流传感器和
负载均衡器集成指南

(适用于 Stealthwatch 系统 v6.9.2)

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系获取副本。

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

无论在该手册中是否作出了其他担保，来自这些供应商的所有文档文件和软件都按“原样”提供且仍有可能存在缺陷。思科和上面所提及的供应商拒绝所有明示或暗示的保证，包括（但不限于）适销性、特定用途适用性和无侵权保证，或者因买卖或使用以及商业惯例所引发的保证。

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

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

所有打印副本和软拷贝均被视为非受控副本，应以原始在线版本为最新版本。

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 中列有各办事处的地址、电话和传真。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问以下网址：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。使用“合作伙伴”一词并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

© 2017 思科系统公司。版权所有。

目录

简介

如果负载均衡器安装在网络中的资源前面，则会降低可视性，并可能减少对 Stealthwatch 系统中威胁的检测。

请按照本指南中的说明配置负载均衡器和流传感器。此配置将客户端流和服务器端流联系在一起，因此外部主机得以与内部主机相连，从而在流传感器和 Stealthwatch 系统上提供可视性并增强安全性。

目标读者

本指南的主要受众包括负责配置 Stealthwatch 系统的管理员。

准备工作

在开始本指南中的步骤之前，应执行以下操作：

- 确认您的 Stealthwatch 系统正在通信。转到 SMC 客户端界面。检查“警报表”，确保没有活跃的“管理通道故障”或“故障切换通道故障”警报。
- 确认您的 Stealthwatch 系统设备许可证处于有效状态。

联系支持人员

如果需要技术支持人员，请执行以下操作之一：

- 联系您当地的思科合作伙伴
- 联系思科 Stealthwatch 支持
- 通过以下网址反映问题：http://www.cisco.com/c/en/us/support/index.html
- 通过以下电子邮件反映问题：tac@cisco.com
- 美国支持电话：1-800-553-2447
- 全球的支持电话：www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html
- 通过 Stealthwatch 客户社区网站反映问题 (https://lancope.force.com/Customer/CustomerCommLogin)。

©2017 年 思科系统公司。版权所有。

配置负载均衡器

请按照以下说明配置负载均衡器。您将禁用 HTTP 的 X-Forwarded-For (XFF) 选项，创建 iRule，并启用虚拟服务器资源。如果您希望使用现有的 iRule，可以使用此处提供的信息对其进行修改。为了确保成功集成，请对网络中的所有负载均衡器执行本节中的说明。

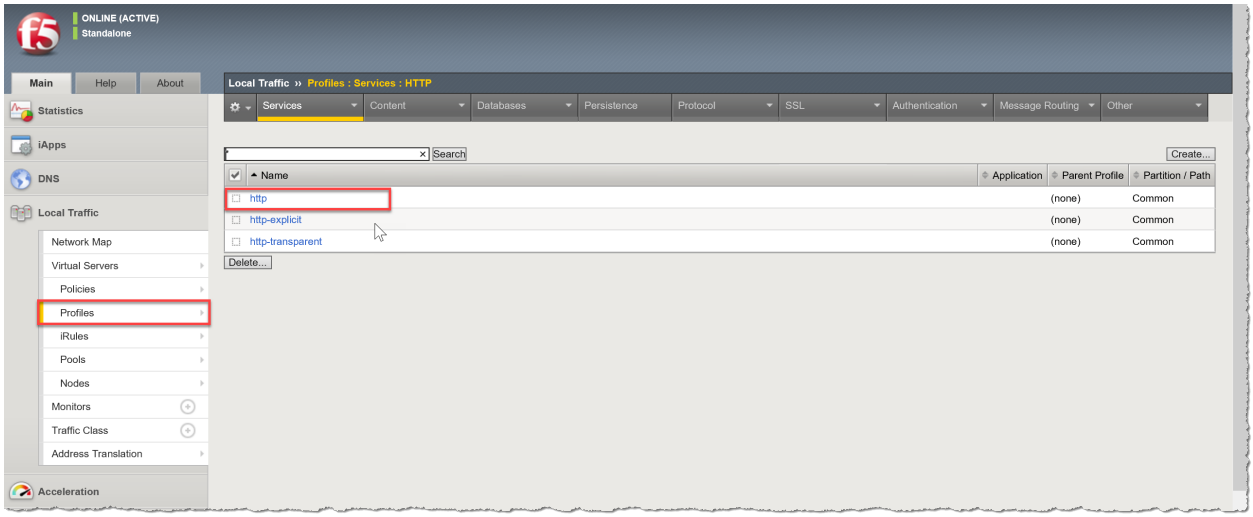
> **注意：**本指南中的说明将使用 F5 负载均衡器上的配置作为示例，但我们认为此配置可用于所有类型的负载均衡器。

禁用 HTTP 的 XFF 选项

请按照以下过程禁用 HTTP 的 XFF 选项。

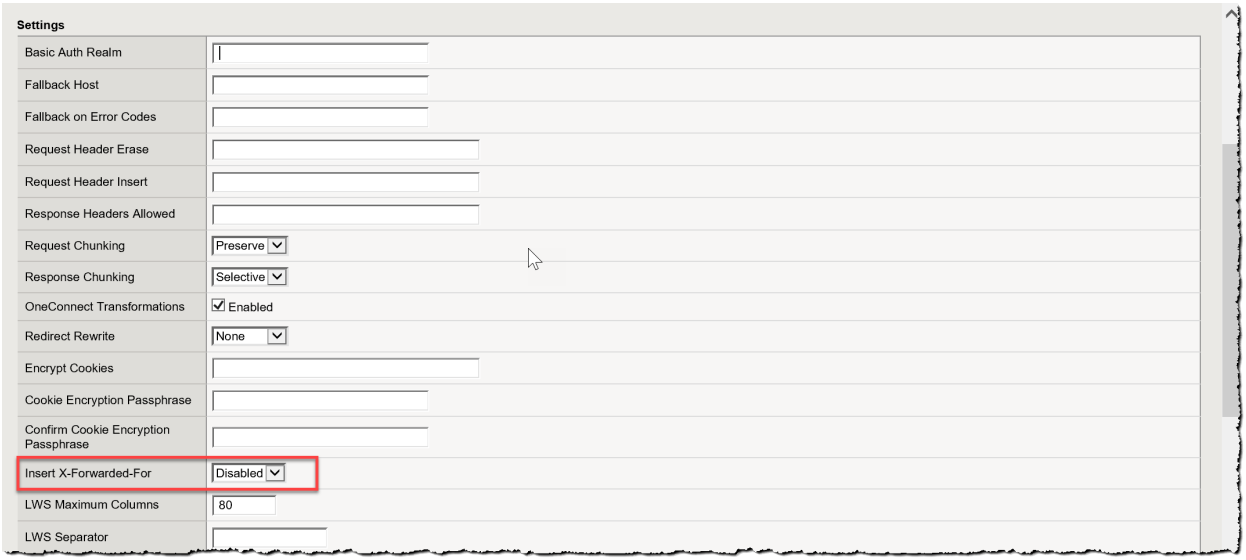
必须在 F5 负载均衡器中禁用可将数据插入 XFF HTTP 报头的内置功能，具体如下所示：

1. 登录 F5 负载均衡器配置实用程序。
2. 在“主”选项卡下，点击**本地流量**。
3. 依次点击**配置文件 > 服务 > HTTP**。
   如果“服务”菜单中未显示 HTTP，则跳到步骤 8。



4. 点击 **http**。
5. 在“设置”下，找到**插入 X-Forwarded-For**。
6. 在下拉列表中选择**已禁用**(或取消选中**已启用**复选框以清除设置)。

©2017 年 思科系统公司。版权所有。



7. 单击**“更新”**按钮。
8. 在**服务**菜单中，点击**快速 HTTP**。
   如果“服务”菜单中的“快速 HTTP”不可用，则跳过本节的其余部分。继续创建 iRule。
9. 找到**插入 X-Forwarded-For**。
10. 在下拉列表中选择**已禁用**(或取消选中**已启用**复选框以清除设置)。
11. 点击**更新**按钮保存并退出。
12. 继续创建 iRule。

创建 iRule

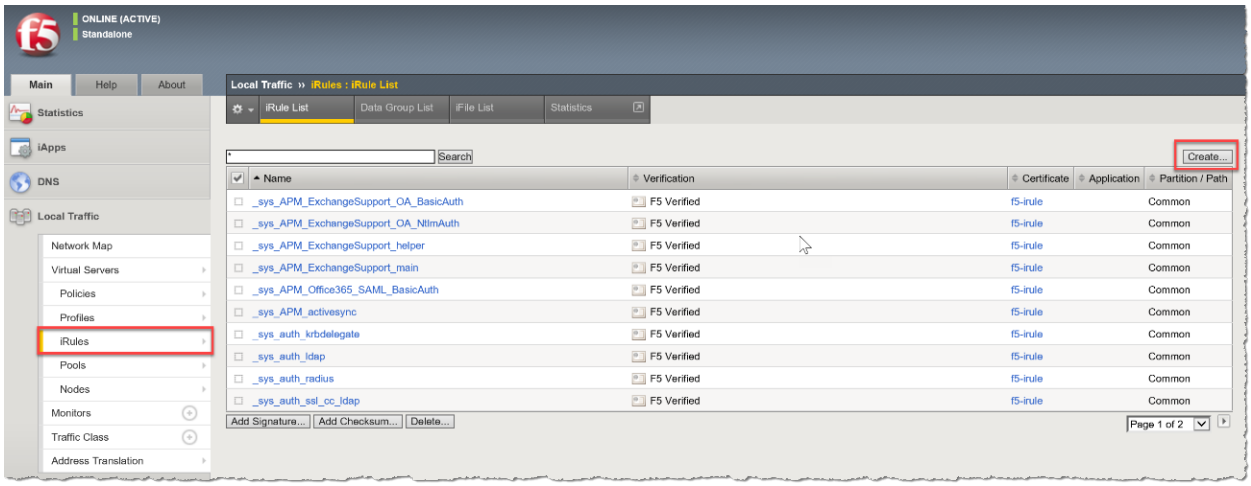
请按照以下说明为 XFF 报头添加 iRule。此过程用于映射负载均衡器 IP 并确保向流传感器报告准确的端口和协议信息。

注意：如果您希望使用现有的 iRule，可以使用此处提供的信息对其进行修改。

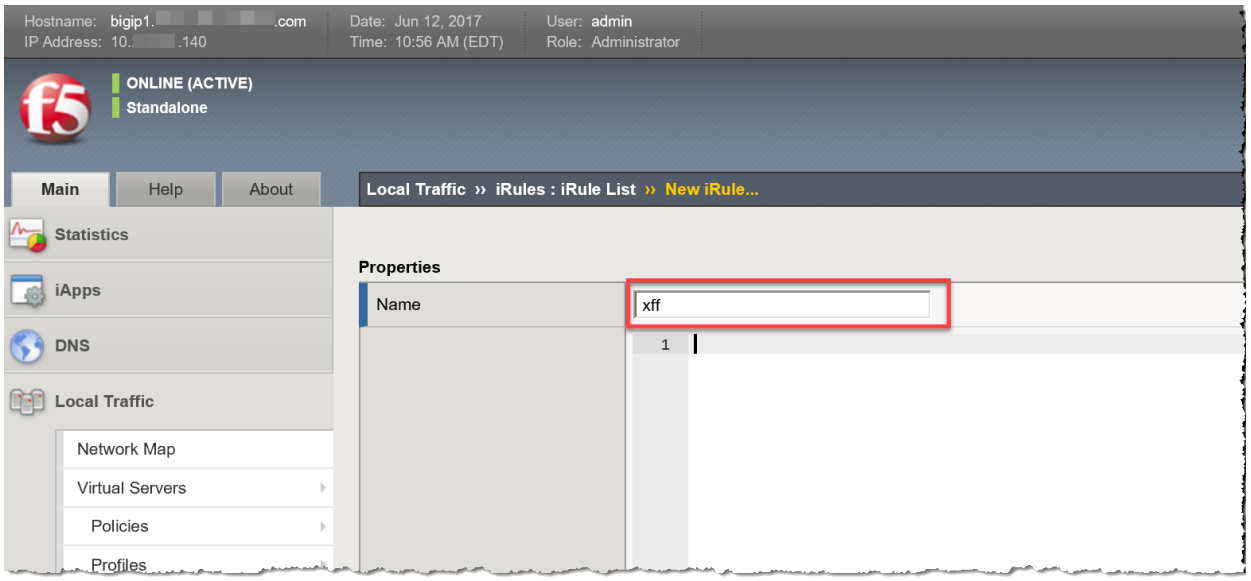
要在 F5 负载均衡器中为 XFF 报头创建 iRule，请完成以下步骤：

1. 在“主”选项卡下，点击**本地流量**。
2. 点击 **iRule**。
3. 点击**创建**按钮。

©2017 年 思科系统公司。版权所有。



4. 在**名称**字段中，输入 **xff**。



续...

©2017年 思科系统公司。版权所有。

5. 将以下文本复制并粘贴到**定义**字段中：

```
when CLIENT_ACCEPTED {
    if { [PROFILE::exists clientssl] } then {
        set client_protocol "https"
        set local_port 443
    } else {
        set client_protocol "http"
        set local_port 80
    }
}
when HTTP_REQUEST {
    if { [HTTP::header exists "X-Forwarded-For"] } {
        HTTP::header replace X-Forwarded-For "[HTTP::header X-Forwarded-For], [IP::client_addr]"
    } else {
        HTTP::header insert "X-Forwarded-For" [IP::client_addr]
    }
    if { [HTTP::header exists "X-Forwarded-Proto"] } {
        HTTP::header replace X-Forwarded-Proto "[HTTP::header X-Forwarded-Proto], $client_protocol"
    } else {
        HTTP::header insert "X-Forwarded-Proto" $client_protocol
    }
    if { [HTTP::header exists "X-Forwarded-Port"] } {
        HTTP::header replace X-Forwarded-Port "[HTTP::header X-Forwarded-Port], [TCP::client_port]"
    } else {
        HTTP::header insert "X-Forwarded-Port" [TCP::client_port]
    }
    if { [HTTP::header exists "X-Forwarded-Host"] } {
        HTTP::header replace X-Forwarded-Host "[HTTP::header X-Forwarded-Host], [IP::local_addr]:$local_port"
    } else {
        HTTP::header insert "X-Forwarded-Host" [IP::local_addr]:$local_port
    }
}
```

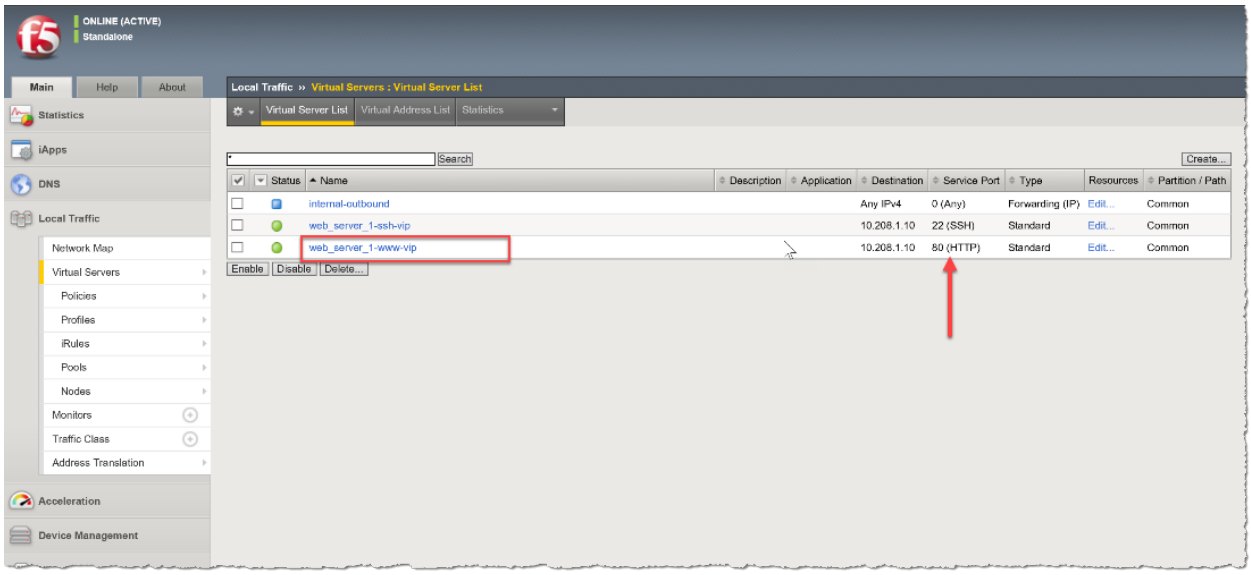
6. 点击**已完成**按钮保存并退出。
7. 继续将 iRule 添加为虚拟服务器资源。

将 iRule 添加为虚拟服务器资源

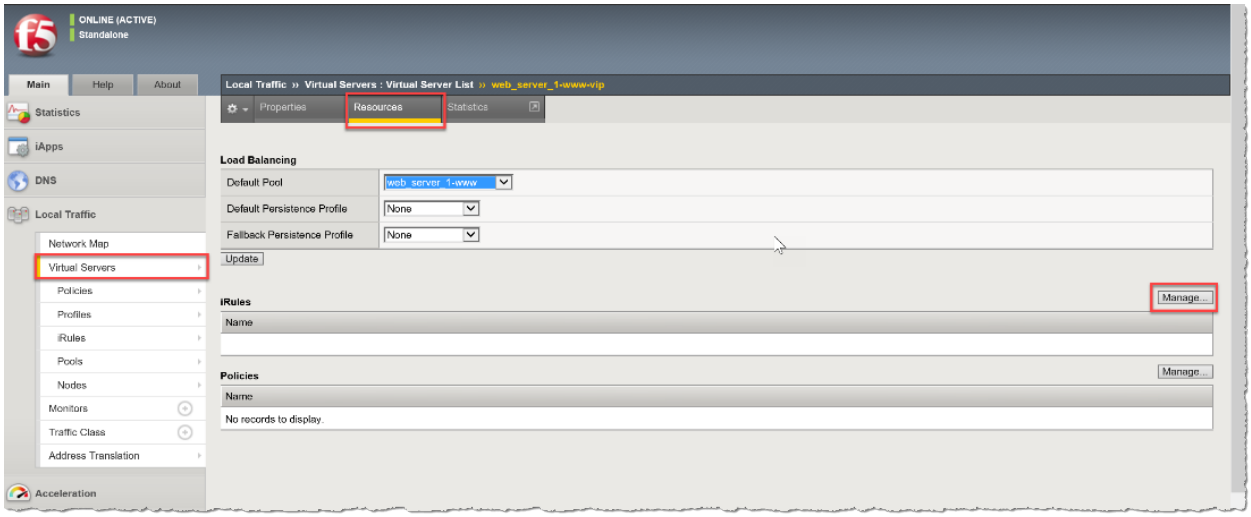
要启用虚拟服务器，必须将新的 XFF iRule 作为资源添加到 F5 负载均衡器中。通过执行此步骤，可使负载均衡器能够报告 XFF 报头。

©2017 年 思科系统公司。版权所有。

1. 在“主”选项卡下，点击**本地流量**。
2. 点击**虚拟服务器**。
3. 找到**服务端口**列，并查找正在处理由设备处理的流量的**服务端口 80 (HTTP)** 或 **443 (HTTPS)**。点击**虚拟服务器**名称。

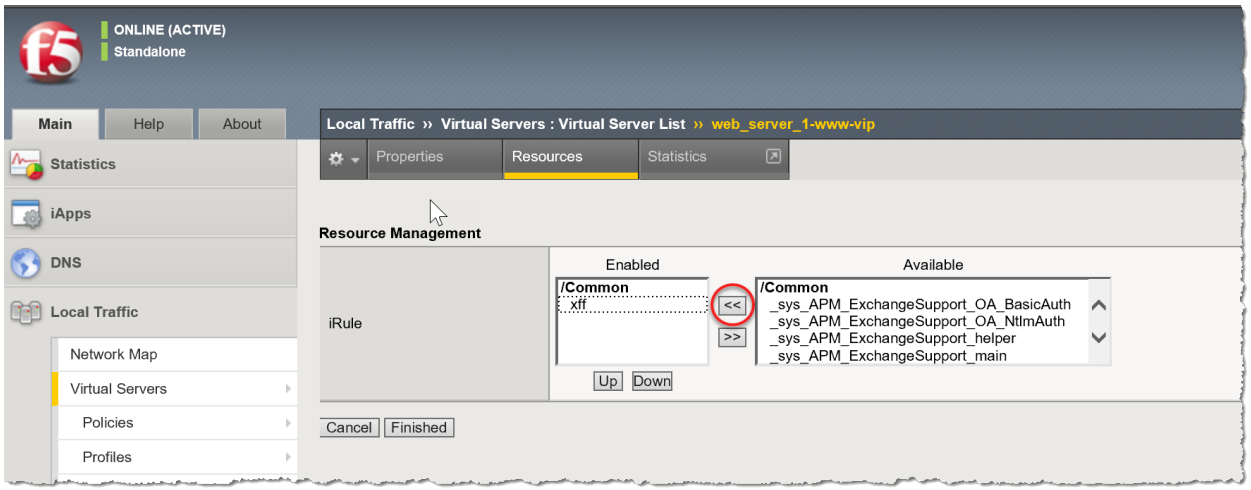


4. 点击 **Resources** 选项卡。
5. 在“iRule”部分中，点击**管理**按钮。



6. 滚动浏览“可用 iRule”，找到新的 XFF iRule。点击**XFF** iRule，将其选中。
7. 点击 **<<** 按钮，将 XFF iRule 添加到**已启用**框中。

©2017 年 思科系统公司。版权所有。



8. 点击**已完成**按钮保存并退出。

配置网络中的所有负载均衡器

如果网络上连接有多个负载均衡器，请在执行在流传感器上启用 XFF 处理之前，对每个负载均衡器执行“配置负载均衡器”一节中前述的说明。

通过配置每个负载均衡器，可保留 XFF 信息并将其附加到负载均衡器中。在此配置中，流传感器将仅报告转换的主机中的原始负载均衡器 IP。

配置负载均衡器相关说明包括以下内容：

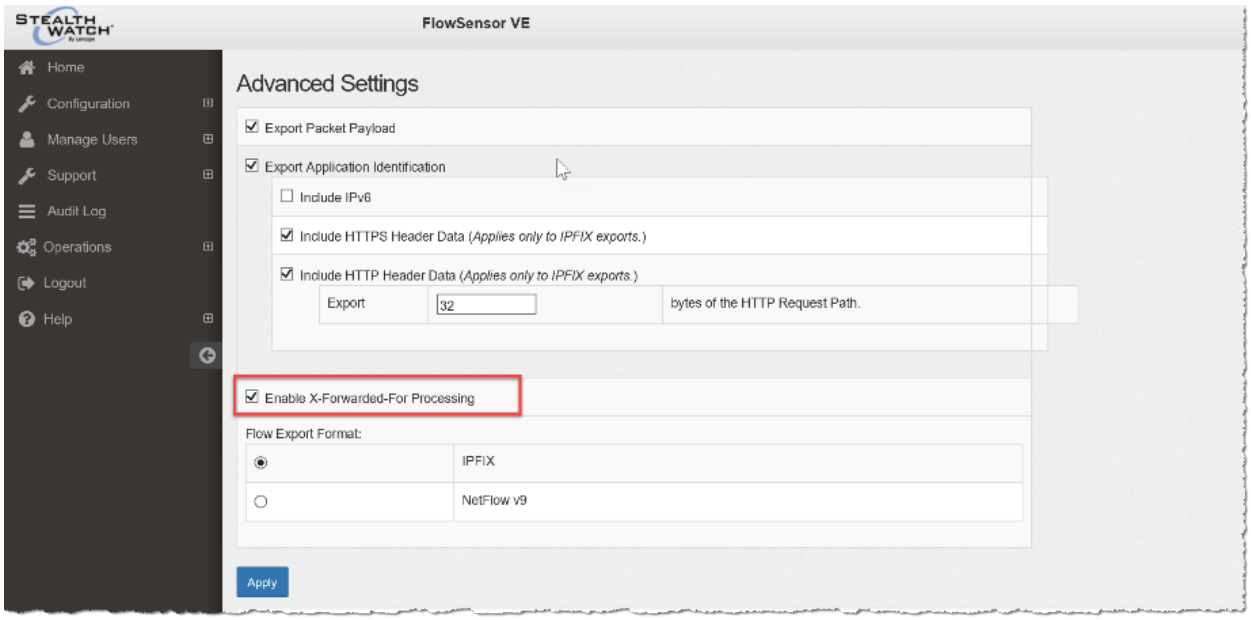
- 禁用 HTTP 的 XFF 选项
- 创建 iRule
- 将 iRule 添加为虚拟服务器资源

©2017 年 思科系统公司。版权所有。

在流传感器上启用 XFF 处理

要在流传感器上处理 XFF 报头字段，请完成以下步骤：

1. 登录流传感器。
2. 单击**Configuration**。
3. 单击 **Advanced Settings** 。
4. 选中**启用 X-Forwarded-For 处理**复选框。



5. 点击**应用**按钮。
6. 对网络中获得负载均衡器支持的所有流传感器重复执行上述说明。
7. 继续验证配置。

©2017 年 思科系统公司。版权所有。

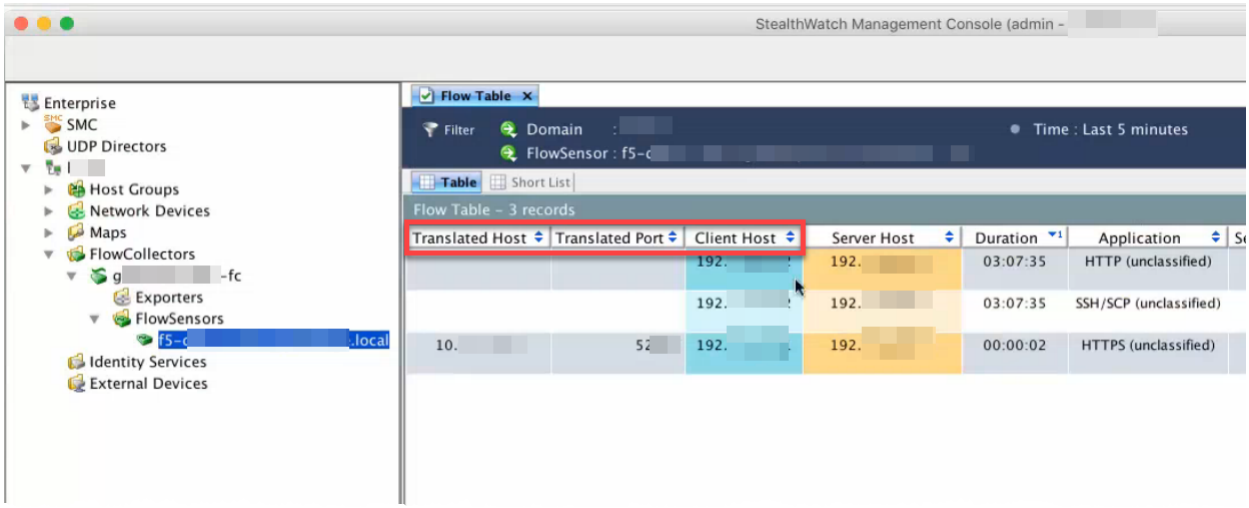
验证配置

要验证负载均衡器配置，请登录 SMC 桌面客户端或 SMC Web 客户端。SMC 桌面客户端提供负载均衡器 IP 地址和端口，SMC Web 客户端提供负载均衡器 IP 地址。

验证 SMC 桌面客户端中的配置

请按照以下说明查看 SMC 桌面客户端中的负载均衡器 IP 地址和端口。

1. 在服务器(位于 F5 负载均衡器后面)上打开一个网页。
2. 登录 SMC 桌面客户端。
3. 在“企业树”中找到流传感器。右键点击流传感器名称(或 IP 地址)。
4. 依次点击**流 > 流表**。
5. 查看“转换的主机”列和“转换的端口”列，确认已显示 F5 负载均衡器 IP 地址和端口。
    - 转换的主机(负载均衡器 IP 地址)
    - 转换的端口(负载均衡器端口)



将列添加到流表(SMC 桌面客户端)

如果 SMC 桌面客户端“流表”中未显示“转换的主机”列和“转换的端口”列，请完成以下步骤：

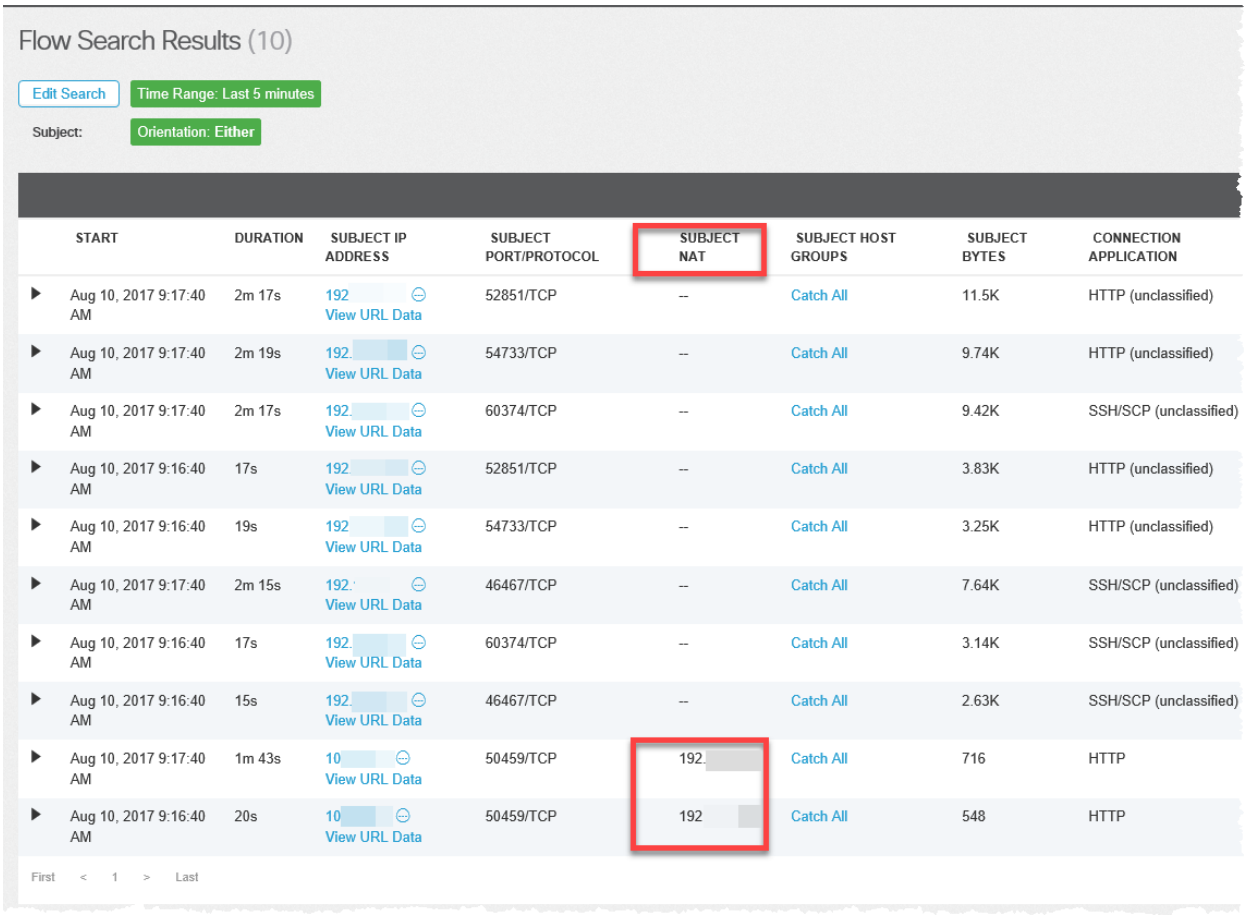
1. 右键点击任意列。
2. 滚动浏览列表。选择**更多**，直至滚动到字母 T。
3. 点击**转换的主机**和**转换的端口**，将其添加到流表中。

©2017 年 思科系统公司。版权所有。

验证 SMC Web 客户端中的配置

请按照以下说明查看 SMC Web 客户端中的负载均衡器 IP 地址。转换的端口在 SMC Web 客户端中不可用。请参阅验证 SMC 桌面客户端中的配置以验证端口。

1. 在服务器(位于 F5 负载均衡器后面)上打开一个网页。
2. 登录 SMC。
3. 依次点击**分析 > 流搜索**。
4. 点击 **Search**。
5. 当流搜索结果显示流时，点击**管理列**。
6. 点击复选框，向**对等点 NAT** 和**主题 NAT** 添加复选标记。
7. 单击**“设置”**。
8. 确认“对等点 NAT”列或“主题 NAT”列中已显示负载均衡器 IP 地址。
   列是由流方向决定的。



©2017 年 思科系统公司。版权所有。

©2017年思科系统公司。版权所有。