 上的 DNS 查找。

步骤 4　在 ASA 上定义您的 DNS 服务器 IP 地址。为此，请点击 Add on this 对话框。这将打开 Add DNS Server Group 对话框。输入 DNS 服务器的 IPv4 或 IPv6 地址；例如 192.168.1.1 或 2001:DB8:2000::1。

步骤 5　点击 **OK** 和 **Apply**。

设置全球 NAC 参数

ASA 会使用经由 UDP 的可扩展身份验证协议 (EAP) (EAPoUDP) 消息来验证远程主机的状态。状态验证涉及在分配网络访问策略之前，检查远程主机符合安全要求的情况。在 ASA 上配置 NAC 前，您必须先为网络准入控制配置访问控制服务器。

字段

NAC 窗格允许您设置应用于所有 NAC 通信的属性。此窗格顶部的以下全局属性会应用于 ASA 和远程主机之间的 EAPoUDP 消息：

- Port - 经由 UDP 的 EAP 与主机上的 Cisco Trust Agent (CTA) 通信的端口号。此端口号必须与在 CTA 上配置的端口号匹配。输入取值范围为 1024 至 65535 的值。默认设置为 21862。
- Retry if no response - ASA 重新发送经由 UDP 的 EAP 消息的次数。此属性限制响应重新质询间隔到期而发送的连续重试的次数。该设置以秒为单位。输入介于 1 和 3 之间的值。默认设置为 3。
- Rechallenge Interval - ASA 在它向主机发送 EAPoUDP 消息时启动该计时器。来自主机的响会清除该计时器。如果计时器在 ASA 收到响应前到期，它会重新发送该消息。该设置以秒为单位。输入介于 1 和 60 之间的值。默认设置为 3。
- Wait before new PV Session - ASA 在它将远程主机的 NAC 会话置于保留状态时启动此计时器。如果它在发送数量等于 “Retry if no response”设置值的 EAPoUDP 消息后，没有收到响应，则会将会话置于保留状态。ASA 在从 ACS 服务器收到 Access Reject 消息后，还会启动此计时器。当计时器到期时， ASA 会尝试发起与此远程主机的经由 UDP 的 EAP 的新关联。该设置以秒为单位。输入介于 60 和 86400 之间的值。默认设置为 180。

NAC 窗格的 Clientless Authentication 区域，允许您为不响应 EAPoUDP 请求的主机配置设置。没有为其运行 CTA 的主机，不会响应这些请求。

- Enable clientless authentication - 点击此项可启用无客户端身份验证。ASA 会以用户身份验证请求的形式，向访问控制服务器发送配置的无客户端用户名和密码。 ACS 反过来，会请求无客户端主机的访问策略。如果将此属性留空， ASA 将应用无客户端主机的默认 ACL。
- Clientless Username - 在 ACS 上，为无客户端主机配置的用户名。默认设置为 clientless。输入 1 至 64 个 ASCII 字符，不包括前导和尾部空格、井号 (#)、问号 (?)、单引号和双引号（“ ”和 "）、星号 (*) 以及尖括号 （< 和 >）。
- Password - 在 ACS 上为无客户端主机配置的密码。默认设置为 clientless。请输入 4 -32 个 ASCII 字符。
- Confirm Password - 重复在 ACS 上为无客户端主机配置的密码，以供验证。
- Enable Audit - 如果客户端不响应状态验证请求，请点击此项将客户端的 IP 地址传送到可选的审核服务器。审核服务器（例如 Trend 服务器）使用主机地址直接质询主机，以评估其运行状态。例如，它可能会质询主机确定它的病毒检查软件是否处于活动和最新状态。审核服务器完成与远程主机后的交互后，它会将标记传送给状态验证服务器，指示远程主机的运行状况。
- None - 点击此项，以便禁用无客户端身份验证和审核服务。

配置网络准入控制策略

NAC 策略表显示在 ASA 上配置的网络准入控制 (NAC) 策略。

要添加、更改或移除 NAC 策略，请执行以下任一操作：

- 要添加 NAC 策略，请选择 **Add**。系统将打开 Add NAC Framework Policy 对话框。
- 要更改 NAC 策略，双击该策略或选择该策略并点击 **Edit**。系统将打开 Edit NAC Framework Policy 对话框。
- 要移除 NAC 策略，选择它并点击 **Delete**。

以下部分描述 NAC、其要求及如何向策略属性分配值：

关于 NAC

NAC 会执行终端合规性和漏洞检查，并以此作为网络生产访问的条件，从而防止企业网络遭受蠕虫、病毒和欺诈应用程序的入侵和感染。我们将这些检查称为*状态验证*。您可以配置状态验证来确保拥有 AnyConnect 或无客户端 SSL VPN 会话的主机上的防病毒文件、个人防火墙规则或入侵防御软件均为最新，然后向内联网上的易受攻击主机提供访问权限。状态验证可以包括，对远程主机上运行的应用程序是否使用最新修补程序进行更新的验证。NAC 仅在用户身份验证和隧道设置之后进行。 NAC 对于防止不受自动网络策略实施约束的主机 （家用 PC）访问企业网络，特别有用。

终端和 ASA 之间的隧道建立会触发状态验证。

您可以将 ASA 配置为，如果客户端不响应状态验证请求，则将客户端的 IP 地址传送到可选的审核服务器。审核服务器（例如 Trend 服务器）使用主机地址直接质询主机，以评估其运行状态。例如，它可能会质询主机确定它的病毒检查软件是否处于活动和最新状态。审核服务器完成与远程主机后的交互后，它会将标记传送给状态验证服务器，指示远程主机的运行状况。

验证状态成功或收到指示远程主机运行状况良好的标记后，状态验证服务器会将一个网络访问策略发送到 ASA，以便应用于隧道上的流量。

在涉及 ASA 的 *NAC Framework* 配置中，只有在客户端上运行的 Cisco Trust Agent 可以履行状态代理角色，而且只有思科访问控制服务器 (ACS) 可以履行状态验证服务器角色。ACS 可使用动态 ACL 确定每个客户端的访问策略。

作为 RADIUS 服务器，除了作为状态验证服务器履行其角色，ACS 可以对建立隧道所需的登录凭证进行身份验证。

注　只有在 ASA 上配置的 NAC 框架策略可支持审核服务器的使用。

在它作为状态验证服务器的角色中，ACS 使用访问控制列表。如果状态验证成功，且 ACS 指定一个重定向 URL 作为它发到 ASA 的访问策略的一部分， ASA 将所有 HTTP 和 HTTPS 请求从远程主机重定向至重定向 URL。一旦状态验证服务器将访问策略上传到 ASA，所有关联流量必须通过安全设备和 ACS （反之亦然）才能到达其目标。

如果 NAC 框架策略被分配给组策略，远程主机和 ASA 之间的隧道建立会触发状态验证。但是，NAC 策略框架可以确定免除状况验证的操作系统和指定筛选这些流量的可选 ACL。

使用、要求和限制

当 ASA 配置为支持 NAC 时，它作为 Cisco 安全访问控制服务器的一个客户端，要求至您在网络中必须安装至少一个访问控制服务器来提供 NAC 身份验证服务。

在网络上配置一个或多个访问控制服务器后，您必须使用 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add or Edit External** 菜单选项，注册访问控制服务器组。然后添加 NAC 策略。

NAC 框架的 ASA 支持只限于远程访问 IPsec 和无客户端 SSL VPN 会话。NAC 框架配置只支持单一模式。

ASA 上的 NAC 不支持第 3 层 （非 VPN）和 IPv6 流量。

字段

- Policy Name - 输入最多 64 个字符给新的 NAC 策略命名。

  在配置 NAC 策略后，策略名称会显示在 Network (Client) Access 组策略中的 NAC Policy 属性旁。分配一个有助于将其属性或用途，与您可能配置的其他属性或用途区分开来的名称。

- Status Query Period - ASA 在每次成功的状态验证和状态查询响应之后，会启动此计时器。此计时器到期，会触发主机状态的变化查询，称为*状态查询*。输入取值范围为 30 至 1800 的秒数。默认设置为 300。

- Revalidation Period - ASA 在每次成功的状态验证后，会启动此计时器。此计时器到期，会触发下一次无条件状态验证。 ASA 在重新验证期间保持状态验证。如果访问控制服务器在状态验证或重新验证期间不可用，则默认组策略开始生效。输入每次成功的状态验证之间的间隔，以秒为单位。取值范围为 300 至 86400。默认设置为 36000。

- Default ACL -（可选）如果状态验证失败，ASA 将应用与选定 ACL 关联的安全策略。选择 None 或从列表中选择一个扩展 ACL。默认设置为 None。如果设置为 None，且状态验证失败， ASA 将应用默认组策略。

  使用 Manage 按钮可填充下拉列表，以及查看列表中的 ACL 配置。

- Manage - 打开 ACL Manager 对话框。点击此项，以便查看、启用、禁用和删除标准 ACL 和每个 ACL 中的 ACE。 Default ACL 属性旁的列表会显示 ACL。

- Authentication Server Group - 指定要用于状态验证的身份验证服务器组。此属性旁的下拉列表显示在此 ASA 上配置的、可用于远程访问隧道的所有类型的 RADIUS 服务器组的名称。选择包含至少一个配置用于支持 NAC 的服务器的 ACS 组。

- Posture Validation Exception List - 显示远程计算机免除状态验证的一个或多个属性。每个条目至少列出操作系统以及 Enabled 设置的 Yes 或 No。一个可选过滤器可标识用于匹配远程计算机的其他属性的 ACL。由一个操作系统和一个过滤器组成的条目，要求远程计算机匹配二者才能免除状态验证。如果 Enabled 设置已设置为 No， ASA 会忽略此条目。

- Add - 向 Posture Validation Exception 列表添加一个条目。

- Edit - 修改 Posture Validation Exception 列表中的一个条目。

- Delete - 从 Posture Validation Exception 列表中移除一个条目。

后续操作

配置 NAC 策略后，您必须将其分配至组策略，它才能变为活动状态。为此，请选择 **Configuration > Remote Access VPN> Network (Client) Access > Group Policies > Add** 或 **Edit > General > More Options**，从 NAC Policy 属性旁的下拉列表选择 NAC 策略名称。

添加/编辑状态验证例外

Add/Edit Posture Validation Exception 对话窗格允许您根据远程计算机的操作系统和匹配过滤器的其他可选属性，免除远程计算机的状态验证。

- Operating System - 选择远程计算机的操作系统。如果该计算机运行此操作系统，它可免除状态验证。默认设置为空。
- Enable - ASA 只有在您选中 Enabled 时，才会为此窗格中显示的属性设置，检查远程计算机。否则，它会忽略属性设置。默认设置为取消选中。
- Filter -（可选）如果计算机的操作系统与 Operating System 属性的值匹配，此项用于应用 ACL 来过滤流量。
- Manage - 打开 ACL Manager 对话框。点击此项，以便查看、启用、禁用和删除标准 ACL 和每个 ACL 中的 ACE。Default ACL 属性旁的列表会显示 ACL。使用此按钮可填充 Filter 属性旁的列表。

常规 VPN 设置

AnyConnect 定制/本地化

您可以定制 AnyConnect VPN 客户端来向远程用户显示您自己的公司图像，包括运行在 Windows、Linux 和 Mac OS X 计算机上的客户端。通过 AnyConnect Customization/Localization 下的以下 ASDM 屏幕，可以导入以下类型的定制文件：

- **Resources** - AnyConnect 客户端的已修改的 GUI 图标。
- **Binary** - 用于替换 AnyConnect 安装程序的可执行文件。这包括 GUI 文件，以及 VPN 客户端配置文件、脚本和其他客户端文件。
- **Script** - 在 AnyConnect 进行 VPN 连接前后将运行的脚本。
- **GUI Text and Messages** - AnyConnect 客户端使用的标题和消息。
- **Customized Installer** - 用于修改客户端安装的转换。
- **Localized Installer** - 用于更改客户端使用的语言的转换。

每个对话框提供以下操作：

- **Import** 启动 Import AnyConnect Customization Objects 对话框，可以在其中指定要作为对象导入的文件。
- **Export** 启动 Export AnyConnect Customization Objects 对话框，可以在其中指定要作为对象导出的文件。
- **Delete** 移除所选对象。

限制

- 在 Windows Mobile 设备上运行的 AnyConnect 客户端不支持定制。

AnyConnect Customization/Localization > Resources

导入的自定义组件的文件名必须与 AnyConnect GUI 使用的文件名匹配，这些文件名对于每个操作系统都不同，并且对于 Mac 和 Linux 区分大小写。例如，如果要替换 Windows 客户端的公司徽标，必须将您的公司徽标导入为 company_logo.png。如果以其他文件名将其导入，则 AnyConnect 安装程序不会更改组件。但是，如果您部署自己的可执行文件来定制 GUI，则该可执行文件可以使用任何文件名调用资源文件。

如果将图像导入为资源文件（如 company_logo.bmp），则导入的图像会定制 AnyConnect，直到使用同一文件名重新导入另一个图像为止。例如，如果将 company_logo.bmp 替换为自定义图像，然后删除该图像，则客户端会继续显示您的图像，直到使用同一文件名导入新图像（或原始思科徽标图像）为止。

AnyConnect Customization/Localization > Binary 和 Script

ES - 在 ASDM 中为 Binary 和 Script 使用了同一链接，因此请暂时共享此链接，然后针对 ASDM 提交一个缺陷，以使其添加另一个链接。

AnyConnect Customization/Localization > Binary

对于 Windows、Linux 或 Mac（基于 PowerPC 或 Intel）计算机，您可以部署自己的使用 AnyConnect 客户端 API 的客户端。通过替换客户端二进制文件来替换 AnyConnect GUI 和 AnyConnect CLI。

Import 对话框的字段包括：

- **Name** 输入您要替换的 AnyConnect 文件的名称。
- **Platform** 选择文件运行所在的操作系统平台。
- **Select a file** 文件名不需要与已导入的文件的名称相同。

AnyConnect Customization/Localization > Script

有关部署脚本及其局限和限制的完整信息，请参阅 《*AnyConnect VPN 客户端管理员指南*》。

Import 对话框的字段包括：

- **Name** - 输入脚本的名称。请确保指定正确的扩展名。例如 *myscript*.bat。
- **Script Type** - 在将要运行脚本时选择。

  AnyConnect 向文件名中添加前缀 *scripts_* 以及前缀 *OnConnect* 或 *OnDisconnect* 以将文件标识为 ASA 上的脚本。当客户端进行连接时，ASA 将该脚本下载到远程计算机上的适当目标目录，从而移除 *scripts_* 前缀并保留剩余的 *OnConnect* 或 *OnDisconnect* 前缀。例如，如果导入脚本 *myscript.bat*，则该脚本在 ASA 上显示为 *scripts_OnConnect_myscript.bat*。在远程计算机上，该脚本显示为 *OnConnect_myscript.bat*。

要确保脚本可靠地运行，请将所有 ASA 配置为部署相同的脚本。如果要修改或替换脚本，请使用与以前版本相同的名称并将替换脚本分配给用户可能连接到的所有 ASA。当用户进行连接时，新脚本会覆盖具有相同名称的脚本。

- **Platform** - 选择文件运行所在的操作系统平台。
- **Select a file** - 文件名不需要与为脚本提供的名称相同。

  ASDM 从任意源文件导入文件，为第 3 步中的 Name 创建指定的新名称。

AnyConnect Customization/Localization > GUI Text and Messages

可以编辑默认转换表或者创建新转换表，以更改 AnyConnect 客户端 GUI 上显示的文本和消息。此窗格还与 Language Localization 窗格共享功能。要获取更全面的语言转换，请转至 Configuration > Remote Access VPN > Language Localization。

除顶部工具栏中的常见按钮外，此窗格还有一个 **Add** 按钮，以及一个带附加按钮的模板区域。

Add - Add 按钮打开默认转换表的副本，可以直接编辑该副本，也可以将其保存。可以选择已保存的文件的语言，并在以后编辑文件内文本的语言。

定制转换表中的消息时，请勿更改 msgid，而是更改 msgstr 中的文本。

为此模板指定语言。此模板即成为缓存中采用您指定的名称的转换表。使用与浏览器的语言选项兼容的缩写。例如，如果创建的是中文的表格并且使用的是 IE，请使用 IE 可识别的缩写 *zh*。

模板部分

- 点击 **Template** 以展开模板区域，它提供对默认英语转换表的访问。
- 点击 **View** 以查看并选择性保存默认英语转换表。
- 点击 **Export** 以保存默认英语转换表的副本而不对其进行查看。

AnyConnect Customization/Localization > Customized Installer Transforms

您可以通过创建自己的使用客户端安装程序部署的转换来对 AnyConnect 客户端 GUI 执行更全面的定制 （仅适用于 Windows）。将转换导入到 ASA，它使用安装程序来部署转换。

Windows 是应用转换的唯一有效选项。有关转换的详细信息，请参阅 《*AnyConnect 管理员指南*》。

AnyConnect Customization/Localization > Localized Installer Transforms

可以通过转换来转换客户端安装程序显示的消息。转换会修改安装，但会将原始的安全签名 MSI 保留完好。这些转换仅转换安装程序屏幕，而不转换客户端 GUI 屏幕。

IPsec VPN 客户端软件

注　**VPN 客户端已停产并终止支持。**有关配置 VPN 客户端的信息，请参阅 ASA V9.2 的 ASDM 文档。**我们建议您升级到 AnyConnect 安全移动客户端。**

编辑客户端软件位置

注　**VPN 客户端已停产并终止支持。**有关配置 VPN 客户端的信息，请参阅 ASA V9.2 的 ASDM 文档。**我们建议您升级到 AnyConnect 安全移动客户端。**

组策略

组策略是在 ASA 上以内部方式或在 RADIUS 或 LDAP 服务器上以外部方式存储的面向用户的属性/值对的集合。组策略会在客户端建立 VPN 连接时向其分配属性。默认情况下， VPN 用户不具有组策略关联。组策略信息供 VPN 连接配置文件 （隧道组）和用户帐户使用。

ASA 提供名为 DfltGrpPolicy 的默认组策略。默认组参数是最可能跨所有用户和组通用的组参数，有助于精简配置任务。新组可以从此默认组 “继承”参数，用户可以从其组或默认组 “继承”参数。可以在配置组和用户时覆盖这些参数。

可以配置内部和外部组策略。内部组策略以本地方式存储，外部组策略在 RADIUS 或 LDAP 服务器上以外部方式存储。

在 Group Policy 对话框中，可配置以下种类的参数：

- 常规属性：名称、条幅、地址池、协议、过滤和连接设置。
- 服务器：DNS 和 WINS 服务器、 DHCP 范围和默认域名。
- 高级属性：拆分隧道、 IE 浏览器代理以及 AnyConnect 客户端和 IPSec 客户端。

在配置这些参数之前，应该配置以下各项：

- 访问时长。
- 过滤器。
- 用于过滤和拆分隧道的网络列表。
- 用户身份验证服务器和内部身份验证服务器。

可以配置以下类型的组策略：

- 配置外部组策略 - 外部组策略将 ASA 指向 RADIUS 或 LDAP 服务器，以检索会在内部组策略中以其他方式配置的大部分策略信息。对于 Network (Client) Access VPN 连接、Clientless SSL VPN 连接和 Site-to-Site VPN 连接，外部组策略以相同方式进行配置。
- 配置网络（客户端）访问组策略 - 这些连接由安装在终端上的 VPN 客户端发起。VPN 客户端的示例包括 AnyConnect 安全移动客户端和思科 VPN IPSec 客户端。在对 VPN 客户端进行身份验证后，远程用户可以访问公司网络或应用，就像其在现场一样。远程用户与公司网络之间的数据流量在通过互联网时利用加密来受保护。
- 配置无客户端 SSL VPN 内部组策略 - 这也称为基于浏览器的 VPN 访问。成功登录到 ASA 的门户页面时，远程用户可以从网页中显示的链接访问公司网络和应用。远程用户与公司网络之间的数据流量通过流经 SSL 隧道来受保护。
- 配置站点到站点内部组策略

组策略窗格字段

列出当前配置的组策略及 Add、 Edit 和 Delete 按钮，以帮助管理 VPN 组策略。

- Add - 提供一个下拉列表，可在其中选择添加内部还是外部组策略。如果只是点击 Add，则默认情况下将创建内部组策略。点击 Add 会打开 Add Internal Group Policy 对话框或 Add External Group Policy 对话框，通过它可向列表中添加新的组策略。此对话框包含三个菜单部分。点击各菜单项以显示其参数。在项之间移动时， ASDM 会保留设置。设置所有菜单部分上的参数完成后，点击 **Apply** 或 **Cancel**。
- Edit - 显示 Edit Group Policy 对话框，通过它可修改现有组策略。
- Delete - 通过它可从列表中移除 AAA 组策略。无确认或撤消功能。
- Assign - 通过它可向一个或多个连接配置文件分配组策略。
- Name - 列出当前配置的组策略的名称。
- Type - 列出每个当前配置的组策略的类型。
- Tunneling Protocol - 列出每个当前配置的组策略使用的隧道协议。
- Connection Profiles/Users Assigned to - 列出直接在 ASA 上配置的与该组策略关联的连接配置文件和用户。

配置外部组策略

外部组策略从外部服务器检索属性值授权和身份验证。组策略标识 ASA 可以查询属性的 RADIUS 或 LDAP 服务器组，并指定检索这些属性时要使用的密码。

ASA 上的外部组名引用 RADIUS 服务器上的用户名。换句话说，如果在 ASA 上配置外部组 X，则 RADIUS 服务器将查询视为对用户 X 的身份验证请求。因此，外部组实际只是 RADIUS 服务器上对于 ASA 有特殊意义的用户帐户。如果外部组属性与计划进行身份验证的用户存在于同一 RADIUS 服务器中，则其之间不得有任何名称重复。

在配置 ASA 以使用外部服务器之前，必须使用正确的 ASA 授权属性配置该服务器，并从这些属性的子集向个人用户分配特定权限。请遵循 “用于授权和身份验证的外部服务器”中的说明配置外部服务器。

外部组策略字段

- Name - 标识要添加或更改的组策略。对于 Edit External Group Policy，此字段为仅显示字段。
- Server Group - 列出将此策略应用到的可用服务器组。
- New - 打开一个对话框，通过它可选择创建新 RADIUS 服务器组还是新 LDAP 服务器组。其中任一选项都会打开 Add AAA Server Group 对话框。
- Password - 指定此服务器组策略的密码。

有关创建和配置 AAA 服务器的信息，请参阅《*Cisco ASA 系列常规操作 ASDM 配置指南*》的“*AAA 服务器和本地数据库*”一章。

使用 AAA 服务器进行密码管理

ASA 支持 RADIUS 和 LDAP 协议的密码管理。它仅对 LDAP 支持“password-expire-in-days”选项。其他参数对于支持此类通知的 AAA 服务器有效；即 RADIUS、使用 NT 服务器的 RADIUS 以及 LDAP 服务器。如果尚未配置 RADIUS 或 LDAP 身份验证， ASA 将忽略此命令。

注　某些支持 MS-CHAP 的 RADIUS 服务器当前不支持 MS-CHAPv2。此功能需要 MS-CHAPv2，因此请咨询供应商。

ASA 在使用 LDAP 或使用任何支持 MS-CHAPv2 的 RADIUS 配置进行身份验证时，通常支持以下连接类型的密码管理：

- AnyConnect VPN 客户端
- IPsec VPN 客户端
- IPsec IKEv2 客户端
- 无客户端 SSL VPN

Kerberos/Active Directory （Windows 密码）或 NT 4.0 域*不*支持密码管理。某些 RADIUS 服务器（例如 Cisco ACS）可以将身份验证请求代理到另一个身份验证服务器。但是，从 ASA 的角度而言，它仅传达到 RADIUS 服务器。

注　对于 LDAP，市场上不同的 LDAP 服务器有专有的密码更改方法。目前， ASA 仅对 Microsoft Active Directory 和 Sun LDAP 服务器实施专有密码管理逻辑。

本机 LDAP 需要 SSL 连接。在尝试执行 LDAP 密码管理之前，必须先启用基于 SSL 的 LDAP。默认情况下， LDAP 使用端口 636。

使用 AnyConnect 进行密码支持

ASA 支持 AnyConnect 的以下密码管理功能：

- 密码到期通知 （在用户尝试连接时）。
- 密码到期提醒 （在密码到期之前）。
- 密码到期覆盖。 ASA 忽略来自 AAA 服务器的密码到期通知，并对用户的连接进行授权。

配置密码管理后， ASA 会在远程用户尝试登录时通知他们其当前密码已到期或即将到期。然后，ASA 为用户提供机会更改密码。如果当前密码尚未到期，则用户仍然可以使用旧密码登录，并在以后更改密码。

AnyConnect 客户端不能启动密码更改，它只能通过 ASA 对来自 AAA 服务器的变更请求作出响应。AAA 服务器必须是代理到 AD 的 RADIUS 服务器，或者是 LDAP 服务器。

ASA 在以下条件下不支持密码管理：

- 使用 LOCAL （内部）身份验证时
- 使用 LDAP 授权时
- 仅使用 RADIUS 身份验证时，以及用户驻留在 RADIUS 服务器数据库上时

设置密码到期覆盖将指导 ASA 忽略来自 AAA 服务器的帐户已禁用指示。这可能是一项安全风险。例如，您可能不希望更改管理员密码。

启用密码管理会造成 ASA 向 AAA 服务器发送 MS-CHAPv2 身份验证请求。

配置网络 （客户端）访问组策略

为内部组策略配置常规属性

通过 Add or Edit Group Policy 对话框，可以为进行添加或修改的组策略指定隧道协议、过滤器、连接设置和服务器。对于此对话框中的每一个字段，如果选中 Inherit 复选框，则相应的设置将从默认组策略获取其值。 Inherit 是此对话框中所有属性的默认值。

可以通过启动 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit Internal Group Policy > General** 来配置内部组策略的常规属性。

字段

以下属性显示在 Add Internal Group Policy > General 对话框中。它们适用于 SSL VPN 和 IPsec 会话。因此，某些属性对于一种类型的会话显示，但对于另一种类型的会话则不显示。

- Name - 指定该组策略的名称 （最多 64 个字符）；允许空格。对于 Edit 功能，此字段为只读。
- Banner - 指定登录时要向用户显示的条幅文本。长度最多可以为 491 个字符。没有默认值。

  IPsec VPN 客户端对于条幅支持完全 HTML。但是，无客户端门户和 AnyConnect 客户端支持部分 HTML。要确保向远程用户正确显示条幅，请遵循以下准则：

  – 对于 IPsec 客户端用户，请使用 /n 标记。

  – 对于 AnyConnect 客户端用户，请使用
 标记。
- SCEP forwarding URL - CA 的地址，当客户端配置文件中配置了 SCEP 代理时需要该地址。
- Address Pools - 指定要用于该组策略的一个或多个 IPv4 地址池的名称。如果选中 Inherit 复选框，则组策略将使用 Default Group Policy 中指定的 IPv4 地址池。有关添加或编辑 IPv4 地址池的信息，请参阅第 4-3 页上的配置本地 IP 地址池。

  Select - 取消选中 Inherit 复选框以激活 Select 命令按钮。点击 Select 以打开 Address Pools 对话框，其中显示池名称、开始和结束地址以及可用于客户端地址分配的地址池的子网掩码，并且通过此对话框可从该列表中选择、添加、编辑、删除和分配条目。
- IPv6 Address Pools - 指定要用于该组策略的一个或多个 IPv6 地址池的名称。

  Select - 取消选中 Inherit 复选框以激活 Select 命令按钮。点击 Select 以打开 Select Address Pools 对话框，如先前所述。有关添加或编辑 IPv6 地址池的信息，请参阅第 4-3 页上的配置本地 IP 地址池。

注　可以为内部策略组同时指定 IPv4 和 IPv6 地址池。

- More Options - 点击字段右侧的向下箭头以显示该组策略的其他可配置选项。
- Tunneling Protocols - 指定该组可以使用的隧道协议。用户只能使用所选协议。选项如下：

  – Clientless SSL VPN - 指定通过 SSL/TLS 来使用 VPN，该 VPN 使用网络浏览器建立到 ASA 的安全远程访问隧道；无需软件和硬件客户端。无客户端 SSL VPN 可以提供从几乎任何可到达 HTTPS 互联网站点的计算机到范围广泛的企业资源的轻松访问，包括企业网站、启用网络功能的应用、 NT/AD 文件共享 （启用网络功能）、邮件和其他基于 TCP 的应用。

  – SSL VPN Client - 指定使用 Cisco AnyConnect VPN 客户端或传统 SSL VPN 客户端。如果使用的是 AnyConnect 客户端，必须选择此协议以支持移动用户安全 (MUS)。

  – IPsec IKEv1 - IP 安全协议。IPsec 被视为最安全的协议，为 VPN 隧道提供最完整的架构。站点间 （对等）连接和思科 VPN 客户端到 LAN 连接均可使用 IPsec IKEv1。

  - IPsec IKEv2 - 由 AnyConnect 安全移动客户端提供支持。将 IPsec 与 IKEv2 配合使用的 AnyConnect 连接提供高级功能，如软件更新、客户端配置文件、 GUI 本地化 （转换）和定制、 Cisco Secure Desktop 和 SCEP 代理。
  - L2TP over IPsec - 允许具有若干公共 PC 随附的 VPN 客户端和移动 PC 操作系统的远程用户通过公用 IP 网络建立到安全设备和专用企业网络的安全连接。L2TP 使用 PPP over UDP（端口 1701）来通过隧道传送数据。必须为 IPsec 传输模式配置安全设备。

- Filter - 指定要用于 IPv4 或 IPv6 连接的访问控制列表，或者是否从组策略继承值。过滤器由规则组成，这些规则根据诸如源地址、目标地址和协议之类的条件来确定允许还是拒绝隧道数据包通过 ASA。要配置过滤器和规则，请点击 **Manage**。
- NAC Policy - 选择要应用到该组策略的网络准入控制策略。可以向每个组策略分配一个可选 NAC 策略。默认值为 --None--。
- Manage - 打开 Configure NAC Policy 对话框。配置一个或多个 NAC 策略后，NAC 策略名称显示为 NAC Policy 属性旁的下拉列表中的选项。
- Access Hours - 选择应用到此用户的现有访问时长策略（如果有）的名称，或者创建新访问时长策略。默认值为 Inherit，或者，如果未选中 Inherit 复选框，则默认值为 --Unrestricted--。点击 **Manage** 以打开 Browse Time Range 对话框，可在其中添加、编辑或删除时间范围。
- Simultaneous Logins - 指定此用户允许的最大同时登录数。默认值为 3。最小值为 0，表示禁止登录并阻止用户访问。

  注　在没有最大限制时，允许多个同时连接可能会降低安全性并影响性能。

- Restrict Access to VLAN - （可选）也称为 “VLAN 映射”，此参数指定该组策略应用到的会话的出口 VLAN 接口。 ASA 将所有流量从该组转发到所选 VLAN。使用此属性向组策略分配 VLAN 以简化访问控制。向此属性赋值是在会话中使用 ACL 过滤流量的替代方法。除默认值 (Unrestricted) 外，下拉列表仅显示此 ASA 中配置的 VLAN。

  注　此功能适用于 HTTP 连接，但不适用于 FTP 和 CIFS。

- Connection Profile (Tunnel Group) Lock - 此参数仅允许通过所选连接配置文件 （隧道组）进行远程 VPN 访问，并会阻止通过其他连接配置文件进行访问。默认继承值为 None。
- Maximum Connect Time - 如果未选中 Inherit 复选框，则此参数指定最大用户连接时间 （以分钟为单位）。此时间结束时，系统会终止连接。最小值为 1 分钟，最大值为 35791394 分钟 （4000 多年，如果我们有幸如此长寿）。要允许无限连接时间，请选中 Unlimited （默认）。
- Idle Timeout - 如果未选中 Inherit 复选框，则此参数指定该用户的空闲超时时间段 （以分钟为单位）。如果在此时间段内用户连接上没有通信活动，则系统会终止连接。最短时间为 1 分钟，最长时间为 10080 分钟。默认值为 30 分钟。要允许无限连接时间，请选中 **Unlimited**。该值不适用于无客户端 SSL VPN 用户。
- Security Group Tag (SGT) - 输入将分配给与该组策略连接的 VPN 用户的 SGT 标记的数字值。
- On smart card removal - 在使用默认选项 Disconnect 的情况下，如果移除用于身份验证的智能卡，则客户端将拆除连接。如果希望不要求用户在连接期间将其智能卡保留在计算机中，请点击 **Keep the connection**。

  智能卡移除配置仅在使用 RSA 智能卡的 Microsoft Windows 上适用。

为内部组策略配置服务器属性

在 Group Policy > Servers 窗口中配置 DNS 服务器、WINS 服务器和 DHCP 范围。DNS 和 WINS 服务器仅应用于全通道客户端 （IPsec、 AnyConnect、 SVC 和 L2TP/IPsec），并且用于名称解析。进行 DHCP 地址分配时会使用 DHCP 范围。

注　此处进行的更改将覆盖 **Configuration > Remote Access VPN > DNS** 窗口中 ASDM 上配置的 DNS 设置。

步骤 1　选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Servers**。

步骤 2　除非编辑的是 DefaultGroupPolicy，否则请取消选中 DNS Servers **Inherit** 复选框。

步骤 3　在 DNS Servers 字段中，添加希望该组使用的 DNS 服务器的 IPv4 或 IPv6 地址。

如果指定多个 DNS 服务器，则远程访问客户端将尝试按其在该字段中的指定顺序使用这些 DNS 服务器。

AnyConnect 3.0.4 和更高版本在 DNS Servers 字段中支持最多 25 个 DNS 服务器条目，较早发行版仅支持最多 10 个 DNS 服务器条目。

步骤 4　通过点击 More Options 栏中的双向下箭头展开 **More Options** 区域。

步骤 5　如果在 **Configuration > Remote Access VPN > DNS** 窗口中未指定默认域，则必须在 **Default Domain** 字段中指定默认域。使用域名和顶级域，例如 **example.com**。

步骤 6　点击 **OK**。

步骤 7　点击 **Apply**。

为内部组策略配置 WINS 服务器

使用此操作步骤配置主 WINS 服务器和辅助 WINS 服务器。 WINS 服务器仅应用于全通道客户端（IPsec、 AnyConnect、 SVC 和 L2TP/IPsec），并且用于名称解析。每种情况下的默认值为 none。

步骤 1　选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Servers**。

步骤 2　取消选中 WINS Servers **Inherit** 复选框。

步骤 3　在 WINS Servers 字段中，输入主 WINS 服务器和辅助 WINS 服务器的 IP 地址。指定的第一个 IP 地址是主 WINS 服务器的 IP 地址。指定的第二个 （可选） IP 地址是辅助 WINS 服务器的 IP 地址。

步骤 4　点击 **OK**。

关于为 AnyConnect 流量配置拆分隧道

拆分隧道将一些 AnyConnect 网络流量引导通过 VPN 隧道 （加密），将另一些网络流量引导位于 VPN 隧道外部 （未加密或 “无保护”）。

通过如下方式配置拆分隧道：创建拆分隧道策略，为该策略配置访问控制列表，然后将拆分隧道策略添加到组策略。当组策略发送到客户端时，该客户端将使用拆分隧道策略中的 ACL 来决定要将网络流量引导到的位置。

对于 Windows 客户端，首先评估 ASA 中的防火墙规则，然后评估客户端上的防火墙规则。对于 Mac OS X，没有使用客户端上的防火墙和过滤器规则。对于 Linux 系统，从 AnyConnect V3.1.05149 开始，可以配置 AnyConnect 以评估客户端的防火墙和过滤器规则，方法是向组配置文件中添加名为 circumvent-host-filtering 的自定义属性，然后将其设置为 true。

创建访问列表时：

- 可以在访问控制列表中同时指定 IPv4 和 IPv6 地址。
- 如果使用标准 ACL，则仅使用一个地址或网络。
- 如果使用扩展 ACL，则源网络是拆分隧道网络。目标网络会被忽略。
- 使用 any 或者使用拆分-包含/排除 0.0.0.0/0.0.0.0 或 ::/0 配置的访问列表将不会发送到客户端。要通过隧道发送所有流量，请为拆分隧道 **Policy** 选择 **Tunnel All Networks**。
- 仅当拆分隧道策略为 **Exclude Network List Below** 时，才会将地址 0.0.0.0/255.255.255.255 或 ::/128 发送到客户端。此配置指示客户端不要通过隧道传送以任意本地子网为目标的流量。
- AnyConnect 将流量传递到在拆分隧道策略中指定的所有站点**和**与 ASA 分配的 IP 地址属于同一子网的所有站点。例如，如果 ASA 分配的 IP 地址为 10.1.1.1 且掩码为 255.0.0.0，则无论拆分隧道策略如何，终端设备都会传递所有目标为 10.0.0.0/8 的流量。因此，请为正确引用预期本地子网的分配的 IP 地址使用网络掩码。

先决条件

- 必须使用适当的 ACE 创建访问列表。
- 如果已为 IPv4 网络创建一个拆分隧道策略并为 IPv6 网络创建另一个拆分隧道策略，则指定的网络列表同时用于两种协议。因此，网络列表应同时包含 IPv4 和 IPv6 流量的访问控制项 (ACE)。如果尚未创建这些 ACL，请参阅常规操作配置指南。

注　拆分隧道是流量管理功能，而不是安全功能。为实现最佳安全性，建议不要启用拆分隧道。

在以下操作步骤中，在字段旁有 Inherit 复选框的所有情况下，保持选中 Inherit 复选框意味着您配置的组策略将为该字段使用与默认组策略相同的值。取消选中 Inherit 可指定特定于组策略的新值。

为 AnyConnect 流量配置拆分隧道

步骤 1　使用 ASDM 连接到 ASA 并导航到 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**。

步骤 2　点击 **Add** 以添加新的组策略，或者选择现有组策略并点击 **Edit**。

步骤 3　选择 **Advanced > Split Tunneling**。

步骤 4　在 **DNS Names** 字段中，输入将由 AnyConnect 通过隧道解析的域名。这些名称对应于专用网络中的主机。如果配置了拆分-包含隧道，则网络列表必须包含指定的 DNS 服务器。可以在 IPv4 或 IPv6 地址字段中输入完全限定域名。

步骤 5　要禁用拆分隧道，请点击 **Yes** 以启用 **Send All DNS Lookups Through Tunnel**。此选项确保 DNS 流量不会泄漏到物理适配器；它不允许使用无保护流量。如果 DNS 解析失败，则地址保持未解析状态，并且 AnyConnect 客户端不会尝试解析 VPN 外部的地址。

要启用拆分隧道，请选择 **No**（默认）。此设置指示客户端根据拆分隧道策略通过隧道发送 DNS 查询。

步骤 6　要配置拆分隧道，请取消选中 Inherit 复选框并选择拆分隧道策略。如果不选中 Inherit，则组策略使用默认组策略 **DfltGrpPolicy** 中定义的拆分隧道设置。默认组策略中的默认拆分隧道策略设置为 Tunnel All Networks。

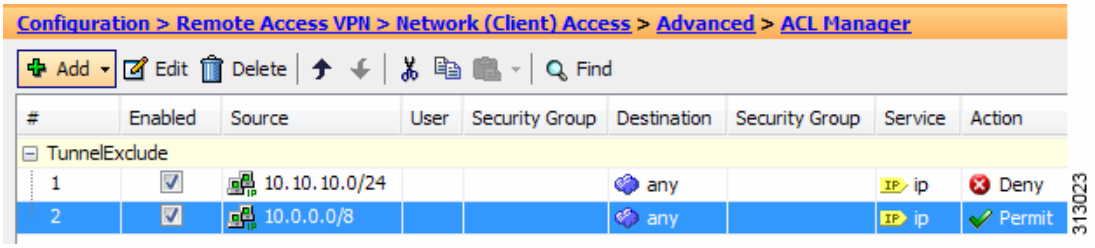
要定义拆分隧道策略，请从下拉列表 **Policy** 中选择 **IPv6 Policy**。Policy 字段定义 IPv4 网络流量的拆分隧道策略。IPv6 Policy 字段选择 IPv6 网络流量的拆分隧道策略。除该差异以外，这些字段还具有相同的用途。

通过取消选中 Inherit，可以选择以下策略选项之一：

- **Exclude Network List Below** - 定义流量在无保护情况下发送到的网络列表。此功能对于希望在其通过隧道连接到公司网络时访问其本地网络上的设备 （如打印机）的远程用户有所帮助。
- **Tunnel Network List Below** - 在 Network List 中指定的网络上通过隧道传入或传出所有流量。到包含网络列表中的地址的流量通过隧道传送。到所有其他地址的数据在无保护情况下传播，并由远程用户的互联网服务提供商进行路由。

  对于 ASA V9.1.4 和更高版本，在指定包含列表时，还可以指定排除列表，它是包含范围内的子网。这些已排除的子网将不进行隧道传送，而其余包含列表网络将进行隧道传送。客户端将忽略排除列表中的并非包含列表的子网的网络。对于 Linux，必须向组策略中添加自定义属性来支持已排除的子网。

  例如：



注　如果拆分-包含网络是本地子网的完全匹配（如 192.168.1.0/24），则对应流量通过隧道传送。如果拆分-包含网络是本地子网的超集 （如 192.168.0.0/16），则除本地子网流量以外的对应流量通过隧道传送。要另外通过隧道传送本地子网流量，必须添加匹配的拆分-包含网络（将 192.168.1.0/24 和 192.168.0.0/16 均指定为拆分-包含网络）。

如果拆分-包含网络无效（如 0.0.0.0/0.0.0.0），则会禁用拆分隧道（全部都通过隧道传送）。

- **Tunnel All Networks** - 此策略指定所有流量都通过隧道传送。这实际上会禁用拆分隧道。远程用户通过公司网络到达互联网，并且无权访问本地网络。此为默认选项。

步骤 7　在 **Network List** 字段中，选择拆分隧道策略的访问控制列表。如果选中 Inherit，则组策略使用默认组策略中指定的网络列表。

选择 **Manage** 命令按钮以打开 ACL Manager 对话框，可以在其中配置要用作网络列表的访问控制列表。有关如何创建或编辑网络列表的详细信息，请参阅常规操作配置指南。

扩展 ACL 列表可以同时包含 IPv4 和 IPv6 地址。

步骤 8　**Intercept DHCP Configuration Message from Microsoft Clients** 显示特定于 DHCP 拦截的其他参数。通过 DHCP 拦截， Microsoft XP 客户端可以将拆分隧道与 ASA 配合使用。

- Intercept - 指定是否允许发生 DHCP 拦截。如果不选中 Inherit，则默认设置为 No。
- Subnet Mask - 选择要使用的子网掩码。

步骤 9　点击 **OK**。

配置 Linux 以支持扩展子网

在为拆分隧道配置了 **Tunnel Network List Below** 时， Linux 需要额外配置以支持排除子网。必须创建名为 circumvent-host-filtering 的自定义属性，将其设置为 true，然后与为拆分隧道配置的组策略相关联。

步骤 1　连接到 ASDM，然后导航到 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes**。

步骤 2　点击 **Add**，创建名为 **circumvent-host-filtering** 的自定义属性，然后将值设置为 **true**。

步骤 3　编辑计划用于客户端防火墙的组策略，然后导航到 **Advanced > AnyConnect Client > Custom Attributes**。

步骤 4　将已创建的自定义属性 **circumvent-host-filtering** 添加到将用于拆分隧道的组策略。

使用内部组策略配置浏览器代理

Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Advanced > Browser Proxy

此对话框配置 Microsoft Internet Explorer 的属性。

浏览器代理字段

- Proxy Server Policy - 为客户端 PC 配置 Microsoft Internet Explorer 浏览器代理操作 （“方法”）。
  - Do not modify client proxy settings - 为此客户端 PC 保持 Internet Explorer 中的 HTTP 浏览器代理服务器设置不变。
  - Do not use proxy - 为此客户端 PC 禁用 Internet Explorer 中的 HTTP 代理设置。
  - Select proxy server settings from the following - 为您的选择启用以下复选框 Auto detect proxy、Use proxy server settings given below 和 Use proxy auto configuration (PAC) given below。
  - Auto detect proxy - 为此客户端 PC 启用 Internet Explorer 中的自动代理服务器检测。
  - Use proxy server settings specified below - 设置 Internet Explorer 中的 HTTP 代理服务器设置，以使用 Proxy Server Name 或 IP Address 字段中配置的值。
  - Use proxy auto configuration (PAC) given below - 指定将在 Proxy Auto Configuration (PAC) 字段中指定的文件用作自动配置属性源。
- Proxy Server Settings - 使用 Microsoft Internet Explorer 配置 Microsoft 客户端的代理服务器参数。
  - Server Address and Port - 指定为此客户端 PC 应用的 Microsoft Internet Explorer 服务器的 IP 地址或名称和端口。

  - Bypass Proxy Server for Local Addresses - 为客户端 PC 配置 Microsoft Internet Explorer 浏览器代理本地旁路设置。点击 **Yes** 以启用本地旁路，或者点击 **No** 以禁用本地旁路。
  - Exception List - 列出要从代理服务器访问中排除的服务器名称和 IP 地址。输入不希望通过代理服务器访问的地址列表。此列表与 Internet Explorer 中 “代理设置”对话框内的 “例外”列表对应。

- Proxy Auto Configuration Settings - PAC URL 指定自动配置文件的 URL。此文件告知浏览器代理信息的查找位置。要使用代理自动配置 (PAC) 功能，远程用户必须使用 Cisco AnyConnect VPN 客户端。

  许多网络环境会定义用于将网络浏览器连接到特定网络资源的 HTTP 代理。仅当在浏览器中指定了代理并且客户端将 HTTP 流量路由到代理时，HTTP 流量才可以到达网络资源。SSL VPN 隧道会将 HTTP 代理的定义复杂化，因为在通过隧道传送到企业网络时所需的代理与通过宽带连接来连接到互联网时或位于第三方网络上时所需的代理不同。

  此外，具有大型网络的公司可能需要配置多个代理服务器并让用户根据瞬态条件在其之间进行选择。通过使用 .pac 文件，管理员可以编写一个脚本文件来确定众多代理中的哪些代理将用于整个企业内的所有客户端计算机。

以下是可能会使用 PAC 文件的一些示例：

  - 从列表中随机选择代理以进行负载平衡
  - 按时刻或周时间轮换代理以适应服务器维护计划。
  - 指定在主代理发生故障的情况下将使用的备份代理服务器。
  - 根据本地子网为漫游用户指定位置最近的代理。

  可以使用文本编辑器为浏览器创建代理自动配置 (.pac) 文件。 .pac 文件是一个 JavaScript 文件，其中包含用于根据 URL 的内容来指定要使用的一个或多个代理服务器的逻辑。使用 PAC URL 字段指定要从其检索 .pac 文件的 URL。然后，浏览器使用 .pac 文件确定代理设置。

- 代理锁定
  - Allow Proxy Lockdown for Client System - 启用此功能将会在 AnyConnect VPN 会话期间隐藏 Microsoft Internet Explorer 中的 “连接”选项卡。禁用此功能将保持 “连接”选项卡的显示不变；根据用户注册表设置，可以显示或隐藏该选项卡。

在内部组策略中配置高级 AnyConnect 客户端属性

Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Advanced > AnyConnect Client 在该组策略中包含 AnyConnect 客户端的可配置属性。

- Keep Installer on Client System - 在远程计算机上启用永久客户端安装。启用此项会禁用客户端的自动卸载功能。客户端在后续连接时保持安装在远程计算机上，从而缩短远程用户的连接时间。

注　AnyConnect 客户端 V2.5 之后的版本不支持 Keep Installer on Client System。

- Datagram Transport Layer Security (DTLS) - 避免与某些 SSL 连接关联的延迟和带宽问题，并且改进对于数据包延迟敏感的实时应用的性能。
- DTLS Compression - 配置 DTLS 压缩。
- SSL Compression - 配置 SSL/TLS 压缩。
- Ignore Don’t Defrag (DF) Bit - 此功能允许强制将已设置 DF 位的数据包分片，从而使其能够通过隧道传递。示例用例适用于网络中未正确响应 TCP MSS 协商的服务器。

- Client Bypass Protocol - 客户端协议旁路配置在 ASA 仅预期 IPv6 流量时如何管理 IPv4 流量，或者在其仅预期 IPv4 流量时如何管理 IPv6 流量。

  当 AnyConnect 客户端与 ASA 进行 VPN 连接时， ASA 可能会为其分配 IPv4 和/或 IPv6 地址。Client Bypass Protocol 确定是丢弃 ASA 没有为其分配 IP 地址的流量，还是允许该流量绕过 ASA 并且未加密或 “无保护”地从客户端进行发送。

  例如，假设 ASA 仅向 AnyConnect 连接分配 IPv4 地址，并且终端进行双重堆叠。当终端尝试到达 IPv6 地址时，如果禁用 Client Bypass Protocol，则会丢弃 IPv6 流量；但是，如果启用 Client Bypass Protocol，则会从客户端安全发送 IPv6 流量。

- FQDN of This Device - 此信息供客户端在网络漫游后使用，以便解析用于重新建立 VPN 会话的 ASA IP 地址。此设置对于支持不同 IP 协议的网络之间的漫游（例如 IPv4 到 IPv6）至关重要。

  注　漫游后，无法使用 AnyConnect 配置文件中的 ASA FQDN 来派生 ASA IP 地址。地址可能与负载平衡方案中的正确设备 （与之建立隧道的设备）不匹配。

  如果未将设备 FQDN 推送到客户端，则客户端将尝试重新连接到隧道以前建立的任意 IP 地址。为支持在不同协议的网络之间漫游（从 IPv4 到 IPv6），AnyConnect 必须在漫游后对设备 FQDN 执行名称解析，以便其可以确定使用哪个 ASA 地址重新建立隧道。客户端在初始连接期间使用其配置文件中的 ASA FQDN。在后续会话重新连接期间，它在适用时始终使用由 ASA 推送（并由组策略中的管理员配置）的设备 FQDN。如果未配置 FQDN，则 ASA 从 Device Setup > Device Name/Password and Domain Name 下设置的任意内容派生设备 FQDN （并将其发送到客户端）。

  如果设备 FQDN 不是由 ASA 推送，则漫游后客户端无法在不同 IP 协议的网络之间重新建立 VPN 会话。

- MTU - 调整 SSL 连接的 MTU 大小。输入一个值（以字节为单位），介于 256 和 1410 字节之间。默认情况下， MTU 大小根据连接使用的接口的 MTU 减去 IP/UDP/DTLS 开销自动进行调整。

- Keepalive Messages - 在 Interval 字段中输入从 15 和 600 秒的数字来启用并调整保活消息的间隔，以确保通过代理、防火墙或 NAT 设备的连接保持开放，即使设备限制连接可以空闲的时间也如此。调整间隔还确保当远程用户未在积极运行基于套接字的应用 （如 Microsoft Outlook 或 Microsoft Internet Explorer）时客户端不会断开连接并重新连接。

- Optional Client Modules to Download - 为尽量缩短下载时间，AnyConnect 客户端请求仅为其支持的每个功能 （从 ASA）下载其需要的模块。必须指定启用其他功能的模块的名称。 AnyConnect 客户端 V3.0 包含以下模块 （以前版本具有较少的模块）：

  - AnyConnect DART - Diagnostic AnyConnect Reporting Tool (DART) 捕获系统日志和其他诊断信息的快照并在桌面上创建 .zip 文件，因此您可以便利地将疑难解答信息发送到 Cisco TAC。
  - AnyConnect Network Access Manager - 以前称为思科安全服务客户端，此模块提供 802.1X （第 2 层），并且将对有线和无线网络的访问的身份验证集成到 AnyConnect 3.0 中。
  - AnyConnect SBL - 登录前启动 (SBL) 强制用户在登录到 Windows 之前通过 VPN 连接来连接到企业基础设施，方法是在 Windows 登录对话框显示之前启动 AnyConnect。
  - AnyConnect Web Security Module - 以前称为 ScanSafe Hostscan，此模块集成到 AnyConnect 3.0 中。
  - AnyConnect Telemetry Module - 将有关恶意内容来源的信息发送到思科 IronPort 网络安全设备 (WSA) 的网络过滤基础设施，它使用此数据提供更好的 URL 过滤规则。

注　AnyConnect 4.0 不支持遥测。

  - AnyConnect Posture Module - 以前称为 Cisco Secure Desktop 主机扫描功能，安全状态模块集成到 AnyConnect 3.0 中，并且使 AnyConnect 可以在创建与 ASA 的远程访问连接之前收集凭证以进行安全状态评估。

- Always-On VPN - 确定是否禁用了 AnyConnect 服务配置文件中的永久在线 VPN 标志设置，或者是否应使用 AnyConnect 服务配置文件设置。通过永久在线 VPN 功能，AnyConnnect 可以在用户登录到计算机之后自动建立 VPN 会话。VPN 会话保持运行，直到用户注销计算机为止。如果物理连接丢失，会话将保持运行，并且 AnyConnect 将连续尝试与自适应安全设备重新建立物理连接以恢复 VPN 会话。

  永久在线 VPN 允许实施公司策略来保护设备免受安全威胁。可以使用它帮助确保只要终端不在受信任网络中，AnyConnect 便会建立 VPN 会话。如果启用，将会配置策略来确定在没有连接时如何管理网络连接。

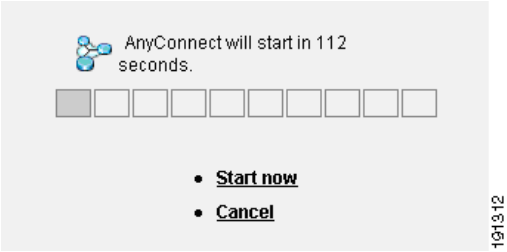
  注　永久在线 VPN 需要支持 AnyConnect 安全移动功能的发行版。有关其他信息，请参阅《*思科 AnyConnect VPN 客户端管理员指南*》。

- Client Profiles to Download - 配置文件是 AnyConnect 客户端用于配置 VPN、网络访问管理器、网络安全和遥测设置的一组配置参数。点击 Add 以启动 Select AnyConnect Client Profiles 窗口，可以在其中为该组策略指定以前创建的配置文件。

在内部组策略中配置 AnyConnect 登录设置

在内部组策略的 **Advanced > AnyConnect Client > Login Setting** 窗格中，可以启用 ASA 以提示远程用户下载 AnyConnect 客户端，或者将连接定向到无客户端 SSL VPN 门户页面。图 3-1 显示向客户端显示的提示：

图 3-1　　向远程用户显示的 AnyConnect 客户端下载提示



登录设置字段

- Post Login Setting - 选择以提示用户并设置超时以执行默认登录后选择。
- Default Post Login Selection - 选择登录后要执行的操作。

在内部组策略中配置 AnyConnect 客户端防火墙属性

在内部组策略的 **Advanced > AnyConnect Client > Client Firewall** 窗格中，可以将规则配置为向下发送至表明客户端如何影响公用和专用网络的客户端系统防火墙。

在 ASA 9.0(1) 和更高发行版中，客户端防火墙的访问控制列表同时支持 IPv4 和 IPv6 地址的访问控制项。

有关使用公用网络规则来允许客户端对本地资源进行访问的信息，请参阅第 3-26 页上的使用客户端防火墙为 VPN 启用本地设备支持。

在内部组策略中配置 AnyConnect 客户端密钥重新生成

在内部组策略的 **Advanced > AnyConnect Client > Key Regeneration** 窗格中，可以为重新生成密钥配置参数。

当 ASA 和客户端执行重新生成密钥并重新协商加密密钥和初始化向量时，将发生重新生成密钥协商，从而提高连接的安全性。

密钥重新生成字段

- Renegotiation Interval - 取消选中 **Unlimited** 复选框以指定从会话开始直到发生密钥重新生成的分钟数，介于 1 到 10080 （1 周）之间。
- Renegotiation Method - 取消选中 Inherit 复选框以指定不同于默认组策略的重新协商方法。选择 **None** 单选按钮以禁用密钥重新生成，选择 **SSL** 或 **New Tunnel** 单选按钮以在密钥重新生成期间建立新隧道。

注　将 Renegotiation Method 配置为 **SSL** 或 **New Tunnel** 指定客户端在密钥重新生成期间建立新隧道，而不是在密钥重新生成期间发生 SSL 重新协商。有关 **anyconnect ssl rekey** 命令的历史记录，请参阅命令参考。

在内部组策略中配置 AnyConnect 客户端失效对等体检测

在内部组策略的 **Advanced > AnyConnect Client > Dead Peer Detection** 窗格中，可以配置何时使用 DPD。

失效对等体检测 (DPD) 确保安全设备（网关）或客户端可以快速检测对等体不响应且连接已失败的情况。

如果在 ASA 上启用 DPD，则可以使用最佳 MTU (OMTU) 功能查找最大终端 MTU，客户端可以按该 MTU 成功传递 DTLS 数据包。通过向最大 MTU 发送填充的 DPD 数据包来实施 OMTU。如果从头端接收到负载的正确回显，则接受 MTU 大小。否则，将减小 MTU 并再次发送探测，直到达到协议允许的最小 MTU 为止。

注　使用 OMTU 不会影响现有隧道 DPD 功能。

限制

此功能不适用于 IPsec，因为 DPD 基于不允许填充的标准实施。

失效对等体检测字段

- Gateway Side Detection - 取消选中 **Disable** 复选框以指定由安全设备（网关）执行 DPD。输入从 30 到 3600 秒的间隔，安全设备按此间隔执行 DPD。
- Client Side Detection - 取消选中 **Disable** 复选框以指定由客户端执行 DPD。输入从 30 到 3600 秒的间隔，客户端按此间隔执行 DPD。

在内部组策略中定制 VPN 访问门户

在内部组策略的 **Advanced > AnyConnect Client > Customization** 窗格中，可以为组策略定制无客户端门户登录页面。

定制字段

- Portal Customization - 选择要应用于 AnyConnect 客户端/SSL VPN 门户页面的定制。可以选择预先配置的门户定制对象，或者接受默认组策略中提供的定制。默认值为 DfltCustomization。
  - Manage - 打开 Configure GUI Customization Objects 对话框，可以在其中指定要添加、编辑、删除、导入或导出定制对象。
- Homepage URL (optional) - 指定要在无客户端门户中为与组策略关联的用户显示的主页 URL。字符串必须以 http:// 或 https:// 开头。身份验证成功后，会立即将无客户端用户引向此页面。成功建立 VPN 连接时， AnyConnect 将默认网络浏览器启动到此 URL。

注　AnyConnect 目前在 Linux 平台、 Android 移动设备和 Apple iOS 移动设备上不支持此字段。如果设置了此字段，这些 AnyConnect 客户端会将其忽略。

- Use Smart Tunnel for Homepage - 创建要连接到门户的智能隧道而不是使用端口转发。
- Access Deny Message - 要创建将向为其拒绝访问的用户显示的消息，请在此字段中输入该消息。

关于内部组策略中的 AnyConnect 客户端自定义属性

内部组策略的 **Advanced > AnyConnect Client > Custom Attributes pane** 列出当前分配给此策略的自定义属性。在此对话框中，可以将先前定义的自定义属性与此策略相关联，或者定义自定义属性，然后将其与此策略相关联。

自定义属性会被发送到 AnyConnect 客户端，并由其用于配置诸如延迟升级的功能。一个自定义属性有一个类型和一个命名值。先定义属性的类型，然后可以定义此类型的一个或多个命名值。有关为某个功能配置特定自定义属性的详细信息，请参阅所用 AnyConnect 版本的 《*思科 AnyConnect 安全移动客户端管理员指南*》。

自定义属性可在 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes** 和 **AnyConnect Custom Attribute Names** 中预定义。动态访问策略和组策略都可使用预定义的自定义属性。

有关自定义属性的 DAP 使用情况的信息，请参阅第 5-22 页上的配置 DAP 访问和授权策略属性。

要为此策略配置自定义属性，请执行以下操作：

- **添加**新的自定义属性 - 选择或配置自定义属性类型，然后选择或配置命名值。下面对此操作步骤进行了描述。
- **编辑**已配置的自定义属性 - 为此属性选择其他命名值，或者省略该值。
- **删除**已配置的自定义属性 - 从此策略中移除该属性。

注　如果自定义属性还与其他组策略关联，则无法对其进行编辑或删除。

向组策略中添加自定义属性

步骤 1　转至 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Advanced > AnyConnect Client > Custom Attributes**。

步骤 2　点击 **Add** 以打开 **Create Custom Attribute** 窗格。

步骤 3　从下拉列表中选择预定义**属性类型**，或者通过执行以下操作来配置属性类型：

a. 点击 **Manage**，在 **Configure Custom Attribute Types** 窗格中，点击 **Add**。

b. 在 **Create Custom Attribute Type** 窗格中，输入新属性 **Type** 和 **Description**，两个字段均是必填项。

c. 点击 **OK** 以关闭此窗格，然后再次点击 **OK** 以选择新近定义的自定义属性类型。

步骤 4　选择 **Select Value**。

步骤 5　从 **Select value** 下拉列表中选择预定义命名值，或者通过执行以下操作来配置新的命名值：

a. 点击 **Manage**，在 Configure Custom Attributes 窗格中，点击 **Add**。

b. 在 **Create Custom Attribute Name** 窗格中，选择先前选择或配置的属性 **Type**，然后输入新属性 **Name** 和 **Value**，两个字段均是必填项。

要添加值，请点击 **Add**，输入值，然后点击 **OK**。值不能超过 420 个字符。如果值超过此长度，请为其他值内容添加多个值。配置的值在发送到 AnyConnect 客户端之前将串连。

c. 点击 **OK** 以关闭此窗格，然后再次点击 **OK** 以选择此属性的新近定义的命名值。

步骤 6　点击 **Create Custom Attribute** 窗格中的 OK。自定义属性类型和命名值将显示在列表中。

内部组策略 - IPsec (IKEv1) 客户端设置

在内部组策略中配置 IPsec (IKEv1) 客户端的常规属性

Configuration > Remote Access > Network (Client) Access > Group Policies > Advanced > IPsec (IKEv1) Client

通过 Add or Edit Group Policy > IPsec 对话框，可以为进行添加或修改的组策略指定隧道协议、过滤器、连接设置和服务器。

字段

- Re-Authentication on IKE Re-key - 除非选中 Inherit 复选框，否则在发生 IKE 重新生成密钥时启用或禁用重新身份验证。用户在 SA 到期大约两分钟且隧道终止之前有 30 秒时间来输入凭证，并且最多可以尝试输入三次。
- Allow entry of authentication credentials until SA expires - 为用户预留时间以重新输入身份验证凭证，直到达到所配置的 SA 的最大生存期为止。
- IP Compression - 除非选中 Inherit 对话框，否则启用或禁用 IP 压缩。
- Perfect Forward Secrecy - 除非选中 Inherit 复选框，否则启用或禁用完全向前保密 (PFS)。PFS 确保指定的 IPsec SA 的密钥不是派生自任何其他机密 （类似于一些其他密钥）。换句话说，如果某人要破解密钥，则 PFS 确保攻击者无法派生任何其他密钥。如果未启用 PFS，则某人理论上可以破解 IKE SA 密钥，复制所有 IPsec 受保护数据，然后使用 IKE SA 机密信息破坏此 IKE SA 设置的 IPsec SA。通过 PFS，破解 IKE 不会为攻击者提供对 IPsec 的立即访问。攻击者必须逐个破解每个 IPsec SA。
- Store Password on Client System - 启用或禁用在客户端系统上存储密码。

注　在客户端系统上存储密码可构成潜在安全风险。

- IPsec over UDP - 启用或禁用 IPsec over UDP。
- IPsec over UDP Port - 指定要用于 IPsec over UDP 的 UDP 端口。
- Tunnel Group Lock - 除非选中 Inherit 复选框或值 None，否则锁定所选隧道组。
- IPsec Backup Servers - 激活 Server Configuration 和 Server IP Addresses 字段，从而可以指定在未继承这些值的情况下要使用的 UDP 备份服务器。
  - Server Configuration - 列出要用作 IPsec 备份服务器的服务器配置选项。可用的选项包括：Keep Client Configuration（默认）、Use the Backup Servers Below 和 Clear Client Configuration。
  - Server Addresses (space delimited) - 指定 IPsec 备份服务器的 IP 地址。仅当 Server Configuration 选项的值为 Use the Backup Servers Below 时，此字段才可用。

关于内部组策略中的 IPsec (IKEv1) 客户端访问规则

通过此对话框中的 Client Access Rules 表，可以查看最多 25 条客户端访问规则。添加客户端访问规则时，请配置以下字段：

- Priority - 为此规则选择优先级。
- Action - 根据此规则允许或拒绝访问。
- VPN Client Type - 指定此规则应用到的 VPN 设备的类型（软件或硬件），并且对于软件客户端，以自由格式文本形式指定所有 Windows 客户端或其子集。
- VPN Client Version - 指定此规则应用到的 VPN 客户端的一个或多个版本。此列包含适合于此客户端的软件或固件映像的逗号分隔列表。条目是自由形式文本，***** 与任何版本都匹配。

客户端访问规则定义

- 如果不定义任何规则， ASA 将允许所有连接类型。但是，用户可能仍然会继承默认组策略中存在的任何规则。
- 当客户端与所有规则都不匹配时， ASA 会拒绝连接。如果定义拒绝规则，则还必须定义至少一个允许规则；否则， ASA 将拒绝所有连接。
- * 字符是通配符，可以在每个规则中多次输入。
- 整个规则集的限制为 255 个字符。
- 对于不发送客户端类型和/或版本的客户端，可以输入 **n/a**。

在内部组策略中为 IPsec (IKEv1) 客户端配置客户端防火墙

通过 Add or Edit Group Policy Client Firewall 对话框，可以为进行添加或修改的组策略配置 VPN 客户端防火墙设置。只有运行 Microsoft Windows 的 VPN 客户端才能使用这些防火墙功能。它们当前对于硬件客户端或其他 （非 Windows）软件客户端不可用。

通过 VPN 客户端连接到 ASA 的远程用户可以选择相应的防火墙选项。

在第一个方案中，远程用户在 PC 上安装有个人防火墙。 VPN 客户端实施在本地防火墙上定义的防火墙策略，并监控该防火墙以确保其正在运行。如果防火墙停止运行，则 VPN 客户端将断开与 ASA 的连接。（此防火墙实施机制被称为 *Are You There (AYT)*，因为 VPN 客户端通过向防火墙发送定期“are you there?”消息来对其进行监控；如果没有应答，则 VPN 客户端知道防火墙关闭并会终止其与 ASA 的连接。）网络管理员原先可能会配置这些 PC 防火墙，但通过此方法，每个用户可以定制其自己的配置。

在第二个方案中，您可能首选为 VPN 客户端 PC 上的个人防火墙实施集中式防火墙策略。常见的示例是使用拆分隧道阻止到组中远程 PC 的互联网流量。此方法在建立了隧道的情况下保护 PC 并因此保护中心站点免遭来自互联网的入侵。此防火墙方案称为*推送策略*或*中心保护策略 (CPP)*。在 ASA 中，可以创建要在 VPN 客户端上实施的流量管理规则集，将这些规则与过滤器相关联，并将该过滤器指定为防火墙策略。ASA 将此策略向下推送到 VPN 客户端。然后， VPN 客户端又反过来将策略传递到本地防火墙，由其实施此策略。

Configuration > Remote Access > Network (Client) Access > Group Policies > Advanced > IPsec (IKEv1) Client > Client Firewall 选项卡

字段

- Inherit - 确定组策略是否从默认组策略获取其客户端防火墙设置。此选项为默认设置。设置后，它会覆盖此对话框中的剩余属性来使其名称变暗。
- Client Firewall Attributes - 指定客户端防火墙属性，包括实施的防火墙 （如果有）的类型和该防火墙的防火墙策略。
- Firewall Setting - 列明防火墙是否存在，如果存在，它是必需还是可选。如果选择 No Firewall（默认），则此对话框中无任何剩余字段处于活动状态。如果希望该组中的用户受防火墙保护，请选择 Firewall Required 或 Firewall Optional 设置。

  如果选择 Firewall Required，则该组中的所有用户都必须使用指定防火墙。ASA 会丢弃在未安装并运行指定的受支持防火墙情况下尝试进行连接的任何会话。在此情况下，ASA 通知 VPN 客户端其防火墙配置不匹配。

注　如果对于组需要防火墙，请确保该组不包含除 Windows VPN 客户端以外的任何客户端。该组中的所有其他客户端 （包括处于客户端模式的 ASA 5505 和 VPN 3002 硬件客户端）都无法连接。

  如果该组中包含尚未有防火墙容量的远程用户，请选择 Firewall Optional。Firewall Optional 设置允许组中的所有用户进行连接。具有防火墙的用户可以使用该设置；进行连接而没有防火墙的用户会接收到警告消息。如果创建的组中的其中一些用户具有防火墙支持而其他用户没有，则此设置有用。例如，您可能具有一个处于逐渐过渡状态的组，其中某些成员已设置防火墙容量，而其他成员尚未执行此操作。

- Firewall Type - 列出来自多个供应商的防火墙，包括思科。如果选择 Custom Firewall，则 Custom Firewall 下的字段会激活。指定的防火墙必须与可用的防火墙策略关联。配置的特定防火墙确定哪些防火墙策略选项受支持。
- Custom Firewall - 指定自定义防火墙的供应商 ID、产品 ID 和描述。
  - Vendor ID - 指定该组策略的自定义防火墙的供应商。
  - Product ID - 指定为该组策略配置的自定义防火墙的产品或型号名称。
  - Description - （可选）描述自定义防火墙。
- Firewall Policy - 指定自定义防火墙策略的类型和源。
  - Policy defined by remote firewall (AYT) - 指定防火墙策略由远程防火墙 (Are You There) 定义。远程防火墙 (AYT) 定义的策略意味着该组中的远程用户在其 PC 上有防火墙。本地防火墙在 VPN 客户端上实施防火墙策略。仅当该组中的 VPN 客户端已安装并运行指定的防火墙时，ASA 才允许其进行连接。如果指定防火墙未在运行，则连接失败。一旦建立连接， VPN 客户端便会每 30 秒轮询一次防火墙，以确保其仍然运行。如果防火墙停止运行，VPN 客户端将结束会话。

- Policy pushed (CPP) - 指定从对等体推送策略。如果选择此选项， Inbound Traffic Policy 和 Outbound Traffic Policy 列表及 Manage 按钮会激活。 ASA 在该组中的 VPN 客户端上实施通过从 Policy Pushed (CPP) 下拉列表中选择的过滤器定义的流量管理规则。菜单上可用的选项即是此 ASA 中定义的过滤器，包括默认过滤器。请注意， ASA 会将这些规则向下推送到 VPN 客户端，因此，应相对于 VPN 客户端而不是 ASA 创建和定义这些规则。例如 “in” 和 “out” 分别是指进入 VPN 客户端或从 VPN 客户端出站的流量。如果 VPN 客户端也具有本地防火墙，则从 ASA 推送的策略可与本地防火墙的策略配合使用。将丢弃任一防火墙的规则阻止的任何数据包。
- Inbound Traffic Policy - 列出入站流量的可用推送策略。
- Outbound Traffic Policy - 列出出站流量的可用推送策略。
- Manage - 显示 ACL Manager 对话框，可以在其中配置访问控制列表 (ACL)。

在内部组策略中配置 IPsec (IKEv1) 的硬件客户端属性

注　VPN 3002 硬件客户端已停产并终止支持。有关配置此客户端的信息，请参阅 ASA 9.2 文档。

为本地用户配置 VPN 策略属性

步骤 1　启动 ASDM 并选择 **Configuration > Remote Access VPN > AAA/Local Users > Local Users**。

步骤 2　选择要配置的用户，然后点击 **Edit**。

系统将显示 Edit User Account 对话框。

步骤 3　在左侧窗格中，点击 **VPN Policy**。

步骤 4　为该用户指定一个组策略。用户策略将继承该组策略的属性。如果有其他字段设置为从 Default Group Policy 继承配置，则该组策略中指定的属性将优先于 Default Group Policy 中设置的属性。

步骤 5　指定可供用户使用的隧道协议，或是否从组策略继承值。选中所需的 **Tunneling Protocols** 复选框，以选择要可供使用的 VPN 隧道协议。选项如下：

- Clientless SSL VPN （通过 SSL/TLS 连接的 VPN），使用网络浏览器建立到 VPN 集中器的安全远程访问隧道；此选项无需软件和硬件客户端。无客户端 SSL VPN 可以提供从几乎任何可通过 HTTPS 到达安全互联网站点的计算机到范围广泛的企业资源的轻松访问，包括企业网站、启用网络功能的应用、启用网络功能的 NT/AD 文件共享、邮件和其他基于 TCP 的应用。
- SSL VPN Client，通过它可在下载 Cisco AnyConnect 客户端应用后进行连接。这是首次使用无客户端 SSL VPN 连接来下载此应用。然后，只要进行连接，便会根据需要自动进行客户端更新。
- IPsec IKEv1 - IP 安全协议。 IPsec 被视为最安全的协议，为 VPN 隧道提供最完整的架构。站点间 （对等）连接和思科 VPN 客户端到 LAN 连接均可使用 IPsec IKEv1。
- IPsec IKEv2 - 由 AnyConnect 安全移动客户端提供支持。将 IPsec 与 IKEv2 配合使用的 AnyConnect 连接提供高级功能，如软件更新、客户端配置文件、GUI 本地化（转换）和定制、Cisco Secure Desktop 和 SCEP 代理。
- 采用互联网协议安全的第二层隧道协议允许具有若干公共 PC 和移动 PC 操作系统的随附的 VPN 客户端远程用户通过公用 IP 网络与 ASA 和专用企业网络建立安全连接。

步骤 6　指定要使用的过滤器 （IPv4 或 IPv6），或者是否从组策略继承值。过滤器由规则组成，这些规则根据诸如源地址、目标地址和协议之类的条件来确定允许还是拒绝隧道数据包通过 ASA。要配置过滤器和规则，请选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > General > More Options > Filter**。

点击 **Manage** 以显示 ACL Manager 窗格，可以在其中添加、编辑及删除 ACL 和 ACE。

步骤 7　指定继承连接配置文件 （隧道组）锁定还是使用所选隧道组锁定 （如果有）。选择特定锁定会限定用户只能通过此组进行远程访问。隧道组锁定通过查看 VPN 客户端中配置的组是否与用户分配的组相同来限制用户。如果不相同，ASA 将阻止用户进行连接。如果未选中 Inherit 复选框，则默认值为 None。

步骤 8　指定是否从该组继承 Store Password on Client System 设置。取消选中 **Inherit** 复选框以激活 Yes 和 No 单选按钮。点击 **Yes** 以将登录密码存储在客户端系统上 （该选项可能不太安全）。点击 **No**（默认）以要求用户输入每个连接的密码。为确保最高安全性，我们建议您*不允许*密码存储。

步骤 9　指定要应用于此用户的访问时长策略，为用户创建新的访问时长策略，或者保持选中 Inherit 框。默认值为 Inherit，或者，如果未选中 Inherit 复选框，则默认值为 Unrestricted。

点击 **Manage** 以打开 Add Time Range 对话框，可以在其中指定一组新的访问时长。

步骤 10　指定用户执行的同时登录数。同时登录设置指定对此用户允许的最大同时登录数。默认值为 3。最小值为 0，表示禁止登录并阻止用户访问。

注　在没有最大限制时，允许多个同时连接可能会降低安全性并影响性能。

步骤 11　为用户连接时间指定最大连接时间 （以分钟为单位）。此时间结束时，系统会终止连接。最小值为 1 分钟，最大值为 2147483647 分钟 （4000 多年）。要允许无限连接时间，请选中 **Unlimited** 复选框（默认）。

步骤 12　指定用户的空闲超时 （以分钟为单位）。如果在此期间，用户在连接上没有通信活动，系统会终止连接。最短时间为 1 分钟，最长时间为 10080 分钟。该值不适用于无客户端 SSL VPN 连接的用户。

步骤 13　配置会话警报间隔。如果取消选中 Inherit 复选框，则会自动选中 Default 复选框，并将会话警报间隔设置为 30 分钟。如果您要指定新值，可以取消选中 **Default** 复选框，并在分钟框中指定 1 至 30 分钟的会话警报间隔。

步骤 14　配置空闲警报间隔。如果您取消选中 Inherit 复选框，系统将自动选中 Default 复选框。这会将空闲警报间隔设置为 30 分钟。如果您要指定新值，可以取消选中 **Default** 复选框，并在分钟框中指定 1 至 30 分钟的会话警报间隔。

步骤 15　要为此用户设置专用 IPv4 地址，请在 Dedicated IPv4 Address (Optional) 区域中输入 IPv4 地址和子网掩码。

步骤 16　要为此用户设置专用 IPv6 地址，请在 Dedicated IPv6 Address (Optional) 区域中输入一个带 IPv6 前缀的 IPv6 地址。 IPv6 前缀表示 IPv6 地址所驻留的子网。

步骤 17　点击 **OK**。

更改会保存到运行配置。

配置无客户端 SSL VPN 内部组策略

在内部组策略中配置无客户端 SSL VPN 常规属性

Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add/Edit > Add or Edit Internal Group Policy > General

通过 Add or Edit Group Policy 对话框，可以为进行添加或修改的组策略指定隧道协议、过滤器、连接设置和服务器。对于此对话框中的每个字段，选中 Inherit 复选框可使对应的设置从默认组策略中获取其值。 Inherit 是此对话框中所有属性的默认值。

字段

以下属性显示在 Add Internal Group Policy > General 对话框中。

- Name - 指定该组策略的名称 （最多 64 个字符）；允许空格。对于 Edit 功能，此字段为只读。
- Banner - 指定登录时要向用户显示的条幅文本。长度最多可以为 491 个字符。没有默认值。

  无客户端门户和 AnyConnect 客户端支持部分 HTML。要确保向远程用户正确显示条幅，请遵循以下准则：

  – 对于无客户端用户，请使用
 标记。
- Tunneling Protocols - 指定该组可以使用的隧道协议。用户只能使用所选协议。选项如下：

  – Clientless SSL VPN - 指定通过 SSL/TLS 来使用 VPN，该 VPN 使用网络浏览器建立到 ASA 的安全远程访问隧道；无需软件和硬件客户端。无客户端 SSL VPN 可以提供从几乎任何可到达 HTTPS 互联网站点的计算机到范围广泛的企业资源的轻松访问，包括企业网站、启用网络功能的应用、 NT/AD 文件共享 （启用网络功能）、邮件和其他基于 TCP 的应用。

  – SSL VPN Client - 指定使用 Cisco AnyConnect VPN 客户端或传统 SSL VPN 客户端。如果使用的是 AnyConnect 客户端，必须选择此协议以支持 MUS。

  – IPsec IKEv1 - IP 安全协议。IPsec 被视为最安全的协议，为 VPN 隧道提供最完整的架构。站点间 （对等）连接和思科 VPN 客户端到 LAN 连接均可使用 IPsec IKEv1。

  – IPsec IKEv2 - 由 AnyConnect 安全移动客户端提供支持。将 IPsec 与 IKEv2 配合使用的 AnyConnect 连接提供高级功能，如软件更新、客户端配置文件、 GUI 本地化 （转换）和定制、 Cisco Secure Desktop 和 SCEP 代理。

  – L2TP over IPsec - 允许具有若干公共 PC 随附的 VPN 客户端和移动 PC 操作系统的远程用户通过公用 IP 网络建立到安全设备和专用企业网络的安全连接。L2TP 使用 PPP over UDP（端口 1701）来通过隧道传送数据。必须为 IPsec 传输模式配置安全设备。
- Web ACL - （仅适用于无客户端 SSL VPN）如果要过滤流量，请从下拉列表中选择访问控制列表 (ACL)。如果要在进行选择之前查看、修改、添加或移除 ACL，请点击列表旁的 Manage。
- Access Hours - 选择应用到此用户的现有访问时长策略 （如果有）的名称，或者创建新访问时长策略。默认值为 Inherit，或者，如果未选中 Inherit 复选框，则默认值为 --Unrestricted--。点击列表旁的 Manage 以查看或添加时间范围对象。
- Simultaneous Logins - 指定此用户允许的最大同时登录数。默认值为 3。最小值为 0，表示禁止登录并阻止用户访问。

  注　在没有最大限制时，允许多个同时连接可能会降低安全性并影响性能。

- Restrict Access to VLAN - （可选）也称为 “VLAN 映射”，此参数指定该组策略应用到的会话的出口 VLAN 接口。ASA 将该组中的所有流量都转发到所选 VLAN。使用此属性向组策略分配 VLAN 以简化访问控制。向此属性赋值是在会话中使用 ACL 过滤流量的替代方法。除默认值 (Unrestricted) 外，下拉列表仅显示此 ASA 中配置的 VLAN。

注　此功能适用于 HTTP 连接，但不适用于 FTP 和 CIFS。

- Connection Profile (Tunnel Group) Lock - 此参数仅允许通过所选连接配置文件 （隧道组）进行远程 VPN 访问，并会阻止通过其他连接配置文件进行访问。默认继承值为 None。
- Maximum Connect Time - 如果未选中 Inherit 复选框，则此参数指定最大用户连接时间 （以分钟为单位）。此时间结束时，系统会终止连接。最小值为 1 分钟，最大值为 35791394 分钟 （4000 多年）。要允许无限连接时间，请选中 Unlimited （默认）。

- Idle Timeout - 如果未选中 Inherit 复选框，则此参数指定该用户的空闲超时时间段 （以分钟为单位）。如果在此时间段内用户连接上没有通信活动，则系统会终止连接。最短时间为 1 分钟，最长时间为 10080 分钟。默认值为 30 分钟。要允许无限连接时间，请选中 **Unlimited**。该值不适用于无客户端 SSL VPN 用户。
- Session Alert Interval - 如果取消选中 Inherit 复选框，则会自动选中 Default 复选框。这将会话警报间隔设置为 30 分钟。如果您要指定新值，可以取消选中 Default 复选框，并在分钟框中指定 1 至 30 分钟的会话警报间隔。
- Idle Alert Interval - 如果取消选中 Inherit 复选框，则会自动选中 Default 复选框。这会将空闲警报间隔设置为 30 分钟。如果您要指定新值，可以取消选中 Default 复选框，并在分钟框中指定 1 至 30 分钟的会话警报间隔。

在内部组策略中配置无客户端 SSL VPN 访问门户

门户属性确定在门户页面上为建立无客户端 SSL VPN 连接的该组策略成员显示的内容。在此窗格中，可以启用书签列表和 URL 输入、文件服务器访问、端口转发和智能隧道、ActiveX 中继及 HTTP 设置。

字段

- Bookmark List - 选择以前配置的书签列表，或者点击 **Manage** 以创建新书签列表。书签显示为链接，用户可以通过它们从门户页面进行导航。
- URL Entry - 启用以允许远程用户将 URL 直接输入到门户 URL 字段中。
- File Access Control - 控制通用互联网文件系统 (CIFS) 文件的 “隐藏共享”的可见性。隐藏共享通过共享名称末尾的美元符号 ($) 进行标识。例如，驱动器 C 共享为 C$。在使用隐藏共享的情况下，不会显示共享文件夹，并会限制用户浏览或访问这些隐藏资源。
  - File Server Entry - 启用以允许远程用户输入文件服务器的名称。
  - File Server Browsing - 启用以允许远程用户浏览可用文件服务器。
  - Hidden Share Access - 启用以隐藏共享文件夹。
- Port Forwarding Control - 通过 Java Applet 为用户提供借助无客户端 SSL VPN 连接对基于 TCP 的应用的访问。
  - Port Forwarding List - 选择要与该组策略关联的以前配置的列表 TCP 应用。点击 **Manage** 以创建新列表或编辑现有列表。
  - Auto Applet Download - 支持在用户首次登录时自动安装并启动 Applet。
  - Applet Name - 将 Applet 对话框标题栏的名称更改为指定的名称。默认情况下，名称为 Application Access。
- Smart Tunnel - 使用无客户端 （基于浏览器） SSL VPN 会话以 ASA 作为通道并以安全设备作为代理服务器来指定智能隧道选项：
  - Smart Tunnel Policy - 从网络列表中选择并指定其中一个隧道选项：use smart tunnel for the specified network、 do not use smart tunnel for the specified network 或 use tunnel for all network traffic。向组策略或用户名分配智能隧道网络将为其会话与该组策略或用户名相关联的所有用户启用智能隧道访问，但会将智能隧道访问限用于列表中指定的应用。要查看、添加、修改或删除智能隧道列表，请点击 **Manage**。
  - Smart Tunnel Application - 从下拉列表中选择以将终端站上安装的基于 TCP 的 Winsock 2 应用连接到内部网上的服务器。要查看、添加、修改或删除智能隧道应用，请点击 **Manage**。
  - Smart Tunnel all Applications - 选中此复选框以通过隧道传送所有应用。所有应用都通过隧道传送，而无需从网络列表中进行选择或者知道最终用户可能会为外部应用调用哪些可执行文件。

  - Auto Start - 选中此复选框以在用户登录时自动启动智能隧道访问。用于在用户登录时启动智能隧道访问的此选项仅适用于 Windows。取消选中此复选框可在用户登录时启用智能隧道访问，但要求用户使用无客户端 SSL VPN 门户页面上的 Application Access > Start Smart Tunnels 按钮手动将其启动。
  - Auto Sign-on Server List - 如果要在用户与服务器建立智能隧道连接时重新发出用户凭证，请从下拉列表中选择列表名称。每个智能隧道自动登录列表条目标识一个用于自动提交用户凭证的服务器。要查看、添加、修改或删除智能隧道自动登录列表，请点击 **Manage**。
  - Windows Domain Name (Optional) - 如果身份验证需要通用命名约定 （域\用户名），请指定 Windows 域以在自动登录期间将其添加到用户名中。例如，在对用户名 qu_team 进行身份验证时，请输入 CISCO 以指定 CISCO\qa_team。配置自动登录服务器列表中的关联条目时，还必须选中 “Use Windows domain name with user name”选项。

- ActiveX Relay - 无客户端用户可通过它从浏览器启动 Microsoft Office 应用。应用使用会话来下载和上载 Microsoft Office 文档。 ActiveX 中继一直有效，直到无客户端 SSL VPN 会话关闭。

更多选项：

- HTTP Proxy - 启用或禁用将 HTTP applet 代理转发到客户端。对于使用适当内容转换进行介入的技术 （如 Java、 ActiveX 和 Flash），代理十分有用。它会绕过破坏，同时确保安全设备的持续使用。转发的代理自动修改旧浏览器代理配置并将所有 HTTP 和 HTTPS 请求重定向到新代理配置。它支持几乎所有客户端技术，包括 HTML、CSS、JavaScript、VBScript、ActiveX 和 Java。它唯一支持的浏览器是 Microsoft Internet Explorer。
- Auto Start (HTTP Proxy) - 选中以在用户登录时自动启用 HTTP 代理。取消选中将在用户登录时启用智能隧道访问，但是要求用户手动将其启动。
- HTTP Compression - 通过无客户端 SSL VPN 会话启用 HTTP 数据压缩。

为无客户端 SSL VPN 内部组策略配置门户定制

要为组策略配置定制，请选择预先配置的门户定制对象，或者接受默认组策略中提供的定制。还可以配置要显示的 URL。

为无客户端 SSL VPN 访问连接定制访问门户的操作步骤与为网络客户端访问连接定制访问门户的操作步骤相同。请参阅第 3-17 页上的在内部组策略中定制 VPN 访问门户。

为无客户端 SSL VPN 内部组策略配置登录设置

在此对话框中，可以启用 ASA 以提示远程用户下载 AnyConnect 客户端或转至无客户端 SSL VPN 门户页面。请参阅第 3-15 页上的在内部组策略中配置 AnyConnect 登录设置。

为无客户端 SSL VPN 访问内部组策略配置单点登录和自动登录服务器

要配置单点登录服务器和自动登录服务器，请参阅第 15 章，“无客户端 SSL VPN 用户”。。

配置站点到站点内部组策略

Configuration > Site-to-Site VPN > Group Policies

站点到站点 VPN 连接的组策略指定隧道协议、过滤器和连接设置。对于此对话框中的每一个字段，如果选中 Inherit 复选框，则相应的设置将从默认组策略获取其值。 Inherit 是此对话框中所有属性的默认值。

字段

以下属性显示在 Add Internal Group Policy > General 对话框中。它们适用于 SSL VPN 和 IPsec 会话或无客户端 SSL VPN 会话。因此，若干属性对于一种类型的会话存在，但对于另一种类型的会话则不存在。

- Name - 指定该组策略的名称。对于 Edit 功能，此字段为只读。
- Tunneling Protocols - 指定该组允许的隧道协议。用户只能使用所选协议。选项如下：
  - Clientless SSL VPN - 指定通过 SSL/TLS 来使用 VPN，该 VPN 使用网络浏览器建立到 ASA 的安全远程访问隧道；无需软件和硬件客户端。无客户端 SSL VPN 可以提供从几乎任何可到达 HTTPS 互联网站点的计算机到范围广泛的企业资源的轻松访问，包括企业网站、启用网络功能的应用、 NT/AD 文件共享 （启用网络功能）、邮件和其他基于 TCP 的应用。
  - SSL VPN Client - 指定使用 Cisco AnyConnect VPN 客户端或传统 SSL VPN 客户端。如果使用的是 AnyConnect 客户端，必须选择此协议以支持 MUS。
  - IPsec IKEv1 - IP 安全协议。IPsec 被视为最安全的协议，为 VPN 隧道提供最完整的架构。站点间 （对等）连接和思科 VPN 客户端到 LAN 连接均可使用 IPsec IKEv1。
  - IPsec IKEv2 - 由 AnyConnect 安全移动客户端提供支持。将 IPsec 与 IKEv2 配合使用的 AnyConnect 连接提供高级功能，如软件更新、客户端配置文件、 GUI 本地化 （转换）和定制、 Cisco Secure Desktop 和 SCEP 代理。
  - L2TP over IPsec - 允许具有若干公共 PC 随附的 VPN 客户端和移动 PC 操作系统的远程用户通过公用 IP 网络建立到安全设备和专用企业网络的安全连接。L2TP 使用 PPP over UDP（端口 1701）来通过隧道传送数据。必须为 IPsec 传输模式配置安全设备。
- Filter -（仅适用于网络（客户端）访问）指定要使用的访问控制列表或者是否从组策略继承值。过滤器由规则组成，这些规则根据诸如源地址、目标地址和协议之类的条件来确定允许还是拒绝隧道数据包通过 ASA。要配置过滤器和规则，请参阅 Group Policy 对话框。点击 Manage 以打开 ACL Manager，可以在其中查看和配置 ACL。
- Idle Timeout - 如果未选中 Inherit 复选框，则此参数指定该用户的空闲超时时间段 （以分钟为单位）。如果在此时间段内用户连接上没有通信活动，则系统会终止连接。最短时间为 1 分钟，最长时间为 10080 分钟。默认值为 30 分钟。要允许无限连接时间，请选中 **Unlimited**。该值不适用于无客户端 SSL VPN 用户。
- Maximum Connect Time - 如果未选中 Inherit 复选框，则此参数指定最大用户连接时间 （以分钟为单位）。此时间结束时，系统会终止连接。最小值为 1 分钟，最大值为 35791394 分钟 （4000 多年）。要允许无限连接时间，请选中 Unlimited （默认）。

使用客户端防火墙为 VPN 启用本地设备支持

当远程用户连接到 ASA 时，所有流量都通过 VPN 连接以隧道传送，因此用户无法访问其本地网络上的资源。这包括打印机、摄像头和与本地计算机同步的 Windows Mobile 设备 （受限设备）。在客户端配置文件中启用 Local LAN Access 可解决此问题，但由于对本地网络的访问不受限制，因此这可能造成某些企业对安全或策略的担忧。可以配置 ASA 来部署用于将访问限用于特定类型的本地资源 （如打印机和受限设备）的终端操作系统防火墙规则。

为此，请为用于打印的特定端口启用客户端防火墙规则。客户端区分入站和出站规则。为获取打印功能，客户端会打开出站连接所需的端口，但是阻止所有传入流量。

注　请注意，以管理员身份登录的用户能够修改由 ASA 部署到客户端的防火墙规则。具有有限特权的用户无法修改规则。对于任一用户，当连接终止时，客户端会重新应用防火墙规则。

如果配置客户端防火墙，并且用户向 Active Directory (AD) 服务器进行身份验证，则客户端仍然从 ASA 应用防火墙策略。但是，在 AD 组策略中定义的规则优先于客户端防火墙的规则。

以下各节描述有关如何执行此操作的操作步骤：

- 第 3-27 页上的为本地打印机支持部署客户端防火墙
- 第 3-29 页上的为 VPN 配置受限设备支持

有关防火墙行为的使用说明

以下说明阐释 AnyConnect 客户端如何使用防火墙：

- 没有为防火墙规则使用源 IP。客户端会忽略从 ASA 发送的防火墙规则中的源 IP 信息。客户端根据规则是公共还是专用来确定源 IP。公共规则应用于客户端上的所有接口。专用规则应用于虚拟适配器。
- ASA 支持 ACL 规则的许多协议。但是， AnyConnect 防火墙功能仅支持 TCP、 UDP、 ICMP 和 IP。如果客户端接收到具有其他协议的规则，则会将其视为无效防火墙规则，然后出于安全原因禁用拆分隧道并使用完整隧道。
- 在 ASA 9.0 中开始，公用网络规则和专用网络规则支持统一访问控制列表。这些访问控制列表可用于在同一规则中定义 IPv4 和 IPv6 流量。

请注意各操作系统的行为方面的以下差异：

- 对于 Windows 计算机，在 Windows 防火墙中拒绝规则优先于允许规则。如果 ASA 将允许规则向下推送到 AnyConnect 客户端，但是用户已创建自定义拒绝规则，则不会实施 AnyConnect 规则。
- 在 Windows Vista 上，创建防火墙规则后，Vista 采用逗号分隔的字符串形式的端口号范围。端口范围最多可以是 300 个端口。例如，从 1 到 300 或从 5000 到 5300。如果指定大于 300 个端口的范围，则防火墙规则仅应用于前 300 个端口。
- 其防火墙服务必须由 AnyConnect 客户端启动（不是由系统自动启动）的 Windows 用户建立 VPN 连接所需的时间可能会明显增加。
- 在 Mac 计算机上， AnyConnect 客户端按照 ASA 应用规则的顺序依次应用这些规则。全局规则应该始终最后应用。
- 对于第三方防火墙，仅当 AnyConnect 客户端防火墙和第三方防火墙均允许该流量类型时，才会传递流量。如果第三方防火墙阻止 AnyConnect 客户端允许的特定流量类型，则客户端将阻止该流量。

为本地打印机支持部署客户端防火墙

ASA 通过 ASA V8.3(1) 或更高版本以及 ASDM V6.3(1) 或更高版本来支持 AnyConnect 客户端防火墙功能。本节描述在 VPN 连接失败时如何配置客户端防火墙以允许访问本地打印机，以及如何配置客户端配置文件以使用防火墙。

客户端防火墙的局限和限制

以下局限和限制适用于使用客户端防火墙限制本地 LAN 访问：

- 由于操作系统的限制，仅对入站流量实施运行 Windows XP 的计算机上的客户端防火墙策略。将忽略出站规则和双向规则。这将包括诸如 “permit ip any any” 之类的防火墙规则。
- 主机扫描和某些第三方防火墙可能会干扰防火墙。

下表阐释受源和目标端口设置影响的流量方向：

源端口	目标端口	受影响的流量方向
特定端口号	特定端口号	入站和出站
范围或 “All” （值为 0）	范围或 “All” （值为 0）	入站和出站
特定端口号	范围或 “All” （值为 0）	仅入站
范围或 “All” （值为 0）	特定端口号	仅出站

适用于本地打印的示例 ACL 规则

ACL AnyConnect_Client_Local_Print 随附于 ASDM，用于轻松配置客户端防火墙。为组策略的 Client Firewall 窗格中的 Public Network Rule 选择该 ACL 时，该列表包含以下 ACE：

。

表 3-1　　AnyConnect_Client_Local_Print 中的 ACL 规则

说明	权限	接口	协议	源端口	目标地址	目标端口
全部拒绝	拒绝	公用	任意	默认	任意	默认
LPD	允许	公用	TCP	默认	任意	515
IPP	允许	公用	TCP	默认	任意	631
打印机	允许	公用	TCP	默认	任意	9100
mDNS	允许	公用	UDP	默认	224.0.0.251	5353
LLMNR	允许	公用	UDP	默认	224.0.0.252	5355
NetBios	允许	公用	TCP	默认	任意	137
NetBios	允许	公用	UDP	默认	任意	137

注　默认端口范围是 1 到 65535。

注　要启用本地打印，必须在已定义 ACL 规则 *allow Any Any* 的客户端配置文件中启用 **Local LAN Access** 功能。

为 VPN 配置本地打印支持

要使最终用户能够打印到其本地打印机，请在组策略中创建标准 ACL。ASA 将该 ACL 发送到 VPN 客户端，然后 VPN 客户端修改客户端的防火墙配置。

步骤 1　在组策略中启用 AnyConnect 客户端防火墙。转至 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**。

步骤 2　选择组策略，然后点击 **Edit**。系统将显示 Edit Internal Group Policy 窗口。

步骤 3　选择 **Advanced > AnyConnect Client > Client Firewall**。为 Private Network Rule 点击 **Manage**。

步骤 4　创建包含表 3-1中描述的 ACE 的 ACL。将此 ACL 添加为专用网络规则。

步骤 5　如果已启用 Automatic VPN Policy always-on 并指定已关闭的策略，则在 VPN 发生故障的情况下，用户无权访问本地资源。可以通过转至**配置文件编辑器中的 Preferences (Cont)** 并选中 **Apply last local VPN resource rules** 在此场景中应用防火墙规则。

为 VPN 配置受限设备支持

要支持受限设备并保护企业网络，请在组策略中创建标准 ACL，从而指定受限设备使用的范围内的目标地址。然后，将拆分隧道的 ACL 指定为要从通过隧道传递的 VPN 流量中排除的网络列表。您还必须配置客户端配置文件，以在 VPN 发生故障的情况下使用最后的 VPN 本地资源规则。

注　对于需要与运行 AnyConnect 的计算机同步的 Windows Mobile 设备，请将 IPv4 目标地址指定为 169.254.0.0，或者在 ACL 中指定 IPv6 目标地址 fe80::/64。

步骤 1　在 ASDM 中，转至 **Group Policy > Advanced > Split Tunneling**。

步骤 2　取消选中 Network List 字段旁的 **Inherit**，然后点击 **Manage**。系统将显示 ACL Manager。

步骤 3　点击 **Extended ACL** 复选框。

步骤 4　点击 **Add**，然后点击 **Add ACL**。指定新 ACL 的名称。

步骤 5　选择表中的新 ACL 并点击 **Add**，然后点击 **Add ACE**。系统将显示 Edit ACE 窗口。

步骤 6　对于 Action，选择 **Permit** 单选按钮。

步骤 7　在目标条件字段中，将 IPv4 目标地址指定为 169.254.0.0 或将 IPv6 目标地址指定为 fe80::/64。

步骤 8　对于 Service，选择 *IP*。

步骤 9　点击 **OK**。

步骤 10　点击 OK 以保存 ACL。

步骤 11　在内部组策略的 Split Tunneling 窗格中，根据在步骤 7 中指定的 IP 地址为 Policy 或 IPv6 Policy 取消选中 Inherit，然后选择 **Exclude Network List Below**。对于 Network List，选择已创建的 ACL。

步骤 12　点击 **OK**。

步骤 13　点击 **Apply**。

配置 AnyConnect VPN 客户端连接

Internal Group Policy > Advanced > AnyConnect Client

AnyConnect 客户端字段

- Keep Installer on Client System - 启用以在远程计算机上允许永久客户端安装。启用此项会禁用客户端的自动卸载功能。客户端在后续连接时保持安装在远程计算机上，从而缩短远程用户的连接时间。
- Compression - 压缩通过减小进行传输的数据包的大小来提高安全设备与客户端之间的通信性能。
- Datagram TLS - 数据报传输层安全可避免与某些 SSL 连接关联的延迟和带宽问题，并且改进对于数据包延迟敏感的实时应用的性能。
- Ignore Don't Defrag (DF) Bit - 此功能允许强制将已设置 DF 位的数据包分片，从而使其能够通过隧道传递。示例用例适用于网络中未正确响应 TCP MSS 协商的服务器。
- Client Bypass Protocol - 通过客户端协议旁路功能，可以配置在 ASA 仅预期 IPv6 流量时如何管理 IPv4 流量，或者在其仅预期 IPv4 流量时如何管理 IPv6 流量。

  当 AnyConnect 客户端与 ASA 进行 VPN 连接时，ASA 可能会为其分配 IPv4 和/或 IPv6 地址。如果 ASA 为 AnyConnect 连接仅分配 IPv4 地址或仅分配 IPv6 地址，此时可以配置 Client Bypass Protocol 以丢弃 ASA 没有为其分配 IP 地址的网络流量，或者允许该流量绕过 ASA 并且未加密或“无保护”地从客户端进行发送。

  例如，假设 ASA 仅向 AnyConnect 连接分配 IPv4 地址，并且终端进行双重堆叠。当终端尝试到达 IPv6 地址时，如果禁用 Client Bypass Protocol，则会丢弃 IPv6 流量；但是，如果启用 Client Bypass Protocol，则会从客户端安全发送 IPv6 流量。
- FQDN of This Device - 此信息供客户端在网络漫游后使用，以便解析用于重新建立 VPN 会话的 ASA IP 地址。此设置对于支持不同 IP 协议的网络之间的漫游（例如 IPv4 到 IPv6）至关重要。

  注　漫游后，无法使用 AnyConnect 配置文件中的 ASA FQDN 来派生 ASA IP 地址。地址可能与负载平衡方案中的正确设备 （与之建立隧道的设备）不匹配。

  如果未将设备 FQDN 推送到客户端，则客户端将尝试重新连接到隧道以前建立的任意 IP 地址。为支持在不同协议的网络之间漫游（从 IPv4 到 IPv6），AnyConnect 必须在漫游后对设备 FQDN 执行名称解析，以便其可以确定使用哪个 ASA 地址重新建立隧道。客户端在初始连接期间使用其配置文件中的 ASA FQDN。在后续会话重新连接期间，它在适用时始终使用由 ASA 推送（并由组策略中的管理员配置）的设备 FQDN。如果未配置 FQDN，则 ASA 从 Device Setup > Device Name/Password and Domain Name 下设置的任意内容派生设备 FQDN （并将其发送到客户端）。

  如果设备 FQDN 不是由 ASA 推送，则漫游后客户端无法在不同 IP 协议的网络之间重新建立 VPN 会话。
- MTU - 调整 SSL 连接的 MTU 大小。输入一个值（以字节为单位），介于 256 和 1410 字节之间。默认情况下， MTU 大小根据连接使用的接口的 MTU 减去 IP/UDP/DTLS 开销自动进行调整。
- Keepalive Messages - 在 Interval 字段中输入从 15 和 600 秒的数字来启用并调整保活消息的间隔，以确保通过代理、防火墙或 NAT 设备的连接保持开放，即使设备限制连接可以空闲的时间也如此。调整间隔还确保当远程用户未在积极运行基于套接字的应用 （如 Microsoft Outlook 或 Microsoft Internet Explorer）时客户端不会断开连接并重新连接。

- **Optional Client Modules to Download** - 为尽量缩短下载时间，AnyConnect 客户端请求仅为其支持的每个功能下载其需要的模块（从 ASA）。必须指定启用其他功能的模块的名称。AnyConnect 客户端 V3.0 包含以下模块 （以前版本具有较少的模块）：
  - AnyConnect DART - Diagnostic AnyConnect Reporting Tool (DART) 捕获系统日志和其他诊断信息的快照并在桌面上创建 .zip 文件，因此您可以便利地将疑难解答信息发送到 Cisco TAC。
  - AnyConnect Network Access Manager - 以前称为思科安全服务客户端，此模块提供 802.1X（第 2 层），并且将对有线和无线网络的访问的身份验证集成到 AnyConnect 3.0 中。
  - AnyConnect SBL - 登录前启动 (SBL) 强制用户在登录到 Windows 之前通过 VPN 连接来连接到企业基础设施，方法是在 Windows 登录对话框显示之前启动 AnyConnect。
  - AnyConnect Web Security Module - 以前称为 ScanSafe Hostscan，此模块集成到 AnyConnect 3.0 中。
  - AnyConnect Telemetry Module - 将有关恶意内容来源的信息发送到思科 IronPort 网络安全设备 (WSA) 的网络过滤基础设施，它使用此数据提供更好的 URL 过滤规则。

注　自 AnyConnect V4.0 起不支持 Telemetry 模块。

  - AnyConnect Posture Module - 以前称为 Cisco Secure Desktop 主机扫描功能，安全状态模块集成到 AnyConnect 3.0 中，并且使 AnyConnect 可以在创建与 ASA 的远程访问连接之前收集凭证以进行安全状态评估。
- Always-On VPN - 确定是否禁用了 AnyConnect 服务配置文件中的永久在线 VPN 标志设置，或者是否应使用 AnyConnect 服务配置文件设置。通过永久在线 VPN 功能，AnyConnnect 可以在用户登录到计算机之后自动建立 VPN 会话。VPN 会话保持运行，直到用户注销计算机为止。如果物理连接丢失，会话将保持运行，并且 AnyConnect 将连续尝试与自适应安全设备重新建立物理连接以恢复 VPN 会话。

  永久在线 VPN 允许实施公司策略来保护设备免受安全威胁。可以使用它帮助确保只要终端不在受信任网络中，AnyConnect 便会建立 VPN 会话。如果启用，将会配置策略来确定在没有连接时如何管理网络连接。

注　永久在线 VPN 需要支持 AnyConnect 安全移动功能的发行版。有关其他信息，请参阅《*思科 AnyConnect VPN 客户端管理员指南*》。

- Client Profiles to Download - 配置文件是 AnyConnect 客户端用于配置 VPN、网络访问管理器、网络安全和遥测设置的一组配置参数。点击 Add 以启动 Select Anyconnect Client Profiles 窗口，可以在其中为该组策略指定先前创建的配置文件。

配置 AnyConnect 客户端配置文件

您可以配置 ASA 来为所有 AnyConnect 用户全局部署 AnyConnect 客户端配置文件，或者根据用户的组策略向其部署客户端配置文件。通常，用户对于安装的每个 AnyConnect 模块都有一个客户端配置文件。在某些情况下，可能要为用户提供多个配置文件。从多个位置工作的人员可能需要多个配置文件。请注意，某些配置文件设置 （如 SBL）在全局级别控制连接体验。其他设置对于特定主机唯一并且取决于所选主机。

有关创建和部署 AnyConnect 客户端配置文件及控制客户端功能的详细信息，请参阅 《*AnyConnect VPN 客户端管理员指南*》。

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile

AnyConnect 客户端配置文件中的字段

Add - 显示 Add AnyConnect Client Profiles 对话框，可以在其中将闪存中的文件指定为配置文件，或者浏览闪存以查找要指定为配置文件的文件。您还可以将文件从本地计算机上载到闪存。

Edit - 显示 Edit SSL VPN Client Profile 窗口，可以在其中更改 AnyConnect 客户端功能配置文件中包含的设置。

Delete - 从表中删除配置文件。这不会从闪存中删除 XML 文件。

AnyConnect Client Profiles Table - 显示指定为 AnyConnect 客户端配置文件的 XML 文件：

- **Profile Name** - 添加配置文件时指定的配置文件的名称。
- **Profile Usage/Type** - 显示此配置文件的用法 （如 VPN、网络访问管理器或遥测）。

向组策略中 AnyConnect 客户端配置文件

有关创建和部署 AnyConnect 客户端配置文件及控制客户端功能的详细信息，请参阅 《*AnyConnect VPN 客户端管理员指南*》。

字段

- **Profile Name -** 指定该组策略的 AnyConnect 客户端配置文件。
- **Profile Usage** - 显示最初创建配置文件时向其分配的用法：VPN、网络访问管理器、网络安全或遥测。如果 ASDM 无法识别 XML 文件中指定的用法，则下拉列表变为可选，然后可以手动选择用法类型。
- **Profile Location** - 指定 ASA 闪存中配置文件的路径。如果文件不存在，ASA 将根据配置文件模板创建该文件。

向内部组策略中导入 AnyConnect 客户端配置文件

您可以从本地设备或远程服务器导入配置文件。

有关创建和部署 AnyConnect 客户端配置文件及控制客户端功能的详细信息，请参阅 《*AnyConnect VPN 客户端管理员指南*》。

字段

- **Profile Name** - 指定添加的配置文件的名称。
- **Profile Usage** - 显示最初创建配置文件时向其分配的用法：VPN、网络访问管理器、网络安全或遥测。如果 ASDM 无法识别 XML 文件中指定的用法，则下拉列表变为可选，然后可以手动选择用法类型。
- **Group Policy** - 指定此配置文件的组策略。配置文件随 AnyConnect 客户端一起下载到属于该组策略的用户。
- **Profile Location** - 指定 ASA 闪存中配置文件的路径。如果文件不存在，ASA 将根据配置文件模板创建该文件。

导出 AnyConnect 客户端配置文件

从此窗口导出 AnyConnect VPN 客户端配置文件。可以导出到本地设备或远程服务器。

有关创建和部署 AnyConnect 客户端配置文件及控制客户端功能的详细信息，请参阅 《*AnyConnect VPN 客户端管理员指南*》。

字段

Device Profile Path - 显示配置文件的路径和文件名。

Local Path - 指定用于导出配置文件的路径和文件名。

Browse Local - 点击启动用于浏览本地设备文件系统的窗口。

免除 AnyConnect 流量执行网络地址转换

如果已配置 ASA 执行网络地址转换 (NAT)，必须免除远程访问 AnyConnect 客户端流量进行转换，以便 DMZ 上的 AnyConnect 客户端、内部网络和企业资源可以相互发起网络连接。免除转换 AnyConnect 客户端流量失败将阻止 AnyConnect 客户端和其他企业资源进行通信。

通过 “身份 NAT”（也称为 “NAT 免除”），可以将地址转换为其自身，从而有效绕过 NAT。身份 NAT 可以应用在两个地址池之间、地址池与子网之间或两个子网之间。

此操作步骤说明在示例网络拓扑中将会如何在这些假定网络对象之间配置身份 NAT：Engineering VPN 地址池、 Sales VPN 地址池、内部网络、 DMZ 网络和互联网。每个身份 NAT 配置都需要一条 NAT 规则。

表 3-2　　用于为 VPN 客户端配置身份 NAT 的网络寻址

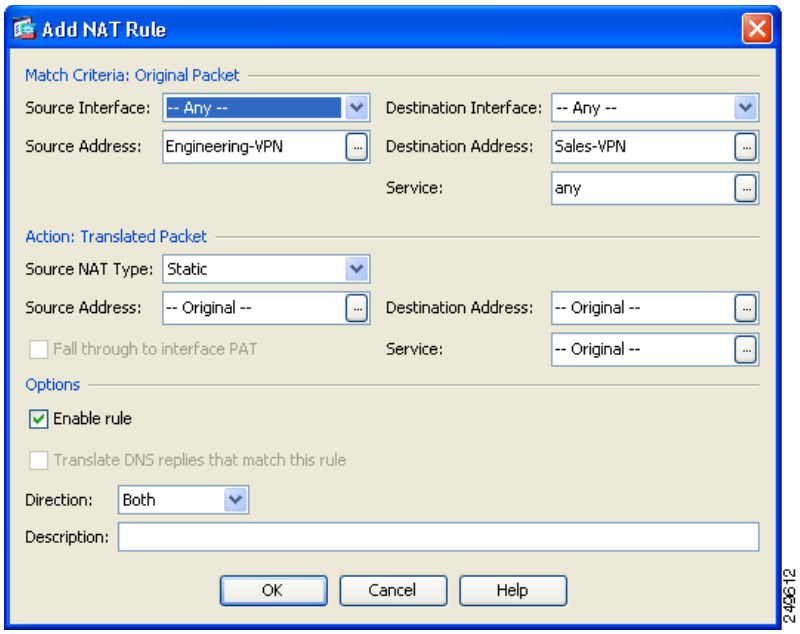
网络或地址池	网络或地址池名称	地址范围
内部网络	inside-network	10.50.50.0 - 10.50.50.255
工程 VPN 地址池	Engineering-VPN	10.60.60.1 - 10.60.60.254
销售 VPN 地址池	Sales-VPN	10.70.70.1 - 10.70.70.254
DMZ 网络	DMZ-network	192.168.1.0 - 192.168.1.255

步骤 1　登录 ASDM 并导航到 **Configuration > Firewall > NAT Rules**。

步骤 2　创建 NAT 规则，以便 Engineering VPN 地址池中的主机可以到达 Sales VPN 地址池中的主机。在 NAT Rules 窗格中，导航到 **Add > Add NAT Rule Before “Network Object” NAT rules**，以便 ASA 在统一 NAT 表中的其他规则之前评估此规则。

注　NAT 规则评估按照自顶向下、最先匹配的基础来应用。一旦 ASA 将数据包与特定 NAT 规则相匹配，它便不执行任何进一步评估。请务必将最具体的 NAT 规则置于统一 NAT 表的顶部，以便 ASA 不会过早地将其与更广泛的 NAT 规则相匹配。

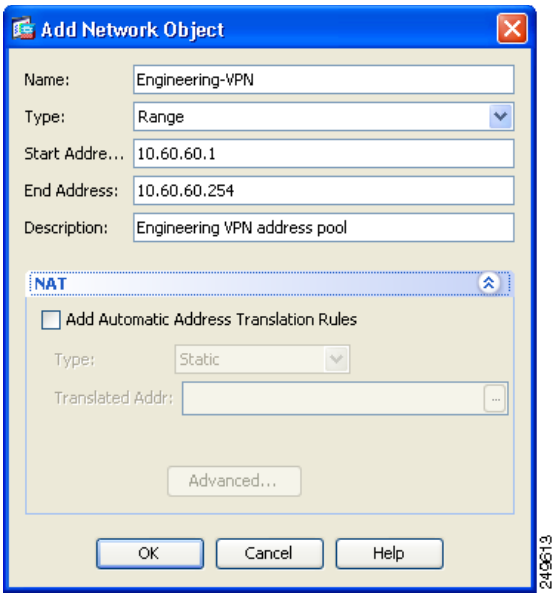
图 3-2　　Add NAT Rule 对话框



a. 在 **Match Criteria: Original Packet** 区域中，配置以下字段：

- Source Interface：Any
- Destination Interface：Any
- Source Address：点击 Source Address 浏览按钮并创建表示 Engineering VPN 地址池的网络对象。将对象类型定义为地址的**范围**。请勿添加自动地址转换规则。有关示例，请参阅图 3-3。
- Destination Address：点击 Destination Address 浏览按钮并创建表示 Sales VPN 地址池的网络对象。将对象类型定义为地址的**范围**。请勿添加自动地址转换规则。

图 3-3　　为 VPN 地址池创建网络对象



b. 在 **Action Translated Packet** 区域中，配置以下字段：
   - Source NAT Type：Static
   - Source Address：Original
   - Destination Address：Original
   - Service：Original

c. 在 **Options** 区域中，配置以下字段：
   - 选中 **Enable rule**。
   - 取消选中 **Translate DNS replies that match this rule** 或将其留空。
   - Direction：Both
   - Description：Add a Description for this rule。

d. 点击 **OK**。

e. 点击 **Apply**。您的规则应类似于第 3-38 页上的图 3-5 中统一 NAT 表内的规则 1。

   CLI 示例：

```
nat source static Engineering-VPN Engineering-VPN destination static Sales-VPN Sales-VPN
```

f. 点击 **Send**。

步骤 3　当 ASA 执行 NAT 时，为使同一个 VPN 池中的两台主机相互连接，或者使这些主机通过 VPN 隧道到达互联网，必须启用 **Enable traffic between two or more hosts connected to the same interface** 选项。为此，请在 ASDM 中选择 **Configuration > Device Setup > Interfaces**。在 Interface 面板的底部，选中 **Enable traffic between two or more hosts connected to the same interface** 并点击 **Apply**。

CLI 示例：

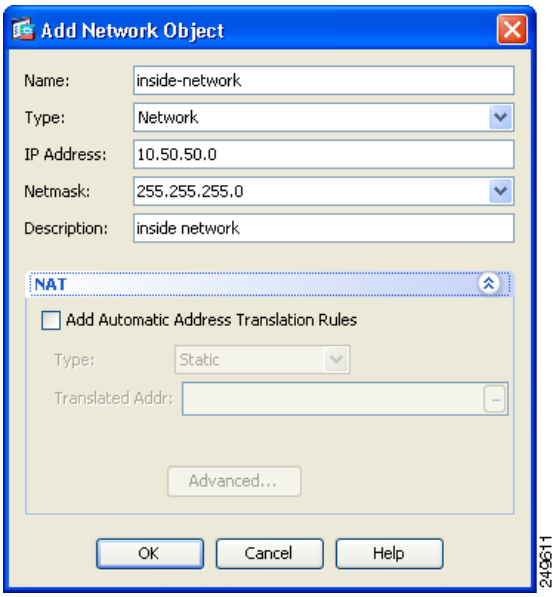
```
same-security-traffic permit inter-interface
```

步骤 4　创建 NAT 规则，以便 Engineering VPN 地址池中的主机可以到达 Engineering VPN 地址池中的其他主机。创建此规则就如同在步骤 2 中创建规则一样，不同在于在 **Match Criteria: Original Packet** 区域中将 Engineering VPN 地址池同时指定为 Source Address 和 Destination Address。

步骤 5　创建 NAT 规则，以便 Engineering VPN 远程访问客户端可以到达 “内部” 网络。在 NAT Rules 窗格中，选择 **Add > Add NAT Rule Before “Network Object” NAT rules**，以便将在其他规则之前处理此规则。

a. 在 **Match Criteria: Original Packet** 区域中，配置以下字段：
   - Source Interface：Any
   - Destination Interface：Any
   - Source Address：点击 Source Address 浏览按钮并创建表示内部网络的网络对象。将对象类型定义为地址的**网络**。请勿添加自动地址转换规则。
   - Destination Address：点击 Destination Address 浏览按钮并选择表示 Engineering VPN 地址池的网络对象。

图 3-4　添加 inside-network 对象



b. 在 **Action: Translated Packet** 区域中，配置以下字段：
   - Source NAT Type：Static
   - Source Address：Original
   - Destination Address：Original
   - Service：Original

c. 在 **Options** 区域中，配置以下字段：
   - 选中 **Enable rule**。
   - 取消选中 **Translate DNS replies that match this rule** 或将其留空。
   - Direction：Both
   - Description：Add a Description for this rule。

d. 点击 **OK**。

e. 点击 **Apply**。您的规则应类似于第 3-38 页上的图 3-5 中统一 NAT 表内的规则 2。

CLI 示例

```
nat source static inside-network inside-network destination static Engineering-VPN
Engineering-VPN
```

步骤 6　按照步骤 5 中的方法创建新规则，以配置 Engineering VPN 地址池和 DMZ 网络之间的连接的身份 NAT。使用 DMZ 网络作为 Source Address 并使用 Engineering VPN 地址池作为 Destination Address。

步骤 7　创建新 NAT 规则，以允许 Engineering VPN 地址池通过隧道访问互联网。在此情况下，您不希望使用身份 NAT，因为要将源地址从专用地址更改为互联网可路由地址。要创建此规则，请遵循以下操作步骤：

a. 在 NAT Rules 窗格中，选择 **Add > Add NAT Rule Before "Network Object" NAT rules**，以便将在其他规则之前处理此规则。

b. 在 **Match Criteria: Original Packet** 区域中，配置以下字段：

   - Source Interface：Any
   - Destination Interface：Any。在 **Action: Translated Packet** 区域中选择 outside 作为 Source Address 时，将使用 "outside" 自动填充此字段。
   - Source Address：点击 Source Address 浏览按钮并选择表示 Engineering VPN 地址池的网络对象。
   - Destination Address：Any。

c. 在 **Action: Translated Packet** 区域中，配置以下字段：

   - Source NAT Type：Dynamic PAT (Hide)
   - Source Address：点击 Source Address 浏览按钮并选择 **outside** 接口。
   - Destination Address：Original
   - Service：Original

d. 在 **Options** 区域中，配置以下字段：

   - 选中 **Enable rule**。
   - 取消选中 **Translate DNS replies that match this rule** 或将其留空。
   - Direction：Both
   - Description：Add a Description for this rule。

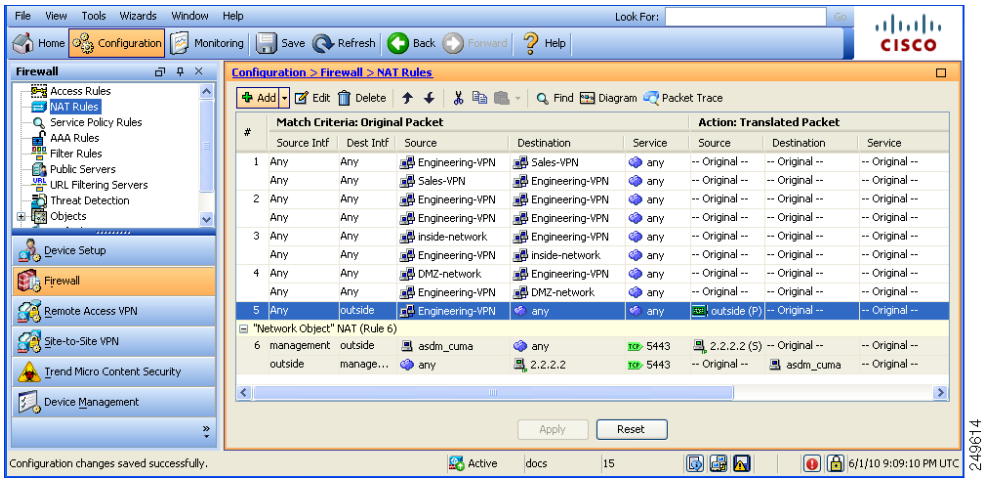
e. 点击 **OK**。

f. 点击 **Apply**。您的规则应类似于第 3-38 页上的图 3-5 中统一 NAT 表内的规则 5。

   CLI 示例：

   nat (any,outside) source dynamic Engineering-VPN interface

图 3-5　　统一 NAT 表



步骤 8　将 Engineering VPN 地址池配置为到达其自身、 Sales VPN 地址池、内部网络、 DMZ 网络和互联网后，必须为 Sales VPN 地址池重复此过程。使用身份 NAT 免除 Sales VPN 地址池流量在其自身，内部网络、 DMZ 网络和互联网之间执行网络地址转换。

步骤 9　从 ASA 上的 **File** 菜单中，选择 **Save Running Configuration to Flash** 以实施身份 NAT 规则。

关于连接配置文件

连接配置文件（也称为隧道组）配置 VPN 连接的连接属性。这些属性应用于 Cisco AnyConnect VPN 客户端、无客户端 SSL VPN 连接以及 IKEv1 和 IKEv2 第三方 VPN 客户端。

AnyConnect 连接配置文件 - 主窗格

在主窗格中，可以在所选接口上启用客户端访问，并且可以选择、添加、编辑和删除连接配置文件（隧道组）。您还可以指定是否要允许用户在登录时选择特定连接。

字段

- Access Interfaces - 可从表中选择要启用访问的接口。此表中的字段包括接口名称和指定是否允许访问的复选框。
  - 在 Interface 表内为 AnyConnect 连接配置的接口所对应的行中，选中要在接口上启用的协议。可以允许 SSL 访问和/或 IPsec 访问。

    选中 SSL 时，默认情况下会启用 DTLS（数据报传输层安全）。DTLS 可避免与某些 SSL 连接关联的延迟和带宽问题，并且改进对于数据包延迟敏感的实时应用的性能。

    选中 IPsec (IKEv2) 访问时，默认情况下会启用客户端服务。客户端服务包含增强的 Anyconnect 功能，包括软件更新、客户端配置文件、 GUI 本地化 （转换）和定制、 Cisco Secure Desktop 及 SCEP 代理。如果禁用客户端服务，AnyConnect 客户端仍然会与 IKEv2 建立基本 IPsec 连接。
  - Device Certificate - 可以为 RSA 密钥或 ECDSA 密钥指定用于身份验证的证书。请参阅第 3-39 页上的指定设备证书。

  - Port Setting - 配置 HTTPS 和 DTLS （仅适用于 RA 客户端）连接的端口号。请参阅第 3-40 页上的在连接配置文件中配置端口设置。
  - Bypass interface access lists for inbound VPN sessions - 默认情况下会选中 Enable inbound VPN sessions to bypass interface ACLs。安全设备允许所有 VPN 流量通过接口 ACL。例如，即使外部接口 ACL 不允许已解密流量通过，安全设备仍然信任远程专用网络并允许已解密数据包通过。可以更改此默认行为。如果希望接口 ACL 检查 VPN 受保护流量，请取消选中此框。
- 登录页面设置
  - 允许用户在登录页面上选择通过其别名进行标识的连接配置文件。如果不选中此复选框，则默认连接配置文件为 DefaultWebVPNGroup。
  - Shutdown portal login page - 显示禁用登录时的网页。
- Connection Profiles - 为连接 （隧道组）配置特定于协议的属性。
  - Add/Edit - 点击以添加或编辑连接配置文件 （隧道组）。
  - Name - 连接配置文件的名称。
  - Aliases - 用于标识连接配置文件的其他名称。
  - SSL VPN Client Protocol - 指定 SSL VPN 客户端是否具有访问权。
  - Group Policy - 显示此连接配置文件的默认组策略。
  - Allow user to choose connection, identified by alias in the table above, at login page - 选中以支持在登录页面上显示连接配置文件 （隧道组）别名。
- Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile matches the certificate map will be used - 此选项在连接配置文件选择过程中指定组 URL 和证书值的相对首选项。如果 ASA 与首选值匹配失败，它将选择与其他值匹配的连接配置文件。仅当依靠许多旧 ASA 软件发行版使用的首选项将 VPN 终端所指定的组 URL 与指定同一个组 URL 的连接配置文件相匹配时，才选中此选项。默认情况下，未选中此选项。如果未选中此选项，则 ASA 首选将连接配置文件中指定的证书字段值与供终端用于分配连接配置文件的证书的字段值相匹配。

指定设备证书

通过 **Specify Device Certificate** 屏幕，可以指定在客户端尝试创建连接时将向其标识 ASA 的证书。此屏幕用于 AnyConnect 连接配置文件和无客户端连接配置文件。

远程访问 VPN 限制

- 某些 AnyConnect 功能 （如永久在线 IPsec/IKEv2）要求有效并受信任的证书在 ASA 上可用。
- 如果 AnyConnect 客户端配置为仅使用 SSL，则只需指定 RSA 证书，因为 AnyConnect 对于 SSL VPN 不支持 ECDSA 证书。如果 AnyConnect 客户端配置为使用 IPsec 和/或 SSL，则可以同时配置两种证书。
- ECDSA 证书仅在 IPsec 连接上受支持。

步骤 1　（仅适用于 VPN 连接）在 Certificate with RSA Key 区域中，执行以下任务之一：

- 如果要选择一个证书以对使用任一协议的客户端进行身份验证，请保持选中 **Use the same device certificate for SSL and IPsec IKEv2** 框。可以从列表框中可用的证书选择证书，或者点击 **Manage** 以创建要使用的身份证书。
- 取消选中 **Use the same device certificate for SSL and IPsec IKEv2** 复选框来为 SSL 连接或 IPsec 连接指定不同的证书。

步骤 2　从 Device Certificate 列表框中选择证书。

如果未显示所需的证书，请点击 **Manage** 按钮以管理 ASA 上的身份证书。

步骤 3　（仅适用于 VPN 连接）在 Certificate with ECDSA key 字段中，从列表框中选择 ECDSA 证书，或者点击 **Manage** 以创建 ECDSA 身份证书。

步骤 4　点击 **OK**。

在连接配置文件中配置端口设置

在连接配置文件窗格中的以下位置配置 SSL 和 DTLS 连接的端口号 （仅适用于远程访问）：

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles

字段

- HTTPS Port - 要为 HTTPS （基于浏览器） SSL 连接启用的端口。范围为 1-65535。默认值为端口 443。
- DTLS Port - 要为 DTLS 连接启用的 UDP 端口。范围为 1-65535。默认值为端口 443。

AnyConnect 连接配置文件 - 基本属性

要设置 AnyConnect VPN 连接的基本属性，请在 Anyconnect Connection Profiles 部分中选择 Add 或 Edit。系统将打开 Add （或 Edit） AnyConnect Connection Profile > Basic 对话框。

字段

在 Add AnyConnect Connection Profile > Basic 对话框中设置属性，如下所示：

- Name - 对于 Add，指定进行添加的连接配置文件的名称。对于 Edit，此字段不可编辑。
- Aliases - （可选）输入连接的一个或多个替代名称。可以使用空格或标点符号分隔名称。
- Authentication - 选择要用于对连接进行身份验证的以下方法之一，并指定要在身份验证中使用的 AAA 服务器组。
  - AAA, Certificate, or Both - 选择要使用的身份验证类型：AAA 和 / 或 Certificate。如果选择 Certificate 或 Both，用户必须提供证书以进行连接。
  - AAA Server Group - 从下拉列表中选择 AAA 服务器组。默认设置为 LOCAL，它指定由 ASA 处理身份验证。在进行选择之前，可以点击 **Manage** 以在此对话框上叠加打开一个对话框来查看 AAA 服务器组的 ASA 配置或对其进行更改。
  - 选择除 LOCAL 以外的其他内容将使 Use LOCAL if Server Group Fails 复选框可供使用。
  - Use LOCAL if Server Group fails - 选中以在 Authentication Server Group 属性指定的组失败的情况下启用 LOCAL 数据库。
- Client Address Assignment - 选择要使用的 DHCP 服务器、无客户端地址池和客户端 IPv6 地址池。
  - DHCP Servers - 输入要使用的 DHCP 服务器的名称或 IP 地址。
  - Client Address Pools - 输入要用于客户端地址分配的 IPv4 地址的可用已配置池的池名称。在进行选择之前，可以点击 **Select** 以在此对话框上叠加打开一个对话框来查看地址池或对其进行更改。有关添加或编辑 IPv4 地址池的详细信息，请参阅第 4-3 页上的配置本地 IP 地址池。

  - Client IPv6 Address Pools - 输入要用于客户端地址分配的 IPv6 地址的可用已配置池的池名称。在进行选择之前，可以点击 **Select** 以在此对话框上叠加打开一个对话框来查看地址池或对其进行更改。有关添加或编辑 IPv6 地址池的详细信息，请参阅第 4-3 页上的配置本地 IP 地址池。

- Default Group Policy - 选择要使用的组策略。
  - Group Policy - 选择要分配作为此连接的默认组策略的 VPN 组策略。VPN 组策略是可以在设备上内部存储或在 RADIUS 服务器上外部存储的面向用户的属性 - 值对的集合。默认值为 DfltGrpPolicy。可以点击 **Manage** 以在此对话框上叠加打开一个对话框来对组策略配置进行更改。
  - Enable SSL VPN client protocol - 选中以为此 VPN 连接启用 SSL。
  - Enable IPsec (IKEv2) client protocol - 选中以为此连接启用使用 IKEv2 的 IPsec。
  - DNS Servers - 为此策略输入 DNS 服务器的一个或多个 IP 地址。
  - WINS Servers - 为此策略输入 WINS 服务器的一个或多个 IP 地址。
  - Domain Name - 输入默认域名。
- Find - 输入要用作搜索字符串的 GUI 标签或 CLI 命令，然后点击 Next 或 Previous 以开始搜索。

AnyConnect 连接配置文件 - 高级属性

通过 Advanced 菜单项及其对话框，可以配置此连接的以下特性：

- 常规属性
- 客户端寻址属性
- 身份验证属性
- 授权属性
- 记帐属性
- 名称服务器属性
- 无客户端 SSL VPN 属性

注　SSL VPN 和辅助身份验证属性仅适用于 SSL VPN 连接配置文件。

AnyConnect 连接配置文件 - 通用属性

字段

- Enable Simple Certificate Enrollment (SCEP) for this Connection Profile
- Strip the realm from username before passing it on to the AAA server
- Strip the group from username before passing it on to the AAA server
- Group Delimiter

密码管理

- Enable Password Management - 通过它可以配置与覆盖来自 AAA 服务器的帐户已禁用指示和通知用户密码到期相关的参数。

  注　允许覆盖帐户已禁用指示是一项潜在安全风险。

  - Notify user __ days prior to password expiration - 指定 ASDM 必须在用户登录时通知其距离密码到期的具体天数。默认是在密码到期前 14 天通知用户，并且此后每天通知，直到用户更改密码为止。范围是 1 到 180 天。
  - Notify user on the day password expires - 仅在密码到期当天通知用户。

    并且在任一情况下，如果密码到期而未更改， ASA 将为用户提供机会来更改密码。如果当前密码未到期，用户仍可使用该密码登录。

  注　这不会更改距离密码到期的天数，而是会启用通知。如果选择此选项，还必须指定天数。

  - Override account-disabled indication from AAA server - 覆盖来自 AAA 服务器的帐户已禁用指示。
- Translate Assigned IP Address to Public IP Address - 在少数情况下，可能要在内部网络上使用 VPN 对等体的真实 IP 地址而不是分配的本地 IP 地址。通常在使用 VPN 的情况下，会给定对等体分配的本地 IP 地址来访问内部网络。但是，在例如内部服务器和网络安全基于对等体的真实 IP 地址的情况下，可能要将本地 IP 地址重新转换为对等体的真实公有 IP 地址。可以在每个隧道组一个接口的基础上启用此功能。
  - Enable the address translation on interface - 启用地址转换并允许选择地址显示在的接口。*outside* 是 AnyConnect 客户端连接到的接口， *inside* 是特定于新隧道组的接口。

  注　由于路由问题和其他限制，除非您知道需要此功能，否则不建议使用此功能。

- Find - 输入要用作搜索字符串的 GUI 标签或 CLI 命令，然后点击 Next 或 Previous 以开始搜索。

在连接配置文件中配置客户端寻址

连接配置文件上的 Client Addressing 窗格分配特定接口上的 IP 地址池来与此连接配置文件配合使用。 Client Addressing 窗格对于所有客户端连接配置文件都通用，并且可从以下 ASDM 路径获取：

- Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles
- Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles
- Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv2) Connection Profiles

此处配置的地址池也可以在连接配置文件的 Basic 窗格上进行配置。

AnyConnect 连接配置文件可以分配 IPv6 以及 IPv4 地址池。

要配置客户端寻址，请打开远程访问客户端连接配置文件 （AnyConnect、 IKEv1 或 IKEv2），然后选择 **Advanced > Client Addressing**。

- 要查看或更改地址池的配置，请点击对话框中的 **Add** 或 **Edit**。系统将打开 Assign Address Pools to Interface 对话框。通过此对话框，可以将 IP 地址池分配到 ASA 上配置的接口。点击 **Select**。系统将打开 Select Address Pools 对话框。使用此对话框查看地址池的配置。可以按如下更改其地址池配置：

- 要向 ASA 中添加地址池，请点击 **Add**。系统将打开 Add IP Pool 对话框。
- 要在 ASA 上更改地址池的配置，请点击 **Edit**。如果池中的地址未在使用，系统将打开 Edit IP Pool 对话框。

注　如果地址池已在使用中，则无法对其进行修改。如果点击 **Edit** 并且地址池在使用中， ASDM 将显示错误消息并列出正在使用该池中的地址的连接名称和用户名。

- 要在 ASA 上移除地址池，请在表中选择该条目并点击 **Delete**。

注　如果地址池已在使用中，则无法将其移除。如果点击 **Delete** 并且地址池在使用中，ASDM 将显示错误消息并列出正在使用该池中的地址的连接名称。

- 要向接口分配地址池，请点击 **Add**。系统将打开 Assign Address Pools to Interface 对话框。选择要向其分配地址池的接口。点击 Address Pools 字段旁的 **Select**。系统将打开 Select Address Pools 对话框。双击要向接口分配的每个未分配池，或者选择每个未分配池并点击 **Assign**。相邻字段将显示池分配列表。点击 **OK** 以使用相应地址池的名称填充 Address Pools 字段，然后再次点击 **OK** 以完成分配的配置。
- 要更改向接口分配的地址池，请双击该接口，或者选择该接口并点击 **Edit**。系统将打开 Assign Address Pools to Interface 对话框。要移除地址池，请双击每个池名称并按键盘上的 Delete 键。如果要向接口分配其他字段，请点击 Address Pools 字段旁的 **Select**。系统将打开 Select Address Pools 对话框。请注意，Assign 字段显示保持分配给接口的地址池名称。双击要向接口添加的每个未分配池。 Assign 字段将更新池分配列表。点击 **OK** 以使用相应地址池的名称修改 Address Pools 字段，然后再次点击 **OK** 以完成分配的配置。
- 要移除条目，请选择该条目并点击 **Delete**。

以下各节描述 Add 对话框中用于配置地址池的字段：

- 在连接配置文件中向接口分配地址池
- 选择地址池
- 添加或编辑 IP 池

在连接配置文件中向接口分配地址池

要向连接配置文件分配地址池，请选择 Advanced > Client Addressing，然后选择 Add 或 Edit。

- Interface - 选择要向其分配地址池的接口。默认值为 DMZ。
- Address Pools - 指定要分配到指定接口的地址池。
- Select - 打开 Select Address Pools 对话框，可以在其中选择要向此接口分配的一个或多个地址池。选择显示在 Assign Address Pools to Interface 对话框的 Address Pools 字段中。

选择地址池

Select Address Pools 对话框显示可用于客户端地址分配的地址池的池名称、开始和结束地址以及子网掩码，并且使您可从该列表中添加、编辑或删除条目。

- Add - 打开 Add IP Pool 对话框，可以在其中配置新 IP 地址池。
- Edit - 打开 Edit IP Pool 对话框，可以在其中修改所选 IP 地址池。
- Delete - 移除所选地址池。无确认或撤消功能。
- Assign - 显示保持分配给接口的地址池名称。双击要向接口添加的每个未分配池。Assign 字段将更新池分配列表。

添加或编辑 IP 池

通过 Add or Edit IP Pool 对话框，可以指定或修改客户端地址分配的 IP 地址范围。

- Name - 指定分配给 IP 地址池的名称。
- Starting IP Address - 指定池中的第一个 IP 地址。
- Ending IP Address - 指定池中的最后一个 IP 地址。
- Subnet Mask - 选择要应用于池中的地址的子网掩码。

AnyConnect 连接配置文件 - 身份验证属性

- Interface-specific Authentication Server Groups - 管理身份验证服务器组到特定接口的分配。
  - Add or Edit - 打开 Assign Authentication Server Group to Interface 对话框，可以在其中指定接口和服务器组，并且指定在所选服务器组发生故障的情况下是否允许回退到 LOCAL 数据库。此对话框中的 Manage 按钮将打开 Configure AAA Server Groups 对话框。您的选择显示在 Interface/Server Group 表中。
  - Delete - 从表中移除所选服务器组。无确认或撤消功能。
- Username Mapping from Certificate - 使您可以在数字证书中指定要从其提取用户名的方法和字段。
  - Pre-fill Username from Certificate - 根据此面板中后面的选项，从指定的证书字段提取用户名并将其用于用户密码/密码身份验证和授权。
  - Hide username from end user- 指定不向最终用户显示提取的用户名。
  - Use script to choose username - 指定要用于从数字证书中选择用户名的脚本的名称。默认值为 --None--。
  - Add or Edit - 打开 Add or Edit Script Content 对话框，可以在其中定义要用于从证书映射用户名的脚本。
  - Delete - 删除所选脚本。无确认或撤消功能。
  - Use the entire DN as the username - 指定要将证书的整个 Distinguished Name 字段用作用户名。
  - Specify the certificate fields to be used as the username - 指定要组成用户名的一个或多个字段。

    主属性和辅助属性的可能的值包括：

属性	定义
C	国家/地区：所在国家/地区的双字母缩写。这些代码符合 ISO 3166 国家/地区缩写。
CN	公用名：人员、系统或者其他实体的名称。不可用作辅助属性。
DNQ	域名限定符。
EA	邮件地址。
GENQ	辈分词。
GN	名字。
I	首字母。
L	区域：组织所在的城市或城镇。
N	姓名。
O	组织：公司、机构、代理、协会或其他实体的名称。
OU	组织单位：组织 (O) 内的子组。
SER	序列号。

属性	定义
SN	姓氏。
SP	州/省：组织所在的州或省
T	职位。
UID	用户标识符。
UPN	用户主体名称。

  - Primary Field - 从证书中为用户名选择要使用的第一个字段。如果找到该值，将会忽略辅助字段。
  - Secondary Field - 选择在找不到主字段的情况下要使用的字段。
- Find - 输入要用作搜索字符串的 GUI 标签或 CLI 命令，然后点击 Next 或 Previous 以开始搜索。

AnyConnect 连接配置文件 - 辅助身份验证属性

通过 Secondary Authentication 对话框，可以为此连接配置文件配置辅助或 “双重”身份验证。启用双重身份验证后，最终用户必须提供两组有效身份验证凭证以进行登录。可以将辅助身份验证与从证书预填充用户名结合使用。此对话框中的字段类似于为主身份验证配置的字段，但是这些字段仅与辅助身份验证相关。

启用双重身份验证后，这些属性会在证书中选择一个或多个字段来用作用户名。从证书属性配置辅助用户名将强制安全设备使用指定的证书字段作为第二次用户名/密码身份验证的第二个用户名。

注　如果还指定辅助身份验证服务器组以及证书中的辅助用户名，仅主用户名会用于身份验证。

字段

- Secondary Authorization Server Group - 指定要从其提取辅助凭证的授权服务器组。
  - Server Group - 选择要用作辅助服务器 AAA 组的授权服务器组。默认值为 none。辅助服务器组不能是 SDI 服务器组。
  - Manage - 打开 Configure AAA Server Groups 对话框。
  - Use LOCAL if Server Group fails - 指定在指定的服务器组发生故障的情况下回退到 LOCAL 数据库。
  - Use primary username - 指定登录对话框必须要求仅提供一个用户名。
  - Attributes Server - 选择这是主属性服务器还是辅助属性服务器。

    注　如果还为此连接配置文件指定授权服务器，则授权服务器设置优先， ASA 忽略此辅助身份验证服务器。

  - Session Username Server - 选择这是主会话用户名服务器还是辅助会话用户名服务器。
- Interface-Specific Authorization Server Groups - 管理授权服务器组到特定接口的分配。
  - Add or Edit - 打开 Assign Authentication Server Group to Interface 对话框，可以在其中指定接口和服务器组，并且指定在所选服务器组发生故障的情况下是否允许回退到 LOCAL 数据库。此对话框中的 Manage 按钮将打开 Configure AAA Server Groups 对话框。您的选择显示在 Interface/Server Group 表中。

  - Delete - 从表中移除所选服务器组。无确认或撤消功能。
- Username Mapping from Certificate - 在数字证书中指定要从其提取用户名的字段。
- Pre-fill Username from Certificate - 选中以从此面板中指定的主字段和辅助字段中提取要用于辅助身份验证的名称。选中此属性之前，必须配置 AAA 和证书的身份验证方法。为此，请返回到同一窗口中的 Basic 面板并选中 Method 旁的 Both。
- Hide username from end user - 选中以对 VPN 用户隐藏要用于辅助身份验证的用户名。
- Fallback when a certificate is unavailable - 仅在选中 “Hide username from end user”的情况下才可配置此属性。如果证书不可用，请使用 Cisco Secure Desktop 主机扫描数据预填充用于辅助身份验证的用户名。
- Password - 选择以下方法之一来检索要用于辅助身份验证的密码：
  - Prompt - 提示用户输入密码。
  - Use Primary - 重复使用主身份验证密码进行所有身份验证。
  - Use - 输入用于所有辅助身份验证的公共辅助密码。
- Specify the certificate fields to be used as the username - 指定要作为用户名匹配的一个或多个字段。要在从证书预填充用户名功能中使用此用户名进行辅助用户名/密码身份验证或授权，还必须配置预填充用户名和辅助预填充用户名。
  - Primary Field - 从证书中为用户名选择要使用的第一个字段。如果找到该值，将会忽略辅助字段。
  - Secondary Field - 选择在找不到主字段的情况下要使用的字段。

  主字段和辅助字段属性的选项包括：

属性	定义
C	国家/地区：所在国家/地区的双字母缩写。这些代码符合 ISO 3166 国家/地区缩写。
CN	公用名：人员、系统或者其他实体的名称。不可用作辅助属性。
DNQ	域名限定符。
EA	邮件地址。
GENQ	辈分词。
GN	名字。
I	首字母。
L	区域：组织所在的城市或城镇。
N	姓名。
O	组织：公司、机构、代理、协会或其他实体的名称。
OU	组织单位：组织 (O) 内的子组。
SER	序列号。
SN	姓氏。
SP	州/省：组织所在的州或省
T	职位。
UID	用户标识符。
UPN	用户主体名称。

- Use the entire DN as the username - 使用整个主题 DN (RFC1779) 从数字证书为授权查询派生名称。
- Use script to select username - 从数字证书对要从其提取用户名的脚本进行命令。默认值为 --None--。
  - Add or Edit - 打开 Add or Edit Script Content 对话框，可以在其中定义要用于从证书映射用户名的脚本。
  - Delete - 删除所选脚本。无确认或撤消功能。

AnyConnect 连接配置文件 - 授权属性

通过 Authorization 对话框，可以查看、添加、编辑或删除特定于接口的授权服务器组。此对话框中表的每一行都显示一个特定于接口的服务器组的状态：接口名称、其关联服务器组以及在所选服务器组发生故障的情况下是否启用到本地数据库的回退。

此窗格中的字段对于 AnyConnect、 IKEv1、 IKEv2 和无客户端 SSL 连接配置文件相同。

授权服务器组字段

- Authorization Server Group - 指定要从其提取授权参数的授权服务器组。
  - Server Group - 选择要使用的授权服务器组。默认值为 none。
  - Manage - 打开 Configure AAA Server Groups 对话框。有关配置 AAA 服务器的信息，请参阅第 3-54 页上的在无客户端 SSL VPN 连接配置文件中向接口分配身份验证服务器组。
  - Users must exist in the authorization database to connect - 选择此复选框以要求用户必须满足此条件。
- Interface-specific Authorization Server Groups - 管理授权服务器组到特定接口的分配。
  - Add or Edit - 打开 Assign Authentication Server Group to Interface 对话框，可以在其中指定接口和服务器组，并且指定在所选服务器组发生故障的情况下是否允许回退到 LOCAL 数据库。此对话框中的 Manage 按钮将打开 Configure AAA Server Groups 对话框。您的选择显示在 Interface/Server Group 表中。
  - Delete - 从表中移除所选服务器组。无确认或撤消功能。
- Username Mapping from Certificate - 在数字证书中指定要从其提取用户名的字段。
  - Use script to select username - 指定要用于从数字证书中选择用户名的脚本的名称。默认值为 --None--。有关创建脚本以选择从证书字段创建用户名的详细信息，请参阅第 3-48 页上的添加脚本内容来为证书预填充用户名选择用户名。
  - Add or Edit - 打开 Add or Edit Script Content 对话框，可以在其中定义要用于从证书映射用户名的脚本。
  - Delete - 删除所选脚本。无确认或撤消功能。
  - Use the entire DN as the username - 指定要将证书的整个 Distinguished Name 字段用作用户名。
  - Specify the certificate fields to be used as the username - 指定要组成用户名的一个或多个字段。
  - Primary Field - 在证书中为用户名选择要使用的第一个字段。如果找到该值，将会忽略辅助字段。
  - Secondary Field - 选择在找不到主字段的情况下要使用的字段。
- Find - 输入要用作搜索字符串的 GUI 标签或 CLI 命令，然后点击 Next 或 Previous 以开始搜索。

添加脚本内容来为证书预填充用户名选择用户名

如果使用脚本来选择用户名，则可以创建或编辑使用其他映射选项中未列出的证书字段进行授权的脚本。

注　当使用脚本从证书预填充用户名在客户端证书中找不到用户名时， AnyConnect 客户端和无客户端 WebVPN 在用户名字段中均会显示 “Unknown”。

字段

- Script Name - 指定脚本的名称。脚本名称在授权和身份验证中必须相同。可以在此处定义脚本，然后 CLI 使用同一脚本执行此功能。
- Select script parameters - 指定脚本的属性和内容。
- Value for Username - 从标准 DN 属性的下拉列表中选择一个属性用作用户名 (Subject DN)。
- No Filtering - 指定要使用整个指定 DN 名称。
- Filter by substring - 指定开始索引 （要匹配的第一个字符在字符串中的位置）和结束索引 （要搜索的字符数）。如果选择此选项，则开始索引不能为空。如果将结束索引留空，则其默认为 -1，表示搜索整个字符串来查找匹配项。

  例如，假设选择 DN 属性 Common Name (CN)，其中包含主机/用户的值。表 3-3 显示使用子字符串选项过滤该值以将各种返回值存档的一些可能方法。返回值是实际预填充作为用户名的内容。

表 3-3　　按子字符串过滤

开始索引	结束索引	返回值
1	5	host/
6	10	user
6	-1	user

使用负索引 （例如在该表的第三行中）将指定从字符串末尾到子字符串末尾 （在本例中，即 “user” 的 “r”）向后进行计数。

使用按子字符串过滤时，您应该了解所寻求的子字符串的长度。从以下示例中，使用正则表达式匹配或 Lua 格式的自定义脚本：

- 示例 1：Regular Expression Matching - 在 Regular Expression 字段中输入要应用于搜索的正则表达式。标准正则表达式运算符适用。例如，假设要使用正则表达式过滤所有内容，直至 “Email Address (EA)” DN 值的 @ 符号。正则表达式 ^[^@]* 将是执行此操作的一种方法。在本示例中，如果 DN 值包含值 user1234@example.com，则正则表达式之后的返回值将为 user1234。
- 示例 2：Use custom script in Lua format - 指定以 Lua 编程语言编写的自定义脚本来解析搜索字段。选择此选项将使可在其中输入自定义 Lua 脚本的字段可供使用；例如，脚本：

  ```
  return cert.subject.cn..'/'..cert.subject.l
  ```

  将两个 DN 字段 username (cn) 和 locality (l) 组合用作单个用户名，并在两个字段之间插入斜杠 (/) 字符。

  表 3-4 列出可以在 Lua 脚本中使用的属性名称和描述。

注　Lua 区分大小写。

表 3-4　　属性名称和描述

属性名称	说明
cert.subject.c	国家/地区
cert.subject.cn	通用名称
cert.subject.dnq	DN 限定符
cert.subject.ea	邮件地址
cert.subject.genq	辈分词
cert.subject.gn	名字
cert.subject.i	首字母
cert.subject.l	区域
cert.subject.n	名称
cert.subject.o	组织
cert.subject.ou	组织单位
cert.subject.ser	主题序列号
cert.subject.sn	姓氏
cert.subject.sp	州/省
cert.subject.t	职位
cert.subject.uid	用户 ID
cert.issuer.c	国家/地区
cert.issuer.cn	通用名称
cert.issuer.dnq	DN 限定符
cert.issuer.ea	邮件地址
cert.issuer.genq	辈分词
cert.issuer.gn	名字
cert.issuer.i	首字母
cert.issuer.l	区域
cert.issuer.n	名称
cert.issuer.o	组织
cert.issuer.ou	组织单位
cert.issuer.ser	颁发者序列号
cert.issuer.sn	姓氏
cert.issuer.sp	州/省
cert.issuer.t	职位
cert.issuer.uid	用户 ID
cert.serialnumber	证书序列号
cert.subjectaltname.upn	用户主体名称

如果在激活隧道组脚本时发生错误，导致脚本未激活，则管理员控制台会显示错误消息。

在无客户端 SSL VPN 连接配置文件中向接口分配授权服务器组

通过此对话框，可将接口与 AAA 服务器组相关联。结果显示在 Authorization 对话框上的表中。

字段

- Interface - 选择接口：DMZ、 Outside 或 Inside。默认值为 DMZ。
- Server Group - 选择要分配给所选接口的服务器组。默认值为 LOCAL。
- Manage - 打开 Configure AAA Server Groups 对话框。

在连接配置文件中配置记帐

此对话框中的设置在整个 ASA 上全局适用于连接配置文件 （隧道组）。通过此对话框可配置以下属性：

- Accounting Server Group - 选择以前定义的用于记帐的服务器组。
- Manage - 打开 Configure AAA Server Groups 对话框，可以在其中创建 AAA 服务器组。

在 AnyConnect 连接配置文件中配置别名和 URL

此对话框配置可影响远程用户在登录时显示的内容的属性。此对话框中的字段对于 AnyConnect 客户端和无客户端 SSL VPN 相同，不同在于无客户端 SSL VPN 具有一个附加字段。连接配置文件中的选项卡的名称对于 AnyConnect 为 Group URL/Group Alias，对于无客户端 SSL VPN 为 Clientless SSL VPN。

连接别名和组 URL 的字段

- Enable the display of Radius Reject-Message on the login screen - 选择此复选框以在拒绝身份验证时在登录对话框上显示 RADIUS 拒绝消息。
- Enable the display of SecurId message on the login screen - 选择此复选框以在登录对话框上显示 SecurID 消息。
- Manage - 打开 Configure GUI Customization Objects 对话框。
- Connection Aliases - 在表中列出现有连接别名及其状态，并可在该表中添加或删除项。如果连接配置为允许用户在登录时选择特定连接 （隧道组），则在用户登录页面上会显示连接别名。该表中的行可适当编辑，因此没有 Edit 按钮。点击表上方的“i”图标将打开编辑功能的工具提示。
  - Add - 打开 Add Connection Alias 对话框，可以在其中添加并启用连接别名。
  - Delete - 从连接别名表中移除所选行。无确认或撤消功能。
  - 要编辑表中所列的别名，请双击行。
- Group URLs - 在表中列出现有组 URL 及其状态，并可在该表中添加或删除项。如果连接配置为允许用户在登录时选择特定组，则在用户登录页面上会显示组 URL。该表中的行可适当编辑，因此没有 Edit 按钮。点击表上方的 “i” 图标将打开编辑功能的工具提示。
  - Add - 打开 Add Group URL 对话框，可以在其中添加并启用组 URL。
  - Delete - 从连接别名表中移除所选行。无确认或撤消功能。
  - 要编辑表中所列的 URL，请双击行。
- 使用以上定义的组 URL 访问 ASA 时，请勿在客户端计算机上运行 Cisco Secure Desktop (CSD)。(If a client connects using a connection alias, this setting is ignored.) - 如果要免除使用与 Group URLs 表中的条目匹配的 URL 的用户运行 CSD，请选中此项。请注意，执行此操作会阻止安全设备从这些用户接收终端条件，因此可能必须更改 DAP 配置来为其提供 VPN 访问。

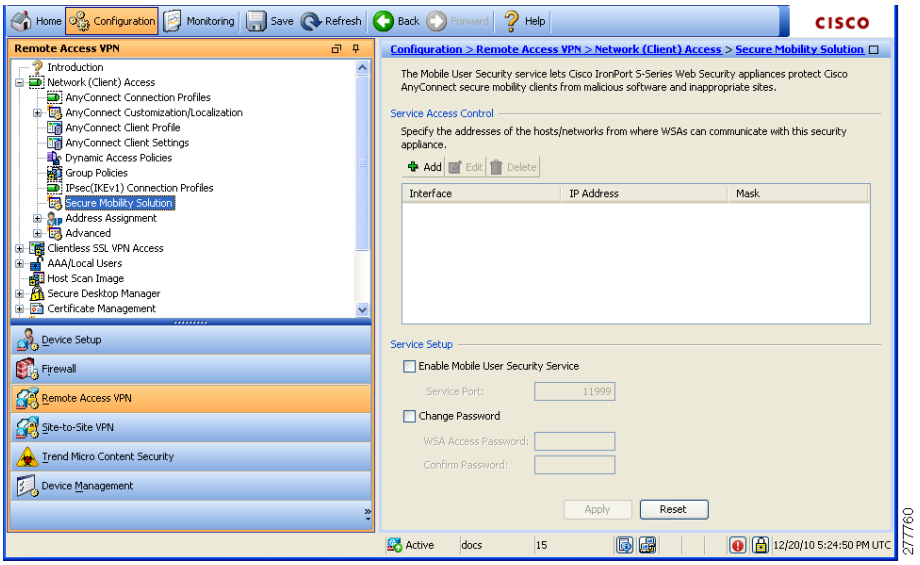
配置 AnyConnect 安全移动

当员工处于移动状态时， AnyConnect 安全移动保护公司利益和资产免受互联网威胁。使用 Mobile User Security 对话框配置此功能。通过 AnyConnect 安全移动， Cisco IronPort S 系列网络安全设备可以扫描 Cisco AnyConnect 安全移动客户端来确保客户端可防范恶意软件和/或不适当的站点。客户端定期检查以确保启用 Cisco IronPort S 系列网络安全设备保护。

要配置安全移动解决方案，请选择 **Configuration > Remote Access VPN > Network (Client) Access > Mobile User Security**。

注　此功能需要可为 Cisco AnyConnect 安全移动客户端提供 AnyConnect 安全移动许可支持的 Cisco IronPort 网络安全设备发行版。它还需要支持 AnyConnect 安全移动功能的 AnyConnect 发行版。 AnyConnect 3.1 和更高版本不支持此功能。

图 3-6　　移动用户安全窗口



字段

- Service Access Control - 指定 WSA 可从其进行通信的主机或网络地址。
  - Add - 为所选连接打开 Add MUS Access Control Configuration 对话框。
  - Edit - 为所选连接打开 Edit MUS Access Control Configuration 对话框。
  - Delete - 从表中移除所选连接。无确认或撤消功能。
- Enable Mobile User Security Service - 通过 VPN 启动与客户端的连接。如果启用，需要输入供 WSA 在联系 ASA 时使用的密码。如果 WSA 不存在，则状态为已禁用。
- Service Port - 如果选择启用服务，请指定要使用服务的哪个端口号。端口必须介于 1 和 65535 之间，并且必须与通过管理系统配置到 WSA 中的对应值相匹配。默认值为 11999。
- Change Password - 支持更改 WSA 访问密码。
- WSA Access Password - 指定在 ASA 和 WSA 之间进行身份验证所需的共享密码。此密码必须与通过管理系统配置到 WSA 中的对应密码相匹配。
- Confirm Password- 重新输入指定密码。
- Show WSA Sessions - 允许查看连接到 ASA 的 WSA 的会话信息。所连接 （或已连接）的 WSA 的主机 IP 地址和连接持续时间会在对话框中返回。

添加或编辑 MUS 访问控制

通过 Add or Edit MUS Access Control 对话框，可以配置 MUS 访问。

字段

- Interface Name - 使用下拉列表选择进行添加或编辑的接口名称。
- IP Address - 输入 IPv4 或 IPv6 地址。
- Mask - 使用下拉列表选择相应的掩码。

配置无客户端 SSL VPN 连接配置文件

Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles 对话框列出当前定义的无客户端 SSL VPN 连接配置文件和全局无客户端选项。

Connection Profiles 窗格中的字段

- Access Interfaces - 通过它可选择要为访问启用的接口。此表中的字段包括接口名称和指定是否允许访问的复选框。
  - Device Certificate - 通过它可为 RSA 密钥或 ECDSA 密钥或信任点指定用于身份验证的证书。可以选择配置两个信任点。客户端通过供应商 ID 负载来指示 ECDSA 支持。ASA 扫描已配置的信任点列表并选择客户端支持的第一个信任点。如果首选 ECDSA，则应该在 RSA 信任点之前配置该信任点。
  - Manage - 打开 Manage Identity Certificates 对话框，可以在其中添加、编辑、删除、导出和显示所选证书的详细信息。
  - Port Setting - 配置无客户端 SSL 和 IPsec (IKEv2) 连接的端口号。范围为 1-65535。默认值为端口 443。
- 登录页面设置
  - 允许在登录页面上选择通过其别名进行标识的连接配置文件。否则，连接配置文件将是 DefaultWebVPNGroup。指定用户登录页面为用户提供一个下拉列表，用户可以从中选择要与其连接的特定隧道组。
  - Allow user to enter internal password on the login page - 添加用于在访问内部服务器时输入其他密码的选项。
  - Shutdown portal login page - 显示禁用登录时的网页。
- Connection Profiles - 提供一个连接表，其中显示用于确定此连接（隧道组）的连接策略的记录。每个记录标识连接的默认组策略并包含特定于协议的连接参数。
  - Add - 为所选连接打开 Add Clientless SSL VPN 对话框。
  - Edit - 为所选连接打开 Edit Clientless SSL VPN 对话框。
  - Delete - 从表中移除所选连接。无确认或撤消功能。
  - Name - 连接配置文件的名称。
  - Enabled - 在启用时选中。
  - Aliases - 用于标识连接配置文件的其他名称。
  - Authentication Method - 指定使用的身份验证方法。
  - Group Policy - 显示此连接配置文件的默认组策略。

- Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile matches the certificate map will be used - 此选项在连接配置文件选择过程中指定组 URL 和证书值的相对首选项。如果 ASA 无法将终端指定的首选值与连接配置文件指定的首选值相匹配，它将选择与其他值匹配的连接配置文件。仅当依靠许多旧 ASA 软件发行版使用的首选项将 VPN 终端所指定的组 URL 与指定同一个组 URL 的连接配置文件相匹配时，才选中此选项。默认情况下，未选中此选项。如果未选中此选项，则 ASA 首选将连接配置文件中指定的证书字段值与供终端用于分配连接配置文件的证书的字段值相匹配。

在无客户端 SSL VPN 连接配置文件中配置基本属性

Clientless SSL VPN Connection Profile > Advanced > Basic 对话框设置 Basic 属性。

Basic 窗格中的字段

- Name - 指定连接的名称。对于 Edit 功能，此字段为只读。
- Aliases - （可选）指定此连接的一个或多个替代名称。如果在 Clientless SSL VPN Access Connections 对话框中配置该选项，则在登录页面上会显示别名。
- Authentication - 指定身份验证参数。
  - Method - 指定为此连接使用 AAA 身份验证、证书身份验证还是同时使用这两种方法。默认值为 AAA 身份验证。
  - AAA server Group - 选择要用于对此连接进行身份验证的 AAA 服务器组。默认值为 LOCAL。
  - Manage - 打开 Configure AAA Server Groups 对话框。
- DNS Server Group - 选择要用作此连接的 DNS 服务器组的服务器。默认值为 DefaultDNS。
- Default Group Policy - 指定要用于此连接的默认组策略参数。
  - Group Policy - 选择要用于此连接的默认组策略。默认值为 DfltGrpPolicy。
  - Clientless SSL VPN Protocol - 为此连接启用或禁用无客户端 SSL VPN 协议。

在无客户端 SSL VPN 连接配置文件中配置常规属性

使用 Clientless SSL VPN Connection Profile > Advanced > General 对话框指定在用户名传递到 AAA 服务器之前是否要从中剥除领域和组，并且指定密码管理选项。

General Attributes 窗格中的字段

- Password Management - 通过它可以配置与覆盖来自 AAA 服务器的帐户已禁用指示和通知用户密码到期相关的参数。
  - Enable notification password management - 选中此复选框将使以下两个参数可用。决定在用户登录时通知其距离密码到期的具体天数还是仅在密码到期当天通知用户。默认是在密码到期前 14 天通知用户，并且此后每天通知，直到用户更改密码为止。范围是 1 到 180 天。

注　这不会更改距离密码到期的天数，而是会启用通知。如果选择此选项，还必须指定天数。

并且在任一情况下，如果密码到期而未更改， ASA 将为用户提供机会来更改密码。如果当前密码未到期，用户仍可使用该密码登录。

此参数对于支持此类通知的 AAA 服务器有效；即 RADIUS、使用 NT 服务器的 RADIUS 以及 LDAP 服务器。如果尚未配置 RADIUS 或 LDAP 身份验证， ASA 将忽略此命令。

– Override account-disabled indication from AAA server - 覆盖来自 AAA 服务器的帐户已禁用指示。

注　允许覆盖帐户已禁用指示是一项潜在安全风险。

在无客户端 SSL VPN 连接配置文件中配置身份验证

通过 Clientless SSL VPN Connection Profile > Advanced > Authentication 对话框，可以查看、添加、编辑或删除特定于接口的身份验证服务器组。此对话框中表的每一行都显示一个特定于接口的服务器组的状态：接口名称、其关联服务器组以及在所选服务器组发生故障的情况下是否启用到本地数据库的回退。

Authentication 窗格中的字段与用于 AnyConnect 身份验证的字段相同，并在以下位置进行了描述：第 3-44 页上的 AnyConnect 连接配置文件 - 身份验证属性。

在无客户端 SSL VPN 连接配置文件中向接口分配身份验证服务器组

通过 Clientless SSL VPN Connection Profile > Advanced > Authentication 对话框，可以将接口与 AAA 服务器组相关联。结果显示在 Authentication 对话框上的表中。

第 3-50 页上的在无客户端 SSL VPN 连接配置文件中向接口分配授权服务器组中对执行此配置的字段进行了描述。

在无客户端 SSL VPN 连接配置文件中配置辅助身份验证

无客户端 SSL 的 Secondary_authentication 配置字段与用于 AnyConnect 客户端访问的配置字段相同，这在第 3-45 页上的 AnyConnect 连接配置文件 - 辅助身份验证属性中进行了描述。

在无客户端 SSL VPN 连接配置文件中配置授权

无客户端 SSL 的授权配置字段与 AnyConnect、IKEv1 和 IKEv2 的授权配置字段相同。有关这些字段的信息，请参阅第 3-47 页上的 AnyConnect 连接配置文件 - 授权属性。

在无客户端 SSL VPN 连接配置文件中配置 NetBIOS 服务器

Clientless SSL VPN Connection Profile > Advanced > NetBIOS Servers 对话框中的表显示已经配置的 NetBIOS 服务器的属性。通过无客户端 SSL VPN 访问的 Add or Edit Tunnel Group 对话框 > NetBIOS 对话框，可以配置隧道组的 NetBIOS 属性。无客户端 SSL VPN 使用 NetBIOS 和通用互联网文件系统协议访问或共享远程系统上的文件。尝试通过使用 Windows 计算机的计算机名称与其进行文件共享连接时，指定的文件服务器与用于标识网络上的资源的特定 NetBIOS 名称对应。

ASA 查询 NetBIOS 名称服务器以将 NetBIOS 名称映射到 IP 地址。无客户端 SSL VPN 需要 NetBIOS 来访问或共享远程系统上的文件。

要使 NBNS 功能可运作，必须配置至少一个 NetBIOS 服务器（主机）。可以配置最多三个 NBNS 服务器以实现冗余。 ASA 使用列表中的第一个服务器进行 NetBIOS/CIFS 名称解析。如果查询失败，将使用下一个服务器。

NetBIOS Servers 窗格中的字段

- IP Address - 显示已配置的 NetBIOS 服务器的 IP 地址。
- Master Browser - 显示服务器是 WINS 服务器还是也可以充当 CIFS 服务器 （即，主浏览器）的服务器。
- Timeout (seconds) - 显示服务器在将 NBNS 查询发送到下一个服务器之前等待对该查询的响应的初始时间 （以秒为单位）。
- Retries - 显示重试将 NBNS 查询顺序发送到已配置的服务器的次数。换句话说，这是在返回错误之前对服务器列表进行循环的次数。最小重试次数为 0。默认重试次数为 2。最大重试次数为 10。
- Add/Edit - 点击添加 NetBIOS 服务器。这将打开 Add or Edit NetBIOS Server 对话框。
- Delete - 从列表中移除突出显示的 NetBIOS 行。
- Move Up/Move Down - ASA 按照 NBNS 查询在此框中的显示顺序将其发送到 NetBIOS 服务器。使用此框以通过将服务器在列表中上移或下移来更改其优先级顺序。

在无客户端 SSL VPN 连接配置文件中配置组 URL 和别名

通过 Clientless Connect Profile 中的 Advanced > Clientless SSL VPN 窗格，可以配置会影响远程用户在登录时显示的内容的属性。

字段

- Portal Page Customization(Clientless SSL VPN only) - 通过指定要应用的预配置定制属性来配置用户登录页面的外观。默认值为 DfltCustomization。

此对话框和 AnyConnect 连接配置文件的其余字段相同。有关详细信息，请参阅第 3-50 页上的在 AnyConnect 连接配置文件中配置别名和 URL。

配置 DNS 服务器组

Configuration > Remote Access VPN > DNS 对话框在表中显示已配置的 DNS 服务器，包括服务器组名、服务器、超时 （以秒为单位）、允许的重试次数和域名。可以在此对话框中添加、编辑或删除 DNS 服务器组。

字段

- Add or Edit - 打开 Add or Edit DNS Server Group 对话框。
- Delete - 从表中移除所选行。无确认或撤消功能。
- DNS Server Group - 选择要用作此连接的 DNS 服务器组的服务器。默认值为 DefaultDNS。
- Manage - 打开 Configure DNS Server Groups 对话框。

IKEv1 连接配置文件

此窗格配置 IKEv1 客户端的连接配置文件，包括 L2TP-IPsec。

Connection Profile 窗格中的字段

- Access Interfaces - 选择要为 IPsec 访问启用的接口。默认值为无访问。

- Connection Profiles - 以表格格式显示现有 IPsec 连接的已配置参数。Connections 表包含用于确定连接策略的记录。记录标识连接的默认组策略并包含特定于协议的连接参数。该表包含以下列：
  - Name - 指定 IPsec IKEv1 连接的名称或 IP 地址。
  - IPsec Enabled - 指示是否已启用 IPsec 协议。可以在 Add or Edit IPsec Remote Access Connection Basic 对话框中启用此协议。
  - L2TP/IPsec Enabled - 指示是否已启用 L2TP/IPsec 协议。可以在 Add or Edit IPsec Remote Access Connection Basic 对话框中启用此协议。
  - Authentication Server Group - 可以提供身份验证的服务器组的名称。
  - Group Policy - 指示此 IPsec 连接的组策略的名称。

注　Delete - 从表中移除所选服务器组。无确认或撤消功能。

配置 IPsec 远程访问连接配置文件 - Basic 选项卡

通过 Add or Edit IPsec Remote Access Connection Profile Basic 对话框，可以配置 IPsec IKEv1 VPN 连接的通用属性，包括 L2TP-IPsec。

IPsec Connection Profile Basic 选项卡上的字段

- Name - 此连接配置文件的名称。
- IKE Peer Authentication - 配置 IKE 对等体。
  - Pre-shared key - 指定连接的预共享密钥的值。预共享密钥的最大长度为 128 个字符。
  - Identity Certificate - 选择身份证书的名称 （如果已配置并注册任何身份证书）。
  - Manage - 打开 Manage Identity Certificates 对话框，可以在其中添加、编辑、删除、导出和显示所选证书的详细信息。
- User Authentication - 指定有关用于用户身份验证的服务器的信息。可以在 Advanced 部分中配置更多身份验证信息。
  - Server Group - 选择要用于用户身份验证的服务器组。默认值为 LOCAL。如果选择除 LOCAL 以外的内容，则 Fallback 复选框变得可用。要添加服务器组，请点击 Manage 按钮。
  - Fallback - 指定在所指定的服务器组发生故障的情况下是否使用 LOCAL 进行用户身份验证。
- Client Address Assignment - 指定与分配客户端属性相关的属性。
  - DHCP Servers - 指定要使用的 DHCP 服务器的 IP 地址。最多可以添加 10 个服务器，以空格分隔。
  - Client Address Pools - 指定最多 6 个预定义地址池。要定义地址池，请转至 Configuration > Remote Access VPN > Network Client Access > Address Assignment > Address Pools，或者点击 Select 按钮。
- Default Group Policy - 指定与默认组策略相关的属性。
  - Group Policy - 选择要用于此连接的默认组策略。默认值为 DfltGrpPolicy。要定义与该组策略关联的新组策略，请点击 Manage。
  - Enable IPsec Protocol and Enable L2TP over IPsec protocol - 选择要用于此连接的一个或多个协议。

配置客户端寻址

客户端寻址配置对于客户端连接配置文件是通用的。有关详细信息，请参阅第 3-42 页上的在连接配置文件中配置客户端寻址。

配置身份验证

配置身份验证对于客户端连接配置文件是通用的。有关详细信息，请参阅第 3-44 页上的 AnyConnect 连接配置文件 - 身份验证属性。

配置授权

配置授权对于客户端连接配置文件是通用的。有关详细信息，请参阅第 3-44 页上的 AnyConnect 连接配置文件 - 身份验证属性。

配置记帐

配置记帐对于客户端连接配置文件是通用的。有关详细信息，请参阅。

在 IKEv1 连接配置文件中配置 IPsec

帮助链接位于站点间列表中，因此这需要更多工作。

在 IKEv1 连接配置文件中配置 PPP

要使用此 IKEv1 连接配置文件配置 PPP 连接允许的身份验证协议，请打开 Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles，然后添加或编辑其中一个连接配置文件。

此对话框*仅*适用于 IPsec IKEv1 远程访问连接配置文件。

PPP 窗格中的字段

- CHAP - 为 PPP 连接启用 CHAP 协议。
- MS-CHAP-V1 - 为 PPP 连接启用 MS-CHAP-V1 协议。
- MS-CHAP-V2 - 为 PPP 连接启用 MS-CHAP-V2 协议。
- PAP - 为 PPP 连接启用 PAP 协议。
- EAP-PROXY - 为 PPP 连接启用 EAP-PROXY 协议。 EAP 是指可扩展身份验证协议。

第三方和本机 VPN 的 IKEv2 连接配置文件

IKEv2 连接配置文件为本机和第三方 VPN 客户端定义 EAP、基于证书以及基于预共享密钥的身份验证。 ASDM 中的配置面板是 **Configuration > Remote Access VPN > Network (Client) Access > IPsec (IKEv2) Connection Profiles**。

字段

- Access Interfaces - 选择要为 IPsec 访问启用的接口。默认是未选择任何访问。
- Bypass interface access lists for inbound VPN sessions - 选中此复选框以绕过入站 VPN 会话的接口访问列表。组策略和用户策略的访问列表始终适用于所有流量。
- Connection Profiles - 以表格格式显示现有 IPsec 连接的已配置参数。Connection Profiles 表包含用于确定连接策略的记录。记录标识连接的默认组策略并包含特定于协议的连接参数。该表包含以下列：
  - Name - 指定 IPsec 连接的名称或 IP 地址。
  - IKEv2 Enabled - 如果选中，则指定已启用 IKEv2 协议。
  - Authentication Server Group - 指定用于身份验证的服务器组的名称。
  - Group Policy - 指示此 IPsec 连接的组策略的名称。

注　Delete - 从表中移除所选服务器组。无确认或撤消功能。

添加或编辑 IPsec IKEv2 连接配置文件 - Basic 选项卡

Add or Edit IPsec Remote Access Connection Profile Basic 对话框配置 IPsec IKEv2 连接的通用属性。

字段

- Name - 标识连接的名称。
- IKE Peer Authentication - 配置 IKE 对等体。
  - Pre-shared key - 指定连接的预共享密钥的值。预共享密钥的最大长度为 128 个字符。
  - Enable Certificate Authentication - 如果选中，则允许使用证书进行身份验证。
  - Enable peer authentication using EAP - 如果选中，则允许使用 EAP 进行身份验证。如果选中此复选框，则必须使用证书进行本地身份验证。
  - Send an EAP identity request to the client - 支持向远程访问 VPN 客户端发送 EAP 身份验证请求。
  - Identity Certificate - 选择身份证书的名称 （如果已配置并注册任何身份证书）。
  - Manage - 打开 Manage Identity Certificates 对话框，可以在其中添加、编辑、删除、导出和显示所选证书的详细信息。
- User Authentication - 指定有关用于用户身份验证的服务器的信息。可以在 Advanced 部分中配置更多身份验证信息。
  - Server Group - 选择要用于用户身份验证的服务器组。默认值为 LOCAL。如果选择除 LOCAL 以外的内容，则 Fallback 复选框变得可用。
  - Manage - 打开 Configure AAA Server Groups 对话框。
  - Fallback - 指定在所指定的服务器组发生故障的情况下是否使用 LOCAL 进行用户身份验证。

- Client Address Assignment - 指定与分配客户端属性相关的属性。
  - DHCP Servers - 指定要使用的 DHCP 服务器的 IP 地址。最多可以添加 10 个服务器，以空格分隔。
  - Client Address Pools - 指定最多 6 个预定义地址池。要定义地址池，请转至 Configuration > Remote Access VPN > Network Client Access > Address Assignment > Address Pools。
  - Select - 打开 Select Address Pools 对话框。
- Default Group Policy - 指定与默认组策略相关的属性。
  - Group Policy - 选择要用于此连接的默认组策略。默认值为 DfltGrpPolicy。
  - Manage - 打开 Configure Group Policies 对话框，从中可以添加、编辑或删除组策略。
  - Client Protocols - 选择要用于此连接的一个或多个协议。默认情况下，会选择 IPsec 和 L2TP over IPsec。
  - Enable IKEv2 Protocol - 启用 IKEv2 协议以在远程访问连接配置文件中使用。这是刚选择的组策略的属性。

IPsec Remote Access Connection Profile - Advanced > IPsec 选项卡

字段

- Send certificate chain - 选中以启用或禁用发送整个证书链。此操作在传输中包含根证书和任何从属 CA 证书。
- IKE Peer ID Validation - 从下拉列表中选择未选中、必需还是已选中 IKE 对等体 ID 验证 （如果其受证书支持）。

将证书映射到 IPsec 或 SSL VPN 连接配置文件

当 ASA 接收到带有客户端证书身份验证的 IPsec 连接请求时，它会根据配置的策略向连接分配连接配置文件。该策略可以是使用配置的规则、使用证书 OU 字段、使用 IKE 身份（即主机、IP 地址、密钥 ID）、对等体 IP 地址或默认连接配置文件。对于 SSL 连接， ASA 仅使用配置的规则。

对于使用规则的 IPsec 或 SSL 连接， ASA 根据规则评估证书的属性，直到找到匹配项为止。当找到匹配项时，它会向连接分配与匹配的规则关联的连接配置文件。如果未能找到匹配项，它会向连接分配默认连接配置文件（对于 IPsec 为 DefaultRAGroup，对于 SSL VPN 为 DefaultWEBVPNGroup），并使用户从门户页面上显示的下拉列表 （如果已启用）中选择连接配置文件。此配置文件中一次连接尝试的结果取决于证书是否有效以及连接配置文件的身份验证设置。

证书组匹配策略定义要用于标识证书用户的权限组的方法。可以使用其中任意或所有方法。

首先，在 Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Maps 中配置用于将证书与连接配置文件相匹配的策略。如果选择使用配置的规则，请转至 Rules 以指定规则。以下操作步骤显示如何为每个 IPsec 和 SSL VPN 连接配置文件创建基于证书的条件：

使用顶部的表 (Certificate to Connection Profile Maps) 执行以下操作之一：

步骤 1　创建列表名称 （称为 “map”），指定列表的优先级，然后将列表分配给连接配置文件。

将列表添加到表中之后， ASDM 会突出显示该列表。

步骤 2　确认列表会分配给要为其添加基于证书的规则的连接配置文件。

将列表添加到表中之后，ASDM 会突出显示该列表，并在窗格底部显示表中的任何关联列表条目。

步骤 3　使用底部的表 (Mapping Criteria) 查看、添加、更改或删除条目到所选列表。

列表中的每个条目包含一条基于证书的规则。映射条件列表中的所有规则都需要与 ASA 的证书内容相匹配，以选择关联映射索引。要在一个条件或另一个条件匹配的情况下分配连接，请为每个匹配条件创建一个列表。

要了解字段，请参阅以下各节：

- 设置证书匹配策略
- 添加/编辑证书匹配规则
- 添加/编辑证书匹配规则条件

设置证书匹配策略

对于 IPsec 连接，证书组匹配策略定义要用于标识证书用户的权限组的方法。可以使用其中任意或所有方法：

字段

- Use the configured rules to match a certificate to a group - 通过它可以使用已在 Rules 下定义的规则。
- Use the certificate OU field to determine the group - 通过它可以使用组织单位字段确定要与证书相匹配的组。默认情况下会选择此项。
- Use the IKE identity to determine the group - 通过它可以使用以前在 Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Parameters 下定义的身份。IKE 标识可以是主机名、 IP 地址，密钥 ID 或自动。
- Use the peer IP address to determine the group - 通过它可以使用对等体的 IP 地址。默认情况下会选择此项。
- Default to group - 通过它可以为证书用户选择在先前方法未产生匹配项的情况下所使用的默认组。默认情况下会选择此项。点击 Default to group 列表中的默认组。该组必须已存在于配置中。如果该组未显示在列表中，必须通过使用 Configuration > Remote Access VPN > Network (Client) Access > Group Policies 对其进行定义。

添加/编辑证书匹配规则

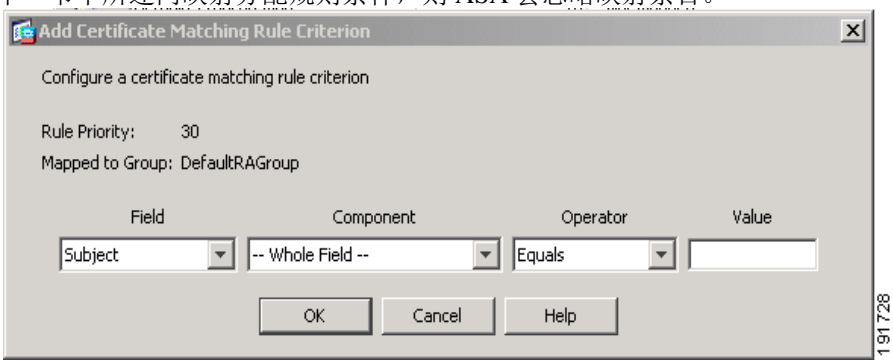
Configuration > VPN > IKE > Certificate Group Matching > Rules > Add/Edit Certificate Matching Rule

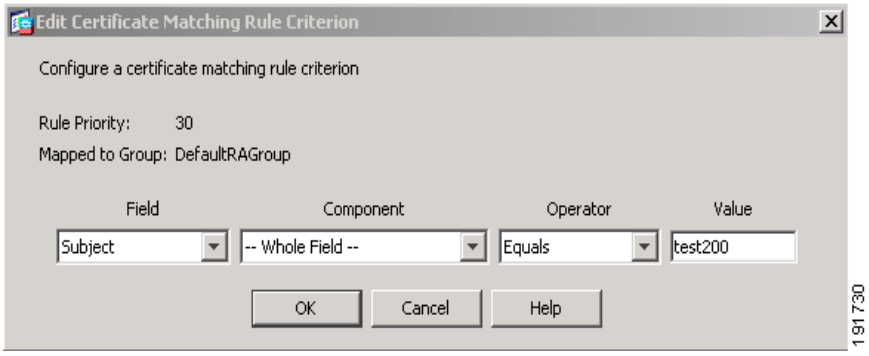
使用 Add/Edit Certificate Matching Rule 对话框将列表 （映射）的名称分配到连接配置文件。

字段

- Map - 选择下列之一：
  - Existing - 选择要包含规则的映射的名称。
  - New - 为规则输入新的映射名称。
- Rule Priority - 输入一个小数以指定 ASA 在接收到连接请求时评估映射的顺序。对于定义的第一条规则，默认优先级为 10。 ASA 首先根据具有最低优先级数字的映射评估每个连接。
- Mapped to Connection Profile - 选择要映射到此规则的连接配置文件，以前称为 “隧道组”。

如果没有按下一节中所述向映射分配规则条件，则 ASA 会忽略映射条目。





添加/编辑证书匹配规则条件

Configuration > VPN > IKE > Certificate Group Matching > Rules > Add/Edit Certificate Matching Rule Criterion

使用 Add/Edit Certificate Matching Rule Criterion 对话框配置所选连接配置文件的证书匹配规则条件。

字段

- Rule Priority -（仅显示）。 ASA 在接收到连接请求时评估映射的顺序。 ASA 首先根据具有最低优先级数字的映射评估每个连接。
- Mapped to Group - （仅显示）。将规则分配到的连接配置文件。
- Field - 从下拉列表中选择要评估的证书部分。
  - Subject - 使用证书的个人或系统。对于 CA 根证书， Subject 和 Issuer 相同。
  - Alternative Subject - 主题替代扩展名允许其他身份绑定到证书的主题。
  - Issuer - 颁发证书的 CA 或其他实体 （辖区）。
  - Extended Key Usage - 提供可以选择匹配的进一步条件的客户端证书扩展。

- Component -（仅在选定 Issuer 的 Subject 的情况下才适用）选择规则中使用的可分辨名称组件：

DN 字段	定义
Whole Field	整个 DN。
Country (C)	所在国家/地区的双字母缩写。这些代码符合 ISO 3166 国家/地区缩写。
Common Name (CN)	人员、系统或者其他实体的名称。这是标识层次结构中的最低（最具体）级别。
DN Qualifier (DNQ)	特定 DN 属性。
E-mail Address (EA)	拥有证书的个人、系统或实体的邮件地址。
Generational Qualifier (GENQ)	辈分词，如 Jr.、 Sr. 或 III。
Given Name (GN)	证书所有者的名字。
Initials (I)	证书所有者姓名的每个部分的第一个字母。
Locality (L)	组织所在的城市或城镇。
Name (N)	证书所有者的姓名。
Organization (O)	公司、机构、代理、协会或其他实体的名称。
Organizational Unit (OU)	组织内的子组。
Serial Number (SER)	证书的序列号。
Surname (SN)	证书所有者的姓氏。
State/Province (S/P)	组织所在的州或省。
Title (T)	证书所有者的头衔，例如博士。
User ID (UID)	证书所有者的标识号。
Unstructured Name (UNAME)	unstructuredName 属性类型将主题的一个或多个名称指定为非结构化 ASCII 字符串。
IP Address (IP)	IP 地址字段。

- Operator - 选择规则中使用的运算符：
  - Equals - 可分辨名称字段必须与值完全匹配。
  - Contains - 可分辨名称字段中必须包含值。
  - Does Not Equal - 可分辨名称字段不得与值匹配。
  - Does Not Contain - 可分辨名称字段中不得包含值。

- Value - 输入最多 255 个字符以指定运算符的对象。对于 Extended Key Usage，请选择下拉列表中的其中一个预定义值，或者可以输入其他扩展的 OID。预定义值包括：

选项	密钥用途	OID 字符串
clientauth	客户端身份验证	1.3.6.1.5.5.7.3.2
codesigning	代码签名	1.3.6.1.5.5.7.3.3
emailprotection	安全邮件保护	1.3.6.1.5.5.7.3.4
ocspsigning	OCSP 签名	1.3.6.1.5.5.7.3.9
serverauth	服务器身份验证	1.3.6.1.5.5.7.3.1
timestamping	时间戳	1.3.6.1.5.5.7.3.8

站点间连接配置文件

Connection Profiles 对话框显示当前配置的站点间连接配置文件（隧道组）的属性，通过该对话框可以选择解析连接配置文件名称时要使用的定界符，以及添加、修改或删除连接配置文件。

ASA 使用 IKEv1 或 IKEv2 支持 IPv4 或 IPv6 的 IPsec LAN 到 LAN VPN 连接，使用内层和外层 IP 头支持内部和外部网络。

Site to Site Connection Profile 窗格中的字段

- Access Interfaces - 显示设备接口表，可以在其中启用由接口上的远程对等设备进行的访问。
  - Interface - 要启用或禁用访问的设备接口。
  - Allow IKEv1 Access - 选中以启用由对等设备进行的 IPsec IKEv1 访问。
  - Allow IKEv2 Access - 选中以启用由对等设备进行的 IPsec IKEv2 访问。
- Connection Profiles - 显示连接配置文件表，可以在其中添加、编辑或删除配置文件：
  - Add - 打开 Add IPsec Site-to-Site connection profile 对话框。
  - Edit - 打开 Edit IPsec Site-to-Site connection profile 对话框。
  - Delete - 移除所选连接配置文件。无确认或撤消功能。
  - Name - 连接配置文件的名称。
  - Interface - 启用连接配置文件时所在的接口。
  - Local Network - 指定本地网络的 IP 地址。
  - Remote Network - 指定远程网络的 IP 地址。
  - IKEv1 Enabled - 显示对于连接配置文件已启用 IKEv1。
  - IKEv2 Enabled - 显示对于连接配置文件已启用 IKEv2。
  - Group Policy - 显示连接配置文件的默认组策略。

配置站点间连接配置文件

通过 Add or Edit IPsec Site-to-Site Connection 对话框，可以创建或修改 IPsec 站点间连接。通过这些对话框，可以指定对等体 IP 地址（IPv4 或 IPv6），指定连接名称，选择接口，指定 IKEv1 和 IKEv2 对等体和用户身份验证参数，指定受保护网络以及指定加密算法。

当两个思科或第三方对等体具有 IPv4 内部和外部网络（IPv4 地址位于内部和外部接口上）时，ASA 支持与这些对等体的 LAN 到 LAN VPN 连接。

对于使用混合 IPv4 和 IPv6 寻址或全部使用 IPv6 寻址的 LAN 到 LAN 连接，如果两个对等体均是 Cisco ASA 5500 系列安全设备，并且如果两个内部网络均有匹配的寻址方案 （均为 IPv4 或均为 IPv6），则安全设备支持 VPN 隧道。

具体而言，当两个对等体均是 Cisco ASA 5500 系列时， ASA支持以下拓扑：

- ASA 具有 IPv4 内部网络且外部网络是 IPv6（IPv4 地址位于内部接口上且 IPv6 地址位于外部接口上）。
- ASA 具有 IPv6 内部网络且外部网络是 IPv4（IPv6 地址位于内部接口上且 IPv4 地址位于外部接口上）。
- ASA 具有 IPv6 内部网络且外部网络是 IPv6 （IPv6 地址位于内部和外部接口上）。

Basic 面板上的字段

- Peer IP Address - 通过它可以指定 IP 地址 （IPv4 或 IPv6）以及该地址是否为静态。
- Connection Name - 指定分配给此连接配置文件的名称。对于 Edit 功能，此字段为仅显示。可以指定连接名称与 Peer IP Address 字段中指定的 IP 地址相同。
- Interface - 选择要用于此连接的接口。
- Protected Networks - 选择或指定此连接的受保护本地和远程网络。
  - IP Address Type - 指定地址是 IPv4 还是 IPv6 地址。
  - Local Network - 指定本地网络的 IP 地址。
  - ... - 打开 Browse Local Network 对话框，可以在其中选择本地网络。
  - Remote Network - 指定远程网络的 IP 地址。
- IPsec Enabling - 指定此连接配置文件的组策略和在该组策略中指定的密钥交换协议：
  - Group Policy Name - 指定与此连接配置文件关联的组策略。
  - Manage - 打开 Browse Remote Network 对话框，可以在其中选择远程网络。
  - Enable IKEv1 - 在指定组策略中启用密钥交换协议 IKEv1。
  - Enable IKEv2 - 在指定组策略中启用密钥交换协议 IKEv2。
- IKEv1 Settings 选项卡 - 指定 IKEv1 的身份验证和加密设置：
  - Pre-shared Key - 指定隧道组的预共享密钥的值。预共享密钥的最大长度为 128 个字符。
  - Device Certificate - 指定要用于身份验证的身份证书的名称 （如果适用）。
  - Manage - 打开 Manage Identity Certificates 对话框，可以在其中查找已经配置的证书，添加新证书，显示证书的详细信息以及编辑或删除证书。
  - IKE Policy - 指定要用于 IKE 建议的一个或多个加密算法。
  - Manage - 打开 Configure IKEv1 Proposals 对话框。
  - IPsec Proposal - 指定要用于 IPsec IKEv1 建议的一个或多个加密算法。
- IKEv2 Settings 选项卡 - 指定 IKEv2 的身份验证和加密设置：

- Local Pre-shared Key - 指定隧道组的预共享密钥的值。预共享密钥的最大长度为 128 个字符。
- Local Device Certificate - 指定要用于身份验证的身份证书的名称 （如果适用）。
- Manage - 打开 Manage Identity Certificates 对话框，可以在其中查找已经配置的证书，添加新证书，显示证书的详细信息以及编辑或删除证书。
- Remote Peer Pre-shared Key - 指定隧道组的远程对等体预共享密钥的值。预共享密钥的最大长度为 128 个字符。
- Remote Peer Certificate Authentication - 选中 *Allowed* 以允许此连接配置文件的 IKEv2 连接的证书身份验证。
- Manage - 打开 Manage CA Certificates 对话框，可以在其中查看证书和添加新证书。
- IKE Policy - 指定要用于 IKE 建议的一个或多个加密算法。
- Manage - 打开 Configure IKEv1 Proposals 对话框。
- IPsec Proposal - 指定要用于 IPsec IKEv1 建议的一个或多个加密算法。
- Select - 打开 Select IPsec Proposals (Transform Sets) 对话框，可以在其中向 IKEv2 连接的连接配置文件分配建议。
- 此连接配置文件也具有 Advanced > Crypto Map Entry 和 Adv

配置站点间隧道组

您可以通过各种路径转至此面板。

通过 Add or Edit IPsec Site-to-Site Tunnel Group 对话框，可以指定进行添加的 IPsec 站点间连接的属性。此外，还可以选择 IKE 对等体和用户身份验证参数，配置 IKE Keepalive 监控以及选择默认组策略。

字段

- Name - 指定分配给此隧道组的名称。对于 Edit 功能，此字段为仅显示。
- IKE Authentication - 指定对 IKE 对等体进行身份验证时要使用的预共享密钥和身份证书参数。
  - Pre-shared Key - 指定隧道组的预共享密钥的值。预共享密钥的最大长度为 128 个字符。
  - Identity Certificate - 指定要用于身份验证的 ID 证书的名称 （如果适用）。
  - Manage - 打开 Manage Identity Certificates 对话框，可以在其中查找已经配置的证书，添加新证书，显示证书的详细信息以及编辑或删除证书。
  - IKE Peer ID Validation - 指定是否选中 IKE 对等体 ID 验证。默认值为 Required。
- IPsec Enabling - 指定此连接配置文件的组策略和在该组策略中指定的密钥交换协议：
  - Group Policy Name - 指定与此连接配置文件关联的组策略。
  - Manage - 打开 Browse Remote Network 对话框，可以在其中选择远程网络。
  - Enable IKEv1 - 在指定组策略中启用密钥交换协议 IKEv1。
  - Enable IKEv2 - 在指定组策略中启用密钥交换协议 IKEv2。
- IKEv1 Settings 选项卡 - 指定 IKEv1 的身份验证和加密设置：
  - Pre-shared Key - 指定隧道组的预共享密钥的值。预共享密钥的最大长度为 128 个字符。
  - Device Certificate - 指定要用于身份验证的身份证书的名称 （如果适用）。
  - Manage - 打开 Manage Identity Certificates 对话框，可以在其中查找已经配置的证书，添加新证书，显示证书的详细信息以及编辑或删除证书。
  - IKE Policy - 指定要用于 IKE 建议的一个或多个加密算法。

  - Manage - 打开 Configure IKEv1 Proposals 对话框。
  - IPsec Proposal - 指定要用于 IPsec IKEv1 建议的一个或多个加密算法。
- IKEv2 Settings 选项卡 - 指定 IKEv2 的身份验证和加密设置：
  - Local Pre-shared Key - 指定隧道组的预共享密钥的值。预共享密钥的最大长度为 128 个字符。
  - Local Device Certificate - 指定要用于身份验证的身份证书的名称 （如果适用）。
  - Manage - 打开 Manage Identity Certificates 对话框，可以在其中查找已经配置的证书，添加新证书，显示证书的详细信息以及编辑或删除证书。
  - Remote Peer Pre-shared Key - 指定隧道组的远程对等体预共享密钥的值。预共享密钥的最大长度为 128 个字符。
  - Remote Peer Certificate Authentication - 选中 *Allowed* 以允许此连接配置文件的 IKEv2 连接的证书身份验证。
  - Manage - 打开 Manage CA Certificates 对话框，可以在其中查看证书和添加新证书。
  - IKE Policy - 指定要用于 IKE 建议的一个或多个加密算法。
  - Manage - 打开 Configure IKEv1 Proposals 对话框。
  - IPsec Proposal - 指定要用于 IPsec IKEv1 建议的一个或多个加密算法。
  - Select - 打开 Select IPsec Proposals (Transform Sets) 对话框，可以在其中向 IKEv2 连接的连接配置文件分配建议。
- IKE Keepalive - 启用并配置 IKE 保活监控。只能选择以下属性之一。
  - Disable Keep Alives - 启用或禁用 IKE 保活。
  - Monitor Keep Alives - 启用或禁用 IKE 保活监控。选择此选项将使 Confidence Interval 和 Retry Interval 字段可供使用。
  - Confidence Interval - 指定 IKE 保活置信区间。这是 ASA 应该允许对等体在开始保活监控之前空闲的秒数。最小值为 10 秒；最大值为 300 秒。远程访问组的默认值为 10 秒。
  - Retry Interval - 指定在 IKE 保活重试之间等待的秒数。默认值为 2 秒。
  - Head end will never initiate keepalive monitoring - 指定中心站点 ASA 绝不会启动保活监控。

在站点间连接配置文件中配置加密映射条目

在此对话框中，指定当前站点间连接配置文件的加密参数。

加密映射中的字段

- **Priority** - 唯一优先级（1 到 65,543，1 为最高优先级）。当 IKE 协商开始时，发起协商的对等体将其所有策略发送到远程对等体，然后远程对等体按优先级顺序搜索其自己的策略的匹配项。
- **Perfect Forward Secrecy** - 确保给定 IPsec SA 的密钥不是派生自任何其他机密（类似于其他一些密钥）。如果某人要破解密钥，则 PFS 确保攻击者将无法派生任何其他密钥。如果启用 PFS，则 Diffie-Hellman Group 列表会激活。
  - **Diffie-Hellman Group** - 供两个 IPsec 对等体用于派生共享机密而不将其相互传输的标识。选项为 Group 1 （768 位）、 Group 2 （1024 位）和 Group 5 （1536 位）。
- **Enable NAT-T** - 为此策略启用 NAT 遍历 (NAT-T)，使 IPsec 对等体能够通过 NAT 设备同时建立远程访问连接和 LAN 到 LAN 连接。
- **Enable Reverse Route Injection** - 为静态路由提供自动插入到受远程隧道终端保护的网络和主机的路由进程中的能力。

- **Security Association Lifetime** - 配置安全关联 (SA) 的持续时间。此参数指定 IPsec SA 密钥生存期的度量方式，即 IPsec SA 过期并必须用新的密钥重新协商前，它可以持续的时长。
  - **Time** - 根据小时 (hh)、分钟 (mm) 和秒 (ss) 指定 SA 生存期。
  - **Traffic Volume** - 根据流量的千字节数定义 SA 生存期。输入负载数据的千字节数量，IPsec SA 在达到该数量后到期。最小值为 100 KB，默认值为 10000 KB，最大值为 2147483647 KB。

Crypto Map Entry for Static Peer Address

在此对话框中，当对等体 IP 地址为静态地址时，指定连接配置文件的加密参数。

字段

- Priority - 唯一优先级（1 到 65,543，1 为最高优先级）。当 IKE 协商开始时，发起协商的对等体将其所有策略发送到远程对等体，然后远程对等体按优先级顺序搜索其自己的策略的匹配项。
- Perfect Forward Secrecy - 确保给定 IPsec SA 的密钥不是派生自任何其他机密（类似于其他一些密钥）。如果某人要破解密钥，则 PFS 确保攻击者将无法派生任何其他密钥。如果启用 PFS，则 Diffie-Hellman Group 列表会激活。
  - Diffie-Hellman Group - 供两个 IPsec 对等体用于派生共享机密而不将其相互传输的标识。选项为 Group 1（768 位）、 Group 2（1024 位）和 Group 5（1536 位）。
- Enable NAT-T - 为此策略启用 NAT 遍历 (NAT-T)，使 IPsec 对等体能够通过 NAT 设备同时建立远程访问连接和 LAN 到 LAN 连接。
- Enable Reverse Route Injection - 为静态路由提供自动插入到受远程隧道终端保护的网络和主机的路由进程中的能力。
- Security Association Lifetime - 配置安全关联 (SA) 的持续时间。此参数指定 IPsec SA 密钥生存期的度量方式，即 IPsec SA 过期并必须用新的密钥重新协商前，它可以持续的时长。
  - Time - 根据小时 (hh)、分钟 (mm) 和秒 (ss) 指定 SA 生存期。
  - Traffic Volume - 根据流量的千字节数定义 SA 生存期。输入负载数据的千字节数量，IPsec SA 在达到该数量后到期。最小值为 100 KB，默认值为 10000 KB，最大值为 2147483647 KB。
- Static Crypto Map Entry Parameters - 当 Peer IP Address 指定为 Static 时，配置以下附加参数：
  - Connection Type - 将允许的协商指定为 bidirectional、 answer-only 或 originate-only。
  - Send ID Cert.Chain - 启用整个证书链的传输。
  - IKE Negotiation Mode - 设置有关设置 SA 的密钥信息的交换模式（Main 或 Aggressive）。它还设置协商发起方使用的模式；响应方自动协商。攻击性模式速度较快，使用的数据包较少，交换次数较少，但是它不会保护通信方的身份。主模式速度较慢，使用的数据包较多，交换次数较多，但是它会保护通信方的身份。此模式更安全，并且是默认选择。如果选择 Aggressive，则 Diffie-Hellman Group 列表会激活。
  - Diffie-Hellman Group - 供两个 IPsec 对等体用于派生共享机密而不将其相互传输的标识。选项为 Group 1（768 位）、 Group 2（1024 位）和 Group 5（1536 位）。

管理 CA 证书

点击 IKE Peer Authentication 下的 Manage 以打开 Manage CA Certificates 对话框。使用此对话框查看、添加、编辑和删除可用于 IKE 对等体身份验证的 CA 证书列表上的条目。

Manage CA Certificates 对话框列出有关当前配置的证书的信息，包括有关证书被颁发者、证书颁发者、证书到期时间和使用情况数据的信息。

字段

- Add or Edit - 打开 Install Certificate dialog box 或 Edit Certificate 对话框，通过它可以指定有关证书和安装证书的信息。
- Show Details - 显示有关在表中选择的证书的详细信息。
- Delete - 从表中移除所选证书。无确认或撤消功能。

Install Certificate

使用此对话框安装新的 CA 证书。可以通过以下方式之一获取证书：

- 通过浏览至证书文件来从文件进行安装。
- 将以前获取的 PEM 格式的证书粘贴到此对话框中的框内。
- Use SCEP - 指定为在 Windows Server 2003 系列上运行的证书服务使用简单证书注册协议 (SCEP) 附件。它为 SCEP 协议提供支持，从而允许思科路由器和其他中间网络设备获取证书。
  - SCEP URL: http:// - 指定要从其下载 SCEP 信息的 URL。
  - Retry Period - 指定 SCEP 查询之间必须间隔的分钟数。
  - Retry Count - 指定允许的最大重试次数。
- More Options - 打开 Configure Options for CA Certificate 对话框。

Configure Options for CA Certificate

使用此对话框指定有关检索此 IPsec 远程访问连接的 CA 证书的详细信息。此对话框中的对话框包括：Revocation Check、 CRL Retrieval Policy、 CRL Retrieval Method、 OCSP Rules 和 Advanced。

Revocation Check 对话框

使用此对话框指定有关 CA 证书撤销检查的信息。

字段

- 单选按钮指定是否检查证书以进行撤销。这些按钮的值如下：
  - Do not check certificates for revocation
  - Check Certificates for revocation
- Revocation Methods 区域 - 通过它可以指定要用于撤销检查的方法（CRL 或 OCSP）以及使用这些方法的顺序。可以选择任一方法，也可以同时选择两种方法。

Add/Edit Remote Access Connections > Advanced > General

使用此对话框指定在将用户名传递到 AAA 服务器之前是否要从中剥除领域和组，并且指定密码管理参数。

字段

- Strip the realm from username before passing it on to the AAA server - 启用或禁用在将用户名传递到 AAA 服务器之前从中剥除领域（管理域）。选中 Strip Realm 复选框以在身份验证期间移除用户名的领域限定符。可以向 AAA 的用户名追加领域名：authorization、authentication 和 accounting。领域唯一有效定界符是 @ 字符。格式为 username@realm，例如 JaneDoe@example.com。如果选中此 Strip Realm 复选框，则身份验证仅基于用户名。否则，身份验证基于完整的 username@realm 字符串。如果服务器无法解析定界符，则必须选中此框。

注　可以向用户名追加领域和组，在此情况下，ASA 对于 AAA 功能使用为组*和*领域配置的参数。此选项的格式为 *username[@realm]]<#or!>group]*，例如 *JaneDoe@example.com#VPNGroup*。如果选择此选项，必须为组定界符使用 # 或 !字符，因为如果 @ 也显示为领域定界符，则 ASA 无法将其解析为组定界符。

Kerberos 领域是一种特殊情况。Kerberos 领域的命名约定是将与该 Kerberos 领域中的主机关联的 DNS 域名大写。例如，如果用户在 example.com 域中，则可能会调用 Kerberos 领域 EXAMPLE.COM。

与 VPN 3000 集中器一样，ASA 不包含对 user@grouppolicy 的支持。只有 L2TP/IPsec 客户端支持通过 user@tunnelgroup 进行隧道交换。

- Strip the group from the username before passing it on to the AAA server - 启用或禁用在将用户名传递到 AAA 服务器之前从中剥除组名。选中 Strip Group 以在身份验证期间从用户名中移除组名。仅当还选中 Enable Group Lookup 框时，此选项才有意义。使用定界符向用户名追加组名并启用组查找时，ASA 将定界符左侧的所有字符都解释为用户名，将右侧的所有字符都解释为组名。有效组分隔符为 @、# 和 !字符，其中 @ 字符作为组查找的默认值。可以通过格式 *username<delimiter>group* 向用户名追加组，可能的值为例如 *JaneDoe@VPNGroup*、*JaneDoe#VPNGroup* 和 *JaneDoe!VPNGroup*。
- Password Management - 通过它可以配置与覆盖来自 AAA 服务器的帐户已禁用指示和通知用户密码到期相关的参数。
  - Override account-disabled indication from AAA server - 覆盖来自 AAA 服务器的帐户已禁用指示。

注　允许覆盖帐户已禁用指示是一项潜在安全风险。

  - Enable notification upon password expiration to allow user to change password - 选中此复选框将使以下两个参数可用。可以选择在用户登录时通知其距离密码到期的具体天数还是仅在密码到期当天通知用户。默认是在密码到期前 14 天通知用户，并且此后每天通知，直到用户更改密码为止。范围是 1 到 180 天。

注　这不会更改距离密码到期的天数，而是会启用通知。如果选择此选项，还必须指定天数。

并且在任一情况下，如果密码到期而未更改， ASA 将为用户提供机会来更改密码。如果当前密码未到期，用户仍可使用该密码登录。

此参数对于支持此类通知的 AAA 服务器有效；即 RADIUS、使用 NT 服务器的 RADIUS 以及 LDAP 服务器。如果尚未配置 RADIUS 或 LDAP 身份验证， ASA 将忽略此命令。

此功能需要使用 MS-CHAPv2。

Add/Edit Connection Profile > General > Authentication

此对话框可用于 IPsec on Remote Access 和 Site-to-Site 隧道组。此对话框中的设置在整个 ASA 上全局适用于此连接配置文件 （隧道组）。要逐个接口设置身份验证服务器组设置，请点击 Advanced。通过此对话框可配置以下属性：

- Authentication Server Group - 列出可用身份验证服务器组，包括 LOCAL 组 （默认）。您也可以选择 None。选择除 None 或 LOCAL 以外的其他内容将使 Use LOCAL if Server Group Fails 复选框可供使用。要逐个接口设置身份验证服务器组，请点击 Advanced。
- Use LOCAL if Server Group fails - 在 Authentication Server Group 属性指定的组发生故障的情况下启用或禁用到 LOCAL 数据库的回退。

Add/Edit SSL VPN Connection > General > Authorization

此对话框中的设置在整个 ASA 上全局适用于连接配置文件 （隧道组）。通过此对话框可配置以下属性：

- Authorization Server Group - 列出可用的授权服务器组，包括 LOCAL 组。您也可以选择 None （默认）。选择除 None 以外的内容将使 Users must exist in authorization database to connect 复选框可供使用。
- Users must exist in the authorization database to connect - 指示 ASA 仅允许授权数据库中的用户进行连接。缺省情况下，会禁用此功能。必须具有已配置的授权服务器才能使用此功能。
- Interface-Specific Authorization Server Groups - （可选）通过它可以逐个接口配置授权服务器组。特定于接口的授权服务器组优先于全局服务器组。如果没有明确配置特定于接口的授权，则仅在组级别进行授权。
  - Interface - 选择要在其之上执行授权的接口。标准接口是 outside （默认）、 inside 和 DMZ。如果已配置其他接口，则这些接口也显示在列表中。
  - Server Group - 选择可用的以前配置的授权服务器组或服务器组，包括 LOCAL 组。可以将服务器组与多个接口相关联。
  - Add - 点击 Add 以将接口/服务器组添加到表中并从可用列表中移除接口。
  - Remove - 点击 Remove 以从表中移除接口/服务器组并将接口还原到可用列表。
- Authorization Settings - 通过它可以为 ASA 识别用于授权的用户名设置值。这适用于通过数字证书进行身份验证并需要 LDAP 或 RADIUS 授权的用户。
  - Use the entire DN as the username - 允许使用整个可分辨名称 (DN) 作为用户名。
  - Specify individual DN fields as the username - 支持使用单个 DN 字段作为用户名。
  - Primary DN Field - 列出供选择的所有 DN 字段标识符。

DN 字段	定义
Country (C)	所在国家/地区的双字母缩写。这些代码符合 ISO 3166 国家/地区缩写。
Common Name (CN)	人员、系统或者其他实体的名称。这是标识层次结构中的最低（最具体）级别。

DN 字段	定义
DN Qualifier (DNQ)	特定 DN 属性。
E-mail Address (EA)	拥有证书的个人、系统或实体的邮件地址。
Generational Qualifier (GENQ)	辈分词，如 Jr.、 Sr. 或 III。
Given Name (GN)	证书所有者的名字。
Initials (I)	证书所有者姓名的每个部分的第一个字母。
Locality (L)	组织所在的城市或城镇。
Name (N)	证书所有者的姓名。
Organization (O)	公司、机构、代理、协会或其他实体的名称。
Organizational Unit (OU)	组织内的子组。
Serial Number (SER)	证书的序列号。
Surname (SN)	证书所有者的姓氏。
State/Province (S/P)	组织所在的州或省。
Title (T)	证书所有者的头衔，例如博士。
User ID (UID)	证书所有者的标识号。
User Principal Name (UPN)	与智能卡证书身份验证配合使用。

  - Secondary DN Field - 列出供选择的所有 DN 字段标识符 （请参阅前面的表）并添加表示无选择的选项 None。

Add/Edit Tunnel Group > General > Client Address Assignment

要指定使用 DHCP 还是地址池进行地址分配，请转至 Configuration > VPN > I P Address Management > Assignment。通过 Add or Edit Tunnel Group 对话框 > General > Client Address Assignment 对话框，可以配置以下 Client Address Assignment 属性：

- DHCP Servers - 指定要使用的 DHCP 服务器。可以一次一个添加最多 10 个服务器。
  - IP Address - 指定 DHCP 服务器的 IP 地址。
  - Add - 将指定的 DHCP 服务器添加到客户端地址分配列表。
  - Delete - 从客户端地址分配列表中删除指定的 DHCP 服务器。无确认或撤消功能。
- Address Pools - 通过它可以使用以下参数指定最多 6 个地址池：
  - Available Pools - 列出可以选择的可用的已配置地址池。
  - Add - 将所选地址池添加到客户端地址分配列表。
  - Remove - 将所选地址池从 Assigned Pools 列表移至 Available Pools 列表。
  - Assigned Pools - 列出为地址分配选择的地址池。

注　要配置特定于接口的地址池，请点击 Advanced。

Add/Edit Tunnel Group > General > Advanced

通过 Add or Edit Tunnel Group 对话框 > General > Advanced 对话框，可以配置以下特定于接口的属性：

- Interface-Specific Authentication Server Groups - 通过它可以为授权配置接口和服务器组。
  - Interface - 列出供选择的可用接口。
  - Server Group - 列出可用于此接口的身份验证服务器组。
  - Use LOCAL if server group fails - 在服务器组发生故障的情况下启用或禁用到 LOCAL 数据库的回退。
  - Add - 将所选可用接口与身份验证服务器组之间的关联添加到分配的列表。
  - Remove - 将所选接口与身份验证服务器组的关联从分配的列表移至可用列表。
  - Interface/Server Group/Use Fallback - 显示已添加到分配的列表的选择。
- Interface-Specific Client IP Address Pools - 通过它可以指定接口和客户端 IP 地址池。最多可以具有 6 个池。
  - Interface - 列出要添加的可用接口。
  - Address Pool - 列出可用于与此接口相关联的地址池。
  - Add - 将所选可用接口与客户端 IP 地址池之间的关联添加到分配的列表。
  - Remove - 将所选接口/地址池关联从分配的列表移至可用列表。
  - Interface/Address Pool - 显示已添加到分配的列表的选择。

Add/Edit Tunnel Group > IPsec for Remote Access > IPsec

Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > IPSec for Remote Access > IPSec 选项卡

在 IPsec for Remote Access 的 Add or Edit Tunnel Group 对话框中，通过 IPsec 对话框可以配置或编辑特定于 IPsec 的隧道组参数。

字段

- Pre-shared Key - 通过它可以指定隧道组的预共享密钥的值。预共享密钥的最大长度为 128 个字符。
- Trustpoint Name - 如果配置了任何信任点，请选择信任点名称。信任点是证书颁发机构的表示。信任点包含 CA 的身份、特定于 CA 的配置参数，以及与一个已注册身份证书的关联。
- Authentication Mode = 指定身份验证模式：none、 xauth 或 hybrid。
  - none - 指定无身份验证模式。
  - xauth - 指定使用 IKE 扩展身份验证模式，它提供使用 TACACS+ 或 RADIUS 在 IKE 内对用户进行身份验证的功能。
  - hybrid - 指定使用混合模式，通过它可以使用数字证书进行安全设备身份验证，并使用其他的传统方法（如 RADIUS、TACACS+ 或 SecurID）进行远程 VPN 用户身份验证。此模式将互联网密钥交换 (IKE) 的第 1 阶段分为以下步骤，统称为混合身份验证。
    1. 安全设备使用标准公钥方法对远程 VPN 用户进行身份验证。这会建立单向身份验证的 IKE 安全关联。
    2. 然后，扩展身份验证 (xauth) 交换对远程 VPN 用户进行身份验证。此扩展身份验证可以使用其中一种受支持的传统身份验证方法。

注　在将身份验证类型设置为 hybrid 之前，必须配置身份验证服务器并创建预共享密钥。

- IKE Peer ID Validation - 选择忽略、必需还是仅在证书支持的情况下才选中 IKE 对等体 ID 验证。
- Enable sending certificate chain - 启用或禁用发送整个证书链。此操作在传输中包含根证书和任何从属 CA 证书。
- ISAKMP Keep Alive - 启用并配置 ISAKMP 保活监控。
  - Disable Keep Alives - 启用或禁用 ISAKMP 保活。
  - Monitor Keep Alives - 启用或禁用 ISAKMP 保活监控。选择此选项将使 Confidence Interval 和 Retry Interval 字段可供使用。
  - Confidence Interval - 指定 ISAKMP 保活置信区间。这是 ASA 应该允许对等体在开始保活监控之前空闲的秒数。最小值为 10 秒；最大值为 300 秒。远程访问组的默认值为 300 秒。
  - Retry Interval - 指定在 ISAKMP 保活重试之间等待的秒数。默认值为 2 秒。
  - Head end will never initiate keepalive monitoring - 指定中心站点 ASA 绝不会启动保活监控。
- Interface-Specific Authentication Mode - 逐个接口指定身份验证模式。
  - Interface - 选择指定接口。默认接口为 inside 和 outside，但是如果已配置其他接口名称，则该名称也会显示在列表中。
  - Authentication Mode - 通过它可以选择如上所述的身份验证模式：none、 xauth 或 hybrid。
  - Interface/Authentication Mode 表 - 显示选择的接口名称及其关联身份验证模式。
  - Add - 向 Interface/Authentication Modes 表中添加接口/身份验证模式对选择。
  - Remove - 从 Interface/Authentication Modes 表中移除接口/身份验证模式对选择。
- Client VPN Software Update Table - 列出安装的每个客户端 VPN 软件包的客户端类型、VPN 客户端修订版本和映像 URL。对于每个客户端类型，可以指定可接受的客户端软件修订版本以及要从其下载软件升级的 URL 或 IP 地址 （如有必要）。客户端更新机制 （在 Client Update 下进行了详细描述）使用此信息来确定每个 VPN 客户端运行的软件是否处于适当的修订级别，并在适当情况下向运行过时软件的客户端提供通知消息和更新机制。
  - Client Type - 标识 VPN 客户端类型。
  - VPN Client Revisions - 指定可接受的 VPN 客户端修订级别。
  - Image URL - 指定可以从其下载正确的 VPN 客户端软件映像的 URL 或 IP 地址。对于基于对话框的 VPN 客户端， URL 的格式必须为 http:// 或 https://。对于处于客户端模式下的 ASA 5505 或 VPN 3002 硬件客户端， URL 的格式必须为 tftp://。

Add/Edit Tunnel Group for Site-to-Site VPN

Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > IPSec for Remote Access > IPSec 选项卡

通过 Add or Edit Tunnel Group 对话框，可以配置或编辑此站点间连接配置文件的隧道组参数。

字段

- Certificate Settings - 设置以下证书链和 IKE 对等体验证属性：
  - Send certificate chain - 启用或禁用发送整个证书链。此操作在传输中包含根证书和任何从属 CA 证书。
  - IKE Peer ID Validation - 选择忽略、必需还是仅在证书支持的情况下才选中 IKE 对等体 ID 验证。
- IKE Keep Alive - 启用并配置 IKE (ISAKMP) 保活监控。
  - Disable Keepalives - 启用或禁用 IKE 保活。
  - Monitor Keepalives - 启用或禁用 IKE 保活监控。选择此选项将使 Confidence Interval 和 Retry Interval 字段可供使用。
  - Confidence Interval - 指定 IKE 保活置信区间。这是 ASA 应该允许对等体在开始保活监控之前空闲的秒数。最小值为 10 秒；最大值为 300 秒。远程访问组的默认值为 300 秒。
  - Retry Interval - 指定在 IKE 保活重试之间等待的秒数。默认值为 2 秒。
  - Head end will never initiate keepalive monitoring - 指定中心站点 ASA 绝不会启动保活监控。
- Default Group Policy - 指定以下组策略属性：
  - Group Policy - 选择要用作默认组策略的组策略。默认值为 DfltGrpPolicy。
  - Manage - 打开 Configure Group Policies 对话框。
  - IPsec Protocol - 启用或禁用对此连接配置文件使用 IPSec 协议。

Add/Edit Tunnel Group > IPsec for LAN to LAN Access > General > Basic

Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > IPSec for LAN to LAN Access > General 选项卡 > Basic 选项卡

在 Add or Edit Tunnel Group 对话框 > Site-to-Site Remote Access > General > Basic 对话框中，可以指定进行添加 （仅适用于 Add 功能）的隧道组的名称并选择组策略。

在 Edit Tunnel Group 对话框中， General 对话框显示进行修改的隧道组的名称和类型。

字段

- Name - 指定分配给此隧道组的名称。对于 Edit 功能，此字段为仅显示。
- Type -（*仅显示*）显示进行添加或编辑的隧道组的类型。此字段的内容取决于在前一个对话框中的选择。
- Group Policy - 列出当前配置的组策略。默认值为默认组策略 DfltGrpPolicy。

- Strip the realm (administrative domain) from the username before passing it on to the AAA server - 启用或禁用在将用户名传递到 AAA 服务器之前从中剥除领域。选中 Strip Realm 复选框以在身份验证期间移除用户名的领域限定符。可以向 AAA 的用户名追加领域名：authorization、authentication 和 accounting。领域唯一有效定界符是 @ 字符。格式为 username@realm，例如 JaneDoe@example.com。如果选中此 Strip Realm 复选框，则身份验证仅基于用户名。否则，身份验证基于完整的 username@realm 字符串。如果服务器无法解析定界符，则必须选中此框。

注　可以向用户名追加领域和组，在此情况下，ASA 对于 AAA 功能使用为组*和*领域配置的参数。此选项的格式为 *username[@realm]]<#or!>group]*，例如 *JaneDoe@example.com#VPNGroup*。如果选择此选项，必须为组定界符使用 # 或 !字符，因为如果 @ 也显示为领域定界符，则 ASA 无法将其解析为组定界符。

Kerberos 领域是一种特殊情况。Kerberos 领域的命名约定是将与该 Kerberos 领域中的主机关联的 DNS 域名大写。例如，如果用户在 example.com 域中，则可能会调用 Kerberos 领域 EXAMPLE.COM。

与 VPN 3000 集中器一样，ASA **不包含对** user@grouppolicy **的支持。只有** L2TP/IPsec **客户端支持通过** user@tunnelgroup **进行隧道交换。**

- Strip the group from the username before passing it on to the AAA server - 启用或禁用在将用户名传递到 AAA 服务器之前从中剥除组名。选中 Strip Group 以在身份验证期间从用户名中移除组名。仅当还选中 Enable Group Lookup 框时，此选项才有意义。使用定界符向用户名追加组名并启用组查找时，ASA 将定界符左侧的所有字符都解释为用户名，将右侧的所有字符都解释为组名。有效组分隔符为 @、# 和 !字符，其中 @ 字符作为组查找的默认值。可以通过格式 *username<delimiter>group* 向用户名追加组，可能的值为例如 *JaneDoe@VPNGroup*、*JaneDoe#VPNGroup* 和 *JaneDoe!VPNGroup*。
- Password Management - 通过它可以配置与覆盖来自 AAA 服务器的帐户已禁用指示和通知用户密码到期相关的参数。
  - Override account-disabled indication from AAA server - 覆盖来自 AAA 服务器的帐户已禁用指示。

注　允许覆盖帐户已禁用指示是一项潜在安全风险。

  - Enable notification upon password expiration to allow user to change password - 选中此复选框将使以下两个参数可用。如果没有另外选中 Enable notification prior to expiration 复选框，则用户仅在密码到期后才会接收到通知。
  - Enable notification prior to expiration - 当选中此选项时， ASA 在远程用户登录时通知其当前密码即将到期或已到期，然后为用户提供机会更改密码。如果当前密码未到期，用户仍可使用该密码登录。此参数对于支持此类通知的 AAA 服务器有效；即 RADIUS、使用 NT 服务器的 RADIUS 以及 LDAP 服务器。如果尚未配置 RADIUS 或 LDAP 身份验证，ASA 将忽略此命令。

    请注意，这不会更改距离密码到期的天数，而是会启用通知。如果选中此复选框，还必须指定天数。
  - Notify...days prior to expiration - 指定距离当前密码到期的天数以通知用户即将到期。范围是 1 到 180 天。

Add/Edit Tunnel Group > IPsec for LAN to LAN Access > IPsec

Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > IPSec for LAN to LAN Access > IPSec 选项卡

通过 Add or Edit Tunnel Group 对话框 > IPsec for Site-to-Site Access > IPsec 对话框，可以配置或编辑特定于 IPsec 站点间访问的隧道组参数。

字段

- Name - 指定分配给此隧道组的名称。对于 Edit 功能，此字段为仅显示。
- Type -（*仅显示*）显示进行添加或编辑的隧道组的类型。此字段的内容取决于在前一个对话框中的选择。
- Pre-shared Key - 通过它可以指定隧道组的预共享密钥的值。预共享密钥的最大长度为 128 个字符。
- Trustpoint Name - 如果配置了任何信任点，请选择信任点名称。信任点是证书颁发机构的表示。信任点包含 CA 的身份、特定于 CA 的配置参数，以及与一个已注册身份证书的关联。
- Authentication Mode = 指定身份验证模式：none、 xauth 或 hybrid。
  - none - 指定无身份验证模式。
  - xauth - 指定使用 IKE 扩展身份验证模式，它提供使用 TACACS+ 或 RADIUS 在 IKE 内对用户进行身份验证的功能。
  - hybrid - 指定使用混合模式，通过它可以使用数字证书进行安全设备身份验证，并使用其他的传统方法（如 RADIUS、TACACS+ 或 SecurID）进行远程 VPN 用户身份验证。此模式将互联网密钥交换 (IKE) 的第 1 阶段分为以下步骤，统称为混合身份验证。
    1. 安全设备使用标准公钥方法对远程 VPN 用户进行身份验证。这会建立单向身份验证的 IKE 安全关联。
    2. 然后，扩展身份验证 (xauth) 交换对远程 VPN 用户进行身份验证。此扩展身份验证可以使用其中一种受支持的传统身份验证方法。

注　在将身份验证类型设置为 hybrid 之前，必须配置身份验证服务器并创建预共享密钥。

- IKE Peer ID Validation - 选择忽略、必需还是仅在证书支持的情况下才选中 IKE 对等体 ID 验证。
- Enable sending certificate chain - 启用或禁用发送整个证书链。此操作在传输中包含根证书和任何从属 CA 证书。
- ISAKMP Keep Alive - 启用并配置 ISAKMP 保活监控。
  - Disable Keep Alives - 启用或禁用 ISAKMP 保活。
  - Monitor Keep Alives - 启用或禁用 ISAKMP 保活监控。选择此选项将使 Confidence Interval 和 Retry Interval 字段可供使用。
  - Confidence Interval - 指定 ISAKMP 保活置信区间。这是 ASA 应该允许对等体在开始保活监控之前空闲的秒数。最小值为 10 秒；最大值为 300 秒。远程访问组的默认值为 300 秒。
  - Retry Interval - 指定在 ISAKMP 保活重试之间等待的秒数。默认值为 2 秒。
  - Head end will never initiate keepalive monitoring - 指定中心站点 ASA 绝不会启动保活监控。
- Interface-Specific Authentication Mode - 逐个接口指定身份验证模式。
  - Interface - 选择指定接口。默认接口为 inside 和 outside，但是如果已配置其他接口名称，则该名称也会显示在列表中。
  - Authentication Mode - 通过它可以选择如上所述的身份验证模式：none、 xauth 或 hybrid。

  - Interface/Authentication Mode 表 - 显示选择的接口名称及其关联身份验证模式。
  - Add - 向 Interface/Authentication Modes 表中添加接口/身份验证模式对选择。
  - Remove - 从 Interface/Authentication Modes 表中移除接口/身份验证模式对选择。
- Client VPN Software Update Table - 列出安装的每个客户端 VPN 软件包的客户端类型、VPN 客户端修订版本和映像 URL。对于每个客户端类型，可以指定可接受的客户端软件修订版本以及要从其下载软件升级的 URL 或 IP 地址 （如有必要）。客户端更新机制 （在 Client Update 下进行了详细描述）使用此信息来确定每个 VPN 客户端运行的软件是否处于适当的修订级别，并在适当情况下向运行过时软件的客户端提供通知消息和更新机制。
  - Client Type - 标识 VPN 客户端类型。
  - VPN Client Revisions - 指定可接受的 VPN 客户端修订级别。
  - Image URL - 指定可以从其下载正确的 VPN 客户端软件映像的 URL 或 IP 地址。对于基于 Windows 的 VPN 客户端， URL 的格式必须为 http:// 或 https://。对于处于客户端模式下的 ASA 5505 或 VPN 3002 硬件客户端， URL 的格式必须为 tftp://。

Clientless SSL VPN Access > Connection Profiles > Add/Edit > General > Basic

Configuration > VPN > General > Tunnel Group > Add/Edit> WebVPN Access > General 选项卡 > Basic 选项卡

通过 Add/Edit 窗格 > General > Basic 对话框，可以指定进行添加的隧道组的名称，选择组策略，以及配置密码管理。

在 Edit Tunnel Group 对话框中， General 对话框显示所选隧道组的名称和类型。至于 Add Tunnel Group 对话框，所有其他功能都相同。

字段

- Name - 指定分配给此隧道组的名称。对于 Edit 功能，此字段为仅显示。
- Type - 显示进行添加或编辑的隧道组的类型。对于 Edit，这是一个仅显示字段，其内容取决于在 Add 对话框中的选择。
- Group Policy - 列出当前配置的组策略。默认值为默认组策略 DfltGrpPolicy。
- Strip the realm - 不适用于无客户端 SSL VPN。
- Strip the group - 不适用于无客户端 SSL VPN。
- Password Management - 通过它可以配置与覆盖来自 AAA 服务器的帐户已禁用指示和通知用户密码到期相关的参数。
  - Override account-disabled indication from AAA server - 覆盖来自 AAA 服务器的帐户已禁用指示。

注　允许覆盖帐户已禁用指示是一项潜在安全风险。

  - Enable notification upon password expiration to allow user to change password - 选中此复选框将使以下两个参数可用。如果没有另外选中 Enable notification prior to expiration 复选框，则用户仅在密码到期后才会接收到通知。
  - Enable notification prior to expiration - 当选中此选项时， ASA 在远程用户登录时通知其当前密码即将到期或已到期，然后为用户提供机会更改密码。如果当前密码未到期，用户仍可使用该密码登录。此参数对于支持此类通知的 AAA 服务器有效；即 RADIUS、使用 NT 服务器的 RADIUS 以及 LDAP 服务器。如果尚未配置 RADIUS 或 LDAP 身份验证，ASA 将忽略此命令。

请注意，这不会更改距离密码到期的天数，而是会启用通知。如果选中此复选框，还必须指定天数。

– Notify...days prior to expiration - 指定距离当前密码到期的天数以通知用户即将到期。范围是 1 到 180 天。

为 SSL VPN 连接配置客户端寻址

使用此对话框指定全局客户端地址分配策略和配置特定于接口的地址池。您还可以使用此对话框添加、编辑或删除特定于接口的地址池。对话框底部的表列出已配置的特定于接口的地址池。

字段

- Interface-Specific IPv4 Address Pools - 列出已配置的特定于接口的地址池。
- Interface-Specific IPv6 Address Pools - 列出已配置的特定于接口的地址池。
- Add - 打开 Assign Address Pools to Interface 对话框，可以在其中选择接口并选择要分配的地址池。
- Edit - 打开 Assign Address Pools to Interface 对话框，其中接口和地址池字段已填充。
- Delete - 删除所选的特定于接口的地址池。无确认或撤消功能。

Assign Address Pools to Interface

使用此对话框选择接口并向该接口分配一个或多个地址池。

字段

- Interface - 选择要向其分配地址池的接口。默认值为 DMZ。
- Address Pools - 指定要分配到指定接口的地址池。
- Select - 打开 Select Address Pools 对话框，可以在其中选择要向此接口分配的一个或多个地址池。选择显示在 Assign Address Pools to Interface 对话框的 Address Pools 字段中。

Select Address Pools

Select Address Pools 对话框显示可用于客户端地址分配的地址池的池名称、开始和结束地址以及子网掩码，并且使您可从该列表中添加、编辑或删除条目。

字段

- Add - 打开 Add IP Pool 对话框，可以在其中配置新 IP 地址池。
- Edit - 打开 Edit IP Pool 对话框，可以在其中修改所选 IP 地址池。
- Delete - 移除所选地址池。无确认或撤消功能。
- Assign - 显示保持分配给接口的地址池名称。双击要向接口添加的每个未分配池。Assign 字段将更新池分配列表。

添加或编辑 IP 地址池

配置或修改 IP 地址池。

字段

- Name - 指定分配给 IP 地址池的名称。
- Starting IP Address - 指定池中的第一个 IP 地址。
- Ending IP Address - 指定池中的最后一个 IP 地址。
- Subnet Mask - 选择要应用于池中的地址的子网掩码。

对 SSL VPN 连接进行身份验证

通过 SSL VPN Connections > Advanced > Authentication 对话框，可以配置 SSL VPN 连接的身份验证属性。

System Options

可以通过导航以下路径到达此面板：

- Configuration > Site-to-Site VPN > Advanced > System Options
- Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > System Options

通过 System Options 窗格，可以在 ASA 上配置特定于 VPN 会话的功能。

字段

- Limit the maximum number of active IPsec VPN sessions - 启用或禁用限制最大活动 IPsec VPN 会话数。范围取决于硬件平台和软件许可证。
  - Maximum IPsec Sessions - 指定允许的最大活动 IPsec VPN 会话数。仅当选择先前复选框以限制最大活动 IPsec VPN 会话数时，此字段才处于活动状态。
- L2TP Tunnel Keep-alive Timeout - 指定保活消息的频率（以秒为单位）。范围是 10 到 300 秒。默认值为 60 秒。这是仅适用于网络 （客户端）访问的高级系统选项。
- Reclassify existing flows when VPN tunnels establish
- Preserve stateful VPN flows when the tunnel drops - 启用或禁用在网络扩展模式 (NEM) 下保留 IPsec 隧道化流量。在启用持续 IPsec 隧道化流量功能情况下，只要在超时对话框中重新创建隧道，数据便会成功继续流动，因为安全设备仍然有权访问状态信息。默认情况下会禁用此选项。

  注　未丢弃隧道化 TCP 流量，因此其依靠 TCP 超时进行清除。但是，如果为特定隧道化流量禁用了超时，则该流量会保留在系统中，直到手动或通过其他方法 （例如，通过来自对等体的 TCP RST）清除为止。

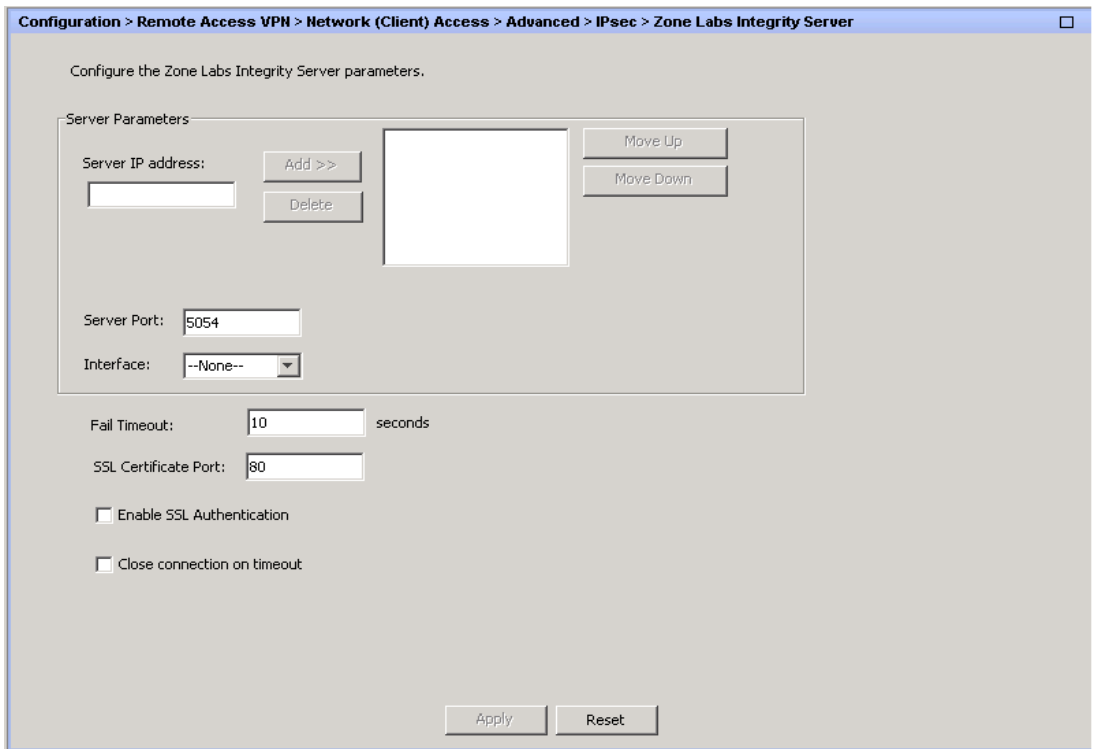
- IPsec Security Association Lifetime - 配置安全关联 (SA) 的持续时间。此参数指定 IPsec SA 密钥生存期的度量方式，即 IPsec SA 过期并必须用新的密钥重新协商前，它可以持续的时长。
  - **Time** - 根据小时 (hh)、分钟 (mm) 和秒 (ss) 指定 SA 生存期。

  - **Traffic Volume** - 根据流量的千字节数定义 SA 生存期。输入负载数据的千字节数量， IPsec SA 在达到该数量后到期，或者选择 unlimited。最小值为 100 KB，默认值为 10000 KB，最大值为 2147483647 KB。
- Enable PMTU (Path Maximum Transmission Unit) Aging - 允许管理员启用 PMTU 老化。
  - Interval to Reset PMTU of an SA (Security Association) - 输入将 PMTU 值重置为其原始值的间隔秒数。

Zone Labs Integrity 服务器

Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Zone Labs Integrity Server

通过 Zone Labs Integrity Server 面板，可以将 ASA 配置为支持 Zone Labs Integrity 服务器。此服务器是 Integrity 系统的一部分，该系统旨在进入专用网络的远程客户端上实施安全策略。实际上， ASA 充当客户端 PC 到防火墙服务器的代理，并在 Integrity 客户端和 Integrity 服务器之间中继所有必要的 Integrity 信息。



注　安全设备的当前发行版一次支持一台 Integrity 服务器，即使用户接口支持最多五台 Integrity 服务器的配置也如此。如果活动服务器发生故障，请在 ASA 上配置另一台 Integrity 服务器，然后重新建立客户端 VPN 会话。

字段

- Server IP address - 键入 Integrity 服务器的 IP 地址。使用点分十进制表示法。
- Add - 向 Integrity 服务器列表中添加新服务器 IP 地址。当在 Server IP address 字段中输入地址时，此按钮处于活动状态。
- Delete - 从 Integrity 服务器列表中删除所选服务器。
- Move Up - 将所选服务器在 Integrity 服务器列表中上移。仅当列表中有多台服务器时，此按钮才可用。
- Move Down - 将所选服务器在 Integrity 服务器列表中下移。仅当列表中有多台服务器时，此按钮才可用。
- Server Port - 键入 ASA 侦听活动 Integrity 服务器所在的端口号。仅当 Integrity 服务器列表中至少有一台服务器时，此字段才可用。默认端口号为 5054，并且其范围可以是从 10 到 10000。仅当 Integrity 服务器列表中有服务器时，此字段才可用。
- Interface - 选择 ASA 与活动 Integrity 服务器进行通信所在的接口。仅当 Integrity 服务器列表中有服务器时，此接口名称菜单才可用。
- Fail Timeout - 键入 ASA 在其声明活动 Integrity 服务器不可达之前应等待的秒数。默认值为 10，范围是从 5 到 20。
- SSL Certificate Port：指定要用于 SSL 授权的 ASA 端口。默认值为端口 80。
- Enable SSL Authentication - 选中以由 ASA 启用远程客户端 SSL 证书身份验证。默认情况下，会禁用客户端 SSL 身份验证。
- Close connection on timeout - 选中以在超时情况下关闭 ASA 和 Integrity 服务器之间的连接。默认情况下，连接保持打开。
- Apply - 点击以将 Integrity 服务器设置应用于 ASA 运行配置。
- Reset - 点击以移除尚未应用的 Integrity 服务器配置更改。

用于 AnyConnect 3.1 的 AnyConnect 基础版

AnyConnect 基础版是完全在 ASA 上配置的单独许可的 SSL VPN 客户端，提供除下列以外的完整 AnyConnect 功能：

- 没有 CSD （包括主机扫描/保管库/缓存清理器）
- 没有无客户端 SSL VPN
- 可选 Windows Mobile 支持 （需要用于 Windows Mobile 的 AnyConnect 许可证）

AnyConnect 基础版客户端为运行 Microsoft Windows Vista、 Windows Mobile、 Windows XP 或 Windows 2000、 Linux 或 Macintosh OS X 的远程最终用户提供 Cisco SSL VPN 客户端的优点：

要启用 AnyConnect 基础版，请选中 AnyConnect 基础版窗格上的 **Enable AnyConnect Essentials** 复选框，仅在 ASA 上安装了 AnyConnect 基础版许可证的情况下才会显示该复选框。

启用 AnyConnect 基础版后，AnyConnect 客户端使用 Essentials 模式，并会禁用无客户端 SSL VPN 访问。禁用 AnyConnect 基础版后， AnyConnect 客户端使用完整 AnyConnect SSL VPN 客户端。

注　Configuration > Device Management > Licensing > Activation Key 窗格上有关 AnyConnect 基础版的状态信息只是反映是否安装了 AnyConnect 基础版许可证。此状态不受 Enable AnyConnect Essentials License 复选框的设置的影响。

当设备存在活动无客户端会话时，无法启用 AnyConnect 基础版模式。要查看 SSL VPN 会话详细信息，请点击 部分中的 **Monitoring > VPN > VPN Sessions** 链接。这将打开 Monitoring > VPN > VPN > VPN Statistics > Sessions 窗格。要查看会话详细信息，请选择 **Filter By: Clientless SSL VPN** 并点击 **Filter**。这将显示会话详细信息。

要查看当前处于活动状态的无客户端 SSL VPN 会话数而不显示会话详细信息，请点击 **Check Number of Clientless SSL Sessions**。如果 SSL VPN 会话计数为零，则可以启用 AnyConnect 基础版。

注　启用 AnyConnect 基础版后， Secure Desktop 不工作。但是，可以在启用 Secure Desktop 时禁用 AnyConnect 基础版。

DTLS 设置

通过启用数据报传输层安全 (DTLS)，建立 SSL VPN 连接的 AnyConnect VPN 客户端可以使用两个同时隧道：SSL 隧道和 DTLS 隧道。使用 DTLS 可避免与某些 SSL 连接关联的延迟和带宽问题，并且改进对于数据包延迟敏感的实时应用的性能。

如果不启用 DTLS，则建立 SSL VPN 连接的 AnyConnect 客户端用户将仅与 SSL VPN 隧道进行连接。

字段

- Interface - 显示 ASA 上的接口的列表。
- DTLS Enabled - 点击以使用接口上的 AnyConnect 客户端启用 DTLS 连接。
- UDP Port （默认 443） - （可选）为 DTLS 连接指定单独的 UDP 端口。

AnyConnect VPN Client Images

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software

此窗格列出在 ASDM 中配置的 AnyConnect 客户端映像。

字段

- AnyConnect Client Images 表 - 显示在 ASDM 中配置的软件包文件，并允许确定 ASA 将映像下载到远程 PC 的顺序。
  - Add - 显示 Add AnyConnect Client Image 对话框，可以在其中将闪存中的文件指定为客户端映像文件，也可以浏览闪存以查找要指定为客户端映像的文件。您还可以将文件从本地计算机上载到闪存。
  - Replace - 显示 Replace AnyConnect Client Image 对话框，可以在其中将闪存中的文件指定为客户端映像来替换 SSL VPN Client Images 表中突出显示的映像。您还可以将文件从本地计算机上载到闪存。
  - Delete - 从表中删除映像。这不会从闪存中删除软件包文件。
  - Move Up 和 Move Down - 向上和向下箭头会更改 ASA 将客户端映像下载到远程 PC 的顺序。它首先下载表格顶部的映像。因此，应该将最常遇到的操作系统使用的映像移至顶部。

Add/Replace AnyConnect VPN Client Image

在此窗格中，可以指定 ASA 闪存中要添加为 AnyConnect 客户端映像或者替换表中已经列出的映像的文件的文件名。您也可以浏览闪存以查找要标识的文件，或者可以从本地计算机上载文件。

字段

- Flash SVC Image - 指定闪存中要标识为 SSL VPN 客户端映像的文件。
- Browse Flash - 显示 Browse Flash 对话框，可以在其中查看闪存中的所有文件。
- Upload - 显示 Upload Image 对话框，可以在其中从本地 PC 上载要标识为客户端映像的文件。
- Regular expression to match user-agent - 指定 ASA 用于与浏览器传递的 User-Agent 字符串相匹配的字符串。对于移动用户，可以使用此功能减少移动设备的连接时间。当浏览器连接到 ASA 时，它将在 HTTP 头中包含 User-Agent 字符串。当 ASA 接收到该字符串时，如果字符串与为映像配置的表达式相匹配，它将立即下载该映像而不测试其他客户端映像。

Upload Image

在此窗格中，可以指定要标识为 AnyConnect 客户端映像的文件在本地计算机上或在安全设备闪存中的路径。您也可以浏览本地计算机或安全设备闪存以查找要标识的文件。

字段

- Local File Path - 确定本地计算机上要标识为 SSL VPN 客户端映像的文件的文件名。
- Browse Local Files - 显示 Select File Path 对话框，可以在其中查看本地计算机上的所有文件，并可选择要标识为客户端映像的文件。
- Flash File System Path - 确定安全设备闪存中要标识为 SSL VPN 客户端映像的文件的文件名。
- Browse Flash - 显示 Browse Flash 对话框，可以在其中查看安全设备闪存中的所有文件，并可选择要标识为客户端映像的文件。
- Upload File - 启动文件上载。

Bypass Interface ACL

通过取消选中此复选框，可以需要适用于本地 IP 地址的访问规则。访问规则适用于本地 IP 地址，而不适用于在解密 VPN 数据包之前使用的原始客户端 IP 地址。

- 支持入站 IPsec 会话绕过接口访问列表。Group policy and per-user authorization ACLs still apply to the traffic - 默认情况下， ASA 允许在 ASA 接口上终止 VPN 流量；无需在访问规则中允许 IKE 或 ESP（或其他类型的 VPN 数据包）。选中此复选框时，也无需解密的 VPN 数据包的本地 IP 地址的访问规则。由于使用 VPN 安全机制成功终止了 VPN 隧道，因此此功能会简化配置并最大程度地提高ASA性能，而没有任何安全风险。（组策略和逐个用户授权 ACL 仍然适用于流量。）

AnyConnect 主机扫描映像

Configuration > Remote Access VPN > Host Scan Image

AnyConnect 状态模块为 AnyConnect 安全移动客户端提供标识主机上安装的操作系统、防病毒软件、防间谍软件和防火墙软件的能力。主机扫描应用会收集此信息。

主机扫描支持图表包含您在安全状态策略中使用的防病毒应用、防间谍软件应用和防火墙应用的产品信息及版本信息。我们在主机扫描软件包中提供主机扫描和主机扫描支持图表以及其他组件。

本章包含以下各节：

主机扫描依赖关系和系统要求

具有安全状态模块的 AnyConnect 安全移动客户端需要以下最低版本 ASA 组件：

- ASA 8.4
- ASDM 6.4

这些 AnyConnect 功能要求安装安全状态模块。

- SCEP 身份验证
- AnyConnect 遥测模块

系统要求

安全状态模块可以安装在以下任何平台上：

- Windows XP （x86 和在 x64 上运行的 x86）
- Windows Vista （x86 和在 x64 上运行的 x86）
- Windows 7 （x86 和在 x64 上运行的 x86）
- Mac OS X 10.5 和 10.6 （32 位和在 64 位上运行的 32 位）
- Linux （32 位和在 64 位上运行的 32 位）
- Windows Mobile

许可

以下是安全状态模块的 AnyConnect 许可要求：

- 用于基本主机扫描的 AnyConnect 基础版。
- 以下功能必需高级终端评估许可证
  - 补救
  - 移动设备管理

输入激活密钥以支持高级终端评估

高级终端评估包括所有终端评估功能，并允许配置对于将不相容计算机更新为符合版本要求的尝试。您可以在从思科获取密钥后使用 ASDM 将其激活来支持高级终端评估，如下所示：

步骤 1　选择 **Configuration > Device Management > Licensing > Activation Key**。

步骤 2　在 **New Activation Key** 字段中输入密钥。

步骤 3　点击 **Update Activation Key**。

步骤 4　选择 **File > Save Running Configuration to Flash**。

系统将显示高级终端评估条目，并且 Configure 按钮在 **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan** 窗格的 Host Scan Extensions 区域中会激活，仅在启用 CSD 的情况下才可访问该区域。

主机扫描包装

您可以通过以下方式之一将主机扫描软件包加载到 ASA 上：

- 可以将其作为独立软件包上载：**hostscan-*version*.pkg**
- 可以通过上载 AnyConnect 安全移动软件包来将其上载：**anyconnect-win-*version*-k9.pkg**
- 可以通过上载 Cisco Secure Desktop 软件包来将其上载：**csd_version-k9.pkg**

文件	说明
hostscan-*version*.pkg	此文件包含主机扫描软件以及主机扫描库和支持图表。
anyconnect-NGC-win-*version*-k9.pkg	此软件包包含所有 Cisco AnyConnect 安全移动客户端功能，包括 hostscan-*version*.pkg 文件。
csd_*version*-k9.pkg	此文件包含所有 Cisco Secure Desktop 功能，包括主机扫描软件以及主机扫描库和支持图表。 此方法需要单独的适用于 Cisco Secure Desktop 的许可证。

在 ASA 上安装并启用主机扫描

安装或升级主机扫描

使用此操作步骤在 ASA 上上载或升级及启用新的主机扫描映像。此映像可以启用 AnyConnect 的主机扫描功能，也可以使用其升级 Cisco Secure Desktop (CSD) 的现有部署的主机扫描支持图表。

可以在字段中指定独立主机扫描软件包或 AnyConnect 安全移动客户端 3.0 版或更高版本的软件包。

如果以前将 CSD 映像上载到 ASA，则指定的主机扫描映像将升级或降级该 CSD 软件包随附的现有主机扫描文件。

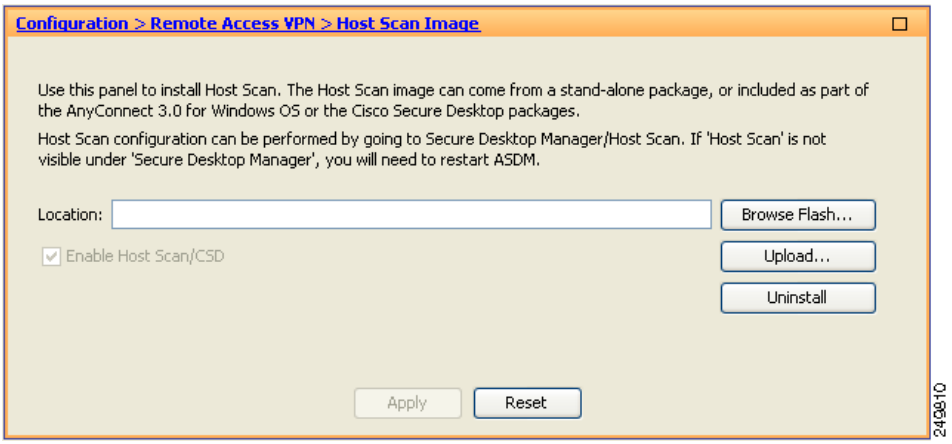
在安装或升级主机扫描之后，无需重新启动安全设备；但是，必须退出并重新启动自适应安全设备管理器 (ASDM) 才能访问 Secure Desktop Manager。

注　主机扫描需要 AnyConnect 安全移动客户端高级许可证。

步骤 1　将 **hostscan_*version*-k9.pkg** 文件或 **anyconnect-NGC-win-*version*-k9.pkg** 文件下载到计算机。

步骤 2　打开 ASDM 并选择 **Configuration > Remote Access VPN > Host Scan Image**。ASDM 将打开 Host Scan Image 面板。

图 3-7　　Host Scan Image 面板



步骤 3　点击 **Upload** 以准备将主机扫描软件包的副本从计算机传输到 ASA 上的驱动器。

步骤 4　在 Upload Image 对话框中，点击 **Browse Local Files** 以在本地计算机上搜索主机扫描软件包。

步骤 5　选择在第 1 步中下载的 **hostscan_*version*.pkg** 文件或 **anyconnect-NGC-win-*version*-k9.pkg** 文件，然后点击 **Select**。您选择的文件的路径在 Local File Path 字段中，并且 Flash File System Path 字段反映主机扫描软件包的目标路径。如果 ASA 具有多个闪存驱动器，则可以编辑 Flash File System Path 以指示其他闪存驱动器。

步骤 6　点击 **Upload File**。 ASDM 会将文件的副本传输到闪存卡。 Information 对话框显示以下消息：

```
File has been uploaded to flash successfully。
```

步骤 7　点击 **OK**。

步骤 8　在 Use Uploaded Image 对话框中，点击 **OK** 以使用刚上载的主机扫描软件包作为当前映像。

步骤 9　如果尚未选中 **Enable Host Scan/CSD**，请将其选中。

步骤 10　点击 **Apply**。

注　如果在 ASA 上启用 AnyConnect 基础版，您会接收到一条消息，表明 CSD 将不与其配合使用。可以选择 **Disable** 或 **Keep** AnyConnect 基础版。

步骤 11　从 File 菜单中，选择 **Save Running Configuration To Flash**。

启用或禁用主机扫描

首次使用 ASDM 安装或升级主机扫描映像时，可以在该操作步骤过程中启用此映像。请参阅第 3-85 页上的在 ASA 上安装并启用主机扫描。

否则，要使用 ASDM 启用或禁用主机扫描映像，请遵循以下操作步骤：

步骤 1　打开 ASDM 并选择 **Configuration > Remote Access VPN > Host Scan Image**。ASDM 将打开 Host Scan Image 面板 （图 3-7）。

步骤 2　选中 **Enable Host Scan/CSD** 以启用主机扫描，或者取消选中 **Enable Host Scan/CSD 以禁用主机扫描。**

步骤 3　点击 **Apply**。

在 ASA 上启用或禁用 CSD

启用 CSD 会将 CSD 配置文件 data.xml 从闪存设备加载到运行配置。

禁用 CSD 不会修改 CSD 配置。

请按如下使用 ASDM 启用或禁用 CSD：

步骤 1　选择 **Configuration > Clientless SSL VPN > Secure Desktop > Setup**。

ASDM 将打开 Setup 窗格 （图 3-7）。

注　Secure Desktop Image 字段显示当前安装的映像（和版本）。 Enable Secure Desktop 复选框指示是否启用 CSD。

步骤 2　选中或取消选中 **Enable Secure Desktop**，然后点击 **Apply**。

ASDM 将启用或禁用 CSD。

步骤 3　点击 ASDM 窗口右上角的 **X** 以退出。

窗口将显示以下消息：

```
The configuration has been modified. Do you want to save the running configuration to
flash memory?
```

步骤 4　点击 **Save**。 ASDM 保存配置并关闭。

查看 ASA 上启用的主机扫描版本

步骤 1　打开 ASDM 并导航到 **Configuration > Remote Access VPN > Host Scan Image**。

如果有在 Host Scan Image Location 字段中指定的主机扫描映像，并且选中 Enable HostScan/CSD 框，则该映像的版本是 ASA 使用的主机扫描版本。

如果 Host Scan Image 字段为空，并且选中 Enable HostScan/CSD 框，请导航到 **Configuration > Remote Access VPN > Secure Desktop Manager**。 Secure Desktop Image Location 字段中的 CSD 版本是 ASA 使用的主机扫描版本。

卸载主机扫描

卸载主机扫描软件包会在 ASDM 界面上将其隐藏并防止 ASA 对其进行部署，即使启用主机扫描或 CSD 也如此。卸载主机扫描不会从闪存驱动器中删除主机扫描软件包。

请按如下卸载安全设备上的主机扫描：

步骤 1　打开 ASDM 并导航到 **Configuration > Remote Access VPN > Host Scan Image**。

步骤 2　在 Host Scan Image 窗格中，点击 **Uninstall**。 ASDM 将从 Location 文本框中移除文本。

步骤 3　从 File 菜单中，选择 **Save Running Configuration to Flash**。

从 ASA 卸载 CSD

卸载 CSD 会将 CSD 配置文件 data.xml 从闪存卡上的 desktop 目录中删除。如果要保留文件，请使用备用名称复制该文件或将其下载到工作站，然后再卸载 CSD。

请按如下卸载安全设备上的 CSD：

步骤 1　打开 ASDM 并选择 **Configuration > Remote Access VPN > Secure Desktop Manager > Setup**。

ASDM 将打开 Setup 窗格 （图 3-7）。

步骤 2　点击 **Uninstall**。

确认窗口将显示以下消息：

```
Do you want to delete disk0:/csd_<n>.<n>.*.pkg and all CSD data files?
```

步骤 3　点击 **Yes**。

ASDM 将从 Location 文本框中移除文本，并且移除 Setup 下方的 Secure Desktop Manager 菜单选项。

步骤 4　点击 ASDM 窗口右上角的 **X** 以退出。

窗口将显示以下消息：

```
The configuration has been modified. Do you want to save the running configuration to
flash memory?
```

步骤 5　点击 **Save**。 ASDM 保存配置并关闭。

将 AnyConnect 安全状态模块分配到组策略

步骤 1　打开 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**。

步骤 2　在 Group Policies 面板中，点击 **Add** 以创建新的组策略，或者选择要将主机扫描软件包分配到的现有组策略并点击 **Edit**。

步骤 3　在 Edit Internal Group Policy 面板中，展开面板左侧的 **Advanced** 导航树，然后选择 **AnyConnect Client**。

步骤 4　取消选中 Optional Client Modules to Download **Inherit** 复选框。

步骤 5　在 Optional Client Modules to Download 下拉菜单中，选中 AnyConnect Posture Module 并点击 **OK**。

步骤 6　点击 **OK**。

其他重要文档寻址主机扫描

一旦主机扫描从终端计算机收集安全状态凭证，您就将需要了解诸如配置预登录策略、配置动态访问策略以及使用 Lua 表达式利用信息之类的主题。

以下文档中详细涵盖这些主题：

- 《Cisco Secure Desktop 配置指南》
- 《Cisco 自适应安全设备管理器配置指南》

另请参阅《*Cisco AnyConnect 安全移动客户端管理员指南，发行版 3.0*》以获取有关主机扫描如何与 AnyConnect 客户端配合工作的详细信息。

配置最大 VPN 会话数

要指定允许的最大 VPN 会话数或 AnyConnect 客户端 VPN 会话数，请执行以下步骤：

步骤 1　选择 **Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions**。

步骤 2　在 Maximum AnyConnect Sessions 字段中，输入允许的最大会话数。

有效值范围为从 1 到许可证允许的最大会话数。

步骤 3　在 Maximum Other VPN Sessions 字段中，输入允许的最大 VPN 会话数，其中包括 Cisco VPN 客户端 (IPsec IKEv1) LAN 到 LAN VPN 会话和无客户端 SSL VPN 会话。

有效值范围为从 1 到许可证允许的最大会话数。

步骤 4　点击 **Apply**。

配置加密核心池

可以在对称多处理 (SMP) 平台上更改加密核心的分配，以提高 AnyConnect TLS/DTLS 流量的吞吐量性能。这些更改可以加速 SSL VPN 数据路径，并在 AnyConnect、智能隧道和端口转发方面提供客户可见的性能提升。要配置加密核心池，请执行以下步骤。

限制

- 加密核心再平衡在以下平台上可用：
  - 5585-X
  - 5545-X
  - 5555-X
  - ASASM

步骤 1　选择 **Configuration > Remote Access VPN > Advanced > Crypto Engine**。

步骤 2　从 Accelerator Bias 下拉菜单中，选择以下之一：

注　仅当此功能在 ASA 中可用时，才会显示此字段。

- **balanced** - 平均分配加密硬件资源 （Admin/SSL 和 IPsec 核心）。
- **ipsec** - 将加密硬件资源优先分配给 IPsec （包括 SRTP 加密语音流量）。
- **ssl** - 将加密硬件资源优先分配给 Admin/SSL。

步骤 3　点击 **Apply**。

	命令	用途
步骤 1	`asa1(config)# crypto engine ?` `asa1(config)# crypto engine accelerator-bias ?`	指定如何分配密码加速器处理器： • balanced - 平均分配加密硬件资源 • ipsec - 将加密硬件资源优先分配给 IPsec/加密语音 (SRTP) • ssl - 将加密硬件资源优先分配给 SSL

配置 ISE 策略实施

思科身份服务引擎 (ISE) 是一个安全策略管理和控制平台。它可自动化并简化有线连接、无线连接和 VPN 连接的访问控制和安全合规性。思科 ISE 主要用于与 Cisco TrustSec 结合提供安全访问和来宾访问，支持 BYOD 计划和实施使用策略。

ISE 授权变更 (CoA) 功能提供一种机制在建立身份验证、授权和记帐 (AAA) 会话后更改其属性。当 AAA 中的用户或用户组的策略发生更改时，可以将 CoA 数据包从 ISE 直接发送到 ASA，以重新初始化身份验证并应用新策略。不再需要内联安全状态实施点 (IPEP) 来为与 ASA 建立的每个 VPN 会话应用访问控制列表 (ACL)。

在以下 VPN 客户端上支持 ISE 策略实施：

- IPSec
- AnyConnect
- L2TP/IPSec

系统流程如下：

1. 最终用户请求 VPN 连接。
2. ASA 向 ISE 对用户进行身份验证，并且接收提供有限网络访问的用户 ACL。
3. 系统向 ISE 发送记帐启动消息以注册会话。
4. 直接在 NAC 代理和 ISE 之间进行安全状态评估。此过程对于 ASA 是透明的。
5. ISE 通过 CoA “策略推送”向 ASA 发送发送策略更新。这将标识提供提高的网络访问特权的新用户 ACL。

注　在连接的生存期内，可能会通过后续 CoA 更新进行对于 ASA 而言透明的其他策略评估。

为授权变更配置 AAA 服务器组

以下步骤显示授权变更配置的示例。

步骤 1　在 ASDM 中，选择 **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**

步骤 2　使用 RADIUS 协议创建或编辑现有 AAA 服务器组。

步骤 3　选择 **Accounting Mode** 类型 **Single**。

步骤 4　选择 **Reactivation Mode** 类型 **Depletion**。

步骤 5　在 **Dead Time** 字段中，输入 **10**。

步骤 6　在 **Max Failed Attempts** 字段中，输入 **3**。

步骤 7　选中 **Enable Interim Accounting Update** 复选框。

步骤 8　在 **Update Interval** 字段中，输入 **1**。

步骤 9　确保未选中 **Enable Active Directory Agent Mode** 复选框。

步骤 10　选中 **Enable Dynamic Authorization** 复选框。

步骤 11　在 **Dynamic Authorization Port** 字段中，输入 **1700**。

步骤 12　选中 **Use Authorization Only Mode** 复选框。

步骤 13　点击 **OK** 以应用更改。或者，点击 **Cancel** 放弃更改。

有关详细信息，请参阅常规操作配置指南中的 “为 AAA 配置 RADIUS 服务器”。

为 AnyConnect 配置 AAA 服务器可选步骤

如果使用的是 AnyConnect，还必须在该隧道组的 **AnyConnect Connection Profile** 屏幕中指定隧道组 URL：

步骤 1　导航到所需隧道组的 **AnyConnect Connection Profile** 屏幕。

步骤 2　在 **Group URLs** 部分中，点击 **Add** 并输入 URL，例如 http://10.10.10.4/ISE-Tunnel-Group。

步骤 3　确保选中 **Enabled** 复选框。

步骤 4　点击 **OK** 以应用更改。

注　有关此功能的疑难解答信息，请参阅VPN 配置指南中的 “配置 ISE 策略实施”一节。

VPN 的 IP 地址

本章介绍 IP 地址分配方法。

IP 地址使互联网络连接成为可能。它们就像电话号码：发送方和接收方必须具有要连接的分配号码。但是，对于 VPN，实际上存在两组地址：第一组连接公用网络的客户端和服务器。连接建立后，第二组通过 VPN 隧道连接客户端和服务器。

在 ASA 地址管理方面，我们处理第二组的 IP 地址：这些专用 IP 地址通过隧道与具有专用网络资源的客户端连接，并且让客户端的运行看起来像直接连接至专用网络一样。此外，我们仅处理分配给客户端的专用 IP 地址。分配给专用网络上其他资源的 IP 地址是您的网络管理职责而非 VPN 管理的一部分。因此，当我们在这里讨论 IP 地址时，我们是指让客户端用作隧道终端的专用网络寻址方案中可用的 IP 地址。

配置 IP 地址分配策略

ASA 可使用以下一种或多种方法将 IP 地址分配给远程访问客户端。如已配置多个地址分配方法，则 ASA 将搜索每一个选项，直到找到一个 IP 地址为止。默认情况下，所有方法均已启用。

- 使用身份验证服务器 - 从外部身份验证、授权和记帐服务器逐个用户检索 IP 地址。如在使用已配置 IP 地址的身份验证服务器，我们建议使用此方法。可在 Configuration > AAA Setup 窗格中配置 AAA 服务器。此方法适用于 IPv4 和 IPv6 分配策略。
- 使用 DHCP - 从 DHCP 服务器获取 IP 地址。如要使用 DHCP，则必须配置 DHCP 服务器。还必须定义 DHCP 服务器可使用的 IP 地址范围。如果使用 DHCP，请在 Configuration > Remote Access VPN > DHCP Server 窗格中配置服务器。此方法适用于 IPv4 分配策略。
- **使用内部地址池** - 内部配置的地址池是配置地址池分配的最简单方法。如果使用此方法，请在 Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools 窗格中配置 IP 地址池。此方法适用于 IPv4 和 IPv6 分配策略。
  - 在 IP 地址释放的一段时间之后允许重新使用 IP 地址，在 IP 地址返回到地址池之后会延迟重新使用它。添加延迟有助于在 IP 地址快速重新分配后防止防火墙可能遇到的问题。默认情况下，已取消选中该选项，表示 ASA 将不强制执行延迟。如果需要延迟，请选中此框并输入介于 1 与 480 之间的分钟数以延迟 IP 地址重新分配。此可配置元素适用于 IPv4 分配策略。

使用以下方法之一指定将 IP 地址分配给远程访问客户端的方法。

使用 ASDM 配置 IP 地址分配选项

步骤 1　**选择 Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy**

步骤 2　在 IPv4 Policy 区域 中，请选中地址分配方法以将其启用，或取消选中以将其禁用。默认情况下，这些方法已启用：

- 使用身份验证服务器。启用已配置的验证、授权和记帐 (AAA) 服务器，以提供 IP 地址。
- 使用 DHCP。启用已配置的动态主机配置协议 (DHCP) 服务器，以提供 IP 地址。
- 使用内部地址池：启用在 ASA 上配置的本地地址池。

如果启用 **Use internal address pools**，则也可在 IPv4 地址释放后重新使用它。可指定 0 至 480 分钟的时间范围，过了这段时间，就可重新使用 IPv4 地址。

步骤 3　在 IPv6 Policy 区域 中，请选中地址分配方法以将其启用，或取消选中以将其禁用。默认情况下，这些方法已启用：

- 使用身份验证服务器。启用已配置的验证、授权和记帐 (AAA) 服务器，以提供 IP 地址。
- 使用内部地址池：启用在 ASA 上配置的本地地址池。

步骤 4　点击 **Apply**。

步骤 5　点击 **OK**。

模式

下表显示了此功能可用的模式：

防火墙模式		安全情景		
			多个	
路由	透明	单个	情景	系统
•	—	•	—	—

查看地址分配方法

使用以下方法之一查看在 ASA 上配置的地址分配方法：

使用 ASDM 查看 IPv4 和 IPv6 地址分配

选择 **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy**

配置本地 IP 地址池

要配置 VPN 远程访问隧道的 IPv4 或 IPv6 地址池，请打开 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add/Edit IP Pool**。要删除地址池，请打开 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools**。选择要删除的地址池，然后点击 **Delete**。

ASA 根据连接配置文件或连接的组策略使用地址池。池的指定顺序非常重要。如已为连接配置文件或组策略配置多个地址池，则 ASA 将按您向 ASA 添加地址池的顺序使用地址池。

如果从非本地子网分配地址，我们建议添加位于子网边界的池，从而可更轻松地添加这些网络的路由。

使用下列方法之一配置本地 IP 地址池：

- 第 4-3 页上的使用 ASDM 配置本地 IPv4 地址池
- 第 4-4 页上的使用 ASDM 配置本地 IPv6 地址池

使用 ASDM 配置本地 IPv4 地址池

IP Pool 区域按名称显示已配置地址池及其 IP 地址范围，例如 10.10.147.100 至 10.10.147.177。如果池不存在，该区域为空。 ASA 按所列顺序使用这些池：如果第一个池中的所有地址已分配，则它使用下一个池，以此类推。

如果从非本地子网分配地址，我们建议添加位于子网边界的池，从而可更轻松地添加这些网络的路由。

步骤 1　**选择 Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools。**

步骤 2　要添加 IPv4 地址，请点击 **Add > IPv4 Address pool**。要编辑现有地址池，请选择地址池表中的地址池，然后点击 **Edit**。

步骤 3　在 Add/Edit IP Pool 对话框中输入以下信息：

- 池名称 - 输入地址池的名称。最多可包含 64 个字符
- 起始地址 - 输入每个已配置池中可用的第一个 IP 地址。使用点分隔的十进制符号，例如：10.10.147.100。
- 结束地址 - 输入每个已配置池中可用的最后一个 IP 地址。使用点分隔的十进制符号，例如：10.10.147.177。
- 子网掩码 - 标识此 IP 地址池所驻留的子网掩码。

步骤 4　点击 **Apply**。

步骤 5　点击 **OK**。

使用 ASDM 配置本地 IPv6 地址池

IP Pool 区域按名称显示已配置地址池，及其起始 IP 地址范围、地址前缀和可在池中配置的地址数量。如果池不存在，该区域为空。ASA 按所列顺序使用这些池：如果第一个池中的所有地址已分配，则它使用下一个池，以此类推。

如果从非本地子网分配地址，我们建议添加位于子网边界的池，从而可更轻松地添加这些网络的路由。

步骤 1　**选择 Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools。**

步骤 2　要添加 IPv6 地址，请点击 **Add > IPv6 Address pool**。要编辑现有地址池，请选择地址池表中的地址池，然后点击 **Edit**。

步骤 3　在 Add/Edit IP Pool 对话框中输入以下信息：

- 名称 - 显示每个已配置地址池的名称。
- 起始 IP 地址 - 输入已配置池中可用的第一个 IP 地址。例如：2001:DB8::1。
- 前缀长度 - 输入 IP 地址前缀长度 （位数）。例如 32 表示 CIDR 表示法的 /32。前缀长度定义 IP 地址池所驻留的子网。
- 地址数量 - 标识池中从起始 IP 地址开始的 IPv6 地址的数量。

步骤 4　点击 **Apply**。

步骤 5　点击 **OK**。

配置 DHCP 寻址

要使用 DHCP 为 VPN 客户端分配地址，必须首先配置 DHCP 服务器和 DHCP 服务器可使用的 IP 地址范围。然后根据连接配置文件定义 DHCP 服务器。或者，也可在与连接配置文件或用户名相关的组策略中定义 DHCP 网络范围。它可能是 IP 网络编号，也可能是 IP 地址，用于向 DHCP 服务器标识要使用的 IP 地址池。

以下示例为名为 **firstgroup** 的连接配置文件定义 IP 地址为 172.33.44.19 的 DHCP 服务器。它们还为名为 **remotegroup** 的组策略将 DHCP 网络范围定义为 192.86.0.0。（名为 remotegroup 的组策略与名为 firstgroup 的连接配置文件关联）。如不定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将经过各个池，直到其发现未分配的地址为止。

以下配置包括多个绝对需要执行的步骤，在这些步骤中，您可能已将连接配置文件类型命名和定义为远程访问，并将组策略命名和标识为内部或外部。这些步骤会在以下示例中作为一则提醒显示，提示您只有先设置这些值，然后才有权访问后续命令 tunnel-group 和 group-policy。

准则和限制

您只能使用 IPv4 地址标识要分配客户端地址的 DHCP 服务器。

使用 DHCP 分配 IP 地址。

配置 DHCP 服务器，然后创建使用这些服务器的组策略。当用户选择该组策略时， DHCP 服务器将为 VPN 连接分配地址。

配置 DHCP 服务器

无法使用 DHCP 服务器将 IPv6 地址分配给 AnyConnect 客户端，

步骤 1　**使用 ASDM 连接至 ASA。**

步骤 2　确认已在 Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy 中启用 DHCP。

步骤 3　通过选择 Configuration > Remote Access VPN > DHCP Server 配置 DHCP 服务器。

将 DHCP IP 寻址分配给组策略

步骤 1　**选择 Configuration > Remote Access VPN > Network (Client) Access> AnyConnect Connection Profiles。**

步骤 2　在 Connection Profiles 区域中，点击 **Add** 或 **Edit**。

步骤 3　在连接配置文件的配置树中，点击 **Basic**。

步骤 4　在 Client Address Assignment 区域中，输入要用于向客户端分配 IP 地址的 DHCP 服务器的 IPv4 地址。例如， **172.33.44.19**。

步骤 5　编辑与连接配置文件关联的组策略，以定义 DHCP 范围。选择 **Configuration > Remote Access VPN > Network (Client) Access> Group Policies**。

步骤 6　双击要编辑的组策略。

步骤 7　在配置树中点击 **Servers**。

步骤 8　通过点击向下箭头，展开 **More Options** 区域。

步骤 9　取消选中 DHCP 范围 **Inherit**。

步骤 10　输入用于向 DHCP 服务器标识要使用的 IP 地址池的 IP 网络编号或 IP 地址。例如， **192.86.0.0**。

步骤 11　点击 **OK**。

步骤 12　点击 **Apply**。

将 IP 地址分配给本地用户

可将本地用户帐户配置为使用组策略，且可配置某些 AnyConnect 属性。当 IP 地址的其他源出现故障时，这些用户帐户将提供回退，以便管理员仍有访问权限。

本小节介绍如何为本地用户配置所有属性。

先决条件

此操作步骤描述如何编辑现有用户。要添加用户，请选择 **Configuration > Remote Access VPN > AAA/Local Users > Local Users**，然后点击 **Add**。有关详细信息，请参阅常规操作配置指南。

默认情况下，对于 Edit User Account 屏幕上的每项设置，均将选中 **Inherit** 复选框，这表明用户帐户从默认组策略 DfltGrpPolicy 继承该设置的值。

要覆盖每项设置，请取消选中 **Inherit** 复选框，并输入新值。下面的详细步骤介绍 Edit User Account 屏幕上的每项设置。

步骤 1　**启动 ASDM 并选择 Configuration > Remote Access VPN > AAA/Local Users > Local Users。**

步骤 2　选择要配置的用户，然后点击 **Edit**。

步骤 3　在左侧窗格中，点击 **VPN Policy**。

步骤 4　为该用户指定一个组策略。用户策略继承该组策略的属性。如果此屏幕中的其他字段设置为从 Default Group Policy **继承**配置，则此组策略中指定的属性优先于 Default Group Policy 中的属性。

步骤 5　指定可供用户使用的隧道协议，或是否从组策略继承值。选中所需的 **Tunneling Protocols** 复选框，以选择可供使用的 VPN 隧道协议。仅所选协议可供使用。选项如下：

- 无客户端 SSL VPN（通过 SSL/TLS 的 VPN）使用网络浏览器建立与 VPN 集中器连接的安全远程访问隧道；不需要软件和硬件客户端。无客户端 SSL VPN 可提供广泛企业资源的便捷访问，包括企业网站、支持网络的应用程序、NT/AD 文件共享（支持网络）、邮件和几乎任何计算机中的可访问 HTTPS 互联网网站的其他基于 TCP 的应用程序。
- IPsec IKEv1 - IP 安全协议。 IPsec 被视为最安全的协议，为 VPN 隧道提供最完整的架构。站点到站点（对等网络）连接使用 IPsec IKEv1。
- IPsec IKEv2 - AnyConnect 安全移动客户端支持的 IPsec IKEv2。组合使用 IPsec 与 IKEv2 的 AnyConnect 连接能够利用向 SSL VPN 连接提供的相同功能集。
- 采用互联网协议安全的第二层隧道协议允许具有若干公共 PC 和移动 PC 操作系统的随附的 VPN 客户端远程用户通过公用 IP 网络与 ASA 和专用企业网络建立安全连接。

注　如未选择协议，系统会显示错误消息。

步骤 6　指定要使用的过滤器（IPv4 或 IPv6），或者是否从组策略继承值。过滤器由规则组成，这些规则根据诸如源地址、目标地址和协议之类的条件来确定允许还是拒绝隧道数据包通过 ASA。要配置过滤器和规则，请选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > General > More Options > Filter**。

点击 **Manage** 以显示 ACL Manager 窗格，可以在其中添加、编辑及删除 ACL 和 ACE。

步骤 7　指定继承连接配置文件（隧道组）锁定还是使用所选隧道组锁定（如果有）。选择特定锁定会限定用户只能通过此组进行远程访问。隧道组锁定通过检查在 VPN 客户端上配置的组是否与用户分配的组相同来限制用户。如果不相同，ASA 将阻止用户进行连接。如果未选中 Inherit 复选框，则默认值为 None。

步骤 8　指定是否从该组继承 Store Password on Client System 设置。取消选中 **Inherit** 复选框以激活 Yes 和 No 单选按钮。点击 **Yes**，将登录密码存储在客户端系统上 （可能是不太安全的选项） 。点击 **No** （默认）以要求用户输入每个连接的密码。为确保最高安全性，我们建议您 *不允许*密码存储。

步骤 9　指定要应用于此用户的访问时长策略，为用户创建新的访问时长策略，或者保持选中 Inherit 框。默认值为 Inherit，或者，如果未选中 Inherit 复选框，则默认值为 Unrestricted。

点击 **Manage** 以打开 Add Time Range 对话框，可以在其中指定一组新的访问时长。

步骤 10　按用户指定同时登录数。 Simultaneous Logons 参数指定允许该用户执行的最多同时登录数。默认值为 3。最小值为 0，表示禁止登录并阻止用户访问。

注　在没有最大限制时，允许多个同时连接可能会降低安全性并影响性能。

步骤 11　为用户连接时间指定**最大连接时间** （以分钟为单位）。此时间结束时，系统会终止连接。最小值为 1 分钟，最大值为 2147483647 分钟 （4000 多年）。要允许无限连接时间，请选中 **Unlimited** 复选框（默认）。

步骤 12　指定用户的空闲超时 （以分钟为单位）。如果在此期间连接上没有该用户的通信活动，系统就会终止连接。最短时间为 1 分钟，最长时间为 10080 分钟。该值不适用于无客户端 SSL VPN 连接的用户。

步骤 13　配置会话警报间隔。如果取消选中 Inherit 复选框，则自动选中 Default 复选框。这将会话警报间隔设置为 30 分钟。如果您要指定新值，可以取消选中 Default 复选框，并在分钟框中指定 1 至 30 分钟的会话警报间隔。

步骤 14　配置空闲警报间隔。如果取消选中 Inherit 复选框，则自动选中 Default 复选框。这会将空闲警报间隔设置为 30 分钟。如果您要指定新值，可以取消选中 Default 复选框，并在分钟框中指定 1 至 30 分钟的会话警报间隔。

步骤 15　要为此用户设置专用 IPv4 地址，请在 Dedicated IPv4 Address (Optional) 区域中输入 IPv4 地址和子网掩码。

步骤 16　要为此用户设置专用 IPv6 地址，请在 Dedicated IPv6 Address (Optional) 区域中输入一个带 IPv6 前缀的 IPv6 地址。 IPv6 前缀表示 IPv6 地址所驻留的子网。

步骤 17　要配置无客户端 SSL 设置，请在左侧格中点击 **Clientless SSL VPN**。要覆盖每项设置，请取消选中 **Inherit** 复选框，并输入新值。

步骤 18　点击 **Apply**。

更改会保存到运行配置。

动态访问策略

本章介绍如何配置动态访问策略。其中包括以下部分

关于动态访问策略

VPN 网关在动态环境下运行。许多可变因素都可能会影响 VPN 连接，例如，频繁更改的内联网配置、每个用户在组织中可能有不同的角色，以及使用不同配置和安全级别从远程访问站点进行的登录。授权用户的任务在 VPN 环境中，比在采用静态配置的网络中要复杂得多。

ASA 上的动态访问策略 (DAP)，允许您配置解决这些众多可变因素的授权。您可以设置一个与特定用户隧道或会话关联的访问控制属性集合，从而创建动态访问策略。这些属性可解决多重组成员资格和终端安全的问题。即， ASA 会根据您定义的策略，为特定的会话向特定用户授予访问权限。从一个或多个 DAP 记录选择和/或汇聚属性时，该 ASA 会生成一个 DAP。它会根据远程设备的终端安全信息，以及经过身份验证的用户的 AAA 授权信息，选择这些 DAP 记录。然后它会将 DAP 记录应用至用户隧道或会话。

DAP 系统包含需要您注意的以下组件：

- DAP Selection Configuration File - 一个文本文件，该文件包含会话建立期间，ASA 用于选择和应用 DAP 记录的条件。该文件存储在 ASA 之上。您可以使用 ASDM 对其进行修改，并以 XML 数据格式上传至 ASA。 DAP 选择配置文件包含您配置的所有属性。这些属性包括 AAA 属性、终端属性、在网络和网络类型 ACL 过滤器中配置的访问策略、端口转发以及 URL 列表。
- DfltAccess Policy - 始终是 DAP 摘要表中的最后一个条目，而且优先级始终为 0。您可以配置默认访问策略的访问策略属性，但是它不包含而且您也无法配置 AAA 或终端属性。您不能删除 DfltAccessPolicy，它必须是摘要表中的最后一个条目。

有关详细信息，请参阅 *《动态访问部署指南》*(https://supportforums.cisco.com/docs/DOC-1369)。

远程访问协议的 DAP 支持和状态评估工具

ASA 通过使用您配置的状态评估工具来获取终端安全属性。这些状态评估工具包括 AnyConnect 状态模块、独立主机扫描软件包、思科安全桌面和 NAC。

下表确定了 DAP 支持的每个远程访问协议、可用于该方法的状态评估工具，以及该工具提供的信息。

受支持的 远程访问协议	**AnyConnect 状态模块 主机扫描包 思科安全桌面 （不启用终端评估主机扫描 扩展）** 返回文件信息、注册表项值、运行的进程、操作系统	**AnyConnect 状态模块 主机扫描包 思科安全桌面 （启用终端评估主机扫描 扩展）** 返回防病毒、反间谍软件和个人防火墙软件信息	**NAC** 返回 NAC 状态	**思科 NAC 设备** 返回 VLAN 类型和 VLAN ID
IPSec VPN	否	否	是	是
思科 AnyConnect VPN	是	是	是	是
无客户端 （基于浏览器的） SSL VPN	是	是	否	否
PIX 直通代理 （状况评估不可用）	否	否	否	否

使用 DAP 的远程访问连接操作序列

以下操作序列概述典型远程访问连接的建立。

1. 远程客户端会尝试 VPN 连接。
2. ASA 使用配置的 NAC 和思科安全桌面主机扫描值执行状态评估。
3. ASA 通过 AAA 对用户进行身份验证。 AAA 服务器还会返回该用户的授权属性。
4. ASA 将 AAA 授权属性应用至该会话，并建立 VPN 隧道。
5. ASA 根据用户 AAA 授权信息和会话状态评估信息选择 DAP 记录。
6. ASA 汇聚选定 DAP 记录中的 DAP 属性，随后它们会成为 DAP 策略。
7. ASA 将 DAP 策略应用至该会话。

动态访问策略许可

注　此功能在无负载加密型号上不可用。

型号	许可证要求
ASAv	高级许可证
所有其他型号	AnyConnect 高级许可证 高级终端评估许可证 AnyConnect 移动许可证

注　ASA 管理员将根据他们已安装的 AnyConnect 许可证，以不同方式使用 AnyConnect 移动状态 DAP 属性。有关详细信息，请参阅第 5-9 页上的向 DAP 添加 AnyConnect 终端属性。

配置动态访问策略

准备工作

- 除非另有说明，您必须在配置 DAP 终端属性之前，安装思科安全桌面或主机扫描。
- 在配置文件、进程和注册表终端属性前，先配置文件、进程和注册表基本主机扫描属性。如需说明，启动 ASDM 并选择 **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**，然后点击 **Help**。
- DAP 仅支持 ASCII 字符。

步骤 1　启动 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access** 或 **Clientless SSL VPN Access > Dynamic Access Policies**。

步骤 2　要包括特定病毒、反间谍软件或个人防火墙终端属性，点击靠近窗格顶部的 **CSD configuration**。然后启用思科安全桌面和主机扫描扩展。如果您之前已启用这两个功能，此链接不会显示。

如果您启用思科安全桌面，但是不启用主机扫描扩展，您应用更改时， ASDM 会包含一个用于启用**主机扫描配置**的链接。

步骤 3　查看先前配置的 DAP 列表。以下字段会显示在表格中：

- ACL Priority - 显示 DAP 记录的优先级。

  ASA 在汇聚来自多个 DAP 记录的网络和网络类型 ACL 时，会使用此值来对 ACL 进行逻辑排序。 ASA 会将记录按优先级数值从大到小排序，数值最小的位于表格底部。较大的数值拥有较高的优先级，即值为 4 的 DAP 记录的优先级高于值为 2 的记录。您不能对其进行手动排序。
- Name - 显示 DAP 记录的名称。
- Network ACL List - 显示应用至该会话的防火墙 ACL 的名称。
- Web-Type ACL List - 显示应用到该会话的 SSL VPN ACL 的名称。
- Description - 描述 DAP 记录的用途。

步骤 4　点击 **Add** 或 **Edit**，以便第 5-4 页上的添加或编辑动态访问策略。

步骤 5　点击 **Apply** 以便保存您的 DAP 配置。

步骤 6　使用 **Find** 字段，可以搜索动态访问策略 (DAP)。

在该字段中开始键入字符时，该工具将会搜索 DAP 表的每个字段的起始字符以获取匹配项。您可以使用通配符扩大搜索。

例如，在 **Find** 字段中键入 `sal` 将会匹配名为 `Sales` 的 DAP，但不会匹配名为 `Wholesalers` 的 DAP。如果您在 **Find** 字段中键入 `*sal`，搜索将会找到表中的 Sales 或 Wholesalers 的第一个实例。

步骤 7　第 5-5 页上的测试动态访问策略可验证您的配置。

添加或编辑动态访问策略

步骤 1　启动 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access**，或者 **Clientless SSL VPN Access > Dynamic Access Policies > Add** 或 **Edit**。

步骤 2　提供此动态访问策略的名称 （必需）和说明 （可选）。

- **Policy Name** 是一个 4 至 32 个字符的字符串，不允许包含空格。
- 您可在 DAP 的 **Description** 字段中，输入最多 80 个字符。

步骤 3　在 **ACL Priority** 字段中，设置动态访问策略的优先级。

安全设备会以您在此处设置的顺序应用访问策略，最大的数值拥有最高的优先级。 0 至 2147483647 的值为有效值。默认值为 0。

步骤 4　为此 DAP 指定您的选择条件：

a.　在 Selection Criteria 窗格中，请使用 ANY/ALL/NONE 下拉列表 （无标签）来选择，对于您为使用此动态访问策略配置的 AAA 属性值，用户是必须拥有任意属性值、拥有所有属性值，还是不需要拥有这些值，以及是否需要满足每一个终端属性。

不允许有重复的条目。如果您配置没有 AAA 和终端属性的 DAP 记录， ASA 会始终选择该记录，因为所有选择标准都已满足。

b.　点击 AAA Attributes 字段中的 **Add** 或 **Edit**，以便第 5-5 页上的配置 DAP 中的 AAA 属性选择条件。

c.　点击 Endpoint Attributes 区域中的 **Add** 或 **Edit**，以便第 5-8 页上的配置 DAP 中的终端属性选择条件。

d.　点击 **Advanced** 字段，以便第 5-16 页上的使用 LUA 在 DAP 中创建其他 DAP 选择条件。使用此功能需要 Lua 编程语言方面的知识。

- AND/OR - 点击定义基本选择规则和您在此处输入的逻辑表达式之间的关系，即是将新属性添加至已设置的 AAA 和终端属性，还是替代已设置的属性。默认值为 AND。
- Logical Expressions - 您可以配置每个终端属性类型的多个实例。输入定义新的 AAA 和/或终端选择属性的自由形式 Lua 文本。 ASDM 不会验证您在此处输入的文本；它只将此文本复制到 DAP XML 文件，然后 ASA 会对其进行处理，放弃它无法解析的所有表达式。

步骤 5　指定此 DAP 的 **Access/Authorization Policy Attributes**。

您在此处配置的属性值会覆盖 AAA 系统中的授权值，包括现有用户、组、隧道组和默认组记录中的授权值。请参阅第 5-22 页上的配置 DAP 访问和授权策略属性。

步骤 6　点击 **OK**。

测试动态访问策略

此窗格允许您指定授权属性值对，从而测试设备上配置的 DAP 记录集的检索。

步骤 1　可以使用与 AAA 属性和终端属性表关联的 Add/Edit 按钮，来指定属性值对。

您点击这些 Add/Edit 按钮时显示的对话框，与 Add/Edit AAA Attributes 和 Add/Edit Endpoint Attributes 对话框中的对话框类似。

步骤 2　点击 **Test** 按钮。

评估每个记录的 AAA 和终端选择属性时，该设备上的 DAP 子系统会引用这些值。结果会显示在 **Test Results** 区域中。

配置 DAP 中的 AAA 属性选择条件

DAP 可提供授权属性的有限集合，该集合可覆盖 AAA 提供的属性，从而补充 AAA 服务。您可以指定 AAA 属性，这些属性来自思科 AAA 属性层次结构，或者来自 ASA 从 RADIUS 或 LDAP 服务器收到的全部响应属性。 ASA 会根据该用户的 AAA 授权信息和该会话的状态评估信息选择 DAP 记录。 ASA 可根据此信息选择多个 DAP 记录，然后将其汇聚以创建 DAP 授权属性。

步骤 1　要将 AAA 属性配置为 DAP 记录的选择条件，请在 Add/Edit AAA Attributes 对话框中，设置您想要使用的 Cisco、LDAP 或 RADIUS 属性。您可以将这些属性设置为 = 或 != 您输入的值。每个 DAP 记录的 AAA 属性数量没有限制。有关 AAA 属性的详细信息，请参阅 AAA 属性定义。

AAA Attributes Type - 使用下拉列表选择 Cisco、 LDAP 或 RADIUS 属性：

- Cisco - 指存储在 AAA 分层模型中的用户授权属性。您可以为 DAP 记录中的 AAA 选择属性，指定这些属性的小的子集。这些属性包括：
  - Group Policy - 与 VPN 用户会话关联的组策略名称。该名称可以在安全设备上本地设置，也可以作为 IETF-Class (25) 属性通过 RADIUS/LDAP 服务器发送。最多 64 个字符。
  - 分配的 IP 地址 - 输入您想要为策略指定的 IPv4 地址。全隧道 VPN 客户端的分配 IP 地址（IPsec、 L2TP/IPsec、 SSL VPN AnyConnect）不会应用至无客户端 SSL VPN，因为没有为无客户端会话**分配地址**。
  - Assigned IPv6 Address - 输入您想要为策略指定的 IPv6 地址。
  - Connection Profile - 连接或隧道组的名称。最多 64 个字符。
  - Username - 经过身份验证的用户的用户名。最多 64 个字符。在您使用 Local、RADIUS、LDAP 身份验证/授权，或者任何其他身份验证类型 （如 RSA/SDI、 NT Domain 等）时应用。
  - =/!= - 等于/不等于。
- LDAP - LDAP 客户端 （安全设备）会将所有本机 LDAP 响应属性值对，存储在与该用户的 AAA 会话关联的数据库中。 LDAP 客户端会按收到响应属性的顺序，将响应属性写入数据库。它会放弃使用该名称的所有后续属性。当从 LDAP 服务器读取用户记录和组记录时，可能会发生此情况。用户记录属性会被先读取，而且其优先级始终高于组记录属性。

为支持 Active Directory 组成员资格， AAA LDAP 客户端会提供 LDAP memberOf 响应属性的特殊处理。 AD memberOf 属性指定 AD 中的组记录的 DN 字符串。该组的名称是 DN 字符串中的第一个 CN 值。LDAP 客户端从 DN 字符串中提取组名，将它作为 AAA memberOf 属性存储，并作为 LDAP memberOf 属性存储在响应属性数据库中。如果在 LDAP 响应消息中有其他的 memberOf 属性，则会从这些属性中提取组名称，然后将组名称与之前的 AAA memberOf 属性结合，形成以逗号分隔的组名称字符串，这些字符串也会在响应属性数据库中更新。

对于通向 LDAP 身份验证/授权服务器的 VPN 远程访问会话返回以下三个 Active Directory 组（memberOf 枚举）的情况：

cn=Engineering,ou=People,dc=company,dc=com

cn=Employees,ou=People,dc=company,dc=com

cn=EastCoastast,ou=People,dc=company,dc=com

ASA 会处理三个 Active Directory 组：Engineering、 Employees 和 EastCoast，可以将其随意组合用作 aaa.ldap 选择条件。

LDAP 属性包含 DAP 记录中的属性名称和属性值对。 LDAP 属性名称对语法敏感/区分大小写。例如，如果您指定 LDAP 属性 Department，用来代替 AD 服务器作为 department 返回的属性，DAP 记录不会根据此属性设置进行匹配。

注　要在 Value 字段中输入多个值，请使用分号 (;) 作为分隔符。例如：

eng;sale; cn=Audgen VPN,ou=USERS,o=OAG

- RADIUS - RADIUS 客户端会将所有本机 RADIUS 响应属性值对，存储在与该用户的 AAA 会话关联的数据库中。 RADIUS 客户端会按收到响应属性的顺序，将响应属性写入数据库。它会放弃使用该名称的所有后续属性。当从 RADIUS 服务器读取用户记录和组记录时，可能会发生此情况。用户记录属性会被先读取，而且其优先级始终高于组记录属性。

  RADIUS 属性包含 DAP 记录中的属性名称和属性值对。有关列出安全设备支持的 RADIUS 属性的表格，请参阅安全设备支持的 RADIUS 属性和值。

  注　对于 RADIUS 属性， DAP 定义 Attribute ID = 4096 + RADIUS ID。

  例如：

  RADIUS 属性 “Access Hours”的 Radius ID = 1，因此 DAP 属性值 = 4096 + 1 = 4097。

  RADIUS 属性“Member Of”的 Radius ID = 146，因此 DAP 属性值 = 4096 + 146 = 4242。

- LDAP 和 RADIUS 属性包括：
  - Attribute ID - 属性的名称/编号。最多 64 个字符。
  - Value - 属性名称 (LDAP) 或编号 (RADIUS)。

    要在 Value 字段中输入多个值，请使用分号 (;) 作为分隔符。例如：
    ```
    eng;sale; cn=Audgen VPN,ou=USERS,o=OAG
    ```
  - =/!= - 等于/不等于。
- LDAP 包含 Gep AD Groups 按钮。请参阅第 5-7 页上的检索 Active Directory 组。

检索 Active Directory 组

您可以在此窗格中查询 Active Directory 服务器，获取可用 AD 组。此功能仅适用于使用 LDAP 的 Active Directory 服务器。此按钮可以查询 Active Directory LDAP 服务器，获取此用户所属的组的列表 （memberOf 枚举）。可以使用组信息来指定动态访问策略 AAA 选择条件。

在后台使用 CLI 的 **how-ad-groups** 命令，可从 LDAP 服务器检索 AD 组。ASA 等待服务器响应的默认时间为 10 秒。您可在 aaa-server 主机配置模式下，使用 **group-search-timeout** 命令调整此时间。

您可以在 Edit AAA Server 窗格中更改 Group Base DN，从而更改搜索在 Active Directory 层次结构中的起始层次。您也可以在此窗口中，更改 ASA 等待服务器响应的时间。要配置这些功能，请选择 **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups > Edit AAA Server**。

注　如果 Active Directory 服务器有大量的组，检索的 AD 组列表 （或者 **show ad-groups** 命令的输出），可能会根据服务器可填充至响应数据包的数据数量限制进行截断。要避免此问题，请使用过滤器功能 来减少服务器报告的组的数量。

AD Server Group - 用于检索 AD 组的 AAA 服务器组的名称。

Filter By - 指定一个组或组的部分名称，以便减少显示的组。

组名称 - 从该服务器检索到的 AD 组的列表。

AAA 属性定义

下表可定义可供 DAP 使用的 AAA 选择属性的名称。Attribute Name 字段显示有您能以 Lua 逻辑表达式输入每个属性名称的方式，您可以在 Add/Edit Dynamic Policy 窗格的 Advanced 部分中输入表达式。

属性类型	属性名称	来源	值	最大字符串长度	说明
Cisco	aaa.cisco.grouppolicy	AAA	字符串	64	ASA 上的组策略名称，或者作为 IETF-Class (25) 属性通过 Radius/LDAP 服务器发送的组策略名称
	aaa.cisco.ipaddress	AAA	数值	-	为全隧道 VPN 客户端分配的 IP 地址 （IPsec、 L2TP/IPsec、 SSL VPN AnyConnect）
	aaa.cisco.tunnelgroup	AAA	字符串	64	连接配置文件 （隧道组）名称
	aaa.cisco.username	AAA	字符串	64	经过身份验证的用户的名称 （在使用本地身份验证/授权时应用）
LDAP	aaa.ldap.<*label*>	LDAP	字符串	128	LDAP 属性值对
RADIUS	aaa.radius.<number>	RADIUS	字符串	128	Rddius 属性值对

有关列出安全设备支持的 RADIUS 属性的表格，请参阅安全设备支持的 RADIUS 属性和值。

配置 DAP 中的终端属性选择条件

终端属性包含终端系统环境、状态评估结果和应用的相关信息。ASA 会在会话建立期间动态生成终端属性的集合，并将这些属性存储在与此会话关联的数据库中。每个 DAP 记录指定终端选择属性，这些属性必须得到满足， ASA 才能选择将其用于会话。 ASA 仅选择满足每个配置的条件的 DAP 记录。

准备工作

- 将终端属性配置为 DAP 记录的选择条件配置是第 5-3 页上的配置动态访问策略的较大流程的一部分，请在将终端属性配置为 DAP 选择条件前，先审阅此操作步骤。
- 有关终端属性的详细信息，请参阅终端属性定义。
- 有关主机扫描如何检查驻留内存的防病毒、反间谍软件和个人防火墙程序的详细信息，请参阅第 5-14 页上的DAP 以及防病毒软件、反间谍软件和个人防火墙程序。

步骤 1　点击 **Add** 或 **Edit**，将以下任意终端属性添加为选择条件。

您可以创建每个终端属性类型的多个实例。每个 DAP 记录的终端属性数量没有限制。

- 第 5-9 页上的向 DAP 添加反间谍软件或防病毒终端属性
- 第 5-9 页上的向 DAP 添加应用属性
- 第 5-9 页上的向 DAP 添加 AnyConnect 终端属性
- 第 5-11 页上的向 DAP 添加文件终端属性
- 第 5-11 页上的向 DAP 添加设备终端属性
- 第 5-12 页上的向 DAP 添加 NAC 终端属性
- 第 5-12 页上的向 DAP 添加操作系统终端属性
- 第 5-12 页上的向 DAP 添加个人防火墙终端属性
- 第 5-12 页上的向 DAP 添加策略终端属性
- 第 5-13 页上的向 DAP 添加进程终端属性
- 第 5-13 页上的向 DAP 添加注册表终端属性

步骤 2　指定 DAP 策略匹配条件。

对于这些终端属性类型，请决定 DAP 策略是否应要求用户拥有一个类型的所有实例 （Match All = AND，默认设置），还是其中的一个 （Match Any = OR）。

a.　点击 **Logical Op**。

b.　为每个终端属性类型，选择 **Match Any** （默认）或 **Match All**。

c.　点击 OK。

步骤 3　返回至第 5-4 页上的添加或编辑动态访问策略。

向 DAP 添加反间谍软件或防病毒终端属性

步骤 1　在 **Endpoint Attribute Type** 列表框中，选择 Anti-Spyware 或 Anti-Virus。

步骤 2　点击适当的 **Enabled、Disabled 或 Not Installed** 按钮，指示选定终端属性及其附带限定词（Enabled/Disabled/Not Installed 按钮下面的字段）必须启用、禁用或不安装。

步骤 3　从 **Vendor ID** 列表框中，点击您要测试的反间谍软件或防病毒软件的供应商的名称。

步骤 4　选中 **Product Description** 复选框，从列表框中选择您要测试的供应商产品名称。

步骤 5　选中 **Version** 复选框，将运算字段设为等于 (=) 、不等于 (!=)、小于 (<)、大于 (>)、小于或等于 (<=)，或者大于或等于 (>=) 您从 **Version** 列表框中选择的产品版本号。

如果版本列表框中的选项包含 x，如 3.x，可以将 x 替换为特定版本号，如 3.5。

步骤 6　选中 Last Update 复选框。指定距离上次更新的天数。您可能希望指明更新应在小于 (<) 或大于 (>) 您在此处输入的天数的时间进行。

步骤 7　点击 **OK**。

向 DAP 添加应用属性

步骤 1　在 **Endpoint Attribute Type** 列表框中，选择 **Application**。

步骤 2　在 Client Type 的运算字段中，请选择等于 (=) 或者不等于 (!=)。

步骤 3　在 Client type 列表框中，请指明要测试的远程访问连接类型。

步骤 4　点击 **OK**。

向 DAP 添加 AnyConnect 终端属性

AnyConnect 终端属性，也称为移动状态或 AnyConnect 标识扩展 (ACIDex)，AnyConnect VPN 客户端会使用这些属性来进行与 ASA 的状态信息通信。动态访问策略可使用这些终端属性来授权用户。

这些移动状态属性可以包含在动态访问策略中，并且在没有在终端上安装主机扫描或思科安全桌面的情况下实施。

一些移动状态属性仅与移动设备上运行的 AnyConnect 客户端相关，还有一些移动状态属性与在移动设备和 AnyConnect 桌面客户端上运行的 AnyConnect 客户端均相关。

准备工作

使用移动状况需要在 ASA 上安装 AnyConnect 移动许可证和 AnyConnect 高级许可证。安装有这些许可证的企业能够根据 DAP 属性和其他现有终端属性，在受支持的移动设备上实施 DAP 策略。这包括允许或拒绝来自移动设备的远程访问。

步骤 1　在 **Endpoint Attribute Type** 列表框中，选择 **AnyConnect**。

步骤 2　选中 **Client Version** 复选框，将运算字段设为等于 (=) 、不等于 (!=)、小于 (<)、大于 (>)、小于或等于 (<=)，或者大于或等于 (>=) 您随后在 **Client Version** 字段中指定的 AnyConnect 客户端版本号。

您可以使用此字段来评估移动设备 （如移动电话和平板电脑），或者台式计算机和便携式计算机设备上的客户端的版本。

步骤 3　选中 **Platform** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您随后从 **Platform** 列表框中选择的操作系统。

您可以使用此字段来评估移动设备上的操作系统，如移动电话和平板电脑，以及台式计算机和便携式计算机设备上的操作系统。选择一个平台将激活 Device Type 和 Device Unique ID 的其他属性字段。

步骤 4　选中 **Platform Version** 复选框，将运算字段设为等于 (=) 、不等于 (!=)、小于 (<)、大于 (>)、小于或等于 (<=)，或者大于或等于 (>=) 您随后在 **Platfrom Version** 字段中指定的操作系统版本号。

如果您想要创建包含此属性的 DAP 记录，请确保也在上一步指定平台。

步骤 5　如果您已选中 Platform 复选框，可以选中 **Device Type** 复选框。将运算字段设为等于 (=) 或不等于 (!=) 您随后在 **Device Type** 字段中选择或输入的设备。

如果您有未在 Device Type 字段中列出的受支持设备，可在 Device Type 字段中输入该设备。获取设备类型信息的最可靠方法是，在终端上安装 AnyConnect 客户端，连接到 ASA，然后执行 DAP 跟踪。在 DAP 跟踪结果中，请查找 **endpoint.anyconnect.devicetype** 的值。这是您需要在 Device Type 字段中输入的值。

步骤 6　如果您已选择 Platform 复选框，可以选中 **Device Unique ID** 复选框。将运算字段设为等于 (=) 或不等于 (!=) 您随后在 **Device Unique ID** 字段中指定的设备唯一 ID。

设备唯一 ID 可区分允许您设置为特定移动设备设置策略的个别设备。要获得设备的唯一 ID，您将需要将此设备连接至 ASA，并执行 DAP 跟踪，请查找值 **endpoint.anyconnect.deviceuniqueid**。这是您需要在 Device Unique ID 字段中输入的值。

步骤 7　如果您已选择平台，可以将 MAC 地址添加至 **MAC Addresses Pool** 字段。将运算字段设为等于 (=) 或不等于 (!=) 指定的 MAC 地址。每个 MAC 地址必须为 xx-xx-xx-xx-xx-xx 格式，其中 “x” 是有效的十六制字符 （0-9、 A-F 或 a-f）。 MAC 地址应至少用一个空格分隔。

MAC 地址可区分允许您为特定设备设置策略的个别系统。要获得系统的 MAC 地址，您将需要将此设备连接至 ASA，并执行 DAP 跟踪，然后查找值 **endpoint.anyconnect.macaddress**。这是您需要在 MAC Address Pool 字段中输入的值。

步骤 8　点击 **OK**。

向 DAP 添加文件终端属性

准备工作

在配置文件终端属性之前，请为思科安全桌面定义要在 Host Scan 窗口中扫描的文件。在 ASDM 中，选择 **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**。有关详细信息，请点击该页面上的 **Help**。

步骤 1　在 **Endpoint Attribute Type** 列表框中，选择 **File**。

步骤 2　选择适当的 **Exists** 或 **Does not exist** 单选按钮，指示选定终端属性及其附带限定词 （Exists/Does not exist 按钮下方的字段）是否应存在。

步骤 3　在 **Endpoint ID** 列表框中，从下拉列表中选择等同于要扫描的文件条目的终端 ID。

文件信息显示在 Endpoint ID 列表框的下方。

步骤 4　选中 **Last Update** 复选框，将运算字段设为小于 (<) 或大于 (>) 特定过去的天数。在 **days** 字段中输入过去的天数。

步骤 5　选中 **Checksum** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您要测试的文件的校验和值。

步骤 6　点击 **Compute CRC32 Checksum** 可确定您要测试的文件的校验和值。

步骤 7　点击 OK。

向 DAP 添加设备终端属性

步骤 1　在 **Endpoint Attribute Type** 列表框中，选择 **Device**。

步骤 2　选中 **Host Name** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您要测试的设备的主机名称。此处仅会使用计算机的主机名，而不是完全限定域名 (FQDN)。

步骤 3　选中 **MAC address** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您要测试的网络接口的 MAC 地址。一个条目只允许有一个 MAC 地址。地址必须是 xxxx.xxxx.xxxx 格式，其中 x 是十六进制字符。

步骤 4　选中 **BIOS Serial Number** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您要测试的设备的 BIOS 序列号值。此编号格式为制造商特定格式。没有格式要求。

步骤 5　选中 **TCP/UDP Port Number** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您要测试的处于侦听状态的 TCP 或 UDP 端口。

在 TCP/UDP 组合框中，选择您要测试的端口的类型：TCP (IPv4)、UDP (IPv4)、TCP (IPv6) 或 UDP (IPv6)。如果您将要测试多个端口，可以在 DAP 中创建多个单独的终端属性规则，并在每个规则中指定一个端口。

步骤 6　选中 **Version of Secure Desktop (CSD)** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 在此终端上运行的主机扫描映像的版本。

步骤 7　选中 **Version of Endpoint Assessment** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您要测试的终端评估 (OPSWAT) 的版本。

步骤 8　点击 OK。

向 DAP 添加 NAC 终端属性

步骤 1　在 **Endpoint Attribute Type** 列表框中，选择 **NAC**。

步骤 2　选中 **Posture Status** 复选框，将运算字段设为等于 (=) 或不等于 (!=) ACS 收到的状态标记字符串。在 Postune Status 文本框中输入状态标记字符串。

步骤 3　点击 **OK**。

向 DAP 添加操作系统终端属性

步骤 1　在 **Endpoint Attribute Type** 列表框中，选择 **Operating System**。

步骤 2　选中 **OS Version** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您在 **OS Version** 列表框中设置的 Windows、 Mac 或 Linux 操作系统。

步骤 3　选中 **OS Update** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您在 **OS Update** 文本框中输入的操作系统的 Windows、 Mac 或 Linux 服务包。

步骤 4　点击 **OK**。

向 DAP 添加个人防火墙终端属性

步骤 1　在 **Endpoint Attribute Type** 列表框中，选择 **Operating System**。

步骤 2　点击适当的 **Enabled**、**Disabled** 或 **Not Installed** 按钮，指示选定终端属性及其附带限定词（Enabled/Disabled/Not Installed 按钮下面的字段）必须启用、禁用或不安装。

步骤 3　从 **Vendor ID** 列表框中，点击您要测试的个人防火墙的供应商的名称。

步骤 4　选中 **Product Description** 复选框，从列表框中选择您要测试的供应商产品名称。

步骤 5　选中 **Version** 复选框，将运算字段设为等于 (=) 、不等于 (!=)、小于 (<)、大于 (>)、小于或等于 (<=)，或者大于或等于 (>=) 从 **Version** 列表框选择的产品版本号。

如果 **Version** 列表框中的选项包含 x，如 3.x，可以将 x 替换为特定版本号，如 3.5。

步骤 6　点击 **OK**。

向 DAP 添加策略终端属性

步骤 1　在 **Endpoint Attribute Type** 列表框中，选择 **Policy**。

步骤 2　选中 **Location** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 思科安全桌面 Microsoft Windows 位置配置文件。在 **Location** 文本框中输入思科安全桌面 Microsoft Windows 位置配置文件字符串。

步骤 3　点击 **OK**。

向 DAP 添加进程终端属性

准备工作

在配置进程终端属性之前，请为思科安全桌面定义要在 Host Scan 窗口中扫描的进程。在 ASDM 中，选择 **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**。有关详细信息，请点击该页面上的 **Help**。

步骤 1　在 **Endpoint Attribute Type** 列表框中，选择 **Process**。

步骤 2　点击适当的 **Exists 或 Does not exist** 按钮，指示选定终端属性及其附带限定词 （Exists 和 Does not exist 按钮下方的字段）是否应存在。

步骤 3　在 **Endpoint ID** 列表框中，从下拉列表中选择要扫描的终端 ID。

终端 ID 进程信息会显示在列表框的下方。

步骤 4　点击 **OK**。

向 DAP 添加注册表终端属性

注册表扫描终端属性仅适用于 Windows 操作系统。

准备工作

在配置注册表终端属性之前，请为思科安全桌面定义要在 Host Scan 窗口中扫描的注册表项。在 ASDM 中，选择 **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**。有关详细信息，请点击该页面上的 **Help**。

步骤 1　在 **Endpoint Attribute Type** 列表框中，选择 **Registry**。

步骤 2　点击适当的 **Exists 或 Does not exist** 按钮，指示**注册表**终端属性及其附带限定词 （Exists 和 Does not exist 按钮下方的字段）是否应存在。

步骤 3　在 **Endpoint ID** 列表框中，从下拉列表中选择等同于要扫描的注册表条目的终端 ID。

注册表信息显示在 Endpoint ID 列表框的下方。

步骤 4　选中 **Value** 复选框，将运算字段设为等于 (=) 或不等于 (!=)。

步骤 5　在第一个 **Value** 列表框，将注册表项确定为 dword 或字符串。

步骤 6　在第二个 Value 运算列表框中，输入您要扫描的注册表项的值。

步骤 7　如果要在扫描时忽略注册表项的大小写，请点击该复选框。如果要搜索区分大小写，请勿选中该复选框。

步骤 8　点击 **OK**。

DAP 以及防病毒软件、反间谍软件和个人防火墙程序

当用户属性与配置的 AAA 和终端属性匹配时，则安全设备会使用 DAP 策略。思科安全桌面的登录前评估和主机扫描模块向该安全设备返回关于配置的终端属性的信息，则 DAP 子系统使用该信息来选择与这些属性的值匹配的 DAP 记录。

大多数（但不是所有）防病毒、反间谍软件和个人防火墙程序支持活动扫描，这意味着这些程序会驻留在内存中，所以会始终运行。主机扫描检查按照以下步骤查看该终端是否安装了程序，以及它是否驻留在内存中：

- 如果安装的程序不支持活动扫描，主机扫描将报告系统存在此软件。 DAP 系统选择指定该程序的 DAP 记录。
- 如果安装的程序确实支持活动扫描，并且为该程序启用了活动扫描，主机扫描将报告此软件的存在。同样，安全设备会选择指定该程序的 DAP 记录。
- 如果安装的程序确实支持活动扫描，并且为该程序禁用了活动扫描，主机扫描将忽略此软件的存在。安全设备不会选择指定该程序的 DAP 记录。此外，**debug trace** 命令的输出包括有关 DAP 的大量信息，不指示该程序的存在，即使安装了此程序。

终端属性定义

以下终端选择属性可供 DAP 使用。 Attribute Name 字段显示有您能以 Lua 逻辑表达式输入每个属性名称的方式，您可以在 Dynamic Access Policy Selection Criteria 窗格的 Advanced 区域中输入表达式。*label* 变量标识应用程序、文件名、进程或注册表条目。

属性类型	属性名称	来源	值	最大字符串长度	说明
反间谍软件（需要思科安全桌面）	endpoint.as["*label*"].exists	主机扫描	true	—	反间谍软件存在
	endpoint.as["*label*"].version		字符串	32	版本
	endpoint.as["*label*"].description		字符串	128	反间谍软件描述
	endpoint.as["*label*"].lastupdate		整数	—	反间谍软件定义更新以来经过的秒数
防病毒（需要思科安全桌面）	endpoint.av["*label*"].exists	主机扫描	true	—	防病毒软件存在
	endpoint.av["*label*"].version		字符串	32	版本
	endpoint.av["*label*"].description		字符串	128	防病毒软件描述
	endpoint.av["*label*"].lastupdate		整数	—	防病毒软件定义更新以来经过的秒数

属性类型	属性名称	来源	值	最大字符串长度	说明
AnyConnect （不需要思科安全桌面或主机扫描）。	endpoint.anyconnect.clientversion	终端	版本	—	AnyConnect 客户端版本。
	endpoint.anyconnect.platform		字符串	—	安装 AnyConnect 客户端的操作系统。
	endpoint.anyconnect.platformversion		版本	64	安装 AnyConnect 客户端的操作系统的版本。
	endpoint.anyconnect.devicetype		字符串	64	安装 AnyConnect 客户端的移动设备的类型。
	endpoint.anyconnect.deviceuniqueid			64	安装 AnyConnect 客户端的移动设备的唯一 ID。
	endpoint.anyconnect.macaddress		字符串	必须为 xx-xx-xx-xx-xx-xx 格式，其中 'x' 是有效的十六进制字符	安装 AnyConnect 客户端的设备的唯一 MAC。
Application	endpoint.application.clienttype	应用	字符串	—	客户端类型： CLIENTLESS ANYCONNECT IPSEC L2TP
Device	endpoint.device.hostname	终端	字符串	64	仅主机名，而不是 FQDN。
	endpoint.device.MAC		字符串	必须是 xxxx.xxxx.xxxx 格式，其中 x 是十六进制字符。	网卡接口卡的 Mac 地址。一个条目只允许有一个 Mac 地址。
	endpoint.device.id		字符串	64	BIOS 序列号：此编号格式为制造商特定格式。没有格式要求。
	endpoint.device.port		字符串	介于 1 和 65535 之间的整数。	TCP 端口处于侦听状态。您可以为一条线路定义一个端口。
	endpoint.device.protection_version		字符串	64	它们运行的主机扫描镜像的版本。
	endpoint.device.protection_extension		字符串	64	终端评估版本 (OPSWAT)

属性类型	属性名称	来源	值	最大字符串长度	说明
File	endpoint.file["*label*"].exists	安全桌面	true	—	此文件存在
	endpoint.file["label"].endpointid				
	endpoint.file["*label*"].lastmodified		整数	—	文件上次修改以来经过的秒数
	endpoint.file["*label*"].crc.32		整数	—	此文件的 CRC32 哈希值
NAC	endpoint.nac.status	NAC	字符串	—	用户定义的状态字符串
Operating System	endpoint.os.version	安全桌面	字符串	32	操作系统
	endpoint.os.servicepack		整数	—	Windows 服务包
Personal firewall （需要安全桌面）	endpoint.fw["*label*"].exists	主机扫描	true	—	此个人防火墙存在
	endpoint.fw["*label*"].version		字符串	32	版本
	endpoint.fw["*label*"].description		字符串	128	个人防火墙描述
Policy	endpoint.policy.location	安全桌面	字符串	64	来自思科安全桌面的位置值
Process	endpoint.process["*label*"].exists	安全桌面	true	—	此进程存在
	endpoint.process["*label*"].path		字符串	255	此进程的完整路径
Registry	endpoint.registry["*label*"].type	安全桌面	*dword* *字符串*	—	dword
	endpoint.registry["*label*"].value		字符串	255	注册表项的值
VLAN	endoint.vlan.type	CNA	字符串	—	VLAN 类型： ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

使用 LUA 在 DAP 中创建其他 DAP 选择条件

本部分提供为 AAA 或终端属性构建逻辑表达式的相关信息。请注意，执行此操作需要精通 Lua 知识。有关 LUA 编程的详细信息，请您可以在 http://www.lua.org/manual/5.1/manual.html 找到。

在 Advance 字段中，您可以输入代表 AAA 和/或终端选择逻辑运算的自由格式 Lua 文本。ASDM 不会验证您在此处输入的文本；它只将此文本复制到 DAP 策略文件，然后 ASA 会对其进行处理，放弃它无法解析的所有表达式。

对于添加上文所述的 AAA 和终端属性区域中无法添加的属性，该选项十分有用。例如，在您将 ASA 配置为使用 AAA 属性，这些属性满足任意、所有指定条件，或者不需要满足指定条件，而终端属性则是累计的，必须全部满足时。要让安全设备使用一个或另一个终端属性，您需要创建适当的 Lua 逻辑表达式，并在此处输入它们。

以下章节提供创建 Lua EVAL 表达式的详细解释以及示例。

创建 Lua EVAL 表达式的语法

注　如果您必须使用 Advanced 模式，出于明确起见，我们建议您尽可能使用 EVAL 表达式，这能使程序验证变得简单明了。

EVAL(<*attribute*> , <comparison>, {<*value*> | <*attribute*>}, [<type>])

<attribute>	AAA 属性或思科安全桌面返回的属性，有关属性定义的信息，请参阅第 5-14 页上的终端属性定义。	
<comparison>	以下任一字符串 （需要双引号）	
	“EQ”	等于
	“NE”	不等于
	“LT”	小于
	“GT”	大于
	“LE”	小于或等于
	“GE”	大于或等于
<value>	双引号中的字符串包含与该属性比较的值	
<type>	以下任一字符串 （需要双引号）	
	“string”	区分大小写的字符串比较
	“”	不区分大小写的字符串比较
	“integer”	数值比较，将字符串值转换为数值
	“hex”	使用十六进制值比较数值，将十六进制字符串转换为十六进制数值
	“version”	比较 X.Y.Z 形式的版本。其中 X、 Y 和 Z 是数值

DAP CheckAndMsg 函数

CheckAndMsg 是您可以配置 DAP 使其调用的 Lua 函数。它根据条件生成一条用户消息。

您可以使用 ASDM，通过 DAP 中的 Advanced 字段配置 CheckAndMsg。 ASA 仅在选择包括 LUA CheckAndMsg 函数的 DAP 记录，并导致无客户端 SSL VPN 或 AnyConnect 终止时，才会向用户显示消息。

CheckAndMsg 函数的语法如下：

```
CheckAndMsg(value, "<message string if value is true>", "<message string if value if false>")
```

在创建 CheckAndMsg 函数时，请注意以下事项：

- CheckAndMsg 会返回作为其第一个参数传入的值。
- 如果您不想使用字符串比较，请将 EVAL 函数用作第一个参数。例如：

  ```
  (CheckAndMsg((EVAL(...)) , "true msg", "false msg"))
  ```

  CheckandMsg 返回 EVAL 函数的结果，并且安全设备会使用它来确定是否选择 DAP 记录。如果选择此记录，并导致终止，安全设备会显示适当的消息。

DAP EVAL 表达式示例

研究这些示例将有助于创建 Lua 逻辑表达式：

说明	示例
Windows XP 的终端测试	`EVAL(endpoint.os.version, "EQ", "Windows XP", "string")`

CLIENTLESS 或 CVC 客户端类型上的终端表达式匹配测试。	`(EVAL(endpoint.application.clienttype,"EQ","CLIENTLESS")`
	`or`
	`EVAL(endpoint.application.clienttype, "EQ","CVC"))`

Norton Antivirus versions 10.x，但不包括 10.5.x 的终端表达式测试。	`(EVAL(endpoint.av["NortonAV"].version, "GE",`
	`"10","version") and`
	`EVAL(endpoint.av["NortonAV"].version,"LT", "10.5",`
	`"version") or`
	`EVAL(endpoint.av["NortonAV"].version, "GE", "10.6",`
	`"version")))`

检查用户 PC 上是否安装有防病毒程序 McAfee，如未安装，则显示一条消息。	`(CheckAndMsg(EVAL(endpoint.av["McAfeeAV"].exists,"NE","true"),"McAfee AV was not found on your computer", nil))`
检查 McAfee 防病毒定义在过去 10 天 （864000 秒）内是否更新，如需要更新则显示一条消息。	`((CheckAndMsg(EVAL(endpoint.av["McAfeeAV"].lastupdate,"GT","864000","integer"),"AV Update needed!Please wait for the McAfee AV till it loads the latest dat file.",nil) ))`
debug dap trace 后，检查特定修补程序，将返回： `endpoint.os.windows.hotfix["KB923414"] = "true";`	`(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"NE","true"),"The required hotfix is not installed on your PC.",nil))`

检查防病毒程序

您可以配置消息，以便最终用户了解并能够解决防病毒程序缺失或未在运行的问题。所以，如果访问被拒绝， ASA 会收集导致 “终止”情况的 DAP 的所有消息，并在登录页面上的浏览器中显示这些消息。如果允许访问， ASA 会在门户页面上显示 DAP 评估过程中生成的所有消息。

以下示例将展示如何使用此功能来检查 Norton AntiVirus 程序。

1. 将以下 Lua 表达式复制并粘贴至 Add/Edit Dynamic Access Policy 窗格的 Advanced 字段中（请点击最右侧的双箭头，以便展开此字段）。

```
(CheckAndMsg(EVAL(endpoint.av[“NortonAV”].exists, "EQ", "false"),"Your Norton AV was found but the active component of it was not enabled", nil) or
CheckAndMsg(EVAL(endpoint.av[“NortonAV”].exists, "NE", "true"),"Norton AV was not found on your computer", nil) )
```

2. 在同一 Advanced 字段中，点击 **OR** 按钮。
3. 在 Access Attributes 部分的下方，在最左侧的选项卡 Action 中，点击 **Terminate**。
4. 从确实没有或已禁用 Norton AntiVirus 的 PC 进行连接。预期结果是连接不会被允许，*并且*消息会以闪烁的！的形式 显示。
5. 点击闪烁的！ 以便查看此消息。

检查防病毒程序*和*超过 1 1/2 天的定义

此示例检查 Norton 和 McAfee 防病毒程序是否存在，以及病毒定义是否超过 1 1/2 天 （10000 秒）。如果定义超过 1 1/2 天， ASA 将终止此会话，并显示一条消息和补救链接。要完成此任务，请执行以下步骤。

1. 将以下 Lua 表达式复制并粘贴至 Add/Edit Dynamic Access Policy 窗格的 Advanced 字段中（请点击最右侧的双箭头，以便展开此字段）：

```
((EVAL(endpoint.av[“NortonAV”].exists,”EQ”,”true”,”string”) and
CheckAndMsg(EVAL(endpoint.av[“NortonAV”].lastupdate,”GT”,”10000”,integer”),To remediate <a href=’http://www.symantec.com’>Click this link </a>”,nil)) or
(EVAL(endpoint.av[“McAfeeAV”].exists,”EQ”,”true”,”string”) and
CheckAndMsg(EVAL(endpoint.av[“McAfeeAV”].lastupdate,”GT”,”10000”,integer”),To remediate <a href=’http://www.mcafee.com’>Click this link</a>”,nil))
```

2. 在同一 Advanced 字段中，点击 **AND** 按钮。
3. 在 Access Attributes 部分的下方，在最左侧的选项卡 Action 中，点击 **Terminate**。
4. 从具有 Norton 和 McAfee 防病毒程序，并且版本已有超过 1 天半的时间未更新的 PC 进行连接。预期结果是此连接不会被允许，*并且*消息会以闪烁的！的形式 显示。
5. 点击闪烁的！ 以便查看此消息和补救链接。

其他 Lua 函数

将动态访问策略用于无客户端 SSL VPN 时，您可能需要匹配条件的额外灵活性。例如，您可能想要根据以下内容应用一个不同的 DAP：

- 用户对象层次结构的组织单位 (OU) 或其他层次
- 遵循命名约定但有许多匹配的组名称 - 您可能需要在组名称上使用通配符的能力。

您可以在 ASDM 中的 DAP 窗格的 Advanced 部分中创建 Lua 逻辑表达式，从而实现这一灵活性。

基于 OU 的匹配示例

DAP 可在逻辑表达式中使用从 LDAP 服务器返回的许多属性。有关此示例的输出，请参阅 DAP 跟踪部分，或运行 debug dap trace。

LDAP 服务器将返回用户的可分辨名称 (DN)。这会明确确定用户对象在目录中所处的位置。例如，如果用户 DN 是 CN=Example User,OU=Admins,dc=cisco,dc=com，则此用户位于 OU=Admins,dc=cisco,dc=com 中。如果所有管理员都在此 OU （或此层次下的任何容器）中，可如下使用逻辑表达式匹配此条件：

```
assert(function()
   if ( (type(aaa.ldap.distinguishedName) == "string") and
        (string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$") ~= nil) )
then
       return true
   end
   return false
end)()
```

在本示例中， string.find 函数允许使用正则表达式。在字符串结尾处使用 $，将此字符串定位至 distinguishedName 字段末尾。

组成员资格示例

您可以为 AD 组成员资格的模式匹配，创建基本逻辑表达式。由于用户可以是多个组的成员， DAP 会将 LDAP 服务器响应解析为表格中的不同条目。您需要一个高级函数来完成以下操作：

- 将 memberOf 字段作为字符串进行比较 （用户仅属于一个组的情况）。
- 如果返回的数据的类型为 “table”，则循环访问每个返回的 memberOf 字段。

我们为此编写并测试过的函数如下所示。在本示例中，如果用户是以 “-stu” 结尾的任意组的成员，它们会与此 DAP 匹配。

```
assert(function()
   local pattern = "-stu$"
   local attribute = aaa.ldap.memberOf
   if ((type(attribute) == "string") and
       (string.find(attribute, pattern) ~= nil)) then
       return true
   elseif (type(attribute) == "table") then
       local k, v
       for k, v in pairs(attribute) do
           if (string.find(v, pattern) ~= nil) then
               return true
           end
       end
   end
   return false
end)()
```

防病毒示例

以下示例使用一个自定义函数，检查是否检测到任何防病毒软件。

```
assert(function()
    for k,v in pairs(endpoint.av) do
         if (EVAL(v.exists, "EQ", "true", "string")) then
              return true
         end
    end
    return false
end)()
```

反间谍软件示例

以下示例使用一个自定义函数，检查是否检测到任何反间谍软件。

```
assert(function()
    for k,v in pairs(endpoint.as) do
         if (EVAL(v.exists, "EQ", "true", "string")) then
              return true
         end
    end
    return false
end)()
```

防火墙示例

以下示例使用一个自定义函数，检查是否检测到防火墙。

```
assert(function()
    for k,v in pairs(endpoint.fw) do
         if (EVAL(v.exists, "EQ", "true", "string")) then
              return true
         end
    end
    return false
end)()
```

防病毒软件、反间谍软件*或*任意防火墙示例

以下示例使用一个自定义函数，检查是否检测到任意防病毒软件、反间谍软件或防火墙。

```
assert(function()
       function check(antix)
           if (type(antix) == "table") then
               for k,v in pairs(antix) do
                   if (EVAL(v.exists, "EQ", "true", "string")) then
                       return true
                   end
               end
           end
           return false
       end
       return (check(endpoint.av) or check(endpoint.fw) or check(endpoint.as))
   end)()
```

拒绝访问示例

您可以使用以下函数，以便在没有防病毒程序的情况下拒绝访问。将它与 Action 已设置为 Terminate 的 DAP 配合使用。

```
assert( function()
for k,v in pairs(endpoint.av) do
    if (EVAL(v.exists, "EQ" , "true", "string")) then
        return false
    end
    end
    return CheckAndMsg(true, "Please install antivirus software before connecting.", nil)
end)()
```

如果缺少防病毒程序的用户尝试登录， DAP 会显示以下消息：

```
Please install antivirus software before connecting.
```

配置 DAP 访问和授权策略属性

点击以下的每个选项卡，并配置其中包含的字段。

Action 选项卡

指定要应用至特定连接或会话的特殊处理。

- Continue - （默认值）点击它可将访问策略属性应用于此会话。
- Quarantine - 通过过使用隔离，您可以限制拥有通过 VPN 已建立的隧道的特定客户端。 ASA 可根据选定的 DAP 记录，将受限的 ACL 应用于会话，以形成一个受限组。当终端不符合管理定义策略时，用户仍然可以访问补救服务 （例如更新防病毒软件等），但会对用户施加限制。补救后，用户可重新连接，这会调用新的状态评估。如果通过此评估，用户可进行连接。此参数需要支持 AnyConnect 安全移动功能的 AnyConnect 版本。
- Terminate - 点击它可终止此会话。
- User Message - 输入一个文本消息，该消息在此 DAP 记录被选择时，会在门户页面上显示。最多 490 个字符。用户消息显示为黄色球体。当用户登录时，它会闪烁三次以引起注意，然后停止闪烁。如果选择了多个 DAP 记录，并且它们都有用户消息，系统会显示所有用户信息。

  您可以包含 URL 或其他嵌入式文本，这需要您使用正确的 HTML 标记。例如：有关升级您的防病毒软件的操作步骤，请所有承包商阅读说明。

Network ACL Filters 选项卡

允许您选择和配置网络 ACL，以便应用至此 DAP 记录。DAP 的 ACL 可以包含允许或拒绝规则，但不能同时包含二者。如果 ACL 同时包含允许和拒绝规则，则 ASA 会拒绝它。

- Network ACL 下拉列表 - 选择已配置的网络 ACL，以便添加至此 DAP 记录。只有包含所有允许或所有拒绝规则的 ACL 合格，此处仅会显示这些 ACL。此字段支持可定义 IPv4 和 IPv6 网络流量访问规则的统一 ACL。
- **Manage...** - 点击以便添加、编辑和删除网络 ACL。
- **Network ACL 列表** - 显示此 DAP 记录的网络 ACL。
- **Add>>** - 点击以便将下拉列表中的选定网络 ACL，添加至右侧的 Network ACL 列表。
- **Delete** - 点击以便将突出显示的网络 ACL 从 Network ACL 列表中删除。您不能从 ASA 中删除 ACL，除非您先将其从 DAP 记录中删除。

Web-Type ACL Filters (clientless) 选项卡

允许您选择和配置网络类型 ACL，以便应用至此 DAP 记录。DAP 的 ACL 仅可以包含允许或拒绝规则。如果 ACL 同时包含允许和拒绝规则，则 ASA 会拒绝它。

- **Web-Type ACL** 下拉列表 - 选择已配置的网络类型 ACL，以便添加至此 DAP 记录。只有包含所有允许或所有拒绝规则的 ACL 合格，此处仅会显示这些 ACL。
- **Manage...** - 点击以便添加、编辑和删除网络类型 ACL。
- **Web-Type ACL** 列表 - 显示此 DAP 记录的网络类型 ACL。
- **Add>>** - 点击以便将下拉列表中的选定网络类型 ACL，添加至右侧的 Web-Type ACL。
- **Delete** - 点击以便将网络类型 ACL 从 Web-Type ACL 列表中删除。您不能从 ASA 中删除 ACL，除非您先将其从 DAP 记录中删除。

Functions 选项卡

允许您为 DAP 记录配置文件服务器条目和浏览、 HTTP 代理以及 URL 条目。

- **File Server Browsing** - 启用或禁用文件服务器或共享功能的 CIFS 浏览。

  浏览要求使用 NBNS（Master Browser 或 WINS）。如果该协议发生故障或未配置，则使用 DNS。CIFS 浏览功能不支持国际化。
- **File Server Entry** - 允许或阻止用户在门户页面上输入文件服务器路径和名称。启用时，系统会将文件服务器条目部分放在门户页面上。用户可以直接输入 Windows 文件的路径名。他们可以下载、编辑、删除、重命名和移动文件。他们还可以添加文件和文件夹。另外还必须在适用的 Windows 服务器上为用户访问配置共享。用户可能必须通过身份验证才能访问文件，具体取决于网络要求。
- **HTTP Proxy** - 能够影响 HTTP 小程序代理向客户端的转发。对于使用适当内容转换进行介入的技术 （如 Java、 ActiveX 和 Flash），代理十分有用。它会绕过破坏，同时确保安全设备的持续使用。转发的代理会自动修改浏览器的旧代理配置，并将所有 HTTP 和 HTTPS 请求重定向到新的代理配置。它支持几乎所有客户端技术，包括 HTML、CSS、JavaScript、VBScript、ActiveX 和 Java。它唯一支持的浏览器是 Microsoft Internet Explorer。
- **URL Entry** - 允许或阻止用户在门户页面上输入 HTTP/HTTPS URL。如果启用此功能，用户可在 URL 输入框中输入网络地址，并使用无客户端 SSL VPN 来访问这些网站。

使用 SSL VPN 不能保证与每个站点的通信是安全的。SSL VPN 可确保远程用户 PC 或工作站和企业网络上的 ASA 之间的数据传输的安全性。如果用户之后访问非 HTTPS 网络资源 （位于互联网或内部网络上），则从企业 ASA 到目标网络服务器之间的通信不安全。

在无客户端 VPN 连接中， ASA 会充当最终用户网络浏览器和目标网络服务器之间的代理。当用户连接到支持 SSL 的网络服务器时，ASA 将建立安全连接，并验证服务器的 SSL 证书。最终用户浏览器从不接收提交的证书，因此无法检查并验证证书。SSL VPN 的当前实施不允许与提交已到期证书的站点进行通信。ASA 也不会执行可信 CA 证书验证。因此，用户在与支持 SSL 的网络服务器通信前，无法分析其提供的证书。

要限制用户访问互联网，请为 URL Entry 字段选择 Disable。这可以防止 SSL VPN 用户在进行无客户端 VPN 连接的过程中使用网络。

- **Unchanged** - （默认值）点击以便使用应用至此会话的组策略中的值。
- **Enable/Disable** - 点击以便启用或禁用该功能。
- **Auto-start** - 点击它可以启用 HTTP 代理，并让 DAP 记录自动启动与这些功能关联的小程序。

Port Forwarding Lists 选项卡

允许您为用户会话选择和配置端口转发列表。

端口转发为此组中的远程用户，提供对经由已知固定 TCP/IP 端口进行通信的客户端/服务器应用程序的访问权限。远程用户可以使用安装在其本地 PC 上的客户端应用程序，并安全访问支持该应用程序的远程服务器。思科已经测试了以下应用程序：Windows Terminal Services、Telnet、Secure FTP（经由 SSH 的 FTP）、Perforce、Outlook Express 和 Lotus Notes。其他基于 TCP 的应用程序可能也能正常使用，但是思科没有对其进行过测试。

注　端口转发不能与某些 SSL/TLS 版本配合使用。

注意事项　确保在远程计算机上安装 Sun Microsystems Java Runtime Environment (JRE) 1.4+ 来支持端口转发（应用程序访问）和数字证书。

- Port Forwarding - 为应用于此 DAP 记录的端口转发列表选择一个选项。此字段中的其他属性只在您将 Port Forwarding 设为 Enable 或 Auto-start 时启用。
- **Unchanged** - 点击以便将属性从运行的配置中删除。
- **Enable/Disable** - 点击以便启用或禁用端口转发。
- **Auto-start** - 点击以便启用端口转发，并让 DAP 记录自动启动与此端口转发列表关联的端口转发小程序。
- **Port Forwarding List** 下拉列表 - 选择已经配置的端口转发列表，以便添加至 DAP 记录。
- **New...** - 点击以便配置新的端口转发列表。
- **Port Forwarding Lists （无标签）** - 显示 DAP 记录的端口转发列表。
- **Add** - 点击以便将下拉列表中的选定端口转发列表，添加至右侧的 Port Forwarding 列表。
- **Delete** - 点击以便从 Port Forwarding 列表中删除选定的端口转发列表。您不能从 ASA 删除端口转发列表，除非您先将其从 DAP 记录中删除。

Bookmarks 选项卡

允许您为特定用户会话 URL，选择和配置书签。

- **Enable bookmarks** - 点击以便启用。如果取消选中，连接的门户页面中不会显示书签。
- **Bookmark** 下拉列表 - 选择已配置的书签，以便添加至 DAP 记录。
- **Manage...** - 点击以便添加、导入、导出和删除书签。
- **Bookmarks （无标签）** - 显示 DAP 记录的 URL 列表。
- **Add>>** - 点击以便将下拉列表中的选定书签，添加至右侧的 URL 区域。
- **Delete** - 点击以便从 URL 列表区域中删除选定书签。您不能从 ASA 中删除书签，除非您先将其从 DAP 记录中删除。

Access Method 选项卡

允许您配置允许的远程访问类型。

- **Unchanged** - 继续使用当前的远程访问方式。
- **AnyConnect Client** - 使用思科 AnyConnect VPN 客户端进行连接。
- **Web-Portal** - 使用无客户端 VPN 进行连接。
- **Both-default-Web-Portal** - 通过无客户端或 AnyConnect 客户端进行连接，默认使用无客户端。
- **Both-default-AnyConnect Client** - 通过无客户端或 AnyConnect 客户端进行连接，默认使用 AnyConnect。

AnyConnect 选项卡

允许您选择 Always-on VPN 标志的状态。

- Always-On VPN for AnyConnect client - 确定 AnyConnect 服务配置文件中的 Always-on VPN 标志设置是不变、禁用，还是应使用 AnyConnect 配置文件设置。

  此参数需要思科 IronPort 网络安全设备的能为思科 AnyConnect VPN 客户端提供安全移动解决方案许可支持的版本。它还需要支持“安全移动解决方案”功能的 AnyConnect 版本。有关其他信息，请参阅 *《思科 AnyConnect VPN 客户端管理员指南》*。

AnyConnect Custom Attributes 选项卡

列出当前分配给此策略的自定义属性。在此对话框中，可以将先前定义的自定义属性与此策略相关联，或者定义自定义属性，然后将其与此策略相关联。

自定义属性会被发送到 AnyConnect 客户端，并由其用于配置诸如延迟升级的功能。一个自定义属性有一个类型和一个命名值。先定义属性的类型，然后可以定义此类型的一个或多个命名值。有关为某个功能配置特定自定义属性的详细信息，请参阅所用 AnyConnect 版本的 *《思科 AnyConnect 安全移动客户端管理员指南》*。

自定义属性可在 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes** 和 **AnyConnect Custom Attribute Names** 中预定义。动态访问策略和组策略都可使用预定义的自定义属性。

有关自定义属性的配置操作步骤的信息，请参阅第 3-17 页上的关于内部组策略中的 AnyConnect 客户端自定义属性，因为对于两种类型的策略而言，配置操作步骤是相同的。

执行 DAP 跟踪

DAP 跟踪显示所有连接的设备的 DAP 终端属性。

步骤 1　从 SSH 终端登录至 ASA，并进入 Privileged Exec 模式。

在 Privileged Exec 模式中， ASA 会提示：`hostname#`。

步骤 2　请启用 DAP 调试，以便在终端窗口中显示此会话的所有 DAP 属性：

```
hostname# debug dap trace
endpoint.anyconnect.clientversion="0.16.0021";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.platformversion="4.1";
endpoint.anyconnect.devicetype="iPhone1,2";
endpoint.anyconnect.deviceuniqueid="dd13ce3547f2fa1b2c3d4e5f6g7h8i9j0fa03f75";
```

步骤 3　（可选）为搜索 DAP 跟踪的输出，请将此命令的输出结果发送至系统日志。要了解有关登录 ASA 的详细信息，请参阅 *《思科 ASA 系列常规操作 ASDM 配置指南》*的*配置登录*。

DAP 示例

- 使用 DAP 定义网络资源
- 使用 DAP 应用 WebVPN ACL
- 执行 CSD 检查，并通过 DAP 应用策略

使用 DAP 定义网络资源

本示例展示如何配置动态访问策略，从而使其成为给用户或组配置网络资源的一种方法。名为 Trusted_VPN_Access 的 DAP 策略允许无客户端和 AnyConnect VPN 访问。名为 Untrusted_VPN_Access 的策略只允许无客户端 VPN 访问。

步骤 1　在 ASDM 中，转至 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > Endpoint**，为每个策略配置以下属性：

属性	Trusted_VPN_Access	Untrusted_VPN_Access
Endpoint Attribute Type Policy	Trusted	Untrusted
Endpoint Attribute Process	ieexplore.exe	—
Advanced Endpoint Assessment	AntiVirus= McAfee Attribute	
CSD Location	Trusted	Untrusted
LDAP memberOf	Engineering, Managers	Vendors
ACL		Web-Type ACL
Access	**AnyConnect** *and* **Web Portal**	**Web Portal**

使用 DAP 应用 WebVPN ACL

DAP 可直接实施访问策略属性的子集，包括网络 ACL（用于 IPsec 和 AnyConnect）、无客户端 SSL VPN 网络类型 ACL、 URL 列表和函数。它不能直接实施，例如欢迎信息或分割隧道列表，这些由组策略实施。Add/Edit Dynamic Access Policy 窗格中的 Access Policy Attributes 选项卡提供了 DAP 可直接实施的属性的完整菜单。

Active Directory/LDAP 将用户组策略成员资格存储为用户条目中的 “memberOf” 属性。定义一个 DAP，以便对于 AD 组 (memberOf) = Engineering 中的用户，ASA 会应用一个配置的网络类型 ACL。

步骤 1　在 ASDM 中，转至 Add AAA attributes 窗格，**Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > AAA Attributes section > Add AAA Attribute**。

步骤 2　对于 AAA 属性类型，请使用下拉列表选择 **LDAP**。

步骤 3　在 Attribuet ID 字段中，输入 memberOf，正如此处所示。大小写非常重要。

步骤 4　在 Value 字段中，请使用下拉列表选择 =，在相邻字段中输入 Engineering。

步骤 5　在此窗格的 Access Policy Attributes 区域中，点击 Web-Type ACL Filters 选项卡。

步骤 6　使用 Web-Type ACL Filters 下拉列表，以便选择您要应用于 AD 组 (memberOf) = Engineering 中的用户的 ACL。

执行 CSD 检查，并通过 DAP 应用策略

本示例将创建检查用户是否属于两个特定 AD/LDAP 组（Engineering 和 Employees）和特定 ASA 隧道组的 DAP。然后将一个 ACL 应用至该用户。

DAP 应用的 ACL 将控制资源的访问。它们将覆盖在 ASA 上定义组策略的任意 ACLS。此外， ASA 为该 DAP 应用了未定义或控制的常规 AAA 组策略继承规则和属性，例如分割隧道列表、欢迎信息和 DNS。

步骤 1　在 ASDM 中，转至 Add AAA attributes 窗格，**Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > AAA Attributes section > Add AAA Attribute**。

步骤 2　对于 AAA 属性类型，请使用下拉列表选择 LDAP。

步骤 3　在 Attribuet ID 字段中，输入 memberOf，正如此处所示。大小写非常重要。

步骤 4　在 Value 字段中，请使用下拉列表选择 =，在相邻字段中输入 Engineering。

步骤 5　在 Attribuet ID 字段中，输入 memberOf，正如此处所示。大小写非常重要。

步骤 6　在 Value 字段中，请使用下拉列表选择 =，在相邻字段中输入 Employees。

步骤 7　对于 AAA 属性类型，请使用下拉列表选择 Cisco。

步骤 8　选中 Tunnel 分组框，使用下拉列表选择 =，并且在相邻下拉列表中选择适当的隧道组（连接策略）。

步骤 9　在 Access Policy Attributes 区域的 Network ACL Filters 选项卡中，选择要应用于符合之前步骤定义的 DAP 条件的用户的 ACL。

邮件代理

邮件代理可将远程邮件功能扩展至无客户端 SSL VPN 用户处。用户通过邮件代理尝试进行邮件会话时，邮件客户端将使用 SSL 协议建立一个隧道。

邮件代理协议如下所示：

POP3S

POP3S 是无客户端 SSL VPN 支持的一种邮件协议。默认情况下，安全设备会侦听端口 995，并自动允许连接端口 995 或配置的端口。POP3 代理仅允许该端口上的 SSL 连接。建立 SSL 隧道后，POP3 协议将会开始工作，接着将会进行身份验证。 POP3S 用于接收邮件。

IMAP4S

IMAP4S 是无客户端 SSL VPN 支持的一种邮件协议。默认情况下，安全设备会侦听端口 993，并自动允许连接端口 993 或配置的端口。 IMAP4S 代理仅允许该端口上的 SSL 连接。建立 SSL 隧道后，IMAP4S 协议将会开始工作，接着将会进行身份验证。 IMAP4S 用于接收邮件。

SMTPS

SMTPS 是无客户端 SSL VPN 支持的一种邮件协议。默认情况下，安全设备会侦听端口 988，并自动允许连接端口 988 或配置的端口。 SMTPS 代理仅允许该端口上的 SSL 连接。建立 SSL 隧道后，SMTPS 协议将会开始工作，接着将会进行身份验证。 SMTPS 用于接收邮件。

配置邮件代理

要求

- 如果用户从本地和远程位置通过邮件代理存取邮件，用户在他们的邮件程序上需要单独的邮件帐户才能进行本地和远程存取。
- 邮件代理会话需要进行用户身份验证。

设置 AAA 服务器组

步骤 1　浏览至 **Configuration> Features > VPN> E-mail Proxy > AAA**。

步骤 2　选择适当的选项卡 （POP3S、 IMAP4S 或 SMTPS）来关联 AAA 服务器组，并为这些会话配置默认的组策略。

- AAA server groups - 点击以便转至 AAA Server Groups 面板 (Configuration > Features > Properties > AAA Setup > AAA Server Groups)，您可以在其中添加或编辑 AAA 服务器组。
- group policies - 点击以便转至 Group Policy 面板 (Configuration > Features > VPN > General > Group Policy)，您可以在其中添加或编辑组策略。
- Authentication Server Group - 选择用于用户身份验证的身份验证服务器组。默认设置为未配置身份验证服务器。如果您将 AAA 设为身份验证方法 (Configuration > Features AAA > VPN > E-Mail Proxy > Authentication panel)，必须配置 AAA 服务器并在此选择，否则身份验证会始终失败。
- Authorization Server Group - 选择用于用户授权的授权服务器组。默认设置为未配置授权服务器。
- Accounting Server Group - 选择用于用户记帐的记帐服务器组。默认设置为未配置记帐服务器。
- Default Group Policy - 选择 AAA 未返回 CLASSID 属性时，应用至用户的组策略。长度必须在 4 至 15 个字母数字字符之间。如果不指定默认组策略，且没有 CLASSID，则 ASA 无法建立会话。
- Authorization Settings - 为用户名设置 ASA 识别授权的值。这适用于通过数字证书进行身份验证并需要 LDAP 或 RADIUS 授权的用户。
  - Use the entire DN as the username - 选择以便将可分辨名称用于授权。
  - Specify individual DN fields as the username - 选择以便指定用于用户授权的特定 DN 字段。

    您可以选择两个 DN 字段，主要和辅助。例如，如果您选择 EA，用户将根据其邮件地址进行身份验证。这样，使用公用名 (CN) John Doe 和邮件地址 johndoe@cisco.com 的用户无法作为 John Doe 或 johndoe 进行身份验证。他必须作为 johndoe@cisco.com 进行身份验证。如果选择 EA 和 O，John Doe 的身份必须验证为 johndoe@cisco.com 和 Cisco Systems, Inc。
  - Primary DN Field - 选择您要配置用于授权的主要 DN 字段。默认设置为 CN。选项包括以下内容：

DN 字段	定义
Country (C)	所在国家/地区的双字母缩写。这些代码符合 ISO 3166 国家/地区缩写。
Common Name (CN)	人员、系统或者其他实体的名称。这是标识层次结构中的最低（最具体）级别。
DN Qualifier (DNQ)	特定 DN 属性。
E-mail Address (EA)	拥有此证书的人员、系统或实体的邮件地址。
Generational Qualifier (GENQ)	辈分词，如 Jr.、 Sr. 或 III。
Given Name (GN)	证书所有者的名字。
Initials (I)	证书所有者姓名的每个部分的第一个字母。
Locality (L)	组织所在的城市或城镇。
Name (N)	证书所有者的姓名。
Organization (O)	公司、机构、代理、协会或其他实体的名称。
Organizational Unit (OU)	组织内的子组。

DN 字段	定义
Serial Number (SER)	证书的序列号。
Surname (SN)	证书所有者的姓氏。
State/Province (S/P)	组织所在的州或省。
Title (T)	证书所有者的头衔，例如博士。
User ID (UID)	证书所有者的标识号。

- Secondary DN Field -（可选）选择您要配置用于授权的辅助 DN 字段。默认设置为 OU。选项包括前表中的所有选项，加上 **None**，如果您不想包括辅助字段可选择此项。

标识邮件代理接口

Email Proxy Access 屏幕允许您标识在其上配置邮件代理的接口。您可以在各个接口上配置和编辑邮件代理，而且您可以为一个接口配置和编辑邮件代理，然后将您的设置应用至所有接口。您无法为管理专用接口或子接口配置邮件代理。

步骤 1　浏览至 **Configuration > VPN> E-Mail Proxy > Access** 以显示为接口启用的内容。

- POP3S Enabled - 显示所有已配置接口的名称。
- POP3S Enabled - 显示是否为接口启用 POP3S。
- IMAP4s Enabled - 显示是否为接口启用 IMAP4S。
- SMTPS Enabled - 显示是否为接口启用 SMTPS。

步骤 2　点击 **Edit** 可更改突出显示的接口的邮件代理设置。

配置邮件代理的身份验证

为所有身份验证类型配置身份验证方法。

步骤 1　浏览至 **Configuration > Features > VPN >E-mail Proxy > Authentication**。

步骤 2　从多种身份验证方式中选择：

- AAA - 选择此项表示需要 AAA 身份验证。此选项需要一个配置的 AAA 服务器。用户要提交用户名、服务器和密码。用户必须同时提交 VPN 用户名和邮件用户名，以 VPN 名称分隔符分隔（仅在用户名各不相同时）。
- Certificate - 选择此项表示需要进行证书身份验证。
- 证书身份验证对于当前ASA软件版本Piggyback HTTPS - 选择以便要求进行 Piggyback 身份验证。

  此身份验证方案要求用户已建立无客户端 SSL VPN 会话。用户只提交邮件用户名。不需要密码。用户必须同时提交 VPN 用户名和邮件用户名，以 VPN 名称分隔符分隔 （仅在用户名各不相同时）。

  因为大多数 SMTP 服务器不允许用户登录，所以 SMTPS 邮件最常使用 Piggyback 身份验证。

注　IMAP 可生成不受同时用户计数限制的一些会话，但会对某个用户名允许的同时登录数量进行计数。如果 IMAP 会话数超过此最大数量，且无客户端 SSL VPN 连接到期，则用户随后无法建立新连接。有多种解决方案：

- 用户可以关闭 IMAP 应用以便通过 ASA 清除会话，然后建立新的无客户端 SSL VPN 连接。
- 管理员可增加 IMAP 用户的同时登录 (Configuration > Features > VPN > General > Group Policy > Edit Group Policy > General)。
- 为邮件代理禁用 HTTPS/Piggyback 身份验证。

- Mailhost -（仅 SMTPS）选择以便要求进行邮件主机身份验证。此选项只面向 SMTPS 显示，因为 POP3S 和 IMAP4S 始终进行邮件主机身份验证。它需要用户的邮件用户名、服务器和密码。

标识代理服务器

此 Default Server 面板允许您标识至 ASA 的代理服务器，并为邮件代理配置默认服务器、端口和未经身份验证的会话的限制。

步骤 1　浏览至 **Configuration> Features > VPN> E-mail Proxy> Default Servers**。

步骤 2　配置以下字段：

- Name or IP Address - 为默认邮件代理服务器键入 DNS 名称或 IP 地址。
- Port - 键入 ASA 在其上侦听邮件代理流量的端口号。通向配置的端口的连接会被自动允许。邮件代理只允许该端口上的 SSL 连接。建立 SSL 隧道后，此电子邮件代理将会开始工作，接着将会进行身份验证。

  默认设置如下：

  - 995 （用于 POP3s）
  - 993 （用于 IMAP4S）
  - 988 （用于 SMTPS）
- Enable non-authenticated session limit - 选择以便限制未经身份验证的邮件代理会话的数量。允许您为处于正在进行身份验证过程中的会话设置限制，从而防止 DOS 攻击。当新会话超过设置限制时， ASA 将会终止最早的未在进行身份验证的连接。如果不存在未在进行身份验证的连接，最早的正在进行身份验证的连接会被终止，而不会终止已完成身份验证的会话。

  邮件代理连接有三个状态：

  1. Unauthenticated - 新邮件连接的状态。
  2. Authenticating - 连接提交用户名时的状态。
  3. Authenticated - ASA 已完成连接的身份验证时的状态。

配置分隔符

此面板允许您为邮件代理身份验证配置用户名/密码分隔符和服务器分隔符。

步骤 1　浏览至 **Configuration> Features > VPN> E-mail Proxy > Delimiters**。

步骤 2　配置以下字段：

- Username/Password Delimiter - 选择用于分隔 VPN 用户名与邮件用户名的分隔符。将 AAA 身份验证用于邮件代理，并且 VPN 用户名和邮件用户名不同时，用户需要两个用户名。当用户登录至邮件代理会话时，会输入两个用户名，以您在此配置的分隔符分隔，另外还有邮件服务器名称。

注　无客户端 SSL VPN 电子邮件代理用户的密码不能包含用作分隔符的字符。

- Server Delimiter - 选择用于分隔用户名与邮件服务器的名称的分隔符。它必须与 VPN 名称分隔符不同。当用户登录至邮件代理会话时，会在用户名字段中同时输入其用户名和服务器。

  例如，使用 : 作为 VPN 名称分隔符，使用 @ 作为服务器分隔符，通过邮件代理登录邮件程序时，用户会以如下格式输入其用户名：vpn_username:e-mail_username@server。

监控 VPN

监控 VPN 连接图

有关以图形或表格形式为 ASA 显示 VPN 连接数据，请参阅以下屏幕。

Monitor IPsec Tunnels - Monitoring > VPN > VPN Connection Graphs > IPSec Tunnels

用于指定要查看或预备导出或打印的 IPsec 隧道类型的图形和表格。

Monitor L2TP - Monitoring > Features > VPN > VPN Connection Graphs > L2TP

用于指定要显示的图形或表格类型。

Monitor Sessions - Monitoring > VPN > VPN Connection Graphs > Sessions

用于指定要查看或预备导出或打印的 VPN 会话类型的图形和表格。

监控 VPN 统计信息

有关显示特定远程访问、LAN 对 LAN、无客户端 SSL VPN 或邮件代理会话的详细参数和统计信息，请参阅以下屏幕。参数和统计信息因会话协议而异。统计信息表的内容取决于您选择的连接类型。详细信息表显示每个会话的所有相关参数。

Monitor Session Window - Monitoring > VPN > VPN Statistics> Sessions

用于查看 ASA 的 VPN 会话统计信息。此窗格中的第二个表的内容取决于 Filter By 列表中的选择。

注 管理员可跟踪处于非活动状态的用户数量，也可以查看统计信息。处于非活动状态时间最长的会话会被标记为空闲（并自动注销），以便不会达到许可证容量限制，而且新用户可以登录。您还可以使用 **show vpn-sessiondb** CLI 命令访问这些统计信息（请参阅《思科安全设备命令参考指南》）。

- All Remote Access

指示此表中的值与远程访问 （IPSec 软件和硬件客户端）流量相关。

  - Username/Connection Profile - 显示用户名或登录名和会话的连接配置文件（隧道组）会话。如果客户端使用数字证书进行身份验证，此字段显示此证书的主题 CN 或主题 OU。
  - Group Policy Connection Profile - 显示会话的隧道组策略连接配置文件。

– Assigned IP Address/Public IP Address - 显示分配给此会话远程客户端的专用 （“已分配”） IP 地址。这也称为“内部”或“虚拟” IP 地址，它允许客户端在专用网络上显示为主机。同样显示的还有此远程访问会话的客户端的公用 IP 地址。这也称为“外部” IP 地址。它通常由 ISP 分配给客户端，并且允许客户端在公用网络上充当主机。

注　Assigned IP Address 字段不适用于无客户端 SSL VPN 会话，因为 ASA（代理）是所有流量的来源。对于处于网络扩展模式的硬件客户端会话，Assigned IP Address 是硬件客户端的专用/内部网络接口的子网。

– Ping - 发送 ICMP `Ping` （数据包互联网探测器）数据包测试网络连接。具体而言， ASA 将 ICMP 回显请求消息发送到选定主机。如果主机可以访问，它会返回回显回复消息，且 ASA 会显示一条带被测主机名称的成功消息，以及请求发送和收到响应之间经过的时间。如果系统由于任何原因无法访问（如，主机故障、ICMP 未在主机上运行、路由未配置、中间路由器故障或者网络故障或堵塞）， ASA 会显示一个带被测主机名称的错误屏幕。

– Logout By - 选择一个用于过滤要被注销的会话的条件。如果您选择除 --All Sessions-- 外的任意项，位于 Logout By 列表右侧的框会变为活动状态。如果您为 Logout By 选择值 Protocol，此框会变为一个列表，您可以从中选择用作注销过滤器的协议类型。此列表的默认值是 IPsec。对于 Protocol 以外的所有选项，您必须在此列中提供适当的值。

Monitor Active AnyConnect Sessions - Monitoring > VPN > VPN Statistics > Sessions

用于查看按用户名、 IP 地址、地址类型或公用地址排序的 AnyConnect 客户端会话。

Monitor VPN Session Details - Monitoring > VPN > VPN Statistics > Sessions > Details

用于查看关于选定会话的配置设置、统计和状态信息。

- NAC Result and Posture Token

仅当您已在 ASA 上配置网络准入控制时， ASDM 才会在此列中显示值。

– Accepted - ACS 已成功验证远程主机的状态。

– Rejected - ACS 未能成功验证远程主机的状态。

– Exempted - 根据 ASA 上配置的 Posture Validation Exception 列表，远程主机已被免除状态验证。

– Non-Responsive - 远程主机没有响应 EAPoUDP Hello 消息。

– Hold off - ASA 在状态验证成功后丢失与远程主机的 EAPoUDP 通信。

– N/A - 根据 VPN NAC 组策略，已为远程主机禁用 NAC。

– Unknown - 状态验证正在进行中。

状态标记是可在访问控制服务器上配置的信息文本字符串。ACS 将状态标记下载至 ASA，以用于协助系统监控、报告、调试和记录的信息性用途。在 NAC 结果之后出现的典型状态标记如下：Healthy、 Checkup、 Quarantine、 Infected 或 Unknown。

Session Details 窗格中的 Details 选项卡会显示以下列：

– ID - 动态分配给会话的唯一 ID。ID 充当此会话的 ASA 索引。它使用此索引维护和显示会话的相关信息。

– Type - 会话类型：IKE、 IPSec 或 NAC。

– Local Addr.、Subnet Mask、Protocol、Port、Remote Addr.、Subnet Mask、Protocol 和 Port - 分配给实际 （本地）对等体的地址和端口，以及出于外部路由用途分配给此对等体的地址和端口。

– Encryption - 此会话正在使用的数据加密算法 （如有）。

- Assigned IP Address and Public IP Address - 显示分配给此会话远程对等体的专用 IP 地址。也称为内部或虚拟 IP 地址，分配的 IP 地址允许远程对等体似乎位于专用网络上。第二个字段显示此会话的远程计算机的公用 IP 地址。也称为外部 IP 地址，公用 IP 地址通常由 ISP 分配给远程计算机。它允许远程计算机在公用网络上充当主机。
- Other - 与此会话关联的其他属性。

以下属性应用于 IKE 会话、 IPsec 会话和 NAC 会话：

- Revalidation Time Interval - 每次成功的状态验证之间所需的间隔，以秒为单位。
- Time Until Next Revalidation - 如果上次状态验证尝试未成功，则为 0。否则，此项为 Revalidation Time Interval 和上次成功的状态验证后的秒数差。
- Status Query Time Interval - 每次成功的状态验证或状态查询响应和下次状态查询响应之间允许的时间，以秒为单位。状态查询是 ASA 向远程主机发出的请求，请求远程主机指示主机在上次状态验证后是否有任何状态更改。
- EAPoUDP Session Age - 自上次成功的状态验证起经过的秒数。
- Hold-Off Time Remaining - 如果上次状态验证成功，则为 0 秒。否则，则为下次状态验证尝试之前的剩余秒数。
- Posture Token - 访问控制服务器上可配置的信息文本字符串。ACS 将状态标记下载至 ASA，以用于协助系统监控、报告、调试和记录的信息性用途。典型的状态标记为 Healthy、Checkup、 Quarantine、 Infected 或 Unknown。
- Redirect URL - 状态验证或无客户端身份验证之后，ACS 会将此会话的访问策略下载到 ASA。Redirect URL 是访问策略负载的可选部分。 ASA 将此远端主机的所有 HTTP （端口 80）和 HTTPS （端口 443）请求重定向至 Redirect URL （如有） 。如果访问策略不包含 Redirect URL， ASA 不会重定向来自远程主机的 HTTP 和 HTTPS 请求。

  重定向 URL 仍然有效，直到 IPsec 会话结束或直到状态重新验证，为此， ACS 会下载包含不同重定向 URL 或没有重定向 URL 的新访问策略。

  More - 按此按钮可重新验证或初始化此会话或隧道组。

ACL 选项卡显示包含与此会话匹配的 ACE 的 ACL。

Monitor Cluster Loads - Monitoring > VPN > VPN Statistics > Cluster Loads

用于查看 VPN 负载均衡集群中的服务器之间的当前流量负载分布。如果服务器不是集群的一部分，您将收到一条表示此服务器不参与 VPN 负载均衡集群的信息消息。

Monitor Crypto Statistics - Monitoring > VPN > VPN Statistics > Crypto Statistics

用于查看 ASA 上当前活动用户和管理员会话的加密统计信息。表中每一行表示一个加密统计信息。

Monitor Compression Statistics - Monitoring > VPN > VPN Statistics > Compression Statistics

用于查看 ASA 上当前活动用户和管理员会话的压缩统计信息。表中每一行表示一个压缩统计信息。

Monitor Encryption Statistics - Monitoring > VPN > VPN Statistics > Encryption Statistics

用于查看 ASA 上当前活动用户和管理员会话使用的数据加密算法。表中每一行表示一个加密算法类型。

Monitor Global IKE/IPsec Statistics—Monitoring > VPN > VPN Statistics > Global IKE/IPSec Statistics

用于查看 ASA 上当前活动用户和管理员会话的全局 IKE/IPsec 统计信息。表中每一行表示一个全局统计信息。

监控 NAC 会话摘要

用于查看活动和积累的网络准入控制会话。

- Active NAC Sessions - 有关要进行状态验证的远端对等体的常规统计信息。
- Cumulative NAC Sessions - 有关要进行或已经进行状态验证的远端对等体的常规统计信息。
- Accepted - 传递状态验证并由访问控制服务器授予访问策略的对等体的数量。
- Rejectd - 状态验证失败或访问控制服务器未授予访问策略的对等体的数量。
- Exempted - 不进行状态验证的对等体的数量，因为它们与在 ASA 上配置的 Posture Validation Exception 列表中的一个条目匹配。
- Non-responsive - 未响应状态验证的经由 UDP 的可扩展身份验证协议 (EAP) 请求的对等体的数量。其上没有运行 CTA 的对等体不会响应这些请求。如果 ASA 配置支持无客户端主机，访问控制服务器会为这些对等体将与无客户端主机关联的访问策略下载至 ASA。否则，ASA 会分配 NAC 默认策略。
- Hold-off - ASA 状态验证成功后，丢失 EAPoUDP 通信的对等体的数量。 NAC Hold Timer 属性 (Configuration > VPN > NAC) 可确定此事件类型和下次状态验证尝试之间的延迟。
- N/A - 根据 VPN NAC 组策略禁用 NAC 的对等体的数量。
- Revalidate All - 如果对等体的状态或分配的访问策略 （即下载的 ACL）已发生变化，请点击此按钮。点击此按钮可发起 ASA 管理的所有 NAC 会话的新的无条件状态验证。在您点击此按钮之前，有效的状态验证和分配的访问策略会仍然保持有效，直到新的状态验证成功或失败。点击此按钮不会影响已免除状态验证的会话。
- Initializa All - 如果对等体的状态或分配的访问策略 （即下载的 ACL）已发生变化，而且您想要清除分配给会话的资源，可以点击此按钮。点击此按钮可清除 EAPoUDP 关联和用于 ASA 管理的所有 NAC 会话的状态验证的已分配访问策略，并发起新的无条件状态验证。 NAC 默认 ACL 在重新验证期间有效，因此会话初始化可能会中断用户流量。点击此按钮不会影响已免除状态验证的会话。

Monitor Protocol Statistics - Monitoring > VPN > VPN Statistics > Protocol Statistics

用于查看 ASA 上当前活动用户和管理员会话使用的协议。表中每一行表示一种协议类型。

Monitor VLAN Mapping Sessions

用于查看分配至出口 VLAN 的会话的数量，这取决于每个所用组策略的 Restrict Access to VLAN 参数的值。 ASA 会将所有流量转发至指定的 VLAN。

Monitor SSO Statistics for Clientless SSL VPN Session - Monitoring > VPN > WebVPN > SSO Statistics

用于查看为 ASA 配置的当前活动 SSO 服务器的单一登录统计信息。

注　这些统计信息仅用于使用 SiteMinder 和 SAML Browser Post Profile 服务器的 SSO。

SSL 设置

SSL 设置

Configuration > Device Management > Advanced > SSL Settings

Configuration > Remote Access VPN > Advanced > SSL Settings

ASA 使用安全套接字层 (SSL) 协议和传输层安全性 (TLS) 为 ASDM、无客户端 SSL VPN、VPN 和基于浏览器的会话提供安全消息传输支持。SSL Settings 面板允许您未客户端和服务器配置 SSL 版本和加密算法。它还允许您将以前配置的信任点应用于特定接口以及为没有关联信任点的接口配置备用信任点。

注 对于版本 9.3(2)，SSLv3 已作废。现在，默认的是 **tlsv1** 而不是 **any**。The **any** 已作废。如果您选择 **any**、**sslv3** 或 **sslv3-only**，系统将接受设置，但是会显示一条警告。点击 **OK** 继续操作。在下一个主要 ASA 版本中，这些关键字都将从 ASA 中删除。

字段

- **Server SSL Version** - 指明 ASA 用做下拉列表中的服务器时其所使用的最低 SSL/TLS 协议版本。

任意	接受 SSLv2 客户端 hello 并协商最高的通用版本。
SSL V3	接受 SSLv2 客户端 hello 并协商 SSLv3 （或更高版本）。
TLS V1	接受 SSLv2 客户端 hello 并协商 TLSv1 （或更高版本）。
TLSV1.1	接受 SSLv2 客户端 hello 并协商 TLSv1.1 （或更高版本）。
TLSV1.2	接受 SSLv2 客户端 hello 并协商 TLSv1.2 （或更高版本）。

- **Client SSL Version** - 指明 ASA 用做下拉列表中的客户端时其所使用的最低 SSL/TLS 协议版本。

任意	传输 SSLv3 客户端 hello 并协商 SSLv3 （或更高版本）。
SSL V3	传输 SSLv3 客户端 hello 并协商 SSLv3 （或更高版本）。
TLS V1	传输 TLSv1 客户端 hello 并协商 TLSv1 （或更高版本）。
TLSV1.1	传输 TLSv1.1 客户端 hello 并协商 TLSv1.1 （或更高版本）。
TLSV1.2	传输 TLSv1.2 客户端 hello 并协商 TLSv1.2 （或更高版本）。

- **Diffie-Hellmann group to be used with SSL** - 从下拉列表选择一个组。可用选项为 Group1 - 768 位模数、Group2 - 1024 位模数、Group5 - 1536 位模数、Group14 - 2048 位模数、224 位模数和 Group24 - 2048 位模数、 256 位素数阶。默认值为 Group2。

- **Encryption** - 指定您想要支持的版本、安全级别和 SSL 加密算法。点击 **Edit**，使用 Configure Cipher Algorithms/Custom String 对话框定义或修改表项。选择 SSL 密码安全级别，然后点击 **OK**。
  - **Cipher Version** - 列出 ASA 支持和用于 SSL 连接的密码版本。
  - **Cipher Security Level** - 列出 ASA 支持和用于 SSL 连接的密码安全级别。选择以下一个选项：

    All 包括 NULL-SHA 等所有密码。

    Low 包括除 NULL-SHA 之外的所有密码。

    Medium 包括所有密码，但 NULL-SHA、DES-CBC-SHA、RC4-SHA 和 RC4-MD5（这是默认密码）除外。

    Fips 包括所有符合 FIPS 的密码，但 NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA 和 DES-CBC3-SHA 除外。

    High 只包括使用 SHA-2 密码的 AES-256 并且只适用于 TLS 版本 1.2。

    Custom 包括您在 Cipher algorithms/custom string 框中指定的一个或多个密码。此选项让您可以使用 OpenSSL 密码定义字符串对密码套件进行全面控制。
  - **Cipher Algorithms/Custom String** - 列出 ASA 支持和用于 SSL 连接的密码算法。有关使用 OpenSSL 的密码的详细信息，请参阅 https://www.openssl.org/docs/apps/ciphers.html。

    ASA 指定受支持密码的优先级顺序如下：

    仅受 TLSv1.2 支持的密码

DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES128-SHA256
DHE-RSA-AES256-SHA
AES256-SHA
DHE-RSA-AES128-SHA
AES128-SHA
DES-CBC3-SHA

TLSv1.1 或 TLSv1.2 不支持的密码

RC4-SHA
RC4-MD5
DES-CBC-SHA
NULL-SHA

- **Server Name Indication (SNI)** - 指定域名和与该域关联的信任点。点击 **Add** 或 **Edit**，使用 Add/Edit Server Name Indication (SNI) 对话框定义或编辑每个接口的域和信任点。
  - Specify domain - 输入域名。
  - Select trustpoint to associate with domain - 从下拉列表选择信任点。
- **Certificates** - 为每个接口上的 SSL 身份验证分配要使用的证书。点击 **Edit**，使用 Select SSL Certificate 对话框为每个接口定义或修改信任点。
  - Primary Enrolled Certificate - 为此接口上的证书选择要使用的信任点。
  - Load Balancing Enrolled Certificate - 选择配置 VPN 负载平衡时用于证书的信任点。
- **Fallback Certificate** 点击以选择要用于没有关联证书的接口的证书。如果您选择 **None**，则 ASA 将使用默认 RSA 密钥对和证书。
- **Forced Certification Authentication Timeout** - 配置证书身份验证超时之前等待的分钟数。
- **Apply** - 点击以保存您的更改。
- **Reset** - 点击以删除所做的更改并将 SSL 参数重置为之前定义的值。

第 9 章

用于授权和身份验证的外部服务器

本章介绍如何配置外部 LDAP、 RADIUS 或 TACACS+ 服务器来支持 ASA 的 AAA。在您配置 ASA 以便使用外部服务器之前，必须使用正确的 ASA 授权属性配置 AAA 服务器，并且从这些属性子集中，将特定权限分配给个别用户。

了解授权属性的策略实施

ASA 支持将用户授权属性 （也称为用户授权或权限）应用到 VPN 连接的多种方法。您可以配置 ASA，以便通过以下任意组合获取用户属性：

- ASA 上的动态访问策略 (DAP)
- 外部 RADIUS 或 LDAP 身份验证和/或授权服务器
- ASA 上的组策略

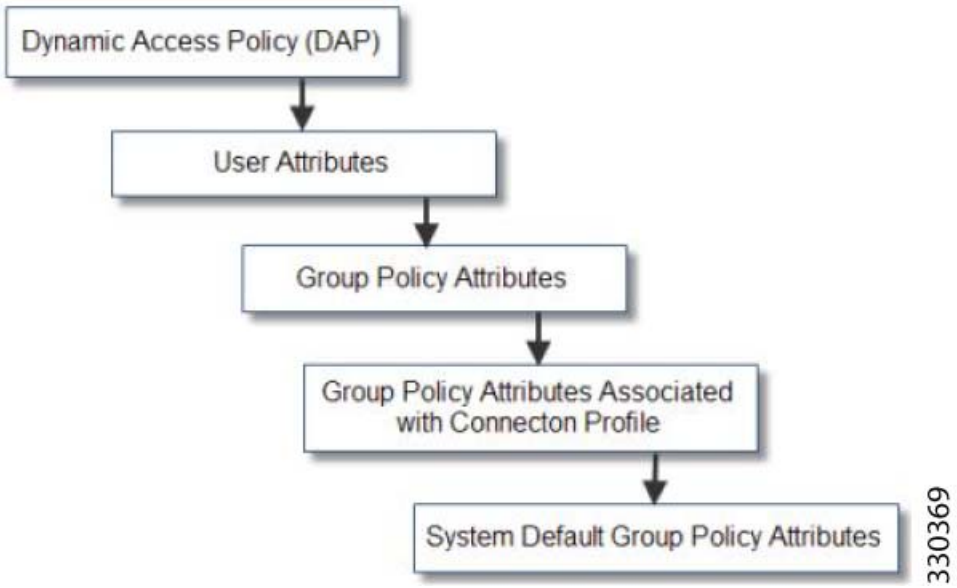
如果 ASA 收到来自所有来源的属性，将会对这些属性进行评估、合并，并将其应用至用户策略。如果属性之间有冲突， DAP 属性优先。

ASA 按照以下顺序应用属性 （请参阅图 9-1）。

1. ASA 上的 DAP 属性 - 在 8.0(2) 版本中引入，这些属性优先于所有其他的属性。如果您在 DAP 中设置书签或 URL 列表，它会覆盖组策略中设置的书签或 URL 列表。
2. AAA 服务器上的用户属性 - 该服务器在用户身份验证和/或授权成功后返回这些属性。请不要将这些属性与为 ASA 本地 AAA 数据库中的个别用户 （ASDM 中的用户帐户）设置的属性混淆。
3. 在 ASA 上配置的组策略 - 如果 RADIUS 服务器为该用户返回 RADIUS CLASS 属性 IETF-Class-25 (OU=*group-policy*) 值， ASA 会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。

   对于 LDAP 服务器，任何属性名称都可用于设置该会话的组策略。您在 ASA 上配置的 LDAP 属性映射会将该 LDAP 属性映射至思科属性 IETF-Radius-Class。
4. 连接配置文件分配的组策略（在 CLI 中称为隧道组）- 连接配置文件具有该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。连接至 ASA 的所有用户最初都属于此组，这可以提供 DAP 缺失的所有属性、服务器返回的用户属性或分配给用户的组策略。
5. ASA 分配的默认组策略 (DfltGrpPolicy) - 系统默认属性提供 DAP、用户属性、组策略或连接配置文件中缺失的所有值。

图 9-1　　策略实施流程



定义 ASA LDAP 配置

授权是指实施权限或属性的过程。 LDAP 服务器的定义是实施权限或属性的身份验证或授权服务器（如已配置）。

准则

ASA 会根据属性名称，而不是数值 ID 来实施 LDAP 属性。RADIUS 属性会按数值 ID 而不是名称来实施。

对于 ASDM 7.0 版本， LDAP 属性包含 cVPN3000 前缀。对于 ASDM 7.1 版本及更高版本，此前缀已移除。

LDAP 属性是已在 Radius 章节中列出的 Radius 属性的子集。

Active Directory/LDAP VPN 远程访问授权示例

本部分提供在 ASA 上使用 Microsoft Active Directory 服务器配置身份验证和授权的示例操作步骤。包括下列主题：

Cisco.com 提供的其他配置示例包括以下技术说明。

- *处于以下 URL 的《ASA/PIX：通过 LDAP 配置将 VPN 客户端映射至 VPN 组策略的示例》：*
  http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008089149d.shtml
- *处于以下 URL 的《PIX/ASA 8.0：登录时使用 LDAP 身份验证来分配组策略》：*
  http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00808d1a7c.shtml

基于用户的属性策略实施

您可以将任意标准 LDAP 属性映射至一个已知的供应商特定属性 (VSA)，也可以将一个或多个 LDAP 属性映射至一个或多个思科 LDAP 属性。

以下示例展示如何配置 ASA，以便为在 AD LDAP 服务器上配置的用户实施简单欢迎信息。在服务器上，使用 General 选项卡中的 Office 字段输入欢迎信息文本。此字段使用名为 physicalDeliveryOfficeName 的属性。在 ASA 中，创建将 physicalDeliveryOfficeName 映射至 Cisco 属性 Banner1 的属性映射。在身份验证过程中， ASA 从该服务器检索 physicalDeliveryOfficeName 的值，将该值映射至 Cisco 属性 Banner1，然后向用户显示该欢迎信息。

此示例适用于任意连接类型，包括 IPSec VPN 客户端、AnyConnect SSL VPN 客户端或无客户端 SSL VPN。在此示例中， User1 通过无客户端 SSL VPN 连接进行连接。

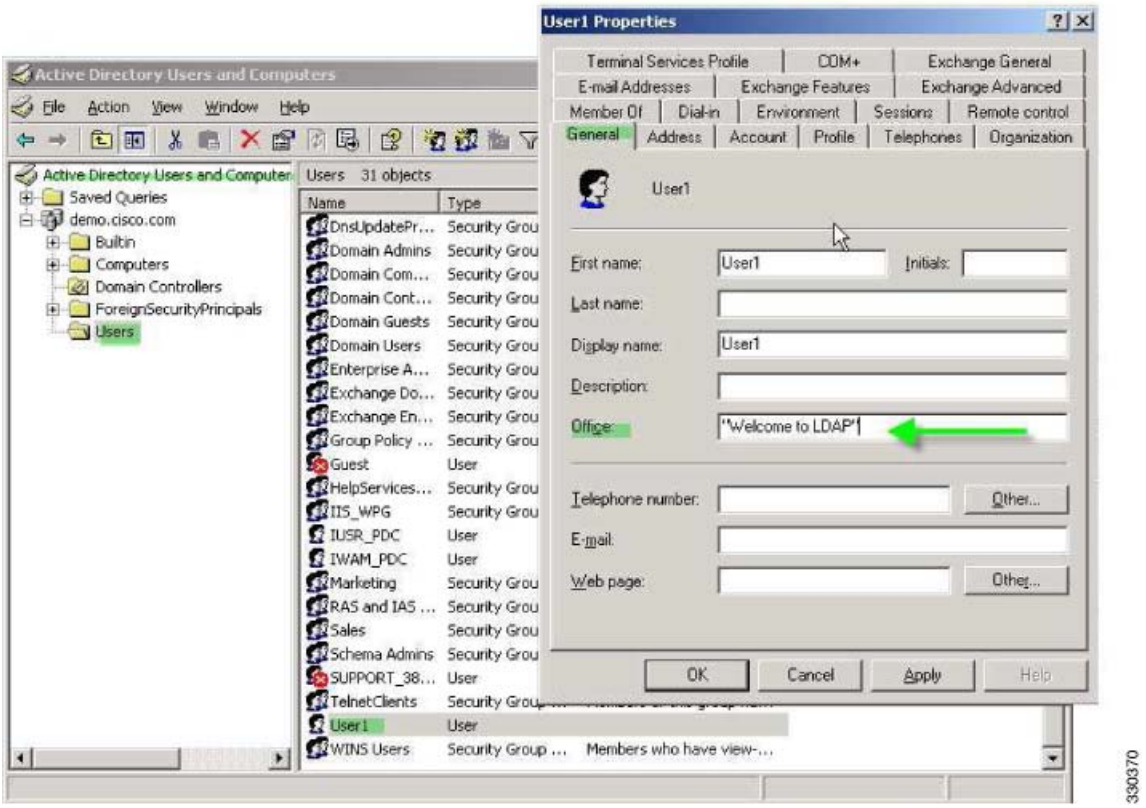
要在 AD 或 LDAP 服务器上为用户配置属性，请执行以下步骤：

步骤 1　右键单击用户。

系统将显示 Properties 对话框 （请参阅图 9-2）。

步骤 2　点击 **General** 选项卡，在 Office 字段中输入欢迎信息文本，这会使用 AD/LDAP 属性 physicalDeliveryOfficeName。

图 9-2　　LDAP 用户配置



步骤 3　在 ASA 上创建一个 LDAP 属性映射。

以下示例创建映射 Banner，并将 AD/LDAP 属性 physicalDeliveryOfficeName 映射至 Cisco 属性 Banner1：

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

步骤 4　将 LDAP 属性映射关联到 AAA 服务器。

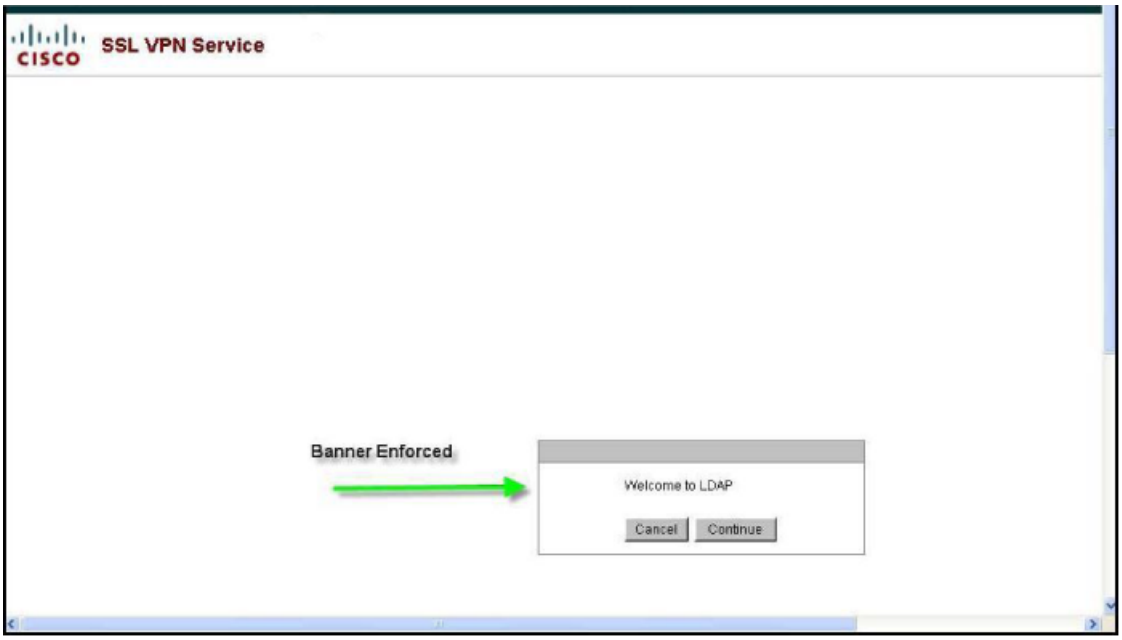
以下示例进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您在步骤 3 中创建的属性映射 Banner：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

步骤 5　测试此欢迎信息的实施。

以下示例展示无客户端 SSL 连接，以及用户完成身份验证后通过属性映射实施的欢迎信息 （请参阅图 9-3）。

图 9-3　　显示的欢迎信息



将 LDAP 用户置于特定组策略中

以下示例展示如何在 AD LDAP 服务器上对 User1 进行身份验证，以便将其置于 ASA 上的特定组策略。在服务器上，使用 Organization 选项卡的 Department 字段输入组策略的名称。然后创建一个属性映射，将 Department 映射到思科属性 IETF-Radius-Class。在身份验证过程中，ASA 从服务器检索 Department 的值，将此值映射到 IETF-Radius-Class，然后将 User1 置于该组策略中。

此示例适用于任意连接类型，包括 IPSec VPN 客户端、AnyConnect SSL VPN 客户端或无客户端 SSL VPN。在此示例中， User1 通过无客户端 SSL VPN 连接进行连接。

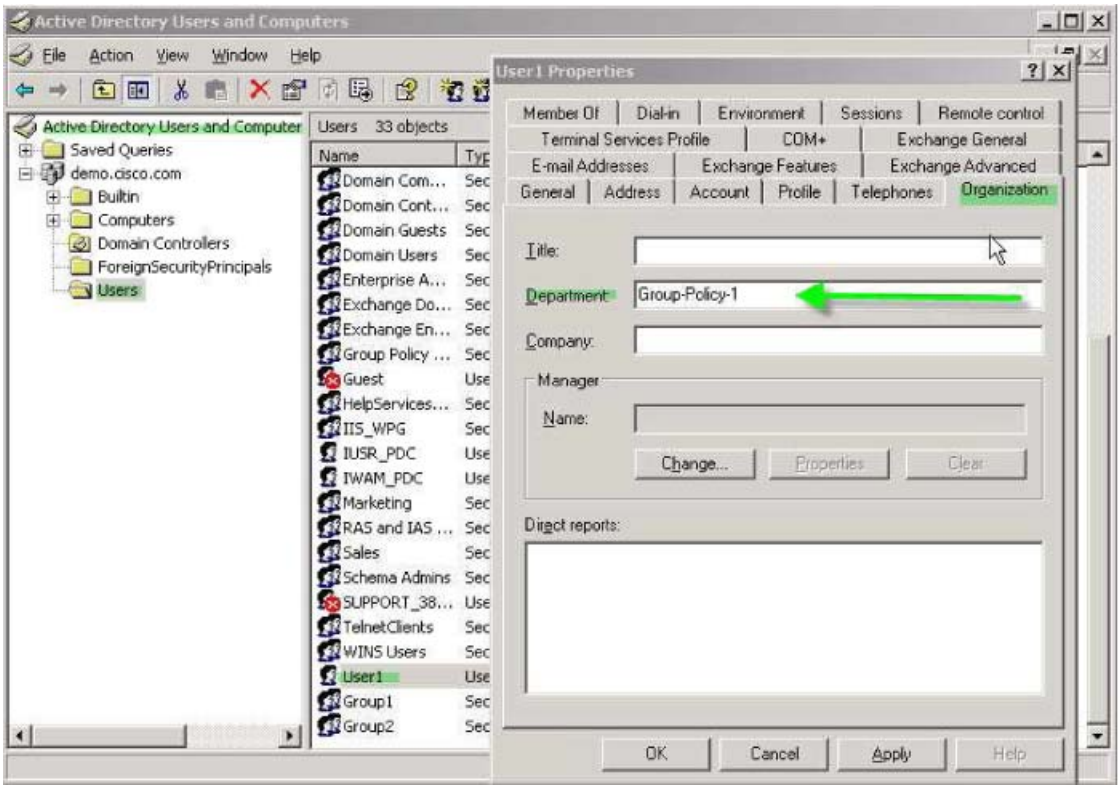
要在 AD LDAP 服务器上为用户配置属性，请执行以下步骤：

步骤 1　右键单击该用户。

系统将显示 Properties 对话框 （请参阅图 9-4）。

步骤 2　点击 **Organization** 选项卡，在 Department 字段中输入 **Group-Policy-1**。

图 9-4　　AD/LDAP 部门属性



步骤 3　为步骤 1 中显示的 LDAP 配置定义一个属性映射。

以下示例展示如何将 AD 属性 Department 映射到思科属性 IETF-Radius-Class。

```
hostname(config)# ldap attribute-map group_policy
hostname(config-ldap-attribute-map)# map-name Department IETF-Radius-Class
```

步骤 4　将 LDAP 属性映射关联到 AAA 服务器。

以下示例进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您在步骤 3 中创建的属性映射 group_policy：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map group_policy
```

步骤 5　在 ASA 上添加新的组策略，配置将分配给该用户的所需策略属性。以下示例创建 Group-policy-1，即在服务器的 Department 字段中输入的名称。

```
hostname(config)# group-policy Group-policy-1 external server-group LDAP_demo
hostname(config-aaa-server-group)#
```

步骤 6　像用户一样建立 VPN 连接，并验证会话是否会继承 Group-Policy1 中的属性 （以及默认组策略中的任何其他适用属性）。

步骤 7　通过从特权 EXEC 模式启用 **debug ldap 255** 命令，监控 ASA 和该服务器之间的通信。以下是此命令的示例输出，此输出已经过编辑，以便提供关键信息。

```
[29] Authentication successful for user1 to 10.1.1.2
[29] Retrieving user attributes from server 10.1.1.2
[29] Retrieved Attributes:
[29] department: value = Group-Policy-1
[29] mapped to IETF-Radius-Class: value = Group-Policy-1
```

为 AnyConnect 隧道实施静态 IP 地址分配

在此示例中，将会配置 AnyConnect 客户端用户 Web1，以便接收静态 IP 地址。然后在 AD LDAP 服务器上的 Dialin 选项卡的 Assign Static IP Address 字段中输入地址。此字段使用 msRADIUSFramedIPAddress 属性。创建将此属性映射到 Cisco 属性 IETF-Radius-Framed-IP-Address 的属性映射。

在身份验证过程中，ASA 从服务器检索 physicalDeliveryOfficeName 的值，将该值映射到 Cisco 属性 IETF-Radius-Framed-IP-Address，并向 User1 提供静态地址。

以下示例适用于全隧道客户端，包括 IPSec 客户端和 SSL VPN 客户端 （AnyConnect 客户端 2.x 和 SSL VPN 客户端）。

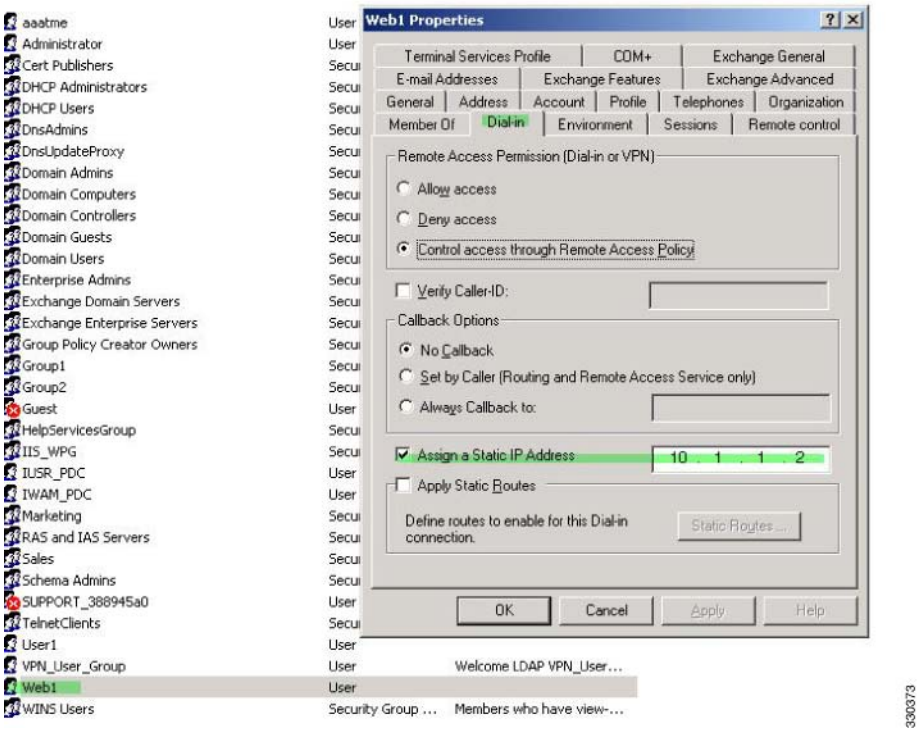
要在 AD/LDAP 服务器上配置用户属性，请执行以下步骤：

步骤 1　右键单击该用户名。

系统将显示 Properties 对话框 （请参阅图 9-5）。

步骤 2　点击 **Dialin** 选项卡，选择 **Assign Static IP Address** 复选框，然后输入 IP 地址 10.1.1.2。

图 9-5　　分配静态 IP 地址



步骤 3　为步骤 1 中显示的 LDAP 配置创建一个属性映射。

以下示例展示如何将 Static Address 字段使用的 AD 属性 msRADIUSFramedIPAddress 映射至 Cisco 属性 IETF-Radius-Framed-IP-Address：

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

步骤 4　将 LDAP 属性映射关联到 AAA 服务器。

以下示例进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您在步骤 3 中创建的属性映射 static_address：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

步骤 5　通过使用 **show run all vpn-addr-assign** 命令查看此部分的配置，验证是否已配置 **vpn-address-assignment** 命令来指定 AAA：

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa    << 确保配置此项 >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

步骤 6　使用 AnyConnect 客户端建立与 ASA 的连接。请观察以下内容：

- 欢迎信息以与无客户端连接相同顺序接收 （请参阅图 9-6）。
- 用户会收到在服务器上配置并映射至 ASA 的 IP 地址 （请参阅图 9-7）。

图 9-6　　验证 AnyConnect 会话的欢迎信息

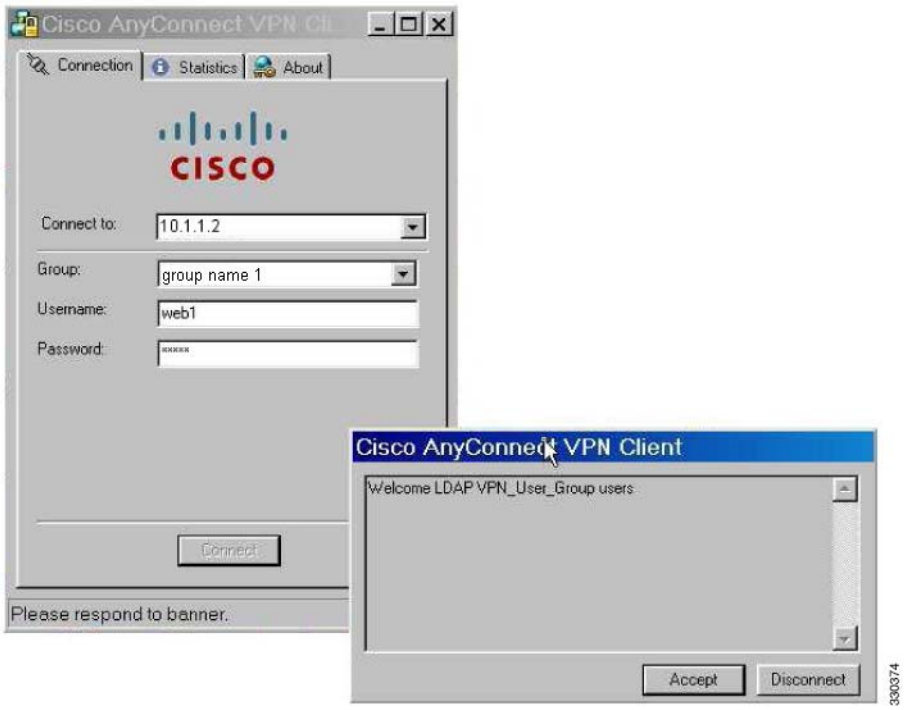


图 9-7　　建立的 AnyConnect 会话

步骤 7　使用 **show vpn-sessiondb svc** 命令来查看会话详细信息，并验证分配的地址：

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

实施拨入允许或拒绝访问

以下示例创建指定用户允许的隧道协议的 LDAP 属性映射。您可以将 Dialin 选项卡上的允许访问和拒绝访问设置映射至思科属性 Tunneling-Protocol，该属性支持表 9-1中显示的映射值。

表 9-1　　思科 Tunneling-Protocol 属性的位映射值

值	隧道协议
1	PPTP
2	L2TP
4[1]	IPsec (IKEv1)
8[2]	L2TP/IPsec
16	无客户端 SSL

表 9-1　思科 Tunneling-Protocol 属性的位映射值 （续）

值	隧道协议
32	SSL 客户端 - AnyConnect 或 SSL VPN 客户端
64	IPsec (IKEv2)

1. 不同时支持 IPsec 和经由 IPsec 的 L2TP。因此，值 4 和 8 是互相排斥的。
2. 请参阅注释 1。

使用此属性创建协议的允许访问 (TRUE) 或拒绝访问 (FALSE) 条件，并实施允许用户访问的方法。

对于此简化示例，通过映射隧道协议 IPsec/IKEv1 (4)，您可以为该思科 VPN 客户端创建允许 (true) 条件。您还可以映射 WebVPN (16) 和 SVC/AC (32)，它们会被映射为值 48 (16+32)，以及创建拒绝 (false) 条件。这允许用户使用 IPsec 连接到 ASA，但是任何使用无客户端 SSL 或 AnyConnect 客户端的连接尝试会被拒绝。

位于以下 URL 的技术说明 *《ASA/PIX：通过 LDAP 配置将 VPN 客户端映射至 VPN 组策略的示例》* 中提供了实施拨入允许访问或拒绝访问的另一示例：

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008089149d.shtml

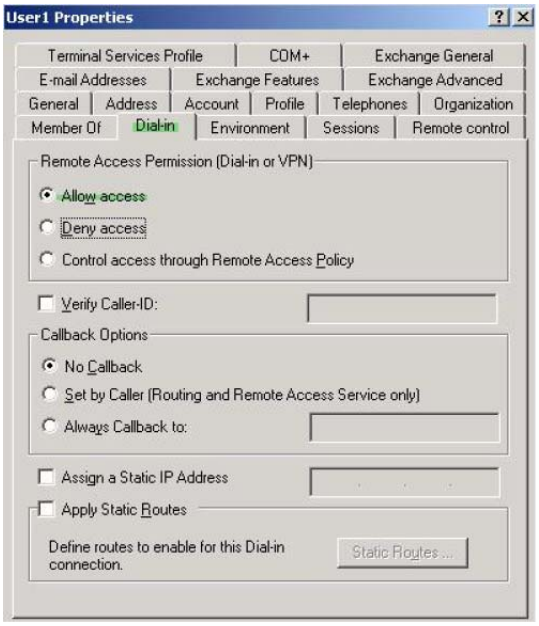
要在 AD/LDAP 服务器上配置用户属性，请执行以下步骤：

步骤 1　右键点击该用户。

系统将显示 Properties 对话框。

步骤 2　点击 **Dial-in** 选项卡，然后点击 **Allow Access** 单选按钮 （图 9-8）。

图 9-8　AD/LDAP User1 - 允许访问



注　如果您通过 Remote Access Policy 选项选择控制访问，则服务器不会返回值，实施的权限会基于 ASA 的内部组策略设置。

步骤 3　创建一个属性映射允许 IPsec 和 AnyConnect 连接，但是拒绝无客户端 SSL 连接。

以下示例展示如何创建映射 tunneling_protocols，使用 **map-name** 命令将 Allow Access 设置使用的 AD 属性 msNPAllowDialin 映射到思科属性 Tunneling-Protocols，以及使用 **map-value** 命令添加映射值：

```
hostname(config)# ldap attribute-map tunneling_protocols
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

步骤 4　将 LDAP 属性映射关联到 AAA 服务器。

以下示例进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您在步骤 2 中创建的属性映射 tunneling_protocols：

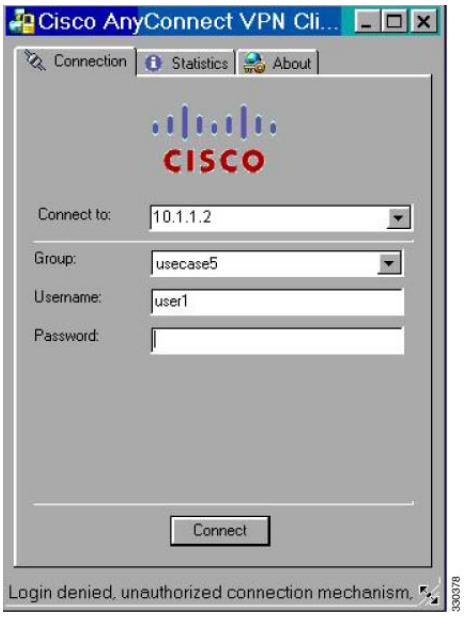
```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

步骤 5　验证属性映射是否如配置工作。

步骤 6　使用无客户端 SSL、 AnyConnect 客户端和 IPSec 客户端尝试连接。无客户端和 AnyConnect 连接应该会失败，并且应该会通知用户，未经授权的连接机制是连接失败的原因。 IPSec 客户端应进行连接，因为根据属性映射， IPsec 是允许的隧道协议 （请参阅图 9-9和图 9-10）。

图 9-9　　无客户端用户的登录被拒绝消息

图 9-10　　AnyConnect 客户端用户的登录被拒绝消息



实施登录时段和时间规则

以下示例展示如何配置和实施允许无客户端 SSL 用户 （例如业务合作伙伴）访问网络的时段。

在 AD 服务器上，使用 Office 字段输入合作伙伴的名称，该字段使用 physicalDeliveryOfficeName 属性。然后我们在 ASA 上创建一个属性映射，以便将该属性映射到思科属性 Access-Hours。在身份验证过程中， ASA 会检索 physicalDeliveryOfficeName 的值，并将其映射到 Access-Hours。

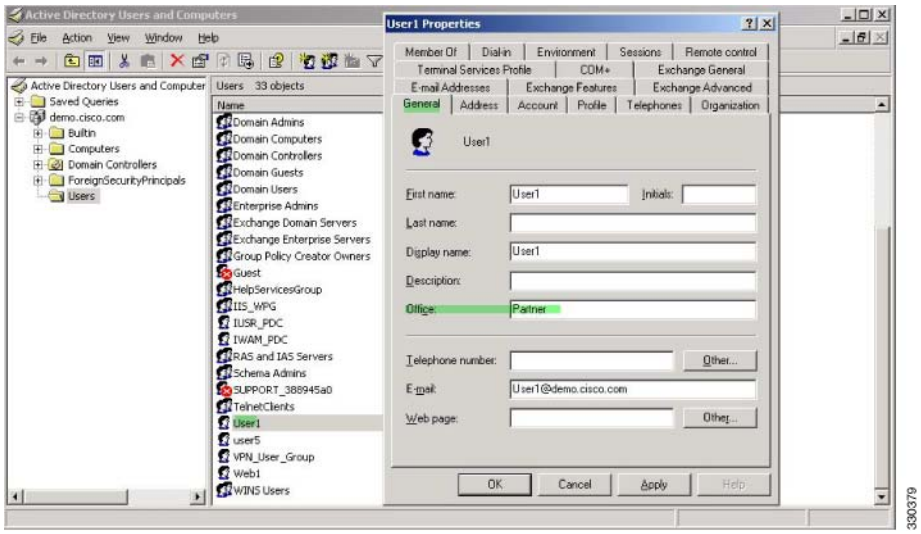
要在 AD/LDAP 服务器上配置用户属性，请执行以下步骤：

步骤 1　选择该用户，然后右键单击 **Properties**。

系统将显示 Properties 对话框 （请参阅图 9-11）。

步骤 2　点击 **Search** 选项卡。

图 9-11　　Active Directory Properties 对话框



步骤 3　创建属性映射。

以下示例展示如何创建属性映射 access_hours，并将 Office 字段使用的 AD 属性 physicalDeliveryOfficeName 映射到思科属性 Access-Hours。

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

步骤 4　将 LDAP 属性映射关联到 AAA 服务器。

以下示例进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您在步骤 3 中创建的属性映射 access_hours：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

步骤 5　为服务器上允许的每个值配置时间范围。

以下示例将合作伙伴访问时段配置为周一至周五上午 9 点到下午 5 点：

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

为本地用户创建组策略的示例

先决条件

此操作步骤描述如何编辑现有用户。要添加用户，请选择 **Configuration > Remote Access VPN > AAA/Local Users**，然后点击 **Add**。有关详细信息，请参阅常规操作配置指南。

准则

默认情况下，对于 Edit User Account 屏幕上的每项设置，均将选中 **Inherit** 复选框，这表明用户帐户从默认组策略 DfltGrpPolicy 继承该设置的值。

要覆盖每项设置，请取消选中 **Inherit** 复选框，并输入新值。下面的详细步骤介绍 Edit User Account 屏幕上的每项设置。

详细步骤

步骤 1　启动 ASDM 并选择 **Configuration > Remote Access VPN > AAA/Local Users > Local Users**。

步骤 2　选择要配置的用户，然后点击 **Edit**。

系统将打开 Edit User Account 屏幕。

步骤 3　在左侧窗格中，点击 **VPN Policy**。

步骤 4　为该用户指定一个组策略。用户策略将继承该组策略的属性。如果此屏幕有其他字段设为从默认组策略 **Inherit** 配置，在此组策略中指定的属性将优先于默认组策略中设置的那些属性。

步骤 5　指定可供用户使用的隧道协议，或是否从组策略继承值。选择所需的 **Tunneling Protocols** 复选框，以便选择以下某个隧道协议：

- 无客户端 SSL VPN （通过 SSL/TLS 的 VPN）使用网络浏览器建立与 VPN 集中器连接的安全远程访问隧道；不需要软件和硬件客户端。无客户端 SSL VPN 可提供广泛企业资源的便捷访问，包括企业网站、支持网络的应用程序、 NT/AD 文件共享 （支持网络）、邮件和几乎任何计算机中的可访问 HTTPS 互联网网站的其他基于 TCP 的应用程序。
- SSL VPN 客户端允许用户在下载思科 AnyConnect 客户端应用程序后进行连接。第一次，用户可以使用无客户端 SSL VPN 连接来下载此应用程序。随后，每当用户连接时，都会视需要进行客户端更新。
- IPsec IKEv1 - IP 安全协议。 IPsec 被视为最安全的协议，为 VPN 隧道提供最完整的架构。站点间 （对等）连接和思科 VPN 客户端到 LAN 连接均可使用 IPsec IKEv1。
- IPsec IKEv2 - 由 AnyConnect 安全移动客户端提供支持。将 IPsec 与 IKEv2 配合使用的 AnyConnect 连接提供高级功能，如软件更新、客户端配置文件、GUI 本地化（转换）和定制、Cisco Secure Desktop 和 SCEP 代理。
- 采用互联网协议安全的第二层隧道协议允许具有若干公共 PC 和移动 PC 操作系统的随附的 VPN 客户端远程用户通过公用 IP 网络与 ASA 和专用企业网络建立安全连接。

注　如未选择协议，系统会显示错误消息。

步骤 6　指定要使用的过滤器 （IPv4 或 IPv6），或者是否从组策略继承值。过滤器由规则组成，这些规则根据诸如源地址、目标地址和协议之类的条件来确定允许还是拒绝隧道数据包通过 ASA。要配置过滤器和规则，请选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > General > More Options > Filter**。

点击 **Manage** 以显示 ACL Manager 窗格，可以在其中添加、编辑及删除 ACL 和 ACE。

步骤 7　指定继承连接配置文件 （隧道组）锁定还是使用所选隧道组锁定 （如果有）。选择特定锁定会限定用户只能通过此组进行远程访问。隧道组锁定通过检查在 VPN 客户端上配置的组是否与用户分配的组相同来限制用户。如果不相同， ASA 将阻止用户进行连接。如果未选中 Inherit 复选框，则默认值为 None。

步骤 8　指定是否从该组继承 Store Password on Client System 设置。取消选中 **Inherit** 复选框以激活 Yes 和 No 单选按钮。点击 **Yes** 以将登录密码存储在客户端系统上 （该选项可能不太安全）。点击 **No** （默认）以要求用户输入每个连接的密码。为确保最高安全性，我们建议您 *不允许*密码存储。此参数对于 VPN 3002 的交互式硬件客户端身份验证或个人用户身份验证没有影响。

步骤 9　指定要应用于此用户的访问时长策略，为用户创建新的访问时长策略，或者保持选中 Inherit 框。默认值为 Inherit，或者，如果未选中 Inherit 复选框，则默认值为 Unrestricted。

点击 **Manage** 以打开 Add Time Range 对话框，可以在其中指定一组新的访问时长。

步骤 10　指定用户执行的同时登录数。 Simultaneous Logins 参数可指定此用户同时登录的最大数量。默认值为 3。最小值为 0，表示禁止登录并阻止用户访问。

注　在没有最大限制时，允许多个同时连接可能会降低安全性并影响性能。

步骤 11　为用户连接时间指定**最大连接时间** （以分钟为单位）。此时间结束时，系统会终止连接。最小值为 1 分钟，最大值为 2147483647 分钟 （4000 多年，如果我们都那么幸运）。要允许无限连接时间，请选中 **Unlimited** 复选框 （默认）。

步骤 12　指定用户的空闲超时 （以分钟为单位）。如果在此期间，用户在连接上没有通信活动，系统会终止连接。最短时间为 1 分钟，最长时间为 10080 分钟。该值不适用于无客户端 SSL VPN 连接的用户。

步骤 13　配置会话警报间隔。如果您取消选中 Inherit 复选框，系统将自动选中 Default 复选框。这将会话警报间隔设置为 30 分钟。如果您要指定新值，可以取消选中 Default 复选框，并在分钟框中指定 1 至 30 分钟的会话警报间隔。

步骤 14　配置空闲警报间隔。如果您取消选中 Inherit 复选框，系统将自动选中 Default 复选框。这会将空闲警报间隔设置为 30 分钟。如果您要指定新值，可以取消选中 Default 复选框，并在分钟框中指定 1 至 30 分钟的会话警报间隔。

步骤 15　要为此用户设置专用 IPv4 地址，请在 Dedicated IPv4 Address (Optional) 区域中输入 IPv4 地址和子网掩码。

步骤 16　要为此用户设置专用 IPv6 地址，请在 Dedicated IPv6 Address (Optional) 区域中输入一个带 IPv6 前缀的 IPv6 地址。 IPv6 前缀表示 IPv6 地址所驻留的子网。

步骤 17　要配置无客户端 SSL 设置，可以在左侧窗格中，点击 **Clientless SSL VPN**。要覆盖每项设置，请取消选中 **Inherit** 复选框，并输入新值。

步骤 18　点击 **Apply**。

更改会保存到运行配置。

第 2 部分

无客户端 SSL VPN

第 10 章

无客户端 SSL VPN

无客户端 SSL VPN 简介

无客户端 SSL VPN 让最终用户可以使用支持 SSL 的网络浏览器随时随地安全地访问公司网络上的资源。用户首先利用无客户端 SSL VPN 网关进行身份验证，然后允许用户访问预配置的网络资源。

注 启用无客户端 SSL VPN 时，不支持安全情景 （也称为多模防火墙）和主动/主动状态故障切换。

无客户端 SSL VPN 使用网络浏览器创建访问 ASA 的安全远程访问隧道，而不要求使用软件或硬件客户端。通过它可以从无法通过 HTTP 连接互联网的几乎任何设备安全和便捷地访问各种网络资源以及支持网络的和旧版的应用。具体包括：

- 内部网站。
- 支持网络的应用。
- NT/Active Directory 文件共享。
- 邮件代理，包括 POP3S、 IMAP4S 和 SMTPS。
- Microsoft Outlook Web Access Exchange Server 2000、 2003 和 2007。
- 8.4(2) 和更低版本中适用于 Exchange Server 2010 的 Microsoft Web App。
- Application Access （对其他基于 TCP 的应用的智能隧道或端口转发访问）。

无客户端 SSL VPN 使用安全套接字层协议及其后继传输层安全性协议 (SSL/TLS1) 为远程用户和您配置为内部服务器的特定受支持的内部资源之间提供安全连接。ASA 将识别必须代理的连接，并且 HTTP 服务器会与身份验证子系统交互以对用户进行身份验证。

网络管理员以组为基础为无客户端 SSL VPN 的用户提供对资源的访问。用户无权直接访问内部网络上的资源。

先决条件

关于 9.0 版本 ASA 支持的平台和浏览器，请参阅*支持的 VPN 平台、思科 ASA 系列*。

准则和限制

- ActiveX 页面要求您启用 ActiveX 中继或为关联的组策略输入 **activex-relay**。如果您这么做或给策略分配一个智能隧道列表，并且终端上的浏览器代理特例列表指定了一个代理，则用户必须向该列表添加一个 “shutdown.webvpn.relay.” 条目。
- ASA 不支持从 Windows 7、Vista、Internet Explorer 8 至 10、Mac OS X 或 Linux 对 Windows Shares (CIFS) Web Folders 进行无客户端访问。
- 证书身份验证，包括美国国防部通用存取卡和智能卡，仅适用于 Safari 钥匙串。
- ASA 不支持无客户端 SSL VPN 连接的 DSA 或 RSA 证书。
- 一些基于域的安全产品要求可能高于源自 ASA 的这些请求。
- 不支持在模块化策略框架下配置控件检查和其他检查功能。
- NAT 或 PAT 都不适用于客户端。
- 无客户端 SSL VPN 某些组件需要在 Mac OS X v10.7 和更低版本中运行的 Java Runtime Environment (JRE)。默认情况下不安装 Java。有关如何在 Mac OS X 上安装 Java 的详细信息，请参阅 http://java.com/en/download/faq/java_mac.xml。

当您为无客户端门户配置了几个组策略时，它们将显示在登录页面上的下拉列表中。当列表中的第一个组策略要求提供证书时，用户必须具有匹配的证书。如果某些组策略不使用证书，则必须将列表配置为首先显示非证书策略。或者，您可能希望创建一个名称为 “0-Select-a-group” 的虚拟组策略。

提示　您可以通过按照字母顺序给组策略命名或在其名称前面加上数字前缀，从而控制首先显示哪个策略。例如 1-AAA, 2-Certificate。

基本无客户端 SSL VPN 配置

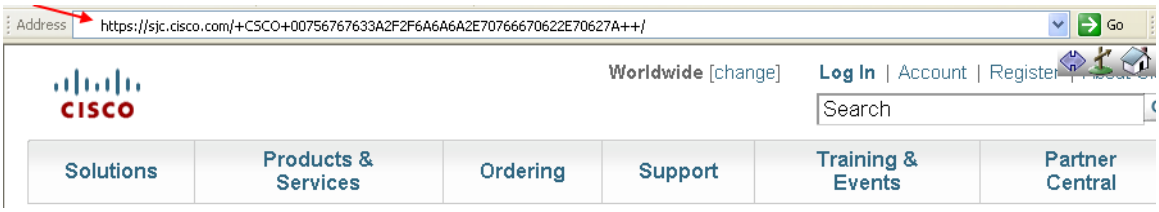
修订日期：2014 年 3月 12 日

无客户端 SSL VPN 安全预防措施

默认情况下，ASA 允许所有门户网站流量流向所有网络资源（例如 HTTPS、CIFS、RDP 和插件）。无客户端 SSL VPN 将每个 URL 重写入仅对 ASA 有意义的 URL。用户无法使用此 URL 确认其已连接至其所请求的网站。为了避免用户遭受钓鱼网站所带来的风险，请将网络 ACL 分配给为无客户端访问配置的策略（如组策略和/或动态访问策略），以控制源自门户网站的流量。我们建议关闭这些策略上的 URL Entry，以防止用户弄不清哪些内容才是可访问的。

图 11-1　　用户输入的 URL 示例

图 11-2　　安全设备重写以及浏览器窗口中显示的相同 URL



详细步骤

步骤 1　为需要无客户端 SSL VPN 访问权限的所有用户配置组策略，并仅为该组策略启用无客户端 SSL VPN。

步骤 2　在组策略打开后，选择 **General** > **More Options** > **Web ACL**，并点击 **Manage**。

步骤 3　创建网络 ACL 以执行以下操作之一：

- 仅允许访问专用网络内的特定目标。
- 仅允许访问专用网络，拒绝互联网访问，或仅允许访问信誉良好的站点。

步骤 4　将网络 ACL 分配给已为无客户端 SSL VPN 访问配置的任何策略（组策略和/或动态访问策略）。要将网络 ACL 分配给 DAP，请编辑 DAP 记录，并在 **Network ACL Filters** 选项卡上选择 Web ACL。

步骤 5　关闭*门户网站网页*上的 URL Entry，该网页在建立基于浏览器的连接后打开。点击组策略门户网站帧和 DAP **Functions** 选项卡上 URL Entry 旁边的 **Disable**。要关闭 DAP 上的 URL Entry，请使用 ASDM 编辑 DAP 记录，点击 **Functions** 选项卡，并选中 URL Entry 旁边的 **Disable**。

步骤 6　指示用户在门户网站网页上方本机浏览器地址字段中输入外部 URL，或另行打开一个浏览器窗口，以访问外部站点。

配置无客户端 SSL VPN 访问

在配置无客户端 SSL VPN 访问时，可执行以下操作：

- 为无客户端 SSL VPN 会话启用或关闭 ASA 界面。
- 为无客户端 SSL VPN 连接选择端口。
- 设置并行无客户端 SSL VPN 会话的最大数量。

详细步骤

步骤 1　要为无客户端访问配置或创建组策略，请选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies** 窗格。

步骤 2　导航至 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**。

a. 为每个 ASA 界面启用或关闭 **Allow Access**。

Interface 列将列出已配置的接口。WebVPN Enabled 字段显示界面上无客户端 SSL VPN 的状态。Yes 旁边的绿色勾号表示无客户端 SSL VPN 已启用。 No 旁边的红圈表示无客户端 SSL VPN 已关闭。

b. 点击 **Port Setting**，然后输入要用于无客户端 SSL VPN 会话的端口号 （1 至 65535）。默认值为 443。如果更改端口号，则所有当前无客户端 SSL VPN 连接均将终止，且当前用户必须重新连接。系统还将提示您重新连接 ASDM 会话。

步骤 3　导航至 **Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions**，然后在 Maximum Other VPN Sessions 字段中输入要允许的无客户端 SSL VPN 会话的最大数。

验证无客户端 SSL VPN 服务器证书

在通过无客户端 SSL VPN 连接至支持 SSL 的远程服务器时，务必知悉您可信任该远程服务器，且该服务器实际上就是您在尝试连接的服务器。 ASA 9.0 引入了以下支持功能：根据无客服端 SSL VPN 的受信任证书颁发机构 (CA) 证书的列表执行 SSL 服务器证书验证。

在使用 HTTPS 协议连接至带有网络浏览器的远程服务器时，该服务器提供证书颁发机构 (CA) 签署的数字证书进行自我标识。网络浏览器包括用于验证服务器证书有效性的 CA 证书集合。这是一种形式的公共密钥基础结构 (PKI)。

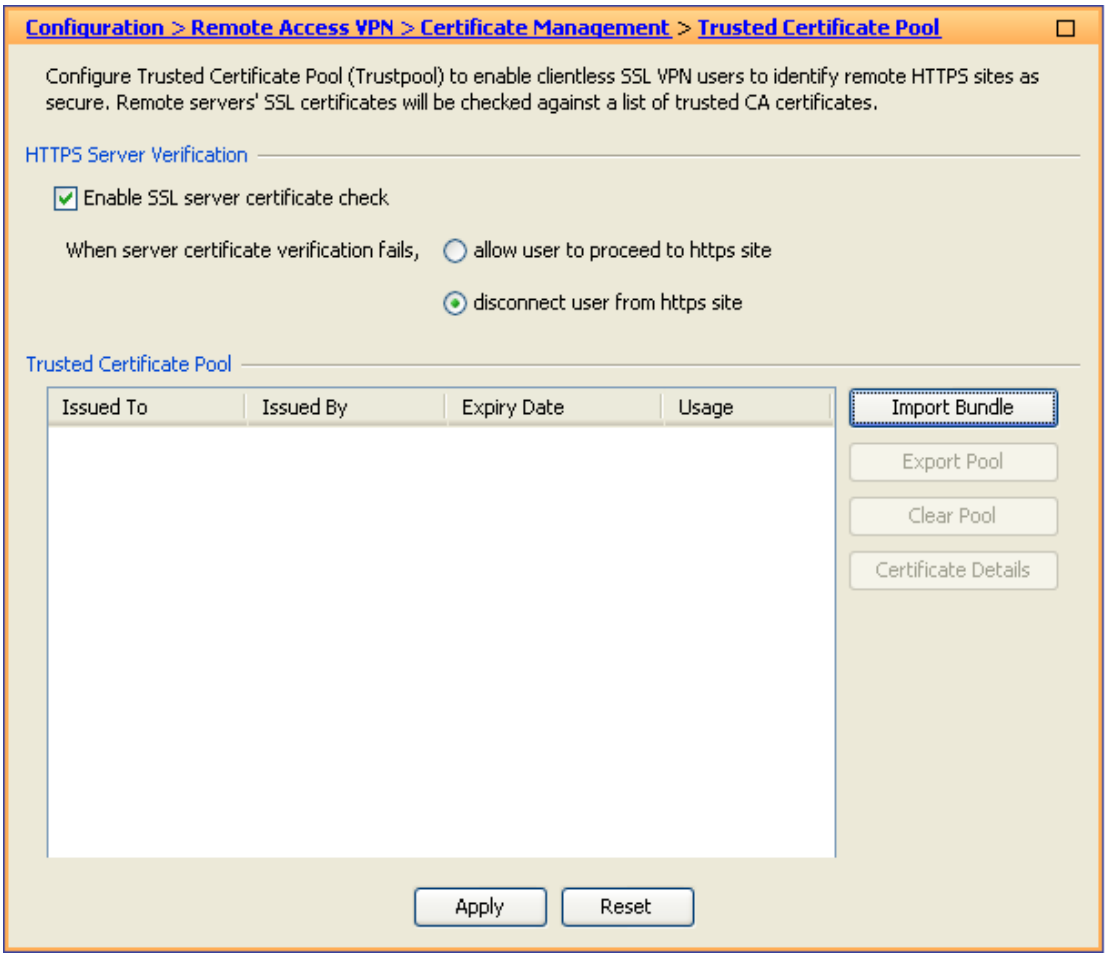
ASA 提供 trustpool 形式的受信任池证书管理设施。这可视为表示多个已知 CA 证书的信任点的特殊案例。ASA 包括一个默认的证书捆绑包，与随网络浏览器提供的证书捆绑包相似。只有管理员后才会激活它。

注　ASA trustpool 与 Cisco IOS trustpool 类似，但不完全相同。

启用 HTTP 服务器验证

步骤 1　在 ASDM 中，选择 **Configuration** > **Remote Access VPN** > **Certificate Management** > **Trusted Certificate Pool**。

图 11-3　在 ASDM 中，启用 HTTPS 服务器验证



步骤 2　选择 **Enable SSL Certificate Check** 复选框。

步骤 3　如果无法验证服务器，请点击 **Disconnect User From HTTPS Site** 以断开连接。或者，点击 **Allow User to Proceed to HTTPS Site**，允许用户继续进行连接，即使检查失败。

步骤 4　点击 **Apply** 保存更改。

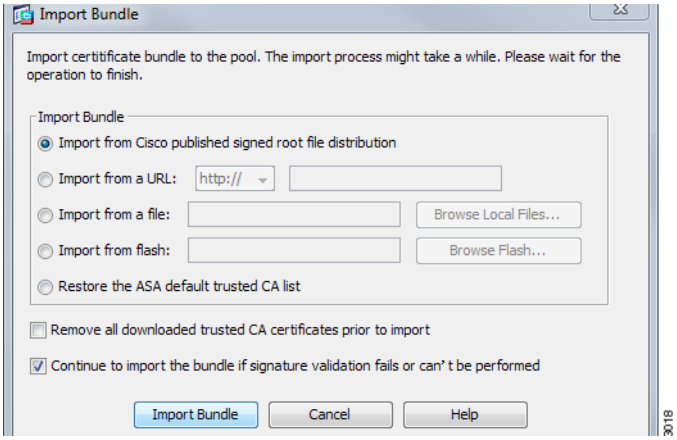
导入证书捆绑包

可用以下格式之一从多个位置导入各个证书或证书捆绑包：

- pkcs7 结构中封装的 DER 格式的 x509 证书。
- PEM 格式的串连 x509 证书文件 （包括 PEM 报头）。

步骤 1　在 ASDM 中，选择 **Configuration** > **Remote Access VPN** > **Certificate Management** > **Trusted Certificate Pool**。

步骤 2　点击 **Import Bundle**。



步骤 3　选择捆绑包的位置：

- 如果捆绑包存储在计算机上，请依次点击 **Import From a File** 和Browse Local Files，并选择该捆绑包。
- 如果捆绑包存储在 ASA 闪存文件系统中，请依次点击 **Import From Flash** 和 **Browse Flash**，并选择文件。
- 如果捆绑包托管在服务器上，请点击 **Import From a URL**，从列表中选择协议，然后在字段中输入 URL。
- 如果选择 Continue to import the bundle if signature validation fails or cannot be performed，则可导入捆绑包，并在稍后修复各个证书错误。如果任何证书导入失败，则请取消选中该选项以使整个捆绑包导入失败。

步骤 4　点击 **Import Bundle**。或者，点击 **Cancel** 放弃更改。

注　可选中 **Remove All Downloaded Trusted CA Certificates Prior to Import** 复选框，以在导入新捆绑包之前清除 trustpool。

导出 Trustpool

如已正确配置 trustpool，则应导出该池。这时，您就可恢复 trustpool，例如，导出后移除已添加至 trustpool 的证书。可将该池导出到 ASA 闪存文件系统或本地文件系统。

在 ASDM 中，选择 **Configuration** > **Remote Access VPN** > **Certificate Management** > **Trusted Certificate Pool**，然后点击 **Export Pool**。

步骤 1　点击 **Export to a File**。

步骤 2　点击 **Browse Local Files**。

步骤 3　选择要将 trustpool 保存到的文件夹。

步骤 4　在 **File Name** 框中，输入 trustpool 的唯一易记名称。

步骤 5　点击 **Select**。

步骤 6　点击 **Export Pool to save the file**。或者，点击 **Cancel** 停止保存。

移除证书

要移除所有证书，在 ASDM 中，选择 **Configuration** > **Remote Access VPN** > **Certificate Management** > **Trusted Certificate Pool**，然后点击 **Clear Pool**。

注　在清除 trustpool 之前，应导出当前 trustpool，以便能够恢复当前设置。

恢复默认受信任证书颁发机构列表

要恢复默认受信任证书颁发机构 (CA) 列表，在 ASDM 中，选择 **Configuration** > **Remote Access VPN** > **Certificate Management** > **Trusted Certificate Pool**，然后依次点击 **Restore Default Trusted CA List** 和 **Import Bundle**。

更新 Trustpool

如果存在以下任一种情况，则应更新 trustpool：

- trustpool 中的任何证书即将到期或已重新发布。
- 已发布的 CA 证书捆绑包包含特定应用所需的其他证书。

完整更新将替换 trustpool 中的所有证书。

实用更新可供您添加新证书或替换现有证书。

移除证书捆绑包

清除 trustpool 将移除不属于默认捆绑包的所有证书。

无法移除默认捆绑包。要清除 trustpool，在 ASDM 中，选择 **Configuration** > **Remote Access VPN** > **Certificate Management** > **Trusted Certificate Pool**，然后点击 **Clear Pool**。

Java 代码签名人

代码签名会将数字签名附加至可执行代码本身。此数字签名提供足够信息以对签名人进行身份验证，并确保自签名以来代码尚未后续修改。

代码签名人证书是特殊证书，其关联私钥用于创建数字签名。代码签名证书从 CA 获取，已签名代码本身表示证书来源。

从下拉列表中选择要在 Java 对象签名中使用的已配置证书。

要配置 Java Code Signer，请选择 Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Java Code Signer。

对于无客户端 SSL VPN 转换的 Java 对象，可随后使用与信任点关联的 PKCS12 数字证书对其进行签名。在 Java Trustpoint 窗格中，可配置无客户端 SSL VPN Java 对象签名设施，以使用源自指定信任点位置的 PKCS12 证书和密钥材料。

要导入 trustpoint，请选择 **Configuration > Properties > Certificate > Trustpoint > Import**。

配置浏览器对插件的访问

以下各节介绍如何为无客户端 SSL VPN 浏览器访问集成浏览器插件：

- 第 11-8 页上的为安装插件准备安全设备
- 第 11-9 页上的安装思科重新分发的插件
- 第 11-10 页上的提供对 Citrix XenApp 服务器的访问

浏览器插件是网络浏览器在执行专用功能时 （例如，将客户端连接至浏览器窗口中的服务器）调用的一个单独程序。借助于 ASA，可在无客户端 SSL VPN 会话中导入要下载至远程浏览器的插件。当然，思科将测试其重新分发的插件，在某些情况下，将测试其无法重新分发的插件的连接性。但是，我们建议不要导入目前支持流媒体的插件。

在闪存设备上安装插件时， ASA 将执行以下操作：

- （仅限思科分发的插件）解压缩 URL 中指定的 jar 文件。
- 将文件写入 ASA 文件系统。
- 填充 ASDM 中 URL 属性旁边的下拉列表。
- 为所有未来无客户端 SSL VPN 会话启用插件，然后将主菜单选项和选项添加至门户网站网页 Address 字段旁边的下拉列表。

表 11-1 显示在添加以下各节中描述的插件时对门户网站网页的主菜单和 Address 字段做出的更改。

*不是推荐的插件。

表 11-1　　无客户端 SSL VPN 门户网站网页上插件的效果

插件	已添加至门户网站网页的主菜单选项	已添加至门户网站网页的 Address 字段选项
ica	Citrix MetaFrame Services	ica://
rdp	Terminal Servers	rdp://
rdp2*	Terminal Servers Vista	rdp2://
ssh,telnet	Secure Shell	ssh://
	Telnet Services (supporting v1 and v2)	telnet://
vnc	Virtual Network Computing services	vnc://

当用户在无客户端 SSL VPN 会话中点击门户网站网页上的关联菜单选项时，门户网站网页显示界面窗口和帮助窗格。用户可选择下拉列表中显示的协议，并在 Address 字段中输入 URL，以建立连接。插件支持单点登录 (SSO)。请参阅第 15-5 页上的使用 HTTP 表单协议配置 SSO，了解实施详细信息。

先决条件

- 无客户端 SSL VPN 只有在 ASA 上启用才能提供对插件的远程访问。
- 要为插件配置 SSO 支持，需安装插件，添加书签条目以显示服务器链接，并在添加书签时指定 SSO 支持。
- 远程使用所需的最低访问权限属于宾客特权模式。
- 使用插件需要安装 ActiveX 或 Oracle Java Runtime Environment (JRE)；请参阅兼容性矩阵了解版本要求。

限制

注 远程桌面协议插件不支持用会话代理程序进行负载平衡。由于协议处理源自会话代理程序的重定向的方法不当，连接失败。如未使用会话代理程序，插件将发挥正常作用。

- 插件支持单点登录 (SSO)。它们使用所输入的*相同凭据*打开无客户端 SSL VPN 会话。因为插件不支持宏替换，所以，您无法选择对不同的字段（如内部域密码）或 RADIUS 或 LDAP 服务器上的属性执行 SSO。
- 有状态故障转移不保留使用插件建立的会话。出现故障转移后，用户必须重新连接。
- 如果使用无状态故障转移替代有状态故障转移，则无客户端功能（例如书签、自定义和动态访问策略）不会在故障转移 ASA 对之间同步。在发生故障转移时，这些功能不起作用。

为安装插件准备安全设备

在安装插件之前，请按以下所示准备 ASA：

先决条件

确保在 ASA 界面上已启用无客户端 SSL VPN。

限制

请勿将 IP 地址指定为 SSL 证书的通用名称 (CN)。远程用户尝试使用 FQDN 与 ASA 进行通信。远程 PC 必须能够使用 DNS 或 System32\drivers\etc\hosts 文件中的条目解析 FQDN。

转至与标识要为无客户端 SSL VPN 访问提供的插件类型相对应的那部分。

- 第 11-9 页上的安装思科重新分发的插件
- 第 11-10 页上的提供对 Citrix XenApp 服务器的访问

安装思科重新分发的插件

思科重新分发以下基于 Java 的开源组件，作为无客户端 SSL VPN 会话中网络浏览器的插件来访问。

先决条件

确保无客户端 SSL VPN 已在 ASA 的界面上启用。为此，请输入 **show running - config** 命令。

表 11-2　　思科重新分发的插件

协议	说明	重新分布的插件的来源*
RDP	访问 Windows Vista 和 Windows 2003 R2 托管的 Microsoft 终端服务。 支持远程桌面 ActiveX 控件。 我们建议使用支持 RDP 和 RDP2 的此插件。仅支持最高版本为 5.1 的 RDP 和 RDP2 协议。不支持版本 5.2 及更高版本。	http://properjavardp.sourceforge.net/
RDP2	访问 Windows Vista 和 Windows 2003 R2 托管的 Microsoft 终端服务。 支持远程桌面 ActiveX 控件。 **注**　此旧版插件仅支持 RDP2。我们不建议使用此插件；请换用上述 RDP 插件。	http://properjavardp.sourceforge.net/
SSH	安全外壳 Telnet 插件可供远程用户建立到远程计算机的安全外壳 （v1 或 v2）或 Telnet 连接。 **注**　由于 JavaSSH 不支持键盘交互身份验证，它不受 SSH 插件 （用于实施不同的身份验证机制）支持。	http://javassh.org/
VNC	虚拟网络计算插件可供远程用户使用显示器、键盘和鼠标查看和控制已打开远程桌面共享（也称为 VNC 服务器或服务）的计算机。此版本更改文本的默认颜色并包含更新的法语和日语帮助文件。	http://www.tightvnc.com/

*有关部署配置和限制的信息，请参阅插件文档。

这些插件可从思科自适应安全设备软件下载站点下载。

详细步骤

步骤 1　在用于建立与 ASA 之间 ASDM 会话的计算机上创建以插件命名的临时目录，并且从思科网站将所需插件下载到插件目录。

步骤 2　选择 **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Portal** > **Client-Server Plug-ins**。

此窗格显示当前加载的可用于无客户端 SSL 会话的插件。还提供这些插件的哈希值和日期。

步骤 3　点击 **Import**。

Import Client-Server Plug-in 对话框打开。

步骤 4　使用以下说明输入 Import Client-Server Plug-in 对话框字段值。

- 插件名称 — 选择以下一个值：
  - **ica**，以提供对 Citrix MetaFrame 或 Web Interface 服务的插件访问。
  - **rdp**，以提供对 Remote Desktop Protocol 服务的插件访问。
  - **ssh,telnet**，以提供对安全外壳*和* Telnet 服务的插件访问。
  - **vnc**，提供对虚拟网络计算服务的插件访问。

注　此菜单中任何未记录的选项为实验性选项，不受支持。

- 选择插件文件的位置 - 选择以下选项之一，并将路径插入其文本字段。
  - Local computer - 在关联的 Path 字段中输入插件的位置和名称，或点击 **Browse Local Files** 并选择插件，然后点击 **Select**。
  - Flash file system - 在关联的 Path 字段中输入插件的位置和名称，或点击 **Browse Flash** 并选择插件，然后点击 **OK**。
  - Remote Server - 根据远程服务器上运行的服务，从关联 Path 属性旁边的下拉菜单中选择 **ftp**、**tftp** 或 **HTTP**。在邻近的文本字段中输入服务器的主机名或地址以及插件路径。

步骤 5　点击 **Import Now**。

步骤 6　点击 **Apply**。

插件现可用于未来无客户端 SSL VPN 会话。

提供对 Citrix XenApp 服务器的访问

作为如何提供无客户端 SSL VPN 浏览器对第三方插件的访问的示例，本节介绍如何添加无客户端 SSL VPN 对 Citrix XenApp 服务器客户端的支持。

借助于 ASA 上安装的 Citrix 插件，无客户端 SSL VPN 用户可以使用 ASA 的连接访问 Citrix XenApp 服务。

有状态故障转移不保留使用 Citrix 插件建立的会话。Citrix 用户必须在故障转移后重新进行身份验证。

要提供对 Citrix 插件的访问，请遵循以下各节中的操作步骤。

- 为无客户端 SSL VPN 访问准备 Citrix XenApp 服务器
- 创建和安装 Citrix 插件

为无客户端 SSL VPN 访问准备 Citrix XenApp 服务器

必须将 Citrix Web Interface 软件配置为在不使用 (Citrix) “安全网关” 的模式下运行。否则，Citrix 客户端无法连接至 Citrix XenApp 服务器。

注　如果尚未提供对插件的支持，则必须遵守第 11-8 页上的为安装插件准备安全设备中的说明，才可使用本节内容。

创建和安装 Citrix 插件

详细步骤

步骤 1　从思科软件下载网站下载文件 ica-plugin.zip。

此文件包含思科自定义的可与 Citrix 插件配合使用的文件。

步骤 2　从 Citrix 站点下载 Citrix Java 客户端。

在 Citrix 网站的下载区域，选择 **Citrix Receiver** 和 **Receiver for Other Platforms** 并点击 **Find**。点击 **Receiver for Java** 超链接并下载存档文件。

步骤 3　从存档文件中提取以下文件，然后将它们添加到 ica plugin.zip 文件：

- JICA-configN.jar
- JICAEngN.jar

步骤 4　确保 Citrix Java 客户端随附的 EULA 授予您在网络服务器上部署客户端的权利和权限。

步骤 5　通过使用 ASDM 或在特权 EXEC 模式中输入以下 CLI 命令来安装插件：

import webvpn plug-in protocol ica *URL*

URL 是主机名或 IP 地址以及 ica plugin.zip 文件的路径。

注　提供对 Citrix 会话的 SSO 支持需要添加书签。我们建议您在书签中使用 URL 参数，以方便查看，例如：

ica://10.56.1.114/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

步骤 6　建立 SSL VPN 无客户端会话并点击书签或输入 Citrix 服务器的 URL。

使用 《适用于 Java 的客户端的管理员指南》（根据需要）。

配置端口转发

以下各节介绍端口转发以及如何配置它：

有关端口转发的信息

借助于端口转发，用户可通过无客户端 SSL VPN 连接访问基于 TCP 的应用。此类应用包括：

- Lotus Notes
- Microsoft Outlook
- Microsoft Outlook Express
- Perforce
- Sametime
- Secure FTP (FTP over SSH)
- SSH
- Telnet
- Windows Terminal Service
- XDDTS

其他基于 TCP 的应用也可能起作用，但是，我们尚未对其进行测试。使用 UDP 的协议不起作用。

端口转发是通过无客户端 SSL VPN 连接支持基于 TCP 的应用的传统技术。可以选择使用端口转发，因为您已构建支持此技术的早期配置。

考虑端口转发的以下替代项：

- 智能隧道接入为用户提供以下优势：
  - 智能隧道性能比插件更好。
  - 不同于端口转发，智能隧道不要求用户将本地应用连接至本地本地端口，简化了用户体验。
  - 不同于端口转发，智能隧道不要求用户拥有管理员权限。
- 与端口转发和智能隧道接入不同，插件不需要将客户端应用安装在远程计算机上。

在 ASA 上配置端口转发时，指定应用使用的端口。在配置智能隧道接入时，指定可执行文件的名称或其路径。

先决条件

- 远程主机必须运行以下操作系统的 32 位版本：
  - Microsoft Windows Vista、 Windows XP SP2 或 SP3；或 Windows 2000 SP4。
  - 安装了 Safari 2.0.4(419.3) 的 Apple Mac OS X 10.4 或 10.5。
  - Fedora Core 4
- 远程主机还必须运行 Oracle Java Runtime Environment (JRE) 5 或更高版本。
- Mac OS X 10.5.3 上基于浏览器的 Safari 用户必须标识与 ASA URL 配合使用的客户端证书，由于 Safari 解释 URL 的方法，此 URL 一次用反斜杠，一次不用。例如，
  - https://example.com/
  - https://example.com

  有关详细信息，请转至 Safari, Mac OS X 10.5.3：客户端证书身份验的变更。
- 使用端口转发或智能隧道的 Microsoft Windows Vista 或更高版本的用户必须将 ASA 的 URL 添加至 Trusted Site 区域。要访问 Trusted Site 区域，它们必须启动 Internet Explorer 并选择 **Tools > Internet Options > Security** 选项卡。 Vista（或更高版本）用户还可关闭保护模式以简化智能隧道接入；但是，由于此方法会使计算机更易于遭受攻击，我们建议不要使用此方法。

- 确保 Oracle Java Runtime Environment (JRE) 1.5.x 或更高版本已安装在远程计算机上，以支持端口转发（应用接入）和数字证书。如在运行 JRE 1.4.x 且用户使用数字证书进行身份验证，则应用未能启动，因为 JRE 无法访问网络浏览器证书存储区。

限制

- 端口转发仅支持使用静态 TCP 端口的 TCP 应用。使用动态端口或多个 TCP 端口的应用不受支持。例如，使用端口 22 的 SecureFTP 通过无客户端 SSL VPN 端口转发进行工作，但是使用端口 20 和 21 的标准 FTP 却不是这样。
- 端口转发不支持使用 UDP 的协议。
- 端口转发不支持 Microsoft Outlook Exchange (MAPI) 代理。但是，可为 Microsoft Office Outlook 和 Microsoft Outlook Exchange Server 一起配置智能隧道支持。
- 有状态故障转移不保留使用 Application Access （端口转发或智能隧道接入）建立的会话。出现故障转移后，用户必须重新连接。
- 端口转发不支持与个人数字助理的连接。
- 由于端口转发需要下载 Java 小程序和配置本地客户端，并且，由于这样做需要本地系统的管理员权限，因此，在用户从公共远程系统进行连接时可能无法使用应用。

  Java 小程序显示在其自带窗口中的最终用户 HTML 界面上。它显示可向用户提供的已转发端口列表的内容，以及活动的端口和收发的流量 （以字节为单位）。
- 在使用本地 IP 地址 127.0.0.1 时，端口转发小程序会将本地端口和远程端口显示为同一端口，并且无法由源自 ASA 的无客户端 SSL VPN 连接进行更新。因此，ASA 为本地代理 ID 创建新的 IP 地址 127.0.0.2、 127.0.0.3 等等。由于可以修改主机文件并使用不同的环回，因此远程端口用作小程序中的本地端口。要连接，可使用含主机名的 Telnet，无需指定端口。本地主机文件中提供正确的本地 IP 地址。

为端口转发配置 DNS

端口转发会将远程服务器的域名或其 IP 地址转发至 ASA 以进行解析和连接。换句话说，端口转发小程序接受来自应用的请求并将其转发至 ASA。 ASA 执行适当的 DNS 查询并代表端口转发小程序建立连接。端口转发小程序只对 ASA 执行 DNS 查询。它更新主机文件，以便在端口转发应用尝试执行 DNS 查询时，查询重定向至环回地址。

步骤 1　点击 **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Connection Profiles**。

默认无客户端 SSL VPN 组条目是用于无客户端连接的默认连接配置文件。

步骤 2　如果您的配置将默认无客户端 SSL VPN 组条目用于无客户端连接，请突出显示该组条目，然后点击 **Edit**。否则，突出显示在无客户端连接的配置中使用的连接配置文件，然后点击 **Edit**。

Basic 窗口将打开。

步骤 3　扫描至 DNS 区域并从下拉列表中选择 DNS 服务器。请记住域名，忽略剩余步骤，如果 ASDM 显示要使用的 DNS 服务器，请转至下一节。在指定远程服务器后需要输入相同的域名，同时配置端口转发列表中的条目。如果配置中没有 DNS 服务器，请继续执行剩余步骤。

步骤 4　点击 DNS 区域中的 **Manage**。

Configure DNS Server Groups 窗口将打开。

步骤 5　点击 **Configure Multiple DNS Server Groups**。

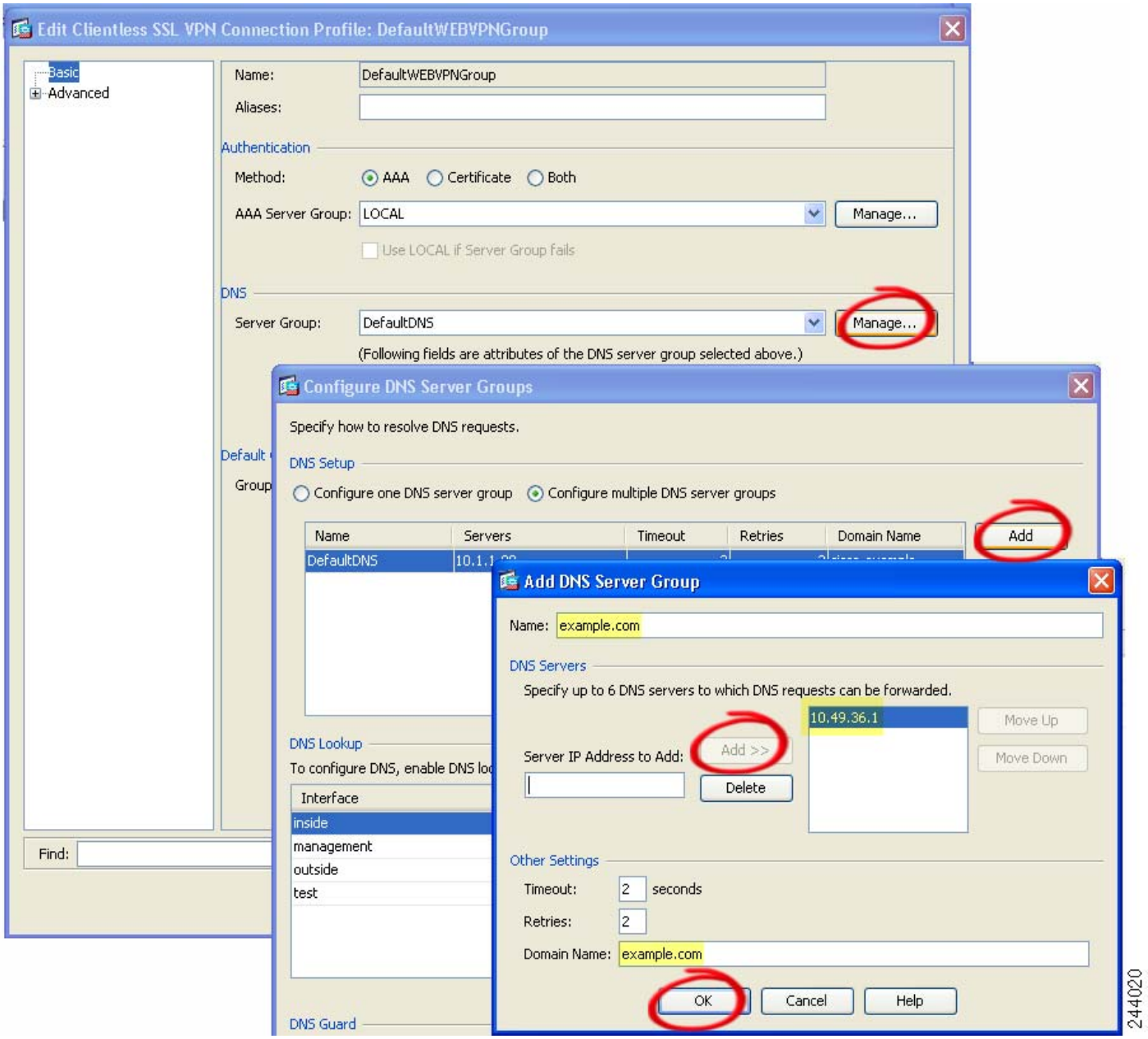
窗口显示 DNS 服务器条目表。

步骤 6　点击 **Add**。

Add DNS Server Group 窗口将打开。

步骤 7　在 Name 字段中输入新服务器组名称，然后输入 IP 地址和域名 （请参阅图 11-4）。

图 11-4　　用于端口转发的 DNS 服务器值的示例



请记住已输入的域名。稍后在配置端口转发条目的同时，指定远程服务器时需要此域名。

步骤 8　点击 **OK**，直至 Connection Profiles 窗口再次激活。

步骤 9　对于无客户端连接的配置中使用的每个剩余连接配置文件，请重复第 2 步至到第 8 步。

步骤 10　点击 **Apply**。

使应用符合端口转发条件

每个 ASA 的无客户端 SSL VPN 配置均支持*端口转发列表*，每一个列表均指定为其提供访问的应用所使用的本地和远程端口。由于每个组策略或用户名仅支持一个端口转发列表，因此，必须将每个受支持的 ca 集分组到列表中。要显示 ASA 配置中已存在的端口转发列表条目，输入以下命令：

如下一节中所述，遵循端口转发列表的配置，将列表分配给组策略或用户名。

添加/编辑端口转发条目

在 Add/Edit Port Forwarding Entry 对话框中，可指定与通过无客户端 SSL VPN 连接接入的用户或组策略关联的 TCP 应用。为这些窗口中的属性分配值，如下所示：

先决条件

根据第 11-15 页上的分配端口转发列表中的说明，分配给 Remote Server 参数的 DNS 名称必须与 Domain Name 和 Server Group 参数匹配，以建立隧道并解析为 IP 地址。 Domain 和 Server Group 参数的默认设置为 DefaultDNS。

详细步骤

步骤 1　点击 **Add**。

步骤 2　键入要使应用使用的 TCP 端口号。只能针对列表名称使用一次本地端口号。为了避免与本地 TCP 服务发生冲突，请使用介于 1024 与 65535 之间的端口号。

步骤 3　输入远程服务器的域名或 IP 地址。我们建议使用域名，这样就无需为特定 IP 地址配置客户端应用。

步骤 4　为应用键入已知端口号。

步骤 5　键入应用说明。说明不得超过 64 个字符。

步骤 6　（可选）突出显示端口转发列表，然后点击 **Assign**，以将所选列表分配给一个或多个组策略、动态访问策略或用户策略。

分配端口转发列表

可添加或编辑要与通过无客户端 SSL VPN 连接接入的用户或组策略关联的已命名 TCP 列表。对于每个组策略和用户名，可以配置无客户端 SSL VPN 执行以下任一操作：

- 在用户登录时自动启动端口转发访问。
- 用户登录时启用端口转发访问，但需要用户使用无客户端 SSL VPN 门户网站网页上的 **Application Access** > **Start Applications** 手动启动它。

注　对于每个组策略和用户名，这些选项相互排斥。只能使用一个。

详细步骤

在 Add or Edit Port Forwarding List 对话框中，可添加或编辑以下项：

步骤 1　为列表提供一个字母数字名称。说明不得超过 64 个字符。

步骤 2　输入侦听应用流量的本地端口。只能针对列表名称使用一次本地端口号。为了避免与本地 TCP 服务发生冲突，请使用介于 1024 与 65535 之间的端口号。

注　输入远程服务器的 IP 地址或 DNS 名称。我们建议使用域名，这样就无需为特定 IP 地址配置客户端应用。

步骤 3　输入侦听应用流量的远程端口。

步骤 4　说明 TCP 应用。说明不得超过 64 个字符。

启用和关闭端口转发

默认情况下，端口转发已关闭。

如果启用端口转发，用户必须使用无客户端 SSL VPN 门户网站网页上的 **Application Access** > **Start Applications** 手动启动它。

配置文件访问

无客户端 SSL VPN 为远程用户提供与 ASA 上运行的代理 CIFS 和/或 FTP 客户端连接的 HTTPS 门户网站网页。通过使用 CIFS 或 FTP，无客户端 SSL VPN 向用户提供网络文件的网络访问，在某种程度上，用户需满足身份验证需求并且文件属性不会限制访问。CIFS 和 FTP 客户端是透明的；无客户端 SSL VPN 所交付的门户网站网页提供直接访问文件系统的外观。

在用户请求文件列表时，无客户端 SSL VPN 将查询为包含列表的服务器 IP 地址指定为主浏览器的服务器。 ASA 获取列表并将其交付给门户网站网页的远程用户。

借助于无客户端 SSL VPN，用户可根据用户身份验证需求和文件属性调用以下 CIFS 和 FTP 功能。

- 导航并列出域和工作组、域或工作组中的服务器、服务器内的共享以及共享或目录内的文件。
- 创建目录。
- 下载、上传、重命名、移动和删除文件。

当远程用户点击门户网站网页的菜单中或在无客户端 SSL VPN 会话期间显示的工具栏上的 **Browse Networks** 时， ASA 使用通常与 ASA 处于同一网络或从该网络访问的主浏览器、 WINS 服务器或 DNS 服务器在该网络中查询服务器列表。

主浏览器或 DNS 服务器向 ASA 上的 CIFS/FTP 客户端提供网络资源的列表，无客户端 SSL VPN 向远程用户提供该列表。

注　在配置文件访问之前，必须在服务器上配置共享供用户访问。

CIFS 文件访问要求和限制

要访问*文件夹* `\\server\share\subfolder\personal`，用户必须具有所有父文件夹（包括共享本身）的最低读取权限。

使用 **Download** 或 **Upload**，在 CIFS 目录和本地桌面之间复制和粘贴文件。Copy and Paste 按钮仅适用于远程到远程操作，不适用于本地到远程或远程到本地操作。

CIFS 浏览服务器功能不支持双字节字符共享名称 （长度超过 13 个字符的共享名称）。这仅影响显示的文件夹的列表，不影响用户对文件夹的访问。作为解决方法，可为使用双字节共享名称的 CIFS 文件夹预配置书签，用户也可输入 URL 或用 cifs://server/<long-folder-name> 格式为文件夹添加书签。例如：

```
cifs://server/Do you remember?
cifs://server/Do%20you%20remember%3F
```

添加对文件访问的支持

按以下所示配置文件访问：

注　此操作步骤说明如何指定主浏览器和 WINS 服务器。或者，可使用 ASDM 配置 URL 列表和条目以提供文件共享访问。

在 ASDM 中添加共享不需要主浏览器或 WINS 服务器。但是，它不提供对浏览网络链接的支持。在输入 **nbns - server** 命令时，可使用主机名或 IP 地址指代 ServerA。如使用主机名，ASA 需要 DNS 服务器将其解析为 IP 地址。

有关这些命令的完整说明，请参阅命令参考。

确保 SharePoint 访问的时钟准确性

ASA 上的无客户端 SSL VPN 服务器使用 cookie 与应用 （如终端上的 Microsoft Word）交互。如果 ASA 上的时间不正确，在访问 SharePoint 服务器上的文档时， ASA 设置的 cookie 过期时间可导致 Word 出现故障。为防止此故障，请正确设置 ASA 时钟。我们建议将 ASA 配置为与 NTP 服务器动态同步时间。有关说明，请参阅常规操作配置指南中关于设置日期和时间的小节。

虚拟桌面基础设施 (VDI)

ASA 支持与 Citrix 和 VMWare VDI 服务器的连接。

- 对于 Citrix， ASA 允许通过无客户端门户网站访问用户运行的 Citrix Receiver。
- VMWare 已配置为 （智能隧道）应用。

与其他服务器应用一样，还可通过无客户端门户网站上的书签访问 VDI 服务器。

限制

- 由于这些形式的身份验证不允许中间的 ASA，因此，不支持在自动登录时使用证书或智能卡进行的身份验证。
- XML 服务必须在 XenApp 和 XenDesktop 服务器上安装和配置。
- 在使用独立移动客户端时，不支持客户端证书验证、双重身份验证、内部密码和　CSD （全部 CSD，不只是 Vault）。

Citrix 移动支持

运行 Citrix Receiver 的移动用户可按以下方式连接至 Citrix 服务器：

- 使用 AnyConnect 连接至 ASA，然后连接至 Citrix 服务器。
- 通过 ASA 连接至 Citrix 服务器，无需使用 AnyConnect 客户端。登录凭据可能包括：
  - Citrix 登录屏幕中的连接配置文件别名（也称为隧道组别名）。VDI 服务器可能有多个组策略，每个都具有不同的授权和连接设置。
  - 配置 RSA 服务器时的 RSA SecureID 令牌值。 RSA 支持包括无效条目的下一个令牌，还包括用于为初始或过期 PIN 输入新 PIN 的下一个令牌。

受支持的移动设备

- iPad—Citrix Receiver 版本 4.x 或更高版本
- iPhone/iTouch—Citrix Receiver 版本 4.x 或更高版本
- Android 2.x/3.x/4.0/4.1 phone—Citrix Receiver 版本 2.x 或更高版本
- Android 4.0 phone—Citrix Receiver 版本 2.x 或更高版本

限制

证书限制

- 不支持将证书/智能卡身份验证作为自动登录方式。
- 客户端证书验证和 CSD 不受支持
- 由于安全问题，证书中的 Md5 签名无效，此问题为 iOS 中的已知问题，网址为 http://support.citrix.com/article/CTX132798
- 只有 Windows 支持 SHA2 签名，如 Citrix 网站上所述，网址为 http://www.citrix.com/
- 超过 1024 的密钥大小不受支持

其他限制

- 不支持 HTTP 重定向；Citrix Receiver 应用不适用于重定向。
- XML 服务必须在 XenApp 和 XenDesktop 服务器上安装和配置。

关于 Citrix Mobile Receiver 用户登录

连接 Citrix 服务器的移动用户登录取决于 ASA 是将 Citrix 服务器配置为 VDI 服务器，还是配置为 VDI 代理服务器。

当 Citrix 服务器配置为 VDI 服务器时：

1. 通过使用 AnyConnect 安全移动客户端，连接至具有 VPN 凭证的 ASA。
2. 通过使用 Citrix Mobile Receiver，连接至具有 Citrix 服务器凭据的 Citrix 服务器 （如已配置单点登录，则不需要 Citrix 凭据）。

当 ASA 配置为 VDI 代理服务器时：

1. 通过使用 Citrix Mobile Receiver 并输入 VPN 和 Citrix 服务器的凭据，连接至 ASA。在第一次连接后，如果配置正确，后续连接只需要 VPN 凭据。

已将 ASA 配置为代理 Citrix 服务器

可将 ASA 配置为充当 Citrix 服务器的代理，因此，对于用户而言，ASA 的连接看起来与 Citrix 服务器的连接相似。在 ASDM 中启用 VDI 代理时，不需要 AnyConnect 客户端。以下高级别步骤显示最终用户如何连接至 Citrix。

1. 移动用户打开 Citrix Receiver 并连接至 ASA 的 URL。
2. 用户为 XenApp 服务器提供凭据和 Citrix 登录屏幕上的 VPN 凭据。
3. 对于 Citrix 服务器的每个后续连接，用户只需输入 VPN 凭据。

如将 ASA 用作 XenApp 和 XenDesktop 的代理，则会移除 Citrix 访问网关的要求。XenApp 服务器信息记录在 ASA 上并显示在 ASDM 中。

配置 Citrix 服务器的地址和登录凭据，并将该 VDI 服务器分配给组策略或用户名。如已配置用户名和组策略，则用户名设置将覆盖组策略设置。

其他信息

http://www.youtube.com/watch?v=JMM2RzppaG8 — 此视频介绍将 ASA 用作 Citrix 代理的优势。

配置 VDI 服务器

对于一台服务器：

1. 选择 Configuration > Remote Access VPN > Clientless SSL VPN Access > VDI Access
2. 选中 Enable VDI Server Proxy，然后配置 VDI 服务器。

要将多个组策略分配给 VDI 服务器，请执行以下操作：

1. 选择 Configuration > Remote Access VPN > Clientless SSL VPN Access > VDI Access
2. 选中 Configure All VDI Servers。
3. 添加 VDI 服务器，并分配一个或多个组策略。

配置 VDI 代理服务器

对于分配给一个组策略的一台 VDI 服务器：

1. 选择 Configuration > Remote Access VPN > Clientless SSL VPN Access > VDI Access
2. 选中 Enable VDI Server Proxy，然后配置 VDI 服务器。

要将多个组策略分配给 VDI 服务器，请执行以下操作：

1. 导航至 Configuration > Remote Access VPN > Clientless SSL VPN Access > VDI Access
2. 选中 Configure All VDI Servers。
3. 添加 VDI 服务器，并分配一个或多个组策略。

将 VDI 服务器分配给组策略

已按以下方式配置 VDI 服务器并将其分配给组策略：

- 在 VDI Access 窗格上添加 VDI 服务器，并将组策略分配给该服务器。
- 将 VDI 服务器添加至组策略。

步骤 1　浏览至 Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies。

步骤 2　编辑 DfltGrpPolicy，并从左侧菜单展开 More Options 菜单。

步骤 3　选择 **VDI Access**。点击 **Add** 或 **Edit**，以提供 VDI 服务器详细信息。

- Server (Host Name or IP Address) - XenApp 或 XenDesktop 服务器的地址。该值可能是无客户端宏。
- Port Number (Optional) - 连接至 Citrix 服务器的端口号。该值可能是无客户端宏。
- Active Directory Domain Name - 用于登录虚拟化基础设施服务器的域。该值可能是无客户端宏。
- Use SSL Connection - 如果想要服务器使用 SSL 进行连接，请选中该复选框。
- Username - 用于登录虚拟化基础设施服务器的用户名。该值可能是无客户端宏。
- Password - 用于登录虚拟化基础设施服务器的密码。该值可能是无客户端宏。

	命令	用途
步骤 1	`webvpn`	切换至组策略无客户端 SSL VPN 配置模式。
步骤 2	`url-entry disable`	关闭 URL Entry。

配置客户端服务器插件的浏览器访问

客户端服务器插件表显示 ASA 向无客户端 SSL VPN 会话中浏览器提供的插件。

要添加、更改或移除插件，请执行以下操作之一：

- 要添加插件，点击 **Import**。 Import Plug-ins 对话框将打开。

要移除插件，选定它并点击 **Delete**。以下各节介绍如何为无客户端 SSL VPN 浏览器访问集成浏览器插件：

- 关于安装浏览器插件
- 为安装插件准备安全设备
- 安装思科重新分发的插件

关于安装浏览器插件

浏览器插件是网络浏览器在执行专用功能时 （例如，将客户端连接至浏览器窗口中的服务器）调用的一个单独程序。借助于 ASA，可在无客户端 SSL VPN 会话中导入要下载至远程浏览器的插件。当然，思科将测试其重新分发的插件，在某些情况下，将测试其无法重新分发的插件的连接性。但是，我们建议不要导入目前支持流媒体的插件。

在闪存设备上安装插件时， ASA 将执行以下操作：

- （仅限思科分发的插件）解压缩 *URL* 中指定的 jar 文件。
- 将文件写入 ASA 文件系统上的 csco-config/97/plugin 目录。
- 填充 ASDM 中 URL 属性旁边的下拉列表。
- 为所有未来无客户端 SSL VPN 会话启用插件，然后将主菜单选项和选项添加至门户网站网页 Address 字段旁边的下拉列表。

  表 11-3 显示在添加以下各节中描述的插件时对门户网站网页的主菜单和 Address 字段做出的更改。

表 11-3　　无客户端 SSL VPN 门户网站网页上插件的效果

插件	已添加至门户网站网页的主菜单选项	已添加至门户网站网页的 Address 字段选项
ica	Citrix Client	citrix://
rdp	Terminal Servers	rdp://
rdp2	Terminal Servers Vista	rdp2://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

注　辅助 ASA 从主 ASA 获取插件。

当用户在无客户端 SSL VPN 会话中点击门户网站网页上的关联菜单选项时，门户网站网页显示界面窗口和帮助窗格。用户可选择下拉列表中显示的协议，并在 Address 字段中输入 URL，以建立连接。

注　即使目标服务的会话未建立，某些 Java 插件也可能报告已连接或联机状态。开源插件报告状态，而不是 ASA。

在安装第一个插件之前，必须遵循下一节中的说明。

先决条件

- 如果安全设备配置要使用代理服务器的无客户端会话，则插件不起作用。

注　远程桌面协议插件不支持用会话代理程序进行负载平衡。由于协议处理源自会话代理程序的重定向的方法不当，连接失败。如未使用会话代理程序，插件将发挥正常作用。

- 插件支持单点登录 (SSO)。它们使用所输入的*相同凭据*打开无客户端 SSL VPN 会话。因为插件不支持宏替换，所以，您无法选择对不同的字段（如内部域密码）或 RADIUS 或 LDAP 服务器上的属性执行 SSO。
- 要为插件配置 SSO 支持，需安装插件，添加书签条目以显示服务器链接，并在添加书签时指定 SSO 支持。
- 远程使用所需的最低访问权限属于宾客特权模式。

要求

- 根据 GNU 通用公共许可证 (GPL)，思科重新分发插件，但未对其做出任何更改。根据 GPL，思科无法直接增强这些插件的功能。
- 无客户端 SSL VPN 只有在 ASA 上启用才能提供对插件的远程访问。
- 有状态故障转移不保留使用插件建立的会话。出现故障转移后，用户必须重新连接。
- 插件要求在浏览器上启用 ActiveX 或 Oracle Java Runtime Environment (JRE) 1.4.2（或更高版本）。对于 64 位浏览器， RDP 插件没有 ActiveX 版本。

RDP 插件 ActiveX 调试快速参考

要设置和使用 RDP 插件，必须添加新的环境变量。

步骤 1　右键单击 **My Computer** 以访问 System Properties，并选择 **Advanced** 选项卡。

步骤 2　在 Advanced 选项卡上，选择环境变量按钮。

步骤 3　在 New User Variable 对话框中，输入变量 RF_DEBUG。

步骤 4　验证用户变量部分中的新环境变量。

步骤 5　如将客户端计算机与低于版本 8.3 版本的无客户端 SSL VPN 使用，则必须移除旧版 Cisco Portforwarder Control。转至目录 C:/WINDOWS/Downloaded Program Files，右键单击 portforwarder 控件，然后选择 **Remove**。

步骤 6　清除 Internet Explorer 浏览器的所有缓存。

步骤 7　启动无客户端 SSL VPN 会话并用 RDP ActiveX 插件建立 RDP 会话。

现可查看 Windows 应用事件查看器中的事件。

为安装插件准备安全设备

步骤 1　确保在 ASA 界面上已启用无客户端 SSL VPN。

步骤 2　在远程用户使用完全限定域名 (FQDN) 连接到的 ASA 界面上安装 SSL 证书。

注　请勿将 IP 地址指定为 SSL 证书的通用名称 (CN)。远程用户尝试使用 FQDN 与 ASA 进行通信。远程 PC 必须能够使用 DNS 或 System32\drivers\etc\hosts 文件中的条目解析 FQDN。

第 12 章

高级无客户端 SSL VPN 配置

Microsoft Kerberos 约束委派解决方案

很多组织都想要对其无客户端 VPN 用户进行身份验证并使用超出现在 ASA 可以提供的身份验证方法将身份验证凭据无缝扩展至基于网络的资源。随着对使用智能卡和一次性密码 (OTP) 的远程访问用户进行身份验证的需求日益增长， SSO 功能无法满足这种需求，因为当需要进行身份验证时，它只是向基于网络的无客户端资源转发静态用户名和密码等传统用户凭据。

例如，证书和基于 OTP 的身份验证方法都不包含 ASA 对基于网络的资源无缝地进行 SSO 访问所需的传统用户名和密码。利用证书进行身份验证时， ASA 不需要用户名和密码即可扩展至基于网络的资源，使其成为 SSO 不支持的一种身份验证方法。另一方面，虽然 OTP 确实包括静态用户名，但密码是动态的，并且随后在整个 VPN 会话期间也会发生改变。一般来说，基于网络的资源都配置为接受静态用户名和密码，因此也使 OTP 成为 SSO 不支持的一种身份验证方法。

Microsoft 的 Kerberos 约束委派 (KCD) 是 ASA 的 8.4 版本软件中引入的一个新功能，可提供对专用网络中受 Kerberos 保护的网络应用的访问。利用此优势，您可以无缝地将基于证书和 OTP 的身份验证方法扩展至网络应用。因此，通过同时但独立地使用 SSO 和 KCD，现在很多组织都可以对无客户端 VPN 用户进行身份验证，并将他们的身份验证凭据无缝扩展至使用 ASA 支持的所有身份验证方法的网络应用。

要求

为了让 **kcd-server** 命令正常运行， ASA 必须在*源*域（即 ASA 所在的域）和*目标*或*资源*域（即网络服务所在的域）之间建立信任关系。ASA 使用其独特的格式，跨越从源到目标域的证书路径并代表远程访问用户获取访问服务所需的票证。

这种跨越证书路径的操作叫做跨域身份验证。在跨域身份验证的每个阶段，ASA 依赖于特定域上的凭据和与后续域的信任关系。

KCD 运行机制

Kerberos 依赖受信任的第三方来验证网络中实体的数字身份。这些实体 （例如用户、主机和主机上运行的服务）称为主体，并且必须位于同一个域内。 Kerberos 使用票证，而不是使用密钥，来验证访问服务器的客户端。票证源于密钥，由客户端的身份、加密的会话密钥和标志组成。每个票证由密钥发行中心发行并具有设定的生命期。

Kerberos 安全系统是一种身份验证协议，用于验证实体 （用户、计算机或应用）并通过打乱数据从而使只有指定接收该信息的设备可以解密这些数据保护网络传输。您可以配置 KCD，向无客户端 SSL VPN 用户提供对任何受 Kerberos 保护的网络服务的 SSO 访问。这类网络服务或应用示例包括 Outlook Web Access (OWA)、 Sharepoint 和互联网信息服务器 (IIS)。

Kerberos 协议实施了两项扩展：*协议转换*和*约束委派*。这两项扩展允许无客户端 SSL VPN 远程访问用户访问专用网络中通过 Kerberos 身份验证的应用。

*协议转换*在用户身份验证层面支持不同的身份验证机制，而且会在随后的应用层中切换至 Kerberos 协议以获得更多安全功能 （例如相互身份验证和约束委派），从而为您提供了更高的灵活性和安全性。*约束委派*为域管理员提供了一种通过限制应用服务可以代表用户的情况指定并执行应用信任边界的方法。这种灵活性减少了受不信任服务危害的几率，改善了应用安全设计。

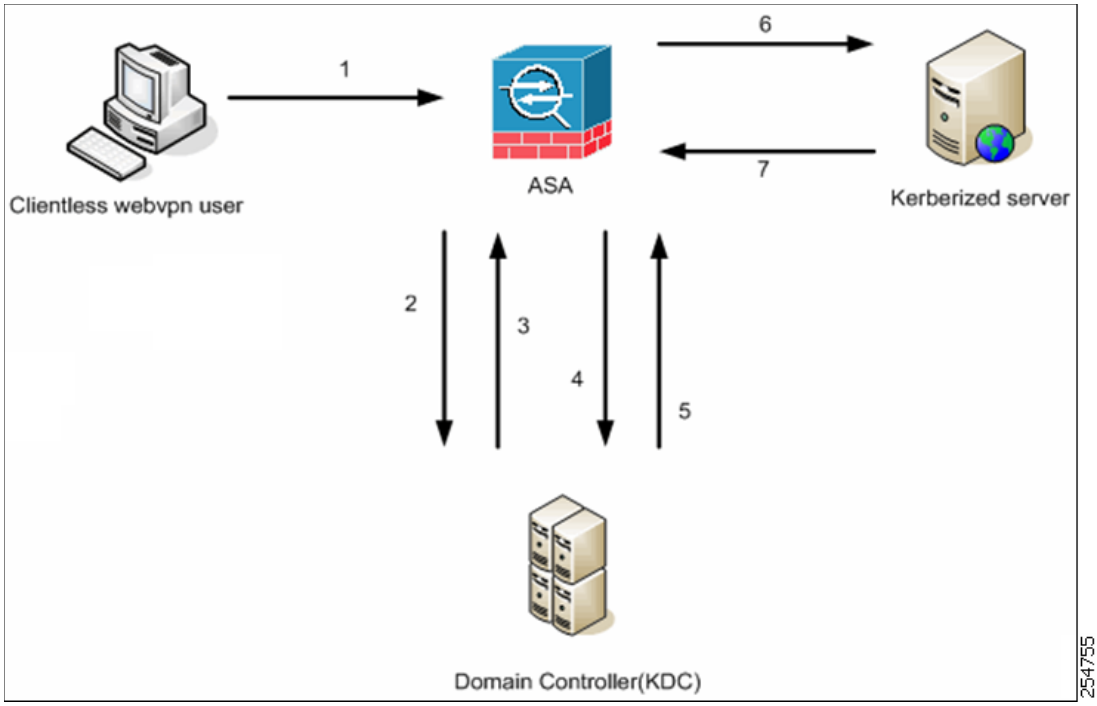
有关约束委派的详细信息，请通过 IETF 网站参阅 RFC 1510 (http://www.ietf.org)。

使用 KCD 的身份验证流程

图 12-1 描述了用户通过无客户端门户访问被信任进行委派的资源时直接和间接体验的数据包和流程。此流程假设已完成以下任务：

- 已在 ASA 上配置 KCD
- 已加入 Windows Active Directory，并已确保服务被信任进行委派
- 已委派 ASA 作为 Windows Active Directory 域的成员

图 12-1　　KCD 流程



注　无客户端用户会话由 ASA 使用为用户配置的身份验证机制进行身份验证。（在使用智能卡凭据的情况下，ASA 使用数字证书的 userPrincipalName 对 Windows Active Directory 执行 LDAP 授权）。

1. 身份验证成功后，用户登录进入 ASA 无客户端门户页面。用户可以通过在门户页面中输入 URL 或点击书签访问网络服务。如果网络服务要求进行身份验证，服务器将请求 ASA 提供凭据并发送一份受服务器支持的身份验证方法列表。

   注　适用于无客户端 SSL VPN 的 KCD 支持所有身份验证方法 （RADIUS、 RSA/SDI、LDAP、数字证书等等）。请参阅 AAA 支持表格，网址为 http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_aaa.html#wp1069492。

2. 根据请求中的 HTTP 报头， ASA 确定服务器是否要求进行 Kerberos 身份验证。（这是 SPNEGO 机制的一部分。）如果连接到后端服务器要求进行 Kerberos 身份验证， ASA 将代表密钥发行中心为自身请求获取服务票证。
3. 密钥发行中心将向 ASA 返回所请求的票证。即使这些票证传递到 ASA，它们仍包含用户的授权数据。 ASA 就用户想要访问的特定服务向 KDC 请求获取服务票证。

   注　第 1 步至第 3 步包含协议转换。完成这些步骤后，任何使用非 Kerberos 身份验证协议进行身份验证访问 ASA 的用户都显然已使用 Kerberos 向密钥发行中心完成身份验证。

4. ASA 为用户想要访问的特定服务向密钥发行中心请求获取服务票证。

5. 密钥发行中心将特定服务的服务票证返回至 ASA。
6. ASA 使用此服务票证请求访问网络服务。
7. 网络服务器对 Kerberos 服务票证进行身份验证并授权访问此服务。如果身份验证失败，系统将显示相应的错误消息并要求确认。如果 Kerberos 身份验证失败，预期行为是退回到基本身份验证。

在 Active Directory 中添加 Windows 服务帐户

ASA 上的 KCD 实施要求使用服务帐户，也就是具备添加计算机所需的权限的 Active Directory 用户帐户，例如将 ASA 添加到域中。在我们的示例中，Active Directory 用户名 JohnDoe 即具备所需权限的服务帐户。有关如何在 Active Directory 中实施用户权限的详细信息，请与 Microsoft 支持部门联系或访问 http://microsoft.com。

为 KCD 配置 DNS

本节将描述在 ASA 上配置 DNS 所需执行的配置步骤。当将 KCD 用做 ASA 上的身份验证委派方法时，需要 DNS 才能启用主机名解析以及ASA、域控制器 (DC) 和受信任进行委派的服务之间的通信。

步骤 1　从 ASDM 导航至 **Configuration > Remote Access VPN > DNS** 并配置 DNS 设置：

- DNS Server Group - 输入 DNS 服务器 IP 地址，例如 192.168.0.3。
- Domain Name - 输入域控制器所属的域名。

步骤 2　在恰当的接口上启用 DNS 查找。无客户端 VPN 部署要求通过内部公司网络进行 DNS 查找，通常是通过*内部*接口查找。

配置 ASA 加入 Active Directory 域

本节概述启用 ASA 以用作 Active Directory 域的一部分所需执行的配置步骤。 KCD 要求 ASA 是 Active Directory 域的成员。此配置将为 ASA 和 KCD 服务器之间的约束委派事务启用所需的功能。

步骤 1　从 ASDM 导航至 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Microsoft KCD Server**。

步骤 2　点击 **New** 为约束委派添加 Kerberos 服务器组并执行以下配置：

- 服务器组配置
  - Server Group Name - 定义 ASA 上约束委派配置的名称，例如默认值 MSKCD。您可以配置冗余的多个服务器组；但是，只能将一个服务器组分配给 KCD 服务器配置，用于代表 VPN 用户请求获取服务票证。
  - Reactivation Mode - 点击所需模式的单选按钮（**Depletion** 或 **Timed**）。在 Depletion 模式下，只有在组中所有服务器都处于非活动状态后，故障服务器才重新激活。在 Timed 模式下，故障服务器在 30 秒停机时间后重新激活。 Depletion 是默认配置。
  - Dead Time - 如果选择 Depletion 重新激活模式，您必须添加失效时间间隔。十分钟是默认配置。间隔代表组中上一个服务器停用到随后所有服务器重新启用之间经过的时间，以分钟为单位。
  - Max Failed Attempts - 设置宣布无响应的服务器处于非活动状态之前允许的失败连接尝试次数。三次是默认值。

- 服务器配置
  - Interface Name - 选择服务器所在的接口。一般来说，身份验证服务器部署在公司内部网络上，通常通过*内部*接口部署。
  - Server Name - 定义域控制器的主机名，例如 ServerHostName。
  - Timeout - 以秒为单位指定获得服务器响应之前最长的等待时间。十秒是默认值。
- Kerberos 参数
  - Server Port - 88 是用于 KCD 的默认值和标准端口。
  - Retry Interval - 选择所需的重试间隔。十秒是默认配置。
  - Realm - 以全部大写的格式输入域控制器的域名。在 ASA 上的 KCD 配置要求领域值为大写。领域是一个身份验证域。服务只能接受同一领域的实体提供的身份验证凭证。领域必须与 ASA 所加入的域名匹配。

步骤 3　点击 **OK** 应用您的配置，然后配置 Microsoft KCD服务器代表远程访问用户请求获取服务票证。

配置使用外部代理服务器

使用 Proxies 窗格配置 ASA 使用外部代理服务器来处理 HTTP 请求和 HTTPS 请求。这些服务器担任用户和互联网之间的中介。要求所有互联网访问都通过您控制的服务器提供了另一个过滤机会，确保安全的互联网访问和管理控制台。

限制

HTTP 和 HTTPS 代理服务不支持与个人数字助理的连接。

步骤 1　点击 **Use an HTTP Proxy Server**。

步骤 2　按照 IP 地址或主机名标识 HTTP 代理服务器。

步骤 3　输入外部 HTTP 代理服务器的主机名或 IP 地址。

步骤 4　输入侦听 HTTP 请求的端口。默认端口为 80。

步骤 5　（可选）输入 URL 或逗号分隔的多个 URL 的列表，将其从可以发送到 HTTP 代理服务器的 URL 中排除。字符串没有字符限制，但是整个命令不能超过 512 个字符。您可以指定文本 URL 或使用以下通配符：

- ***** 匹配任意字符串，包括斜线 (/) 和句点 (.)。必须将此通配符与字母数字字符串结合使用。
- **?**匹配任意单个字符，包括斜线和句点。
- [*x*-*y*] 匹配 *x* 至 *y* 的范围内的任意单个字符，其中 *x* 代表一个字符，*y* 代表 ANSI 字符集中的另一个字符。
- [**!***x*-*y*] 匹配不属于该范围的任意单个字符。

步骤 6　（可选）输入此关键字，为每个 HTTP 代理请求加上提供基本代理身份验证的用户名。

步骤 7　输入要随每个 HTTP 请求一起发送至代理服务器的密码。

步骤 8　除了指定 HTTP 代理服务器的 IP 地址，您也可以选择 Specify PAC File URL 以指定下载到浏览器的代理自动配置文件。下载后，该 PAC 文件将使用 JavaScript 功能标识每个 URL 的代理。输入 **http://** 并将代理自动配置文件的 URL 键入到相邻字段。如果您省略 **http://** 部分， ASA 会忽略它。

步骤 9　选择是否使用 HTTPS 代理服务器。

步骤 10　点击以按照 IP 地址或主机名标识 HTTPS 代理服务器。

步骤 11　输入外部 HTTPS 代理服务器的主机名或 IP 地址。

步骤 12　输入侦听 HTTPS 请求的端口。默认端口为 443。

步骤 13　（可选）输入 URL 或逗号分隔的多个 URL 的列表，将其从可以发送到 HTTPS 代理服务器的那些 URL 中排除。字符串没有字符限制，但是整个命令不能超过 512 个字符。您可以指定文本 URL 或使用以下通配符：

- * 匹配任意字符串，包括斜线 (/) 和句点 (.)。必须将此通配符与字母数字字符串结合使用。
- **?**匹配任意单个字符，包括斜线和句点。
- [*x*-*y*] 匹配 *x* 至 *y* 的范围内的任意单个字符，其中 *x* 代表一个字符，*y* 代表 ANSI 字符集中的另一个字符。
- [**!***x*-*y*] 匹配不属于该范围的任意单个字符。

步骤 14　（可选）输入关键字，为个每 HTTPS 代理请求加上要提供基本代理身份验证的用户名。

步骤 15　输入要随每个 HTTPS 请求一起发送至代理服务器的密码。

SSO 服务器

SSO Server 窗格允许为连接至 Computer Associates SiteMinder SSO 服务器或 Security Assertion Markup Language (SAML) 1.1 版本、 Browser Post Profile SSO 服务器的无客户端 SSL VPN 的用户配置或删除单一登录 (SSO)。 SSO 支持只适用于无客户端 SSL VPN，让用户可以跨越不同服务器上的不同安全服务，而不需要不止一次地输入用户名和密码。

配置 SSO 时您可以选择以下方法：

- 使用基本 HTTP 和/或 NTLMv1 身份验证的自动登录。
- HTTP Form 协议或者 Computer Associates eTrust SiteMinder （前称为 Netegrity SiteMinder）。
- SAML、 1.1 版本 Browser Post Profile。

限制

不支持交换断言的 SAML Browser Artifact 配置文件方法。

以下节将介绍使用 SiteMinder 和 SAML Browser Post Profile 设置 SSO 的步骤。

- 第 12-7 页上的配置 SiteMinder 和 SAML Browser Post Profile - 用基本 HTTP 或 NTLM 身份验证配置 SSO。
- 配置会话设置 - 用 HTTP Form 协议配置 SSO。

SSO 机制要做作为 AAA 进程的一部分开始 (HTTP Form)，要么在刚刚对 AAA服务器 (SiteMinder) 或 SAML Browser Post Profile 服务器成功完成用户身份验证之后开始。在这些情况下，在 ASA 上运行的无客户端 SSL VPN 服务器用作用户对进行身份验证服务器的代理。当用户登录时，无客户端 SSL VPN 服务器将向使用 HTTPS 的身份验证服务器发送 SSO 身份验证请求。

如果身份验证服务器批准身份验证请求，则会向无客户端 SSL VPN 服务器返回 SSO 身份验证 cookie。此 cookie 保存在代表用户的 ASA 上并用于对用户进行身份验证，保障受 SSO 服务器保护的域内的网站安全。

配置 SiteMinder 和 SAML Browser Post Profile

使用 SiteMinder 或使用 SAML Browser Post Profile 的 SSO 身份验证与 AAA 是分开的并且发生于 AAA 进程完成之后。要为用户或组设置 SiteMinder SSO，必须先配置 AAA 服务器（例如 RADIUS、LDAP）。在 AAA 服务器对用户进行身份验证后，无客户端 SSL VPN 服务器将使用 HTTPS 向 SiteMinder SSO 服务器发送身份验证请求。

除配置 ASA 以外，对于 SiteMinder SSO，您还必须使用思科身份验证方案配置您的 CA SiteMinder 策略服务器。对于 SAML Browser Post Profile，您必须配置身份验证网络代理（受保护的资源 URL）。

使用服务器软件供应商提供的 SAML 服务器文档在信赖方模式下配置 SAML 服务器。系统将显示以下字段：

- Server Name - *只显示*。显示已配置的 SSO 服务器的名称。最少 4 个字符，最多 31 个字符。
- Authentication Type - *只显示*。显示 SSO 服务器的类型。ASA 当前支持 SiteMinder 类型和 SAML Browser Post Profile 类型。
- URL - *只显示*。显示 ASA 向其发出 SSO 身份验证请求的 SSO 服务器 URL。
- Secret Key - *只显示*。显示用于加密与 SSO 服务器的身份验证通信的密钥。此密钥可包含任何常规或移位的字母数字字符。无字符最小或最大数量限制。
- Maximum Retries - *只显示*。显示 ASA 失败的 SSO 身份验证尝试次数。范围是 1 至 5 次重试，重试默认次数为 3 次。
- Request Timeout（秒）- *只显示*。显示在失败的 SSO 身份验证尝试超时之前持续的秒数。范围是 1 至 30 秒，默认为 5 秒。
- Add/Edit - 打开 Add/Edit SSO Server 对话框。
- Delete - 删除选择的 SSO 服务器。
- Assign - 突出显示 SSO 服务器，点击此按钮可将选择的服务器分配给一个或多个 VPN 组策略或用户策略。

步骤 1　配置 SAML 服务器参数来代表断言方 (ASA)：

- 接收方使用者（网络代理）URL（与 ASA 上配置的断言使用者 URL 相同）
- 发行者 ID，一个字符串，通常是设备的主机名
- 配置文件类型 - Browser Post Profile

步骤 2　配置证书。

步骤 3　指明必须对断言方的断言进行签名。

步骤 4　选择 SAML 服务器如何标识用户：

- 使用者名称类型为 DN
- 使用者名称格式为 uid=<user>

后续操作

请参阅向 SiteMinder 添加思科身份验证方案。

向 SiteMinder 添加思科身份验证方案

除了使用 SiteMinder 为 SSO 配置 ASA 之外，您还必须使用作为 Java 插件提供的思科身份验证方案配置您的 CA SiteMinder 策略服务器。本节描述的是一般步骤，并非完整的步骤。有关添加自定义身份验证方案的完整步骤，请参阅 CA SiteMinder 文档。要在您的 SiteMinder 策略服务器上配置思科身份验证方案，请执行以下步骤。

先决条件

配置 SiteMinder 策略服务器要求具备使用 SiteMinder 的经验。

步骤 1　使用 SiteMinder Administration 实用程序，创建一个自定义身份验证方案，确保使用以下特定值：

- 在 Library 字段中，输入 **smjavaapi**。
- 在 Secret 字段中，输入在后面的 Add SSO Server 对话框的 Secret Key 字段中配置的相同密钥。
- 在 Parameter 字段中，输入 **CiscoAuthApi**。

步骤 2　使用 Cisco.com 登录名，从 http://www.cisco.com/cisco/software/navigator.html 下载文件 **cisco_vpn_auth.jar**，并将其复制到 SiteMinder 服务器的默认库目录。思科 ASA CD 中也提供了此 .jar 文件。

添加或编辑 SSO 服务器

此 SSO 方法使用 CA SiteMinder 和 SAML Browser Post Profile。还可以使用 HTTP Form 协议或基本 HTML 和 NTLM 身份验证设置 SSO。要设置使用基本 HTML 或 NTLM 身份验证，请在命令行界面上使用 **auto sign-on** 命令。

步骤 1　如果添加服务器，请输入新的 SSO 服务器的名称。如果编辑服务器，此字段只显示；它显示选择的 SSO 服务器的名称。

步骤 2　输入用于加密向 SSO 服务器发送的身份验证请求的密钥。密钥字符可以是任何常规或移位的字母数字字符。无字符最小或最大数量限制。密钥类似于密码：您可以创建、保存和配置密钥。使用思科 Java 插件身份验证方案，在ASA、 SSO 服务器和 SiteMinder 策略服务器中进行配置。

步骤 3　输入身份验证超时之前 ASA 重试失败的 SSO 身份验证尝试的次数。重试次数范围为 1 - 5 次（包括端值），默认为 3 次。

步骤 4　输入在失败的 SSO 身份验证尝试超时之前持续的秒数。范围是 1 - 30 秒（包括端值），默认为 5 秒。

步骤 5　点击 **OK** 应用您的配置，然后配置 Microsoft KCD服务器代表远程访问用户请求获取服务票证 （请参阅图 12-1）。点击 **OK** 时系统将显示 Microsoft KCD 服务器配置窗口。

后续操作

要使用 HTTP Form 协议，请参阅第 12-15 页上的配置会话设置。

配置 Kerberos 服务器组

约束委派的 Kerberos 服务器组 MSKCD 自动应用于 KCD 服务器配置。您还可以在 **Configuration > Remote Access VPN > AAA/Local User > AAA Server Groups** 下配置和管理 Kerberos 服务器组。

步骤 1　在 Server Access Credential 部分，进行以下配置：

- Username - 定义一个被授予向 Active Directory 域添加计算机帐户所需权限的服务帐户 （Active Directory 用户名），例如 JohnDoe。该用户名不对应特定管理用户，只是对应具有服务级别权限的某个用户。此服务帐户由 ASA 用于在每次重新启动时向 Active Directory 域添加计算机帐户。您必须单独配置计算机帐户，以代表远程用户请求获取 Kerberos 票证。

注　首次加入需要具备管理权限。域控制器上具有服务级别权限的用户不会获得访问权限。

- Password - 定义与用户名关联的密码 （例如 cisco123）。该密码不对应特定密码，而只是对应在 Window 域控制器上添加设备的服务级别密码权限。

步骤 2　在 Server Group Configuration 部分，进行以下配置：

- Reactivation Mode - 点击要使用的模式 （**Depletion** 或 **Timed**）。在 Depletion 模式下，只有在组中所有服务器都处于非活动状态后，故障服务器才重新激活。在 Timed 模式下，故障服务器在 30 秒停机时间后重新激活。 Depletion 是默认配置。
- Dead Time - 如果选择 Depletion 重新激活模式，您必须添加失效时间间隔。间隔代表组中上一个服务器停用到随后所有服务器重新启用之间经过的时间，以分钟为单位。十分钟是默认值。
- Max Failed Attempts - 设置宣布无响应的服务器处于非活动状态之前允许的失败连接尝试次数。三次是默认值。

注　在 Server Table 部分下，以前配置的 DC 主机名 ServerHostName 自动应用于 KCD 服务器配置（请参阅图 12-1）。

步骤 3　点击 **Apply**。

注　在应用您的配置后， ASA 自动启动加入 Active Directory 域的进程。 ASA 的主机名显示在 Active Directory Users and Computers 中 Computers 目录下。

要确认 ASA 是否已成功加入域，请从 ASA 提示符执行以下命令：

```
host# show webvpn kcd
Kerberos Realm: WEST.LOCAL
Domain Join: Complete
```

配置书签访问通过 Kerberos 身份验证的服务

要使用 ASA 无客户端门户访问 Outlook Web Access 等通过 Kerberos 身份验证的服务，您必须配置书签列表。书签列表会分配和显示根据远程访问用户关联的 VPN 安全策略向远程访问用户分配和显示书签列表。

限制

为使用 Kerberos 约束委派 (KCD) 的应用创建书签时，请勿选中 Enable Smart Tunnel。

步骤 1　在 ASDM GUI 中导航至 **Configuration > Remote Access VPN > Clientless VPN Access > Portal > Bookmarks**。

步骤 2　在书签列表中，请输入指向服务位置的 URL。

配置应用程序配置文件自定义框架

无客户端 SSL VPN 包含一个 Application Profile Customization Framework (APCF) 选项，其允许 ASA 处理非标准应用和网络资源，以便通过 SSL VPN 连接正确显示它们。APCF 配置文件包含为特定应用指定何时 （之前、之后）、在何处 （报头、正文、请求、响应）转换什么内容 （数据）的脚本。脚本在 XML 中并使用 sed （数据流编辑器）语法转换字符串/文本。

您可以同时在 ASA 上配置和运行多个 APCF 配置文件。在 APCF 配置文件脚本中，可应用多个 APCF 规则。 ASA 根据配置历史记录首先处理最早的规则，接下来处理下一个最早的规则。

您可以将 APCF 配置文件存储在 ASA 闪存上，或者存储在 HTTP、 HTTPS 或 TFTP 服务器上。

限制

我们建议您只有在思科人员的帮助下方可配置 APCF 配置文件。

管理 APCF 配置文件

您可以将 APCF 配置文件存储在 ASA 闪存上，或者存储在 HTTP、HTTPS、FTP 或 TFTP 服务器上。使用该窗格添加、编辑和删除 APCF 数据包以及按优先顺序进行排列。

步骤 1　导航到 Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Application Helper，在此您可以执行以下功能。

- 点击 **Add/Edit**，创建新的 APCF 配置文件或更改现有的 APCF 配置文件。
  - 选择 **Flash file**，在 ASA 闪存上查找 APCF 文件。

    然后点击 **Upload** 将 APCF 文件从本地计算机传送至 ASA 闪存文件系统，也可以点击 Browse to upload 从闪存中选择已有的 APCF 文件。
  - 选择 URL，从 HTTP、 HTTPS、 FTP 或 TFTP 服务器检索 APCF 文件。
- 点击 **Delete**，删除现有 APCF 配置文件。没有确认或取消选项。
- 点击 **Move Up** 或 **Move Down**，在列表内重新排列 APCF 配置文件。该排列顺序决定着使用哪个 APCF 配置文件。

步骤 2　如果您未在列表中发现您所作的更改，请点击 **Refresh**。

上载 APCF 数据包

步骤 1　系统显示您的计算机中指向 APCF 文件的路径。点击 **Browse Local**，自动在此字段插入该路径或输入该路径。

步骤 2　点击以查找和选择在您的计算机上要传输的 APCF 文件。Select File Path 对话框将显示您上一次在您的本地计算机上访问的文件夹的内容。导航至 APCF 文件，选择该文件，然后点击 **Open**。ASDM 将该文件路径插入到 Local File Path 字段。

步骤 3　Flash File System Path 中将显示 ASA 上要上载 APCF 文件的路径。点击 **Browse Flash**，确定 ASA 上要上载 APCF 文件的位置。 Browse Flash 对话框将显示闪存的内容。

步骤 4　系统将显示您在本地计算机上选择的 APCF 文件的文件名。我们建议您使用此名称以防止混乱。确认此文件显示的是正确的文件名，然后点击 **OK**。系统将关闭 Browse Flash 对话框。ASDM 将在 Flash File System Path 字段插入目标文件路径。

步骤 5　确定您的计算机上 APCF 文件的位置以及要下载到 ASA 中的位置后，请点击 **Upload File**。

步骤 6　系统将显示 Status 窗口，并且在文件传输过程中此窗口将保持打开。传输之后， Information 窗口将显示消息 “File is uploaded to flash successfully.” 点击 **OK**。Upload Image 对话框窗口将删除 Local File Path 和 Flash File System Path 的内容，这表示您可以上载另一个文件。要上载另一个文件，请重复上述说明。否则，请点击 **Close**。

步骤 7　关闭 Upload Image 对话框窗口。将 APCF 文件上载至闪存中之后或您决定不上载此文件时，请点击 **Close**。如果您选择上载，在 APCF 窗口的 APCF File Location 字段将显示文件名。如果您选择不上载，系统将显示 Close Message 对话框，提示您 “Are you sure you want to close the dialog without uploading the file?” 如果不想上载文件，请点击 **OK**。系统将关闭 Close Message 和 Upload Image 对话框，显示 APCF Add/Edit 窗格。否则，请在 Close Message 对话框中点击 **Cancel**。系统将关闭此对话框，再次显示 Upload Image 对话框，并且字段中的值保持不变。点击 **Upload File**。

管理 APCF 数据包

步骤 1　切换至无客户端 SSL VPN 配置模式。

```
webvpn
```

步骤 2　确定并找到要加载到 ASA 上的 APCF 配置文件。

本示例显示如何启用位于闪存上的 APCF 配置文件 apcf1.xml，以及如何启用位于 HTTPS 服务器 myserver 端口 1440上的 APCF 配置文件 apcf2.xml，其中路径为 /apcf。

apcf

示例：

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml

hostname(config)# webvpn
hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
```

步骤 1　使用以下命令添加、编辑和删除 APCF 数据包并按优先顺序进行排列：

- APCF File Location - 显示关于 APCF 数据包位置的信息。这个位置可能是在 ASA 闪存中，或者在 HTTP、 HTTPS、 FTP 或 TFTP 服务器上。
- Add/Edit - 点击以添加或编辑新的或现有的 APCF 配置文件。
- Delete - 点击以删除现有的 APCF 配置文件。无确认或撤消功能。
- Move Up - 点击以在列表内重新排列 APCF 配置文件。该列表决定着 ASA 尝试使用 APCF 配置文件的顺序。

步骤 2　点击 **Flash File**，查找存储在 ASA 闪存中的 APCF 文件。

步骤 3　输入指向存储在闪存中的 APCF 文件的路径。如果您已添加路径，则当您浏览查找此路径后，它将重定向到存储在闪存中的 APCF 文件。

步骤 4　点击 **Browse Flash**，浏览闪存以查找 APCF 文件。系统将显示 Browse Flash Dialog 窗格。使用 Folders 和 Files 列来查找 APCF 文件。突出显示 APCF 文件并点击 **OK**。然后在 Path 字段将显示指向该文件的路径。

注　如果您看不到您最近下载的 APCF 文件的名称，请点击 **Refresh**。

- Upload - 点击以将 APCF 文件从本地计算机上载至 ASA 闪存文件系统。系统将显示 Upload APCF Package 窗格。
- URL - 点击以使用 HTTP、 HTTPS 或 TFTP 服务器上存储的 APCF 文件。
- ftp、 http、 https 和 tftp （未标记的） - 标识服务器类型。
- URL （未标记的） - 输入指向 FTP、 HTTP、 HTTPS 或 TFTP 服务器的路径。

APCF 语法

APCF 配置文件采用 XML 格式和 sed 脚本语法，同时采用表 12-1 中的 XML 标签。

准则

APCF 配置文件使用错误可能导致性能下降和出现内容呈现意外。在大多数情况下，思科工程部供应 APCF 配置文件来解决特定应用呈现问题。

表 12-1　APCF XML 标签

标签	使用
<APCF>...</APCF>	打开任何 APCF XML 文件的强制性根元素。
<version>1.0</version>	指定 APCF 实施版本的强制性标签。目前唯一的版本是 1.0。
<application>...</application>	包围 XML 说明的正文的强制性标签。
<id>文本</id>	描述这个特定 APCF 功能的强制性标签。
<apcf-entities>...</apcf-entities>	包围一个或多个 APCF 实体的强制性标签。

表 12-1　　APCF XML 标签 （续）

标签	使用
<js-object>…</js-object> <html-object>…</html-object> <process-request-header>...</process-request-header> <process-response-header>...</process-response-header> <preprocess-response-body>...</preprocess-response-body> <postprocess-response-body>...</postprocess-response-body>	这些标签之一指定内容的类型或应该发生 APCF 处理的阶段。
<conditions>… </conditions>	指定处理标准的处理前/后标签的子元素，例如： • http-version （例如 1.1、 1.0、 0.9） • http-method （get、 put、 post、 webdav） • http-scheme （“http/”、 “https/”、其他） • server-regexp regular expression containing ("a".."z" | "A".."Z" | "0".."9" | ".-_*[]?") • server-fnmatch （正则表达式，包含 ("a".."z" | "A".."Z" | "0".."9" | ".-_*[]?+()\{},"）， • user-agent-regexp • user-agent-fnmatch • request-uri-regexp • request-uri-fnmatch • 如果存在不止一个条件标签，ASA 将对所有标签执行逻辑 AND 运算。
<action> … </action>	包围在特定条件下对内容执行的一项或多项操作；您可以使用以下标签来定义这些操作 （如下所示）： • <do> • <sed-script> • <rewrite-header> • <add-header> • <delete-header>
<do>…</do>	用于定义一个以下操作的操作标签子元素： • <no-rewrite/> - 请勿改变从远程服务器接收的内容。 • <no-toolbar/> - 请勿插入工具栏。 • <no-gzip/> - 请勿压缩内容。 • <force-cache/> - 保留原始缓存说明。 • <force-no-cache/> - 使对象不可缓存。 • < downgrade-http-version-on-backend> - 向远程服务器发送请求时使用 HTTP/1.0。

表 12-1　　APCF XML 标签（续）

标签	使用
<sed-script> 文本 </sed-script>	用于更改基于文本的对象内容的操作标签子元素。文本必须是有效的 Sed 脚本。 <sed-script> 适用于之前定义的 <conditions> 标签。
<rewrite-header></rewrite-header>	操作标签的子元素。更改如下所示子元素 <header> 标签中指定的 HTTP 报头的值。
<add-header></add-header>	用于添加在如下所示子元素 <header> 标签中指定的新 HTTP 报头的操作标签的子元素。
<delete-header></delete-header>	用于删除如下所示子元素 <header> 标签指定的 HTTP 报头的操作标签子元素。

<header></header>	指定要重写、添加或删除的名称 HTTP 报头。例如，以下标签将更改名为 Connection 的 HTTP 报头的值：
	`<rewrite-header>`
	`<header>Connection</header>`
	`<value>close</value>`
	`</rewrite-header>`

APCF 的配置示例

示例：

```
<APCF>
<version>1.0</version>
<application>
  <id>Do not compress content from example.com</id>
  <apcf-entities>
      <process-request-header>
         <conditions>
           <server-fnmatch>*.example.com</server-fnmatch>
         </conditions>
           <action>
             <do><no-gzip/></do>
           </action>
      </process-request-header>
  </apcf-entities>
</application>
</APCF>
```

示例：

```
<APCF>
<version>1.0</version>
<application>
 <id>Change MIME type for all .xyz objects</id>
 <apcf-entities>
      <process-response-header>
        <conditions>
            <request-uri-fnmatch>*.xyz</request-uri-fnmatch>
        </conditions>
         <action>
           <rewrite-header>
                <header>Content-Type</header>
                <value>text/html</value>
           </rewrite-header>
```

```
        </action>
      </process-response-header>
 </apcf-entities>
</application>
</APCF>
```

配置会话设置

Clientless SSL VPN Add/Edit Internal Group Policy > More Options > Session Settings 窗口允许您指定在无客户端 SSL VPN 会话之间显示的个性化用户信息。默认情况下，每个组策略都将继承默认组策略的设置。使用此窗口为您想要区分这些值的默认组策略和任意组策略指定个性化无客户端 SSL VPN 用户信息。

步骤 1　点击 **none** 或从 User Storage Location 下拉菜单选择文件服务器协议（smb 或 ftp）。思科建议将 CIFS 用于用户存储。您可以设置 CIFS，无需使用用户名/密码或端口号。如果选择 CIFS，请输入以下语法：

```
cifs//cifs-share/user/data
```

如果选择 smb 或 ftp，请使用以下语法将文件系统目标输入到相邻的文本字段：

```
username:password@host:port-number/path
```

例如

mike:mysecret@ftpserver3:2323/public

注　虽然配置将显示用户名、密码和预共享密钥，但是 ASA 将使用内部算法以加密形式存储数据以保护数据。

步骤 2　如有必要，请键入字符串，使安全设备可以提供对存储位置的用户访问。

步骤 3　从 Storage Objects 下拉菜单选择以下一个选项，指定服务器用于与该用户关联的对象。ASA 将存储这些对象以支持无客户端 SSL VPN 连接。

- cookie、凭据
- cookie
- 凭据

步骤 4　以 KB 为单位输入会话超时的事务大小限制。此属性仅适用于单个事务。仅大于该值的事务将重置会话过期时钟。

编码

字符编码，又称为“字符代码”和“字符集”，是指使用字符来表示数据对原始数据进行配对（例如 0s 和 1s）。语言决定着要使用的字符编码方法。有些语言使用单一方法，有些语言则不是的。通常，地理区域决定着浏览器使用的默认编码方法，但是远程用户可以进行更改。浏览器也可检测页面上指定的编码，并相应地呈现文档。

编码属性允许指定在门户页面上使用的字符编码方法的值，从而确保正确呈现此页面，无论用户是在什么区域使用该浏览器，也无论对浏览器进行了任何更改。

默认情况下，ASA 将对来自通用互联网文件系统 (CIFS) 服务器的页面应用 “Global Encoding Type”。在正确呈现文件名或目录路径以及页面方面遇到问题时，在全局使用 “Global Encoding Type” 属性并且对个别页面使用表格中显示的文件编码特例，将 CIFS 服务器映射为对应的字符编码，提供对 CISF 页面的正确处理和显示。

查看或指定字符编码

通过编码，您可查看或指定无客户端 SSL VPN 门户页面的字符编码。

步骤 1　Global Encoding Type 决定着所有无客户端 SSL VPN 门户页面继承的字符编码，表中列出来自 CIFS 服务器的字符编码除外。您可以键入字符串或从下拉列表中选择以下选项之一，此下拉列表包含大多数常用值，如下所示：

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis
- unicode
- windows-1252
- none

注　如果您点击 **none** 或指定无客户端 SSL VPN 会话上的浏览器不支持的值，它将使用自己的默认编码。

您可以键入最多包含 40 个字符并且等于 http://www.iana.org/assignments/character-sets 中确定的一个有效字符集的字符串。您可以使用该页列出的字符集的名称或别名。字符串不区分大小写。当保存 ASA 配置时，命令解释程序会将大写转换为小写。

步骤 2　输入编码要求与 “Global Encoding Type” 属性设置不同的 CIFS 服务器的名称或 IP 地址。ASA 将保留您指定的大小写，不过，它在将名称与服务器匹配时将忽略大小写。

步骤 3　选择 CIFS 服务器应该为无客户端 SSL VPN 门户页面提供的字符编码。您可以键入字符串或从下拉列表中选择以下选项之一，此下拉列表只包含大多数常用值，如下所示：

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis

注　如果使用的是日文 Shift_jis 字符编码，请在关联的 Select Page Font 窗格的 Font Family 区域点击 **Do Not Specify** 以删除该字体系列。

- unicode
- windows-1252
- none

如果您点击 **none** 或指定无客户端 SSL VPN 会话上的浏览器不支持的值，它将使用自己的默认编码。

您可以键入最多包含 40 个字符并且等于 http://www.iana.org/assignments/character-sets 中确定的一个有效字符集的字符串。您可以使用该页列出的字符集的名称或别名。字符串不区分大小写。当保存 ASA 配置时，命令解释程序会将大写转换为小写。

存储经常重复使用的对象

缓存增强了无客户端 SSL VPN 的性能。它将经常重复使用的对象存储在系统缓存中，这会减少对内容执行重复重写和压缩的需要。使用缓存可有效地减少流量，其结果是很多应用运行更加高效。

步骤 1　选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Content Cache**。

步骤 2　如果未选中 **Enable Cache**，请选中它。

步骤 3　定义缓存的条件。

- Maximum Object Size - 以 KB 为单位输入 ASA 可以缓存的文档的最大大小。ASA 将衡量对象的原始内容长度，而不是已重写或压缩的内容。此范围为 0 至 10,000 KB；默认值为 1000 KB
- Minimum Object Size - 以 KB 为单位输入 ASA 可以缓存的文档的最小大小。ASA 将衡量对象的原始内容长度，而不是已重写或压缩的内容。此范围为 0 至 10,000 KB；默认值为 0 KB

注　Maximum Object Size 必须大于 Minimum Object Size。

- Expiration Time - 以分钟为单位输入 0 至 900 之间的一个整数来设置缓存对象而不重新验证对象的时间。默认值为一分钟。
- LM Factor - 输入 1 至 100 之间的一个整数；默认值为 20。

  LM 因数为只有最后一次修改时间戳的缓存对象设置策略。这将重新验证没有服务器集更改值的对象。 ASA 估算自从对象更改后的时间长度，又叫做到期时间。估算的到期时间等于自从上一次更改之后经过的时间乘以 LM 因数。将 LM 因数设置为 0 可以迫使立即进行重新验证，而设置为 100 则会经历最长的允许时间才会重新验证。

  到期时间设置 ASA 缓存既没有上 - 次修改的时间戳也没有明确的服务器集到期时间的对象的时间长度。
- Cache static content - 选中即可缓存不可重写的所有内容，例如 PDF 文件和图像。
- Restore Cache Default - 点击以恢复所有缓存参数的默认值。

内容重写

Content Rewrite 窗格中列出要启用或关闭内容重写的所有应用。

无客户端 SSL VPN 处理流经内容转换/重写引擎的应用流量，此引擎包含 JavaScript、VBScript、Java 和多字节字符，用以代理可能具有不同语义和访问控制规则的 HTTP 流量，具体取决于用户是在 SSL VPN 设备内部还是独立于 SSL VPN 设备来使用某个应用。

默认情况下，安全设备会重写或转换所有无客户端流量。您可能会不想让某些应用和网络资源（例如公共网站）通过 ASA。因此，ASA 允许您创建允许用户浏览某些网站和应用程序，而不通过 ASA 的重写规则。这类似于 VPN 连接中的分离隧道。

注　ASA 9.0 中内容重写程序进行了以下改进：

- 内容重写增加了对 HTML5 的支持。
- 显著改进无客户端 SSL VPN 重写程序引擎以提供更好的质量和效率。因此，您可以预计无客户端 SSL VPN 用户将获得更好的最终用户体验。

创建重写规则

您可以创建多个重写规则。规则编号很重要，因为安全设备将按照序号搜索重写规则，从最低的序号开始，并应用匹配的第一个规则。

内容重写表有以下几列：

- 规则编号 - 显示指示规则在列表中的位置的整数。
- 规则名称 - 提供要应用该规则的应用的名称。
- 重写已启用 - 显示内容重写的启用或关闭状态。
- 资源掩码 - 显示资源掩码。

步骤 1　导航至 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Content Rewrite**。

步骤 2　点击 Add 或 Edit，创建或更新内容重写规则。

步骤 3　选中 **Enable content rewrite**，启用此规则。

步骤 4　请为此规则输入一个编号。此编号指定规则相对于列表中其他规则的优先级。无编号的规则位于列表的结尾。范围为 1 至 65534。

步骤 5　（可选）提供描述规则的字母数字字符串，最多 128 个字符。

步骤 6　输入与要应用规则的应用或资源匹配的字符串。字符串最多可以包含 300 个字符。您可以使用以下一种通配符，但是，您必须至少指定一个字母数字字符。

* - 匹配任意字符。 ASDM 不接受 * 或 *.* 组成的掩码

? - 匹配任意单个字符。

[!seq] - 匹配无先后顺序的任意字符。

[!seq] - 匹配有先后顺序的任意字符。

内容重写规则的配置示例

表 12-2　　内容重写规则

功能	启用内容重写	规则编号	规则名称	资源掩码
为 youtube.com 上的 HTTP URL 关闭重写程序	取消选中	1	no-rewrite-youtube	*.youtube.com/*
为不匹配上述规则的所有 HTTP URL 启用重写程序	检查	65,535	rewrite-all	*

在无客户端 SSL VPN 上使用邮件

配置网络邮件：MS Outlook Web App

ASA 支持 Microsoft Outlook Web App 对 Exchange Server 2010 以及 Microsoft Outlook Web Access 对 Exchange Server 2007、 2003 和 2000。

步骤 1　在地址字段输入邮件服务的 URL 或点击无客户端 SSL VPN 会话中的关联书签。

步骤 2　系统提示时，按照*域\用户名*的格式输入邮件服务器用户名。

步骤 3　输入邮件密码。

配置书签

Bookmarks 面板可以添加、编辑、删除、导入和导出书签列表。

使用 Bookmarks 面板配置服务器和 URL 列表以通过 SSL VPN 进行访问。配置书签列表之后，您可以将列表分配给一个或多个策略 - 组策略、动态访问策略或两者。每个策略只能有一个书签列表。列表名称会填充在每个 DAP 的 URL Lists 选项卡中的下拉列表上。

您现在可以利用宏替换使用书签自动登录某些网页。之前创建的 POST 插件方法使管理员可以指定带登录宏的 POST 书签和接收发布 POST 请求之前要加载的启动页面。这种 POST 插件方法消除了需要有 cookie 或其他标头项的那些请求。现在管理员要确定预加载页面和 URL，其指定向何处发送 POST 登录请求。预加载页面使终端浏览器可以获取一起发送至网络服务器或网络应用的特定信息，而不仅仅是使用包含凭据的 POST 请求。

系统将显示现有书签列表。您可以添加、编辑、删除、导入或导出书签列表。您可以配置访问的服务器和 URL 的列表并排列指定 URL 列表中项目的顺序。

准则

配置书签并不会阻止用户访问欺诈网站或违反公司的可接受使用策略的网站。除了向组策略、动态访问策略或两者分配书签列表之外，还可以向这些策略应用网络 ACL 以控制对流量的访问。关闭这些策略上的 URL 项以防用户对于可以访问的内容产生困惑。

步骤 1　指定要添加的列表的名称或选择要修改或删除的列表的名称。

系统显示书签标题和实际关联的 URL。

步骤 2　（可选）点击 **Add** 以配置新服务器或 URL。您可以执行一项以下操作：

- 使用 GET 或 Post 方法为 URL 添加书签
- 为预定义的应用模板添加 URL
- 为自动登录应用添加书签

步骤 3　（可选）点击 **Edit**，更改服务器、 URL 或显示名称。

步骤 4　（可选）点击 **Delete**，从 URL 列表删除选择的项目。没有确认或取消选项。

步骤 5　（可选）选择导入或导出文件的位置：

- Local computer - 点击以导入或导出位于本地 PC 上的文件。
- Flash file system - 点击以导入或导出位于 ASA 上的文件。
- Remote server - 点击以导入可以从 ASA 访问的远程服务器上的文件。
- Path - 确定访问文件的方法 （ftp、 http 或 https），并提供指向该文件的路径。
- Browse Local Files/Browse Flash... - 浏览该文件的路径。

步骤 6　（可选）突出显示书签并点击 **Assign**，将选择的书签分配给一个或多个组策略、动态访问策略或本地用户。

步骤 7　（可选）使用 **Move Up** 或 **Move Down** 选项更改选择的项目在 URL 列表中的位置。

步骤 8　点击 **OK**。

后续操作

请参阅无客户端 SSL VPN 安全预防措施。

使用 GET 或 Post 方法为 URL 添加书签

您可以通过 Add Bookmark Entry 对话框为 URL 列表创建链接或书签。

先决条件

要访问您的网络上的共享文件夹，请使用这种格式 \\服务器\共享\子文件夹\<*个人文件夹*>。用户必须具备<*个人文件夹*>上所有点的列表权限。

步骤 1　导航到 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks**，并点击 **Add** 按钮。

步骤 2　选择用于书签创建的使用 GET 或 POST 方法的 **URL**。

步骤 3　为该书签输入一个名称，其将显示在门户上。

步骤 4　使用 URL 下拉菜单选择 URL 类型：http、https、cifs 或 ftp。URL 下拉列表显示标准 URL 类型以及您安装的所有插件的类型。

步骤 5　为该书签输入 DNS 名称或 IP 地址 (URL)。对于插件，请输入服务器的名称。请在服务器名称后面输入一个正斜杠和一个问号 (/?)，指定可选的参数，然后使用 & 号分隔参数值对，如以下语法中所示：

server`/?`*Parameter*`=`*Value*`&`*Parameter*`=`*Value*

例如：

host/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

具体插件决定了您可以输入的可选参数值对。

要为插件提供单一登录支持，请使用参数值对 **csco_sso=1**。例如：

host/?csco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

步骤 6　（可选）输入预加载 URL。当您输入预加载 URL 时，也可以输入等待时间，即您允许在将您转发到实际 POST URL 之前加载页面的时间。

步骤 7　至于副标题，请提供描述书签项的用户可见的其他文本。

步骤 8　使用 Thumbnail 下拉菜单选择与最终用户门户上的书签关联的图标。

步骤 9　点击 **Manage**，导入或导出用做缩略图的图像。

步骤 10　点击以在新窗口中打开书签，此窗口使用智能隧道功能在 ASA 和目标服务器之间往返传递数据。所有浏览器流量都通过 SSL VPN 隧道安全传递。此选项允许您为基于浏览器的应用提供智能隧道支持，而同样位于 Clientless SSL VPN > Portal 菜单中的 Smart Tunnels 选项则允许您将基于非浏览器的应用添加到向组策略和用户名分配的智能隧道列表中。

步骤 11　选中 **Allow the Users to Bookmark the Link** 以允许无客户端 SSL VPN 用户使用其浏览器上的 Bookmarks 或 Favorites 选项。取消选中则会阻止访问这些选项。如果您取消选中此选项，则书签不会出现在无客户端 SSL VPN 门户的 Home 部分。

步骤 12　（可选）选择 **Advanced Options** 以配置其他书签属性。

- URL Method - 选择 **Get** 用于简单数据检索。当处理数据可能会涉及更改数据时，例如存储或更新数据、订购产品或发送邮件时，请选择 **Post**。
- Post Parameters - 配置 Post URL 方法的详情。

为预定义的应用模板添加 URL

此选项让用户选择 ASDM 模板，简化了书签创建，其中此模板包含特定明确定义的应用的预填必要值。

先决条件

预定义的应用模板目前仅可用于以下应用：

- Citrix XenApp
- Citrix XenDesktop
- Domino WebAccess
- Microsoft Outlook Web Access 2010
- Microsoft Sharepoint 2007
- Microsoft SharePoint 2010

步骤 1　为书签输入一个向用户显示的名称。

步骤 2　至于副标题，请提供描述书签项的用户可见的其他文本。

步骤 3　使用 **Thumbnail** 下拉菜单选择与最终用户门户上的书签关联的图标。

步骤 4　点击 **Manage**，导入或导出用做缩略图的图像。

步骤 5　（可选）选择 **Place This Bookmark on the VPN Home Page** 复选框。

步骤 6　在 **Select Auto Sign-on Application** 列表中，点击所需的应用。可用的应用如下：

- Citrix XenApp
- Citrix XenDesktop
- Domino WebAccess
- Microsoft Outlook Web Access 2010
- Microsoft Sharepoint 2007
- Microsoft SharePoint 2010

步骤 7　输入在登录页面之前加载的页面的 URL。此页面将要求用户交互才能继续进入登录屏幕。URL 将允许用 * 代替任意数量的符号，例如 http*://www.example.com/test。

步骤 8　输入**登录前页面控件 ID**。这是在登录前页面 URL 上获得点击事件以继续进入登录页面的控件/标签的 ID。

步骤 9　输入**应用参数**。根据应用可能包括以下参数：

- **Protocol**。 HTTP 或 HTTPs。
- **hostname**。例如 `www.cisco.com`。
- **Port Number**。应用使用的端口。
- **URL Path Appendix**。例如 `/Citrix/XenApp`。这通常会自动填充。
- **Domain**。要连接的域。
- **User Name**。用做用户名的 SSL VPN 变量。点击 **Select Variable** 选择不同的变量。
- **Password**。用做密码的 SSL VPN 变量。点击 **Select Variable** 选择不同的变量。

步骤 10　（可选）点击 **Preview** 查看模板输出。您可以点击 **Edit** 修改模板。

步骤 11　点击 **OK** 确定您的更改。或者，点击 **Cancel** 放弃更改。

为自动登录应用添加书签

此选项允许您为任何复杂的自动登录应用创建书签。

先决条件

配置自动登录应用需要两个步骤：

1. 用一些基本初始数据而不用 POST 参数定义书签。保存书签并将其分配用于组或用户策略。
2. 重新编辑书签。在书签中使用捕获功能捕获 SSL VPN 参数并进行编辑。

步骤 1　为书签输入一个向用户显示的名称。

步骤 2　使用 URL 下拉菜单选择 URL 类型：http、https、cifs 或 ftp。所有导入的插件的 URL 类型也会填充在此菜单上。选择在门户页面上显示为链接的插件的 URL 类型。

步骤 3　为该书签输入 DNS 名称或 IP 地址。对于插件，请输入服务器的名称。请在服务器名称后面输入一个正斜杠和一个问号 (/?)，指定可选的参数，然后使用 & 号分隔参数值对，如以下语法中所示：

server`/?`*Parameter*`=`*Value*`&`*Parameter*`=`*Value*

例如：

host/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

具体插件决定了您可以输入的可选参数值对。

要为插件提供单一登录支持，请使用参数值对 **csco_sso=1**。例如：

host/?csco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

步骤 4　至于副标题，请提供描述书签项的用户可见的其他文本。

步骤 5　使用 **Thumbnail** 下拉菜单选择与最终用户门户上的书签关联的图标。

步骤 6　点击 **Manage**，导入或导出用做缩略图的图像。

步骤 7　（可选）选择 **Place This Bookmark on the VPN Home Page** 复选框。

步骤 8　输入**登录页面 URL**。在您输入的 URL 中可以使用通配符。例如，您可以输入 http*://www.example.com/myurl*。

步骤 9　输入**登陆页面 URL**。 ASA 要求将登陆页面配置为检测是否成功登录应用。

步骤 10　（可选）输入 **Post 脚本**。 Microsoft Outlook Web Access 等一些网络应用在提交登录表单之前可能会执行 JavaScript 来更改请求参数。 **Post Script** 字段允许您输入这类应用的 JavaScript。

步骤 11　添加必要的**表单参数**。对于每个所需的 SSL VPN 变量，点击 **Add**，输入 **Name**，并从列表中选择变量。您可以点击 **Edit** 更改参数，也可以点击 **Delete** 删除参数。

步骤 12　输入在登录页面之前加载的页面的 URL。此页面将要求用户交互才能继续进入登录屏幕。URL 将允许用 * 代替任意数量的符号，例如 http*://www.example.com/test。

步骤 13　输入**登录前页面控件 ID**。这是在登录前页面 URL 上获得点击事件以继续进入登录页面的控件/标签的 ID。

步骤 14　点击 **OK** 确定您的更改。或者，点击 **Cancel** 放弃更改。

当您编辑书签时可以使用 HTML Parameter Capture 功能捕获 VPN 自动登录参数。必须首先保存书签并将其分配给组策略或用户。

输入 **SSL VPN Username**，然后点击 **Start Capture**。然后使用网络浏览器启动 VPN 会话并导航至内联网页面。要结束该进程，请点击 **Stop Capture**。参数然后就可以进行编辑并插入书签中。

导入和导出书签列表

您可以导入或导出已经配置的书签列表。导入现成可用的列表。导出列表进行修改或编辑，然后重新导入。

步骤 1　按照名称标识书签列表。最多 64 个字符，不能包含空格。

步骤 2　选择导入或导出列表文件的方法。

- Local computer - 点击以导入位于本地 PC 上的文件。
- Flash file system - 点击以导出位于 ASA 上的文件。
- Remote server - 点击以导入可以从 ASA 访问的远程服务器上的 url 列表文件。
- Path - 确定访问文件的方法 （ftp、 http 或 https），并提供指向该文件的路径。
- Browse Local Files/Browse Flash - 浏览该文件的路径。
- Import/Export Now - 点击以导入或导出列表文件。

导入和导出 GUI 自定义对象 （网络内容）

此对话框允许您导入和导出网络内容对象。系统将显示网络内容对象的名称及其文件类型。

网络内容包括从完全配置的主页到自定义最终用户门户时使用的图标或图像。您可以导入或导出已配置的网络内容和导入现成可用的网络内容。导出网络内容进行修改或编辑，然后重新导入。

步骤 1　选择要导入或导出文件的位置：

- Local computer - 点击以导入或导出位于本地 PC 上的文件。
- Flash file system - 点击以导入或导出位于 ASA 上的文件。
- Remote server - 点击以导入可以从 ASA 访问的远程服务器上的文件。
- Path - 确定访问文件的方法 （ftp、 http 或 https），并提供指向该文件的路径。
- Browse Local Files.../Browse Flash... - 浏览至该文件的路径

步骤 2　确定访问该内容是否需要身份验证。

路径的前缀会根据您是否要求身份验证而变化。对于要求身份验证的对象，ASA 使用 /+CSCOE+/；对于不要求身份验证的对象，则使用 /+CSCOU+/。ASA 在门户页面只显示 /+CSCOE+/，而在登录或门户页面 /+CSCOU+/ 对象都会显示而且可用。

步骤 3　点击以导入或导出文件。

添加和编辑 POST 参数

使用此窗格配置书签条目和 URL 列表的 POST 参数。

无客户端 SSL VPN 变量允许在 URL 和基于表单的 HTTP POST 操作中进行替换。这些变量，也称为宏，可以配置用户访问包含用户 ID 和密码或其他输入参数的个性化资源。此类资源的示例包括书签条目、 URL 列表和文件共享。

步骤 1　提供和对应 HTML 表单中完全一样的参数名称和值，例如：

```
<input name="param_name" value="param_value">
```

您可以从下拉列表中选择其中一个已提供的变量，也可以构建变量。您可以从下拉列表中选择的变量包括：

表 12-3　无客户端 SSL VPN 变量

序号	变量替换	定义
1	CSCO_WEBVPN_USERNAME	SSL VPN 用户登录 ID。
2	CSCO_WEBVPN_PASSWORD	SSL VPN 用户登录密码。
3	CSCO_WEBVPN_INTERNAL_PASSWORD	SSL VPN 用户内部资源密码。这是缓存的凭据而且未由 AAA 服务器进行身份验证。如果用户输入此值，它将用作自动登录的密码，代替密码值。
4	CSCO_WEBVPN_CONNECTION_PROFILE	SSL VPN 用户登录组下拉列表，连接配置文件中的组别名

表 12-3　无客户端 SSL VPN 变量 （续）

序号	变量替换	定义
5	CSCO_WEBVPN_MACRO1	通过 RADIUS/LDAP 供应商特定属性设置。如果通过 ldap-attribute-map 从 LDAP 映射这个变量，则使用此变量的思科属性为 WEBVPN-Macro-Substitution-Value1。 通过 RADIUS 进行的变量替换由 VSA#223 执行。
6	CSCO_WEBVPN_MACRO2	通过 RADIUS/LDAP 供应商特定属性设置。如果通过 ldap-attribute-map 从 LDAP 映射这个变量，则使用此变量的思科属性为 WEBVPN-Macro-Substitution-Value2。 通过 RADIUS 进行的变量替换由 VSA#224 执行。
7	CSCO_WEBVPN_PRIMARY_USERNAME	双重身份验证的主要用户登录 ID。
8	CSCO_WEBVPN_PRIMARY_PASSWORD	双重身份验证的主要用户登录密码。
9	CSCO_WEBVPN_SECONDARY_USERNAME	双重身份验证的二级用户登录 ID。
10	CSCO_WEBVPN_SECONDARY_PASSWORD	双重身份验证的二级用户登录 ID。

当 ASA 识别书签或发布表单中这六个变量字符串中的一个时，在将请求传递至远程服务器之前它会将它替换为用户特定值。

注　可以通过执行 HTTP 探查器跟踪 （不涉及安全设备），为任意应用获取 http-post 参数。以下是一个免费浏览器捕获工具，又叫做 HTTP 分析器的链接：http://www.ieinspector.com/httpanalyzer/downloadV2/IEHttpAnalyzerV2.exe。

使用变量 1 至 4

ASA 为 SSL VPN 登录页面前四个替换获取变量，这包括用于用户名、密码、内部密码 （可选）和组的字段。它将识别用户请求中的这些字符串并将其替换为用户特定的值，再将请求传递至远程服务器。

例如，如果 URL 列表包含链接 http://someserver/homepage/CSCO_WEBVPN_USERNAME.html，ASA 会将其转换为以下唯一性链接：

- 对于 USER1，此链接变为 http://someserver/homepage/USER1.html
- 对于 USER2，此链接变为 http://someserver/homepage/USER2.html

在以下情况下，cifs://server/users/CSCO_WEBVPN_USERNAME 允许 ASA 将文件驱动器映射至特定用户：

- 对于 USER1，此链接变为 cifs://server/users/USER1
- 对于 USER 2，此链接变为 cifs://server/users/USER2

使用变量 5 至 6

宏 5 和 6 的值是 RADIUS 或 LDAP 供应商特定属性 (VSA)。这些变量让您可以设置 RADIUS 或 LDAP 服务器上配置的替换。

使用变量 7 至 10

每次 ASA 识别最终用户请求 （书签或发布表单）中这四个字符串中的一个时，它会将其替换为用户特定值再将此请求传递给远程服务器。

设置主页的示例

以下示例将为主页设置 URL：

- WebVPN-Macro-Value1 (ID=223) 类型字符串返回为 *wwwin-portal.example.com*
- WebVPN-Macro-Value2 (ID=224) 类型字符串返回为 *401k.com*

要设置主页值，您需要将变量替换配置为

https://CSCO_WEBVPN_MACRO1，这将转换为 https://wwwin-portal.example.com。

执行此操作的最佳方法是在 ASDM 中配置主页 URL 参数。无需写入脚本或上载任何内容，管理员可以指定通过智能隧道连接组策略中的哪个主页。

从 ASDM 的 Network Client SSL VPN 或 Clientless SSL VPN Access 部分转到 Add/Edit Group Policy 窗格。路径如下所示：

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit Group Policy > Advanced > SSL VPN Client > Customization > Homepage URL attribute
- Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add/Edit Group Policy > More Options > Customization > Homepage URL attribute

设置书签或 URL 项的配置示例

您可以使用 HTTP POST 登录使用 SSL VPN 身份验证的 RSA 一次性密码 (OTP) 的 OWA 资源，然后使用静态内部密码访问 OWA 邮件。执行此操作的最好方法是在 ASDM 中添加或编辑书签。

有多条路径指向 Add Bookmark Entry 窗格，包括以下路径：

- Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks > Add/Edit Bookmark Lists > Add/Edit Bookmark Entry > Advanced Options area > Add/Edit Post Parameters（在 URL Method 属性中点击 **Post** 之后可用）
- Network (Client) Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > URL Lists 选项卡 > Manage 按钮 > Configured GUI Customization Objects > Add/Edit 按钮 > Add/Edit Bookmark List > Add/Edit Bookmark Entry > Advanced Options 区域 > Add/Edit Post Parameters

配置文件共享 (CIFS) URL 替换的配置示例

您可以通过 CIFS URL 的变量替换，允许进行更灵活的书签配置。

如果您配置 URL cifs://server/CSCO_WEBVPN_USERNAME， ASA 会将其自动映射到用户的文件共享主目录。此方法还允许进行密码和内部密码替换。以下是 URL 替换示例：

cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server

cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server

cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server

cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server

cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server/CSCO_WEBVPN_USERNAME

cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server/CSCO_WEBVPN_USERNAME

自定义外部端口

您可以使用外部门户功能创建自己的门户，代替使用预配置的门户。如果您设置了自己的门户，您可以绕过无客户端门户并发送 POST 请求以检索您的门户。

步骤 1　选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization**。突出显示相应的自定义对象并选择 **Edit**。

步骤 2　选中 **Enable External Portal** 复选框。

步骤 3　在URL 字段中，输入相应的外部门户以允许使用 POST 请求。

策略组

配置智能隧道访问

下节将说明如何使用无客户端 SSL VPN 会话启用智能隧道访问，指定此访问提供的应用，并提供其使用说明。

配置智能隧道访问

要配置智能隧道访问，您要创建一份包含一个或多个可以执行智能隧道访问的智能隧道列表以及与此列表关联的终端操作系统。由于每个组策略或本地用户策略都支持一个智能隧道列表，您必须将要支持的基于非浏览器的应用归类到智能隧道列表中。创建此列表后，请将其分配给一个或多个组策略或本地用户策略。

以下节将介绍智能隧道以及如何配置智能隧道：

关于智能隧道

智能隧道是基于 TCP 的应用与专用站点之间的一种连接，其使用无客户端 （基于浏览器的） SSL VPN 会话，以安全设备作为通道并以 ASA 作为代理服务器。您可以确定要授权智能隧道访问的应用并指定每个应用的本地路径。对于 Microsoft Windows 上运行的应用，您还可以要求匹配校验和的 SHA-1 哈希值，作为授权智能隧道访问的条件。

Lotus Sametime 和 Microsoft Outlook 是您可能要授权智能隧道访问的应用示例。

配置智能隧道需要执行以下步骤之一，具体取决于应用是客户端还是支持网络的应用：

- 创建客户端应用的一个或多个智能隧道列表，然后将列表分配给需要智能隧道访问的组策略或本地用户策略。
- 创建一个或多个书签列表条目来指定符合智能隧道访问条件、支持网络的应用的 URL，然后将列表分配给需要智能隧道访问的组策略或本地用户策略。

您还可以列出通过无客户端 SSL VPN 会话在智能隧道连接中自动提交登录凭据的支持网络的应用。

为什么选择智能隧道？

智能隧道访问让客户端基于 TCP 的应用可以使用基于浏览器的 VPN 连接访问服务。与插件和端口转发传统技术相比，它可给用户提供以下优势：

- 智能隧道性能比插件更好。
- 不同于端口转发，智能隧道不要求用户将本地应用连接至本地本地端口，简化了用户体验。
- 不同于端口转发，智能隧道不要求用户拥有管理员权限。

插件的优点在于它不要求在远程计算机上安装客户端应用。

先决条件

有关 ASA 9.0 版本智能隧道支持的平台和浏览器，请参阅*受支持的 VPN 平台、思科 ASA 系列*。

下列要求和限制适用于 Windows 上的智能隧道访问：

- 在 Windows 中必须在浏览器上启用 ActiveX 或 Oracle Java Runtime Environment (JRE) 4 更新 15 或更高版本 （推荐 JRE 6 或更高版本）。
- 仅 Winsock 2、基于 TCP 的应用符合智能隧道访问条件。
- 仅适用于 Mac OS X，必须在浏览器上启用 Java Web Start。

限制

- 智能隧道仅支持放在运行 Microsoft Windows 的计算机和安全设备之间的代理。智能隧道使用 Internet Explorer 配置，其设置 Windows 中的全系统参数。此配置可能包括代理信息：
  - 如果 Windows 计算机需要代理才能访问 ASA，则客户端浏览器中必须有一个静态代理条目，并且要连接的主机必须在客户端的代理异常列表上。
  - 如果 Windows 计算机不需要代理就能访问 ASA，但是，需要代理才能访问主机应用，则 ASA 必须在客户端的代理异常列表上。

  代理系统可以由静态代理条目的客户端配置或自动配置定义，或者由 PAC 文件定义。目前智能隧道仅支持静态代理配置。
- 智能隧道不支持 Kerberos 约束委派 (KCD)。

- 对于 Windows，要向从命令提示符启动的应用添加智能隧道访问，您必须在智能隧道列表一个条目的 Process Name 中指定 “cmd.exe”，然后在另一个条目中指定指向该应用本身的路径，因为 “cmd.exe” 是该应用的父级。
- 对于基于 HTTP 的远程访问，某些子网可能会阻止用户访问 VPN 网关。要解决此问题，请在 ASA 前面放一个代理，路由网络和最终用户之间的流量。该代理必须支持此连接方法。对于需要身份验证的代理，智能隧道仅支持基本摘要式身份验证类型。
- 智能隧道启动时，默认情况下，如果浏览器进程相同，ASA 会将所有浏览器流量传递通过 VPN 会话。只有在应用全隧道策略（默认配置）的情况下，ASA 才会也这么做。如果用户启动浏览器进程的另一个实例，它会将所有流量传递通过 VPN 会话。如果浏览器进程相同，但安全设备不提供对 URL 的访问，用户将无法打开它。作为应急方案，请分配不属于全隧道的隧道策略。
- 状态故障转移不保留智能隧道连接。出现故障转移后，用户必须重新连接。
- Mac 版本的智能隧道不支持 POST 书签、基于表单的自动登录或 POST 宏替换。
- 对于 Mac OS X 用户，只有从门户页面启动的那些应用才可以建立智能隧道连接。此要求包括对 Firefox 的智能隧道支持。在首次使用智能隧道期间使用 Firefox 启动 Firefox 的另一个实例要求使用名称为 csco_st 的用户配置文件。如果没有此用户配置文件，会话将提示用户创建一个此配置文件。
- 在 Mac OS X 中，使用与 SSL 库动态链接的 TCP 的应用可通过智能隧道运行。
- 智能隧道在 Mac OS X 上不提供以下支持：
  - 代理服务。
  - 自动登录。
  - 使用两层名称空间的应用。
  - 基于控制台的应用，如 Telnet、 SSH 和 cURL。
  - 使用 dlopen 或 dlsym 来查找 libsocket 调用的应用。
  - 静态链接的应用查找 libsocket 调用。
- Mac OS X 需要指定进程的完整路径并区分大小写。为避免指定每个用户名的路径，请在部分路径前面插入波形符 (~)（例如 ~/bin/vnc）。

配置智能隧道 （Lotus 示例）

注　这些示例说明提供了为应用增加智能隧道支持所需的最少说明。有关详细信息，请参阅以下节中的字段描述。

详细步骤

步骤 1　选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**。

步骤 2　双击要添加应用的智能隧道列表；或者点击 **Add** 创建应用列表，在 List Name 字段为此列表输入一个名称，然后点击 **Add**。

例如，在 Smart Tunnels 窗格点击 **Add**，在 List Name 字段输入 **Lotus**，然后点击 **Add**。

步骤 3　在 Add or Edit Smart Tunnel List 对话框中点击 **Add**。

步骤 4　在 Application ID 字段输入一个字符串作为指向智能隧道列表中该条目的唯一索引。

步骤 5　在 Process Name 对话框中输入该应用的文件名和扩展名。

表 13-1 显示了示例应用 ID 字符串和要支持 Lotus 所需的关联路径。

表 13-1　智能隧道示例：使用 Domino Server 6.5.5 的 Lotus 6.0 胖客户端

应用 ID 示例	最低进程名称要求
lotusnotes	notes.exe
lotusnlnotes	nlnotes.exe
lotusntaskldr	ntaskldr.exe
lotusnfileret	nfileret.exe

步骤 6　选择 OS 旁的 **Windows**。

步骤 7　点击 **OK**。

步骤 8　为要向列表添加的每个应用分别重复第 3 步至第 7 步。

步骤 9　在 Add or Edit Smart Tunnel List 对话框中点击 **OK**。

步骤 10　将此列表分配给组策略或本地用户策略，提供对关联应用的智能隧道访问，如下所述：

- 要将此列表分配给组策略，请选择 **Configuration > Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add** or **Edit > Portal** 并从 Smart Tunnel List 属性旁的下拉列表中选择智能隧道名称。
- 要将此列表分配给本地用户策略，请选择 **Configuration > Remote Access VPN> AAA Setup > Local Users > Add** or **Edit > VPN Policy > Clientless SSL VPN** 并从 Smart Tunnel List 属性旁的下拉列表选择智能隧道名称。

简化要授权隧道访问的应用的配置

智能隧道应用列表实质上是确定哪些应用授予了隧道访问的一种过滤器。默认情况是允许浏览器启动的所有进程的访问。使用支持智能隧道的书签，无客户端会话将只授权对网络浏览器启动的进程的访问。对于非浏览器应用，管理员可以选择通过隧道访问所有应用，从而无需了解最终用户可能调用哪些应用。表 13-2 显示了进程被授权访问的情况。

表 13-2　智能隧道应用的访问和支持智能隧道的书签

情况	支持智能隧道的书签	智能隧道应用访问
已指定应用列表	与应用列表中进程名称匹配的任何进程都被授权访问。	只有与应用列表中进程名称匹配的进程才被授权访问。
智能隧道关闭	所有进程 （及其子进程）都被授权访问。	无任何进程被授权访问。
已选中 Smart Tunnel all Applications 复选框。	所有进程 （及其子进程）都被授权访问。 **注**　如果网页是由相同浏览器进程提供服务，这将包括由非智能隧道网页启动的进程。	由启动浏览器的用户发起的所有进程都被授权访问，但不包括这些原始进程的任何子进程。

限制

此配置仅适用于 Windows 平台。

详细步骤

步骤 1　选择**Configuration > Remote Access VPN > AAA/Local Users > Local Users**。

步骤 2　在 User Account 窗口中，突出显示要编辑的用户名。

步骤 3　点击 **Edit**。系统将显示 Edit User Account 窗口。

步骤 4　在 Edit User Account 窗口的边栏，点击 **VPN Policy > Clientless SSL VPN**。

步骤 5　执行下列操作之一：

- 选中 **smart tunnel_all_applications** 复选框。所有应用都将通过隧道访问，无需制定列表或知道最终用户可能对外部程序调用哪些可执行文件。
- 或从以下隧道策略选项进行选择：
  - 在 Smart Tunnel Policy 参数上，取消选中 **Inherit** 复选框。
  - 从网络列表进行选择并指定以下一个隧道选项：为指定网络使用智能隧道、不为指定网络使用智能隧道或为所有网络流量使用隧道。

添加符合智能隧道访问条件的应用

每个 ASA 的无客户端 SSL VPN 配置都支持 *智能隧道列表*，每个列表都会确定一个或多个符合智能隧道访问条件的应用。由于每个组策略或用户名都只支持一个智能隧道列表，您必须将每组要支持的应用分别归类为一个智能隧道列表。

Add or Edit Smart Tunnel Entry 对话框允许您指定智能隧道列表中应用的属性。

步骤 1　导航至 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels** 并选择要编辑的智能隧道应用列表，或添加一个新列表。

步骤 2　对于新列表，请为该应用或程序列表添加唯一名称。不要使用空格。

配置智能隧道列表后，在无客户端 SSL VPN 组策略或本地用户策略中在 Smart Tunnel List 属性旁将显示该列表名称。请分配一个可以帮助您将其内容或用途与您可能要配置的其他列表区分开来的名称。

步骤 3　点击 **Add** 并按照您的需求向此智能隧道列表添加相应数量的应用。以下是参数说明：

- Application ID - 输入一个字符串，为智能隧道列表中的条目命名。系统将保存这个用户指定的名称，然后将其返回至 GUI 上。此字符串对于操作系统是唯一的。它通常命名的是要被授权智能隧道访问的应用。要支持同一应用的多个版本，其中您选择为这些应用指定不同的路径或哈希值，您可以使用这个属性来区分不同条目，指定操作系统以及每个列表条目支持的应用的名称和版本。此字符串最多可以包含 64 个字符。
- Process Name - 输入文件名或指向应用的路径。此字符串最多可以包含 128 个字符。

  Windows 要求此值与远程主机上应用路径的右边完全匹配，才向此应用授权智能隧道访问。如果您只指定 Windows 的文件名，SSL VPN 无法在远程主机上强制执行位置限制来向应用授权智能隧道访问。

  如果您指定了路径，但是用户将应用安装在了另一个位置上，该应用程序将无法获得授权。只要该字符串的右边与您输入的值匹配，该应用就可以放在任何路径上。

  要向应用授权智能隧道访问，如果应用位于远程主机若干个路径之一上，请在此字段中只指定应用的名称和扩展名，或为每个路径创建一个唯一的智能隧道条目。

注　智能隧道访问突然出现问题可能表明 *Process Name* 值未随着应用升级一起更新。例如，某个应用的路径有时候会随着生产此应用的公司被收购和下一次应用升级而变化。

对于 Windows，要向从命令提示符启动的应用添加智能隧道访问，您必须在智能隧道列表一个条目的 Process Name 中指定 “cmd.exe”，然后在另一个条目中指定指向该应用本身的路径，因为 “cmd.exe” 是该应用的父级。

- OS - 点击 **Windows** 或 **Mac**，指定应用的主机操作系统。
- Hash （可选，而且只适用于 Windows） - 要获得此值，请将应用的校验和 （即可执行文件的校验和）输入使用 SHA-1 算法计算哈希值的实用程序。有一个此类实用程序示例是 Microsoft File Checksum Integrity Verifier (FCIV)，可从 http://support.microsoft.com/kb/841290/ 获取。安装 FCIV 之后，将要进行哈希运算的应用的临时副本放在不包含任何空格的路径上 （例如 c:/fciv.exe），然后在命令行输入 **fciv.exe -sha1** *应用*（例如 **fciv.exe -sha1 c:\msimn.exe**），显示 SHA-1 哈希值。

  SHA-1 哈希值始终是 40 个十六进制字符。

  向应用授权智能隧道访问之前，无客户端 SSL VPN 将计算与 *Application ID* 匹配的应用的哈希值。如果其结果与 *Hash* 的值匹配，则会向此应用授权智能隧道访问。

  输入哈希值可提供一个合理的保障，即 SSL VPN 不会向与您在 *Application ID* 字段指定的字符串匹配的不合法文件授权。由于校验和随应用的各个版本或补丁而变化，您输入的*哈希*只能与远程主机上的一个版本或补丁匹配。要为应用的多个版本指定哈希，请为每个*哈希*值创建一个唯一的智能隧道条目。

注　如果您输入*哈希*值并且您需要智能隧道访问支持应用的未来版本或补丁，您必须不断更新智能隧道列表。智能隧道访问突然出现问题可能表明包含*哈希*值的应用列表没有用最新的应用升级进行更新。您可以通过不输入哈希避免此问题。

步骤 4　点击 **OK**，保存应用，然后确定此智能隧道列表需要多少个应用。

步骤 5　当您完成创建您的智能隧道列表时，您必须按照以下步骤将其分配给组策略或本地用户策略才能激活它：

- 要将此列表分配给组策略，请选择 **Config > Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add** or **Edit > Portal**，然后从 Smart Tunnel List 属性旁的下拉列表选择智能隧道名称。
- 要将此列表分配给本地用户策略，请选择 **Config > Remote Access VPN> AAA Setup > Local Users > Add** or **Edit > VPN Policy > Clientless SSL VPN** 并从 Smart Tunnel List 属性旁的下拉列表选择智能隧道名称。

表 13-3　　示例智能隧道条目

智能隧道支持	应用 ID （任意唯一的字符串均可。）	进程名称	操作系统
Mozilla Firefox。	firefox	firefox.exe	Windows
Microsoft Outlook Express。	Outlook Express	msimn.exe	Windows
如果可执行文件位于预定义路径上，则限制更严格，只可选择备选的 Microsoft Outlook Express。	Outlook Express	\Program Files\Outlook Express\msimn.exe	Windows

表 13-3　　示例智能隧道条目 （续）

智能隧道支持	应用 ID （任意唯一的字符串均可。）	进程名称	操作系统
在 Mac 上打开新 Terminal 窗口。（由于实施一次性密码，从同一 Terminal 窗口内启动的所有后续应用会出故障。）	terminal	Terminal	Mac
打开新窗口的智能隧道	new-terminal	Terminal open -a MacTelnet	Mac
从 Mac Terminal 窗口启动应用。	curl	Terminal curl www.example.com	Mac

有关智能隧道列表

对于每个组策略和用户名，可以配置无客户端 SSL VPN 执行以下任一操作：

- 在用户登录时自动启动智能隧道访问。
- 在用户登录时启动智能隧道访问，但是要求用户手动启动，即使用无客户端 SSL VPN 门户页面上的 **Application Access > Start Smart Tunnels** 按钮。

限制

对于每个组策略和用户名，智能隧道登录选项是互相排斥的。只能使用一个。

创建智能隧道自动登录服务器列表

Smart Tunnel Auto Sign-on Server List 对话框允许您添加或编辑将在智能隧道设置期间自动提交登录凭据的服务器列表。通过智能隧道的自动登录可用于 Internet Explorer 和 Firefox。

步骤 1　导航至 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**，并确保展开显示 Smart Tunnel Auto Sign-on Server List。

步骤 2　点击 **Add**，然后为远程服务器列表输入一个可以帮助您将其内容或用途与您可能配置的其他列表区分开的唯一名称。此字符串最多可以包含 64 个字符。不要使用空格。

创建智能隧道自动登录列表之后，在无客户端 SSL VPN 组策略和本地用户策略配置中 Smart Tunnel 下方 Auto Sign-on Server List 属性旁将显示此列表名称。

将服务器添加到智能隧道自动登录服务器列表中

以下步骤说明了如何将服务器添加到要在智能隧道连接中提供自动登录的服务器列表中以及如何将该列表分配给组策略或本地用户。

步骤 1　导航至 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**，选择一个列表，然后点击 **Edit**。

步骤 2　在 Add Smart Tunnel Auto Sign-On Server List 对话框上点击 **Add** 按钮，再添加一个智能隧道服务器。

步骤 3　输入要执行自动身份验证的服务器的主机名或 IP 地址：

- 如果您选择 Hostname，请输入要执行自动身份验证的主机名或通配符掩码。您可以使用以下通配符：
  - * 匹配任意数量的字符或零字符。
  - ?匹配任意单个字符。
  - [] 匹配方括号中表示的范围内的任何单个字符。
  - 例如，输入 *.example.com。使用此选项避免配置出现 IP 地址动态变化。
- 如果您选择 IP Address，请输入 IP 地址。

注　Firefox 不支持使用通配符的主机掩码、使用 IP 地址的子网或网络掩码；您必须使用完全匹配的主机名或 IP 地址。例如，在 Firefox 中，您不能输入 *.cisco.com，否则将无法自动登录主机 email.cisco.com。

步骤 4　Windows Domain （可选） - 如果身份验证要求，点击此选项即可将 Windows 域添加至用户名中。如果您这么做，请确保在将智能隧道列表分配到一个或多个组策略或本地用户策略时指定域名。

步骤 5　基于 HTTP 的自动登录 （可选）

- Authentication Realm - 该领域与网站的受保护区域关联，并且在身份验证期间在身份验证提示中或 HTTP 报头中回传至浏览器。在此处配置了自动登录并且指定了领域字符串之后，用户可以配置网络应用 （例如 Outlook Web Access）的领域字符串，然后无需登录即可访问网络应用。

  使用内联网上网页的源代码中使用的地址格式。如果您在为浏览器访问配置智能隧道自动登录，并且某些网页使用主机名，而其他网页使用 IP 地址，或者您不知道使用的是什么，请指定两个不同的智能隧道自动登录条目。否则，如果网页上的链接使用不同于您所指定格式的格式，则用户点击此链接时会出现故障。

注　如果管理员不知道对应的领域，他们应该执行一次登录并从提示对话框获取该字符串。

- Port Number - 为对应的主机指定端口号。对于 Firefox，如果没有指定端口号，则在 HTTP 和 HTTPS 上执行自动登录，其分别用默认端口号 80 和 443 访问。

步骤 6　点击 **OK**。

步骤 7　配置智能隧道自动登录服务器列表后，您必须将其分配给组策略或本地用户策略才能使它激活，如下所述：

- 要将列表分配给组策略：
  1. 导航至 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**，并打开组策略。
  2. 选择 Portal 选项卡，找到 Smart Tunnel 区域，然后从 Auto Sign-On Server List 旁的下拉列表中选择自动登录服务器列表。
- 要将列表分配给本地用户策略：
  1. 选择 **Configuration > Remote Access VPN > AAA/Local Users > Local Users**，然后编辑要向其分配自动登录服务器列表的本地用户。
  2. 导航至 **VPN Policy > Clientless SSL VPN**，在 Smart Tunnel 区域下面找到 Auto Sign-on Server 设置
  3. 取消选中 **Inherit**，然后从 Auto Sign-On Server List 属性旁的下拉列表选择一个服务器列表。

启用和关闭智能隧道访问

默认情况下，智能隧道处于关闭状态。

如果您启用智能隧道访问，用户必须手动启动，即使用无客户端 SSL VPN 门户页面上的 **Application Access > Start Smart Tunnels** 按钮。

配置智能隧道注销

本节介绍如何确保正确注销智能隧道。当所有浏览器窗口都已关闭时可以注销智能隧道，也可以右键单击通知图标并确认注销。

注　我们强烈建议使用门户上的注销按钮。此方法适合于无客户端 SSL VPN 和不管是否使用智能隧道都要注销的情况。只有在使用独立应用而不使用服务器的时候才可以使用通知图标。

当父进程终止时

这种做法要求所有浏览器都关闭才表示注销。目前智能隧道生命期与启动进程生命期关联。例如，如果您从 Internet Explorer 启动智能隧道，无 iexplore.exe 运行时智能隧道就会关闭。即使用户关闭了所有浏览器而不注销，智能隧道仍可确定 VPN 会话已经结束。

注　有些情况下，浏览器进程会延迟，那属于意外情况，并且严格地讲应该是错误导致的。此外，使用安全桌面时，即使用户在安全桌面中关闭所有浏览器，浏览器进程仍然可以在另一个桌面上运行。因此，在当前桌面中再也没有可见窗口时，智能隧道即宣布所有浏览器实例都已关闭。

使用通知图标

您还可以选择关闭在父进程终止时注销，这样当您关闭浏览器时会话将继续。对于这个做法，您要使用系统托盘中的通知图标注销。此图标将一直显示，直到用户点击该图标注销。如果会话在用户注销之前到期，该图标仍继续显示，直到下一次尝试连接。您可能需要等待系统托盘中更新会话状态。

注　此图标是 SSL VPN 注销的备选方法。它不指示 VPN 会话状态。

详细步骤

步骤 1　选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**。

步骤 2　在系统托盘单选按钮上启用 **Click on smart-tunnel logoff** 图标。

步骤 3　在窗口的 Smart Tunnel Networks 部分，选中 **Add** 并输入应该包含此图标的网络的 IP 地址和主机名。

注　如果右键单击此图标，系统将显示单菜单项，提示用户注销 SSL VPN。

使用代理旁路

当应用和网络资源利用此功能提供的特殊内容重写效果更好时，您可以配置 ASA 使用代理旁路。代理旁路是对原始内容更改最少的一种内容重写备选方法。通常适用于自定义网络应用。

您可以配置多个代理旁路条目。您配置条目的顺序并不重要。接口和路径掩码或接口和端口将唯一标识代理旁路规则。

如果使用端口而不是路径掩码配置代理旁路，根据您的网络配置，您可能需要更改您的防火墙配置以允许这些端口访问 ASA。使用路径掩码可避免此限制。但是，请注意，路径掩码可能会改变，因此您可能需要使用多个 pathmask 语句来穷尽各种可能性。

路径是 URL 中 .com 或 .org 或其他类型域名之后的任何内容。例如，在 URL www.example.com/hrbenefits 中， *hrbenefits* 就是路径。同样，对于 URL www.example.com/hrinsurance， *hrinsurance* 就是路径。要为所有 hr 站点使用代理旁路，您可以通过使用 * 通配符避免多次使用此命令，如下所示：/hr*。

对于何时 ASA 执行较少的内容重写或根本不执行内容重写，您可以设置规则：

步骤 1　导航至 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Proxy Bypass**。

步骤 2　为代理旁路选择 Interface 名称。

步骤 3　为代理旁路指定端口或 URI：

- Port -（单选按钮）点击即可为代理旁路使用端口。有效端口号是 20000 至 21000。
- Port （字段） - 输入 ASA 的高号端口，以备用于代理旁路。
- Path Mask -（单选按钮）点击即可为代理旁路使用 URL。
- Path Mask -（字段）输入代理旁路的 URL。可以包含正则表达式。

步骤 4　定义代理旁路的目标 URL：

- URL -（下拉列表）点击将 http 或 https 作为协议。
- URL -（文本字段）输入要应用代理旁路的 URL。

步骤 5　指定要重写的内容。可以选择无或 XML、链接和 cookie 的组合。

- XML - 选中以重写 XML 内容。
- Hostname - 选中以重写链接。

配置门户访问规则

此增强功能让客户可以配置全局无客户端 SSL VPN 访问策略以根据 HTTP 报头中的数据允许或拒绝无客户端 SSL VPN 会话。如果 ASA 拒绝无客户端 SSL VPN 会话，它将立即向终端返回错误代码。

ASA 在终端向 ASA 进行身份验证之前，评估此访问策略。因此，一旦访问被拒绝，终端的其他连接尝试消耗的 ASA 处理资源会更少。

先决条件

登录 ASA 并进入全局配置模式。在全局配置模式下， ASA 显示以下提示符：

```
hostname(config)#
```

详细步骤

步骤 1　启动 ASDM，然后选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Portal Access Rule**。

系统将打开 Portal Access Rule 窗口。

步骤 2　点击 **Add**，创建门户访问规则或选择现有的规则，然后点击 **Edit**。

系统显示 Add （或 Edit） Portal Access Rule 对话框。

步骤 3　在 Rule Priority 字段输入 1 至 65535 的规则编号。

规则按照 1 至 65535 的优先级顺序处理。

步骤 4　在 User Agent 字段输入要在 HTTP 报头中查找的用户代理的名称。

- 在字符串前后加上通配符 (*)，从而生成字符串；例如 *Thunderbird*。建议在您的搜索字符串中使用通配符。不使用通配符，规则可能不匹配任何字符串或者匹配的字符串数量远远低于您的预期。
- 如果您的字符串包含空格， ASDM 在保存规则时将自动在字符串前后加上引号。例如，如果您输入 `my agent`，ASDM 会将此字符串保存为“`my agent`”。然后，ASA 将搜索 `my agent` 的匹配项。

  除非您要求 ASA 匹配您向字符串添加的引号，否则请勿给字符串添加引号。例如，如果您输入“`my agent`”， ASDM 会将此字符串保存为 “`\ “my agent\”`” 并尝试找到 “`my agent`” 的匹配项，而不会查找 `my agent`。
- 要将通配符用于包含空格的字符串，请在整个字符串前后加上通配符，例如 `*my agent*`，然后 ASDM 在保存规则时将自动在该字符串前后加上引号。

步骤 5　在 Action 字段，选择 **Deny** 或 **Permit**。

ASA 将根据此设置拒绝或允许无客户端 SSL VPN 连接。

步骤 6　在 Returned HTTP Code 字段输入一个 HTTP 消息代码。

此字段预先填充了第 403 号 HTTP 消息，这是门户访问规则的默认值。允许的消息代码范围为 200 至 599。

步骤 7　点击 **OK**。

步骤 8　点击 **Apply**。

第 14 章 无客户端 SSL VPN 远程用户

本章总结了用户远程系统的配置要求和任务。本章还将帮助用户开始使用无客户端 SSL VPN。其中包括以下各节：

- 用户名和密码
- 传达安全提示
- 配置远程系统使用无客户端 SSL VPN 功能
- 捕获无客户端 SSL VPN 数据

注 确保已经为无客户端 SSL VPN 配置了 ASA。

用户名和密码

根据您的网络，在远程会话期间，可能需要登录以下任一项或所有项：计算机、互联网服务提供程序、无客户端 SSL VPN、邮件或文件服务器或企业应用。用户可能必须在许多不同情景下进行身份验证，这要求提供不同的信息，例如唯一用户名、密码或 PIN。确保用户具备所需的访问权限。

表 14-1 列出了无客户端 SSL VPN 用户可能需要知道的用户名和密码的类型。

表 14-1 要向无客户端 SSL VPN 用户提供的用户名和密码

登录用户名/密码类型	用途	输入时间
计算机	访问计算机	启动计算机
互联网服务提供商	访问互联网	连接互联网服务提供商
无客户端 SSL VPN	访问远程网络	启动无客户端 SSL VPN 会话
文件服务器	访问远程文件服务器	使用无客户端 SSL VPN 文件浏览功能访问远程文件服务器
企业应用登录	访问受防火墙保护的内部服务器	使用无客户端 SSL VPN 网络浏览功能访问受保护的内部网站
邮件服务器	通过无客户端 SSL VPN 访问远程邮件服务器	发送或接收邮件信息

传达安全提示

传达以下安全提示：

- 始终从无客户端 SSL VPN 会话注销，点击无客户端 SSL VPN 工具栏上的登录图标或关闭浏览器。
- 使用无客户端 SSL VPN 并不能保证与每个站点的通信都是安全的。无客户端 SSL VPN 将确保远程计算机或工作站与公司网络上的 ASA 之间数据传输的安全性。然后，如果用户访问非 HTTPS 网络资源（位于互联网或内部网络上），从公司 ASA 到目标网络服务器之间的通信就不安全。

配置远程系统使用无客户端 SSL VPN 功能

表 14-2 包括设置远程系统使用无客户端 SSL VPN 所涉及的任务、任务的要求/先决条件和推荐用法：

您可能以不同的方式配置了用户帐户，因此每个无客户端 SSL VPN 用户可以使用的功能可能有所不同。此外，表 14-2 还是按照用户活动组织信息的。

表 14-2　　无客户端 SSL VPN 远程系统配置和最终用户要求

任务	远程系统或最终用户要求	规范或使用建议
启动无客户端 SSL VPN	连接到互联网	支持各种互联网连接，包括： • 家庭数字用户线、电缆或拨号 • 公共终端机 • 酒店联结线路 • 机场无线节点 • 网吧
	支持无客户端 SSL VPN 的浏览器	我们推荐适用于无客户端 SSL VPN 的以下浏览器。其他浏览器可能不完全支持无客户端 SSL VPN 功能。 在 Microsoft Windows 上： • Internet Explorer 8 • Firefox 8 在 Linux 上： • Firefox 8 在 Mac OS X 上： • Safari 5 • Firefox 8
	在浏览器上启用 Cookie	要通过端口转发访问应用，必须在浏览器上启用 Cookie。
	适用于无客户端 SSL VPN 的 URL	以下形式的一个 HTTPS 地址： https://*地址* 其中*地址*是启用无客户端 SSL VPN 的 ASA （或负载平衡集群）的接口的 IP 地址或 DNS 主机名。例如：https://10.89.192.163 或 https://cisco.example.com。
	无客户端 SSL VPN 用户名和密码	
	[可选] 本地打印机	无客户端 SSL VPN 不支持从网络浏览器打印到网络打印机。不支持打印到本地打印机。

表 14-2　无客户端 SSL VPN 远程系统配置和最终用户要求 （续）

任务	远程系统或最终用户要求	规范或使用建议
在无客户端 SSL VPN 连接中使用浮动工具栏		浮动工具栏可简化无客户端 SSL VPN 的使用。此工具栏允许您输入 URL、浏览文件位置以及选择预配置的网络连接，而不会干扰主浏览器窗口。 如果将浏览器配置为阻止弹出窗口，则无法显示浮动工具栏。 浮动工具栏显示当前无客户端 SSL VPN 会话。如果点击 **Close** 按钮，ASA 会提示您关闭无客户端 SSL VPN 会话。 **提示**　要将文本粘贴到文本字段，请使用 **Ctrl-V**。（无客户端 SSL VPN 工具栏上不支持右键单击。）
网络浏览	受保护网站的用户名和密码	使用无客户端 SSL VPN 并不能保证与每个站点的通信都是安全的。请参阅 “传达安全提示”。
		使用无客户端 SSL VPN 进行网络浏览时，用户可能会体验到不同于以往的外观和感受。例如： • 无客户端 SSL VPN 标题栏显示在每个网页上方。 • 您可以通过以下方式访问网站： – 在无客户端 SSL VPN 主页 Enter Web Address 字段输入 URL。 – 点击无客户端 SSL VPN 主页上预配置的网站链接。 – 单击通过前两个方法之一访问的网页的链接。 此外，根据您配置特定帐户的方式，可能存在以下情况： • 某些网站会被拦截。 • 只有在无客户端 SSL VPN 主页上显示为链接的网站才可用。
网络扫描和文件管理	为共享远程访问配置的文件权限	仅共享文件夹和文件可通过无客户端 SSL VPN 进行访问。
	受保护的文件服务器的服务器名称和密码	—
	文件夹和文件所在的域、工作组和服务器名称	用户可能并不熟悉如何在您的组织网络中查找他们的文件。
	—	在复制过程中，请勿中断 **Copy File to Server** 命令或导航至其他屏幕。中断操作可能会导致在服务器上保存的文件不完整。

表 14-2　　无客户端 SSL VPN 远程系统配置和最终用户要求 （续）

任务	远程系统或最终用户要求	规范或使用建议
使用应用 （称为端口转发或应用访问）	**注**　在 Mac OS X 上，仅 Safari 浏览器支持此功能。	
	注　由于此功能需要安装 Oracle Java Runtime Environment (JRE) 和配置本地客户端，并且因为这样做需要具备本地系统的管理员权限，因此用户在通过公共远程系统连接时可能无法使用应用。	
	注意事项　当用户结束使用应用时，始终应该通过点击 **Close** 图标关闭 Application Access 窗口。不正确关闭此窗口可能会导致无法访问 Application Access 或应用本身。	
	安装的客户端应用	—
	在浏览器上启用 Cookie	—
	管理员权限	如果您使用 DNS 名称来指定服务器，则必须具备计算机上的管理员访问权限，因为修改主机要求具有此权限。
	已安装 Oracle Java Runtime Environment (JRE) 1.4.x 和 1.5.x 版本 必须在浏览器上启用 JavaScript。默认情况下， JavaScript 已启用。	如果未安装 JRE，系统将显示弹出窗口，指导用户浏览至提供此 JRE 的站点。 极少数情况下，端口转发小程序将出现故障，显示 Java 异常错误。如果出现这种情况，请执行以下操作： 1. 清除浏览器缓存并关闭浏览器。 2. 确认计算机任务栏上没有任何 Java 图标。结束 Java 的所有实例。 3. 建立一个无客户端 SSL VPN 会话并启动端口转发 Java 小程序。
	必要时，要配置客户端应用。 **注**　Microsoft Outlook 客户端不需要执行此配置步骤。 所有非 Windows 客户端应用都要求此配置。 要查看 Windows 是否要求执行此配置，请检查 Remote Server 字段的值。 • 如果 Remote Server 字段包含服务器主机名，则不需要配置客户端应用。 • 如果 Remote Server 字段包含 IP 地址，则必须配置客户端应用。	要配置客户端应用，请使用服务器的本地映射 IP 地址和端口号。要查找此信息，请执行以下操作： 1. 在远程系统上启动无客户端 SSL VPN 并点击无客户端 SSL VPN 主页上的 Application Access 链接。系统将显示 Application Access 窗口。 2. 在 Name 列，找到要使用的服务器名称，然后确定其相应的客户端 IP 地址和端口号（在 Local 列）。 3. 使用该 IP 地址和端口号来配置客户端应用。配置步骤因各客户端应用而异。
	注　在通过无客户端 SSL VPN 运行的应用中点击 URL （例如邮件信息中的一个 URL）不会通过无客户端 SSL VPN 打开站点。要通过无客户端 SSL VPN 打开站点，请剪切此 URL 并将其粘贴到 Enter (URL) Address 字段。	

表 14-2　无客户端 SSL VPN 远程系统配置和最终用户要求 （续）

任务	远程系统或最终用户要求	规范或使用建议
使用邮件 （通过 Application Access）	满足 Application Access 的要求（请参阅“使用应用”）	要使用邮件，请从无客户端 SSL VPN 主页启动 Application Access。这样即可使用邮件客户端。
	注　如果在使用 IMAP 客户端时失去与邮件服务器之间的连接或者无法建立新的连接，请关闭 IMAP 应用并重新启动无客户端 SSL VPN。	
	其他邮件客户端	我们测试了 Microsoft Outlook Express 5.5 和 6.0 版本。 无客户端 SSL VPN 应该支持通过端口转发的其他 SMTPS、 POP3S 或 IMAP4S 邮件程序，例如 Lotus Notes 和 Eudora，但我们未进行验证。
通过网络访问使用邮件	已安装基于网络的邮件产品	支持的产品包括： • Outlook Web Access 为了获得最佳效果，请在 Internet Explorer 8.x 或更高版本或 Firefox 8.x 上使用 OWA。 • Lotus Notes 其他基于网络的邮件产品应该也可以使用，但我们未进行验证。
通过电子邮件代理使用邮件	已安装支持 SSL 的邮件应用 请勿将 ASA SSL 版本设置为仅 TLSv1。Outlook 和 Outlook Express 不支持 TLS。	支持的邮件应用： • Microsoft Outlook • Microsoft Outlook Express 5.5 和 6.0 版本 其他支持 SSL 的邮件客户端应该也可以使用，但我们未进行验证。
	已配置邮件应用	

捕获无客户端 SSL VPN 数据

CLI capture 命令允许您记录通过无客户端 SSL VPN 连接无法正确显示的网站的信息。此数据可帮助您的思科客户支持工程师对问题进行故障排除。以下节介绍了如何使用 capture 命令：

- 创建捕获文件
- 使用浏览器显示捕获数据

注　启用无客户端 SSL VPN 捕获会影响 ASA 的性能。在生成故障排除所需的捕获文件之后，请确保关闭捕获。

创建捕获文件

操作步骤

步骤 1　启动无客户端 SSL VPN 捕获实用程序，捕获数据包

capture *capture-name* **type webvpn user** *csslvpn-username*

示例：

```
hostname# capture hr type webvpn user user2
```

- *capture-name* 是您分配给捕获的名称，也是捕获文件名称的前缀。
- *csslvpn-username* 是要与捕获匹配的用户名。

步骤 2　使用该命令的 **no** 版本停止捕获：

no capture *capture-name*

示例：

```
hostname# no capture hr
```

捕获实用程序将创建一个 *capture-name*.zip 文件，这个文件将用密码 **koleso** 加密

步骤 3　将该 .zip 文件发送给思科或将其添加在思科技术支持中心服务请求中。

步骤 4　要查看该 .zip 文件的内容，请使用密码 **koleso** 解压该文件。

使用浏览器显示捕获数据

操作步骤

步骤 1　启动无客户端 SSL VPN 捕获实用程序：

capture *capture-name* **type webvpn user** *csslvpn-username*

示例：

```
hostname# capture hr type webvpn user user2
```

- *capture-name* 是您分配给捕获的名称，也是捕获文件名称的前缀。
- *csslvpn-username* 是要与捕获匹配的用户名。

步骤 2　打开浏览器并在地址栏输入：

https://*ASA的 IP 地址或主机名*/**webvpn_capture.html**

被捕获的内容以探查器的格式显示。

步骤 3　使用该命令的 **no** 版本停止捕获：

no capture *capture-name*

示例：

```
hostname# no capture hr
```

第 15 章 无客户端 SSL VPN 用户

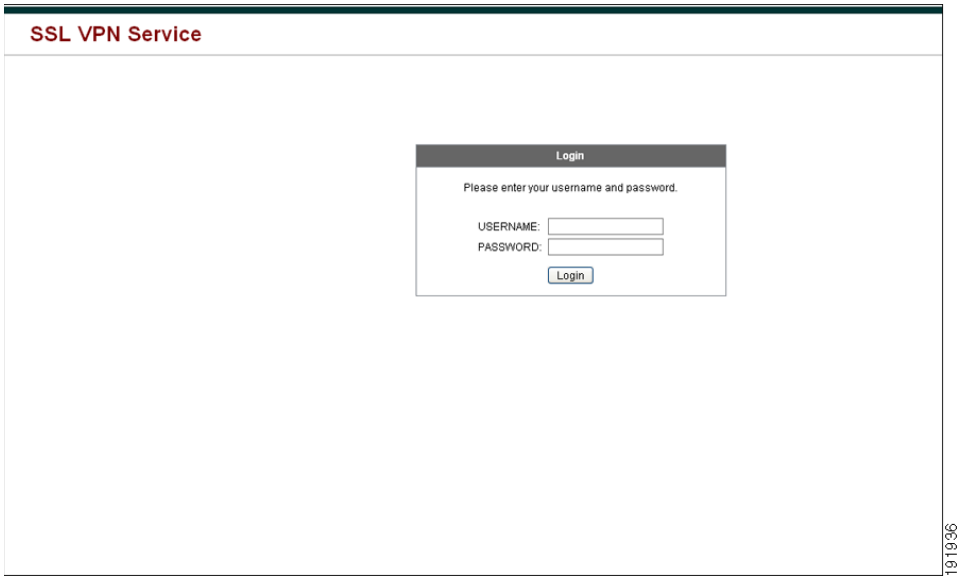
概述

本节向用户提供有关无客户端 SSL VPN 的使用入门的信息。包括下列主题：

定义最终用户界面

无客户端 SSL VPN 最终用户界面包括一系列 HTML 面板。用户按照 https://地址的形式输入 ASA *接口的 IP 地址即可登录无客户端 SSL VPN*。显示的第一个面板是登录屏幕 （图 15-1）。

图 15-1　　无客户端 SSL VPN 登录屏幕



查看无客户端 SSL VPN 主页

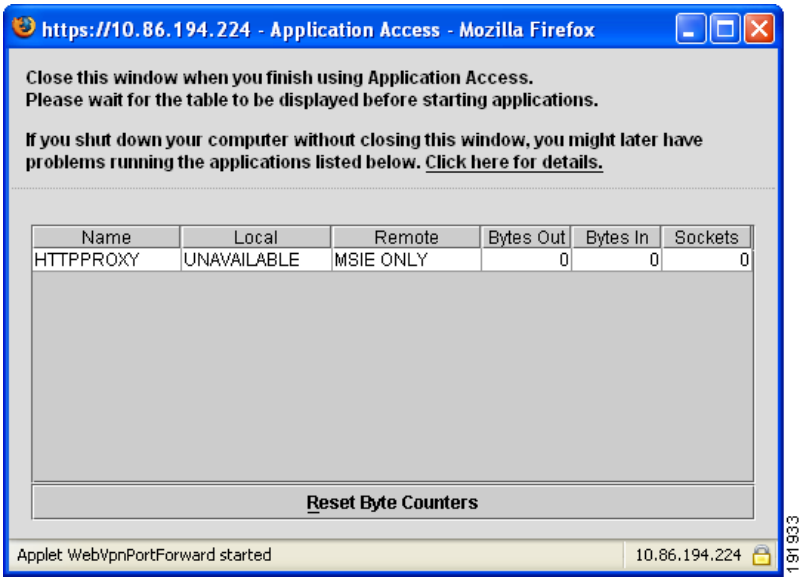
用户登录后，门户页面将会打开。

主页显示已配置的所有无客户端 SSL VPN 功能，其外观反映所选的徽标、文本和颜色。除了不能标识特定文件共享，此示例主页包括所有可用的无客户端 SSL VPN 功能。用户可以通过此主页浏览网络，输入 URL，访问特定网站，以及使用应用访问 （端口转发和智能隧道）来访问 TCP 应用。

查看无客户端 SSL VPN 应用访问面板

要启动端口转发或智能隧道，用户可点击 Application Access 框中的 **Go** 按钮。 Application Access 窗口将会打开 （图 15-2）。

图 15-2　　无客户端 SSL VPN Application Access 窗口



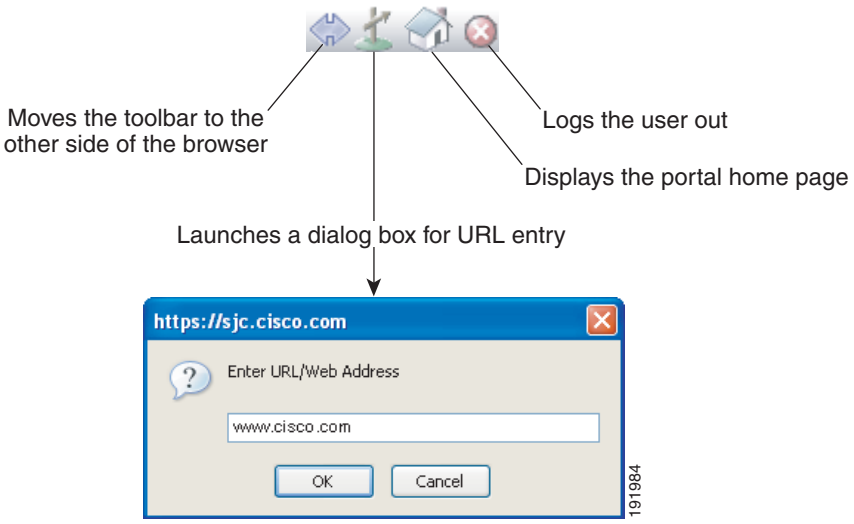
此窗口显示为此无客户端 SSL VPN 连接配置的 TCP 应用。要在此面板打开的情况下使用某应用，用户可以按照正常方式启动该应用。

注　状态故障转移将不保留使用 Application Access 建立的会话。出现故障转移后，用户必须重新连接。

查看浮动工具栏

图 15-3 中显示的浮动工具栏显示当前无客户端 SSL VPN 会话。

图 15-3　　无客户端 SSL VPN 浮动工具栏



请注意浮动工具栏的以下特征：

- 此工具栏允许您输入 URL、浏览文件位置以及选择预配置的网络连接，而不会干扰主浏览器窗口。
- 如果将浏览器配置为阻止弹出窗口，则无法显示浮动工具栏。
- 如果关闭此工具栏， ASA 会提示您结束无客户端 SSL VPN 会话。

有关使用无客户端 SSL VPN 的详细信息，请参阅第 15-10 页上的表 15-1。

管理密码

如有需要，可以将 ASA 配置为会在最终用户的密码即将到期时向他们发出警告。

ASA 支持 RADIUS 和 LDAP 协议的密码管理。对于 LDAP，它仅支持 “password-expire-in-days” 选项。

可以为 IPsec 远程访问和 SSL VPN 隧道组配置密码管理。配置密码管理时，ASA 会在远程用户登录时通知其当前密码即将到期或已到期。然后， ASA 允许用户更改密码。如果当前密码未到期，用户仍可使用该密码登录。

此命令对于支持此类通知的 AAA 服务器有效。

使用 LDAP 或支持 MS-CHAPv2 的任何 RADIUS 配置进行身份验证时，ASA 版本 7.1 及更高版本通常支持以下连接类型的密码管理：

- AnyConnect VPN 客户端
- IPsec VPN 客户端
- 无客户端 SSL VPN

RADIUS 服务器（例如，思科 ACS）可能会将身份验证请求以代理方式发送到另一个身份验证服务器。但是， ASA 仅与 RADIUS 服务器进行通信。

先决条件

- 本机 LDAP 需要 SSL 连接。在尝试执行 LDAP 密码管理之前，必须先启用基于 SSL 的 LDAP。默认情况下， LDAP 使用端口 636。

  如果将 LDAP 目录服务器用于身份验证， Sun Java 系统目录服务器 （原称为 SunONE 目录服务器）和 Microsoft Active Directory 支持密码管理。

  Sun - 在 ASA 上配置的用于访问 Sun 目录服务器的 DN 必须能够访问该服务器上的默认密码策略。我们建议将目录管理员或具有目录管理员权限的用户用作 DN。或者，可以在默认密码策略中创建 ACI。
  Microsoft - 要启用 Microsoft Active Directory 的密码管理，必须配置基于 SSL 的 LDAP。限制
- 支持 MSCHAP 的某些 RADIUS 服务器目前不支持 MSCHAPv2。此命令需要 MSCHAPv2，因此，请与供应商联系。
- Kerberos/Active Directory （Windows 密码）或 NT 4.0 域的任何连接类型都*不*支持密码管理。
- 对于 LDAP，市场上不同的 LDAP 服务器有专有的密码更改方法。目前， ASA 仅对 Microsoft Active Directory 和 Sun LDAP 服务器实施专有密码管理逻辑。
- 如果尚未配置 RADIUS 或 LDAP 身份验证， ASA 将忽略此命令。

详细步骤

步骤 1　导航至 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles > Add or Edit > Advanced > General > Password Management**。

步骤 2　点击 Enable Password Management 选项。

将思科身份验证方案添加到 SiteMinder

除了使用 SiteMinder 配置 ASA 来实现 SSO 之外，还必须使用思科身份验证方案 （一个可从思科网站下载的 Java 插件）配置 CA SiteMinder 策略服务器。

先决条件

配置 SiteMinder 策略服务器要求具备使用 SiteMinder 的经验。

详细步骤

本节介绍一般任务，而非完整的操作步骤。

步骤 1　如果使用 SiteMinder Administration 实用程序创建自定义身份验证方案，请务必使用以下特定参数：

- 在 Library 字段中，输入 **smjavaapi**。
- 在 Secret 字段中，输入在 ASA 上配置的那个密钥。

  通过在命令行界面上使用 **policy-server-secret** 命令可以在 ASA 上配置密钥。
- 在 Parameter 字段中，输入 **CiscoAuthApi**。

步骤 2　使用 Cisco.com 登录名，从 http://www.cisco.com/cisco/software/navigator.html 下载文件 **cisco_vpn_auth.jar**，并将其复制到 SiteMinder 服务器的默认库目录。思科 ASA CD 中也提供了此 .jar 文件。

配置 SAML POST SSO 服务器

使用服务器软件供应商提供的 SAML 服务器文档在信赖方模式下配置 SAML 服务器。

详细步骤

步骤 1　配置 SAML 服务器参数来代表断言方 (ASA)：

- 接收使用者 URL （与 ASA 上配置的断言使用者 URL 相同）
- 颁发者 ID （字符串，通常是设备的主机名）
- 配置文件类型 - 浏览器 Post 配置文件

步骤 2　配置证书。

步骤 3　指明必须对断言方的断言进行签名。

步骤 4　选择 SAML 服务器如何标识用户：

- 使用者名称类型为 DN
- 使用者名称格式为 uid=<user>

使用 HTTP 表单协议配置 SSO

本节介绍使用 HTTP 表单协议来配置 SSO。 HTTP 表单协议是一种 SSO 身份验证方法，也可用作 AAA 方法。它提供了一种安全的方法用于在无客户端 SSL VPN 用户与身份验证网络服务器之间交换身份验证信息。此协议可以与其他 AAA 服务器 （例如 RADIUS 或 LDAP 服务器）配合使用。

先决条件

要使用 HTTP 协议正确配置 SSO，必须全面了解 SSO 身份验证和 HTTP 协议交换的工作原理。

限制

HTTP 表单协议是一种常见协议，仅在用于进行身份验证的网络服务器应用符合以下条件时才适用：

- 必须为成功的请求设置身份验证 Cookie，但不为未授权的登录设置身份验证 Cookie。在这种情况下， ASA 无法区分成功和失败的身份验证。

详细步骤

ASA 同样充当身份验证网络服务器的无客户端 SSL VPN 用户的代理，但在这种情况下，它使用 HTTP 表单协议和 POST 请求方法。必须将 ASA 配置为可发送和接收表单数据。图 15-4 介绍以下 SSO 身份验证步骤：

步骤 1　无客户端 SSL VPN 用户首先输入用户名和密码，以登录到 ASA 上的无客户端 SSL VPN 服务器。

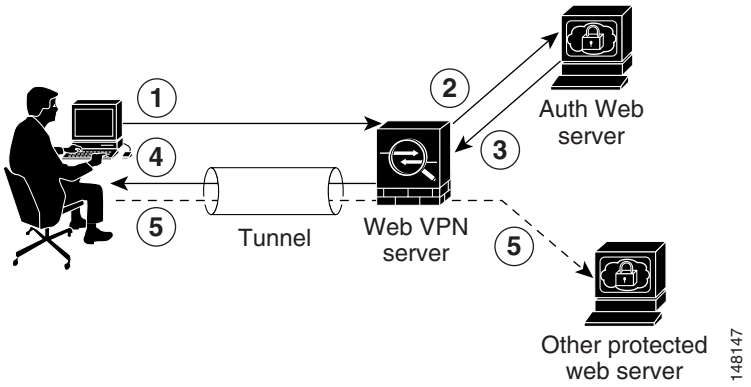
步骤 2　无客户端 SSL VPN 服务器充当用户的代理，并使用 POST 身份验证请求将表单数据 （用户名和密码）转发到身份验证网络服务器。

步骤 3　如果身份验证网络服务器批准用户数据，它会将身份验证 Cookie 返回到无客户端 SSL VPN 服务器（该服务器会代表用户存储该 Cookie）。

步骤 4　无客户端 SSL VPN 服务器建立通向用户的隧道。

步骤 5　这样，用户无需重新输入用户名和密码即可访问受保护 SSO 环境中的其他网站。

图 15-4　　使用 HTTP 表单的 SSO 身份验证



虽然您通常会配置允许 ASA 包含 POST 数据（例如用户名和密码）的表单参数，但是，您最初可能不会注意到网络服务器需要的其他隐藏参数。某些身份验证应用会遇到一些既不向用户显示也不是由用户输入的隐藏数据。但是，可以通过以下方法发现身份验证网络服务器会遇到的隐藏参数：从浏览器向身份验证网络服务器发送直接身份验证请求，而不使用 ASA 作为中间代理。使用 HTTP 报头分析器分析网络服务器响应能够以类似于以下的格式显示隐藏参数：

```
<param name>=<URL encoded value>&<param name>=<URL encoded>
```

有些隐藏参数是必填的，有些是可选的。如果网络服务器需要隐藏参数的数据，它将拒绝忽略这些数据的任何身份验证 POST 请求。由于报头分析器不会指出隐藏参数是否为必填的，因此，我们建议将所有隐藏参数包括在内，直至确定哪些是必填的。

收集 HTTP 表单数据

本节介绍发现和收集必要的 HTTP 表单数据的步骤。如果不知道身份验证网络服务器需要哪些参数，可以通过分析身份验证交换来收集参数数据。

先决条件

这些步骤需要使用浏览器和 HTTP 报头分析器。

详细步骤

步骤 1　启动浏览器和 HTTP 报头分析器，并直接连接到网络服务器登录页面 （而不是通过 ASA 连接）。

步骤 2　在浏览器中加载网络服务器登录页面后，检查登录序列以确定是否已在交换过程中设置了 Cookie。如果网络服务器已使用登录页面加载了 Cookie，请将该登录页面 URL 配置为 *start-URL*。

步骤 3　输入用户名和密码以登录到网络服务器，然后按 **Enter**。此操作会生成使用身份验证 POST 请求（可使用 HTTP 报头分析器检查该请求）。

包含主机 HTTP 报头和正文的 POST 请求示例如下：

```
POST
/emco/myemco/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000430e1-7443-125c-ac05-83
846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2b
J0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2FHTT
P/1.1

Host: www.example.com

(BODY)
```

```
SMENC=ISO-8859-1&SMLOCALE=US-EN&USERID=Anyuser&USER_PASSWORD=XXXXXX&target=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0
```

步骤 4　检查 POST 请求并复制协议、主机和完整的 URL，以配置操作 URI 参数。

步骤 5　检查 POST 请求正文并复制以下内容：

a. 用户名参数。在上一个示例中，此参数是 *USERID*，而不是值 *anyuser*。

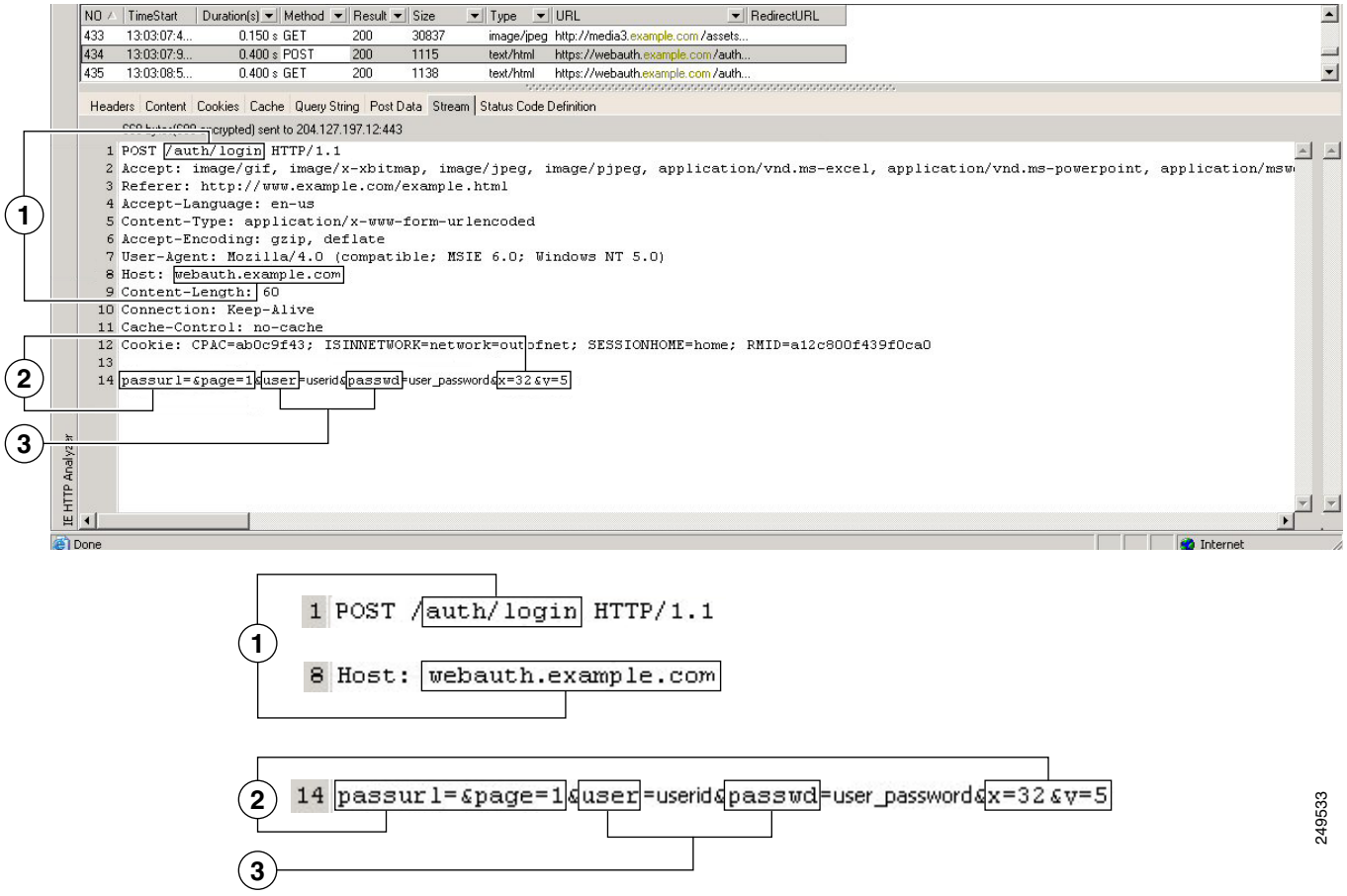
b. 密码参数。在上一个示例中，此参数是 *USER_PASSWORD*。

c. 隐藏参数。此参数是 POST 正文中除用户名和密码参数之外的一切内容。在上一个示例中，隐藏参数如下所示：

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0

图 15-5 突出显示了 HTTP 分析器的输出示例中的操作 URI 参数、隐藏参数、用户名参数和密码参数。这只是一个示例；不同网站的输出会有所不同。

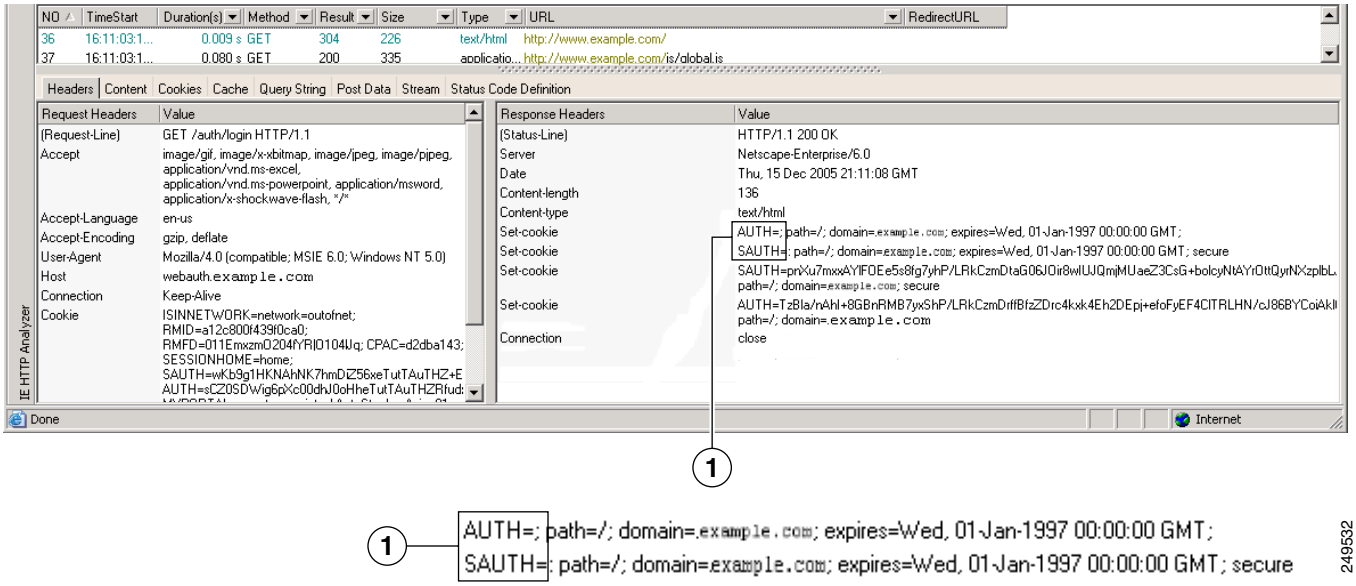
图 15-5　操作 URI 参数、隐藏参数、用户名参数和密码参数



步骤 6　如果成功登录到网络服务器，请使用 HTTP 报头分析器检查服务器响应，以查找浏览器中服务器设置的会话 Cookie 名称。这是 **auth-cookie-name** 参数。

在以下服务器响应报头中，会话 Cookie 名称是 SMSESSION。只需要名称，不需要值。图 15-6 显示了 HTTP 分析器输出中授权 Cookie 的示例。这只是一个示例；不同网站的输出会有所不同。

图 15-6　　HTTP 分析器输出示例中的授权 Cookie



1	授权 Cookie

步骤 7　在某些情况下，不管身份验证是否成功，服务器都可能会设置相同的 Cookie，且该 Cookie 不可用于 SSO。要确认 Cookie 是否不同，请使用无效的登录凭证重复第步骤 1 到第步骤 6 步，并将 “失败” Cookie 与 “成功” Cookie 作比较。到此，已具备使用 HTTP 表单协议将 ASA 配置为支持 SSO 所需的参数数据。

使用自动登录

可以使用 Auto Sign-on 窗口或选项卡为无客户端 SSL VPN 用户配置或编辑自动登录。自动登录 是一种简化的单点登录方法，可在内部网络上未部署 SSO 方法的情况下使用。如果为特定内部服务器配置了自动登录， ASA 会将无客户端 SSL VPN 用户输入的用于登录 ASA 的登录凭证 （用户名和密码）传递到这些特定内部服务器。可以将 ASA 配置为会响应面向特定系列服务器的具体身份验证方法。可以将 ASA 配置会对以下身份验证方法作出响应：Basic (HTTP)、NTLM、FTP/CIFS 或者所有这些方法。

如果未能在 ASA 上找到用户名和密码，将会替换空字符串，且行为将会恢复为如同没有自动登录可用时一样。

自动登录是一种可用于为特定内部服务器配置 SSO 的简单明了的方法。本节介绍使用自动登录设置 SSO 的步骤。本节的内容以如下假设为前提：用户已经使用 Computer Associates SiteMinder SSO 服务器部署了 SSO，或者用户拥有安全断言标记语言 (SAML) 浏览器 Post 配置文件 SSO。要将 ASA 配置为支持此解决方案，请参阅第 12-6 页上的SSO 服务器。

系统将显示以下字段：

- IP Address - 与下面的 Mask 字段配合使用，显示使用 Add/Edit Auto Sign-on 对话框配置的要进行身份验证的服务器的 IP 地址范围。可以使用服务器 URI 或服务器的 IP 地址和掩码来指定服务器。
- Mask - 与上面的 IP Address 字段配合使用，显示使用 Add/Edit Auto Sign-on 对话框配置的支持自动登录的服务器的 IP 地址范围。
- URI - 显示用于标识使用 Add/Edit Auto Sign-on 对话框配置的服务器的 URI 掩码。
- Authentication Type - 显示使用 Add/Edit Auto Sign-on 对话框配置的身份验证类型，包括 Basic (HTTP)、 NTLM、 FTP/CIFS 或者所有这些方法。

限制

- 请勿对不要求身份验证或使用不同于 ASA 的凭证的服务器启用自动登录。启用自动登录后，ASA 会传递用户输入的用于登录 ASA 的登录凭据，无论用户存储中有什么凭证。
- 如果为一系列服务器配置了一种方法（例如，HTTP 基本身份验证），当其中一台服务器尝试使用其他方法 （例如， NTLM）进行身份验证时， ASA 不会将用户登录凭证传递到该服务器。

详细步骤

步骤 1　点击以添加或编辑自动登录说明。自动登录说明定义使用自动登录功能和特定身份验证方法的一系列内部服务器。

步骤 2　点击以删除在 Auto Sign-on 表中选择的自动登录说明。

步骤 3　点击 **IP Block**，以指定使用 IP 地址和掩码的一系列内部服务器。

- IP Address - 输入要为其配置自动登录的一系列服务器当中第一台服务器的 IP 地址。
- Mask - 从子网掩码菜单中选择定义支持自动登录的服务器的服务器地址范围。

步骤 4　点击 URI 以指定支持通过 URI 进行自动登录的服务器，然后在此按钮旁边的字段中输入具体 URI。

步骤 5　确定分配给服务器的身份验证方法。对于指定的一系列服务器，可以将 ASA 配置为会响应 HTTP 基本身份验证请求、 NTLM 身份验证请求、 FTP 和 CIFS 身份验证请求或使用任何这些方法的请求。

- Basic - 如果服务器支持基本 (HTTP) 身份验证，请点击此按钮。
- NTLM - 如果服务器支持 NTLMv1 身份验证，请点击此按钮。
- FTP/CIFS - 如果服务器支持 FTP 和 CIFS 身份验证，请点击此按钮。
- Basic, NTLM, and FTP/CIFS - 如果服务器支持上述所有方法，请点击此按钮。

需要用户名和密码

在远程会话过程中，用户可能必须登录以下任意或所有设备或程序：具体取决于网络：计算机、互联网服务提供商、无客户端 SSL VPN、邮件或文件服务器、企业应用。用户可能必须在许多不同情景下进行身份验证，这要求提供不同的信息，例如唯一用户名、密码或 PIN。

表 15-1 列出了无客户端 SSL VPN 用户可能需要知道的用户名和密码的类型。

表 15-1　要向无客户端 SSL VPN 会话用户提供的用户名和密码

登录用户名/密码类型	用途	输入时间
计算机	访问计算机	启动计算机
互联网服务提供商	访问互联网	连接互联网服务提供商
无客户端 SSL VPN	访问远程网络	启动无客户端 SSL VPN
文件服务器	访问远程文件服务器	使用无客户端 SSL VPN 文件浏览功能访问远程文件服务器
企业应用登录	访问受防火墙保护的内部服务器	使用无客户端 SSL VPN 网络浏览功能访问受保护的内部网站
邮件服务器	通过无客户端 SSL VPN 访问远程邮件服务器	发送或接收邮件信息

传达安全提示

建议用户在关闭无客户端 SSL VPN 会话时始终点击工具栏上的注销图标。（关闭浏览器窗口不会关闭会话。）

无客户端 SSL VPN 将确保远程计算机或工作站与公司网络上的 ASA 之间数据传输的安全性。告知用户使用无客户端 SSL VPN 并不能保证与每个站点的通信都是安全的。如果用户在收到该提醒后访问非 HTTPS 网络资源（位于互联网或内部网络上），公司 ASA 与目标网络服务器之间的通信不是专用的，因为它未加密。

第 1 页上的“无客户端 SSL VPN 安全预防措施”中根据在该节中执行的步骤提供了有关与用户进行通信的其他提示。

配置远程系统以使用无客户端 SSL VPN 功能

本节介绍如何设置远程系统以使用无客户端 SSL VPN。

- 第 15-11 页上的启动无客户端 SSL VPN
- 第 15-11 页上的使用无客户端 SSL VPN 浮动工具栏
- 第 15-12 页上的浏览网络
- 第 15-12 页上的浏览网络（文件管理）
- 第 15-14 页上的使用端口转发
- 第 15-15 页上的通过端口转发使用邮件
- 第 15-16 页上的通过网络访问使用邮件
- 第 15-16 页上的通过邮件代理使用邮件
- 第 15-17 页上的使用智能隧道

可采用不同的方式配置各个用户帐户，以使每个用户可以使用不同的无客户端 SSL VPN 功能。

启动无客户端 SSL VPN

可以使用任何受支持的连接方法连接到互联网，这些方法包括：

- 家庭 DSL、电缆或拨号。
- 公共信息亭。
- 酒店热点。
- 机场无线节点。
- 网吧。

注　有关无客户端 SSL VPN 支持的网络浏览器的列表，请参阅《*支持的 VPN 平台（思科 ASA 系列）*》。

先决条件

- 要通过端口转发访问应用，必须在浏览器上启用 Cookie。
- 必须有无客户端 SSL VPN 的 URL。 URL 必须是采用以下格式的 https 地址：*//address*，其中，*address* 是启用了 SSL VPN 的 ASA（或负载平衡集群）的接口的 IP 地址或 DNS 主机名。例如，https://cisco.example.com。
- 必须有无客户端 SSL VPN 用户名和密码。

限制

- 无客户端 SSL VPN 支持本地打印，但不支持通过 VPN 连接到公司网络上的打印机进行打印。

使用无客户端 SSL VPN 浮动工具栏

浮动工具栏可简化无客户端 SSL VPN 的使用。此工具栏允许您输入 URL、浏览文件位置以及选择预配置的网络连接，而不会干扰主浏览器窗口。

浮动工具栏显示当前无客户端 SSL VPN 会话。如果点击 **Close** 按钮， ASA 会提示您关闭无客户端 SSL VPN 会话。

提示　要将文本粘贴到文本字段，请使用 **Ctrl-V**。（对于在无客户端 SSL VPN 会话期间显示的工具栏，右键单击操作不可用。）

限制

如果将浏览器配置为阻止弹出窗口，则无法显示浮动工具栏。

浏览网络

使用无客户端 SSL VPN 并不能保证与每个站点的通信都是安全的。请参阅传达安全提示。

使用无客户端 SSL VPN 进行网络浏览时，用户可能会体验到不同于以往的外观和感受。例如：

- 无客户端 SSL VPN 的标题栏显示在每个网页的上方。
- 您可以通过以下方式访问网站：
  - 在无客户端 SSL VPN 主页的 **Enter Web Address** 字段中输入 URL
  - 点击无客户端 SSL VPN 主页上的预配置网站链接
  - 点击通过上述两种方法之一访问的网页上的链接

此外，根据您配置特定帐户的方式，可能存在以下情况：

- 某些网站被阻止
- 只有在无客户端 SSL VPN 主页上显示为链接的网站可用

先决条件

需要有受保护网站的用户名和密码。

限制

此外，根据您配置特定帐户的方式，可能存在以下情况：

- 某些网站被阻止
- 只有在无客户端 SSL VPN 主页上显示为链接的网站可用

浏览网络 （文件管理）

用户可能并不熟悉如何在您的组织网络中查找他们的文件。

注　在复制过程中，请勿中断 **Copy File to Server** 命令或导航至其他屏幕。中断操作可能会导致在服务器上保存的文件不完整。

先决条件

- 必须配置共享远程访问的文件权限。
- 必须有受保护文件服务器的服务器名称和密码。
- 必须有文件夹和文件所在的域、工作组和服务器的名称。

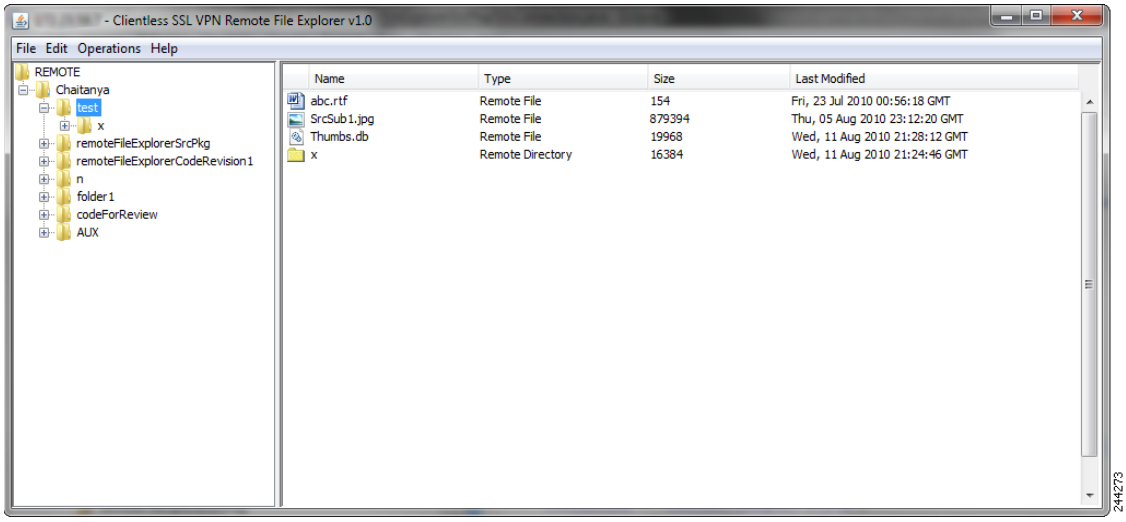
限制

仅共享文件夹和文件可通过无客户端 SSL VPN 进行访问。

使用 Remote File Explorer

有了 Remote File Explorer，用户可以从网络浏览器浏览公司网络。用户点击思科 SSL VPN 门户页面上的 Remote File System 图标时，用户系统上会启动一个小程序，在文件夹树视图中显示远程文件系统。

图 15-7　　无客户端 SSL VPN Remote File Explorer



此浏览器使用户可以：

- 浏览远程文件系统。
- 重命名文件。
- 移动或复制远程文件系统中以及远程文件系统与本地文件系统之间的文件。
- 执行文件批量上传和下载。

注　要使用此功能，用户计算机上需要安装 Oracle Java Runtime Environment (JRE) 1.4 或更高版本，还需要在网络浏览器中启用 Java。启动远程文件需要 JRE 1.6 或更高版本。

重命名文件或文件夹

要重命名文件或文件夹，请执行以下操作：

步骤 1　点击要重命名的文件或文件夹。

步骤 2　选择 **Edit > Rename**。

步骤 3　出现提示时，在对话框中输入新名称。

步骤 4　点击 **OK** 重命名文件或文件夹。或者，点击 **Cancel** 保留原来的名称。

移动或复制远程服务器上的文件或文件夹

要移动或复制远程服务器上的文件或文件夹，请执行以下操作：

步骤 1　导航至包含要移动或复制的文件或文件夹的源文件夹。

步骤 2　点击所需的文件或文件夹。

步骤 3　要复制文件，请选择 **Edit > Copy**。要移动文件，请选择 **Edit > Cut**。

步骤 4　导航至目标文件夹。

步骤 5　选择 **Edit > Paste**。

将文件从本地系统驱动器复制到远程文件夹

可以在本地文件系统与远程文件系统之间复制文件，方法是，在远程文件浏览器的右侧窗格与本地文件管理器应用之间拖放文件。

上传和下载文件

下载文件的具体操作如下：在浏览器中点击要下载的文件，选择 **Operations > Download**，然后在 **Save** 对话框中提供用于保存该文件的位置和名称。

上传文件的具体操作如下：在目标文件夹中点击要上传的文件，选择 **Operations > Upload**，然后在 **Open** 对话框中提供该文件的位置的名称。

此功能有以下限制：

- 用户不能查看他们无权访问的子文件夹。
- 不能移动或复制用户无权访问的文件，即使这些文件显示在浏览器中。
- 嵌套文件夹的最大深度为 32 级。
- 树视图不支持拖放复制。
- 在 Remote File Explorer 的多个实例之间移动文件时，所有实例必须浏览同一台服务器 （根目录共享）。
- Remote File Explorer 在一个文件夹中最多可显示 1500 个文件和文件夹。如果文件夹数量超过这个限制，文件夹将无法显示。

使用端口转发

注　当用户结束使用应用时，始终应该通过点击 **Close** 图标关闭 Application Access 窗口。未能正确退出窗口可能会导致应用访问或应用本身关闭。有关详细信息，请参阅第 18-1 页上的使用 Application Access 时从 hosts 文件错误中恢复。

先决条件

- 在 Mac OS X 上，仅 Safari 浏览器支持此功能。
- 必须已安装客户端应用。
- 必须已在浏览器上启用了 Cookie。

- 如果使用 DNS 名称指定服务器，必须具有管理员权限，因为修改主机文件需要这一权限。
- 必须已安装 Oracle Java Runtime Environment (JRE) 1.4.x 和 1.5.x。

  如果未安装 JRE，系统将显示弹出窗口，指导用户浏览至提供此 JRE 的站点。极少数情况下，端口转发小程序将出现故障，显示 Java 异常错误。如果出现这种情况，请执行以下操作：

  a. 清除浏览器缓存并关闭浏览器。
  b. 确认计算机任务栏上没有任何 Java 图标。
  c. 结束 Java 的所有实例。
  d. 建立一个无客户端 SSL VPN 会话并启动端口转发 Java 小程序。
- 必须在浏览器上启用 JavaScript。默认情况下， JavaScript 已启用。
- 如有需要，必须配置客户端应用。

注 Microsoft Outlook 客户端不需要执行此配置步骤。所有非 Windows 客户端应用都要求此配置。要确定 Windows 应用是否需要进行配置，请检查 Remote Server 字段的值。如果 Remote Server 字段包含服务器主机名，不需要配置客户端应用。如果 Remote Server 字段包含 IP 地址，则必须配置客户端应用。

限制

由于此功能要求安装 Oracle Java Runtime Environment (JRE) 并配置配置本地客户端，而且，这样做需要具有本地系统的管理员权限或者对 C:\windows\System32\drivers\etc 的完全控制权，因此，用户从公共远程系统连接时将无法使用应用。

详细步骤

要配置客户端应用，请使用服务器的本地映射 IP 地址和端口号。要查找此信息，请执行以下操作：

1. 启动无客户端 SSL VPN 会话，并点击主页上的 **Application Access** 链接。系统将显示 Application Access 窗口。
2. 在 Name 列，找到要使用的服务器名称，然后确定其相应的客户端 IP 地址和端口号（在 Local 列）。
3. 使用该 IP 地址和端口号来配置客户端应用。配置步骤因各客户端应用而异。

注 点击通过无客户端 SSL VPN 会话运行的应用中的 URL （例如，邮件中的 URL）不会打开会话站点。要打开会话站点，请将 URL 粘贴到 Enter Clientless SSL VPN (URL) Address 字段中。

通过端口转发使用邮件

要使用邮件，请从无客户端 SSL VPN 主页启动应用访问。这样即可使用邮件客户端。

注 如果在使用 IMAP 客户端时失去与邮件服务器之间的连接或者无法建立新的连接，请关闭 IMAP 应用并重新启动无客户端 SSL VPN。

先决条件

必须满足应用访问及其他邮件客户端的要求。

限制

我们测试了 Microsoft Outlook Express 5.5 和 6.0 版本。

无客户端 SSL VPN 应能够通过端口转发支持其他 SMTPS、POP3S 或 IMAP4S 邮件程序（例如 Lotus Notes 和 Eudora），但是我们尚未验证这一点。

通过网络访问使用邮件

支持以下邮件应用：

- 在 Exchange Server 2010 上运行的 Microsoft Outlook Web App。

  OWA 要求使用 Internet Explorer 7 或更高版本，或者 Firefox 3.01 或更高版本。
- Exchange Server 2007、 2003 和 2000 上运行的 Microsoft Outlook Web Access。

  为了获得最佳效果，请在 Internet Explorer 8.x 或更高版本或者 Firefox 8.x 上使用 OWA。
- Lotus iNotes

先决条件

必须已安装基于网络的邮件产品。

限制

应该也支持其他基于网络的邮件应用，但我们尚未验证这一点。

通过邮件代理使用邮件

支持以下旧版邮件应用：

- Microsoft Outlook 2000 和 2002
- Microsoft Outlook Express 5.5 和 6.0

有关邮件应用的说明和示例，请参阅第 12-19 页上的在无客户端 SSL VPN 上使用邮件。

先决条件

- 必须已安装支持 SSL 的邮件应用。
- 请勿将 ASA SSL 版本设置为仅 TLSv1。 Outlook 和 Outlook Express 不支持 TLS。
- 必须已正确配置邮件应用。

限制

应该也支持其他支持 SSL 的客户端，但我们尚未验证这一点。

使用智能隧道

使用智能隧道不需要具有管理权限。

注　与使用端口转发程序时不同，使用智能隧道时不会自动下载 Java。

先决条件

- 智能隧道要求 Windows 上必须安装 ActiveX 或 JRE（1.4x 和 1.5x），要求 Mac OS X 上必须安装 Java Web Start。
- 必须确保浏览器上已启用 Cookie。
- 必须确保浏览器上已启用 JavaScript。

限制

- Mac OS X 不支持前端代理。
- 仅支持第 13-1 页上的配置智能隧道访问中指定的操作系统和浏览器。
- 仅支持基于 TCP 套接字的应用。

将无客户端 SSL VPN 用于移动设备

将无客户端 SSL VPN 用于移动设备

您可以从 Pocket PC 或其他已获认证的移动设备访问无客户端 SSL VPN。 ASA 管理员和无客户端 SSL VPN 用户无需任何特殊操作即可将无客户端 SSL VPN 用于已获认证的移动设备。

思科已认证以下移动设备平台：

HP iPaq H4150

Pocket PC 2003

Windows CE 4.20.0，内部版本 14053

Pocket Internet Explorer (PIE)

ROM 版本 1.10.03ENG

ROM 日期：7/16/2004

移动设备版本的无客户端 SSL VPN 存在一些不同之处：

- 横幅网页代替了无客户端 SSL VPN 弹出窗口。
- 图标栏代替了标准无客户端 SSL VPN 浮动工具栏。此栏显示 Go、 Home 和 Logout 按钮。
- 无客户端 SSL VPN 门户主页上不包含 Show Toolbar 图标。
- 注销 SSL VPN 时，系统将显示警告消息，提供关于正确关闭 PIE 浏览器的说明。如果您不遵循这些说明并按照常规方式关闭浏览器窗口，PIE 将不断开无客户端 SSL VPN 或使用 HTTPS 的任何安全网站。

限制

- 无客户端 SSL VPN 支持 OWA 2000 和 OWA 2003 基本身份验证。如果在 OWA 服务器上未配置基本身份验证并且无客户端 SSL VPN 用户尝试访问该服务器，访问将被拒绝。
- 不支持的无客户端 SSL VPN 功能：
  - Application Access 和其他 Java 相关功能。
  - HTTP 代理。
  - Citrix Metaframe 功能 （如果 PDA 没有对应的 Citrix ICA 客户端软件）。

自定义无客户端 SSL VPN

自定义无客户端 SSL VPN 用户体验

您可以自定义无客户端 SSL VPN 用户体验，包括登录、门户和注销页面。您可采用以下两种方法。您可以自定义 Add/Edit Customization Object 窗口中的预定义页面组件。通过此窗口可添加或更改 ASA 上存储的用于自定义页面的 XML 文件（自定义对象）。或者，您也可以将此 XML 文件导出到本地计算机或服务器上，更改 XML 标签，然后将此文件重新导入到 ASA 中。两种方法都可以创建应用到连接配置文件或组策略中的自定义对象。

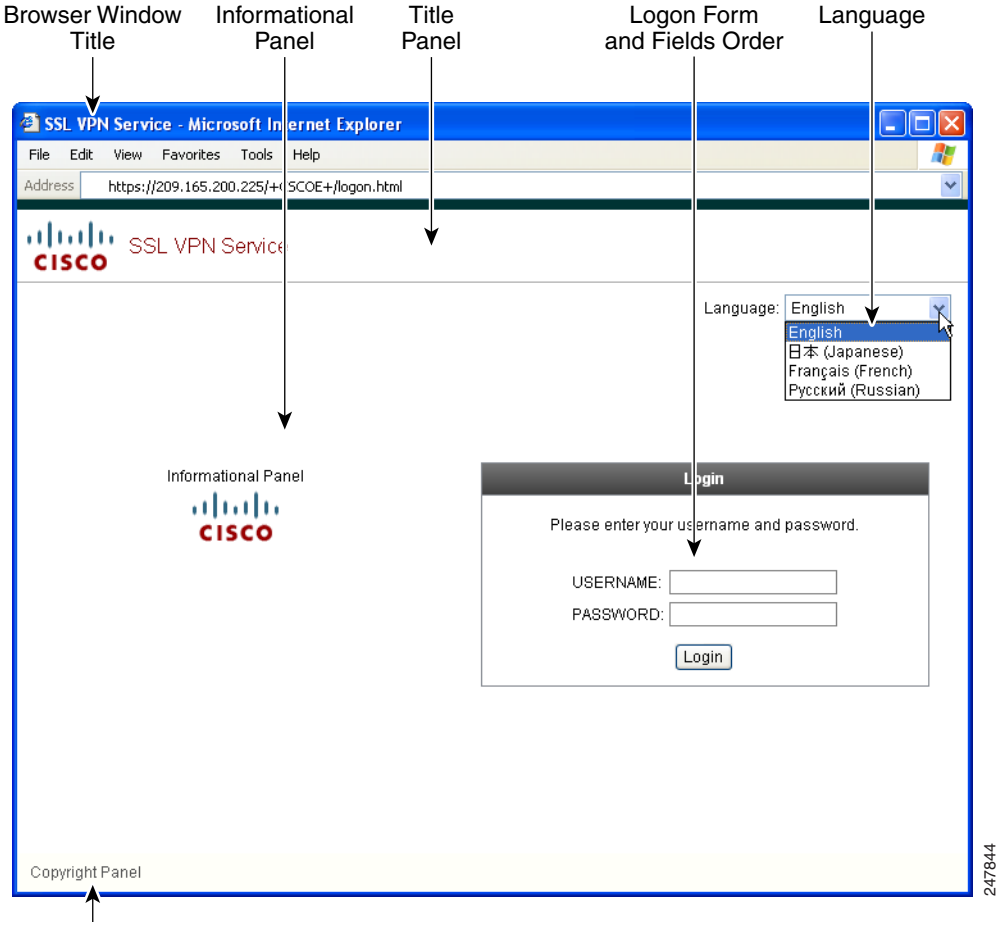
除了自定义登录页面的预定义组件，您也可以创建您自己的页面并将其导入到 ASA 中进行完全自定义。

您可以自定义登录页面的预定义组件，包括标题、语言选项和向用户显示的消息。或者，您也可以完全用您自己的自定义页面替换该页面 （完全自定义）。

使用自定义编辑器自定义登录页面

图 17-1 显示了您可以自定义的登录页面和预定义组件：

图 17-1　　无客户端登录页面组件



要自定义登录页面的所有组件，请执行以下步骤。您可以点击 Preview 按钮，预览您对每个组件的更改：

步骤 1　指定要自定义的预定义组件。转至 Logon Page 并选择 **Customize pre-defined logon page components**。为浏览器窗口指定标题。

步骤 2　显示并自定义标题面板。转至 Logon Page > Title Panel 并选中 **Display title panel**。输入作为标题显示的文本并指定徽标。指定任意字体样式。

步骤 3　指定显示的语言选项。转至 Logon Page > Language 并选中 **Enable Language Selector**。添加或删除向远程用户显示的任意语言。列表中的语言要求使用您在 Configuration > Remote Access VPN > Language Localization 中配置的转换表。

步骤 4　自定义登录表单。转至 Logon Page > Logon Form。在面板中自定义表单文本和字体样式。只有在连接配置文件中配置了二级身份验证服务器的情况下，系统才会向用户显示二级密码字段。

步骤 5　安排登录表单字段的位置。转至 Logon Page > Form Fields Order。使用上下箭头按钮更改字段的显示顺序。

步骤 6　添加向用户显示的消息。转至 Logon Page > Informational Panel 并选中 **Display informational panel**。在面板中添加要显示的文本，更改面板相对于登录表单的位置，并指定要在此面板中显示的徽标。

步骤 7　显示版权声明。转至 Logon Page > Copyright Panel 并选中 **Display copyright panel**。添加要用于版权声明显示的文本。

步骤 8　点击 **OK**，然后将更改应用到您编辑的自定义对象上。

后续操作

请参阅 “用您自己的完全自定义页面替换登录页面”。

用您自己的完全自定义页面替换登录页面

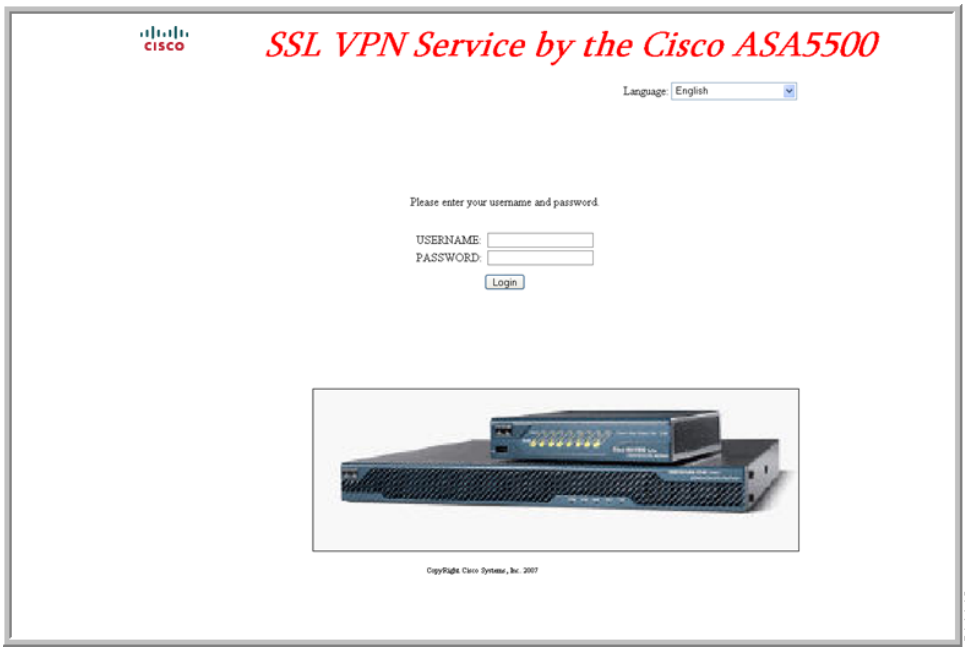
如果您希望使用自己的自定义登录屏幕，而不是更改我们所提供的登录页面的特定组件，您可以使用 “完全自定义”功能执行这种高级自定义。

利用 “完全自定义”功能，您可以为您自己的登录屏幕提供 HTML 并插入调用 ASA 上创建登录表单和语言选择器下拉列表的函数的思科 HTML 代码。

本文描述为了配置 ASA 使用您的代码您需要对您的 HTML 代码所做的修改和所需完成的任务。

图 17-2 显示了 “完全自定义”功能启用的一个简单的自定义登录屏幕示例。

图 17-2　　登录页面的完全自定义示例



创建自定义登录屏幕文件

以下 HTML 代码是一个示例，也是系统显示的代码：

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>New Page 3</title>
<base target="_self">
</head>

<p align="center">
```

```
<img border="0" src="/+CSCOU+/cisco_logo.jpg" width="188" height="48"><font face="Snap
ITC" size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7"> </font><i><b><font
color="#FF0000" size="7" face="Sylfaen"> SSL VPN Service by the Cisco
ASA5500</font></b></i></p>

    <body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

    <table>

    <tr><td colspan=3 height=20 align=right><div id="selector" style="width:
    300px"></div></td></tr>
    <tr><td></td><td></td><td></td></tr>
    <tr>
    <td height="379"></td>
    <td height="379"></td>
    <td align=middle valign=middle>
    <div id=lform >
    <p> </p>
    <p> </p>
    <p> </p>
    <p>Loading...</p>
    </div>
    </td>
    </tr>
    <tr>
    <td width="251"></td>
    <td width="1"></td>
    <td align=right valign=right width="800">
    <img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
    </td></tr>

    </table>
```

这种缩进的代码将在屏幕上注入登录表单和语言选择器。函数 **csco_ShowLoginForm('lform')** 注入登录表单。 **csco_ShowLanguageSelector('selector')** 注入语言选择器。

步骤 1　将您的文件命名为 **logon.inc**。当您导入文件时， ASA 将此文件名识别为登录屏幕。

步骤 2　修改该文件使用的映像的路径以包含 **/+CSCOU+/**。

在身份验证之前向远程用户显示的文件必须放在 ASA 缓存的特定区域，以路径 /+CSCOU+/ 表示。因此，该文件中每个映像的源都必须包含此路径。例如：

```
src="/+CSCOU+/asa5520.gif"
```

步骤 3　插入下面的特殊 HTML 代码。此代码包含之前描述的在屏幕上注入登录表单和语言选择器的思科函数。

```
<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
<p> </p>
```

```
<p> </p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>

</table>
```

导入文件和映像

步骤 1　转到 **Clientless SSL VPN Access > Portal > Web Contents**。

步骤 2　点击 **Import**。

a. 选择 **Source** 选项，然后输入网站内容文件的路径。

b. 在 **Destination** 区域，为 *Require Authentication to access its content* 选择 **No**。这可确保将这些文件存储于用户在身份验证之前可以访问的闪存区域。

步骤 3　点击 **Import Now**。

配置安全设备使用自定义登录屏幕

步骤 1　从 **Clientless SSL VPN Access > Portal > Customization** 的表格中选择一个自定义对象，然后点击 **Edit**。

步骤 2　在 Navigation 窗格中，选择 **Logon Page**。

步骤 3　选择 **Replace pre-defined logon page with a custom page**。

步骤 4　点击 **Manage**，导入您的登录页面文件。

步骤 5　在 Destination 区域，请选择 **No**，确保在用户进行身份验证之前可以访问您的登录页面。

步骤 6　返回 Edit Customization Object 窗口，点击 **General** 并启用连接配置文件和/或组策略中您想要自定义的对象。

无客户端 SSL VPN 最终用户设置

此节适用于为最终用户设置无客户端 SSL VPN 的系统管理员。此节将介绍如何自定义最终用户界面并总结远程系统的配置要求和任务。此节将详细说明要让用户开始使用无客户端 SSL VPN 需要向他们传递的信息。

定义最终用户界面

无客户端 SSL VPN 最终用户界面包括一系列 HTML 面板。用户按照 https://*地址*的形式输入 ASA 接口的 IP 地址即可登录无客户端 SSL VPN。系统显示的第一个面板是登录屏幕。

查看无客户端 SSL VPN 主页

用户登录后，系统将打开门户页面。

主页显示已配置的所有无客户端 SSL VPN 功能，其外观反映所选的徽标、文本和颜色。除了不能标识特定文件共享，此示例主页包括所有可用的无客户端 SSL VPN 功能。用户可以通过此主页浏览网络，输入 URL，访问特定网站，以及使用应用访问 （端口转发和智能隧道）来访问 TCP 应用。

查看无客户端 SSL VPN Application Access 面板

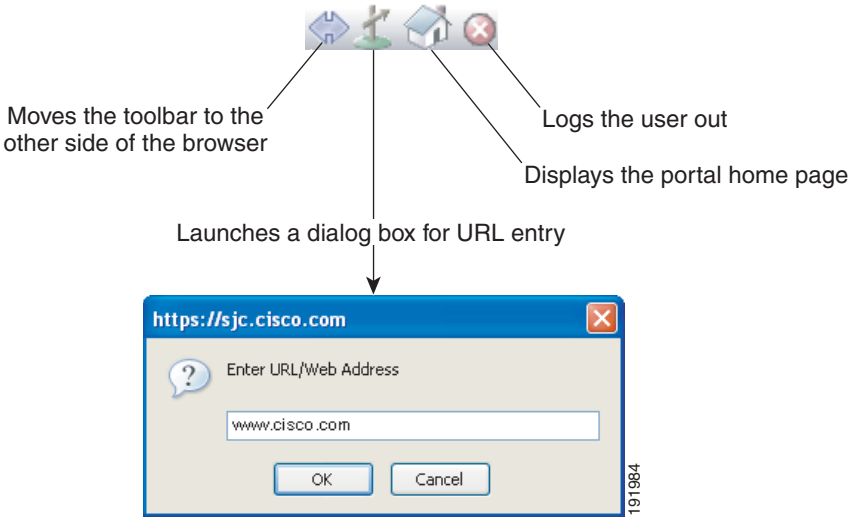
要启动端口转发或智能隧道，用户可点击 Application Access 框中的 **Go** 按钮。系统将显示 Application Access 窗口，然后将显示为此无客户端 SSL VPN 连接配置的 TCP 应用。要在此面板打开的情况下使用某应用，用户可以按照正常方式启动该应用。

注　状态故障转移将不保留使用 Application Access 建立的会话。出现故障转移后，用户必须重新连接。

查看浮动工具栏

图 17-3 中显示的浮动工具栏显示当前无客户端 SSL VPN 会话。

图 17-3　　无客户端 SSL VPN 浮动工具栏



请注意浮动工具栏的以下特征：

- 此工具栏允许您输入 URL、浏览文件位置以及选择预配置的网络连接，而不会干扰主浏览器窗口。
- 如果将浏览器配置为阻止弹出窗口，则无法显示浮动工具栏。
- 如果关闭此工具栏， ASA 会提示您结束无客户端 SSL VPN 会话。

自定义无客户端 SSL VPN 页面

您可以更改向无客户端 SSL VPN 用户显示的门户页面的外观。这包括当用户连接至安全设备时向用户显示的登录页面、安全设备对用户进行身份验证之后向用户显示的主页、用户启动某个应用时显示的 Application Access 窗口以及用户注销无客户端 SSL VPN 会话时显示的注销页面。

自定义门户页面后，可以保存您的自定义配置并将其应用于特定连接配置文件、组策略或用户。直到您重新加载 ASA，或者关闭再重新启用无客户端 SSL 之后，更改才会生效。

您可以创建和保存很多自定义对象，让安全设备可以更改单个用户或用户组的门户页面的外观。

有关自定义的信息

ASA 使用自定义对象定义用户屏幕的外观。自定义对象从包含 XML 标签的 XML 文件进行编译，其中 XML 标签适用于向远程用户显示的所有可自定义屏幕项。ASA 软件包含您可以导出到远程 PC 的自定义模板。您可以编辑此模板，然后将此模板重新导入 ASA，用做新的自定义对象。

导出自定义对象时，将在您指定的 URL 位置创建包含 XML 标签的 XML 文件。名称为 *Template* 的自定义对象创建的 XML 文件包含空 XML 标签，为创建新的自定义对象提供基础。无法从缓存中更改或删除此对象，但可以将其导出、编辑并重新导入回到 ASA 中，作为新的自定义对象。

自定义对象、连接配置文件和组策略

首先，当用户首次连接时，连接配置文件（隧道组）中标识的默认自定义对象（名称为 *DfltCustomization*）将确定登录屏幕的显示方式。如果已启用连接配置文件列表，并且用户选择有自己的不同自定义配置的组，此屏幕会改为反映该新组的自定义对象。

远程用户进行身份验证之后，屏幕外观取决于是否给组策略分配了自定义对象。

编辑自定义模板

本节显示自定义模板的内容并提供方便的图示，帮助您快速选择正确的 XML 标签和进行影响屏幕的更改。

您可以使用文本编辑器或 XML 编辑器编辑此 XML 文件。以下示例显示了自定义模板的 XML 标签。为了便于查看，某些冗余标签已删除。

示例：

```
<custom>
   <localization>
      <languages>en,ja,zh,ru,ua</languages>
      <default-language>en</default-language>
   </localization>
    <auth-page>
      <window>
          <title-text l10n="yes"><![CDATA[SSL VPN Service]]></title-text>
      </window>
      <full-customization>
          <mode>disable</mode>
          <url></url>
      </full-customization>
      <language-selector>
```

```
          <mode>disable</mode>
          <title l10n="yes">Language:</title>
          <language>
            <code>en</code>
            <text>English</text>
          </language>
          <language>
            <code>zh</code>
            <text>ä¸å›½ (Chinese)</text>
          </language>
          <language>
            <code>ja</code>
            <text>æ—¥æœ¬ (Japanese)</text>
          </language>
          <language>
            <code>ru</code>
            <text>Ð ÑƒÑÑкий (Russian)</text>
          </language>
          <language>
            <code>ua</code>
            <text>Ð£ÐºÑ?ÐºÑ—Ð½ÑÑŒÐºÐ° (Ukrainian)</text>
          </language>
        </language-selector>
        <logon-form>
            <title-text l10n="yes"><![CDATA[Login]]></title-text>
            <title-background-color><![CDATA[#666666]]></title-background-color>
            <title-font-color><![CDATA[#ffffff]]></title-font-color>
            <message-text l10n="yes"><![CDATA[Please enter your username and
password.]]></message-text>
            <username-prompt-text l10n="yes"><![CDATA[USERNAME:]]></username-prompt-text>
            <password-prompt-text l10n="yes"><![CDATA[PASSWORD:]]></password-prompt-text>
            <internal-password-prompt-text l10n="yes">Internal
Password:</internal-password-prompt-text>
            <internal-password-first>no</internal-password-first>
            <group-prompt-text l10n="yes"><![CDATA[GROUP:]]></group-prompt-text>
            <submit-button-text l10n="yes"><![CDATA[Login]]></submit-button-text>
            <title-font-color><![CDATA[#ffffff]]></title-font-color>
            <title-background-color><![CDATA[#666666]]></title-background-color>
            <font-color>#000000</font-color>
            <background-color>#ffffff</background-color>
            <border-color>#858A91</border-color>
        </logon-form>
        <logout-form>
            <title-text l10n="yes"><![CDATA[Logout]]></title-text>
            <message-text l10n="yes"><![CDATA[Goodbye.<br>

For your own security, please:<br>

<li>Clear the browser's cache

<li>Delete any downloaded files

<li>Close the browser's window]]></message-text>
            <login-button-text l10n="yes">Logon</login-button-text>
            <hide-login-button>no</hide-login-button>
            <title-background-color><![CDATA[#666666]]></title-background-color>
            <title-font-color><![CDATA[#ffffff]]></title-font-color>
            <title-font-color><![CDATA[#ffffff]]></title-font-color>
            <title-background-color><![CDATA[#666666]]></title-background-color>
            <font-color>#000000</font-color>
            <background-color>#ffffff</background-color>
            <border-color>#858A91</border-color>
        </logout-form>
        <title-panel>
```

```
      <mode>enable</mode>
      <text l10n="yes"><![CDATA[SSL VPN Service]]></text>
      <logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
      <gradient>yes</gradient>
      <style></style>
      <background-color><![CDATA[#ffffff]]></background-color>
      <font-size><![CDATA[larger]]></font-size>
      <font-color><![CDATA[#800000]]></font-color>
      <font-weight><![CDATA[bold]]></font-weight>
    </title-panel>
    <info-panel>
      <mode>disable</mode>
      <image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
      <image-position>above</image-position>
      <text l10n="yes"></text>
    </info-panel>
    <copyright-panel>
      <mode>disable</mode>
      <text l10n="yes"></text>
    </copyright-panel>
  </auth-page>
  <portal>
    <title-panel>
      <mode>enable</mode>
      <text l10n="yes"><![CDATA[SSL VPN Service]]></text>
      <logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
      <gradient>yes</gradient>
      <style></style>
      <background-color><![CDATA[#ffffff]]></background-color>
      <font-size><![CDATA[larger]]></font-size>
      <font-color><![CDATA[#800000]]></font-color>
      <font-weight><![CDATA[bold]]></font-weight>
    </title-panel>
    <browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
    <access-network-title l10n="yes">Start AnyConnect</access-network-title>
    <application>
      <mode>enable</mode>
      <id>home</id>
      <tab-title l10n="yes">Home</tab-title>
      <order>1</order>
    </application>
    <application>
      <mode>enable</mode>
      <id>web-access</id>
      <tab-title l10n="yes"><![CDATA[Web Applications]]></tab-title>
      <url-list-title l10n="yes"><![CDATA[Web Bookmarks]]></url-list-title>
      <order>2</order>
    </application>
    <application>
      <mode>enable</mode>
      <id>file-access</id>
      <tab-title l10n="yes"><![CDATA[Browse Networks]]></tab-title>
      <url-list-title l10n="yes"><![CDATA[File Folder Bookmarks]]></url-list-title>
      <order>3</order>
    </application>
    <application>
      <mode>enable</mode>
      <id>app-access</id>
      <tab-title l10n="yes"><![CDATA[Application Access]]></tab-title>
      <order>4</order>
    </application>
    <application>
      <mode>enable</mode>
      <id>net-access</id>
```

```
   <tab-title l10n="yes">AnyConnect</tab-title>
   <order>4</order>
</application>
<application>
   <mode>enable</mode>
   <id>help</id>
   <tab-title l10n="yes">Help</tab-title>
   <order>1000000</order>
</application>
<toolbar>
   <mode>enable</mode>
   <logout-prompt-text l10n="yes">Logout</logout-prompt-text>
   <prompt-box-title l10n="yes">Address</prompt-box-title>
   <browse-button-text l10n="yes">Browse</browse-button-text>
</toolbar>
<column>
   <width>100%</width>
   <order>1</order>
</column>
<pane>
   <type>TEXT</type>
   <mode>disable</mode>
   <title></title>
   <text></text>
   <notitle></notitle>
   <column></column>
   <row></row>
   <height></height>
</pane>
<pane>
   <type>IMAGE</type>
   <mode>disable</mode>
   <title></title>
   <url l10n="yes"></url>
   <notitle></notitle>
   <column></column>
   <row></row>
   <height></height>
</pane>
<pane>
   <type>HTML</type>
   <mode>disable</mode>
   <title></title>
   <url l10n="yes"></url>
   <notitle></notitle>
   <column></column>
   <row></row>
   <height></height>
</pane>
<pane>
   <type>RSS</type>
   <mode>disable</mode>
   <title></title>
   <url l10n="yes"></url>
   <notitle></notitle>
   <column></column>
   <row></row>
   <height></height>
</pane>
<url-lists>
   <mode>group</mode>
</url-lists>
<home-page>
   <mode>standard</mode>
```

```
        <url></url>
      </home-page>
    </portal>
</custom>
```

图 17-4 显示了登录页面及其自定义 XML 标签。所有这些标签都嵌套于更高级别的标签 <auth-page> 中。

图 17-4　登录页面和关联的 XML 标签

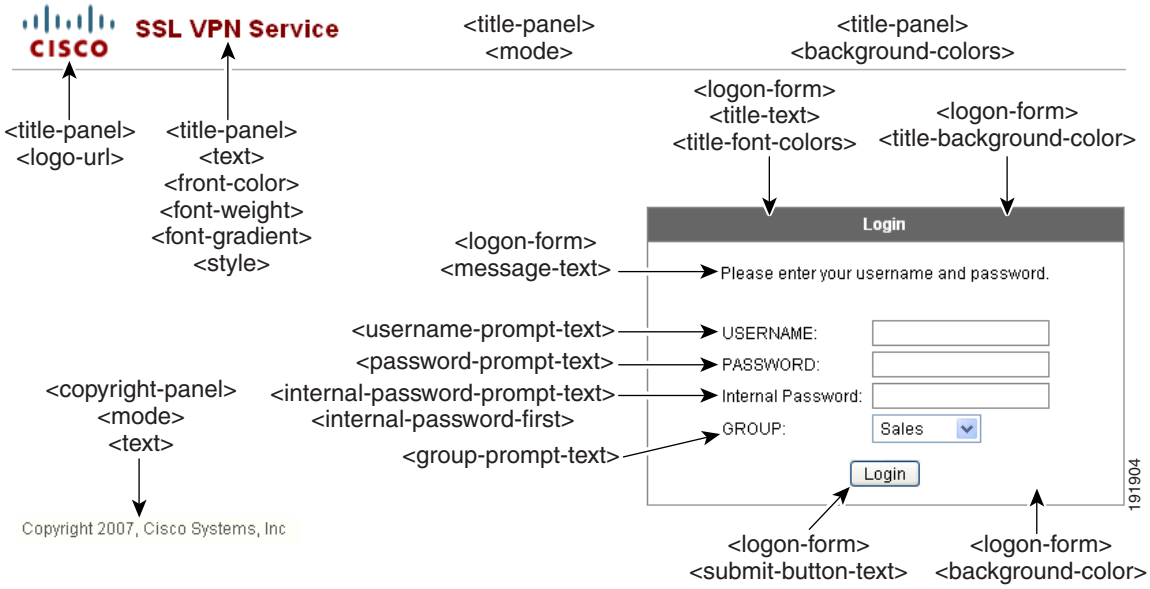


图 17-5 显示了在登录页面上可用的语言选择器下拉列表以及用于自定义此功能的 XML 标签。所有这些标签都嵌套于更高级别的 <auth-page> 标签中。

图 17-5　登录屏幕上的语言选择器和关联的 XML 标签

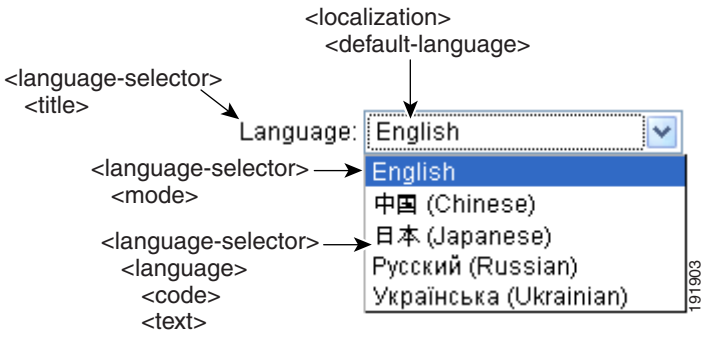


图 17-6 显示了在登录页面上可用的信息面板以及用于自定义此功能的 XML 标签。此信息可显示在登录框的左侧或右侧。这些标签都嵌套于更高级别的 <auth-page> 标签中。

图 17-6　登录屏幕上的信息面板和关联的 XML 标签

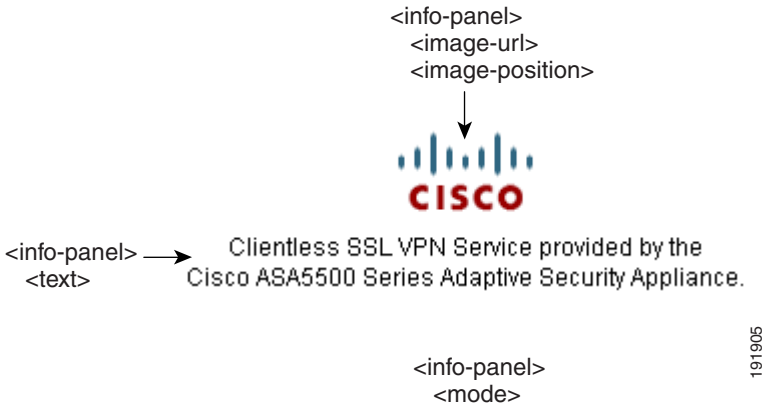
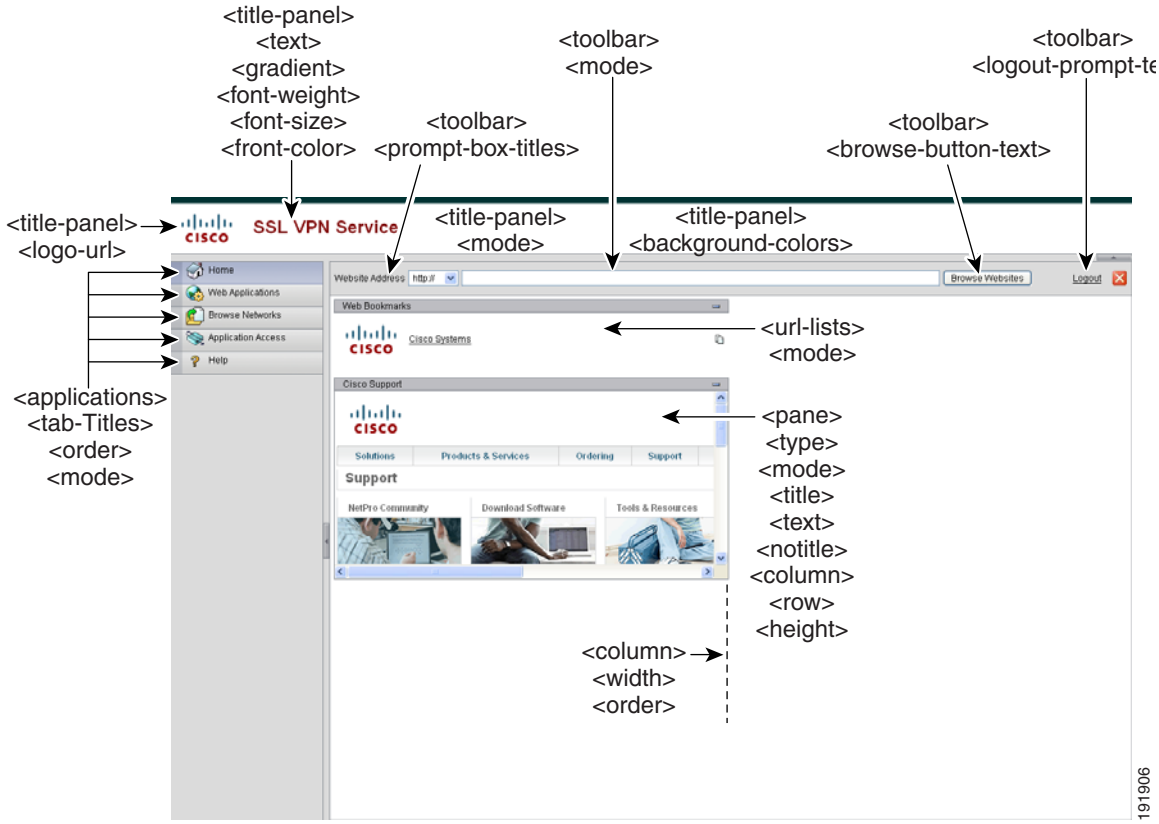


图 17-7 显示了门户页面以及自定义此功能的 XML 标签。这些标签都嵌套于更高级别的 <auth-page> 标签中。

图 17-7　门户页面和关联的 XML 标签



步骤 7

请参阅连接配置文件、组策略和用户。

登录屏幕高级自定义

如果您希望使用自己的自定义登录屏幕，而不是更改我们所提供的登录页面的特定屏幕元素，您可以使用 “*完全自定义*”功能执行这种高级自定义。

利用 “完全自定义”功能，您可以为您自己的登录屏幕提供 HTML 并插入调用 ASA 上创建登录表单和语言选择器下拉列表的函数的思科 HTML 代码。

本节描述您需要对您的 HTML 代码所做的修改和配置 ASA 使用您的代码所需完成的任务。

图 17-8 显示了向无客户端 SSL VPN 用户显示的标准思科登录屏幕。登录表单由 HTML 代码调用的函数显示。

图 17-8　　标准思科登录页面

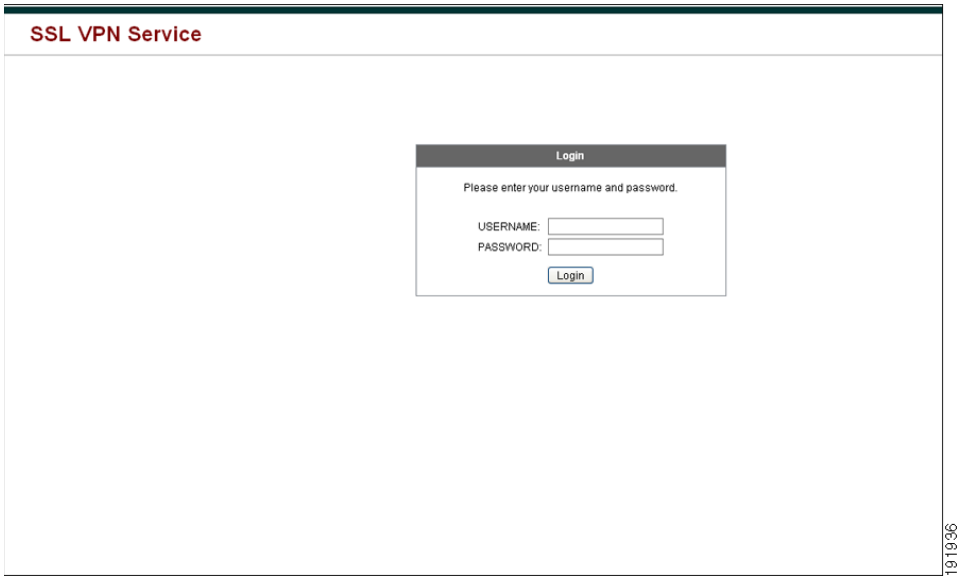


图 17-9 显示了语言选择器下拉列表。此功能是无客户端 SSL VPN 用户的一个选项，也是由登录屏幕的 HTML 代码中的函数调用。

图 17-9　　语言选择器下拉列表

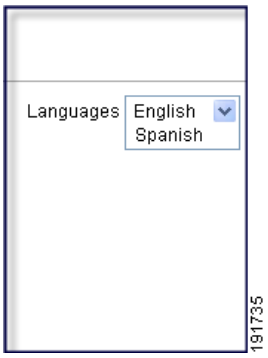
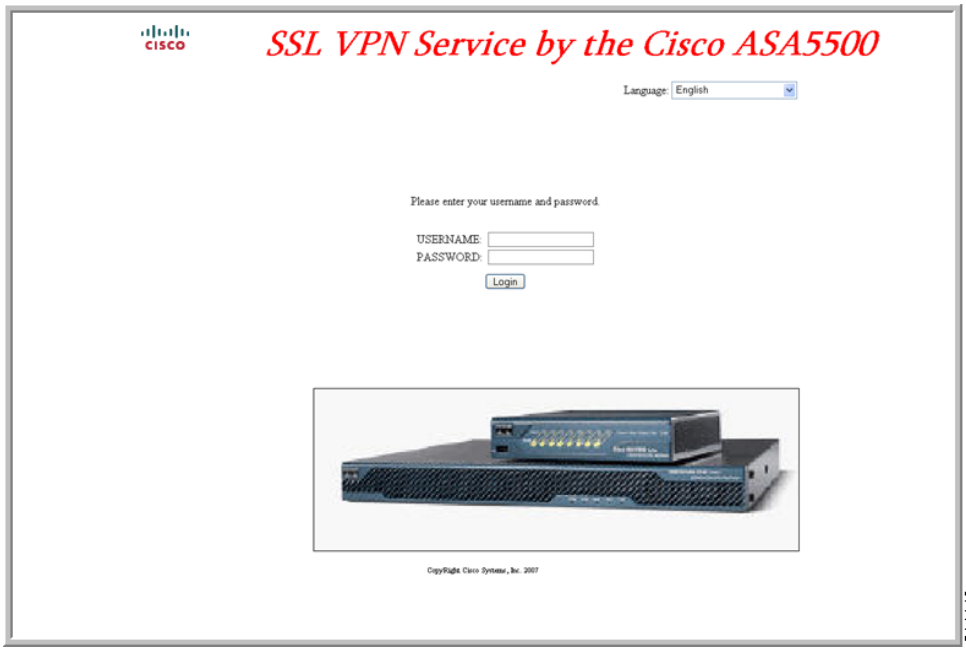


图 17-10 显示了 “完全自定义”功能启用的一个简单的自定义登录屏幕示例。

图 17-10　　登录屏幕的完全自定义示例



以下 HTML 代码是一个示例，也是系统显示的代码：

示例：

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>New Page 3</title>
<base target="_self">
</head>

<p align="center">
<img border="0" src="/+CSCOU+/cisco_logo.jpg" width="188" height="48"><font face="Snap
ITC" size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7"> </font><i><b><font
color="#FF0000" size="7" face="Sylfaen"> SSL VPN Service by the Cisco
ASA5500</font></b></i></p>

    <body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

    <table>

    <tr><td colspan=3 height=20 align=right><div id="selector" style="width:
    300px"></div></td></tr>
    <tr><td></td><td></td><td></td></tr>
    <tr>
    <td height="379"></td>
    <td height="379"></td>
    <td align=middle valign=middle>
    <div id=lform >
    <p> </p>
    <p> </p>
    <p> </p>
    <p>Loading...</p>
    </div>
```

```
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>

</table>
```

这种缩进的代码将在屏幕上注入登录表单和语言选择器。函数 **csco_ShowLoginForm('lform')** 注入登录表单。 **csco_ShowLanguageSelector('selector')** 注入语言选择器。

修改您的 HTML 文件

步骤 1　将您的文件命名为 **logon.inc**。当您导入文件时， ASA 将此文件名识别为登录屏幕。

步骤 2　修改该文件使用的映像的路径以包含 **/+CSCOU+/**。

在身份验证之前向远程用户显示的文件必须放在 ASA 缓存的特定区域，以路径 /+CSCOU+/ 表示。因此，该文件中每个映像的源都必须包含此路径。例如：

```
src="/+CSCOU+/asa5520.gif"
```

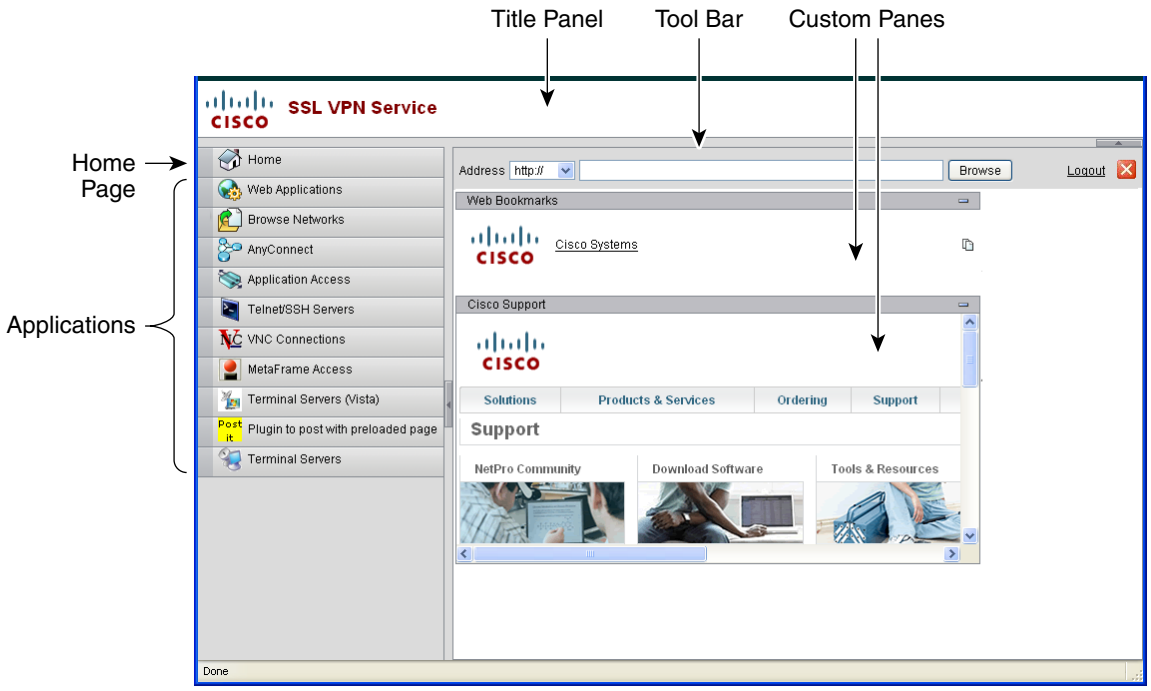
步骤 3　插入下面的特殊 HTML 代码。此代码包含之前描述的在屏幕上注入登录表单和语言选择器的思科函数。

```
<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>

</table>
```

自定义门户页面

图 17-11 显示了门户页面和您可以自定义的预定义组件。

图 17-11　　门户页面的自定义组件



除了自定义页面组件之外，您还可以将门户页面分为显示文本、图像、 RSS 源或 HTML 的自定义窗格。

要自定义门户页面，请执行以下步骤。您可以点击 **Preview** 按钮，预览您对每个组件的更改：

步骤 1　转到 Portal Page 并为浏览器窗口指定标题。

步骤 2　显示并自定义标题面板。转至 Portal Page > Title Panel 并选中 **Display title panel**。输入作为标题显示的文本并指定徽标。指定任意字体样式。

步骤 3　启用和自定义工具栏。转到 Portal Page > Toolbar 并选中 **Display toolbar**。根据需要自定义 Prompt Box、 Browse 按钮和 Logout 提示。

步骤 4　自定义 Applications 列表。转到 Portal Page > Applications 并选中 **Show navigation panel**。此表格中填充的应用即您在 ASA 配置中启用的那些应用，包括客户端-服务器插件和端口转发应用。

步骤 5　在门户页面空间创建自定义窗格。转至 Portal Page > Custom Panes，按照需要为文本、图像、RSS 源或 HTML 页面将该窗口分为相应数量的行和列。

步骤 6　指定主页 URL。转至 Portal Page > Home Page 并选中 **Enable custom intranet Web page**。选择定义书签组织方式的书签模式。

配置超时警报和工具提示。转至 Portal Page > Timeout Alerts。

后续操作

请参阅 “配置自定义门户超时警报”。

配置自定义门户超时警报

为使无客户端 SSL VPN 功能用户可以管理他们在 VPN 会话中的时间，无客户端 SSL VPN 门户页面将显示倒计时计时器，提示距离 VPN 会话过期剩余的总时间。会话会因为不活动或达到了您配置的最长允许连接时间而超时。

您可以创建自定义消息，提醒用户由于空闲超时或会话超时，他们的会话即将终止。自定义消息将取代默认的空闲超时消息。默认消息为 "`Your session will expire in %s .`" 在您的消息中 **%s** 占位符将被一个滴答作响的倒计时计时器代替。

步骤 1　启动 ASDM 并选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization**。

步骤 2　点击 **Add** 以添加新的自定义对象或选择现有的自定义对象，然后点击 **Edit**，向现有自定义对象添加自定义空闲超时消息。

步骤 3　在 Add / Edit Customization Object 窗格，展开导航树上的 Portal Page 节点，然后点击 **Timeout Alerts**。

步骤 4　选中 **Enable alert visual tooltip (red background for timer countdown)**。这会将倒计时计时器显示为红色背景上的一个工具提示。当用户点击 Time left 区域时，此时间区域将展开显示您的自定义超时警报消息。如果您未选中此复选框，用户会在弹出窗口中看到自定义超时消息。

步骤 5　在 Idle Timeout Message 框和 Session Timeout Message 框中输入消息。消息可以写成这样：`Warning: Your session will end in %s. Please complete your work and prepare to close your applications.`

步骤 6　点击 **OK**。

步骤 7　点击 **Apply**。

在自定义对象文件中指定自定义超时警报

如果需要，您可以在 ASA 外面编辑现有的自定义对象文件，然后将其导入到 ASA 中。

超时消息在您的 XML 自定义对象文件的 <timeout-alerts> XML 元素中配置。<timeout-alerts> 元素是 <portal> 元素的子元素。 <portal> 元素是 <custom> 元素的子元素。

此 <timeout-alerts>元素按照 <portal> 子元素的顺序放在 <home-page> 元素的后面和所有 <application> 元素的前面。

您需要指定 <timeout-alerts> 的这些子元素：

- <alert-tooltip> - 如果设置为 "yes"，用户将在红色背景上看到作为工具提示的倒计时计时器。点击倒计时计时器可展开此工具提示，显示您的自定义消息。如果设置为 "no" 或未定义，用户将在弹出窗口中收到您的自定义消息。
- <session-timeout-message> - 在此元素中输入您的自定义会话超时消息。如果已经设置而且不是空的，用户将收到您的自定义消息而不是默认消息。消息中的 %s 占位符将替换为滴答作响的倒计时计时器。
- <idle-timeout-message> - 在此元素中输入您的自定义空闲超时消息。如果已经设置而且不是空的，用户将收到您的自定义消息而不是默认消息。其中 %s 占位符将替换为滴答作响的倒计时计时器。

后续操作

请参阅 "导入和导出自定义对象" 和 "创建基于 XML 的门户自定义对象与 URL 列表"。

超时警报元素和子要素的配置示例

此示例只显示了 <portal> 元素的 <timeout-alerts> 元素。

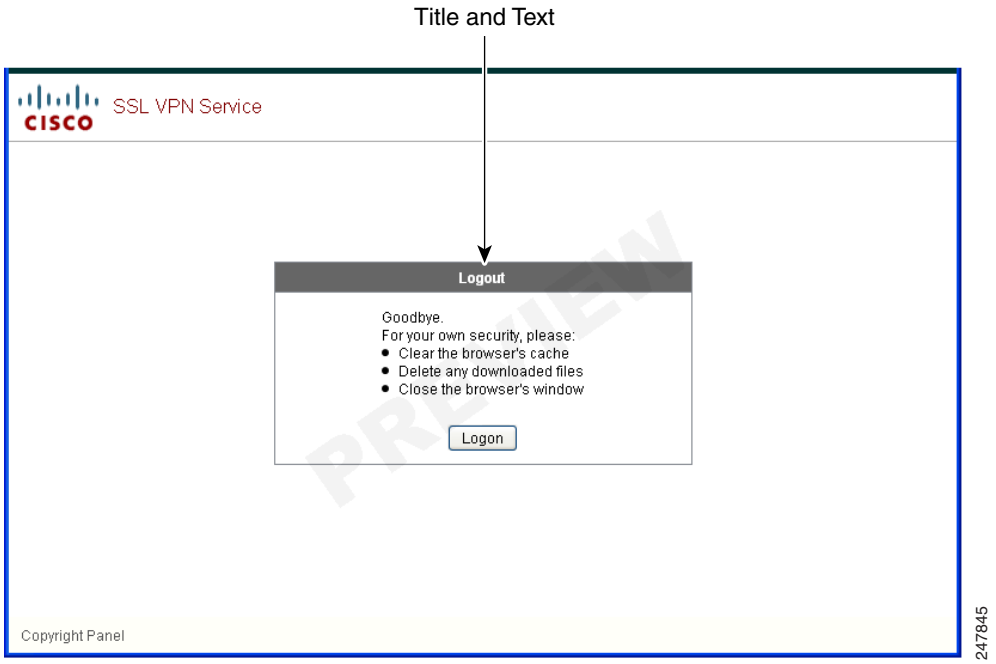
注　请勿将该示例剪切并粘贴到现有自定义对象中。

```
<portal>
    <window></window>
    <title-panel></title-panel>
    <toolbar></toolbar>
    <url-lists></url-lists>
    <navigation-panel></navigation-panel>
    <home-page>
    <timeout-alerts>
        <alert-tooltip>yes</alert-tooltip>
        <idle-timeout-message>You session expires in %s due to idleness.</idle-timeout-message>
        <session-timeout-message>Your session expires in %s.</session-timeout-message>
    </timeout-alerts>
    <application></application>
    <column></column>
    <pane></pane>
    <external-portal></external-portal>
</portal>
```

自定义注销页面

图 17-12 显示了您可以自定义的注销页面：

图 17-12　注销页面的组件



要自定义注销页面，请执行以下步骤。您可以点击 **Preview** 按钮，预览您对每个组件的更改：

步骤 1　转至 Logout Page。按照需要自定义标题或文本。

步骤 2　为方便用户起见，您可以在 Logout 页面显示 Login 按钮。为此，请选中 **Show logon button**。按照需要自定义按钮文本。

步骤 3　按照需要自定义标题字体或背景。

步骤 4　点击 **OK**，然后将更改应用到您编辑的自定义对象上。

添加自定义对象

步骤 1　点击 **Add**，然后为新自定义对象输入一个名称。最多 64 个字符，不能包含空格。

步骤 2　（可选）点击 **Find**，搜索自定义对象。开始在字段中键入，此工具会搜索每个字段的开头字符进行匹配。您可以使用通配符扩大搜索。例如，在 Find 字段键入 *sal* 将匹配一个名称为 sales 的自定义对象，但是不会匹配名称为 wholesalers 的自定义对象。如果您在 Find 字段键入 **sal*，搜索结果会找到表中的第一个 sales 或 wholesales 实例。

使用上下箭头向上或向下跳到下一个字符串匹配项。选中 **Match Case** 复选框，确保您的搜索区分大小写。

步骤 3　指定何时在门户页面上显示屏幕键盘。选项如下：

- Do not show OnScreen Keyboard
- Show only for the login page
- Show for all portal pages requiring authentication

步骤 4　（可选）突出显示一个自定义对象，然后点击 **Assign**，将选择的对象分配给一个或多个组策略、连接配置文件或本地用户。

导入/导出自定义对象

您可以导入或导出已经存在的自定义对象。导入对象可应用于最终用户。导出 ASA 上已有的自定义对象进行编辑，然后再将其重新导入。

步骤 1　按照名称标识自定义对象。最多 64 个字符，不能包含空格。

步骤 2　选择导入或导出自定义文件的方法：

- Local computer - 选择此方法导入位于本地 PC 上的文件。
- Path - 提供指向文件的路径。
- Browse Local Files - 浏览到文件的路径。
- Flash file system - 选择此方法导出放在 ASA 上的文件。
- Path - 提供指向文件的路径。
- Browse Flash - 浏览到文件的路径。
- Remote server - 选择此选项可导入位于可以从 ASA 访问的远程服务器上的自定义文件。

- Path - 确定访问文件的方法 （ftp、 http 或 https），并提供指向该文件的路径。

步骤 3　点击以导入或导出文件。

了解 XML 自定义文件结构

表 17-1 显示了 XML 自定义对象的文件结构。

注　缺乏参数/标签会导致使用默认/继承的值，有参数/标签则会导致设置参数/标签的值，哪怕是空字符串。

表 17-1　基于 XML 的自定义文件结构

标签	类型	值	预设值	说明
custom	**节点**	—	—	**根标签**
auth-page	**节点**	—	—	**身份验证页面配置的标签容器**
window	**节点**	—	—	**浏览器窗口**
title-text	字符串	任意字符串	空字符串	—
title-panel	**节点**	—	—	**包含徽标和文本的页面顶部窗格**
mode	文本	启用|禁用	禁用	—
text	文本	任意字符串	空字符串	—
logo-url	文本	任意 URL	空图像 URL	—
copyright-panel	**节点**	—	—	**包含版权信息的页面底部窗格**
mode	文本	启用|禁用	禁用	—
text	文本	任意 URL	空字符串	—
info-panel	**节点**	—	—	**带自定义文本和图像的窗格**
mode	字符串	启用|禁用	禁用	—
image-position	字符串	上面|下面	上面	相对于文本的图像位置
image-url	字符串	任意 URL	空图像	—
text	字符串	任意字符串	空字符串	—
logon-form	**节点**	—	—	**包含用户名、密码、组提示的表单**
title-text	字符串	任意字符串	登录	—
message-text	字符串	任意字符串	空字符串	—
username-prompt-text	字符串	任意字符串	用户名	—
password-prompt-text	字符串	任意字符串	密码	—

表 17-1　　基于 XML 的自定义文件结构 （续）

internal-password-prompt-text	字符串	任意字符串	内部密码	—
group-prompt-text	字符串	任意字符串	组	—
submit-button-text	字符串	任意字符串	登录	
logout-form	**节点**	**—**	**—**	**包含注销信息以及登录或关闭窗口的按钮的表单**
title-text	字符串	任意字符串	注销	—
message-text	字符串	任意字符串	空字符串	—
login-button-text	字符串	任意字符串	登录	
close-button-text	字符串	任意字符串	关闭窗口	—
language-selector	**节点**	**—**	**—**	**用于选择语言的下拉列表**
mode	字符串	启用|禁用	禁用	—
title	文本	—	语言	用于选择语言的提示文本
language	**节点（多个）**	**—**	**—**	**—**
code	字符串	—	—	—
text	字符串	—	—	—
portal	**节点**	**—**	**—**	**门户页面配置的标签容器**
window	**节点**	**—**	**—**	**请参阅身份验证页面说明**
title-text	字符串	任意字符串	空字符串	—
title-panel	**节点**	**—**	**—**	**请参阅身份验证页面说明**
mode	字符串	启用|禁用	禁用	—
text	字符串	任意字符串	空字符串	—
logo-url	字符串	任意 URL	空图像 URL	—
navigation-panel	**节点**	**—**	**—**	**左边带应用选项卡的窗格**
mode	字符串	启用|禁用	启用	—
application	**节点（多个）**	**—**	**无**	**此节点更改已配置的（按照 id）应用的默认设置**

表 17-1　　基于 XML 的自定义文件结构 （续）

id	字符串	对于库存应用 网络访问 文件访问 应用访问 网络访问 帮助 对于 ins： 唯一插件	无	—
tab-title	字符串	—	无	—
order	数值	—	无	用于给元素排序的值。默认元素顺序值的步长为 1000、2000、 3000 等。例如，要在第一和第二个元素之间插入一个元素，请使用值 1001 - 1999。
url-list-title	字符串	—	无	如果应用有书签，则是指包含分组书签的面板的标题
mode	字符串	启用|禁用	无	v
toolbar	**节点**	**—**	**—**	**—**
mode	字符串	启用|禁用	启用	—
prompt-box-title	字符串	任意字符串	地址	URL 提示列表的标题
browse-button-text	字符串	任意字符串	浏览	浏览按钮文本
logout-prompt-text	字符串	任意字符串	注销	—
column	**节点（多个）**	**—**	**—**	**默认情况下将显示一列**
width	字符串	—	无	—
order	数值	—	无	用于给元素排序的值。
url-lists	**节点**	**—**	**—**	**如果没有明确关闭 URL 列表，则在门户主页上 URL 列表将被视为默认元素。**

表 17-1　　基于 XML 的自定义文件结构 （续）

mode	字符串	组|无组	组	模式： 组 - 按照应用类型分组的元素 （即网络书签、文件书签） 无组 - 在单独窗格中显示 URL 列表 禁用 - 默认情况下不显示 URL 列表
panel	节点 （多个）	—	—	允许配置额外的窗格
mode	字符串	启用|禁用	—	用于暂时关闭面板，但不删除其配置
title	字符串	—	—	—
type	字符串	—	—	支持的类型： RSS IMAGE TEXT HTML
url url-mode	字符串 字符串	— —	— —	RSS、 IMAGE 或 HTML 类型窗格的 URL 模式：改变、不改变
text	字符串	—	—	TEXT 类型窗格的文本
column	数值	—	—	—

自定义的配置示例

以下示例说明了下列自定义选项：

- 对文件访问应用隐藏选项卡
- 更改网络访问应用的标题和顺序
- 在主页定义两列
- 添加 RSS 窗格
- 在第二个窗格的顶部添加三个窗格 （文本、图像和 html）

```
<custom name="Default">
  <auth-page>

    <window>
          <title-text l10n="yes">title WebVPN Logon</title>
    </window>
```

```
    <title-panel>
         <mode>enable</mode>
         <text l10n="yes">EXAMPLE WebVPN</text>
         <logo-url>http://www.example.com/images/EXAMPLE.gif</logo-url>
    </title-panel>

    <copyright>
         <mode>enable</mode>
         <text l10n="yes">(c)Copyright, EXAMPLE Inc., 2006</text>
    </copyright>

    <info-panel>
        <mode>enable</mode>
        <image-url>/+CSCOE+/custom/EXAMPLE.jpg</image-url>
      <text l10n="yes">
            <![CDATA[
            <div>
            <b>Welcome to WebVPN !.</b>
            </div>
            ]]>
      </text>
    </info-panel>
    <logon-form>
      <form>
          <title-text l10n="yes">title WebVPN Logon</title>
          <message-text l10n="yes">message WebVPN Logon</title>
          <username-prompt-text l10n="yes">Username</username-prompt-text>
          <password-prompt-text l10n="yes">Password</password-prompt-text>
          <internal-password-prompt-text l10n="yes">Domain
password</internal-password-prompt-text>
          <group-prompt-text l10n="yes">Group</group-prompt-text>
          <submit-button-text l10n="yes">Logon</submit-button-text>
      </form>
    </logon-form>
    <logout-form>
      <form>
          <title-text l10n="yes">title WebVPN Logon</title>
          <message-text l10n="yes">message WebVPN Logon</title>
          <login-button-text l10n="yes">Login</login-button-text>
          <close-button-text l10n="yes">Logon</close-button-text>
      </form>
    </logout-form>

    <language-slector>
      <language>
          <code l10n="yes">code1</code>
          <text l10n="yes">text1</text>
      </language>
      <language>
          <code l10n="yes">code2</code>
          <text l10n="yes">text2</text>
      </language>
    </language-slector>

  </auth-page>
  <portal>

    <window>
          <title-text l10n="yes">title WebVPN Logon</title>
    </window>

    <title-panel>
         <mode>enable</mode>
         <text l10n="yes">EXAMPLE WebVPN</text>
```

```
          <logo-url>http://www.example.com/logo.gif</logo-url>
      </title-panel>

      <navigation-panel>
          <mode>enable</mode>
      </navigation-panel>

      <application>
              <id>file-access</id>
              <mode>disable</mode>
      </application>
      <application>
              <id>web-access</id>
              <tab-title>EXAMPLE Intranet</tab-title>
              <order>3001</order>
      </application>

     <column>
              <order>2</order>
              <width>40%</width>
    <column>
     <column>
              <order>1</order>
              <width>60%</width>
    <column>

    <url-lists>
      <mode>no-group</mode>
    </url-lists>

    <pane>
     <id>rss_pane</id>
      <type>RSS</type>
     <url>rss.example.com?id=78</url>
    </pane>
    <pane>
      <type>IMAGE</type>
     <url>http://www.example.com/logo.gif</url>
      <column>1</column>
      <row>2</row>
     </pane>

    <pane>
      <type>HTML</type>
     <title>EXAMPLE news</title>
     <url>http://www.example.com/news.html</url>
      <column>1</column>
      <row>3</row>
     </pane>

    </portal>

  </custom>
```

使用自定义模板

自定义模板，名称为 *Template*，包含当前所用的所有标签以及描述如何使用这些标签的对应备注。使用 **export** 命令从 ASA 下载自定义模板，如下所示：

```
hostname# export webvpn customization Template tftp://webserver/default.xml
hostname#
```

您无法更改或删除文件 *Template*。当导出它时，像本例中一样，它将保存为新名称 *default.xml*。当您更改完此文件，创建符合您的组织需求的自定义对象之后，请将其导入 ASA，可以采用名称 *default.xml* 或选择其他名称。例如：

```
hostname# import webvpn customization General tftp://webserver/custom.xml
hostname#
```

其中，您将导入名称为 *custom.xml* 的 XML 对象并在 ASA 上将其命名为 *General*。

自定义模板

自定义模板，名称为 *Template*，如下所示：

```
<?xml version="1.0" encoding="UTF-8" ?>
- <!--

Copyright (c) 2008,2009 by Cisco Systems, Inc.
All rights reserved.

Note: all white spaces in tag values are significant and preserved.


Tag: custom
Description: Root customization tag

Tag: custom/languages
Description: Contains list of languages, recognized by ASA
Value: string containing comma-separated language codes.Each language code is
       a set dash-separated alphanumeric characters, started with
       alpha-character (for example: en, en-us, irokese8-language-us)
Default value: en-us
Tag: custom/default-language
Description: Language code that is selected when the client and the server
             were not able to negotiate the language automatically.
             For example the set of languages configured in the browser
             is "en,ja", and the list of languages, specified by
             'custom/languages' tag is "cn,fr", the default-language will be
             used.
Value: string, containing one of the language coded, specified in
'custom/languages' tag above.
Default value: en-us

*****************************************************

Tag: custom/auth-page
Description: Contains authentication page settings

*****************************************************
Tag: custom/auth-page/window
Description: Contains settings of the authentication page browser window

Tag: custom/auth-page/window/title-text
```

```
Description: The title of the browser window of the authentication page
Value: arbitrary string
Default value: Browser's default value

*******************************************************

Tag: custom/auth-page/title-panel
Description: Contains settings for the title panel

Tag: custom/auth-page/title-panel/mode
Description: The title panel mode
Value: enable|disable
Default value: disable
Tag: custom/auth-page/title-panel/text
Description: The title panel text.
Value: arbitrary string
Default value: empty string

Tag: custom/auth-page/title-panel/logo-url
Description: The URL of the logo image (imported via "import webvpn webcontent")
Value: URL string
Default value: empty image URL

Tag: custom/auth-page/title-panel/background-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #FFFFFF

Tag: custom/auth-page/title-panel/font-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/auth-page/title-panel/font-weight
Description: The font weight
Value: CSS font size value, for example bold, bolder,lighter etc.
Default value: empty string

Tag: custom/auth-page/title-panel/font-size
Description: The font size
Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc.
Default value: empty string



Tag: custom/auth-page/title-panel/gradient
Description: Specifies using the background color gradient
Value: yes|no
Default value:no

Tag: custom/auth-page/title-panel/style
Description: CSS style of the title panel
Value: CSS style string
Default value: empty string

*******************************************************

Tag: custom/auth-page/copyright-panel
Description: Contains the copyright panel settings

Tag: custom/auth-page/copyright-panel/mode
Description: The copyright panel mode
Value: enable|disable
```

```
Default value: disable

Tag: custom/auth-page/copyright-panel/text
Description: The copyright panel text
Value: arbitrary string
Default value: empty string

*******************************************************
Tag: custom/auth-page/info-panel
Description: Contains information panel settings

Tag: custom/auth-page/info-panel/mode
Description: The information panel mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/info-panel/image-position
Description: Position of the image, above or below the informational panel text
Values: above|below
Default value: above

Tag: custom/auth-page/info-panel/image-url
Description: URL of the information panel image (imported via "import webvpn webcontent")
Value: URL string
Default value: empty image URL

Tag: custom/auth-page/info-panel/text
Description: Text of the information panel
Text: arbitrary string
Default value: empty string

*******************************************************

Tag: custom/auth-page/logon-form
Description: Contains logon form settings

Tag: custom/auth-page/logon-form/title-text
Description: The logon form title text
Value: arbitrary string
Default value: "Logon"

Tag: custom/auth-page/logon-form/message-text
Description: The message inside of the logon form
Value: arbitrary string
Default value: empty string

Tag: custom/auth-page/logon-form/username-prompt-text
Description: The username prompt text
Value: arbitrary string
Default value: "Username"

Tag: custom/auth-page/logon-form/password-prompt-text
Description: The password prompt text
Value: arbitrary string
Default value: "Password"

Tag: custom/auth-page/logon-form/internal-password-prompt-text
Description: The internal password prompt text
Value: arbitrary string
Default value: "Internal Password"

Tag: custom/auth-page/logon-form/group-prompt-text
Description: The group selector prompt text
Value: arbitrary string
```

```
Default value: "Group"


Tag: custom/auth-page/logon-form/submit-button-text
Description: The submit button text
Value: arbitrary string
Default value: "Logon"

Tag: custom/auth-page/logon-form/internal-password-first
Description: Sets internal password first in the order
Value: yes|no
Default value: no


Tag: custom/auth-page/logon-form/title-font-color
Description: The font color of the logon form title
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/auth-page/logon-form/title-background-color
Description: The background color of the logon form title
Value: HTML color format, for example #FFFFFF
Default value: #000000


Tag: custom/auth-page/logon-form/font-color
Description: The font color of the logon form
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/auth-page/logon-form/background-color
Description: The background color of the logon form
Value: HTML color format, for example #FFFFFF
Default value: #000000


*******************************************************

Tag: custom/auth-page/logout-form
Description: Contains the logout form settings

Tag: custom/auth-page/logout-form/title-text
Description: The logout form title text
Value: arbitrary string
Default value: "Logout"

Tag: custom/auth-page/logout-form/message-text
Description: The logout form message text
Value: arbitrary string
Default value: Goodbye.
               For your own security, please:
               Clear the browser's cache
               Delete any downloaded files
               Close the browser's window

Tag: custom/auth-page/logout-form/login-button-text
Description: The text of the button sending the user to the logon page
Value: arbitrary string
Default value: "Logon"

*******************************************************
```

```
Tag: custom/auth-page/language-selector
Description: Contains the language selector settings

Tag: custom/auth-page/language-selector/mode
Description: The language selector mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/language-selector/title
Description: The language selector title
Value: arbitrary string
Default value: empty string

Tag: custom/auth-page/language-selector/language (multiple)
Description: Contains the language settings

Tag: custom/auth-page/language-selector/language/code
Description: The code of the language
Value (required): The language code string

Tag: custom/auth-page/language-selector/language/text
Description: The text of the language in the language selector drop-down box
Value (required): arbitrary string

*******************************************************

Tag: custom/portal
Description: Contains portal page settings

*******************************************************

Tag: custom/portal/window
Description: Contains the portal page browser window settings

Tag: custom/portal/window/title-text
Description: The title of the browser window of the portal page
Value: arbitrary string
Default value: Browser's default value

*******************************************************

Tag: custom/portal/title-panel
Description: Contains settings for the title panel

Tag: custom/portal/title-panel/mode
Description: The title panel mode
Value: enable|disable
Default value: disable

Tag: custom/portal/title-panel/text
Description: The title panel text.
Value: arbitrary string
Default value: empty string

Tag: custom/portal/title-panel/logo-url
Description: The URL of the logo image (imported via "import webvpn webcontent")
Value: URL string
Default value: empty image URL

Tag: custom/portal/title-panel/background-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #FFFFFF
```

```
Tag: custom/auth-pa/title-panel/font-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/portal/title-panel/font-weight
Description: The font weight
Value: CSS font size value, for example bold, bolder,lighter etc.
Default value: empty string

Tag: custom/portal/title-panel/font-size
Description: The font size
Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc.
Default value: empty string
Tag: custom/portal/title-panel/gradient
Description: Specifies using the background color gradient
Value: yes|no
Default value:no

Tag: custom/portal/title-panel/style
Description: CSS style for title text
Value: CSS style string
Default value: empty string

*******************************************************

Tag: custom/portal/application (multiple)
Description: Contains the application setting

Tag: custom/portal/application/mode
Description: The application mode
Value: enable|disable
Default value: enable

Tag: custom/portal/application/id
Description: The application ID.Standard application ID's are: home, web-access,
file-access, app-access, network-access, help
Value: The application ID string
Default value: empty string

Tag: custom/portal/application/tab-title
Description: The application tab text in the navigation panel
Value: arbitrary string
Default value: empty string

Tag: custom/portal/application/order
Description: The order of the application's tab in the navigation panel.Applications with
lesser order go first.
Value: arbitrary number
Default value: 1000

Tag: custom/portal/application/url-list-title
Description: The title of the application's URL list pane (in group mode)
Value: arbitrary string
Default value: Tab tite value concatenated with "Bookmarks"

*******************************************************

Tag: custom/portal/navigation-panel
Description: Contains the navigation panel settings

Tag: custom/portal/navigation-panel/mode
Description: The navigation panel mode
Value: enable|disable
```

```
Default value: enable

*******************************************************

Tag: custom/portal/toolbar
Description: Contains the toolbar settings

Tag: custom/portal/toolbar/mode
Description: The toolbar mode
Value: enable|disable
Default value: enable

Tag: custom/portal/toolbar/prompt-box-title
Description: The universal prompt box title
Value: arbitrary string
Default value: "Address"
Tag: custom/portal/toolbar/browse-button-text
Description: The browse button text
Value: arbitrary string
Default value: "Browse"

Tag: custom/portal/toolbar/logout-prompt-text
Description: The logout prompt text
Value: arbitrary string
Default value: "Logout"

*******************************************************

Tag: custom/portal/column (multiple)
Description: Contains settings of the home page column(s)

Tag: custom/portal/column/order
Description: The order the column from left to right.Columns with lesser order values go
first
Value: arbitrary number
Default value: 0

Tag: custom/portal/column/width
Description: The home page column width
Value: percent
Default value: default value set by browser
Note: The actual width may be increased by browser to accommodate content


*******************************************************


Tag: custom/portal/url-lists
Description: Contains settings for URL lists on the home page

Tag: custom/portal/url-lists/mode
Description: Specifies how to display URL lists on the home page:
             group URL lists by application (group) or
             show individual URL lists (nogroup).
             URL lists fill out cells of the configured columns, which are not taken
             by custom panes.
             Use the attribute value "nodisplay" to not show URL lists on the home page.

Value: group|nogroup|nodisplay
Default value: group
*******************************************************
```

```
Tag: custom/portal/pane (multiple)
Description: Contains settings of the custom pane on the home page

Tag: custom/portal/pane/mode
Description: The mode of the pane
Value: enable|disable
Default value: disable

Tag: custom/portal/pane/title
Description: The title of the pane
Value: arbitrary string
Default value: empty string

Tag: custom/portal/pane/notitle
Description: Hides pane's title bar
Value: yes|no
Default value: no

Tag: custom/portal/pane/type
Description: The type of the pane.Supported types:
             TEXT - inline arbitrary text, may contain HTML tags;
             HTML - HTML content specified by URL shown in the individual iframe;
             IMAGE - image specified by URL
             RSS - RSS feed specified by URL
Value: TEXT|HTML|IMAGE|RSS
Default value: TEXT

Tag: custom/portal/pane/url
Description: The URL for panes with type HTML, IMAGE or RSS
Value: URL string
Default value: empty string

Tag: custom/portal/pane/text
Description: The text value for panes with type TEXT
Value: arbitrary string
Default value:empty string

Tag: custom/portal/pane/column
Description: The column where the pane located.
Value: arbitrary number
Default value: 1

Tag: custom/portal/pane/row
Description: The row where the pane is located
Value: arbitrary number
Default value: 1

Tag: custom/portal/pane/height
Description: The height of the pane
Value: number of pixels
Default value: default value set by browser


*********************************************************

Tag: custom/portal/browse-network-title
Description: The title of the browse network link
Value: arbitrary string
Default value: Browse Entire Network


Tag: custom/portal/access-network-title
Description: The title of the link to start a network access session
Value: arbitrary string
```

```
Default value: Start AnyConnect

-->
- <custom>
- <localization>
<languages>en,ja,zh,ru,ua</languages>
<default-language>en</default-language>
</localization>
- <auth-page>
- <window>
- <title-text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</title-text>
</window>
- <language-selector>
<mode>disable</mode>
<title l10n="yes">Language:</title>
- <language>
<code>en</code>
<text>English</text>
</language>
- <language>
<code>zh</code>
<text>??(Chinese)</text>
</language>
- <language>
<code>ja</code>
<text>??(Japanese)</text>
</language>
- <language>
<code>ru</code>
<text>???????(Russian)</text>
</language>
- <language>
<code>ua</code>
<text>??????????(Ukrainian)</text>
</language>
</language-selector>
- <logon-form>
- <title-text l10n="yes">
- <![CDATA[
Login
]]>
</title-text>
- <title-background-color>
- <![CDATA[
#666666
]]>
</title-background-color>
- <title-font-color>
- <![CDATA[
#ffffff
]]>
</title-font-color>
- <message-text l10n="yes">
- <![CDATA[
Please enter your username and password.
]]>
</message-text>
- <username-prompt-text l10n="yes">
- <![CDATA[
```

```
USERNAME:
]]>
</username-prompt-text>
- <password-prompt-text l10n="yes">
- <![CDATA[
PASSWORD:
]]>
</password-prompt-text>
<internal-password-prompt-text l10n="yes" />
<internal-password-first>no</internal-password-first>
- <group-prompt-text l10n="yes">
- <![CDATA[
GROUP:
]]>
</group-prompt-text>
- <submit-button-text l10n="yes">
- <![CDATA[
Login
]]>
</submit-button-text>
- <title-font-color>
- <![CDATA[
#ffffff
]]>
</title-font-color>
- <title-background-color>
- <![CDATA[
#666666
]]>
</title-background-color>
<font-color>#000000</font-color>
<background-color>#ffffff</background-color>
</logon-form>
- <logout-form>
- <title-text l10n="yes">
- <![CDATA[
Logout
]]>
</title-text>
- <message-text l10n="yes">
- <![CDATA[
Goodbye.
]]>
</message-text>
</logout-form>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</text>
<logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
- <![CDATA[
#ffffff
]]>
</background-color>
- <font-size>
- <![CDATA[
larger
]]>
```

```
</font-size>
- <font-color>
- <![CDATA[
#800000
]]>
</font-color>
- <font-weight>
- <![CDATA[
bold
]]>
</font-weight>
</title-panel>
- <info-panel>
<mode>disable</mode>
<image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
<image-position>above</image-position>
<text l10n="yes" />
</info-panel>
- <copyright-panel>
<mode>disable</mode>
<text l10n="yes" />
</copyright-panel>
</auth-page>
- <portal>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</text>
<logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
- <![CDATA[
#ffffff
]]>
</background-color>
- <font-size>
- <![CDATA[
larger
]]>
</font-size>
- <font-color>
- <![CDATA[
#800000
]]>
</font-color>
- <font-weight>
- <![CDATA[
bold
]]>
</font-weight>
</title-panel>
<browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
<access-network-title l10n="yes">Start AnyConnect</access-network-title>
- <application>
<mode>enable</mode>
<id>home</id>
<tab-title l10n="yes">Home</tab-title>
<order>1</order>
</application>
- <application>
```

```
<mode>enable</mode>
<id>web-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Web Applications
]]>
</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
Web Bookmarks
]]>
</url-list-title>
<order>2</order>
</application>
- <application>
<mode>enable</mode>
<id>file-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Browse Networks
]]>
</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
File Folder Bookmarks
]]>
</url-list-title>
<order>3</order>
</application>
- <application>
<mode>enable</mode>
<id>app-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Application Access
]]>
</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>net-access</id>
<tab-title l10n="yes">AnyConnect</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>help</id>
<tab-title l10n="yes">Help</tab-title>
<order>1000000</order>
</application>
- <toolbar>
<mode>enable</mode>
<logout-prompt-text l10n="yes">Logout</logout-prompt-text>
<prompt-box-title l10n="yes">Address</prompt-box-title>
<browse-button-text l10n="yes">Browse</browse-button-text>
</toolbar>
- <column>
<width>100%</width>
<order>1</order>
</column>
- <pane>
<type>TEXT</type>
<mode>disable</mode>
```

```
<title />
<text />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>IMAGE</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>HTML</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>RSS</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <url-lists>
<mode>group</mode>
</url-lists>
</portal>
</custom>
```

自定义帮助

ASA 在无客户端会话期间在应用窗格上显示帮助内容。每个无客户端应用窗格都用预定的文件名显示自己的帮助文件内容。例如，在 Application Access 面板上显示的帮助内容来自名称为 app-access-hlp.inc 的文件。表 17-2 显示了无客户端应用面板和帮助内容的预定文件名。

表 17-2　　无客户端应用

应用类型	面板	文件名
标准	Application Access	app-access-hlp.inc
标准	Browse Networks	file-access-hlp.inc
标准	AnyConnect Client	net-access-hlp.inc
标准	Web Access	web-access-hlp.inc
插件	MetaFrame Access	ica-hlp.inc

表 17-2　　无客户端应用 （续）

应用类型	面板	文件名
插件	Terminal Servers	rdp-hlp.inc
插件	Telnet/SSH Servers[1]	ssh,telnet-hlp.inc
插件	VNC Connections	vnc-hlp.inc

1. 此插件同时支持 sshv1 和 sshv2。

您可以自定义思科提供的帮助文件或用其他语言创建帮助文件。然后使用 Import 按钮将其复制到 ASA 的闪存中，以在后续无客户端会话期间显示。您还可以导出之前导入的帮助内容文件、自定义这些文件，然后将其重新导入到闪存中。

步骤 1　点击 **Import**，启动 Import Application Help Content 对话框，您可以在此处将要在无客户端会话期间显示的新帮助内容导入到闪存中。

步骤 2　（可选）点击 **Export**，检索之前导入的从表格中选择的帮助内容。

步骤 3　（可选）点击 **Delete**，删除之前导入的从表格中选择的帮助内容。

步骤 4　系统显示浏览器呈现的语言的缩写。此字段*不*是用于文件转换，而是指示文件中使用的语言。要确定与表格中缩写相关的语言的名称，请显示您浏览器呈现的语言的列表。例如，当您使用下列步骤之一时，对话框窗口将显示语言和相关语言代码：

- 打开 Internet Explorer，选择**工具 > Internet 选项 > 语言 > 添加**。
- 打开 Mozilla Firefox，选择**工具 > 选项 > 高级 > 常规**，点击语言旁边的**选择**，然后点击**选择要添加的语言**。

系统将提供导入帮助内容文件使用的文件名。

自定义思科提供的帮助文件

要自定义思科提供的帮助文件，您首先需要从闪存卡上获取该文件的副本。

步骤 1　使用浏览器与 ASA 建立一个无客户端会话。

步骤 2　通过将表 17-3 中 “安全设备闪存中的帮助文件的 URL”中的字符串追加到 ASA 的地址中，替换 *language* （如下所示），然后按 **Enter**。

表 17-3　　思科提供的无客户端应用帮助文件

应用类型	面板	安全设备闪存中帮助文件的 URL
标准	Application Access	/+CSCOE+/help/*language*/app-access-hlp.inc
标准	Browse Networks	/+CSCOE+/help/*language*/file-access-hlp.inc
标准	AnyConnect Client	/+CSCOE+/help/*language*/net-access-hlp.inc
标准	Web Access	/+CSCOE+/help/*language*/web-access-hlp.inc
插件	Terminal Servers	/+CSCOE+/help/*language*/rdp-hlp.inc
插件	Telnet/SSH Servers	/+CSCOE+/help/*language*/ssh,telnet-hlp.inc
插件	VNC Connections	/+CSCOE+/help/*language*/vnc-hlp.inc

language 指浏览器呈现的语言的缩写。它*不*是用于文件转换，而是指示文件中使用的语言。对于思科提供的英语帮助文件，请输入缩写 **en**。

以下地址示例显示了 Terminal Servers 帮助的英文版本：

https://*address_of_security_appliance***/+CSCOE+/help/en/rdp-hlp.inc**

步骤 3　选择 **File > Save (Page) As**。

注　请勿更改 File name 框中的内容。

步骤 4　将 Save as 类型选项改为 **Web Page, HTML only**，然后点击 **Save**。

步骤 5　用您的首选 HTML 编辑器自定义文件。

注　您可以使用大多数 HTML 标签，但是*请勿*使用定义文件及其结构的标签（例如，请勿使用 <html>、<title>、<body>、<head>、<h1>、<h2> 等标签。您可以使用 <b> 等字符标签和 <p>、<ol>、 以及 <li> 标签来构造内容。）

步骤 6　使用原始文件名和扩展名，将文件保存为仅 HTML。

步骤 7　确保文件名与表 17-4 中的文件名匹配并且没有多余的文件名扩展名。

返回到 ASDM 并选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization > Import**，将修改的帮助文件导入闪存中。

为思科未提供的语言创建帮助文件

使用标准 HTML 以其他语言创建帮助文件。建议为支持的每个语言创建单独的文件夹。

注　您可以使用大多数 HTML 标签，但是*请勿*使用定义文件及其结构的标签（例如，请勿使用 <html>、<title>、<body>、<head>、<h1>、<h2> 等标签。您可以使用 <b> 等字符标签和 <p>、<ol>、 以及 <li> 标签来构造内容。）

将文件另存为仅 HTML。使用 Filename 列中的文件名。

返回到 ASDM 并选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization > Import**，将新帮助文件导入闪存中。

导入/导出应用帮助内容

使用 Import Application Help Content 对话框将要在无客户端会话期间门户页面上显示的帮助文件导入到闪存中。使用 Export Application Help Content 对话框检索以前导入的帮助文件，以便随后进行编辑。

步骤 1　Language 字段是指定浏览器呈现的语言，而不是用于文件转换。（在 Export Application Help Content 对话框中此字段处于非活动状态。）点击 Language 旁边的点，然后双击包含 Browse Language Code 对话框中显示的语言的行。确认 Language Code 字段中的缩写与该行中的缩写匹配，然后点击 **OK**。

步骤 2　如果 Browse Language Code 对话框中未显示提供帮助内容所要求的语言，请执行以下操作

1. 显示您的浏览器呈现的语言列表和缩写。
2. 在 Language Code 字段输入该语言的缩写，然后点击 **OK**。或

   您也可以将其输入到这些点左侧的 Language 文本框中。

当您使用下列步骤之一时，对话框将显示语言和相关语言代码：

- 打开 Internet Explorer，选择**工具 > Internet 选项 > 语言 > 添加**。
- 打开 Mozilla Firefox，选择**工具 > 选项 > 高级 > 常规**，点击语言旁边的**选择**，然后点击**选择要添加的语言**。

步骤 3　如果您正在导入，请从 File Name 下拉列表中选择新的帮助内容文件。如果您正在导出，则该字段不可用。

步骤 4　配置源文件 （如果导入）或目标文件 （如果导出）的参数：

- Local computer - 指示源文件或目标文件是否位于本地计算机上：
  - Path - 确定源文件或目标文件的路径。
  - Browse Local Files - 点击即可浏览源文件或目标文件的本地计算机。
- Flash file system - 指示源文件或目标文件是否位于 ASA 上的闪存中：
  - Path - 确定闪存中源文件或目标文件的路径。
  - Browse Flash - 点击即可浏览源文件或目标文件的闪存。
- Remote server - 指示源文件或目标文件是否位于远程服务器上：
  - Path - 选择文件转换 （复制）方法，可选择 ftp、 tftp 或 http （仅限于导入），并指定其路径。

自定义思科提供的帮助文件

要自定义思科提供的帮助文件，您首先需要从闪存卡上获取该文件的副本。

步骤 1　使用浏览器与 ASA 建立一个无客户端会话。

步骤 2　通过将表 17-4 中 “安全设备闪存中的帮助文件的 URL”中的字符串追加到 ASA 的地址中，替换 *language* （如下所示），然后按 **Enter**。

表 17-4　　思科提供的无客户端应用帮助文件

应用类型	面板	安全设备闪存中帮助文件的 URL
标准	Application Access	/+CSCOE+/help/*language*/app-access-hlp.inc
标准	Browse Networks	/+CSCOE+/help/*language*/file-access-hlp.inc
标准	AnyConnect Client	/+CSCOE+/help/*language*/net-access-hlp.inc
标准	Web Access	/+CSCOE+/help/*language*/web-access-hlp.inc
插件	Terminal Servers	/+CSCOE+/help/*language*/rdp-hlp.inc
插件	Telnet/SSH Servers	/+CSCOE+/help/*language*/ssh,telnet-hlp.inc
插件	VNC Connections	/+CSCOE+/help/*language*/vnc-hlp.inc

language 指浏览器呈现的语言的缩写。它 *不*是用于文件转换，而是指示文件中使用的语言。对于思科提供的英语帮助文件，请输入缩写 **en**。

以下地址示例显示了 Terminal Servers 帮助的英文版本：

https://*address_of_security_appliance***/+CSCOE+/help/en/rdp-hlp.inc**

步骤 3　选择 **File > Save (Page) As**。

注　请勿更改 File name 框中的内容。

步骤 4　将 Save as 类型选项改为 “Web Page, HTML only”，然后点击 **Save**。

步骤 5　用您的首选 HTML 编辑器自定义文件。

注　您可以使用大多数 HTML 标签，但是*请勿*使用定义文件及其结构的标签 （例如，请勿使用 <html>、 <title>、 <body>、 <head>、 <h1>、 <h2> 等标签。您可以使用 <b> 等字符标签和 <p>、 、 以及 <li> 标签来构造内容。

步骤 6　使用原始文件名和扩展名，将文件保存为仅 HTML。

步骤 7　确保文件名与表 17-4 中的文件名匹配并且没有多余的文件名扩展名。

返回到 ASDM 并选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization > Import**，将修改的帮助文件导入闪存中。

为思科未提供的语言创建帮助文件

使用标准 HTML 以其他语言创建帮助文件。建议为支持的每个语言创建单独的文件夹。

注　您可以使用大多数 HTML 标签，但是*请勿*使用定义文件及其结构的标签（例如，请勿使用 <html>、<title>、<body>、<head>、<h1>、<h2> 等标签。您可以使用 <b> 等字符标签和 <p>、<ol>、 以及 <li> 标签来构造内容。

将文件另存为仅 HTML。使用表 17-5 中 Filename 列中的文件名。

返回到 ASDM 并选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization > Import**，将新帮助文件导入闪存中。

自定义书签帮助

ASA 为选择的每个书签在应用面板上显示帮助内容。您可以自定义这些帮助文件或创建其他语言的帮助文件。然后将其导入到闪存中，以便在后续会话期间显示这些帮助文件。您还可以检索之前导入的帮助内容文件、修改这些文件，然后将其重新导入到闪存中。

每个应用面板都用预定的文件名显示其自己的帮助文件内容。每个文件的预期位置在 ASA 的闪存内的 /+CSCOE+/help/*language*/ URL 中。表 17-5 显示了您可以为 VPN 会话保留的每个帮助文件的详细信息。

表 17-5　　VPN 应用帮助文件

应用类型	面板	安全设备闪存中帮助文件的 URL	思科是否提供了英文版的帮助文件？
标准	Application Access	/+CSCOE+/help/*language*/app-access-hlp.inc	是
标准	Browse Networks	/+CSCOE+/help/*language*/file-access-hlp.inc	是
标准	AnyConnect Client	/+CSCOE+/help/*language*/net-access-hlp.inc	是
标准	Web Access	/+CSCOE+/help/*language*/web-access-hlp.inc	是
插件	MetaFrame Access	/+CSCOE+/help/*language*/ica-hlp.inc	否
插件	Terminal Servers	/+CSCOE+/help/*language*/rdp-hlp.inc	是
插件	Telnet/SSH Servers	/+CSCOE+/help/*language*/ssh,telnet-hlp.inc	是
插件	VNC Connections	/+CSCOE+/help/*language*/vnc-hlp.inc	是

language 指浏览器呈现的语言的缩写。此字段*不*是用于文件转换，而是指示文件中使用的语言。要指定特定语言代码，请从您的浏览器呈现的语言列表复制语言缩写。例如，当您使用下列步骤之一时，对话框窗口将显示语言和相关语言代码：

- 打开 Internet Explorer，选择**工具 > Internet 选项 > 语言 > 添加**。
- 打开 Mozilla Firefox，选择**工具 > 选项 > 高级 > 常规**，点击语言旁边的**选择**，然后点击**选择要添加的语言**。

自定义思科提供的帮助文件

要自定义思科提供的帮助文件，您首先需要从闪存卡上获取该文件的副本。获取副本并按照如下步骤进行自定义：

步骤 1　使用浏览器与 ASA 建立一个无客户端 SSL VPN 会话。

步骤 2　通过将表 17-5 中“安全设备闪存中的帮助文件的 URL”中的字符串追加到 ASA 的地址中，然后按 **Enter**。

注　输入 **en** 替换 *language*，获取英文版帮助文件。

以下地址示例显示了 Terminal Servers 帮助的英文版本：

https://*address_of_security_appliance***/+CSCOE+/help/en/rdp-hlp.inc**

步骤 3　选择 **File > Save (Page) As**。

注　请勿更改 File name 框中的内容。

步骤 4　将 Save as 类型选项改为 **Web Page, HTML only**，然后点击 **Save**。

步骤 5　用您的首选 HTML 编辑器修改此文件。

注　您可以使用大多数 HTML 标签，但是*请勿*使用定义文件及其结构的标签。例如，请勿使用 <html>、 <title>、 <body>、 <head>、 <h1> 或 <h2>。您可以使用 <b> 等字符标签和 <p>、 、 以及 <li> 标签来构造内容。

步骤 6　使用原始文件名和扩展名，将文件保存为仅 HTML。

步骤 7　确保文件名与表 17-5 中的文件名匹配并且没有多余的文件名扩展名。

返回到 ASDM 并选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization > Import**，将新帮助文件导入闪存中。

为思科未提供的语言创建帮助文件

使用 HTML 以其他语言创建帮助文件。

建议为支持的每个语言创建单独的文件夹。

将文件另存为仅 HTML。使用表 17-5 中 “安全设备闪存中帮助文件的 URL”最后一个斜线后面的文件名。

请参阅下一节，导入要在 VPN 会话期间显示的文件。

限制

您可以使用大多数 HTML 标签，但是*请勿*使用定义文件及其结构的标签，例如，请勿使用 <html>、<title>、<body>、<head>、<h1> 或 <h2>。您可以使用 <b> 等字符标签和 <p>、<ol>、 以及 <li> 标签来构造内容。

了解语言转换

ASA 为整个无客户端 SSL VPN 会话提供语言转换。这包括登录、注销横幅以及在身份验证之后显示的插件和 AnyConnect 等门户页面。向远程用户显示的功能区域及其消息归入转换域。表 17-6 显示了转换域和转换的功能区域。

表 17-6　语言转换域选项

转换域	转换的功能区域
AnyConnect	在思科 AnyConnect VPN 客户端的用户界面上显示的消息。
banners	无客户端连接的 VPN 访问被拒绝时显示的消息。
CSD	思科安全桌面 (CSD) 的消息。
customization	登录和注销页面与门户页面上显示的消息以及用户可自定义的所有消息。
plugin-ica	Citrix 插件的消息。
plugin-rdp	远程桌面协议插件的消息。

转换域	转换的功能区域
plugin-rdp2	Java 远程桌面协议插件的消息。
plugin-telnet,ssh	Telnet 和 SSH 插件的消息。
plugin-vnc	VNC 插件的消息。
PortForwarder	向端口转发用户显示的消息。
url-list	用户为门户页面上的 URL 书签指定的文本。
webvpn	不可自定义的所有第7 层、 AAA 和门户消息。

ASA 包括每个域属于标准功能组成部分的转换表模板。插件的模板随附于插件中并定义其自己的转换域。

您可以导出转换域的模板，在您提供的 URL 位置创建模板的 XML 文件。此文件中该消息字段为空。您可以编辑消息并导入模板，创建位于闪存中的新转换表对象。

您还可以导出现有转换表。创建的 XML 文件将显示您之前编辑的消息。重新导入具有相同语言名称的此 XML 文件将创建一个新版的转换表对象，并覆盖以前的消息。

有些模板是静态的，而有些模板则根据 ASA 的配置而变化。因为您可以自定义无客户端用户的 *登录与注销页面，门户页面和 URL 书签*，**ASA 将动态生成 customization** 和 **url-list** 转换域模板，并且此模板将动态地反映您对这些功能区域的更改。

创建转换表后，就可用于您创建并应用于组策略或用户属性的自定义对象。除 AnyConnect 转换域外，转换表没有任何影响，消息不会在用户屏幕上转换，直到您创建自定义对象，确定该对象要使用的转换表，并指定将该自定义对象应用于组策略或用户。对 AnyConnect 域的转换表的更改会立即向 AnyConnect 客户端用户显示。

编辑转换表

步骤 1　导航至 **Configuration > Remote Access VPN > Language Localization**。当系统显示 Language Localization 窗格时，点击 **Add**。

步骤 2　从下拉框中选择 Language Localization Template。此框中的条目对应转换的功能区域。

步骤 3　为此模板指定语言。此模板即成为缓存中采用您指定的名称的转换表。使用与浏览器的语言选项兼容的缩写。例如，如果创建的是中文的表格并且使用的是 IE，请使用 IE 可识别的缩写 *zh*。

步骤 4　编辑转换表。对于 msgid 字段表示的要转换的每个消息，请在关联的 msgstr 字段的引号内输入转换的文本。下面的示例显示的是消息 Connected，其中 msgstr 字段为西班牙文本：

```
msgid "Connected"
msgstr "Conectado"
```

步骤 5　点击 **OK**。

添加转换表

您可以根据模板添加新转换表，也可以修改此窗格中已导入的转换表。

步骤 1　选择要修改的模板并将其用做新转换表的基础。模板归入转换域并影响功能的特定区域。表 17-6 显示了转换域和受影响的功能区域。（GUI Text 和 Messages 窗格上此字段显示为灰色）。

步骤 2　从下拉列表中选择转换域。（GUI Text 和 Messages 窗格上此字段显示为灰色）。

步骤 3　指定语言。使用与浏览器的语言选项兼容的缩写。 ASA 用该名称创建新的转换表。

步骤 4　使用编辑器更改消息转换。消息 ID 字段 (msgid) 包含默认转换。接在 msgid 之后的消息字符串字段 (msgstr) 提供转换。要创建转换，请在 msgstr 字符串的引号内输入转换的文本。例如，要使用西班牙转换选项来转换消息 “Connected”，请在 msgstr 引号内插入西班牙文本：

```
msgid "Connected"
msgstr "Conectado"
```

进行更改后，点击 **Apply** 导入转换表。

第 18 章 无客户端 SSL VPN 故障排除

关闭 Application Access 以防 hosts 文件错误

为防止出现可能会干扰 Application Access 的 hosts 文件错误，使用完 Application Access 之后请正确关闭 Application Access 窗口。为此，请点击关闭图标。

使用 Application Access 时从 hosts 文件错误中恢复

如未正确关闭 Application Access 窗口，可能会出现以下错误：

- 您下一次尝试启动 Application Access 时，它可能会关闭；您会收到 `Backup HOSTS File Found` 错误消息。
- 即使您在本地位置运行应用程序，这些应用程序也可能会关闭或出现故障。

不正确停止 Application Access 可能会导致这些错误。例如：

- 当您使用 Application Access 时，您的浏览器会崩溃。
- 当您使用 Application Access 时，电源会中断或系统会关闭。
- 您在工作时可以将 Application Access 窗口最小化，然后在此窗口处于活动状态（但是已最小化）的情况下关闭您的计算机。

- 了解 hosts 文件
- 错误停止 Application Access
- 使用无客户端 SSL VPN 自动重新配置主机的文件
- 手动重新配置 hosts 文件

了解 hosts 文件

您本地系统上的 hosts 文件会将 IP 地址映射到主机名上。当您启动 Application Access 时，无客户端 SSL VPN 将修改 hosts 文件，增加无客户端 SSL VPN 特定条目。通过正确关闭 Application Access 来停止 Application Access 可以让文件恢复其原始状态。

激活 Application Access 之前 ……	hosts 文件处于原始状态。
当 Application Access 启动时 ……	• 无客户端 SSL VPN 将 hosts 文件复制到 hosts.webvpn，从而创建备份。 • 无客户端 SSL VPN 然后编辑 hosts 文件，插入无客户端 SSL VPN 的特定信息。
当 Application Access 停止时 ……	• 无客户端 SSL VPN 将备份文件复制到 `hosts` 文件，从而将 hosts 文件恢复到其原始状态。 • 无客户端 SSL VPN 删除 hosts.webvpn。
完成 Application Access 后 ……	hosts 文件处于原始状态。

注　Microsoft 反间谍软件将拦截端口转发 Java 小程序对 hosts 文件的更改。有关使用反间谍软件时如何允许更改 hots 文件，请参阅 www.microsoft.com。

错误停止 Application Access

当 Application Access 异常停止时，`hosts` 文件将保持处于无客户端 SSL VPN 自定义的状态。下次您启动 Application Access 时，无客户端 SSL VPN 将通过搜索 hosts.webvpn 文件检查此状态。如果发现了一个，系统将显示 `Backup HOSTS File Found` 错误消息（图 18-1），并且 Application Access 将暂时关闭。

如果您错误地关闭 Application Access，您的远程访问客户端/服务器应用将处于不稳定状态。如果您尝试启动这些应用，而不使用无客户端 SSL VPN，它们可能会发生故障。您会发现自己通常连接的主机不可用。如果在家远程运行应用，并且在关闭计算机前未退出 Application Access 窗口，然后再尝试从办公室运行这些应用，通常会发生这种情况。

使用无客户端 SSL VPN 自动重新配置主机的文件

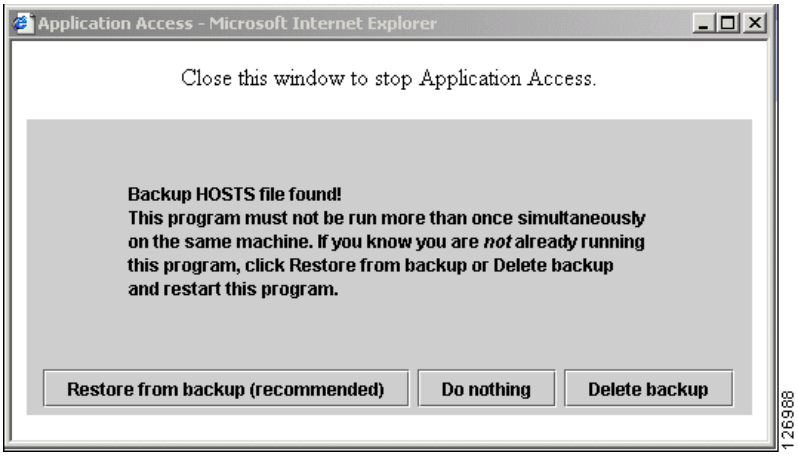
如果能够连接到远程访问服务器，请执行以下步骤以重新配置主机的文件并重新启用 Application Access 和应用。

详细步骤

步骤 1　启动无客户端 SSL VPN 并登录。系统将打开主页。

步骤 2　点击 **Applications Access** 链接。系统将显示 `Backup HOSTS File Found` 消息。（请参阅图 18-1。）

图 18-1　　Backup HOSTS File Found 消息



步骤 3　选择以下一个选项：

- **Restore from backup** - 无客户端 SSL VPN 强制执行正确的关闭操作。它会将 hosts.webvpn 备份文件复制到 `hosts` 文件，将其恢复原始状态，然后删除 hosts.webvpn。然后，您必须重新启动 Application Access。
- **Do nothing** - Application Access 不启动。系统重新显示远程访问主页。
- **Delete backup** - 无客户端 SSL VPN 删除 hosts.webvpn 文件，使 hosts 文件处于无客户端 SSL VPN 自定义状态。原始 `hosts` 文件设置将丢失。然后 Application Access 将启动，将无客户端 SSL VPN 自定义的 hosts 文件作为新的原始状态。只有在您不担心丢失 hotst 文件设置时，才可以选择此选项。如果您或您使用的程序在 Application Access 不正确关闭之后编辑了 hosts 文件，请选择一个其他选项或手动编辑 hosts 文件。（请参阅 “手动重新配置 hosts 文件”。）

手动重新配置 hosts 文件

如果您无法从当前位置连接到远程访问服务器，或者您已自定义 hosts 文件并且不想丢失您的编辑，请按照以下步骤重新配置 hosts 文件并重新启用 Application Access 和应用。

详细步骤

步骤 1　查找并编辑您的 hosts 文件。最常见的位置是 c:\windows\sysem32\drivers\etc\hosts。

步骤 2　检查是否有些行包含字符串：`# added by WebVpnPortForward` 如果任何行包含此字符串，则您的 hosts 文件是无客户端 SSL VPN 自定义的。如果您的 hosts 文件是无客户端 SSL VPN 自定义的，则它会类似于以下示例：

```
server1 # added by WebVpnPortForward
server1.example.com invalid.cisco.com # added by WebVpnPortForward
server2 # added by WebVpnPortForward
server2.example.com invalid.cisco.com # added by WebVpnPortForward
server3 # added by WebVpnPortForward
server3.example.com invalid.cisco.com # added by WebVpnPortForward

# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
```

```
# This file contains the mappings of IP addresses to hostnames.Each
# entry should be kept on an individual line.The IP address should
# be placed in the first column followed by the corresponding hostname.
# The IP address and the hostname should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     cisco.example.com          # source server
#       38.25.63.10     x.example.com              # x client host

123.0.0.1       localhost
```

步骤 3　删除包含此字符串的行：`# added by WebVpnPortForward`

步骤 4　保存并关闭文件。

步骤 5　启动无客户端 SSL VPN 并登录。

系统将显示主页。

步骤 6　点击 **Application Access** 链接。

系统将显示 Application Access 窗口。 Application Access 现已启动成功。

向无客户端 SSL VPN 用户发送管理员警报

步骤 1　在 ASDM 应用主窗口，选择 **Tools > Administrator's Alert Message to Clientless SSL VPN Users**。

系统将显示 Administrator's Alert Message to Clientless SSL VPN Users 对话框。

步骤 2　输入要发送的新的或已编辑的警报内容，然后点击 **Post Alert**。

步骤 3　要删除当前警报内容并输入新的警报内容，请点击 **Cancel Alert**。

第 19 章

无客户端 SSL VPN 许可

许可

注 此功能在无负载加密型号上不可用。

型号	许可证要求
ASA 5506-X	AnyConnect 高级版许可证： • *基础许可证：2 个会话。* • *增强型安全许可证：4 个会话。可选 SSL VPN 许可证：10 个会话。* *不支持共享许可证。*
ASA 5512-X	AnyConnect 高级版许可证： • *基础许可证：2 个会话。* • *可选永久性或基于时间的许可证：10、 25、 50、 100 或 250 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5515-X	AnyConnect 高级版许可证： • *基础许可证：2 个会话。* • *可选永久性或基于时间的许可证：10、 25、 50、 100 或 250 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5525-X	AnyConnect 高级版许可证： • *基础许可证：2 个会话。* • *可选永久性或基于时间的许可证：10、 25、 50、 100、 250、 500 或 750 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*

型号	许可证要求
ASA 5545-X	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000 或 2500 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5555-X	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500 或 5000 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5585-X，带 SSP-10	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500 或 5000 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5585-X，带 SSP-20、 -40 和 -60	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500、5000 或 10000 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASASM	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500、5000 或 10000 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASAv5	标准版许可证：250 个会话。
ASAv10	• 标准版许可证：(9.3(1)) 2 个会话。 (9.3(2)) 250 个会话。 • 高级版许可证：250 个会话。
ASAv30	• 标准版许可证：(9.3(1)) 2 个会话。 (9.3(2)) 750 个会话。 • 高级版许可证：750 个会话。

如果您启动无客户端 SSL VPN 会话，然后从门户启动 AnyConnect 客户端会话，总计使用的是 1 个会话。但是，如果先启动 AnyConnect 客户端 （例如从独立客户端启动），然后登录无客户端 SSL VPN 门户，则使用的是 2 个会话。

*所有*类型的最大组合 VPN 会话数量不能超过此表中所示的最大会话数。

（AnyConnect 4 及更高版本）：同步用户数量和 VPN 功能由 AnyConnect 许可证控制，可单独提供。在 ASA 上会启用最高级别的 VPN 许可证。

（AnyConnect 3 或更早版本）一个共享许可证允许 ASA 用作多个客户端 ASA 的共享许可证服务器。共享许可证池很大，但是，每个 ASA 使用的会话数不能超过永久许可证列出的最大数量。