配置网络安全

关于网络安全模块

AnyConnect 网络安全模块是将 HTTP 流量路由至思科云网络安全扫描代理的终端组件。

思科云网络安全解构网页的元素，以便同时分析各个元素。例如，如果特定网页包含 HTTP、闪存和 Java 元素，则单独的“scanlets”会并行分析这些元素中的每一个。然后，思科云网络安全基于 Cisco ScanCenter 管理门户中定义的安全策略接受良好或可接受的内容并阻止恶意或不可接受的内容。这样，当整个网页因少数内容不可接受而被限制时，可防止“过度阻止”；当整个网页获准但其中仍有一些不可接受或可能有害的内容正通过网页传递时，可防止“阻止不力”。当用户进入或离开企业网络时，思科云网络安全都会保护用户。

全球有很多思科云网络安全扫描代理，用户可以利用 AnyConnect 网络安全将其流量路由至思科云网络安全扫描代理，该代理将以最快的速度响应，从而最小化延迟。

您可以配置“安全值得信赖的网络检测”功能以识别处于企业局域网中的终端。如果启用此功能，来自企业局域网的任何网络流量会绕过思科云网络安全扫描代理。流量安全是通过企业局域网中的其他方法和设备进行管理的，而不是通过思科云网络安全。

AnyConnect 网络安全功能是使用 AnyConnect 网络安全客户端配置文件配置的，您可以使用 AnyConnect 配置文件编辑器对其进行编辑。

Cisco ScanCenter 是思科云网络安全的管理门户。使用 Cisco ScanCenter 创建或配置的某些组件也会纳入 AnyConnect 网络安全客户端配置文件。

注释 ISE 服务器必须始终列在静态例外列表中，该列表在网络安全客户端配置文件的“例外”(Exceptions) 窗格中配置。

典型网络安全配置

过程

步骤 1 配置客户端配置文件中的思科云网络安全扫描代理。

步骤 2 （可选）如果在配置文件编辑器内将现有思科云网络安全扫描代理列表与从 http://www.scansafe.cisco.com/ 网站下载的扫描代理列表进行比较，会显示出差异，则更新扫描代理列表。

步骤 3 （可选）向用户显示或隐藏扫描代理。

步骤 4 选择默认扫描代理。

步骤 5 （可选）指定 HTTP(S) 流量侦听端口以过滤 HTTPS 网络流量。

步骤 6 配置 排除或包含来自网络扫描服务的终端流量的主机、代理或静态例外。此配置会限制对来自指定 IP 地址的网络流量的评估。

步骤 7 配置用户控制和计算最快的扫描代理响应时间。此配置用于选择您希望用户连接的思科云网络安全扫描代理。

步骤 8 如果要使源自公司局域网的网络流量绕过思科云网络安全扫描代理，请使用安全值得信赖的网络检测。

步骤 9 配置身份验证和将组成员身份发送到思科云网络安全代理。此配置根据用户的企业域或 Active Directory 组的 Cisco ScanCenter 对用户进行身份验证。

客户端配置文件中的思科云网络安全扫描代理

思科云网络安全分析网络内容，允许根据安全策略向浏览器传输无害内容并且阻止恶意内容。扫描代理是思科云网络安全在其上分析网络内容的思科云网络安全代理服务器。AnyConnect 网络安全配置文件编辑器中的扫描代理面板定义 AnyConnect 网络安全模块向哪些思科云网络安全扫描代理发送网络流量。

IPv6 网络流量指南

除非指定了 IPv6 地址、域名、地址范围或通配符的异常情况，否则会向扫描代理发送 IPv6 网络流量。扫描代理执行 DNS 查找可查看是否存在用户尝试访问的 URL 的 IPv4 地址。如果扫描代理找到了 IPv4 地址，它会使用该地址进行连接。如果找不到 IPv4 地址，将放弃连接。

要让所有 IPv6 流量绕过扫描代理，请为所有 IPv6 流量添加 ::/0 静态异常。此异常使所有 IPv6 流量绕过所有扫描代理。因此，IPv6 流量不会受到网络安全保护。

注释 在运行 Windows 的计算机上，如果 AnyConnect 无法确定用户 ID，则会将内部 IP 地址用作用户 ID。例如，如果未指定 enterprise_domains 配置文件条目，则使用内部 IP 地址在 Cisco ScanCenter 中生成报告。

在运行 Mac OS X 的计算机上，如果 Mac 绑定到某个域，网络安全模块可以报告计算机所登录的域。如果 Mac 未绑定到域，网络安全模块可以报告 Mac 的 IP 地址或当前登录的用户名。

用户如何选择扫描代理

根据配置文件的配置方式，用户可选择扫描代理，或者通过 AnyConnect 网络安全模块连接到具有最快响应时间的扫描代理。

- 如果客户端配置文件允许用户控制，用户可以从 Cisco AnyConnect Secure Mobility Client网络安全托盘的“设置”选项卡中选择扫描代理。
- 如果客户端配置文件启用了“自动扫描代理选择”(Automatic Scanning Proxy Selection) 首选项，AnyConnect 网络安全将以最快到最慢的顺序对扫描代理排序，并将用户连接到具有最快响应时间的扫描代理。
- 如果客户端配置文件不允许用户控制，但启用了**自动扫描代理选择 (Automatic Scanning Proxy Selection)**，AnyConnect 网络安全会将用户从默认扫描代理切换至具有最快响应时间的扫描代理，前提是响应时间明显快于用户最初连接到的默认扫描代理。
- 如果用户开始从当前扫描代理漫游，并且在客户端配置文件中配置了**自动扫描代理选择 (Automatic Scanning Proxy Selection)**，AnyConnect 网络安全会将用户切换到新扫描代理，前提是其响应时间明显快于当前扫描代理。

用户清楚他们连接到的扫描代理，因为 AnyConnect 网络安全在 Windows 的展开的 AnyConnect 托盘图标中、“高级设置”(Advanced Settings) 选项卡和 AnyConnect GUI 的“高级统计信息”(Advanced Statistics) 选项卡上显示了启用的扫描代理名称。

更新扫描代理列表

网络安全配置文件编辑器的扫描代理列表不可编辑，您无法在网络安全配置文件编辑器的表中添加或删除思科云网络安全扫描代理。

网络安全配置文件编辑器启动后，会通过访问思科云网络安全网站（该网站维护扫描代理的当前列表）来自动更新扫描代理列表。

添加或编辑 AnyConnect 网络安全客户端配置文件时，配置文件编辑器将现有思科云网络安全扫描代理列表与从 http://www.scansafe.cisco.com 下载的扫描代理列表进行比较。如果列表过时，会显示 Scanning Proxy list is out of date 消息以及标有 Update List 的命令按钮。单击 **Update List** 可使用最新的思科云网络安全扫描代理列表更新扫描代理列表。

单击 Update List 时，配置文件编辑器会尽可能保持现有配置。配置文件编辑器会保留现有思科云网络安全扫描代理的默认扫描代理设置和显示/隐藏设置。

向用户显示或隐藏扫描代理

在用户建立了到 ASA 的 VPN 连接后，ASA 会将客户端配置文件下载到终端设备。AnyConnect 网络安全客户端配置文件确定向用户显示哪些思科云网络安全扫描代理。

为了使漫游用户获得最大利益，我们建议您向所有用户显示所有思科云网络安全扫描代理。

用户采用以下方式，与 AnyConnect 网络安全客户端配置文件扫描代理列表中标示为 Display 的扫描代理进行交互：

- 在其 Cisco AnyConnect Secure Mobility Client 界面的网络安全面板的“高级”设置中向用户显示思科云网络安全扫描代理。
- 按响应时间对扫描代理进行排序时，AnyConnect 网络安全模块会测试标示为“Display”的思科云网络安全扫描代理。
- 如果其配置文件允许用户控制，用户可以选择所连接的思科云网络安全扫描代理。
- 按响应时间对扫描代理进行排序时，AnyConnect 网络安全客户端配置文件扫描代理表格中标示为“Hide”的思科云网络安全扫描代理不会向用户显示，也不会进行评估。用户无法连接至标示为“Hide”的扫描代理。

开始之前

创建一个 AnyConnect 网络安全客户端配置文件。

过程

步骤 1 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**。
- 在 Windows 单机型号下，选择 **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**。

步骤 2 打开要编辑的网络安全客户端配置文件。

步骤 3 要隐藏或显示思科云网络安全扫描代理，请执行以下操作：

- 选择要隐藏的扫描代理并单击 Hide。
- 选择要显示的扫描代理名称，然后单击 Display。建议配置为显示所有思科云网络安全扫描代理。

步骤 4 保存 AnyConnect 网络安全客户端配置文件。

选择默认扫描代理

当用户首次连接网络时，用户会被路由到其默认扫描代理。默认情况下，您创建的配置文件具有以下思科云网络安全扫描代理属性：

- 扫描代理列表填入的是用户有权访问的所有思科云网络安全扫描代理，并且它们都标记为“Display”。
- 已预先选择一个默认的思科云网络安全扫描代理。
- 在侦听 HTTP 流量的 AnyConnect 网络安全模块的端口列表中调配若干端口。

过程

步骤 1 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**。
- 在 Windows 单机型号下，选择 **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**。

步骤 2 打开要编辑的网络安全客户端配置文件。

步骤 3 从**默认扫描代理**字段选择默认扫描代理。

步骤 4 保存 AnyConnect 网络安全客户端配置文件。

指定 HTTP(S) 流量侦听端口

默认情况下，扫描安全网络扫描服务会分析 HTTP 网络流量，因此，您可以通过配置过滤 HTTPS 网络流量。在网络安全客户端配置文件中，指定面对这些网络流量类型，要让网络安全“侦听”哪些端口。

过程

步骤 1 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**。
- 在 Windows 单机型号下，选择 **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**。

步骤 2 打开要编辑的网络安全客户端配置文件。

步骤 3 在 **Traffic Listen Port** 字段中，输入面向 HTTP 流量和/或 HTTPS 流量，要让网络安全模块“侦听”的逻辑端口号。

步骤 4 保存网络安全客户端配置文件。

配置 Windows Internet 选项以配置公共代理

公共代理通常用于将网络流量匿名化。公共代理服务器称为身份验证代理服务器，并且可能需要用户名和密码。AnyConnect 网络安全支持两种类型的身份验证：基本和 NTLM。当代理服务器配置为需要身份验证时，AnyConnect 网络安全会在运行时检测代理并管理身份验证过程。成功对代理服务器进行身份验证后，AnyConnect 网络安全通过公共代理将网络流量路由到思科云网络安全扫描代理：AnyConnect 网络安全加密代理凭证，将其安全缓存在内存中，并且不再需要凭证，即使用户从代理访问非代理网络并返回到同一网络也如此。无需重新启动服务即可与公共代理结合使用。当用户移至非代理网络时，AnyConnect 网络安全在运行时自动对其进行检测，并开始将网络流量直接发送到思科云网络安全扫描代理。

当 Windows Internet 选项被配置为在客户端上使用公共代理时，AnyConnect 将使用该连接。

注释 在 Windows 上支持基本和 NTLM 公共代理。在 Mac 上仅支持基本公共代理。

1. 从 Internet Explorer 或控制面板打开 Internet Options。
2. 选择 Connections 选项卡，然后单击 **LAN settings**。
3. 将 LAN 配置为使用代理服务器。
4. 输入代理服务器的 IP 地址或主机名。如果为 FTP/HTTP/HTTPS 配置了单独的代理，则仅考虑 HTTPS 代理。

限制

- 不支持基于 IPv6 和 TND 的公共代理。
- 在 AnyConnect 网络安全异常列表中不应包含代理 IP。否则，不会将流量定向到 AnyConnect 网络安全。
- 如果代理端口与默认 Web 端口不同，则需要在 AnyConnect 网络安全配置文件的 kdf 侦听端口列表中添加代理端口。

排除或包含来自网络扫描服务的终端流量

要排除或包含来自思科云网络安全扫描的特定网络流量，请使用网络安全配置文件编辑器来配置流量的异常。可配置以下几种类别的异常：

- Host Exceptions 或 Host Inclusions - 在已配置 Host Exceptions 的情况下，会绕过所输入的 IP 地址（公共或专用，主机名或子网）。在已配置 Host Inclusions 的情况下，所输入的 IP 地址（公共或专用，主机名或子网）会转发到网络安全代理，而所有剩余流量会被绕过。

注释 AnyConnect 仍然可以拦截 Host Exceptions 中列出的流量。

- Proxy Exceptions - 将从扫描中排除此处列出的内部代理服务器。
-
- Static Exceptions - 将从扫描和 AnyConnect 中排除此处列出的 IP 地址或主机名。

ISE 服务器要求

ISE 服务器必须始终列在静态例外列表中，该列表在网络安全客户端配置文件的 Exceptions 窗格中配置。此外，网络安全模块必须绕过 ISE 终端安全评估探测，以便 ISE 终端安全评估客户端可访问 ISE 服务器。ISE 终端安全评估配置文件发送网络探头以查找 ISE 服务器，顺序如下：

1. 默认网关
2. 发现主机
3. enroll.cisco.com
4. 以前连接过的 ISE 服务器

排除或包含主机例外

开始之前

- 请勿在顶级域的两端使用通配符（如 *.cisco.*），因为这可能包括网络钓鱼网站。
- 请勿删除或更改任何默认主机例外条目。

您可以选择配置 Host Exceptions 或 Host Inclusions。如果选择 Host Exceptions，则指定的 IP 地址会被思科云网络安全代理绕过。如果选择 Host Inclusions，则会将指定的 IP 地址转发到思科云网络安全代理，同时绕过所有其他流量。请注意，AnyConnect 仍可以拦截来自排除的主机例外的互联网流量。要从网络安全和 AnyConnect 中排除流量，请配置静态例外。

过程

步骤 1 选择 Host Exceptions 或 Host Inclusions。

步骤 2 根据在步骤 1 中的选择，添加要绕过或转发的 IP 地址（公共或专用，主机名或子网）。

步骤 3 使用以下语法输入子网和 IP 地址：

语法	示例
单个 IPv4 和 IPv6 地址	10.255.255.255 2001:0000:0234:C1AB:0000:00A0:AABC:003F

无类域间路由 (CIDR) 表示法	10.0.0.0/8 2001:DB8::/48
完全限定域名	windowsupdate.microsoft.com ipv6.google.com 注释　不支持部分域。例如，不支持 example.com。
完全限定域名或 IP 地址中的通配符	127.0.0.* *.cisco.com

注释　当 WebSecurity 被配置为使用主机例外列表中的域名时，用户可以欺骗主机 HTTP 报头条目，以便绕过网络安全代理。通过使用 IP 地址而不是例外列表中的主机名，可以缓解此风险。

网络安全和漫游的安全兼容性所需的主机例外

如果您在通过网络安全模块部署 Umbrella 漫游安全模块，您必须配置 *.opendns.com 作为主机例外。这样操作失败会导致 Umbrella 漫游安全 DNS 保护完全绕过。

此外，您必须配置此处所述的排除静态例外：网络安全与 Umbrella 漫游安全模块兼容性所需的静态例外，第 9 页

排除代理例外

在 Proxy Exceptions 区域中，输入授权内部代理的 IP 地址（例如 `172.31.255.255`）。

您可在字段中指定 IPv4 和 IPv6 地址，但是您无法为其指定端口号。使用 CIDR 标记，您无法指定 IP 地址。

指定 IP 地址将禁止思科云网络安全拦截流向这些服务器的网络数据，并禁止使用 SSL 使数据以隧道方式通过这些服务器。随后代理服务器即可无中断地运行。如果不在此处添加代理服务器，则会将思科云网络安全流量视为 SSL 隧道。

如果您想豁免任何通过代理服务器的浏览器流量，则必须在 Host Exceptions 中列出这些主机名，以使它们不会被转发。对于流经 Proxy Exception 列表中未列出的代理的流量，不能仅配置静态例外。

对于列表中未列出的代理，网络安全将尝试使用 SSL 以隧道方式通过它们。因此，如果您的用户位于不同的公司站点，且该站点需要一个网外代理以访问互联网，则思科云网络安全可为其提供相同级别的支持，就像他们拥有开放互联网连接一样。

排除静态例外

确定应绕过思科云网络安全的流量，并添加使用无类域间路由 (CIDR) 表示法的单个 IP 地址或 IP 地址范围列表。在该列表中，请包括 VPN 网关的入口 IP 地址。对于 AnyConnect 版本 4.3.02039 或更

高版本，现在您可以添加要从扫描中排除的主机名。网络安全不会将该 HTTP/HTTPS 流量转发给云网络安全代理进行检查。

如果您有多个主机名具有相同的 IP 地址，但仅在静态例外列表中配置了其中一个主机名，则网络安全将豁免该流量。

默认情况下，http://www.ietf.org/rfc/rfc1918.txt 所述的私有 IP 地址包括在静态例外列表中。

注释 如果存在一个代理服务器，并且它的 IP 地址在静态例外列表的其中一个范围内，则将该例外移到主机例外列表中。例如，10.0.0.0/8 出现在静态例外列表中。如果存在一个位于 10.1.2.3 的代理，则将 10.0.0.0/8 移动到主机例外列表。否则，发送到此代理的流量会绕过云网络安全。

可以指定使用 CIDR 表示法的 IPv4 和 IPv6 地址或地址范围。您无法指定完全限定域名或在 IP 地址中使用通配符。正确的语法示例如下所示：

```
10.10.10.5
192.0.2.0/24
```

注释 将 SSL VPN 集中器 IP 地址添加到静态例外列表。

网络安全与 Umbrella 漫游安全模块兼容性所需的静态例外

为了确保 Umbrella 漫游安全与网络安全模块之间的兼容性，必须在调配给 AnyConnect 的网络安全配置文件中配置以下例外：

- 77.67.54.0/27
- 77.67.54.32/27
- 77.67.54.64/27
- 77.67.54.96/27
- 77.67.54.128/27
- 77.67.54.160/27
- 67.215.64.0/19
- 204.194.232.0/21
- 208.67.216.0/21
- 208.69.32.0/21
- 185.60.84.0/22
- 146.112.61.0/22
- 146.112.128.0/18

- 146.112.255.101

此外，您还必须配置此处所述的排除主机例外：网络安全和漫游的安全兼容性所需的主机例外，第 8 页。

配置用户控制和计算最快的扫描代理响应时间

为了允许用户选择要连接到哪个思科云网络安全扫描代理，请执行以下操作：

过程

步骤 1 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**。
- 在 Windows 单机型号下，选择 **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**。

步骤 2 打开要编辑的网络安全客户端配置文件。

步骤 3 单击 **Preferences**。

步骤 4 选择 **User Controllable**。（这是默认设置。）User Controllable 确定用户是否可以更改 AnyConnect 界面中的 Automatic Tower Selection 和 Order Scanning Proxies by Response Time 设置。

步骤 5 为了让网络安全自动选择扫描代理，请选择 **Automatic Scanning Proxy Selection**。如果您执行此操作，将自动选择 **Order Scanning Proxies by Response Time**。

- 如果您选择 **Automatic Scanning Proxy Selection**，网络安全将确定哪个扫描代理的响应时间最快并自动将用户连接到该扫描代理。
- 如果没有选择**自动选择扫描代理**，且仍然选择了**按响应时间排序扫描代理**，则将向用户呈现可以连接的扫描代理列表（按最快到最慢的响应时间排序）。
- 如果没有选择 **Automatic Scanning Proxy Selection**，用户仍然可以从 AnyConnect 用户界面启用此功能，但是一旦启用，则无法将其再次关闭。

  注释 您启用 Automatic Scanning Proxy Selection 后，瞬时通信中断和故障会导致当前选择的扫描代理自动更改。有时更改扫描代理可能产生不利影响，导致发生意外行为，例如，从使用其他语言的不同国家/地区中的扫描代理返回搜索结果。

步骤 6 如果您选择 **Order Scanning Proxies by Response Time**，请配置以下设置来计算哪个扫描代理的响应时间最短。

- **启用测试间隔**：运行每次性能测试之间间隔的时间，以小时和分钟为单位（默认为 2 分钟）。清除 Enable Test Interval 复选框可关闭测试间隔，从而阻止测试运行。

- **Test Inactivity Timeout**：以分钟为单位的时间，若用户处于非活动状态的时间超过此值，网络安全将暂停响应时间测试。只要扫描代理遇到连接尝试，网络安全就立即恢复测试。不应该更改此设置，除非客户端支持人员指导您这么做。

注释 **Ordering Scanning Proxies by Response Time** 测试将根据 Test Interval 时间连续运行，以下情况除外：

- 安全值得信赖的网络检测已启用并检测到计算机在企业 LAN 中。
- 网络安全许可证密钥丢失或无效。
- 用户处于非活动状态的时间达到所配置的时间，因此满足了“测试非活动超时”阈值。

步骤 7 单击可启用安全受信任的网络检测，该检测会以物理或 VPN 连接方式检测终端位于企业 LAN 上的时间。如果启用，源自企业 LAN 的任何网络流量将会绕过思科云网络安全扫描代理。

步骤 8 在 https 字段中，输入每个受信任的服务器的 URL，然后单击**添加**。URL 可包括端口地址。配置文件编辑器此时将尝试连接受信任服务器。如果不可行，但您知道服务器证书的 SHA-256 散列，请在**证书散列**框中输入相应值，然后单击**设置**。

步骤 9 保存网络安全客户端配置文件。

下一步做什么

请参阅 *ScanCenter* 管理员指南，版本 *5.2* 以获取更多信息。

使用安全值得信赖的网络检测

当终端通过物理方式或VPN连接方式接入企业局域网时，安全受信网络检测功能将进行检测。如果启用安全受信网络检测功能，所有来自企业局域网的网络流量都会绕过思科云网络安全扫描代理。这类流量的安全将通过其他方法和位于企业局域网中的设备（而非思科云网络安全）进行管理。

安全受信网络检测将使用已知 URL（地址、IP 或 FQDN）的服务器上 SSL 证书的 SHA-256 哈希值（拇指指纹）验证客户端是否连接到企业网络。证书使用的加密算法无关紧要，但仅可使用SHA-256哈希。

如果您选择不使用安全受信网络检测，且网络中存在代理（例如思科云网络安全连接器），则必须在配置文件编辑器中，将每个代理添加到例外面板的代理例外列表中。

多个服务器：如果您定义多台服务器，则客户端在连续两次尝试后仍无法连接到第一台服务器时将尝试连接到第二台服务器。尝试连接列表中的所有服务器之后，客户端将等待五分钟，然后再次尝试连接第一台服务器。

注释 当安全受信网络检测在内部网络以外运行时，它将发出 DNS 请求，并尝试与您调配的 HTTPS 服务器通信。思科强烈建议使用别名，以确保在内部网络以外使用的机器不会通过这些请求泄露您组织的名称和内部结构。

开始之前

- 排除代理例外
- 对数据丢失防护 (DLP) 设备等某些要求流量不受网络安全影响的第三方解决方案而言，您必须配置安全受信网络检测功能。
- 编辑配置文件时，请确保您与托管 SSL 证书的服务器建立了直接连接。

过程

步骤 1 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**。
- 在 Windows 单机型号下，选择 **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**。

步骤 2 打开要编辑的网络安全客户端配置文件。

步骤 3 单击网络安全树状窗格中的 **Preferences**。

步骤 4 选择 **Enable Trusted Network Detection**。

步骤 5 在 **https** 字段中，输入每个受信任服务器的 URL，然后单击 **Add**。URL 可包括端口地址。配置文件编辑器此时将尝试连接受信任服务器。如果无法连接，而您知道服务器证书的 SHA-256 哈希值，请在 **Certificate hash** 框中输入该值并单击 **Set**。

注释 代理后的受信任服务器不受支持。

步骤 6 保存网络安全客户端配置文件。

不使用安全值得信赖的网络检测

如果选择不使用安全值得信赖的网络检测，并且在网络中有代理（例如，思科云网络安全连接器），则您必须将每个代理添加到配置文件编辑器的 Exceptions 面板中的代理例外列表。

配置身份验证和将组成员身份发送到思科云网络安全代理

开始之前

使用 Windows 关闭和启用过滤器， 第 20 页

过程

步骤 1 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**。
- 在 Windows 单机型号下，选择 **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**。

步骤 2 打开要编辑的网络安全客户端配置文件。

步骤 3 单击 **Authentication**。

步骤 4 在 **Proxy Authentication License Key** 字段中，输入与在 Cisco ScanCenter 中创建的公司密钥、组密钥或用户密钥对应的许可证密钥。要根据用户的企业域对用户进行身份验证，请输入您创建的公司密钥。要根据用户的 Cisco ScanCenter 或 Active Directory 组对用户进行身份验证，请输入您创建的组密钥。该标记默认为空。如果将其留空，网络安全以直通型号运行。

步骤 5 输入 **Service Password**。网络安全的默认密码是 websecurity。请在定制配置文件时更改此密码。密码只能包含字母数字字符（a-z、A-Z、0-9）和以下特殊字符，因为其他字符可能被 Windows 命令外壳误认为控制字符或在 XML 中有特殊意义。

```
~ @ # $ % * - _ + = { } [ ] : , . ? /
```

使用此密码时，具有管理员权限的用户可以停止网络安全服务。无论是否具有管理员权限，用户都可以在不提供此密码的情况下启动网络安全服务。

步骤 6 随每个 HTTP 请求发送扫描代理服务器企业域信息和思科云网络安全或 Active Directory 组信息。扫描代理根据其对用户域和组成员身份的了解应用流量过滤规则。

注释 要将用户的定制用户名和定制组信息发送到扫描服务器代理，请跳过此步骤并转到步骤7。如果企业不使用 Active Directory，也请跳到步骤 7。

a) 单击 **Enable Enterprise Domains**。在列表中，单击 **All Domains**。当选择 All Domains 选项并且计算机在域中时，则将匹配用户所属的域，并且将用户名和组成员身份信息发送到思科云网络安全扫描代理。此选项适用于具有多个域的公司。

b) 或者，单击 **Specify Individual Domains**。

以 NetBIOS 格式输入每个域名，然后单击 Add。例如，`example.cisco.com` 的 NetBIOS 格式是 cisco。使用 DNS 格式，请不要输入域：abc.def.com。

如果在 Enterprise Domain name 字段中指定域名，思科云网络安全会识别当前登录的 Active Directory 用户、枚举该用户的 Active Directory 组，并将该信息随每个请求发送到扫描代理。

c) 在 Use 列表中，单击 **Group Include List** 或 **Group Exclude List**，以在发送到思科云网络安全扫描代理的 HTTP 请求中包含或排除组信息。值可以是要匹配的字符串的任何子字符串。

Group Include List。选择 **Group Include List** 之后，将思科云网络安全或 Active Directory 组名称添加到 Group Include List 中。这些组名称将随 HTTP 请求发送到思科云网络安全扫描代理服务器。如果请求来自指定企业域中的用户，将根据用户的组成员身份对 HTTP 请求进行过滤。如果用户没有组成员身份，将使用一组默认的规则对 HTTP 请求进行过滤。

Group Exclude List. 将思科云网络安全或 Active Directory 组名称添加到 **Group Exclude List**。这些组名不发送到 HTTP 请求的思科云网络安全扫描代理服务器。如果用户属于 Group Exclude List 中的一个组，该组名称不会发送到扫描代理服务器，并将根据其他组成员身份或至少根据一组默

认过滤规则对用户的 HTTP 请求进行过滤，该组规则为没有 Active Directory 或思科云网络安全组附属关系的用户进行定义。

步骤 7 单击**未加入域的计算机的自定义匹配和报告**，可发送扫描代理服务器的自定义名称。

a) 在列表中，单击 **Computer Name** 可使用该计算机的名称。或者，单击 **Local User** 可使用本地用户名。或者，单击 **Custom Name**，然后输入定制用户名。它可由任何字符串定义。如果不输入字符串，则会将计算机的 IP 地址发送到扫描代理服务器。此用户名或 IP 地址用于任何 Cisco ScanCenter 报告中，以识别来自定制用户的 HTTP 流量。

b) 在 **Authentication Group** 字段中，输入最多 256 个字母数字字符的定制组名称，然后单击 **Add**。

当 HTTP 请求发送到扫描代理服务器时，如果定制组名称已发送，并且扫描代理服务器上有对应的组名，则根据与定制组名称关联的规则对 HTTP 流量进行过滤。如果在扫描代理服务器上未定义对应的定制组，将根据默认规则对 HTTP 请求进行过滤。

如果仅配置定制用户名而未配置定制组，将根据扫描代理服务器默认规则对 HTTP 请求进行过滤。

步骤 8 保存网络安全客户端配置文件。

高级网络安全设置

网络安全客户端配置文件的“高级”(Advanced) 面板显示多项设置，它们可帮助思科客户端支持工程师进行故障排除。您不应更改此面板的设置，除非客户端支持人员明确要求您更改它们。

在配置文件编辑器的“高级”(Advanced) 面板中，可执行以下任务：

- 配置 KDF 侦听端口，第 14 页
- 配置端口如何侦听传入连接，第 15 页
- 配置超时/重试的发生时间，第 16 页
- DNS 查找，第 16 页
- 调试设置，第 16 页
- 阻止和允许流量，第 16 页

配置 KDF 侦听端口

内核驱动程序框架 (KDF) 拦截将某个流量侦听端口用作其目标端口的所有连接并将流量转发到 KDF 侦听端口。网络扫描服务分析转发到 KDF 侦听端口的所有流量。

开始之前

不应该更改此设置，除非客户端支持人员指导您这么做。

过程

步骤 1 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**。
- 在 Windows 单机型号下，选择 **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**。

步骤 2 打开要编辑的网络安全客户端配置文件。

步骤 3 在 Web Security 树窗格中单击 **Advanced**。

步骤 4 在 **KDF Listen Port** 字段中指定 KDF 侦听端口。

步骤 5 保存网络安全客户端配置文件。

配置端口如何侦听传入连接

服务通信端口是网络扫描服务侦听从AnyConnect GUI组件及某些其他实用程序组件传入的连接的端口。

开始之前

不应该更改此设置，除非客户端支持人员指导您这么做。

过程

步骤 1 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**。
- 在 Windows 单机型号下，选择 **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**。

步骤 2 选择要编辑的网络安全客户端配置文件，然后单击 **Edit**。在 **Web Security** 树窗格中单击 **Advanced**。

步骤 3 编辑**服务通信端口**字段。

步骤 4 保存网络安全客户端配置文件。

注释 如果更改端口的默认值 5300，必须重新启动网络安全服务和 AnyConnect GUI 组件。

配置超时/重试的发生时间

连接超时设置使您可以设置网络安全尝试访问互联网之前的超时值（不使用扫描代理）。如果保留为空，则使用的默认值为 4 秒。此设置使用户可以更快地访问已付费的网络服务，而不必等待发生超时再重试。

过程

步骤 1 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**。
- 在 Windows 单机型号下，选择 **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**。

步骤 2 打开要编辑的网络安全客户端配置文件。

步骤 3 在 Web Security 树窗格中单击 **Advanced**。

步骤 4 更改 **Connection Timeout** 字段。

步骤 5 保存网络安全客户端配置文件。

DNS 查找

配置文件编辑器的 Advanced 面板包含几个用于管理域名服务器查询的字段。这些设置已经为 DNS 查找配置了最佳值。

指南

不应该更改此设置，除非客户端支持人员指导您这么做。

调试设置

Debug Level 是一个可配置字段。

指南

不应该更改此设置，除非客户端支持人员指导您这么做。

阻止和允许流量

在连接故障策略列表中，选择 **Fail Close** 以在无法与思科云网络安全代理服务器建立连接时阻止流量。或者，选择 **Fail Open** 以允许流量。

在 **When a captive portal is detected** 列表中，选择 **Fail Open** 以在无法与思科云网络安全代理服务器建立连接但检测到强制网络门户（如 Wi-Fi 热点）时允许流量。或者，选择 **Fail Close** 以阻止流量。

注释 如果主机、代理或静态例外配置为包括强制网络门户地址，则 **Fail Close** 不会阻止流量。

其他可定制的网络安全选项

导出选项

导出纯文本网络安全客户端配置文件

从 ASA 导出模糊的网络安全客户端配置文件并将其分配到终端设备。

过程

步骤 1 打开 ASDM，并选择**配置** > **远程接入 VPN** > **网络 (客户端) 接入** > **AnyConnect 客户端配置文件**。

步骤 2 选择要编辑的网络安全客户端配置文件，然后单击 **Export**。

步骤 3 浏览到本地文件夹以保存文件。编辑 Local Path 字段中的文件名，以使用此新文件名来保存网络安全客户端配置文件。

步骤 4 单击 **Export**。

ASDM 即导出网络安全客户端配置文件的明文版本 `filename.wsp`。

导出 DART 捆绑包的纯文本网络安全客户端配置文件

如果需要将诊断 AnyConnect 报告工具 (DART) 捆绑包发送到思科客户服务，请连同 DART 捆绑包一起发送网络安全客户端配置文件（`filename.wsp` 或 `filename.xml`）的明文版本。思科客户服务无法读取模糊的版本。

配置文件编辑器的独立版本可创建两个版本的网络安全配置文件：一个为模糊处理版本，文件名为 `filename.wso`，；另一个为纯文本版本，文件名为 filename.xml。

向思科客户服务发送 DART 捆绑包前，将纯文本版本的网络安全客户端配置文件添加到 DART 捆绑包中。

从 ASDM 编辑并导入明文网络安全客户端配置文件

导出明文网络安全客户端配置文件后，可使用任何明文或XML编辑器在本地计算机上编辑此文件，该编辑器允许编辑AnyConnect网络安全配置文件编辑器不支持的文件。除非客户端支持人员有明确指示，否则您不应更改网络安全客户端配置文件的明文版本。使用此过程来导入编辑器。

开始之前

导入该文件将覆盖所选的网络安全客户端配置文件的内容。

过程

步骤 1 打开 ASDM，并选择**配置** > **远程接入 VPN** > **网络 (客户端) 接入** > **AnyConnect 客户端配置文件**。

步骤 2 选择要编辑的网络安全客户端配置文件，然后单击 **Export**。

步骤 3 在更改 `filename.wsp` 后，返回到 AnyConnect Client Profile 页面，然后选择您编辑的文件的配置文件名称。

步骤 4 单击 **Import**。

步骤 5 浏览到网络安全客户端配置文件的已编辑版本，然后单击 **Import**。

导出经过模糊处理的网络安全客户端配置文件

过程

步骤 1 打开 ASDM 并选择**工具** > **文件管理**。

步骤 2 在“文件管理”屏幕中选择**文件传输** > **本地 PC 与闪存之间**，并使用“文件传输”对话框将模糊处理的 `filename.wso` 客户端配置文件传输到您的本地计算机中。

为网络安全配置分割隧道排除

当用户建立 VPN 会话后，所有网络流量均通过 VPN 隧道发送。但是，当 AnyConnect 用户使用网络安全时，在终端产生的 HTTP 流量需要从隧道排除，并直接发送到云网络安全扫描代理。

要为用于云网络安全扫描代理的流量设置分割隧道排除，请使用组策略中的 **Set up split exclusion for Web Security** 按钮。

开始之前

- 配置用于 AnyConnect 客户端的网络安全。
- 创建一个组策略，然后为其分配使用网络安全配置的 AnyConnect 客户端的一个连接配置文件。

如果使用安全值得信赖的网络检测功能，并且想确保网络安全和 VPN 同时处于活动状态，请配置网络，以便 HTTPS 服务器不可通过 VPN 隧道连接。这样，仅当用户在企业局域网中时，网络安全功能才进入旁路模式。

过程

步骤 1 在 ASDM 中，转到**配置** > **远程接入 VPN** > **网络 (客户端) 接入** > **组策略**。

步骤 2 选择组策略，单击 **Edit** 或 **Add** 可编辑或新增组策略。

步骤 3 选择**高级** > **分割隧道**。

步骤 4 单击 **Set up split exclusion for Web Security**。

步骤 5 输入新的或选择现有的用于网络安全分隔排除的接入列表。ASDM 设置要用于网络列表的访问列表。

步骤 6 对新列表单击 **Create Access List**，或者对现有列表单击 **Update Access List**。

步骤 7 单击 **OK**。

下一步做什么

添加其他扫描代理时，请使用新信息更新您在此过程中创建的统一访问列表。

使用思科云网络安全托管配置文件

从 AnyConnect 版本 3.0.4 开始，通过网络安全托管客户端配置文件的思科 ScanCenter 托管配置可以为网络安全客户端提供新配置。带网络安全功能的设备可以从云端（位于思科 ScanCenter 服务器上的托管配置文件）下载新的网络安全托管客户端配置文件。

AnyConnect 客户端还必须通过采用 AnyConnect 二进制文件硬编码的主机名，从资源服务下载其配置文件。将向 **hostedconfig.scansafe.net/** (IP: 46.155.41.2) 提出请求。该交换将通过 TCP 端口 443 进行加密。

托管配置允许通过 TCP 端口 443（在简单模式下部署时，还可通过端口 8080）访问 AnyConnect 网络安全的 CWS 塔/代理的入口 IP。思科 ScanCenter 管理员指南**准备**部分提供了 AnyConnect 网络安全的塔/代理的完整列表。客户端必须能够访问 TCP 端口 80 上的 80.254.145.118，它可在此获取代理塔的列表，并使自己保持最新。必须将网络安全模块设置为通过 TCP 端口 80 连接到 Verisign。在此范围内，客户端在 **trust.quovadisglobal.com**、 **crl.quovadisglobal.com** 和 **ocsp.quovadisglobal.com** 上检查证书吊销情况。

使用网络安全配置文件编辑器创建客户端配置文件，然后将明文 XML 文件上传到 Cisco ScanCenter 服务器。此 XML 文件必须包含有效的许可证密钥，该密钥具有与在思科云网络安全中定义和托管的托管配置相关的相同公司、组或用户许可证密钥。新配置文件应用于托管配置服务器后，客户端最多可在 8 小时内将其取回。

在从托管配置（思科 ScanCenter）服务器取回新客户端配置文件时，托管配置功能使用该许可证密钥。如果现有网络安全客户端配置文件中的许可证与托管服务器上客户端配置文件关联的许可证相同，则一旦服务器上出现新客户端配置文件，带网络安全的设备就会自动轮询服务器并下载新客户端配置文件。下载新客户端配置文件后，在您使新客户端配置文件可用之前，网络安全不会再次下载同一文件。

有关许可证密钥的详细信息，请参阅思科 *ScanCenter* 管理指南，版本 *5.2*。

开始之前

- 使用包含思科云网络安全许可证密钥的有效客户端配置文件安装网络安全客户端设备。
- 重启网络安全代理服务选项仅供拥有重启服务所需权限的用户使用。
- 运行 ACWS 代理的客户端计算机必须在受信任的根证书颁发机构存储库中具有 Thawte 主根 CA 和 Thawte SSL CA - G2。

过程

步骤 1 使用网络安全配置文件编辑器，为网络安全设备创建新的客户端配置文件。该客户端配置文件必须包含思科云网络安全许可证密钥。

步骤 2 将该客户端配置文件另存为明文 XML 文件。将此文件上传到思科 ScanCenter 服务器。文件上传后，使新的客户端配置文件可用于网络安全客户端。

步骤 3 如果为公司启用了托管配置功能，则通过思科 ScanCenter 为公司上传新的客户端配置文件并应用该配置文件。托管客户端配置文件与某个许可证关联。如果正在使用不同的许可证（例如，不同的组许可证密钥），则每个许可证可让自己的客户端配置文件与其关联。您可以在随后根据为不同用户配置了哪些许可证，向它们向下推送不同的客户端配置文件。您可以为每个许可证存储多个配置，并设置供客户端下载的默认客户端配置文件。用户随后可以切换到存储在思科 ScanCenter 的托管配置区域中的其他配置修订版之一，方法是选择该客户端配置文件作为默认客户端配置文件。一个许可证只与一个客户端配置文件关联。因此，当有多个修订版与许可证关联时，只能有一个默认客户端配置文件。

关闭和启用思科 AnyConnect 网络安全代理

您可通过执行以下步骤关闭和启用思科 AnyConnect 网络安全代理拦截网络流量的功能。

使用 Windows 关闭和启用过滤器

过程

步骤 1 打开命令提示符窗口。

步骤 2 转到 **%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client** 文件夹。

步骤 3 打开或关闭过滤：

- 要启用过滤，请输入 **acwebsecagent.exe -enablesvc**
- 要禁用过滤，请输入 **acwebsecagent.exe -disablesvc -servicepassword**

使用 Mac OS X 关闭和启用过滤器

服务密码在网络安全配置文件编辑器的 Authentication 面板中配置。

过程

步骤 1 启动 Terminal 应用。

步骤 2 转到 `/opt/cisco/anyconnect/bin` 文件夹。

步骤 3 启用或关闭过滤：

- 要启用过滤，请输入 **./acwebsecagent -enablesvc**。
- 要禁用过滤，请输入 **./acwebsecagent -disablesvc -servicepassword**。

网络安全日志记录

Windows

所有网络安全消息都记录在 `Event Viewer (Local)\Cisco AnyConect Web Security Module` 文件夹的 Windows 事件查看器中。该事件查看器中的事件网络安全记录由思科技术支持中心的工程师进行分析。

Mac OS X

查看来自系统日志或控制台的网络安全消息。