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 30 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 8 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 10 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 15 页
- 站点到站点内部组策略，第 36 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。

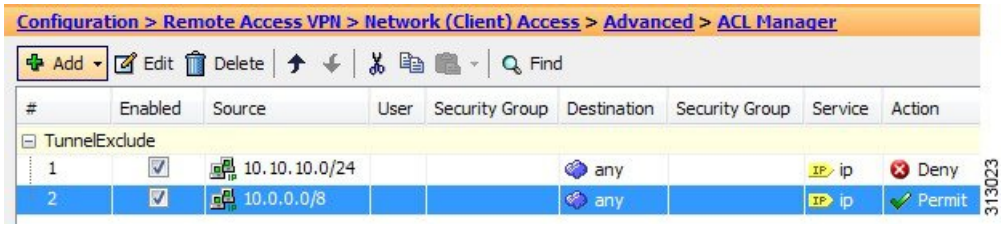
要定义分割隧道策略，请从下拉列表 **Policy** 和 **IPv6 Policy** 进行选择。Policy 字段定义 IPv4 网络流量的分割隧道策略。IPv6 Policy 字段选择 IPv6 网络流量的分割隧道策略。除该差异以外，这些字段还具有相同的用途。

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 91 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 76 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 27 页
- 为 VPN 配置系留设备支持，第 29 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 *1: 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 91 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 41 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 41 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 75 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 46 页
连接配置文件，地址池 ，第 47 页
连接配置文件，高级，添加或编辑 IP 池 ，第 47 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 *2:* 按子字符串过滤

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

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

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

- 示例 1：Regular Expression Matching - 在 Regular Expression 字段中输入要应用于搜索的正则表达式。标准正则表达式运算符适用。例如，假设要使用正则表达式过滤所有内容，直至“Email Address (EA)”DN 值的 @ 符号。正则表达式 ^[^@]* 将是执行此操作的一种方法。在本示例中，如果 DN 值包含值 user1234@example.com，则正则表达式之后的返回值将为 user1234。
- 示例 2：“使用 Lua 格式的自定义脚本”- 指定以 LUA 编程语言编写的自定义脚本，用于解析搜索字段。选择此选项将为您提供一个字段，可用于输入自定义的 LUA 脚本；例如，脚本：

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

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

  下表列出了可在 LUA 脚本中使用的属性名称和说明。

注释 LUA 区分大小写。

表 3: 属性名称和说明

属性名称	说明
cert.subject.c	国家/地区
cert.subject.cn	通用名称
cert.subject.dnq	DN 限定符
cert.subject.ea	邮件地址
cert.subject.genq	辈分词
cert.subject.gn	名字
cert.subject.i	首字母缩写
cert.subject.l	区域
cert.subject.n	名称
cert.subject.o	组织
cert.subject.ou	组织单位
cert.subject.ser	主题序列号
cert.subject.sn	姓氏
cert.subject.sp	省/自治区/直辖市
cert.subject.t	职位
cert.subject.uid	用户 ID
cert.issuer.c	国家/地区
cert.issuer.cn	通用名称
cert.issuer.dnq	DN 限定符
cert.issuer.ea	邮件地址
cert.issuer.genq	辈分词
cert.issuer.gn	名字

cert.issuer.i	首字母缩写
cert.issuer.l	区域
cert.issuer.n	名称
cert.issuer.o	组织
cert.issuer.ou	组织单位
cert.issuer.ser	颁发者序列号
cert.issuer.sn	姓氏
cert.issuer.sp	省/自治区/直辖市
cert.issuer.t	职位
cert.issuer.uid	用户 ID
cert.serialnumber	证书序列号
cert.subjectaltname.upn	用户主体名称

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

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 45 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 47 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 55 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。

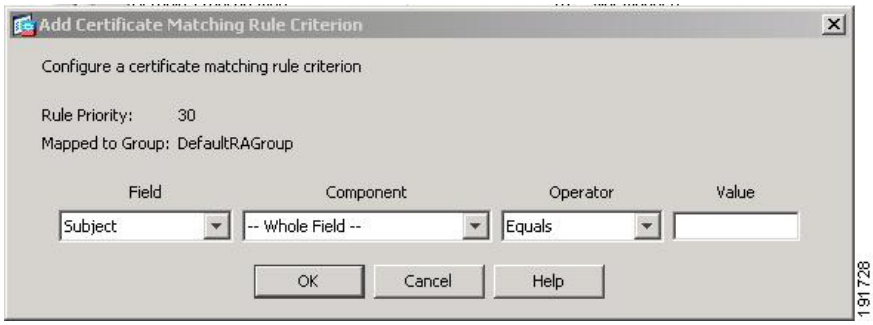
此窗格具有一个证书到连接配置文件映射及映射条件的列表。

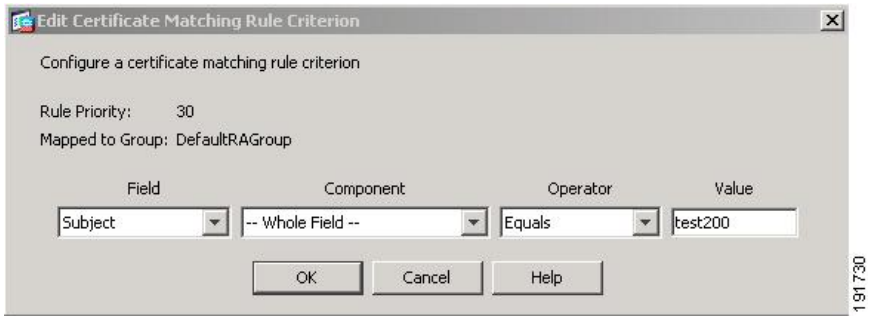
证书到连接配置文件映射，添加证书匹配规则条件

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 71 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 72 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。

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 4: 用于为 VPN 客户端配置身份 NAT 的网络寻址

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

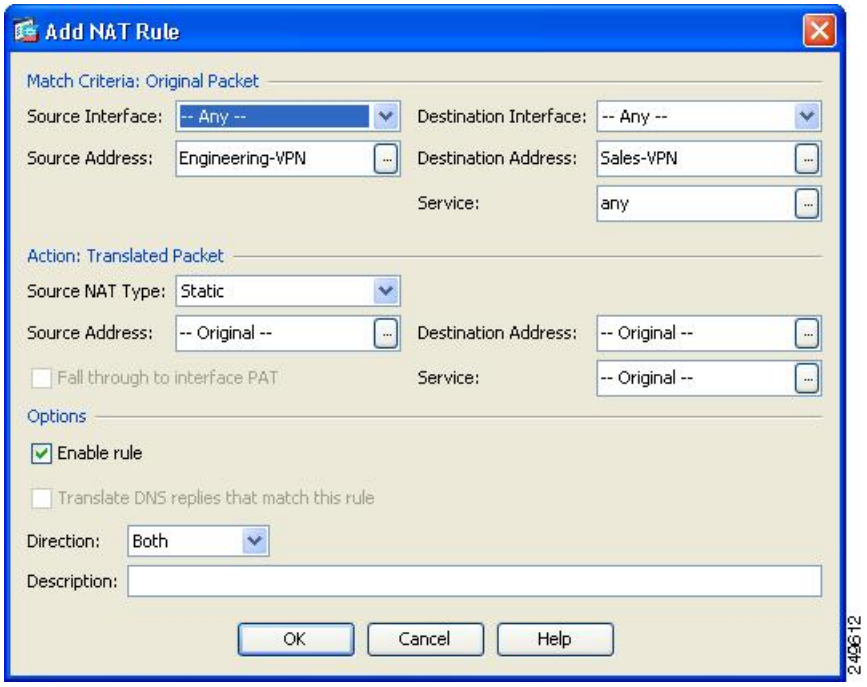
过程

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

步骤 2 创建 NAT 规则，以便 Engineering VPN 地址池中的主机可以到达 Sales VPN 地址池中的主机。在“NAT 规则”窗格中，依次导航到**添加 > 在“网络对象”NAT 规则前添加 NAT 规则**，以便 ASA 在统一 NAT 表中的其他规则之前评估此规则。

注释 NAT 规则评估按照自顶向下、最先匹配的基础来应用。在 ASA 与数据包到特定 NAT 规则，因此不会执行任何评估。请务必将最具体的 NAT 规则置于统一 NAT 表的顶部，以便 ASA 不会过早地将其与更广泛的 NAT 规则相匹配。

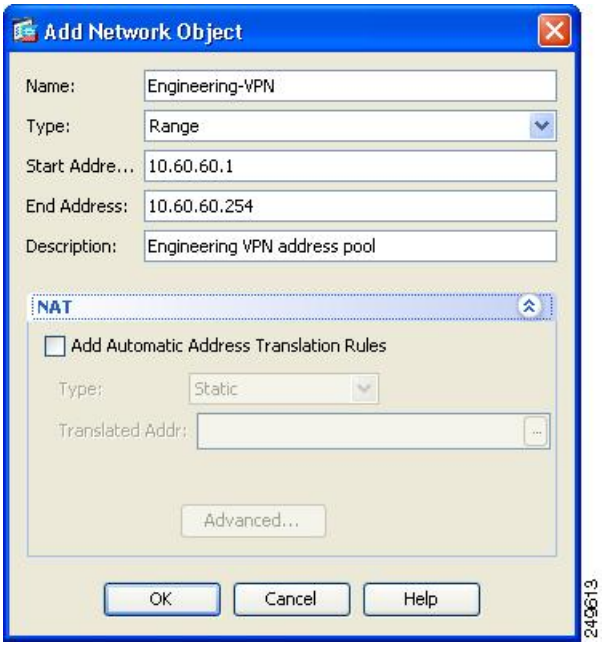
图 1: Add NAT Rule 对话框



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

- **源接口**：“任意”
- **目的接口**：“任意”
- **源地址**：点击“源地址”浏览按钮并创建表示工程 VPN 地址池的网络对象。将对象类型定义为地址的范围。请勿添加自动地址转换规则。
- **目的地址**：点击“目的地址”浏览按钮并创建表示销售 VPN 地址池的网络对象。将对象类型定义为地址的范围。请勿添加自动地址转换规则。

图 *2:* 为 *VPN* 地址池创建网络对象



b) 在**操作：转换后的数据包**区域中，配置以下字段：

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

c) 在 Options 区域中，配置以下字段：

- 选中 **Enable rule**。
- 取消选中 **Translate DNS replies that match this rule** 或将其留空。
- **方向**：“双向”
- **说明**：添加此规则的说明。

d) 点击**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
```

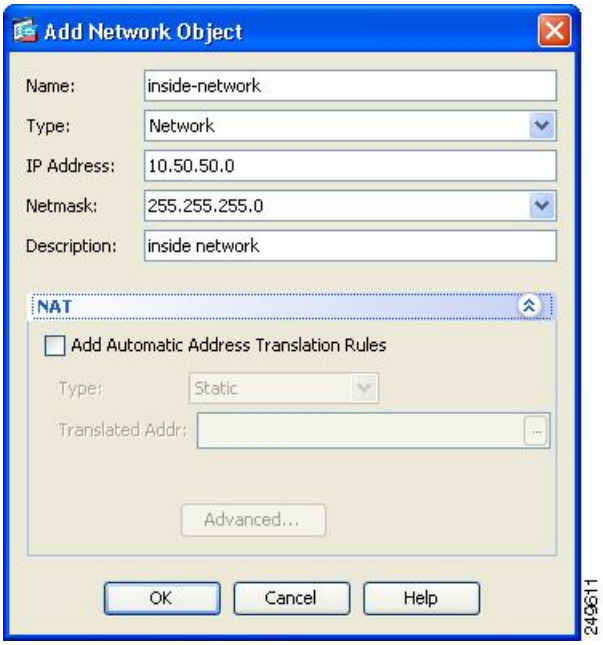
步骤 4 创建 NAT 规则，以便 Engineering VPN 地址池中的主机可以到达 Engineering VPN 地址池中的其他主机。创建此规则的过程就与先前创建该规则一样，不同之处在于，您需要在“匹配条件：原始数据包”区域中将工程 VPN 地址池同时指定为源地址和目的地址。

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 3: 添加 *inside-network* 对象



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

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

c) 在 **Options** 区域中，配置以下字段：

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

d) 点击**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。

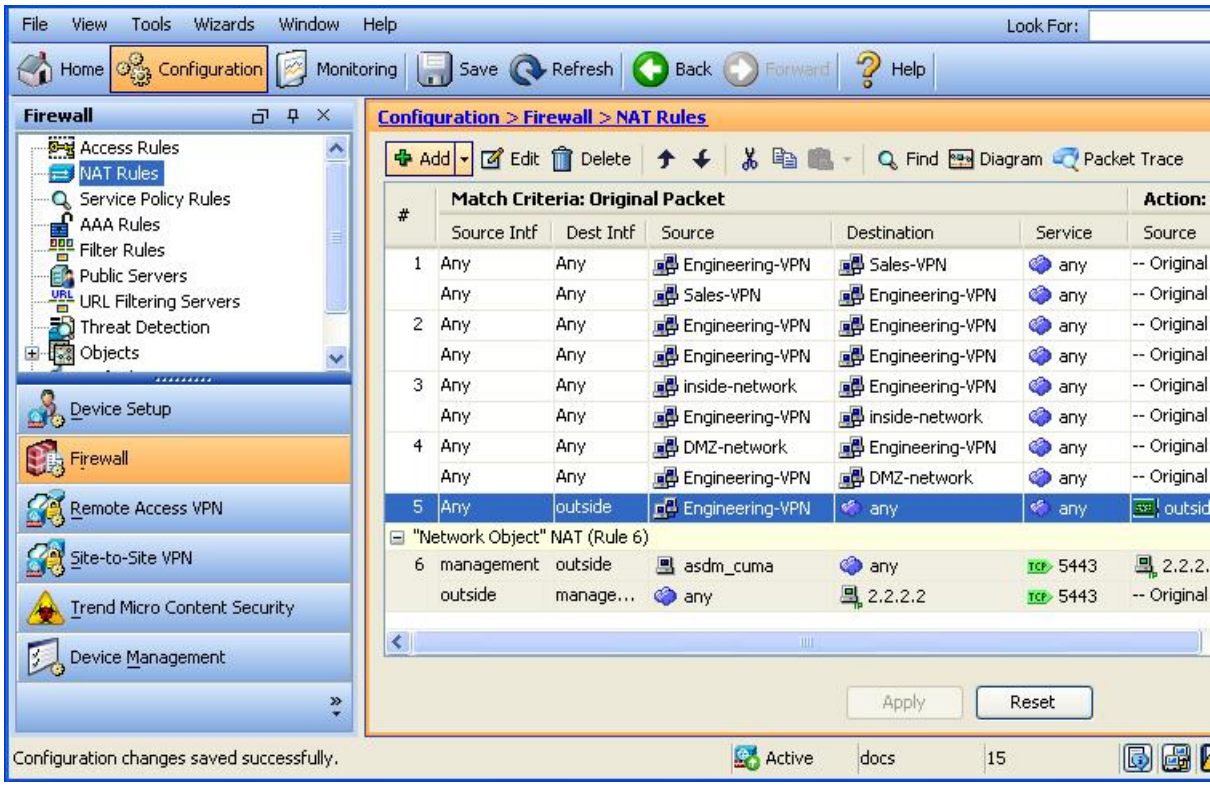
e) 点击**确定**。

f) 点击**应用**。

CLI 示例：

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

图 *4:* 统一 *NAT* 表



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

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

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。

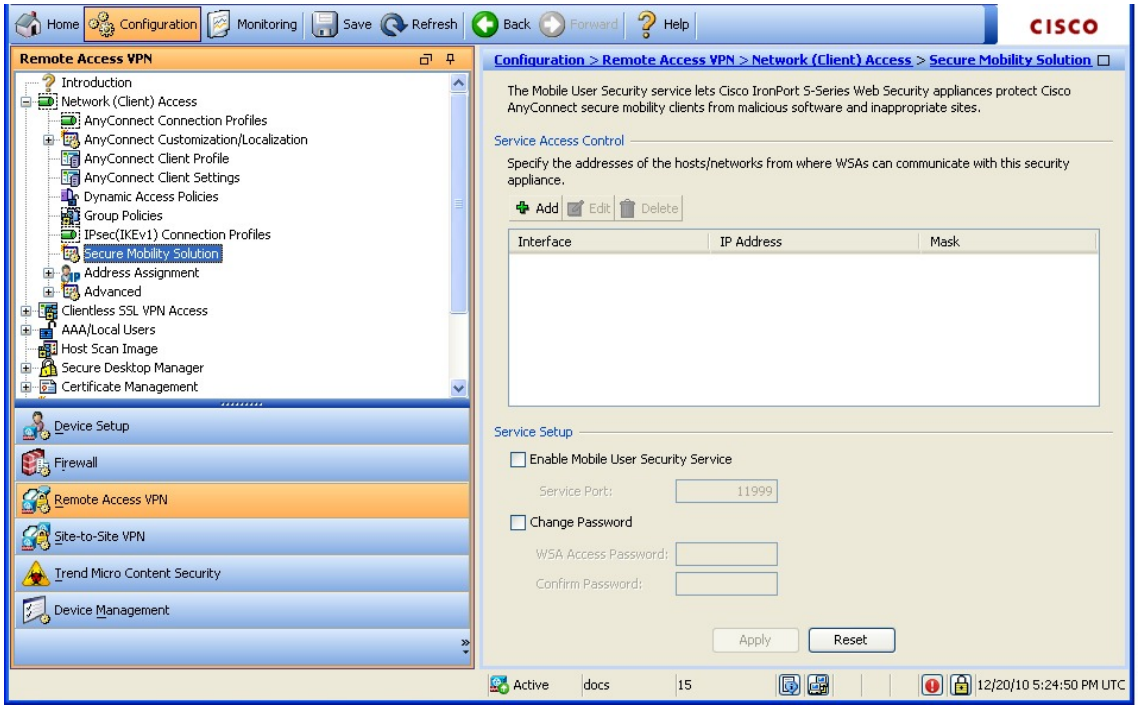
Cisco Secure Client 解决方案

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 *5:* 移动用户安全窗口



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

添加或编辑 MUS 访问控制

在“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 23 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。

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。