ASDM 手册 3：Cisco Secure Firewall ASA 系列 VPN ASDM 配置指南，7.20

首次发布日期: 2023 年 9 月 7 日

上次修改日期: 2024 年 5 月 23 日

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

目录

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在 Cisco Secure Firewall ASA 上配置 VPN。自适应安全设备管理器 (ASDM)，一个基于 Web 的 GUI 应用。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
boldface	命令、关键字、按钮标签、字段名称及用户输入的文本以**boldface**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。 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。注释部分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

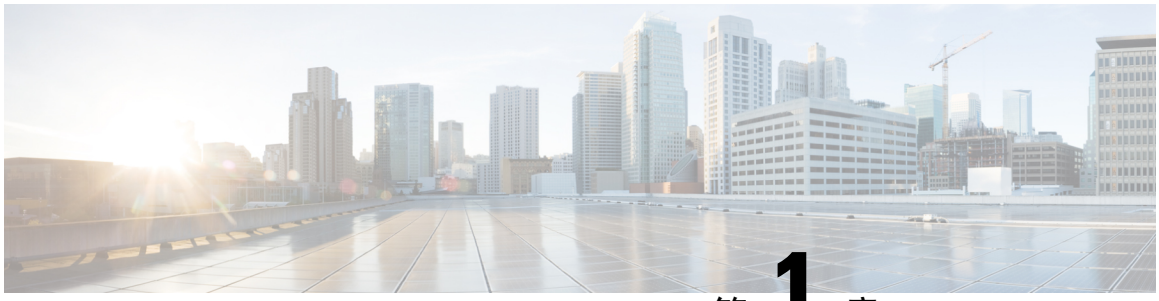
- 要及时从思科收到相关信息，请注册思科配置文件管理器。

- 要使用重要技术实现您期望实现的业务影响，请访问思科服务。
- 要提交服务请求，请访问思科支持。
- 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，该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漏洞信息。

关于本指南



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：

- Secure Client VPN 向导， 第 4 页

  Cisco Secure 客户端的 AnyConnect VPN 型号 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，Secure Client 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 Secure Client 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 Secure Client 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 Secure Client 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 2 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。

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。默认组 14（2048 位 Diffie-Hellman）。

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。

Secure Client VPN 向导

使用此向导配置 ASA 以接受来自 Cisco 安全客户端 AnyConnect VPN 模块的 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Cisco 安全客户端 AnyConnect VPN 模块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。

Secure Client 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 Secure Client，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，请参阅安全客户端管理员指南。

- SSL
- IPsec (IKEv2)
- Device Certificate - 向远程访问客户端标识 ASA。一些 Secure Client 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 Secure Client 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 Secure Client 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。

Secure Client 部署

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

- Web launch - 使用 Web 浏览器访问 ASA 时， Secure Client 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 Secure Client 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 Secure Client 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 Secure Client 软件包中，以确保 IPsec 连接按预期工作。

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 Cisco Secure 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。第 2 阶段创建用于保护数据的隧道。

使用 IKE Policy 窗格设置第 1 阶段 IKE 协商的条款，其中包括保护数据和确保隐私的加密方法、确保对等体身份的身份验证方式，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 DH 组 14（2048 位）被认为比组 2 和组 5 更安全。

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 DH 组 14（2048 位）被认为比组 2 和组 5 更安全。

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。

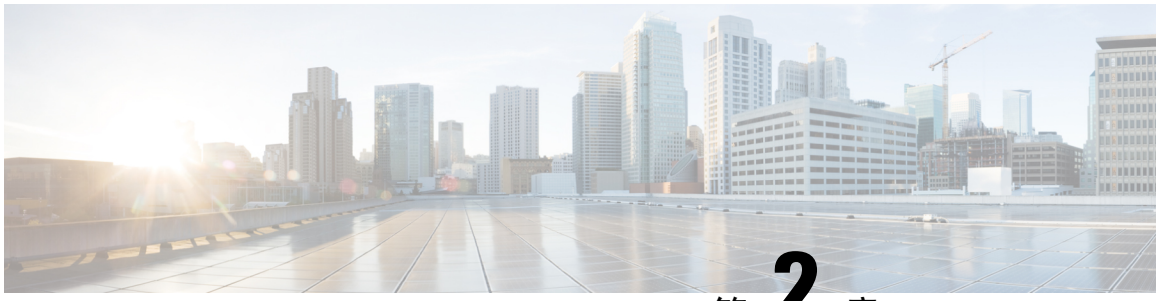
网络名解析服务器

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。



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 13 页。

步骤 2 设置站点到站点 VPN 的 IKE 参数， 第 14 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**配置 > 远程接入 VPN > 网络（客户端）接入 > 安全客户端 连接配置文件**。

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。

IPsec over TCP 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 间连接。

- ASA 可同时支持标准 IPsec、IPsec over TCP、NAT 遍历和 IPsec over UDP，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： • 预共享密钥的 IP 地址 • 证书身份验证的证书 DN。

会话控制

- Disable Inbound Aggressive Mode Connections

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

- Alert Peers Before Disconnecting
  - 客户端或 LAN 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。

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。

关于 IKEv2 多对等体加密映射

从 9.14(1) 版本开始，ASA IKEv2 支持多对等体加密映射 - 当隧道中的对等体关闭时，IKEv2 尝试与列表中的下一个对等体建立隧道。最多可以使用 10 个对等体地址来配置加密映射。IKEv2 上的这种多对等体支持非常有用，特别是从具有多对等体加密映射的 IKEv1 迁移时。

IKEv2 仅支持双向加密映射。因此，在双向加密映射上也配置了多个对等体，并使用相同的方法接受来自发起隧道的对等体的请求。

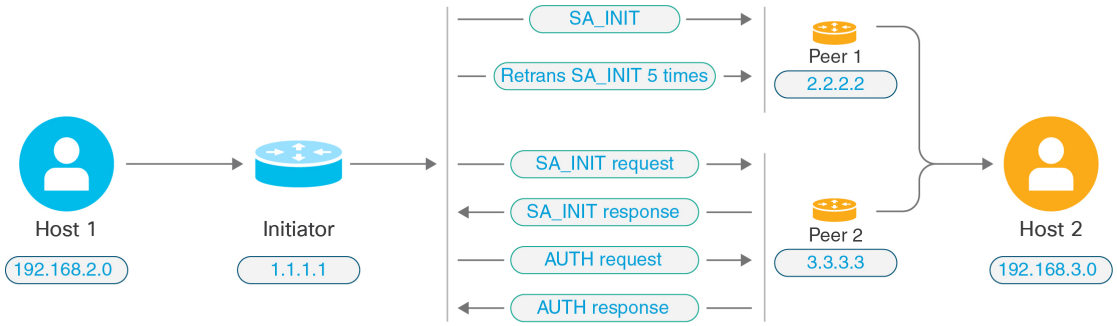
IKEv2 发起方行为

IKEv2 发起与对等体（例如 Peer1）的会话。如果对等体 1 无法访问 5 次 SA_INIT 重传，则会发送最终重传。此活动大约需要 2 分钟。

当 Peer1 发生故障时，SA_INIT 消息会被发送到 Peer2。如果 Peer2 也无法访问，则在 2 分钟后发起与 Peer3 的会话。

在加密映射的对等体列表中的所有对等体都用尽后，IKEv2 会再次从 Peer1 发起会话，直到与任何对等体建立 SA。下图描述了该行为。

图 *1:* 发起方流程



注释 发起 IKE SA 需要持续的流量，以便每次失败尝试都会移动到下一个对等体，并最终由某个可访问的对等体建立 SA。在流量中断的情况下需要手动触发，以便启动与下一个对等体的 IKE SA。

IKEv2 响应方行为

如果在加密映射中为 IKE SA 的响应方设备配置了多个对等体，则每次尝试 IKE SA 时，都会使用加密映射中的当前活动对等体的地址来验证发起方 IKE SA 的地址。

例如，如果加密映射中的当前活动对等体（用作响应方）是第一个对等体，则会从 Peer1 IP 地址发起IKE SA。同样，如果加密映射中的当前活动对等体（用作响应方）是第二个对等体，则会从Peer2 IP 地址发起 IKE SA。

注释 IKEv2 多对等体拓扑的响应方侧不支持对等体遍历。

加密映射更改时重置对等体索引

对加密映射所做的任何更改都会将对等体索引重置为零，并且隧道启动将从列表中的第一个对等体开始。下表提供了特定条件下的多对等体索引转换：

表 *1: SA* 之前的多对等体索引转换

SA 之前的条件	对等体索引已移动 是/否/重置
对等体无法访问	是
第 1 阶段提议不匹配	是
第 2 阶段提议不匹配	是
未收到 DPD 确认	是
身份验证阶段的流量选择器不匹配	是
身份验证失败	是
由于对等体无法访问，密钥更新失败	重置

表 *2: SA* 之后的多对等体索引转换

SA 后的条件	对等体索引已移动 是/否/重置
由于提议不匹配，密钥更新失败	重置
重新生成密钥期间流量选择器不匹配	重置
加密映射修改	重置
HA 切换	否
清除加密 IKEv2 SA	重置
清除 ipsec sa	重置
IKEv2 SA 超时	重置

IKEv2 多对等体的准则

IKEv1 和 IKEv2 协议

如果加密映射同时配置了 IKE 版本和多个对等体，则在移动到下一个对等体之前，将在两个版本的每个对等体上进行 SA 尝试。

例如，如果加密映射配置了两个对等体（例如 P1 和 P2），则会使用 IKEv2 向 P1 发起隧道，使用 IKEv1 向 P1 发起隧道，使用 IKEv2 向 P2 发起隧道，以此类推。

高可用性

具有多个对等体的加密映射会启动通往 HA 中的响应方设备的隧道。当第一台设备无法访问时，它就会移至下一台响应方设备。

发起方设备发起到响应方设备的隧道。如果主用设备发生故障，备用设备会尝试从 Peer1 IP 地址建立隧道，而不管主用设备上的 Peer2 IP 地址的加密映射如何。

集中式集群

具有多个对等体的加密映射可以启动通往集中式集群部署中的响应方设备的隧道。如果第一台设备无法访问，它会尝试移至下一台响应方设备。

发起方设备发起到响应方设备的隧道。如果无法访问 Peer1，那么集群中的每个节点都会移动到下一个 Peer2。

分布式集群

如果配置了 IKEv2 多对等体加密映射，则不支持分布式集群。

多情景模式

在多情景模式下，多对等体行为将特定于每个情景。

调试命令

如果隧道建立失败，请启用这些命令以对问题作进一步分析。

- **debug crypto ikev2 platform 255**
- **debug crypto ikev2 protocol 255**
- **debug crypto ike-common 255**

以下示例是特定于 IKEv2 多对等体的调试日志，显示了对等体的转换。

```
Sep 13 10:08:58 [IKE COMMON DEBUG]Failed to initiate ikev2 SA with peer 192.168.2.2,
initiate to next peer 192.168.2.3 configured in the multiple peer list of the crypto map.
```

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）。
- 身份验证方法，用于确保对等体的身份。
- 加密方法，用于保护数据并确保隐私。
- HMAC 方法，用于确保发送方身份，以及确保消息在传输过程中未被修改。
- Diffie-Hellman 群，用于确立 encryption-key-determination 算法的强度。ASA 使用此算法派生加密密钥和散列密钥。
- 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）	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）	

14	组 14（2048 位）	默认 Diffie-Hellman 组为 Group 14（2048 位 Diffie-Hellman）

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 间 VPN 可连接不同地理位置的网络。在 IPsec LAN 间 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
- 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。从 9.14(1) 开始，ASA 支持 IKEv2 中的多个对等体。您最多可以向加密映射中添加 10 个对等体。
- 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 (2048-bits) = 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。如果将任何源/目标 (0.0.0.0/0.0.0.0) 指定为受保护网络，请勿启用 RRI，否则会影响使用默认路由的流量。
  - “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 ... 以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。

注释 在配置 MTU 时，您必须考虑 ESP 开销。由于加密期间添加到 MTU 的 ESP 开销，数据包的大小会在加密后增加。如果收到“数据包太大”(packet too big) 错误，请确保检查 MTU 大小并配置较低的 MTU。

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，系统将使用此方法。
  - 使用此方法时，系统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 Secure Client）提供的唯一方法，或者两个对等体都指定了协商期间的支持和首选项，则系统将使用此方法。
  - 使用此方法时，系统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，将影响应用该配置后所建立的后续 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**配置** > **站点间 VPN** > **高级** > **IKE 参数**。

步骤 2 选择或取消选择**启用分片 (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。

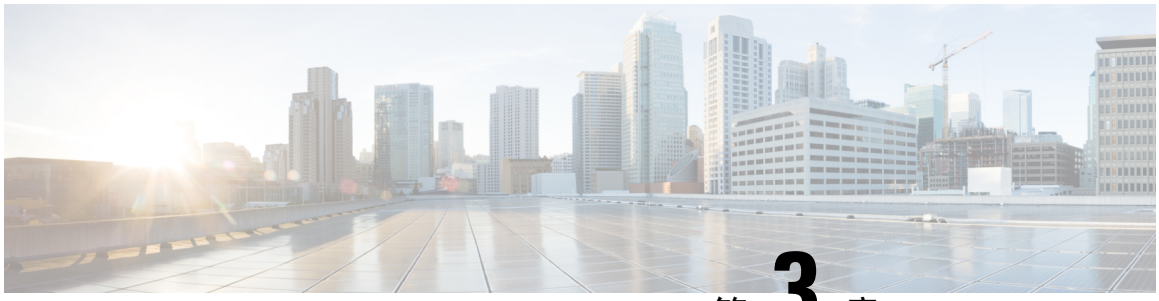
    此模式的优势是每个数据包只需增加几个字节并且允许公共网络上的设备查看数据包的最终源和目标。在传输模式下，可以根据 IP 报头中的信息在中间网络上启用特殊处理（例如 QoS）。然而，第 4 层报头将被加密，这就限制了对数据包的检查。
  - **传输必要** - 封装模式将为仅传输模式，不允许回退到隧道模式。

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“没有选择建议”。

- **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、负载均衡和故障转移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和故障转移的详细信息，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。

Secure Firewall eXtensible 操作系统 (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，仅与集群的控制设备建立 VPN 连接。

  VPN 功能仅限控制设备使用，且不能利用集群的高可用性功能。如果控制设备发生故障，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。选择新的控制设备后，必须重新建立 VPN 连接。

  将 VPN 隧道连接到跨接口地址时，连接会自动转移到控制设备。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访问 VPN。

VPN 负载均衡

VPN 负载均衡是在 VPN 负载均衡组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。VPN 负载均衡组由两台或更多设备组成。一台设备是导向器，而其他设备是成员设备。组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。

VPN 负载均衡组中的所有主用设备都会承载会话负载。VPN 负载均衡可以将流量定向至组中负载最低的设备，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。

故障转移

故障转移配置需要通过专用故障转移链路和状态故障转移链路（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转移条件的时刻。如果这些条件得到满足，则会进行故障转移。故障转移同时支持 VPN 和防火墙配置。

ASA 支持两种故障转移配置：主用/主用故障转移和主用/备用故障转移。

使用主用/主用故障转移时，两台设备都可以传送网络流量。这不是真正的负载均衡，尽管看似具有相同的效果。发生故障转移时，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/主用故障转移时，您必须确保两台设备的合并流量在每台设备的容量之内。

使用主用/备用故障转移时，只有一台设备会传送流量，而另一台设备会在备用状态下进行等待，不会传送流量。主用/备用故障转移允许使用第二台 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。

VPN 负载均衡

关于 VPN 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，则可以通过创建 VPN 负载均衡组来将这些设备配置为共享其会话负载。VPN 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。

VPN 负载均衡组中的所有设备都会承载会话负载。组中的一台设备，即导向器会将传入的连接请求定向至称为成员设备的其他设备。导向器会监控组中的所有设备、追踪每台设备的繁忙情况，然后相应地分配会话负载。导向器的角色不会与某台物理设备绑定；它可以在设备之间切换。例如，如果当前的导向器发生故障，该组的一台成员设备会接管该角色，立即成为新的导向器。

VPN 负载均衡组会对外部客户端显示为单个虚拟 IP 地址。此 IP 地址不与特定物理设备绑定。它属于当前导向器。VPN 客户端会尝试建立连接，先与虚拟 IP 地址连接。随后，导向器会将组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，VPN 负载均衡组导向器就能在资源之间均匀、高效地定向流量。

如果组中的一个 ASA 发生故障，终止的会话可以立即重新连接到虚拟 IP 地址。随后，导向器会将这些连接，定向至组中的另一活动设备。如果导向器发生故障，则组中的成员设备会立即自动接管，成为新的导向器。即便该组中的多台设备发生故障，只要该组中的任一设备正常运行，并且可用，用户仍然可以继续与该组连接。

对于每个 VPN 负载均衡集群设备，必须配置公共/外部 (lbpublic) 和专用/内部 (lbprivate) 接口。

- 公共接口：设备的外部接口，用于与集群 IP 地址进行初始通信。此接口用于 Hello 握手。
- 专用接口：用于在负载均衡集群成员之间进行消息传送的设备内部接口。这些消息包括与负载均衡相关的保持连接、拓扑消息和服务中断消息。

VPN 负载均衡算法

VPN 负载均衡组导向器会维护一个按 IP 地址升序排列的组成员列表。每个成员的负载计算为整数百分比（活动会话数）。Secure Client 非活动会话不会被计入 VPN 负载均衡的 SSL VPN 负载。导向器会将 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%。当所有成员都比导向器高 1% 时，导向器就会将流量重定向到自身。

例如，如果您有一个导向器和两个成员，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导向器高出 1%，则导向器会接受连接。
2. 如果导向器没有接受连接，则哪台成员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，则由会话数最少的成员获得会话。
4. 如果所有成员的负载百分比值和会话数都相同，则由 IP 地址最少的成员获得会话。

VPN 负载均衡组配置

VPN 负载均衡组可由相同版本或混合版本的 ASA 组成，并会受到以下限制：

- 包含两个相同版本 ASA 的 VPN 负载均衡组，可以为混合的 IPsec、Secure Client 和无客户端 SSL VPN 客户端会话进行 VPN 负载均衡。
- 包含混合版本 ASA 的 VPN 负载均衡组可支持 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。

组的主管会将会话请求分配给组的成员。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 VPN 负载均衡组中的最多 10 个节点。更大的组可能能够正常工作，但是我们不正式支持此类拓扑。

VPN 负载均衡导向器选举

导向器选举过程

虚拟集群中的每个非主设备都会维护一个本地拓扑数据库。每当集群的拓扑发生更改时，主设备都会更新该数据库。如果在最大重试次数后未收到主设备的 Hello 响应或未收到主设备的保持连接响应，则每个非主设备都会进入主设备选举状态。

成员在导向器选举期间执行以下功能：

- 比较本地拓扑数据库中找到的每个负载均衡设备的优先级。
- 如果找到两台具有相同优先级的设备，则选择具有较低 IP 地址的设备。
- 如果成员本身当选，则它会申领虚拟 IP 地址。
- 如果选举了其他成员之一，则该成员将向当选的主设备发送 Hello 请求。
- 当两台成员设备尝试申领虚拟 IP 地址时，ARP 子系统会检测到重复的 IP 地址情况，并发送通知要求具有更高 MAC 地址的成员放弃导向器角色。

Hello 握手

每个成员会在启动时向外部接口上的虚拟集群 IP 地址发送 Hello 请求。如果收到 Hello 请求，主设备会向成员发送自己的 Hello 请求。非导向器成员在收到导向器的 Hello 请求后会返回 Hello 响应。Hello 握手到此结束。

完成 Hello 握手后，如果配置了加密，则会在内部接口上发起连接。如果在最大重试次数后成员仍未收到 Hello 响应，则该成员将进入主设备选举状态。

Keepalive 消息

在成员和导向器之间完成 Hello 握手后，每台成员设备都会定期向主设备发送保持连接请求及其负载信息。如果导向器没有未完成的保持连接响应，则在正常处理期间，成员设备会以一秒为间隔发送保持连接请求。这意味着只要收到来自上一个请求的保持连接响应，就会在下一秒发送下一个保持连接请求。如果成员未从导向器收到上一个保持连接请求的保持连接响应，则下一秒不会发送保持连接请求。相反，成员的保持连接超时逻辑将启动。

保持连接超时的工作原理如下：

1. 如果成员正在等待导向器的未决保持连接响应，则该成员不会发送常规的一秒间隔保持连接请求。
2. 成员将等待 3 秒，并在第 4 秒时发送保持连接请求。
3. 只要导向器没有保持连接响应，成员就会重复五 (5) 次上述步骤 2。
4. 然后，该成员宣布该导向器已消失，并开始新的导向器选举周期。

有关 VPN 负载均衡的常见问题

- 多情景模式
- IP 地址池耗尽
- 唯一 IP 地址池
- 在相同设备上使用 VPN 负载均衡和故障转移
- 多个接口上的 VPN 负载均衡
- VPN 负载均衡集群的最大并行会话数

多情景模式

问: 在多情景模式下是否支持 VPN 负载均衡？

答: 在多情景模式下，既不支持 VPN 负载均衡也不支持状态故障转移。

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 Secure Client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 VPN 负载均衡和故障转移

问: 一台设备可以同时使用 VPN 负载均衡和故障转移吗？

答: 是。在此配置中，客户端连接至组的IP地址，然后被重定向至组中负载最低的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 VPN 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 VPN 负载平衡？

答: 只能定义一个接口作为公共接口加入 VPN 负载平衡组。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 VPN 负载均衡这个概念不会改善性能。

VPN 负载均衡集群的最大并行会话数

问: 请考虑有两台 Firepower 1150 的部署，每台设备均有一个 100 位用户的 SSL VPN 许可证。在 VPN 负载均衡组中，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，因此您的组可以支持的最大会话数为组中每台设备的会话数量的总和，在这种情况下为 300。

VPN 负载均衡的许可

VPN 负载均衡需要有效的 3DES/AES 许可证。ASA 会在启用 VPN 负载均衡前检查是否存在此加密许可证。如果没有检测到有效的 3DES 或 AES 许可证，ASA 会阻止启用 VPN 负载均衡，也会阻止 VPN 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 负载均衡的前提条件

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 VPN 负载均衡。您必须显式启用 VPN 负载均衡。
- 必须先配置公共（外部）接口和专用（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 IP 地址所引用的接口。建立组通用的虚拟 IP 地址、UDP 端口（如需要）和 IPsec 共享密钥。
- 加入组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。
- 要使用 VPN 负载均衡组加密，请先使用 **crypto ikev1 enable** 命令在内部接口上启用 IKEv1，同时指定内部接口；否则，在尝试配置 VPN 负载均衡组加密时，您将收到错误消息。
- 如果使用主用/主用状态故障转移或 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。

VPN 负载均衡准则和限制

符合条件的客户端

VPN 负载均衡仅在使用以下客户端发起的远程会话上有效：

- 安全客户端（3.0 版本及更高版本）
- ASA 5505（用作简易 VPN 客户端时）
- Firepower 1010（用作简易 VPN 客户端时）
- 支持 IKE 重定向的 IOS EZVPN 客户端设备 (IOS 831/871)

客户端注意事项

VPN 负载均衡可与 IPsec 客户端和 SSL VPN 客户端会话配合使用。包括 LAN 间连接在内的所有其他 VPN 连接类型（L2TP、PPTP、L2TP/IPsec）可以连接到在其上启用了 VPN 负载均衡的 ASA，但不能加入 VPN 负载均衡。

当多个 ASA 节点分组进行负载均衡并且 Secure Client连接需要使用组 URL 时，必须在各个 ASA 节点执行以下操作：

- 使用每个 VPN 负载均衡虚拟地址（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。

负载均衡组

ASA 支持每个 VPN 负载均衡组包含 10 台设备。

情景模式

多情景模式下不支持 VPN 负载均衡。

FIPS

FIPS 不支持集群加密。

证书验证

使用 Secure Client 为 VPN 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 VPN 负载均衡组情况下，该地址取决于证书配置。如果该组使用一个证书，则该证书应该具有包含虚拟 IP 地址和组 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。如果该组使用多个证书，则每个 ASA 的证书均应具有包含虚拟 IP、组 FQDN 和各 ASA 的 IP 地址和 FQDN 的 SAN 扩展。

地理 VPN 负载均衡

在定期更改 DNS 解析的 VPN 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 Secure Client 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。如果在输入凭证前，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。如果在输入凭证前，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。当用户输入凭证并建立隧道时，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。

IKE/IPSec 安全关联

集群加密会话不会同步到 VPN 负载均衡器拓扑中的备用设备。

配置 VPN 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VPN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。VPN 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 VPN 负载均衡，请在组中的每台设备上执行以下操作：

- 建立通用的 VPN 负载均衡组属性以配置 VPN 负载均衡组。这包括组的虚拟 IP 地址、UDP 端口（如需要）和 IPsec 共享密钥。除组内的设备优先级外，组中的所有参与者都必须具有相同的组配置。
- 在设备上启用 VPN 负载均衡并定义设备特定属性（例如其公共和专有地址），从而配置加入的设备。这些值因设备而异。

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**向导 (Wizards)** > **高可用性和可扩展性 (High Availability and Scalability)**。

步骤 2 在“配置类型”(Configuration Type) 屏幕中，点击**配置 VPN 集群负载均衡 (Configure VPN Cluster Load Balancing)**，然后点击**下一步 (Next)**。

步骤 3 选择代表整个 VPN 负载均衡组的单一 IP 地址。在公共子网地址范围内，指定由组中所有 ASA 共享的 IP 地址。

步骤 4 为此设备要参与的 VPN 负载均衡组指定 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 VPN 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 VPN 负载均衡信息会被加密，请选中**启用 IPSec 加密 (Enable IPSec Encryption)** 复选框。

步骤 6 指定并验证 **IPsec 共享密钥**。您输入的值会显示为连续的星号字符。

步骤 7 指定在组内分配给此设备的优先级。范围是从 1 到 10。该优先级指示，在启动或现有导向器发生故障时，设备成为组导向器设备的可能性。设置的优先级越高（例如 10），此设备就越有可能将会成为导向器。

注释 如果 VPN 负载均衡组中的设备在不同时间加电，第一台加电的设备会承担导向器的角色。组中的每台设备都会在其通电时进行检查，以确保该组具有导向器。如果不存在主用设备，则该设备会承担此角色。启动并添加到组的设备稍后将成为组成员。如果在组中的所有设备同时加电，优先级设置最高的设备会成为导向器。如果在组中，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导向器。

步骤 8 选择**此设备的公共接口 (Public Interface of This Device)**。

步骤 9 选择**此设备的专用接口 (Private Interface of This Device)**。

步骤 10 选中**重定向时向客户端发送 FQDN 而不是 IP 地址 (Send FQDN to client instead of an IP address when redirecting)** 复选框，以便使导向器在将 VPN 客户端连接重定向至该设备时，发送使用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**下一步 (Next)**。请在 Summary 屏幕中审阅您的配置。

步骤 12 点击**完成 (Finish)**。

VPN 负载均衡组配置将被发送到 ASA。

下一步做什么

当多个 ASA 节点分组进行负载均衡并且 Secure Client连接需要使用组 URL 时，必须在各个 ASA 节点执行以下操作：

- 使用每个 VPN 负载均衡虚拟地址（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 可在**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端）访问 (Network [Client] Access) >** Secure Client **连接配置文件 (Connection Profiles) >** 连接配置文件名称 > **添加或编辑 (Add or Edit) > 高级 (Advanced) > 组别名/组 URL (Group Alias / Group 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**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **负载均衡 (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 Secure Client 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 Secure Client 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 间隧道进行通信。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。
- **将 FQDN 发送到客户端 (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。

下一步做什么

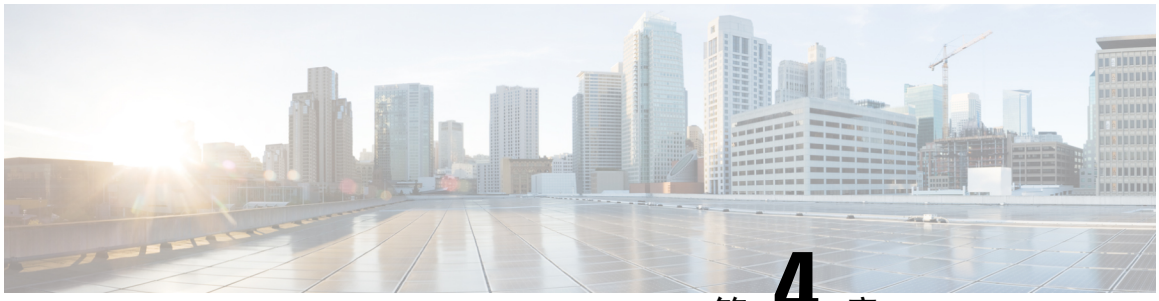
当多个 ASA 节点组成集群进行负载均衡并且 Secure Client连接需要使用组 URL 时，必须在各个 ASA 节点执行以下操作：

- 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 可在**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端）访问 (Network [Client] Access) >** Secure Client **连接配置文件 (Connection Profiles) >** 连接配置文件名称 > **添加或编辑 (Add or Edit) > 高级 (Advanced) > 组别名/组 URL (Group Alias / Group URL)** 窗格中配置。

VPN 负载均衡的功能历史记录

功能名称	版本	功能信息
使用 SAML 的 VPN 负载均衡	9.17(1)	ASA 现在支持使用 SAML 身份验证的 VPN 负载
VPN 负载均衡	7.2(1)	引入了此功能。



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 Secure Client 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 Secure Client 会话** 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 Secure Client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，Secure Client，对等体存活检测，第 78 页。

过程

步骤 1 为 Secure Client VPN 连接指定 DTLS 选项：

a) 转到**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端）访问 (Network [Client] Access) > 安全客户端 (Secure Client)连接配置文件 (Connection Profiles)**，访问接口 **(Access Interfaces)** 部分。

b) 在**接口 (Interface)** 表内为 Secure Client 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 (Port Settings)** 以配置 **SSL 端口 (SSL Ports)**。

- **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) 转到**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)**，然后转到**添加/编辑 (Add/Edit) > 高级 (Advanced) >** Secure Client。

b) 对**数据报传输层安全 (DTLS) (Datagram Transport Layer Security [DTLS])**，选择“继承（默认）”(Inherit [default])、“启用”(Enable) 或“禁用”(Disable)。

c) 对 **DTLS 压缩 (DTLS Compression)**（用于配置 DTLS 压缩），选择“继承（默认）”(Inherit [default])、“启用”(Enable) 或“禁用”(Disable)。

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 Secure Client TLS/DTLS 流量的吞吐量。这些更改可以加速 SSL VPN 数据路径，并在 Secure Client、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。

过程

步骤 1 依次选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **高级 (Advanced)** > **加密引擎 (Crypto Engine)**。

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　仅当设备上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。当您支持基于 SSL 的 Secure Client 远程访问 VPN 会话时，请使用此偏差。

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 Secure Client 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 Secure Client 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 网络（客户端）访问 VPN 连接和站点间 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 客户端的示例包括安全客户端和思科 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。
- Secure Client 内部组策略，第 63 页
- 站点到站点内部组策略，第 84 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：

- Cisco Secure 客户端 AnyConnect VPN 模块
- IPsec VPN 客户端
- IPsec IKEv2 客户端

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 Secure Client进行密码支持

ASA 支持 Secure Client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。

Secure Client 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 Secure Client 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 Secure Client 用户，请使用
 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 Cisco Secure 客户端 AnyConnect VPN 模块或传统 SSL VPN 客户端。如果使用的是 Secure Client，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。站点间（点对点）连接和思科 VPN 客户端到 LAN 连接均可使用 IPsec IKEv1。
  - **IPsec IKEv2** - 受 Secure Client支持。将 IPsec 与 IKEv2 结合使用的 Secure Client 连接提供高级功能，例如软件更新、客户端配置文件、GUI 本地化（转换）和自定义、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。请注意，VPN 过滤器仅适用于初始连接。它不适用于因应用检查操作而打开的辅助连接，例如 SIP 媒体连接。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。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。
- **禁用在同步会话抢占中无延迟地删除隧道** - 当给定用户达到允许的**同时登录**限制时，用户的下一次登录尝试要求系统首先删除最早的会话。此删除操作可能需要几秒钟，这可能会阻止用户立即建立新会话。选择此选项可指示系统建立新会话，而无需等待最早会话的删除完成。
- **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、 Secure Client、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 除非您正在编辑 DefaultGroupPolicy，否则请取消选中 DNS 服务器 **继承** 复选框，并添加您希望此组使用的 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 3 取消选中 WINS 服务器 **继承** 复选框，然后输入主 WINS 服务器和辅助 WINS 服务器的 IP 地址。指定的第一个 IP 地址是主 WINS 服务器的 IP 地址。指定的第二个（可选）IP 地址是辅助 WINS 服务器的 IP 地址。。

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

步骤 5 取消选中 DHCP 范围**继承**并定义 DHCP 范围。

如果在连接配置文件中为地址池配置了 DHCP 服务器，DHCP 作用域会标识要用于此组的地址池的子网。DHCP 服务器的地址还必须来自此作用域标识的同一个子网。作用域允许您选择 DHCP 服务器中定义的部分地址池，用于此特定组。

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。

要指定范围，请输入与所需池位于同一子网上但不在池内的可路由地址。DHCP 服务器确定此 IP 地址所属的子网并从该地址池分配 IP 地址。

建议尽可能将接口的IP地址用于路由目的。例如，如果池为 10.100.10.2-10.100.10.254，接口地址为 10.100.10.1/24，则使用 10.100.10.1 作为 DHCP 范围。请不要使用网络编号。DHCP 仅可用于 IPv4 寻址。如果您选择的地址不是接口地址，可能需要为范围地址创建静态路由。

步骤 6 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 7 点击**确定**。

步骤 8 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 Cisco Secure 客户端的 AnyConnect VPN 模型。

  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 Secure Client VPN 会话期间隐藏 Microsoft Internet Explorer 中的 Connections 选项卡。此外，从 Windows 10 版本 1703（或更高版本）开始，启用此功能还会在 Secure Client VPN 会话期间隐藏“设置”应用中的“系统代理”选项卡。禁用该功能后，Microsoft Internet Explorer 中的“连接”选项卡和“设

置”应用中的“代理”选项卡的显示保持不变;它们的默认设置可以是显示或隐藏，具体取决于用户注册表设置。

注释 在 Secure Client VPN 会话期间隐藏“设置”应用中的“系统代理”选项卡需要 AnyConnect 版本 4.7.03052 或更高版本。

Secure Client 内部组策略

内部组策略、高级、 Secure Client

- 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 Secure Client 仅预期 IPv6 流量时如何管理 IPv4 流量，或者在 ASA 仅预期 IPv4 流量时如何管理 IPv6 流量。

  当 Secure Client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 Secure Client 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。

  例如，假设 ASA 只将一个 IPv4 地址分配到 Secure Client 连接，且终端为双协议栈。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。

  如果建立 IPsec 隧道（而不是 SSL 连接），则不会通知 ASA 是否在客户端上启用了 IPv6，因此 ASA 始终推送客户端旁路协议设置。

- 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 Secure Client 配置文件中的 ASA FQDN 来获取 ASA IP 地址。在负载均衡场景中，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，Secure Client 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 ASA 未推送设备 FQDN，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， Secure Client 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。Secure Client 包含以下模块（一些较早的版本的模块较少）：
  - Secure Client DART - Diagnostic Secure Client 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。
  - Secure Client 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。
  - Secure Client SBL - 登录前启动 (SBL) 强制用户在登录到 Windows 之前通过 VPN 连接来连接到企业基础网络构架，方法是在 Windows 登录对话框显示之前启动 Secure Client 。
  - Cisco Secure 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 Secure Client 中，并且使 Secure Client 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 Secure Client 服务配置文件中的永久在线 VPN 标志设置，或者是否应使用 Secure Client 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 Secure Client 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，Secure Client 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 安全客户端 功能的发行版 Secure Client 。

- 要下载的客户端配置文件 - 配置文件是 Secure Client 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** 以启动“选择 Secure Client 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 Secure Client 流量的分割隧道

分割隧道将一些 Secure Client 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 Secure Client 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。
- Secure Client 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 Secure Client 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。

除顶级域外，动态分割隧道域名还需要至少一个域名标签。由于动态分割隧道旨在以匹配特定域名的流为目标，因此仅指定顶级域（例如 *org*）是不可接受的。您需要输入顶级域和至少一个域名标签（例如 *domain.org*）。

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 Secure Client 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。

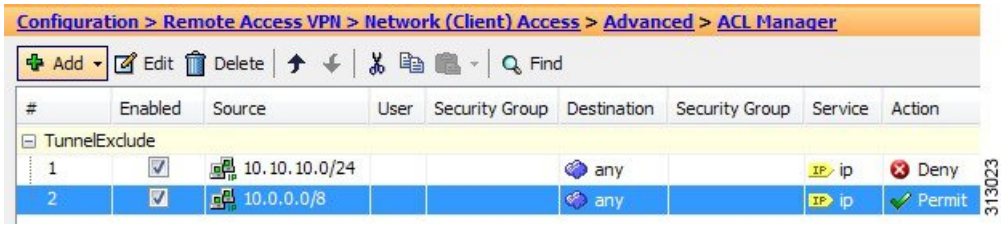
要定义分割隧道策略，请从下拉列表 **Policy** 和 **IPv6 Policy** 进行选择。Policy 字段定义 IPv4 网络流量的分割隧道策略。IPv6 Policy 字段选择 IPv6 网络流量的分割隧道策略。除该差异以外，这些字段还具有相同的用途。

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 (OK)**。

配置动态分割隧道

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 > 远程访问 VPN > 网络 (客户端) 访问 > 高级 >** Secure Client **自定义属性** 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 **Secure Client 自定义属性名称** 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。在 Secure Client 自定义属性名单屏幕的“值”部分中，使用逗号分隔值 (CSV) 格式（用逗号分隔域）定义这些域。 Secure Client 仅考虑前 20,000 个字符，不包括分隔符（大约 300 个通常大小的域名）。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 Secure Client 要求的 动态分割隧道 部分。

过程

步骤 1 浏览到 **配置 > 远程访问 VPN > 网络 (客户端) 访问 > 高级 >** Secure Client **自定义属性** 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 **Secure Client 自定义属性名称** 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。在 Secure Client Custom Attribute Names 屏幕的 Value 部分中，使用逗号分隔值 (CSV) 格式（用逗号分隔域）定义这些域。 Secure Client 仅考虑前 5000 个字符，不包括分隔符（大约 300 个通常大小的域名）。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 >** Secure Client **> 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 Secure Client 要求的 动态分割隧道 部分。

过程

步骤 1 浏览到 **配置 > 远程访问 VPN > 网络 (客户端) 访问 > 高级 > Secure Client 自定义属性** 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 **Secure Client 自定义属性名称** 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。在 Secure Client Custom Attribute Names 屏幕的 Value 部分中，使用逗号分隔值 (CSV) 格式（用逗号分隔域）定义这些域。 Secure Client 仅考虑前 5000 个字符，不包括分隔符（大约 300 个通常大小的域名）。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 > Secure Client > 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《Cisco 安全客户端 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 您必须将隧道组的身份验证方法配置为“仅证书”，方法是导航到**配置 > 远程访问 > 网络（客户端）访问 > Secure Client 连接配置文件 > 添加/编辑**，然后从“身份验证”下的“方法”下拉菜单中选择该方法。

步骤 2 然后，在同一个窗口中，依次选择**高级 (Advanced) > 组别名/组 URL (Group Alias/Group 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 (Remote Access VPN) > 网络（客户端）访问 (Network [Client] Access) > 组策略 (Group Policies) > 编辑 (Edit) > 高级 (Advanced) > 分割隧道 (Split Tunneling)**中选择“下面的隧道网络列表”(Tunnel Network List Below)。

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（因为其本意是为了实现透明性）。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：Secure Client 自定义属性，第 139 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 Secure Client 配置文件，第 124 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，然后导航到**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端）访问 (Network [Client] Access) > 高级 (Advanced) > Secure Client自定义属性 (Custom Attributes)**。

步骤 2 点击**添加 (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 (Advanced) > Secure Client > 自定义属性 (Custom Attributes)**。

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， Secure Client 属性

远程访问 VPN > 网络（客户端）访问 > 组策略的配置 > 添加/编辑 > 高级 > Secure Client，包含此组策略中 Secure Client 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 Secure Client 版本 2.5 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 Secure Client 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 Secure Client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。

  例如，假设 ASA 只将一个 IPv4 地址分配到 Secure Client 连接，且终端为双协议栈。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 Secure Client 配置文件中的 ASA FQDN 来获取 ASA IP 地址。在负载均衡场景中，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，Secure Client 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 ASA 未推送设备 FQDN，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， Secure Client 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。 Secure Client 版本 4.0 包含以下模块（以前版本具有较少的模块）：
  - Secure Client DART - Diagnostic Secure Client 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。
  - Secure Client 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。
  - Secure Client SBL - 登录前启动 (SBL) 强制用户在登录到 Windows 之前通过 VPN 连接来连接到企业基础网络构架，方法是在 Windows 登录对话框显示之前启动 Secure Client 。
  - Secure Client Web Security Module - 以前称为 ScanSafe Hostscan，此模块集成到 Secure Client 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。
  - Secure Client 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 Secure Client 中，并且使 Secure Client 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 Secure Client 服务配置文件中的永久在线 VPN 标志设置，或者是否应使用 Secure Client 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 Secure Client 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，Secure Client 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 安全客户端 功能的发行版 Secure Client 。

- 要下载的客户端配置文件 - 配置文件是 Secure Client 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** 以启动 Select Secure 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，Secure Client 登录设置

在内部组策略的 **Advanced** > Secure Client > **Login Setting** 窗格中，可以启用 ASA 以提示远程用户下载 Secure Client，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 **高级 > Secure Client > 客户端防火墙** 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。

当在 ASA 上配置客户端防火墙规则，并且正在终端上建立 VPN 连接时，

- ASA 将防火墙规则信息发送到客户端。
- 然后，客户端将根据需要应用防火墙规则。

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 75 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 Secure Client 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，Secure Client 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 Secure Client，但用户创建了一条自定义拒绝规则，则不会实施 Secure Client 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 Secure Client 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，Secure Client 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 Secure Client 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 Secure Client 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 Secure Client 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：

- 不允许使用 *deny ip any any* 专用规则。
- 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。
- HostScan (现在称为 Cisco Secure Firewall Posture) 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 (Source Port)	目的端口	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 Secure Client_Local_Print 随附于 ASDM，用于轻松配置客户端防火墙。为组策略的 Client Firewall 窗格中的 Public Network Rule 选择该 ACL 时，该列表包含以下 ACE：

.

表 *3: Secure Client _Local_Print* 中的 *ACL* 规则

说明	权限	接口	协议	源端口 (Source Port)	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
NetBios	允许	公共	UDP	默认	任意	137

说明	权限	接口	协议	源端口 (Source Port)	目的地址	目标端口
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 Secure Client 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 选择 高级 > Secure Client > 客户端防护墙哦i昂。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 Secure Client 的计算机同步的 Windows Mobile 设备，请将 IPv4 目标地址指定为 169.254.0.0，或者在 ACL 中指定 IPv6 目标地址 fe80::/64。

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，Secure Client 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 **高级 > Secure Client > 密钥重新生成** 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，Secure Client，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 Secure Client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 Secure Client 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。

- 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。

- 转到**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)**，添加或**编辑**所需的组策略，然后打开**高级 (Advanced)** > Secure Client > **对等体存活检测 (Dead Peer Detection)** 窗格。
- 或者，如要访问特定的用户策略，请转到**配置 (Configuration) > 设备管理 (Device Management) > 用户/AAA (Users/AAA) > 用户帐户 (User Accounts)**，添加或编辑所需用户账户，然后打开 **VPN 策略 (VPN Policy)** > Secure Client > **对等体存活检测 (Dead Peer Detection)** 窗格。

步骤 2 设置网关端检测。

取消选中**禁用 (Disable)** 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 (Disable)** 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。建议的值为 30 秒。

内部组策略，Secure Client 无客户端门户定制

在内部组策略的 **高级 > Secure Client > 自定义** 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 Secure Client/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。成功进行身份验证后，无客户端用户会立即进入此页面。成功建立 VPN 连接后， Secure Client 将启动此 URL 的默认 Web 浏览器。

注释 Secure Client 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，这些 Secure Client将忽略它。

- 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 Secure Client 自定义属性

内部组策略的 **高级 > Secure Client > 自定义属性窗格** 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 Secure Client，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 Secure Client 版本的 *Cisco Secure Client*管理员指南。

自定义属性也可在 **配置 > 远程访问 VPN > 网络 (客户端) 访问 > 高级 > Secure Client 自定义属性** 和 **Secure Client 自定义属性名称**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 转至 **配置 > 远程访问 VPN > 网络 (客户端) 访问 > 组策略 > 添加/编辑 > 高级 > Secure Client > 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。 有关 Secure Client 自定义属性选项，请参阅 Secure Client 自定义属性，第 139 页。

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 Secure Client 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。
- 对整组规则的限制为 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；如果没有应答，则VPN客户端知道防火墙已关闭并终止与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)。

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。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 Cisco Secure 客户端的 AnyConnect VPN 模型 或传统 SSL VPN 客户端。如果使用的是 Secure Client，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。站点间（点对点）连接和思科 VPN 客户端到 LAN 连接均可使用 IPsec IKEv1。
  - IPsec IKEv2 - 受 Secure Client 支持。将 IPsec 与 IKEv2 结合使用的 Secure Client 连接提供高级功能，例如软件更新、客户端配置文件、GUI 本地化（转换）和自定义、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**-（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。请注意，VPN过滤器仅适用于初始连接。它不适用于因应用检查操作而打开的辅助连接，例如 SIP 媒体连接。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。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**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > AAA/本地用户 (AAA/Local Users) > 本地用户 (Local Users)**，然后点击**添加 (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**继承 (Inherit)** 复选框，并输入新值。

过程

步骤 1 启动 ASDM 并依次选择**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > AAA/本地用户 (AAA/Local Users) > 本地用户 (Local Users)**。

步骤 2 选择要配置的用户，然后点击**编辑 (Edit)**。

步骤 3 在左侧窗格中，点击 **VPN 策略 (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**隧道协议 (Tunneling Protocols)** 复选框，以便选择以下某个隧道协议：

- SSL VPN 客户端允许用户在下载 Secure Client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。站点间（点对点）连接和思科 VPN 客户端到 LAN 连接均可使用 IPsec IKEv1。
- IPsec IKEv2 - Secure Client 支持。将 IPsec 与 IKEv2 配合使用的 Secure Client 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。请注意，VPN 过滤器仅适用于初始连接。它不适用于因应用检查操作而打开的辅助连接，例如 SIP 媒体连接。

a) 要配置过滤器和规则，请依次选择**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)** > **添加/编辑 (Add/Edit)** > **常规 (General)** > **更多选项 (More Options)** > **过滤器 (Filter)**。
b) 点击**管理 (Manage)** 以显示“ACL 管理器”(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“继承”(Inherit) 复选框，则默认值为“无”(None)。

步骤 8 指定是否从该组继承 Store Password on Client System 设置。

取消选中**继承 (Inherit)** 复选框以激活 Yes 和 No 单选按钮。点击**是 (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**否 (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“继承”(Inherit) 复选框。默认值为“继承”(Inherit)，或者，如果未选中“继承”(Inherit)复选框，则默认值为“未限制”(Unrestricted)。

   点击**管理 (Manage)** 以打开“添加时间范围”(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 (Inherit)** 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 (Inherit)** 复选框，则此参数指定空闲超时值（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 (Inherit)** 复选框，系统将自动选中**默认 (Default)** 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 (Inherit)** 复选框，系统将自动选中**默认 (Default)** 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 Secure Client设置。如要覆盖每项设置，请取消选中**继承 (Inherit)** 复选框，并输入新值。

步骤 14 点击**确定 (OK)** 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 安全客户端 AnyConnect VPN 模块、无客户端 SSL VPN 连接以及 IKEv1 和 IKEv2 第三方 VPN 客户端。

Secure Client 连接配置文件，主窗格

在 Secure Client 连接配置文件主窗格上，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。
  - 在接口表内为 Secure Client 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 Secure Client 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， Secure Client 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 89 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 89 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 Secure Client 连接配置文件和无客户端连接配置文件。某些 Secure Client 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 Secure Client和无客户端 Clientless SSL 进行连接）。在此版本之前，ECDSA 证书仅受 Secure Client 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 (OK)**。

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 > Secure Client 连接配置文件

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。

Secure Client 连接配置文件，基本属性

要设置 Cisco Secure 客户端连接的 AnyConnect VPN 模型的基本属性，请在 Secure Client Connection Profiles 部分中选择添加或编辑。系统将打开添加（或编辑）Secure Client Connection Profile > 基础对话框。

- 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 Secure Client 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、多证书、SAML 和证书、或多证书和 SAML。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。
- SAML 身份提供程序 - 选择用于单点登录 (SSO) 身份验证的 SAML IdP 服务器。
  - SAML 服务器 - 从 Secure Client 单点登录身份验证的下拉列表中选择 SAML 服务器，或点击 **管理** 以添加 SSO 服务器并配置以下参数：
    - **IDP 实体 ID**- SAML Idp 的实体 ID。
    - **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，当主机名为 `ssl-vpn` 且域名为 `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。
    - **本地基本 URL (Local Base URL)** -（可选）在 DNS 负载均衡集群中，当在 ASA 上配置 SAML 身份验证时，您可以指定唯一解析为应用配置的设备的基本 URL。

- **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 (Request Signature)** - 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（秒）。范围为 1 到 7200。

  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。
- **启用仅在内部网络上可访问的 IDP** - **选中此复选框可仅在可在**内部网络上访问时启用 IDP。
- **登录时请求 IDP 重新身份验证**- 选中此复选框可在登录时启用 IDP 重新身份验证。
- **Clock-skew** - 允许 NotBefore 和 NotOnOrAfter SAML 断言的时钟偏差。默认情况下，必须禁用时钟偏差。默认值为 1 秒，范围是 1 至 180 秒。

- SAML IDP 信任点 - 选择用于单点登录 (SSO) 身份验证的 SAML IdP 信任点。
  - IDP 信任点 - 选择包含供 ASA 用于验证 SAML 断言的 ASML IdP 证书的信任点。
- SAML 登录体验 - 选择用于单点登录 (SSO) 身份验证的 SAML IdP 信任点。
  - VPN 客户端嵌入式浏览器 - VPN 客户端使用其嵌入式浏览器进行 Web 身份验证，因此该身份验证仅适用于 VPN 连接。
  - 默认操作系统浏览器 - VPN 客户端使用系统的默认浏览器进行 Web 身份验证。此选项启用单点登录 (SSO) 并支持无法在嵌入式浏览器中执行的 Web 身份验证方法，例如生物识别身份验证。

    选择默认操作系统浏览器进行 SSO 身份验证时，必须为 Secure Client 配置外部浏览器包才能使用默认浏览器。请参阅Secure Client 外部浏览器 SAML 软件包，第 123 页。
- SAML 用户名匹配 - 选择以将证书用户名与 SAML 用户名进行匹配。
- 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。
- 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。
- “查找”(Find) - 输入要用作搜索字符串的 GUI 标签或 CLI 命令，然后点击**下一个 (Next)** 或**上一个 (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

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。

Secure Client 连接配置文件，常规属性

- 为此连接配置文件启用简单身份验证注册协议
- 将用户名传递到 AAA 服务器之前从中剥除领域
- 将用户名传递到 AAA 服务器之前从中剥除组
- 为组定界符
- “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。外部 是 Secure Client 连接至的接口，而 内部 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。

- “查找”(Find) - 输入要用作搜索字符串的 GUI 标签或 CLI 命令，然后点击**下一个 (Next)** 或**上一个 (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 > 远程接入 VPN > 网络（客户端）接入 > 安全客户端 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。

Secure Client 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（Secure Client、IKEv1 或 IKEv2），然后依次选择 **高级** > **客户端地址**。

- 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 94 页
连接配置文件，地址池 ，第 95 页
连接配置文件，高级，添加或编辑 IP 池 ，第 95 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。

Secure Client 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。
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。

属性	定义
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。

- 用于多证书身份验证的证书映射 - 管理要用于主身份验证的证书的分配。
  - 第一个证书 - 如果要将计算机颁发的证书用于主要身份验证，请点击此选项。
  - 第二个证书 - 如果要将从客户端颁发的用户证书用于主身份验证，请点击此选项。
- “查找”(Find) - 输入要用作搜索字符串的 GUI 标签或 CLI 命令，然后点击**下一个 (Next)** 或**上一个 (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 HostScan (现在称为 Cisco Secure Firewall Posture) 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。

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。

- 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。
- 用于多证书身份验证的证书映射 - 管理要用于辅助身份验证的证书的分配。
  - 第一个证书 - 如果要将计算机颁发的证书用于辅助身份验证，请点击此选项。
  - 第二个证书 - 如果要将从客户端颁发的用户证书用于辅助身份验证，请点击此选项。

Secure Client 连接配置文件，身份验证属性

通过 Secure Client 连接配置文件中的“授权”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 Secure Client、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。
  - 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。

Secure Client 连接配置文件，授权，添加脚本内容以选择用户名

如果在 Secure Client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， Secure Client 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 *4:* 按子字符串过滤

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

  使用负索引（例如在该表的第三行中）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 5: 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。

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。

连接配置文件中的选项卡名称为 Secure Client的组 URL/组别名。

- **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。

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 93 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Secure Client 连接配置文件，身份验证属性，第 95 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 103 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 Cisco Secure 客户端的 AnyConnect VPN 型号定义 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。

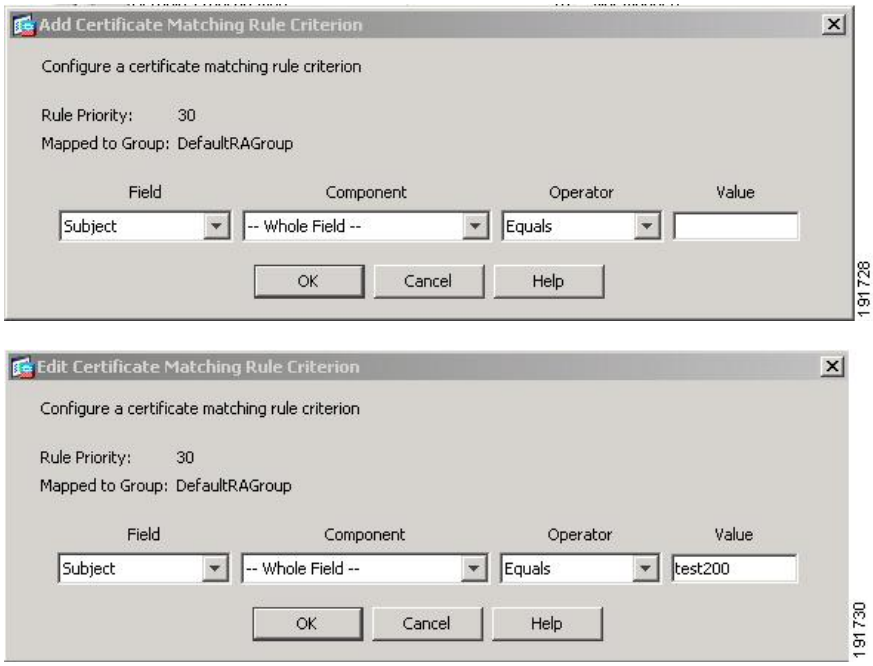
此窗格具有一个证书到连接配置文件映射及映射条件的列表。

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 字段	定义
DN Qualifier (DNQ)	特定 DN 属性。
E-mail Address (EA)	拥有证书的个人、系统或实体的邮件地址。
Generational Qualifier (GENQ)	辈分词，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。
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。

注释 当您创建站点间VPN连接配置文件时，打开连接配置文件，然后将其取消而不进行任何配置更改。如果您看到应用按钮突出显示，请放弃更改。

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 IPv6 寻址的 LAN 到 LAN 连接，如果两个对等体均是 ASA，并且如果两个内部网络均具有匹配的寻址方案（均为IPv4或均为IPv6），则安全设备支持VPN隧道。

具体而言，当两个对等体均是 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

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

- “管理”(Manage) - 打开“浏览远程网络”(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。
  - “远程对等体后量子密钥”(Remote Peer Post Quantum Key) - 选中此复选框可为 IKEv2 指定后量子预共享密钥 (PPK)，而不是预共享密钥。PPK 是一个包含 64 个字符的 256 位十六进制字符串。

    PPK 类似于预共享密钥，可保护 IKEv2 免受量子计算机攻击。
  - “显示密码”(Show Password) - 选中此复选框可查看 PPK 密钥。
  - “远程对等体后量子密钥身份”(Remote Peer Post Quantum Key Identity) - 指定 PPK 的 ID。
  - 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。
  - 对于动态 VTI：
    - “IKEv2 路由接受任意”(IKEv2 Route Accept Any) - 选中此复选框可使 ASA 接受在 IKEv2 交换期间接收的隧道接口 IP 地址。默认情况下，此选项处于已启用状态。

- “IKEv2 路由集接口”(IKEv2 Route Set Interface) - 选中此复选框可在 IKEv2 交换期间发送隧道接口 IP 地址。此选项配置通往对等体隧道接口的动态路由，并通过隧道在中心和分支之间运行动态路由协议。

- Enable RSA Signature Hash - 选中此复选框可启用 RSA 签名散列。RSA 是加密类型的一种。
- 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。

此连接配置文件还具有以下参数：

- 高级 > 加密映射条目。有关详细信息，请参阅 站点到站点连接配置文件，加密映射条目，第 119 页。
- 高级 > 隧道组。有关详细信息，请参阅 站点间连接配置文件隧道组，第 120 页。

站点间隧道组

ASDM 窗格上的 **配置 (Configuration) > 站点间 VPN (Site-to-Site VPN) > 高级 (Advanced) > 隧道组 (Tunnel Groups)** 指定用于 IPsec 站点间连接配置文件（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。
  - “管理”(Manage) - 打开“浏览远程网络”(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。
  - “远程对等体后量子密钥”(Remote Peer Post Quantum Key) - 选中此复选框可为 IKEv2 指定后量子预共享密钥 (PPK)，而不是预共享密钥。PPK 是一个包含 64 个字符的 256 位十六进制字符串。

PPK 类似于预共享密钥，可保护 IKEv2 免受量子计算机攻击。

- “显示密码”(Show Password) - 选中此复选框可查看 PPK 密钥。
- “远程对等体后量子密钥身份”(Remote Peer Post Quantum Key Identity) - 指定 PPK 的 ID。
- 对于动态 VTI：
  - “IKEv2 路由接受任意”(IKEv2 Route Accept Any) - 选中此复选框可使 ASA 接受在 IKEv2 交换期间接收的隧道接口 IP 地址。默认情况下，此选项处于已启用状态。
  - “IKEv2 路由集接口”(IKEv2 Route Set Interface) - 选中此复选框可在 IKEv2 交换期间发送隧道接口 IP 地址。此选项配置通往对等体隧道接口的动态路由，并通过隧道在中心和分支之间运行动态路由协议。

- 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“置信区间”(Confidence Interval) 和“重试间隔”(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。

- 对于动态 VTI - 将虚拟模板附加到隧道组。
  - 虚拟模板 - 从下拉列表中选择虚拟模板。您可以将同一虚拟模板连接到多个隧道组。ASA 会使用虚拟模板来为每个 VPN 会话创建单独的虚拟访问接口。

    要成功完成虚拟模板配置，您必须配置以下 DVTI 接口参数（**配置 (Configuration) > 设备设置 (Device Setup) > 接口设置 (Interface Settings) > 接口 (Interfaces) > 添加 (Add) > 添加 DVTI 接口 (Add DVTI Interface)**）
    - DVTI 接口名称
    - 启用接口
    - 为 IPSec 启用隧道模式 IP 重叠（IPv4 或 IPv6）
    - 使用 IPsec 配置文件进行隧道保护

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）。

站点间连接配置文件隧道组

在此对话框中，指定当前站点间连接配置文件的隧道组参数。

- 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 Peer ID Validation - 选择忽略、必需还是仅在证书支持的情况下才选中 IKE 对等体 ID 验证。
- IKE 保持连接 - 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“置信区间”(Confidence Interval) 和“重试间隔”(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。远程访问组的默认间隔值为 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。

- 对于动态 VTI - 将虚拟模板附加到隧道组。
  - 虚拟模板 - 从下拉列表中选择虚拟模板。您可以将同一虚拟模板连接到多个隧道组。ASA 会使用虚拟模板来为每个 VPN 会话创建单独的虚拟访问接口。

    要成功完成虚拟模板配置，您必须配置以下 DVTI 接口参数（**配置 (Configuration) > 设备设置 (Device Setup) > 接口设置 (Interface Settings) > 接口 (Interfaces) > 添加 (Add) > 添加 DVTI 接口 (Add DVTI Interface)**）
    - DVTI 接口名称
    - 启用接口
    - 为 IPSec 启用隧道模式 IP 重叠（IPv4 或 IPv6）
    - 使用 IPsec 配置文件进行隧道保护

-

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。

思科安全客户端映像的 AnyConnect VPN 模块

配置 > 远程访问 VPN > 网络（客户端）访问 > Secure Client软件窗格列出了 ASDM 中配置的 Secure Client 映像。

Secure Client 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 Secure Client 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 Secure Client 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。
- “上移”和“下移”- 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。

思科安全客户端映像的 AnyConnect VPN 模块，添加/替换

在此窗格中，可以指定 ASA 闪存中要添加为 Secure Client 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。

思科安全客户端映像的 AnyConnect VPN 模块，上传映像

在此窗格中，可以指定要标识为 Secure Client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。

Secure Client 外部浏览器 SAML 软件包

配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端）访问 (Network [Client] Access) > 安全客户端 (Secure Client) 外部浏览器 (External Browser) 窗格会列出可用于 Secure Client SAML 单点登录 (SSO) 身份验证的 Secure Client 外部浏览器软件包。

Secure Client 外部浏览器软件包映像 - 显示 ASDM 中配置的外部浏览器软件包文件。

- **添加** - 显示“添加 Secure Client 外部浏览器映像”对话框，您可以在其中将闪存中的文件指定为外部软件包映像文件，或者可以浏览闪存中的文件以将其指定为外部浏览器软件包文件。
- **替换** - 显示“替换 Secure Client 外部浏览器软件包”对话框，您可以在其中将闪存中的文件指定为外部浏览器软件包，以替换现有的软件包文件。
- **删除** - 从表中删除外部浏览器软件包文件。这不会从闪存中删除软件包文件。
- **“上移”和“下移”** - 向上和向下箭头会更改ASA将外部浏览器软件包下载到远程PC的顺序。

Secure Client 外部浏览器 SAML 软件包映像，添加/替换

在此窗格中，可以指定 ASA 闪存中要添加为 Secure Client外部浏览器软件包映像，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。

- **Secure Client 外部浏览器软件包** - 指定闪存中要标识为外部浏览器软件包映像的文件。
- **浏览闪存** - 显示“浏览闪存”(Browse Flash) 对话框，您可以在其中查看闪存中的所有文件。
- **上传** - 显示“上传映像”(Upload Image) 对话框，您可以在其中从本地 PC 上传要标识为外部浏览器软件包的文件。

Secure Client 外部浏览器 SAML 软件包映像，上传映像

在此窗格中，可以指定要标识为 Secure Client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。

- **本地文件路径** - 确定本地计算机上要标识为外部浏览器软件包映像的文件的文件名。
- **浏览本地文件** - 显示“选择文件路径”(Select File Path) 对话框，可以在其中查看本地计算机上的所有文件，并可选择要标识为外部浏览器软件包映像的文件。
- **闪存文件系统路径** - 确定安全设备闪存中要标识为外部浏览器软件包映像的文件的文件名。
- **浏览闪存** - 显示“浏览闪存”(Browse Flash) 对话框，您可以在其中查看安全设备闪存中的所有文件，并可选择要标识为外部浏览器软件包映像的文件。
- **上传文件** - 启动文件上传。

配置 Secure Client VPN 连接

Secure Client 连接的准则和限制

会话令牌建议

当 ASA 对来自 Secure Client的 VPN 连接请求进行身份验证时，会向客户端返回会话令牌以增强安全性。从 AnyConnect 4.9 (MR1) 开始，ASA 和 Secure Client 支持为会话令牌提供增强安全性的机制。您可以将 DAP 规则配置为拒绝来自不支持令牌安全的 Secure Client 版本的连接尝试。请参阅使用 DAP 检查会话令牌安全，第 189 页。

配置 Secure Client 配置文件

您可以配置 ASA，以便向所有 Secure Client 用户全局部署 Secure Client 配置文件，或基于用户的组策略向用户部署。通常，用户对于安装的每个 Secure Client 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 Secure Client配置文件及控制客户端功能的详细信息，请参阅《Cisco Secure 客户端的 AnyConnect VPN 模块管理员指南》。

客户端配置文件在**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端）访问 (Network [Client] Access) > Secure Client 配置文件 (AnyConnect Profile)**：

添加/导入 - 显示 Secure Client 配置文件“(Add AnyConnect 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。

- 配置文件名称 - 指定该组策略的 Secure Client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 安全状态、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 Secure Client一起下载到属于该组策略的用户。

编辑 - 显示“编辑 SSL VPN 客户端配置文件”(Edit SSL VPN Client Profile) 窗口，可以在其中更改 Secure Client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。
- 浏览本地 (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。

Secure Client配置文件表 - 显示指定为 Secure Client配置文件的 XML 文件：

豁免 Secure Client 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 Secure Client 流量进行转换，以便 DMZ 上的 Secure Client、内部网络和企业资源可以相互发起网络连接。豁免转换 Secure Client 流量失败将阻止 Secure Client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 *6:* 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

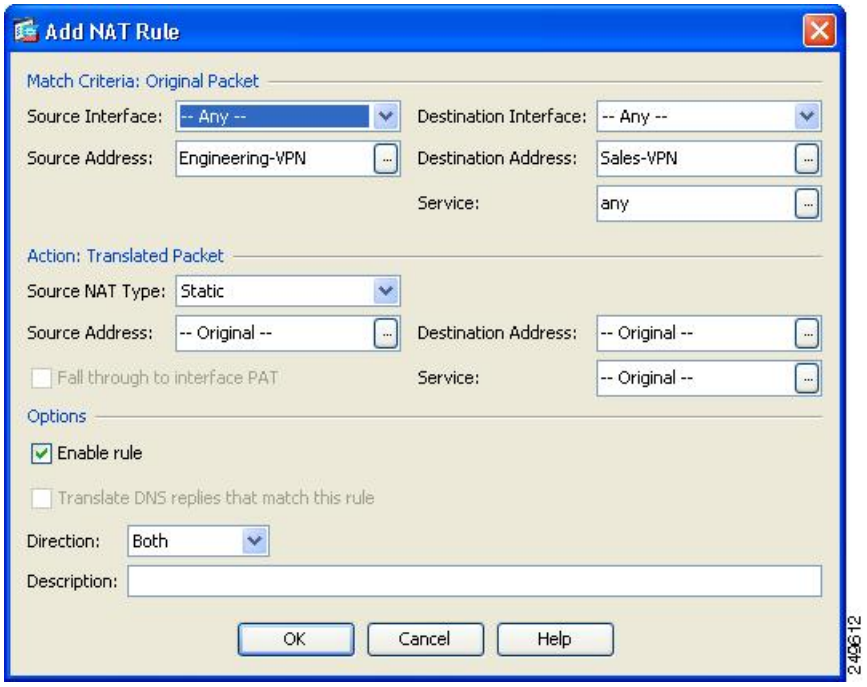
过程

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。

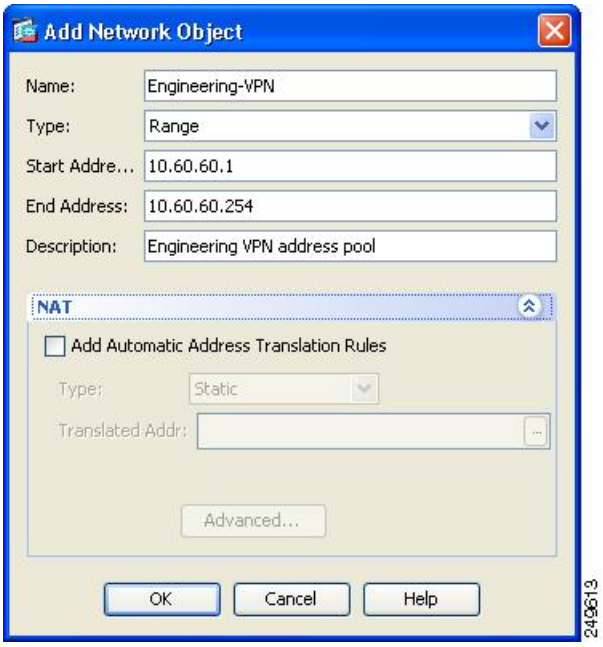
图 *2: Add NAT Rule* 对话框



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 *3:* 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**确定**。
e) 点击**应用**。

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
```

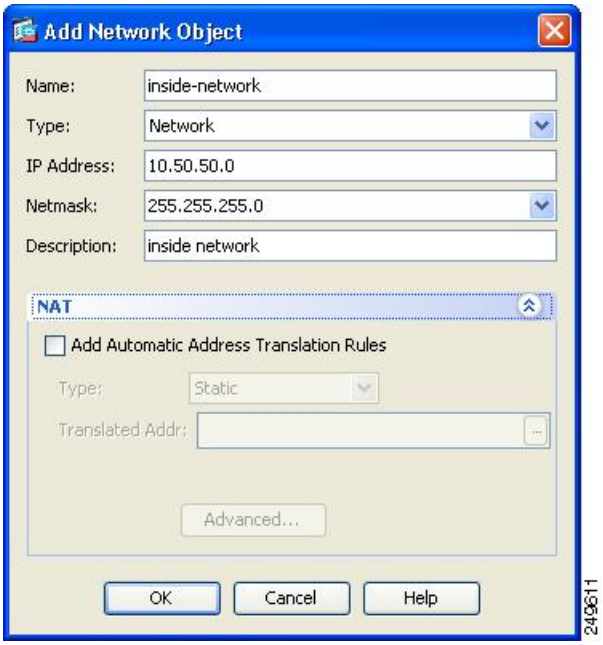
步骤 4 创建 NAT 规则，以便 Engineering VPN 地址池中的主机可以到达 Engineering VPN 地址池中的其他主机。创建此规则的过程就与先前创建该规则一样，不同之处在于，您需要在“匹配条件：原始数据包”区域中将工程 VPN 地址池同时指定为源地址和目的地址。

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 *4:* 添加 *inside-network* 对象



b) 在 Action: Translated Packet 区域中，配置以下字段：

- Source NAT Type：Static
- Source Address：Original
- Destination Address：Original
- Service：Original

c) 在 **Options** 区域中，配置以下字段：

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

d) 点击**确定**。

e) 点击**应用**。

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。

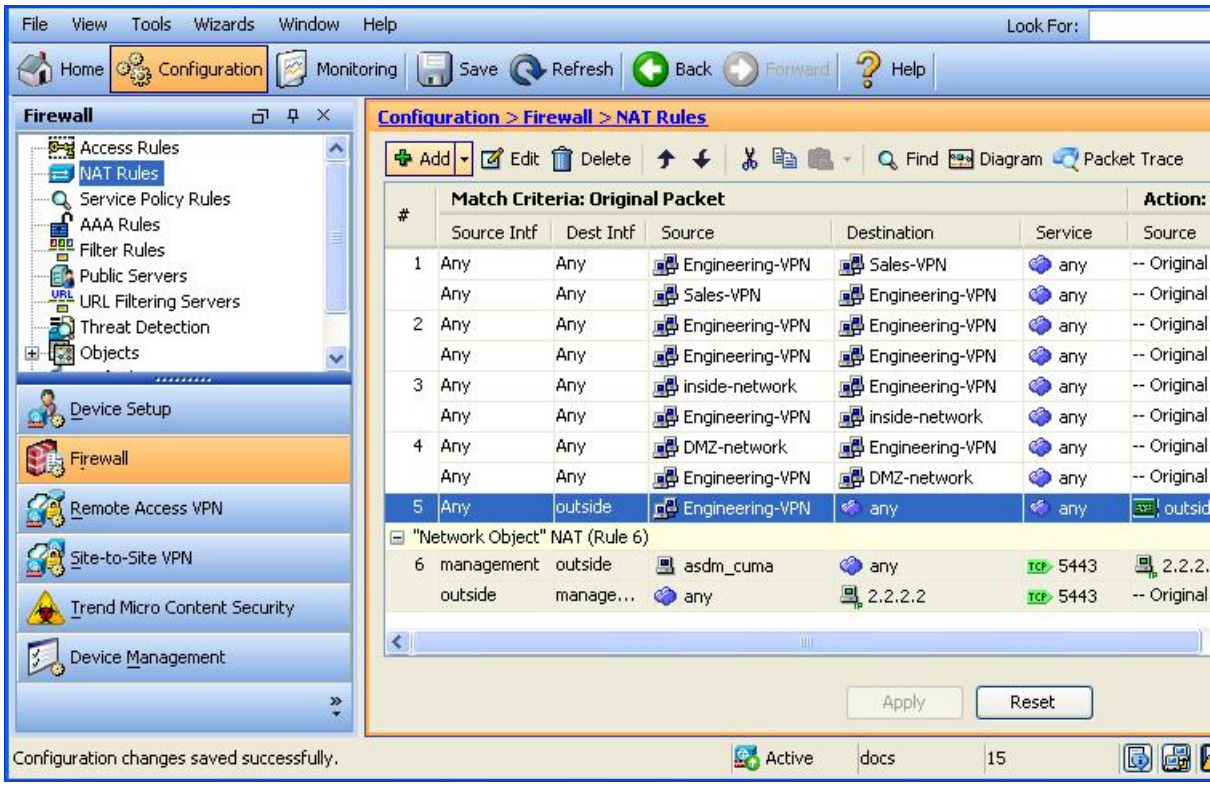
e) 点击**确定**。

f) 点击**应用**。

CLI 示例：

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

图 5: 统一 NAT 表



步骤 8 将 Engineering VPN 地址池配置为到达其自身、Sales VPN 地址池、内部网络、DMZ 网络和互联网后，必须为 Sales VPN 地址池重复此过程。使用身份 NAT 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。

Secure Client HostScan

Secure Client HostScan（现在称为 Secure Firewall Posture）使 Secure Client 能够识别主机上安装的操作系统、反恶意软件、 和防火墙软件。Cisco Secure Firewall Posture/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 Cisco Secure Firewall Posture/HostScan。

ASDM UI 是动态的，因为如果加载了 HostScan，它将反映 HostScan。在加载 Cisco Secure Firewall Posture 后，它将反映安全防火墙安全评估。不同的命名取决于您所运行的版本。

HostScan/Cisco Secure Firewall Posture 的前提条件

具有 Cisco Secure Firewall Posture/HostScan 的 Secure Client至少需要以下 ASA 组件：

- ASA 8.4

- ASDM 6.4

您必须安装 Cisco Secure Firewall Posture/HostScan 才能使用 SCEP 身份验证功能。

有关 Cisco Secure Firewall Posture/HostScan 安装支持的操作系统，请参阅支持的 VPN 平台，思科 ASA 系列。

Secure Client HostScan/Cisco Secure Firewall Posture 的许可

以下是 Cisco Secure Firewall Posture/HostScan 的许可要求：

- Secure Client 适用于基本 HostScan/安全防火墙安全评估的 Advantage (Apex)。
- 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/Cisco Secure Firewall Posture

使用 ASDM，按照以下程序安装或升级 HostScan/Cisco Secure Firewall Posture 程序包并启用 HostScan。ASDM UI 是动态的，因为如果加载了 HostScan，它将反映 HostScan。在加载 Cisco Secure Firewall Posture 后，它将反映安全防火墙安全评估。不同的命名取决于您所运行的版本。

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《Secure Client 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 如果您使用的是版本 5，请将 secure-firewall-posture-*version*-k9.pkg 文件下载到您的计算机。对于版本 4.x，文件为 hostscan_*version*-k9.pkg。

步骤 2 打开 ASDM 并选择**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 安全状态**（对于 **Cisco Secure Firewall**）**(Posture [for Secure Firewall]) > 安全状态映像 (Posture Image)**。如果您使用的是 HostScan 4.x 版本，路径将为**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 安全桌面管理器 (Secure Desktop Manager) > 主机扫描映像 (Host Scan Image)**。

步骤 3 点击**上传 (Upload)**，准备从您的计算机上将 HostScan/Cisco Secure Firewall Posture 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 (Browse Local Files)**，在本地计算机上搜索 HostScan/Cisco Secure Firewall Posture 程序包。

步骤 5 选择前文所述已下载的 hostscan_*version*-k9.pkg or secure-firewall-posture-*version*-k9.pkg 文件，然后点击**选择 (Select)**。您所选文件的路径显示在“本地文件路径”(Local File Path) 字段中，而“闪存文件系统路径”字段显示的是 HostScan/Cisco Secure Firewall Posture 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 (Upload File)**。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 (OK)**。

步骤 8 在“使用上传的映像”(Use Uploaded Image) 对话框中，点击**确定 (OK)**使用您刚上传的 HostScan/Cisco Secure Firewall Posture 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 (Enable HostScan)** 或**启用安全状态映像 (Enable Posture Image)**。

步骤 10 单击**应用 (Apply)**。

步骤 11 从“文件”(File) 菜单中，选择**将运行配置保存到闪存中 (Save Running Configuration To Flash)**。

卸载 HostScan/Cisco Secure Firewall Posture

卸载 HostScan/Cisco Secure Firewall Posture 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，即使启用了它也是如此。卸载 HostScan/Cisco Secure Firewall Posture 不会从闪存驱动器中删除程序包。

过程

步骤 1 在 ASDM 中，导航至**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 安全状态 (Posture)**（对于 **Cisco Secure Firewall**）**> 安全状态映像 (Posture Image)** 以卸载 Cisco Secure Firewall Posture。如果您正在使用 AnyConnect 4.x 版本并卸载 HostScan，请导航至**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 安全桌面管理器 (Secure Desktop Manager) > 主机扫描映像 (Host Scan Image)**。

步骤 2 点击**卸载 (Uninstall)**，然后点击**是 (Yes)** 确认。

步骤 3 点击**卸载 (Uninstall)**。

将 Secure Client 功能模块分配到组策略

此程序将 Secure Client 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 Secure Client 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 Secure Client 功能模块。

anyconnect modules value *Cisco Secure Firewall 模块 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	Cisco Secure Firewall 模块/功能名称
dart	安全客户端 DART（诊断和报告工具）
vpngina	安全客户端 SBL（登录前开始）
posture	Cisco Secure Firewall Posture/HostScan
nam	安全客户端 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	安全客户端 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

磁盘加密

对于 Windows、macOS 和 Linux，点击“配置 > 远程访问 VPN > Posture (对于 Cisco Secure Firewall) > Posture 设置 > 配置 > 高级终端评估窗口”中的 **身份加密磁盘** 复选框，启用安装在终端上的磁盘加密产品的报告终端。在 csc_cscan 日志中，您可以找到磁盘的版本详细信息和加密状态。

此功能仅适用于 Secure Client 5.0.02075（或更高版本）和 ASDM 7.19.1（或更高版本）。

HostScan/Cisco Secure Firewall Posture 相关文档

在 HostScan/Cisco Secure Firewall Posture 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。

以下文档详细介绍了这些主题：《思科自适应安全设备管理器配置指南》。另请参阅《思科安全客户端（包括 *AnyConnect*）管理员指南》，以获取有关 HostScan/Cisco Secure Firewall Posture 如何与 Secure Client配合工作的详细信息。

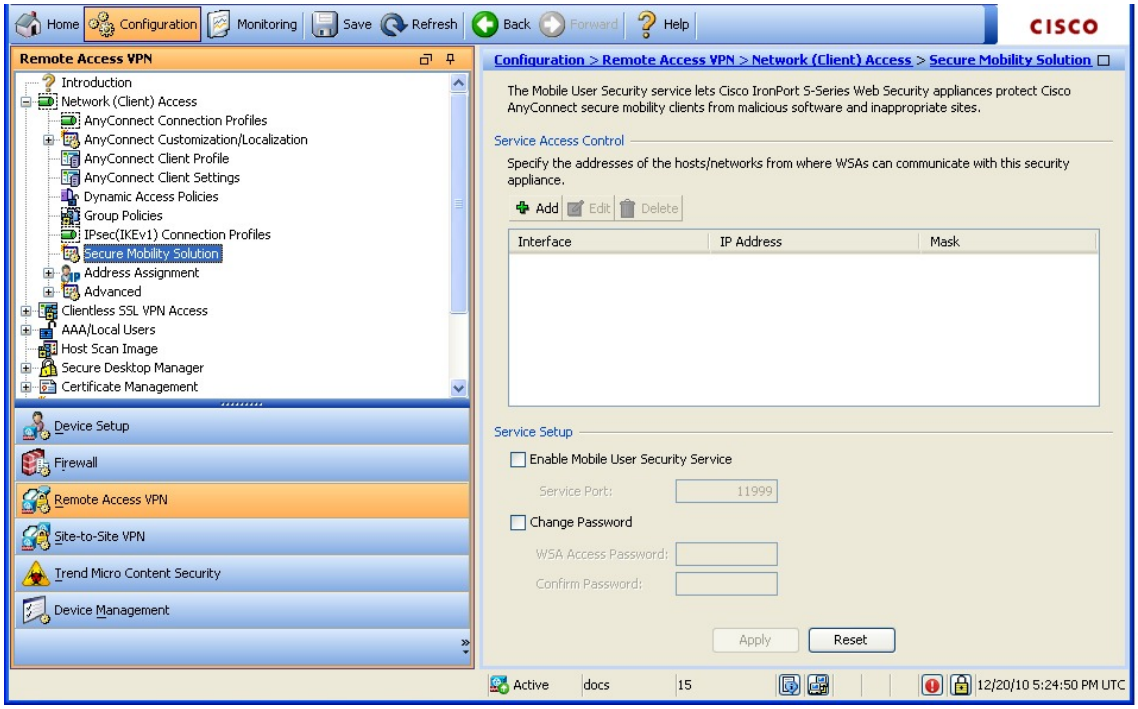
Cisco Secure Client 解决方案

当员工处于移动状态时，安全客户端保护公司利益和资产免受互联网威胁。通过安全客户端，IronPort S 系列网络安全设备可以扫描安全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 此功能需要可为安全客户端提供安全客户端许可支持的 Cisco IronPort Web 安全设备发行版。它还需要支持安全客户端功能的 Secure Client 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 *6:* 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“配置 > 远程访问 VPN > 网络（客户端）访问 > 安全移动解决方案”下的“添加或编辑 MUS 访问控制”对话框为 Secure Client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。

Secure Client 自定义和本地化

您可以定制Cisco 安全客户端 AnyConnect VPN 模块，向远程用户显示您自己的公司图像。通过 Secure Client 自定义/本地化下的以下字段，可以导入以下类型的定制文件：

- **Resources**- 修改的 Secure Client GUI 图标。
- **Binary**- 用于替换 Secure Client 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 Secure Client 进行 VPN 连接前后运行的脚本。
- **GUI Text and Messages**- Secure Client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：

- **导入** 启动“导入 Secure Client 自定义对象”对话框，可以在其中指定要作为对象导入的文件。
- **导出** 启动“导出 Secure Client 自定义对象”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。

Secure Client 定制和本地化，资源

导入的自定义组件的文件名必须与 Secure Client 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 Secure Client 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。

如果导入图像作为资源文件（如 company_logo.bmp），导入的图像将自定义 Secure Client，直至您重新导入另一个使用相同文件名的图像。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。

Secure Client 定制和本地化、二进制和脚本

Secure Client 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 Secure Client API 的客户端。通过替换客户端二进制文件来替换 Secure Client GUI 和 Secure Client CLI。

Import对话框的字段包括：

- **Name** 输入要替换的 Secure Client 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。

Secure Client 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《思科安全客户端的 AnyConnect VPN 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。

  Secure Client 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。

Secure Client 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 Secure Client 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。

Secure Client 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 Secure Client 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 安全客户端 管理指南。

Secure Client 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。

Secure Client 自定义属性

自定义属性会被发送到Secure Client，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。有关配置这些自定义属性的信息，请参阅在内部组策略中配置安全客户端自定义属性。创建并设置自定义属性用于许多不同用途：

- **DSCPPreservationAllowed**：要启用 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)。它让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《Cisco 安全客户端管理指南》中的启用 *DSCP* 预留部分。

值 - 默认情况下，Secure Client 会执行 DSCP 预留 (True)。要禁用该功能，请将头端上的自定义属性值设置为 false，并重新启动连接。

- **DeferredUpdateAllowed or DeferredUpdateAllowed_ComplianceModule**：要在 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，Secure Client 会打开一个对话框，询问用户希望立即更新还是延迟更新。有关其他信息，请参阅启用 Secure Client延迟升级或《Cisco 安全客户端管理指南》中的在 *ASA* 上配置延迟更新。

  值 - True/False：True 可以启用延迟更新。如果延迟更新被禁用 (false)，以下设置会被忽略。

  - **DeferredUpdateMinimumVersion_ComplianceModule 或 DeferredUpdateMinimumVersion** - 要使更新可延迟，必须安装的最低版本 Secure Client。

    值 - xxx，默认值为 0.0.0

  - **DeferredUpdateDismissTimeout** - 延迟升级提示在自动关闭之前显示的秒数。仅在显示延迟更新提示时适用。

    值 - 0 到 300 秒。默认值为 150 秒。

  - **DeferredUpdateDismissResponse** - 发生 DeferredUpdateDismissTimeout 时采取的操作。

    值 - Defer 或 update。默认值为 update。

- **dynamic-split-exclude-domains <attribute name> <list of domains> 或 dynamic-split-include-domains <attribute name> <list of domains>**：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《Cisco 安全客户端管理指南》中的关于动态分割隧道。

  值 - 属性名称是您选择的任何名称。例如，anyconnect-custom-data dynamic-split-exclude-domains excludedomains webex.com, ciscospark.com。

- **managementTunnelAllAllowed**：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）。

  值 - true/false。要覆盖此行为，请将属性名称和值都设置为 *true*。如果配置为全隧道、分割包含、分割排除或绕过两种 IP 协议这几种配置之一，则 Secure Client 会继续进行管理隧道连接。

- **UseLocalProfileAsAlternative**：如果要分发带外配置文件（使用 SCCM、MDM、SecureX 云管理等），而不在 Cisco Secure Firewall ASA 上配置 Cisco Secure 客户端配置文件（以前称为 AnyConnect 配置文件），则可以使用 *UseLocalProfileAsAlternative* 自定义属性。在配置此自定义属性时，客户端会将本地（磁盘上）Cisco Secure 客户端配置文件用于其设置和首选项（而不是通常的默认值）。有关其他信息，请参阅管理指南中的《预部署 Cisco Secure 客户端》。

  仅当 1) 将 *UseLocalProfileAsAlternative* 设为已启用，并且 2) 未配置 ASA 组策略配置文件时，才会使用本地配置文件来建立会话。如果配置此自定义属性，并且未从 ASA 上的组策略配置中撤消或删除 Cisco Secure 客户端配置文件，则在组策略上配置的 Cisco Secure 客户端配置文件将保留并用于每个连接，其中自定义属性设置将被忽略。

  名称 - 已禁用/已启用

  值 - true/false

- **no-dhcp-server-route**：设置公共 DHCP 服务器路由 - 此自定义属性允许本地 DHCP 流量在配置“隧道发送所有网络”(Tunnel All Network) 时以明文传输。Secure Client 会在 Secure Client 连接时向本地 DHCP 服务器添加特定路由，并在主机的 LAN 适配器上应用隐式过滤器，从而阻止该路由的所有流量（DHCP 流量除外）。有关其他信息，请参阅《Cisco 安全客户端管理指南》中的设置公共 *DHCP* 服务器路由部分

  值 - true/false。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。

- **circumvent-host-filtering**：用于配置 Linux 以支持排除的子网 - 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。

  值 - true/false。将其设为 true。

- **tunnel-from-any-source** -（仅限 Linux）Secure Client 允许在“拆分-包含”或“拆分-排除”隧道模式下具有任何源地址的数据包。它可以允许虚拟机实例或 Docker 容器内部的网络访问。

注释 VM/Docker 使用的网络最初必须从隧道中排除。

- **perapp** - VPN 连接用于移动设备上的特定应用集（仅限 Android 和 Apple iOS）。有关其他信息，请参阅《*Cisco* 安全客户端管理指南》中的“创建 Per App 定制属性”部分。

  值 - 通过从策略工具复制 BASE64 格式并将其粘贴在此处来添加一个或多个值。

要进一步完成这些功能的使用，必须在**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 Polices)** > 菜单中，将大部分定义的自定义属性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 Cisco Secure 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、授权和记帐 (AAA) 会话后更改其属性。当 AAA 中的用户或用户组的策略发生更改时，可以将 CoA 数据包从 ISE 直接发送到 ASA，以重新

初始化身份验证并应用新策略。不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
- Secure Client
- L2TP/IPSec

系统流程如下：

1. 最终用户请求 VPN 连接。
2. ASA 向 ISE 对用户进行身份验证，并且接收提供有限网络访问的用户 ACL。
3. 系统向 ISE 发送记帐启动消息以注册会话。
4. 直接在 NAC 代理和 ISE 之间进行安全状态评估。此过程对 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）收到的记帐记录，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（记帐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 发送定期临时记帐更新消息。

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 隧道中记帐。

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**Secure Client **连接配置文件**。

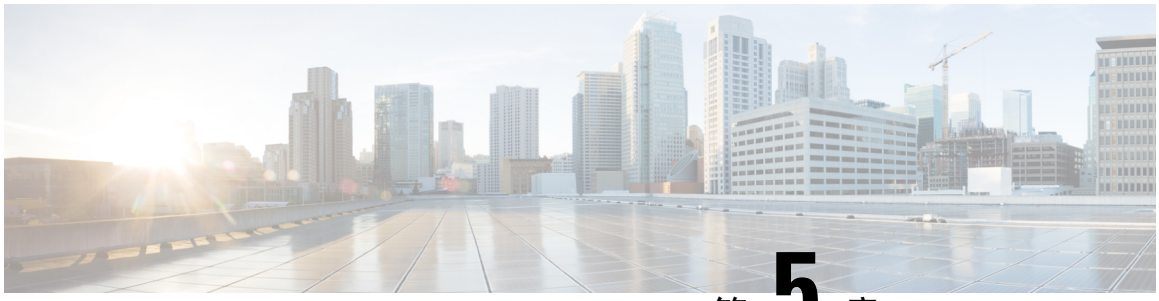
b) 在**连接配置文件**表中，添加或编辑配置文件。

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 (OK)**，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 IP 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 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **地址分配 (Address Assignment)** > **分配策略 (Assignment Policy)**

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、授权和记帐 (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。
- 使用内部地址池：启用在 ASA 上配置的本地地址池。

如果启用 **Use internal address pools**，则也可在释放 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、授权和记帐 (AAA) 服务器，以提供 IP 地址。
- 使用内部地址池：启用在 ASA 上配置的本地地址池。

步骤 4 单击**应用 (Apply)**。

步骤 5 点击**确定 (OK)**。

查看地址分配方法

过程

依次选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **地址分配 (Address Assignment)** > **分配策略 (Assignment Policy)**。

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 **配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **地址管理 (Address Management)** > **地址池 (Address Pools)** > **添加/编辑 IP 池 (Add/Edit IP Pool)**。如要删除地址池，请打开 ASDM 并依次选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络**

（客户端）访问 **(Network [Client] Access) > 地址管理 (Address Management) > 地址池 (Address Pools)**。选择要删除的地址池，然后点击**删除 (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 (Select Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端）访问 (Network [Client] Access) > 地址分配 (Address Assignment) > 地址池 (Address Pools)**。

步骤 2 要添加 IPv4 地址，请依次点击**添加 (Add) > IPv4 地址池 (IPv4 Address pool)**。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**编辑 (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 单击**应用 (Apply)**。

步骤 5 点击**确定 (OK)**。

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 (Select Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **地址分配 (Address Assignment)** > **地址池 (Address Pools)**。

步骤 2 要添加 IPv6 地址，请依次点击**添加 (Add)** > **IPv6 地址池 (IPv6 Address pool)**。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**编辑 (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 单击**应用 (Apply)**。

步骤 5 点击**确定 (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**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)**。

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“组策略”(Group Policy) 对话框中选择“常规属性”(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“选择”(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“选择”(Select) 以添加或编辑 IPv6 地址池。

步骤 5 点击**确定**。

步骤 6 点击**应用**。

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。

以下示例为名为 **firstgroup** 的连接配置文件定义为 172.33.44.19 的 DHCP 服务器。该示例还为名为 **remotegroup** 的组策略将 DHCP 网络范围定义为 10.100.10.1。（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。

开始之前

您只能使用 IPv4 地址标识要分配客户端地址的 DHCP 服务器。此外，DHCP 选项不会转发给用户，他们只会收到地址分配。

过程

步骤 1 配置 DHCP 服务器。

无法使用 DHCP 服务器将 IPv6 地址分配给 Secure Client。

a) 确认已在**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > > **地址分配 (Address Assignment)** > **分配策略 (Assignment Policy)** 中启用 DHCP。

b) 通过选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **DHCP 服务器 (DHCP Server)** 来配置 DHCP 服务器。

步骤 2 在连接配置文件中定义 DHCP 服务器。

a) 选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **安全客户端 (Secure Client) 连接配置文件 (Connection Profiles)**。

b) 在“连接配置文件”(Connection Profiles) 区域中，点击**添加 (Add)** 或**编辑 (Edit)**。

c) 在连接配置文件的配置树中，点击**基本 (Basic)**。

d) 在 Client Address Assignment 区域中，输入要用于向客户端分配 IP 地址的 DHCP 服务器的 IPv4 地址。例如：**172.33.44.19**。

步骤 3 编辑与连接配置文件关联的组策略，以定义 DHCP 范围。

a) 选择**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)**。

b) 双击要编辑的组策略。
c) 在配置树中点击**服务器 (Server)**。
d) 通过点击向下箭头，展开**更多选项 (More Options)** 区域。
e) 取消选中 DHCP 范围**继承**并定义 DHCP 范围。

如果在连接配置文件中为地址池配置了 DHCP 服务器，DHCP 作用域会标识要用于此组的地址池的子网。DHCP 服务器的地址还必须来自此作用域标识的同一个子网。作用域允许您选择 DHCP 服务器中定义的部分地址池，用于此特定组。

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。

要指定范围，请输入与所需池位于同一子网上但不在池内的可路由地址。DHCP 服务器确定此 IP 地址所属的子网并从该地址池分配 IP 地址。

建议尽可能将接口的 IP 地址用于路由目的。例如，如果池为 10.100.10.2-10.100.10.254，接口地址为 10.100.10.1/24，则使用 10.100.10.1 作为 DHCP 范围。请不要使用网络编号。DHCP 仅可用于 IPv4 寻址。如果您选择的地址不是接口地址，可能需要为范围地址创建静态路由。

f) 点击**确定**。
g) 点击**应用**。

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 Secure Client 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 (Configuration) > 远程访问 VPN (Remote Access VPN) > AAA/本地用户 (AAA/Local Users) > 本地用户 (Local Users)**，然后点击**添加 (Add)** 或**编辑 (Edit)**。

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

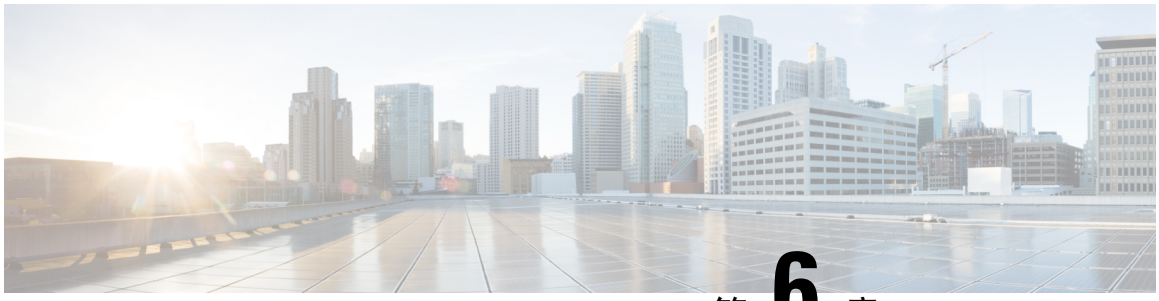
要覆盖每项设置，请取消选中**继承 (Inherit)** 复选框，并输入新值。接下来的详细步骤介绍 IP 地址设置。有关完整的配置详情，请参阅为本地用户配置 VPN 策略属性，第 85 页。

过程

步骤 1 启动 ASDM 并依次选择**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > AAA/本地用户 (AAA/Local Users) > 本地用户 (Local Users)**。
步骤 2 选择要配置的用户，然后点击**编辑 (Edit)**。
步骤 3 在左侧窗格中，点击 **VPN 策略 (VPN Policy)**。
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 (Apply)**，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 Cisco Secure Firewall 终端安全评估模块、独立的 HostScan/Cisco Secure Firewall 终端安全评估软件包和 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	**Cisco Secure Firewall 终端安全评估模块** 主机扫描包 **Cisco Secure Firewall Posture**	**Cisco Secure Firewall 终端安全评估模块** **HostScan 软件包** **Cisco Secure Firewall Posture**	**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	不兼容	不兼容	兼容	兼容
Cisco AnyConnect VPN	兼容	兼容	兼容	兼容
无客户端（基于浏览器的）SSL VPN	兼容	兼容	不兼容	不兼容
PIX 直通代理（终端安全评估不可用）	不兼容	不兼容	不兼容	不兼容

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 HostScan/Cisco Secure Firewall Posture 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。

动态访问策略 (DAP) 需要以下许可证之一：

- Secure Client Premier- 使用所有 DAP 功能。
- Secure Client Advantage- 仅适用于操作系统和操作系统/Secure Client 版本检查。

相关主题

向 DAP 添加 Secure Client 终端属性，第 166 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 HostScan/Cisco Secure Firewall Posture。
- 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》。
- 由于 Java Web Start 安全问题，如果您在设备上使用基于 webvpn 的配置，您可能会发现无法使用配置的值填充高级终端属性。要解决此问题，请使用 ASDM 桌面应用或将 AEA 相关 URL 添加为 Java Security 中的例外项。
- 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 HostScan/Cisco Secure Firewall Posture 属性。有关说明，请在 ASDM 中导航至相应的 UI 屏幕，然后点击 **帮助**。
- DAP 仅支持 ASCII 字符。

过程

步骤 1 启动 ASDM 并选择 **配置** > **远程访问 VPN** > **Network**（客户端）访问 **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**配置**。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 158 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 160 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 161 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 164 页。

d) 点击 **Advanced** 字段，以便#unique_178。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。

有关导入/导出 *dap.xml* 文件的信息，请参阅 在两个 ASA 之间导入和导出 DAP XML 文件，第 159 页。

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 181 页。

步骤 6 点击**确定 (OK)**。

在两个 ASA 之间导入和导出 DAP XML 文件

ASA 的动态访问策略 (DAP) 配置存储在 ASA 闪存上名为 *dap.xml* 的文件中。该文件包含 DAP 策略选择属性。

注释 虽然您可以导出 *dap.xml* 文件，对其进行编辑（如果您了解 xml 语法）并将其重新导入，但要非常小心，因为如果配置错误，可能会导致 ASDM 停止处理 DAP 记录。没有用于操作此部分配置的 CLI。

使用以下步骤在两个 ASA 之间导入和导出 *dap.xml* 文件。

该程序使用从 ASA#1 导出 *dap.xml* 文件并在 ASA#2 上导入 的示例。

有关使用 ASDM 处理 ASA 上的文件的信息，请参阅 *Cisco ASA* 系列常规操作 *ASDM* 配置指南的管理文件部分。

过程

步骤 1 清除 ASA#2 上的 *dap.xml* 文件。

a) 将 ASA#2 配置和 *dap.xml* 从 外部保存到 tftp 或 ftp 服务器。
b) 退出 ASA#2 的 ASDM。

注释 您还可以使用 **ASDM** > **工具** > **备份配置** > **DAP 配置** 选项保存 *dap.xml* 文件。

您还可以重命名或删除 ASA#2 闪存上的 *dap.xml* 文件。

步骤 2 在 ASA#2 命令提示符下，输入 **clear configure dynamic-access-policy-record** 命令以删除 DAP 记录配置。

步骤 3 从 ASA#1 闪存中导出 *dap.xml* 文件，并将其导入到 ASA#2 闪存中。

步骤 4 使用 **dynamic-access-policy-record** 命令在 ASA#2 上配置来自 ASA#1 的 DAP 记录条目。

步骤 5 在 ASA#2 上，使用 **dynamic-access-policy-config activate** 命令启用 DAP。

注释 您还可以重新启动 ASA#2 的 ASDM 以激活 DAP 配置。

步骤 6 在 ASA#2 上重新启动 ASDM。
在 ASA#2 中配置新的 DAP 策略。

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 163 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。
  - 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 163 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 模型）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）

属性类型	属性名称	来源	值	最大字符串长度	说明
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 157 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 172 页。
-
- 有关 HostScan/Cisco Secure Firewall 终端安全评估如何检查内存驻留的反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 171 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 165 页
- 向 DAP 添加应用属性，第 166 页
- 向 DAP 添加 Secure Client 终端属性，第 166 页
- 向 DAP 添加文件终端属性，第 167 页
- 向 DAP 添加设备终端属性，第 168 页
- 向 DAP 添加 NAC 终端属性，第 168 页
- 向 DAP 添加操作系统终端属性，第 169 页
- 向 DAP 添加个人防火墙终端属性，第 169 页
- 向 DAP 添加策略终端属性，第 170 页

- 向 DAP 添加流程终端属性，第 170 页
- 向 DAP 添加注册表终端属性，第 170 页
- 向 DAP 添加多证书身份验证属性，第 171 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 158 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**确定 (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**确定 (OK)**。

向 DAP 添加 Secure Client 终端属性

Secure Client 终端属性，也称为移动终端安全评估或 AnyConnect 标识扩展 (ACIDex)，Cisco 安全客户端 AnyConnect VPN 模块会使用这些属性与 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 HostScan/Secure Firewall Posture 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 Secure Client 相关。某些移动终端安全评估属性与在移动设备上运行的 Secure Client和 Secure Client 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 Secure Client 移动许可证和 Secure Client 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 **终端属性类型** 列表框中，选择 Secure Client。

步骤 2 选中**客户端版本**复选框，并将操作字段设置为等于（=）、不等于（！=）、小于（<）、大于（>）、小于或等于（<=）或大于或等于（>=）然后在**客户端版本**字段中指定的 Secure Client 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 Secure Client，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**确定 (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，请定义要在 HostScan/Cisco Secure Firewall Posture 窗口中扫描的文件。

对于 HostScan 版本 4.x，在 ASDM 中，选择 **配置 > 远程访问 VPN > 安全桌面管理器 > HostScan**。对于 Cisco Secure Firewall Posture 版本 5.x，在 ASDM中，选择 **配置 > 远程访问 VPN > Posture (对于 Cisco Secure Firewall) > Posture 设置**。

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**确定 (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 HostScan/Secure Firewall Posture 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**确定 (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**确定 (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**确定 (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**确定 (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 HostScan/Cisco Secure Firewall Posture 窗口中扫描的进程。

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**确定 (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，请定义要在 HostScan/Cisco Secure Firewall Posture 窗口中扫描的注册表密钥。

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**确定 (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/Secure Firewall Posture 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/Secure Firewall Posture 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/Secure Firewall Posture 将报告系统存在此软件。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/Secure Firewall Posture 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，并且为该程序启用了活动扫描，HostScan/Secure Firewall Posture 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	endpoint.am["*label*"].exists	HostScan/Secure Firewall Posture	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	endpoint.pfw["*label*"].exists	HostScan/Secure Firewall Posture	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 HostScan/Secure Firewall Posture）	endpoint.anyconnect.clientversion	终端	版本	-	Secure Client 版本
	endpoint.anyconnect.platform		字符串	—	Secure Client 上安装了哪个操作系统？
	endpoint.anyconnect.platformversion		版本	64	Secure Client 上安装了哪个版本的操作系统？
	endpoint.anyconnect.devicetype		字符串	64	安装 Secure Client 的移动设备的类型
	endpoint.anyconnect.deviceuniqueid			64	安装 Secure Client 的移动设备的唯一 ID
	endpoint.anyconnect.macaddress		字符串	—	安装 Secure Client 的设备的 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
应用	endpoint.application.clienttype	应用	字符串	—	客户端类型： CLIENTLESS ANYCONNECT IPSEC 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 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 您可以为一条线路定义一个端口 介于 1 和 65535 之间的整数
	endpoint.device. protection_version		字符串	64	设备运行的 HostScan/Cisco Secure Firewall Posture 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		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

属性类型	属性名称	来源	值	最大字符串长度	说明
操作系统	endpoint.os.version		字符串	32	操作系统
	endpoint.os.servicepack		整数	-	Windows 服务包
策略	endpoint.policy.location		字符串	64	
流程	endpoint.process["*label*"].exists		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		*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： [illegible]

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 176 页
- DAP EVAL 表达式示例，第 180 页
- 其他 LUA 函数，第 177 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 172 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）和 Secure Firewall Posture 版本 5 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.
```

多证书身份验证示例

您可以在 DAP 规则中使用多证书身份验证来确定通配符颁发者 CN。

如果您已配置由两个不同的证书颁发机构（例如 abc.cisco.com 和 xyz.cisco.com）颁发给两台不同计算机的两个证书，则 DAP 规则必须具有多个证书身份验证的条件，其中颁发者 CN 为*.cisco.com 或 cisco.com。

您可以使用以下函数为用户和计算机证书使用通配符 issuer_cn cisco.com 定义证书的 DAP 规则：

```
assert(
 function()
```

```
  if ((string.find(endpoint.cert[1].issuer.cn[0], "cisco.com") ~= nil) and
   (string.find(endpoint.cert[2].issuer.cn[0], "cisco.com") ~= nil)) then
     return true;
 end
 return false;
end)()
```

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"))`
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“访问属性”部分，在最左侧的选项卡“操作”中，点击 **终止**。
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 安全客户端 功能的发行版 Secure Client 。

- 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，请所有承包商阅读说明。

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。

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。
- **Secure Client**-使用 Cisco Secure 客户端映像的 AnyConnect VPN 模块连接

  。
- **Web-Portal** - 使用无客户端 VPN 进行连接。
- **Both-default-Web-Portal**-通过无客户端或 Secure Client客户端进行连接，默认使用无客户端。
- **Both-default-Secure Client**-通过无客户端或 Secure Client进行连接，默认使用 Secure Client。

步骤 8 选择 **Secure Client** 选项卡，以选择永远在线 VPN 标志状态。

- Secure Client Always-On VPN - 确定是否没有改变、禁用了 Secure Client 服务配置文件中的永久在线 VPN 标志设置，或者是否应使用 Secure Client 服务配置文件设置。

  此参数需要为 Cisco 安全客户端的 AnyConnect VPN 模块提供安全移动解决方案许可支持的思科网络安全设备版本。它还需要支持“安全移动解决方案”功能的 Secure Client 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 Secure Client **自定义属性** 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 Secure Client，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 Secure Client 版本的 *Cisco Secure Client*管理员指南。

自定义属性可以在**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 >** Secure Client**自定义属性**和**Secure ClientYY 自定义属性名称**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 DAP 配置 SAML 授权

您可以使用 DAP 配置 SAML 授权和组策略选择，而不必依赖外部服务器（RADIUS 或 LDAP）来检索授权属性。

可以将 SAML 身份提供程序配置为除身份验证断言外还发送授权属性。ASA 中的 SAML 服务提供程序组件解释 SAML 断言，并根据收到的断言进行授权或组策略选择。使用 ASDM 配置的 DAP 规则处理断言属性。

组策略属性必须使用属性名称 **cisco_group_policy**。此属性不依赖于正在配置的 DAP。但是，如果配置了 DAP，则可以将其用作 DAP 策略的一部分。

组策略对象选择

当接收到名为 **cisco_group_policy** 的属性时，相应的值会被用于选择连接组策略。

建立连接后，可以从多个源获取组策略信息，并将其组合以形成应用于连接的有效组策略。

组合收到的组策略信息时，可能出现以下情况：

在 SAML 身份验证中接收的组策略，未配置授权

在这种情况下，有效的组策略按优先级降序确定：

1. SAML 属性中指定的组策略。
2. 在隧道组中指定的组策略。
3. 默认组策略。

在 SAML 身份验证中接收的组策略，已配置授权

在这种情况下，有效的组策略按优先级降序确定：

1. 授权属性中指定的组策略。
2. 用户组策略：使用从授权服务器返回的值（如果有）。
3. 用户组策略：使用 SAML 属性中返回的值。
4. 在隧道组中指定的组策略。

5. 默认组策略。

过程

步骤 1 在 ASDM，选择 **配置** > **远程访问 VPN** > **网络 (客户端) 访问** > **动态访问策略** > **添加/编辑动态访问策略** 。

步骤 2 在 AAA 属性选择区域中，点击 **添加**。

a) 从 **AAA 属性类型** 下拉列表中，选择 SAML。

b) 指定 *memberOf* 作为 **属性 ID**。

c) 输入 *memberOf* 属性 **值** ，如果已配置 AD 服务器组，请点击 **Get AD Group** 。

要配置其他 AD 服务器组，请转至 **配置** > **远程访问 VPN** > **AAA/本地用户** > **AAA 服务器组**。

要配置组策略选择属性，请根据需要在同一 DAP 策略或另一个 DAP 策略中选择以下设置：

- **AAA 属性类型**：SAML
- **属性 ID**：cisco_group_policy
- **值**：组策略的名称

步骤 3 点击**确定 (OK)**。

步骤 4 点击 **确定 (OK)** 保存 DAP 策略。

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

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 Cisco Secure 客户端的 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	不受信任
Endpoint Attribute Process	ieexplore.exe	-
Advanced Endpoint Assessment	AntiVirus= McAfee Attribute	
CSD Location	Trusted	不受信任
LDAP memberOf	Engineering, Managers	Vendors
ACL		Web-Type ACL
Access	**Secure Client** 和 **Web** 门户	**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 Secure Client）、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。

使用 DAP 检查会话令牌安全

当 ASA 对来自 Secure Client的 VPN 连接请求进行身份验证时，ASA 会向客户端返回会话令牌。从 AnyConnect 4.9 (MR1) 开始，ASA 和 Secure Client 支持为会话令牌提供增强安全性的机制。您必须配置 DAP 以确保 Secure Client 支持会话令牌安全。

使用此DAP与终端属性设置和LUA脚本拒绝来自不支持令牌安全的Secure Client版本的连接尝试。

过程

步骤 1 在 ASDM，选择 **配置** > **远程访问 VPN** > **网络 (客户端) 访问** > **动态访问策略** > **添加/编辑动态访问策略** 。

步骤 2 在终端属性选择区域中，点击 **添加**。

a) 从 **终端属性类型** 下拉列表中，选择应用。

b) 对于 **客户端类型**，选择等号 (=) 运算符，然后从下拉列表中选择 Secure Client 。

c) 点击**确定 (OK)**。

步骤 3 配置 **高级** 选择条件：

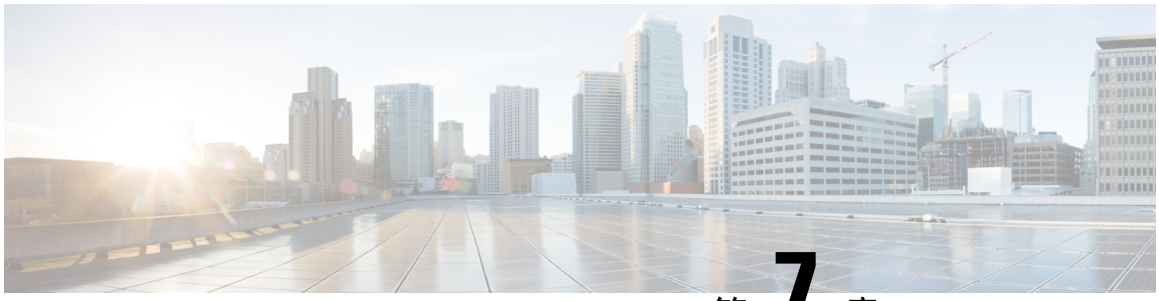
a) 选择 **AND** 运营商。

b) 添加 **逻辑表达式**

```
(type(endpoint.anyconnect.session_token_security)~="string" or
EVAL(endpoint.anyconnect.session_token_security,"NE","true","string"))
```

步骤 4 在 **操作** 区域中，选择 **终止**。

步骤 5 添加可选的用户消息，然后点击 **确定**。



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**。

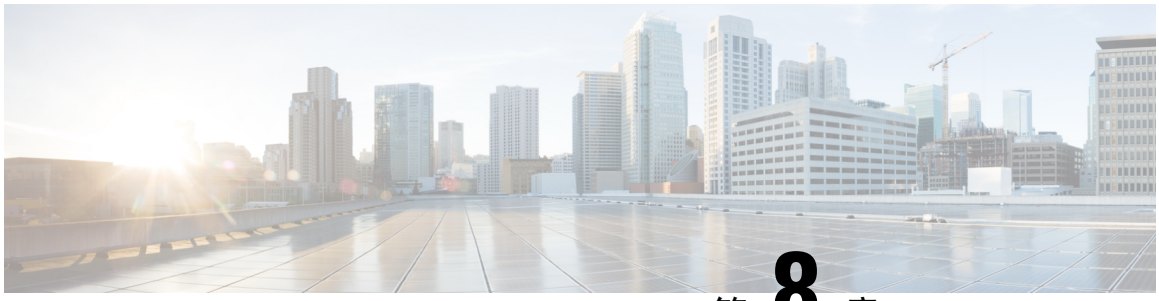
步骤 2 配置以下字段：

- 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或 LAN 到 LAN 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。
- 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。

监控主用 VPN 会话

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 Secure Client 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。

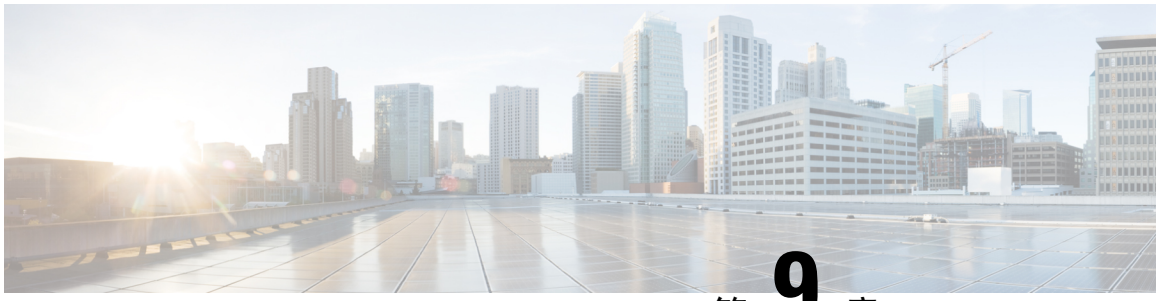
Monitor Protocol Statistics

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。



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，DTLS 还会用于安全客户端连接。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**确定 (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）。

SSL 设置

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）。
TLSV1.3	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 的配置和使用方法仅适用于 Cisco Secure 客户端的 AnyConnect VPN 模块连接。

请使用与 DTLS 版本相等或更高版本的 TLS，确保 TLS 会话与 DTLS 会话同样安全或更安全。DTLSV1.2 支持 TLSV1.2 和 TLSV1.2。任何 TLS 版本均可与 DTLS1 配合使用，因为它们都等于或大于 DTLS 1。

TLSV1.3 需要使用 Cisco Secure 客户端版本 5.0 及更高版本。

- **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）。
TLSv1.3	传输 TLSv1.3 客户端问候并协商 TLSv1.3（或更高版本）。

- **要与 SSL 配合使用的 Diffie-Hellmann 组 (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。
- **要与 SSL 配合使用的 ECDH 组 (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**编辑 (Edit)**，使用“配置密码算法/自定义字符串”(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**确定 (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 包含带有 SHA-2 加密的 AES-256，并且仅适用于 TLS 版本 1.2 和 TLS 版本 1.3 支持的密码。

    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 TLSv1.3/TLSv1.2 支持的密码，优先级最低的是 TLSv1.1、TLSv1.2 或 TLSv1.2 不支持的密码。

支持以下密码：

- **服务器名称指示 (SNI)** - 指定域名并与之关联。点击**添加 (Add)** 或**编辑 (Edit)**，使用“添加/编辑服务器名称指示”(Add/Edit Server Name Indication [SNI]) 对话框定义或编辑每个接口的域和信任点。

密码	TLSv1.1/DTLSV1	TLSV1.2/DTLSV1.2	TLSv1.3
TLS_AES_128_GCM_SHA256	否	否	是
TLS_CHACHA20_POLY1305_SHA256	否	否	是
AES256-GCM-SHA384	否	否	是
AES128-GCM-SHA256	否	是	否
AES128-SHA	是	是	否
AES128-SHA256	否	是	否

密码	TLSv1.1/DTLSV1	TLSV1.2/DTLSV1.2	TLSv13
AES256-GCM-SHA384	否	是	否
AES256-SHA	是	是	否
AES256-SHA256	否	是	否
DERS-CBC-SHA	否	否	否
DES-CBC-SHA	是	是	否
DHE-RSA-AES128-GCM-SHA256	否	是	否
DHE-RSA-AES128-SHA	是	是	否
DHE-RSA-AES128-SHA256	否	是	否
DHE-RSA-AES256-GCM-SHA384	否	l	否
DHE-RSA-AES256-SHA	是	是	否
ECDHE-ECDSA-AES128-GCM-SHA256	否	是	否
ECDHE-ECDSA-AES128-SHA256	否	是	否
ECDHE-ECDSA-AES256-GCM-SHA384	否	是	否
ECDHE-ECDSA-AES256-SHA384	否	是	否
ECDHE-RSA-AES128-GCM-SHA256	是	是	否
ECDHE-RSA-AES128-SHA256	否	是	否
ECDHE-RSA-AES256-GCM-SHA384	否	是	否
ECDHE-RSA-AES256-SHA384	否	是	否
NULL-SHA	否	否	否
RC4-MD5	否	否	否
RC4-SHA	否	否	否

注释 DTLS1.2 隧道适用于 TLSv1.3，但 DTLS1.2 不支持 TLSv1.3 密码。为 DTLS1.2 隧道选择支持的最高优先级密码。

- Specify domain - 输入域名。

  - “选择要与域关联的信任点 ”(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**编辑 (Edit)**，使用“选择 SSL 证书”(Select SSL Certificate) 对话框为每个接口定义或修改信任点。
  - “主要登记的证书”(Primary Enrolled Certificate) - 为此接口上的证书选择要使用的信任点。
  - “负载均衡登记的证书”(Load Balancing Enrolled Certificate) - 选择配置 VPN 负载均衡时用于证书的信任点。
- **回退证书 (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 (None)**，则 ASA 将使用默认 RSA 密钥对和证书。
- **Forced Certification Authentication Timeout** - 配置证书身份验证超时之前等待的分钟数。
- **应用 (Apply)** - 点击以保存您的更改。
- **重置 (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。

SSL 设置

第 10 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。作为策略型 VPN 的替代方案，您可以在 VTI 的对等体之间创建 VPN 隧道。VTI 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。您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。

静态 VTI

您可以使用静态 VTI 配置进行站点间连接，其中两个站点之间的隧道会始终在线。对于静态 VTI 接口，您必须将物理接口定义为隧道源。每个设备最多可以关联 1024 个 VTI。要创建静态 VTI 接口，请参阅添加 VTI 接口，第 215 页。

动态 VTI

动态 VTI 为站点间 VPN 提供高度安全且可扩展的连接。动态 VTI 简化了大型企业中心辐射型部署的对等体配置。单个动态 VTI 可以替换中心上的多个静态 VTI 配置。您可以将新的分支添加到中心，而无需更改中心配置。动态 VTI 取代动态加密映射和用于建立隧道的动态中心辐射型方法。在管理中心，动态 VTI 仅支持中心辐射型拓扑。

动态 VTI 会使用虚拟模板来进行 IPsec 接口的动态实例化和管理。虚拟模板会为每个 VPN 会话动态生成独一无二的虚拟访问接口。动态 VTI 支持多个 IPsec 安全关联，并接受分支提议的多个 IPsec 选

择器。动态 VTI 也支持动态 (DHCP) 分支。要创建动态 VTI 接口，请参阅添加动态 VTI 接口，第 218 页。

ASA 如何为 VPN 会话创建动态 VTI 隧道

1. 在 ASA 上创建虚拟模板（选择**配置 (Configuration) > 设备设置 (Device Setup) > 接口设置 (Interface Settings) > 接口 (Interfaces) > 添加 (Add) > DVTI 接口 (DVTI Interface)**）。

   您可以将此模板用于多个 VPN 会话。
2. 将此模板附加到隧道组。您可以将虚拟模板连接到多个隧道组。
3. 分支会向中心发起隧道请求。
4. 中心对分支进行身份验证。
5. ASA 使用虚拟模板来为与分支的 VPN 会话动态创建虚拟访问接口。
6. 中心会使用虚拟接入接口与分支建立动态 VTI 隧道。
7. 配置 IKEv2 路由集接口 选项，以通告 VTI 接口 IP over IKEv2 交换。此选项可在 VTI 接口之间启用单播可访问性，以便 BGP 或路径监控通过隧道运行。
8. 在 VPN 会话结束后，隧道将断开连接，中心将删除相应的虚拟接入接口。

Virtual Tunnel Interface 准则

情景模式和集群

- 仅支持单一模式。
- 不支持集群。

防火墙模式

仅在路由模式中受支持。

BGP IPv4 和 IPv6 支持

支持 VTI 上的 IPv4 和 IPv6 BGP 路由。

EIGRP 支持

支持 VTI 上的 IPv4 和 IPv6 EIGRP 路由。

OSPF IPv4 和 IPv6 支持

支持 VTI 上的 IPv4 和 IPv6 OSPF 路由。

IPv6 支持

- 可以配置 IPv6 寻址的 VTI。
- VTI 的隧道源和隧道目标都可以有 IPv6 地址。
- 支持以下 VTI IP（或内部网络 IP 版本）与公共 IP 版本的组合：
  - IPv6 over IPv6
  - 基于 IPv6 的 IPv4
  - IPv4 over IPv4
  - 基于 IPv4 的 IPv6
- 仅支持将静态 IPv6 地址作为隧道源和目的地址。
- 隧道源接口可以有一个 IPv6 地址，并且您可以将该地址指定用作隧道终端。如果不指定，列表中的第一个 IPv6 全局地址会被默认用作隧道终端。
- 您可以将隧道模式指定为 IPv6。如已指定，则 IPv6 流量可以通过 VTI 进行隧道传输。但是，单个 VTI 的隧道模式可以是 IPv4 或 IPv6。

常规配置准则

- 如果在 LAN 到 VPN VPN 中使用动态加密映射和动态 VTI，则仅会出现动态 VTI 隧道。出现此问题的原因是，加密映射和动态 VTI 都尝试使用默认隧道组。

  我们的建议操作如下动作之一：
  - 将 LAN 间 VPN 迁移到动态 VTI。
  - 使用静态加密映射及其自己的隧道组。
- VTI 只有在 IPsec 模式下才可配置。不支持在 ASA 上终止 GRE 隧道。
- 您可以将静态、BGP、OSPF 或 EIGRP IPv4 路由用于使用这种隧道接口的流量。
- 对于静态和动态 VTI，请确保不将借用 IP 接口用作任何 VTI 接口的隧道源 IP 地址。
- VTI 的 MTU 将根据底层物理接口自动设置。但是，如果在启用 VTI 后更改物理接口 MTU，则您必须禁用并重新启用 VTI 才能使用新的 MTU 设置。
- 对于动态 VTI，虚拟接入接口会从配置的隧道源接口继承 MTU。如果不指定隧道源接口，虚拟接入接口将从源接口继承 MTU，而 ASA 会从该接口接受 VPN 会话请求。
- 您最多可以在一台设备上配置 1024 个 VTI。在计算 VTI 计数时，请考虑以下事项：
  - 包括 nameif 子接口，以便得出可在设备上配置的 VTI 总数。
  - 您不能在端口通道的成员接口上配置 nameif。因此，隧道计数只会随实际主端口通道接口的数量减少，而不会随其任何成员接口的数量减少。

- 即使平台支持超过 1024 个接口，VTI 计数也限于该平台上可配置的 VLAN 数量。例如，如果型号支持 5510 VLAN，则隧道计数为 500 减去配置的物理接口数。

- VTI 支持 IKE 版本 v1 和 v2，并使用 IPsec 在隧道的源地址与目的地址之间收发数据。
- 如果必须应用 NAT，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 隧道始终处于活动状态。
- 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。
- 对于站点间隧道组中的 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。
- 可以在 VTI 接口上应用访问规则来控制通过 VTI 的流量。
- VTI 接口之间支持 ICMP ping。
- 如果 IKEv2 站点间 VPN 隧道的对等设备发送 IKEv2 配置请求负载，则 ASA 无法与该设备建立 IKEv2 隧道。您必须在对等设备上禁用 config-exchange 请求，ASA 才能与对等设备建立 VPN 隧道。
- 动态 VTI 支持 HA 和 IKEv2。

默认设置

- 默认情况下，通过 VTI 的所有流量都经过加密。
- 默认情况下，VTI 接口的安全级别为 0。您无法配置安全级别。

动态 VTI 的限制

动态 VTI 不支持：

- ECMP 和 VRF
- 集群
- IKEv1
- QoS

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。此操作不适用于 VTI 逻辑接口。

可以在 VTI 接口上应用访问控制列表来控制通过 VTI 的流量。如要在不检查源和目标接口的 ACL 的情况下允许来自 IPsec 隧道的所有数据包，请在全局配置模式下输入 sysopt connection permit-vpn 命令。

您可以使用以下命令在不检查 ACL 的情况下允许 IPsec 流量通过 ASA：

hostname(config)# sysopt connection permit-vpn

当外部接口和 VTI 接口的安全级别为 0 时，如果您在 VTI 接口上应用了 ACL，并且尚未配置 same-security-traffic，则不会命中该接口。

要配置此功能，请在全局配置模式下使用 **same-security-traffic** 命令及其 **intra-interface** 参数。

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 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 **(Configuration)** > 站点间 **VPN (Site-to-Site VPN)** > 高级 **(Advanced)** > **IPsec** 提议（转换集）**(IPsec Proposals [Transform Sets])**。

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）”(IKEv1 IPsec Proposals [Transform Sets])面板中，点击**添加 (Add)**。
b) 输入**转换集名称**.
c) 保留**隧道 (Tunnel)** 复选框的默认选择。
d) 选择 **ESP 加密 (ESP Encryption)**和 **ESP 身份验证 (ESP Authentication)**。
e) 点击**确定 (OK)**。

- 配置 IKEv2。

a) 在“IKEv2 IPsec 提议”(IKEv2 IPsec Proposals) 面板中，点击**添加 (Add)**。
b) 输入**名称**和**加密**。
c) 选择**完整性散列 (Integrity Hash)**。
d) 点击**确定 (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 **(Configuration)** > 站点间 **VPN (Site-to-Site VPN)** > 高级 **(Advanced)** > **IPsec** 提议（转换集）**(IPsec Proposals [Transform Sets])**。

步骤 2 在 **IPsec 配置文件 (IPsec Profile)** 面板中，点击**添加 (Add)**。

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 (Responder only)** 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 (Enable security association lifetime)** 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 (PFS Settings)** 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 (Enable sending certificate)** 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 (Chain)** 复选框。

步骤 9 选中**启用反向路由注入 (Enable Reverse Route Injection)** 复选框，为此 IPsec 配置文件启用反向路由注入 (RRI)。

RRI 会填充运行动态路由协议（例如 OSPF、EIGRP）的内部路由器的路由表，或者为远程 VPN 客户端或 LAN 到 LAN 会话填充 RIP。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。如果将任何源/目标 (0.0.0.0/0.0.0.0) 指定为受保护网络，请勿启用 RRI，否则会影响使用默认路由的流量。

步骤 10 选中**动态 (Dynamic)** 复选框，将反向路由设置为动态。

步骤 11 点击**确定 (OK)**。

步骤 12 在 **IPsec 提议（转换集）(IPsec Proposals [Transform Sets])**主面板中，点击**应用 (Apply)**。

步骤 13 在**预览 CLI 命令 (Preview CLI Commands)** 对话框中，点击**发送 (Send)**。

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 选择**配置 (Configuration)** > **设备设置 (Device Setup)** > **接口设置 (Interface Settings)** > **接口 (Interfaces)**。

步骤 2 选择**添加 (Add)** > **VTI 接口 (VTI Interface)**。系统将显示**添加 VTI 接口**窗口。

步骤 3 在**常规 (General)** 选项卡上：

a) 输入 **VTI ID**。范围为 0 到 10413。最多可支持 10413 个 VTI 接口。

b) 输入 **Interface Name**。

c) 确保**启用接口 (Enable Interface)** 复选框已选中。

d) 从**路径监控 (Path Monitoring)** 下拉列表中选择 **IPv4** 或 **IPv6**，然后输入对等体的 IP 地址。

e) 输入**成本 (Cost)**。范围是从 1 到 65535。

成本将决定在多个 VTI 之间对流量进行负载均衡的优先级。最小的数字具有最高优先级。

f) 对于配置 IP 地址：

点击**地址 (Address)** 单选按钮，以便配置 IP 地址和子网掩码。

或

点击**未编号 (Unnumbered)** 单选按钮，以便从**未编号 IP (IP Unnumbered)** 下拉列表选择要借用其 IP 地址的接口。您可以从列表中选择环回接口或物理接口。

步骤 4 在**高级 (Advanced)** 选项卡中。

a) 输入**目标 IP** (Destination IP)。

b) 从**源接口 (Source Interface)** 下拉列表中选择隧道源接口。

您可以选择环回接口或物理接口。

c) 在**使用 IPsec 策略实现隧道保护 (Tunnel Protection with IPsec Policy)** 字段中选择 IPsec 策略。

d) 在**使用 IPsec 配置文件实现隧道保护 (Tunnel Protection with IPsec Profile)** 字段中选择 IPsec 配置文件。

e) 选中**确保启用隧道模式 IPv4 IPsec (Ensure the Enable Tunnel Mode IPv4 IPsec)** 复选框。

步骤 5 点击**确定 (OK)**。

步骤 6 在**接口 (Interfaces)** 面板中，点击**应用 (Apply)**。

步骤 7 在**预览 CLI 命令 (Preview CLI Commands)** 对话框中，点击**发送 (Send)**。

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。

示例

ASA 与 IOS 设备之间的 VTI 隧道（采用 IKEv2）配置示例：

```
ASA□

crypto ikev2 policy 1
 encryption aes-gcm-256
 integrity null
 □ 21
 prf sha512
 lifetime seconds 86400
!
```

```
crypto ipsec ikev2 ipsec-proposal gcm256
 protocol esp encryption aes-gcm-256
 protocol esp integrity null
!
crypto ipsec profile asa-vti
 set ikev2 ipsec-proposal gcm256
!
interface Tunnel 100
 nameif vti
 ip address 10.10.10.1 255.255.255.254
 tunnel source interface [asa-source-nameif]
 tunnel destination [router-ip-address]
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile asa-vti
!
tunnel-group [router-ip-address] ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
crypto ikev2 enable [asa-interface-name]


IOS□

!
crypto ikev2 proposal asa-vti
 encryption aes-gcm-256
 prf sha512
 □ 21
!
crypto ikev2 policy asa-vti
 match address local [router-ip-address]
 proposal asa-vti
!
crypto ikev2 profile asa-vti
 match identity remote address [asa-ip-address] 255.255.255.255
 authentication local pre-share key cisco
 authentication remote pre-share key cisco
 no config-exchange request
!
crypto ipsec transform-set gcm256 esp-gcm 256
!
crypto ipsec profile asa-vti
 set ikev2-profile asa-vti
 set transform-set gcm256
!
interface tunnel 100
 ip address 10.10.10.0 255.255.255.254
 tunnel mode ipsec ipv4
 tunnel source [router-interface]
 tunnel destination [asa-ip-address]
 tunnel protection ipsec profile asa-vti
!
```

添加动态 VTI 接口

要为动态 VTI 创建虚拟模板，请执行以下操作：

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》中的“配置静态路由跟踪”，地址是：http://www.cisco.com/go/asa-config。

开始之前

确保您已配置 IPsec 配置文件和 IP 未编号接口。

过程

步骤 1 选择**配置 (Configuration)** > **设备设置 (Device Setup)** > **接口设置 (Interface Settings)** > **接口 (Interfaces)**。

步骤 2 选择**添加 (Add)** > **DVTI 接口 (DVTI Interface)**。系统将显示**添加 DVTI 接口 (Add DVTI Interface)** 窗口。

步骤 3 在**常规 (General)** 选项卡上：

a) 输入 **DVTI ID**。该 ID 可以是 1 到 10413 之间的任何值。每台设备最多可支持 1024 个 VTI 接口。

b) 输入 **Interface Name**。

c) 确保选中**启用接口 (Enable Interface)** 复选框。

d) 从**未编号 IP (IP Unnumbered)** 下拉列表中选择一个接口。

虚拟模板将继承所选接口的 IP 地址。确保使用不同于隧道源 IP 地址的 IP 地址。您还可以选择物理接口或设备上配置的环回接口。

e) 在**说明 (Description)** 字段中，输入此动态 VTI 的说明。

步骤 4 在**高级 (Advanced)** 选项卡中：

a) 从**源接口 (Source Interface)** 下拉列表中选择隧道源接口。该接口的 IP 地址将是分支的目标 IP 地址。您只能从列表中选择物理接口和环回接口。

b) 选中**启用 IPv6 源地址 (Enable IPv6 Source Address)** 复选框，以仅接受来自配置了隧道源 IP 地址的接口的 VPN 会话请求。如果没有启用此选项，ASA 将接受来自任何接口的 VPN 会话请求。

虚拟访问接口还会从配置的隧道源接口继承 MTU。如果没有启用上述选项，虚拟访问接口将从源接口继承 MTU，而 ASA 会从该接口接受 VPN 会话请求。

c) 在**使用 IPsec 配置文件实现隧道保护 (Tunnel Protection with IPsec Profile)** 下拉列表中选择 IPsec 配置文件。

d) 选中**为 IPSec 启用隧道模式 IP 覆盖 (Enable Tunnel Mode IP Overlay for IPSec)** 复选框，然后选择 **IPv4** 或 **IPv6** 单选按钮以启用 IPsec 隧道模式。

步骤 5 在 **IPv6** 选项卡中：

a) 点击**未编号的 IPv6 地址 (IPv6 Address Unnumbered)** 浏览按钮，然后从列表中选择 IPv6 地址。

从虚拟模板克隆的所有虚拟访问接口都将具有相同的 IP 地址。

b) 点击**确定 (OK)**。

步骤 6 在**预览 CLI 命令 (Preview CLI Commands)** 对话框中，您可以查看虚拟模板命令。

步骤 7 点击**发送 (Send)**。

下一步做什么

将此模板附加到隧道组。有关详细信息，请参阅 站点间隧道组 ， 第 117 页。

Virtual Tunnel Interface 的功能历史记录

功能名称	版本	功能信息
动态 Virtual Tunnel Interface 支持	9.19(1)	您可以创建动态 VTI 并使用它在中心辐射型拓扑配置基于路由的站点间 VPN。动态 VTI 简化了大型企业中心辐射型部署的对等体配置。单个动态 VTI 可以替换中心上的多个静态 VTI 配置。您可以将新的分支添加到中心，而无需更改中心配置。 新增/修改的屏幕： **配置 > 设备设置 > 接口设置 > 接口 > 添加 > DVTI 接口**
OSPF IPv4 和 IPv6 支持	9.19(1)	支持 VTI 上的 OSPF IPv4 和 IPv6 路由协议。
EIGRP 支持	9.19(1)	支持 VTI 上的 EIGRP IPv4 和 IPv6 路由协议。
静态和动态 VTI 的环回接口支持	9.19(1)	现在，您可以将环回接口设置为 VTI 的源接口。还添加了支持以从环回接口继承 IP 地址，而不是静态配置的 IP 地址。环回接口有助于克服路径故障。如果接口发生故障，您可以通过分配给环回接口的 IP 地址来访问所有接口。 新增/修改的屏幕： **配置 > 设备设置 > 接口设置 > 接口 > 添加 VTI 接口 > 高级**
本地隧道 ID 支持	9.17(1)	ASA 支持唯一本地隧道 ID，它允许 ASA 在 NAT 后面有多个 IPsec 隧道，以便连接到 Cisco Umbrella 安全互联网网关 (SIG)。本地身份用于为每个 IKEv2 隧道配置唯一身份，而不是为所有隧道配置一个全局身份。
在静态 VTI 上支持 IPv6	9.16（1）	ASA 在虚拟隧道接口 (VTI) 配置中支持 IPv6 地址。 VTI 隧道源接口可以具有 IPv6 地址，您可以将其配置为用作隧道终端。如果隧道源接口有多个 IPv6 地址，您可以指定要使用的地址，否则默认使用列表中的第一个 IPv6 全局地址。 隧道模式可以是 IPv4 或 IPv6，但必须与 VTI 上配置的 IP 地址类型相同，隧道才能处于活动状态。IPv6 地址可以分配给 VTI 中的隧道源或隧道目标接口。

功能名称	版本	功能信息
支持每个设备 1024 个 VTI 接口	9.16（1）	要在设备上配置的最大VTI数量已从 100 增加到 1024。 即使平台支持超过1024个接口，VTI计数也限于该平台上可配置的VLAN数量。例如，ASA 5510 支持 100 个VLAN，隧道计数为 100 减去配置的物理接口数。 新增/修改的菜单项：无
VTI 上的 DHCP 中继服务器支持	9.14(1)	ASA 允许将 VTI 接口配置为 DHCP 中继服务器连接接口。 我们修改了以下屏幕，为 DHCP 中继指定 VTI 接口： **配置 > 设备管理 > DHCP > DHCP 中继 > DHCP 中继接口服务器**
VTI 中支持 IKEv2、基于证书的身份验证和 ACL	9.8.(1)	虚拟隧道接口 (VTI) 现在支持 BGP（静态 VTI）。现在可在独立和高可用性模式下使用 IKEv2。可以通过在IPsec配置文件中设置信任点来使用基于证书的身份验证。还可以使用 access-group 命令，将 VTI 上的访问列表应用于过滤进口流量。 在以下屏幕中引入了几个选项，用于为基于证书的身份验证选择信任点： **配置 (Configuration) > 站点间 VPN (Site-to-Site VPN) > 高级 (Advanced) > IPsec 提议（转换集）(IPsec Proposals [Transform Sets]) > IPsec 配置文件 (IPsec Profile) > 添加 (Add)**
虚拟隧道接口 (VTI) 支持	9.7.(1)	使用新的逻辑接口（称为“虚拟隧道接口 (VTI)”）可增强 ASA，该接口用于向对等体表示 VPN 隧道。这可通过将 IPSec 配置文件连接到隧道的每一端，为基于 VPN 的路由提供支持。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。 引入了以下菜单项： **配置 (Configuration) > 站点间 VPN (Site-to-Site VPN) > 高级 (Advanced) > IPSec 提议（转换集）(IPsec Proposals [Transform Sets]) > IPSec 配置文件 (IPsec Profile)** **配置 (Configuration) > 站点间 VPN (Site-to-Site VPN) > 高级 (Advanced) > IPSec 提议（转换集）(IPsec Proposals [Transform Sets]) > IPSec 配置文件 (IPsec Profile) > 添加 (Add) > 添加 IPSec 配置文件 (Add IPsec Profile)** **配置 (Configuration) > 设备设置 (Device Setup) > 接口设置 (Interface Settings) > 接口 (Interfaces) > 添加 (Add) > VTI 接口 (VTI Interface)** **配置 (Configuration) > 设备设置 (Device Setup) > 接口设置 (Interface Settings) > 接口 (Interfaces) > 添加 (Add) > VTI 接口 (VTI Interface) > 通用 (General)** **配置 (Configuration) > 设备设置 (Device Setup) > 接口设置 (Interface Settings) > 接口 (Interfaces) > 添加 (Add) > VTI 接口 (VTI Interface) > 高级 (Advanced)**

第 11 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 服务器使用准则

ASA 会根据属性名称而不是数值 ID 来实施 LDAP 属性。RADIUS 属性会按数值 ID 而不是名称来实施。

对于 ASDM 7.0 版本，LDAP 属性包含 cVPN3000 前缀。对于 ASDM 7.1 版本及更高版本，此前缀已移除。

LDAP 属性是已在 Radius 章节中列出的 Radius 属性的子集。

配置多证书身份验证

现在，您可以使用 Secure Client SSL 和 IKEv2 客户端协议验证每个会话的多重证书。例如，可以确保计算机证书的颁发者名称匹配特定的 CA，因此，设备是公司发布的设备。

通过多证书选项，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。

注释 由于多证书身份验证需要一个计算机证书和一个用户证书（或两个用户证书），因此不能使用 Secure Client 登录前启动 (SBL) 功能。

通过预填充用户名字段，可以解析第二个（用户）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二个（用户）证书检索主用和辅助用户名预填充。

从 9.14(1) 开始，ASA 允许您在配置多证书身份验证并使用“身份验证”或“授权”的预填充用户名选项时指定主用户名和辅助用户名应来自哪个证书。有关信息，请参阅Secure Client 连接配置文件，身份验证属性，第 95 页

通过多证书身份验证对两个证书进行身份验证：从自客户端收到的第二个（用户）证书解析 pre-fill 和 username-from-certificate 主用和辅助用户名。

您也可以配置通过 SAML 进行多证书身份验证。

通过多证书身份验证，可以根据证书字段制定策略决策，该证书用于对该连接尝试进行身份验证。将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加载到 DAP，以确保能够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：

- 基于用户的属性的策略实施 ， 第 223 页
- 为 Secure Client 隧道实施静态 IP 地址分配 ， 第 224 页
- 实施拨入允许或拒绝访问 ， 第 226 页
- 实施登录时长和时间规则 ， 第 228 页

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

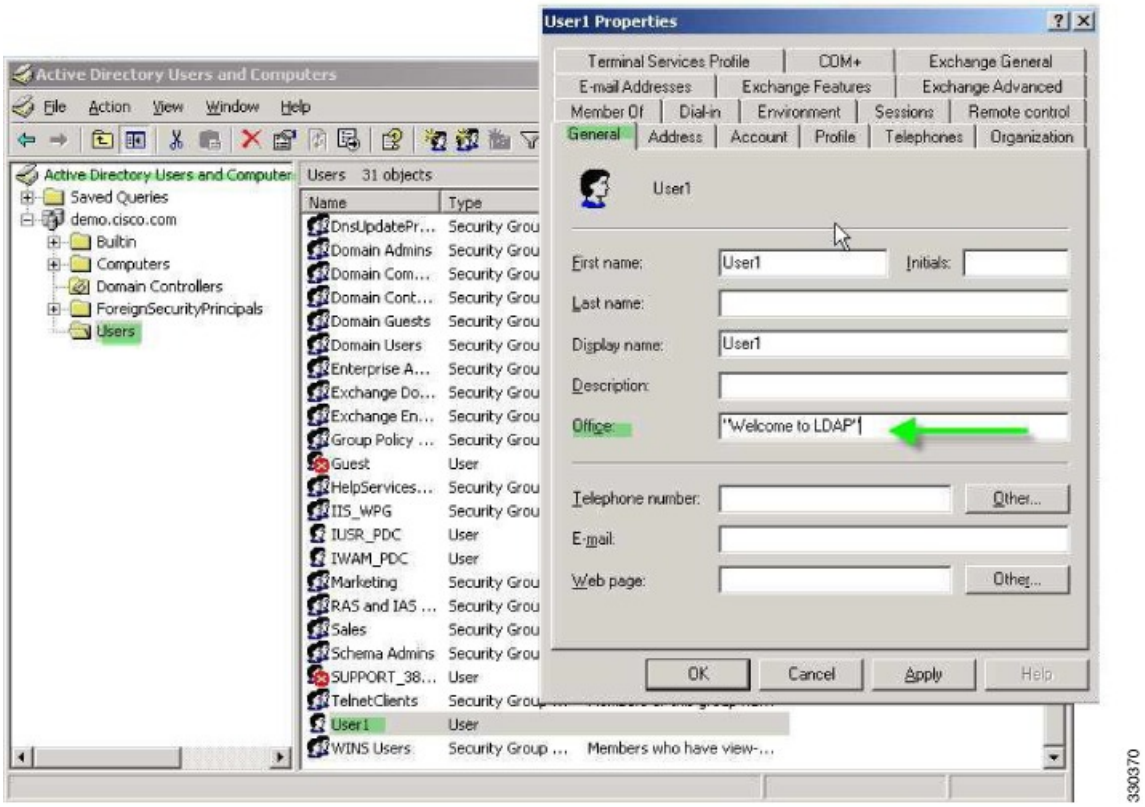
此示例向用户显示一个简单的欢迎信息，说明如何将任意标准 LDAP 属性映射至一个已知的供应商特定属性 (VSA)，或者将一个或多个 LDAP 属性映射至一个或多个思科 LDAP 属性。此示例适用于任意连接类型，包括 IPSec VPN 客户端和 Secure Client。

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，然后向用户显示该欢迎信息。

过程

步骤 1 右键点击用户名打开“属性”(Properties) 对话框，然后点击**常规 (General)** 选项卡，在“办公室”(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。

为 Secure Client 隧道实施静态 IP 地址分配

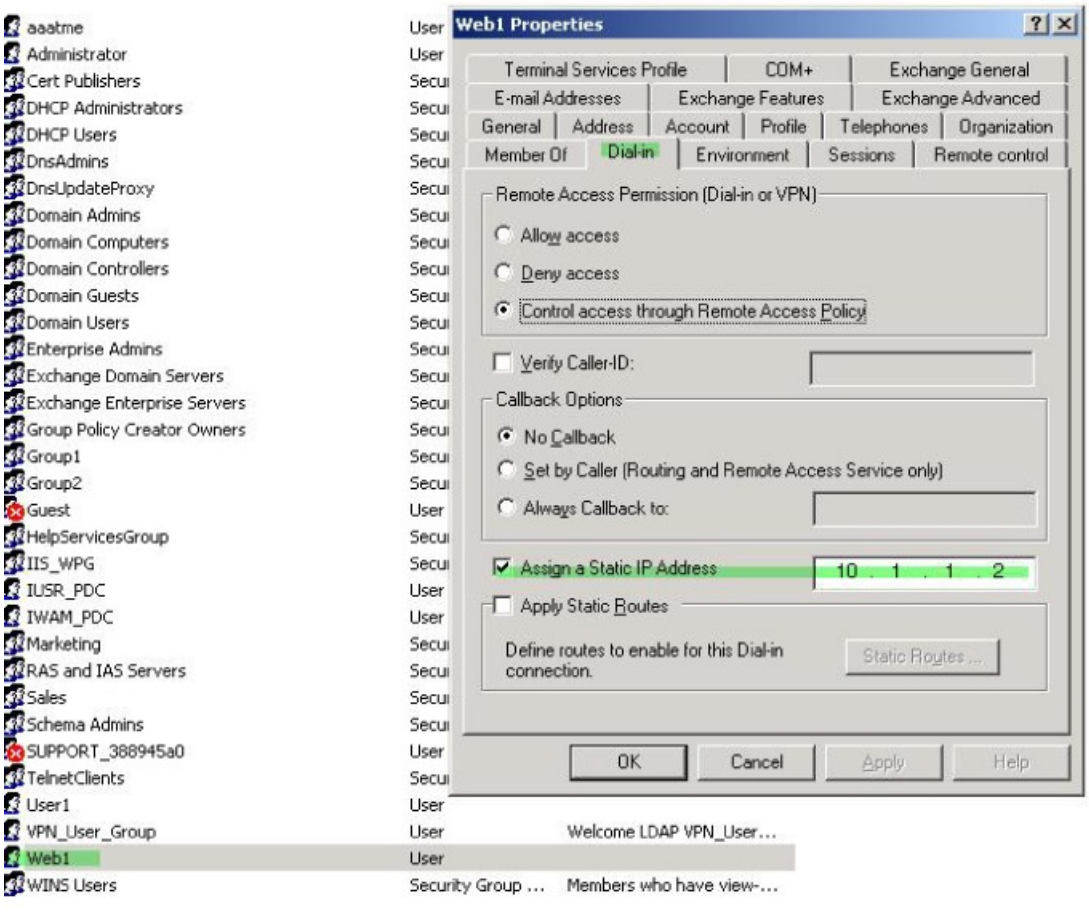
此示例适用于完全隧道客户端，例如 IPsec 客户端和 SSL VPN 客户端。

如要实施静态 Secure Client 静态 IP 分配，请将 Secure Client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“属性”(Properties) 对话框，然后点击**拨入 (Dial-in)** 选项卡，选中**分配静态 IP 地址 (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 Secure Client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

值	隧道协议
16	无客户端 SSL
32	SSL 客户端 - Secure Client 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”(Properties) 对话框，然后点击**拨入 (Dial-in)** 选项卡，再点击“允许访问”(Allow Access) 单选按钮。

注释　如果您通过“远程访问策略”(Remote Access Policy) 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 Secure Client 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。

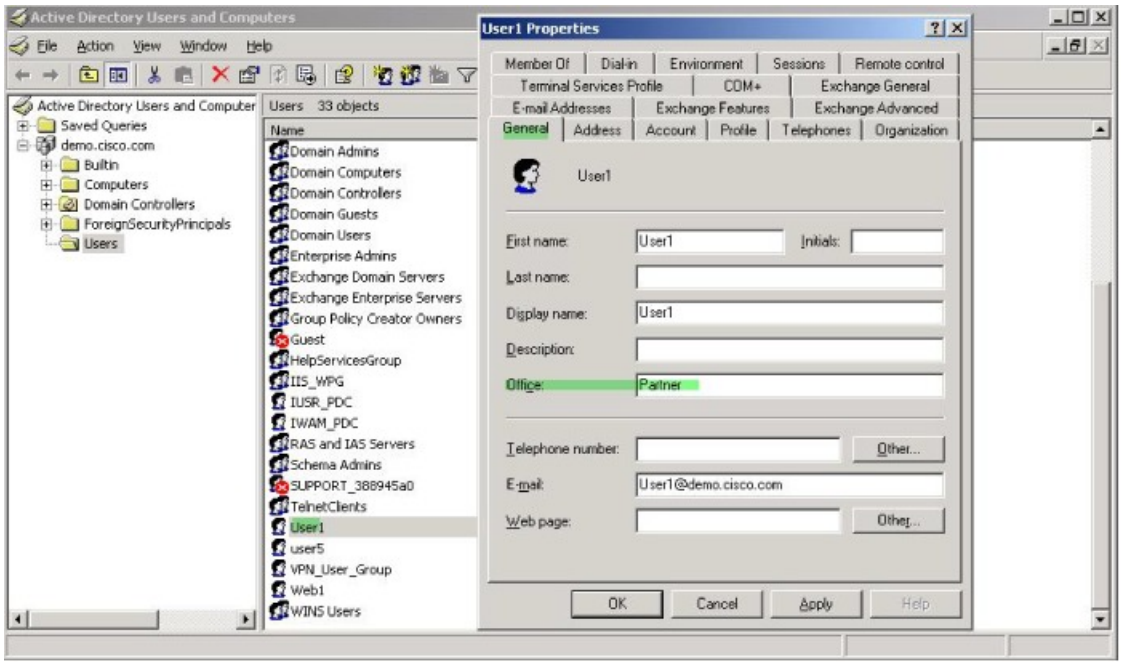
实施登录时长和时间规则

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。在身份验证过程中，ASA 会检索 physicalDeliveryOfficeName 的值，并将其映射至 Access-Hours。

过程

步骤 1 选择用户，右键点击**属性 (Properties)**，然后打开**常规 (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
```

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。