# ASDM 手册 3：思科 ASA 系列 VPN ASDM 配置指南，7.10

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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，请与思科代表联系以获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克利分校 (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。© 1981，加州大学董事会。

无论本手册中是否有任何其他保证，这些供应商的所有文档文件和软件均按“原样”提供，并可能包含缺陷。思科和上面所提及的提供商拒绝所有明示或暗示保证，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。

本文档的所有打印副本和复制的电子副本均被视为非受控副本。最新版本请参阅当前在线版本。

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 上列出了各办事处的地址和电话号码。

# 目录

第 14 章 无客户端 SSL VPN 基本配置 241

# 关于本指南

以下主题介绍如何使用本指南。



## 文档目标

本指南旨在帮助您使用自适应安全设备管理器 (ASDM) 这一基于 Web 的 GUI 应用在自适应安全设备 (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。在本指南中，除非有专门指定，否则术语“ASA”一般适用于受支持的模型。

## 相关文档

有关详细信息，请参阅思科 *ASA* 系列文档一览，网址：http://www.cisco.com/go/asadocs。

## 文档约定

本文档遵循以下文本、显示和警报约定。

### 文本约定

| 约定 | 指示 |
|---|---|
| **黑体字** | 命令、关键字、按钮标签、字段名称及用户输入的文本以**黑体字**字体显示。对于基于菜单的命令，显示指向该命令的完整路径。 |

| 约定 | 指示 |
|---|---|
| 斜体 | 为其赋值的变量以斜体字体显示。<br>斜体字体还用于文档标题和一般强调。 |
| 等宽字体 | 系统显示的终端会话和信息以等宽字体格式显示。 |
| {x \| y \| z} | 必需的备选关键字集中在大括号内，以竖线分隔。 |
| [ ] | 方括号中的元素是可选项。 |
| [x \| y \| z] | 可选的备选关键字集中在方括号内，以竖线分隔。 |
| [] | 对于系统提示符的默认响应也位于方括号内。 |
| < > | 非打印字符（例如密码）位于尖括号内。 |
| !, # | 一行代码开头带有叹号 (!) 或星号 (#) 表示这是注释行。 |

### 读者提示

本文档采用以下格式的读者提示：

**注释** 表示读者需要注意的地方。“注”中包含有用的建议或本文档未涵盖材料的引用信息。

**提示** 表示以下信息可帮助您解决问题。

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

**便捷程序** 表示所述操作可以节省时间。按照该段落中的说明执行操作，有助于节省时间。

**警告** **表示读者需要注意。在这种情况下，操作可能会造成人身伤害。**

# 通信、服务和其他信息

- 要及时从思科收到相关信息，请注册思科简档管理器。

- 要使用重要技术实现您理想的业务影响，请访问思科服务。
- 要提交服务请求，请访问思科支持部门。
- 要了解并浏览安全且经过验证的企业级应用、产品、解决方案和服务，请访问思科Marketplace。
- 要获取一般网络、培训和认证主题相关的信息，请访问思科出版社.
- 要查找有关特定产品或产品系列的保修信息，请访问思科保修服务查找工具。

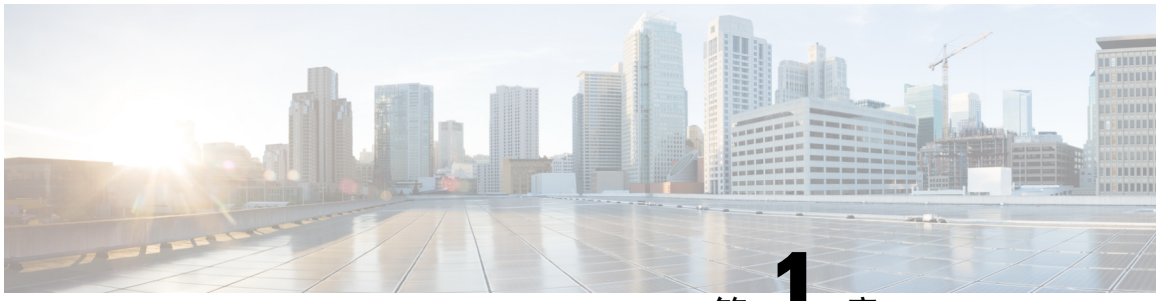
### 思科漏洞搜索工具

思科漏洞搜索工具 (BST) 是一款基于 Web 的工具，用作思科漏洞跟踪系统的网关，其中思科漏洞跟踪系统包含一个关于思科产品和软件的缺陷和漏洞的综合列表。BST 提供关于您的产品和软件的详细缺陷信息。

关于本指南

第 部分

# 站点到站点 VPN 和客户端 VPN



第 1 章

# VPN 向导



## 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。

这种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，通过隧道收发数据包，然后再对它们解除封装。ASA 相当于一个双向隧道终端：可以接收普通数据包，封装它们，再将它们发送到隧道的另一端，在那里系统将对数据包解除封装并将其发送到最终目标。它也可以接收已封装的数据包，解除数据包封装，然后将它们发送到最终目标。

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：

- 无客户端 SSL VPN 向导， 第 2 页

  ASA 无客户端 SSL VPN 仅使用 Web 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。

- AnyConnect VPN 向导， 第 3 页

  思科 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，并在连接终止时自行保留或自行卸载（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。

当 ASA 处于多情景模式下时，AnyConnect VPN 向导仅在用户情景中可用。必须在系统情景中配置所需情景的存储和资源类。

每个情景都需要存储来容纳思科AnyConnect软件包文件和配置文件。每个情景的许可证分配都需要资源类。使用的许可证是 AnyConnect 高级版许可证。

**注释** 此向导的其余配置部分与单情景模式相同。

- IPsec IKEv2 远程访问向导，第 10 页

  IKEv2 允许其他供应商的VPN客户端连接到ASA。这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。

  当 ASA 处于多情景模式下时，IPSec IKEv2 远程访问向导仅在用户情景中可用。必须在系统情景中配置所需情景的资源类。使用的许可证是 AnyConnect 高级版许可证。

  **注释** 此向导的其余配置部分与单情景模式相同。

- IPsec IKEv1 远程访问向导，第 6 页
- IPsec 站点到站点 VPN 向导，第 12 页

  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，并且双方的内部网络具有匹配的寻址方案（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。

# 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。
- “数字证书”- 指定 ASA 发送到远程 Web 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 Web 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。

### 用户身份验证

在此窗格中指定身份验证信息。

- “使用 AAA 服务器组进行身份验证”- 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。
- “使用本地用户数据库进行身份验证”- 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。

### 组策略

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 - 选择现有组策略进行修改。

### 书签列表

将门户页面中显示的组内联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。

### 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对 VPN 连接进行访问的名称。
- VPN Access Interface - 选择远程访问用户将对 VPN 连接进行访问的接口。

### 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 Web 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（例如“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 - 突出显示要删除的证书并点击 **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口令的文件。
  - 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 软件包上传到客户端设备。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。

### 认证方式

在此屏幕上指定身份验证信息。

- “AAA 服务器组”- 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。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。
- “本地用户数据库详细信息”- 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。

### 客户端地址分配

向远程 AnyConnect 用户提供一系列 IP 地址。

- “IPv4 地址池”- 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 Pool - 选择现有 IP 地址池，或者点击 **New** 以创建新池。

注释 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，则必须豁免 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 Web 浏览器访问 ASA 时，AnyConnect 客户端软件包自动进行安装。

注释 在多情景模式下不支持 Web 启动。

- 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 向导

相关主题

IPsec IKEv1 远程访问向导，第 6 页
IPsec IKEv2 远程访问向导，第 10 页

# IPsec IKEv1 远程访问向导

注释 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（例如移动用户）配置安全远程访问权限，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。
- “支持入站 IPsec 会话绕过接口访问列表”- 支持始终允许通过 IPsec 身份验证的入站会话经过 ASA（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 代理”- 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 客户端身份验证方式及隧道组名称

使用 VPN Client Authentication Method and Name 窗格配置身份验证方式和创建连接策略（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。
  - “预共享密钥”- 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。
  - “证书”- 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。数字证书还包含公共密钥的副本。

    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。

- 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、授权和记账服务器、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方法并使用 ASA 默认组策略。

### 客户端身份验证

使用“客户端身份验证”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：

- “使用本地用户数据库进行身份验证”- 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 上为个人用户创建账户。
- 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。

### 用户账户

使用“用户账户”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“地址池”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“推送至客户端的属性（可选）”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。阶段 2 创建保护数据的隧道。

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式，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散列密钥。

- “加密”- 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散列算法。默认值为 SHA。MD5 具有比 SHA 更小的摘要并认为其比 SHA 稍快一些。已成功（但极其困难）演示过对 MD5 的攻击。不过，ASA 所使用的带密钥的散列消息认证码 (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。

### 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 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降到最低，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 豁免规则，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。

**注释** 如果希望豁免所有主机和网络执行 NAT，不要在此窗格上进行任何配置。如果即使有一个条目，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豁免的主机或网络的 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 客户端会对发往 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输到互联网而不涉及 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 技术来生成密钥。

  PFS 确保在将来其中一个私钥被泄漏的情况下，从一组长期公共密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。

### 汇总

如果对配置满意，请点击 **Finish**。ASDM 将保存 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 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）配置安全远程访问权限，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、授权和记账服务器、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方法并使用 ASA 默认组策略。
- 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。

### “基于标准的 IPSec (IKEv2) 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。

MobIKE RRC

- “为 Mobike 启用返回路由能力检查”- 对已启用 MobIKE 的 IKE/IPSEC 安全关联中的动态 IP 地址更改启用返回路由能力检查。

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。
  - “证书”- 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。数字证书还包含公共密钥的副本。

    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。

### 身份验证方式

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

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 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。
- Crypto Map Type - 指定将用于此对等体的映射类型为静态还是动态。

### 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 版身份验证方式

- 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。数字证书还包含公共密钥的副本。

  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 版身份验证方式
  - Local Pre-shared Key - 指定 IPsec IKEv2 身份验证方式和加密算法。
  - 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 身份验证方式。
  - 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 技术来生成密钥。

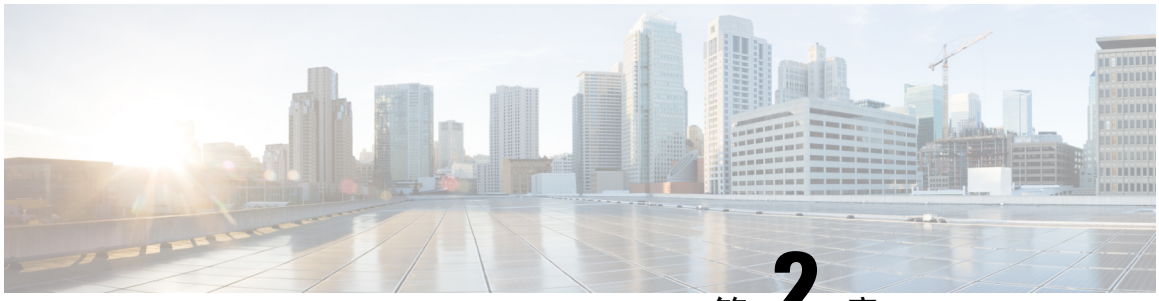
    PFS 确保在将来其中一个私钥被泄漏的情况下，从一组长期公共密钥和私钥派生的会话密钥不被泄漏。

    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



## 配置 IKE

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。

### 过程

**步骤 1** 启用 IKE，第 15 页。

**步骤 2** 设置站点到站点 VPN 的 IKE 参数，第 16 页。

**步骤 3** 配置 IKE 策略，第 19 页。

## 启用 IKE

### 过程

**步骤 1** 要为 VPN 连接启用 IKE，请执行以下操作：

a) 在 ASDM 中，依次选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**。

b) 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**。

**步骤 2** 要为站点到站点 VPN 启用 IKE，请执行以下操作：

a) 在 ASDM 中，依次选择 **Configuration > Site-to-Site VPN > Connection Profiles**。

b) 选择您想要在其上使用 IKEv1 和 IKEv2 的接口。

# 站点到站点 VPN 的 IKE 参数

在 ASDM 中，依次选择**配置 > 站点间 VPN > 高级 > IKE 参数**。

**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 到 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。默认情况下启用此功能。

  - 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 到 LAN 连接。
  - LAN 到 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。

  **注释** 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 到 LAN 连接。

- ASA 可同时支持标准 IPsec、经由 TCP 的 IPsec、NAT 遍历和经由 UDP 的 IPsec，具体取决于与其交换数据的客户端。
- 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）。此名称包含主机名和域名。 |
| **Key ID** | 远程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：<br>• 预共享密钥的 IP 地址<br>• 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 到 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、超过最大连接时间或管理员切断。

- ASA 可以通知合格的对等体（在 LAN 到 LAN 配置中）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，并将其显示在事件日志或弹出窗格中。默认情况下会禁用此功能。
- 您可以通过此窗格启用该功能，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）。

- 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 质询”- 使得 ASA 可以响应 SA 发起数据包，向对等设备发送 Cookie 质询。
  - “对传入 SA 进行 Cookie 质询前的百分比阈值”- ASA 允许协商的 SA 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。范围为 0 到 100%。默认为 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。
- “允许的最大 SA 数”- 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。
- Notify Invalid Selector - 当 SA 上接收的入站数据包与该 SA 的流量选择器不匹配时，允许管理员启用或禁用向对等体发送 IKE 通知。发送此通知默认为已禁用。

### 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。

在 DoS 攻击中，当对等设备发送 SA 发起数据包并且 ASA 发送其响应但对等设备不再响应时，攻击者发起 DoS 攻击。如果对等设备持续这样做，ASA 上所有允许的 SA 请求会用尽，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“允许的最大 SA 数”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。

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

# IKE 策略

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

使用该窗格可通过 Add 添加、通过 Edit 编辑或通过 Delete 删除 IKEv1 和 IKEv2 策略。

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）。
- 身份验证方式，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散列密钥。
- ASA 在更换加密密钥前可使用该加密密钥的时长限制。

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。

对于 IKEv1，您只能为一个参数启用一个设置。对于 IKEv2，每个提议对于加密、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。

### 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 - 显示散列算法。
- D-H Group - 显示 Diffie-Hellman 群。
- Authentication - 显示身份验证方式。
- Lifetime (secs) - 显示以秒为单位的 SA 生存期。

- 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 - 显示散列算法。
  - PRF Hash - 显示伪随机功能 (PRF) 散列算法。
  - D-H Group - 显示 Diffie-Hellman 群。
  - Lifetime (secs) - 显示以秒为单位的 SA 生存期。

## 添加或编辑 IKEv1 策略

**Configuration > Site-to-Site VPN > Advanced > IKE Policies > Add/Edit IKE Policy**

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，但速度比备选提议快。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散列算法。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 | |

“身份验证”- 选择 ASA 用于建立每个 IPSec 对等体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。 |

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。生命期越长，ASA 设置未来 IPsec 安全关联的速度就越慢。加密强度大到足以确保安全性，无需使用非常快的再生密钥时间（大约每隔几分钟再生一次）。建议接受默认值。

Time Measure - 选择时间度量值。ASA 接受以下值：

| |
|---|
| 120 - 86,400 秒 |
| 2 - 1440 分钟 |
| 1 - 24 小时 |
| 1 天 |

## 添加或编辑 IKEv2 策略

**Configuration > Site-to-Site VPN > Advanced > IKE Policies > Add/Edit IKEv2 Policy**

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 指定带有 128 位密钥加密的 AES。 |
| **aes-192** | 为 ESP 指定带有 192 位密钥加密的 AES。 |
| **aes-256** | 为 ESP 指定带有 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散列算法。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 | |
| **sha256** | SHA 2，256 位摘要 | 指定具有 256 位摘要的安全散列算法 SHA 2。 |
| **sha384** | **SHA 2, 384-bit digest** | 指定具有 384 位摘要的安全散列算法 SHA 2。 |
| **sha512** | **SHA 2, 512-bit digest** | 指定具有 512 位摘要的安全散列算法 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** | 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 | |
| **sha256** | SHA 2，256 位摘要 | 指定具有 256 位摘要的安全散列算法 SHA 2。 |
| **sha384** | SHA 2，384 位摘要 | 指定具有 384 位摘要的安全散列算法 SHA 2。 |
| **sha512** | SHA 2，512 位摘要 | 指定具有 512 位摘要的安全散列算法 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。生命期越长，ASA 设置未来 IPsec 安全关联的速度就越快。加密强度大到足以确保安全性，无需使用非常快的再生密钥时间（大约每隔几分钟再生一次）。建议接受默认值。

ASA 接受以下值：

| |
|---|
| 120 - 86,400 秒 |
| 2 - 1440 分钟 |

| |
|---|
| 1 - 24 小时 |
| 1 天 |

# 配置 IPsec

ASA 会将 IPsec 用于 LAN 到 LAN VPN 连接，并提供将 IPsec 用于客户端到 LAN VPN 连接的选项。在 IPsec 术语中，“对等体”是指远程访问客户端或其他安全网关。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 到 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 到 LAN VPN 可连接不同地理位置的网络。在 IPsec LAN 到 LAN 连接中，ASA 可用作发起方或响应方。在 IPsec 客户端到 LAN 连接中，ASA 只能用作响应方。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 数字认证
- 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)

过程

**步骤 1** 配置 加密映射，第 25 页。
**步骤 2** 配置 IPsec 预分片策略，第 32 页。
**步骤 3** 配置 IPsec 提议（转换集），第 34 页。

# 加密映射

**Configuration > Site-to-Site VPN > Advanced > 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。

注释 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。

此外，您还可以通过选择接口、源、目标、目标服务或规则查询，选择是或包含，并输入筛选参数，从而通过 **Find** 来查找规则（过滤规则的显示）。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。使用 **Diagram** 以图示形式显示规则。

IPSec 规则指定以下字段：

- 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（请查看 Show Detail 按钮）下，地址列可能包含带 any 一词的接口名称，例如 inside:any，其中 any 意味着内部接口上的任意主机都会受该规则影响。
  - 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（请查看 Show Detail 按钮）下，地址列可能包含带 any 一词的接口名称，如 outside:any。其中 any 意味着外部接口上的任意主机都会受该规则影响。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。
- “启用反向路由”- 指示是否为此策略启用反向路由注入 (RRI)。RRI 在配置时完成并被视为静态的，在配置更改或被删除之前保持不变。ASA 可自动将静态路由添加到路由表中，并向其使用 OSPF 的专用网络或边界路由器通告这些路由。
  - “动态”- 如果指定动态 RRI，则在成功建立 IPsec 安全关联 (SA) 时创建 RRI 并在删除 IPsec SA 后删除 RRI。

**注释** 动态 RRI 仅适用于基于 IKEv2 的静态加密映射。

- 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）指定此规则的简要说明。对于现有规则，这是您在添加该规则时键入的说明。隐式规则包括以下说明：“Implicit rule”。要编辑除隐式规则之外的任意规则的说明，请右键点击此列，并选择 Edit Description 或双击此列。
- Enable Anti-replay window size - 设置防重放窗口大小，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，未处于防重放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。配置防重放窗口大小可以帮助您避免可能的错误警报。
- “启用 IPsec 内部路由查找”- 默认情况下，不会对通过 IPsec 隧道发送的数据包执行查找，仅对外部 ESP 数据包执行按数据包邻接关系查找。在某些网络拓扑中，当路由更新更改了内部数据包的路径，但本地 IPsec 隧道仍正常运行时，通过隧道的数据包可能无法正确路由，且无法到达其目的地。要避免此情况，请对 IPsec 内部数据包启用按数据包路由查找功能。

## 创建或编辑 IPSec 规则隧道策略（加密映射）- Basic 选项卡

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散列算法。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。

**Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Create / Edit IPsec Rule > Tunnel Policy (Crypto Map) - Basic**

- 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 提议：
  - IKEv1 IPsec Proposal - 为策略选择提议（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提议。您最多可向加密映射条目或动态加密映射条目，添加 11 个提议。
  - IKEv2 IPsec Proposal - 为策略选择提议（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提议。您最多可向加密映射条目或动态加密映射条目，添加 11 个提议。
- 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 到 LAN 连接，请选择双向或仅应答（而非仅发出）。对于 LAN 到 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。此选项比群 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。

## 创建或编辑 IPSec 规则隧道策略（加密映射） - Advanced 选项卡

**Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Create / Edit IPsec Rule > Tunnel Policy (Crypto Map) - Advanced**

- 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 到 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。RRI 在配置时完成并被视为静态的，在配置更改或被删除之前保持不变。ASA 可自动将静态路由添加到路由表中，并向其使用 OSPF 的专用网络或边界路由器通告这些路由。
  - “动态” - 如果指定动态 RRI，则在成功建立 IPsec 安全关联 (SA) 时创建 RRI 并在删除 IPsec SA 后删除 RRI。通常，RRI 路由用于启动隧道（如果尚无隧道），并且需要对流量加密。在支持动态 RRI 的情况下，隧道建立之前并不存在路由。因此，配置了动态 RRI 的 ASA 通常只会用作响应方。

  **注释** 动态 RRI 仅适用于基于 IKEv2 的静态加密映射。

- 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 报头中设置了不分片 (DF) 位。选择如下选项之一：

    **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。

    **注释** 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 提议。

    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。

## 创建或编辑 IPSec 规则流量选择选项卡

**Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Create / Edit IPsec Rule > Traffic Selection**

此窗口允许您定义要保护（允许）或不保护（拒绝）哪些流量。

- 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 - 输入说明。
  - 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 - 输入说明。
  - Selected Destination - 点击 **Destination**，以便包含作为目标的选定条目。
- 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 条目的说明。
- 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，您可以在其中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。

**注释** “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 到 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。

- Options
  - 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。

# IPsec 预分片策略

**Configuration > Site-to-Site VPN > Advanced > IPsec Prefragmentation Policies**

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。此功能为处理 ASA 和客户端之间的路由器或 NAT 设备拒绝或丢弃 IP 分片的情况提供了方法。例如，假设客户端要从 ASA 后面的 FTP 服务器进行 FTP 获取，并且 FTP 服务器在公共接口上传输的数据包在封装后会超过 ASA 的 MTU 大小。此时，选择的选项将决定 ASA 如何处理这些数据包。预分片策略适用于从 ASA 公共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，然后通过公共接口传输它们。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。

**注释** 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。

使用该窗格，可以为在父窗格上选定的接口查看或通过 **Edit** 编辑现有 IPsec 预分片策略和不分片 (DF) 位策略。

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 - 不分片位策略：Copy、Clear 或 Set。

# 配置 IKEv2 分片选项

在 ASA 上，可以启用或禁用 IKEv2 分片，可以指定对 IKEv2 数据包分片时的 MTU（最大传输单位），还可以由管理员在以下屏幕上配置首选分片方法：

**配置 > 站点间 VPN > 高级 > IKE 参数**

默认情况下，启用所有 IKEv2 分片方法， IPv4 的 MTU 为 576，IPv6 的 MTU 为 1280，首选方法为 IETF 标准 RFC-7383。

在考虑以下注意事项的情况下，指定 MTU：

- 使用的 MTU 值应包括 IP (IPv4/IPv6) 报头 + UDP 报头大小。
- 如果管理员未指定，则 IPv4 的默认 MTU 为 576，IPv6 的默认 MTU 为 1280。
- 一旦指定，则对 IPv4 和 IPv6 使用相同的 MTU。
- 有效范围介于 68 至 1500 之间。

可将以下支持的分片方法之一配置为 IKEv2 的首选分片方法：

- 基于 IETF RFC-7383 标准的 IKEv2 分片。
  - 当两个对等体都指定了协商期间的支持和首选项时，将使用此方法。
  - 使用此方法将在分片后执行加密，为每个 IKEv2 分片消息提供单独的保护。
- 思科专有分片。
  - 如果此方法是对等体（例如 AnyConnect 客户端）提供的唯一方法，或者如果两个对等体都指定了协商期间的支持和首选项，将使用此方法。
  - 使用此方法将在加密后执行分片。接收方对等体在收到所有分片之前，无法对消息进行解密或身份验证。
  - 此方法不能与非思科对等体实现互操作。

### 开始之前

- 不支持路径 MTU 发现，需要手动配置 MTU 以符合网络的需求。
- 此配置是全局配置，将影响该配置应用后所建立的未来 SA。较早的 SA 不会受到影响。禁用分片时，同样如此。
- 最多可以接收 100 个分片。

过程

**步骤 1** 在 ASDM 中，依次转到**Configuration > Site-to-Site VPN > Advanced > IKE parameters**。

**步骤 2** 选择或取消选择 **Enable fragmentation** 字段。

**步骤 3** 指定**分片 MTU** 大小。

**步骤 4** 指定**首选分片方法**。

# IPsec 提议（转换集）

**Configuration > Site-to-Site VPN > Advanced > IPsec Proposals (Transform Sets)**

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、数据保密性和数据压缩。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。

使用此窗格可以查看、通过 **Add** 添加、通过 **Edit** 编辑或通过 **Delete** 删除下述 IKEv1 和 IKEv2 转换集。每个表均显示所配置的转换集的名称和详细信息。

### IKEv1 IPsec 提议（转换集）

- **模式** - 应用 ESP 加密和身份验证的模式。此字段确定原始 IP 数据包的哪个部分已应用 ESP。
  - **隧道模式** -（默认）将 ESP 加密和身份验证应用至整个原始 IP 数据包（IP 报头和数据），从而隐藏最终的源地址和目的地址。整个原始 IP 数据报经过加密，成为新 IP 数据包中的负载。此模式允许路由器等网络设备用作 IPsec 代理。也就是说，路由器代表主机执行加密。源路由器加密数据包并将其沿 IPsec 隧道转发。目标路由器解密原始 IP 数据报并将其转发到目标系统。隧道模式的主要优势是不需要修改终端系统即可获得 IPsec 的优势。隧道模式还可以防止流量分析；利用隧道模式，攻击者只能确定隧道终端，而无法确定通过隧道传送的数据包的真正源和目标，即使其与隧道终点一样也无法确定。
  - **传输模式** - 仅加密 IP 负载，原始 IP 报头保持不变。此模式的优势是每个数据包只需增加几个字节并且允许公共网络上的设备查看数据包的最终源和目标。在传输模式下，可以根据 IP 报头中的信息在中间网络上启用特殊处理（例如 QoS）。然而，第 4 层报头将被加密，这就限制了对数据包的检查。
- **ESP 加密** - 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、可选的数据身份验证和防重放服务。ESP 会封装将要保护的数据。
- **ESP 身份验证** - 转换集的 ESP 身份验证算法。

### IKEv2 IPsec 提议

- **模式** - 应用 ESP 加密和身份验证的模式。此字段确定原始 IP 数据包的哪个部分已应用 ESP。
  - **隧道模式** -（默认）封装模式将为隧道模式。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 报头和数据），从而隐藏最终的源地址和目的地址。整个原始 IP 数据报经过加密，成为新 IP 数据包中的负载。

此模式允许路由器等网络设备用作IPsec代理。也就是说，路由器代表主机执行加密。源路由器加密数据包并将其沿 IPsec 隧道转发。目标路由器解密原始 IP 数据报并将其转发到目标系统。

隧道模式的主要优势是不需要修改终端系统即可获得IPsec的优势。隧道模式还可以防止流量分析；利用隧道模式，攻击者只能确定隧道终端，而无法确定通过隧道传送的数据包的真正源和目标，即使其与隧道终点一样也无法确定。

- **传输模式** - 封装模式将为传输模式，且可选择在对等体不支持时回退到隧道模式。在传输模式下，仅加密 IP 负载，原始 IP 报头保持不变。

  此模式的优势是每个数据包只需增加几个字节并且允许公共网络上的设备查看数据包的最终源和目标。在传输模式下，可以根据IP报头中的信息在中间网络上启用特殊处理（例如 QoS）。然而，第 4 层报头将被加密，这就限制了对数据包的检查。

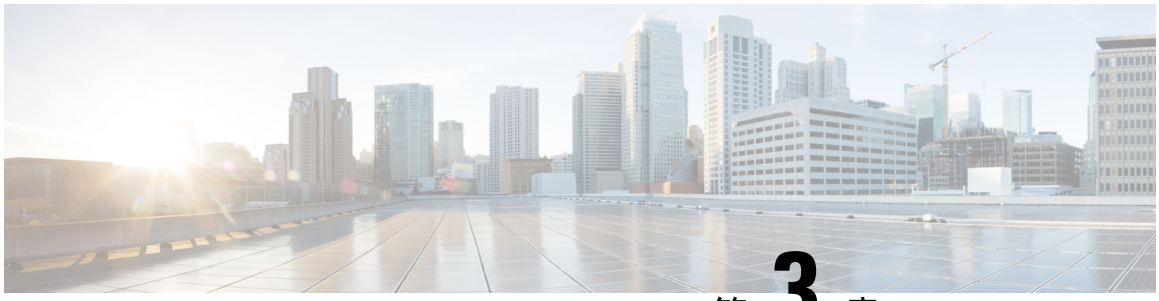
- **传输必要** - 封装模式将为仅传输模式，不允许回退到隧道模式。

**注释** 不建议将传输模式用于远程访问 VPN。

例如，封装模式的协商如下所示：

- 如果发起方提议传输模式而响应方以隧道模式响应，发起人将回退到隧道模式。
- 如果发起方提议隧道模式而响应方以传输模式响应，响应方不会回退到隧道模式。
- 如果发起方提议隧道模式而响应方为传输必要模式，则响应方将发送“没有选择提议”。
- 同样，如果发起方为传输必要模式而响应方为隧道模式，响应方将发送“没有选择提议”。

- **加密** - 显示 IKEv2 IPsec 提议的封装安全协议 (ESP) 加密算法。ESP 可提供数据隐私服务、可选的数据身份验证和防重放服务。ESP 会封装将要保护的数据。
- **完整性散列** - 显示确保 ESP 协议的数据完整性的散列算法。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。



第 3 章

# 高可用性选项



# 高可用性选项

分布式VPN集群、负载均衡和故障切换功能是工作方式不同并具有不同要求的高可用性功能。在某些情况下，您可能会在部署中使用多项功能。以下几节介绍了这些功能：有关分布式VPN和故障切换的详细信息，请参阅相应版本的《ASA常规操作ASDM配置指南》。此处介绍了负载均衡的详细信息。

## FXOS 机箱上的 VPN 和集群

ASA FXOS 集群支持站点间 VPN 两个相互排斥的模式之一，即集中式或分布式：

- 集中式 VPN 模式。默认模式。在集中式模式下，仅与集群的主设备建立 VPN 连接。

  VPN 功能仅限主设备使用，且不能利用集群的高可用性功能。如果主设备发生故障，所有现有的 VPN 连接都将断开，通过 VPN 连接的用户将遇到服务中断。选举出新的主设备后，您必须重新建立 VPN 连接。

  将 VPN 隧道连接到跨接口地址时，连接会自动转移到主设备。与 VPN 相关的密钥和证书将被复制到所有设备。

- 分布式 VPN 模式。在此模式下，站点间 IPsec IKEv2 VPN 连接将跨 ASA 集群成员分布，从而提供可扩展性。在集群成员之间分布 VPN 连接可实现充分利用集群的容量和吞吐量，将 VPN 支持大幅扩展至集中式 VPN 功能之外。

注释 集中式 VPN 集群模式支持站点间 IKEv1 和站点间 IKEv2。

分布式 VPN 集群模式仅支持站点间 IKEv2。

仅在 Firepower 9300 上支持分布式 VPN 集群模式。

集中式和分布式集群模式均不支持远程接入 VPN。

## 负载均衡

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。它基于简单的流量分配，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，一台设备是虚拟主用设备，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。负载均衡可以将流量定向至集群中负载最低的设备，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。

## 故障切换

故障切换配置需要通过专用故障切换链路和状态故障切换链路（后者可选）相互连接的两台相同ASA。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切换条件的时刻。如果这些条件得到满足，则会进行故障切换。故障切换同时支持 VPN 和防火墙配置。

ASA 支持两种故障切换配置：主用/主用故障切换和主用/备用故障切换。

使用主用/主用故障切换时，两台设备都可以传送网络流量。这不是真正的负载均衡，尽管看似具有相同的效果。发生故障切换时，剩下的那台主用设备会根据配置的参数接管合并流量的传送。因此，配置主用/主用故障切换时，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/备用故障切换时，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/备用故障切换允许使用第二台 ASA 来接管故障设备的功能。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

## 关于负载均衡

如果您拥有一个远程客户端配置，在该配置中使用连接至相同网络的两个或更多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，并提高性能和可用性。

要实施负载均衡，您可以将相同专用 LAN 到 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，虚拟集群显示为单一虚拟集群 *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。

如果集群中的一台设备发生故障，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。

## VPN 负载均衡算法

主用设备会维护一份按 IP 地址升序排序的备用集群成员列表。每个备用集群成员的负载会计算为整数百分比（活动会话数）。AnyConnect 非活动会话不会计入负载均衡的 SSL VPN 负载。主用设备将 IPsec 和 SSL VPN 隧道重定向至负载最低的设备，直到其百分比值比其余设备高出 1%。当所有备用集群成员的百分比值都比主用设备高出 1% 时，主用设备会将负载重定向至自身。

例如，如果您有一个主用和两个备用集群成员，则以下循环适用：

注释 所有节点的百分比值都从 0% 开始，而且所有百分比值都会四舍五入。

1. 如果所有成员的负载都比主用设备高出 1%，则主用设备会接受连接。
2. 如果主用设备没有接受连接，则哪台备用设备负载百分比值最低就由哪台备用设备接受会话。
3. 如果所有成员的负载百分比值相同，则由会话数最少的备用设备获得会话。
4. 如果所有成员的负载百分比值和会话数都相同，则由 IP 地址最少的设备获得会话。

## VPN 负载均衡集群配置

负载均衡集群可由相同版本或混合版本的 ASA 组成，并受到以下限制：

- 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。
- 包含混合版本 ASA 或相同版本 ASA 的负载均衡集群仅可支持 IPsec 会话。不过，在这样的配置中，ASA 可能无法达到其最高 IPsec 容量。

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) 版软件的负载均衡计算的不同之处在于，此平台使用加权算法，在某些硬件平台上，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。

## 典型的混合集群场景示例

如果采用混合配置 - 也就是说，如果负载均衡集群包含运行混合版本 ASA 软件的设备 - 则当初始的集群主用设备发生故障而另一台设备作为主用设备接管时，加权算法之间的差异会成为问题。

以下场景说明了如何在运行 ASA 7.1(1) 版本和 ASA 7.0(x) 版本软件的混合 ASA 组成的集群中使用 VPN 负载均衡。

### 场景 1：无 SSL VPN 连接的混合集群

在此场景中，集群由 ASA 混合组成。部分 ASA 集群对等体运行 ASA 7.0(x) 版本软件，部分对等体运行 7.1(1) 版本软件。软件版本低于 7.1(1) 版本的对等体没有任何 SSL VPN 连接，7.1(1) 版本集群对等体只有基本 SSL VPN 许可证，该许可证允许两个 SSL VPN 会话，但没有 SSL VPN 连接。在这种情况下，所有连接均为 IPsec 连接，负载均衡可以正常工作。

### 场景 2：处理 SSL VPN 连接的混合集群

例如，假设运行 ASA 7.1(1) 版本软件的 ASA 是初始的集群主用设备，然后该设备发生故障。集群中的另一台设备作为主用设备自动接管，并应用其自身的负载均衡算法来确定集群内的处理器负载。运行 ASA 7.1(1) 版本软件的集群主用设备不能以该软件提供的方式之外的任何其他方式确定会话负载的权重。因此，它不能正确地向运行更低版本软件的 ASA 设备分配合并的 IPsec 和 SSL VPN 会话负载。以下场景对此困境进行了说明。

此场景与上一场景的类似之处在于，集群由混合的 ASA 组成。部分 ASA 集群对等体运行 ASA 7.0(x) 版本软件，部分对等体运行 7.1(1) 版本软件。然而，在此情况下，集群却可以处理 SSL VPN 连接以及 IPsec 连接。

如果运行低于 ASA 7.1(1) 版本的软件的设备是集群主用设备，则主用设备会应用在 7.1(1) 版本之前生效的协议和逻辑。也就是说，会话可能会被定向至已超过其会话限制的负载均衡对等体。在这种情况下，用户的访问会被拒绝。

如果集群主用设备是运行 ASA 7.0(x) 版本软件的设备，旧版会话加权算法只会应用于集群中 7.1(1) 之前版本的对等体。在这种情况下，用户的访问都不会被拒绝。因为 7.1(1) 之前版本的对等体使用会话加权算法，其负载较低。

然而，因为您无法保证 7.1(1) 版本的对等体始终是集群主用设备，所以将会出现问题。如果集群主用设备发生故障，另一对等体会承担主用设备的角色。新的主用设备可能是任意符合条件的对等体。因为结果不可预测，我们建议您避免配置这种类型的集群。

# 有关负载均衡的常见问题

#### 多情境模式

**问:** 在多情景模式下是否支持负载均衡？

**答:** 在多情景模式下，既不支持负载均衡也不支持状态故障切换。

#### IP 地址池耗尽

**问:** ASA 是否会将 IP 地址池耗尽视为其 VPN 负载均衡方法的一部分？

**答:** 不会。如果远程访问 VPN 会话被定向至已耗尽其 IP 地址池的设备，则会话不会建立。负载均衡算法基于负载，会计算为每个备用集群成员提供的整数百分比（活动会话数和最大会话数）。

#### 唯一 IP 地址池

**问:** 要实施 VPN 负载均衡，不同 ASA 上的 AnyConnect 客户端或 IPsec 客户端的 IP 地址池必须是唯一的吗？

**答:** 是的。IP 地址池对于每台设备必须是唯一的。

#### 在相同设备上使用负载均衡和故障切换

**问:** 一台设备可以同时使用负载均衡和故障切换吗？

**答:** 可以。在此配置中，客户端连接至集群的IP地址，然后被重定向至集群中负载最低的ASA。如果该设备发生故障，备用设备会立即接管，不会对 VPN 隧道产生任何影响。

#### 多个接口上的负载均衡

**问:** 如果我们在多个接口上启用 SSL VPN，是否可以为所有的这些接口实施负载平衡？

**答:** 只能定义一个接口作为公共接口加入集群。这个想法是为了均衡CPU负载，多个接口会在相同 CPU 上融合，因此多个接口上的负载均衡这个概念没有意义。

#### 负载均衡集群的最大并行会话数

**问:** 请考虑有两台 ASA 5525-X 的部署，每台设备均有一个 100 位用户的 SSL VPN 许可证。在负载均衡集群中，最大用户总数是允许 200 个并行会话还是仅允许 100 个并行会话？如果我们随后添加第三台设备，该设备有一个 100 位用户的许可证，我们此时能够支持 300 个并行会话吗？

**答:** 使用VPN负载均衡的情况下，所有设备均处于活动状态，因此集群可以支持的最大会话数为集群中每台设备的会话数量的总和，在这种情况下为 300。

# 负载均衡的许可

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。

# VPN 负载均衡准则和限制

另请参阅负载均衡的必备条件，第 44 页。

### 符合条件的平台

负载均衡集群可以包含 ASA 型号 ASA 5512-X（带增强型安全许可证）以及型号 5515-X 及以上型号。虽然混合配置是可行的，但如果集群是同构的，管理通常更为简单。

### 符合条件的客户端

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）

### 客户端注意事项

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。包括 LAN 到 LAN 在内的所有其他 VPN 连接类型（L2TP、PPTP、L2TP/IPsec）可以连接到在其上启用了负载均衡的 ASA，但不能加入负载均衡。

当多个 ASA 节点组成集群进行负载均衡并且 AnyConnect 客户端连接需要使用组 URL 时，各个 ASA 节点必须：

- 使用每个负载均衡虚拟集群地址（IPv4 和 IPv6）的组 URL 配置每个远程访问连接配置文件。
- 为此节点的 VPN 负载均衡公共地址配置组 URL。

### 情景模式

多情景模式下不支持 VPN 负载均衡。

### 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，则该证书应该具有包含集群 IP 地址和集群 FQDN 的 SAN 扩展，并应包含带每个 ASA 的 IP 和 FQDN 的使用者备用名称扩展。如果该集群使用多个证书，则每个 ASA 的证书均应具有包含集群 IP、集群 FQDN 和各 ASA 的 IP 地址和 FQDN 的 SAN 扩展。

### 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。

# 配置负载均衡

如果您拥有一个远程客户端配置，在该配置中使用连接至相同网络的两个或更多 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。

要使用负载均衡，请在集群中的每台设备上执行以下操作：

- 通过建立通用的 VPN 负载均衡集群属性来配置负载均衡集群。这包括集群的虚拟集群 IP 地址、UDP 端口（如需要）和 IPsec 共享密钥。所有加入集群的设备都必须采用相同的集群配置，但集群内的设备优先级除外。
- 在设备上启用负载均衡并定义设备特定属性（例如其公有和私有地址），从而配置加入的设备。这些值因设备而异。

## 负载均衡的必备条件

另请参阅VPN 负载均衡准则和限制，第 43 页。

- 默认情况下会禁用负载均衡。必须显式启用负载均衡。
- 必须先配置公共（外部）和专用（内部）接口。本节中的后续引用使用名称 outside 和 inside。

  要执行此配置，请依次转到**配置 > 设备设置 > 接口设置 > 接口**。
- 您必须事先配置虚拟集群 IP 地址所引用的接口。建立集群通用的虚拟集群 IP 地址、UDP 端口（如需要）和 IPsec 共享密钥。
- 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。
- 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。
- 如果使用主用/主用状态故障切换或 VPN 负载均衡，则不支持本地 CA 功能。本地 CA 不能从属于另一 CA；它只能用作根 CA。

# 使用高可用性和可扩展性向导配置 VPN 负载均衡

过程

**步骤 1** 依次选择**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。在公共子网地址范围内，指定由虚拟集群中所有 ASA 共享的 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 到 LAN 隧道进行通信。要禁用 IPSec 加密，请取消选中 **Enable IPSec Encryption** 复选框。

注释 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 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。范围是从 1 到 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。

注释 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。

### 下一步做什么

当多个 ASA 节点组成集群进行负载均衡并且 AnyConnect 客户端连接需要使用组 URL 时，各个 ASA 节点必须：

- 使用每个负载均衡虚拟集群地址（IPv4 和 IPv6）的组 URL 配置每个远程访问连接配置文件。
- 为此节点的 VPN 负载均衡公共地址配置组 URL。

组 URL 在**配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 连接配置文件 >** 连接配置文件名称 > **添加或编辑 > 高级 > 组别名/组 URL** 窗格中配置。

## 配置 VPN 负载均衡（不使用向导）

### 过程

**步骤 1** 依次选择**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。在公共子网地址范围内，选择由虚拟集群中所有 ASA 共享的 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。
- **集群 IPv6 地址** - 指定代表整个 IPv6 虚拟集群的单一 IPv6 地址。在公共子网地址范围内，选择由虚拟集群中所有 ASA 共享的 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 IPv6 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。

  注释　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 到 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。范围是从 1 到 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。

  **注释** 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，会成为备份设备。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 会将此设备的 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 对此设备的 IP 地址进行转换得到的 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。

  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，证书将在重定向至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。

  **注释** 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。

  有关详细信息，请参见启用使用 FQDN 的无客户端 SSL VPN 负载均衡，第 48 页。

### 下一步做什么

当多个 ASA 节点组成集群进行负载均衡并且 AnyConnect 客户端连接需要使用组 URL 时，各个 ASA 节点必须：

- 使用每个负载均衡虚拟集群地址（IPv4 和 IPv6）的组 URL 配置每个远程访问连接配置文件。
- 为此节点的 VPN 负载均衡公共地址配置组 URL。

组 URL 在**配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 连接配置文件 >** 连接配置文件名称 > **添加或编辑 > 高级 > 组别名/组 URL** 窗格中配置。

## 启用使用 FQDN 的无客户端 SSL VPN 负载均衡

### 过程

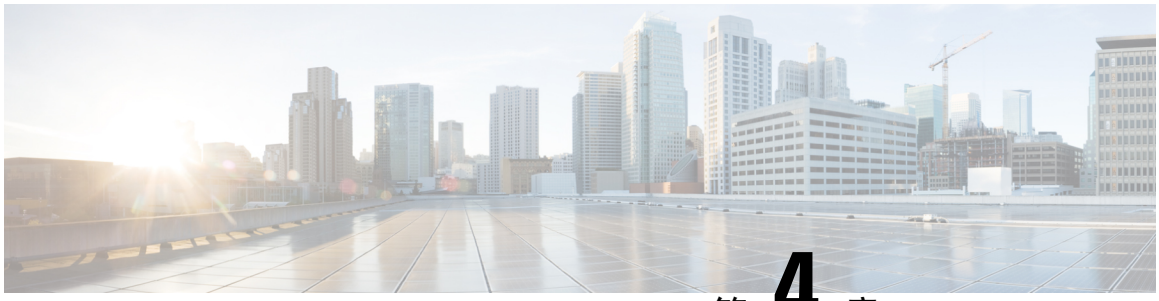
**步骤 1** 通过选中 **Send FQDN to client instead of an IP address when redirecting** 复选框为负载均衡启用 FQDN。

**步骤 2** 将每个 ASA 外部接口的条目添加到 DNS 服务器中（如果其中尚无这些条目）。每个 ASA 外部 IP 地址都应该有一个与其关联的 DNS 条目用于查找。对于反向查找，也必须启用这些 DNS 条目。

**步骤 3** 在 ASA 上的**配置 > 设备管理 > DNS > DNS 客户端**对话框中，对拥有通向 DNS 服务器路由的所有接口启用 DNS 查找。

**步骤 4** 在 ASA 上定义 DNS 服务器 IP 地址。为此，请在此对话框中点击**添加**。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**。



第 4 章

# 常规 VPN 设置

# 系统选项

通过**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPsec > 系统选项**窗格（也可以使用**配置 > 站点间 VPN > 高级 > 系统选项**访问），可以在 ASA 上配置特定于 IPsec 和 VPN 会话的功能。

- 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 - 指定保持连接消息的频率（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。默认情况下该选项处于禁用状态。

  **注释** 未丢弃隧道 TCP 流量，因此其依靠 TCP 超时进行清除。但是，如果为特定隧道流量禁用了超时，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。
- 支持入站 IPsec 会话绕过接口访问列表。“组策略和按用户授权 ACL 仍然适用于流量”- 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）。选中此选项时，也无需解密的 VPN 数据包的本地 IP 地址的访问规则。由于通过 VPN 安全机制成功中断了 VPN 隧道，此功能可简化配置并最大程度地提高 ASA 性能，而且不会带来任何安全风险。（组策略和逐个用户授权 ACL 仍然适用于流量。）

  通过取消选中此选项，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。

- Permit communication between VPN peers connected to the same interface - 启用或禁用此功能。

  您还可以通过同一接口在未加密及已加密的情况下重新引导传入客户端VPN流量回退。如果通过同一接口在未加密的情况下退送 VPN 流量，则应该为接口启用 NAT，以便公用可路由地址替换专用 IP 地址（除非已在本地 IP 地址池中使用公用 IP 地址）。

- Compression Settings - 指定要为其启用压缩的功能：WebVPN 和 SSL VPN 客户端。默认情况下会启用压缩。

# 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：

### 过程

**步骤 1** 依次选择**配置** > **远程访问 VPN** > **高级** > **最大 VPN 会话数**。

**步骤 2** 在**最大 AnyConnect 会话数**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**最大其他 VPN 会话数**字段中，输入允许的最大 VPN 会话数，其中包括思科 VPN 客户端 (IPsec IKEv1) LAN 到 LAN 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**应用**。

# 配置 DTLS

数据报传输层安全 (DTLS) 允许 AnyConnect 客户端建立 SSL VPN 连接，以便使用两个并行隧道 - SSL 隧道和 DTLS 隧道。使用 DTLS 可避免与 SSL 连接关联的延迟和带宽问题，并且提高对于数据包延迟敏感的实时应用的性能。

### 开始之前

请参阅 SSL 设置，第 203 页在此头端上配置 DTLS 和使用的 DTLS 版本。

为使DTLS能够回退至TLS连接，必须启用对等体存活检测(DPD)。如果没有启用DPD，则当DTLS连接遇到问题时，连接会终止而不是回退至 TLS。有关 DPD 的详细信息，请参阅内部组策略，AnyConnect 客户端，对等体存活检测，第 78 页。

过程

步骤 1 为 AnyConnect VPN 连接指定 DTLS 选项：

a) 依次转到**配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 连接配置文件**，访问**接口**部分。

b) 在**接口**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。

- 当您选中或启用 **SSL 访问/允许访问**时，系统会默认选中或启用**启用 DTLS**。
- 要禁用 DTLS，请取消选中**启用 DTLS**。SSL VPN 连接将只与 SSL VPN 隧道连接。

c) 选择**端口设置**以配置 **SSL 端口**。

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

步骤 2 为特定组策略指定 DTLS 选项。

a) 依次转到**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略**，然后依次选择**添加/编辑> 高级 > AnyConnect 客户端**。

b) 对**数据报传输层安全 (DTLS)**，选择“继承（默认）”、“启用”或“禁用”。

c) 对 **DTLS 压缩**（用于配置 DTLS 压缩），选择“继承（默认）”、“启用”或“禁用”。

# 配置 DNS 服务器组

**配置 > 远程访问 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。

- Add or Edit - 打开 Add or Edit DNS Server Group 对话框。在其他位置存在的内容的帮助
- Delete - 从表中删除所选行。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。

# 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。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。以下步骤说明如何在单情景或多情景模式下配置加密核心池。

加密核心再均衡在以下平台上可用：

- 5585-X
- 5545-X
- 5555-X
- ASASM

过程

步骤 1 依次选择配置 > 远程访问 VPN > 高级 > 加密引擎。

步骤 2 在“加速器偏爱”下拉列表中，指定如何分配密码加速器处理器：

注释 仅当 ASA 中提供此功能时，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 点击应用。

# SSL VPN 连接的客户端寻址

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。

- Global Client Address Assignment Policy - 配置会影响所有 IPsec 和 SSL VPN 客户端连接（包括 AnyConnect 客户端连接）的策略。ASA 按顺序使用所选源，直到其找到地址为止：
  - “使用身份验证服务器”- 指定 ASA 应该尝试使用身份验证服务器作为客户端地址源。
  - “使用 DHCP”- 指定 ASA 应该尝试使用 DHCP 作为客户端地址源。
  - “使用地址池”- 指定 ASA 应该尝试使用地址池作为客户端地址源。
- 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。

- 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

“选择地址池”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，并可供您在该列表中添加、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 - 删除所选地址池。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。

#### Add or Edit an IP Address Pool

配置或修改 IP 地址池。

- 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。

# 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 用户没有组策略关联。组策略信息供 VPN 连接配置文件（隧道组）和用户账户使用。

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：分割隧道、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 (General | More Options | Access Hours)。
- 过滤器 (General| More Options | Filters)。
- IPsec 安全关联 (Configuration | Policy Management | Traffic Management | Security Associations)。
- 用于过滤和分割隧道的网络列表 (Configuration | Policy Management | Traffic Management | Network Lists)。
- 用户身份验证服务器和内部身份验证服务器 (Configuration | System | Servers | Authentication)。

可以配置以下类型的组策略：

- 外部组策略，第 56 页 - 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。
- 内部组策略，第 58 页 - 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。
- AnyConnect 客户端内部组策略，第 63 页
- 无客户端 SSL VPN 内部组策略，第 86 页 - 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 隧道来得到保护。
- 站点到站点内部组策略，第 90 页

### 组策略窗格字段

ASDM 中的 Configuration > Remote Access VPN > Network (Client) Access > Group Policies 窗格列出当前配置的组策略。Add、Edit 和 Delete 按钮可帮助您管理 VPN 组策略，如下所述。

- 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 - 通过它可从列表中删除 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。

# 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 服务器将查询视为用户 X 的身份验证请求。因此，外部组其实只是 RADIUS 服务器上对 ASA 具有特殊意义的用户账户。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。

将 ASA 配置为使用外部服务器之前，必须使用正确的 ASA 授权属性来配置该服务器，并从其中一部分属性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。

这些 RADIUS 配置包括使用 LOCAL 身份验证的 RADIUS、使用 Active Directory/Kerberos Windows DC 的 RADIUS、使用 NT/4.0 域的 RADIUS 以及使用 LDAP 的 RADIUS。

### 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，此字段仅作显示用途字段。
- 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《思科 *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。

注释 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（例如思科 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，它仅与 RADIUS 服务器通信。

注释 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 服务器的账户已禁用指示。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。

# 内部组策略

## 内部组策略，常规属性

在**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略**窗格上，可通过“添加或编辑组策略”对话框为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。

在 ASDM 中，通过依次选择**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > 添加/编辑 > 常规**，可以配置内部组策略的常规属性。以下属性适用于 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。

- **名称** - 指定该组策略的名称，最多 64 个字符；允许使用空格。对于 Edit 功能，此字段为只读。
- **横幅** - 指定登录时要向用户显示的横幅文本。长度最多 4000 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 <BR> 标记。

- **SCEP 转发 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。
- **地址池** - 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 。

  **注释** 可以为内部策略组同时指定 IPv4 和 IPv6 地址池。

  **选择** - 取消选中“继承”复选框以激活此按钮。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 地址池** - 指定要用于该组策略的一个或多个 IPv6 地址池的名称。

选择 - 取消选中“继承”复选框以激活此按钮。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 。

- **更多选项** - 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。
- **隧道协议** - 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：
  - **无客户端 SSL VPN** - 指定通过 SSL/TLS 来使用 VPN，该 VPN 使用 Web 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，这些企业资源包括企业网站、启用 Web 功能的应用、NT/AD 文件共享（启用 Web 功能）、邮件和其他基于 TCP 的应用。
  - **SSL VPN 客户端** - 指定使用思科 AnyConnect VPN 客户端或旧版 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，可为 VPN 隧道提供最完整的架构。站点到站点（点对点）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。
  - **经由 IPsec 的 L2TP** - 允许远程用户使用几种常用 PC 和移动 PC 操作系统随附的 VPN 客户端，通过公共 IP 网络与安全设备和专用企业网络建立安全连接。L2TP 使用经由 UDP 的 PPP（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。
- **过滤器** - 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，这些规则根据源地址、目的地址和协议等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 策略** - 选择要应用到该组策略的网络准入控制策略的名称。可以向每个组策略分配一个可选 NAC 策略。默认值为 --None--。
- **管理** - 打开“配置 NAC 策略”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。
- **访问时长** - 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。
- **同时登录数** - 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。

**注释** 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。

- **限制访问 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（未限制）外，该下拉列表仅显示此 ASA 中配置的 VLAN。

注释　此功能适用于 HTTP 连接，但不适用于 FTP 和 CIFS。

- **连接配置文件（隧道组）锁定** - 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，并阻止通过其他连接配置文件进行访问。默认继承值为 None。
- **最大连接时间** - 如果未选中**继承**复选框，则此参数用于设置最大用户连接时间（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**无限**（默认）。
- **空闲超时** - 如果未选中**继承**复选框，则此参数用于设置空闲超时（以分钟为单位）。

  如果在此期间连接上没有通信活动，则系统将终止此连接。最小值为 1 分钟，最大值为 10080 分钟，默认值为 30 分钟。要允许无限连接时间，请选中 **Unlimited**。
- **安全组标记 (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。
- **在智能卡删除时** - 在使用默认选项“断开连接”的情况下，如果删除用于身份验证的智能卡，则客户端将断开连接。如果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**。

  智能卡删除配置仅在使用 RSA 智能卡的 Microsoft Windows 上适用。
- **最大连接时间警告间隔** - 达到最大连接时间之前的时间间隔，此时系统会向用户显示一条消息。

  如果您取消选中**继承**复选框，系统将自动选中**默认**复选框。这将会话警报间隔设置为 30 分钟。如果要指定新值，请取消选中**默认**，然后指定 1 至 30 分钟的会话警报间隔。
- **定期证书身份验证时间间隔** - 定期重新执行证书身份验证之前的时间间隔（以小时为单位）。

  如果未选中**继承**复选框，则可以设置执行定期证书验证的时间间隔。其范围为 1 至 168 小时，默认设置为禁用。要允许无限验证，请选中 Unlimited。

## 配置内部组策略，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 服务器仅应用于完整的通道客户端（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。

过程

**步骤 1**　依次选择**配置** > **远程访问 VPN** > **网络（客户端）访问** > **组策略** > **添加/编辑** > **服务器**。

**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。可以指定两个 IPv4 地址和两个 IPv6 地址。

如果指定多个DNS服务器，则远程访问客户端尝试按在该字段中指定的顺序使用这些DNS服务器。

对于使用此组策略的客户端，此处进行的更改会覆盖 ASDM 上在 **Configuration > Remote Access VPN > DNS** 窗口中配置的 DNS 设置。

**步骤 4** 取消选中 WINS Servers **Inherit** 复选框。

**wins-server value** {**ip_address** [*ip_address*] | **none**}

**步骤 5** 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。

每次输入 **wins-server** 命令后，会覆盖现有设置。例如，如果配置 WINS 服务器 x.x.x.x，然后配置 WINS 服务器 y.y.y.y，第二条命令会覆盖第一条，并且 y.y.y.y 会成为唯一 WINS 服务器。对于多台服务器情况也如此。要添加 WINS 服务器而不覆盖以前配置的服务器，请在输入此命令时包含所有 WINS 服务器的 IP 地址。

**示例：**

以下示例显示如何在 CLI 中为名为 FirstGroup 的组策略配置 IP 地址为 10.10.10.15 和 10.10.10.30 的 WINS 服务器：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30
hostname(config-group-policy)#
```

**步骤 6** 通过点击 More Options 栏中的双向下箭头展开 **More Options** 区域。

**步骤 7** 如果在**配置 > 远程访问 VPN > DNS** 窗口中未指定默认域，则必须在**默认域**字段中指定默认域。使用域名和顶级域，例如 example.com。

**步骤 8** 点击**确定 (OK)**。

**步骤 9** 点击**应用**。

## 内部组策略，浏览器代理

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

此对话框配置将向客户端推送的属性，以重新配置 Microsoft Internet Explorer 设置：

- 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 Proxy Settings 对话框内的 Exceptions 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，远程用户必须使用思科 AnyConnect VPN 客户端。

  许多网络环境都定义将 Web 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。

  以下是如何使用 PAC 文件的一些示例：
  - 从列表中随机选择一个代理以实现负载均衡。
  - 按时刻或星期几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 Connections 选项卡。禁用此功能将保持 Connections 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。

# AnyConnect 客户端内部组策略

## 内部组策略，高级，AnyConnect 客户端

- Keep Installer on Client System - 启用以在远程计算机上允许永久客户端安装。启用此选项会禁用客户端的自动卸载功能。客户端仍保持安装在远程计算机上以进行后续连接，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 客户端对 ASA 进行 VPN 连接时，ASA 可以为客户端分配一个 IPv4、IPv6 或 IPv4 和 IPv6 两个地址。如果 ASA 对 AnyConnect 连接仅分配一个 IPv4 地址或一个 IPv6 地址，则您可以配置客户端旁路协议以丢弃 ASA 尚未分配 IP 地址的网络流量，或允许该流量绕过 ASA 并从客户端以未加密或“明文形式”发送。

  举例来说，假设 ASA 只分配一个 IPv4 地址到 AnyConnect 连接且终端被双堆叠。当终端尝试访问 IPv6 地址时，如果禁用客户端旁路协议，则会丢弃 IPv6 流量；但是，如果启用客户端旁路协议，则会从客户端以明文形式发送 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。

  **注释** 在漫游之后，您无法使用 AnyConnect 配置文件中的 ASA FQDN 来获取 ASA IP 地址。在负载均衡方案中，地址可能与正确的设备（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，则客户端会尝试重新连接到隧道以前建立的任意 IP 地址。为了支持不同 IP 协议（从 IPv4 到 IPv6）的网络之间的漫游，AnyConnect 必须在漫游之后执行设备 FQDN 的名称解析，以便为重新建立隧道确定使用哪个 ASA 地址。在初始连接中，客户端使用其配置文件中的 ASA FQDN。如果可用，在后续会话重新连接期间，它总是使用由 ASA 推送（并由管理员在组策略中配置）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 未由 ASA 推送，则客户端在不同 IP 协议的网络之间漫游后无法重新建立 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持连接消息的间隔，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。
- **用于下载的可选客户端模块** - 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）下载所需的模块。必须指定启用其他功能的模块的名称。AnyConnect客户端包含以下模块（一些较早的版本的模块较少）：
  - 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故障排除信息发送到思科 TAC。
  - AnyConnect 网络访问管理器 - 以前称为思科安全服务客户端，此模块为有线和无线网络访问提供 802.1X（第 2 层）和设备身份验证。
  - AnyConnect SBL - 登录前启动 (SBL) 通过在 Windows 登录对话框出现之前启动 AnyConnect，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。
  - AnyConnect Web Security Module - 以前称为 ScanSafe Hostscan，此模块集成到 AnyConnect 中。它会解构网页的元素，以便同时分析每个元素。然后，它可以根据定义的安全策略，允许可接受的内容并阻止恶意或不可接受的内容。
  - 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 Web 过滤基础设施，它使用此数据提供更好的 URL 过滤规则。

    **注释** 自 AnyConnect 版本 4.0 起不支持 Telemetry 模块。
  - ASA 终端安全评估模块 - 以前称为思科安全桌面主机扫描功能，终端安全评估模块集成到 AnyConnect 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终端安全评估。
  - ISE 终端安全评估 - 使用 OPSWAT v3 库执行终端安全评估检查，评估终端的合规性。然后，您可以限制网络访问权限直至终端合规，或者提高本地用户的权限。
  - AMP 启用程序 - 用作为终端部署高级恶意软件防护 (AMP) 的介质。它将面向终端的 AMP 软件从企业中本地托管的服务器推送到一个终端设备子集，并将AMP服务安装到现有用户群中。
  - 网络可视性模块-提升企业管理员执行容量和服务规划、审计、合规性和安全分析的能力。NVM收集终端遥测数据，在系统日志中记录流数据和文件信誉,并导出流记录给收集器（第三方供应商），由其执行文件分析并提供 UI 接口。
  - Umbrella 漫游安全模块 - 在没有处于活动状态的 VPN 时提供 DNS 层安全。它提供思科 Umbrella 漫游服务或 OpenDNS Umbrella 服务（增加了智能代理和 IP 层实施功能）订用。

Umbrella 安全漫游配置文件将每个部署与相应的服务相关联，并自动启用相应的保护级别（是内容过滤、多项策略、强大的报告功能、Active Directory 集成，还是基本 DNS 层安全）。

- 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。

  **注释** 永久在线 VPN 需要支持 AnyConnect 安全移动功能的发行版。

- 
- 
- 要下载的客户端配置文件 - 配置文件是 AnyConnect 客户端用于配置 VPN、网络访问管理器、Web 安全、ISE 终端安全评估、AMP 启用程序、网络可视性模块和 Umbrella 漫游安全模块设置的一组配置参数。点击**添加**启动“选择 AnyConnect 客户端配置文件”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 流量的分割隧道

分割隧道将一些 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“以明文形式”）。

通过创建分割隧道策略，为该策略配置访问控制列表，然后将分割隧道策略添加到组策略，可以配置分割隧道。当组策略发送到客户端时，该客户端使用分割隧道策略中的ACL来决定要将网络流量定向到的位置。

**注释** 分割隧道是一项流量管理功能而非安全功能。为实现最佳安全性，建议不启用分割隧道。

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，则源网络是分割隧道网络。目标网络会被忽略。
- 使用 any 或者使用分割-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，请为分割隧道**Policy**选择**Tunnel All Networks**。
- 仅当分割隧道策略为**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 将流量传递到在分割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，则无论分割隧道策略如何，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。

### 开始之前

- 必须使用适当的 ACE 创建访问列表。
- 如果已为 IPv4 网络创建一个分割隧道策略并为 IPv6 网络创建另一个分割隧道策略，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)。如果您尚未创建这些 ACL，请参阅常规操作配置指南。

在以下程序中，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会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。

### 过程

**步骤 1** 使用 ASDM 连接到 ASA 并依次导航到**配置** > **远程访问 VPN** > **网络（客户端）访问** > **组策略**。

**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** 依次选择**高级** > **分割隧道**。

**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。如果配置了分割-包含隧道，则网络列表必须包含指定的 DNS 服务器。可以在字段中输入完全限定域名，IPv4 或 IPv6 地址。

**步骤 5** 要禁用分割隧道，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；它不允许使用明文形式的流量。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。

要启用分割隧道，请选择 **No**（默认）。此设置指示客户端根据分割隧道策略通过隧道发送 DNS 查询。

**步骤 6** 要配置分割隧道，请取消选中**继承**复选框并选择分割隧道策略。如果不取消选中**继承**，组策略将使用默认组策略 **DfltGrpPolicy** 中定义的分割隧道设置。默认组策略中的默认分割隧道策略设置为 Tunnel All Networks。

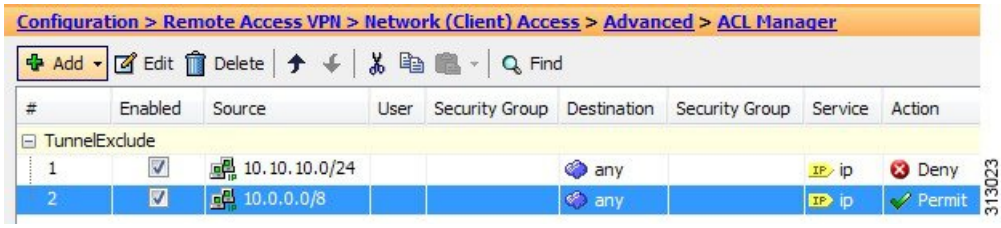
要定义分割隧道策略，请从下拉列表 **Policy** 和 **IPv6 Policy** 进行选择。Policy 字段定义 IPv4 网络流量的分割隧道策略。IPv6 Policy 字段选择 IPv6 网络流量的分割隧道策略。除该差异以外，这些字段还具有相同的用途。

通过取消选中**继承**，可以选择以下策略选项之一：

- **Exclude Network List Below** - 定义流量以明文形式发送到的网络列表。对于想要访问本地网络上的设备（如打印机），而通过隧道连接到公司网络的用户来说，此功能非常有用。
- **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。面向所有其他地址的数据以明文形式传播，并由远程用户的互联网运行商进行路由。

  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。客户端会忽略排除列表中的并非包含列表的子集的网络。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：




  **注释** 如果分割-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。如果分割-包含网络是本地子网的超集（例如 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，必须添加匹配的分割-包含网络（将 192.168.1.0/24 和 192.168.0.0/16 均指定为分割-包含网络）。

  如果分割-包含网络无效（如 0.0.0.0/0.0.0.0），则会禁用分割隧道（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。这实际上会禁用分割隧道。远程用户通过公司网络访问互联网，没有访问本地网络的权限。这是默认选项。

**步骤 7** 在 **Network List** 字段中，选择分割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 客户端可以将分割隧道与 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**确定**。

## 配置动态拆分隧道

通过动态拆分隧道，您可以在建立隧道后基于主机DNS域名动态调配拆分排除隧道。通过创建自定义属性并将其添加到组策略，可配置动态分割隧道。

### 开始之前

要使用此功能，必须具备 AnyConnect 版本 4.5（或更高版本）。有关进一步说明，请参阅关于动态分割隧道。

### 过程

**步骤 1** 浏览到**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络 (客户端) 访问 (Network (Client) Access) > 高级 (Advanced) > AnyConnect 自定义属性 (AnyConnect Custom Attributes)** 屏幕。

**步骤 2** 点击**添加**并输入 `dynamic-split-exclude-domains` 作为属性类型，然后输入说明。

**步骤 3** 点击以应用此新属性后，点击 UI 屏幕顶部的 **AnyConnect 自定义属性名称 (AnyConnect custom attribute names)** 链接。

**步骤 4** 为需要客户端从 VPN 隧道外部进行访问的每个云/Web 服务添加对应的自定义属性名称。例如，添加 Google_domains 以表示有关 Google Web 服务的 DNS 域名的列表。使用逗号分隔值 (CSV) 格式（用逗号分隔域），在“AnyConnect 自定义属性名称”屏幕的“值”部分中定义这些域。AnyConnect 仅考虑前 5000 个字符，不包括分隔符（约 300 个典型大小的域名)。超出该限制的域名会被忽略。

自定义属性不能超过 421 个字符。如果输入更大的值，ASDM 会将其分为多个值，上限为 421 个字符。将配置推送到客户端时，ASA 会连接特定属性类型和名称的所有值。

**步骤 5** 通过浏览到**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络 (客户端) 访问 (Network (Client) Access) > 组策略 (Group Policies)**，将动态拆分排除隧道属性连接到特定组策略。

**步骤 6** 您可以创建新的组策略或点击**编辑 (Edit)** 以管理现有组策略。

### 下一步做什么

如果已配置拆分包含隧道，则仅当至少一个 DNS 响应 IP 地址是拆分包含网络的一部分时，才会实施动态拆分排除。如果在任何 DNS 响应 IP 地址与任何拆分包含网络之间没有重叠，则实施动态拆分排除不是必需的，因为匹配所有 DNS 响应 IP 地址的流量已从隧道中排除。

## 配置动态拆分排除隧道

请使用 ASDM，按照以下配置步骤启用动态分割排除隧道。同时定义动态分割排除域和动态分割包含域时，能够通过域名匹配增强动态分割排除隧道。例如，管理员可以配置除 www.example.com

外，排除发往 example.com 的所有流量。*example.com* 是动态分割排除域，*www.example.com* 是动态分割包含域。

注释 必须具备 AnyConnect 版本 4.5（或更高版本）才能使用动态分割排除隧道。此外，AnyConnect 版本 4.6（及更高版本）增加了细化能力，在同时为动态分割包含和动态分割排除配置了域的情况下，可以增强这两种功能。动态分割排除适用于所有隧道全部、分割包含和分割排除配置。

### 开始之前

请参阅 AnyConnect 要求的动态分割隧道部分。

### 过程

**步骤 1** 浏览到**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络 (客户端) 访问 (Network (Client) Access) > 高级 (Advanced) > AnyConnect 自定义属性 (AnyConnect Custom Attributes)** 屏幕。

**步骤 2** 点击**添加**并输入 `dynamic-split-exclude-domains` 作为属性类型，然后输入说明。

**步骤 3** 点击以应用此新属性后，点击 UI 屏幕顶部的 **AnyConnect 自定义属性名称 (AnyConnect custom attribute names)** 链接。

**步骤 4** 为需要客户端从 VPN 隧道外部进行访问的每个云/Web 服务添加对应的自定义属性名称。例如，添加 Google_domains 以表示有关 Google Web 服务的 DNS 域名的列表。使用逗号分隔值 (CSV) 格式（用逗号分隔域），在“AnyConnect 自定义属性名称”屏幕的“值”部分中定义这些域。AnyConnect 仅考虑前 5000 个字符，不包括分隔符（约 300 个典型大小的域名)。超出该限制的域名会被忽略。

自定义属性不能超过 421 个字符。如果输入更大的值，ASDM 会将其分为多个值，上限为 421 个字符。将配置推送到客户端时，ASA 会连接特定属性类型和名称的所有值。

**步骤 5** 通过浏览到**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络 (客户端) 访问 (Network (Client) Access) > 组策略 (Group Policies)**，将动态拆分排除隧道属性连接到特定组策略。

**步骤 6** 您可以创建新的组策略或点击**编辑 (Edit)** 以管理现有组策略。

**步骤 7** 在左侧菜单中，点击**高级 > AnyConnect 客户端 > 自定义属性**，然后从下拉列表中选择属性类型。

## 配置动态拆分包含隧道

请使用 ASDM，按照以下配置步骤启用动态分割包含隧道。同时定义动态分割排除域和动态分割包含域时，能够通过域名匹配增强动态分割包含隧道。例如，管理员可以配置除 www.domain.com 外，包含发往 domain.com 的所有流量。*domain.com* 是动态分割包含域，*www.domain.com* 是动态分割排除域。

注释 必须具备 AnyConnect 版本 4.6（或更高版本）才能使用动态分割包含隧道。此外，AnyConnect 版本 4.6（及更高版本）增加了细化能力，在同时为动态分割包含和动态分割排除配置了域的情况下，可以增强这两种功能。动态分割包含仅适用于分割包含配置。

### 开始之前

请参阅 AnyConnect 要求的动态分割隧道部分。

### 过程

**步骤 1** 浏览到**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络 (客户端) 访问 (Network (Client) Access) > 高级 (Advanced) > AnyConnect 自定义属性 (AnyConnect Custom Attributes)** 屏幕。

**步骤 2** 点击**添加**并输入 `dynamic-split-include-domains` 作为属性类型，然后输入说明。

**步骤 3** 点击以应用此新属性后，点击 UI 屏幕顶部的 **AnyConnect 自定义属性名称 (AnyConnect custom attribute names)** 链接。

**步骤 4** 为需要客户端从 VPN 隧道外部进行访问的每个云/Web 服务添加对应的自定义属性名称。例如，添加 Google_domains 以表示有关 Google Web 服务的 DNS 域名的列表。使用逗号分隔值 (CSV) 格式（用逗号分隔域），在“AnyConnect 自定义属性名称”屏幕的“值”部分中定义这些域。AnyConnect 仅考虑前 5000 个字符，不包括分隔符（约 300 个典型大小的域名)。超出该限制的域名会被忽略。

自定义属性不能超过 421 个字符。如果输入更大的值，ASDM 会将其分为多个值，上限为 421 个字符。将配置推送到客户端时，ASA 会连接特定属性类型和名称的所有值。

**步骤 5** 依次浏览到**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略**，将动态分割排除隧道属性附加到特定组策略。

**步骤 6** 您可以创建新的组策略或点击**编辑 (Edit)** 以管理现有组策略。

**步骤 7** 在左侧菜单中，点击**高级 > AnyConnect 客户端 > 自定义属性**，然后从下拉列表中选择属性类型。

## 配置管理 VPN 隧道

管理 VPN 隧道可确保客户端系统在开启时连接到企业网络，这不仅限于最终用户建立了 VPN 连接的情况。您可以对办公室外的终端（尤其是用户很少通过VPN连接到办公网络的设备）执行补丁管理。需要企业网络连接的终端操作系统登录脚本也可以得益于此功能。

管理VPN隧道是为了向最终用户提供透明性；因此在默认情况下，用户应用发起的网络流量不会受到影响，而是会被定向到管理 VPN 隧道外部。

如果用户抱怨登录缓慢，可能表示管理隧道配置不当。有关管理 VPN 隧道的其他要求、不兼容问题、限制和故障排除，请参阅《思科 AnyConnect 安全移动客户端管理指南》。

### 开始之前

需要 AnyConnect 版本 4.7（或更高版本）。

### 过程

**步骤 1** 您必须依次导航到**配置 > 远程访问 > 网络（客户端）访问 > AnyConnect 连接配置文件 > 添加/编辑**，并从“身份验证”下的“方法”下拉菜单中选择“仅证书”，将隧道组的身份验证方法配置为“仅证书”。

**步骤 2** 然后，在同一个窗口中，依次选择**高级 > 组别名/组 URL** 并添加管理 VPN 配置文件中要指定的组 URL。

**步骤 3** 此隧道组的组策略必须使用该隧道组中配置的地址池为所有 IP 协议配置分割包含隧道：从**远程访问 VPN > 网络（客户端）访问 > 组策略 > 编辑 > 高级 > 分割隧道**中选择“下面的隧道网络列表”。

**步骤 4** （可选）默认情况下，管理VPN隧道需要分割包含隧道配置，以免影响用户发起的网络通信（因为其本意是为了提供透明性）。您可以在管理隧道连接所使用的组策略中配置自定义属性来覆盖此行为：AnyConnect 自定义属性，第 146 页。
如果未在隧道组中为两种 IP 协议配置地址池，则必须在组策略中启用客户端绕行协议，这样管理 VPN 隧道才不会中断与没有地址池的 IP 协议匹配的流量。

**步骤 5** 创建配置文件，然后选择管理 VPN 隧道供配置文件使用：配置 AnyConnect 客户端配置文件，第 130 页。

## 配置 Linux 以支持扩展子网

在为分割隧道配置了 **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，然后与为分割隧道配置的组策略相关联。

### 过程

**步骤 1** 连接到ASDM，然后依次导航到**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > AnyConnect 自定义属性**。

**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**高级 > AnyConnect 客户端 > 自定义属性**。

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

## 内部组策略、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。启用此选项会禁用客户端的自动卸载功能。客户端仍保持安装在远程计算机上以进行后续连接，从而缩短远程用户的连接时间。

  注释 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 客户端对 ASA 进行 VPN 连接时，ASA 可以为客户端分配一个 IPv4、IPv6 或 IPv4 和 IPv6 两个地址。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“以明文形式”从客户端进行发送。

  举例来说，假设 ASA 只分配一个 IPv4 地址到 AnyConnect 连接且终端被双堆叠。当终端尝试访问 IPv6 地址时，如果禁用客户端旁路协议，则会丢弃 IPv6 流量；但是，如果启用客户端旁路协议，则会从客户端以明文形式发送 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。

  注释 在漫游之后，您无法使用 AnyConnect 配置文件中的 ASA FQDN 来获取 ASA IP 地址。在负载均衡方案中，地址可能与正确的设备（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，则客户端会尝试重新连接到隧道以前建立的任意 IP 地址。为了支持不同 IP 协议（从 IPv4 到 IPv6）的网络之间的漫游，AnyConnect 必须在漫游之后执行设备 FQDN 的名称解析，以便为重新建立隧道确定使用哪个 ASA 地址。在初始连接中，客户端使用其配置文件中的 ASA FQDN。如果可用，在后续会话重新连接期间，它总是使用由 ASA 推送（并由管理员在组策略中配置）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 未由 ASA 推送，则客户端在不同 IP 协议的网络之间漫游后无法重新建立 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持连接消息的间隔，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。
- 用于下载的可选客户端模块 - 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）下载所需的模块。必须指定启用其他功能的模块的名称。AnyConnect客户端版本 4.0 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故障排除信息发送到思科 TAC。
  - AnyConnect 网络访问管理器 - 以前称为思科安全服务客户端，此模块为有线和无线网络访问提供 802.1X（第 2 层）和设备身份验证。
  - AnyConnect SBL - 登录前启动 (SBL) 通过在 Windows 登录对话框出现之前启动 AnyConnect，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。
  - AnyConnect Web Security Module - 以前称为 ScanSafe Hostscan，此模块集成到 AnyConnect 中。它会解构网页的元素，以便同时分析每个元素。然后，它可以根据定义的安全策略，允许可接受的内容并阻止恶意或不可接受的内容。
  - 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 Web 过滤基础设施，它使用此数据提供更好的 URL 过滤规则。

    **注释** AnyConnect 4.0 不支持遥测。

  - ASA 终端安全评估模块 - 以前称为思科安全桌面主机扫描功能，终端安全评估模块集成到 AnyConnect 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终端安全评估。
  - ISE 终端安全评估 - 使用 OPSWAT v3 库执行终端安全评估检查，评估终端的合规性。然后，您可以限制网络访问权限直至终端合规，或者提高本地用户的权限。
  - AMP 启用程序 - 用作为终端部署高级恶意软件防护 (AMP) 的介质。它将面向终端的 AMP 软件从企业中本地托管的服务器推送到一个终端设备子集，并将AMP服务安装到现有用户群中。
  - 网络可视性模块 - 提升企业管理员执行容量和服务规划、审计、合规性和安全分析的能力。NVM收集终端遥测数据，在系统日志中记录流数据和文件信誉,并导出流记录给收集器（第三方供应商），由其执行文件分析并提供 UI 接口。
  - Umbrella 漫游安全模块 - 在没有处于活动状态的 VPN 时提供 DNS 层安全。它提供思科 Umbrella 漫游服务或 OpenDNS Umbrella 服务（增加了智能代理和 IP 层实施功能）订用。

Umbrella 安全漫游配置文件将每个部署与相应的服务相关联，并自动启用相应的保护级别（是内容过滤、多项策略、强大的报告功能、Active Directory 集成，还是基本 DNS 层安全）。

- 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。

  **注释** 永久在线 VPN 需要支持 AnyConnect 安全移动功能的发行版。

- 要下载的客户端配置文件 - 配置文件是 AnyConnect 客户端用于配置 VPN、网络访问管理器、Web 安全、ISE 终端安全评估、AMP 启用程序、网络可视性模块和 Umbrella 漫游安全模块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。

## 内部组策略，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。

- 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。

## 使用客户端防火墙为 VPN 启用本地设备支持

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影响客户端如何处理公用和专用网络的客户端系统防火墙。

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（系留设备）。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（如打印机和系留设备）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。

注释 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。具有有限权限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程序：

- 为本地打印机支持部署客户端防火墙，第 76 页
- 为 VPN 配置系留设备支持，第 77 页

### 有关防火墙行为的使用说明

以下说明阐明了 AnyConnect 客户端如何使用防火墙：

- 源 IP 不能用于防火墙规则。客户端将忽视防火墙规则中从 ASA 发送来的源 IP 信息。客户端将根据规则是公共还是专用来确定源 IP。公共规则适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 规则的很多协议。但是，AnyConnect 防火墙功能仅支持 TCP、UDP、ICMP 和 IP。如果客户端收到一条具有不同协议的规则，它会将它视为无效的防火墙规则，然后禁用分割隧道并出于安全考虑使用完整隧道。
- 从 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。

请注意每个操作系统的以下行为差异：

- 对于 Windows 计算机，拒绝规则在 Windows 防火墙中优先于允许规则。如果 ASA 将一条允许规则下推到 AnyConnect 客户端，但用户创建了一条自定义拒绝规则，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。
- 防火墙服务必须由AnyConnect客户端启动（不能由系统自动启动）的Windows用户在建立VPN连接时所花的时间可能会显著增加。
- 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。全局规则始终都在最后。
- 对于第三方防火墙，只有当AnyConnect客户端防火墙和第三方防火墙都允许该流量类型时才能通过流量。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 8.3(1) 版或更高版本以及 ASDM 6.3(1) 版或更高版本来支持 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 1: AnyConnect_Client_Local_Print 中的 ACL 规则*

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

| 说明 | 权限 | 接口 | 协议 | 源端口 | 目的地址 | 目标端口 |
|---|---|---|---|---|---|---|
| NetBios | 允许 | 公共 | UDP | 默认 | 任意 | 137 |
| 注释 默认端口范围是 1 到 65535。 | | | | | | |

注释 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。

过程

**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**。

**步骤 3** 依次选择 **Advanced > AnyConnect Client > Client Firewall**。为专用网络规则点击 **Manage**。

**步骤 4** 创建包含上述 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。在此情况下，您可以转到配置文件编辑器中的**首选项（第 2 部分）**，并选中**应用最后的 VPN 本地资源规则**。

## 为 VPN 配置系留设备支持

要支持系留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，将分割隧道的 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。

注释 对于需要与运行 AnyConnect 的计算机同步的 Windows Mobile 设备，请在 ACL 中指定 IPv4 目的地址 169.254.0.0 或 IPv6 目的地址 fe80::/64。

过程

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

**步骤 2** 取消选中“网络列表”字段旁的**继承**，然后点击“管理”。

**步骤 3** 点击 **Extended ACL** 选项卡。

**步骤 4** 点击**添加 > 添加 ACL**。指定新 ACL 的名称。

**步骤 5** 选择表中的新 ACL 并点击**添加**，然后点击 **添加 ACE**。

**步骤 6** 对于**操作**，选择**允许**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**服务**，选择 IP。

**步骤 9** 点击 **确定**。

**步骤 10** 点击**确定**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 **确定**。

**步骤 13** 点击**应用**。

## 内部组策略，AnyConnect 客户端密钥重新生成

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，从而提高连接的安全性，此即为重新生成密钥协商。

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：

- 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。

**注释** 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。

## 内部组策略，AnyConnect 客户端，对等体存活检测

对等体存活检测 (DPD) 可确保 ASA（网关）或客户端可以快速检测到对等体无响应且连接已失败的情况。要启用对等体存活检测 (DPD) 并设置 AnyConnect 客户端或 ASA 网关执行 DPD 的频率，请执行以下操作：

### 开始之前

- 此功能仅适用于 ASA 网关与 AnyConnect SSL VPN 客户端之间的连接。它不适用于 IPsec，因为 DPD 基于不允许填充的标准实施，并且不支持无客户端 SSL VPN。
- 如果启用 DTLS，则也要启用对等体存活检测 (DPD)。DPD 允许已失败的 DTLS 连接回退至 TLS。否则，该连接会终止。
- 在 ASA 上启用 DPD 时，可以使用最佳 MTU (OMTU) 功能查找客户端可以成功传输 DTLS 数据包的最大终端 MTU。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。

### 过程

**步骤 1** 转到所需的组策略。

- 依次转到**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略**，**添加**或**编辑**所需组策略，然后打开**高级 > AnyConnect 客户端 > 对等体存活检测**窗格。
- 或者，如要访问特定的用户策略，请依次转到**配置 > 设备管理 > 用户/AAA > 用户账户**，添加或编辑所需用户账户，然后打开 **VPN 策略 > AnyConnect 客户端 > 对等体存活检测**窗格。

**步骤 2** 设置网关端检测。

取消选中**禁用**复选框以指定由安全设备（网关）执行 DPD。输入从 30 秒（默认值）到 3600 秒的间隔，安全设备按此间隔执行 DPD。建议使用值 300。

**步骤 3** 设置客户端检测。

取消选中**禁用**复选框以指定由客户端执行 DPD。然后，输入从 30 秒（默认值）到 3600 秒的间隔，客户端按此间隔执行 DPD。建议使用值 300。

## 内部组策略，AnyConnect 无客户端门户定制

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。

- 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。在身份验证成功后，立即向无客户端用户显示此页面。在 VPN 连接成功建立之后，AnyConnect 启动默认 Web 浏览器并访问此 URL。

注释 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 - 如果面向为其拒绝访问的用户，要创建要显示的消息，请在此字段中输入该消息。

## 在内部组策略中配置 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，并且该客户端用其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》。

自定义属性也可在 **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。

使用此程序添加或编辑自定义属性。您还可以删除已配置的自定义属性，但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。

过程

**步骤 1** 依次转到**配置** > **远程访问 VPN** > **网络（客户端）访问** > **组策略** > **添加/编辑** > **高级** > **AnyConnect 客户端** > **自定义属性**

**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**管理 (Manage)**，在**配置自定义属性类型 (Configure Custom Attribute Types)** 窗格中，点击**添加 (Add)**。

b) 在 **Create Custom Attribute Type** 窗格中，在 **Type** 和 **Description** 中输入新属性类型和说明，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，在 **Type** 中选择先前选择或配置的属性类型，然后在 **Name** 和 **Value** 中输入新属性名称和类型，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 客户端之前会合并。

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

**步骤 6** 点击 **Create Custom Attribute** 窗格中的 **OK**。

# IPsec (IKEv1) 客户端内部组策略

## 内部组策略，IPsec (IKEv1) 客户端的常规属性

通过**配置 > 远程访问 > 网络（客户端）访问 > 组策略 > 高级 > IPsec (IKEv1) 客户端 > 添加或编辑组策略 > IPsec** 对话框，可以为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：

- 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。用户有 30 秒时间输入凭证，在 SA 过期（大约两分钟）并且隧道终止之前最多可进行三次尝试。
- 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 复选框，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密钥（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 密钥信息破坏此 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。

**注释** 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 客户端的类型（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。
- 如果一个客户端与所有规则均不匹配，ASA 将拒绝此连接。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。
- 对整套规则的限制为 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**。

## 内部组策略，IPsec (IKEv1) 客户端的客户端防火墙

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。只有在 Microsoft Windows 上运行的 VPN 客户端才能使用这些防火墙功能。这些功能当前对于硬件客户端或其他（非 Windows）软件客户端不可用。

使用 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。

在第一个场景中，远程用户在 PC 上安装了个人防火墙。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 客户端会断开与 ASA 的连接。（此防火墙实施机制称为 Are You There [AYT]，因为 VPN 客户端通过定期向防火墙发送“are you there?”消息对其进行监控；如果没有响应，则 VPN 客户端知道防火墙关闭并会终止其与 ASA 的连接）。网络管理员可以在最初配置这些 PC 防火墙，但是如果采用此方法，每个用户就可以自定义自己的配置。

在第二个场景中，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。常见的例子是使用分割隧道阻止互联网流量传送到组中的远程PC。在已建立隧道的情况下，此方法可以保护PC，从而帮助中心站点抵御来自互联网的入侵。此防火墙场景称为推送策略或中心保护策略(CPP)。在 ASA 上创建要在 VPN 客户端上实施的流量管理规则集，将这些规则与过滤器关联，然后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 客户端依次将策略传递到本地防火墙，由其实施此策略。

**配置 > 远程访问 > 网络（客户端）访问 > 组策略 > 高级 > IPsec (IKEv1) 客户端 > 客户端防火墙**

### 字段

- **继承** - 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。
- **客户端防火墙属性** - 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。
- **防火墙设置** - 列出防火墙是否存在，如果存在，它是必选还是可选。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**必需防火墙**，则该组中的所有用户都必须使用指定防火墙。如果未安装并运行指定的受支持防火墙，ASA 会丢弃尝试进行连接的任何会话。在此情况下，ASA 会通知 VPN 客户端其防火墙配置不匹配。

  **注释** 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）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。如果创建的组中的某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。

- **防火墙类型** - 列出来自多个供应商（包括思科）的防火墙。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。
- **自定义防火墙** - 指定自定义防火墙的供应商 ID、产品 ID 和说明。
  - **供应商 ID** - 指定该组策略的自定义防火墙的供应商。
  - **产品 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。
  - **说明** -（可选）描述自定义防火墙。
- **防火墙策略** - 指定自定义防火墙策略的类型和源。

- **远程防火墙定义的策略 (AYT)** - 指定防火墙策略由远程防火墙定义 (Are You There)。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。
- **策略推送 (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 客户端上实施您从“策略推送 (CPP)”下拉列表中选择的过滤器所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，其中包括默认过滤器。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 客户端还有本地防火墙，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。
- **入站流量策略** - 列出入站流量的可用推送策略。
- **出站流量策略** - 列出出站流量的可用推送策略。
- **管理** - 显示“ACL 管理器”对话框，可在其中配置访问控制列表 (ACL)。

## 内部组策略，IPsec (IKEv1) 的硬件客户端属性

**配置 > 远程访问 > 网络（客户端）访问 > 组策略 > 高级 > IPsec (IKEv1) 客户端 > 硬件客户端**对话框用于设置将发送到 Easy VPN Remote 客户端的组策略属性。有关 ASA 上的 Easy VPN 支持的完整说明，请参阅 Easy VPN，第 209 页 一章。

**注释** VPN 3002 硬件客户端已停产并终止支持。

- **继承** -（多个实例）表示相应设置从默认组策略获取其值，而不是从其后的显式指定获取值。这是此对话框中所有属性的默认设置。
- **需要交互式客户端身份验证** - 指定是否要求进行交互式客户端身份验证。默认情况下，此参数处于禁用状态。

  当禁用时，将使用硬件客户端上存储的凭证进行身份验证。如果未存储凭证，硬件客户端将手动进行身份验证。如果存储或输入的凭证有效，则会建立隧道。

  当启用时，此选项要求硬件客户端在每次启动隧道时使用用户名和密码（无论客户端上是否存储了用户名和密码）手动进行身份验证，从而提供更高的安全性。如果输入的凭证有效，则会建立隧道。

  安全设备身份验证要求为硬件客户端使用的连接配置文件配置身份验证服务器组。如果需要在主要 ASA 上进行安全设备身份验证，请务必在所有备用服务器上也进行配置。

注释 在启用此功能的情况下，如要启动 VPN 隧道，必须有用户来输入用户名和密码。

- **需要个人用户身份验证** - 指定是否要求进行个人用户身份验证。个人用户身份验证可防止硬件客户端的专用网络中未经授权的人员访问中心站点。默认情况下，此参数处于禁用状态。

  启用个人用户身份验证时，即使隧道已存在，通过硬件客户端连接的每个用户仍然必须打开Web浏览器并手动输入有效的用户名和密码，才能访问 ASA 背后的网络。

  要进行身份验证，用户必须在浏览器的“位置”或“地址”字段中输入硬件客户端专用接口的IP地址。然后，浏览器会向硬件客户端显示登录对话框。要进行身份验证，请点击“连接/登录状态”。如果您的默认主页位于 ASA 背后的远程网络中，或者如果您将浏览器定向到 ASA 背后的远程网络中的网站，硬件客户端会将浏览器定向到正确的用户登录页面。当您成功登录后，浏览器将显示您最初输入的页面。

  如果启用用户身份验证，则用户无法使用命令行界面登录。您必须使用浏览器。如果您尝试访问 ASA 背后的网络中并非基于 Web 的资源（例如邮件），则在您使用浏览器进行身份验证之前，连接会失败。

  要显示横幅，必须启用个人用户身份验证。一个用户最多可以同时登录四个会话。

  如果需要在主要 ASA 上进行用户身份验证，请务必在所有备用服务器上也进行配置。

- **用户身份验证空闲超时** - 配置用户超时期限。安全设备如果在此期间未收到用户流量，则会终止连接。您可以指定超时期限为具体的分钟数或无限：
  - **无限** - 指定连接永不超时。此选项可防止从默认或指定的组策略继承值。
  - **分钟** - 指定超时期限（以分钟为单位）。使用 1 和 35791394 之间的一个整数。默认值为“无限”。

  响应 show uauth 命令所指示的空闲超时始终是思科 Easy VPN Remote 设备上进行隧道身份验证的用户的空闲超时值。

- **思科 IP 电话绕行** - 可让思科 IP 电话绕过交互式个人用户身份验证过程（如已启用）。默认情况下会禁用“思科 IP 电话绕行”。

  您必须将硬件客户端配置为对 IP 电话连接使用网络扩展模式。

- **LEAP 绕行** - 仅当启用**需要个人用户身份验证**时应用。可让来自思科无线设备的 LEAP 数据包绕过个人用户身份验证过程。默认情况下会禁用 LEAP 绕行。

  硬件客户端背后的 LEAP 用户面临着循环困境：他们无法协商 LEAP 身份验证，因为他们无法通过隧道将自己的凭证发送到中心站点设备背后的 RADIUS 服务器。而他们无法通过隧道发送凭证的原因是他们尚未在无线网络中进行身份验证。为解决此问题，LEAP 绕行让 LEAP 数据包（并且仅限 LEAP 数据包）穿过隧道，在个人用户进行身份验证之前，向 RADIUS 服务器进行无线连接身份验证。然后，用户继续进行个人用户身份验证。

  在以下情况下，LEAP 绕行可以正确运行：

- **需要交互式客户端身份验证**必须禁用。如果启用了交互式设备身份验证，则必须由一台非 LEAP（有线）设备对硬件客户端进行身份验证后，LEAP 设备才能使用该隧道进行连接。
- **需要个人用户身份验证**已启用。否则，LEAP 绕行不会应用。
- 无线环境中的无线接入点必须是运行思科发现协议 (CDP) 的思科 Aironet 无线接入点。PC 的无线网卡可以是其他品牌。

- **允许网络扩展模式** - 确定对该组中的硬件客户端使用网络扩展模式。默认情况下，此参数处于禁用状态。如果禁用网络扩展模式，硬件客户端必须以端口地址转换模式连接到此 ASA。

  硬件客户端需要网络扩展模式才能支持 IP 电话连接，因为呼叫管理器只能与实际 IP 地址进行通信。

**注释** 此组中的硬件客户端必须采用相似的配置。如果将硬件客户端配置为使用网络扩展模式而连接的 ASA 并未如此配置，则硬件客户端会每 4 秒尝试连接一次，但每个尝试都会被拒绝。在此情况下，硬件客户端会对其连接的 ASA 造成不必要的处理负载；如果大量硬件客户端采用这种方式错误配置，则会降低安全设备提供服务的能力。

# 无客户端 SSL VPN 内部组策略

## 内部组策略，无客户端 SSL VPN 常规属性

**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 组策略 > 添加/编辑 > 常规**

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。

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。整体横幅长度最多 4000 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 <BR> 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：
  - “无客户端 SSL VPN”- 指定通过 SSL/TLS 来使用 VPN，该 VPN 使用 Web 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，这些企业资源包

括企业网站、启用 Web 功能的应用、NT/AD 文件共享（启用 Web 功能）、邮件和其他基于 TCP 的应用。

- SSL VPN Client - 指定使用思科 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，可为 VPN 隧道提供最完整的架构。站点到站点（点对点）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。
- “经由 IPsec 的 L2TP”- 允许远程用户使用几种常用 PC 和移动 PC 操作系统随附的 VPN 客户端，通过公共 IP 网络与安全设备和专用企业网络建立安全连接。L2TP 使用经由 UDP 的 PPP（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、添加或删除 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。

  **注释** 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（“无限”）外，该下拉列表仅显示此 ASA 上配置的 VLAN。

  **注释** 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。
- **最大连接时间** - 如果未选中**继承**复选框，则此参数用于设置最大用户连接时间（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**无限**（默认）。
- **空闲超时** - 如果未选中**继承**复选框，则此参数用于设置空闲超时（以分钟为单位）。

如果在此期间连接上没有通信活动，则系统将终止此连接。最小值为 1 分钟，最大值为 10080 分钟，默认值为 30 分钟。要允许无限连接时间，请选中 **Unlimited**。

- **最大连接时间警告间隔** - 达到最大连接时间之前的时间间隔，此时系统会向用户显示一条消息。

  如果您取消选中**继承**复选框，系统将自动选中**默认**复选框。这将会话警报间隔设置为 30 分钟。如果要指定新值，请取消选中**默认**，然后指定 1 至 30 分钟的会话警报间隔。

- **空闲超时警告间隔** - 达到空闲超时之前的时间间隔，此时系统会向用户显示一条消息。

  如果您取消选中**继承**复选框，系统将自动选中**默认**复选框。这会将空闲警报间隔设置为 30 分钟。如果要指定新值，请取消选中**默认**，然后指定 1 至 30 分钟的会话警报间隔。

- **定期证书身份验证时间间隔** - 定期重新执行证书身份验证之前的时间间隔（以小时为单位）。

  如果未选中**继承**复选框，则可以设置执行定期证书验证的时间间隔。其范围为 1 至 168 小时，默认设置为禁用。要允许无限验证，请选中 Unlimited。

## 内部组策略，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。

- 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。隐藏共享通过位于共享名称结尾的美元符号 ($) 来标识。例如，驱动器 C 作为 C$ 来共享。采用隐藏共享时，不会显示共享文件夹，并且用户无法浏览或访问这些隐藏的资源。
  - 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。
- “智能隧道”- 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 应用连接到内联网上的服务器。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。此选项在用户登录时启动智能隧道访问，它仅适用于 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。应用使用会话下载和上传 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 小应用程序代理转发到客户端。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。它会绕过处理，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。支持几乎所有客户端技术，包括 HTML、CSS、JavaScript、VBScript、ActiveX 和 Java。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。

## 配置内部组策略，无客户端 SSL VPN 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程序与为网络客户端访问连接定制访问门户的程序相同。请参阅内部组策略，AnyConnect 无客户端门户定制，第 79 页。

## 内部组策略，无客户端 SSL VPN 的登录设置

您可以启用 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。请参阅内部组策略，AnyConnect 登录设置，第 74 页。

## 内部组策略，用于无客户端 SSL VPN 访问的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，请参阅内部组策略，无客户端 SSL VPN 访问门户，第 88 页。

# 站点到站点内部组策略

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。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：
  - “无客户端 SSL VPN”- 指定通过 SSL/TLS 来使用 VPN，该 VPN 使用 Web 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，这些企业资源包括企业网站、启用 Web 功能的应用、NT/AD 文件共享（启用 Web 功能）、邮件和其他基于 TCP 的应用。
  - SSL VPN Client - 指定使用思科 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，可为 VPN 隧道提供最完整的架构。站点到站点（点对点）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。
  - “经由 IPsec 的 L2TP”- 允许远程用户使用几种常用 PC 和移动 PC 操作系统随附的 VPN 客户端，通过公共 IP 网络与安全设备和专用企业网络建立安全连接。L2TP 使用经由 UDP 的 PPP（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，这些规则根据源地址、目的地址和协议等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。
- **空闲超时** - 如果未选中**继承**复选框，则此参数用于设置空闲超时（以分钟为单位）。

  如果在此期间连接上没有通信活动，则系统将终止此连接。最小值为 1 分钟，最大值为 10080 分钟，默认值为 30 分钟。要允许无限连接时间，请选中 **Unlimited**。
- **最大连接时间** - 如果未选中**继承**复选框，则此参数用于设置最大用户连接时间（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**无限**（默认）。
- **定期证书身份验证时间间隔** - 定期重新执行证书身份验证之前的时间间隔（以小时为单位）。

  如果未选中**继承**复选框，则可以设置执行定期证书验证的时间间隔。其范围为 1 至 168 小时，默认设置为禁用。要允许无限验证，请选中 Unlimited。

# 为本地用户配置 VPN 策略属性

此程序描述如何编辑现有用户。要添加用户，请依次选择 **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。

### 开始之前

默认情况下，用户账户从默认组策略 DfltGrpPolicy 继承每个设置的值。要覆盖每项设置，请取消选中 **Inherit** 复选框，并输入新值。

### 过程

**步骤 1** 启动 ASDM 并依次选择**配置** > **远程访问 VPN** > **AAA/本地用户** > **本地用户**。

**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。用户策略将继承该组策略的属性。如果此屏幕中的其他字段设置为 **Inherit** 以从 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 Web 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 可提供一种访问各种企业资源的便捷方式，包括企业网站、支持 Web 的应用、NT/AD 文件共享（支持 Web）、电子邮件，以及几乎所有计算机中可访问 HTTPS 互联网网站的其他基于 TCP 的应用。

- SSL VPN 客户端允许用户在下载 Cisco AnyConnect 客户端应用后进行连接。在第一次使用时，用户将使用无客户端 SSL VPN 连接下载此应用。在此之后，每当用户连接时，都会视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，可为 VPN 隧道提供最完整的架构。站点到站点（点对点）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。
- 经由 IPsec 的 L2TP 允许远程用户使用几种常用 PC 和移动 PC 操作系统随附的 VPN 客户端，通过公共 IP 网络与 ASA 和专用企业网络建立安全连接。

  **注释** 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，这些规则根据源地址、目的地址和协议等条件来确定允许还是拒绝隧道数据包通过 ASA。

a) 要配置过滤器和规则，请依次选择**配置** > **远程访问 VPN** > **网络（客户端）访问** > **组策略** > **添加/编辑** > **常规** > **更多选项** > **过滤器**。
b) 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VPN客户端中配置的组与用户分配的组是否相同来限制用户。如果不一样，ASA 会阻止用户进行连接。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** 配置**连接设置**。

a) 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，或者选中 Inherit 复选框。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。

b) 按用户指定同时登录数。Simultaneous Logins 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。

   **注释** 当没有最大限制时，允许多个同时连接可能会降低安全性并影响性能。

c) 指定 VPN 连接的**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。

   如果未选中**继承**复选框，则此参数指定最大用户连接时间（以分钟为单位）。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**无限**（默认）。

d) 指定 VPN 连接的**空闲超时**（以分钟为单位）。如果在此期间连接上没有通信活动，则系统将终止此连接。

如果未选中**继承**复选框，则此参数指定空闲超时（以分钟为单位）。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**。

**步骤 10** 配置**超时警报**。

a) 指定**最大连接时间警报间隔**。

如果您取消选中**继承**复选框，系统将自动选中**默认**复选框。这会将最大连接警报间隔设置为 30 分钟。如果要指定新值，请取消选中**默认**，然后指定 1 至 30 分钟的会话警报间隔。

b) 指定**空闲警报间隔**。

如果您取消选中**继承**复选框，系统将自动选中**默认**复选框。这会将空闲警报间隔设置为 30 分钟。如果要指定新值，请取消选中**默认**，然后指定 1 至 30 分钟的会话警报间隔。

**步骤 11** 要为此用户设置专用 IPv4 地址，请在**专用 IPv4 地址**（**可选**）区域中输入 IPv4 地址和子网掩码。

**步骤 12** 要为此用户设置专用 IPv6 地址，请在**专用 IPv6 地址**（**可选**）区域中输入带 IPv6 前缀的 IPv6 地址。IPv6 前缀表示 IPv6 地址所属的子网。

**步骤 13** 点击左侧窗格中的相应选项，配置具体的**无客户端 SSL VPN** 或 **AnyConnect 客户端**设置。如要覆盖每项设置，请取消选中 **Inherit** 复选框，并输入新值。

**步骤 14** 点击**确定**将更改应用到运行配置。

# 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 AnyConnect Connection Profile 主窗格上，您可以在接口上启用客户端访问，并且可以添加、编辑和删除连接配置文件。您还可以指定是否要允许用户在登录时选择特定连接。

- 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，并改进对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 客户端仍会建立与 IKEv2 的基本 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。请参阅指定设备证书，第 95 页。
- Port Setting - 配置 HTTPS 和 DTLS（仅适用于 RA 客户端）连接的端口号。请参阅连接配置文件，端口设置，第 95 页。
- 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**指定设备证书**窗格，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。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。

从 ASA 版本 9.4.1 开始，ECDSA 证书可用于 SSL 连接（从 AnyConnect 客户端和无客户端 Clientless SSL 进行连接）。在此版本之前，ECDSA 证书仅受 AnyConnect IPsec 连接支持并针对其进行配置。

### 过程

**步骤 1** （仅适用于 VPN 连接）在**证书和 RSA 密钥**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**设备证书**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**确定**。

# 连接配置文件，端口设置

在 ASDM 中的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）：

**配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 连接配置文件**

**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。默认为端口 443。
- DTLS Port - 要为 DTLS 连接启用的 UDP 端口。范围为 1-65535。默认为端口 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 or Edit。系统将打开 Add（或 Edit）AnyConnect Connection Profile > Basic 对话框。

- 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。可以添加空格或标点符号来分隔名称。
- 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。
  - “方法”-身份验证协议经过扩展，可定义用于多证书身份验证的协议交换并将此功能用于两种会话类型。您可以使用 AnyConnect SSL 和 IKEv2 客户端协议验证每个会话的多重证书。选择要使用的身份验证类型：AAA、AAA 和证书、仅证书、SAML、多证书和 AAA 或多证书。根据您的选择，您可能需要提供证书才能进行连接。
  - AAA Server Group - 从下拉列表中选择 AAA 服务器组。默认设置为“本地”，它指定由 ASA 处理身份验证。在进行选择之前，可以点击**管理**在此对话框上叠加打开一个对话框，用于查看 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 。
  - 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 。
- 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。

# 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
- 记账属性
- 名称服务器属性
- 无客户端 SSL VPN 属性

注释 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，常规属性

- 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
- “启用密码管理”- 通过它可以配置与通知用户密码到期相关的参数。
  - 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。

    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。

    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。

- 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，对等体会获得分配的本地 IP 地址以访问内部网络。但是，例如在内部服务器和网络安全基于对等体的实际 IP 地址情况下，可能要将本地 IP 地址重新转换为对等体的实际公有 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。

**注释** 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。

# 连接配置文件，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：

- **配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 连接配置文件**
- **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），然后依次选择 **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**。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。

    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 上删除地址池，请在表中选择该条目并点击**Delete**。

    如果地址池已在使用中，则无法将其删除。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。要删除地址池，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。
- 要删除条目，请选择该条目并点击 **Delete**。

### 相关主题

连接配置文件，客户端寻址，添加或编辑，第 99 页
连接配置文件，地址池，第 99 页
连接配置文件，高级，添加或编辑 IP 池，第 99 页

## 连接配置文件，客户端寻址，添加或编辑

要向连接配置文件分配地址池，请依次选择 **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。

## 连接配置文件，地址池

Connection Profile > Advanced 中的 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。可以添加、编辑或从该列表中删除连接配置文件。

- 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 - 删除所选地址池。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。

## 连接配置文件，高级，添加或编辑 IP 池

通过 Connection Profile > Advanced 中的 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

在 Connection Profile > Advanced >Authentication 选项卡上，您可以配置以下字段：

- 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 - 从表中删除所选服务器组。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。

  **注释** 此功能不支持多情景模式。

  - 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。

    主要和辅助属性可能的值包括：

| 属性 | 定义 |
|---|---|
| C | 国家/地区：两个字母的国家/地区缩写。这些代码符合 ISO 3166 国家/地区缩写。 |

| 属性 | 定义 |
| --- | --- |
| CN | 公用名称：人员、系统或其他实体的名称。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 | 首字母缩写。 |
| L | 区域：组织所在的城市或城镇。 |
| N | 名称。 |
| O | 组织：公司、机构、办事处、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 | 省/自治区/直辖市：组织所在的省/自治区/直辖市 |
| 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。

# 连接配置文件，辅助身份验证属性

可通过 Connection Profile > Advanced 下的 Secondary Authentication 配置辅助身份验证，又称双重身份验证。启用辅助身份验证后，最终用户必须提供两组有效身份验证凭证才能登录。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。

注释 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。

- 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。

    注释 如果还为此连接配置文件指定了授权服务器，则授权服务器设置优先，ASA 会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 - 从表中删除所选服务器组。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式。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：两个字母的国家/地区缩写。这些代码符合 ISO 3166 国家/地区缩写。 |
| CN | 公用名称：人员、系统或其他实体的名称。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 | 首字母缩写。 |
| L | 区域：组织所在的城市或城镇。 |
| N | 名称。 |
| O | 组织：公司、机构、办事处、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 | 省/自治区/直辖市：组织所在的省/自治区/直辖市 |

| 属性 | 定义 |
|---|---|
| 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 AnyConnect Connection 配置文件中的 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。

- 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，请参阅无客户端 SSL VPN 连接配置文件，身份验证，添加服务器组 ，第 111 页
  - 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 - 从表中删除所选服务器组。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

- 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 - 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，授权，添加脚本内容以选择用户名

如果在 AnyConnect Connection 配置文件的 Authorization 窗格中选择 **use a script to select username**，然后点击 Add or Edit 按钮，则会看到以下字段。

脚本可以将证书字段用于其他映射选项中未列出的授权。

注释 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”。

- 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。下表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行方法。返回值是实际预填充作为用户名的内容。

**表 *2:* 按子字符串过滤**

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

| 开始索引 | 结束索引 | 返回值 |
|---|---|---|
| 6 | -1 | user |

使用负索引（例如在该表的第三行中）可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：“使用 Lua 格式的自定义脚本”- 指定以 LUA 编程语言编写的自定义脚本，用于解析搜索字段。选择此选项将为您提供一个字段，可用于输入自定义的 LUA 脚本；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。

下表列出了可在 LUA 脚本中使用的属性名称和说明。

**注释** LUA 区分大小写。

**表 *3:* 属性名称和说明**

| 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 | 首字母缩写 |
| 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 | 省/自治区/直辖市 |
| 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 | 首字母缩写 |
| 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 | 省/自治区/直辖市 |
| 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。

## 无客户端 SSL VPN 连接配置文件，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。

- Interface - 选择一个接口。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。

# 连接配置文件，记账

“连接配置文件”>“高级”中的“记账”窗格用于在 ASA 上全局设置记账选项。

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

# 连接配置文件，组别名和组 URL

Connection Profile > Advanced 中的 GroupAlias/Group URL 对话框配置影响远程用户在登录时所看到内容的属性。

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。

- **登录和注销（门户）页面自定义**（仅适用于无客户端 SSL VPN）- 通过指定要应用的预配置自定义属性来配置用户登录页面的外观。默认值为 DfltCustomization。点击**管理**创建新的自定义对象。
- **启用在登录屏幕上显示 RADIUS 拒绝消息** - 选中此复选框将在拒绝身份验证时在登录对话框中显示 RADIUS 拒绝消息。
- **启用在登录屏幕上显示 SecurId 消息** - 选中此复选框将在登录对话框中显示 SecurID 消息。
- **连接别名** - 连接别名及其状态。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。点击相应按钮可**添加**或**删除**别名。要编辑别名，请双击表中的别名并编辑该条目。要更改启用状态，请在表中选中或取消选中相应复选框。
- **组 URL** - 组 URL 及其状态。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。点击相应按钮可**添加**或**删除** URL。要**编辑** URL，请双击表中的 URL 并编辑该条目。要更改启用状态，请在表中选中或取消选中相应复选框。
- 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)。（如果客户端使用连接别名进行连接，将忽略此设置。）- 选择是否要在连接到某个组 URL 的客户端上运行思科安全桌面的 Hostscan 应用。这些选项仅当添加组 URL 时可见。如果豁免客户端，则安全设备不会从这些用户接收终端条件，因此您可能必须更改 DAP 配置来为其提供 VPN 访问。有以下选项可供选择。

- “始终运行 CSD”- 在连接到该组 URL 的所有客户端上运行 Hostscan。
- “对 AnyConnect 和无客户端 SSL VPN 均禁用 CSD”- 对连接到的该组 URL 的所有客户端豁免 Hostscan 处理。
- “仅对 AnyConnect 禁用 CSD”- 对连接到该组 URL 的 AnyConnect 客户端豁免 Hostscan 处理，但对无客户端连接使用 Hostscan。

# 连接配置文件，无客户端 SSL VPN

**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。

- 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该客户端支持的第一个信任点。如果首选 ECDSA，则您应先配置 ECDSA 信任点，再配置 RSA 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 - 从表中删除所选连接。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式。
- 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。

# 无客户端 SSL VPN 连接配置文件，基本属性

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

- 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。

# 无客户端 SSL VPN 连接配置文件，常规属性

使用**无客户端 SSL VPN 连接配置文件 > 高级 > 常规**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。

- **密码管理** - 通过它可以配置与覆盖来自 AAA 服务器的账户已禁用指示和通知用户密码到期相关的参数。

- **启用通知密码管理** - 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。

  **注释** 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。

  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。

# 无客户端 SSL VPN 连接配置文件，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说明：AnyConnect 连接配置文件，身份验证属性，第 100 页。

## 无客户端 SSL VPN 连接配置文件，身份验证，添加服务器组

当您依次点击 Clientless SSL VPN Connection Profile > Advanced > Authentication 对话框中的 Add 按钮时，可以将接口与 AAA 服务器组关联。

无客户端 SSL VPN 连接配置文件，向接口分配授权服务器组，第 108 页中对执行此配置的字段进行了说明。

# 无客户端 SSL VPN 连接配置文件，辅助身份验证

无客户端 SSL 的辅助身份验证配置字段与用于 AnyConnect 客户端访问的配置字段相同，这在连接配置文件，辅助身份验证属性，第 101 页中进行了说明。

# 无客户端 SSL VPN 连接配置文件，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AnyConnect 连接配置文件，授权属性，第 104 页。

# 无客户端 SSL VPN 连接配置文件，NetBIOS 服务器

Clientless SSL VPN Connection Profile Advanced > NetBIOS Servers 对话框显示当前配置的 NetBIOS 服务器的属性。通过 Clientless SSL VPN access > NetBIOS 对话框的 > Add or Edit Tunnel Group 对话框，可以为隧道组配置 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。当尝试使用 Windows 计算机的计算机名称来与其建立文件共享连接时，指定的文件服务器与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 要求 NetBIOS 访问或共享远程系统上的文件。

如要使 NBNS 功能可运行，必须配置至少一个 NetBIOS 服务器（主机）。可以配置最多三个 NBNS 服务器来实现冗余。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，则使用下一个服务器。

### 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 - 从列表中删除突出显示的 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。

# 无客户端 SSL VPN 连接配置文件，无客户端 SSL VPN

通过“无客户端连接配置文件”中的**高级 > 无客户端 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。

此对话框和 AnyConnect 连接配置文件的字段类似；有关详细信息，请参阅连接配置文件，组别名和组 URL，第 108 页。

# IKEv1 连接配置文件

IKEv1 连接配置文件定义用于本机和第三方 VPN 客户端的身份验证策略，包括 L2TP-IPsec。IKEv1 连接配置文件在**配置 > 远程访问 VPN > 网络（客户端）访问 > IPsec(IKEv1) 连接配置文件**窗格中进行配置。

- **访问接口** - 选择要为 IPsec 访问启用的接口。默认值为无访问。
- **连接配置文件** - 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：
  - **名称** - 指定 IPsec IKEv1 连接的名称或 IP 地址。
  - **IPsec 已启用** - 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 已启用** - 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。
  - **身份验证服务器组** - 可以提供身份验证的服务器组的名称。
  - **组策略** - 指示此 IPsec 连接的组策略的名称。

注释 Delete - 从表中删除所选服务器组。无确认或撤消功能。

## IPsec 远程访问连接配置文件，Basic 选项卡

通过**配置 > 远程访问 VPN > 网络（客户端）访问 > IPsec(IKEv1) 连接配置文件 > 添加/编辑 > 基本**上的“添加或编辑 IPsec 远程访问连接配置文件 - 基本”对话框，可以配置 IPsec IKEv1 VPN 连接的常用属性（包括 L2TP-IPsec）。

- **名称** - 此连接配置文件的名称。
- **IKE 对等体身份验证** - 配置 IKE 对等体。
  - **预共享密钥** - 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。
  - **身份证书** - 选择身份证书的名称（如果已配置并注册任何身份证书）。**管理**可打开**管理身份证书**对话框，可在其中添加、编辑、删除、导出和显示所选证书的详细信息。
- **用户身份验证** - 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。
  - **服务器组** - 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。
  - **回退**-指定在所指定的服务器组发生故障的情况下是否使用“本地”组进行用户身份验证。

- **客户端地址分配** - 指定与分配客户端属性相关的属性。
  - **DHCP 服务器** - 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。
  - **客户端地址池** - 指定最多 6 个预定义地址池。要定义地址池，请点击**选择**按钮。
- **默认组策略** - 指定与默认组策略相关的属性。
  - **组策略** - 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**。
  - **启用 IPsec 协议**和**启用经由 IPsec 的 L2TP 协议** - 选择要用于此连接的一个或多个协议。

# 添加/编辑远程访问连接，高级，常规

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。

- **将用户名传递到 AAA 服务器之前从中剥除领域** - 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删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。

  **注释** 可以向用户名追加领域和组，在此情况下，ASA 会将为该组和该领域配置的参数用于 AAA 功能。此选项的格式为 username[@realm]]<#or!>group]，例如 JaneDoe@example.com#VPNGroup。如果选择此选项，则必须使用 # 或 ! 作为组定界符，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。

  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。

- **将用户名传递到 AAA 服务器之前从中剥除组** - 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删除组名。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。有效的组定界符为 @、# 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。

- **密码管理** - 通过它可以配置与覆盖来自 AAA 服务器的账户已禁用指示和通知用户密码到期相关的参数。
  - **启用密码到期时通知以便用户更改密码** - 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。

    **注释** 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。

    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。

# IKEv1 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，请参阅连接配置文件，客户端寻址，第 98 页。

# IKEv1 连接配置文件，身份验证

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：

- **身份验证服务器组** - 列出可用的身份验证服务器组，包括“本地”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。
- **如果服务器组发生故障则使用“本地”组** - 启用或禁用在“身份验证服务器组”属性所指定的组发生故障的情况下回退到“本地”数据库。

  可以通过取消选中 Enable Group Lookup 框仅基于用户名来配置身份验证。通过选中 Enable Group Lookup 框和 Strip Group，可以使用在 AAA 服务器上追加的组名来维护用户数据库，并同时仅基于用户的用户名对用户进行身份验证。

# IKEv1 连接配置文件，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AnyConnect 连接配置文件，身份验证属性，第 100 页。

# IKEv1 连接配置文件，记账

配置记账对于客户端连接配置文件是通用的。有关详细信息，请参阅连接配置文件，记账，第 108 页。

# IKEv1 连接配置文件，IPsec

**配置 > 远程访问 VPN > 网络（客户端）访问 > IPSec (IKEv1) 连接配置文件 > 添加/编辑 > 高级 > IPSec**

- **发送证书链** - 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 对等体 ID 验证** - 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 保持连接** - 启用并配置 ISAKMP 保持连接监控。
  - **禁用保持连接** - 启用或禁用 ISAKMP 保持连接。
  - **监控保持连接** - 启用或禁用 ISAKMP 保持连接监控。选择此选项将使 Confidence Interval 和 Retry Interval 字段可供使用。
  - **置信区间** - 指定 ISAKMP 保持连接置信区间。这是 ASA 在开始保持连接监控之前应该允许对等体空闲的秒数。最小值为 10 秒；最大值为 300 秒。远程访问组的默认值为 300 秒。
  - **重试间隔** - 指定在 ISAKMP 保持连接重试之间等待的秒数。默认值为 2 秒。
  - **头端从不启动保持连接监控** - 指定中心站点 ASA 绝不会启动保持连接监控。

## IKEv1 连接配置文件，IPsec，IKE 身份验证

**配置 > 远程访问 VPN > 网络（客户端）访问 > IPSec (IKEv1) 连接配置文件 > 添加/编辑 > 高级 > IPSec > IKE 身份验证**

- **默认模式** - 通过它可以如上所示选择默认身份验证模式：“无”、“xauth”或“混合”。
- **接口特定模式** - 逐个接口指定身份验证模式。
  - **添加/编辑/删除** “添加/编辑/删除”可从“接口/身份验证模式”表中删除接口/身份验证模式对选择。
  - **接口** - 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。
  - **身份验证模式** - 通过它可以选择如上所述的身份验证模式：“无”、“xauth”或“混合”。

## IKEv1 连接配置文件，IPsec，客户端软件更新

**配置 > 远程访问 VPN > 网络（客户端）访问 > IPSec (IKEv1) 连接配置文件 > 添加/编辑 > 高级 > IPSec > 客户端软件更新**

**客户端 VPN 软件更新表** - 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 对话框下进行了详细描述）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。

- **客户端类型** - 标识 VPN 客户端类型。
- **VPN 客户端修订版本** - 指定可接受的 VPN 客户端修订级别。
- **位置 URL** - 指定可以从中下载正确的 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，URL 的格式必须为 tftp://。

# IKEv1 连接配置文件，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，请依次打开**配置 > 远程访问 VPN > 网络（客户端）访问 > IPsec(IKEv1) 连接配置文件 > 添加/编辑 > 高级 > PPP**。

此对话框仅适用于 IPsec IKEv1 远程访问连接配置文件。

- **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。

# IKEv2 连接配置文件

IKEv2 连接配置文件为 AnyConnect 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**。

- 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。

注释 Delete - 从表中删除所选服务器组。无确认或撤消功能。

# 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。

- **名称** - 标识连接的名称。
- **IKE 对等体身份验证** - 配置 IKE 对等体。
  - **预共享密钥** - 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。
  - **启用证书身份验证** - 如果选中，则允许使用证书进行身份验证。
  - **启用使用 EAP 的对等体身份验证** - 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。
  - **向客户端发送 EAP 身份请求** - 支持向远程访问 VPN 客户端发送 EAP 身份验证请求。
- **Mobike RRC** - 启用/禁用 Mobike RRC。
  - **为 Mobike 启用返回路由能力检查** - 对已启用 MobIKE 的 IKE/IPSEC 安全关联中的动态 IP 地址更改启用/禁用返回路由能力检查。
- **用户身份验证** - 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。
  - **服务器组** - 选择要用于用户身份验证的服务器组。默认值为“本地”。如果选择除 LOCAL 以外的内容，则 Fallback 复选框变得可用。
  - **管理** - 打开“配置 AAA 服务器组”对话框。
  - **回退**-指定在所指定的服务器组发生故障的情况下是否使用“本地”组进行用户身份验证。
- **客户端地址分配** - 指定与分配客户端属性相关的属性。
  - **DHCP 服务器** - 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。
  - **客户端地址池** - 指定最多 6 个预定义地址池。点击“选择”打开“地址池”对话框。
- **默认组策略** - 指定与默认组策略相关的属性。
  - **组策略** - 选择要用于此连接的默认组策略。默认值为 DfltGrpPolicy。

- **管理** - 打开“配置组策略”对话框，可在其中添加、编辑或删除组策略。
- **客户端协议** - 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。
- **启用 IKEv2 协议** - 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 远程访问连接配置文件，高级，IPsec 选项卡

IPsec (IKEv2) Connection Profiles 上的 IPsec 表具有以下字段。

- 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 收到采用客户端证书身份验证的 IPsec 连接请求时，它将根据您配置的策略为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。

在 Policy 窗格上配置匹配的策略。如果选择使用规则进行匹配，请转至 Rules 窗格以指定规则。

## 证书到连接配置文件的映射，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。这些策略的设置在**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPsec > 证书到连接配置文件的映射 > 策略**中进行创建。

- **使用配置的规则匹配证书与组** - 通过它可以使用已在“规则”下定义的规则。
- **使用证书 OU 字段来确定组** - 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。
- **使用 IKE 身份来确定组** - 通过它可以使用以前在**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPsec > IKE 参数**下定义的身份。IKE 标识可以是主机名、IP 地址，密钥 ID 或自动。

- **使用对等体 IP 地址来确定组** - 通过它可以使用对等体的 IP 地址。默认情况下会选择此项。
- **默认为连接配置文件** - 通过它可以为证书用户选择当前面的方法未产生匹配项时所使用的默认组。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，必须使用**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略**对其进行定义。

# 证书到连接配置文件的映射规则

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。配置文件映射在**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPsec > 证书到连接配置文件的映射 > 规则**中进行创建。

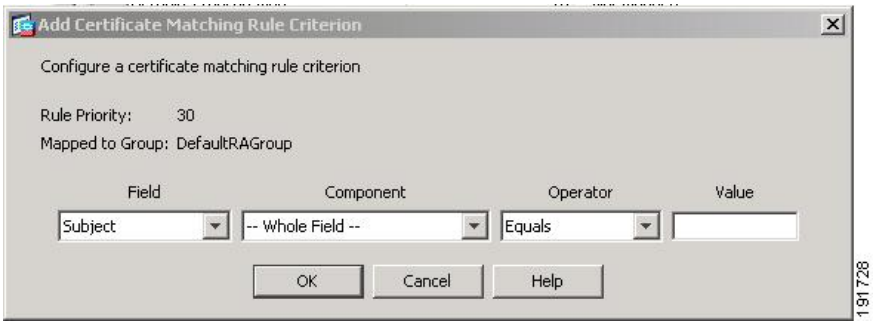
此窗格具有一个证书到连接配置文件映射及映射条件的列表。

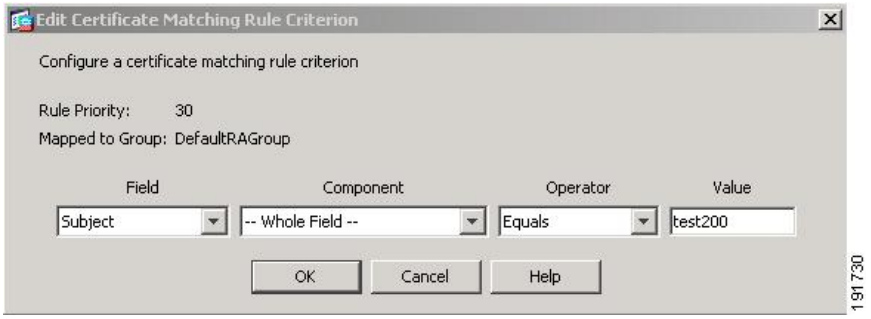
## 证书到连接配置文件映射，添加证书匹配规则条件

创建映射配置文件，将连接配置文件映射到映射规则。

- 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。
- “优先级”- 输入一个十进制数以指定 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

使用此对话框配置您可以映射到连接配置文件的证书匹配规则条件。

- 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 -（仅在选择 Subject of Issuer 的情况下适用。) 选择规则所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，例如 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。 |

| DN 字段 | 定义 |
|---|---|
| **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)** | 组织所在的省、自治区或直辖市。 |
| **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：

| 选择项 | 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 |

# 站点到站点连接配置文件

Connection Profiles 对话框显示当前配置的站点到站点连接配置文件（隧道组）的属性，通过该对话框还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，使用内部和外部 IP 报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 - 删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。

# 站点间连接配置文件，添加或编辑

通过 Add or Edit IPsec Site-to-Site Connection 对话框，可以创建或修改 IPsec 站点到站点连接。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。

尤其是，两个对等方均为思科 ASA 5500 系列 ASA 时，支持以下拓扑：

- ASA 具有 IPv4 内部网络，外部网络为 IPv6（内部接口使用 IPv4 地址，外部接口使用 IPv6 地址）。
- ASA 具有 IPv6 内部网络，外部网络为 IPv4（内部接口使用 IPv6 地址，外部接口使用 IPv4 地址）。
- ASA 具有 IPv6 内部网络，外部网络为 IPv6（内部接口和外部接口都使用 IPv6 地址）。

### Basic 面板上的字段

- “对等体 IP 地址”- 通过它可以指定 IP 地址（IPv4 或 IPv6）以及该地址是否为静态地址。
- Connection Name - 指定分配给此连接配置文件的名称。对于 Edit 功能，此字段仅作显示用途字段。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。

# 站点到站点隧道组

ASDM 窗格上的 Configuration > Site-to-Site VPN > Advanced > Tunnel Groups 指定用于 IPsec 站点到站点连接配置文件（隧道组）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。

- Name - 指定分配给此隧道组的名称。对于 Edit 功能，此字段仅作显示用途字段。
- 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）。

**注释** 某些配置文件可能无法确定终端是远程访问还是 LAN 到 LAN。如果它无法确定隧道组，则默认为

```
tunnel-group-map default-group <tunnel-group-name>
```

（默认值为 *DefaultRAGroup*）。

  - 
  - 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 保持连接监控。只能选择以下属性之一。
  - Disable Keep Alives - 启用或禁用 IKE 保持连接。
  - Monitor Keep Alives - 启用或禁用 IKE 保持连接监控。选择此选项将使 Confidence Interval 和 Retry Interval 字段可供使用。
  - Confidence Interval - 指定 IKE 保持连接置信区间。这是 ASA 在开始保持连接监控之前应该允许对等体空闲的秒数。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 保持连接重试之间等待的秒数。默认值为 2 秒。
  - 头端从不启动保持连接监控 - 指定中心站点 ASA 绝不会启动保持连接监控。

# 站点到站点连接配置文件，加密映射条目

在此对话框中，指定当前站点到站点连接配置文件的加密参数。

- **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密钥（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密钥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密钥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

管理 CA 证书适用于远程访问和站点间 VPN：

- 对站点间 VPN：点击“IKE 对等体身份验证”下的“管理”打开“管理 CA 证书”对话框。
- 对远程访问 VPN，依次点击**证书管理** > **CA 证书**。

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。“管理 CA 证书”对话框列出有关当前配置的证书的信息，包括有关证书颁发对象、证书颁发者、证书到期时间和使用情况数据的信息。

- 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 - 从表中删除所选证书。无确认或撤消功能。

# 站点到站点连接配置文件，安装证书

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。

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。

使用 Revocation Check 对话框指定有关 CA 证书撤销检查的信息。

- 单选按钮指定是否检查证书以进行撤销。选择 **Do not check certificates for revocation** 或 Check Certificates for revocation。
- Revocation Methods 区域 - 通过此区域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。

# AnyConnect VPN 客户端映像

**配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 客户端软件**窗格列出了 ASDM 中配置的 AnyConnect 客户端映像。

AnyConnect 客户端映像表 - 显示在 ASDM 中配置的软件包文件，并可用于确定 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传到闪存。
- 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传到闪存。
- 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。

### AnyConnect VPN 客户端映像，添加/更换

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传文件。

- 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 上传要标识为客户端映像的文件。
- “用于匹配用户代理的正则表达式”- 指定 ASA 用于与浏览器传递的用户代理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报头中包含用户代理字符串。在ASA收到该字符串后，如果字符串与为映像配置的表达式匹配，它会立即下载该映像，而不测试其他客户端映像。

### AnyConnect VPN 客户端映像，上传映像

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。

- 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 - 启动文件上传。

# 配置 AnyConnect VPN 客户端连接

## 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》。

客户端配置文件在 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile** 中进行配置：

Add/Import - 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传到闪存。

- 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、Web 安全、ISE 终端安全评估、AMP 启用程序、网络可视性模块、Umbrella 漫游安全或管理 VPN 隧道。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。
- 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。

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。

导出

- 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。

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：

# 豁免 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)，必须豁免远程访问 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。豁免转换 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 豁免”），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。

此程序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 *4:* 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 |
| Sales 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 |

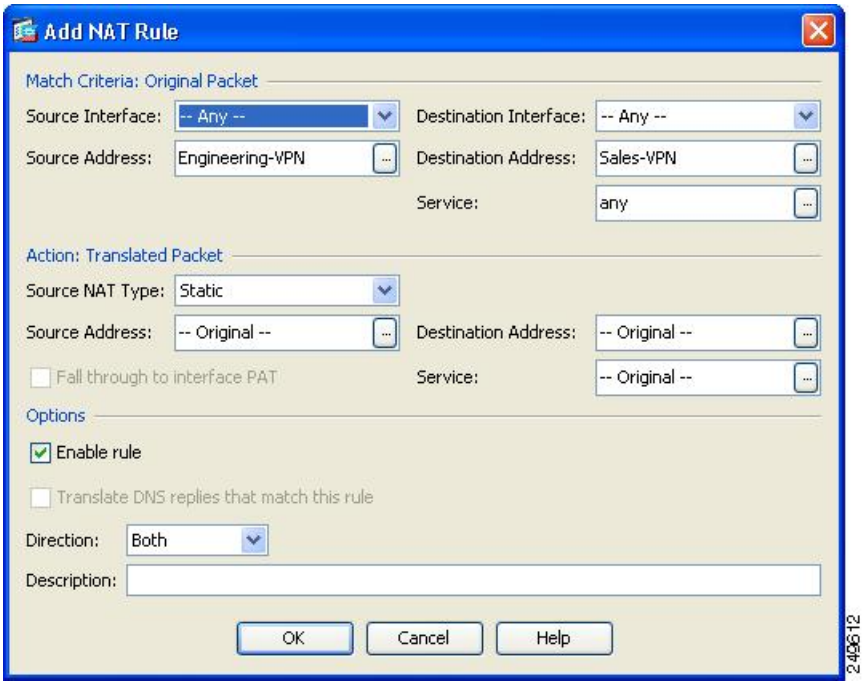
**过程**

**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 规则”窗格中，依次导航到**添加 > 在“网络对象”NAT 规则前添加 NAT 规则**，以便 ASA 在统一 NAT 表中的其他规则之前评估此规则。

**注释** NAT 规则评估按照自顶向下、最先匹配的基础来应用。在 ASA 与数据包到特定 NAT 规则，因此不会执行任何评估。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。

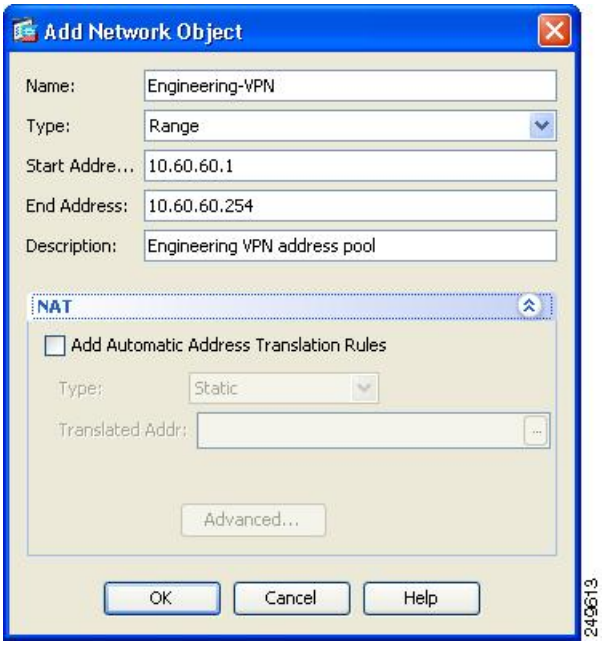
图 *1: Add NAT Rule* 对话框




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

- **源接口**：“任意”
- **目的接口**：“任意”
- **源地址**：点击“源地址”浏览按钮并创建表示工程 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。
- **目的地址**：点击“目的地址”浏览按钮并创建表示销售 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 2: 为 VPN 地址池创建网络对象




b) 在操作：转换后的数据包区域中，配置以下字段：

- 源 NAT 类型：“静态”
- 源地址：“原始”
- 目的地址：“原始”
- 服务：“原始”

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。
- 方向：“双向”
- 说明：添加此规则的说明。

d) 点击 **OK**。

e) 点击 **Apply**。

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 中依次选择**Configuration > DeviceSetup > Interface Settings > 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
```

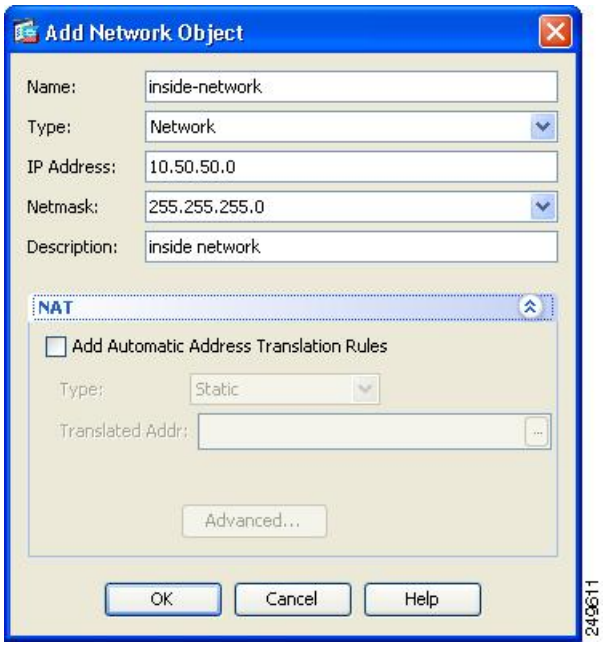
**步骤 4** 创建 NAT 规则，以便 Engineering VPN 地址池中的主机可以到达 Engineering VPN 地址池中的其他主机。创建此规则的过程就与先前创建该规则一样，不同之处在于，您需要在“匹配条件：原始数据包”区域中将工程 VPN 地址池同时指定为源地址和目的地址。

**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，依次选择 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:* 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**。

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，为工程 VPN 地址池和 DMZ 网络之间的连接配置身份 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。在这种情况下，因为要将源地址从私有地址更改为互联网路由地址，所以不使用身份 NAT。要创建此规则，请遵循以下程序：

a) 在 NAT Rules 窗格中，依次选择 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。

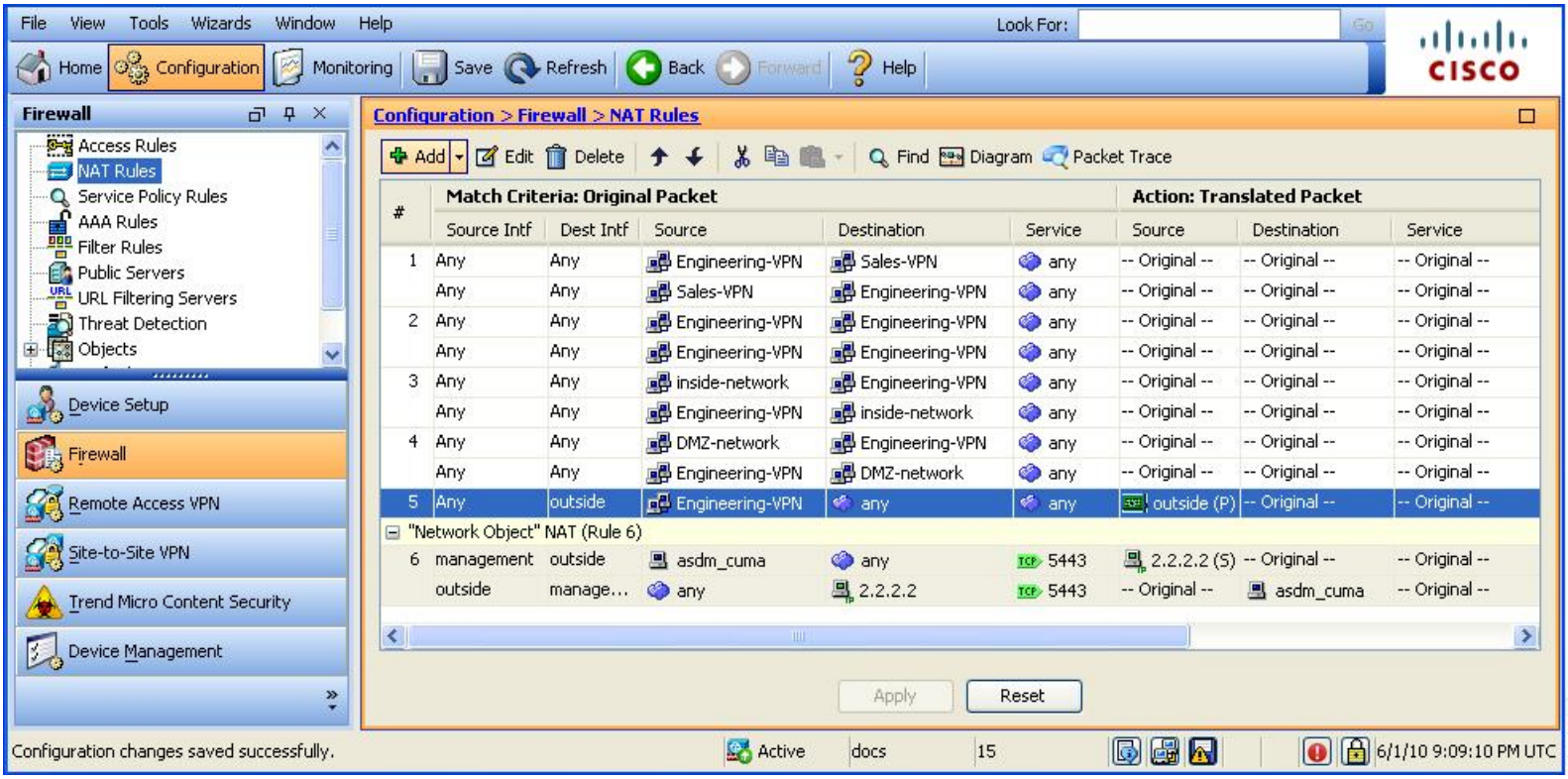
e) 点击 **OK**。

f) 点击 **Apply**。

CLI 示例：

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

图 *4:* 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 豁免 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。

# AnyConnect HostScan

AnyConnect 终端安全评估模块为 AnyConnect 安全移动客户端提供标识主机上安装的操作系统防恶意软件和防火墙软件的能力。HostScan 应用会收集此信息。终端安全状态评估要求在主机上安装 HostScan。

## HostScan 前提条件

具有终端安全评估模块的 AnyConnect 安全移动客户端至少需要以下 ASA 组件：

- ASA 8.4
- ASDM 6.4

这些 AnyConnect 功能要求安装终端安全评估模块。

- SCEP 身份验证
- AnyConnect 遥测模块

终端安全评估模块可以安装在以下任意平台上：

- Windows 7、8、8.1、10、10 RS1、10 RS2 和 10 RS3 x86（32 位）和 x64（64 位）
- macOS 10.11、10.12 和 10.13
- Linux Red Hat 6、7 及 Ubuntu 14.04 (LTS) 和 16.04 (LTS)（仅限 64 位）

## AnyConnect HostScan 的许可

以下是终端安全评估模块的 AnyConnect 许可要求：

- 适用于基本 HostScan 的 AnyConnect Apex 许可证。
- 补救功能需要高级终端评估许可证。

## HostScan 程序包

您可以将 HostScan 程序包作为独立的程序包加载至 ASA：**hostscan-version.pkg**。此文件包含 HostScan 软件，以及 HostScan 库和支持图表。

# 安装或升级 HostScan

使用 ASDM，按照以下程序安装或升级 HostScan 程序包并启用 HostScan。

### 开始之前

注释 如果您尝试从 HostScan 4.3.x 版或更低版本升级到 4.6.x 版或更高版本，由于您之前已制定的所有现有 AV/AS/FW DAP 策略和 LUA 脚本与 HostScan 4.6.x 版或更高版本不兼容，所以您将收到错误信息。

您必须完成一个一次性迁移程序来调整您的配置。此程序需要在保存此配置之前离开此对话框去迁移需要与 HostScan 4.4.x 兼容的配置。有关详细说明，请中止此程序并参阅《AnyConnect HostScan 4.3.x 到 4.6.x 迁移指南》。简而言之，迁移过程涉及以下操作：导航到 ASDM DAP 策略页面检查并手动删除不兼容的 AV/AS/FW 属性，然后检查并重写 LUA 脚本。

### 过程

**步骤 1** 将 hostscan_version-k9.pkg 文件下载到计算机。

**步骤 2** 打开 ASDM 并依次选择**配置 > 远程访问 VPN > 安全桌面管理器 > Host Scan 映像** > 。

**步骤 3** 点击**上传**，准备从您的计算机上将 HostScan 程序包副本传输至 ASA 的驱动器。

**步骤 4** 在“上传映像”对话框中，点击**浏览本地文件**，在本地计算机上搜索 HostScan 程序包。

**步骤 5** 选择前文所述已下载的 hostscan_*version*-k9.pkg 文件，然后点击**选择**。您所选文件的路径显示在“本地文件路径”字段中，而“闪存文件系统路径”字段显示的是 HostScan 程序包的目的路径。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**上传文件**。ASDM 会将文件的副本传输到闪存卡。“信息”对话框将显示文件已成功上传到闪存。

**步骤 7** 点击**确定**。

**步骤 8** 在“使用上传的映像”对话框中，点击**确定**使用您刚上传的 HostScan 程序包文件作为当前映像。

**步骤 9** 如果尚未选中，则请选中**启用 HostScan**。

**步骤 10** 点击**应用**。

**步骤 11** 从文件菜单中，选择 **将运行配置保存到闪存中**。

# 卸载 HostScan

卸载 HostScan 程序包会将其从 ASDM 界面的视图中移除并防止 ASA 部署该程序包，即使启用了 HostScan 也是如此。卸载 HostScan 不会从闪存驱动器中删除 HostScan 程序包。

过程

步骤 1 在 ASDM 中，依次导航到**配置 > 远程访问 VPN > 安全桌面管理器 > Host Scan 映像** > ，卸载 HostScan。

步骤 2 点击**卸载**，然后点击**是**确认。

步骤 3 点击**卸载**。

# 将 AnyConnect 功能模块分配到组策略

此程序将 AnyConnect 功能模块与组策略关联。在 VPN 用户连接到 ASA 时，ASA 将下载这些 AnyConnect 功能模块并将其安装到终端计算机上。

### 开始之前

登录 ASA 并进入全局配置模式。在全局配置模式下，ASA 将显示以下提示符：hostname(config)#

### 过程

步骤 1 为网络客户端访问添加内部组策略

**group-policy** *name* **internal**

示例：

```
hostname(config)# group-policy PostureModuleGroup internal
```

步骤 2 编辑新的组策略。输入该命令后，您会收到组策略配置模式的提示符：hostname(config-group-policy)#。

**group-policy** *name* **attributes**

示例：

```
hostname(config)# group-policy PostureModuleGroup attributes
```

步骤 3 进入组策略 webvpn 配置模式。输入该命令后，ASA 将返回以下提示符：hostname(config-group-webvpn)#

**webvpn**

步骤 4 配置组策略以便为组中的所有用户下载 AnyConnect 功能模块。

**anyconnect modules value** *AnyConnect Module Name*

anyconnect模块命令的值可能包含下列一个或多个值。当指定多个模块时，请用逗号将这些值隔开。

| 值 | AnyConnect 模块/功能名称 |
|---|---|
| dart | AnyConnect DART（诊断和报告工具） |

| 值 | AnyConnect 模块/功能名称 |
|---|---|
| vpngina | AnyConnect SBL（登录前开始） |
| websecurity | AnyConnect 网络安全模块 |
| telemetry | AnyConnect 遥测模块 |
| posture | AnyConnect 终端安全评估模块 |
| nam | AnyConnect 网络访问管理器 |
| none | 单独使用可从组策略中删除所有 AnyConnect 模块。 |
| profileMgmt | AnyConnect 管理隧道 VPN |

**示例：**

```
hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture
```

要删除某个模块，请重新发出命令，只指定要保留的模块值。例如，以下命令将删除 websecurity 模块：

```
hostname(config-group-webvpn)# anyconnect modules value telemetry,posture
```

**步骤 5** 将运行配置保存到闪存中。

成功地将新配置保存到闪存中后，您将收到消息 [OK]，并且 ASA 将返回以下提示符：
hostname(config-group-webvpn)#

**write memory**

# HostScan 相关文档

HostScan 从终端计算机收集安全状态凭证后，您需要了解配置动态访问策略和使用 LUA 表达式来利用信息等主题。

以下文档中详细介绍了这些主题：

- 《思科安全桌面配置指南》
- 《思科自适应安全设备管理器配置指南》

另请参阅《思科 *AnyConnect* 安全移动客户端管理员指南》，以获取有关 HostScan 如何与 AnyConnect 客户端配合工作的详细信息。

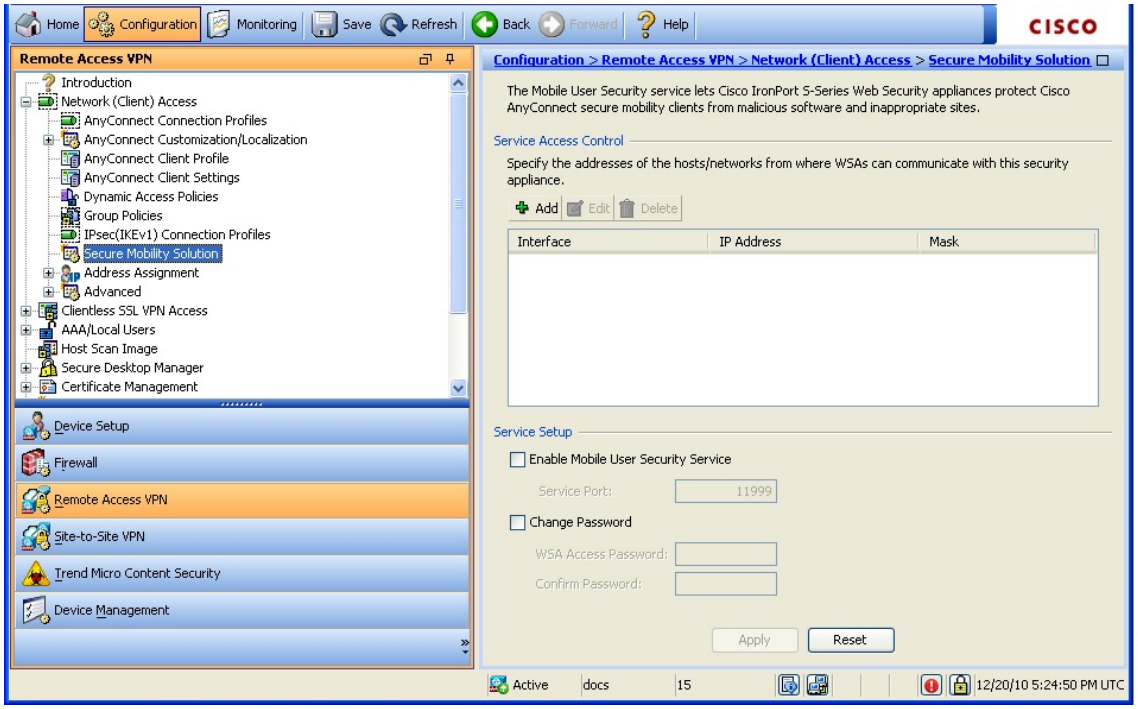
# AnyConnect 安全移动解决方案

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。通过 AnyConnect 安全移动，Cisco IronPort S 系列 Web 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 Web 安全设备保护。

注释 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 Web 安全设备发行版。它还需要支持 AnyConnect 安全移动功能的 AnyConnect 版本。AnyConnect 3.1 和更高版本不支持此功能。

要配置安全移动解决方案，请依次选择 **Configuration > Remote Access VPN > Network (Client) Access > Secure Mobility Solution**。

**图 *5:* 移动用户安全窗口**




- 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 - 从表中删除所选连接。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钥密码。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

在 Configuration > Remote Access VPN > Network (Client) Access > Secure Mobility Solution 下的 Add or Edit MUS Access Control 对话框为 AnyConnect 客户端配置移动用户安全 (MUS) 访问权限。

- 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。

# AnyConnect 定制和本地化

您可以定制 AnyConnect VPN 客户端，向远程用户显示您自己的公司图像。通过 AnyConnect Customization/Localization 下的以下字段，可以导入以下类型的定制文件：

- **Resources**- 经过修改的 AnyConnect 客户端 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**- 将在 AnyConnect 进行 VPN 连接前后运行的脚本。
- **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**- 用于更改客户端所使用语言的转换。

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** 删除所选对象。

注释 此功能不支持多情景模式。

# AnyConnect 定制和本地化，资源

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 定制和本地化、二进制和脚本

### AnyConnect 自定义/本地化，二进制

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 自定义/本地化，脚本

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**- 选择运行脚本的时间。

  AnyConnect 向文件名添加前缀 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，删

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，脚本显示为 OnConnect_myscript.bat。

为确保脚本能够稳定运行，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 Name 创建指定的新名称。

# AnyConnect 定制和本地化、GUI 文本和消息

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**-“添加”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。请更改 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 定制和本地化，定制的安装程序转换

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，由其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《思科 *AnyConnect* 安全移动客户端管理指南》。

# AnyConnect 定制和本地化，本地化的安装程序转换

可以通过转换来转换客户端安装程序显示的消息。转换文件将更改安装，但已签署安全性的原始MSI将保持原样。这些转换文件仅翻译安装程序屏幕，不会翻译客户端 GUI 屏幕。

# 用于 AnyConnect 3.1 的 AnyConnect 基础版

AnyConnect 基础版是单独许可的 SSL VPN 客户端，完全在 ASA 上配置，可提供完整的 AnyConnect 功能，但存在以下例外：

- 不提供无客户端 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思科 SSL VPN 客户端的优点：

要启用 AnyConnect 基础版，请选中“AnyConnect 基础版”窗格中的**启用 AnyConnect 基础版**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。

注释 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 SSL VPN Sessions 部分中的 **Monitoring > VPN > VPN Sessions** 链接。这将依次打开 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。

注释 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。

# AnyConnect 自定义属性

自定义属性会被发送到 AnyConnect 客户端，并且该客户端用其配置下列功能等许多功能。一个自定义属性有一个类型和一个命名值。动态访问策略和组策略都可使用预定义的自定义属性。创建并设置自定义属性用于许多不同用途：

- **用于启用 DSCP 预留** - 设置此自定义属性可以为 DTLS 连接控制 Windows 或 Mac 操作系统平台上的差分服务代码点 (DSCP)。通过 DSCPPreservationAllowed 自定义属性类型，设备可以优先处理延迟敏感型流量，并标记优先化的流量以提高出站连接质量。有关其他信息，请参阅《思科 AnyConnect 安全移动客户端管理指南》中的启用 *DSCP* 预留部分。
- **用于在 ASA 上启用延迟更新** - 如果配置了这些自定义属性，则当客户端更新可用时，AnyConnect 会打开一个对话框，询问用户希望立即更新还是延迟更新。例如，用于延迟更新的一些自定义属性包括 DeferredUpdateAllowed、DeferredUpdateMinimumVersion、DeferredUpdateDismissTimeout 和 DeferredDismissResponse，具体取决于 ASA 的版本。有关其他信息，请参阅启用 AnyConnect 客户端延迟升级或《思科 AnyConnect 安全移动客户端管理指南》中的在 *ASA* 上配置延迟更新。
- **用于启用动态分割隧道** - 通过创建此自定义属性，您可以在建立隧道后基于主机 DNS 域名动态分割排除隧道。通过添加 dynamic-split-exclude-domains，您可以进入客户端需要从 VPN 隧道外部进行访问的云或 Web 服务。有关其他信息，请参阅《思科 AnyConnect 安全移动客户端管理指南》中的关于动态分割隧道。
- **用于启用管理 VPN 隧道** - 默认情况下，管理 VPN 隧道需要分割包含隧道配置，以免影响用户发起的网络通信（因为其本意是为了提供透明性）。要覆盖此行为，可以创建一个自定义属性，将类型设置为 *ManagementTunnelAllAllowed*，将值设置为 *true/true*。那么，如果配置为隧道全部、分割包含、分割排除或绕过两种 IP 协议这几种配置之一，AnyConnect 就会继续进行管理隧道连接。
- **用于设置公共 DHCP 服务器路由** - 通过此自定义属性，本地 DHCP 流量就能在配置隧道全部网络的情况下以明文传输。AnyConnect 将在 AnyConnect 客户端连接时向本地 DHCP 服务器添加特定路由，并对主机计算机的局域网适配器应用隐式过滤器，在该路由中阻止除 DHCP 流量外的所有流量。no-dhcp-server-route 自定义属性必须存在并设置为 true，才能避免在建立隧道后创建公共 DHCP 服务器路由。有关其他信息，请参阅《思科 AnyConnect 安全移动客户端管理指南》中的设置公共 *DHCP* 服务器路由部分。
- **用于配置 Linux 以支持排除的子网** - circumvent-host-filtering 自定义属性将 Linux 设置为在为分割隧道配置了“下面的隧道网络列表”时支持排除子网。有关其他信息，请参阅配置 Linux 以支持扩展子网，第 71 页。

要进一步完成这些功能的使用，大部分已经定义的自定义属性必须在**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略** > 菜单中与特定组策略进行关联。

# IPsec VPN 客户端软件

注释 **VPN 客户端为寿命终止产品并且无法获得相关支持**。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**。

# Zone Labs Integrity 服务器

通过**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPsec > Zone Labs Integrity 服务器**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 用作客户端 PC 到防火墙服务器的代理，并在 Integrity 客户端与 Integrity 服务器之间中继所有必要的 Integrity 信息。

注释 安全设备的当前版本每次只支持一个 Integrity Server，即使用户接口支持多达五个 Integrity Server 的配置也一样。如果活动的 Integrity 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 VPN 客户端会话。

- **服务器 IP 地址** - 键入 Integrity 服务器的 IP 地址。使用点分十进制表示法。
- **添加** - 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。
- **删除** - 从 Integrity 服务器列表中删除所选服务器。
- **上移** - 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。
- **下移** - 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。
- **服务器端口** - 键入 ASA 侦听活动 Integrity 服务器所在的端口号。仅当 Integrity Server 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 Server 列表中有服务器时，此字段才可用。
- **接口** - 选择 ASA 与活动 Integrity 服务器进行通信所在的接口。仅当 Integrity Server 列表中有服务器时，此接口名称菜单才可用。
- **失败超时**- 键入 ASA 在其声明活动 Integrity 服务器无法访问之前应等待的秒数。默认值为 10，范围是从 5 到 20。
- **SSL 证书端口** - 指定要用于 SSL 授权的 ASA 端口。默认为端口 80。
- **启用 SSL 身份验证** - 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。

- **超时情况下关闭连接** - 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。
- **应用** - 点击以将 Integrity 服务器设置应用于 ASA 运行配置。
- **重置** - 点击以移除尚未应用的 Integrity 服务器配置更改。

# 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。可自动化并简化有线连接、无线连接和 VPN 连接的接入控制和安全合规性管理。思科 ISE 主要用于与思科 TrustSec 结合提供安全接入和访客接入、支持自带设备 (BYOD) 计划和执行使用策略。

ISE 授权变更 (CoA) 功能提供一种机制，以在建立身份验证、授权和记账 (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。不需要内联安全状态实施点 (IPEP) 即可为与 ASA 设备建立的每个 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 发送记账启动消息以注册会话。
4. 直接在 NAC 代理和 ISE 之间进行终端安全评估。此过程对 ASA 透明。
5. ISE 通过 CoA“policy push”向 ASA 发送策略更新。这样可以识别提供更多网络访问权限的新用户 ACL。

**注释** 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。

# 配置 ISE 授权更改

配置 ISE 授权更改需要创建一个包含 ISE RADIUS 服务器的服务器组，然后将该服务器组用于远程访问 VPN 配置文件（隧道）。

过程

**步骤 1** 为 ISE 服务器配置 RADIUS AAA 服务器组。

以下程序介绍的是最低配置。您可以根据需要调整组的其他设置。大多数设置的默认值适用于大多数网络。有关配置 RADIUS AAA 服务器组的完整信息，请参阅常规配置指南。

a) 依次选择**配置** > **远程访问 VPN** > **AAA/本地用户** > **AAA 服务器组**。

b) 在 **AAA Server Groups** 区域中，点击 **Add**。

c) 在 **AAA Server Group** 字段中输入组的名称。

d) 从 **Protocol** 下拉列表中选择 RADIUS 服务器类型。

e) 选择**启用临时记账更新**和**更新间隔**，以便能定期生成 RADIUS interim-accounting-update 消息。

ISE 将基于其从 NAS 设备（如 ASA）收到的记账记录，保留一个活动会话的目录。不过，如果 ISE 为期 5 天没有接收到该会话仍处于活动状态的任何指示（记账消息或终端安全评估事务处理），则它将删除从其数据库中删除该会话记录。为了确保长期 VPN 连接不被删除，请将该组配置为针对所有活动会话向 ISE 发送定期临时记账更新消息。

可以更改发送这些更新的间隔（以小时为单位）。默认值为 24 小时，范围为 1 至 120。

f) 选择**启用动态授权**。

此选项为 AAA 服务器组启用 RADIUS 动态授权（ISE 授权更改，CoA）服务。当您在 VPN 隧道中使用服务器组时，RADIUS 服务器组将注册接收 CoA 通知，并且 ASA 会侦听用于从 ISE 获取 CoA 策略更新的端口。请勿更改端口 (1700)，除非已将 ISE 服务器配置为使用不同的端口。有效范围为 1024 至 65535。

g) 如果不希望使用 ISE 进行身份验证，请选择**使用仅授权模式**。

此选项表示当此服务器组用于授权时，RADIUS 访问请求消息将会构建为“仅授权”请求，而不是为 AAA 服务器定义的已配置的密码方法。如果您为 RADIUS 服务器配置公用密码，则它将被忽略。

例如，如果您想将证书用于身份验证而不是此服务器组，则应使用仅授权模式。您仍可将此服务器组用于授权和在 VPN 隧道中记账。

h) 点击**确定**保存服务器组。

i) 对所选服务器组，点击**所选组中的服务器**列表中的**添加**，将 ISE RADIUS 服务器添加到组。

以下是关键属性。您可以根据需要调整其他设置的默认值。

- **接口名称** - 可以通过其访问 ISE 服务器的接口。
- **服务器名称或 IP 地址** - ISE 服务器的主机名或 IP 地址。
- （可选。）**服务器密钥** - 用于对连接进行加密的密钥。如果不配置密钥，则不对连接加密（明文）。该密钥是一个区分大小写的字母数字字符串，最多 127 个字符，其值与 RADIUS 服务器上的密钥相同。

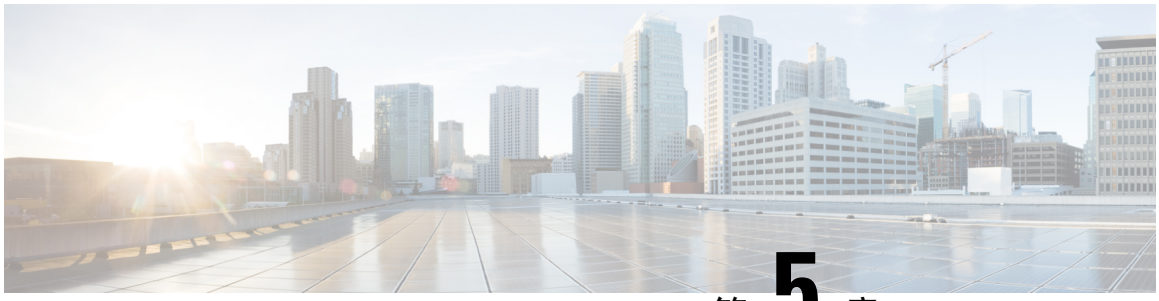
j) 点击**确定**将服务器添加到组。

将任何其他 ISE 服务器添加到服务器组。

**步骤 2** 更新远程访问 VPN 的配置文件以使用该 ISE 服务器组。

以下步骤只介绍了与 ISE 相关的配置选项。要创建能够正常工作的远程访问 VPN，还需要配置一些其他选项。请按照本指南中其他部分的说明实施远程访问 VPN 。

a) 依次选择**配置** > **远程访问 VPN** > **网络（客户端）访问** > **AnyConnect 连接配置文件**。
b) 在**连接配置文件**表中，添加或编辑配置文件。
c) 在**基本**页面中，配置身份验证方法。
   - 如果使用 ISE 服务器进行身份验证，请为**身份验证** > **方法**选择 **AAA**，然后选择 ISE AAA 服务器组。
   - 如果已配置 ISE 服务器组仅用于授权，请选择不同的身份验证方法，例如**证书**。
d) 在**高级** > **授权**页面中，为**授权服务器组**选择 ISE 服务器组。
e) 在**高级** > **记账**页面中，选择 ISE 服务器组。
f) 点击 **确定**，保存更改。



第 5 章

# VPN 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。如已配置多种地址分配方法，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、授权和记账服务器逐个用户检索地址。如果使用已配置 IP 地址的身份验证服务器，建议使用此方法。您可以在“配置”>“AAA 设置”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分配地址池以进行配置的最简单方法。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。
  - 允许释放 IP 地址一段时间之后对其重新使用 - 在 IP 地址返回到地址池之后，延迟一段时间方可重新使用。增加延迟有助于防止防火墙在快速重新分配 IP 地址时遇到的问题。默认情况下，已取消选中该选项，表示 ASA 不会强制执行延迟。如果需要延迟，请选中此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。此配置元素适用于 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。

# 配置 IP 地址分配选项

过程

**步骤 1** 依次选择**配置** > **远程访问 VPN** > **网络（客户端）访问** > **地址分配** > **分配策略**

**步骤 2** 在 IPv4 Policy 区域中，选中相应地址分配方法即表示启用，取消选中即表示禁用。默认情况下，这些方法已启用：

- Use Authentication server。启用已配置的身份验证、授权和记账 (AAA) 服务器，以提供 IP 地址。
- Use 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。
- Use internal address pools：启用在 ASA 上配置的本地地址池。

如果启用 **Use internal address pools**，则也可在释放 IPv4 地址之后对其重新使用。可指定 0 至 480 分钟的时间范围，经过此时间范围，就可重新使用 IPv4 地址。

**步骤 3** 在 IPv6 Policy 区域中，选中相应地址分配方法即表示启用，取消选中即表示禁用。默认情况下，这些方法已启用：

- Use Authentication server。启用已配置的身份验证、授权和记账 (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**应用**。

**步骤 5** 点击**确定**。

# 查看地址分配方法

过程

依次选择**配置 > 远程访问 VPN > 网络（客户端）访问 > 地址分配 > 分配策略**。

# 配置本地 IP 地址池

如要配置 VPN 远程访问隧道的 IPv4 或 IPv6 地址池，请打开 ASDM 并依次选择 **Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add/Edit IP Pool**。如要删除地址池，请打开 ASDM 并依次选择 **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。地址池的指定顺序非常重要。如果为连接配置文件或组策略配置了多个地址池，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地址池，从而可更轻松地添加这些网络的路由。

# 配置本地 IPv4 地址池

IP Pool 区域按名称显示已配置的地址池及其 IP 地址范围，例如：10.10.147.100 至 10.10.147.177。如果地址池不存在，该区域为空。ASA 按所列顺序使用这些地址池：如果第一个地址池中的所有地址已分配，则使用下一个地址池，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地址池，从而可更轻松地添加这些网络的路由。

**过程**

**步骤 1** 依次选择**配置** > **远程访问 VPN** > **网络（客户端）访问** > **地址分配** > **地址池**。

**步骤 2** 要添加 IPv4 地址，请依次点击**添加** > **IPv4 地址池**。如要编辑现有地址池，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：

- Pool Name - 输入地址池的名称。最多可包含 64 个字符
- Starting Address - 输入每个已配置地址池中可用的第一个 IP 地址。使用点分十进制表示法，例如：10.10.147.100。
- Ending Address - 输入每个已配置地址池中可用的最后一个 IP 地址。使用点分十进制表示法，例如：10.10.147.177。
- Subnet Mask - 标识此 IP 地址池所属的子网。

**步骤 4** 点击**应用**。

**步骤 5** 点击**确定**。

# 配置本地 IPv6 地址池

IP Pool 区域按名称显示已配置的地址池，及其起始 IP 地址范围、地址前缀和可在地址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地址池：如果第一个地址池中的所有地址已分配，则使用下一个地址池，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地址池，从而可更轻松地添加这些网络的路由。

过程

步骤 1 依次选择**配置** > **远程访问 VPN** > **网络（客户端）访问** > **地址分配** > **地址池**。

步骤 2 要添加 IPv6 地址，请依次点击**添加** > **IPv6 地址池**。如要编辑现有地址池，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：

- Name - 显示每个已配置地址池的名称。

  Starting IP Address - 输入已配置地址池中可用的第一个 IP 地址。例如：2001:DB8::1。

- Prefix Length - 输入 IP 地址前缀长度（位数）。例如，32 代表 CIDR 表示法中的 /32。前缀长度定义 IP 地址池所属的子网。

- Number of Addresses — 标识地址池中从起始 IP 地址开始的 IPv6 地址的数量。

步骤 4 点击 **Apply**。

步骤 5 点击 **OK**。

# 将内部地址池分配给组策略

在 Add or Edit Group Policy 对话框中，可为正在添加或修改的内部网络（客户端）访问组策略指定地址池、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。

可为同一个组策略同时配置 IPv4 和 IPv6 地址池。如果在同一个组策略中配置了两个版本的 IP 地址，则配置了 IPv4 的客户端将获得 IPv4 地址，配置了 IPv6 的客户端将获得 IPv6 地址，而同时配置了 IPv4 和 IPv6 地址的客户端将获得 IPv4 和 IPv6 地址。

过程

步骤 1 使用 ASDM 连接至 ASA，并依次选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**。

步骤 2 创建新的组策略或要使用内部地址池配置的组策略，然后点击 Edit。

默认情况下，会在 Group Policy 对话框中选择 General attributes 窗格。

步骤 3 使用 Address Pools 字段指定该组策略的 IPv4 地址池。点击 Select 以添加或编辑 IPv4 地址池。

步骤 4 使用 IPv6 Address Pools 字段指定要用于此组策略的 IPv6 地址池。点击 Select 以添加或编辑 IPv6 地址池。

步骤 5 点击 **OK**。

步骤 6 点击 **Apply**。

# 配置 DHCP 寻址

如要使用 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关联的组策略中定义 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。这些示例还为名为 **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）。如未定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将检查各个池，直到发现未分配的地址为止。

以下配置包括多个必须执行的步骤，在这些步骤中，您可能已经为连接配置文件类型命名并将其定义为远程访问，同时为组策略命名并将其标识为内部或外部组策略。这些步骤在以下示例中显示为一则提醒，提示您只有先设置这些值，然后才有权访问后续 tunnel-group 和 group-policy 命令。

### 规定和限制

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。

1. 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。
    1. 使用 ASDM 连接至 ASA。
    2. 确认已在 Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy 中启用 DHCP。
    3. 通过依次选择 Configuration > Remote Access VPN > DHCP Server 配置 DHCP 服务器。
2. 将 DHCP IP 寻址分配给组策略。
    1. 依次选择 **Configuration > Remote Access VPN > Network (Client) Access> AnyConnect Connection Profiles**。
    2. 在 Connection Profiles 区域中，点击 **Add** 或 **Edit**。
    3. 在连接配置文件的配置树中，点击 **Basic**。
    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**。
    5. 编辑与连接配置文件关联的组策略，以定义 DHCP 范围。依次选择 **Configuration > Remote Access VPN > Network (Client) Access> Group Policies**。
    6. 双击要编辑的组策略。

7. 在配置树中点击**服务器**。
8. 点击向下箭头展开**更多选项**区域。
9. 取消选中 DHCP 范围的**继承**。
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**。
11. 点击 **OK**。
12. 点击 **Apply**。

# 将 IP 地址分配给本地用户

可将本地用户账户配置为使用组策略，还可配置某些 AnyConnect 属性。当 IP 地址的其他源出现故障时，这些用户账户将提供回退，以便管理员仍然可以访问。

### 开始之前

要添加或编辑用户，请依次选择**配置 > 远程访问 VPN > AAA/本地用户 > 本地用户**，然后点击**添加**或**编辑**。

默认情况下，Edit User Account 屏幕上的每项设置均将选中 **继承** 复选框，这表明用户账户从默认组策略 DfltGrpPolicy 继承该设置的值。

要覆盖每项设置，请取消选中**继承**复选框，并输入新值。接下来的详细步骤介绍 IP 地址设置。有关完整的配置详情，请参阅为本地用户配置 VPN 策略属性，第 91 页。

### 过程

**步骤 1** 启动 ASDM 并依次选择**配置** > **远程访问 VPN** > **AAA/本地用户** > **本地用户**。

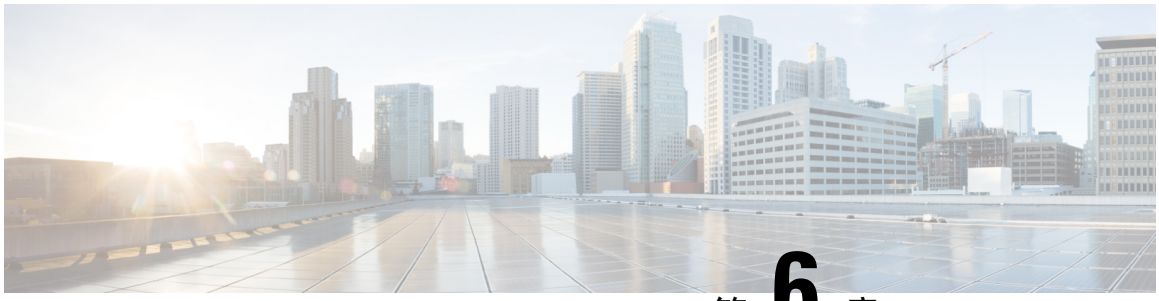
**步骤 2** 选择要配置的用户，然后点击**编辑**。

**步骤 3** 在左侧窗格中，点击 **VPN 策略**。

**步骤 4** 要为此用户设置专用 IPv4 地址，请在**专用 IPv4 地址**（**可选**）区域中输入 IPv4 地址和子网掩码。

**步骤 5** 要为此用户设置专用 IPv6 地址，请在**专用 IPv6 地址**（**可选**）区域中输入带 IPv6 前缀的 IPv6 地址。IPv6 前缀表示 IPv6 地址所属的子网。

**步骤 6** 点击**应用**，将更改保存到运行配置。



第 6 章

# 动态访问策略

本章介绍如何配置动态访问策略。



## 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各个 VPN 连接，例如，频繁更改内联网配置、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登录。相比采用静态配置的网络，授权用户的任务在 VPN 环境中更为复杂。

利用 ASA 上的动态访问策略 (DAP)，您可以配置兼顾上述众多可变因素的授权方法。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身份和终端安全的问题。换言之，ASA 会根据您定义的策略，为特定用户授予特定会话的访问权限。从一个或多个 DAP 记录选择和/或汇聚属性时，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 系统包含的以下组件需要您加以注意：

- DAP 选择配置文件 - 一个文本文件，该文件包含 ASA 在会话建立期间用于选择和应用 DAP 记录的条件。该文件存储在 ASA 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 Web 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 AAA 或终端属性（用户无法配置）。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 支持和终端安全评估工具

ASA 使用您配置的终端安全评估工具来获取终端安全属性。这些终端安全评估工具包括 AnyConnect 终端安全评估模块、独立主机扫描软件包和 NAC。

下表确定了 DAP 支持的每个远程访问协议、可用于该方法的终端安全评估工具，以及该工具提供的信息。

| 支持远程访问协议 | AnyConnect 终端安全评估模块<br>主机扫描包<br>思科安全桌面<br>（不启用终端评估主机扫描扩展） | AnyConnect 终端安全评估模块<br>主机扫描包<br>思科安全桌面<br>（启用终端评估主机扫描扩展） | NAC | 思科 NAC 设备 |
|---|---|---|---|---|
| | 返回文件信息、注册表项值、运行的进程、操作系统 | 返回防恶意软件和个人防火墙软件信息 | 返回 NAC 状态 | 返回 VLAN 类型和 VLAN ID |
| IPSec VPN | 否 | 不支持 | 支持 | 支持 |
| Cisco AnyConnect VPN | 支持 | 支持 | 支持 | 支持 |
| 无客户端（基于浏览器的）SSL VPN | 支持 | 是 | 否 | 否 |
| PIX 直通代理（终端安全评估不可用） | 否 | 否 | 否 | 否 |

# 使用 DAP 的远程访问连接操作程序

以下操作程序概述典型远程访问连接的建立过程。

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 HostScan 值执行终端安全评估。
3. ASA 通过 AAA 对用户进行身份验证。AAA 服务器还会返回用户的授权属性。

4. ASA 将 AAA 授权属性应用至会话，并建立 VPN 隧道。
5. ASA 根据用户 AAA 授权信息和会话终端安全评估信息选择 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 策略应用至会话。

# 动态访问策略许可

注释 此功能不适用于无负载加密型号。

| 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<br>高级终端评估许可证<br>AnyConnect 移动许可证 |

注释 ASA 管理员根据其已安装的 AnyConnect 许可证，以不同方式使用 AnyConnect 移动终端安全评估 DAP 属性。高级终端评估许可证通过 DAP 实现高级终端评估功能（例如补救、Windows Mobile 设备 LUA 表达式等）。您还可以将 DAP 与基本许可证配合使用。高级 DAP 的实施基于 ASA 中的许可证和功能（例如，启用 AnyConnect 高级版许可证的防病毒检查）。

**相关主题**

向 DAP 添加 AnyConnect 终端属性，第 167 页

# 配置动态访问策略

**开始之前**

- 除非另有说明，否则您必须在配置 DAP 终端属性之前安装主机扫描。
- 如果从 HostScan 4.3.x 升级到 HostScan 4.6.x 或更高版本，必须在升级前将任何现有的 AV/AS/FW 终端属性迁移到取代其的相应 AM/FW 终端属性。有关完整的升级和迁移程序，请参阅《AnyConnect HostScan 4.3.x 到 4.6.x 迁移指南》。

- 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。如需相关说明，请启动 ASDM 并依次选择 **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**，然后点击 **Help**。
- DAP 仅支持 ASCII 字符。

过程

**步骤 1** 启动 ASDM 并依次选择**Configuration > Remote Access VPN > Network (Client) Access or Clientless SSL VPN Access > Dynamic Access Policies**。

注释 如果“添加”、“编辑”和“删除”操作下显示**不兼容**操作按钮，则表示您已尝试将HostScan升级到某个版本（4.6.x或更高版本），该版本的内部库更新使其与您现有的DAP策略（创建于使用Hostscan 4.3.x或更低版本时）不兼容。您必须执行一个一次性迁移程序来调整您的配置。

**不兼容**操作按钮的出现表示HostScan升级已启动，您现在需要迁移配置。有关详细说明，请参阅《AnyConnect Hostscan 4.3.x 到 4.6.x 迁移指南》。

**步骤 2** 要包括特定防恶意软件或个人防火墙终端属性，请点击靠近窗格顶部的**CSD配置**。然后，启用思科安全桌面和 HostScan 扩展。如果您之前已启用这两个功能，此链接不会显示。

**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 Web 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 - 显示对会话应用的防火墙 ACL 的名称。
- Web-Type ACL List - 显示对会话应用的 SSL VPN ACL 的名称。
- Description - 描述 DAP 记录的用途。

**步骤 4** 点击 **Add** 或 **Edit**，以便添加或编辑动态访问策略，第 161 页。

**步骤 5** 点击 **Apply** 以便保存 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`** 匹配名为 `Sales` 的 DAP，但不会匹配名为 `Wholesalers` 的 DAP。如果您在**查找**字段中键入 **`*sal`**，搜索结果会找到表中的第一个 **`Sales`** 或 **`Wholesalers`** 实例。

**步骤 7** 测试动态访问策略，第 162 页可验证您的配置。

# 添加或编辑动态访问策略

过程

**步骤 1** 启动 ASDM 并依次选择**配置** > **远程访问 VPN** > **网络（客户端）访问**或**无客户端 SSL VPN 访问** > **动态访问策略** > **添加**或**编辑**。

**步骤 2** 提供此动态访问策略的名称（必选）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。有效值范围为 0 至 2147483647。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（未标记）就使用此动态访问策略所需配置的 AAA 属性值进行选择，用户是只需配置任意一个值，还是必须配置所有值，抑或是无需配置这些值，以及是否需要满足每一个终端属性。

不允许重复的条目。如果您配置没有 AAA 或终端属性的 DAP 记录，ASA 会始终选择该记录，因为所有选择条件都已满足。

b) 点击 AAA Attributes 字段中的 **Add** 或 **Edit**，以便配置 DAP 中的 AAA 属性选择条件，第 162 页。

c) 点击 Endpoint Attributes 区域中的 **Add** 或 **Edit**，以便配置 DAP 中的终端属性选择条件，第 165 页。

d) 点击 **Advanced** 字段，以便使用 LUA 在 DAP 中创建其他 DAP 选择条件，第 177 页。使用此功能需要 Lua 编程语言方面的知识。

- AND/OR - 点击以便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。输入用于定义新的 AAA 和/或终端选择属性的任何形式的 LUA 文本。ASDM 不会验证您在此处输入的文本；只是将此文本复制到 DAP XML 文件，然后 ASA 会对其进行处理，丢弃其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。请参阅配置 DAP 访问和授权策略属性，第 183 页。

**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一组 DAP 记录的检索。

过程

**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。

点击这些 Add/Edit 按钮时显示的对话信息与 Add/Edit AAA Attributes 和 Add/Edit Endpoint Attributes 对话框中的对话信息类似。

**步骤 2** 点击 **Test** 按钮。

评估每个记录的 AAA 和终端选择属性时，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 可提供一组限定的授权属性，这些属性可覆盖 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 会根据用户的 AAA 授权信息和会话的终端安全评估信息选择 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。

过程

要将 AAA 属性配置为 DAP 记录的选择条件，请在 Add/Edit AAA Attributes 对话框中设置要使用的 Cisco、LDAP 或 RADIUS 属性。可以将这些属性设置为所输入的 = 或 != 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，第 165 页。

AAA Attributes Type - 使用下拉列表选择 Cisco、LDAP 或 RADIUS 属性：

- Cisco - 指存储在 AAA 层次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一小部分。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。
  - Assigned IP Address - 输入要为策略指定的 IPv4 地址。为完整的隧道 VPN 客户端（IPsec、L2TP/IPsec、SSL VPN AnyConnect）分配的 IP 地址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。使用 Local、RADIUS、LDAP 身份验证/授权，或者任何其他身份验证类型（例如 RSA/SDI、NT Domain 等）时适用。
- =/!= - 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。它会丢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。用户记录属性会先被读取，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 客户端会对 LDAP memberOf 响应属性进行特殊处理。AD memberOf 属性指定 AD 中的组记录的 DN 字符串。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。

  在与 LDAP 身份验证/授权服务器进行 VPN 远程访问会话的情况下，会返回以下三个 Active Directory 组（memberOf 枚举）：

  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 属性名称与语法有关且区分大小写。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。

  **注释** 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用户的 AAA 会话关联的数据库中。RADIUS 客户端会按接收到响应属性的顺序，将响应属性写入数据库。它会丢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。用户记录属性会先被读取，而且其优先级始终高于组记录属性。

  RADIUS 属性包含 DAP 记录中的属性编号和属性值对。

注释　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。请参阅检索 Active Directory 组，第 164 页。

# 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。

可以在后台使用 CLI 的**how-ad-groups** 命令从 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，请依次选择**配置 > 远程访问 VPN > AAA/本地用户 > AAA 服务器组 > 编辑 AAA 服务器**。

注释　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 服务器组** - 用于检索 AD 组的 AAA 服务器组的名称。

**过滤依据** - 指定一个组或组的部分名称，以便减少显示的组。

**组名称** - 从服务器检索到的 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。“属性名称”字段显示以 LUA 逻辑表达式输入每个属性名称的方式，您可以在“添加/编辑动态访问策略”窗格的“高级”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 | 数字 | - | 为完整的隧道 VPN 客户端（IPsec、L2TP/IPsec、SSL VPN AnyConnect）分配的 IP 地址 |
| | 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/授权的情况下适用） |
| LDAP | aaa.ldap.<*label*> | LDAP | 字符串 | 128 | LDAP 属性值对 |
| RADIUS | aaa.radius.<number> | RADIUS | 字符串 | 128 | Radius 属性值对 |

# 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、终端安全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记录都指定了终端选择属性，这些属性必须得到满足，ASA才能选择将其用于会话。ASA仅选择满足配置的每个条件的 DAP 记录。

### 开始之前

- 将终端属性配置为 DAP 记录的选择条件是配置动态访问策略，第 159 页大流程的一个环节。将终端属性配置为 DAP 的选择条件之前，请查阅此程序。
- 有关终端属性的详细信息，请参阅终端属性定义，第 174 页。
- 
- 有关 HostScan 如何检查驻留内存的防恶意软件和个人防火墙程序的详细信息，请参阅 DAP 以及防恶意软件和个人防火墙程序，第 173 页。

过程

**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。

- 向 DAP 添加防恶意软件终端属性，第 166 页
- 向 DAP 添加应用属性，第 167 页
- 向 DAP 添加 AnyConnect 终端属性，第 167 页
- 向 DAP 添加文件终端属性，第 169 页
- 向 DAP 添加设备终端属性，第 169 页
- 向 DAP 添加 NAC 终端属性，第 170 页
- 向 DAP 添加操作系统终端属性，第 170 页
- 向 DAP 添加个人防火墙终端属性，第 171 页
- 向 DAP 添加策略终端属性，第 171 页
- 向 DAP 添加流程终端属性，第 172 页
- 向 DAP 添加注册表终端属性，第 172 页
- 向 DAP 添加多证书身份验证属性，第 173 页

**步骤 2** 指定 DAP 策略匹配条件。

对于每个此类终端属性类型，请确定 DAP 策略应要求用户是配置一个类型的所有实例（Match All = AND，默认设置），还是仅配置其中的一个实例 （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 添加或编辑动态访问策略，第 161 页。

# 向 DAP 添加防恶意软件终端属性

开始之前

如果从 HostScan 4.3.x 升级到 HostScan 4.6.x 或更高版本，必须在升级前将任何现有的 AV/AS/FW 终端属性迁移到取代其的相应 AM/FW 终端属性。有关完整的升级和迁移程序，请参阅《AnyConnect HostScan 4.3.x 到 4.6.x 迁移指南》。

过程

**步骤 1** 在**终端属性类型**列表框中，选择**防恶意软件**。

**步骤 2** 点击相应的“**安装**”或“**不安装**”按钮，指示安装还是不安装所选终端属性及其附带限定词（“名称”/“操作”/“值”列下面的字段）。

**步骤 3** 确定要启用还是禁用实时扫描。

**步骤 4** 从**供应商 ID** 列表框中，选择要测试的防恶意软件的供应商的名称。

**步骤 5** 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 6** 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 Version 列表框中的选项包含 x（例如 3.x），可以将 x 替换为特定版本号（例如 3.5）。

**步骤 7** 选中 **Last Update** 复选框。指定距离上次更新的天数。您可能想要指明更新时间应小于 (<) 或大于 (>) 您在此处输入的天数。

**步骤 8** 点击**OK**。

# 向 DAP 添加应用属性

过程

**步骤 1** 在 **Endpoint Attribute Type** 列表框中，选择 **Application**。

**步骤 2** 在 Client Type 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，也称为移动终端安全评估或 AnyConnect 标识扩展 (ACIDex)，AnyConnect VPN 客户端会使用这些属性与 ASA 进行终端安全评估信息通信。动态访问策略使用这些终端属性向用户进行授权。

这些移动终端安全评估属性可以包含在动态访问策略中，并且在在终端上没有安装主机扫描或思科安全桌面的情况下实施。

某些移动终端安全评估属性仅与在移动设备上运行的 AnyConnect 客户端相关。某些移动终端安全评估属性与在移动设备上运行的 AnyConnect 客户端和 AnyConnect 桌面客户端都相关。

### 开始之前

移动终端安全评估需要在 ASA 上安装 AnyConnect 移动许可证和 AnyConnect 高级许可证。安装这些许可证的企业将能够根据 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。

### 过程

**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（例如移动电话和平板电脑）或者台式计算机和笔记本电脑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（例如移动电话和平板电脑）以及台式计算机和笔记本电脑设备上的操作系统。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 **Platform 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，您需要将此设备连接至 ASA，并执行 DAP 跟踪，然后查找 **endpoint.anyconnect.deviceuniqueid** 的值。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”是有效的十六进制字符（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，您需要将此设备连接至 ASA，并执行 DAP 跟踪，然后查找 **endpoint.anyconnect.macaddress** 的值。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

### 开始之前

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，依次选择 **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**。有关详细信息，请点击该页面上的 **Help**。

### 过程

**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 (>) 已经过去的特定天数。在 **days** 字段中输入已经过去的特定天数。

**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

### 过程

**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卡的 MAC 地址。每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。此编号格式由制造商指定。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

过程

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 收到的终端安全评估标记字符串。在 Postune Status 文本框中输入终端安全评估标记字符串。

步骤 3 点击**OK**。

# 向 DAP 添加操作系统终端属性

过程

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

### 开始之前

如果从 HostScan 4.3.x 升级到 HostScan 4.6.x 或更高版本，必须在升级前将任何现有的 AV/AS/FW 终端属性迁移到取代其的相应 AM/FW 终端属性。有关完整的升级和迁移程序，请参阅《AnyConnect HostScan 4.3.x 到 4.6.x 迁移指南》。

### 过程

**步骤 1** 在 **Endpoint Attribute Type** 列表框中，选择 **Operating System**。

**步骤 2** 点击相应的“**安装**”或“**不安装**”按钮，指示安装还是不安装所选终端属性及其附带限定词（“名称”/“操作”/“值”列下面的字段）。

**步骤 3** 在**供应商**列表框中，点击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 (>=) 您从 **Version** 列表框中选择的产品版本号。

如果 **Version** 列表框中的选项包含 x（例如 3.x），可以将 x 替换为特定版本号（例如 3.5）。

**步骤 6** 选中 **Last Update** 复选框。指定距离上次更新的天数。您可能想要指明更新时间应小于 (<) 或大于 (>) 您在此处输入的天数。

**步骤 7** 点击 **OK**。

# 向 DAP 添加策略终端属性

### 过程

**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 添加流程终端属性

### 开始之前

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，依次选择 **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**。有关详细信息，请点击该页面上的 **Help**。

### 过程

**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

扫描注册表终端属性仅适用于 Windows 操作系统。

### 开始之前

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，依次选择 **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**。有关详细信息，请点击该页面上的 **Help**。

### 过程

**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 **Registry** 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项的终端 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** 列表框中，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**。

# 向 DAP 添加多证书身份验证属性

您可以对每个证书编制索引，以便配置的规则可以引用接收到的任何证书。以这些证书字段为基础，您可以配置 DAP 规则来允许或禁止连接尝试。

过程

**步骤 1** 依次浏览至**配置 > 远程访问 VPN > 网络（客户端）访问 > 动态访问策略 > 添加终端属性**。

**步骤 2** 在下拉菜单中选择**多证书身份验证**作为“终端属性类型”。

**步骤 3** 根据您的首选项进行以下一项或多项配置：

- 证书持有者名称
- 颁发机构名称
- 主题备用名称
- 序列号

**步骤 4** 将“证书存储区”保留默认值“无”以允许来自任一存储区的证书，或者选择允许的存储区 - 仅用户还是仅计算机。如果选择“用户”或“计算机”，必须输入证书来自哪个存储区。客户端将在协议中发送此信息。

# DAP 以及防恶意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，安全设备会使用 DAP 策略。登录前评估和 HostScan 模块将向安全设备返回关于配置的终端属性的信息，DAP 子系统则会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）防恶意软件和个人防火墙程序都支持活动扫描，这意味着这些程序会驻留在内存中，因而会始终运行。HostScan 按照以下方式检查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，HostScan 将报告此软件的存在。DAP 系统选择指定程序的 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，HostScan 将报告此软件的存在。同样，安全设备会选择指定程序的 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，HostScan 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，即使安装了此程序也是如此。

**注释** 如果从 HostScan 4.3.x 升级到 HostScan 4.6.x 或更高版本，必须在升级前将任何现有的 AV/AS/FW 终端属性迁移到取代其的相应 AM/FW 终端属性。有关完整的升级和迁移程序，请参阅《AnyConnect HostScan 4.3.x 到 4.6.x 迁移指南》。

# 终端属性定义

以下终端选择属性可供 DAP 使用。“属性名称”字段显示以 LUA 逻辑表达式输入每个属性名称的方式，您可以在“动态访问策略选择条件”窗格的“高级”区域中输入表达式。*label* 变量标识应用、文件名、进程或注册表项。

| 属性类型 | 属性名称 | 来源 | 值 | 最大字符串长度 | 说明 |
|---|---|---|---|---|---|
| 反恶意软件（需要思科安全桌面） | endpoint.am["*label*"].exists | 主机扫描 | true | - | 防恶意软件程序存在 |
| | endpoint.am["*label*"].version | | 字符串 | 32 | 版本 |
| | endpoint.am["*label*"].description | | 字符串 | 128 | 防恶意软件说明 |
| | endpoint.am["*label*"].lastupdate | | 整数 | - | 防恶意软件定义更新以来经过的秒数 |
| 个人防火墙（需要安全桌面） | endpoint.pfw["*label*"].exists | 主机扫描 | true | - | 此个人防火墙存在 |
| | endpoint.pfw["*label*"].version | | 字符串 | 字符串 | 版本 (Version) |
| | endpoint.pfw["*label*"].description | | 字符串 | 128 | 个人防火墙说明 |

| 属性类型 | 属性名称 | 来源 | 值 | 最大字符串长度 | 说明 |
|---|---|---|---|---|---|
| AnyConnect（不需要安装思科安全桌面或 HostScan） | 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 | — | 安装 AnyConnect 客户端的设备的 MAC 地址。<br>必须为 xx-xx-xx-xx-xx-xx 格式，其中 'x' 是有效的十六进制字符 |
| 应用 | endpoint.application.clienttype | 应用 | 字符串 | - | 客户端类型：<br>CLIENTLESS<br>ANYCONNECT<br>IPSEC<br>L2TP |

| 属性类型 | 属性名称 | 来源 | 值 | 最大字符串长度 | 说明 |
|---|---|---|---|---|---|
| 设备 | endpoint.device. hostname | 终端 | 字符串 | 64 | 仅主机名，而不是 FQDN |
| | endpoint.device.MAC | | 字符串 | — | 网络接口卡的 Mac 地址。每个条目只允许有一个 MAC 地址<br>必须是 xxxx.xxxx.xxxx 格式，其中 x 是十六进制字符。 |
| | endpoint.device.id | | 字符串 | 64 | BIOS 序列号。此编号格式由制造商指定。没有格式要求 |
| | endpoint.device.port | | 字符串 | — | TCP 端口处于侦听状态<br>您可以为一条线路定义一个端口<br>介于 1 和 65535 之间的整数 |
| | endpoint.device. protection_version | | 字符串 | 64 | 设备运行的 HostScan 映像的版本 |
| | endpoint.device. protection_extension | | 字符串 | 64 | 终端评估版本 (OPSWAT) |
| 文件 | endpoint.file["*label*"].exists | 安全桌面 | true | - | 此文件存在 |
| | endpoint.file[“label”]. endpointid | | | | |
| | endpoint.file["*label*"]. lastmodified | | 整数 | - | 文件上次修改之后经过的时间（秒） |
| | endpoint.file["*label*"]. crc.32 | | 整数 | - | 此文件的 CRC32 散列值 |
| NAC | endpoint.nac.status | NAC | 字符串 | - | 用户定义的状态字符串 |
| 操作系统 | endpoint.os.version | 安全桌面 | 字符串 | 32 | 操作系统 |
| | endpoint.os.servicepack | | 整数 | - | Windows 服务包 |

| 属性类型 | 属性名称 | 来源 | 值 | 最大字符串长度 | 说明 |
|---|---|---|---|---|---|
| 策略 | endpoint.policy.location | 安全桌面 | 字符串 | 64 | 来自思科安全桌面的位置值 |
| 流程 | 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 |
| 注册表 | 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：ACCESSAUTHERRORGUESTQUARANTINEERRORSTATICTIMEOUT |

# 使用 LUA 在 DAP 中创建其他 DAP 选择条件

本节提供为 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。您可以在 http://www.lua.org/manual/5.1/manual.html 找到有关 LUA 编程的详细信息。

在“高级”字段中，您可以输入代表 AAA 和/或终端选择逻辑运算的任何格式的 LUA 文本。ASDM 不会验证您在此处输入的文本；只是将此文本复制到 DAP 策略文件，然后 ASA 会对其进行处理，丢弃其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选择条件，该选项十分有用。例如，虽然您可以将 ASA 配置为使用满足任意指定条件、满足所有指定条件或不满足所有指定条件的 AAA 属性，但终端属性是累计的，必须全部满足。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。

以下各节将详细介绍创建 LUA EVAL 表达式的相关信息及示例。


- 创建 LUA EVAL 表达式的语法，第 178 页
- DAP EVAL 表达式示例，第 181 页
- 其他 LUA 函数，第 179 页

# 创建 LUA EVAL 表达式的语法

注释 如果您必须使用 Advanced 模式，为使内容清晰易懂，我们建议您尽可能使用 EVAL 表达式，以便使程序验证简单明了。

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，请参阅终端属性定义，第 174 页。 | |
| <comparison> | 以下任一字符串（需要括在双引号中） | |
| | "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（需要括在双引号中） | |
| | “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 为数字。 |

# HostScan 4.6 及更高版本的 LUA 程序

## 用于检查应用了上次更新的“任意”防恶意软件 (endpoint.am) 的 LUA 脚本

使用以下 LUA 脚本检查“任意”防恶意软件产品/供应商 (endpoint.am)。可以进行修改以适应不同的“上次更新”间隔。以下示例显示了如何表示执行“上次更新”的时间必须在30天（记为2592000秒）以内。

```
assert(function()
  for k,v in pairs(endpoint.am) do
    if(EVAL(v.activescan, "EQ", "ok", "string")and EVAL (v.lastupdate, "LT", "2592000",
"integer"))
     then
              return true
         end
  end
  return false
end)()
```

## 用于检查“任意”个人防火墙的 LUA 脚本

使用以下 LUA 脚本检查“任意”防火墙产品/供应商 (endpoint.pfw)：

```
assert(function()
    for k,v in pairs(endpoint.pfw) do
         if (EVAL(v.enabled, "EQ", "ok", "string")) then
              return true
         end
    end
    return false
end)()
```

## 其他 LUA 函数

在与动态访问策略配合使用时，您可能需要增加匹配条件的灵活性。例如，您可能想要根据以下内容应用一个不同的 DAP：

- 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。
- 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项的组名称可能需要您能够使用通配符。

您可以在 ASDM 中的 DAP 窗格的“高级”部分中创建 LUA 逻辑表达式，从而实现这种灵活性。

### DAP CheckAndMsg 函数

ASA 仅在选择了包括 LUA CheckAndMsg 函数的 DAP 记录并导致连接终止时，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，安全设备会显示相应的消息。

### 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来匹配此条件：

```
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。

### 组成员身份示例

您可以为 AD 组成员身份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。

我们出于此目的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)()
```

### 拒绝访问示例

您可以使用以下函数，以便在没有防恶意软件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.am) do

        if (EVAL(v.exists, "EQ”, "true", "string")) then

            return false

        end
    end
    return CheckAndMsg(true, "Please install antimalware software before connecting.", nil)
end)()
```

如果缺少防恶意软件程序的用户尝试登录，DAP 会显示以下消息：

```
Please install antimalware software before connecting.
```

# 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 |
|---|---|
| 终端 LUA 检查：检查 Windows 10 | `(EVAL(endpoint.os.version,"EQ","Windows 10","string"))` |
| 终端 LUA 检查：检查 CLIENTLESS 或 CVC 客户端类型的匹配项。 | `(EVAL(endpoint.application.clienttype,”EQ”,"CLIENTLESS") or EVAL(endpoint.application.clienttype, “EQ”,"CVC"))` |

| 说明 | 示例 |
| --- | --- |
| 终端 LUA 检查：检查用户 PC 上是否安装有一个防恶意软件程序 Symantec Enterprise Protection，如未安装则显示一条消息。 | `(CheckAndMsg(EVAL(endpoint.am["538"].description,"NE","Symantec Endpoint Protection","string"),"Symantec Endpoint Protection was not found on your computer", nil))` |
| 终端 LUA 检查：检查 McAfee Endpoint Protection 版本 10 到 10.5.3 及 10.6 以上的版本。 | `(EVAL(endpoint.am["1637"].version,"GE","10","version") and EVAL(endpoint.am["1637"].version,"LT","10.5.4","version") or EVAL(endpoint.am["1637"].version,"GE","10.6","version"))` |
| 终端 LUA 检查：检查 McAfee 防恶意软件定义在过去 10 天（864000 秒）内是否更新，如需要更新则显示一条消息。 | `(CheckAndMsg(EVAL(endpoint.am["1637"].lastupdate,"GT","864000","integer"),"Update needed! Please wait for McAfee to load the latest dat file.", nil))` |
| debug dap trace 返回 `endpoint.os.windows.hotfix["KB923414"] = "true";` 后，检查特定修补程序 | `(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"NE","true"), "The required hotfix is not installed on your PC.",nil))` |

### 检查防恶意软件程序并提供消息

您可以配置消息，以便最终用户了解并能够修复防恶意软件的问题。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。如果访问被拒绝，ASA 会收集导致“终止”情况的 DAP 的所有消息，并于浏览器中在登录页面上显示这些消息。

以下示例显示了如何使用此功能检查 Symantec Endpoint Protection 的状态。

1. 将以下 LUA 表达式复制并粘贴至“添加/编辑动态访问策略”窗格的“高级”字段中（请点击最右侧的双箭头，以便展开此字段）。

   ```
   (CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint Protection","string") and EVAL(endpoint.am["538"].activescan,"NE","ok","string") "Symantec Endpoint Protection is disabled. You must enable before being granted access", nil))
   ```

2. 在同一 Advanced 字段中，点击 **OR** 按钮。
3. 在下面的 Access Attributes 部分，在最左侧的选项卡 Action 中，点击 **Terminate**。
4. 从已安装 Symantec Endpoint Protection 但 Symantec Endpoint Protection 已被禁用的 PC 进行连接。预期结果应该是不允许该连接，并且用户将看到消息“Symantec Endpoint Protection 已被禁用。您必须将其启用后才能获得访问权限”

### 检查防恶意软件程序和超过 2 天的定义

此示例检查 Symantec 和 McAfee 防恶意软件程序是否存在，以及病毒定义是否超过 2 天（172800 秒）。如果定义超过 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“添加/编辑动态访问策略”窗格的“高级”字段中：

```
(CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint
Protection","string") and EVAL(endpoint.am["538"].lastupdate,"GT","172800","integer"),
"Symantec Endpoint Protection Virus Definitions are Out of Date. You must run LiveUpdate
 before being granted access", nil)) or
(CheckAndMsg(EVAL(endpoint.am["1637"].description,"EQ","McAfee Endpoint
Security","string") and EVAL(endpoint.am["1637"].lastupdate,"GT","172800","integer"),
"McAfee Endpoint Security Virus Definitions are Out of Date. You must update your McAfee
 Virus Definitions before being granted access", nil))
```

2. 在同一 Advanced 字段中，点击 **AND**。
3. 在下面的 Access Attributes 部分，在最左侧的选项卡 Action 中，点击 **Terminate**。
4. 从安装了 Symantec 和 McAfee 防恶意软件程序并且版本已超过 2 天未更新的 PC 进行连接。

   预期结果应该是不允许该连接，并且用户将看到一条消息，说明病毒定义已过期。

# 配置 DAP 访问和授权策略属性

点击以下每个选项卡，并配置其中包含的字段。

### 过程

**步骤 1** 选择 **Action** 选项卡指定应用至特定连接或会话的特殊处理。

- Continue -（默认值）点击以将访问策略属性应用于会话。
- Quarantine - 通过使用隔离，您可以限制已通过 VPN 建立隧道的特定客户端。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，但会对用户施加限制。修复后，用户可以重新连接，调用新的终端安全评估。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 - 点击以终止会话。
- User Message - 输入一条文本消息，当此 DAP 记录选定时，该消息会显示在门户页面上。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。如果选择了多条 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：有关升级防恶意软件的程序，请所有承包商阅读<a href='http://wwwin.example.com/procedure.html'>说明</a>。

**步骤 2** 选择 **Network ACL Filters** 选项卡可配置应用至此 DAP 记录的网络 ACL。

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。ACL 可以是允许和拒绝规则的任意组合。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 list** - 显示此 DAP 记录的网络 ACL。
- **添加** - 点击以便将下拉列表中选定的网络 ACL 添加至右侧的网络 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。

**步骤 3** 选择 **Web-Type ACL Filters (clientless)** 选项卡以配置应用至此 DAP 记录的 Web 类型 ACL。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 Web 类型 ACL，以便添加至此 DAP 记录。ACL 可以是允许和拒绝规则的任意组合。
- **管理** - 点击以便添加、编辑和删除 Web 类型 ACL。
- **Web-Type ACL** 列表 - 显示此 DAP 记录的 Web 类型 ACL。
- **添加** - 点击以便将下拉列表中选定的 Web 类型 ACL 添加至右侧的 Web 类型 ACL 列表。
- **Delete** - 点击以便将 Web 类型 ACL 从 Web 类型 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。

**步骤 4** 选择 **Functions** 选项卡为 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（主浏览器或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。可以下载、编辑、删除、重命名和移动文件。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 小应用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。它会绕过处理，同时确保安全设备的持续使用。转发的代理自动修改浏览器的原有代理配置，并将所有 HTTP 和 HTTPS 请求重定向到新的代理配置。支持几乎所有客户端技术，包括HTML、CSS、JavaScript、VBScript、ActiveX 和 Java。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 Web 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 或工作站与企业网络上的 ASA 之间数据传输的安全性。如果用户届时访问非 HTTPS Web 资源（位于互联网或内部网络上），则从企业 ASA 到目的 Web 服务器之间的通信不安全。

在无客户端 VPN 连接中，ASA 用作最终用户 Web 浏览器和目标 Web 服务器之间的代理。当用户连接到支持 SSL 的 Web 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供的证书，因此无法检查并验证证书。SSL VPN 的当前实施不允许与提供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 Web 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 Web。

- **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** - 点击以启用 HTTP 代理，并让 DAP 记录自动启动与这些功能关联的小应用程序。

**步骤 5** 选择 **Port Forwarding Lists** 选项卡为用户会话配置端口转发列表。

端口转发为此组中的远程用户提供对客户端/服务器应用的访问权限，这些应用经由已知的固定 TCP/IP 端口进行通信。远程用户可以使用安装在其本地 PC 上的客户端应用，并安全访问支持该应用的远程服务器。思科已经测试了以下应用：Windows Terminal Services、Telnet、Secure FTP (FTP over SSH)、Perforce、Outlook Express 和 Lotus Notes。其他基于 TCP 的应用可能也可以正常使用，但是思科没有对其进行过测试。

**注释** 端口转发不能与某些 SSL/TLS 版本配合使用。

**注意** 确保在远程计算机上安装 Sun Microsystems Java Runtime Environment (JRE) 来支持端口转发（应用访问）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** - 点击以将属性从运行配置中删除。
- **Enable/Disable** - 点击以启用或禁用端口转发。
- **Auto-start** - 点击以启用端口转发，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应用程序。
- **Port Forwarding List** 下拉列表 - 选择已经配置的端口转发列表，以添加至 DAP 记录。
- **New...** - 点击以配置新的端口转发列表。
- **Port Forwarding Lists**（未标记）- 显示 DAP 记录的端口转发列表。
- **Add** - 点击以将下拉列表中的选定端口转发列表添加至右侧的 Network ACL 列表。
- **Delete** - 点击以从 Port Forwarding 列表中删除选定的端口转发列表。不能从 ASA 中删除端口转发列表，除非您先将其从 DAP 记录中删除。

**步骤 6** 选择 **Bookmarks** 选项卡，为特定用户会话 URL 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。
- **管理...** - 点击以添加、导入、导出和删除书签。
- **Bookmarks (unlabeled)** - 显示 DAP 记录的 URL 列表。
- **Add>>** - 点击以将下拉列表中的选定书签添加至右侧的 URL 区域。
- **Delete** - 点击以从 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。

**步骤 7** 选择 **Access Method** 选项卡，配置允许的远程访问的类型。

- **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。

**步骤 8** 选择 **AnyConnect** 选项卡，以选择 Always-on VPN 标志状态。

- 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 Web 安全设备的版本，该设备为思科 AnyConnect VPN 客户端提供安全移动解决方案许可支持。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》。

**步骤 9** 选择 **AnyConnect Custom Attributes** 选项卡，查看之前定义的自定义属性并将其与此策略关联。您还可以定义自定义属性，然后将其与此策略关联。

自定义属性会被发送到 AnyConnect 客户端，并且该客户端用其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。

# 执行 DAP 跟踪

DAP 跟踪显示所有连接的设备的 DAP 终端属性。

**过程**

**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，第 187 页
- 使用 DAP 应用 WebVPN ACL，第 188 页
- 执行 CSD 检查，并通过 DAP 应用策略，第 188 页


# 使用 DAP 定义网络资源

本示例显示如何将动态访问策略配置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。

**过程**

**步骤 1** 在 ASDM 中，依次转至**Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Dynamic AccessPolicies** > **Add/Edit Dynamic Access Policy** > **Endpoint**。

**步骤 2** 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 Web 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 ASA 对 AD 组 (memberOf) = Engineering 中的用户应用配置的 Web 类型 ACL。

过程

**步骤 1** 在 ASDM 中，转至“添加 AAA 属性”窗格，**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **动态访问策略** > **添加/编辑动态访问策略** > **AAA 属性部分** > **添加 AAA 属性**。

**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，使用下拉列表选择 =，并在相邻字段中输入 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 group (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，对于 DAP 未定义或控制的那些内容（例如分割隧道列表、横幅和 DNS），ASA 将应用常规 AAA 组策略继承规则和属性。

过程

**步骤 1** 在 ASDM 中，转至“添加 AAA 属性”窗格，**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **动态访问策略** > **添加/编辑动态访问策略** > **AAA 属性部分** > **添加 AAA 属性**。

**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，使用下拉列表选择 =，并在相邻字段中输入 Engineering。

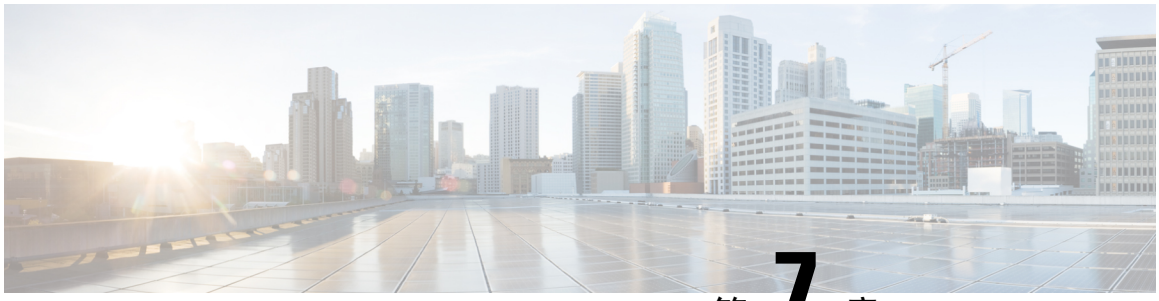
**步骤 5** 在 Attribuet ID 字段中，输入 memberOf，正如此处所示。大小写非常重要。

**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 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。



第 7 章

# 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 支持的一种邮件代理。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，然后会进行身份验证。POP3S 用于接收邮件。

### IMAP4S

IMAP4S 是无客户端 SSL VPN 支持的一种邮件代理。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 支持的一种邮件代理。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

## 邮件代理的要求

- 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账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

过程

**步骤 1** 浏览至**配置** > **功能** > **VPN** > **邮件代理** > **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 - 选择用于用户记账的记账服务器组。默认设置为未配置记账服务器。
- 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。
- Authrization Settings - 为 ASA 用于识别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 - 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，例如 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) | 组织所在的省、自治区或直辖市。 |
| 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。选项包括以前表中的所有选项，加上 **None**，如果您不想包括辅助字段可选择此选项。

# 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。

过程

**步骤 1** 浏览至**配置** > **VPN** > **邮件代理** > **访问**，显示为接口启用的内容。

- Interface - 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**编辑**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

为每种邮件代理类型配置身份验证方法。

过程

**步骤 1** 浏览至**配置** > **功能** > **VPN** > **邮件代理** > **身份验证**。

**步骤 2** 从多种身份验证方法中选择：

- 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。用户要提供用户名、服务器和密码。用户必须同时提供 VPN 用户名和邮件用户名，其以 VPN 名称分隔符分隔（仅当用户名各不相同时）。
- Certificate - 选择此选项表示需要进行证书身份验证。

  **注释** 证书身份验证对于当前 ASA 软件版本中的邮件代理不起作用。

  证书身份验证要求用户拥有 ASA 可在 SSL 协商期间验证的证书。您可以将证书身份验证用作唯一的身份验证方法，如 SMTPS 代理。其他邮件代理需要两种身份验证方法。

  证书身份验证需要均来自相同 CA 的三个证书：

  - ASA 上的 CA 证书。

- 客户端 PC 上的一个 CA 证书。

- 客户端 PC 上的网络浏览器证书，有时称为个人证书或网络浏览器证书。

- 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。用户只提供邮件用户名。不需要密码。用户必须同时提供 VPN 用户名和邮件用户名，其以 VPN 名称分隔符分隔（仅当用户名各不相同时）。

  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：

  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。

  **注释** 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

通过此“默认服务器”面板，您可以向ASA标识代理服务器，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。

**过程**

**步骤 1** 浏览至**配置** > **功能** > **VPN** > **邮件代理** > **默认服务器**。

**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。
- “端口”- 键入 ASA 在其上侦听邮件代理流量的端口号。允许自动建立到已配置端口的连接。邮件代理只允许该端口上的 SSL 连接。建立 SSL 隧道后，此邮件代理将会开始工作，接着将会进行身份验证。

默认值如下：

- 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。允许您为正处于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 将会终止最早的未进行身份验证的连接。如果不存在未进行身份验证的连接，最早的正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：

- Unauthenticated - 新邮件连接的状态。
- Authenticating - 连接提供用户名时的状态。
- Authenticated - ASA 已完成连接的身份验证时的状态。

# 配置分隔符

此面板用于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。

**过程**

**步骤 1** 浏览至**配置** > **功能** > **VPN** > **邮件代理** > **分隔符**。

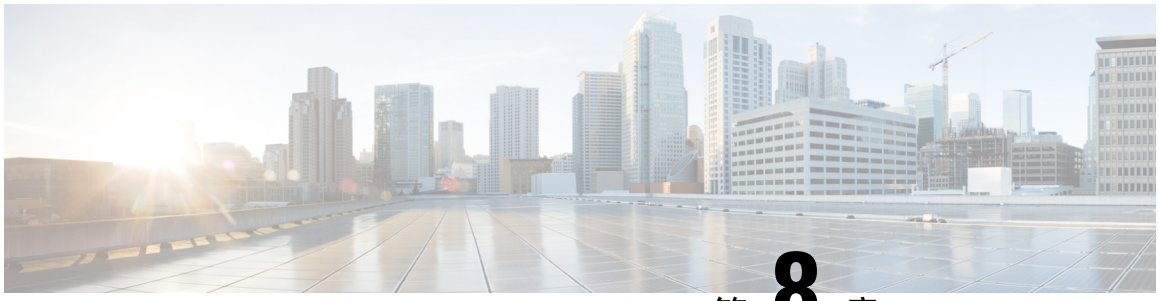
**步骤 2** 配置以下字段：

- 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，以您在此处配置的分隔符分隔，另外还有邮件服务器名称。

  **注释** 无客户端 SSL VPN 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。它必须不同于 VPN 名称分隔符。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。



第 8 章

# 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 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 到 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。

注释 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），这样就不会达到许可证容量限制，而且新用户也可以登录。您还可以使用 **show vpn-sessiondb** CLI 命令访问这些统计信息（请参阅相应版本的《思科 ASA 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以及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。

  注释 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 回应请求消息发送到选定主机。如果主机可以访问，它会返回回应应答消息，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（例如，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-- 外的任意选项，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

**监控 > VPN > VPN 统计信息 > 会话**

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终端安全评估。
- Rejected - ACS 未能成功验证远程主机的终端安全评估。
- “豁免”- 根据 ASA 上配置的“终端安全评估验证豁免”列表，远程主机被豁免终端安全评估验证。
- Non-Responsive - 远程主机没有响应 EAPoUDP Hello 消息。
- Hold-off - ASA 在终端安全评估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 - 终端安全评估验证正在进行中。

终端安全评估标记是可在访问控制服务器上配置的信息文本字符串。ACS 将终端安全评估标记下载至 ASA，以实现协助系统监控、报告、调试和记录的参考用途。在 NAC 结果之后出现的典型终端安全评估标记如下：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 用作此会话的 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（如果有）。
- 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。公用 IP 地址也称为外部 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 - 每次成功的终端安全评估验证之间所需的间隔，以秒为单位。
- Time Until Next Revalidation - 如果上次终端安全评估验证尝试未成功，则为 0。否则，为重新验证时间间隔与上次成功终端安全评估验证以来的秒数之间的差值。
- Status Query Time Interval - 每次成功的终端安全评估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，指示主机在上次终端安全评估验证后是否有任何终端安全评估更改。
- EAPoUDP Session Age - 自上次成功的终端安全评估验证起经过的秒数。

- Hold-Off Time Remaining - 如果上次终端安全评估验证成功，则为 0 秒。否则，为下一终端安全评估验证尝试之前剩余的秒数。
- Posture Token - 访问控制服务器上可配置的信息文本字符串。ACS 将终端安全评估标记下载至 ASA，以实现协助系统监控、报告、调试和记录的参考用途。典型的终端安全评估标记为 Healthy、Checkup、Quarantine、Infected 或 Unknown。
- Redirect URL- 终端安全评估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 将此远程主机的所有 HTTP（端口 80）和 HTTPS（端口 443）请求重定向至“重定向 URL”（如果有）。如果访问策略不包含“重定向 URL”，ASA 不会重定向来自远程主机的 HTTP 和 HTTPS 请求。

  重定向 URL 保持有效，直到 IPsec 会话结束或直到终端安全评估重新验证为止，对此，ACS 下载新的访问策略，其中可以包含其他重新定向 URL 或不包含重定向 URL。

  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。表中每一行表示一则加密统计信息。

### 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。表中每一行表示一则压缩统计信息。

### 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。表中每一行表示一则全局统计信息。

### Monitor NAC Session Summary

用于查看活动和积累的网络准入控制会话。

- Active NAC Sessions - 有关要进行终端安全评估验证的远程对等体的常规统计信息。
- Cumulative NAC Sessions - 有关要进行或已经进行终端安全评估验证的远程对等体的常规统计信息。
- Accepted - 传递终端安全评估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 - 终端安全评估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 - 由于与 ASA 上配置的“终端安全评估验证豁免”列表中的条目匹配而不进行终端安全评估验证的对等体数量。
- Non-responsive - 未响应终端安全评估验证的经由 UDP 的可扩展身份验证协议 (EAP) 请求的对等体的数量。未在其中运行 CTA 的对等体不响应这些请求。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 将分配 NAC 默认策略。
- Hand-off - 终端安全评估验证成功后，ASA 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终端安全评估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 - 如果对等体的终端安全评估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。点击此按钮可对 ASA 管理的所有 NAC 会话发起新的无条件终端安全评估验证。在您点击此按钮之前，有效的终端安全评估验证和分配的访问策略仍然有效，直到新的终端安全评估验证成功或失败。点击此按钮不会影响已豁免终端安全评估验证的会话。
- Initializa All - 如果对等体的终端安全评估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 会话的终端安全评估验证的已分配访问策略，并发起新的无条件终端安全评估验证。NAC 默认 ACL 在重新验证期间是有效的，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豁免终端安全评估验证的会话。

### 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。

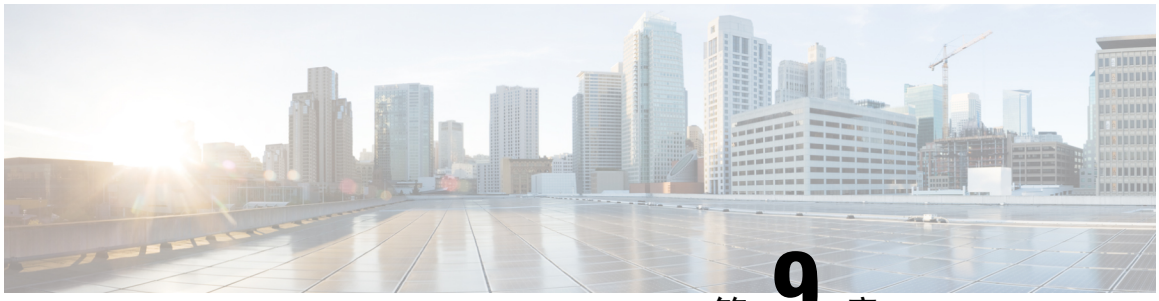
### Monitor VLAN Mapping Sessions

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。

### 监控无客户端 SSL VPN 会话的 SSO 统计信息

**Monitoring> VPN> WebVPN > SSO Statistics**

用于查看为 ASA 配置的当前活动 SSO 服务器的单点登录统计信息。



第 9 章

# SSL 设置



## SSL 设置

在以下位置之一配置 SSL 设置：

- **Configuration > Device Management > Advanced > SSL Settings**
- **配置 > 远程访问 VPN > 高级 > SSL 设置**

ASA 使用安全套接字层 (SSL) 协议和传输层安全 (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。此外，还将 DTLS 用于 AnyConnect VPN 客户端连接。SSL Settings 面板允许您为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。

注释 对于版本 9.3(2)，SSLv3 已废弃。默认值现在为 **tlsv1** 而不是 **any**。**any** 关键字已废弃。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，这些关键字将从 ASA 中删除。

对于版本 9.4(1)，所有 SSLv3 关键字都已从 ASA 配置中删除，而且 SSLv3 支持也已从 ASA 中删除。如果您启用了 SSLv3，带 SSLv3 选项的命令将出现引导时间错误。ASA 随后将恢复为默认使用 TLSv1。

Citrix Mobile Receiver 可能不支持 TLS 1.1/1.2 协议；有关兼容性，请参阅 https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf

### 字段 (Fields)

- **服务器 SSL 版本** - 指定 ASA 用作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 客户端问候并协商最高通用版本。 |

| | |
|---|---|
| **SSL V3** | 接受 SSLv2 客户端问候并协商 SSLv3（或更高版本）。 |
| **TLS V1** | 接受 SSLv2 客户端问候并协商 TLSv1（或更高版本）。 |
| **TLSV1.1** | 接受 SSLv2 客户端问候并协商 TLSv1.1（或更高版本）。 |
| **TLSV1.2** | 接受 SSLv2 客户端问候并协商 TLSv1.2（或更高版本）。 |
| **DTLSv1** | 接受 DTLSv1 客户端问候并协商 DTLSv1（或更高版本） |
| **DTLS1.2** | 接受 DTLSv1.2 客户端问候并协商 DTLSv1.2（或更高版本） |

注释 DTLS 的配置和使用仅适用于思科 AnyConnect 远程访问连接。

请使用与 DTLS 版本相等或更高版本的 TLS 来确保 TLS 会话与 DTLS 会话同样安全或更安全。鉴于此点，TLSV1.2 是选择 DTLSV1.2 时唯一可接受的 TLS 版本；而任何 TLS 版本均可与 DTLS1 配合使用，因为其版本均等于或高于 DTLS 1。

- **Client SSL Version** - 指定 ASA 用作下拉列表中的客户端时其所使用的最低 SSL/TLS 协议版本。（DTLS 对 SSL 客户端角色不可用）

| | |
|---|---|
| 任意 | 传输 SSLv3 客户端问候并协商 SSLv3（或更高版本）。 |
| SSL V3 | 传输 SSLv3 客户端问候并协商 SSLv3（或更高版本）。 |
| TLS V1 | 传输 TLSv1 客户端问候并协商 TLSv1（或更高版本）。 |
| TLSV1.1 | 传输 TLSv1.1 客户端问候并协商 TLSv1.1（或更高版本）。 |
| TLSV1.2 | 传输 TLSv1.2 客户端问候并协商 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 位素数阶和 Group24 - 2048 位模数、256 位素数阶。默认值为 Group2。

- **ECDH group to be used with SSL** - 从下拉列表选择一个组。可用选项为 Group19 - 256 位 EC、Group20 - 384 位 EC 和 Group21 - 521 位 EC。默认值为 Group19。

注释 ECDSA 和 DHE 密码具有最高优先级。

- **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**。
  - **密码版本** - 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。选择以下选项之一：

    **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-MD5（这是默认密码）、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。此选项使您可以使用 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 连接的加密算法。有关使用 OpenSSL 的加密的详细信息，请参阅https://www.openssl.org/docs/manmaster/man1/ciphers.html。

    ASA 将受支持密码的优先级顺序指定为：优先级最高的是仅受 TLSv1.2 支持的密码，优先级最低的是 TLSv1.1 或 TLSv1.2 不支持的密码。

  支持以下密码（如下表所述）：

- **Server Name Indication (SNI)** - 指定域名和与该域关联的

| 密码 | TLSv1.1/DTLS V1 | TLSV1.2/DTLSV 1.2 |
|---|---|---|
| AES128-GCM-SHA256 | 否 | 是 |
| AES128-SHA | 是 | 是 |
| AES128-SHA256 | 否 | 是 |
| AES256-GCM-SHA384 | 否 | 是 |
| AES256-SHA | 是 | 是 |
| AES256-SHA256 | 否 | 是 |
| DERS-CBC-SHA | 否 | 否 |

| 密码 | TLSv1.1/DTLS V1 | TLSV1.2/DTLSV 1.2 |
|---|---|---|
| DES-CBC-SHA | 是 | 是 |
| DHE-RSA-AES128-GCM-SHA256 | 否 | 是 |
| DHE-RSA-AES128-SHA | 是 | 是 |
| DHE-RSA-AES128-SHA256 | 否 | 是 |
| DHE-RSA-AES256-GCM-SHA384 | 否 | l |
| DHE-RSA-AES256-SHA | 是 | 是 |
| ECDHE-ECDSA-AES128-GCM-SHA256 | 否 | 是 |
| ECDHE-ECDSA-AES128-SHA256 | 否 | 是 |
| ECDHE-ECDSA-AES256-GCM-SHA384 | 否 | 是 |
| ECDHE-ECDSA-AES256-SHA384 | 否 | 是 |
| ECDHE-RSA-AES128-GCM-SHA256 | 是 | 是 |
| ECDHE-RSA-AES128-SHA256 | 否 | 是 |
| ECDHE-RSA-AES256-GCM-SHA384 | 否 | 是 |
| ECDHE-RSA-AES256-SHA384 | 否 | 是 |
| NULL-SHA | 否 | 否 |
| RC4-MD5 | 否 | 否 |
| RC4-SHA | 否 | 否 |

。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 负载均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**无**，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 10 章

# Easy VPN

本章介绍如何将任何 ASA 配置为 Easy VPN 服务器，以及如何将 FirePOWER-5506-X、5506w-x、5506h-x-X 和 5508-X 型号的思科 ASA 配置为 Easy VPNRemote 硬件客户端。



## 关于 Easy VPN

思科 Ezvpn 可显著简化远程办公室和移动员工的 VPN 配置和部署。思科 Easy VPN 提供灵活、可扩展且易用的站点间 VPN 与远程访问 VPN。它实施思科 Unity 客户端协议，让管理员可以在 Easy VPN 服务器上定义大多数 VPN 参数，从而简化 Easy VPN Remote 配置。

具备 FirePOWER 服务的思科 ASA 型号 5506-X、5506W-X、5506H-X 和 5508-X 支持 Easy VPN Remote 作为硬件客户端发起与 Easy VPN 服务器之间的 VPN 隧道。Easy VPN 服务器可以是另一台 ASA（任意型号）或基于思科 IOS 的路由器。ASA 不能同时用作 Easy VPN Remote 和 Easy VPN 服务器。

**注释** 思科 ASA 5506-X、5506W-X、5506H-X 和 5508-X 型号支持第 3 层交换而非第 2 层交换。将 Easy VPN Remote 用于内部网络中的多个主机或设备时，请使用外部交换机。如果 ASA 的内部网络中只有一台主机，则不需要交换机。

以下各节介绍 Easy VPN 选项和设置：在 ASDM 中，依次转到**配置 > VPN > Easy VPN Remote**，将 ASA 配置为 Easy VPN Remote 硬件客户端。依次转到 **配置 > 远程访问 > 网络（客户端）访问 > 组策略 > 高级 > IPsec (IKEv1) 客户端 > 硬件客户端**，在 Easy VPN 服务器上配置组策略属性。

### Easy VPN 接口

在系统启动时，Easy VPN 外部和内部接口取决于其安全级别。拥有最低安全级别的物理接口用于与 Easy VPN 服务器的外部连接。拥有最高安全级别的物理或虚拟接口用于内部连接，以便保护资源。如果 Easy VPN 确定有两个或更多接口同样拥有最高安全级别，Easy VPN 会被禁用。

您可以根据需要，使用 **vpnclient secure interface** 命令将内部安全接口更改为某个物理或虚拟接口，或从某个物理或虚拟接口更改为其他接口。外部接口是自动选择的默认物理接口，此接口无法更改。

例如，在 ASA5506 平台上，出厂配置将拥有最高安全级别接口的 BVI 的安全级别设置为 100（其成员接口的安全级别也为 100），而一个外部接口的安全级别为零。默认情况下，Easy VPN 会选择这些接口。

启动时选择或管理员分配虚拟接口（桥接虚拟接口，即 BVI）作为内部安全接口时，适用以下几点：

- 所有 BVI 成员接口都被视为内部安全接口，不考虑其本身的安全级别。
- 需要在所有成员接口上添加 ACL 和 NAT 规则。单独在 BVI 接口上添加 AAA 规则。

### Easy VPN 连接

Easy VPN 使用 IPsec IKEv1 隧道。Easy VPN Remote 硬件客户端的配置必须与 Easy VPN 服务器头端上的 VPN 配置兼容。如果使用辅助服务器，其配置必须与主服务器相同。

ASA Easy VPN Remote 配置主 Easy VPN 服务器的 IP 地址，并选择性地配置最多 10 个辅助（备用）服务器的 IP 地址。如果无法建立通向主服务器的隧道，客户端会尝试与第一台辅助 VPN 服务器的连接，然后以 8 秒为间隔按自上而下的顺序相继尝试 VPN 服务器列表中的其他服务器。如果与第一台辅助服务器建立隧道失败，并且主服务器在此期间联机，客户端将继续建立通向第二台辅助 VPN 服务器的隧道。

默认情况下，Easy VPN 硬件客户端和服务器将 IPsec 封装在用户数据报协议 (UDP) 数据包中。某些环境（如具有某些防火墙规则或 NAT 和 PAT 设备）禁止 UDP。要在此类环境中使用标准封装安全协议（ESP、Protocol 50）或互联网密钥交换（IKE、UDP 500），必须将客户端和服务器配置为将 IPsec 封装在 TCP 数据包内以实现安全的隧道传输。但如果您的环境允许 UDP，配置 IPsec over TCP 会添加不必要的开销。

### Easy VPN 隧道组

隧道建立后，Easy VPN Remote 指定将用于连接的隧道组（在 Easy VPN 服务器上配置）。Easy VPN 服务器将组策略或用户属性推送到 Easy VPN Remote 硬件客户端，决定隧道行为。要更改某些属性，必须在配置为主 Easy VPN 服务器或辅助 Easy VPN 服务器的 ASA 上对其进行修改。

### Easy VPN 运行模式

此模式决定了是否可以通过隧道从企业网络访问位于 Easy VPN Remote 之后的主机：

- 客户端模式也称为端口地址转换 (PAT) 模式，将 Easy VPN Remote 专用网络中的所有设备与企业网络中的设备隔离。Easy VPN Remote 对其内部主机的所有 VPN 流量执行端口地址转换 (PAT)。Easy VPN Remote 专用端的网络和地址会隐藏，不能直接进行访问。Easy VPN 客户端内部接口或内部主机不需要 IP 地址管理。
- 网络扩展模式 (NEM) 使内部接口和所有内部主机可以通过隧道在整个企业网络中路由。内部网络中的主机从预先配置了静态 IP 地址的可访问子网（静态或通过 DHCP）获取 IP 地址。在 NEM 模式下，PAT 不适用于 VPN 流量。此模式不需要为内部网络中的每个主机提供 VPN 配置或隧道，Easy VPN Remote 将为所有主机提供隧道。

Easy VPN 服务器默认为客户端模式。因为 Easy VPN Remote 没有默认模式，必须先在其上指定一种运行模式后才能建立隧道。

注释 为 NEM 模式配置的 Easy VPN Remote ASA 支持自动隧道启动。自动启动需要配置并存储用于建立隧道的凭证。如果启用了安全设备身份验证，则会禁用自动隧道启动。

处于网络扩展模式并配置了多个接口的 Easy VPN Remote 只为来自安全级别最高的接口的本地加密流量建立隧道。

### Easy VPN 用户身份验证

ASA Easy VPN Remote 可以存储用于自动登录的用户名和密码。。

为增加安全性，Easy VPN 服务器可能需要：

- 安全设备身份验证 (SUA) - 忽略配置的用户名和密码而要求用户手动进行身份验证。默认情况下，SUA 已禁用，请在 Easy VPN 服务器上启用 SUA。
- 个人用户身份验证 (IUA) - 要求位于 Easy VPN Remote 之后的用户进行身份验证后才能获得企业 VPN 网络的访问权限。默认情况下，IUA 已禁用，请在 Easy VPN 服务器上启用 IUA。

  使用 IUA 时，位于硬件客户端之后的思科 IP 电话或打印机等特定设备需要绕过个人用户身份验证。要进行此配置，请在 Easy VPN 服务器上指定 IP 电话绕行，并在 Easy VPN Remote 上指定 MAC 地址豁免。

  此外，Easy VPN 服务器还可以设置或删除空闲超时期限，Easy VPN 服务器将在此时间后终止客户端的访问。

如果未配置用户名和密码或禁用了 SUA 或启用了 IUA，思科 Easy VPN 服务器将拦截 HTTP 流量并将用户重定向至登录页。HTTP 重定向会自动执行，不需要在 Easy VPN 服务器上进行配置。

### 远程管理

作为 Easy VPN Remote 硬件客户端运行的 ASA 支持使用 SSH 或 HTTPS 的管理访问，有无额外的 IPsec 加密均可。

默认情况下，管理隧道在 SSH 或 HTTPS 加密内使用 IPsec 加密。您可以清除 IPsec 加密层，允许 VPN 隧道外的管理访问。清除隧道管理只是移除了 IPsec 加密级别，并不会影响连接上存在的任何其他加密，例如 SSH 或 HTTPS。

为增加安全性，Easy VPN Remote 可能需要 IPsec 加密，并限制对公司侧的特定主机或网络进行管理访问。

注释 如果 ASA Easy VPN Remote 与互联网之间运行着 NAT 设备，请勿在 ASA Easy VPN Remote 上配置管理隧道。在该配置中，清除远程管理。

无论您如何配置，DHCP 请求（包括更新消息）都不应该流经 IPsec 隧道。即使是 vpnclient 管理隧道，也禁止 DHCP 流量。

# 配置 Easy VPN Remote

将 ASA 配置为 Easy VPN Remote 硬件客户端。

注释 只能将具备 FirePOWER 服务的思科 5506-X、5506W-X、5506H-X 和 5508-X 型号配置为 Easy VPN Remote 硬件客户端。

### 准备工作

收集以下信息用于配置 Easy VPN Remote：

- 主 Easy VPN 服务器和可用的辅助服务器的地址。
- Easy VPN Remote 的运行应采用的寻址模式（客户端还是 NEM）。
- Easy VPN 服务器组策略名称和密码（预共享密钥），或将要选择所需组策略并进行身份验证的预配置信任点。
- Easy VPN 服务器上配置的有权使用 VPN 隧道的用户。

### 配置 > VPN > Easy VPN Remote

**启用 Easy VPN Remote** - 启用 Easy VPN Remote 功能并使此对话框中的其余字段可进行配置。

**模式** - 选择客户端模式或网络扩展模式。

- **客户端模式** - 使用端口地址转换 (PAT) 模式隔离内部主机（相对于客户端而言）的地址与企业网络。
- **网络扩展模式** - 使这些地址可从企业网络进行访问。

  注释 如果 Easy VPN Remote 使用 NEM 模式并已连接到辅助服务器，请与每个头端建立ASDM连接，并对您在“配置”>“远程访问VPN”>“网络（客户端）访问”>“高级”>“IPsec”>“加密映射”中创建的加密映射选中“启用反向路由注入”，以配置动态通告使用 RRI 的远程网络。

- **自动连接** - Easy VPN Remote 将建立自动 IPsec 数据隧道，除非以下两种情况均属实：在本地配置了网络扩展模式，并且对推送到 Easy VPN Remote 的组策略配置了分割隧道。如果以上两者均属实，选中此属性将自动建立 IPsec 数据隧道。否则，此属性无效。

**组设置** - 指定使用预共享密钥还是 X.509 证书进行用户身份验证。

- **预共享密钥** - 使用预共享密钥进行身份验证并使后续的“组名称”、“组密码”和“确认密码”字段可用于指定组策略名称和包含该密钥的密码。
  - **组名称** - 指定要用于身份验证的组策略的名称。

- **组密码** - 指定要用于指定组策略的密码。
- **确认密码** - 要求您确认刚才输入的组密码。

- **X.509 证书** - 指定使用证书颁发机构提供的 X.509 数字证书进行身份验证。
  - **选择信任点** - 通过它可以从下拉列表中选择信任点，信任点可为 IP 地址或主机名。要定义信任点，请点击此区域底部的信任点配置链接。
  - **发送证书链** - 能够发送证书链而不仅是证书本身。此操作在传输中包含根证书和任何从属 CA 证书。

**用户设置** - 配置用户登录信息。

- **用户名** - 为 Easy VPN Remote 连接配置 VPN 用户名。Xauth 提供使用 TACACS+ 或 RADIUS 在 IKE 内对用户进行身份验证的功能。Xauth 使用 RADIUS 或支持的任何其他用户身份验证协议对用户（在此情况下是 Easy VPN 硬件客户端）进行身份验证。当安全设备身份验证被禁用且服务器请求 Xauth 凭证时，会使用 Xauth 用户名和密码参数。如果安全设备身份验证已启用，这些参数将被忽略，并且 ASA 将提示用户输入用户名和密码。
- **用户密码**和**确认密码** - 为 Easy VPN Remote 连接配置并确认 VPN 用户密码。

**要添加的 Easy VPN 服务器** - 添加或删除 Easy VPN 服务器。任何 ASA 均可用作 Easy VPN 服务器。必须先配置服务器，然后才能建立连接。ASA 支持 IPv4 地址、名称数据库或 DNS 名称并按照这个顺序解析地址。Easy VPN 服务器列表中的第一个服务器是主服务器。除主服务器之外，您最多还可以指定十台备用服务器。

- **Easy VPN 服务器** - 按优先级顺序列出配置的 Easy VPN 服务器。
- **名称或 IP 地址** - 要添加到列表中的 Easy VPN 服务器的名称或 IP 地址。
- **添加**和**删除** - 将指定的服务器移到 Easy VPN 服务器列表中或从中移除。
- **上移**和**下移** - 更改服务器在 Easy VPN 服务器列表中的位置。仅当列表中有多台服务器时，这些按钮才可用。

**安全客户端接口** - 在启动时，拥有最高安全级别的物理接口或 BVI 用于内部连接，以便保护资源。如果希望使用其他接口，请从下拉列表中选择一个选项。可以分配物理或虚拟接口。

### 配置 > VPN > Easy VPN Remote > 高级

**MAC 豁免** - 为 Easy VPN Remote 连接配置一组用于设备直通的 MAC 地址和掩码。某些设备（如思科 IP 电话和打印机）无法执行身份验证，因此无法加入到单个设备身份验证中。为满足这些设备的需求，通过“MAC 豁免”属性启用的设备直通功能可以在启用个人用户身份验证时豁免具有指定 MAC 地址的设备的身份验证。

- **MAC 地址** - 豁免具有指定 MAC 地址的设备的身份验证。

  此字段中用于指定 MAC 地址的格式为三个十六进制数字（以点号分隔）；例如，45ab.ff36.9999。MAC 地址的前 24 位表示这台设备的制造商。最后 24 位是十六进制格式的设备序列号。

- **MAC 掩码** - 此字段中用于指定 MAC 掩码的格式为三个十六进制数字（以点号分隔）；例如，MAC 掩码 ffff.ffff.ffff 只匹配指定的 MAC 地址。全零的 MAC 掩码不匹配任何 MAC 地址，而 ffff.ff00.0000 的 MAC 掩码匹配同一制造商生产的所有设备。
- **添加**和**删除** - 在 MAC 地址/掩码列表中添加或删除指定的 MAC 地址和掩码对。

**隧道管理** - 配置 IPsec 加密用于设备管理，并指定允许通过隧道管理 Easy VPN 硬件客户端连接的一个或多个网络。

- **启用隧道管理** - 向管理隧道中已有的 SSH 或 HTTPS 加密添加 IPsec 加密层。
- **清除隧道管理** - 使用管理隧道中已有的加密，而无需额外加密。选择“清除隧道管理”只是移除了 IPsec 加密级别，并不会影响连接上存在的任何其他加密，例如 SSH 或 HTTP。
- **IP 地址/掩码** - 列出已配置的 IP 地址和掩码对，它们是此区域中的“启用”或“清除”功能的操作对象。
  - **IP 地址** - 指定要向其授予管理访问权限的主机或网络的 IP 地址，以使主机或网络能够通过 VPN 隧道访问 Easy VPN 硬件客户端。
  - **掩码** - 为相应的 IP 地址指定网络掩码。
  - **添加/删除** - 在 IP 地址/掩码列表中添加或删除指定的 IP 地址和掩码。

**经由 TCP 的 IPsec** - 将 Easy VPN Remote 连接配置为使用 PCT 封装的 IPsec。

注释 如果将 Easy VPN Remote 连接配置为使用 PCT 封装的 IPsec，则必须配置 ASA 以发送大数据包。

依次转到**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPsec > IPsec 分片策略**，双击外部接口，将“DF 位设置策略”设置为“清除”。

- **启用** - 启用经由 TCP 的 IPsec。
- **输入端口号** - 指定要用于经由 TCP 的 IPsec 连接的端口号。

**服务器证书** - 将 Easy VPN Remote 连接配置为只接受具有证书映射指定的特定证书的 Easy VPN 服务器连接。使用此参数启用 Easy VPN 服务器证书过滤。

# 配置 Easy VPN 服务器

### 开始之前

确保所有辅助 Easy VPN 服务器配置的选项和设置与主 Easy VPN 服务器相同。

过程

**步骤 1** 配置 Easy VPN 服务器以支持 IPsec IKEv1。请参阅常规 VPN 设置，第 49 页。

**步骤 2** 设置特定 Easy VPN 服务器属性。请参阅内部组策略，IPsec (IKEv1) 的硬件客户端属性，第 84 页。

# Easy VPN 的功能历史记录

| 功能名称 | 版本 | 功能信息 |
|---|---|---|
| ASA 5506-X、5506W-X、5506H-X 和 5508-X 上的思科 Easy VPN 客户端 | 9.5(1) | 此版本支持在 ASA 5506-X 系列和 ASA 5508-X 型号的设备上使用思科 Easy VPN。当连接到 VPN 头端时，ASA 会充当 VPN 硬件客户端。当一个 ASA 设备连接到 Easy VPN 端口，其下面连接的所有设备（计算机、打印机等）都可通过 VPN 进行通信；这些设备无需单独运行VPN 客户端。请注意只有一个 ASA 接口可用作 Easy VPN 端口；要使多个设备连接到该端口，您需在该端口安置一个第二层交换机，再将您的设备连接至交换机。<br>引入了以下菜单项：**配置 > VPN > Easy VPN Remote** |

| 功能名称 | 版本 | 功能信息 |
| --- | --- | --- |
| 实现 BVI 支持的 Easy VPN 增强功能 | 9.9(2) | Easy VPN 经过增强，可支持使用网桥虚拟接口作为其内部安全接口，并且现在允许管理员直接使用新的 **vpnclient secure interface** [*interface-name*] 命令来配置内部安全接口。<br><br>可以将物理接口或网桥虚拟接口分配为内部安全接口。如果管理员未设置此选项，Easy VPN 将会使用与以前一样的安全级别选择其内部安全接口，而不论此接口是独立的物理接口还是 BVI。<br><br>此外，现在如果在 BVI 上启用了管理访问，则可以在其上面配置 **telnet**、**http** 和 **ssh** 等管理服务。 |

第 11 章

# Virtual Tunnel Interface

本章介绍如何配置 VTI 隧道。



# 关于 Virtual Tunnel Interface

ASA 支持称为虚拟隧道接口 (VTI) 的逻辑接口。作为基于策略的 VPN 的替代方案，可以在配置了虚拟隧道接口的对等体之间创建 VPN 隧道。这可通过将 IPSec 配置文件连接到每个隧道的端部，为基于 VPN 的路由提供支持。这样，就可以使用动态或静态路由。VTI 的出口流量经加密发送至对等体，而关联的 SA 会解密 VTI 的进口流量。

使用 VTI 将不再需要配置静态加密映射访问列表并将其映射到接口。您不再需要跟踪所有远程子网并将其包含在加密映射访问列表中。这可以简化部署，而且静态 VTI 通过动态路由协议支持基于路由的 VPN，还能满足虚拟私有云的诸多要求。

# Virtual Tunnel Interface 指南

### IPv6

- 不支持 IPv6。

### 常规配置准则

- VTI 只有在 IPsec 模式下才可配置。不支持在 ASA 上终止 GRE 隧道。
- 可以将动态或静态路由用于使用隧道接口的流量。
- VTI 的 MTU 将根据底层物理接口自动设置。
- 如果必须应用网络地址转换，则将 IKE 和 ESP 数据包封装在 UDP 报头中。

- 无论隧道中的数据流量如何，IKE 和 IPsec 安全关联都将不断重新生成密钥。这可确保 VTI 隧道始终处于启动状态。
- 隧道组名称必须与对等体作为其 IKEv1 身份发送的内容相符。
- 隧道组名称必须与对等体作为其 IKEv1 或 IKEv2 身份发送的内容相符。
- 对于 LAN 到 LAN 隧道组中的 IKEv1，仅当隧道身份验证方法为数字证书和/或对等体配置为使用积极模式时，才能使用非 IP 地址的名称。
- 只要加密映射中配置的对等体地址与 VTI 的隧道目的地址不同，VTI 和加密映射配置就可以在同一个物理接口上共存。
- 默认情况下，通过 VTI 的所有流量都经过加密。
- VTI 接口没有安全级别配置。
- 可以在 VTI 接口上应用访问列表来控制通过 VTI 的流量。
- 仅 VTI 上支持 BGP。

### 情景模式

仅支持单一模式。

### 防火墙模式

仅在路由模式中受支持。

# 创建 VTI 隧道

要配置 VTI 隧道，请创建 IPsec 提议（转换集）。您需要创建引用该 IPsec 提议的 IPsec 配置文件，然后使用该 IPsec 配置文件创建 VTI 接口。使用相同 IPsec 提议和 IPsec 配置文件参数配置远程对等体。SA 协商将在所有隧道参数配置完后开始。

**注释** 对于同时属于两个 VPN VTI 域并且物理接口上存在 BGP 邻接关系的 ASA：

因接口运行状况检查而触发状态更改时，系统将删除物理接口中的路由，直至与新的活动对等体重新建立 BGP 邻接关系。此行为不适用于 VTI 逻辑接口。

### 过程

**步骤 1** 添加 IPsec 提议（转换集）。

**步骤 2** 添加 IPsec 配置文件。

**步骤 3** 添加 VTI 隧道。

# 添加 IPsec 提议（转换集）

为了保护 VTI 隧道中的流量，需要使用转换集。转换集作为 IPsec 配置文件的一部分使用，是安全协议和算法的集合，用于保护 VPN 中的流量。

### 开始之前

- 可以使用预共享密钥或证书对与 VTI 关联的 IKEv1 会话进行身份验证。必须在用于 VTI 的隧道组下配置预共享密钥。
- 对于使用 IKEv1 的基于证书的身份验证，必须指定要在发起方使用的信任点。对于响应方，必须在 tunnel-group 命令中配置信任点。
- 可以使用预共享密钥或证书对与 VTI 关联的 IKE 会话进行身份验证。IKEv2 允许使用不对称身份验证方法和密钥。对于 IKEv1 和 IKEv2，必须在用于 VTI 的隧道组下配置预共享密钥。
- 对于使用 IKEv1 的基于证书的身份验证，必须指定要在发起方使用的信任点。对于响应方，必须在 tunnel-group 命令中配置信任点。对于 IKEv2，必须同时在发起方和响应方的 tunnel-group 命令下配置用于身份验证的信任点。

### 过程

**步骤 1** 依次选择**配置** > **站点间 VPN** > **高级** > **IPsec 提议（转换集）**。

**步骤 2** 配置 IKEv1 或 IKEv2，以建立安全关联。

- 配置 IKEv1。

a) 在“IKEv1 IPsec 提议（转换集）”面板中，点击**添加**。
b) 输入**转换集名称**。
c) 保留**隧道**复选框的默认选择。
d) 选择 **ESP 加密**和 **ESP 身份验证**。
e) 点击 **OK**。

- 配置 IKEv2。

a) 在“IKEv2 IPsec 提议”面板中，点击**添加**。
b) 输入**名称**和**加密**。
c) 选择**完整性散列**。
d) 点击**OK**。

# 添加 IPsec 配置文件

IPsec 配置文件包含其引用的 IPsec 提议或转换集中所需的安全协议和算法。这能够确保两个站点间 VIT VPN 对等体之间存在安全的逻辑通信路径。

过程

**步骤 1** 依次选择**配置** > **站点间 VPN** > **高级** > **IPsec 提议**（**转换集**）。

**步骤 2** 在 **IPsec 配置文件**面板中，点击**添加**。

**步骤 3** 输入 IPsec 配置文件**名称**。

**步骤 4** 输入为 IPsec 配置文件创建的 **IKE v1 IPsec 提议**或 **IKE v2 IPsec 提议**。可以选择 IKEv1 转换集或 IKEv2 IPsec 提议。

**步骤 5** 如果需要 VTI 隧道一端仅用作响应方，请选中**仅响应方**复选框。

- 可以将 VTI 隧道的一端配置为仅用作响应方。仅响应方端不会发起隧道或重新生成密钥。
- 如果使用的是IKEv2，请设置安全关联生命周期的持续时间，此值应大于发起方端的IPsec配置文件中的生命周期值。这是为了方便发起方端成功地重新生成密钥，并确保隧道保持活动状态。
- 如果发起方端的重新生成密钥配置未知，请删除仅响应方模式以便双向建立SA，或在仅响应方端配置无限 IPsec 生命周期值以防止到期。

**步骤 6** （可选）选中**启用安全关联生命周期**复选框，并输入以**千字节**和**秒**为单位的安全关联持续时间值。

**步骤 7** （可选）选中 **PFS 设置**复选框启用 PFS，并选择所需的 Diffie-Hellman 组。

完美前向保密 (PFS) 为每个加密交换生成唯一会话密钥。此唯一会话密钥可保护交换免于后续解密。要配置 PFS，必须选择在生成 PFS 会话密钥时要使用的 Diffie-Hellman 密钥导出算法。该密钥导出算法将生成 IPsec 安全关联 (SA) 密钥。每组具有不同的长度模数。模数越大，安全性越高，但需要的处理时间更长。两个对等体上的 Diffie-Hellman 组必须匹配。

这可以确立 encryption-key-determination 算法的强度。ASA 使用此算法派生加密密钥和散列密钥。

**步骤 8** （可选）选中**启用发送证书**复选框，然后选择用于定义发起VTI隧道连接时要使用的证书的**信任点**。根据需要选中**链**复选框。

**步骤 9** 点击 **OK**。

**步骤 10** 在 **IPsec 提议**（**转换集**）主面板中，点击**应用**。

**步骤 11** 在**预览 CLI 命令**对话框中，点击**发送**。

# 添加 VTI 接口

要创建新 VTI 接口并建立 VTI 隧道，请执行以下步骤：

注释 实施 IP SLA，确保当活动隧道中的路由器不可用时，隧道仍保持活动状态。请参阅《ASA 常规操作配置指南》(http://www.cisco.com/go/asa-config) 中的“配置静态路由跟踪”。

过程

步骤 1 依次选择**配置** > **设备设置** > **接口设置** > **接口**。

步骤 2 依次选择**添加** > **VTI 接口**。系统将显示**添加 VTI 接口**窗口。

步骤 3 在**常规**选项卡中，输入 **VTI ID**。这可以是 0 到 100 之间的任意值。最多可支持 100 个 VTI 接口。

注释 如果您准备将配置从其他设备迁移到 ASA 5506 设备，请使用 1 到 100 的隧道 ID 范围。这是为了确保与 ASA 5506 设备中可用的 1 到 100 的隧道范围兼容。

步骤 4 输入**接口名称**。

确保已选中“启用接口”复选框。

步骤 5 输入隧道的源 **IP 地址**和**子网掩码**。

步骤 6 点击 **高级** 选项卡。

所有字段都需要具有有效的值或选项，VPN 向导中才会显示隧道。

步骤 7 输入**目的 IP** 地址。

步骤 8 选择**源接口**。

步骤 9 在**使用 IPsec 配置文件保护隧道**字段中，选择 IPsec 配置文件。

步骤 10 选中**确保启用隧道模式 IPv4 IPsec** 复选框。

步骤 11 点击 **OK**。

步骤 12 在**接口**面板中，点击**应用**。

步骤 13 在**预览 CLI 命令**对话框中，点击**发送**。

更新后的配置加载完毕后，新 VTI 将显示于接口列表中。此新 VTI 可用于创建 IPsec 站点间 VPN。

第 12 章

# 为 VPN 配置外部 AAA 服务器



## 关于外部 AAA 服务器

此 ASA 可配置为使用外部 LDAP、RADIUS 或 TACACS+ 服务器来支持 ASA 的认证、授权和审计 (AAA)。外部 AAA 服务器会实施配置的权限和属性。将 ASA 配置为使用外部服务器之前，必须使用正确的 ASA 授权属性来配置外部 AAA 服务器，并从其中一部分属性向个人用户分配特定权限。

### 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。您可以将 ASA 配置为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：

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 ASA 本地 AAA 数据库中为单个用户（ASDM 中的用户账户）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（在 CLI 中称为隧道组）分配的组策略 - 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、服务器返回的用户属性或分配给用户的组策略中缺失的所有属性。

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。

# 外部 AAA 服务器使用规定

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。

# 配置多证书身份验证

现在，您可以使用 AnyConnect SSL 和 IKEv2 客户端协议验证每个会话的多重证书。我们对汇聚身份验证协议进行了扩展，以便定义用于多证书身份验证的协议交换并将此功能用于两种会话类型。例如，您可以确保计算机证书的颁发机构名称匹配特定的 CA，从而确保设备是公司分发的设备。

使用多证书选项，可以同时通过证书对计算机和用户进行证书身份验证。如果没有此选项，则只能对其中之一执行证书身份验证，但不能二者兼顾。

通过预填充用户名字段，可以解析证书中的字段并将其用于 AAA 和证书身份验证连接中的后续 AAA 身份验证。始终从自客户端收到的第一个证书检索主要和辅助用户名预填充。

使用多证书身份验证时，要对两个证书进行身份验证：从客户端收到的第一个证书才是从中解析 pre-fill 和 username-from-certificate 主要和辅助用户名的证书。于是，您可以为客户端配置相关规则，用于选择先发送的证书与后发送的证书。

通过多证书身份验证，可以根据用于对该连接尝试进行身份验证的证书字段来制定策略决策。在多证书身份验证期间从客户端收到的用户和计算机证书被加载到 DAP，因此可以根据证书字段配置策略。要使用动态访问策略 (DAP) 添加多证书身份验证，以设置允许或禁止连接尝试的规则，请参阅中向 *DAP* 添加多证书身份验证一节相应版本的《ASA VPN ASDM 配置指南》。

# Active Directory/LDAP VPN 远程访问授权示例

本节提供在 ASA 上使用 Microsoft Active Directory 服务器配置身份验证和授权的示例程序。包括以下主题：



Cisco.com 提供的其他配置示例包括以下技术说明。

- ASA/PIX：通过 LDAP 配置将 VPN 客户端映射至 VPN 组策略的示例
- PIX/ASA 8.0：登录时使用 LDAP 身份验证来分配组策略

## 基于用户的属性的策略实施

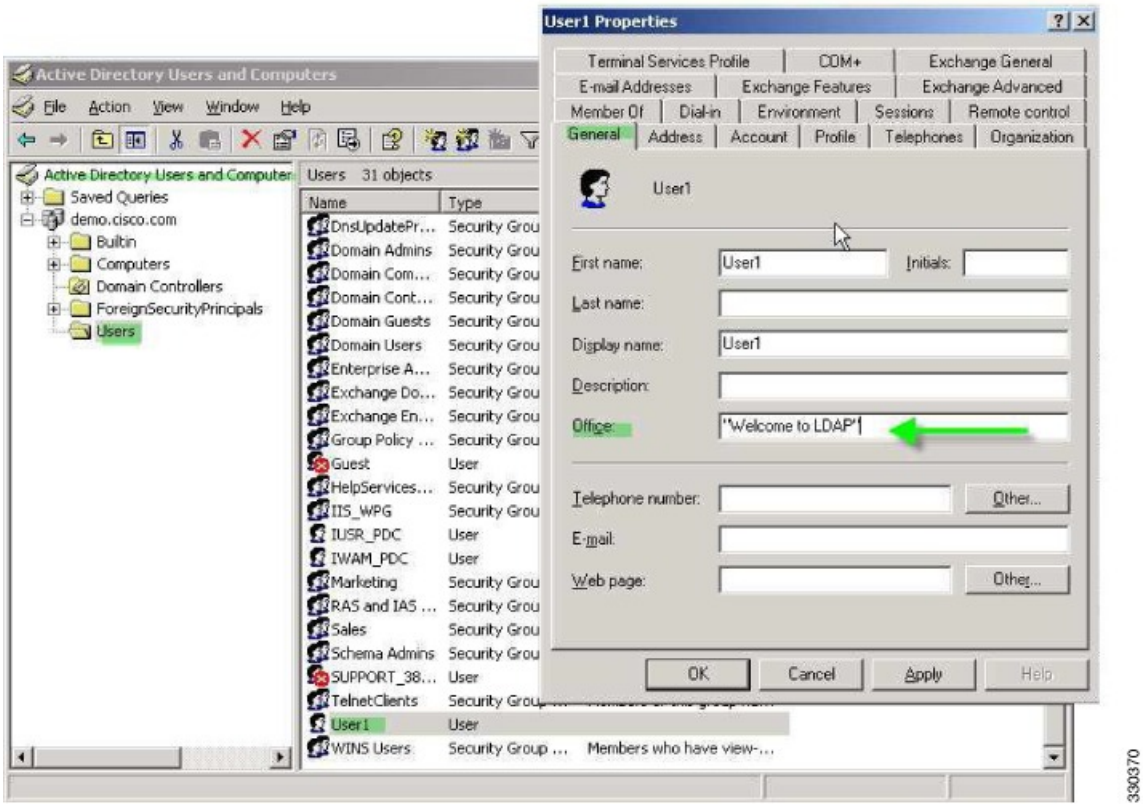
此示例向用户显示一个简单的欢迎信息，说明如何将任意标准 LDAP 属性映射至一个已知的供应商特定属性 (VSA)，或者将一个或多个 LDAP 属性映射至一个或多个思科 LDAP 属性。此示例适用于任意连接类型，包括 IPSec VPN 客户端、AnyConnect SSL VPN 客户端或无客户端 SSL VPN。

如要为 AD LDAP 服务器上配置的用户实施简单的欢迎信息，请使用 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 映射至思科属性 Banner1 的属性映射。

在身份验证过程中，ASA 从服务器检索 physicalDeliveryOfficeName 的值，将该值映射至思科属性 Banner1，然后向用户显示该横幅。

### 过程

**步骤 1** 右键点击用户名打开 Properties 对话框，然后点击 **General** 选项卡，在 Office 字段中输入欢迎信息文本，该字段使用 AD/LDAP 属性 physicalDeliveryOfficeName。




**步骤 2** 在 ASA 上创建一个 LDAP 属性映射。

创建映射 Banner，并将 AD/LDAP 属性 physicalDeliveryOfficeName 映射至思科属性 Banner1：

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

**步骤 3** 将 LDAP 属性映射关联到 AAA 服务器。

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，然后关联您先前创建的属性映射 Banner：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

**步骤 4** 测试此欢迎信息的实施。

# 将 LDAP 用户置于特定组策略中

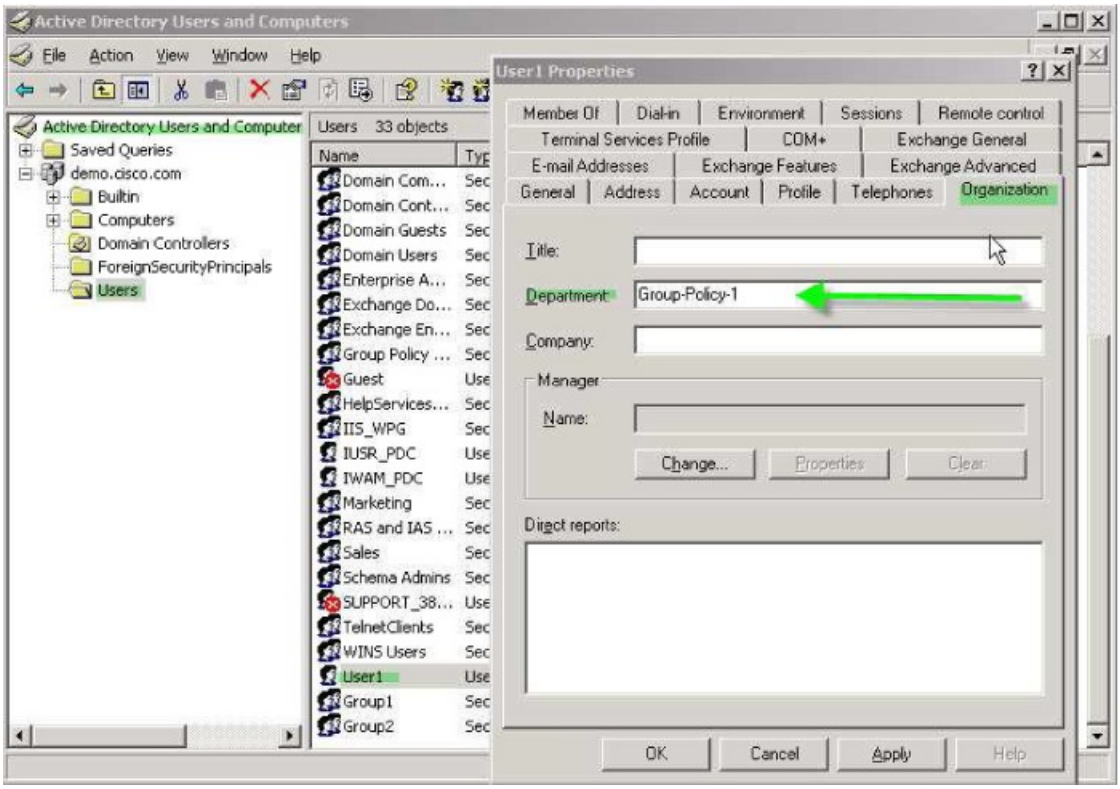
此示例适用于任意连接类型，包括 IPSec VPN 客户端、AnyConnect SSL VPN 客户端或无客户端 SSL VPN。在此示例中，User1 通过无客户端 SSL VPN 连接进行连接。

如要将 LDAP 用户置于特定组策略中，请使用 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 映射至思科属性 IETF-Radius-Class。

在身份验证过程中，ASA 从服务器检索 Department 的值，将此值映射至 IETF-Radius-Class，然后将 User1 置于该组策略中。

过程

**步骤 1** 右键点击用户名打开 Properties 对话框，然后点击 **Organization** 选项卡，在 Department 字段中输入 **Group-Policy-1**。




**步骤 2** 为 LDAP 配置定义一个属性映射。

将 AD 属性 Department 映射至思科属性 IETF-Radius-Class。

```
hostname(config)# ldap attribute-map group_policy
hostname(config-ldap-attribute-map)# map-name Department IETF-Radius-Class
```

**步骤 3** 将 LDAP 属性映射关联到 AAA 服务器。

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，然后关联您先前创建的属性映射 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 4** 按照服务器上 Department 字段中输入的值，在 ASA 上添加组策略 *Group-policy-1*，并配置将分配给用户的所需策略属性。

```
hostname(config)# group-policy Group-policy-1 external server-group LDAP_demo
hostname(config-aaa-server-group)#
```

**步骤 5** 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 6** 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

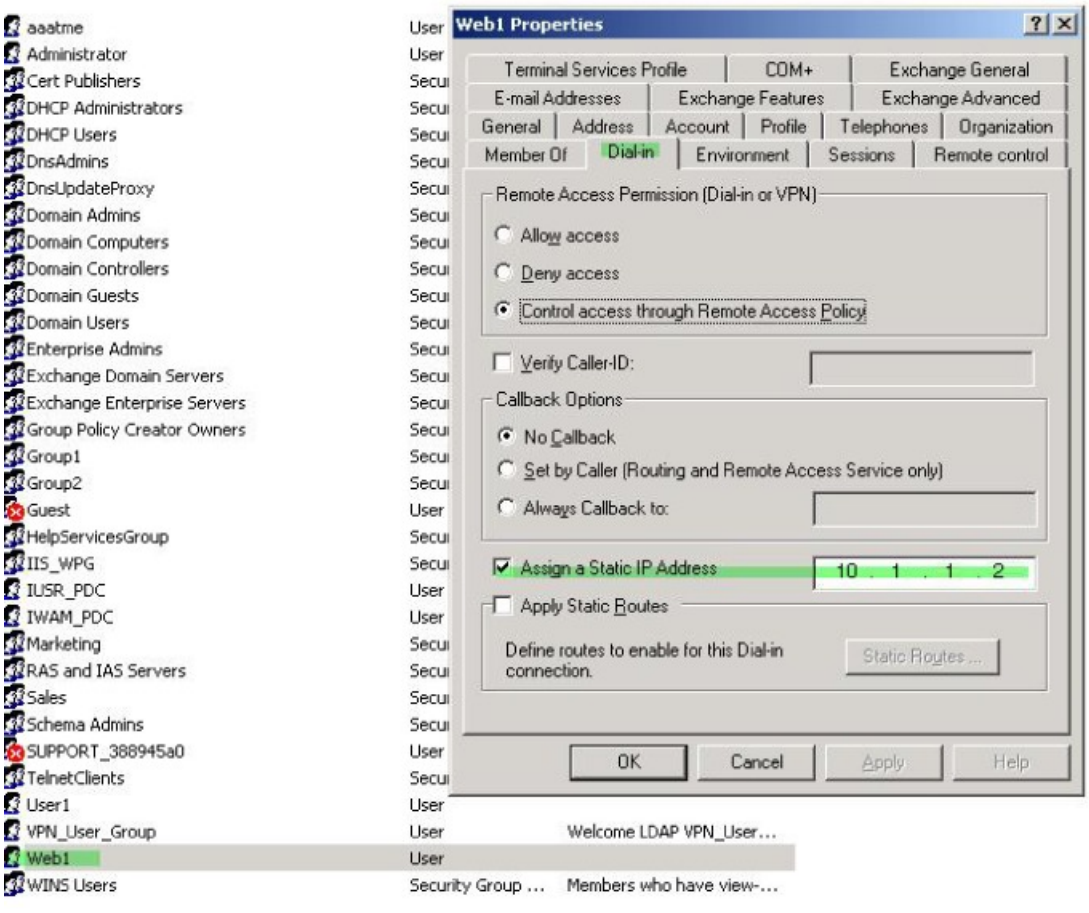
此示例适用于完全隧道客户端，例如 IPsec 客户端和 SSL VPN 客户端。

如要实施静态 AnyConnect 静态 IP 分配，请将 AnyConnect 客户端用户 Web1 配置为接受静态 IP 地址，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），然后创建一个可将该属性映射至思科属性 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 msRADIUSFramedIPAddress 的值，将该值映射至思科属性 IETF-Radius-Framed-IP-Address，并向 User1 提供静态地址。

### 过程

**步骤 1** 右键点击用户名打开 Properties 对话框，然后点击 **Dial-in** 选项卡，选中 **Assign Static IP Address** 复选框并输入 IP 地址 10.1.1.2。




**步骤 2** 为显示的 LDAP 配置创建一个属性映射。

将 Static Address 字段使用的 AD 属性 msRADIUSFramedIPAddress 映射至思科属性 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 3** 将 LDAP 属性映射关联到 AAA 服务器。

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，然后关联您先前创建的属性映射 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 4** 通过查看此部分的配置，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    << Make sure this is configured >>
```

```
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

**步骤 5** 使用 AnyConnect 客户端建立与 ASA 的连接。观察用户是否收到在服务器上配置并映射至 ASA 的 IP 地址。

**步骤 6** 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

本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 选项卡中的允许访问和拒绝访问设置映射至思科属性 Tunneling-Protocol，该属性支持以下映射值：

| 值 | 隧道协议 |
|---|---|
| 1 | PPTP |
| 2 | L2TP |
| 4 | IPsec (IKEv1) |
| 8 | L2TP/IPsec |
| 16 | 无客户端 SSL |
| 32 | SSL 客户端 - AnyConnect 或 SSL VPN 客户端 |
| 64 | IPsec (IKEv2) |

[1] (1) 不能同时支持 IPsec 和 L2TP over IPsec。因此，值 4 和 8 只能二选其一。
[2] (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。

有关实施拨入允许访问或拒绝访问的其他示例，请参阅以下技术说明：ASA/PIX：通过 LDAP 配置将 VPN 客户端映射至 VPN 组策略的示例。

过程

**步骤 1** 右键点击用户名打开“属性”对话框，然后点击**拨入**选项卡，再点击“允许访问”单选按钮。


**注释** 如果您通过“远程访问策略”选项选择控制访问，则服务器不会返回值，而实施的权限则根据 ASA 的内部组策略设置而定。

**步骤 2** 创建一个允许 IPsec 和 AnyConnect 连接，但是拒绝无客户端 SSL 连接的属性映射。

a) 创建映射 tunneling_protocols：

```
hostname(config)# ldap attribute-map tunneling_protocols
```

b) 将 Allow Access 设置使用的 AD 属性 msNPAllowDialin 映射至思科属性 Tunneling-Protocols：

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) 添加映射值：

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

**步骤 3** 将 LDAP 属性映射关联到 AAA 服务器。

a) 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：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) 关联您创建的属性映射 tunneling_protocols：

```
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

**步骤 4** 验证属性映射是否按配置工作。

尝试使用无客户端 SSL 的连接，用户应接到通知，告知其未经授权的连接机制是连接失败的原因。IPSec 客户端应该可以连接，因为根据属性映射，IPsec 是允许的隧道协议。

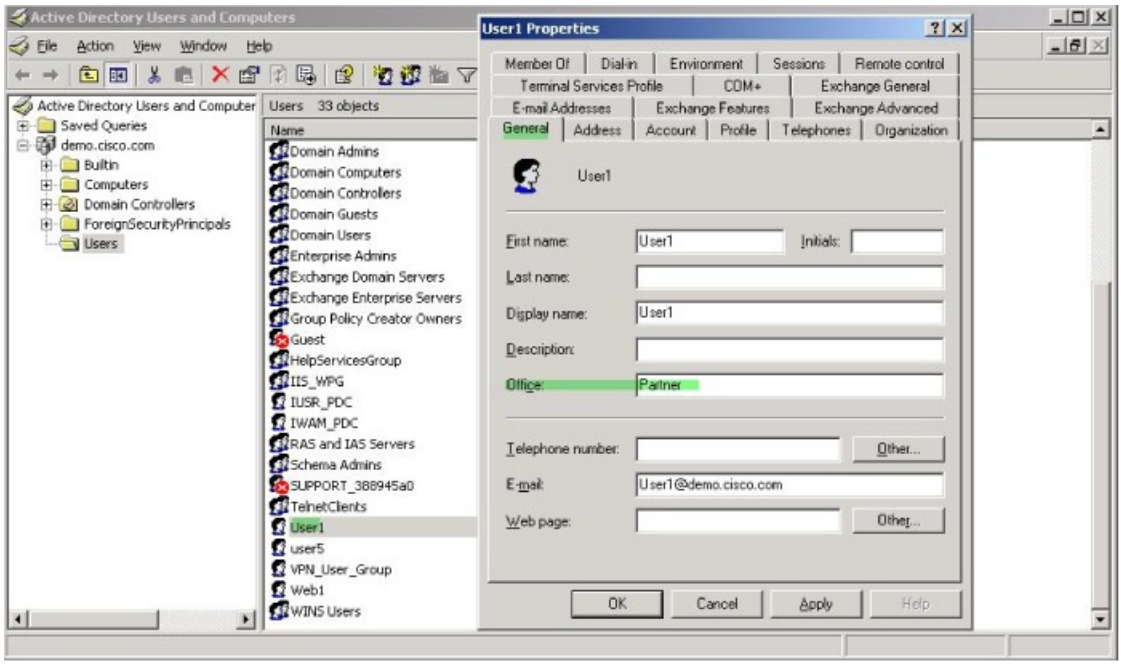
# 实施登录时长和时间规则

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）访问网络的时长。

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 上创建一个可将该属性映射至思科属性 Access-Hours 的属性映射。During authentication, the ASA retrieves the value of physicalDeliveryOfficeName and maps it to Access-Hours.

## 过程

**步骤 1** 选择用户，右键点击 **Properties**，然后打开 **General** 选项卡：




**步骤 2** 创建属性映射。

创建属性映射 access_hours，并将 Office 字段使用的 AD 属性 physicalDeliveryOfficeName 映射至思科属性 Access-Hours。

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

**步骤 3** 将 LDAP 属性映射关联到 AAA 服务器。

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 4** 为服务器上允许的每个值配置时间范围。

将合作伙伴访问时长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
```

第 II 部分

# 无客户端 SSL VPN

第 13 章

# 无客户端 SSL VPN 概述



## 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 Web 浏览器随时随地安全地访问企业网络上的资源。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。

**注释** 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 Web 浏览器与 ASA 创建安全的远程访问 VPN 隧道，不需要使用软件或硬件客户端。几乎任何可通过 HTTP 连接到互联网的设备都可以通过它安全便捷地访问各种 Web 资源以及支持 Web 的应用和旧版应用。具体包括：

- 内部网站。
- 支持 Web 的应用
- NT/Active Directory 文件共享。
- Microsoft Outlook Web Access Exchange Server 2000、2003、2007 和 2013。
- 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继任者传输层安全性协议(SSL/TLS1)，在远程用户与您配置为内部服务器的受支持的特定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。

网络管理员以组为单位为无客户端 SSL VPN 的用户提供资源访问。用户无权直接访问内部网络上的资源。

# 无客户端 SSL VPN 的必备条件

有关 ASA 上无客户端 SSL VPN 支持的平台和浏览器的信息，请参阅支持的 VPN 平台，Cisco ASA 5500 系列。

# 无客户端 SSL VPN 的规定和限制

- ActiveX 页面要求启用 ActiveX 中继或对关联的组策略输入 **activex-relay**。如果执行此操作或将智能隧道列表分配给策略，并且终端上的浏览器代理例外列表指定了代理，则用户必须向该列表添加“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 密钥链。
- 即使您安装了无客户端连接的受信任证书，客户端也可能会收到不受信任证书警告。
- ASA 不支持无客户端 SSL VPN 连接的 DSA 证书。支持 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 的某些组件需要 Java 运行时环境 (JRE)。在 Mac OS X v10.7 及更高版本中，默认情况下未安装 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。
- 启动无客户端 VPN 会话时，系统会生成 RADIUS 记账开始消息。由于地址未分配给无客户端 VPN 会话，因此开始消息不会包含成帧 IP 地址。如果随后从无客户端门户页面启动第 3 层 VPN 连接，系统将分配地址并通过临时更新记账消息向 RADIUS 服务器报告。使用 Weblaunch 功能建立第 3 层 VPN 隧道时，RADIUS 的行为应与此类似。在此情况下，对用户进行身份验证之后、建立第 3 层隧道之前，系统会发送不包含成帧 IP 地址的记账开始消息。继此开始消息之后，系统将在第 3 层隧道建立后发送临时更新消息。

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，您可能需要创建一个名称为“0-Select-a-group”的虚拟组策略。

提示 您可以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。

# 无客户端的SSL VPN 的许可

要使用 AnyConnect 安全移动客户端，需要购买 AnyConnect Plus 或 Apex 许可证。具体需要哪类许可证，应根据您计划使用的 AnyConnect VPN 客户端和安全移动功能以及要支持的会话数量而定。这些基于用户的许可证包含支持和软件更新访问权限，以便用户能够紧跟 BYOD 总体趋势。

AnyConnect 4.4 许可证用于 ASA（还有 ISR、CSR 和 ASR），以及身份服务引擎 (ISE)、云网络安全 (CWS) 和网络安全设备 (WSA) 等其他非 VPN 头端。各类头端均使用一致的模型，因此即使发生头端迁移，也不会造成任何影响。

有关 AnyConnect 许可模式的完整说明，请参阅 http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf。

第 14 章

# 无客户端 SSL VPN 基本配置



## 重写每个 URL

默认情况下，ASA 允许所有门户流量流向所有 Web 资源（例如 HTTPS、CIFS、RDP 和插件）。无客户端 SSL VPN 将每个 URL 重写为只对 ASA 有意义的 URL。用户无法使用此 URL 确认其已连接至所请求的网站。为了避免让用户处于钓鱼网站所带来的风险中，请将 Web ACL 分配给为无客户端访问配置的策略（例如组策略和/或动态访问策略），以便控制源自门户的流量。我们建议关闭这些策略上的 URL Entry，以防用户无法分辨哪些 URL 才是可访问的。

图 *6:* 用户输入的 ***URL*** 示例


图 *7:* 安全设备重写以及浏览器窗口中显示的相同 ***URL***

过程

**步骤 1** 为需要进行无客户端SSL VPN访问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，依次选择 **General** > **More Options** > **Web ACL**，并点击 **Manage**。

**步骤 3** 创建 Web 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 Web 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 Web ACL 分配给 DAP，请编辑 DAP 记录，并在 **Network ACL Filters** 选项卡中选择 Web ACL。

**步骤 5** 关闭门户页面上的“URL 条目”，该页面在建立基于浏览器的连接后打开。点击组策略门户页面的 DAP **Functions** 选项卡上 URL Entry 旁边的 **Disable**。要关闭 DAP 中的 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** 指示用户在门户页面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 接口。
- 为无客户端 SSL VPN 连接选择端口。
- 设置并发无客户端 SSL VPN 会话的最大数量。

过程

**步骤 1** 要为无客户端访问配置或创建组策略，请依次选择**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **组策略**窗格。

**步骤 2** 依次导航至**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **连接配置文件**。

a) 为每个 ASA 接口启用或关闭 **Allow Access**。

Interface 列将列出配置的接口。WebVPN Enabled 字段显示该接口上的无客户端 SSL VPN 的状态。Yes 旁边的绿色复选标记表示无客户端 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** 依次导航至**配置** > **远程访问 VPN** > **高级** > **最大 VPN 会话数**，然后在“最大其他 VPN 会话数”字段中输入允许的无客户端 SSL VPN 会话的最大数。

# 受信任证书池

ASA 将受信任证书分组到信任池中。信任池可视为代表多个已知 CA 证书的信任点的特例。ASA 包括一个默认的证书捆绑包，与 Web 浏览器随附的证书捆绑包相似。只有管理员后才会激活这些证书。

在使用 HTTPS 协议通过 Web 浏览器连接至远程服务器时，该服务器会提供证书颁发机构 (CA) 签名的数字证书进行自我标识。Web 浏览器包括用于验证服务器证书有效性的 CA 证书集合。

在通过无客户端 SSL VPN 连接至支持 SSL 的远程服务器时，知道您可以信任该远程服务器且连接到正确的远程服务器非常重要。ASA 9.0 引入了以下支持功能：根据无客户端 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**配置** > **远程访问 VPN** > **证书管理** > **受信任证书池**中，可以启用 https 站点 SSL 连接的证书验证。您还可以管理受信任证书池中的证书。

**注释** ASA 信任池与思科 IOS 信任池类似，但不完全相同。

# 启用 HTTP 服务器验证

**过程**

**步骤 1** 在 ASDM 中，依次选择**配置 > 远程访问 VPN > 证书管理 > 受信任证书池**。

**步骤 2** 选中 **Enable SSL Certificate Check** 复选框。

**步骤 3** 如果无法验证服务器，请点击**从 HTTPS 站点断开用户连接**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

您可以从多个位置导入以下任一格式的单独证书或证书捆绑包：

- pkcs7 结构中封装的 DER 格式的 x509 证书。
- PEM 格式的串联 x509 证书文件（包括 PEM 报头）。

过程

步骤 1 在 ASDM 中，依次选择**配置 > 远程访问 VPN > 证书管理 > 受信任证书池**。

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**，然后选择该捆绑包。
- 如果捆绑包存储在 ASA 闪存文件系统中，请依次点击**从闪存导入**和**浏览闪存**，然后选择该文件。
- 如果捆绑包托管在服务器上，请点击**从 URL 导入**，从列表中选择协议，然后在字段中输入 URL。
- 继续导入捆绑包。如果签名验证失败或无法导入捆绑包，请稍后修复个别证书错误。如果取消选中该选项，则任何证书导入失败将导致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。

注释 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

正确配置完 trustpool 后，应导出该证书池。这样，您就可以恢复截至此时为止的 trustpool，例如用来删除在导出后添加至 trustpool 的证书。可将该证书池导出到 ASA 闪存文件系统或本地文件系统。

在 ASDM 中，依次选择 Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool，然后点击 Export Pool。

过程

步骤 1 点击**导出到文件**。

步骤 2 点击 **Browse Local Files**。

步骤 3 选择要保存 trustpool 的目标文件夹。

步骤 4 在 File Name 框中，为 trustpool 输入易于记忆的唯一名称。

步骤 5 点击 **Select**。

步骤 6 点击 **Export Pool** 保存文件。或者，点击 **Cancel** 停止保存。

# 删除证书

要删除所有证书，请在 ASDM 中依次选择**配置 > 远程访问 VPN > 证书管理 > 受信任证书池**，然后点击**清除池**。

**注释** 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，请在 ASDM 中依次选择**配置 > 远程访问 VPN > 证书管理 > 受信任证书池**，然后依次点击**恢复默认受信任 CA 列表**和**导入捆绑包**。

# 编辑受信任证书池策略

**过程**

**步骤 1** 吊销检查 - 配置是否对池中证书进行吊销检查，然后选择是使用 CLR 还是 OCSP 以及在吊销检查失败时是否使证书失效。

**步骤 2** 证书匹配规则 - 选择证书映射以豁免吊销或到期检查。证书映射将证书链接到 AnyConnect 或无客户端 SSL 连接配置文件（也称为隧道组）。

有关证书映射的详细信息，请参阅证书到连接配置文件的映射规则，第 120 页。

**步骤 3** CRL 选项 - 确定 CRL 缓存的刷新频率，取值范围介于 1 至 1440 分钟（1140 分钟等于 24 小时）。

**步骤 4** 自动导入 - 思科会定期更新受信任 CA 的“默认”列表。如果您选中“启用自动导入”并保留默认设置，ASA 将每 24 小时检查一次思科站点上受信任 CA 的更新后列表。如果列表已更改，ASA 将下载并导入新的默认受信任 CA 列表。

# 更新 Trustpool

如果存在以下任意一种情况，则应更新 trustpool：

- trustpool 中的任何证书即将到期或已重新颁发。
- 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。

# 删除证书捆绑包

清除 trustpool 将删除不属于默认捆绑包的所有证书。

无法删除默认捆绑包。要清除信任池，请在 ASDM 中依次选择**配置 > 远程访问 VPN > 证书管理 > 受信任证书池**，然后点击**清除池**。

# 编辑受信任证书池策略

**过程**

**步骤 1** 吊销检查 - 配置是否对池中证书进行吊销检查，然后选择是使用 CLR 还是 OCSP 以及在吊销检查失败时是否使证书失效。

**步骤 2** 证书匹配规则 - 选择证书映射以豁免吊销或到期检查。证书映射将证书链接到 AnyConnect 或无客户端 SSL 连接配置文件（也称为隧道组）。

有关证书映射的详细信息，请参阅证书到连接配置文件的映射规则，第 120 页。

**步骤 3** CRL 选项 - 确定 CRL 缓存的刷新频率，取值范围介于 1 至 1440 分钟（1140 分钟等于 24 小时）。

**步骤 4** 自动导入 - 思科会定期更新受信任 CA 的“默认”列表。如果您选中“启用自动导入”并保留默认设置，ASA 将每 24 小时检查一次思科站点上受信任 CA 的更新后列表。如果列表已更改，ASA 将下载并导入新的默认受信任 CA 列表。

# Java 代码签名人

代码签名将数字签名附加到可执行代码本身。此数字签名提供足够信息，用于对签名人进行身份验证，并确保代码未在签名后进行修改。

代码签名人证书是特殊证书，与其关联的私钥用于创建数字签名。代码签名证书从 CA 获取，已签名代码本身可揭示证书来源。

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 代码签名人，请依次选择 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 证书和密钥内容。

要导入信任点，请依次选择**配置 > 属性 > 证书 > 信任点 > 导入**。

# 配置浏览器对插件的访问

浏览器插件是 Web 浏览器在执行专用功能时（例如，在浏览器窗口中将客户端连接至服务器）调用的一个独立程序。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，思科将测试再分发的插件，在某些情况下，还将测试其无法再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。

安装闪存设备中的插件时，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。
- 为所有未来的无客户端 SSL VPN 会话启用插件，然后添加主菜单选项并将一个选项添加至门户页面 Address 字段旁边的下拉列表。

下面显示了在添加以下各节中介绍的插件时门户页面的主菜单和 Address 字段发生的变化。

**表 *5:* 插件在无客户端 *SSL VPN* 门户页面上的效果**

| 插件 | 添加到门户页面的主菜单选项 | 添加到门户页面的 **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:// |

***** 不是推荐的插件。

当无客户端 SSL VPN 会话中的用户在门户页面上点击关联的菜单选项时，门户页面会在界面上显示一个窗口，并显示一个帮助窗格。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)。

## 插件的必备条件

- 只有在 ASA 上启用无客户端 SSL VPN，才能远程访问插件。

- 要为插件配置 SSO 支持，请安装插件，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访客特权模式。
- 插件要求使用 ActiveX 或 Oracle Java 运行时环境 (JRE)。有关版本要求，请参阅支持的 VPN 平台，Cisco ASA 5500 系列兼容性表。

# 插件的限制

注释 远程桌面协议插件不支持用会话代理程序进行负载均衡。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，插件将正常工作。

- 插件支持单点登录 (SSO)。它们使用所输入的相同凭证打开无客户端 SSL VPN 会话。因为插件不支持宏替换，您无法选择对不同的字段（例如内部域密码）或 RADIUS 或 LDAP 服务器上的属性执行 SSO。
- 状态故障切换不保留使用插件建立的会话。完成故障切换之后，用户必须重新连接。
- 如果使用无状态故障切换替代状态故障切换，则无客户端功能（例如书签、自定义和动态访问策略）不会在故障切换 ASA 对之间同步。在发生故障切换时，这些功能无法工作。

# 为插件准备安全设备

### 开始之前

确保已在 ASA 接口上启用无客户端 SSL VPN。

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 文件中的条目来解析 FQDN。

### 过程

**步骤 1** 显示无客户端 SSL VPN 是否已在 ASA 上启用。

**show running-config**

**步骤 2** 在 ASA 接口上安装 SSL 证书，并提供用于远程用户连接的完全限定域名 (FQDN)。

# 安装思科再分发的插件

思科再分发以下基于 Java 的开放源码组件，可作为无客户端 SSL VPN 会话中 Web 浏览器的插件进行访问。

## 开始之前

确保已在 ASA 的一个接口上启用无客户端 SSL VPN。为此，请输入 **show running-config** 命令。

**表 *6:* 思科再分发的插件**

| 协议 | 说明 | 再分发的插件的来源* |
|---|---|---|
| RDP | 访问 Windows Vista 和 Windows 2003 R2 托管的 Microsoft 终端服务。<br>支持远程桌面 ActiveX 控件。<br>我们建议使用此款支持 RDP 和 RDP2 的插件。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。<br>支持远程桌面 ActiveX 控件。<br>此旧版插件仅支持 RDP2。建议不要使用此插件；请换用上述 RDP 插件。 | |
| 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。<br>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。

过程

**步骤 1** 在用于建立 ASA 与 ASDM 之间的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** 依次选择**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 门户 > 客户端-服务器插件**。

此窗格显示当前加载的可用于无客户端 SSL 会话的插件。还提供这些插件的散列值和日期。

**步骤 3** 点击 **Import**。

**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** 使插件可以访问 Citrix MetaFrame 或 Web Interface 服务。
  - **rdp** 使插件可以访问 Remote Desktop Protocol 服务。
  - **ssh,telnet** 使插件可以访问安全外壳和 Telnet 服务。
  - **vnc** 使插件可以访问虚拟网络计算服务。

    注释　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，从关联的 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**。

插件现可用于未来的无客户端 SSL VPN 会话。

# 提供对 Citrix XenApp 服务器的访问

本节介绍如何为 Citrix XenApp 服务器客户端添加无客户端 SSL VPN 支持，可作为为无客户端 SSL VPN 浏览器提供对第三方插件的访问的方法示例。

借助于 ASA 上安装的 Citrix 插件，无客户端 SSL VPN 用户可以使用与 ASA 的连接访问 Citrix XenApp 服务。

状态故障切换不保留使用 Citrix 插件建立的会话。Citrix 用户必须在故障切换后重新进行身份验证。

# 创建和安装 Citrix 插件

### 开始之前

您必须为插件准备安全应用。

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。

### 过程

**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，然后点击 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 Web 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 模式下输入以下 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。

**注释** 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。

根据需要使用《Java 客户端管理员指南》。

# 配置端口转发

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 的应用可能也可以正常工作，但我们没有对其进行过测试。使用 UDP 的协议将无法工作。

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。由于您已构建支持此技术的早期配置，可以选择使用端口转发。

考虑端口转发的以下替代方案：

- 智能隧道访问为用户提供以下优势：
  - 智能隧道所提供的性能优于插件性能。
  - 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访问不同，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，需要指定应用使用的端口。在配置智能隧道访问时，需要指定可执行文件的名称或其路径。

## 端口转发的必备条件

- 确保 Oracle Java 运行时环境 (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。
- 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 一次在末尾加斜杠，一次不加。例如，

- https://example.com/
- https://example.com

有关详细信息，请转至 Safari, Mac OS X 10.5.3：客户端证书身份验证的变更。

- Microsoft Windows Vista 或更高版本的用户若使用端口转发或智能隧道，必须将 ASA 的 URL 添加到“受信任站点”区域。要访问 Trusted Site 区域，必须启动 Internet Explorer 并依次选择 **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访问；但是，由于此方法会使计算机更容易遭受攻击，我们建议不要使用此方法。

# 端口转发的限制

- 端口转发仅支持使用静态 TCP 端口的 TCP 应用。不支持使用动态端口或多个 TCP 端口的应用。例如，使用端口 22 的 SecureFTP 通过无客户端 SSL VPN 端口转发工作，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。
- 状态故障切换不保留使用 Application Access（端口转发或智能隧道访问）建立的会话。用户在故障切换后必须重新连接。
- 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 小应用程序和配置本地客户端，并且此操作需要本地系统的管理员权限，当用户从公共远程系统进行连接时，可能无法使用应用。

  Java 小应用程序显示在最终用户 HTML 界面上其自身窗口中。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，端口转发小应用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 将为本地代理 ID 创建新的 IP 地址 127.0.0.2、127.0.0.3 等。由于可以修改主机文件并使用不同的环回，远程端口将用作小应用程序中的本地端口。要进行连接，可配合使用 Telnet 与主机名，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，端口转发小应用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应用程序建立连接。端口转发小应用程序只对 ASA 执行 DNS 查询。它会更新主机文件，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。

过程

**步骤 1** 依次点击 **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**编辑**。否则，请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**编辑**。

**步骤 3** 浏览至 DNS 区域并从下拉列表中选择 DNS 服务器。如果 ASDM 显示要使用的 DNS 服务器，请记住域名，忽略其余步骤，然后转至下一节。在配置端口转发列表中条目的过程中，指定远程服务器时需要输入该域名。如果配置中没有该 DNS 服务器，请继续执行其余步骤。

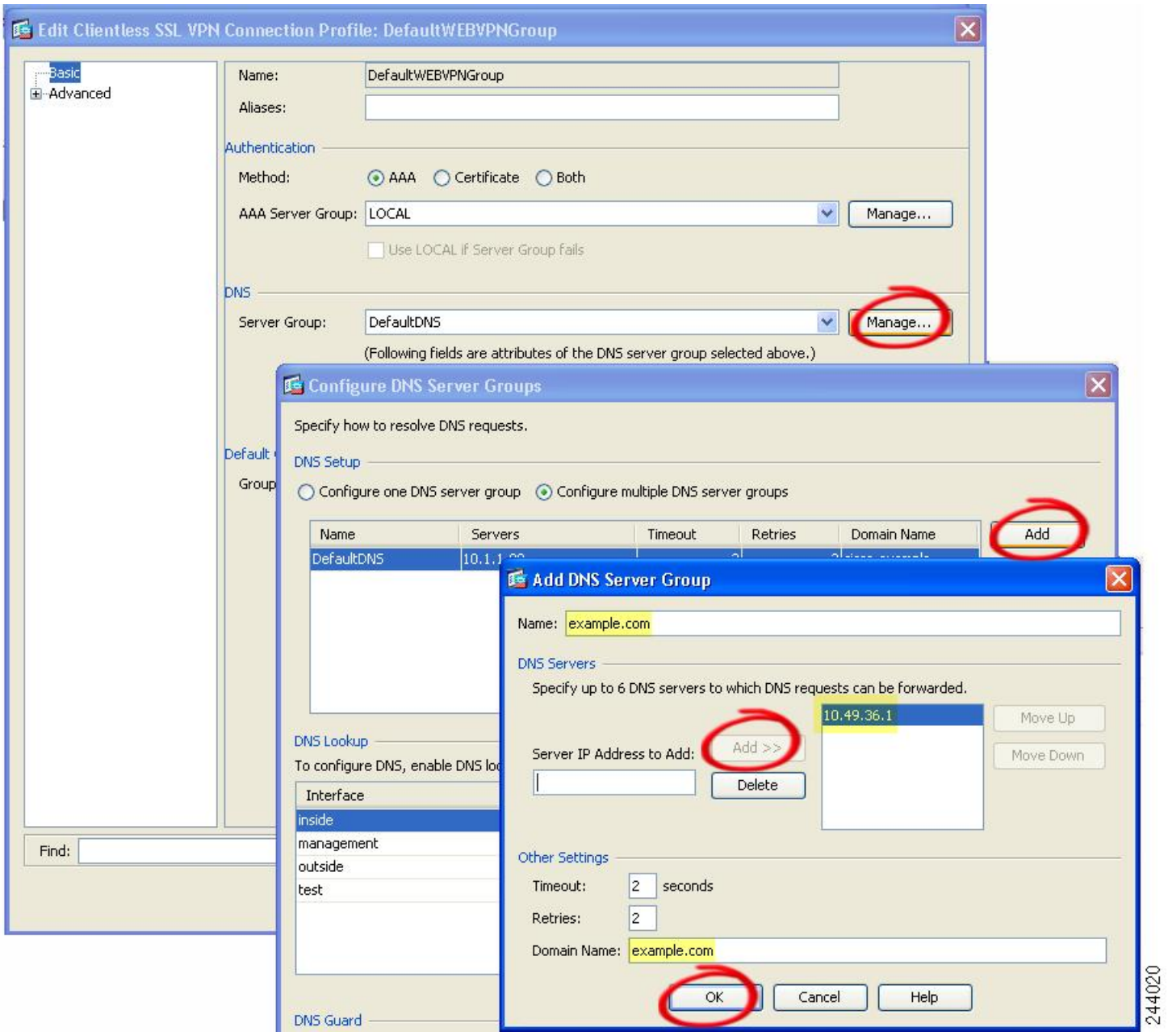
**步骤 4** 点击 DNS 区域中的 **Manage**。

**步骤 5** 点击 **Configure Multiple DNS Server Groups**。

**步骤 6** 点击**添加**。

**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。

图 *8:* 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过程中，指定远程服务器时需要此域名。

**步骤 8** 点击**OK**，直至“连接配置文件”窗口再次激活。

**步骤 9** 对于无客户端连接的配置中使用的其余每个连接配置文件，请重复这些步骤 。

**步骤 10** 点击**Apply**。

# 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：

### 开始之前

分配给 Remote Server 参数的 DNS 名称必须与 Domain Name 和 Server Group 参数匹配，才能建立隧道并解析为 IP 地址。Domain 和 Server Group 参数的默认设置为 DefaultDNS。

### 过程

**步骤 1** 点击 **Add**。

**步骤 2** 键入供应用使用的TCP端口号。一个列表名称只能使用一次本地端口号。为避免与本地TCP服务冲突，请使用 1024 到 65535 范围内的端口号。

**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。最多可包含 64 个字符。

**步骤 6** （可选） 突出显示端口转发列表，然后点击**分配**，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 连接访问的用户或组策略关联的已命名 TCP 应用列表。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：

**注释** 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。

- 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 门户页面上的**应用访问 > 启动应用**将其手动启动。

### 过程

**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。一个列表名称只能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。

注释　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 门户页面上的**应用访问 > 启动应用**将其手动启动。

# 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 门户页面。通过使用 CIFS 或 FTP，无客户端 SSL VPN 向用户提供对网络文件的网络访问，在某种程度上，用户需满足用户身份验证要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 所提供的门户页面提供直接访问文件系统的界面。

当用户请求文件列表时，无客户端 SSL VPN 将在被指定为主浏览器的服务器中查询包含该列表的服务器的 IP 地址。ASA 获取列表并在门户页面上将其提供给远程用户。

借助于无客户端 SSL VPN，用户可根据用户身份验证要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。

当远程用户在门户页面的菜单中或在无客户端 SSL VPN 会话期间显示的工具栏上点击**浏览网络**时，ASA 使用主浏览器、WINS 服务器或 DNS 服务器（通常与 ASA 处于同一网络或可从该网络进行访问）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，而无客户端 SSL VPN 则向远程用户提供该列表。

注释　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 `\\server\share\subfolder\personal` 文件夹，用户至少必须具有所有父文件夹（包括共享本身）的读取权限。

使用 Download 或 Upload，在 CIFS 目录和本地桌面之间复制和粘贴文件。Copy 和 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。

如果您将文件从 Web 文件夹拖放到工作站上的文件夹，则该文件可能会显示为临时文件。刷新工作站上的此文件夹，以更新视图并显示传输的文件。

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

**注释** 此程序说明如何指定主浏览器和 WINS 服务器。或者，可使用 ASDM 配置 URL 列表和条目提供对文件共享的访问。

在 ASDM 中添加共享不需要主浏览器或 WINS 服务器。但是，它不支持浏览网络链接。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。

# 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 与终端上的 Microsoft Word 等应用交互。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一节。

# 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，通过无客户端门户上的书签也可以访问 VDI 服务器。

# VDI 的限制

- 由于这些形式的身份验证不允许中间的 ASA，不支持在自动登录时使用证书或智能卡进行身份验证。
- 必须在 XenApp 和 XenDesktop 服务器上安装和配置 XML 服务。
- 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。登录凭证可能包括：
  - 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 支持包括用于无效条目的下一个令牌，也包括用于为初始或过期 PIN 输入新 PIN 的下一个令牌。

## Citrix 支持的移动设备

- iPad - Citrix Receiver 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 手机 - Citrix Receiver 版本 2.x 或更高版本
- Android 4.0 手机 - Citrix Receiver 版本 2.x 或更高版本

## Citrix 的限制

### 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。
- 不支持客户端证书验证和 CSD
- 由于安全问题，证书中的 MD5 签名无效，此问题已在 iOS 中出现，详情请访问以下网址：http://support.citrix.com/article/CTX132798
- 如 Citrix 网站所述，只有 Windows 支持 SHA2 签名，详情请访问以下网址：http://www.citrix.com/
- 不支持超过 1024 个字节的密钥

### 其他限制

- 不支持 HTTP 重定向；Citrix Receiver 应用不适用于重定向。
- 必须在 XenApp 和 XenDesktop 服务器上安装和配置 XML 服务。

## 关于 Citrix Mobile Receiver 用户登录

连接到 Citrix 服务器的移动用户的登录方式取决于 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. 使用 AnyConnect 安全移动客户端，通过 VPN 凭证连接至 ASA。
2. 使用 Citrix Mobile Receiver，通过 Citrix 服务器凭证连接至 Citrix 服务器（如已配置单点登录，则不需要 Citrix 凭证）。

当 ASA 配置为 VDI 代理服务器时：

1. 使用 Citrix Mobile Receiver 连接至 ASA，同时输入 VPN 和 Citrix 服务器的凭证。在第一次连接后，如果配置正确，后续连接只需要 VPN 凭证。

# 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，使 ASA 的连接对于用户而言看起来与 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。以下概要步骤显示最终用户如何连接至 Citrix。

### 过程

**步骤 1** 移动用户打开 Citrix Receiver 并连接至 ASA 的 URL。

**步骤 2** 用户为 XenApp 服务器提供凭证和 Citrix 登录屏幕上的 VPN 凭证。

**步骤 3** 对于 Citrix 服务器的每个后续连接，用户只需输入 VPN 凭证。

如将 ASA 用作 XenApp 和 XenDesktop 的代理，则不需要 Citrix 访问网关。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证，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。

### 下一步做什么

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 服务器或 VDI 代理服务器

过程

**步骤 1** 依次选择 **Configuration > Remote Access VPN > Clientless SSL VPN Access > VDI Access**。

**步骤 2** 如果只有一台服务器，请选中 **Enable VDI Server Proxy**，然后配置 VDI 服务器。

**步骤 3** 如要将多个组策略分配给 VDI 服务器，请选中 **Configure All VDI Servers**。

**步骤 4** 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。

过程

**步骤 1** 依次浏览至 **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**。

**步骤 4** 点击**添加**或**编辑**，以提供 VDI 服务器详细信息。

- **服务器（主机名或 IP 地址）**- XenApp 或 XenDesktop 服务器的地址。此值可以是无客户端宏。
- **端口号（可选）**- 用于连接至 Citrix 服务器的端口号。此值可以是无客户端宏。
- **Active Directory Domain Name** - 用于登录虚拟化基础设施服务器的域。此值可以是无客户端宏。
- **使用 SSL 连接** - 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。此值可以是无客户端宏。
- **Password** - 用于登录虚拟化基础设施服务器的密码。此值可以是无客户端宏。

# 配置浏览器对客户端-服务器插件的访问

客户端-服务器插件表显示了 ASA 在无客户端 SSL VPN 会话中可供浏览器使用的插件。

要添加、更改或删除插件，请执行以下操作之一：

- 要添加插件，请点击 **Import**。系统将打开 Import Plug-ins 对话框。
- 要删除插件，请将其选中并点击 **Delete**。

# 关于安装浏览器插件

浏览器插件是 Web 浏览器在执行专用功能时（例如，在浏览器窗口中将客户端连接至服务器）调用的一个独立程序。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，思科将测试再分发的插件，在某些情况下，还将测试其无法再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。

安装闪存设备中的插件时，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 文件系统中的 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页面 Address 字段旁边的下拉列表。

下表显示了在添加以下各节中介绍的插件时门户页面的主菜单和地址字段发生的变化。

**表 *7:* 插件在无客户端 *SSL VPN* 门户页面上的效果**

| 插件 | 添加到门户页面的主菜单选项 | 添加到门户页面的 **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:// |

**注释** 辅助 ASA 会从主 ASA 获取插件。

当无客户端 SSL VPN 会话中的用户在门户页面上点击关联的菜单选项时，门户页面会在界面上显示一个窗口，并显示一个帮助窗格。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。

注释 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。报告状态的是开源插件而不是 ASA。

### 安装浏览器插件的前提条件

- 如果安全设备将无客户端会话配置为使用代理服务器，则插件无法工作。

  注释 远程桌面协议插件不支持用会话代理程序进行负载均衡。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，插件将正常工作。

- 插件支持单点登录 (SSO)。它们使用所输入的相同凭证打开无客户端 SSL VPN 会话。因为插件不支持宏替换，您无法选择对不同的字段（例如内部域密码）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访客特权模式。

## 安装浏览器插件的要求

- 按照GNU通用公共许可证(GPL)的规定，思科在不对插件进行任何更改的情况下再分发插件。按照 GPL 的规定，思科不能直接增强这些插件的功能。
- 只有在 ASA 上启用无客户端 SSL VPN，才能远程访问插件。
- 状态故障切换不保留使用插件建立的会话。完成故障切换之后，用户必须重新连接。
- 插件要求对浏览器启用 ActiveX 或 Oracle Java 运行时环境 (JRE)。没有适用于 64 位浏览器的 ActiveX 版本的 RDP 插件。

## 设置 RDP 插件

要设置和使用 RDP 插件，必须添加新的环境变量。

### 过程

**步骤 1** 右键点击 **My Computer** 访问 System Properties，然后选择 **Advanced** 选项卡。

**步骤 2** 在 Advanced 选项卡上，选择 Environment Variables 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版本低于 8.3 版的无客户端 SSL VPN 使用，则必须删除旧版思科 Portforwarder 控件。转至目录 C:/WINDOWS/Downloaded Program Files，右键点击 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。

现在，您可以在 Windows 应用事件查看器中查看事件。

# 为插件准备安全设备

过程

**步骤 1** 确保已在 ASA 接口上启用无客户端 SSL VPN。

**步骤 2** 在远程用户使用完全限定域名 (FQDN) 连接的 ASA 接口上安装 SSL 证书。

**注释** 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 文件中的条目来解析 FQDN。

第 15 章

# 高级无客户端 SSL VPN 配置



## Microsoft Kerberos 约束委派解决方案

很多组织希望使用超出现在 ASA SSO 功能可以提供的身份验证方法对其无客户端 VPN 用户进行身份验证并将其身份验证凭证无缝扩展至基于 Web 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 Web 的无客户端资源转发静态用户名和密码等传统用户凭证。

例如，基于证书和基于 OTP 的身份验证方法都不包含 ASA 对基于 Web 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 Web 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 Web 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 Web 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 Web 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证无缝扩展至使用 ASA 支持的所有身份验证方法的 Web 应用。

# 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 使用票证而非密钥对访问服务器的客户端进行身份验证。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。每个票证由密钥分发中心发行并具有设定的寿命。

Kerberos 安全系统是一种身份验证协议，用于对实体（用户、计算机或应用）进行身份验证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 Web 服务的 SSO 访问。例如，此类 Web 服务或应用包括 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），从而提供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来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。

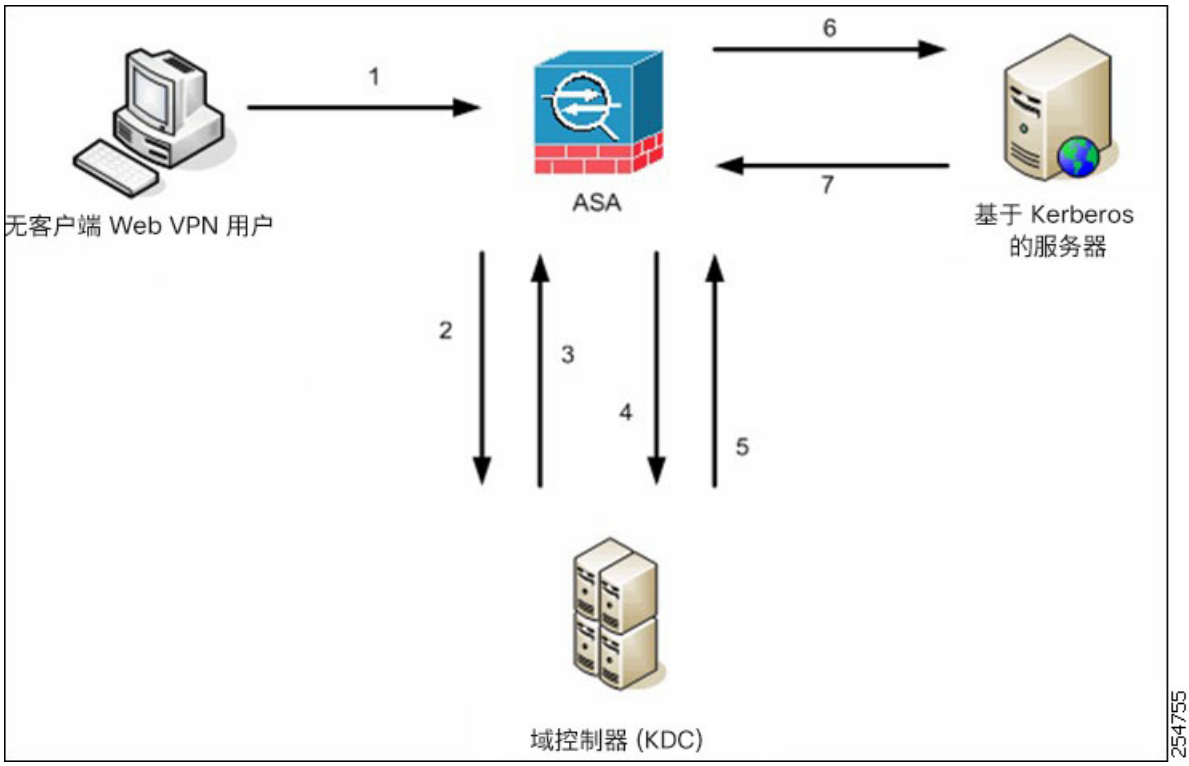
有关约束委派的详细信息，请通过 IETF 网站参阅 RFC 1510 (http://www.ietf.org)。

# 使用 KCD 的身份验证流程

下图说明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 *9: KCD* 流程




注释 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。（在使用智能卡凭证的情况下，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 Web 服务。如果 Web 服务要求进行身份验证，服务器将请求 ASA 提供凭证并发送一份受服务器支持的身份验证方法列表。

注释 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 将代表用户为自身向密钥分发中心请求获取服务票证。
3. 密钥分发中心将向 ASA 返回所请求的票证。即使这些票证是传送到 ASA，其中包含的也是用户的授权数据。ASA 就用户想要访问的特定服务向 KCD 请求获取服务票证。

注释 步骤 1 至步骤 3 包含协议转换。完成这些步骤后，任何使用非 Kerberos 身份验证协议向 ASA 进行身份验证的用户都已使用 Kerberos 向密钥分发中心完成透明身份验证。

4. ASA 为用户想要访问的特定服务向密钥分发中心请求获取服务票证。
5. 密钥分发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 Web 服务。
7. Web 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。

# 调试 KCD

请使用以下命令控制 KCD 特定调试消息的输出，而不要像 9.5.2 版本以前那样控制 ADI 发出系统日志的级别：

**debug webvpn kcd**

# 在 Active Directory 中添加 Windows 服务账户

ASA 上的 KCD 实施要求使用服务账户，也就是具备添加计算机（例如将 ASA 添加到域中）所需的权限的 Active Directory 用户账户。在我们的示例中，Active Directory 用户名 JohnDoe 即具备所需权限的服务账户。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

本节概述在 ASA 上配置 DNS 所需执行的配置程序。当将 KCD 用作 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。

过程

**步骤 1** 在 ASDM 中，依次导航至**配置** > **远程访问 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 部署要求通过内部企业网络进行 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程序。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。

## 过程

**步骤 1** 在 ASDM 中，依次导航至**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **高级** > **Microsoft KCD 服务器**。

**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
  - “服务器组名称”- 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。
  - “重新激活模式”- 点击所需模式的单选按钮（**消耗**或**定时**）。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。默认配置是 Depletion。
  - Dead Time - 如果选择 Depletion 重新激活模式，必须添加失效时间间隔。默认配置是十分钟。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。默认值是三次。
- 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内部企业网络上，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 - 指定获得服务器响应之前最长的等待时间（以秒为单位）。默认值是十秒。
- 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。默认配置是十秒。
  - Realm - 以全部大写的格式输入域控制器的域名。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。

## Microsoft Kerberos 的要求

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 Web 服务所在的域）之间建立信任关系。ASA 使用其独特的格式，跨越从源到目的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称为跨领域身份验证。在跨领域身份验证的每个阶段，ASA 依赖于特定领域上的凭证和与后续领域的信任关系。

# 配置使用外部代理服务器

使用“代理”窗格将 ASA 配置为使用外部代理服务器处理 HTTP 请求和 HTTPS 请求。这些服务器用作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。

注释 HTTP 和 HTTPS 代理服务不支持与个人数字助理的连接。

过程

**步骤 1** 点击 Use an HTTP Proxy Server。

**步骤 2** 以 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。字符串没有字符数限制，但整个命令不能超过 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，包括斜杠 (/) 和句点 (.)。此通配符必须与字母数字字符串一起使用。
- **?** 匹配任意单个字符，包括斜杠和句点。
- [x-y] 匹配 x 与 y 之间的任意单个字符，其中 x 代表 ANSI 字符集中的一个字符，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，随每个 HTTP 代理请求提供一个用户名，用于提供基本的代理身份验证。

**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，还可以选择 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 URL 中排除。字符串没有字符数限制，但整个命令不能超过 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，包括斜杠 (/) 和句点 (.)。此通配符必须与字母数字字符串一起使用。
- **?** 匹配任意单个字符，包括斜杠和句点。
- [x-y] 匹配 x 与 y 之间的任意单个字符，其中 x 代表 ANSI 字符集中的一个字符，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，随每个 HTTPS 代理请求提供一个用户名，用于提供基本的代理身份验证。

**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。

# 将 HTTPS 用于无客户端 SSL VPN 会话

除配置 HTTPS 外，启用 HTTP 严格传输安全 (HSTS) - 一种 Web 安全策略机制有助于保护网站免受协议降级攻击和 Cookie 劫持。HSTS 通过发送以下指令将 UA/浏览器重定向至 HTTPS 网站，以便安全地连接到 Web 服务器，直至指定的超时时间到期：

```
Strict-Transport-Security: max-age=”31536000”; preload;
```

其中：

- max-age -（可配置）指定必须将 Web 服务器视为 HSTS 主机并且只能使用 HTTPS 安全地对其进行访问的时间（以秒为单位）。默认值为 18 周（10886400 秒）。取值范围为 8 小时到 365 天（0-31536000 > 秒）。
- preload - 告知浏览器加载已向 UA/浏览器注册的域的列表；现在必须将其视为 HSTS 主机。预加载列表的实施与UA/浏览器相关，每个UA/浏览器可以对其他指令指定进一步的限制。例如，Chrome 的预加载列表指定，HSTS 最大老化时间至少为 18 周（10886400 秒）。

## 过程

**步骤 1** 依次选择**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 高级 > 代理**。

**步骤 2** 选中**启用 HSTS**。

**步骤 3** 指定 **HSTS 最大老化时间**，即 HSTS 保持有效的时间（以秒为单位）。

值的范围为 <0-31536000> 秒。默认值为 10886400（18 周）。一旦达到此限制，HSTS 将不再有效。

HSTS 保持有效的时间（以秒为单位）。值的范围为 <0-31536000> 秒。默认值为 10886400（18 周）。一旦达到此限制，HSTS 将不再有效。

# 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“应用配置文件自定义框架 (APCF)”选项，ASA 可以通过它处理非标准应用和 Web 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。

可以将 APCF 配置文件存储在 ASA 闪存上，也可以存储在 HTTP、HTTPS 或 TFTP 服务器上。

我们建议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

可以将 APCF 配置文件存储在 ASA 闪存上，也可以存储在 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。

### 过程

**步骤 1** 依次导航到 Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Application Helper，可在其中执行以下功能。

- 点击 **Add/Edit**，创建新的 APCF 配置文件或更改现有的 APCF 配置文件。
  - 点击**闪存文件**，查找存储在 ASA 闪存中的 APCF 文件。

    然后点击**上传**将 APCF 文件从本地计算机传送至 ASA 闪存文件系统，或者点击“浏览以上传”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。无确认或撤消功能。
- 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** 如果未在列表中发现所作更改，请点击 **Refresh**。

# 上传 APCF 数据包

过程

**步骤 1** 系统将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 上要上传 APCF 文件的路径。点击**浏览闪存**，确定 ASA 上要向其中上传 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** 确定计算机上的 APCF 文件位置以及要将其下载到 ASA 中的位置后，请点击**上传文件**。

**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，这表示您可以上传另一个文件。要上传另一个文件，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 文件上传至闪存中之后或决定不上传此文件时，请点击 **Close**。如果选择上传，在 APCF 窗口的 APCF File Location 字段将显示文件名。如果选择不上传，系统将显示 Close Message 对话框，提示“Are you sure you want to close the dialog without uploading the file?” 如果不想上传文件，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

过程

**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 文件位置** - 显示关于 APCF 数据包位置的信息。这个位置可能在 ASA 闪存中，也可能在 HTTP、HTTPS、FTP 或 TFTP 服务器上。
- **添加/编辑** - 点击以添加或编辑新的或现有的 APCF 配置文件。

- **删除** - 点击以删除现有的 APCF 配置文件。无确认或撤消功能。
- **上移** - 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。如果已添加路径，则在浏览找到此路径后，它将重定向到存储在闪存中的 APCF 文件。

**步骤 4** 点击**浏览闪存**，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。

**注释** 如果看不到最近下载的 APCF 文件的名称，请点击 **Refresh**。

- **上传** - 点击以将 APCF 文件从本地计算机上传至 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，同时采用下表中的 XML 标签。

### APCF 规定

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 *8: 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 说明正文的强制性标签。 |
| <id>文本</id> | 说明此特定 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。 |

| 标签 | 使用 |
| --- | --- |
| <js-object>…</js-object><br><html-object>…</html-object><br><process-request-header>...</process-request-header><br><process-response-header>...</process-response-header><br><preprocess-response-body>...</preprocess-response-body><br><postprocess-response-body>...</postprocess-response-body> | 这些标签之一指定内容的类型或应该进行 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：<br>• http-version（例如 1.1、1.0、0.9）<br>• http-method（get、put、post、webdav）<br>• http-scheme（“http/”、“https/”、其他）<br>• server-regexp regular expression containing ("a".."z" \| "A".."Z" \| "0".."9" \| ".-_*[]?")<br>• server-fnmatch（正则表达式，包含 ("a".."z" \| "A".."Z" \| "0".."9" \| ".-_*[]?+()\{},"）<br>• user-agent-regexp<br>• user-agent-fnmatch<br>• request-uri-regexp<br>• request-uri-fnmatch<br>• 如有多个条件标签，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；可以使用以下标签来定义这些操作（如下所示）：<br>• <do><br>• <sed-script><br>• <rewrite-header><br>• <add-header><br>• <delete-header> |

| 标签 | 使用 |
| --- | --- |
| <do>…</do> | 用于定义一个以下操作的操作标签子元素：<br>• <no-rewrite/> - 请勿改变从远程服务器接收的内容。<br>• <no-toolbar/> - 请勿插入工具栏。<br>• <no-gzip/> - 请勿压缩内容。<br>• <force-cache/> - 保留原始缓存说明。<br>• <force-no-cache/> - 使对象不可缓存。<br>• < downgrade-http-version-on-backend> - 向远程服务器发送请求时使用 HTTP/1.0。 |
| <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：<br><br>`<rewrite-header>`<br>`<header>Connection</header>`<br>`<value>close</value>`<br>`</rewrite-header>` |

## APCF 的配置示例

```
<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>

<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。

**过程**

**步骤 1** 点击**无**或从“用户存储位置”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**

**注释** 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、凭证

- Cookie
- 凭证

**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）。语言决定了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。浏览器也可以检测页面上指定的编码，并相应地显示文档。

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，从而确保正确显示此页面，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“全局编码类型”。在正确显示文件名或目录路径以及页面方面遇到问题时，请全局使用“Global Encoding Type”属性并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，可以查看或指定无客户端 SSL VPN 门户页面的字符编码。

**过程**

**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，表中所列来自 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

注释　如果点击 **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

  注释　如果使用日文 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** 以删除该字体族。

- unicode
- windows-1252
- none

如果点击 **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。

# 配置内容缓存

缓存可增强无客户端 SSL VPN 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。使用缓存可减少流量，因此提高了很多应用的运行效率。

注释　启用内容缓存可能会导致一些系统的可靠性下降。如果启用内容缓存后遇到随机崩溃，请将其禁用。

过程

**步骤 1** 依次选择 Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Content Cache。

**步骤 2** 如果未选中 Enable Cache，请将其选中。

**步骤 3** 定义缓存的条件。

- “最大对象大小”- 以 KB 为单位输入 ASA 可以缓存的文档的最大大小。ASA 会衡量对象的原始内容长度，而不是重写或压缩后的内容。此范围为 0 至 10,000 KB；默认值为 1000 KB
- “最小对象大小”- 以 KB 为单位输入 ASA 可以缓存的文档的最小大小。ASA 会衡量对象的原始内容长度，而不是重写或压缩后的内容。此范围为 0 至 10,000 KB；默认值为 0 KB。

  **注释** 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缓存既没有上一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 通过内容转换/重写引擎处理应用流量，此引擎包括 JavaScript、VBScript、Java 和多字节字符等高级元素，用于代理可根据用户是从 SSL VPN 设备内部还是独立于此设备来使用应用而采用不同语义和访问控制规则的 HTTP 流量。

默认情况下，安全设备会重写或转换所有无客户端流量。您可能不想让某些应用和 Web 资源（例如公共网站）通过ASA。因此，ASA 允许您创建重写规则，用于允许用户浏览某些网站和应用而不通过 ASA。这类似于 VPN 连接中的分割隧道。

注释 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

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。

**过程**

**步骤 1** 依次导航至 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 到 65534。

**步骤 5** （可选） 提供说明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。可以使用以下一种通配符，但是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 *9:* 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 | 已取消选中 | 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 | 选中 | 65,535 | rewrite-all | * |

# 在无客户端 SSL VPN 上使用邮件

## 配置 Web 邮件：MS Outlook Web App

ASA 支持通过 Microsoft Outlook Web App 访问 Exchange Server 2010 以及通过 Microsoft Outlook Web Access 访问 Exchange Server 2007、2003 和 2000。

过程

**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，可以将列表分配给一个或多个策略 - 组策略和/或动态访问策略。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 Web 服务器或 Web 应用的特定信息，而不仅仅是使用包含凭证的 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。

### 开始之前

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。除了向组策略和/或动态访问策略分配书签列表之外，还可以向这些策略应用 Web ACL 以控制对流量的访问。请关闭这些策略上的 URL Entry，以防用户无法分辨哪些 URL 才是可访问的。

### 过程

**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。

系统将显示书签标题和实际关联的 URL。

**步骤 2** （可选） 点击**添加**，配置新的服务器或 URL。可以添加一项以下内容：

- 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**编辑**，更改服务器、URL 或显示名称。

**步骤 4** （可选） 点击**删除**，从 URL 列表删除选择的项目。无确认或撤消功能。

**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... - 浏览到文件的路径。

**步骤 6** （可选） 突出显示书签并点击**分配**，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**上移**或**下移**选项更改选择的项目在 URL 列表中的位置。

**步骤 8** 点击“确定”。

### 下一步做什么

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。

### 开始之前

如要访问网络上的共享文件夹，请使用以下格式：\\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。

### 过程

**步骤 1** 依次导航到**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **门户** > **书签**，然后点击**添加**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*

**示例：**

具体插件决定了您可以输入的可选参数值对：

*host*/**?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**

要为插件提供单点登录支持，请使用参数值对 **csco_sso=1**：

host/**?csco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**

**步骤 6** （可选） 输入预加载 URL。输入预加载 URL 时，也可以输入等待时间，即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，请提供说明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**，导入或导出用作缩略图的图像。

**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和目的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**高级选项**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。

### 开始之前

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
- Microsoft SharePoint 2013

### 过程

**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，请提供说明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**，导入或导出用作缩略图的图像。

**步骤 5** （可选） 选中“将此书签置于 VPN 主页上”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
- Microsoft SharePoint 2013

**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：

- 协议。HTTP 或 HTTPs。
- hostname。例如 www.cisco.com。
- Port Number。应用所使用的端口。
- URL Path Appendix。例如 /Citrix/XenApp。这通常会自动填充。
- Domain。要连接的域。
- User Name。用作用户名的 SSL VPN 变量。点击 Select Variable 选择不同的变量。
- 密码。用作密码的 SSL VPN 变量。点击 Select Variable 选择不同的变量。

**步骤 10** （可选） 点击**预览**查看模板输出。可以点击 Edit 修改模板。

**步骤 11** 点击 **OK** 确定更改。或者，点击取消 (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。

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。

### 过程

**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*

示例：

例如，具体插件决定了您可以输入的可选参数值对。

```
host/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768
```

要为插件提供单点登录支持，请使用参数值对 **csco_sso=1**。

```
host/?csco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768
```

**步骤 4** 至于副标题，请提供说明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**，导入或导出用作缩略图的图像。

**步骤 7** （可选） 选中“将此书签置于 VPN 主页上”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 Web 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。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 确定更改。或者，点击 Cancel 放弃更改。

后续操作

下一步做什么

在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 Web 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。

过程

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。
- “闪存文件系统”- 点击以导出位于 ASA 上的文件。
- “远程服务器”- 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 - 浏览到文件的路径。
- 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（Web 内容）

此对话框允许您导入和导出 Web 内容对象。系统将显示 Web 内容对象的名称及其文件类型。

Web 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 Web 内容和导入现成可用的 Web 内容。导出 Web 内容进行修改或编辑，然后重新导入。

过程

步骤 1 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... - 浏览到文件的路径

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 只在门户页面显示 /+CSCOE+/ 对象，而 /+CSCOU+/ 对象则可在登录或门户页面上显示和使用。

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。此类资源的例子包括书签条目、URL 列表和文件共享。

## 过程

**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。可以从下拉列表中选择的变量包括：

**表 *10:* 无客户端 *SSL VPN* 变量**

| 编号 | 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。这是缓存的凭证而且未由 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 |
| 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。<br>通过 RADIUS 进行的变量替换由 VSA#223 执行。 |

| 编号 | 变量替换 | 定义 |
|---|---|---|
| 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。<br>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。 |
| 11 | CSCO_WEBVPN_DYNAMIC_URL | 可在用户门户上生成多个书签链接的单个书签。 |
| 12 | CSCO_WEBVPN_MACROLIST | 静态配置的书签，可以使用 LDAP 属性映射提供的任意大小的列表。 |

当 ASA 识别最终用户请求中（书签或 POST 表单中）这六个字符串中的一个时，会将其替换为用户特定的值，然后再将请求传递至远程服务器。

注释　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（又称为 HTTP 分析器）的链接：http://www.ieinspector.com/httpanalyzer/downloadV2/IEHttpAnalyzerV2.exe。

**步骤 2** 使用以下指导原则选择合适的变量：

- 使用变量 1 至 4 - ASA 为 SSL VPN 登录页面前四个替换获取值，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。

```
For example, if a URL list contains the link,
http://someserver/homepage/CSCO_WEBVPN_USERNAME.html, the ASA translates it to the
following unique links:

For USER1, the link becomes http://someserver/homepage/USER1.html

For USER2, the link is http://someserver/homepage/USER2.html
```

```
In the following case, cifs://server/users/CSCO_WEBVPN_USERNAME lets the ASA map a file
 drive to specific users:
For USER1, the link becomes cifs://server/users/USER1
For USER 2, the link is cifs://server/users/USER2
```

- 使用变量 5 和 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 - 每当 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的值，然后再将请求传递至远程服务器。

```
The following example sets a URL for the homepage:
WebVPN-Macro-Value1 (ID=223), type string, is returned as wwwin-portal.example.com
WebVPN-Macro-Value2 (ID=224), type string, is returned as 401k.com

To set a home page value, you would configure the variable substitution as
https://CSCO_WEBVPN_MACRO1, which would translate to https://wwwin-portal.example.com.
```

- 使用变量 11 - 这些书签根据在其中映射 CSCO_WEBVPN_DYNAMIC_URL 的 LDAP 属性映射生成。使用分隔符参数，将从 LDAP 收到的字符串解析为值列表。用于 url 字段中或作为 POST 参数用于书签中时，将为解析后的 LDAP 字符串中的每个值生成书签。下面提供了使用 CSCO_WEBVPN_DYNAMIC_URL 的书签配置示例：

```
<bookmark>
    <title>Test Bookmark</title>
    <method>post</method>
    <favorite>yes</favorite>
    <url>http://CSCO_WEBVPN_DYNAMIC_URL1(".")</url>
    <subtitle></subtitle>
    <thumbnail></thumbnail>
    <smart-tunnel>no</smart-tunnel>
    <login-page-url></login-page-url>
    <landing-page-url></landing-page-url>
    <pre-login-page-url></pre-login-page-url>
    <control-id></control-id>
    <<post-param>
        <value>value1</value>
        <name>parameter1</name>
    </post-param>
</bookmark>
```

CSCO_WEBVPN_DYNAMIC_URL 在 LDAP 属性映射中配置，并映射到 host1.cisco.com、host2.cisco.com 和 host3.cisco.com。根据分隔符，可以获得三个单独的 URL 并从这一个配置生成三个书签 http://host1.cisco.com、http://host2.cisco.com 和 http://host3.cisco.com。

此外，您还可以将此宏用作 POST 参数的一部分：

```
<bookmark>
    <title>Test Bookmark</title>
    <method>post</method>
    <favorite>yes</favorite>
    <url>http://www.myhost.cisco.com</url>
    <subtitle></subtitle>
    <thumbnail></thumbnail>
    <smart-tunnel>no</smart-tunnel>
    <login-page-url></login-page-url>
    <landing-page-url></landing-page-url>
    <pre-login-page-url></pre-login-page-url>
```

```
<control-id></control-id>
<post-param>
    <value>CSCO_WEBVPN_DYNAMIC_URL(";")</value>
    <name>host</name>
</bookmark>
```

使用映射的相同 LDAP 属性，创建三个目标 URL 为 http://www.myhost.cisco.com 的书签，各有不同的 POST 参数，名称为 *host*，值为 host1.cisco.com、host2.cisco.com 和 host3.cisco.com。

**注释** 只能将 CSCO_WEBVPN_DYNAMIC_URL 用于书签中。不能将其用于支持宏的其他位置，例如 Citrix mobile receiver 的 vdi CLI 配置。也不能将其用于定义外部门户页面。

- 使用变量 12 - 此宏以三个参数作为输入：索引、分隔符和转义。索引是管理员提供的整数，指定要选择的列表中的元素编号。分隔符是管理员提供的字符串，包括用于将 LDAP 映射字符串分隔为值列表的字符，每次使用宏都使用一个分隔符。转义是在代入 ASA 请求中之前应用 LDAP 字符串的选择。

  例如，CSCO_WEBVPN_MACROLIST(2, ",", url-encode) 指定使用列表中的第二个值并使用一个逗号作为分隔符将字符串分隔为列表。值在代入发送到后端的 ASA 请求中时经过 URL 编码。对于转义例程，使用以下值：

  - *None* - 在发送到后端服务器之前不转换字符串值。
  - *url-code* - 对每个解析的值进行 URL 编码，组成 URL 中特殊字符的保留字符列表除外。
  - *url-encode-data* - 使用 URL 编码充分转换每个解析的值。
  - *base64* - 对每个解析的值进行 Base64 编码。

  下面提供了使用 CSCO_WEBVPN_MACROLIST1 的书签配置示例：

```
<bookmark>
    <title>MyHost</title>
    <method>post</method>
    <favorite>yes</favorite>
    <url>http://www.myhost.cisco.com</url>
    <subtitle></subtitle>
    <thumbnail></thumbnail>
    <smart-tunnel>no</smart-tunnel>
    <login-page-url><login-page-url>
    <landing-page-url></landing-page-url>
    <pre-login-page-url></pre-login-page-url>
    <control-id></control-id>
    <post-param>
        <value>CSCO_WEBVPN_MACROLIST1(1, ";", url-encode-data)>/value>
        <name>param1</name>
        <value>CSCO_WEBVON_MACROLIST1(2, ";", url-encode-data)</value>
        <name>param2</name>
        <value>CSCO_WEBVPN_MACROLIST1(3, ";", url-encode-data)</value>
        <name>param3</name>
    </post-param>
</bookmark>
```

使用该书签，您可以浏览到 www.myhost.cisco.com 并自动将以下 3 个 POST 参数发送到服务器：param1、param2 和 param3。ASA 将 CSCO_WEBVPN_MACROLIST1 的值代入这些参数后再发送到后端。

**注释** 在使用其他宏的任何地方都可以使用 CSCO_WEBVPN_MACROLIST。

- 执行此操作的最佳方法是在 ASDM 中配置主页 URL 参数。无需写入脚本或上传任何内容，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

**步骤 3** 设置书签或 URL 条目。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使用下列路径之一在 ASDM 中添加或编辑书签。

- 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

**步骤 4** 通过配置 File Share (CIFS) URL 替换，设置更灵活的书签配置。如果配置 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。

### 过程

**步骤 1** 依次选择**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **门户** > **自定义**。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。

第 16 章

# 策略组



## 智能隧道访问

以下各节介绍如何启用使用无客户端 SSL VPN 会话的智能隧道访问，指定随此类访问提供的应用，并提供其使用说明。

要配置智能隧道访问，需要创建一份智能隧道列表，其中包含一个或多个符合智能隧道访问条件的应用，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只支持一个智能隧道列表，您必须将要支持的非基于浏览器的应用归类到智能隧道列表中。创建列表后，需将其分配给一个或多个组策略或本地用户策略。

以下各节介绍智能隧道及其配置方法：

# 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，还可以要求匹配校验和的 SHA-1 散列值，作为授权智能隧道访问的条件。

例如，Lotus SameTime 和 Microsoft Outlook 可能就是您要授权智能隧道访问的应用。

配置智能隧道需要执行以下程序之一，具体取决于应用是客户端应用还是支持 Web 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并支持 Web 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。

您还可以列出要在通过无客户端 SSL VPN 会话接入的智能隧道连接中自动提交登录凭证的支持 Web 的应用。

### 智能隧道的优势

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，它可为用户提供以下优势：

- 智能隧道所提供的性能要优于插件性能。
- 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。

# 智能隧道的必备条件

有关智能隧道支持的平台和浏览器，请参阅支持的 VPN 平台，Cisco ASA 5500 系列。

下列要求和限制适用于 Windows 上的智能隧道访问：

- 在 Windows 中，必须对浏览器启用 ActiveX 或 Oracle Java 运行时环境 (JRE)（建议使用 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。
- 仅在 Mac OS X 中必须对浏览器启用 Java Web Start。
- 智能隧道与 IE 的增强保护模式不兼容。

# 智能隧道的规定

- 智能隧道仅支持位于运行 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列于客户端的代理例外列表中。
  - 如果 Windows 计算机不需要代理就能访问 ASA，但需要代理才能访问主机应用，则 ASA 必须列于客户端的代理例外列表中。

  代理系统可以由客户端的静态代理条目配置或自动配置定义，也可由 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，如要向从命令提示符启动的应用添加智能隧道访问，必须在智能隧道列表的一个条目的 Process Name 中指定“cmd.exe”，然后在另一个条目中指定该应用本身的路径，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 Web 和最终用户之间的流量。该代理必须支持 CONNECT 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 会让所有浏览器流量通过 VPN 会话。只有在应用隧道全部策略（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，它会让所有流量通过 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。
- 状态故障切换不保留智能隧道连接。用户在故障切换后必须重新连接。
- 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 启动另一个 Firefox 实例需要名为 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。
- 在 Mac OS X 中，与 SSL 库动态链接的使用 TCP 的应用可在智能隧道上运行。
- 智能隧道在 Mac OS X 上不提供以下支持：
  - 代理服务。
  - 自动登录。
  - 使用两级名称空间的应用。
  - 基于控制台的应用，例如 Telnet、SSH 和 cURL。
  - 使用 dlopen 或 dlsym 来查找 libsocket 调用的应用。
  - 用于查找 libsocket 调用的静态链接应用。

- 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）。
- 现已创建了一种新方法，用于 Mac 和 Windows 设备上的 Chrome 浏览器中的智能隧道支持。Chrome 智能隧道扩展 (Chrome Smart Tunnel Extension) 取代了 Chrome 中不再支持的 Netscape 插件应用程序编程接口 (NPAPI)。

  如果您在没有安装该扩展的情况下点击了 Chrome 中启用了智能隧道的书签，则系统会将您重定向到 Chrome 网上应用店以获取该扩展。新的 Chrome 安装会将用户定向到 Chrome 网上应用店以下载该扩展。该扩展将从 ASA 下载运行智能隧道所需的二进制文件。

  Chrome 的默认下载位置需要指向当前用户的“下载”文件夹。或者，如果 Chrome 的下载设置为“每次询问”，则用户应在系统询问时选择“下载”文件夹。

  除安装新扩展以及指定下载位置的过程之外，使用智能隧道时的常规书签和应用配置不变。

# 配置智能隧道（Lotus 示例）

注释 这些示例说明只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，请参阅随后几节中的字段说明。

过程

**步骤 1** 依次选择**配置 > Remote Access VPN > Clientless SSL VPN Access** > 门户 > 智能隧道。

**步骤 2** 双击要添加应用的智能隧道列表；或者点击**添加**创建应用列表，在“列表名称”字段中为此列表输入名称，然后点击**添加**。

例如，在“智能隧道”窗格中点击**添加**，在“列表名称”字段中输入 Lotus，然后点击**添加**。

**步骤 3** 在“添加或编辑智能隧道列表”对话框中点击**添加**。

**步骤 4** 在 Application ID 字段中输入一个字符串，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。

下表显示了示例应用 ID 字符串和支持 Lotus 所需的关联路径。

表 *11:* 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**确定**。

**步骤 8** 为要向列表添加的每个应用分别重复这些步骤。

**步骤 9** 在“添加或编辑智能隧道列表”对话框中点击**确定**。

**步骤 10** 按照以下步骤，将此列表分配给组策略和本地用户策略，以便为关联应用提供智能隧道访问：

- 要将列表分配给组策略，请选择**Configuration > Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add** 或 **Edit > Portal**，然后从“智能隧道列表”下拉列表中选择智能隧道名称。
- 要将列表分配给本地用户策略，请选择**Configuration > Remote Access VPN> AAA Setup > Local Users > Add** 或 **Edit > VPN Policy > Clientless SSL VPN**，然后从“智能隧道列表”下拉列表中选择智能隧道名称。

# 简化应用的隧道访问配置

智能隧道应用列表实质上是一种过滤器，用于确定获准访问隧道的应用。默认情况下，允许浏览器启动的所有进程访问隧道。通过支持智能隧道的书签，无客户端会话可以只授权 Web 浏览器启动的进程访问隧道。对于非浏览器应用，管理员可以选择允许所有应用通过隧道访问，从而无需了解最终用户可能调用哪些应用。

**注释** 此配置仅适用于 Windows 平台。

下表显示了进程获准访问的情况。

| 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获准访问。 | 只有与应用列表中进程名称匹配的进程获准访问。 |
| 智能隧道关闭 | 所有进程（及其子进程）都获准访问。 | 无任何进程获准访问。 |
| 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。<br>**注释** 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获准访问，但不包括这些原始进程的任何子进程。 |

过程

**步骤 1** 依次选择**配置** > **远程访问 VPN** > **AAA/本地用户** > **本地用户**。

**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**编辑**。系统将显示 Edit User Account 窗口。

**步骤 4** 在“编辑用户账户”窗口的左侧边栏，依次点击 **VPN 策略** > **无客户端 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。
- 或者，选择以下隧道策略选项：
  - 在 Smart Tunnel Policy 参数上，取消选中 **Inherit** 复选框。
  - 从网络列表中进行选择并指定以下一个隧道选项：对指定网络使用智能隧道、对指定网络不使用智能隧道或对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。

过程

**步骤 1** 依次导航至**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **门户** > **智能隧道**，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输入唯一名称。请勿使用空格。

配置智能隧道列表后，无客户端 SSL VPN 组策略和本地用户策略中的 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 并根据需要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。系统将保存用户指定的此名称，然后返回 GUI。此字符串对于操作系统是唯一的。它通常用于命名要被授权智能隧道访问的应用。如果您选择为同一应用的多个版本指定不同的路径或散列值，则为了支持这些版本，您可以使用此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。字符串最多可以包含 64 个字符。
- Process Name - 输入应用的文件名或路径。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，该应用就可以位于任何路径。

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，则要么只在此字段中指定应用的名称和扩展名，要么为每个路径创建一个唯一的智能隧道条目。

**注释** 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，某个应用的默认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，如要向从命令提示符启动的应用添加智能隧道访问，必须在智能隧道列表的一个条目的 Process Name 中指定“cmd.exe”，然后在另一个条目中指定该应用本身的路径，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，请在使用 SHA-1 算法计算散列值的实用程序中输入应用的校验和（即可执行文件的校验和）。此类实用程序的一个典型示例是 Microsoft File Checksum Integrity Verifier (FCIV)，可从 http://support.microsoft.com/kb/841290/ 下载。安装 FCIV 后，将要进行散列计算的应用的临时副本放到不含空格的路径上（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**）以显示 SHA-1 散列值。

  SHA-1 散列值始终为 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 匹配的应用的散列值。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。

  输入散列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 Hash 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散列值，请为每个 Hash 值创建一个唯一的智能隧道条目。

  **注释** 如果输入 Hash 值并且需要智能隧道访问支持某个应用的未来版本或补丁，则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 Hash 值的应用列表未随应用升级一起更新。不输入散列值即可避免此问题。

**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** 创建完智能隧道列表后，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将其激活：

- 要将列表分配给组策略，请选择**Config > Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add** 或 **Edit > Portal**，然后从“智能隧道列表”属性旁的下拉列表中选择智能隧道名称。
- 要将列表分配给本地用户策略，请选择**Config > Remote Access VPN> AAA Setup > Local Users > Add** 或 **Edit > VPN Policy > Clientless SSL VPN**，然后从“智能隧道列表”属性旁的下拉列表中选择智能隧道名称。

表 *12:* 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 |
| 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 |

# 关于智能隧道列表

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。
- 用户登录时启用智能隧道访问，但需要用户使用无客户端 SSL VPN 门户页面上的**Application Access** > **Start Smart Tunnels**按钮将其手动启动。

**注释** 对于每个组策略和用户名，智能隧道登录选项相互排斥。只能使用一个。

# 创建智能隧道自动登录服务器列表

通过 Smart Tunnel Auto Sign-on Server List 对话框，可以添加或编辑将在智能隧道设置期间自动提交登录凭证的服务器列表。通过智能隧道自动登录的功能可用于 Internet Explorer 和 Firefox。

过程

**步骤 1** 依次导航至 Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels，并确保展开 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要配置的其他列表区分开的唯一名称。字符串最多可以包含 64 个字符。请勿使用空格。

下一步做什么

注释 创建智能隧道自动登录列表之后，无客户端 SSL VPN 组策略和本地用户策略配置中 Smart Tunnel 下方的 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。

过程

**步骤 1** 依次导航至**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **门户** > **智能隧道**，选择一个列表，然后点击**编辑**。

**步骤 2** 在 Add Smart Tunnel Auto Sign-On Server List 对话框中点击 Add 按钮，再添加一台智能隧道服务器。

**步骤 3** 输入要接受自动身份验证的服务器的主机名或 IP 地址：

- 如果选择 Hostname，请输入要接受自动身份验证的主机名或通配符掩码。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意单个字符。
  - 例如，输入 *.example.com。使用此选项避免配置出现 IP 地址动态变化。
- 如果选择 IP Address，请输入 IP 地址。

注释　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；您必须使用准确的主机名或 IP 地址。例如，在 Firefox 中，如果输入 *.cisco.com，将无法自动登录主机 email.cisco.com。

**步骤 4** Windows Domain（可选）- 如果身份验证需要，点击此选项即可将 Windows 域添加至用户名中。如果执行此操作，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 - 领域与网站的受保护区域关联，并且在身份验证期间通过身份验证提示或 HTTP 报头回传至浏览器。在此配置自动登录并指定领域字符串后，用户可以配置 Web 应用（例如 Outlook Web Access）的领域字符串，然后无需登录即可访问 Web 应用。

  使用内联网上网页的源代码中使用的地址格式。如果是为浏览器访问配置智能隧道自动登录，并且有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，如果网页上的链接所使用的格式与您指定的格式不同，则用户点击此链接时会出现故障。

  注释　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，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，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将其激活：

- 要将列表分配给组策略，请执行以下步骤：
  1. 依次导航至**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 组策略**，，然后打开组策略，
  2. 选择 Portal 选项卡，找到 Smart Tunnel 区域，然后从 Auto Sign-On Server List 属性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，请执行以下步骤：
  1. 依次选择**Configuration > Remote Access VPN > AAA/Local Users > Local Users**，然后编辑本地用户，分配自动登录服务器列表。
  2. 依次导航至 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 属性旁的下拉列表中选择服务器列表。

# 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。

如果启用智能隧道访问，用户必须使用无客户端 SSL VPN 门户页面上的**Application Access** > **Start Smart Tunnels**按钮将其手动启动。

# 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，也可以右键点击通知图标并确认注销。

注释 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浏览器时才应该使用通知图标。

## 配置在父进程终止时注销智能隧道

这种做法要求所有浏览器都关闭才表示注销。目前智能隧道寿命与启动进程寿命关联。例如，如果从 Internet Explorer 启动智能隧道，则没有 iexplore.exe 运行时就会关闭智能隧道。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。

注释 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。

## 配置使用通知图标注销智能隧道

您还可以选择关闭在父进程终止时注销，让会话在浏览器关闭后继续。对于这种做法，需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的会话状态更新。

注释 此图标是 SSL VPN 注销的备选方法。它不指示 VPN 会话状态。

过程

**步骤 1** 依次选择**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **门户** > **智能隧道**。

**步骤 2** 启用**点击智能隧道注销** > **系统托盘中的图标**单选按钮。

**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。

注释 如果右键点击此图标，系统将显示单菜单项，提示用户注销 SSL VPN。

# 无客户端 SSL VPN 捕获工具

无客户端 SSL VPN CLI 包含捕获工具，可用于记录通过 Web VPN 连接无法正确显示的网站的相关信息。此工具记录的数据可帮助思科客户支持代表排除问题。

无客户端 SSL VPN 捕获工具的输出包括两个文件：

- mangled.1、2、3、4……等，具体取决于网页活动。mangle 文件记录无客户端 SSL VPN 连接上传输这些页面的 VPN 集中器的 html 操作。
- original.1、2、3、4……等，具体取决于网页活动。original 文件是 URL 发送到 VPN 集中器的文件。

要通过捕获工具打开并查看文件输出，请转至 Administration | File Management。压缩输出文件并将其发送给思科支持代表。

**注释** 使用无客户端 SSL VPN 捕获工具不会影响 VPN 集中器性能。在生成输出文件后，请确保关闭捕获工具。

# 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，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。

**过程**

**步骤 1** 启动 ASDM，然后依次选择**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **门户** > **门户访问规则**。

系统将打开 Portal Access Rule 窗口。

**步骤 2** 点击**添加**，创建门户访问规则或选择现有的规则，然后点击**编辑** > 。

系统将打开 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*。建议在搜索字符串中使用通配符。如果不使用通配符，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预期。
- 如果字符串包含空格，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。

  除非您需要ASA匹配您向字符串添加的引号，否则请勿给带空格的字符串添加引号。例如，如果输入 `"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**应用**。

# 优化无客户端 SSL VPN 性能

ASA 提供多种优化无客户端 SSL VPN 性能和功能的方法。性能改进包括缓存和压缩 Web 对象。功能调整包括对内容转换和代理绕行的设置限制。APCF 提供调整内容转换的另一种方法。

## 配置内容转换

默认情况下，ASA 通过内容转换/重写引擎处理所有无客户端 SSL VPN 流量，此引擎包括 JavaScript 和 Java 等高级元素，用于代理根据用户是从 SSL VPN 设备内部还是独立于此设备来访问应用而采用不同语义和访问控制规则的 HTTP 流量。

某些 Web 资源需要高度个性化的处理。以下各节将介绍提供这类处理的功能。根据组织的要求和涉及的 Web 内容，您可以使用以下一种功能。

### 使用代理绕行

当应用和Web资源使用代理绕行提供的特殊内容重写效果更好时，可以将ASA配置为使用此功能。代理绕行是对原始内容更改最少的一种内容重写备选方法。此功能通常适用于自定义 Web 应用。

您可以配置多个代理绕行条目。配置这些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绕行规则。

如果使用端口而非路径掩码来配置代理绕行，则根据网络配置，可能需要更改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。要对所有 hr 站点使用代理绕行，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：

过程

**步骤 1** 依次导航至 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Proxy Bypass**。

**步骤 2** 为代理绕行选择 Interface 名称。

**步骤 3** 为代理绕行指定端口或 URI：

- Port -（单选按钮）点击即可将端口用于代理绕行。有效端口号是 20000 至 21000。
- “端口”（字段）- 输入 ASA 的高编号端口，以备用于代理绕行。
- Path Mask -（单选按钮）点击即可将 URL 用于代理绕行。
- Path Mask -（字段）输入代理绕行的 URL。可以包含正则表达式。

**步骤 4** 定义代理绕行的目标 URL：

- URL -（下拉列表）点击作为协议的 http 或 https。
- URL（文本字段）- 输入要应用代理绕行的 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 - 选中即重写 XML 内容。
- Hostname - 选中即重写链接。

第 17 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：

注释 确保已经为无客户端 SSL VPN 配置了 ASA。




# 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：

注释 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。

下表列出了无客户端 SSL VPN 用户可能需要知道的用户名和密码的类型。

**表 *13:* 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 | | 输入时间 |
|---|---|---|
| 计算机 | 访问计算机 | 启动计算机 |
| 互联网运营商 | 访问互联网 | 连接互联网运营商 |

| 登录用户名/密码类型 | | 输入时间 |
|---|---|---|
| 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 Web 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企业网络上的ASA之间数据传输的安全性。如果用户届时访问非HTTPS Web资源（位于互联网或内部网络上），则从企业ASA到目的Web服务器之间的通信不安全。

# 为使用无客户端 SSL VPN 功能配置远程系统

下表包括为使用无客户端 SSL VPN 而设置远程系统所涉及的任务、要求/必备条件和推荐用法：

您可能以不同的方式配置了用户账户，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，此表中的信息是按用户活动排列的。

表 *14:* 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：<br>• 家庭 DSL、电缆或拨号<br>• 公共信息亭<br>• 酒店联结线路<br>• 机场无线节点<br>• 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。<br>在 Microsoft Windows 上：<br>• Internet Explorer 8<br>• Firefox 8<br>在 Linux 上：<br>• Firefox 8<br>在 Mac OS X 上：<br>• Safari 5<br>• 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 | 采用以下格式的 HTTPS 地址：<br>https://address<br>其中，address 是启用了无客户端 SSL VPN 的 ASA（或负载均衡集群）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 | |

| 任务 | 远程系统或最终用户要求 | 规范或使用建议 |
| --- | --- | --- |
| | | 无客户端 SSL VPN 不支持从 Web 浏览器打印到网络打印机。不支持打印到本地打印机。 |
| 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 Web 连接，而不会干扰主浏览器窗口。<br>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。<br>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。<br>**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点击。） |

| 任务 | 远程系统或最终用户要求 | 规范或使用建议 |
|---|---|---|
| **Web 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，第 310 页”。 |
| | | 使用无客户端 SSL VPN 进行 Web 浏览时，用户可能会体验到不同于以往的外观和感受。例如：<br>• 无客户端 SSL VPN 标题栏显示在每个网页上方。<br>• 您可以通过以下方式访问网站：<br>  • 在无客户端 SSL VPN 主页的 Enter Web Address 字段中输入 URL。<br>  • 点击无客户端 SSL VPN 主页上的预配置网站链接。<br>  • 点击通过上述两种方法之一访问的网页上的链接。<br>  此外，根据您配置特定账户的方式，可能存在以下情况：<br>• 某些网站被阻止。<br>• 只有在无客户端 SSL VPN 主页上显示为链接的网站可用。 |
| **网络浏览和文件管理** | 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。 |

| 任务 | 远程系统或最终用户要求 | 规范或使用建议 |
|---|---|---|
| 使用应用<br>（称为端口转发或应用访问） | **注释** 在 Mac OS X 上，仅 Safari 浏览器支持此功能。 | |
| | **注释** 由于此功能需要安装 Oracle Java 运行时环境 (JRE) 和配置本地客户端，而且此操作需要本地系统的管理员权限，当用户从公共远程系统进行连接时，可能无法使用应用。 | |
| | 当用户结束使用应用时，始终应该通过点击**Close**图标关闭“应用访问”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 | 如果使用 DNS 名称指定服务器，用户必须具有计算机上的管理员权限，因为修改主机文件需要这一权限。 |
| | 已安装 Oracle Java 运行时环境 (JRE)。<br>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。<br>极少数情况下，端口转发小应用程序将出现故障，显示 Java 异常错误。如果出现这种情况，请执行以下操作：<br>**1.** 清除浏览器缓存并关闭浏览器。<br>**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。<br>**3.** 建立一个无客户端 SSL VPN 会话并启动端口转发 Java 小应用程序。 |

| 任务 | 远程系统或最终用户要求 | 规范或使用建议 |
|---|---|---|
| | 必要时，要配置客户端应用。<br>注释 Microsoft Outlook 客户端不需要执行此配置步骤。<br>所有非 Windows 客户端应用都要求此配置。<br>要查看 Windows 应用是否需要进行配置，请检查 Remote Server 的值。<br>• 如果 Remote Server 包含服务器主机名，不需要配置客户端应用。<br>• 如果 Remote Server 字段包含 IP 地址，则必须配置客户端应用。 | 如要配置客户端应用，请使用服务器的本地映射 IP 地址和端口号。如要查找此信息，请执行以下操作：<br>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。<br>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）。<br>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。 |
| | 注释 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。 | |
| 通过“应用访问”使用邮件 | 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。 |
| | 注释 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 版本 5.5 和 6.0。 |
| 通过 Web 访问使用邮件 | 已安装基于 Web 的邮件产品 | 支持的产品包括：<br>• Outlook Web Access<br>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。<br>• Lotus Notes<br>其他基于 Web 的邮件产品应该也可以正常工作，但我们尚未验证这一点。 |

| 任务 | 远程系统或最终用户要求 | 规范或使用建议 |
| --- | --- | --- |
| 通过邮件代理使用邮件 | 已安装支持 SSL 的邮件应用<br>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：<br>• Microsoft Outlook<br>• Microsoft Outlook Express 5.5 和 6.0 版本<br>其他支持 SSL 的邮件客户端应该也可以正常工作，但我们尚未验证这一点。 |
| | 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。此数据可帮助思科客户支持工程师排除问题。以下各节介绍如何使用 capture 命令：

- 创建捕获文件，第 316 页
- 使用浏览器显示捕获数据，第 317 页

**注释** 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

过程

**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*

- *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。

示例：

```
hostname# capture hr type webvpn user user2
```

**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

过程

**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*

- *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。

示例：

```
hostname# capture hr type webvpn user user2
```

**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**

捕获的内容以嗅探器格式显示。

**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 18 章

# 无客户端 SSL VPN 用户



## 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 为用户提供机会更改密码。如果当前密码尚未到期，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 服务器通信。

开始之前

- 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。
- 如果是使用 LDAP 目录服务器进行身份验证，则通过 Sun Java 系统目录服务器（以前称为 Sun ONE 目录服务器）和 Microsoft Active Directory 来支持密码管理。
  - 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。建议使用目录管理员或具有目录管理员权限的用户作为 DN。也可以将 ACI 放入默认密码策略。
  - Microsoft - 必须配置 SSL 上的 LDAP 以对 Microsoft Active Directory 启用密码管理。
- 某些支持 MSCHAP 的 RADIUS 服务器当前不支持 MSCHAPv2。此命令需要 MSCHAPv2，因此，请与供应商联系。
- 对于 Kerberos/Active Directory（Windows 密码）或 NT 4.0 域，所有这些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。

过程

**步骤 1** 依次导航至 **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。

# 对无客户端 SSL VPN 使用单点登录

## 使用 SAML 2.0 的 SSO

### 关于 SSO 和 SAML 2.0

ASA 支持 SAML 2.0，因此当无客户端 VPN 最终用户在无客户端 VPN 与专用网络外部其他 SAAS 应用之间切换时，只能输入一次凭证。

例如，某企业客户已启用 PingIdentity 作为其 SAML 身份提供程序 (IdP) 并且具有已启用了 SAML 2.0 SSO 的 Rally、Salesforce、Oracle OEM、Microsoft ADFS、onelogin 或 Dropbox 账户。当您将 ASA 配置为支持 SAML 2.0 SSO 作为服务提供程序 (SP) 时，最终用户能够登录一次，并有权访问包括无客户端 VPN 在内的所有这些服务。

此外还增加了 AnyConnect SAML 支持，因此 AnyConnect 4.4 客户端可以使用 SAML 2.0 访问基于 SAAS 的应用。AnyConnect 4.6 引入了一个增强版的与嵌入浏览器的 SAML 集成，以替换以前版本中的本机（外部）浏览器集成。具有嵌入式浏览器的全新增强版本要求升级到 AnyConnect 4.6（或更高版本）和 ASA 9.7.1.24（或更高版本）、9.8.2.28（或更高版本）或 9.9.2.1（或更高版本）。

当 SAML 配置为隧道组、默认隧道组或任何其他项目的身份验证方法时，ASA 将支持 SP 。无客户端 VPN 最终用户通过访问启用的 ASA 或 SAML IdP 来启动单点登录。下文介绍了上述每种场景。

### SAML SP 发起的 SSO

当最终用户使用无客户端 VPN 访问 ASA 来发起登录时，登录行为的过程如下所示：

1. 当无客户端 VPN 最终用户访问或选择已启用 SAML 的隧道组时，最终用户会被重定向至 SAML IdP进行身份验证。用户将收到提示，除非用户直接访问组URL（在此情况下为无提示重定向）。

   ASA 将生成一个 SAML 身份验证请求，由浏览器将该请求重定向至 SAML IdP。
2. IdP 向最终用户质询凭证，然后最终用户登录。输入的凭证必须满足 IdP 身份验证配置的要求。
3. IdP 响应被发送回浏览器并发布到 ASA 登录 URL。ASA 验证响应以完成登录。

### SAML IdP 发起的 SSL

当用户通过访问 IdP 来发起登录时，登录行为的过程如下所示：

1. 最终用户访问 IdP。IdP 根据 IdP 的身份验证配置向最终用户质询凭证。最终用户提交凭证并登录 IdP。
2. 一般情况下，最终用户会获得 IdP 已配置的启用 SAML 的服务列表。最终用户选择 ASA。
3. SAML 响应被发送回浏览器并发布到 ASA 登录 URL。ASA 验证响应以完成登录。

### 信任圈

ASA 与 SAML 身份提供程序之间的信任关系通过配置的证书建立（ASA 信任点）。

最终用户与 SAML 身份提供程序之间的信任关系通过 IdP 上配置的身份验证建立。

### SAML 超时

SAML 断言中有 NotBefore 和 NotOnOrAfter，如下所示：<saml:Conditions NotBefore="2015-03-10T19:47:41Z" NotOnOrAfter="2015-03-10T20:47:41Z">

如果 NotBefore 与 ASA 上配置的 SAML 超时之和早于 NotOnOrAfter，则 SAML 超时将覆盖 NotOnOrAfter。如果 NotBefore + 超时晚于 NotOnOrAfter，则 NotOnOrAfter 将生效。

超时应该非常短，以防超时后重新使用断言。为了使用 SAML 功能，必须使您的 ASA 网络时间协议 (NTP) 服务器与 IdP NTP 服务器同步。

### 专用网络中的支持

在专用网络中支持基于 SAML 2.0 的服务提供商 IdP。在私有云中部署 SAML IdP 时，ASA 和其他启用 SAML 的服务处于对等位置，并且都在专用网络中。使用 ASA 作为用户与服务之间的网关，可

利用受限的匿名 webvpn 会话来处理 IdP 上的身份验证，并转换 IdP 与用户之间的所有流量。当用户登录时，ASA 会使用相应的属性修改会话并存储 IdP 会话。然后，您可以使用专用网络中的服务提供程序而无需再次输入凭证。

SAML IdP *NameID* 属性确定用户的用户名，并且用于授权、记账和 VPN 会话数据库。

注释 您不能在专用网络和公共网络之间交换身份验证信息。如果将相同的 IdP 同时用于内部和外部服务提供程序，必须分别进行身份验证。仅内部 IdP 无法用于外部服务：仅外部 IdP 无法用于专用网络中的服务提供程序。

## SAML 2.0 的准则和限制

- SAML 2.0 SSO 支持是一项无客户端 VPN 功能，因此其限制和允许的功能与无客户端 VPN 相同，例如：
  - 不支持多情景模式和负载均衡。
  - 支持主用/备用故障切换，不支持主用/主用故障切换。
  - 支持 IPv4 和 IPv6 会话。
- ASA 支持 SAML 2.0 重定向-POST 绑定，所有 SAML IdP 也支持此功能。
- ASA 仅用作 SAML SP。在网关模式或对等模式下，它不能用作身份提供程序。
- 此 SAML SSO SP 功能是互斥的身份验证方法。它不能与 AAA 和证书一起使用。
- 不支持基于用户名/密码身份验证、证书身份验证和 KCD 的功能。例如，用户名/密码预填充功能、基于表单的自动登录、基于宏替换的自动登录、KCD SSO 等。
- 启用 SAML 的隧道组不支持 DAP。
- 现有无客户端 VPN 超时设置仍适用于 SAML 会话。
- ASA 管理员需要确保 ASA 与 SAML IdP 之间的时钟同步，从而正确处理身份验证断言并确保正确的超时行为。
- ASA 管理员有责任在 ASA 和 IdP 上维护有效的签名证书，并考虑以下因素：
  - 在 ASA 上配置 IdP 时，必须配置 IdP 签名证书。
  - ASA 不会对从 IdP 接收的签名证书执行吊销检查。
- SAML 断言中有 NotBefore 和 NotOnOrAfter 条件。ASA SAML 配置的**超时**与这两个条件如下交互：
  - 如果 NotBefore 与超时之和早于 NotOnOrAfter，则超时将覆盖 NotOnOrAfter。
  - 如果 NotBefore + 超时晚于 NotOnOrAfter，则 NotOnOrAfter 生效。

- 如果不存在 NotBefore 属性，ASA 将拒绝登录请求。如果不存在 NotOnOrAfter 属性且未设置 SAML 超时，ASA 将拒绝登录请求。

- 将 SAML 与 AnyConnect 配合使用时，还需遵守以下准则
  - 在嵌入式浏览器中不允许不受信任的服务器证书。
  - CLI 或 SBL 模式中不支持嵌入式浏览器 SAML 集成。
  - 在 Web 浏览器中建立的 SAML 身份验证不会与 AnyConnect 共享，反之亦然。
  - 根据具体配置，在使用嵌入式浏览器连接到前端时，会使用各种不同的方法。例如，尽管 AnyConnect 相比于 IPv6 连接更喜欢 IPv4 连接，但嵌入式浏览器可能更喜欢 IPv6，或反之亦然。同样，在尝试代理和收到失败后，AnyConnect 可能会回退到没有代理状态，而嵌入式浏览器在尝试代理并收到失败后可能会停止导航。
  - 为了使用 SAML 功能，必须使您的 ASA 网络时间协议 (NTP) 服务器与 IdP NTP 服务器同步。
  - ASDM 上的 VPN 向导目前不支持 SAML 配置。
  - 使用内部 IdP 登录后，您将无法访问包含 SSO 的内部服务器。
  - SAML IdP NameID 属性确定用户的用户名，并且用于授权、记账和 VPN 会话数据库。

## 配置 SAML 2.0 身份提供程序 (IdP)

### 开始之前

获取 SAML (IdP) 提供程序的登录和注销 URL。您可以从提供商的网站获取这些 URL，或者，他们可能会在元数据文件中提供该信息。

### 过程

**步骤 1** （可选）要设置确定 IdP　是内部网络的标志，请使用 **internal** 命令。然后，ASA 将在网关模式下工作。

**步骤 2** 使用 **forceauthn** 使身份提供程序在收到 SAML 身份验证请求时直接进行身份验证而不依赖于以前的安全情景。此设置为默认值；因此，要将其禁用，请使用 **no forceauthn**。

**步骤 3** 在 ASDM 中，依次转到**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 高级 > 单点登录服务器**

任何以前配置的 SAML 2.0 IdP 都列于此处，您可以如旁边所述进行**编辑**，以**添加**或**删除** IdP。

**步骤 4** 点击**添加**，添加新 IdP 实体。

**步骤 5** 按照下面的说明，填写以下字段。

- **登录 URL** - 用于登录 IdP 的 URL。URL 值必须包含 4 到 500 个字符。
- **注销 URL** -（可选）在注销 IdP 时用于重定向的 URL。URL 值必须包含 4 到 500 个字符。

- **基本 URL** -（可选）向第三方 IdP 提供 URL，用于将最终用户重定向回 ASA。

  如果配置了 base-url，则将其用作 **show saml metadata** 中 AssertionConsumerService 和 SingleLogoutService 属性的基本 URL。

  如果未配置 base-url，则由 ASA 的 hostname 和 domain-name 决定 URL。例如，当 hostname 为 `ssl-vpn` 且 domain-name 为 `cisco.com` 时，我们使用 `https://ssl-vpn.cisco.com`。

  如果输入 **show saml metadata** 时既未配置 base-url 也未配置 hostname/domain-name，则会出现错误。

- **身份提供程序证书** - 指定包含供 ASA 用于验证 SAML 断言的 IdP 证书的信任点。选择以前配置的信任点。
- **服务提供程序证书** -（可选）指定包含供 IdP 用于验证 ASA 签名或加密 SAML 断言的 ASA (SP) 证书的信任点。选择以前配置的信任点。
- **请求签名** - 使用下拉列表为 SAML IdP 服务器选择首选签名方法。可以选择 rsa-sha1、rsa-sha256、rsa-sha384 或 rsa-sha512。
- **请求超时** -（可选）SAML 请求的超时。

  如果指定，则在 NotBefore 和 timeout-in-seconds 之和早于 NotOnOrAfter 的情况下，此配置会覆盖 NotOnOrAfter。

  如果不指定，则断言中的 NotBefore 和 NotOnOrAfter 用于确定有效性。

- **启用签名** - 在 SAML 请求中启用或禁用（默认设置）签名。
- **启用内部** - 启用或禁用（默认设置）以确定 IdP 是否为　内部网络。

  **注释**　　使用内部 IdP 登录后，您将无法访问包含 SSO 的内部服务器。

- “启用强制重新身份验证”- 收到 SAML 身份验证请求时，启用此设置会导致身份提供程序直接进行身份验证而不依赖于以前的安全情景。“启用强制重新身份验证”是默认值。

**步骤 6** 点击**确定**。
此页面上将列出新的 IdP 实体。

---

**示例**

以下网页显示了如何获取 Onelogin 的 URL 的示例

https://onelogin.zendesk.com/hc/en-us/articles/202767260-Configuring-SAML-for-Clarizen

以下网页是如何使用元数据从 OneLogin 查找 URL 的示例。

http://onlinehelp.tableau.com/current/online/en-us/saml_config_onelogin.htm

### 下一步做什么

如将 ASA 配置为 SAML 2.0 服务提供程序 (SP)，第 325 页中所述，将 SAML 身份验证应用于连接配置文件。

## 将 ASA 配置为 SAML 2.0 服务提供程序 (SP)

按照以下程序将特定隧道组配置为 SAML SP。

注释 如果将 SAML 身份验证用于 AnyConnect 4.4 或 4.5 并且部署了 ASA 版本 9.7.1.24（或更高版本）、9.8.2.28（或更高版本）或 9.9.2.1（或更高版本）（发布日期：2018 年 4 月 18 日），默认的 SAML 行为是 AnyConnect 4.4 和 4.5 上不支持的嵌入式浏览器。因此，您必须选中“连接配置文件”区域中的 **SAML 外部浏览器**复选框，以便 AnyConnect 4.4 和 4.5 客户端使用外部（本地）浏览器进行 SAML 身份验证。

**SAML 外部浏览器**复选框供升级到 AnyConnect 4.6 或更高版本的用户用于迁移。由于安全限制，只能将此解决方案用作 AnyConnect 软件升级时的临时迁移的一部分。该复选框本身今后作用不大。

### 过程

**步骤 1** 在 ASDM 中，依次转到**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 连接配置文件 > 添加/编辑**。

**步骤 2** 选择 **Saml** 作为此隧道组的**身份验证方法**。

**步骤 3** 在 **SAML 身份提供程序**部分中，选择以前配置的 **SAML 服务器**，或者点击**管理**添加新服务器。
如果修改现有 SAML 配置，此操作将为隧道组重新启用 IdP。

**步骤 4** 点击**确定**。
系统将显示“预览 CLI 命令”窗口，告诉您根据您接受的更改生成了哪些 CLI 命令。然后，您可以点击**发送**将命令发送至 ASA。

# 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特定身份验证方法。可以将 ASA 配置为会对以下身份验证方法作出响应：基本 (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 的程序。

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。

### 开始之前

- 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 的登录凭证，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。

### 过程

**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。

# 用户名和密码的要求

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。下表列出了无客户端 SSL VPN 用户可能需要知道的用户名和密码的类型：

| 登录用户名/密码类型 | | 输入时间 |
|---|---|---|
| 计算机 | 访问计算机 | 启动计算机 |
| 互联网运营商 | 访问互联网 | 连接互联网运营商 |
| 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 Web 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PC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。如果用户届时访问非HTTPS Web资源（位于互联网或内部网络上），从企业ASA到目的Web服务器之间的通信不是专用的，因为它未加密。

# 为使用无客户端 SSL VPN 功能配置远程系统

本节介绍如何为使用无客户端 SSL VPN 设置远程系统。


- 关于无客户端 SSL VPN，第 328 页
- 无客户端 SSL VPN 的必备条件，第 328 页
- 使用无客户端 SSL VPN 浮动工具栏，第 329 页
- 浏览 Web，第 329 页

- 浏览网络（文件管理），第 330 页
- 使用端口转发，第 331 页
- 通过端口转发使用邮件，第 332 页
- 通过 Web 访问使用邮件，第 332 页
- 通过邮件代理使用邮件，第 333 页
- 使用智能隧道，第 333 页

可采用不同的方式配置各个用户账户，以使每个用户可以使用不同的无客户端 SSL VPN 功能。

# 关于无客户端 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。

注释 有关无客户端 SSL VPN 支持的 Web 浏览器的列表，请参阅支持的 VPN 平台，Cisco ASA 5500 系列。

# 无客户端 SSL VPN 的必备条件

- 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（或负载均衡集群）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。

注释 无客户端 SSL VPN 支持本地打印，但不支持通过 VPN 连接到企业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 Web 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，右键点击操作不可用。）

**注释** 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 Web

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，第 327 页。

使用无客户端 SSL VPN 进行 Web 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。
- 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
  - 需要有受保护网站的用户名和密码

根据特定账户的配置方式，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

此外，根据特定账户的配置方式，还可能存在以下情况：

- 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。

注释 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。

重要提示：

- 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。

注释 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 Web 浏览器浏览企业网络。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应用程序，在文件夹树视图中显示远程文件系统。

注释 要使用此功能，用户计算机上需要安装 Oracle Java 运行时环境 (JRE)，还需要在 Web 浏览器中启用 Java。启动远程文件需要 JRE 1.6 或更高版本。

此浏览器使用户可以：

- 浏览远程文件系统。
- 重命名文件。
- 在远程文件系统中以及远程文件系统与本地文件系统之间移动或复制文件。
- 执行文件批量上传和下载。

  下载文件的具体操作如下：在浏览器中点击要下载的文件，依次选择 Operations > Download，然后在 Save 对话框中提供用于保存文件的位置和名称。

  上传文件的具体操作如下：点击目标文件夹，依次选择 Operations > Upload，然后在 Open 对话框中提供文件的位置和名称。

  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

要使用端口转发，必须使用服务器的本地映射 IP 地址和端口号配置客户端应用。

- 当用户结束使用应用时，始终应该通过点击**Close**图标关闭“应用访问”窗口。不正确退出窗口可能会导致 Application Access 或应用本身关闭。

### 开始之前

- 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，必须具有计算机上的管理员权限，因为修改主机文件需要这一权限。
- 必须已安装 Oracle Java 运行时环境 (JRE)。

  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，端口转发小应用程序将出现故障，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。
  3. 结束 Java 的所有实例。
  4. 建立一个无客户端 SSL VPN 会话并启动端口转发 Java 小应用程序。

- 必须已在浏览器上启用了 JavaScript。默认情况下，JavaScript 已启用。
- 如有需要，必须配置客户端应用。

注释 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。

过程

**步骤 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。

**步骤 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）。

**步骤 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。

注释 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 Application Access。这样即可使用邮件客户端。

注释 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。

必须满足应用访问及其他邮件客户端的要求。

我们测试了 Microsoft Outlook Express 5.5 和 6.0 版本。

# 通过 Web 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

注释 您必须安装基于 Web 的邮件产品，并且其他基于 Web 的邮件应用也应该可以正常工作，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，请参阅在无客户端 SSL VPN 上使用邮件，第 282 页。

### 准备工作

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。

其他支持 SSL 的客户端应该也可以正常工作，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。

注释 与使用端口转发时不同，使用智能隧道时不会自动下载 Java。

- 智能隧道要求 Windows 上必须安装 ActiveX 或 JRE，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。
- Mac OS X 不支持前端代理。
- 仅使用支持的操作系统和浏览器。
- 仅支持基于 TCP 套接字的应用。

第 19 章

# 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：

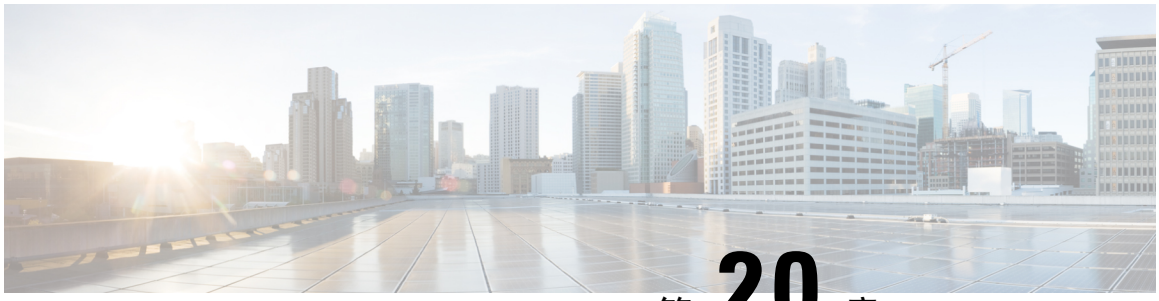
- HP iPaq H4150
- Pocket PC 2003
- Windows CE 4.20.0，内部版本 14053
- Pocket Internet Explorer (PIE)
- ROM 版本 1.10.03ENG
- ROM 日期：7/16/2004

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 门户页面上不包含 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 不会断开与无客户端 SSL VPN 或使用 HTTPS 的任何安全网站的连接。

# 将无客户端 SSL VPN 用于移动设备的限制

- 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）。



第 20 章

# 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于连接配置文件或组策略中的自定义对象。

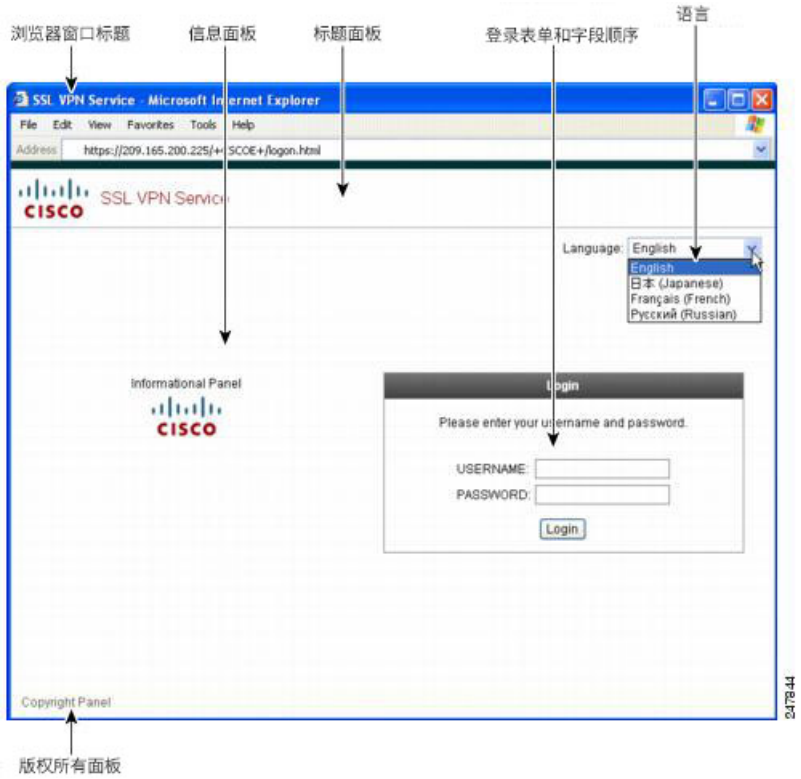
您也可以不自定义登录页面的预定义组件，而是创建自己的页面并将其导入到ASA中进行完全自定义。

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

下图显示您可以自定义的登录页面和预定义组件：

图 *10:* 无客户端登录页面组件




要自定义登录页面的所有组件，请执行以下程序。您可以点击 **Preview** 按钮，预览您对每个组件的更改：

## 过程

**步骤 1** 指定要自定义的预定义组件。转至**登录页面**并选择**自定义预定义登录页面组件**。为浏览器窗口指定标题。

**步骤 2** 显示并自定义标题面板。依次转至**登录页面 > 标题面板**，然后选中**显示标题面板**。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。依次转至**登录页面 > 语言**，然后选中**启用语言选择器**。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。

用户名和密码字段的标签将根据用户所选的语言发生变化。

**步骤 4** 自定义登录表单。依次转至**登录页面 > 登录表单**。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。依次转至**登录页面 > 表单字段顺序**。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。依次转至**登录页面 > 信息面板**，然后选中**显示信息面板**。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。依次转至**登录页面 > 版权面板**，然后选中“显示版权面板”。添加要用于版权声明显示的文本。

**步骤 8** 点击**确定**，然后将更改应用到您编辑的自定义对象上。

### 下一步做什么

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

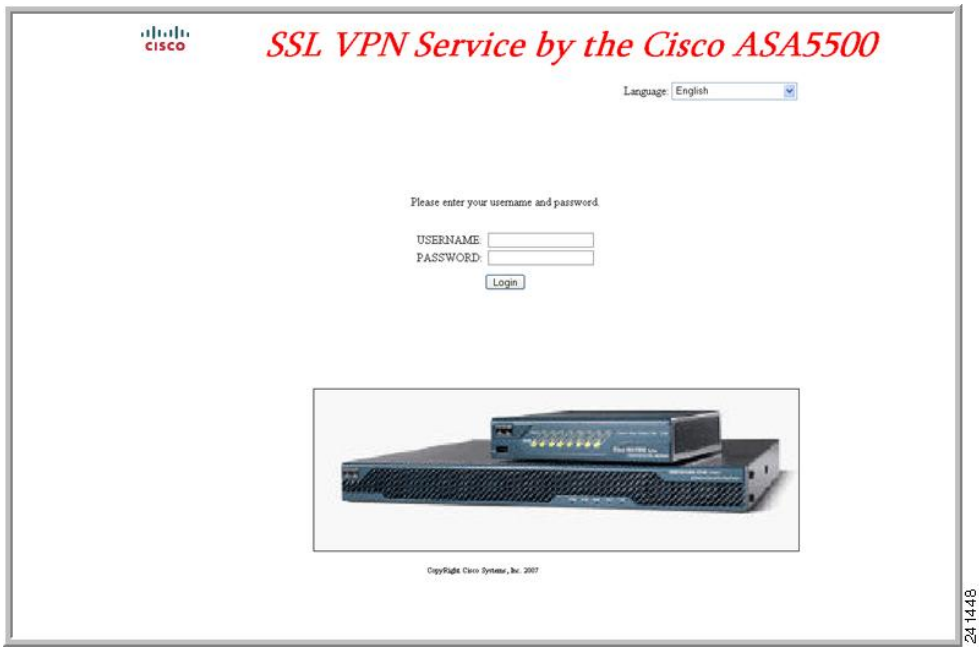
如果您希望使用自己的自定义登录屏幕，而不是更改我们所提供的登录页面的特定组件，您可以使用“完全自定义”功能，进行高级自定义。

利用“完全自定义”功能，您可以为自己的登录屏幕提供 HTML，并插入思科 HTML 代码来调用 ASA 上用于创建登录表单和语言选择器下拉列表的函数。

要配置 ASA 以使用您的代码，您需要修改 HTML 代码并完成相关任务，本文档对此进行了描述。

下图显示“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 *11:*** 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=UTF-8">
```

```
<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。

### 过程

**步骤 1** 将您的文件命名为 logon.inc。当您导入文件时，ASA 会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

**过程**

**步骤 1** 转至 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**目的**区域，对“访问其内容需要身份验证”选择“否”。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

**过程**

**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“编辑自定义对象”窗口，点击**常规**，然后为所需连接配置文件和/或组策略启用自定义对象。

# 无客户端 SSL VPN 最终用户设置

本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://*address* 的格式输入 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

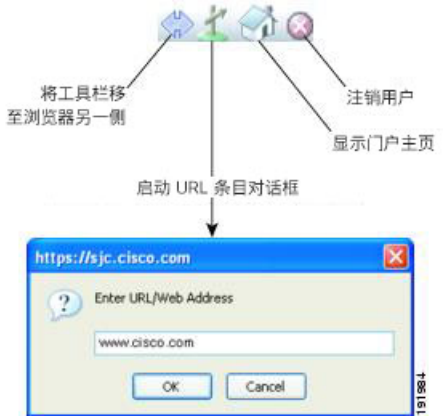
要启动端口转发或智能隧道，用户可点击 Application Access 框中的 **Go** 按钮。系统将显示 Application Access 窗口，然后将显示为此无客户端 SSL VPN 连接配置的 TCP 应用。要在此面板打开的情况下使用某应用，用户可以按照正常方式启动该应用。

**注释** 状态故障切换将不保留使用 Application Access 建立的会话。用户在故障切换后必须重新连接。

### 查看浮动工具栏

下图中显示的浮动工具栏显示当前无客户端 SSL VPN 会话。

图 *12:* 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Web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。自定义对象使用 XML 文件进行编译，该文件包含向远程用户显示的所有可自定义屏幕项的XML标签。ASA软件包含可以导出到远程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，用作新的自定义对象。

导出定制对象时，会在指定的 URL 创建一个包含 XML 标记的 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。此对象无法更改或从缓存中删除，但可以导出、编辑再重新导入到 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。

```
<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>(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>
```

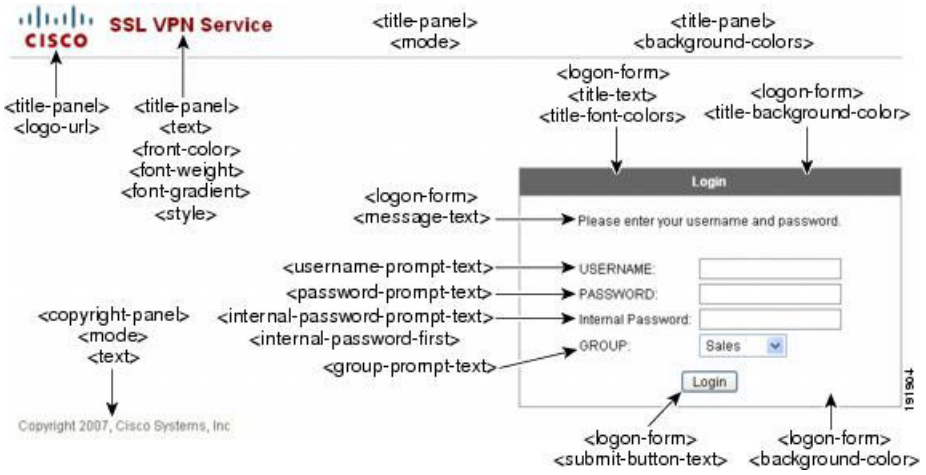
```
          <username-prompt-text l10n="yes"><![CDATA[USERNAME:</username-prompt-text>
          <password-prompt-text l10n="yes"><![CDATA[PASSWORD:</password-prompt-text>
          <internal-password-prompt-text l10n="yes">Internal
Password:</internal-password-prompt-text>
          <internal-password-first>no</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>
   <username-prompt-text l10n="yes"></username-prompt-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>
```

下图显示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 *13:* 登录页面和关联的 ***XML*** 标签

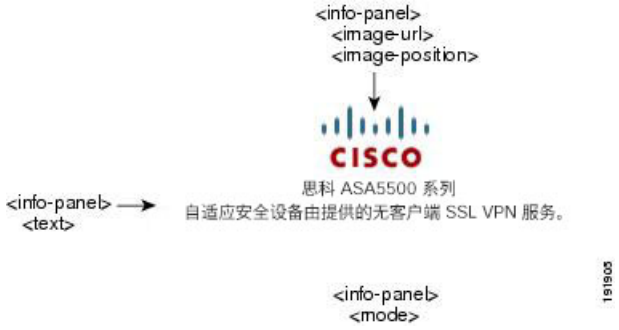


下图显示在登录页面上可用的语言选择器下拉列表以及用于自定义此功能的 XML 标签。所有这些标签都嵌套于更高级别的 <auth-page> 标签中。

图 *14:* 登录屏幕上的语言选择器和关联的 *XML* 标签

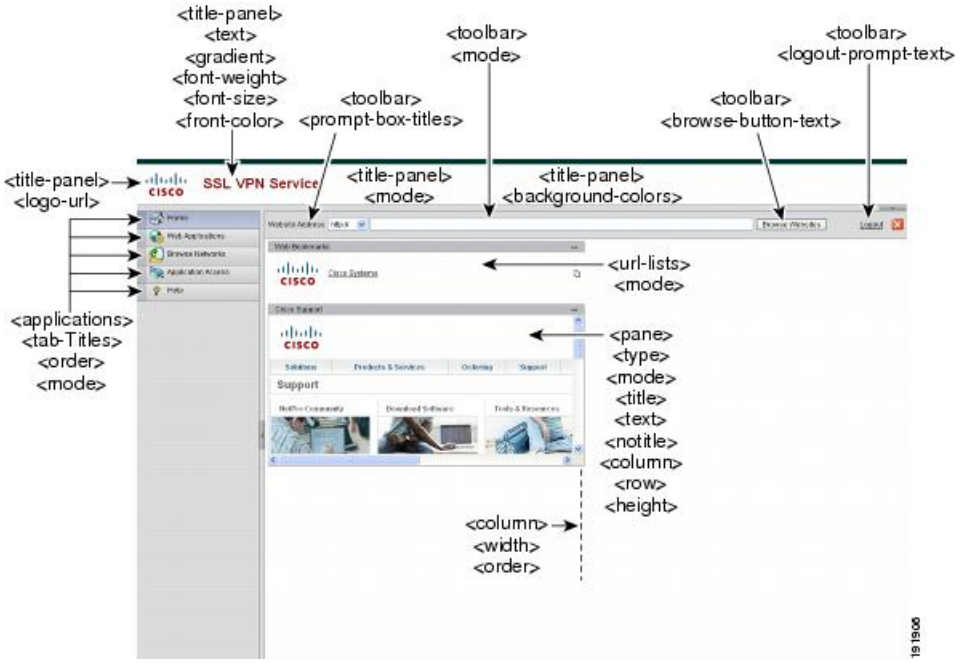

下图显示在登录页面上可用的信息面板以及用于自定义此功能的 XML 标签。此信息可显示在登录框的左侧或右侧。这些标签都嵌套于更高级别的 <auth-page> 标签中。

图 *15:* 登录屏幕上的信息面板和关联的 *XML* 标签




下图显示用于自定义此功能的门户页面和 XML 标签。这些标签都嵌套于更高级别的 <auth-page> 标签中。

图 *16:* 门户页面和关联的 *XML* 标签




# 登录屏幕高级自定义

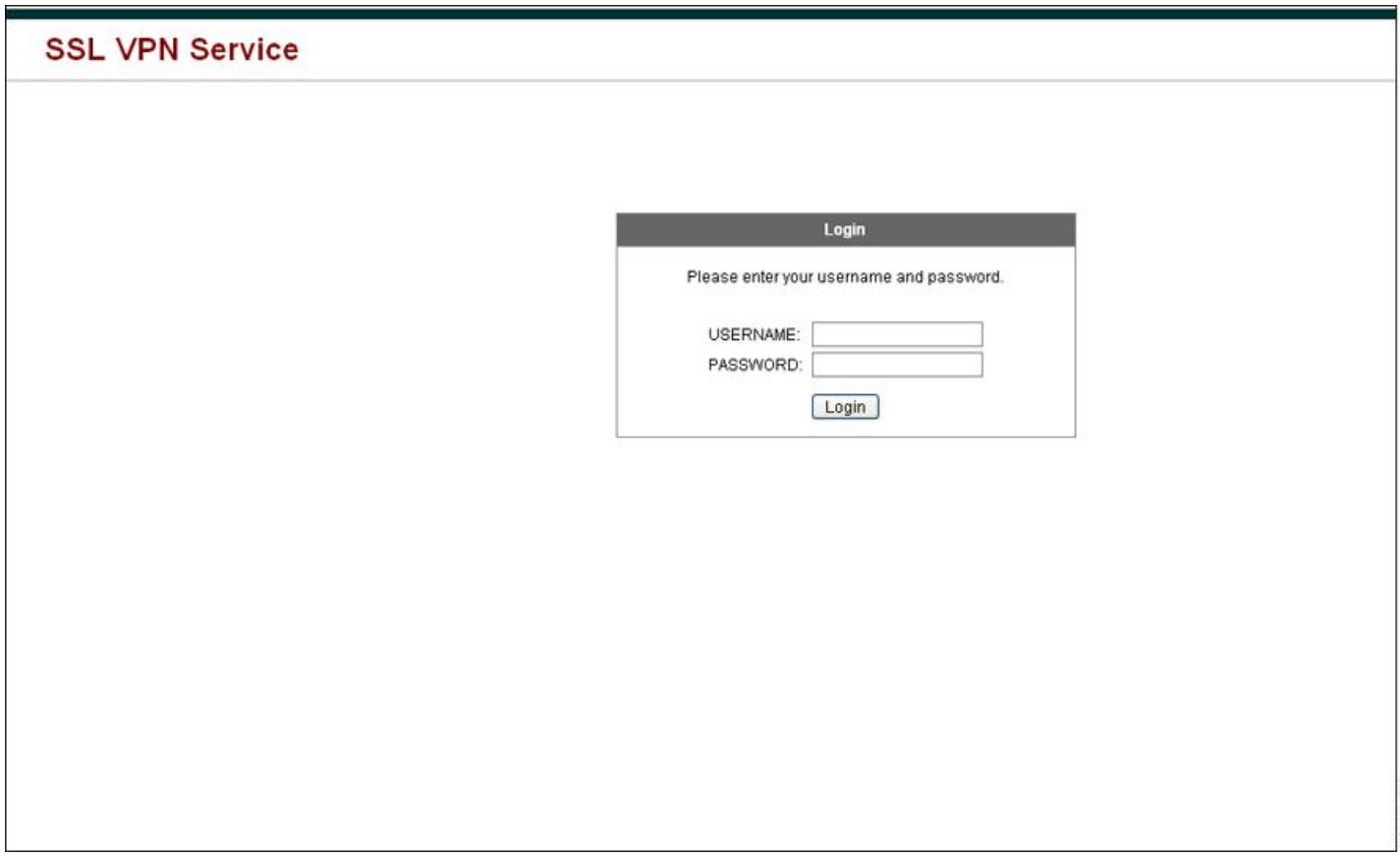
如果您希望使用自己的自定义登录屏幕，而不是更改我们所提供的登录页面的特定屏幕元素，您可以使用“Full Customization”功能执行此高级自定义。

利用“完全自定义”功能，您可以为自己的登录屏幕提供 HTML，并插入思科 HTML 代码来调用 ASA 上用于创建登录表单和语言选择器下拉列表的函数。

要配置 ASA 以使用您的代码，您需要修改 HTML 代码并完成相关任务，本节对此进行了描述。

下图显示向无客户端 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:* 标准思科登录页面

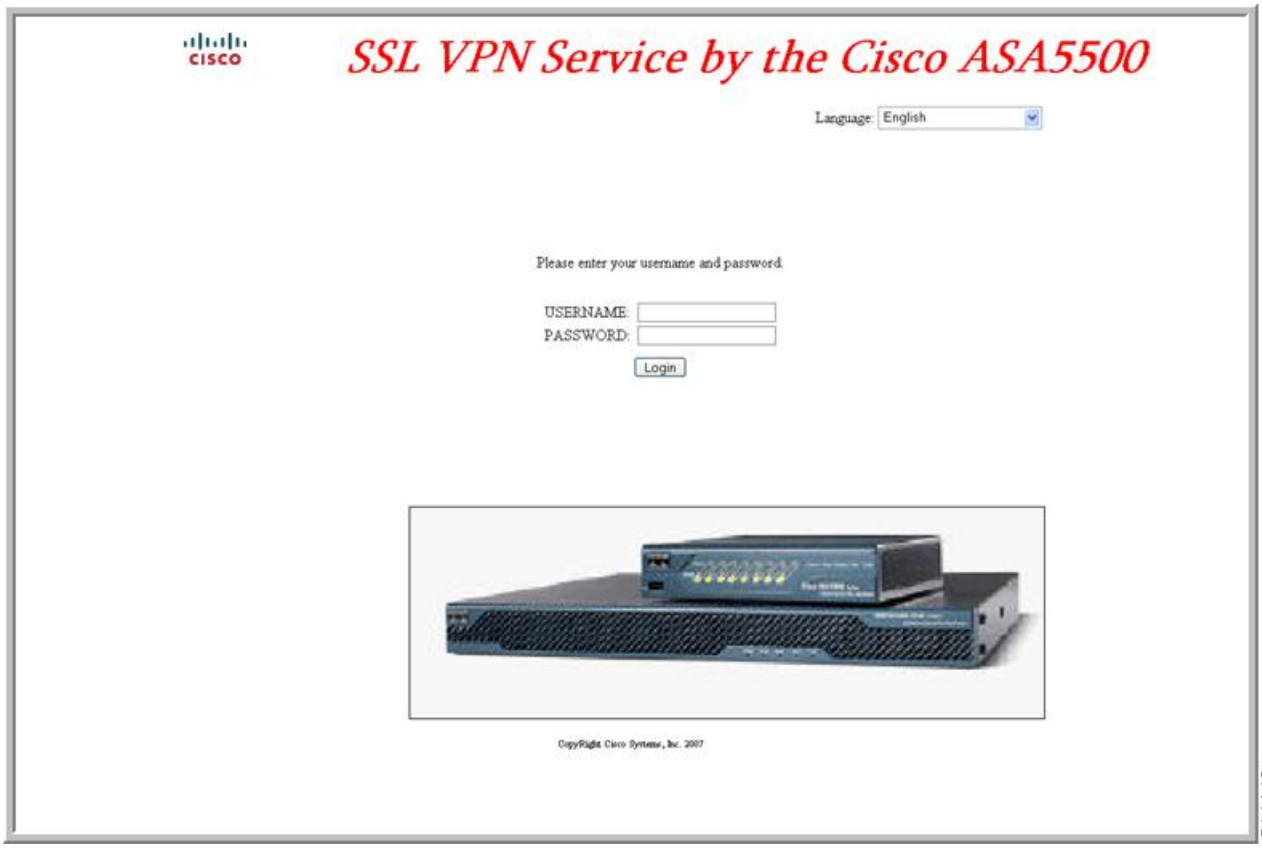



下图显示语言选择器下拉列表。此功能是无客户端 SSL VPN 用户的一个选项，也是由登录屏幕的 HTML 代码中的函数调用。

图 *18:* 语言选择器下拉列表


下图显示“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 *19:* 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：

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<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

过程

**步骤 1** 将您的文件命名为 logon.inc。当您导入文件时，ASA 会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

下图显示您可以自定义的门户页面和预定义组件：

**图 *20:*** 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，请执行以下程序。您可以点击“预览”按钮，预览您对每个组件的更改。

**过程**

**步骤 1** 依次选择**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **门户** > **自定义**。

**步骤 2** 点击**添加**。

**步骤 3** 在**自定义对象名称**字段中，输入自定义的名称。

**步骤 4** 在左侧窗格中，点击**门户页面**。

**步骤 5** 在**浏览器窗口标题**字段中输入标题。

**步骤 6** 要显示并自定义标题面板，请点击**标题面板**，然后选中**显示标题面板**复选框。输入要作为标题显示的文本并指定徽标。您还可以指定任意字体样式。

**步骤 7** 要启用和自定义工具栏，请点击**工具栏**，然后选中**显示工具栏**复选框。根据需要自定义**提示框标题**、**浏览按钮文本**和**注销提示**。

启用工具栏还会显示用于登录的用户名。**用户名**字段必须包含**用户名**作为有效的关键字。

**步骤 8** 要自定义应用列表，请点击**应用**，然后选中**显示导航面板**复选框。ASA 配置中启用的应用将显示于一个表中，其中包括客户端-服务器插件和端口转发应用。根据需要启用或禁用此表中的这些应用程序。

**步骤 9** 要在门户页面空间中创建自定义窗格，请点击**自定义窗格**。配置列数和列宽。根据需要创建自定义窗格，并为文本、图像、RSS 源或 HTML 页面将窗口分为相应数量的行和列。

**步骤 10** 要指定主页 URL，请点击**主页** ，然后选中**启用自定义内网网页**复选框。选择定义书签组织方式的书签模式。

**步骤 11** 点击**超时警报**，配置超时警报消息和工具提示。

**步骤 12** 点击**确定**。

### 下一步做什么

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。默认消息是“您的会话将于 **%s** 内到期。” 消息中的 `%s` 占位符将替换为滴答作响的倒计时计时器。

### 过程

**步骤 1** 启动 ASDM 并依次选择**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **门户** > **自定义**。

**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：警告：您的会话将于 `%s` 内结束。`Please complete your work and prepare to close your applications.`

**步骤 6** 点击 **OK**。

**步骤 7** 点击**应用**。

# 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。

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

下图显示您可以自定义的注销页面：

**图 *21:* 注销页面的组件**


要自定义注销页面，请执行以下程序。您可以点击 Preview 按钮，预览您对每个组件的更改：

**过程**

**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

**过程**

**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**查找**，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** 在登录期间点击门户页面的“密码”字段时，屏幕键盘会启用键盘。“用户名”框不会启用键盘。您可以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。

**过程**

**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。
- “闪存文件系统”- 选择此方法可导出位于 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。
- “远程服务器”- 选择此选项可导入可以从 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

下图显示 XML 自定义对象的文件结构。

注释 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 *15:* 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 | enable\|disable | disable | - |
| 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 | enable\|disable | disable | - |
| 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 | enable\|disable | disable | - |
| image-position | 字符串 | above\|below | above | 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 | Logon | - |

| | | | | |
|---|---|---|---|---|
| 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 | Username | - |
| password-prompt-text | 字符串 | 任意字符串 | Password | - |
| internal-password-prompt-text | 字符串 | 任意字符串 | Internal Password | - |
| group-prompt-text | 字符串 | 任意字符串 | Group | - |
| submit-button-text | 字符串 | 任意字符串 | Logon | |
| 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 | Logout | — |
| 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 | Login | |
| 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 | enable\|disable | disable | - |
| title | 文本 | - | Language | 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 | enable\|disable | Disable | - |
| 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 | enable\|disable | enable | - |
| application | 节点（多个） | - | 不适用 | 此节点更改已配置的（按照 id）应用的默认设置 |
| id | 字符串 | 对于库存应用<br>web-access<br>file-access<br>app-access<br>net-access<br>help<br>对于 ins：<br>唯一插件 | 不适用 | — |
| tab-title | 字符串 | — | 不适用 | — |
| order | 数字 | — | 不适用 | 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 | — | 不适用 | 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 | enable\|disable | 不适用 | v |
| toolbar | 节点 | — | — | — |

| | | | | |
|---|---|---|---|---|
| mode | 字符串 | enable\|disable | Enable | — |
| prompt-box-title | 字符串 | 任意字符串 | Address | URL 提示列表的标题 |
| browse-button-text | 字符串 | 任意字符串 | Browse | 浏览按钮文本 |
| logout-prompt-text | 字符串 | 任意字符串 | Logout | — |
| column | 节点（多个） | — | — | 默认情况下将显示一列 |
| width | 字符串 | — | 不适用 | — |
| order | 数字 | — | 不适用 | 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 URL 列表将被视为门户主页上的默认元素。 |
| mode | 字符串 | group \| nogroup | group | 模式：<br>group - 按照应用类型对元素分组（例如 Web 书签、文件书签）<br>no-group - 在单独窗格中显示 URL 列表<br>disable - 默认情况下不显示 URL 列表 |
| panel | 节点<br>(多个) | — | — | 允许配置额外的窗格 |
| mode | 字符串 | enable\|disable | - | 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：<br>RSS<br>IMAGE<br>TEXT<br>HTML |
| url | 字符串 | — | — | RSS、IMAGE 或 HTML 类型窗格的 URL |
| url-mode | 字符串 | — | — | 模式：改变、不改变 |
| text | 字符串 | — | — | TEXT 类型窗格的文本 |
| column | 数字 | — | — | — |

# 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 Web 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

自定义模板名为 Template，包含当前所用的所有标签以及说明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#
```

无法更改或删除文件 Template。像本例中一样，将其导出时，会保存为新名称 default.xml。通过更改此文件创建符合组织需求的自定义对象后，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。下表显示了无客户端应用面板和帮助内容的预定文件名。

**表 *16:*** 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 |
| 插件 | Terminal Servers | rdp-hlp.inc |
| 插件 | Telnet/SSH 服务器 | ssh,telnet-hlp.inc |
| 插件 | VNC Connections | vnc-hlp.inc |

[3] 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“导入”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。

过程

**步骤 1** 点击 **Import** 启动 Import Application Help Content 对话框，可在其中将新的帮助内容导入到闪存中，供无客户端会话期间显示。

**步骤 2** （可选） 点击**导出**，检索从表格中选择的以前导入的帮助内容。

**步骤 3** （可选） 点击**删除**，删除从表格中选择的以前导入的帮助内容。

**步骤 4** 系统将显示浏览器所显示语言的缩写。此字段并非用于文件转换，而是指示文件中使用的语言。要确定与表格中缩写关联的语言的名称，请显示浏览器所显示语言的列表。例如，当您使用下列程序之一时，对话框窗口将显示语言和关联的语言代码：

- 打开 Internet Explorer，依次选择 **Tools > Internet Options > Languages > Add**。
- 打开 Mozilla Firefox，依次选择 **Tools > Options > Advanced > General**，点击 Languages 旁边的 **Choose**，然后点击 **Select a language to add**。

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，首先需要从闪存卡上获取该文件的副本。

过程

**步骤 1** 使用浏览器与 ASA 建立一个无客户端会话。

**步骤 2** 将下表中“安全设备闪存中帮助文件的URL”中的字符串附加到ASA的地址中，替换*language*（如下所示），然后按 **Enter**，即可显示帮助文件。

**表 *17:* 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 |

| 应用类型 | 面板 | 安全设备闪存中帮助文件的 URL |
|---|---|---|
| 插件 | Telnet/SSH Servers | /+CSCOE+/help/*language*/ssh,telnet-hlp.inc |
| 插件 | VNC Connections | /+CSCOE+/help/*language*/vnc-hlp.inc |

*language* 指浏览器所显示语言的缩写。它并非用于文件转换，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** 依次选择**文件 > 另存（页面）为**。

**注释** 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。

**注释** 您可以使用大多数 HTML 标签，但不得使用定义文档及其结构的标签（例如，不得使用 <html>, <title>, <body>, <head>、<h1>、<h2> 等。您可以使用字符标签（例如 <b> 标签以及 <p>, <ol>、 <ul>和 <li>标签）来构造内容。

**步骤 6** 使用原始文件名和扩展名，将文件另存为仅 HTML。确保文件名没有多余的文件名扩展名。

### 下一步做什么

返回到 ASDM 并依次选择**配置 > Remote Access VPN > Clientless SSL VPN Access** > **门户** > **帮助自定义** > **导入**，将修改后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。建议为要支持的每种语言创建单独的文件夹。

**注释** 您可以使用大多数 HTML 标签，但不得使用定义文档及其结构的标签（例如，不得使用<html>, <title>, <body>, <head>、<h1>、<h2>等。您可以使用字符标签（例如 <b> 标签以及 <p>, <ol>、 <ul>和 <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 并依次选择**配置 > Remote Access VPN > Clientless SSL VPN Access** > **门户** > **帮助自定义** > **导入**，将新的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 对话框将帮助文件导入到闪存中，供无客户端会话期间在门户页面上显示。使用 Export Application Help Content 对话框检索以前导入的帮助文件，供随后编辑之用。

**过程**

**步骤 1** Language 字段用于指定浏览器所显示的语言，而非用于文件转换。（此字段在 Export Application Help Content 对话框中处于非活动状态。）点击 Language 字段旁边的点，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需的语言，请执行以下操作

a) 显示浏览器所显示的语言及其缩写的列表。

b) 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。

当您使用下列程序之一时，对话框将显示语言和关联的语言代码：

- 打开 Internet Explorer，依次选择 **Tools > Internet Options > Languages > Add**。
- 打开 Mozilla Firefox，依次选择 **Tools > Options > Advanced > General**，点击 Languages 旁边的 **Choose**，然后点击 **Select a language to add**。

**步骤 3** 如果是在导入，请从 File Name 下拉列表中选择新的帮助内容文件。如果是在导出，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 - 点击即可浏览本地计算机查找源文件或目标文件。
- 闪存文件系统 - 指示源文件或目的文件是否位于 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 - 点击即可浏览闪存查找源文件或目标文件。
- 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），并指定路径。

# 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，供随后的会话期间显示。您还可以检索以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。

每个应用窗格都用预定的文件名显示自己的帮助文件内容。每个文件的预期位置在 ASA 闪存中的 /+CSCOE+/help/*language*/ URL 中。下表显示了可以为 VPN 会话维护的每个帮助文件的详细信息。

**表 *18: 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* 指浏览器所显示语言的缩写。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，请从浏览器所显示语言的列表复制语言缩写。例如，当您使用下列程序之一时，对话框窗口将显示语言和相关语言代码：

- 打开 Internet Explorer，依次选择 **Tools > Internet Options > Languages > Add**。
- 打开 Mozilla Firefox，依次选择 **Tools > Options > Advanced > General**，点击 Languages 旁边的 **Choose**，然后点击 **Select a language to add**。

# 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。下表显示了转换域和转换的功能区域。

语言转换域选项

| 转换域 | 转换的功能区域 |
| --- | --- |
| AnyConnect | 在 Cisco 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。 |
| 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 包括属于标准功能组成部分的每个域的转换表模板。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，这会在您提供的 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 generates the customization** 和 **url-list** 转换域模板（动态地），并且此模板将自动反映您对这些功能区域的更改。

创建转换表后，就可将其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，确定要在该对象中使用的转换表，并为组策略或用户指定该自定义对象。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

过程

**步骤 1** 依次导航至 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**确定**。

# 添加转换表

您可以在此窗格中根据模板添加新转换表，也可以修改已导入的转换表。

过程

**步骤 1** 选择要修改的模板并将其用作新转换表的基础。模板归入转换域并影响功能的特定区域。

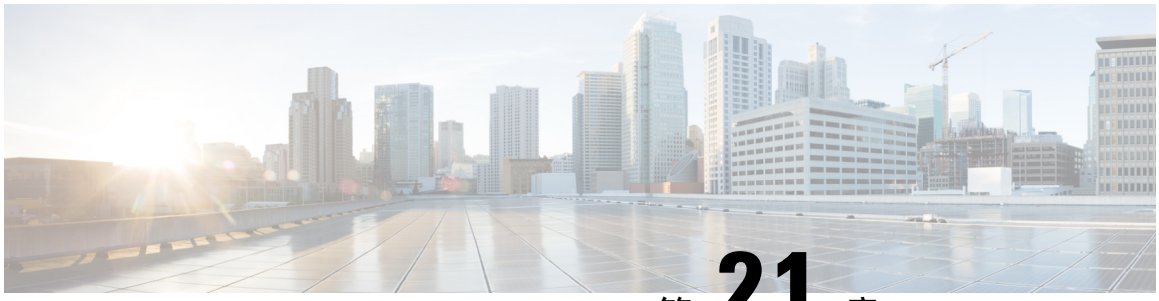
**步骤 2** 从下拉列表中选择转换域。

**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，如要使用西班牙语转换选项转换消息“Connected”，请在 msgstr 引号内插入西班牙语文本：

```
msgid "Connected"
msgstr "Conectado"
```

进行更改后，点击 **Apply** 导入转换表。



第 21 章

# 无客户端 SSL VPN 故障排除



## 使用 Application Access 时从 Hosts 文件错误中恢复

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。

当 Application Access 异常停止时，`hosts` 文件仍然处于无客户端 SSL VPN 自定义的状态。下次启动 Application Access 时，无客户端 SSL VPN 将通过搜索 hosts.webvpn 文件检查此状态。如果发现一个此状态，系统将显示 `Backup HOSTS File Found` 错误消息，并且 Application Access 将暂时关闭。

如果错误地停止 Application Access，远程访问客户端/服务器应用将处于不稳定状态。如果您尝试在不使用无客户端 SSL VPN 的情况下启动这些应用，它们可能会发生故障。您可能会发现自己通常连接的主机不可用。如果在家中远程运行应用，然后在关闭计算机前未退出 Application Access 窗口，则稍后尝试从办公室运行这些应用时，通常会发生这种情况。

如果未正确关闭 Application Access 窗口，可能会出现以下错误：

- 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。

以任何不正确的方式停止 Application Access 都可能导致这些错误。例如：

- 在使用 Application Access 时浏览器崩溃。
- 在使用 Application Access 时电源中断或系统关闭。
- 在工作时将 Application Access 窗口最小化，然后在窗口处于活动状态（但已最小化）的情况下关闭计算机。

# 了解 Hosts 文件

本地系统上的 hosts 文件将 IP 地址映射为主机名。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 窗口来停止 Application Access 可以让该文件恢复其原始状态。

| | |
|---|---|
| 调用 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。<br>• 然后，无客户端 SSL VPN 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。<br>• 无客户端 SSL VPN 删除 hosts.webvpn。 |
| 完成 Application Access 后…… | hosts 文件处于原始状态。 |

**注释** Microsoft 反间谍软件会阻止端口转发 Java 小应用程序对 hosts 文件的更改。有关使用反间谍软件时如何允许更改 hosts 文件的信息，请参阅 www.microsoft.com 。

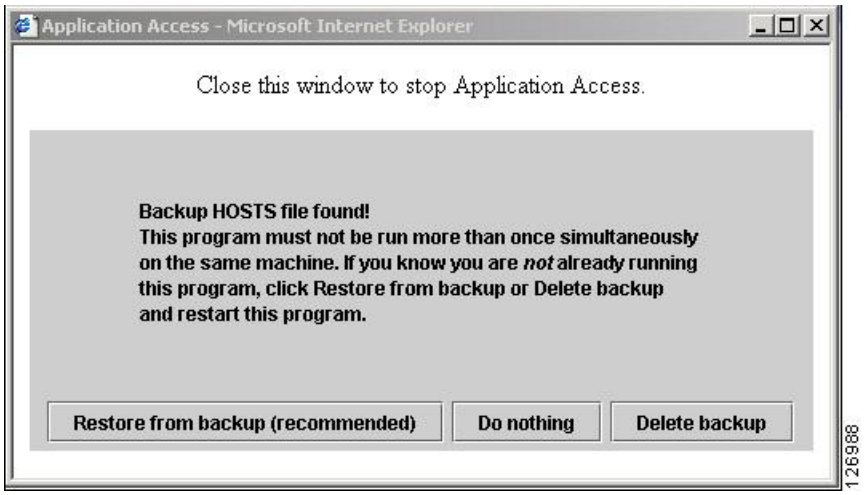
# 使用无客户端 SSL VPN 自动重新配置 Hosts 文件

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 hosts 文件并重新启用 Application Access 和应用。

**过程**

**步骤 1** 启动无客户端 SSL VPN 并登录。

点击 **Applications Access** 链接。




**步骤 2** 选择以下选项之一：

- **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，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。只有在不担心丢失 hosts 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。

# 手动重新配置 Hosts 文件

如果无法从当前位置连接到远程访问服务器，或者已自定义 hosts 文件并且不想丢失所作编辑，请按照以下步骤重新配置 hosts 文件并重新启用 Application Access 和应用。

**过程**

**步骤 1** 查找并编辑 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，则表示 hosts 文件是无客户端 SSL VPN 自定义的。如果 hosts 文件是无客户端 SSL VPN 自定义的，则会类似于以下示例：

```
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 `# added by WebVpnPortForward` 的行：

**步骤 4** 保存并关闭文件。

**步骤 5** 启动无客户端 SSL VPN 并登录。

**步骤 6** 点击 **Application Access** 链接。

# WebVPN 条件调试

在远程接入 VPN 上运行多个会话时，由于日志的大小，可能会很难进行故障排除。可以使用 **debug webvpn condition** 命令设置过滤器，以便更精确地定位调试进程。

**debug webvpn condition** { **group** *name* | **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask* | **prefix** *length*}] | **reset** | **user** *name*}

其中：

- **group** *name* 对组策略进行过滤，而不是隧道组或连接配置文件。
- **p-ipaddress** *ip_address* [{**subnet** *subnet_mask* | **prefix** *length*}] 对客户端的公共 IP 地址进行过滤。子网掩码（用于 IPv4）或前缀（用于 IPv6）是可选的。
- **reset** 重置所有过滤器。可以使用 **no debug webvpn condition** 命令关闭特定的过滤器。
- **user** *Name* 按用户名过滤。

如果配置多个条件，则条件是合并的 ((AND)，因此只有满足所有条件时才显示调试。

设置条件过滤器后，使用基本 **debug webvpn** 命令打开调试。只设置条件不会启用调试。使用 **show debug** 和 **show webvpn debug-condition** 命令查看调试的当前状态。

多个会话在 ASA VPN 上运行时，对单个用户会话进行故障排除比较麻烦。借助条件调试功能，可以根据设置的过滤条件来验证特定会话的日志。SAML、WebVPN 请求/响应、Anyconnect 是支持条件调试的模块。

注释 针对 IPv4 和 IPv6 子网提供“any, any”支持。

下文是在用户 jdoe 上启用条件调试的示例。

```
asa3(config)# debug webvpn condition user jdoe

asa3(config)# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

asa3(config)# debug webvpn
INFO: debug webvpn  enabled at level 1.

asa3(config)# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

# 向无客户端 SSL VPN 用户发送管理员警报

过程

**步骤 1** 在 ASDM 应用主窗口，依次选择**工具** > **向无客户端 SSL VPN 用户发送的管理员警报消息**.

**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**。

# 保护无客户端 SSL VPN 会话 Cookie

嵌入式对象（例如闪存应用和Java小应用应用，以及外部应用）通常依赖现有会话Cookie来与服务器一同工作。它们在初始化时使用某个 Javascript 来获取 Cookie。将 httponly 标记添加到无客户端 SSL VPN会话，这会使得会话Cookie仅对浏览器可见，对客户端侧脚本不可见，并导致无法实现会话共享。

### 开始之前

- 只有在没有活动的无客户端 SSL VPN 会话时，才可以更改 VPN 会话 Cookie。
- 使用 **show vpn-sessiondb webvpn** 命令检查无客户端 SSL VPN 会话的状态。
- 使用 **vpn-sessiondb logoff webvpn** 命令来注销所有无客户端 SSL VPN 会话。
- 当 **http-only-cookie** 命令启用时，以下无客户端 SSL VPN 功能将不可用。
  - Java 插件
  - Java 重写工具
  - 端口转发
  - 文件浏览器
  - 需要桌面应用（例如 MS Office 应用）的 Sharepoint 功能
  - AnyConnect 网络启动
  - Citrix Receiver、XenDesktop 和 Xenon
  - 其他不基于浏览器和浏览器插件的应用

要防止第三方通过 Javascript 等客户端脚本访问无客户端 SSL VPN 会话 Cookie，请执行以下步骤：

### 过程

**步骤 1** 依次选择**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **高级** > **HTTP Cookie**。

**步骤 2** 选中 **Enable HTTP-only VPN cookies** 复选框。

**注释** 仅在思科 TAC 建议您使用此设置时才可以使用。启用此命令会造成安全风险，因为“准则”一节下列出的无客户端 SSL VPN 功能将不运行，不提供任何警告。

**步骤 3** 点击 **Apply** 保存更改。