远程访问 VPN

远程访问虚拟专用网络 (VPN) 允许个人用户使用连接到互联网的计算机或其他受支持的设备，从远程位置连接到您的网络。这样，移动员工就可以从家庭网络或公共 Wi-Fi 网络进行连接。

以下主题介绍如何为您的网络配置远程访问 VPN。

- 远程访问 VPN 概述， 第 1 页
- 远程接入 VPN 的许可证要求， 第 7 页
- 远程接入 VPN 的要求和前提条件， 第 7 页
- 远程访问 VPN 的准则和限制， 第 7 页
- 配置新的远程访问 VPN 连接， 第 10 页
- 创建现有远程接入 VPN 策略的副本， 第 20 页
- 设置远程访问 VPN 策略的目标设备， 第 21 页
- 将本地领域与远程接入 VPN 策略相关联， 第 21 页
- 其他远程访问 VPN 配置， 第 22 页
- 自定义远程接入 VPN AAA 设置， 第 77 页
- 高级 Secure Client 配置， 第 97 页
- 远程访问 VPN 示例， 第 106 页
- 远程接入 VPN 的功能历史记录， 第 110 页

远程访问 VPN 概述

Cisco Secure Firewall Threat Defense 提供安全的网关功能，支持远程访问 SSL 和 IPsec-IKEv2 VPN。全隧道客户端， 安全客户端，可通过 SSL 和 IPsec-IKEv2 安全地连接远程用户的安全网关。客户端与 协商 SSL VPN 连接时，会使用传输层安全 (TLS) 或数据报传输层安全 (DTLS) 进行连接

安全客户端 是终端设备上通过远程 VPN 连接 设备的唯一受支持客户端。该客户端为远程用户提供了 SSL 或 IPsec-IKEv2 VPN 客户端，而无需网络管理员在远程计算机上安装和配置客户端。连接后，即可从安全网关中部署适用于 Windows、Mac 和 Linux 的 安全客户端。从平台应用商店可安装适用于 Apple iOS 和 Android 设备的 安全客户端 应用。

使用远程访问 VPN 策略向导可设置 SSL 和 IPsec-IKEv2 远程访问 VPN 的基本功能。然后，根据需要增强策略配置并将其部署到您的 安全网关设备。

远程访问 VPN 功能

下表介绍了 Cisco Secure Firewall Threat Defense 远程访问 VPN 的功能：

表 *1:* 远程访问 *VPN* 功能

	说明
Cisco Secure Firewall Threat Defense 远程访问 VPN 功能	• 使用 安全客户端 的 SSL 和 IPsec-IKEv2 远程访问。 • Cisco Secure Firewall Management Center 支持所有组合，如 IPv4 隧道上的 IPv6。 • 对 防火墙管理中心 和 设备管理器的配置支持。特定于设备的覆盖。 • 支持 Cisco Secure Firewall Management Center 和 HA 环境。 • 支持多个接口和多个 AAA 服务器。 • 使用 RADIUS CoA 或 RADIUS 动态授权提供快速遏制威胁支持。 • 支持 Cisco 安全客户端 版本 4.7 或更高版本的 DTLS v1.2 协议。 • Secure Client 客户端模块支持远程访问 VPN 连接的其他安全服务。 • VPN 负载均衡。

	说明
AAA 功能	• 使用自签名或 CA 签名的身份证书的服务器身份验证。 • 使用 RADIUS 或 LDAP 或 AD 的基于 AAA 用户名和密码的远程身份验证。 • RADIUS 组和用户授权属性，以及 RADIUS 记帐。 • 提供使用其他 AAA 服务器进行辅助身份验证的双重身份验证支持。 • 使用 VPN 身份的 NGFW 访问控制集成。 • 使用 Cisco Secure Firewall Management Center Web 界面的 LDAP 或 AD 授权属性。 • 支持使用 SAML 2.0 的单一登录。 • 支持使用 Microsoft Azure 的多个身份提供程序信任点，这些信任点可以具有相同实体ID的多个应用，但具有唯一身份证书。 • 根据地理位置限制远程访问 VPN 连接。
VPN 隧道功能	• 地址分配。 • 拆分隧道 • 拆分 DNS。 • 客户端防火墙 ACL。 • 最大连接和空闲时间的会话超时。
远程访问 VPN 监控功能	• 新的 VPN 控制面板构件，按持续时间、客户端应用等各个特性显示 VPN 用户。 • 远程访问 VPN 事件，包括身份验证信息，如用户名和 OS 平台。 • 使用 统一 CLI 提供的隧道统计信息。

安全客户端 组件

安全客户端 部署

远程接入 VPN 策略可包括 安全客户端映像 和 安全客户端配置文件，以便分发到连接终端。您也可以使用其他方法分发客户端软件。请参阅 Cisco Secure Client（包括 AnyConnect）管理指南，版本 5 中的 部署 *Cisco Secure Client* 一章。

在先前未安装客户端的情况下，远程用户可以在他们的浏览器中输入配置为接受 SSL 或 IPsec-IKEv2 VPN 连接的接口的 IP 地址。除非安全设备被配置为将 http:// 请求重定向到 https://，否则远程用户必须以 https://地址形式输入 URL。在用户输入 URL 后，浏览器将连接该接口并显示登录屏幕。

在用户登录后，如果安全网关将用户识别为需要 VPN 客户端，则会下载与远程计算机的操作系统匹配的客户端。下载后，客户端会自行安装和配置、建立安全连接并在连接停止后自行保留或卸载（取决于安全设备配置）。如果是以前安装的客户端，登录后 安全网关会检查客户端版本，并根据需要进行升级。

安全客户端 操作

当客户端与安全设备协商连接时，客户端将使用传输层安全 (TLS) 以及（可选）或数据报传输层安全 (DTLS) 协议进行连接。DTLS 可避免与某些 SSL 连接关联的延迟和带宽问题，并可提高对于数据包延迟敏感的实时应用的性能。

当 IPsec-IKEv2 VPN 客户端发起到安全网关的连接时，协商包括通过互联网密钥交换 (IKE) 验证设备，然后使用 IKE 扩展身份验证 (Xauth) 进行用户验证。系统会将群组配置文件推送到 VPN 客户端，并创建 IPsec 安全关联 (SA) 来完成 VPN。

安全客户端配置文件 和编辑器

安全客户端配置文件 是一组以 XML 文件形式存储的配置参数，VPN 客户端使用该文件来配置客户端的操作和外观。这些参数（XML 标记）包括主机名称和地址以及设置，用于启用更多客户端功能。

您可以使用 安全客户端配置文件编辑器配置配置文件。此编辑器是一款方便的基于 GUI 的配置工具，作为 安全客户端 软件包的一部分提供。该程序可独立于 防火墙管理中心 而运行。

远程访问 VPN 身份验证

远程访问 VPN 服务器身份验证

Cisco Secure Firewall Threat Defense 安全网关通常使用证书来识别和验证自己到 VPN 客户端终端的连接。

当使用远程访问 VPN 策略向导时，您可以在目标 设备上注册选定的证书。在向导中的**访问和证书**阶段，选择“在目标设备上注册所选的证书对象”选项。证书注册过程将在指定设备上自动执行。完成远程访问 VPN 策略配置时，您可以在设备证书主页下查看已注册证书的状态。该状态清晰指明了证书注册是否成功。您的远程访问 VPN 策略配置现已完成，可以进行部署。

有关如何获得安全网关证书（也称为 PKI 注册）的信息，请参阅证书。此章详细说明了如何配置、注册和维护网关证书。

远程访问 VPN 客户端 AAA

对于 SSL 和 IPsec-IKEv2，可只使用用户名和密码、只使用证书或同时使用这两种方法对远程用户进行身份验证。

注释 如果您的部署中正在使用客户端证书，则必须将它们添加到独立于 Cisco Secure Firewall Threat Defense 或 Cisco Secure Firewall Management Center的客户端平台中。不提供 SCEP 或 CA 服务等设施来为客户端填充证书。

AAA 服务器支持使用托管设备作为安全网关来确定用户身份（身份验证）、允许用户执行的操作（授权）以及用户执行的操作（记帐）。AAA 服务器的一些示例有 RADIUS、LDAP/AD、TACACS+ 和 Kerberos.。对于 设备上的远程访问 VPN，支持使用 AD、LDAP 和 RADIUS AAA 服务器进行身份验证。

请参阅 了解权限和属性的策略实施 部分以了解更多有关远程访问 VPN 授权的信息。

在添加或编辑远程访问 VPN 策略之前，必须配置要指定的领域和 RADIUS 服务器组。有关详细信息，请参阅创建 LDAP 领域或 Active Directory 领域和领域目录和添加 RADIUS 服务器组。

如果没有配置 DNS，设备将无法解析 AAA 服务器名称、命名的 URL 和具有 FQDN 或主机名的 CA 服务器，只能解析 IP 地址。

远程用户提供的登录信息由 LDAP 或 AD 领域或 RADIUS 服务器组进行验证。这些实体与 Cisco Secure Firewall Threat Defense 安全网关相集成。

注释 如果用户使用 Active Directory 作为身份验证源通过远程访问 VPN 进行身份验证，则用户必须使用其用户名登录；`domain\username` 或 `username@domain` 格式无效。（Active Directory 将此用户名视为 *logon* 名称，有时也视为 `sAMAccountName`。）有关详细信息，请参阅 MSDN 上的用户命名属性。

如果使用 Radius 进行身份验证，用户可以使用上述任何一种格式登录。

通过 VPN 连接进行身份验证后，远程用户将接受 *VPN* 身份。Cisco Secure Firewall Threat Defense安全网关上的身份策略将使用此 VPN 身份来识别和过滤属于此远程用户的网络流量。

身份策略与访问控制策略相关联，后者用于确定哪些人有权访问网络资源。使用访问控制策略可阻止或允许远程用户访问您的网络资源。

有关详细信息，请参阅关于身份策略和访问控制策略部分：

相关主题

配置远程访问 VPN 的 AAA 设置 ，第 24 页

了解权限和属性的策略实施

Cisco Secure Firewall Threat Defense设备支持将用户授权属性（也称为用户权利或权限）应用于来自外部身份验证服务器和/或授权 AAA 服务器 (RADIUS) 或 设备上的组策略的 VPN 连接。如果 设备从与组策略上配置的属性冲突的外部 AAA 服务器接收属性，则来自 AAA 服务器的属性始终优先。

设备按照以下顺序应用属性：

1. **外部 AAA 服务器上的用户属性** - 该服务器在用户身份验证和/或授权成功后返回这些属性。
2. **在 Firepower Threat Defense 设备上配置的组策略** - 如果 RADIUS 服务器为用户返回 RADIUS Class 属性 IETF-Class-25 (OU=group-policy) 值， 设备会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。
3. **连接配置文件 (也称为隧道组) 分配的组策略** - 连接配置文件具有该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。

注释 设备不支持从默认组策略 *DfltGrpPolicy* 继承系统默认属性。如果分配给连接配置文件的组策略上的属性没有被用户属性或来自 AAA 服务器的上述组策略所覆盖，则这些属性将用于用户会话。

相关主题

配置远程访问 VPN 的 AAA 设置，第 24 页

了解 AAA 服务器连接

必须能够从 设备访问 LDAP、AD 和 RADIUS AAA 服务器以实现预期目的：仅用户身份处理、仅 VPN 身份验证或这两种活动。AAA 服务器在远程接入 VPN 中被用于以下活动：

- **用户身份处理 (User-identity handling)** - 必须能够通过管理接口访问服务器。

  在 设备上管理接口具有区别于数据接口的单独路由过程和配置。

- **VPN 身份验证 (VPN authentication)** - 必须能够通过一个数据接口或管理接口来访问服务器。

  要使用管理接口，您必须明确选择管理接口作为源接口。不能使用其他管理专用接口。

要为两个活动使用相同的 AAA 服务器，建议将管理接口指定为源接口。

有关不同接口的详细信息，请参阅常规防火墙接口。

部署后，请使用以下 CLI 命令从 设备监视和故障排除 AAA 服务器连接：

- **show aaa-server** 显示 AAA 服务器统计信息。
- **show network** 并且 **show network-static-routes** 或者查看管理接口默认路由和静态路由。
- **show route** 查看数据流量路由表项。
- **ping system** 和 **traceroute system** 以验证通过管理接口到 AAA 服务器的路径。
- **ping interface** *ifname* 和 **traceroute** *destination* 验证通过数据接口到 AAA 服务器的路径。

- **test aaa-server authentication** 和 **test aaa-server authorization** 测试 AAA 服务器上的身份验证和授权。
- **clear aaa-server statistics** *groupname* 或 **clear aaa-server statistics protocol** *protocol* 按组或协议清除 AAA 服务器统计信息。
- **aaa-server** *groupname* **active host** *hostname* 激活发生故障的 AAA 服务器；或 **aaa-server** *groupname* **fail host** *hostname* 使 AAA 服务器发生故障。
- **debug ldap level**、**debug aaa authentication**、 **debug aaa authorization** 和 **debug aaa accounting**。

远程接入 VPN 的许可证要求

威胁防御 许可证

FTD 远程访问 VPN 需要 强加密 和以下 安全客户端许可证之一：

- Secure Client Advantage
- Secure Client Premier
- 仅限 Secure Client VPN

远程接入 VPN 的要求和前提条件

型号支持

威胁防御

支持的域

任意

用户角色

管理员

远程访问 VPN 的准则和限制

远程访问 VPN 策略配置

- 您仅可通过使用向导来添加新的远程访问VPN策略。您必须完成整个向导才能创建新的策略；如果在完成向导之前取消，则不会保存任何策略。

- 两个用户必须 不 同时编辑远程访问 VPN 策略，但 Web 界面不会阻止同时编辑。如果发生这种情况，保留最后保存的配置。
- 如果为 Cisco Secure Firewall Threat Defense 设备分配了远程访问 VPN 策略，则无法将该设备从一个域移至另一个域。
- 使用 ECMP 时，远程访问 VPN 不支持 SSL。我们建议您使用 IPsec-IKEv2。
- 在集群模式下的 Firepower 9300 和 4100 系列不支持远程访问 VPN 配置。
- 如果存在配置错误的 NAT 规则，远程访问 VPN 连接可能会失败。
- 如果使用 DHCP 向客户端提供 IP 地址，并且客户端无法获取地址，请检查 NAT 规则。适用于 RA VPN 网络的任何 NAT 规则都应包括路由查找选项。路由查找可以帮助确保 DHCP 请求通过适当的接口发送到 DHCP 服务器。
- 只要使用的是 IKE 端口 500/4500 或 SSL 端口 443 或有一些 PAT 转换处于活动状态，则无法在同一端口上配置 安全客户端 IPSec-IKEv2 或 SSL 远程访问 VPN，因为无法在这些端口上启动服务。配置远程访问 VPN 之前，不得在 设备上使用这些端口。
- 在使用向导配置远程访问 VPN 时，可以创建内联证书注册对象，但不能使用它们安装身份证书。证书注册对象用于在被配置为远程访问 VPN 网关的 设备上生成身份证书。在将远程访问 VPN 配置部署到该设备之前，在该设备上安装身份证书。

  有关如何根据证书注册对象安装身份证书的更多信息，请参阅对象管理器。
- ECMP 区域接口可在启用 IPsec 的远程访问 VPN 中使用。
- ECMP 区域接口不能在启用 SSL 的远程访问 VPN 中使用。如果属于安全区域或接口组的所有远程访问 VPN 接口也属于一个或多个 ECMP 区域，则部署远程访问 VPN（启用 SSL）配置会失败。但是，如果只有属于安全区域或接口组的一些远程访问 VPN 接口也属于一个或多个 ECMP 区域，则远程访问 VPN 配置的部署会成功排除这些接口。
- 更改远程访问 VPN 策略配置后，请重新部署对 设备的更改。部署配置更改所需的时间取决于多个因素，例如策略和规则的复杂性，发送到设备的配置的类型和数量以及内存和设备型号。在部署远程访问 VPN 策略更改之前，请查看 部署配置更改的最佳实践。
- 不直接支持对 RA VPN 前端发出命令（例如 **curl** ），并且可能不会产生所需的结果。例如，前端不响应 HTTP HEAD 请求。
- 如果第三方客户端发送空用户代理， 不接受远程访问 VPN 会话。
- 您可以使用 FlexConfig 配置浏览器代理。
- 在具有高可用性的远程分支部署 (RBD) 中，当您中断高可用性对时，备用设备的 RBD WAN 接口上的 RA VPN 策略分配和 VPN 配置将被删除。
- 当在 上禁用 **已解密流量的绕过访问控制策略** 并且 ISE 发出 DACL 时，首先将流量与 ACP 进行匹配：如果允许，则继续进行 DACL 检查；如果被拒绝，则将绕过 DACL 匹配。

并发 VPN 会话容量规划（Firewall Threat Defense Virtual 型号）

最大并发 VPN 会话数由 Firewall Threat Defense Virtual 安装的智能许可授权层管理，并通过速率限制器实施。根据已许可的设备型号，设备上允许的并发远程访问VPN会话数量有最大值限制。此限制用于确保系统性能不会降低到不可接受的水平。请使用这些限制进行容量规划。

设备型号	最大并发远程访问 VPN 会话数
Firewall Threat Defense Virtual5	50
Firewall Threat Defense Virtual10	250
Firewall Threat Defense Virtual20	250
Firewall Threat Defense Virtual30	250
Firewall Threat Defense Virtual50	750
Firewall Threat Defense Virtual100	10,000

并发 VPN 会话容量规划 （硬件型号）

最大并发VPN会话数受特定于平台的限制约束，而与许可证无关。根据设备型号，设备上允许的并发远程访问VPN会话数量有最大值限制。此限制用于确保系统性能不会降低到不可接受的水平。请使用这些限制进行容量规划。

设备型号	最大并发远程访问 VPN 会话数
Firepower 1010	75
Firepower 1120	150
Firepower 1140	400
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10,000
Cisco Secure Firewall 3110	3000
Cisco Secure Firewall 3120	6000
Cisco Secure Firewall 3130	15,000
Cisco Secure Firewall 3140	20,000
Firepower 4100，所有型号	10,000
Firepower 9300 设备，所有型号	20,000
ISA 3000	25

有关其他硬件型号的容量，请联系您的销售代表。

注释 一旦达到每个平台的最大会话限制，设备就会拒绝VPN连接。连接通过系统日志消息来拒绝。请参阅系统日志消息指南中的系统日志消息 %ASA-4-113029 和 %ASA-4-113038。有关详细信息，请参阅 Cisco Secure Firewall ASA 系列系统日志消息。

控制 VPN 的密码使用

为防止使用大于 DES 的密码，在 防火墙管理中心中的下列位置提供了预部署检查：

设备 (Devices) > **平台设置 (Platform Settings)** > **编辑 (Edit)** > **SSL**。

设备 (Devices) > **VPN** > **远程访问 (Remote Access)** > **编辑 (Edit)** > **高级 (Advanced)** > **IPsec**。

有关 SSL 设置和 IPsec 的详细信息，请参阅 SSL 和 配置远程访问 VPN IPsec/IKEv2 参数，第 56 页。

身份验证、授权和记帐

在拓扑中的每台设备上配置 DNS，以便使用远程访问 VPN。如果没有 DNS，设备将无法解析 AAA 服务器名称、命名的 URL 和具有 FQDN 或主机名的 CA 服务器；只能解析 IP 地址。

您可以使用**平台设置 (Platform Settings)** 来配置 DNS。有关详细信息，请参阅DNS和DNS 服务器组。

客户端证书

如果您的部署中正在使用客户端证书，则必须将它们添加到独立于 Cisco Secure Firewall Threat Defense 或 Cisco Secure Firewall Management Center的客户端平台中。不提供 SCEP 或 CA 服务等设施来为客户端填充证书。

不支持的 安全客户端 功能

唯一支持的 VPN 客户端是思科 安全客户端。不支持任何其他客户端或本机 VPN。在 VPN 连接方面不支持无客户端 VPN；它只用于使用 Web 浏览器部署 Secure Client 客户端。

注释 在 设备上使用多个 安全客户端 软件包可能会增加内存使用量并影响设备的性能。我们建议您不要在低端威胁防御设备上使用多个 安全客户端 软件包，以避免因内存耗尽而导致连续重启。

在连接到 安全网关时，不支持以下 安全客户端 功能：

- TACACS、Kerberos（KCD 身份验证和 RSA SDI）以及 SDI。

配置新的远程访问 VPN 连接

本节介绍如何使用 Cisco Secure Firewall Threat Defense 设备作为 VPN 网关和 Cisco 安全客户端 作为 VPN 客户端配置新的远程访问 VPN 策略。

步骤	相应操作	更多信息
1	查看准则和前提条件。	远程访问 VPN 的准则和限制，第 7 页 配置远程访问 VPN 的前提条件，第 11 页
2	使用向导来添加新的远程访问 VPN 策略。	创建新的远程访问 VPN 策略，第 12 页
3	更新设备上部署的访问控制策略。	在 Cisco Secure Firewall Threat Defense 设备上更新访问控制策略，第 14 页
4	（可选）如果在设备上配置了 NAT，请配置 NAT 免除规则。	（可选）配置 NAT 豁免，第 15 页
5	配置 DNS。	配置 DNS，第 16 页
6	添加 Secure Client 配置文件。	添加 安全客户端配置文件 XML 文件，第 17 页
7	部署远程访问 VPN 策略。	部署配置更改
8	（可选）验证远程访问 VPN 策略配置。	检验配置，第 20 页

配置远程访问 VPN 的前提条件

- 部署 Cisco Secure Firewall Threat Defense 设备并配置 Cisco Secure Firewall Management Center，以便在启用导出控制功能的情况下管理具有所需许可证的设备。有关详细信息，请参阅VPN 许可。
- 配置用于为每台充当远程访问 VPN 网关的 设备获取身份证书的证书注册对象。
- 配置远程访问 VPN 策略使用的任何 AD 或 LDAP 域。
- 在迁移带有远程访问 VPN 的 FTD 时，应在迁移远程访问 VPN 之前在 cdFMC 上预先配置远程访问 VPN 使用的域 （LDAP、AD 或甚至本地）。
- 确保可以通过 设备访问 AAA 服务器，以使远程访问 VPN 配置生效。配置路由（在 **设备 > 设备管理 > 编辑设备 > 路由**）以确保 AAA 服务器连接：

  对于远程访问 VPN 双重身份验证，请确保可以通过 访问主身份验证和辅助身份验证服务器，以使双重身份验证配置生效。
- 要启用 远程访问 VPN 功能，购买并启用以下思科 Secure Client 许可证之一：Secure Client Advantage、 Secure Client Premier或 仅限 Secure Client VPN 。
- 从思科软件下载中心下载最新的 Secure Client 映像文件。

  在 Cisco Secure Firewall Management Center Web 界面上，转至**对象 (Objects) > 对象管理 (Object Management) > VPN > 安全客户端文件 (Secure Client File)**，然后添加新的 Secure Client 映像文件。

- 创建一个安全区或接口组，包含用户将访问的网络接口，用于 VPN 连接。请参阅接口。
- 从 Cisco 软件下载中心下载 安全客户端配置文件编辑器 以创建 安全客户端配置文件。您可以使用独立配置文件编辑器创建新的或修改现有的 安全客户端配置文件。

创建新的远程访问 VPN 策略

远程访问 VPN 策略向导将指导您快速轻松地设置具备基本功能的远程访问 VPN。您可以根据需要通过指定其他属性来增强策略配置并将其部署到您的 Cisco Secure Firewall Threat Defense安全网关设备。

开始之前

- 确保满足配置远程访问 VPN 的前提条件，第 11 页中列出的所有前提条件。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 点击**添加 (Add)** 使用远程访问 VPN 策略向导来新建具有基本策略配置的远程访问 VPN 策略。

您必须完成整个向导才能创建新的策略；如果在完成向导之前取消，则不会保存策略。

步骤 3 选择目标设备和协议。

您在这里选择的 设备将用作 VPN 客户端用户的远程访问 VPN 网关。

您可以在创建远程访问 VPN 策略或稍后更改设备时选择 设备。请参阅设置远程访问 VPN 策略的目标设备，第 21 页。

您可以选择 **SSL** 或 **IPSec-IKEv2**，或同时选择两种VPN协议。 支持两种协议通过 VPN 隧道在公共网络上建立安全连接。

注释
不支持使用 NULL 加密的 IPSec 隧道。如果已选择 IPSec-IKEv2，请确保不为 IPSec IKEv2 提议选择 NULL 加密。请参阅配置 IKEv2 IPsec 方案对象。

有关 SSL 设置，请参阅 SSL。

步骤 4 点击**下一步 (Next)**。

步骤 5 配置 **连接配置文件** 和 **组策略** 设置。

连接配置文件将指定一组参数，用于定义远程用户如何连接到VPN设备。参数包括身份验证的设置和属性、VPN 客户端的地址分配以及组策略。配置远程访问 VPN 策略时，设备将提供名为 *DefaultWEBVPNGroup* 的默认连接配置文件。

有关详细信息，请参阅配置连接配置文件设置，第 22 页。

步骤 6 配置**身份验证、授权和记账 (Authentication, Authorization & Accounting)** 设置。

有关配置的信息，

- AAA 设置，请参阅 配置远程访问 VPN 的 AAA 设置，第 24 页
- LDAP 属性映射，请参阅 配置 LDAP 属性映射，第 47 页
- SAML 2.0 单点登录身份验证，请参阅 配置 SAML 单点登录身份验证，第 94 页

步骤 7 配置**客户端地址分配 (Client Address Assignment)** 设置。

客户端 IP 地址可由 AAA 服务器、DHCP 服务器和 IP 地址池分配。选择多个选项时，IP 地址分配将按照 AAA 服务器、DHCP 服务器和 IP 地址池的顺序进行。AAA 服务器分配客户端 IP 地址仅支持 Realm 和 RADIUS 授权。确保已配置 realm 或 RADIUS 服务器以提供客户端 IP 地址。

步骤 8 配置**组策略 (Group Policy)** 设置。

组策略是存储在组策略对象中的一组属性和值对，用于定义远程访问 VPN 体验的 VPN 用户。您可以使用组策略配置用户授权配置文件、IP 地址、安全客户端 设置、VLAN 映射和用户会话设置等属性。RADIUS 授权服务器将会分配组策略，或从当前连接配置文件中获取。有关详细信息，请参阅 配置组策略，第 46 页。

步骤 9 点击**下一步 (Next)**。

步骤 10 选择 VPN 用户将用于连接到远程访问 VPN 的 **安全客户端映像**。

安全客户端通过企业资源的全 VPN 调配为远程用户提供到 Cisco Secure Firewall Threat Defense 设备的安全 SSL 或 IPSec (IKEv2) 连接。在 设备上部署远程访问 VPN 策略后，VPN 用户可以在其浏览器中输入所配置设备接口的 IP 地址，以下载并安装 Secure Client。

有关配置客户端配置文件和客户端模块的信息，请参阅 组策略 Secure Client 选项。

步骤 11 点击**下一步 (Next)**。

步骤 12 配置**传入 VPN 访问的网络接口 (Network Interface for Incoming VPN Access)**。

接口对象可对网络分段，帮助您管理和分类流量数据流。安全区域对象只是对接口进行分组。这些组可以跨多个设备；您还可以在单个设备上配置多个区域接口对象。有两种类型的接口对象：

- 安全区域 - 接口只能属于一个安全区域。
- 接口组 - 接口可属于多个接口组（和一个安全区域）。

（可选）如果需要，选中**在成员接口上启用 DTLS (Enable DTLS on member interfaces)** 复选框。DTLS 仅适用于 SSL协议。

步骤 13 配置**设备证书 (Device Certificates)**。

设备证书（也称为身份证书）可识别连接至远程访问客户端的 VPN 网关。选择用于对 VPN 网关进行身份验证的证书。从**证书注册**下拉列表中，选择证书或点击 + 添加证书以身份验证 VPN 网关。

步骤 14 配置**服务访问控制 (Service Access Control)**。

您可以在运行 7.7 或更高版本的 设备上使用服务访问对象，以便控制对远程客户访问 VPN 的访问。该对象可在 VPN 验证前为客户端提供基于地理位置的访问控制。默认情况下，RAVPN 没有访问控

制，远程客户端可以从任何地理位置进行连接，除非由服务访问对象指定。有关详细信息，请参阅基于地理位置管理远程用户的 VPN 访问，第 73 页和配置服务访问对象。

步骤 15 配置 **VPN 流量访问控制 (Access Control for VPN Traffic)**。

默认情况下，VPN 隧道中的所有已解密流量受制于访问控制策略。选中**绕过已解密流量 (sysopt permit-vpn) 的访问控制策略 (Bypass Access Control policy for decrypted traffic [sysopt permit-vpn])** 复选框，从访问控制策略中绕过解密流量。此选项会绕过访问控制策略检查，但 VPN 过滤器 ACL 以及从 AAA 服务器下载的身份验证 ACL 仍适用于 VPN 流量。

注释
如果选择此选项，则无需更新在 Cisco Secure Firewall Threat Defense 设备上更新访问控制策略，第 14 页中指定的远程访问 VPN 的访问控制策略。

步骤 16 点击**下一步 (Next)**。

步骤 17 查看远程访问 VPN 策略配置**摘要**。

“摘要”页面显示到目前为止已配置的所有远程访问VPN设置，并提供指向在所选设备上部署远程访问 VPN 策略之前需要执行的其他配置的链接。

如有需要，请点击**返回 (Back)** 以更改配置。

步骤 18 点击**完成 (Finish)**，以完成远程访问 VPN 策略的基本配置。

在完成远程访问 VPN 策略向导后，将出现策略列表页面。稍后，设置 DNS 配置，为 VPN 用户配置访问控制，然后启用 NAT 豁免（如有必要），以完成基本远程访问 VPN 策略配置。

下一步做什么

使用远程访问 VPN 控制面板（**概述 (Overview) > 控制面板 (Dashboards) > 远程访问 VPN (Remote Access VPN)**）来监控设备上主动远程访问 VPN 会话的实时数据。您可以快速确定与用户会话相关的问题，同时缓解网络和用户的问题。有关详细信息，请参阅远程访问 VPN 控制面板。

在 Cisco Secure Firewall Threat Defense 设备上更新访问控制策略

部署远程访问 VPN 策略之前，必须使用允许目标 Cisco Secure Firewall Threat Defense 设备上的 VPN 流量的规则更新访问控制策略。此规则必须允许来自外部接口的所有流量，其中源设备作为定义的 VPN 池网络，目标设备作为公司网络。

注释 如果在“访问接口”选项卡上选择**为已解密的流量绕过访问控制策略 (sysopt permit-vpn)** 选项，则无需更新远程访问 VPN 的访问控制策略。

启用或禁用所有 VPN 连接的选项。如果禁用此选项，请确保访问控制策略或预过滤器策略允许流量。

有关详细信息，请参阅配置远程访问 VPN 的访问接口，第 40 页。

开始之前

使用远程访问 VPN 策略向导完成远程访问 VPN 策略配置。

过程

步骤 1 在您的 Cisco Secure Firewall Management Center Web 界面中，选择**策略**>**访问控制**。

步骤 2 点击要更新的访问控制策略旁边的 **编辑** 。

步骤 3 请点击 **添加规则**来添加新规则。

步骤 4 指定规则的 **名称** 并选择 **启用**。

步骤 5 选择 **操作**、 **允许** 或 **信任**。

步骤 6 在 **区域** 选项卡上选择以下选项：

a) 从可用区域中选择外部区域，然后点击**添加到源 (Add to Source)**。

b) 从可用区域中选择内部区域，然后点击**添加到目标 (Add to Destination)**。

步骤 7 在 **网络** 选项卡上选择以下选项：

a) 从可用网络中选择内部网络（内部接口和/或公司网络），然后点击 **添加到目标**。

b) 从 **可用网络** 中选择 VPN 地址池网络，然后点击 **添加到源网络**。

步骤 8 配置其他所需的访问控制规则设置，然后点击**添加 (Add)**。

步骤 9 保存此规则和访问控制策略。

（可选）配置 NAT 豁免

NAT 豁免将豁免转换地址，并允许已转换的主机和远程主机发起与受保护主机的连接。与身份 NAT 一样，请不要限制特定接口上的主机转换；必须对通过所有接口的连接使用 NAT 豁免。但是，借助 NAT 豁免，您可以在确定要转换的实际地址时指定实际地址和目标地址（类似于策略 NAT）。使用静态身份 NAT 以考虑访问列表中的端口。

为远程访问或站点间 VPN 配置静态身份 NAT 时，必须使用路由查找选项配置 NAT。如果没有路由查询， 会将流量向外发送到在 NAT 命令中指定的接口，无论路由表显示什么。例如，您不希望 通过不正确的接口发送 DHCP 范围流量；它永远不会返回到接口 IP 地址。路由查询选项允许 将流量直接发送到接口 IP 地址，而不是通过接口。对于从 VPN 客户端到内部网络上的主机的流量，路由查询选项仍将导致正确的出口接口（内部），因此，正常业务流不会受到影响。

开始之前

检查部署有远程访问 VPN 策略的目标设备上是否配置了 NAT。如果已在目标设备上启用 NAT，您必须定义 NAT 策略，为 VPN 流量设置豁免。

过程

步骤 1 在您的 Cisco Secure Firewall Management Center Web 界面上，点击**设备** > **NAT**。

步骤 2 选择要更新的 NAT 策略，或点击 **新建策略** 以使用允许所有连接的连接的 NAT 规则创建 NAT 策略。

步骤 3 点击**添加规则**，以添加 NAT 规则。

步骤 4 在“添加 NAT 规则”窗口中，选择以下内容：

a) 为“NAT 规则”选择**手动 NAT 规则**。

b) 为“类型”选择**静态**。

c) 点击 **接口对象** ，然后选择源和目标接口对象。

注释
此接口对象必须与在远程访问 VPN 策略中选择的接口相同。

有关详细信息，请参阅配置远程访问 VPN 的访问接口 ， 第 40 页。

a) 点击 **转换** 并选择源和目标网络：

- **原始源** 和 **转换后的源**
- **原始目标** 和 **转换后的目标**

步骤 5 在“高级”选项卡中，选择**不在目标接口上使用代理 ARP**。

不在目标接口上使用代理 ARP -为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。

步骤 6 点击**确定**。

配置 DNS

在每台 设备上配置 DNS，以便使用远程访问 VPN。如果没有 DNS，设备将无法解析 AAA 服务器名称、命名 URL 和具有 FQDN 或主机名的 CA 服务器。它只能解析 IP 地址。

过程

步骤 1 使用“平台设置”配置 DNS 服务器详细信息和域查找接口。有关详细信息，请参阅DNS和DNS 服务器组。

步骤 2 如果可以通过 VNP 网络访问 DNS 服务器，则在组策略中配置拆分隧道，以允许 DNS 流量通过远程访问 VPN 隧道。有关详细信息，请参阅配置组策略对象。

添加 安全客户端配置文件 XML 文件

安全客户端配置文件 是一组以 XML 文件形式存储的配置参数，客户端使用该文件来配置客户端的操作和外观。这些参数（XML 标记）包括主机名称和地址以及设置，用于启用更多客户端功能。

安全客户端配置文件 编辑器是一款基于 GUI 的配置工具，作为 安全客户端 软件包的一部分提供，您可以使用此编辑器来创建 安全客户端配置文件 。该程序可独立于 防火墙管理中心 而运行。有关安全客户端配置文件 编辑器的详细信息，请参阅 Cisco Secure Client（包括 AnyConnect）管理员指南。

开始之前

Cisco Secure Firewall Threat Defense 远程访问 VPN 策略要求将 安全客户端配置文件 的任务分配给 VPN 客户端。您可以将客户端配置文件连接到组策略。

您可以从 Cisco 软件下载中心下载 安全客户端配置文件 编辑器。

过程

步骤 1 选择 **设备** > **远程访问**。

步骤 2 点击要编辑的远程接入 VPN 策略旁边的 **编辑** 。

步骤 3 点击要添加的 Secure Client 配置文件上的 **编辑** 。

步骤 4 点击 **编辑组策略**。如果您选择添加新的组策略，请点击 **添加**。

步骤 5 选择 **安全客户端** > **配置文件**。

步骤 6 从 **客户端配置文件** 下拉列表中选择一个配置文件。如果您选择添加新的客户端配置文件，请点击 **添加** 并执行以下操作：

a) 指定配置文件 **名称**。

b) 点击 **浏览** 并选择 安全客户端配置文件 XML 文件。

注释
对于双因素身份验证，也要确保在 Secure Client 配置文件中将超时设置为 60 秒或更长。

c) 点击**保存**。

步骤 7 保存更改。

（可选）配置分割隧道

拆分隧道不仅允许 VPN 通过安全隧道连接到远程网络，而且允许连接到 VPN 隧道外的网络。如果要允许 VPN 用户在连接到远程访问 VPN 时访问外部网络，则您可以配置分割隧道。要配置拆分隧道列表，必须创建标准访问列表或扩展访问列表。

有关详细信息，请参阅配置组策略 ， 第 46 页。

过程

步骤 1 选择 **设备** > **远程访问**。

步骤 2 点击要为其配置分割隧道的远程访问 VPN 策略旁边的 **编辑** 。

步骤 3 在请求的连接配置文件上，点击 **编辑** 。

步骤 4 点击 **添加** 以添加组策略，或者点击 **编辑组策略**。

步骤 5 选择 **常规** > **分割隧道**。

步骤 6 从 **IPv4 拆分隧道** 或 **IPv6 拆分隧道** 列表中，选择**排除下面指定的网络** ；然后选择要从 VPN 流量中排除的网络。

默认设置允许所有流量通过 VPN 隧道。

步骤 7 点击**标准访问列表 (Standard Access List)** 或**扩展访问列表 (Extended Access List)**，然后从下拉列表中选择一个访问列表或添加新的访问列表。

步骤 8 如果您选择添加新的标准或扩展访问列表，请执行以下操作：

a) 为新访问列表指定**名称 (Name)**，然后点击**添加 (Add)**。

b) 从 **操作** 下拉列表中选择 **允许** 。

c) 选择允许通过 VPN 隧道的网络流量并点击 **添加**。

步骤 9 保存更改。

相关主题

访问列表

（可选）配置动态分割隧道

通过动态分割隧道，您可以根据 DNS 域名微调分割隧道。您可以配置远程接入 VPN 隧道中必须包含或排除的域。排除的域不会被阻止。相反，流向这些域的流量将保留在VPN隧道之外。例如：您可以将流量发送到公共互联网上的 Cisco WebEx，从而释放 VPN 隧道中的带宽，以用于发往受保护网络中服务器的流量。有关配置此功能的详细信息，请参阅 在 FMC 管理的 FTD 上配置 AnyConnect 动态拆分隧道。

开始之前

您可以使用 防火墙管理中心 和 从7.0或更高版本配置此功能。如果您有旧版本的 防火墙管理中心，可以按照 使用 FMC 进行 Firepower 威胁防御的高级 AnyConnect VPN 部署中的说明使用 FlexConfig 进行配置。

过程

步骤 1 将组策略配置为使用动态拆分隧道。

a) 选择 **设备 > 远程访问**。
b) 点击要为其配置动态分割隧道的远程访问 VPN 策略旁边的 **编辑** 。
c) 在请求的连接配置文件上，点击 **编辑** 。
d) 点击 **编辑组策略**。

步骤 2 在 **添加/编辑组策略** 对话框中配置 Cisco Secure 客户端 自定义属性。

a) 点击Cisco Secure 客户端选项卡。
b) 点击 **自定义属性** ，然后点击 **+**。
c) 从 **Cisco Secure 客户端 属性** 下拉列表中选择 **动态分割隧道** 。
d) 点击 **+** 创建新的自定义属性对象。
e) 输入自定义属性对象的名称。
f) **包含域**-指定将包含在远程访问 VPN 隧道中的域名。

   您可以在隧道中包含将根据 IP 地址排除的域。

g) **排除域**-指定将从远程访问 VPN 中排除的域名。

   排除的域未被阻止，流向这些域的流量将保留在 VPN 隧道之外。

h) 点击**保存**。
i) 点击**添加 (Add)**。

步骤 3 验证已配置的自定义属性，然后点击 **保存**，以保存组策略。

步骤 4 点击**保存**以保存连接文件。

步骤 5 点击**保存**以保存远程访问 VPN 策略。

下一步做什么

1. 在 上部署配置。
2. 验证 和 Secure Client上配置的动态拆分隧道配置。有关详细信息，请参阅验证动态分割隧道配置 ， 第 19 页。

验证动态分割隧道配置

在

使用以下命令验证动态分割隧道配置：

- **show running-config webvpn**
- **show running-config anyconnect-custom-data**
- **show running-config group-policy** <*group-policy-name*>

在 **Secure Client**

点击统计信息 ( ) 图标，然后选择 **VPN > 统计信息**。您可以在动态拆分排除/包含类别下确认域。

检验配置

过程

步骤 1 在外部网络上的计算机上打开 Web 浏览器。

步骤 2 输入配置 远程访问 VPN 网关的 URL。

步骤 3 提示时，输入用户名和密码，然后点击 **登录**。

注释
如果在系统上安装 安全客户端 ，则会自动建立与 VPN 的连接。

如果未安装 安全客户端 ，VPN 会提示您下载 安全客户端 。

步骤 4 下载 安全客户端 （如果尚未安装）并连接到 VPN。
安全客户端 自行安装。成功进行身份验证后，您将连接到 Cisco Secure Firewall Threat Defense 远程访问 VPN 网关。适用的身份或 QoS 策略根据您的远程访问 VPN 策略配置实施。

创建现有远程接入 VPN 策略的副本

复制现有的远程接入 VPN 策略，以便创建具有所有设置（包括连接配置文件和访问接口）的新策略。然后，您可以将设备分配给新策略，同时根据需要在分配的设备上部署 VPN。

注释 具有远程访问 VPN 只读权限的用户无法创建 VPN 的副本。域中拥有只读权限的用户可以复制远程访问 VPN。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 点击要复制的策略上的 **复制** 。

步骤 3 为新的远程访问 VPN 指定 **名称** 。

步骤 4 点击**确定**。

下一步做什么

要将设备分配给新策略，请参阅 设置远程访问 VPN 策略的目标设备，第 21 页。

设置远程访问 VPN 策略的目标设备

在创建远程访问 VPN 策略后，您可以将策略分配给威胁防御设备。

过程

步骤 1 选择 **设备** > **VPN** > **远程访问**。

步骤 2 点击要编辑的远程访问 VPN 策略旁边的 **编辑** (✎) 。

步骤 3 点击**策略分配**。

步骤 4 执行以下任一操作：

- 要将设备、高可用性对或设备组分配给策略，请在 **可用设备** 列表中将其选中，然后点击 **添加**。您还可以拖放可用设备进行选择。
- 要删除设备分配，请点击**所选设备 (Selected Devices)** 列表中的设备、高可用性对或设备组旁边的 **删除** (🗑)。

步骤 5 点击**确定**。

步骤 6 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

将本地领域与远程接入 VPN 策略相关联

您可以将本地领域与远程接入 VPN 策略相关联，以启用本地用户身份验证。

有关创建和管理领域的信息，请参阅管理领域。

有关为远程接入 VPN 配置本地用户认证的信息，请参阅配置远程访问 VPN 的 AAA 设置，第 24 页。

过程

步骤 1 选择 设备 > VPN > 远程访问。
步骤 2 点击要编辑的远程访问 VPN 策略旁边的 编辑 (✎) 。
步骤 3 点击本地领域旁边的链接。
步骤 4 从列表中选择 本地领域服务器 ，或点击 添加 以添加新的本地领域。
步骤 5 点击确定。
步骤 6 点击保存。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

其他远程访问 VPN 配置

配置连接配置文件设置

远程访问VPN策略包含针对特定设备的连接配置文件。这些策略与创建隧道本身有关，如如何完成AAA，以及如何为VPN客户端分配地址（DHCP或地址池）。它们还包括用户属性，这些属性将在设备上配置或从 AAA 服务器上获取的组策略中确定。设备还将提供名为 *DefaultWEBVPNGroup* 的默认连接配置文件。该连接配置文件是使用列表中显示的向导配置的。

如果您决定为不同的VPN用户组授予不同的权限，那么您可以为每个用户组添加特定的连接配置文件，并在远程访问 VPN 策略中维护多个连接配置文件。

过程

步骤 1 选择设备 > VPN > 远程访问。
步骤 2 在列表中选择现有的远程访问策略，然后点击相应的编辑图标。
步骤 3 选择 连接配置文件 (Connection Profile) ，然后点击 编辑 (Edit)。
步骤 4 （可选）如果您选择添加新的连接配置文件，请点击添加 (Add)。
步骤 5 配置 VPN 客户端的 IP 地址。
配置 VPN 客户端的 IP 地址 ， 第 23 页
步骤 6 （可选）更新远程访问 VPN 的 AAA 设置。
配置远程访问 VPN 的 AAA 设置 ， 第 24 页
步骤 7 （可选）创建或更新别名。
创建或更新连接配置文件的别名 ， 第 40 页

步骤 8 保存更改。

配置 VPN 客户端的 IP 地址

客户端地址分配允许您为远程访问 VPN 用户分配 IP 地址。

您可以从本地 IP 地址池、DHCP 服务器和 AAA 服务器为远程 VPN 客户端分配 IP 地址。首先由 AAA 服务器分配，然后由其他服务器分配。在**高级**选项卡中配置**客户端地址分配**策略，以定义分配条件。仅在连接配置文件的关联组策略或系统默认组策略 **DfltGrpPolicy** 中未定义 IP 池时，才会使用此连接配置文件中定义的 IP 池。

IPv4 地址池 - SSL VPN 客户端将在连接到 设备时收到新 IP 地址。地址池定义远程客户端可以接收的地址范围。可分别为 IPv4 和 IPv6 地址添加最多六个池。

注释 可以使用 防火墙管理中心 中现有 IP 池的 IP 地址，也可以使用**添加 (Add)** 选项来创建新的池。另外，还可以使用**对象 > 对象管理 > 地址池**路径在 防火墙管理中心中创建 IP 池。有关详细信息，请参阅地址池。

过程

步骤 1 选择**设备 > VPN > 远程访问**。
系统将列出现有的远程访问策略。

步骤 2 选择远程访问 VPN 策略，然后点击编辑图标。

步骤 3 选择要更新的连接配置文件，然后点击编辑图标。

步骤 4 在**客户端地址分配 (Client Address Assignment)** 选项卡下，执行以下操作：

步骤 5 点击**地址池 (Address Pools)** 旁边的 +：

a) 点击**地址池 (Address Pools)** 旁边的 + 以添加 IP 地址，然后选择 **IPv4** 或 **IPv6** 以添加相应的地址池。从**可用池(Available Pools)** 中选择 IP 地址池，然后点击**添加 (Add)**。

注释
如果在多台 Cisco Secure Firewall Threat Defense 设备之间共享远程访问 VPN 策略，请牢记所有设备都将共享同一地址池，除非使用设备级对象覆盖，将每台设备的全局定义替换为一个唯一地址池。在设备不使用 NAT 的情况下，需要多个唯一地址池，以免重叠地址。

b) 在**地址池 (Address Pools)** 窗口中点击**可用池 (Available Pools)** 旁边的 +，以添加新的 IPv4 或 IPv6 地址池。如果选择 IPv4 池，请提供起始和结束 IP 地址。如果选择包括新的 IPv6 地址池，请输入介于范围 1-16384 之间的**地址数量**。在多台设备之间共享对象时，选择**允许覆盖**选项可以避免与 IP 地址冲突。有关详细信息，请参阅地址池。

c) 点击**确定**。

如果您计划编辑 IP 地址池，则建议您在维护时间窗口期间执行以下步骤：

1. 从远程访问 VPN 取消分配设备。

2. 选择设备并点击**部署 (Deploy)**。

   此部署会从设备中删除所有远程访问 VPN 配置，终止远程访问 VPN 会话，而不会重新建立会话。

3. 点击 IP 地址池旁边的编辑图标可对其进行编辑，如有需要，可在 防火墙管理中心 上编辑任何其他远程访问 VPN 配置。

4. 将设备分配给更新后的远程访问 VPN 策略。

5. 在设备上部署配置。

   远程访问 VPN 客户端可以在维护窗口后连接到设备。

步骤 6 点击 **DHCP 服务器 (DHCP Servers)** 旁边的 + 以添加 DHCP 服务器：

注释
只能通过 IPv4 地址配置 DHCP 服务器地址。

a) 指定名称和 DHCP（动态主机配置协议）服务器地址作为网络对象。点击 **添加** ，然后从对象列表中选择服务器。点击 **删除** 以删除 DHCP 服务器。
b) 点击 **新对象** 页面中的 **添加** 以添加新网络对象。输入新对象名称、说明、网络，然后选择**允许覆盖**选项（如果适用）。有关详细信息，请参阅创建网络对象和允许对象覆盖。
c) 点击**确定**。

步骤 7 点击**保存**。

相关主题

配置连接配置文件设置 ， 第 22 页

配置远程访问 VPN 的 AAA 设置

开始之前

- 确保在终端上部署所需的计算机和用户证书。有关 证书的信息，请参阅 管理 证书。
- 使用所需的证书配置 安全客户端 配置文件。有关详细信息，请参阅《*Cisco Secure Client*（包括 *AnyConnect*）管理员指南》。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。
步骤 2 在列表中选择现有的远程访问策略，然后点击相应的**编辑**图标。
步骤 3 选择要更新 AAA 设置的连接配置文件，然后点击 **编辑** > **AAA**。
步骤 4 为 **身份验证**选择以下选项：

- **身份验证方法** - 确定在允许用户访问网络和网络服务之前对其进行标识的方式。这种方法通过要求提供有效的用户凭据（通常是用户名和密码）来控制访问。它也可能包括来自客户端的证书。受支持的身份验证方法有**仅 AAA**、**仅客户端证书**和 **AAA + 客户端证书**。

  何时选择以下**身份验证方法**：

  - **仅 AAA** - 如果选择 **RADIUS** 作为**身份验证服务器**，则授权服务器默认也采用此选择。从下拉列表中选择**记帐服务器**。每当从“身份验证服务器”下拉列表中选择 **AD** 和 **LDAP** 时，必须手动选择 **授权服务器** 和 **记帐服务器** 。

  - **SAML** - 使用 SAML 单点登录服务器对每个用户进行身份验证。有关详细信息，请参阅使用 SAML 2.0 的单点登录身份验证 ，第 92 页。

    覆盖身份提供程序证书-选择此选项可使用连接配置文件或 SAML 应用特定的 IdP 证书覆盖 SAML 提供程序的主身份提供程序证书。从 IdP 下拉列表中选择证书。

    Microsoft Azure 可以为同一实体 ID 支持多个应用。每个应用（映射到不同的连接配置文件）都需要唯一的证书。如果要在当前连接配置文件中保留单点登录对象的现有实体 ID 并使用其他 IdP 证书，则可以选择此选项。

    这启用每个 Microsoft Azure SAML 身份提供程序支持多个 SAML 应用。

    主身份证书在单点登录服务器对象中配置。

    有关配置单点登陆服务器对象的详细信息，请参阅添加单点登录服务器。

    选择您的 **SAML 登录体验** 以配置用于 SAML Web 身份验证的浏览器：

    - **VPN 客户端嵌入式浏览器**-选择此选项可使用 VPN 客户端嵌入式浏览器进行 Web 身份验证。身份验证仅适用于 VPN 连接。

    - **默认操作系统浏览器**-选择此选项可配置默认操作系统或支持 WebAuthN（用于 Web 身份验证的 FIDO2 标准）的本地浏览器。此选项启用单点登录 (SSO) 支持 Web 身份验证方法，例如生物识别身份验证。

      默认浏览器需要外部浏览器软件包进行 Web 身份验证。默认情况下配置软件包 默认-外部-浏览器-软件包。您可以通过编辑远程访问 VPN 策略并选择**高级 (Advanced)** > **安全客户端映像 (Secure Client Images)** > **软件包文件 (Package File)** 下的文件来更改默认外部浏览器软件包。

      您还可以通过选择添加新的软件包文件。**对象 (Objects)** > **对象管理 (Object Management)** > **VPN** > **安全客户端文件 (Secure Client File)** > **添加安全客户端文件 (Add Secure Client File)**。

  - **仅客户端证书** - 使用客户端证书对每个用户进行身份验证。客户端证书必须在 VPN 客户端终端上配置。默认情况下，用户名派生自客户端证书字段 CN 和 OU。如果在客户端证书的其他字段中指定了用户名，请使用“主”字段和“辅助”字段来映射适当的字段。

    选择 **启用多个证书身份验证** 以使用计算机和用户证书对 VPN 客户端进行身份验证。

    如果已启用多个证书身份验证，则可以选择以下证书之一来映射用户名和对 VPN 用户进行身份验证：

    - **第一个证书** - 选择此选项以映射从 VPN 客户端发送的计算机证书中的用户名。

- **第二个证书** - 选择此选项以映射从客户端发送的用户证书中的用户名。

注释
如果未启用多证书身份验证，则默认情况下使用用户证书（第二证书）进行身份验证。

如果选择**映射特定字段**选项（包括客户端证书中的用户名），则**主**字段和**辅助**字段将分别显示默认值：**CN**（**公用名**）和**OU**（**组织单位**）。如果选择**使用整个DN作为用户名**选项，系统将自动检索用户身份。可分辨名称(DN)是由单个字段组成的唯一标识，将用户与连接配置文件匹配时用作标识符。DN 规则用于增强的证书身份验证。

与**映射特定字段**选项相关的“主”字段和“辅助”字段包含以下公用值：

- C（国家/地区）
- CN（公用名）
- DNQ（DN 限定符）
- EA（邮件地址）
- GENQ（代系限定符）
- GN（名字）
- I（首字母）
- L（地区）
- N（名字）
- O（组织）
- OU（组织单位）
- SER（序列号）
- SN（姓氏）
- SP（省）
- T（职务）
- UID（用户 ID）
- UPN（用户主体名称）

- **客户端证书和 AAA** - 每个用户都使用客户端证书和 AAA 服务器进行身份验证。选择身份验证所需的证书和 AAA 配置。

  无论选择哪种身份验证方法，选择或取消选择**仅当用户位于授权数据库中时才允许连接**。

- **客户端证书和 SAML** - 每个用户都使用客户端证书和 AAA 服务器进行身份验证。选择所需的证书和 SAML 配置以进行身份验证。

- **允许仅在证书中的用户名与 SAML 相同时允许连接**-仅当证书中的用户名与 SAML 单点登录用户名匹配时，选择仅允许 VPN 连接。
- **从客户端证书中使用用户名进行授权**-选择从客户端证书中选择用户名进行授权时，必须配置要从客户端证书中选择的字段。

  您可以选择将特定字段映射为用户名，也可以使用整个可分辨名称 (DN) 进行授权：

  - **映射特定字段**- 从客户端证书中选择要包含的用户名，则 **主要** 和 **辅助** 字段将分别显示默认值： **CN**（**公用名**） 和 **OU**（**组织单位**） 。
  - **使用整个 DN 作为用户名**- 系统将自动检索用户身份用于授权。

您还可以创建动态访问策略 (DAP)，以将用户特定的 SAML 断言属性或用户名与 DAP 证书属性进行匹配。请参阅配置 DAP 的 AAA 条件设置。

- **身份验证服务器** - 身份验证是在允许用户访问网络和网络服务之前对其进行标识的方式。身份验证需要有效的用户凭证和/或证书。您可以单独使用身份验证功能，也可以将其与授权和记帐功能配合使用。

  如果您已添加服务器或创建身份验证服务器，请从列表中选择身份验证服务器：

  - **LOCAL**-使用来自 的本地数据库进行用户身份验证。要配置本地身份验证， 必须为版本 7.0 及更高版本。
    - **本地领域** - 选择本地领域或点击 **添加** 以配置领域。请参阅创建 LDAP 领域或 Active Directory 领域和领域目录。
  - **领域** - 配置 LDAP 或 AD 领域。请参阅创建 LDAP 领域或 Active Directory 领域和领域目录。
  - **RADIUS 服务器组** - 使用 RADIUS 服务器添加 RADIUS 服务器组对象。请参阅添加 RADIUS 服务器组。
  - **单点登录服务器** - 为 SAML 身份验证创建单点登录服务器对象。请参阅添加单点登录服务器。

回退到本地身份验证 - 使用本地数据库对用户进行身份验证，即使 AAA 服务器组不可用，只要已配置本地数据库，即可建立 VPN 隧道。

- **使用辅助身份验证** - 除主身份验证之外，还配置了辅助身份验证，以便为 VPN 会话提供额外的安全保护。辅助身份验证是仅适用于**仅 AAA** 和**客户端证书和 AAA** 身份验证方法。

  辅助身份验证是一项可选功能，该功能要求 VPN 用户在 安全客户端 登录屏幕上输入两组用户名和密码。您还可以配置为从身份验证服务器或客户端证书预填充辅助用户名。仅当主身份验证和辅助身份验证均成功时，才会授予远程访问VPN身份验证。如果任何一个身份验证服务器无法访问或一个身份验证失败，VPN 身份验证将被拒绝。

必须在配置辅助身份验证前，为辅助用户名和密码配置辅助身份验证服务器组（AAA服务器）。例如，可以将主身份验证服务器设置为 LDAP 或 Active Directory 领域，将辅助身份验证设置为 RADIUS 服务器。

注释
默认情况下，无需辅助身份验证。

身份验证服务器 - 为 VPN 用户提供辅助用户名和密码的辅助身份验证服务器。

- **回退到本地身份验证** - 使用本地数据库对此用户进行身份验证，即使 AAA 服务器组不可用，只要已配置本地数据库，即可建立 VPN 隧道。

选择 **辅助身份验证的用户名**以下的选项：

- **提示：** 在登录 VPN 网关时，提示用户输入用户名和密码。
- **使用主身份验证用户名：** 用户名从主身份验证服务器获取，用于主身份验证和辅助身份验证；必须输入两个密码。
- **映射客户端证书中的用户名：** 预填充客户端证书中的辅助用户名。

  如果已启用多个证书身份验证，则可以选择以下证书之一：

  - **第一个证书** - 选择此选项以映射从 VPN 客户端发送的计算机证书中的用户名。
  - **第二个证书** - 选择此选项以映射从客户端发送的用户证书中的用户名。
  - 如果选择**映射特定字段**选项，其中包括来自客户端证书的用户名。则**主**和**辅助**字段将显示默认值：**CN (公用名称)** 和 **OU (组织单位)**。如果选择**使用整个 DN（可分辨名称）作为用户名**选项，系统将自动检索用户身份。

    有关主字段和辅助字段映射的详细信息，请参阅**身份验证方法**说明。
  - **在用户登录窗口预填证书中的用户名 (Prefill username from certificate on user login window)：** 用户通过 安全客户端 VPN 客户端连接时，预填充客户端证书中的辅助用户名。
    - **在登录窗口隐藏用户名：** 辅助用户名是从客户端证书预填充的，但对用户隐藏，确保用户不会修改预填充的用户名。
- **使用 VPN 会话的辅助用户名：** 辅助用户名用于在 VPN 会话期间报告用户活动。

步骤 5 为 **授权**选择以下选项：

- **身份验证服务器** - 身份验证完成后，授权将控制对每个经过身份验证的用户都可用的服务和命令。授权通过组合一组描述用户被授权执行的操作、其实际功能和限制的属性来工作。当您不使用授权，则单独的身份验证将为所有经过身份验证的用户提供相同的访问权限。授权需要进行身份验证。

  要了解有关远程访问 VPN 授权工作原理的更多信息，请参阅 了解权限和属性的策略实施，第 6 页。

在连接配置文件中配置了 RADIUS 服务器以进行用户授权时，远程访问 VPN 系统管理员可以为用户或用户组配置多个授权属性。在 RADIUS 服务器上配置的授权属性可以特定于用户或用户组。用户通过身份验证后，这些特定的授权属性将被推送到 设备。

注释
从授权服务器获得的AAA服务器属性覆盖了之前在组策略或连接配置文件上可能已经配置的属性值。

- 如果需要，请选择**仅当用户位于授权数据库中时才允许连接**。

  启用该选项后，系统检查客户端的用户名必须存在于授权数据库中，才可以成功进行连接。如果授权数据库中不存在该用户名，则连接被拒绝。

- 当您选择领域作为授权服务器时，必须配置 LDAP 属性映射。您可以选择用于身份验证和授权的单个服务器或其他服务器。点击 **配置 LDAP 属性映射** 以添加用于授权的 LDAP属性映射。

  注释
  不支持将 SAML 身份提供程序用作授权服务器。如果 SAML 身份提供程序后面的 Active Directory 可通过 防火墙管理中心 和 访问，则可以按照以下步骤配置授权：

  - 为 AD 服务器添加领域。请参阅创建 LDAP 领域或 Active Directory 领域和领域目录。
  - 选择领域对象作为远程访问 VPN 连接配置文件中的授权服务器。
  - 为所选领域配置 LDAP 属性映射。

  有关配置 LDAP 属性映射的信息，请参阅 配置 LDAP 属性映射 ， 第 47 页。

步骤 6 为 **记帐**选择以下选项：

- **记账服务器** - 记账用于跟踪用户正在访问的服务和他们正在使用的网络资源量。当激活 AAA 记帐时，网络访问服务器会向 RADIUS 服务器报告用户活动。记账信息包括每个会话的开始和停止时间、用户名、会话时通过设备的字节数、使用的服务以及每个会话的持续时间。然后系统可以分析该数据，以进行网络管理、客户端计费或审核。您可以单独使用记帐功能，也可以将其与身份验证和授权功能配合使用。

  指定将用于对远程访问 VPN 会话进行记帐的 RADIUS 服务器组对象。

步骤 7 选择 **高级设置**以下的选项：

- **从用户名删除领域** - 在将用户名传递到 AAA 服务器之前，选择要从用户名删除领域。例如，如果选择此选项并提供域\用户名，则该域将从用户名中删除，并发送到 AAA 服务器进行身份验证。默认情况下，此选项处于取消选中状态。
- **从用户名删除组** - 在将用户名传递到 AAA 服务器之前，选择要从用户名删除组名称。默认情况下，此选项处于取消选中状态。

  注释
  领域是管理域。启用这些选项将允许仅基于用户名进行身份验证。您可以启用这些选项的任意组合。但是，如果服务器无法分析分隔符，则必须选中这两个复选框。

- **密码管理 (Password Management)**：启用远程访问 VPN 用户的密码管理。选择以提前通知密码到期或密码到期的日期。

步骤 8 点击**保存**。

相关主题

了解权限和属性的策略实施，第 6 页
管理领域

Cisco Secure Firewall Threat Defense 的 RADIUS 服务器属性

设备支持将用户授权属性（也称为用户权利或权限）应用到来自外部RADIUS服务器的VPN连接，这些连接被配置为用于远程接入 VPN 策略中的身份验证和/或授权。

注释 Cisco Secure Firewall Threat Defense 设备支持具有供应商 ID 3076 的属性。

以下用户授权属性由 RADIUS 服务器发送到 设备。

- RADIUS 属性 146 和 150 是从 设备发送到 RADIUS 服务器，以提出身份验证和请求授权。
- 所有三个属性（146、150 和 151）都是从 设备发送到 RADIUS 服务器，以提出开始记账、临时更新和停止请求。

*表 2: 从 **Cisco Secure Firewall Threat Defense** 发送到 **RADIUS** 服务器的 **RADIUS** 属性*

属性	属性编号	语法、类型	单值或多值	说明或值
连接配置文件名称或隧道组名称	146	字符串	单值	1 到 253 个字符
客户端类型	150	整数	单值	2 = Secure Client SSL VPN, 6 = Secure Client IPsec VPN (IKEv2)
会话类型	151	整数	单值	1 = Secure Client SSL VPN, 2 = Secure Client IPsec VPN (IKEv2)

*表 3: 支持的 **RADIUS** 授权属性*

属性名称		属性编号	语法/类型	单值或多值	说明或值
Access-Hours	是	1	字符串	单值	时间范围的名称，例如工作时间

属性名称		属性编号	语法/类型	单值或多值	说明或值
Access-List-Inbound	是	86	字符串	单值	这两个访问列表属性都使用 设备上配置的 称。使用Smart CLI扩展访问列表对象类型 （依次选择**设备 (Device)** > **高级配置 (Adv** **Configuration)** > **Smart CLI** > **对象 (Obje** 此类 ACL 用于控制入站流量（流量进入 出站流量（流量离开 设备）。
Access-List-Outbound	是	87	字符串	单值	
Address-Pools	是	217	字符串	单值	设备上定义的网络对象名称，用于识别将 池供客户端连接远程访问 VPN时使用的子 **象** 页面上定义网络对象，然后将网络对象 或连接配置文件相关联。
Allow-Network-Extension-Mode	是	64	布尔值	单值	0 = 已禁用 1 = 已启用
Authenticated-User-Idle-Timeout	是	50	整数	单值	1-35791394 分钟
Authorization-DN-Field	是	67	字符串	单值	可能的值：UID、OU、O、CN、L、SP、 T、N、GN、SN、I、GENQ、DNQ、SER use-entire-name
Authorization-Required		66	整数	单值	0 = 否 1 = 是
Authorization-Type	是	65	整数	单值	0 = 无 1 = RADIUS 2 = LDAP
Banner1	是	15	字符串	单值	要为思科 VPN 远程访问会话显示的横幅等 IPsec IKEv1、 安全客户端 SSL TLS/DTLS Clientless SSL。
Banner2	是	36	字符串	单值	要为思科 VPN 远程访问会话显示的横幅等 IPsec IKEv1、 安全客户端 SSL TLS/DTLS Clientless SSL。如果进行了相应的配置， 字符串会连接到 Banner1 字符串。
Cisco-IP-Phone-Bypass	是	51	整数	单值	0 = 已禁用 1 = 已启用
Cisco-LEAP-Bypass	是	75	整数	单值	0 = 已禁用 1 = 已启用
Client Type	是	150	整数	单值	1 = 思科 VPN 客户端 (IKEv1) 2 = Secure C VPN 3 = 无客户端 SSL VPN 4 = 直接转发 L2TP/IPsec SSL VPN 6 = Secure Client IPs (IKEv2)
Client-Type-Version-Limiting	是	77	字符串	单值	IPsec VPN 版本号字符串
DHCP-Network-Scope	是	61	字符串	单值	IP 地址

属性名称		属性编号	语法/类型	单值或多值	说明或值
Extended-Authentication-On-Rekey	是	122	整数	单值	0 = 已禁用 1 = 已启用
Framed-Interface-Id	是	96	字符串	单值	分配的 IPv6 接口 ID。与 Framed-IPv6-Prefix 用以创建完整的已分配 IPv6 地址。例如：Framed-Interface-ID =1:1:1:1与 Framed-IPv6-P =2001:0db8::/64 组合可提供分配的IP地址 2001:0db8::1:1:1:1。
Framed-IPv6-Prefix	是	97	字符串	单值	分配的 IPv6 前缀和长度。与 Framed-Interfac 合以创建完整的已分配 IPv6 地址。例如：前 2001:0db8::/64 与 Framed-Interface-Id=1:1:1:1 提供IP地址 2001:0db8::1:1:1:1。通过分配前缀 为/128 的完整 IPv6 地址（例如，Framed-IPv6-Prefix=2001:0db8::1/128），可以 属性分配IP地址而不使用 Framed-Interface-Id
Group-Policy	是	25	字符串	单值	为远程访问 VPN 会话设置组策略。您可以使 其中一种格式： • 组策略名称 • OU = 组策略名称 • OU = 组策略名称；
IE-Proxy-Bypass-Local		83	整数	单值	0 = 无 1 = 本地
IE-Proxy-Exception-List		82	字符串	单值	换行符 (\n) 分隔的 DNS 域列表
IE-Proxy-PAC-URL	是	133	字符串	单值	PAC 地址字符串
IE-Proxy-Server		80	字符串	单值	IP 地址
IE-Proxy-Server-Policy		81	整数	单值	1 = 无修改 2 = 无代理 3 = 自动检测 4 = 使用 设置
IKE-KeepAlive-Confidence-Interval	是	68	整数	单值	10 到 300 秒
IKE-Keepalive-Retry-Interval	是	84	整数	单值	2 到 10 秒
IKE-Keep-Alives	是	41	布尔值	单值	0 = 已禁用 1 = 已启用
Intercept-DHCP-Configure-Msg	是	62	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Allow-Passwd-Store	是	16	布尔值	单值	0 = 已禁用 1 = 已启用

属性名称		属性编号	语法/类型	单值或多值	说明或值
IPsec-Authentication		13	整数	单值	0 = 无 1 = RADIUS 2 = LDAP（仅适用于 = NT 域 4 = SDI 5 = 内部 6 = RADIUS 到 Kerberos/Active Directory
IPsec-Auth-On-Rekey	是	42	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Backup-Server-List	是	60	字符串	单值	服务器地址（以空格分隔）
IPsec-Backup-Servers	是	59	字符串	单值	1 = 使用客户端配置的列表 2 = 禁用并清除 表 3 = 使用备份服务器列表
IPsec-Client-Firewall-Filter-Name		57	字符串	单值	指定要作为防火墙策略推送到客户端的过 称
IPsec-Client-Firewall-Filter-Optional	是	58	整数	单值	0 = 必需 1 = 可选
IPsec-Default-Domain	是	28	字符串	单值	指定要发送到客户端的单个默认域名（1 符）。
IPsec-IKE-Peer-ID-Check	是	40	整数	单值	1 = 必需 2 = 如果对等证书支持 3 = 不检
IPsec-IP-Compression	是	39	整数	单值	0 = 已禁用 1 = 已启用
IPsec-Mode-Config	是	31	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP	是	34	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP-Port	是	35	整数	单值	4001 到 49151。默认值为 10000。
IPsec-Required-Client-Firewall-Capability	是	56	整数	单值	0 = 无 1 = 远程 FW Are-You-There (AYT) 略 2 = 策略推送的 CPP 4 = 来自服务器的
IPsec-Sec-Association		12	字符串	单值	安全关联的名称
IPsec-Split-DNS-Names	是	29	字符串	单值	指定要发送到客户端的辅助域名列表（1 符）。
IPsec-Split-Tunneling-Policy	是	55	整数	单值	0 = 无拆分隧道 1 = 拆分隧道 2 = 允许本
IPsec-Split-Tunnel-List	是	27	字符串	单值	指定用于描述分割隧道包含列表的网络或 称。
IPsec-Tunnel-Type	是	30	整数	单值	1 = LAN 到 LAN 2 = 远程访问
IPsec-User-Group-Lock		33	布尔值	单值	0 = 已禁用 1 = 已启用
IPv6-Address-Pools	是	218	字符串	单值	IP 本地池 IPv6 的名称

属性名称		属性编号	语法/类型	单值或多值	说明或值
IPv6-VPN-Filter	是	219	字符串	单值	ACL 值
L2TP-Encryption		21	整数	单值	位图： 1 = 需要加密 2 = 40 位 4 = 128 位 8 无状态 15= 40/128 位加密/需要无状态
L2TP-MPPC-Compression		38	整数	单值	0 = 已禁用 1 = 已启用
Member-Of	是	145	字符串	单值	逗号分隔的字符串，例如： `Engineering, Sales` 可在动态访问策略里使用的管理属性。不设 略。
MS-Client-Subnet-Mask	是	63	布尔值	单值	IP 地址
NAC-Default-ACL		92	字符串		ACL
NAC-Enable		89	整数	单值	0 = 否 1 = 是
NAC-Revalidation-Timer		91	整数	单值	300 到 86400 秒
NAC-Settings	是	141	字符串	单值	NAC 策略名称
NAC-Status-Query-Timer		90	整数	单值	30 到 1800 秒
Perfect-Forward-Secrecy-Enable	是	88	布尔值	单值	0 = 否 1 = 是
PPTP-Encryption		20	整数	单值	位图： 1 = 需要加密 2 = 40 位 4 = 128 位 8 无状态 15= 40/128 位加密/需要无状态
PPTP-MPPC-Compression		37	整数	单值	0 = 已禁用 1 = 已启用
Primary-DNS	是	5	字符串	单值	IP 地址
Primary-WINS	是	7	字符串	单值	IP 地址
Privilege-Level	是	220	整数	单值	介于 0 和 15 之间的整数。
Required-Client- Firewall-Vendor-Code	是	45	整数	单值	1 = 思科系统（使用思科集成客户端） 2 = Zo 3 = NetworkICE 4 = Sygate 5 = 思科系统（使 入侵防御安全代理）
Required-Client-Firewall-Description	是	47	字符串	单值	字符串

属性名称		属性编号	语法/类型	单值或多值	说明或值
Required-Client-Firewall-Product-Code	是	46	整数	单值	思科系统公司产品： 1 = 思科入侵防御安全代理或思科集成客 Zone Labs 产品： 1 = Zone Alarm 2 = Zon 3 = Zone Labs Integrity NetworkICE 产品： 1 = BlackIce Defende Sygate 产品： 1 = Personal Firewall 2 = P Firewall Pro 3 = 安全代理
Required-Individual-User-Auth	是	49	整数	单值	0 = 已禁用 1 = 已启用
Require-HW-Client-Auth	是	48	布尔值	单值	0 = 已禁用 1 = 已启用
Secondary-DNS	是	6	字符串	单值	IP 地址
Secondary-WINS	是	8	字符串	单值	IP 地址
SEP-Card-Assignment		9	整数	单值	未使用
Session Subtype	是	152	整数	单值	0 = 无 1 = 无客户端 2 = 客户端 3 = 仅客 Session Subtype 的适用条件是 Session Typ 性仅具有以下值：1、2、3 和 4。
Session Type	是	151	整数	单值	0 = 无1 = Secure Client SSL VPN 2 = Secu IPSec VPN (IKEv2) 3 = 无客户端 SSL VP 户端邮件代理5 = 思科 VPN 客户端 (IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN
Simultaneous-Logins	是	2	整数	单值	0 到 2147483647
Smart-Tunnel	是	136	字符串	单值	智能隧道的名称
Smart-Tunnel-Auto	是	138	整数	单值	0 = 已禁用 1 = 已启用 2 = 自动启动
Smart-Tunnel-Auto-Signon-Enable	是	139	字符串	单值	智能隧道自动登录名称列表（附带域名）
Strip-Realm	是	135	布尔值	单值	0 = 已禁用 1 = 已启用
SVC-Ask	是	131	字符串	单值	0 = 已禁用 1 = 已启用 3 = 启用默认服务 认无客户端 （未使用 2 和 4）
SVC-Ask-Timeout	是	132	整数	单值	5 到 120 秒
SVC-DPD-Interval-Client	是	108	整数	单值	0 = 关 5-3600 秒
SVC-DPD-Interval-Gateway	是	109	整数	单值	0 = 关） 5-3600 秒

属性名称		属性编号	语法/类型	单值或多值	说明或值
SVC-DTLS	是	123	整数	单值	0 = 错误 1 = 正确
SVC-Keepalive	是	107	整数	单值	0 = 关 15-600 秒
SVC-Modules	是	127	字符串	单值	字符串（模块的名称）
SVC-MTU	是	125	整数	单值	MTU 值 256-1406 字节
SVC-Profiles	是	128	字符串	单值	字符串（配置文件的名称）
SVC-Rekey-Time	是	110	整数	单值	0 = 已禁用 1-10080 分钟
Tunnel Group Name	是	146	字符串	单值	1 到 253 个字符
Tunnel-Group-Lock	是	85	字符串	单值	隧道组的名称或“none”
Tunneling-Protocols	是	11	整数	单值	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2T 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 互斥。 0 - 11、16 - 27、32 - 43、48 - 59 是合
Use-Client-Address		17	布尔值	单值	0 = 已禁用 1 = 已启用
VLAN	是	140	整数	单值	0 到 4094
WebVPN-Access-List	是	73	字符串	单值	访问列表名称
WebVPN ACL	是	73	字符串	单值	设备上的 WebVPN ACL 的名称
WebVPN-ActiveX-Relay	是	137	整数	单值	0 = 已禁用 Otherwise = 已启用
WebVPN-Apply-ACL	是	102	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Auto-HTTP-Signon	是	124	字符串	单值	保留
WebVPN-Citrix-Metaframe-Enable	是	101	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Content-Filter-Parameters	是	69	整数	单值	1 = Java ActiveX 2 = Java 脚本 4 = 映像 8 = 的 Cookie
WebVPN-Customization	是	113	字符串	单值	自定义的名称
WebVPN-Default-Homepage	是	76	字符串	单值	URL，例如 http://example-example.com
WebVPN-Deny-Message	是	116	字符串	单值	有效字符串（最多 500 个字符）
WebVPN-Download_Max-Size	是	157	整数	单值	0x7fffffff
WebVPN-File-Access-Enable	是	94	整数	单值	0 = 已禁用 1 = 已启用

属性名称		属性编号	语法/类型	单值或多值	说明或值
WebVPN-File-Server-Browsing-Enable	是	96	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-File-Server-Entry-Enable	是	95	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	是	78	字符串	单值	带可选通配符 (*) 的逗号分隔的 DNS/IP *.cisco.com、192.168.1.*、wwwin.cisco.co
WebVPN-Hidden-Shares	是	126	整数	单值	0 = 无 1 = 可见
WebVPN-Home-Page-Use-Smart-Tunnel	是	228	布尔值	单值	已启用（如果无客户端主页将通过智能隧
WebVPN-HTML-Filter	是	69	位图	单值	1 = Java ActiveX 2 = 脚本 4 = 映像 8 = C
WebVPN-HTTP-Compression	是	120	整数	单值	0 = 关 1 = Deflate 压缩
WebVPN-HTTP-Proxy-IP-Address	是	74	字符串	单值	逗号分隔的 DNS/IP:端口，带 http= 或 https 如 http=10.10.10.10:80、https=11.11.11.11:
WebVPN-Idle-Timeout-Alert-Interval	是	148	整数	单值	0 到 30 0 = 已禁用。
WebVPN-Keepalive-Ignore	是	121	整数	单值	0 到 900
WebVPN-Macro-Substitution	有	223	字符串	单值	无限制。
WebVPN-Macro-Substitution	有	224	字符串	单值	无限制。
WebVPN-Port-Forwarding-Enable	是	97	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	是	98	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-HTTP-Proxy	是	99	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-List	是	72	字符串	单值	端口转发列表名称
WebVPN-Port-Forwarding-Name	是	79	字符串	单值	字符串名称（例如，“Corporate-Apps”） 此文本将替换无客户端门户主页上的默认 “Application Access”。
WebVPN-Post-Max-Size	是	159	整数	单值	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	是	149	整数	单值	0 到 30 0 = 已禁用。
WebVPN Smart-Card-Removal-Disconnect	是	225	布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-Smart-Tunnel	是	136	字符串	单值	智能隧道的名称
WebVPN-Smart-Tunnel-Auto-Sign-On	是	139	字符串	单值	智能隧道自动登录名称列表（附带域名）

属性名称		属性编号	语法/类型	单值或多值	说明或值
WebVPN-Smart-Tunnel-Auto-Start	是	138	整数	单值	0 = 已禁用 1 = 已启用 2 = 自动启动
WebVPN-Smart-Tunnel-Tunnel-Policy	是	227	字符串	单值	“e networkname”、“i networkname”或“a 一，其中 networkname 是指智能隧道网络列表 称，e表示不包含的隧道，i表示指定的隧道， 所有隧道。
WebVPN-SSL-VPN-Client-Enable	是	103	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSL-VPN-Client-Keep- Installation	是	105	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSL-VPN-Client-Required	是	104	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSO-Server-Name	是	114	字符串	单值	有效字符串
WebVPN-Storage-Key	是	162	字符串	单值	
WebVPN-Storage-Objects	是	161	字符串	单值	
WebVPN-SVC-Keepalive-Frequency	是	107	整数	单值	15 到 600 秒，0 = 关闭
WebVPN-SVC-Client-DPD-Frequency	是	108	整数	单值	5 到 3600 秒，0 = 关闭
WebVPN-SVC-DTLS-Enable	是	123	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-DTLS-MTU	是	125	整数	单值	MTU 值为 256 到 1406 个字节。
WebVPN-SVC-Gateway-DPD-Frequency	是	109	整数	单值	5 到 3600 秒，0 = 关闭
WebVPN-SVC-Rekey-Time	是	110	整数	单值	4 到 10080 分钟，0 = 关闭
WebVPN-SVC-Rekey-Method	是	111	整数	单值	0（关闭）、1 (SSL)、2（新隧道）
WebVPN-SVC-Compression	是	112	整数	单值	0（关闭）、1（Deflate 压缩）
WebVPN-UNIX-Group-ID (GID)	是	222	整数	单值	有效 UNIX 组 ID
WebVPN-UNIX-User-ID (UID)	是	221	整数	单值	有效 UNIX 用户 ID
WebVPN-Upload-Max-Size	是	158	整数	单值	0x7fffffff
WebVPN-URL-Entry-Enable	是	93	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-URL-List	是	71	字符串	单值	URL 列表名称
WebVPN-User-Storage	是	160	字符串	单值	
WebVPN-VDI	是	163	字符串	单值	设置列表

表 *4:* 发送到 *Cisco Secure Firewall Threat Defense* 的 *RADIUS* 属性

属性	属性编号	语法、类型	单值或多值	说明或值
Address-Pools	217	字符串	单值	设备上定义的网络对象名称，用于识别将作为地址池供客户端连接远程访问 VPN 时使用的子网。在 **对象 (Objects)** 页面上定义网络对象。
Banner1	15	字符串	单值	用户登录时显示的横幅。
Banner2	36	字符串	单值	用户登录时显示的横幅的第二部分。横幅 2 附加到横幅 1。
可下载 ACL	Cisco-AV-Pair	merge-dacl {before-avpair | after-avpair}		通过 Cisco-AV-Pair 配置来支持。
过滤器 ACL	86, 87	字符串	单值	过滤器 ACL 由 RADIUS 服务器中的 ACL 名称引用。它要求 设备上已经存在 ACL 配置，以便可以在 RADIUS 授权期间使用该配置。 86=Access-List-Inbound 87=Access-List-Outbound
Group-Policy	25	字符串	单值	要在连接中使用的组策略。必须在远程访问 VPN **组策略** 页面上创建组策略。您可以使用以下其中一种格式： • 组策略名称 • OU = 组策略名称 • OU = 组策略名称；
Simultaneous-Logins	2	整数	单值	允许用户建立的独立并发连接的数量，0 - 2147483647。
VLAN	140	整数	单值	限制用户连接的 VLAN，0 - 4094。还必须在 设备的子接口上配置此 VLAN。

您必须将从 ISE 返回的 IE-Proxy-Server-Method 属性的值设置为以下值之一：

- IE_PROXY_Method_PACFILE: 8
- IE_PROXY_Method_PACFILE_AND_AUTODETECT: 11
- IE_PROXY_Method_PACFILE_AND_USE_SERVER: 12
- IE_PROXY_Method_PACFILE_AND_AUTODETECT_AND_USE_SERVER: 15

仅当上述值之一用于 IE-Proxy-Server-Method 属性时，才会提供代理设置。

创建或更新连接配置文件的别名

别名包含特定连接配置文件的备用名称或 URL。远程访问 VPN 管理员可以启用或禁用别名和别名 URL。VPN 用户可以在连接到 Cisco Secure Firewall Threat Defense设备时选择别名。可以开启或关闭在此设备上配置的所有连接的别名，以开启或关闭别名显示。您还可以配置别名URL列表，您的终端在启动远程访问 VPN 连接时可以从该列表中进行选择。如果用户使用别名 URL 进行连接，则系统将使用与别名 URL 匹配的连接配置文件自动记录它们。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 点击要修改的策略上的**编辑 (Edit)**。

步骤 3 在要为其创建或更新别名的连接配置文件上点击**编辑 (Edit)**。

步骤 4 点击 **别名**。

步骤 5 要添加别名，请执行以下操作：

a) 点击**别名 (Alias Names)** 下的**添加 (Add)**。
b) 指定**别名**。
c) 选中每个窗口中的**已启用**复选框以启用别名。
d) 点击**确定**。

步骤 6 要添加别名 URL，请执行以下操作：

a) 点击 **URL 别名 (URL Alias)** 下的**添加 (Add)**。
b) 从列表中选择 **别名 URL** 或创建新的 URL 对象。有关详细信息，请参阅创建 URL 对象。
c) 选中每个窗口中的**已启用**复选框以启用别名。
d) 点击**确定**。

步骤 7 保存更改。

相关主题

配置连接配置文件设置 ， 第 22 页

配置远程访问 VPN 的访问接口

访问接口表列出了包含设备接口的接口组和安全区域。它们配置用于远程访问 SSL 或 IPsec IKEv2 VPN 连接。该表显示每个接口组或安全区域的名称、接口使用的接口信任点以及是否启用了数据报传输层安全(DTLS)。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 在列表中选择现有的远程访问策略，然后点击相应的**编辑**图标。

步骤 3 点击**访问接口 (Access Interface)** 选项卡。

步骤 4 要添加访问接口，请点击 **+**，并在**添加访问接口 (Add Access Interface)** 对话框中为以下选项指定值：

a) **访问接口** - 选择接口所属的接口组或安全区域。

接口组或安全区域必须是路由类型。远程访问 VPN 连接不支持其他接口类型。

b) 通过选择以下选项将**协议**对象与访问接口关联：

- **启用 IPSet-IKEv2** - 选择此选项可启用 **IKEv2** 设置。
- **启用 SSL** - 选择此选项可启用 **SSL** 设置。
  - 选择**启用数据报传输层安全**。

    选中此选项后，将在接口上启用数据报传输层安全 (DTLS)，并允许 Cisco Secure Client 的 AnyConnect VPN 模块使用两个同步隧道（一个 SSL 隧道和一个 DTLS 隧道）建立 SSL VPN 连接。

    启用 DTLS 可避免与某些 SSL 连接相关的延迟和带宽问题，并可提高对于数据包延迟敏感的实时应用的性能。

    要配置 SSL 设置以及 TLS 和 DTLS 版本，请参阅 关于 SSL 设置。

    要配置 Cisco Secure Client 的 AnyConnect VPN 型号的 SSL 设置，请参阅 组策略 Secure Client 选项。

  - 选中 **配置接口特定身份证书** 复选框，然后从下拉列表中选择 **接口身份证书** 。

    如果不选择接口身份证书，则默认使用 **信任点**。

    如果不选择接口身份证书或信任点，则默认使用 **SSL 全局身份证书** 。

c) 点击**确定 (OK)** 以保存更改。

步骤 5 在 **访问设置**下选择以下选项：

- **允许用户选择将登录的连接配置文件 (Allow Users to select connection profile while logging in)** - 如果您有多个连接配置文件，选中此复选框将允许用户在登录期间选择正确的连接配置文件。必须为 **IPsec-IKEv2** VPN 选择此选项。
- **启用仅 HTTP VPN Cookie (Enable HTTP-only VPN Cookies)** - 选中此复选框可启用仅 HTTP VPN Cookie。

步骤 6 使用以下选项配置 **SSL 设置**：

- **Web 访问端口号** - 用于 VPN 会话的端口。默认端口为 443。

- **DTLS 端口号** - 要用于 DTLS 连接的 UDP 端口。默认端口为 443。
- **SSL 全域身份证书**-如果未提供 **接口特定身份证书** ，则选定的 **SSL 全局身份证书** 将用于所有关联的接口。

步骤 7 对于 **IPsec-IKEv2 设置**，请从列表中选择 **IKEv2 身份证书** 或添加身份证书。

步骤 8 配置**服务访问控制 (Service Access Control)**。从**服务访问对象 (Service Access Object)** 下拉列表中选择服务访问对象，或点击 **+** 创建新对象。

您可以在运行 7.7 或更高版本的 设备上使用服务访问对象，以便控制对远程客户访问 VPN 的访问。该对象可在 VPN 验证前为客户端提供基于地理位置的访问控制。默认情况下，RA VPN 没有访问控制，远程客户端可以从任何地理位置进行连接，除非由服务访问对象指定。有关详细信息，请参阅基于地理位置管理远程用户的 VPN 访问 ，第 73 页和配置服务访问对象。

步骤 9 在 **VPN 流量的访问控制** 部分下，如果要绕过访问控制策略，请选择以下选项：

- **为已解密的流量绕过访问控制策略 (sysopt permit-vpn)** - 默认情况下，已解密流量要经过访问控制策略的检查。启用“为已解密的流量绕过访问控制策略”选项会绕过 ACL 检查，但 VPN 过滤器 ACL 以及从 AAA 服务器下载的身份验证 ACL 仍适用于 VPN 流量。

  注释
  如果选择此选项，则无需更新在 Cisco Secure Firewall Threat Defense 设备上更新访问控制策略 ，第 14 页中指定的远程访问 VPN 的访问控制策略。

步骤 10 点击**保存**，保存接口更改。

相关主题

接口

配置远程访问 VPN 的高级选项

思科 安全客户端 映像

安全客户端 映像

安全客户端通过企业资源的全 VPN 调配为远程用户提供到 设备的安全 SSL 或 IPsec (IKEv2) 连接。如果先前没有安装客户端，远程用户可以输入为在其浏览器中接受无客户端 VPN 连接所配置的接口的 IP 地址，以下载并安装 Secure Client。设备下载与远程计算机的操作系统匹配的客户端。下载后，客户端安装并建立安全连接。如果先前已安装客户端，当用户进行身份验证时， 设备将检查客户端的版本并在必要情况下升级客户端。

远程访问 VPN 管理员将新的或附加的 Secure Client 映像与 VPN 策略相关联。管理员可以取消关联不受支持的或生命周期终止的客户端程序包。

Cisco Secure Firewall Management Center通过使用文件包名称确定操作系统的类型。如果用户重命名文件而不指示操作系统信息，则必须从列表框中选择有效的操作系统类型。

通过访问 Cisco 软件下载中心来下载 Secure Client 映像文件。

相关主题

将 安全客户端 映像添加到 Cisco Secure Firewall Management Center，第 43 页

将 安全客户端 映像添加到 Cisco Secure Firewall Management Center

您可以使用 **安全客户端文件**对象将 安全客户端 映像上传到 Cisco Secure Firewall Management Center。有关详细信息，请参阅文件对象。有关客户端映像的详细信息，请参阅思科 安全客户端 映像，第 42 页。

过程

步骤 1 选择 **设备 (Devices) > 远程访问 (Remote Access)**，选择并编辑列出的远程访问策略，然后选择**高级 (Advanced)** 选项卡。

步骤 2 点击**添加 (Add)** 以添加 安全客户端 映像。

步骤 3 在 **安全客户端映像 (Secure Client Images)** 对话框的**可用安全客户端映像 (Available Secure Client Images)**中点击**添加 (Add)**。

步骤 4 为可用的 安全客户端 映像输入**名称 (Name)** 和**说明 (Description)**（可选）。

步骤 5 点击**浏览 (Browse)**，找到想要上传的客户端映像。

步骤 6 点击**保存**以便将映像上传到 防火墙管理中心。

在将客户端映像上传到 Cisco Secure Firewall Management Center 时，会自动显示映像的操作系统信息。

步骤 7 要更改客户端映像的顺序，请点击**显示重新排序按钮 (Show Re-order buttons)**，然后向上或向下移动客户端映像。

相关主题

思科 安全客户端 映像，第 42 页

更新远程接入 VPN 客户端的 安全客户端映像

当 思科软件下载中心提供新的 安全客户端 更新时，您可以手动下载软件包并将其添加到远程接入 VPN 策略，以便根据其操作系统在 VPN 客户端系统上升级新的客户端软件包。

开始之前

此部分中的说明可帮助您更新连接 Cisco Secure Firewall Threat Defense VPN 网关的远程接入 VPN 客户端的新 安全客户端 客户端映像。更新 安全客户端 映像之前，确保完成以下配置：

- 从思科软件下载中心下载最新的 安全客户端 映像文件。
- 在 Cisco Secure Firewall Management Center Web 界面上，转至 **对象 > 对象管理 > VPN > 安全客户端文件**，然后添加新的 安全客户端 映像文件。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程访问**。

步骤 2 点击要编辑的远程访问 VPN 策略旁边的 **编辑** 。

步骤 3 点击 **高级的** > **安全客户端映像** > **添加**。

步骤 4 从 **可用的安全客户端映像** 中选择客户端图像文件，然后点击 **添加**。

如果未列出所需的客户端映像，点击 **添加** 浏览并上传映像。

步骤 5 点击**确定**。

步骤 6 保存远程访问 VPN 策略。
在部署远程访问 VPN 策略更改之后，新的 安全客户端 映像将在 Cisco Secure Firewall Threat Defense 设备上更新，该设备配置为远程接入 VPN 网关。当新的 VPN 用户连接到 VPN 网关时，用户将根据客户端系统的操作系统获取要下载的新 Secure Client 映像。对于现有 VPN 用户， Secure Client 映像将在其下一个 VPN 会话中更新。

将思科 安全客户端 外部浏览器软件包添加到 Cisco Secure Firewall Management Center

如果您的本地磁盘上有一个 安全客户端 外部浏览器软件包镜像，请使用此程序将其上传到 Cisco Secure Firewall Management Center。上传外部浏览器软件包后，您可以为远程访问 VPN 连接更新外部浏览器软件包。

您可以使用 **安全客户端文件**对象将外部浏览器软件包文件上传到 Cisco Secure Firewall Management Center。有关详细信息，请参阅文件对象。

要点回顾

- 只能向 设备添加一个外部浏览器软件包。
- 将外部浏览器软件包添加到 防火墙管理中心 后，只有在远程接入 VPN 配置中启用外部浏览器后，才会将浏览器推送到 。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备 (Devices)** > **远程访问 (Remote Access)**，选择并编辑列出的远程访问策略，然后选择**高级 (Advanced)** 选项卡。

步骤 2 点击 **安全客户端映像** 页面的 **安全客户端外部浏览器包** 部分中的 **添加** 。

步骤 3 输入 安全客户端 软件包的 **名称** 和 **说明** 。

步骤 4 点击 **浏览** 并找到要上传的外部浏览器软件包文件。

步骤 5 点击**保存**以便将映像上传到 Cisco Secure Firewall Management Center。

注释

如果要使用现有外部浏览器软件包来更新远程访问 VPN 连接，请从 **软件包文件** 下拉列表中选择该文件。

步骤 6 保存远程访问 VPN 策略。

相关主题

思科 安全客户端 映像，第 42 页

远程接入 VPN 地址分配策略

设备可以使用 IPv4 或 IPv6 策略将 IP 地址分配给远程接入 VPN 客户端。如已配置多个地址分配方法，则 设备将尝试每一个选项，直到找到一个 IP 地址为止。

IPv4 或 IPv6 策略

您可以使用 IPv4 或 IPv6 策略对远程接入 VPN 客户端的 IP 地址进行寻址。首先，您必须尝试使用 IPv4 策略，然后再尝试使用 IPv6 策略。

- **使用授权服务器**- 在每个用户的基础上从外部授权服务器检索地址。如果使用已配置 IP 地址的授权服务器，建议使用此方法。只有基于 RADIUS 的授权服务器支持地址分配。AD/LDAP 则不支持。此方法适用于 IPv4 和 IPv6 分配策略。
- **使用 DHCP** - 从在连接配置文件中配置的 DHCP 服务器获取 IP 地址。您还可以通过在组策略中配置 DHCP 网络范围来定义 DHCP 服务器可以使用的 IP 地址的范围。如果使用 DHCP，则在**对象 > 对象管理 > 网络**窗格中配置服务器。此方法适用于 IPv4 分配策略。

  有关 DHCP 网络范围配置的详细信息，请参阅组策略常规选项。
- **使用内部地址池** - 内部配置的地址池是分配地址池以进行配置的最简单方法。如果使用此方法，请在**对象 > 对象管理 > 地址池**窗格中创建 IP 地址池，并在连接配置文件中做出相同的选择。此方法适用于 IPv4 和 IPv6 分配策略。
- **允许释放 IP 地址一段时间之后对其重新使用** - 在 IP 地址返回到地址池之后，延迟一段时间方可重新使用。增加延迟有助于防止防火墙在快速重新分配 IP 地址时遇到的问题。默认情况下，延迟设置为零。如果要延长延迟，请输入取值范围为 0 至 480 内的分钟数，以便延迟 IP 地址重新分配。此配置元素适用于 IPv4 分配策略。

相关主题

配置连接配置文件设置，第 22 页
远程访问 VPN 身份验证，第 4 页

配置证书映射

通过证书映射，您可以根据证书的字段内容定义匹配连接配置文件的用户证书的规则。证书映射提供安全网关上的证书身份验证。

规则或证书映射在证书映射对象中定义。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 在列表中选择现有的远程访问策略，然后点击相应的**编辑**图标。

步骤 3 选择 **高级** > **证书映射**。

步骤 4 从 **连接配置文件映射的常规设置** 窗格中选择以下选项：

选择是基于优先级的，如果没有找到第一个选择的匹配项，则继续向下匹配列表中的选项。当满足规则时，匹配完成。如果不满足规则，则使用默认的连接配置文件（在底部列出）用于此连接。选择以下任意选项或所有选项，以建立身份验证并确定应映射到客户端的连接配置文件（隧道组）。

- **如果组 URL 和证书映射匹配不同的连接配置文件，则使用组 URL**。
- **使用配置的规则将证书匹配到连接配置文件**-启用此功能可以使用连接配置文件映射中定义的规则。

注释
配置证书映射意味着采用基于证书的身份验证方法。系统将提示远程用户输入客户端证书，而不考虑配置的身份验证方法。

步骤 5 在**证书到连接配置文件映射 (Certificate to Connection Profile Mapping)** 部分下，点击**添加映射 (Add Mapping)**，以便为此策略创建证书到连接配置文件的映射。

a) 选择或创建 **证书映射名称** 对象。
b) 选择当满足证书映射对象中的规则时想要使用的 **连接配置文件** 。
c) 点击**确定 (OK)** 以创建映射。

步骤 6 点击**保存**。

配置组策略

组策略是存储在组策略对象中的一组属性和值对，用于定义远程访问VPN体验。例如，在组策略对象中，可以配置地址、协议和连接设置等常规属性。

在建立VPN隧道时，将确定应用于用户的组策略。RADIUS授权服务器将会分配组策略，或从当前连接配置文件中获取。

注释 上没有任何组策略继承属性。对于用户使用完整的组策略对象。使用登录时AAA服务器识别的组策略对象；如果未指定组策略对象，则使用为VPN连接配置的默认组策略。提供的默认组策略可以设置为默认值，但仅在将该策略分配给连接配置文件且用户未识别其他组策略时使用该策略。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 在列表中选择现有的远程访问策略，然后点击相应的**编辑**图标。

步骤 3 选择**高级 (Advanced)** > **组策略 (Group Policies)** > **添加 (Add)**。

步骤 4 从**可用组策略 (Available Group Policy)** 列表中选择组策略并点击**添加 (Add)**。您可以选择与此远程访问 VPN 策略关联的一个或多个组策略。

步骤 5 点击**确定 (OK)** 以完成组策略选择。

步骤 6 保存更改。

相关主题

配置组策略对象

配置 LDAP 属性映射

LDAP 属性名称将 LDAP 用户或组属性名称映射到 Cisco 可理解的名称。属性映射将 Active Directory（AD）或 LDAP 服务器中存在的属性与 Cisco 属性名称等同起来。您可以将任何标准 LDAP 属性映射到公认的供应商特定属性 (VSA)。您可以将一个或多个 LDAP 属性映射到一个或多个 Cisco LDAP 属性。当 AD 或 LDAP 服务器在远程访问 VPN 连接建立期间向 设备返回身份验证时， 设备可以使用该信息调整 Secure Client 如何完成连接。

当您想要为 VPN 用户提供不同的访问权限或 VPN 内容时，您可以在 VPN 服务器上配置不同的 VPN 策略，并根据其凭证将这些策略集分配给每个用户。您可以在 中通过使用 LDAP 属性映射配置 LDAP 授权来实现此目的。要使用 LDAP 将组策略分配给用户，您必须配置映射 LDAP 属性的映射。

LDAP 属性映射包括三个组件：

- **领域** - 指定 LDAP 属性映射的名称；名称根据所选领域生成。
- **属性名称映射 (Attribute Name Map)** - 将 LDAP 用户或组属性名称映射到 Cisco 可理解的名称。
- **属性值映射 (Attribute Value Map)** - 将 LDAP 用户或组属性中的值映射到所选名称映射的 Cisco 属性值.

LDAP 属性映射中使用的组策略将被添加到远程访问 VPN 配置中的组策略列表。从远程访问 VPN 配置中删除组策略也会删除相关的 LDAP 属性映射。

在版本 6.4 到 6.6 中，只能使用 FlexConfig 配置 LDAP 属性映射。有关详细信息，请参阅 使用 FlexConfig 配置 AnyConnect 模块和配置文件。

在 7.0 及更高版本中，可以使用以下程序：

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 在列表中选择现有的远程访问策略，然后点击相应的**编辑**图标。

步骤 3 点击 **高级** > **LDAP 属性映射**。

步骤 4 点击**添加 (Add)**。

步骤 5 在配置 LDAP 属性映射页面上，选择要配置属性映射的 **领域** 。

步骤 6 点击**添加 (Add)**。

您可以配置多个属性映射。每个属性映射都要求您配置名称映射和值映射。

注释

确保在创建 LDAP 属性映射时遵循以下准则：

- 为 LDAP 属性至少配置一个映射；不允许多个具有相同 LDAP 属性名称的映射。
- 配置至少一个名称映射以创建 LDAP 属性映射。
- 如果属性映射未与远程访问 VPN 配置中的任何连接配置文件关联，您可以删除任何 LDAP 属性映射。
- 对 与 Cisco 和 LDAP 属性名称和值使用 LDAP 属性映射中的正确拼写和大写。

a) 指定 **LDAP 属性名称** ，然后从列表中选择所需的 **Cisco 属性名称** 。

b) 点击 **添加值映射** 并指定 **LDAP 属性值** 和 **Cisco 属性值**。

重复此步骤以添加更多值映射。

步骤 7 点击**确定 (OK)** 以完成 LDAP 属性映射配置。

步骤 8 点击 **保存** 以保存对 LDAP 属性映射的更改。

示例

有关详细示例，请参阅 为 FTD 配置具有 LDAP 身份验证和授权的 RA VPN。

相关主题

配置远程访问 VPN 的 AAA 设置 ， 第 24 页
了解权限和属性的策略实施 ， 第 6 页

配置 VPN 负载均衡

关于 VPN 负载均衡

中的 VPN 负载均衡允许您对两台或更多设备进行逻辑分组，并在设备之间平均分配远程接入 VPN 会话。VPN 负载均衡会在负载均衡组中的设备之间共享 Secure Client VPN 会话。

VPN 负载均衡基于简单的流量分配，而不考虑吞吐量或其他因素。VPN 负载均衡组由两台或更多设备组成。一台设备充当导向器，而其他设备是成员设备。组中的设备不需要是完全相同的类型，也不需要具有相同的软件版本和配置。支持远程接入 VPN 的任何 设备都可以加入负载均衡组。 支持使用 AnyConnect 安全客户端 SAML 身份验证进行 VPN 负载均衡。

VPN 负载均衡组中的所有主用设备都会承载会话负载。VPN 负载均衡可以将流量定向至组中负载最低的设备，在所有设备之间分配负载。这样可以高效地利用系统资源，提供更高的性能和高可用性。

VPN 负载均衡的组件

以下是 VPN 负载均衡的组件：

- **负载均衡组 (Load-balancing group)** - 由两台或多台 设备组成的虚拟组，用于共享 VPN 会话。

  VPN 负载均衡组可以包含相同版本或混合版本的 设备；但设备必须要支持远程接入 VPN 配置。

  请参阅配置 VPN 负载均衡的组设置，第 50 页和配置负载均衡的其他设置，第 51 页。

- **导向器 (Director)** - 由组中的一个设备充当导向器。它会在组中的其他成员之间分配负载，并参与为 VPN 会话提供服务。

  导向器会监控组中的所有设备、追踪每台设备的负载情况，然后相应地分配会话负载。导向器的角色不会与某台物理设备绑定；它可以在设备之间切换。例如，如果当前的导向器发生故障，该组的一台成员设备会接管该角色，立即成为新的导向器。

- **成员 (Members)** - 组中除导向器以外的设备均被称为成员。它们会参与负载均衡并共享远程接入 VPN 连接。

  配置参与设备的设置，第 51 页。

VPN 负载均衡的前提条件

- **证书 (Certificates)** - 的证书必须包含连接重定向到的导向器和成员的 IP 地址或 FQDN。否则，证书将被视为不可信。证书必须使用使用者替代名称 (SAN) 或通配符证书
- **组 URL (Group URL)** - 在连接配置文件中添加 VPN 负载均衡组 IP 地址的组 URL。指定组 URL，以便用户在登录时无需再选择组。
- **IP 地址池 (IP Address Pool)** - 为成员设备选择唯一的 IP 地址池，并覆盖 防火墙管理中心 中每个成员设备的 IP 池。
- 网络地址转换 (NAT) 后面的设备也可以作为负载均衡组的一部分。

VPN 负载均衡准则和限制

- 默认情况下会禁用 VPN 负载均衡。您必须显式启用 VPN 负载均衡。
- 只有协同定位的 设备才能被添加到负载均衡组中。
- 一个负载均衡组必须至少有两台 设备。
- 高可用性的设备可以加入负载均衡组。
- 网络地址转换 (NAT) 后面的设备也可以作为负载均衡组的一部分。
- 当成员或导向器设备发生故障时，该设备提供的远程接入VPN连接会被丢弃。您必须再次启动 VPN 连接。
- 每台设备上的身份证书必须具有使用者替代名称 (SAN) 或通配符。

配置 VPN 负载均衡的组设置

您可以启用VPN负载均衡，并配置适用于负载均衡组所有成员的组设置。在创建组时，您可以配置负载均衡的参与设置。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 点击要编辑的远程访问 VPN 策略旁边的 **编辑** 。

步骤 3 点击**高级 (Advanced)** > **负载均衡 (Load Balancing)**。

步骤 4 点击**启用成员设备之间的负载均衡 (Enable Load balancing between member devices)** 切换按钮以启用负载均衡。
系统将打开 **编辑组配置** 页面。组参数适用于负载均衡组下的所有设备。

步骤 5 如果适用，请指定 **组 IPv4 地址** 和 **组 IPv6 地址** 。

此处指定的 IP 地址用于整个负载均衡组，而导向器将为传入 VPN 连接打开此 IP 地址。

步骤 6 为负载均衡组选择 **通信接口** 。点击 **添加** 以添加接口组或安全区域。

通信接口是一个专用接口，导向器和成员都会通过该接口共享有关其负载的信息。

步骤 7 输入用于在组中的导向器和成员之间进行通信的 **UDP 端口** 。默认端口为 9023。

步骤 8 启用 **IPsec 加密** 切换按钮，为导向器和成员之间的通信激活 IPsec 加密。

启用加密后会使用预共享密钥在导向器和成员之间建立 IPsec 隧道。

当您在启用了 **IPsec 加密 (IPsec Encryption)** 选项的情况下升级或降级 设备时，请确保 防火墙管理中心 和 之间的配置没有不匹配，以防部署失败。

步骤 9 输入用于 IPsec 加密的 **加密密钥** 。

步骤 10 点击**确定**。

配置负载均衡的其他设置

VPN 负载均衡的其他设置包括 FQDN 和 IKEv2 重定向。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 点击要编辑的远程访问 VPN 策略旁边的 **编辑** 。

步骤 3 点击**高级 (Advanced)** > **负载均衡 (Load Balancing)**。

步骤 4 如果已经完成，打开 **启用成员设备之间的负载均衡** 切换按钮以启用负载均衡。

步骤 5 点击**设置**。

步骤 6 打开 **将 FQDN 发送到对等设备而不是 IP** 切换按钮以启用使用完全限定域名的重定向。

默认情况下， 只会将 VPN 负载均衡重定向中的 IP 地址发给客户端。

步骤 7 选择 **IKEv2 重定向** 阶段之一：

- **在 SA 身份验证期间重定向**
- **在 SA 初始化期间重定向**

步骤 8 点击**确定**。

步骤 9 保存更改。

配置参与设备的设置

设备参与设置将确定设备如何在 VPN 负载均衡中共享负载。在设备上启用 VPN 负载均衡，并定义设备特定属性，从而配置参与设备。这些值因设备而异。您可以为参与负载均衡的设备提供优先级编号。优先级越高，设备就越有可能成为导向器，而不是其他设备。但您不能选择某个设备作为该组的导向器。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 点击要编辑的远程接入 VPN 策略旁边的 **编辑** 。

步骤 3 点击**高级 (Advanced)** > **负载均衡 (Load Balancing)**。

步骤 4 如果尚未启用负载均衡，打开 **启用成员设备之间的负载均衡** 切换按钮以启用负载均衡。

步骤 5 配置**设备参与 (Device Participation)** 设置：

设备参与 部分列出了所选远程访问 VPN 配置的目标设备。可以配置这些设备，为分担传入 VPN 会话的负载。

a) 打开 **负载均衡** 切换按钮，为设备启用负载均衡，然后点击 **编辑**。

b) 输入设备**优先级**。

默认情况下，设备优先级会被设为 5。您可以从 1 到 10 中选择一个数字。

c) 如果设备位于 NAT 之后，请为 VPN 接口 IP 地址指定 **IPv4 NAT** 或 **IPv6 NAT** 地址。

d) 点击**确定**。

步骤 6 点击**保存**以保存远程访问 VPN 策略设置。

配置远程接入 VPN 的 IPsec 设置

只有在配置远程接入 VPN 策略时选择 IPsec 作为 VPN 协议时，IPsec 设置才适用。否则，可以使用“编辑访问接口”对话框启用 IKEv2。有关详细信息，请参阅配置远程访问 VPN 的访问接口，第 40 页。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 从可用 VPN 策略列表中，选择要修改其设置的策略。

步骤 3 点击 **Advanced**。

IPsec 设置列表将显示在屏幕左侧的导航窗格中。

步骤 4 使用导航窗格编辑下列 IPsec 选项：

a) **加密映射** -“加密映射”页面列出了在其上启用了 IKEv2 协议的接口组。启用 IKEv2 协议的接口将自动生成加密映射。要编辑加密映射，请参阅配置远程接入 VPN 加密映射，第 52 页。可在**访问接口 (Access Interface)** 中，为选定的 VPN 策略添加或删除接口组。有关详细信息，请参阅配置远程访问 VPN 的访问接口，第 40 页。

b) **IKE 策略** - 当 安全客户端 终端使用 IPsec 协议进行连接时，“IKE 策略”页面将列出适用于所选 VPN 策略的所有 IKE 策略对象。有关详细信息，请参阅 远程接入 VPN 中的 IKE 策略，第 54 页。要添加新的 IKE 策略，请参阅 配置 IKEv2 策略对象。 仅支持 安全客户端 IKEv2 客户端。不支持第三方标准 IKEv2 客户端。

c) **IPsec/IKEv2 参数** -“IPsec/IKEv2 参数”页面使您可以修改 IKEv2 会话设置、IKEv2 安全关联设置、IPsec 设置和 NAT 透明度设置。有关详细信息，请参阅配置远程访问 VPN IPsec/IKEv2 参数，第 56 页。

步骤 5 点击**保存**。

配置远程接入 VPN 加密映射

对于已启用 IPsec-IKEv2 协议的接口，将自动生成加密映射。可在**访问接口 (Access Interface)** 中，为选定的 VPN 策略添加或删除接口组。有关详细信息，请参阅配置远程访问 VPN 的访问接口，第 40 页。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 从可用 VPN 策略列表中，选择要修改其设置的策略。

步骤 3 点击**高级 (Advanced)** > **加密映射 (Crypto Maps)**，选择表中的一行并点击**编辑 (Edit)** 以编辑加密映射选项。

步骤 4 选择 **IKEv2 IPsec 提议 (IKEv2 IPsec Proposals)** 并选择对指定将使用哪些身份验证和加密算法来保护隧道中的流量安全的集合进行转换。

步骤 5 选择**启用反向路由注入 (Enable Reverse Route Injection)** 以启用静态路由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。

步骤 6 选择**启用客户端服务 (Enable Client Services)** 并指定端口号。

客户端服务服务器提供 HTTPS (SSL) 访问，以允许 安全客户端下载程序接收软件升级、配置文件、本地化和自定义文档、CSD、SCEP 以及客户端所需的其他文件下载。如果选择此选项，请指定客户端服务端口号。如果不启用客户端服务服务器，用户将无法下载 安全客户端可能需要的任何文件。

注释
您可以使用与在同一设备上运行的 SSL VPN 相同的端口。即使配置了 SSL VPN，您也必须选择此选项，以便通过 SSL 为 IPsec-IKEv2 客户端启用文件下载。

步骤 7 选择**启用完全向前保密 (Enable Perfect Forward Secrecy)**，然后选择**模数组 (Modulus group)**。

使用完美前向保密 (PFS) 为每个加密交换生成和使用唯一会话密钥。唯一会话密钥可保护交换免于后续解密，即使整个交换已被记录且攻击者已经获得终端设备使用的预共享或私有密钥。如果选择此选项，也请选择在**模数组 (Modulus Group)** 列表中生成 PFS 会话密钥时使用的 Diffie-Hellman 密钥导出算法。

模数组是用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数越大，安全性越高，但需要的处理时间更长。两个对等体必须具有匹配的模数组。选择要在远程接入 VPN 配置中允许的模数组。

- 1 - Diffie-Hellman 组 1（768 位模数）。
- 2 - Diffie-Hellman 组 2（1024 位模数）。
- 5 - Diffie-Hellman 组 5（1536 位模数，可为 128 为密钥提供较好的保护，但组 14 更好）。如果使用的是 AES 加密，请使用此组（或更高的组）。
- 14 - Diffie-Hellman 组 14（2048 位模数，可为 128 为密钥提供较好的保护）。
- 19 - Diffie-Hellman 组 19（256 位椭圆曲线字段大小）。
- 20 - Diffie-Hellman 组 20（384 位椭圆曲线字段大小）。
- 21 - Diffie-Hellman 组 21（521 位椭圆曲线字段大小）。
- 24 - Diffie-Hellman 组 24（2048 位模数和 256 位素数阶子组）。

步骤 8 指定**生命周期持续时间（秒）(Lifetime Duration [seconds])**。

安全关联 (SA) 的生命周期（以秒为单位）。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，持续期限越短（某种程度上），IKE 协商就越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。

可指定 120 到 2147483647 秒之间的值。默认值为 28800 秒。

步骤 9 指定**生命周期大小（千字节）(Lifetime Size [kbytes])**。

使用特定安全关联的 Ipsec 对等体之间在该安全关联到期前可通过的流量（以千字节为单位）。

可指定 10 到 2147483647 千字节之间的值。默认值为 4,608,000 千字节。没有规范允许使用无限数据。

步骤 10 选择以下 **ESPv3 设置 (ESPv3 Settings)**：

- **验证传入 ICMP 错误消息 (Validate incoming ICMP error messages)** - 选择是否验证通过 IPsec 隧道接收，并发往专用网络上的内部主机的 ICMP 错误消息。
- **启用“不分段”策略 (Enable 'Do Not Fragment' Policy)** - 定义 IPsec 子系统如何处理大型数据包，这些数据包在 IP 报头中设置了不分片 (DF) 位，然后从**策略 (Policy)** 列表选择以下一项。
  - 复制 - 维护 DF 位。
  - 清除 - 忽略 DF 位。
  - 设置 - 设置和使用 DF 位。
- 选择**启用数据流机密性 (TFC) 数据包 (Enable Traffic Flow Confidentiality [TFC] Packets)** - 启用虚拟 TFC 数据包，这些数据包会通过隧道，用于屏蔽流量配置文件。可以使用 **Burst**、**Payload Size** 和 **Timeout** 参数生成穿过指定 SA 的随机长度的数据包。

  注释
  启用流量保密性 (TFC) 数据包可防止 VPN 隧道处于空闲状态。因此，如果启用了 TFC 数据包，则组策略中配置的 VPN 空闲超时不会按预期工作。请参阅组策略高级选项。

  - 突发 - 指定 1 到 16 字节之间的值。
  - 负载大小 - 指定 64 到 1024 字节之间的值。
  - 超时 - 指定 10 到 60 秒之间的值。

步骤 11 点击**确定**。

相关主题

接口

远程接入 VPN 中的 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之

间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

注释 仅支持将 IKEv2 用于远程接入 VPN。

与 IKEv1 不同，在 IKEv2 方案中，您可以在一个策略中选择多个算法和模数组。由于对等体在第 1 阶段协商期间进行选择，因此可创建单个 IKE 方案，但是考虑创建多个不同的方案，以向最需要的方案提供更高的优先级。对于 IKEv2，策略对象不指定身份验证，其他策略必须定义身份验证要求。

当配置远程接入 IPsec VPN 时，需要 IKE 策略。

配置远程接入 *VPN IKE* 策略

IKE 策略表指定，当 安全客户端端点使用 IPsec 协议进行连接时适用于所选 VPN 配置的所有 IKE 策略对象。有关详细信息，请参阅远程接入 VPN 中的 IKE 策略，第 54 页。

注释 仅支持用于远程接入 VPN 的 IKEv2。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 从可用 VPN 策略列表中，选择要修改其设置的策略。

步骤 3 点击**高级 (Advanced)** > **IKE 策略 (IKE Policy)**。

步骤 4 点击**添加 (Add)** 从可用的 IKEv2 策略中选择，或添加新的 IKEv2 策略并指定以下选项：

- **名称 (Name)** - IKEv2 策略的名称。
- **说明 (Description)** - IKEv2 策略的可选说明
- **优先级** — 当尝试查找常见安全关联 (SA) 时，优先级值可确定两个协商对等体比较的 IKE 策略顺序。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）
- **完整性 (Integrity)** - IKE 策略中使用的散列算法的完整性算法部分。
- **加密 (Encryption)** - 用于建立第 1 阶段 SA（用于保护第 2 阶段协商）的加密算法。
- **PRF 散列 (PRF Hash)** - IKE 策略中使用的散列算法的伪随机函数 (PRF) 部分。在 IKEv2 中，您可以为这些元素指定不同的算法。
- **DH 组 (DH Group)** - 用于加密的 Diffie-Hellman 组。

步骤 5 点击保存。

配置远程访问 VPN IPsec/IKEv2 参数

过程

步骤 1 选择设备 > **VPN** > 远程访问。

步骤 2 从可用 VPN 策略列表中，选择要修改其设置的策略。

步骤 3 点击 高级 **(Advanced)** > **IPsec**> **IPsec/IKEv2 参数 (IPsec/IKEv2 Parameters)**。

步骤 4 为 **IKEv2 会话设置**选择以下选项：

- **发送至对等体的身份**-选择对等体将在 IKE 协商期间用于标识自身的身份：
  - **自动**-按连接类型确定 IKE 协商：用于预共享密钥的 IP 地址或用于证书身份验证的证书 DN（不受支持）。
  - **IP 地址**-使用交换 ISAKMP 身份信息的主机的 IP 地址。
  - **主机名称**-使用交换 ISAKMP 身份信息的主机的完全限定域名 (FQDN)。此名称包含主机名和域名。
- **在断联隧道上启用通知**-当 SA 上接收的入站数据包与该 SA 的流量选择器不匹配时，允许管理员启用或禁用向对等体发送 IKE 通知。默认情况下会禁用发送此通知。
- **请勿允许设备重新引导直至所有会话被终止**-选中以支持等待所有活动在系统重启之前自动终止。默认情况下将禁用此复选框。

步骤 5 为 **IKEv2 安全关联 (SA) 设置**选择以下选项：

- **Cookie 质询**-是否向对等体设备发送 Cookie 质询，以响应 SA 发起的数据包，这可以帮助阻止拒绝服务 (DoS) 攻击。默认情况下，当 50% 的可用 SA 正在协商时使用 Cookie 质询。选择以下选项之一：
  - **自定义**-指定 **向质询传入 Cookie 发出挑战的阈值**，这是指允许进行协商的总 SA 数的百分比。这将对未来的任何 SA 协商都触发 Cookie 质询。范围为 0 到 100%。默认为 50%。
  - 始终-始终选择向对等设备发送 cookie 质询。
  - 从不-选择从不向对等设备发送 cookie 质询。
- **允许协商的 SA 数量**-限制可以随时协商的 SA 的最大数量。如果与 Cookie 质询配合使用，可以配置低于此限制的 Cookie 质询阈值，以便实现有效的交叉检查。默认为 100%。
- **允许的最大 SA 数量**-限制 ASA 上允许的 IKEv2 连接的数量。

步骤 6 为 **IPsec 设置**选择以下选项：

- **解密前启用分片**-此选项允许流量通过不支持 IP 分片的 NAT 设备。这不影响支持 IP 分片的 NAT 设备的运行。
- **路径最大传输单元老化**-选中以启用 PMTU（路径最大传输单元）老化，设置 SA（安全关联）的 PMTU 的间隔。
- **值重置间隔**-输入 SA（安全关联）的 PMTU 值重置为其原始值的分钟数。有效范围是 10 到 30 分钟，默认值为不受限制。

步骤 7 为 **NAT 设置**选择以下选项：

- **保持连接消息穿越** - 选择是否启用 NAT 保持连接消息穿越。NAT 遍历保持连接用于在 VPN 连接的中心和分支之间存在设备（中间设备）并且该设备对 IPsec 流执行 NAT 时，传输保持连接消息时。如果选择此选项，请配置在分支和中间设备之间发送的保持连接信号之间的间隔（以秒为单位），以指示会话处于活动状态。此值可以介于 10 到 3600 秒之间。默认值为 20 秒。
- **间隔**-设置 NAT 保持连接间隔，范围从 10 秒到 3600 秒。默认值为 20 秒。

步骤 8 点击**保存**。

自定义 Cisco Secure Client

您可以使用管理中心配置安全客户端自定义，并将其部署到 VPN 头端。当用户从安全客户端连接时，威胁防御设备会将这些自定义分发到终端。管理员可以在终端上自定义以下元素：

表 *5:* 管理中心中可用的安全客户端自定义

可以定制	说明	更多信息
GUI 文本和消息	自定义或本地化安全客户端 GUI 文本和信息/错误消息。	自定义和本地化安全客户端 GUI 文本和消息，第 59 页
图标和图像	自定义 Secure Client GUI 的徽标、图像或图标。	自定义安全客户端图标和图像，第 60 页
脚本	当客户端建立或断开 VPN 会话时，在终端设备上部署脚本。	使用安全客户端在终端设备上部署脚本，第 61 页
二进制文件	使用安全客户端 API 部署自定义应用。	使用思科安全客户端 API 部署自定义应用，第 63 页
自定义安装程序转换	自定义安全客户端安装程序。	自定义安全客户端安装程序，第 64 页
本地化安装程序转换	本地化客户端安装程序。	本地化客户端安装程序，第 64 页

安全客户端自定义的准则和限制

一般限制

- 如果使用 CLI 在威胁防御上直接配置了早于 7.4 的任何自定义设置，则管理中心会在部署期间删除这些自定义设置。
- 无集群支持。

表 *6:* 安全客户端自定义的限制

可以定制	限制

GUI 文本和消息自定义	• 在使用此自定义之前，必须重新启动安全客户端。
	• 不支持从右到左的语言。
	• 由于硬编码字段的长度要求，有些字符串在 GUI 中会截断。
	• 某些消息在客户端中进行了硬编码。例如：
	  • 状态消息（更新期间）
	  • 不受信任的服务器消息。
	  • 延期更新消息
	• 本地化是特定于版本的。
	如果管理员基于旧版安全客户端的模板创建了转换表，则新消息不会向远程用户显示。管理员必须将最新的模板与转换表合并，以便该表包含新邮件。您可以使用 Get text 等第三方工具执行合并。

图标和图像自定义	• 在使用此自定义之前，必须重新启动安全客户端。 • 自定义对象名称必须与安全客户端 GUI 文件名匹配。每个操作系统的文件名都不同，并且区分大小写。有关每个操作系统的文件名、扩展名和大小的详细信息，请参阅 思科安全客户端管理员指南。 • 如果图像大小不正确，则图像无法正确显示。管理中心或威胁防御设备不验证映像大小。 • MacOS 不支持自定义安全客户端图像和图标。
部署自定义脚本	• 安全客户端只运行一个 OnConnect 和一个 OnDisconnect 脚本；然而，这些脚本可能会启动其他脚本。 • 脚本只能执行用户有权调用的功能。 • 您无法从登录前启动 (SBL) GUI 启动 OnConnect 脚本。

可以定制	限制
使用 Cisco 安全客户端 API（二进制）部署自定义应用	• 使用此自定义后，如果在管理中心部署更新版本的安全客户端，客户端将下载更新并替换您的自定义 UI。
自定义客户端安装程序	• 此自定义仅适用于 Windows。

自定义和本地化安全客户端 GUI 文本和消息

您可以自定义安全客户端 GUI 文本和信息/错误消息。您还可以自定义以首选语言显示的 GUI 文本和所有消息。

自定义 GUI 文本和消息

要自定义 GUI 文本或消息，可以编辑消息文件中的消息。您可以更新消息，以在错误消息中包含更多详细信息。例如：

- 修改登录对话框中的任何标签，例如将 **密码** 修改为 **域密码**。
- 在错误消息中添加您的支持联系人详细信息。

本地化 GUI 文本和消息

威胁防御设备使用转换表来转换安全客户端中显示的标签和用户消息。当用户连接到远程接入 VPN 时，安全客户端会识别终端上设置的区域设置并下载转换文件。威胁防御设备支持 128 种区域设置。默认情况下，安全客户端以英语安装。

- 对于思科安全客户端 5.0，各种语言的默认本地化文件是应用的一部分。
- 对于 AnyConnect 客户端 4.x，您可以从 Cisco.com 下载几种语言的本地化文件，并将其上传到管理中心。

如何自定义安全客户端 *GUI* 文本和消息

开始之前

配置一个或多个远程访问 VPN IKE 策略。

过程

步骤 1 从安全客户端软件包或 Cisco.com 获取基本模板或转换文件。例如，AnyConnect.po。

步骤 2 使用文本编辑器添加翻译或自定义标签或消息。

步骤 3 更新与每个 **msgid** 对应的 **msgstr** 字符串。

步骤 4 保存文件。

步骤 5 创建新的安全客户端自定义对象。

a) 依次选择 **对象 > 对象管理 > VPN > 安全客户端自定义**。
b) 点击 **安全客户端自定义**。
c) 输入自定义的名称和说明。
d) 从 **自定义类型** 下拉列表中，选择 **GUI 文本和消息**。
e) 从 **语言** 下拉列表中，选择要为其添加翻译的语言。
f) 点击 **浏览** 并选择翻译文件。支持的文件扩展名包括 .po、.mo 和 .txt。

步骤 6 将自定义添加到远程接入 VPN 策略。

a) 选择 **设备 > 远程访问**。
b) 点击远程接入 VPN 策略的编辑图标。
c) 点击 **高级 > 安全客户端自定义 > 本地化**。
d) 点击 **+** 选择转换文件。
e) 点击 **添加 (Add)**。
f) 点击**确定**。

步骤 7 点击**保存**。

步骤 8 选择 **部署 > 部署** 并将策略部署到所分配的设备。在部署更改之后，更改才生效。

下一步做什么

验证安全客户端自定义。有关详细信息，请参阅验证安全客户端自定义，第 65 页。

自定义安全客户端图标和图像

您可以使用管理中心自定义 Secure Client GUI 的徽标、图像和图标。

要自定义 Secure Client GUI 的徽标、图像和图标，必须在管理中心创建 Secure Client 自定义对象。此自定义对象的名称必须与安全客户端 GUI 文件名匹配。每个操作系统的文件名都不同，并且区分大小写。有关每个操作系统的文件名、扩展名和大小的详细信息，请参阅 思科安全客户端管理员指南。

例如，如果要替换 Windows 客户端的公司徽标，则必须创建名称为 company_logo 的自定义对象，并将此自定义对象添加到远程接入VPN策略。如果为自定义对象使用不同的名称，则安全客户端安装程序不会更改组件。但是，如果部署自己的可执行文件来自定义 GUI，则自定义对象可以具有任何名称。

所有映像文件的位置：

- Windows: **%PROGRAMFILES%\Cisco\Cisco Secure Client\res**
- Linux: **/opt/cisco/secure client/pixmaps**
- macOS：不支持

如何自定义安全客户端映像和图标

开始之前

配置一个或多个远程访问 VPN IKE 策略。

过程

步骤 1 使用正确的扩展名和大小创建图标或图像。

如果图像大小不正确，则图像无法正确显示。管理中心或威胁防御设备不验证映像大小。

有关文件名、扩展名和大小的详细信息，请参阅 思科安全客户端管理员指南。

步骤 2 创建新的安全客户端自定义对象。

a) 依次选择 **对象 > 对象管理 > VPN > 安全客户端自定义**。
b) 点击 **安全客户端自定义**。
c) 输入自定义对象的名称和说明。

确保自定义对象名称与安全客户端 GUI 文件名匹配。有关文件名的详细信息，请参阅 思科安全客户端管理员指南。

d) 从 **自定义类型** 下拉列表中，选择 **图标和图像**。
e) 从 **平台** 下拉列表中选择平台。
f) 点击 **浏览** 并选择文件。支持的文件扩展名包括 .png、.ico 和 .jpeg。
g) 重复步骤 2a - f 以添加多个图标和图像。

步骤 3 将自定义对象添加到远程接入 VPN 策略。

a) 选择 **设备 > 远程访问**。
b) 点击远程接入 VPN 策略的编辑图标。
c) 点击 **高级 > 安全客户端自定义 > 图标和图像**。
d) 点击 + 以选择文件。
e) 点击 **添加 (Add)**。
f) 点击**确定**。

步骤 4 点击**保存**。

步骤 5 选择 **部署 > 部署** 并将策略部署到所分配的设备。在部署更改之后，更改才生效。

下一步做什么

验证安全客户端自定义。有关详细信息，请参阅验证安全客户端自定义 ， 第 65 页。

使用安全客户端在终端设备上部署脚本

发生以下事件时，您可以通过安全客户端下载和运行脚本：

- 使用威胁防御建立新的客户端 VPN 会话。此事件触发的脚本是 OnConnect 脚本，因为该脚本需要此文件名前缀。重新连接 VPN 会话不会触发此脚本。
- 使用威胁防御断开客户端 VPN 会话。此事件触发的脚本是 OnDisconnect 脚本，因为该脚本需要此文件名前缀。

这些脚本异步运行，不会延迟连接建立或断开连接。它们可以是任何扩展名，并且必须在终端上可执行。安全客户端通过文件名识别 OnConnect 脚本和 onDisconnect 脚本。它查找名称以 OnConnect 或 OnDisconnect 开头的文件，并忽略文件扩展名。

此功能的一些示例如下：

- VPN 连接后刷新组策略。
- 在 VPN 连接上安装网络驱动器。
- 在 VPN 断开连接时卸载网络驱动器。

要启用脚本，请在 VPN 配置文件上选中 **启用脚本** 选项 。默认情况下，客户端不会启动脚本。客户端不要求以特定语言编写脚本。它需要在客户端计算机上安装可以运行脚本的应用。为了保证客户端可以启动脚本，脚本必须从命令行运行。

只有在用户登录并建立 VPN 会话后，安全客户端才能启动脚本。您无法从登录前启动 (SBL) GUI 启动 OnConnect 脚本。您必须在 VPN 配置文件上选中 **启用 Post SBL On Connect 脚本** 选项，才能在用户登录后触发脚本。安全客户端是 32 位应用。在 64 位 Windows 版本中运行脚本时，AnyConnect 将使用 cmd.exe 的 32 位版本。

如何为安全客户端添加自定义脚本

开始之前

1. 配置远程接入 VPN。
2. 在 VPN 配置文件中启用脚本。
3. 将 VPN 配置文件添加到远程访问 VPN 组策略。

过程

步骤 1 为平台创建 OnConnect 和 OnDisconnect 脚本。

步骤 2 创建新的安全客户端自定义对象。

a) 依次选择 **对象 > 对象管理 > VPN > 安全客户端自定义**。
b) 点击 **安全客户端自定义**。
c) 输入自定义的名称和说明。
d) 从 **自定义类型** 下拉列表中，选择 **脚本**。
e) 从 **平台** 下拉列表中选择平台。
f) 选择以下一个选项：

- **On Connect**：选择 OnConnect 脚本。
- **On Disconnect**：选择 OnDisconnect 脚本。

g) 点击 **浏览** 并选择要在终端上执行的脚本。

步骤 3 将自定义添加到远程接入 VPN 策略。

a) 选择 **设备 > 远程访问**。
b) 点击远程接入 VPN 策略的编辑图标。
c) 点击 **高级 > 安全客户端自定义 > 本地化**。
d) 点击 **+** 选择转换文件。
e) 点击 **添加 (Add)**。
f) 点击**确定**。

步骤 4 点击**保存**。

步骤 5 选择 **部署 > 部署** 并将策略部署到所分配的设备。在部署更改之后，更改才生效。

下一步做什么

验证安全客户端自定义。有关详细信息，请参阅验证安全客户端自定义，第 65 页。

使用思科安全客户端 API 部署自定义应用

对于 Windows、Linux 或 MacOs 计算机，您可以创建和部署使用安全客户端 API 的自定义客户端。您可以使用此客户端二进制文件替换安全客户端 GUI 或 CLI 二进制文件。

可执行文件能够调用您导入管理中心的任何资源文件，例如徽标图像。部署自己的可执行文件时，您可以对资源文件使用任意文件名。

下表列出了不同操作系统的客户端可执行文件的文件名：

表 7: 安全客户端可执行文件的文件名

客户端操作系统	客户端 GUI 文件	客户端 CLI 文件
Windows	vpnui.exe	vpncli.exe
Linux	vpnui	vpn
MacOS	管理中心部署不支持。但是，您可以为使用其他方法（例如 Altiris Agent）替换客户端 GUI 的 macOS 部署可执行文件。	vpn

如何使用 *Cisco Secure Client API* 部署自定义应用

开始之前

配置一个或多个远程访问 VPN IKE 策略。

过程

步骤 1 使用思科安全客户端 API 创建自定义应用。

步骤 2 创建新的安全客户端自定义对象。

a) 依次选择 **对象 > 对象管理 > VPN > 安全客户端自定义**。
b) 点击 **安全客户端自定义**。
c) 输入自定义的名称和说明。
d) 从 **自定义类型** 下拉列表中，选择 **二进制文件**。
e) 从 **平台** 下拉列表中选择平台。
f) 点击 **浏览** 并选择自定义应用。

步骤 3 将自定义添加到远程接入 VPN 策略。

a) 选择 **设备 > 远程访问**。
b) 点击远程接入 VPN 策略的编辑图标。
c) 点击 **高级 > 安全客户端自定义 > 二进制文件**。
d) 点击 **+** 选择转换文件。
e) 点击 **添加 (Add)**。
f) 点击**确定**。

步骤 4 点击**保存**。

步骤 5 选择 **部署 > 部署** 并将策略部署到所分配的设备。在部署更改之后，更改才生效。

自定义安全客户端安装程序

您可以通过创建使用客户端安装程序部署的自定义转换来自定义安全客户端 GUI。您可以将转换导入管理中心并将其部署到威胁防御设备。威胁防御使用客户端安装程序将此转换部署到终端。

注释 此自定义仅适用于 Windows。

本地化客户端安装程序

您可以翻译 Cisco Secure Client 安装程序显示的消息。管理中心使用转换功能来翻译安装程序显示的消息。该转换会更改安装，但会保持原始安全签名的 MSI 不变。这些转换仅翻译安装程序屏幕，而不翻译客户端 GUI 屏幕。

Cisco Secure Client 的每个版本都包括本地化转换，管理员可在上传含有新软件的 Cisco Secure Client 软件包时将转换上传到管理中心。如果您使用我们的本地化转换，请确保在上传新的 Cisco Secure Client 软件包时用 Cisco.com 的最新版本更新这些转换。

如何自定义或本地化客户端安装程序

开始之前

配置一个或多个远程访问 VPN IKE 策略。

过程

步骤 1 创建自定义或本地化转换。

步骤 2 创建新的安全客户端自定义对象。

a) 依次选择 **对象 > 对象管理 > VPN > 安全客户端自定义**。
b) 点击 **安全客户端自定义**。
c) 输入自定义的名称和说明。
d) 从**自定义类型 (Customization Type)** 下拉列表中，选择**自定义安装程序转换 (Customized Installer Transform)** 或**本地化安装程序转换 (Localized Installer Transform)**。
e) 从 **平台** 下拉列表中选择平台。
f) 点击 **浏览** 并选择转换。

步骤 3 将自定义添加到远程接入 VPN 策略。

a) 选择 **设备 > 远程访问**。
b) 点击远程接入 VPN 策略的编辑图标。
c) 点击 **高级 > 安全客户端自定义 > 自定义安装程序转换**或 **本地化安装程序转换**。
d) 点击 **+** 选择转换。
e) 点击 **添加 (Add)**。
f) 点击**确定**。

步骤 4 点击**保存**。

步骤 5 选择 **部署 > 部署** 并将策略部署到所分配的设备。在部署更改之后，更改才生效。

验证安全客户端自定义

验证部署

在部署完成后，请在管理中心中验证部署。点击 **脚本详细信息** （）) 图标以验证为自定义生成的命令。

示例

1. 以下示例显示 GUI 文本和消息自定义的脚本详细信息：使用自定义提示保护客户端 en_us 本地化。

```
import webvpn translation-table AnyConnect language en-us disk0:/AnyConnect_en-us.po
```

2. 以下示例显示自定义图标和图像的脚本详细信息：将 Secure Client 徽标自定义为 ABC 徽标。

```
import webvpn AnyConnect-customization type resource platform win name company_logo.png
 disk0:/company_logo.png
```

3. 以下示例显示自定义 OnConnect 和 OnDisconnect 脚本的脚本详细信息。连接时脚本装载网络驱动器，断开连接脚本卸载网络驱动器。

```
import webvpn AnyConnect-customization type binary platform win name
  scripts_OnConnect_mount.bat disk0:/mount.bat
import webvpn AnyConnect-customization type binary platform win name
  scripts_OnDisconnect_unmount.bat disk0:/unmount.bat
```

使用威胁防御命令验证自定义

在威胁防御上使用以下命令验证自定义设置：

- **show import webvpn translation-table detailed**：显示可用的转换表。

```
HQ-FTD# show import webvpn translation-table detailed
 Translation Tables' Templates:
   AnyConnect           ia4DaAXNSvl5pZboQRGJcs9KMXY=
   customization
 Translation Tables:
   fr                   customization        BWWodsOt1PbvDvYOp8hLb3W7a64=
   ja                   customization        lNvUk1+qTLNZyNrBcApMQPHnm1M=
   ru                   customization        UqyKyUAcjR+xTGUtdiIFnoIiW5U=
```

- **show import webvpn AnyConnect-customization detailed**：显示安全客户端自定义的详细信息。

```
HQ-FTD# show import webvpn AnyConnect-customization detailed
OEM resources for AnyConnect client:
  linux-64/binary/scripts_OnConnect_conn.sh           w6+n7z80D/8AR+ul2f7DvTmcDTw=
  linux-64/binary/scripts_OnDisconnect_discon.sh      jx5LJC2XBEmEkGeww59CAkszvnI=
  linux-64/resource/company-logo.png                  GsfBDroqGSQEEwuBDS/3DJNVv88=
  win/binary/scripts_OnConnect_mount.bat              dzjfsLYYft/XMlPlzskKl+Wv1bw=
  win/binary/scripts_OnDisconnect_unmount.bat         k6xlKhF1l2IRyJu08+sdYXgKNgM=
  win/resource/company_logo.png                       cmEvxwqvtaS+Pz/6sb9n3NZudS4=
```

验证安全客户端中的自定义

- 在安全客户端中，点击 **消息历史记录** 选项卡以验证是否已下载自定义设置。

  使用 DART 工具查看客户端诊断。

表 8: 验证安全客户端中的自定义

可以定制	验证
GUI 文本和消息自定义	• 验证安全客户端是否在以下位置具有语言本地化或自定义文件： • Windows: %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\l10n\<language-code>\LC_MESSAGES (AnyConnect 版本 4.9 及更早版本) • Windows: %ProgramData%\Cisco\Cisco Secure Client\l10n\<language-code>\LC_MESSAGES (Secure Client 版本 5.0 及更早版本) • 对于 Mac OS 和 Linux: /opt/cisco/anyconnect/l10n/<LANGUAGE-CODE>/LC_MESSAGES • 验证本地化或自定义文件的内容，并确认它们是否具有自定义或本地化字符串。例如：AnyConnect.mo
图像和图标自定义	• 验证安全客户端是否在以下位置具有自定义文件： • Windows: %PROGRAMFILES%\ Cisco\Cisco AnyConnect Secure Mobility Client\res\ (AnyConnect 版本 4.10 及更早版本) • Windows: %PROGRAMFILES%\ Cisco\Cisco Secure Client\UI\res (Cisco Secure Client 5.0 及更高版本) • Mac OS 和 Linux: /opt/cisco/anyconnect/res • 验证自定义图标或图像文件的内容。
自定义 OnConnect 和 OnDisconnect 脚本	• 验证自定义脚本是否位于以下位置： • Windows: %ProgramData%\Cisco\Cisco Secure Client\Script (Cisco Secure Client 5.0 及更高版本) • Windows: %ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Script (AnyConnect 版本 4.9 及更早版本) • Mac OS 和 Linux: /opt/cisco/anyconnect/Script • 验证脚本。

配置 安全客户端 管理 VPN 隧道

只要客户端系统通电，管理 VPN 隧道就会提供与企业网络的连接，而无需 VPN 用户连接到 VPN。这有助于组织通过软件补丁和更新让终端保持最新状态。在建立用户发起的VPN隧道后，管理隧道将断开连接。

本部分提供有关在 上配置 安全客户端 管理 VPN 隧道的信息。使用 防火墙管理中心 Web 界面在 上配置 安全客户端 管理隧道需要以下设置：

- 具有基于证书的身份验证和组 URL 的**连接配置文件**。
- **为服务器配置了组 URL 和备份服务器（如果需要）的Secure Client 管理 VPN 配置文件**。
- 包含管理 VPN 配置文件（其中明确包含网络的分割隧道、客户端绕行协议且无横幅）的**组策略**。

有关配置 安全客户端 管理 VPN 隧道的详细说明，请参阅 在 上配置 安全客户端 管理 VPN 隧道，第 69 页。

安全客户端 管理 VPN 隧道的要求和前提条件

软件和配置要求

在使用 Web 界面在 防火墙管理中心 上配置 安全客户端 管理隧道之前，请确保您已具备以下条件：

- 确保您使用的是 和 防火墙管理中心 版本 6.7.0 或更高版本。
- 下载 安全客户端 安全客户端 VPN Webdeploy 软件包 4.7 或更高版本，并将其上传到 远程访问 VPN。
- 确保在连接配置文件中配置证书身份验证。
- 确保未在组策略中配置横幅。
- 检查管理隧道组策略中的分割隧道配置。

证书要求

- 必须具有远程访问 VPN 的有效身份证书，并且 上必须存在来自本地证书颁发机构 (CA) 的根证书。
- 连接到管理 VPN 隧道的终端必须具有有效的身份证书。
- 的身份证书的 CA 证书必须安装在终端上，而终端的 CA 证书必须安装在 上。
- 同一本地 CA 颁发的身份证书必须存在于计算机存储区中。

  证书存储区（适用于 Windows）和/或系统密钥链中（适用于 macOS）。

安全客户端 管理 VPN 隧道的限制

- 安全客户端 管理 VPN 隧道仅支持证书身份验证，而不支持基于 AAA 的身份验证。

- 不支持公共或专用代理设置。
- 在已连接管理 VPN 隧道时，不支持安全客户端 升级和 AnyConnect 模块下载。

在 上配置 安全客户端 管理 VPN 隧道

过程

步骤 1 使用向导来创建远程访问 VPN 策略配置：

有关配置远程访问 VPN 的信息，请参阅配置新的远程访问 VPN 连接，第 10 页。

步骤 2 配置管理 VPN 隧道的连接配置文件设置：

注释
建议创建仅用于 安全客户端 管理 VPN 隧道的新连接配置文件。

a) 编辑已创建的远程访问 VPN 策略。
b) 选择并编辑将用于管理 VPN 隧道的连接配置文件。
c) 点击 **AAA** > **身份验证方法 (Authentication Method)** 并选择**仅限客户端证书 (Client Certificate Only)**。根据需要配置授权和记账设置。
d) 点击连接配置文件的**别名 (Aliases)** 选项卡。
e) 在连接配置文件的 URL 别名和 **URL 别名**下，点击**添加 (+) (Add [+])**。
f) 点击**启用 (Enabled)** 以启用 URL。
g) 点击**确定**，然后点击**保存**以保存连接配置文件设置。

有关连接配置文件设置的详细信息，请参阅配置连接配置文件设置，第 22 页。

步骤 3 使用 安全客户端配置文件编辑器来创建管理隧道配置文件：

a) 从 Cisco 软件下载中心 下载 安全客户端 **VPN 管理隧道独立配置文件编辑器** （如果尚未下载）。
b) 使用 VPN 用户的所需设置来创建管理隧道配置文件并保存文件。
c) 使用您在连接配置文件中配置的组 URL 来配置服务器列表中的服务器。

有关使用配置文件编辑器来创建管理配置文件的详细信息，请参阅 *Cisco Secure Client（包括 AnyConnect）管理员指南*。

步骤 4 创建管理隧道对象：

a) 在 Cisco Secure Firewall Management Center Web 接口上，导航至 **对象** > **对象管理** > **VPN** > **安全客户端文件**
b) 点击 **添加安全客户端文件**。
c) 指定 安全客户端 文件的 **名称** 。
d) 点击**浏览 (Browse)** 并选择已保存的管理隧道配置文件。
e) 点击 **文件类型** 下拉列表，然后选择 **安全客户端管理 VPN 配置文件**。
f) 点击**保存**。

注释

您还可以在创建或更新组策略的 安全客户端 设置时创建管理隧道对象。请参阅组策略 Secure Client 选项。

步骤 5 将管理配置文件与组策略关联并配置组策略设置：

您必须将管理 VPN 配置文件添加到与用于管理隧道 VPN 连接的连接配置文件关联的组策略。当用户连接时，系统会下载管理 VPN 配置文件以及已映射到组策略的用户 VPN 配置文件，从而启用管理 VPN 隧道功能。

注意
无横幅 (No Banner)：检查并确保未在组策略设置中配置横幅。您可以在**组策略 (Group Policy)** > **常规设置 (General Settings)** > **横幅 (Banner)** 下检查横幅设置。

a) 编辑为管理 VPN 隧道创建的连接配置文件。
b) 点击 **编辑组策略** > **安全客户端** > **管理配置文件**。
c) 点击**管理 VPN 配置文件 (Management VPN Profile)** 下拉列表，然后选择您创建的管理配置文件对象。

注释
您还可以点击 + 并添加新的 安全客户端 管理 VPN 配置文件对象。

d) 点击**保存**。

步骤 6 在组策略中配置分割隧道：

a) 点击**编辑组策略 (Edit Group Policy)** > **常规 (General)** > **分割隧道 (Split Tunneling)**。
b) 从 IPv4 或 IPv6 分割隧道的下拉菜单中，选择**下面指定的隧道网络 (Tunnel networks specified below)**。
c) 选择拆分隧道网络列表类型：**标准访问列表 (Standard Access List)** 或**扩展访问列表 (Extended Access List)**，然后选择所需的访问列表以允许流量通过管理 VPN 隧道。
d) 点击**保存**，保存分割隧道设置。

安全客户端自定义属性

安全客户端 管理 VPN 隧道要求分割默认包含隧道配置。如果要在组策略中配置 安全客户端 自定义属性，以使用分割隧道来部署管理 VPN 隧道，则可以使用 FlexConfig 执行此操作，因为 防火墙管理中心 6.7 Web 界面不支持 安全客户端 自定义属性。

以下是 安全客户端 自定义属性的示例命令：

```
webvpn
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
anyconnect-custom-data ManagementTunnelAllAllowed true true
group-policy MGMT_Tunnel attributes
 anyconnect-custom ManagementTunnelAllAllowed value true
```

步骤 7 部署、验证和监控远程访问 VPN 策略：

a) 将管理 VPN 隧道配置部署到 。

注释
客户端系统必须连接到 远程访问 VPN 一次，才能将管理隧道 VPN 配置文件下载到客户端计算机。

b) 您可以在 **安全移动客户端** > **VPN** > **统计信息** 中验证 安全客户端 管理 VPN 隧道。

您还可以使用 **show vpn-sessiondb anyconnect** 命令在 命令提示符后检查管理 VPN 会话详细信息。

c) 在 防火墙管理中心 Web 界面上，点击 **分析** 以查看管理隧道会话信息。

相关主题

配置连接配置文件设置，第 22 页
组策略对象

多证书身份验证

基于多个证书的身份验证能够让 验证计算机或设备的证书，以确保设备是企业发放的设备，此外还可以验证用户的身份证书，以允许在 SSL 或 IKEv2 EAP 阶段使用 Secure Client 来进行 VPN 访问。

通过多证书选项，可以同时通过证书对计算机和用户进行证书身份验证。如果未选中此选项，则只能对计算机或用户执行证书身份验证，而不能同时对两者执行证书身份验证。

多重证书身份验证的准则和限制

注释 配置多证书身份验证时，请确保在思科 Secure Client 配置文件设置中将 **AutomaticCertSelection** 的值设置为 true。

- 多证书身份验证当前会将证书数量限制为两个。
- Secure Client 必须指明支持多证书身份验证。如果不是这样，网关将使用其中一种旧版身份验证方法，否则连接将失败。安全客户端 版本 4.4.04030 或更高版本支持基于多证书的身份验证。
- 安全客户端 仅支持基于 RSA 的证书。
- 在 安全客户端 汇聚身份验证期间，仅支持基于 SHA256、SHA384 和 SHA512 的证书。
- 证书身份验证不能与 SAML 身份验证结合使用。

配置多证书身份验证

开始之前

在配置多证书身份验证之前，请确保配置了用于获取每台 设备的身份证书的证书注册对象。有关详细信息，请参阅证书映射对象。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 选择远程访问 VPN 策略，然后点击 **编辑 (Edit)**。

注释
如果尚未配置远程接入 VPN，请点击**添加 (Add)** 以创建新的远程接入 VPN 策略。

步骤 3 选择并**编辑**连接配置文件，以便配置多证书身份验证。

步骤 4 点击 **AAA** 设置，然后选择**身份验证方法 (Authentication Method)** > **仅客户端证书 (Client Certificate Only)** 或**客户端证书和 AAA (Client Certificate & AAA)**。

注释
如果您选择了客户端证书和 AAA 身份验证方法，请选择**身份验证服务器 (Authentication Server)**

步骤 5 选择**启用多证书身份验证 (Enable multiple certificate authentication)**。

步骤 6 选择一个证书以便**映射客户端证书中的用户名**：

- **第一个证书** - 选择此选项以映射从 VPN 客户端发送的计算机证书中的用户名。
- **第二个证书** - 选择此选项以映射从客户端发送的用户证书中的用户名。

如果启用仅证书身份验证，从客户端发送的用户名会被用作 VPN 会话用户名。如果启用了 AAA 和证书身份验证，VPN 会话用户名将基于预填充选项。

注释
如果选择**映射特定字段 (Map specific field)** 选项（包括客户端证书中的用户名），则**主 (Primary)** 字段和**辅助 (Secondary)** 字段将分别显示默认值：**CN**（**公用名**）和 **OU**（**组织单位**）。

如果选择**使用整个 DN**（**可分辨名称**）**作为用户名**选项，系统将自动检索用户身份。可分辨名称 (DN) 是由单个字段组成的唯一标识，可在将用户与连接配置文件匹配时用作标识符。DN 规则用于增强的证书身份验证。

如果您选择了客户证书和 AAA 身份验证，请选择 **在用户登录窗口预填证书中的用户名** 选项，以便在用户通过 Cisco Secure Client 的 AnyConnect VPN 模块连接时预填充辅助用户名。

- **在登录窗口隐藏用户名**： 辅助用户名是从客户端证书预填充的，但对用户隐藏，确保用户不会修改预填充的用户名。

步骤 7 为远程访问 VPN 配置所需的 AAA 设置和连接配置文件设置。

步骤 8 保存连接配置文件和远程访问 VPN 配置并将其部署在您的 设备上。

相关主题

配置远程访问 VPN 的 AAA 设置，第 24 页

基于地理位置管理远程用户的 VPN 访问

您可以根据用户所在的地理位置对其远程访问VPN 连接进行管理。通过配置允许或拒绝来自特定国家或地区的VPN连接，可以满足合规性要求并增强安全性。不符合这些基于位置的条件的连接会被阻止，然后进行身份验证，详细信息记录在 防火墙管理中心（**设备 > 故障排除 > 故障排除日志**）。

此功能支持 Secure Client 的所有版本。

前提条件

设备的必须为 7.7.0 或更高版本。

基于地理位置管理远程用户 VPN 访问的工作流程

步骤	任务	更多信息
1	定义策略以允许对远程客户端进行基于地理位置的访问控制。	配置服务访问对象
2	使用该策略更新远程访问 VPN 配置。	配置远程访问 VPN 的访问接口，第 40 页
3	在设备上部署配置。	—
4	在客户端连接到 设备之后： 1. 在**远程访问 VPN (Remote Access VPN)** 控制面板中验证活动远程访问 VPN 会话。 2. 在**设备 (Devices) > 故障排除 (Troubleshoot) > 故障排除日志 (Troubleshooting Logs)** 中验证被拒绝的远程访问 VPN 会话的日志。	监控服务访问策略并进行故障排除，第 74 页

基于地理位置管理远程接入 VPN 用户的准则和限制

准则

- 在服务访问对象中，如果使用地理位置对象（国家/地区、大洲或地理位置对象），请仅在一个规则中使用该对象。
- 按照正确的顺序配置服务访问规则，因为这些规则不能重新排序。

限制

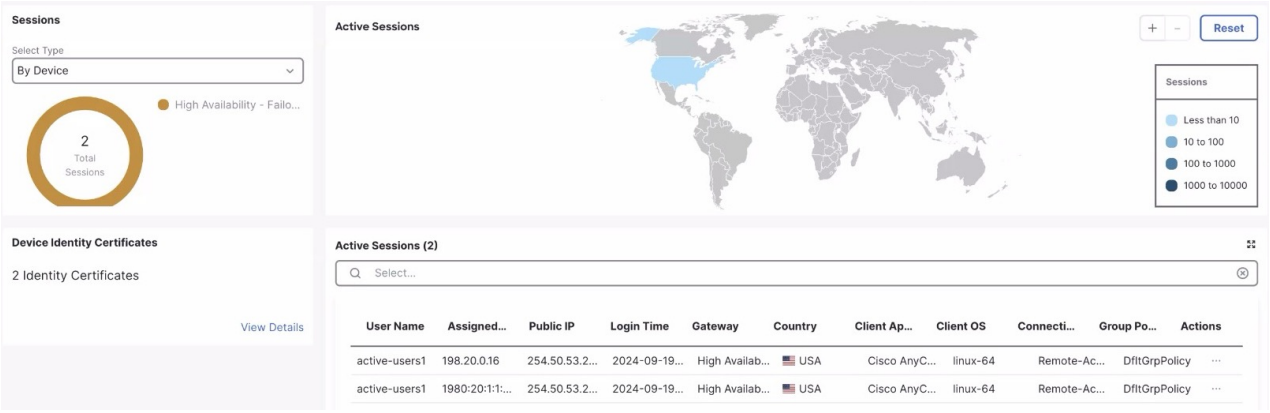
- 不支持群集。

- 基于地理位置的未分类 IP 地址不按其地理来源进行分类。对于此类未分类的 IP 地址，防火墙管理中心 会实施默认服务访问策略操作。
- 来自 IETF RFC1918 地址的连接，无论服务访问策略设置如何，都允许用于基于地理位置的远程访问 VPN。

监控服务访问策略并进行故障排除

在远程访问 VPN 控制面板中监控活动的远程访问 VPN 会话

选择概述 **(Overview)** > 控制面板 **(Dashboards)** > 远程访问 **VPN (Remote Access VPN)**。

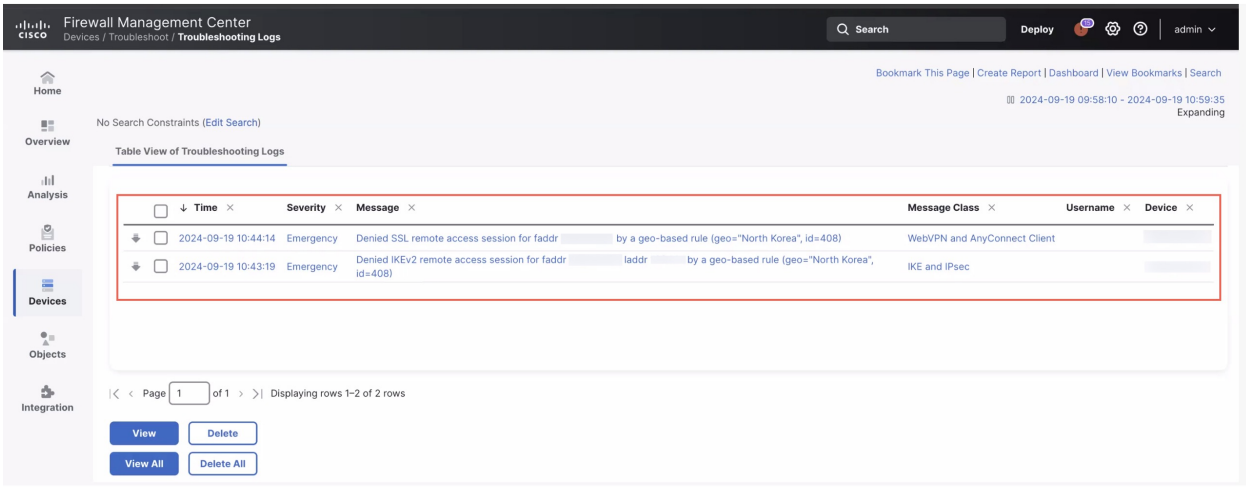


监控被拒绝的远程访问 VPN 会话

在**设备 (Devices)** > **故障排除 (Troubleshoot)** > **故障排除日志 (Troubleshooting Logs)** 中监控被拒绝的远程访问 VPN 会话。要查看拒绝的远程访问 VPN 会话，则必须在 中配置系统日志设置：

1. 选择**设备 (Devices)** > **平台设置 (Platform Settings)** 并创建或编辑威胁防御策略。
2. 在左侧窗格中，点击**系统日志 (Syslog)**。
3. 点击**日志记录设置 (Logging Setup)** 选项卡。
4. 选中 **Enable Logging** 复选框。
5. 点击 **VPN 日志 (VPN Logs)** 单选按钮。
6. 在**日志记录级别 (Logging Level)** 下拉列表中，选择 **6 信息 (6 - informational)**。
7. 点击**保存**。

注释 如果为**所有日志 (All Logs)** 选项配置的**日志记录级别**介于 0 和 2 之间，则您无法查看拒绝的远程访问 VPN 会话。



验证服务访问策略

在 设备 CLI 中，运行以下命令：

- **show running-config service-access**：显示用户定义的服务访问策略。

```
firepower#show running-config service-access
   service-access deny geolocation OBJGRP_Asia1
   service-access permit interface outside ra-ssl-client geolocation OBJGRP_India
   service-access deny ra-ikev2 geolocation any
```

- **show service-access**：显示用户定义的服务访问策略的详细信息。

```
firepower# show service-access
1 outside          : ra-ikev2 ra-ssl-client (permit) hits = 8288
  Last hit time    : 10:58:10.038 IST Tue Jul 16 2024
  object-group     : FMC_INTERNAL_XXY
2 any              : ra-ikev2 ra-ssl-client (deny) hits = 123
  Last hit time    : 11:23:12.032 IST Tue Jul 17 2024
  object-group     : any


firepower# show service-access detail
1 outside          : ra-ikev2 ra-ssl-client (permit) hits = 8288
  Last hit time    : 10:58:10.038 IST Tue Jul 16 2024
  object-group     : FMC_INTERNAL_XXY
  geolocation      : Egypt(818) Jordan(400)
                     Iran (Islamic Republic of)(364)
                     Saudi Arabia(682)
```

- **show geodb**：显示地理位置表的详细信息。

  show geodb {**ipv4** | **ipv6** | **counters** | **context**} [**location** *country_name* | **lookup** *ip_address*] [**detail**]

  - **show geodb** {**ipv4** | **ipv6**}：显示 IPv4 或 IPv6 地址映射总数。

```
firepower# show geodb ipv4
 Geolocation Table - IPv4
 Total number of mappings available: 532507
 Last geolocation data read time:  17:02:13.000 IST Thu Jul 18 2024
```

```
Running geolocation update version: 2024-02-15-019
```

- **show geodb** {**ipv4** | **ipv6**} **location** *country_name* **detail**：显示 IPv4 或 IPv6 地址映射的详细信息。

```
firepower# show geodb ipv4 location Antarctica detail
Geolocation Table - IPv4
id=0x00007fff82c284e0, geo_id=10, hits=0
        range_lower=77.70.176.176, range_upper=77.70.176.183
id=0x00007fff82cca360, geo_id:10, hits=0
     range_lower=79.110.169.69, range_upper=79.110.169.69
Total number of mappings available: 28
```

- **show geodb counters**：显示活动会话、允许会话和被拒绝会话的详细信息。

```
firepower# show geodb counters
current    - ongoing sessions
permitted  - cumulative permitted sessions
denied     - cumulative denied sessions
Location                current          permitted      denied
Egypt                     0                  0             5
India                     45                 1345          45
```

- **show geodb** {**ipv4** | **ipv6lookup** *ip_address*：显示特定 IPv4 或 IPv6 地址的地理位置。

```
firepower# show geodb ipv4 lookup 223.223.128.24
Geolocation of 223.223.128.24 is "India" (356) with id=0x000015114d0aa330
Matching network range: 223.223.128.0 - 223.223.159.255
```

服务访问策略故障排除

- 系统日志

  启用远程访问 VPN 服务访问系统日志：

  1. 选择 **设备 > 平台设置**。
  2. 创建或编辑平台设置策略。
  3. 在左侧窗格中，点击**系统日志 (Syslog)**。
  4. 点击**日志记录设置 (Logging Setup)** 选项卡并选中**启用日志记录 (Enable Logging)** 复选框。
  5. 点击**系统日志设置 (Syslog Settings)** 选项卡，并启用服务访问系统日志 751031 和 716166 的系统日志。

- 命令
  - 使用 **show running-config service-access** 和 **show service-access** 命令查看用户定义的服务访问策略的详细信息。
  - 使用 **show geodb** 命令查看地理位置表的详细信息。
  - 使用 **debug geolocation <debug-level>** 命令发送到捕获与地理位置相关的调试日志。调试级别可以是 1（错误）、2（警告）、3 和 4（信息）、5（调试）或 255（全部调试）。

- 使用 **clear geodb counters** 命令清除地理位置表计数器，例如服务访问策略的命中计数。但是，使用该命令无法清除位置的实际允许和拒绝计数器；只有在重启设备后才能清除这些计数器。

自定义远程接入 VPN AAA 设置

本节提供有关自定义远程接入 VPN 的 AAA 首选项的信息。有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 24 页。

通过客户端证书对 VPN 用户进行身份验证

使用向导创建新的远程接入 VPN 策略或稍后编辑策略时，可以使用客户端证书配置远程接入 VPN 身份验证。

开始之前

配置用于为每台充当 VPN 网关的 设备获取身份证书的证书注册对象。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程访问**。

步骤 2 在远程访问策略，然后点击 **编辑**；或者点击 **添加** 以创建新的远程访问 VPN 策略。

步骤 3 对于新的远程访问VPN策略，请在选择连接配置文件设置时配置身份验证。对于现有配置，选择包含客户端配置文件的连接配置文件，然后点击**编辑**。

步骤 4 点击 **AAA** > **身份验证方法 (Authentication Method)** > **仅限客户端证书 (Client Certificate Only)**。

使用此身份验证方法，用户可以使用客户端证书进行身份验证。必须在VPN客户端终端上配置客户端证书。默认情况下，用户名分别派生自客户端证书字段CN和OU。如果在客户端证书的其他字段中指定了用户名，请使用“主”字段和“辅助”字段来映射适当的字段。

如果选择**映射特定字段**选项，其中包括来自客户端证书的用户名。 **主** 字段和 **辅助** 字段将显示默认值： **CN**（**公用名**） 和**OU**（**组织单位**）。如果选择**使用整个 DN 作为用户名**选项，系统将自动检索用户身份。可分辨名称(DN)是由单个字段组成的唯一标识，可在将用户与连接配置文件匹配时用作标识符。DN 规则用于增强的证书身份验证。

- 与 **映射特定字段** 选项相关的“主”和“辅助”字段包含以下公共值：
  - C（国家/地区）
  - CN（公用名）
  - DNQ（DN 限定符）
  - EA（邮件地址）

- GENQ（代系限定符）
- GN（名字）
- I（首字母）
- L（地区）
- N（名字）
- O（组织）
- OU（组织单位）
- SER（序列号）
- SN（姓氏）
- SP（省）
- T（职务）
- UID（用户 ID）
- UPN（用户主体名称）

- 无论选择哪种身份验证方法，选择或取消选择**仅当用户位于授权数据库中时才允许连接**。

有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 24 页。

步骤 5 保存更改。

相关主题

配置连接配置文件设置，第 22 页
添加证书注册对象

通过客户端证书和 AAA 服务器配置 VPN 用户身份验证

在配置远程接入VPN身份验证以便同时使用客户端证书和身份验证服务器时，会使用客户端证书验证和 AAA 服务器来完成 VPN 客户端身份验证。

开始之前

- 配置用于为每台充当 VPN 网关的 设备获取身份证书的证书注册对象。
- 配置在远程访问 VPN 策略配置中使用的 RADIUS 服务器组对象和任何 AD 或 LDAP 领域。
- 确保可以通过 Cisco Secure Firewall Threat Defense设备访问 AAA 服务器，以使远程接入 VPN 配置生效。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择 **设备** > **远程访问**。

步骤 2 在要更新身份验证的远程接入 VPN 策略上点击 **编辑** ，或点击 **添加** 以创建新的身份验证。

步骤 3 如果选择创建新的远程接入 VPN 策略，请在选择连接配置文件设置时配置身份验证。对于现有配置，选择包含客户端配置文件的连接配置文件，然后点击**编辑**。

步骤 4 转到 **AAA** ，然后从 **身份验证方法** 下拉列表中选择 **客户端证书和 AAA**。

- 何时选择以下**身份验证方法**：

  客户端证书和 AAA - 完成两种类型的身份验证。

  - **AAA** - 如果选择 **RADIUS** 作为**身份验证服务器**，则授权服务器默认也采用此选择。从下拉列表中选择**记帐服务器**。每当从“身份验证服务器”下拉列表中选择 **AD** 和 **LDAP** 时，都必须手动分别选择**授权服务器**和**记帐服务器**。
  - **客户端证书**-使用客户端证书对用户进行身份验证。您必须在 VPN 客户端终端上配置客户端证书。默认情况下，用户名分别派生自客户端证书字段 CN 和 OU。如果使用客户端配置文件中的任何其他字段指定了用户名，请使用 **主字段** 和 **辅助字段** 来映射相应的字段。

    如果选择**映射特定字段**选项，其中包括来自客户端证书的用户名。则**主**和**辅助**字段将显示默认值：**CN (公用名称)** 和 **OU (组织单位)**。如果选择**使用整个 DN 作为用户名**选项，系统将自动检索用户身份。可分辨名称 (DN) 是由单个字段组成的唯一标识，可在将用户与连接配置文件匹配时用作标识符。DN 规则用于增强的证书身份验证。

    与**映射特定字段**选项相关的“主”和“辅助”字段包含以下公共值：

    - C（国家/地区）
    - CN（公用名）
    - DNQ（DN 限定符）
    - EA（邮件地址）
    - GENQ（代系限定符）
    - GN（名字）
    - I（首字母）
    - L（地区）
    - N（名字）
    - O（组织）
    - OU（组织单位）
    - SER（序列号）
    - SN（姓氏）

- SP（省）
- T（职务）
- UID（用户 ID）
- UPN（用户主体名称）

- 无论选择哪种身份验证方法，选择或取消选择**仅当用户位于授权数据库中时才允许连接**。

有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 24 页。

步骤 5 保存更改。

相关主题

配置连接配置文件设置，第 22 页
添加证书注册对象

通过 VPN 会话管理密码更改

通过密码管理，远程访问 VPN 策略管理员可以为远程访问 VPN 用户配置密码到期时的通知设置。密码管理在使用身份验证方法“仅 AAA”和“客户端证书和 AAA”的 AAA 设置中可用。有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 24 页。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择 **设备** > **远程访问**。

步骤 2 点击要编辑的远程访问 VPN 策略旁边的 **编辑** 。

步骤 3 在包含 AAA 设置的连接配置文件上点击 **编辑** 。

步骤 4 选择 **AAA** > **高级设置** >。

步骤 5 选中 **启用密码管理** 复选框并选择以下选项之一：

- 通知用户 - 在密码到期之前；在框中指定天数。
- 在密码到期当天通知用户。

步骤 6 保存更改。

相关主题

配置连接配置文件设置，第 22 页

向 RADIUS 服务器发送记账记录

远程接入 VPN 中的记账记录有助于 VPN 管理员跟踪用户访问的服务以及他们使用的网络资源量。记账信息包括用户会话的开始和停止时间、用户名、会话时通过设备的字节数、使用的服务以及每个会话的持续时间。

您可以单独使用记帐功能，也可以将其与身份验证和授权功能配合使用。激活 AAA 记账时，网络访问服务器会向所配置的记账服务器报告用户活动。您可以将 RADIUS 服务器配置为记账服务器，以便将所有用户活动信息从 防火墙管理中心 发送到 RADIUS 服务器。

注释 您可以在远程接入 VPN AAA 设置中使用相同的 RADIUS 服务器或单独的 RADIUS 服务器进行认证授权和记账。

开始之前

- 使用将向其发送身份验证请求或记账记录的 RADIUS 服务器配置 RADIUS 组对象。有关详细信息，请参阅RADIUS 服务器组选项。
- 确保可从 设备访问 RADIUS 服务器。配置 Cisco Secure Firewall Management Center上的路由（位于**设备** > **设备管理** > **编辑设备** > **路由**），以确保 RADIUS 服务器的连接。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择 **设备** > **远程访问**。

步骤 2 在要配置 RADIUS 服务器的远程访问策略上点击 **编辑**，或创建新的远程访问 VPN 策略。

步骤 3 在包含 AAA 设置的连接的配置文件上点击 **编辑**，然后选择 **AAA**。

步骤 4 从 **记帐服务器** 下拉列表中选择 RADIUS 服务器。

步骤 5 保存更改。

相关主题

配置连接配置文件设置，第 22 页
配置远程访问 VPN 的 AAA 设置，第 24 页

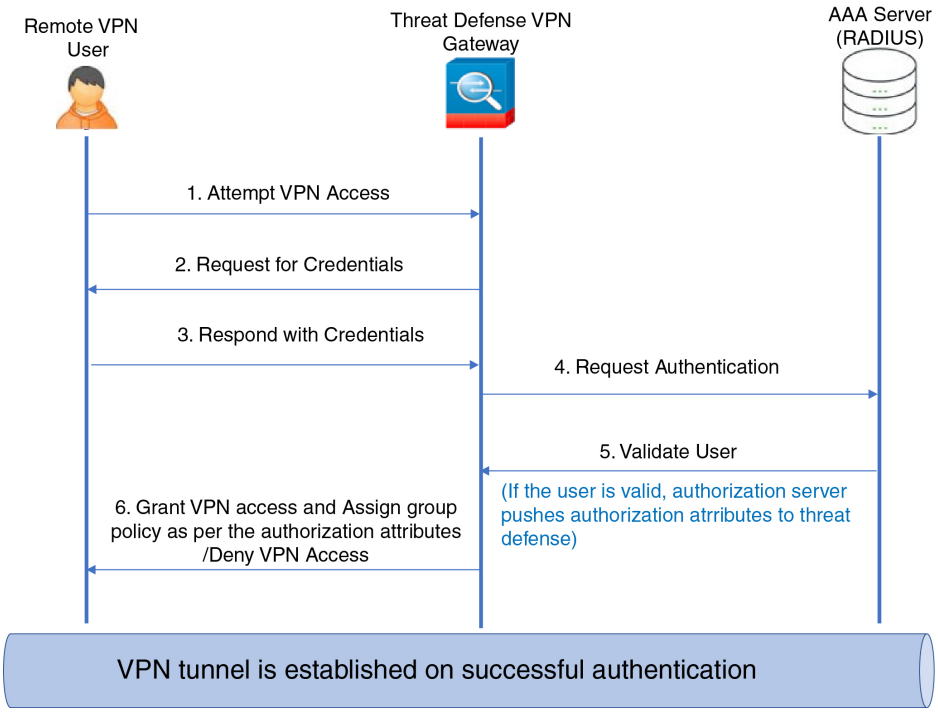
将组策略选择委派给授权服务器

在建立 VPN 隧道时，将确定应用于用户的组策略。您可以在使用向导来创建远程接入 VPN 策略时为连接配置文件选择组策略，也可以稍后再更新连接配置文件的连接策略。但是，您可以配置 AAA (RADIUS) 服务器以分配组策略，或者从当前连接配置文件中获取。如果 设备从与连接配置文件上配置的属性冲突的外部 AAA 服务器接收属性，则来自 AAA 服务器的属性始终优先。

您可以配置 ISE 或 RADIUS 服务器，通过发送 IETF RADIUS 属性 25 并映射到相应的组策略名称来为此用户或用户组设置授权配置文件。您可以为用户或用户组配置特定组策略，以便推送可下载 ACL、设置横幅、限制 VLAN，并配置将 SGT 应用于会话的高级选项。建立 VPN 连接时，这些属性将应用于属于该组的所有用户。

有关更多信息，请参阅《思科身份服务引擎管理员指南》中的“配置标准授权策略”部分和Cisco Secure Firewall Threat Defense 的 RADIUS 服务器属性，第 30 页。

图 *1: AAA* 服务器的远程接入 *VPN* 组策略选择



相关主题

配置组策略对象
配置连接配置文件设置，第 22 页

授权服务器覆盖组策略或其他属性的选择

当远程访问 VPN 用户连接 VPN 时，系统会将连接配置文件中配置的组策略和其他属性分配给用户。但是，远程访问 VPN 系统管理员可以通过配置 ISE 或 RADIUS 服务器为用户或用户组设置授权配置文件，将组策略和其他属性的选择委派给授权服务器。用户通过身份验证后，这些特定的授权属性将被推送到 设备。

开始之前

确保使用 RADIUS 作为身份验证服务器来配置远程访问 VPN 策略。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程访问**。

步骤 2 选择远程访问策略，然后点击 **编辑**。

步骤 3 如果尚未配置，请选择 RADIUS 或 ISE 作为授权服务器。

步骤 4 选择**高级组策略**，并添加所需的组策略。有关组策略对象的详细信息，请参阅 配置组策略对象。

您只可将单个组策略映射到连接配置文件；但是，您可以在远程访问VPN策略中创建多个组策略。可以在 ISE 或 RADIUS 服务器中引用这些组策略，并将其配置为通过在授权服务器中分配授权属性来覆盖连接配置文件中配置的组策略。

步骤 5 在目标 设备上部署配置。

步骤 6 在授权服务器上，使用 IP 地址和可下载 ACL 的 RADIUS 属性创建授权配置文件。

在选择用于远程访问VPN的授权服务器中配置组策略后，组策略将覆盖用户通过身份验证后在远程访问 VPN 用户的连接配置文件中配置的组策略。

相关主题

配置组策略对象

拒绝用户组的 VPN 访问

如果您不希望通过身份验证的用户或用户组使用 VPN，则可以配置组策略以拒绝 VPN 接入。您可以在远程访问 VPN 策略中配置组策略，并在 ISE 或 RADIUS 服务器配置中引用此策略以进行授权。

开始之前

确保已使用远程访问策略向导配置远程访问 VPN，并已为远程访问 VPN 策略配置身份验证设置。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程访问**。

步骤 2 选择远程访问策略，然后点击 **编辑**。

步骤 3 选择**高级组策略**。

步骤 4 选择组策略，点击**编辑 (Edit)** 或添加新增组策略。

步骤 5 选择**高级会话设置**并将**每个用户同时登录数**设置为 0 （零）。
这会阻止用户或用户组连接到 VPN，哪怕只有一次。

步骤 6 点击**保存**以保存组策略，然后保存远程访问 VPN 配置。

步骤 7 配置 ISE 或 RADIUS 服务器，为此用户/用户组设置授权配置文件，以发送 IETF RADIUS 属性 25 并映射到相应的组策略名称。

步骤 8 配置 ISE 或 RADIUS 服务器作为远程访问 VPN 策略中的授权服务器。

步骤 9 保存和部署远程访问 VPN 策略。

相关主题

配置连接配置文件设置，第 22 页

限制用户组的连接配置文件选择

如果要在用户或用户组上强制实施单个连接配置文件，可以选择禁用连接配置文件，以便用户在使用 Cisco Secure Client 的 AnyConnect VPN 模块连接时无法选择组别名或 URL。

例如，如果您的组织要为不同的VPN用户组（如移动用户、公司分发的笔记本电脑用户或个人笔记本电脑用户）使用特定配置，则可以配置特定于每个用户组的连接配置文件，并在用户连接VPN时应用适当的连接配置文件。

默认情况下，Cisco Secure Client 的 AnyConnect VPN 模块将显示在 防火墙管理中心 中配置并在 上部署的连接配置文件列表（按连接配置文件名称、别名或别名 URL）。如果未配置自定义连接配置文件，Cisco Secure Client 的 AnyConnect VPN 模块将显示 *DefaultWEBVPNGroup* 连接配置文件。使用以下程序实施用户组的单个连接配置文件。

开始之前

- 在 Cisco Secure Firewall Management Center Web 界面中，使用远程访问 VPN 策略向导配置远程访问 VPN，将身份验证方法设置为“仅客户端证书”或“客户端证书+AAA”。从证书中选择用户名字段。
- 配置 ISE 或 RADIUS 服务器以进行授权，并将组策略与授权服务器关联。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程访问**。

步骤 2 选择远程访问策略，然后点击 **编辑**。

步骤 3 选择 **访问接口**，然后禁用 **允许用户在登录时选择连接配置文件**。

步骤 4 点击**高级** **证书映射**。

步骤 5 选择 **使用配置的规则将证书与连接配置文件匹配**。

步骤 6 选择**证书映射名称**，或点击**添加**图标以添加证书规则。

步骤 7 选择**连接配置文件**并点击**确定**。
使用此配置，当用户从 Cisco Secure Client 的 AnyConnect VPN 模块连接时，用户将具有映射的连接配置文件，并将进行身份验证以使用 VPN。

相关主题

配置组策略对象
配置连接配置文件设置，第 22 页

更新远程接入 VPN 客户端的 Secure Client 配置文件

Secure Client 客户端配置文件是一个 XML 文件，其中包含管理员定义的最终用户要求以及作为 安全客户端的一部分部署在VPN客户端系统上的身份验证策略。它使最终用户可以使用预配置的网络配置文件。

您可以使用基于GUI的 安全客户端配置文件编辑器（一个独立的配置工具）来创建他们。此独立配置文件编辑器可用于创建新的或修改现有的安全客户端配置文件。您可以从思科软件下载中心下载配置文件编辑器。

有关详细信息，请参见相应版本的 Cisco Secure Client（包括 AnyConnect）管理员指南中的 安全客户端配置文件编辑器 一章。

开始之前

- 确保已使用远程接入策略向导配置远程接入VPN，并已在 设备上部署配置。请参阅创建新的远程访问 VPN 策略， 第 12 页。
- 在 Cisco Secure Firewall Management Center Web 界面上，转至 **对象** > **对象管理** > **VPN** > **安全客户端文件**，然后添加新的 Secure Client 映像。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程访问**。

步骤 2 选择远程访问 VPN 策略，然后点击 **编辑**。

步骤 3 选择包含要编辑的客户端配置文件的连接配置文件，然后点击**编辑**。

步骤 4 点击 **编辑组策略** > **安全客户端** > **配置文件**。

步骤 5 从列表中选择一个客户端配置文件 XML 文件，或者点击**添加 (Add)** 以添加新的客户端配置文件。

步骤 6 保存组策略、连接配置文件，然后保存远程接入 VPN 策略。

步骤 7 部署更改。
客户端配置文件的更改将在 VPN 客户端连接到远程接入 VPN 网关时在 VPN 客户端上进行更新。

相关主题

配置组策略对象

RADIUS 动态授权

Cisco Secure Firewall Threat Defense 可以使用 RADIUS 服务器进行 VPN 远程接入和防火墙直接转发代理会话的用户授权（按用户使用动态访问控制列表 [ACL] 或 ACL 名称）。要实施动态授权或 RADIUS 授权更改 (RADIUS CoA) 的动态 ACL，您必须配置 RADIUS 服务器以支持它们。在用户尝试进行身份验证时，RADIUS 服务器会向 发送可下载的 ACL 或 ACL 名称。ACL 允许或拒绝访问特定服务。身份验证会话到期时，Cisco Secure Firewall Threat Defense会删除 ACL。

相关主题

添加 RADIUS 服务器组

接口

配置 RADIUS 动态授权，第 86 页

Cisco Secure Firewall Threat Defense 的 RADIUS 服务器属性，第 30 页

配置 RADIUS 动态授权

准备工作：

- 如果在 RADIUS 服务器中引用接口，则只能在安全区域或接口组中配置一个接口。
- 启用动态授权的 RADIUS 服务器需要 Cisco Secure Firewall Threat Defense 6.3 或更高版本才能使动态授权生效。
- Cisco Secure Firewall Threat Defense 6.2.3 或更低版本不支持 RADIUS 服务器中的接口选择。在部署期间，接口选项将被忽略。
- 终端安全评估 VPN 不支持通过动态授权或 RADIUS 授权来更改 (CoA) 更改组策略。

表 *9:* 过程

	相应操作	更多信息
步骤 1	登录 Cisco Secure Firewall Management Center Web 界面。	
步骤 2	使用动态授权配置 RADIUS 服务器对象。	RADIUS 服务器组选项
步骤 3	通过已启用授权更改 (CoA) 的接口配置到 ISE 服务器的路由，以通过路由或特定接口建立到 RADIUS 服务器的连接。	RADIUS 服务器组选项 配置 思科身份服务引擎 (Cisco ISE) 身份源的方法
步骤 4	配置远程访问 VPN 策略，选择您通过动态授权创建的 RADIUS 服务器组对象。	创建新的远程访问 VPN 策略，第 12 页
步骤 5	使用“平台设置”配置 DNS 服务器详细信息和域查找接口。	配置 DNS，第 16 页 DNS 服务器组
步骤 6	如果可以通过 VNP 网络访问 DNS 服务器，则在组策略中配置拆分隧道，以允许 DNS 流量通过远程接入 VPN 隧道。	配置组策略对象
步骤 7	部署配置更改。	部署配置更改

双因素身份验证

您可以为远程访问VPN配置双因素身份验证。配置了双因素身份验证时，用户必须提供用户名、静态密码，以及一个额外项，如RSA令牌或密码等。双因素身份验证不同于使用第二个身份验证源，双因素是在单个身份验证源中配置的，其与 RSA 服务器的关系绑定到主身份验证源。

Cisco Secure Firewall Threat Defense 支持 RSA 令牌和 Duo Push 身份验证请求，并将任何 RADIUS 或 AD 服务器作为双因素认证过程中的第一因素，向 Duo Mobile 提出第二因素。

配置 RSA 双因素身份验证

关于此任务：

您可以将 RADIUS 或 AD 服务器配置为 RSA 服务器中的身份验证代理，并将 Cisco Secure Firewall Management Center中的服务器用作远程接入 VPN 中的主身份验证源。

使用此方法时，用户必须使用 RADIUS 或 AD 服务器中配置的用户名进行身份验证，并使用一次性临时 RSA 令牌连接密码，用逗号分隔密码和令牌：密码,令牌。

在此配置中，通常会使用单独的RADIUS服务器 （例如，Cisco ISE 提供的 RADIUS 服务器) 提供授权服务。将第二个 RADIUS 服务器配置为授权、配置或记账服务器。

准备工作：

在 Cisco Secure Firewall Threat Defense上配置 RADIUS 双因素身份验证之前，请确保完成以下配置：

在 RSA 服务器上

- 将 RADIUS 或 Active Directory 服务器配置为身份验证代理。
- 生成并下载配置 (*sdconf.rec*) 文件。
- 创建令牌配置文件，将令牌分配给用户，并将令牌分发给用户。下载并在远程接入VPN客户端系统上安装令牌。

有关详细信息，请参阅 RSA SecureID 套件文档。

在 ISE 服务器上

- 导入 RSA 服务器上生成的配置 (*sdconf.rec*) 文件。
- 添加 RSA 服务器作为外部身份源并指定共享密钥。

表 *10:* 过程

	相应操作	更多信息
步骤 1	登录 Cisco Secure Firewall Management Center Web 界面。	
步骤 2	创建 RADIUS 服务器组。	RADIUS 服务器组选项

	相应操作	更多信息
步骤 3	在新 RADIUS 服务器组中创建 RADIUS 服务器对象，将 RADIUS 或 AD 服务器作为主机，超时时间为 60 秒或更长。	RADIUS 服务器组选项 注释 RADIUS 或 AD 服务器必须与在 RSA 服务器中配置为身份验证代理的服务器相同。 对于双因素身份验证，也要确保在 安全客户端配置文件 配置文件 XML 文件中将超时更新为 60 秒或更长。
步骤 4	使用向导配置新的远程接入 VPN 策略，或者编辑现有的远程接入 VPN 策略。	创建新的远程访问 VPN 策略， 第 12 页
步骤 5	选择 RADIUS 作为身份验证服务器，然后选择新创建的 RADIUS 服务器组作为身份验证服务器。	配置远程访问 VPN 的 AAA 设置， 第 24 页
步骤 7	部署配置更改。	部署配置更改

配置 Duo 双因素身份验证

关于此任务：

可以将 Duo RADIUS 服务器配置为主要身份验证源。此方法使用 Duo RADIUS 身份验证代理。（您不能通过 LDAPS 使用与 Duo 云服务的直接连接。）

有关配置 Duo 的详细步骤，请参阅 https://duo.com/docs/cisco-firepower。

然后，配置 Duo，以转发定向到代理服务器的身份验证请求，并将另一台 RADIUS 服务器或 AD 服务器用作第一个身份验证因素，将 Duo 云服务用作第二个因素。

使用此方法时，用户必须使用 Duo 云和 Web 服务器以及关联的 RADIUS 服务器上配置的用户名进行身份验证。用户必须输入 RADIUS 服务器中配置的密码，后跟以下 Duo 代码之一：

- **Duo-passcode**。例如，*my-password*,123456。
- **push**。例如，*my-password*,**push**。使用 push 告知 Duo 向用户应该已经安装并注册的 Duo 移动应用发送推送身份验证。
- **sms**。例如，*my-password*,**sms**。使用 **sms** 告知 Duo 向用户的移动设备发送包含新一批密码的 SMS 消息。使用 **sms** 时，用户的身份验证尝试将会失败。用户必须重新进行身份验证，并输入新密码作为辅助因素。
- **phone**。例如，*my-password*,**phone**。使用**电话**通过电话呼叫来进行身份验证。

有关登录选项及示例的详细信息，请参阅https://guide.duo.com/anyconnect。

准备工作：

在 上使用 Duo 身份验证代理配置双因素身份验证之前，确保完成以下配置：

- 在开始部署 Duo 之前，为远程接入 VPN 用户配置有效的主身份验证（RADIUS 或 AD）。
- 在网络中的 Windows 或 Linux 计算机上安装 Duo 代理服务，以将 Duo 与 Cisco Secure Firewall Threat Defense远程接入 VPN 集成。此 Duo 代理服务器也可充当 RADIUS 服务器。

  从以下位置下载并安装最新的 Duo 身份验证代理：

  - **Windows**：https://dl.duosecurity.com/duoauthproxy-latest.exe
  - **Linux**：https://dl.duosecurity.com/duoauthproxy-latest-src.tgz
  - 在 https://duo.com/docs/checksums#duo-authentication-proxy 上验证校验和。

- 配置 Duo 身份验证文件 `authproxy.cfg`。按照 https://duo.com/docs/cisco-firepower#configure-the-proxy 页面上的说明配置身份验证配置设置。

  `authproxy.cfg` 配置文件必须包含 RADIUS 或 ISE 服务器、设备的详细信息、Duo 代理服务器详细信息、集成密钥、密钥以及 API 主机详细信息。

- 确保 `authproxy.cfg` 文件中具有正确的 API 主机信息。
- 在 **Duo 安全服务器** > **Duo 管理面板**> **应用** > **思科 ONE RADIUS VPN** 下，在新安装的 Duo 代理服务器中配置其他所需设置，例如辅助身份验证因素。

表 *11:* 过程

	相应操作	更多信息
步骤 1	登录 Cisco Secure Firewall Management Center Web 界面。	
步骤 2	创建 RADIUS 服务器组。	RADIUS 服务器组选项
步骤 3	在新 RADIUS 服务器组中创建 RADIUS 服务器对象，将 Duo 代理服务器作为主机，超时时间为 60 秒或更长。	RADIUS 服务器选项 **注释** 对于双因素身份验证，也要确保在 安全客户端配置文件 配置文件 XML 文件中将超时更新为 60 秒或更长。
步骤 4	使用向导配置新的远程接入 VPN 策略，或者编辑现有的远程接入 VPN 策略。	创建新的远程访问 VPN 策略， 第 12 页
步骤 5	选择 RADIUS 作为身份验证服务器，然后选择使用 Duo 代理服务器创建的 RADIUS 服务器组作为身份验证服务器。	配置远程访问 VPN 的 AAA 设置， 第 24 页

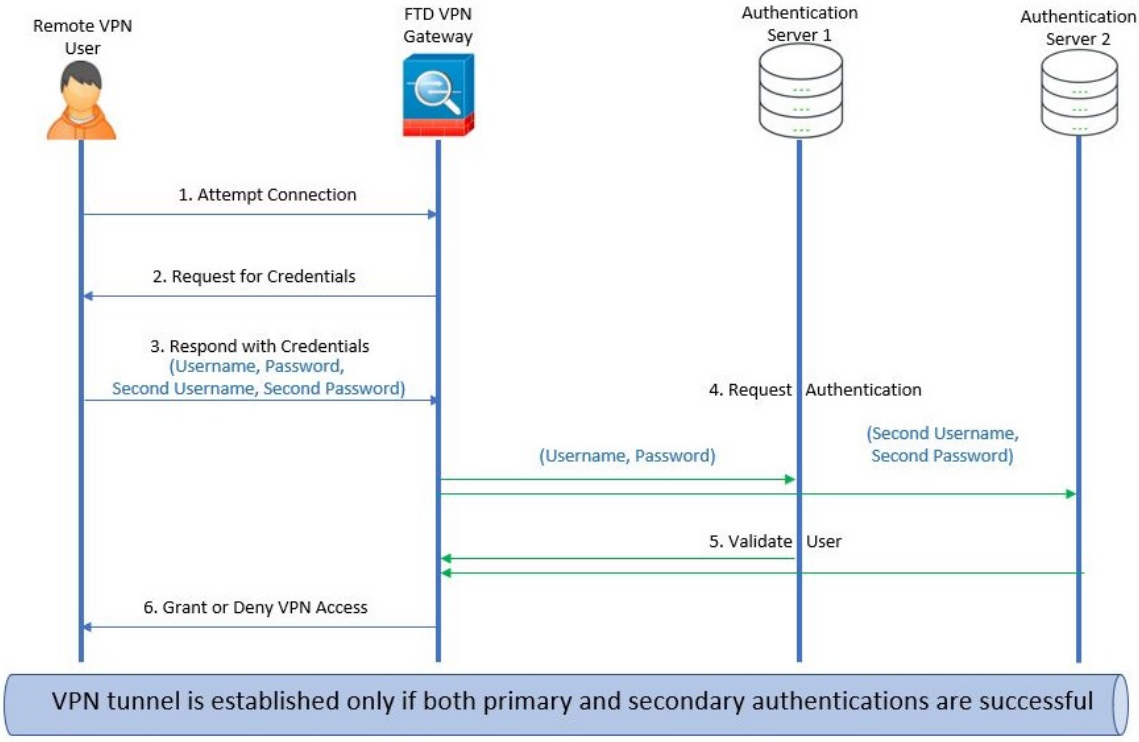
	相应操作	更多信息
步骤 7	部署配置更改。	部署配置更改

辅助身份验证

Cisco Secure Firewall Threat Defense 中的辅助身份验证或双重身份验证，通过使用两个不同的身份验证服务器，为远程访问 VPN 连接额外添加了一层安全性。启用辅助身份验证后， 安全客户端 VPN 用户必须提供两组凭证才能登录 VPN 网关。

Cisco Secure Firewall Threat Defense 远程访问 VPN 支持仅 AAA 和客户端证书以及 AAA 身份验证方法的辅助身份验证。

图 *2:* 远程访问 *VPN* 辅助或双重身份验证



相关主题

配置远程访问 VPN 辅助身份验证 ，第 90 页

配置远程访问 VPN 辅助身份验证

当远程访问VPN身份验证配置为同时使用客户端证书和身份验证服务器时，使用客户端证书验证和 AAA 服务器完成 VPN 客户端身份验证。

开始之前

- 配置两个身份验证(AAA)服务器-主要和辅助身份验证服务器，以及所需的身份证书。身份验证服务器可以是 RADIUS 服务器以及 AD 或 LDAP 领域。
- 确保可以通过 Cisco Secure Firewall Threat Defense 设备访问 AAA 服务器，以使远程访问访问 VPN 配置生效。配置路由（在 **设备 > 设备管理 > 编辑设备 > 路由**）以确保 AAA 服务器连接：

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程访问**。

步骤 2 在远程访问策略，然后点击 **编辑**；或者点击 **添加** 以创建新的远程访问 VPN 策略。

步骤 3 对于新的远程访问VPN策略，请在选择连接配置文件设置时配置身份验证。对于现有配置，选择包含客户端配置文件的连接配置文件，然后点击**编辑**。

步骤 4 点击 **AAA** > **身份验证方式**， **AAA** 或 **客户端证书和 AAA**。

- 何时选择以下**身份验证方法**：

  客户端证书和 AAA-使用客户端证书和 AAA 服务器已完成身份验证。

  - **AAA** - 如果选择 **RADIUS** 作为**身份验证服务器**，则授权服务器默认也采用此选择。从下拉列表中选择**记帐服务器**。每当从“身份验证服务器”下拉列表中选择 **AD** 和 **LDAP** 时，都必须手动分别选择**授权服务器**和**记帐服务器**。
  - 无论选择哪种身份验证方法，选择或取消选择**仅当用户位于授权数据库中时才允许连接**。

- **使用辅助身份验证** - 除主身份验证之外，还配置了辅助身份验证，以便为 VPN 会话提供额外的安全保护。辅助身份验证是仅适用于**仅 AAA** 和**客户端证书和 AAA** 身份验证方法。

  辅助身份验证是一项可选功能，该功能要求 VPN 用户在 安全客户端 登录屏幕上输入两组用户名和密码。您还可以配置为从身份验证服务器或客户端证书预填充辅助用户名。仅当主身份验证和辅助身份验证均成功时，才会授予远程访问VPN身份验证。如果任何一个身份验证服务器无法访问或一个身份验证失败，VPN 身份验证将被拒绝。

  必须在配置辅助身份验证前，为辅助用户名和密码配置辅助身份验证服务器组（AAA服务器）。例如，可以将主身份验证服务器设置为 LDAP 或 Active Directory 领域，将辅助身份验证设置为 RADIUS 服务器。

  注释
  默认情况下，无需辅助身份验证。

  身份验证服务器 - 为 VPN 用户提供辅助用户名和密码的辅助身份验证服务器。

  选择 **辅助身份验证的用户名**以下的选项：

  - **提示**： 在登录 VPN 网关时，提示用户输入用户名和密码。
  - **使用主身份验证用户名**： 用户名从主身份验证服务器获取，用于主身份验证和辅助身份验证；必须输入两个密码。

- **映射客户端证书中的用户名：** 预填充客户端证书中的辅助用户名。
  - 如果选择**映射特定字段**选项，其中包括来自客户端证书的用户名。则**主**和**辅助**字段将显示默认值：**CN (公用名称)** 和 **OU (组织单位)**。如果选择**使用整个 DN（可分辨名称）作为用户名**选项，系统将自动检索用户身份。

    有关主字段和辅助字段映射的详细信息，请参阅**身份验证方法**说明。
  - **在用户登录窗口预填证书中的用户名 (Prefill username from certificate on user login window)：** 用户通过 安全客户端 VPN 客户端连接时，预填充客户端证书中的辅助用户名。
    - **在登录窗口隐藏用户名：** 辅助用户名是从客户端证书预填充的，但对用户隐藏，确保用户不会修改预填充的用户名。

- **使用 VPN 会话的辅助用户名：** 辅助用户名用于在 VPN 会话期间报告用户活动。

有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 24 页。

相关主题

配置连接配置文件设置，第 22 页

使用 SAML 2.0 的单点登录身份验证

关于 SAML 单点登录身份验证

安全断言标记语言（SAML）是一种开放标准，用于通过用户在其他情景中的会话将其登录到应用中。当用户登录其 Active Directory（AD）域或内联网时，组织已经知道用户的身份。他们使用此身份信息通过使用 SAML 将用户登录到其他应用，例如基于 Web 的应用。单个应用无需存储凭证，用户无需记住和管理单个应用的不同凭证集。SAML 单点登录 (SSO) 通过将用户的身份从一个位置（身份提供程序）传输到另一个位置（服务提供商）来工作。

通过 Cisco Secure Firewall Threat Defense 进行 SAML 单点登录

Cisco Secure Firewall Threat Defense 设备支持使用 安全客户端对远程访问 VPN 连接进行 SAML 2.0 单点登录 (SSO) 身份验证。您需要执行以下操作，才能在 Cisco Secure Firewall Threat Defense上配置 SAML 2.0 SSO：

- **身份提供程序 (IdP)** - Duo Access Gateway 充当身份提供程序以执行用户身份验证并发出断言。
- **服务提供商 (SP)** - 设备充当服务提供商并从身份提供商获取身份验证断言。
- **VPN 客户端** - 安全客户端会通过嵌入式浏览器来执行 SAML 2.0 身份验证。

SAML 2.0 的准则和限制

- 支持以下 SAML 身份验证签名：

- 包含 RSA 和 HMAC 的 SHA1
- 包含 RSA 和 HMAC 的 SHA2

- 支持 SAML 2.0 重定向-POST 绑定，所有 SAML IdP 也支持此功能。
- 仅用作 SAML SP。在网关模式或对等模式下，它不能用作身份提供程序。
- 如果您的身份策略与与 SAML 域匹配的 AD 领域相关联，则可以对通过 SAML 身份验证的用户实施访问策略。但是，它不适用于 Azure AD SAML，因为它需要从 Azure AD 的租户 ID 到威胁防御设备上关联领域 ID 的额外映射。
- 不支持在 DAP 评估中使用 SAML 身份验证属性（类似于从 AAA 服务器发送的 RADIUS 身份验证响应中的 RADIUS 属性）。 支持对 DAP 策略启用 SAML 的组策略；但是，在使用 SAML 身份验证时，您无法检查用户名属性，因为用户名属性已被 SAML 身份提供程序屏蔽。
- 管理员需要确保 与 SAML IdP 之间的时钟同步，从而正确处理身份验证断言并确保正确的超时行为。
- 管理员有责任在 和 IdP 上维护有效的签名证书，并考虑以下因素：
  - 在 上配置 IdP 时，必须配置 IdP 签名证书。
  - 不会对从 IdP 接收的签名证书执行吊销检查。
- SAML 断言中有 NotBefore 和 NotOnOrAfter 条件。 SAML 配置的超时与这两个条件如下交互：
  - 如果 NotBefore 与超时之和早于 NotOnOrAfter，则超时将覆盖 NotOnOrAfter。
  - 如果 NotBefore + 超时晚于 NotOnOrAfter，则 NotOnOrAfter 生效。
  - 如果不存在 NotBefore 属性， 将拒绝登录请求。如果不存在 NotOnOrAfter 属性且未设置 SAML 超时， 将拒绝登录请求。
- 不适用于使用内部 SAML 的部署中的 Duo，由于在双因素身份验证（推送、代码、密码）的质询/响应期间发生 FQDN 更改，这会强制到客户端代理的 进行身份验证。
- 将 SAML 与 安全客户端配合使用时，还需遵守这些准则：
  - 在嵌入式浏览器中不允许不受信任的服务器证书。
  - CLI 或 SBL 型号中不支持嵌入式浏览器 SAML 集成。
  - 在网络浏览器中建立的 SAML 身份验证不会与 安全客户端 共享，反之亦然。
  - 根据具体配置，在使用嵌入式浏览器连接到前端时，会使用各种不同的方法。例如，尽管安全客户端 相比于 IPv6 连接更喜欢 IPv4 连接，但嵌入式浏览器可能更喜欢 IPv6，或反之亦然。同样，在尝试代理和收到失败后， 安全客户端 可能会回退到没有代理状态，而嵌入式浏览器在尝试代理并收到失败后可能会停止导航。
  - 为了使用 SAML 功能，必须使您的 网络时间协议 (NTP) 服务器与 IdP NTP 服务器同步。
  - 使用内部 IdP 登录后，您将无法访问包含 SSO 的内部服务器。

- SAML IdP NameID 属性确定用户的用户名，并且用于授权、记帐和 VPN 会话数据库。

- SAML 不支持登录前启动 (SBL)。
- 不支持通过 SAML 断言接收多个属性。
- 防火墙使用身份提供商实体 ID 作为在 防火墙管理中心 中创建的单点登录服务器对象（**对象 > 对象管理 > AAA 服务器 > 单点登录服务器**）中的 SAML 对象名称。因此，您不能在单个防火墙上使用具有相同身份提供商实体 ID 的多个 SAML 对象。

配置 SAML 单点登录身份验证

开始之前

在使用 远程访问 VPN 配置 SAML 单点登录之前，请确保已完成以下操作：

- 使用 Duo 创建帐户。
- 下载并安装 Duo Access Gateway。
- 从您的 SAML身份提供程序（Duo）获取以下信息。
  - 身份提供程序实体 ID URL
  - 登录 URL
  - 注销 URL
  - 标识提供程序证书
- 创建 SAML 单点登录服务器对象。有关详细信息，请参阅添加单点登录服务器。

注释 在使用远程访问 VPN 策略向导创建一个新的策略时，您可以在**连接配置文件 (Connection Profile)** 设置中创建一个单点登录服务器对象。

过程

步骤 1 选择**设备** > **VPN** > **远程访问**。

步骤 2 点击要为其配置 SAML 身份验证的远程访问 VPN 策略旁边的**编辑 (Edit)**。如果要创建新策略，请点击**添加 (Add)**。

步骤 3 点击要修改的连接配置文件上的**编辑 (Edit)**。

步骤 4 选择 **AAA** 设置，然后从**身份验证方式 (Authentication Method)** 下拉列表中选择 **SAML**。

步骤 5 选择所需的 SAML 单点登录服务器作为**身份验证服务器**。

步骤 6 配置远程访问 VPN 所需的设置。

步骤 7 在您的 设备上保存和部署远程访问 VPN 策略。

相关主题

配置远程访问 VPN 的 AAA 设置，第 24 页

配置 SAML 授权

关于 SAML 授权

SAML 授权支持在 AAA 和动态访问策略 (DAP) 框架内的 SAML 断言中提供的用户属性。您可以在身份提供程序上将 SAML 断言属性配置为名称-值对，然后它们会被解析为字符串。接收的属性可供 DAP 使用，以便在 DAP 记录中定义选择条件时使用这些属性。SAML 断言 *cisco_group_policy* 会被用于确定要应用于 VPN 会话的组策略。

动态访问策略属性表示

在 DAP 表中，DAP 属性按以下格式表示：

```
aaa.saml.name = "value”
```

示例，*aaa.saml.department = ”finance"*

此属性可用于 DAP 选择，如下所示：

```
<attr>
<name>aaa.saml.department</name>
<value>finance</value>
<operation>EQ</operation>
</attr>
```

多值属性

DAP 中也支持多值属性，并且 DAP 表已建立索引：

```
aaa.saml.name.1 = "value”
aaa.saml.name.2 = "value"
```

Active Directory memberOf 属性

Active Directory (AD) memberOf 属性接受与通过 LDAP 查询的处理方式一致的特殊处理。

组名称由 DN 的 CN 属性来表示。

从授权服务器接收的属性示例：

```
memberOf = "CN=FTD-VPN-Group,OU=Users,OU=TechspotUsers,DC=techspot,DC=us"
 memberOf = "CN=Domain Admins,OU=Users,DC=techspot,DC=us”
```

动态访问策略属性：

```
aaa.saml.memberOf.1 = "FTD-VPN-Group”
aaa.saml.memberOf.2 = "Domain Admins"
```

cisco_group_policy 属性的解释

组策略可以通过SAML断言属性来指定。当 接收到属性“cisco_group_policy”时，相应的值会被用于选择连接组策略

配置 SAML 授权

开始之前

确保您已在服务器（例如 DUO）上配置单点登录，并完成所需的身份提供程序 (IdP) 和服务提供商 (SP) 设置。

有关详细信息，请参阅使用 SAML 2.0 的单点登录身份验证 ， 第 92 页。

过程

步骤 1 配置单点登录服务器对象（如果尚未配置）。

a) 依次选择 **对象** > **对象管理** > **AAA服务器** > **单点登录服务器**。
b) 点击**添加单点登录服务器 (Add Single Sign-on Server)**。
c) 输入单点登录服务器详细信息，然后点击 **保存**。

有关详细信息，请参阅添加单点登录服务器。

步骤 2 在远程接入 VPN 连接配置文件中配置 SAML 身份验证 。

a) 选择 **设备** > **远程访问**。
b) 点击要为其配置 SAML 授权或创建新策略的远程访问 VPN 策略上的 **编辑** 。
c) 编辑所需的连接配置文件，然后选择 **AAA**。
d) 从 **身份验证服务器** 下拉列表中选择单点登录服务器对象。
e) 保存远程访问 VPN 配置。

步骤 3 匹配 DAP 策略中的 SAML 条件。

a) 选择 **设备** > **Dynamic Access Policy**。
b) 创建新的 DAP 或编辑现有组。
c) 创建 DAP 记录或编辑现有记录。
d) 点击**AAA 条件 (AAA Criteria)** > **SAML 条件 (SAML Criteria)** > 添加 **SAML 条件 (Add SAML Criteria)**。
e) 根据 SSO 服务器返回的 SAML 断言来创建 SAML 条件。

步骤 4 部署远程访问 VPN 配置。

相关主题

配置连接配置文件设置 ， 第 22 页
组策略对象

高级 Secure Client 配置

在 上配置 Secure Client 模块

Secure Client 可以与各种 Cisco 终端安全解决方案集成，并使用不同的 Secure Client 模块提供增强的安全性。

您可以使用托管前端 向终端分发和管理 Secure Client 模块。当用户连接到 时，它会在终端上下载并安装 Secure Client 和所需的模块。

在版本 6.7 及更高版本中，您可以使用由 防火墙管理中心管理的前端 将 Secure Client 模块分发到终端并进行管理。然后，这些模块与相应的 Cisco 终端安全解决方案集成。

在版本 6.4 到 6.6 中，您可以使用 FlexConfig 在 上启用这些模块和配置文件。有关详细信息，请参阅 使用 FlexConfig 配置 AnyConnect 模块和配置文件。

优势

如果使用 向终端分发和管理 Secure Client 模块，则可以轻松执行以下任务：

- 分发和管理每个终端上的 Secure Client 模块和配置文件。
- 在每个终端上升级 Secure Client 。

Secure Client 模块类型

AMP 启用程序

使用此模块在终端上部署 Cisco Secure Endpoint。该模块将 Cisco Secure Endpoint 从企业内本地托管的服务器推送到终端。此模块提供了额外的安全代理，可以检测网络中可能发生的潜在恶意软件威胁、删除这些威胁并保护企业免受危害。

在 Cisco Secure Client 5.0 中，AMP 启用程序仅适用于 macOS。适用于 Windows 的 Cisco Secure Client 提供与 Cisco Secure Endpoint 的完全集成。

ISE 终端安全评估

使用此模块通过 Cisco Identity Services Engine (ISE) 执行终端安全状态检查，例如防病毒软件、反间谍软件、操作系统等，并评估终端的合规性。ISE提供下一代身份和访问控制策略。ISE终端安全评估可执行客户端评估。客户端从头端获得终端安全评估要求策略、执行终端安全评估数据收集、将结果与策略进行比较，并将评估结果发送回头端。

网络可视性

使用此模块通过网络可视性模块监控终端应用的使用情况。您可以发现潜在的行为异常并做出明智的网络设计决策。这可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。可将使用情况数据与 Cisco Stealthwatch 等 NetFlow 分析工具共享。

Umbrella 漫游安全

使用此模块通过 Cisco Umbrella 漫游安全服务实现 DNS 层安全。此外，Cisco Umbrella 订用还将提供内容过滤、多重策略、稳健性报告、Active Directory 集成等更多功能。

网络安全

使用此模块启用由 Cisco Talos 提供支持的 Cisco Secure Web Appliance (SWA)。此模块会通过阻止有风险的网站和测试未知网站，然后再允许用户访问这些网站，从而为终端提供保护。它可以通过本地 WSA 或基于云的 Cisco Cloud Web Security 部署 Web 安全。此模块不是版本 4.5 和 Secure Client 5.0 的 AnyConnect 软件包的一部分。

网络访问管理器

此模块提供安全的第 2 层网络，并执行设备身份验证以访问有线和无线网络。网络访问管理器对安全访问所需的用户及设备身份和网络访问协议进行管理。

网络访问管理器在 macOS 或 Linux 上不支持。

登录前开始

登录前启动 (SBL) 允许用户在登录 Windows 之前建立与企业基础设施的 VPN 连接。安装 SBL 模块后，必须在 Secure Client VPN 配置文件中启用 SBL，并将其添加到远程接入 VPN 组策略。

议价授权请求工具 (DART)

诊断和报告工具 (DART) 会整理系统日志和其他诊断信息，以排除 AnyConnect 安装和连接问题。您可以将此数据发送到 Cisco TAC 进行故障排除。

默认情况下，6.7 及更高版本的新 RA VPN 组策略中未启用 DART。在 6.6 及更早版本中，默认情况下启用 DART。

反馈

客户体验反馈 (CEF) 模块提供有关您使用和启用的功能和模块的信息。此信息将让我们了解用户体验，从而让 Cisco 继续改善 Cisco Secure Client的质量、可靠性、性能和用户体验。 Secure Client 不会将反馈模块下载到终端。反馈数据将发送到 Cisco 反馈服务器。

配置 Secure Client 模块的前提条件

- 根据您要使用的模块配置关联的产品。
- 从 Cisco 软件下载中心 将以下 Secure Client相关软件包下载到本地主机。
  - 适用于所需平台的 Cisco Secure Client 前端部署包。

    此软件包适用于前端，包含所有 Secure Client 模块。对于 Windows，文件名为 cisco-secure-client-win-5.0.03076-webdeploy-k9.pkg。
  - 配置文件编辑器：为需要配置文件的模块创建配置文件。

Secure Client 需要某些模块的 Secure Client 配置文件。配置文件包含用于启用模块和连接到相应安全服务的配置。配置文件编辑器仅支持 Windows。

如果模块需要客户端配置文件，请参阅以下列表：

Secure Client 模块	需要客户端配置文件
AMP 启用程序	是
ISE 终端安全评估	是
网络访问管理器	是
网络可视性模块	是
Umbrella 漫游安全模块	是
反馈	是
网络安全	是
诊断和报告工具 (DART)	否
登录前开始	否

- 许可
  - 您需要以下安全客户端许可证之一： Secure Client Premier、 Secure Client Advantage或 仅限 Secure Client VPN
  - 您的 防火墙管理中心 基础版 许可证必须允许出口控制功能。

    依次选择 **系统 > 许可证 > 智能许可证** 以在管理中心验证此功能。

配置 Secure Client 模块的准则

- AnyConnect 4.8 及更高版本以及 Secure Client 5.0 支持所有 Secure Client 模块。
- 不同的模块支持具有不同文件扩展名的配置文件。下表列出了模块及其配置文件支持的文件扩展名：

表 *12:* 配置文件支持的文件扩展名

模块	文件扩展名
AMP 启用程序	*.xml、*.asp
反馈	*.xml
ISE 终端安全评估	*.xml、*.isp
网络访问管理器	*.xml、*.nsp

模块	文件扩展名
网络可视性	*.xml、*.nvmsp
Umbrella 漫游安全	*.xml、*.json
网络安全	*.xml、*.wsp、*.wso

- 每个客户端模块只能添加一个条目。您可以编辑或删除模块的条目。
- 如果您计划在 Windows 操作系统上使用 ISE 终端安全评估和网络访问管理器模块，则必须在使用 ISE 终端安全评估模块之前安装网络访问管理器。
- 如果启用 Umbrella 漫游安全模块，请确保禁用 VPN 组策略中的分割隧道下的 **始终通过隧道发送 DNS 请求** 选项。
- 如果要使用 SBL，则必须在 Secure Client VPN 配置文件中启用 SBL。

使用 安装 Secure Client 模块

开始之前

确保您查看 配置 Secure Client 模块的前提条件，第 98 页 和 配置 Secure Client 模块的准则，第 99 页 主题。

过程

步骤 1 如果需要，管理员可为所需 Secure Client 模块创建配置文件。

步骤 2 管理员使用 防火墙管理中心 来：

a) 配置模块并在远程接入 VPN 组策略中添加配置文件。

b) 在 上部署配置。

步骤 3 用户使用 Secure Client 启动 VPN 连接。

步骤 4 对用户进行身份验证。

步骤 5 Secure Client 检查更新。

步骤 6 在终端上分发 Secure Client 模块和配置文件。

下一步做什么

使用 Secure Client 模块配置远程接入 VPN 组策略，第 101 页。

使用 Secure Client 模块配置远程接入 VPN 组策略

要使用由 防火墙管理中心管理的 安装和更新终端上的 Secure Client 模块，必须使用模块配置更新远程访问 VPN 组策略 Secure Client 。

开始之前

确保您已在 防火墙管理中心中配置远程接入 VPN 策略。

过程

步骤 1 选择 **设备 > 远程访问**。

步骤 2 选择远程访问 VPN 策略，然后点击**编辑 (Edit)**。

步骤 3 选择一个连接配置文件 ，然后点击**编辑 (Edit)**。

步骤 4 点击**编辑组策略 (Edit Group Policy)**。

步骤 5 点击 **安全客户端** 选项卡。

步骤 6 点击 **客户端模块**。

步骤 7 点击 **+**。

步骤 8 从**客户端模块 (Client Module)** 下拉列表中选择一个模块。

步骤 9 从 **要下载的配置文件** 下拉列表中选择模块的配置文件，或点击 **+** 添加配置文件。

步骤 10 选中 **启用模块下载** 复选框以在终端上下载模块。

步骤 11 点击**添加 (Add)**。

步骤 12 如果要添加更多模块，请重复步骤 7 至 11。

步骤 13 点击**保存**。

下一步做什么

1. 在威胁防御上部署配置。
2. 启动 Secure Client，选择 VPN 配置文件，然后连接到 VPN。 Secure Client 在其上安装已配置的模块。
3. 确认配置。有关详细信息，请参阅验证 Secure Client 模块配置 ， 第 101 页。

验证 Secure Client 模块配置

在

在 上使用以下命令查看配置文件和 Secure Client 模块配置：

- **show disk0:**-查看配置文件及其配置。
- **show run webvpn** - 查看安全客户端配置的详细信息。

- **show run group-policy<ravpn_group_policy_name>** - 查看安全客户端的 RA VPN 组策略的详细信息。
- **show vpn-sessiondb anyconnect** - 查看活动安全客户端 VPN 会话的详细信息。

在终端上

1. 使用 Secure Client 与 建立 VPN 连接。
2. 验证已配置的模块是否已作为 Secure Client的一部分下载并安装。
3. 验证配置的配置文件（如果有）在 所有操作系统的配置文件位置中记录的位置是否可用。

在 防火墙管理中心

您可以使用远程访问 VPN 控制面板（**概述 > 远程访问 VPN**）监控 防火墙管理中心 上的远程接入 VPN 活动会话。您可以快速确定与用户会话相关的问题，同时缓解网络和用户的问题。

在移动设备上配置基于应用的（Per App VPN）远程访问 VPN

当您使用 Secure Client 从移动设备建立 VPN 连接时，所有流量（包括来自个人应用的流量）都通过 VPN 路由。

对于在 Android 或 iOS 上运行的移动设备，可以限制使用 VPN 隧道的应用。这种基于应用的远程访问 VPN 称为 Per App VPN。要使用 Per App VPN，您必须安装和配置第三方移动设备管理器 (MDM) 应用。在 MDM 中，您要定义可通过 VPN 隧道使用的已批准应用的列表。您可以在 头端启用 Per App VPN，以便您的 MDM 可以在移动设备上应用您的策略。

优势

将远程访问 VPN 限制为已批准的应用的好处包括：

- 性能 - 限制企业网络上的 VPN 流量并释放 VPN 前端的资源。
- 保护 - 保护企业 VPN 隧道免受移动设备上未经批准的恶意应用的影响。

配置 Per App VPN 隧道的前提条件和许可

前提条件

- 安装和配置第三方移动设备管理器 (MDM)。

  您必须在 MDM 本身而非 头端设备中配置允许在 VPN 中使用的应用。

- 您可以从 Cisco 软件下载中心下载 Cisco AnyConnect Enterprise Application 选择器。

  您需要此工具来定义 Per App VPN 策略。

许可

- Secure Client Premier，或 Secure Client Advantage。
- 基础版许可证必须允许出口控制功能。

  要在 防火墙管理中心中验证此功能，请依次选择 **系统 > 许可证 > 智能许可证**。

确定移动应用的应用 ID

在配置 前端以允许来自移动设备的基于应用的 VPN 之前，您必须确定应在隧道中允许哪些应用。

我们强烈建议您在用户移动设备上的移动设备管理器 (MDM) 中配置 Per-App 策略。这样可以简化前端配置。如果您决定要在前端配置允许的应用列表，则必须确定每种类型的终端上每个应用的应用 ID。

应用 ID（在 iOS 中称为捆绑包 ID）是反向 DNS 名称。您可以使用星号作为通配符。例如，*.* 表示所有应用，com.cisco.* 表示所有 Cisco 应用。

要确定应用 ID，请执行以下操作：

- **Android**-在网络浏览器中转至 Google Play，然后选择应用类别。点击要允许的应用（或悬停在该应用上），然后查看 URL。应用 ID 位于 URL 中的 **id=** 参数上。例如，Facebook Messenger 的 URL 如下，因此应用 ID 是 com.facebook.orca。

  https://play.google.com/store/apps/details?id=com.facebook.orca

  对于通过 Google Play 无法获得的应用（例如您自己的应用），下载一个程序包名称查看器应用以提取该应用 ID。Cisco 不为任何可用的应用背书，但这些应用之一应能够满足您的需求。

- **iOS**-没有直接的方法来获取捆绑包 ID。以下是一种查找方法：

  1. 使用桌面 web 浏览器（例如 Chrome）搜索应用名称。
  2. 在搜索结果中，查找从 Apple App Store 下载该应用的链接。例如，Facebook Messager 将类似于：

     https://apps.apple.com/us/app/messenger/id454638411
  3. 复制 **id** 字符串后面的数字。在本例中，即 **454638411**。
  4. 打开一个新的浏览器窗口，然后将该数字添加到以下 URL 的末尾：

     https://itunes.apple.com/lookup?id=

     在本例中，即： https://itunes.apple.com/lookup?id=454638411
  5. 系统将提示您下载文本文件，该文件通常命名为 1.txt。下载文件。
  6. 在文本编辑器（例如写字板）中打开文件，然后搜索 bundleId。例如：

     "bundleId":"com.facebook.Messenger",

     在本例中，捆绑包 ID 为 com.facebook.Messenger。以此作为应用 ID。

拥有应用 ID 列表后，您可以如所解释配置策略。

配置基于应用的 VPN 隧道

安装并配置 MDM 软件后，您可以在 头端设备上启用 Per App VPN。在头端启用后，您的 MDM 软件将控制通过 VPN 连接到企业网络的应用。

开始之前

- 确保您已在 防火墙管理中心中远程访问 VPN 策略。
- 使用 MDM 配置 Per App VPN，并将每台设备注册到 MDM 服务器。
- 下载 Cisco AnyConnect 企业应用选择器。

过程

步骤 1 使用 Cisco AnyConnect 企业应用选择器定义 Per App VPN 策略。

我们建议您创建一个简单的 **全部允许** 策略，并在 MDM 中定义允许的应用。但是，您可以从头端指定要允许和控制列表的应用列表。如果要包括特定应用，请使用唯一名称和应用的应用 ID 为每个应用创建单独的规则。有关获取应用 ID 的详细信息，请参阅 确定移动应用的应用 ID。

要使用 AnyConnect 企业应用选择器创建支持 Android 和 iOS 平台的 **全部允许** 策略，请执行以下操作：

a) 从下拉列表中选择 **Android** 作为平台类型，并配置以下选项：

- **友好名称 (Friendly Name)** - 输入策略的名称。例如，Allow_All。
- **App ID**-输入 *.* 以匹配所有可能的应用。
- 其他选项保持不变。

b) 从下拉列表中选择 **iOS** 作为平台类型，并配置以下选项：

- **友好名称 (Friendly Name)** - 输入策略的名称。例如，Allow_All。
- **App ID**-输入 *.* 以匹配所有可能的应用。
- 其他选项保持不变。

c) 依次选择 **策略 > 查看策略** 以获取策略的 base64 编码字符串。

此字符串包含允许 查看策略的加密 XML 文件。复制此值。在 上配置 Per App VPN 时需要此字符串。

步骤 2 使用 防火墙管理中心 在 头端设备上启用 Per App。

a) 选择 **设备 > 远程访问**。
b) 选择远程访问 VPN 策略，然后点击**编辑 (Edit)**。
c) 选择一个连接配置文件 ，然后点击**编辑 (Edit)**。
d) 点击**编辑组策略 (Edit Group Policy)**。

e) 点击 **安全客户端** 选项卡。
f) 点击 **自定义属性**，然后点击 **+**。
g) 从 **安全客户端 属性** 下拉列表中选择 **Per App VPN** 。
h) 从 **自定义属性对象** 下拉列表中选择对象，或点击 **+** 添加对象。

为 Per App VPN 添加新的自定义属性对象时，请输入 Cisco AnyConnect 企业应用选择器中的名称、说明和 base64 编码策略字符串。

i) 点击**保存**。
j) 点击 **添加**，然后点击 **保存**。

步骤 3 在 防火墙管理中心上部署更改。

下一步做什么

1. 启动 Secure Client，选择 VPN 配置文件，然后连接到 VPN。
2. 确认配置。有关详细信息，请参阅验证每个应用配置，第 105 页。

验证每个应用配置

在

在 上使用以下命令查看 Per App 配置：

- **show run webvpn**
- **show run group-policy<ravpn_group_policy_name>**
- **show run anyconnect-custom-data**

在终端上

终端与 建立 VPN 连接后：

1. 点击视图 **统计信息** 图标 Secure Client。
2. **隧道模式 (Tunnel Mode)** 将是“应用隧道”(Application Tunnel)，而不是“隧道所有流量”(Tunnel All Traffic)。
3. **隧道应用 (Tunneled Apps)** 将列出您在 MDM 中启用隧道的应用。

远程访问 VPN 示例

如何限制每个用户的 安全客户端 带宽

本节介绍如何限制 VPN 用户使用 Secure Client 到 Cisco Secure Firewall Threat Defense 远程访问 VPN 网关连接时消耗的最大带宽。您可以通过使用 策略中的服务质量（QoS）限制最大带宽，以确保单个用户或组或多个用户不会接管整个资源。通过此配置，您可以优先处理关键流量，防止带宽占用和管理网络。如果当流量超出最大速率， 会丢弃超额流量。

步骤	相应操作	更多信息
1	创建和设置领域。	创建 LDAP 领域或 Active Directory 领域和领域目录
2	为新创建的领域中可用的用户或组创建 QoS 策略和 QoS 规则。	• 请参阅 创建 QoS 策略 以创建 QoS 策略。 • 请参阅 配置 QoS 规则以创建 QoS 规则。
3	配置远程访问 VPN 策略，并选择新创建的领域进行用户身份验证。	创建新的远程访问 VPN 策略， 第 12 页
4	部署远程访问 VPN 策略。	部署配置更改

如何对基于用户 ID 的访问控制规则使用 VPN 身份

步骤	相应操作	更多信息
1	创建和设置领域。	创建 LDAP 领域或 Active Directory 领域和领域目录。
2	创建身份策略并添加身份规则。	• 请参阅 创建身份策略 以创建身份策略。 • 请参阅 创建身份规则 以创建身份规则。
3	将身份策略与访问控制策略相关联。	将其他策略与访问控制相关联
4	配置远程访问 VPN 策略，并选择新创建的领域进行用户身份验证。	创建新的远程访问 VPN 策略， 第 12 页
5	部署远程访问 VPN 策略。	部署配置更改

配置多证书身份验证

基于多证书的身份验证

基于多证书的身份验证允许 验证计算机或设备证书。可以在远程接入 VPN 连接配置文件中为基于证书的身份验证启用多个证书。它可以与 AAA 身份验证结合使用。远程接入 VPN 连接配置文件中的多证书选项允许通过证书同时对计算机和用户进行证书身份验证。除了对用户的身份证书进行身份验证以允许 RA VPN 访问之外，这样还可以确保设备是公司颁发的设备。管理员可以选择是从计算机证书还是用户证书获取会话的用户名。

如果配置了多个基于证书的身份验证，则会从 VPN 客户端获取两个证书：

- **第一个证书 (First Certificate)** - 对终端进行身份验证的计算机证书。
- **第二个证书 (Second Certificate)** - 对 VPN 用户进行身份验证的用户证书。

有关 证书的详细信息，请参阅管理 证书。

限制

- 多证书身份验证当前会将证书数量限制为两个。
- 安全客户端 仅支持基于 RSA 的证书。
- 在 安全客户端 汇聚身份验证期间，仅支持基于 SHA256、SHA384 和 SHA512 的证书。
- 证书身份验证不能与 SAML 身份验证结合使用。

从证书预填充用户名

预填充用户名选项允许解析证书中的字段，并将其用于后续AAA身份验证（主和辅助）。在使用两个证书进行身份验证时，管理员可以为预填充功能选择应从中派生的用户名的证书。默认情况下，用于预填充的用户名检索自用户证书（从 安全客户端接收的第二个证书）。如果启用“仅证书”(Certificate Only) 身份验证方法，预填充的用户名会被用作 VPN 会话用户名。如果启用 AAA 和证书身份验证，VPN 会话用户名将基于预填充选项。

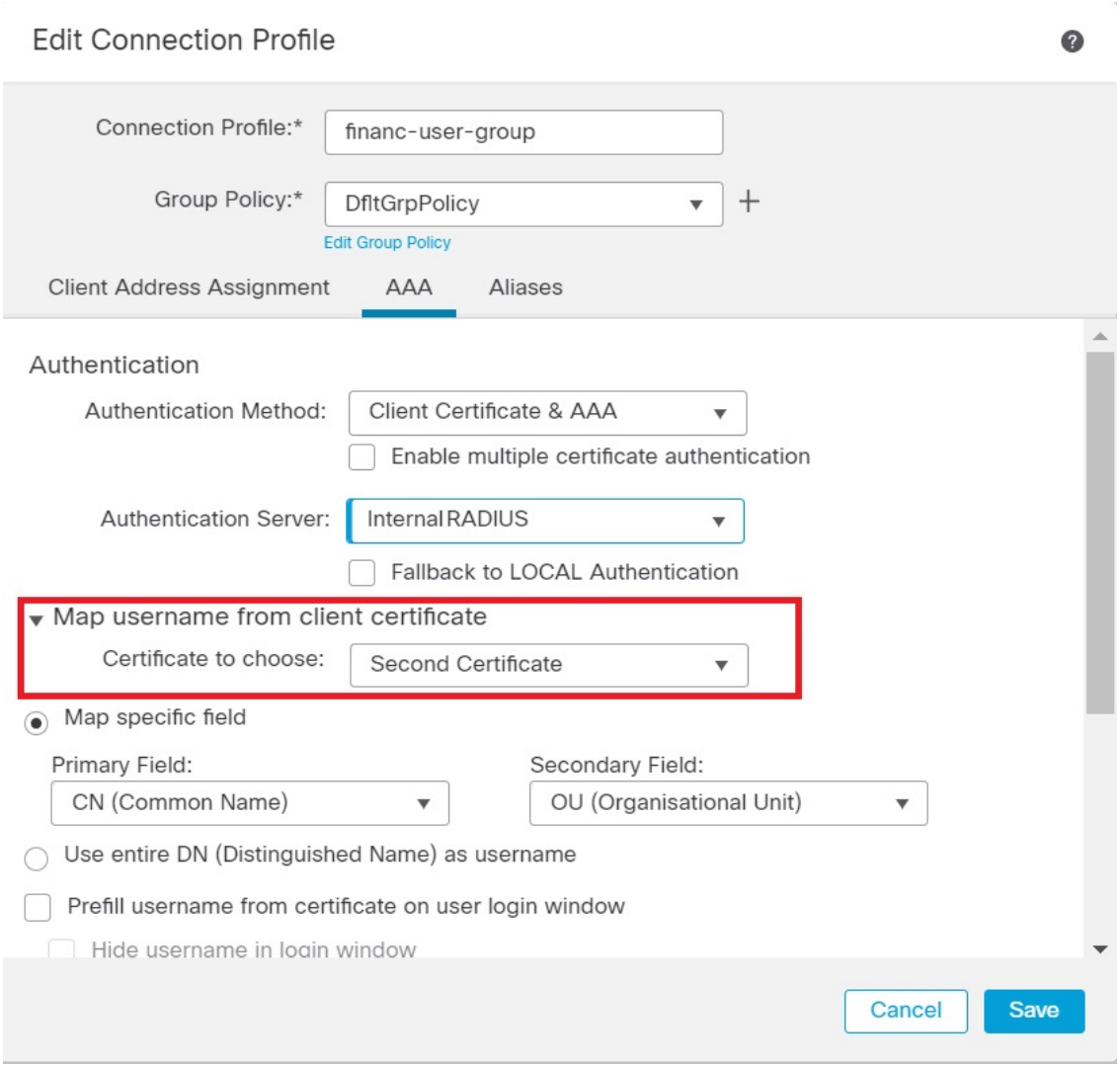
为远程接入 VPN 配置多证书身份验证

1. 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程接入**。
2. 编辑现有远程访问策略，或者创建新的策略并进行编辑。

   请参阅创建新的远程访问 VPN 策略， 第 12 页。
3. 选择连接配置文件以配置多证书身份验证，然后点击**编辑 (Edit)**。

   请参阅配置连接配置文件设置， 第 22 页。
4. 选择 **AAA**，然后选择**身份验证方法 (Authentication Method)**：

图 3:



- **仅客户端证书** - 使用客户端证书对用户进行身份验证。客户端证书必须在 VPN 客户端终端上配置。默认情况下，用户名分别派生自客户端证书字段 CN 和 OU。如果在客户端证书的其他字段中指定了用户名，请使用“主”(Primary) 和“辅助”(Secondary) 字段来映射适当的字段。
- **客户端证书和 AAA (Client Certificate & AAA)** - 使用 AAA 和客户端证书这两种身份验证类型来对用户进行身份验证。

5. 选择**启用多证书身份验证 (Enable multiple certificate authentication)**。
6. 选择**映射客户端证书中的用户名 (Map username from client certificate)**，然后从**可供选择的证书 (Certificate to choose)** 下拉列表中选择证书，以便从计算机证书或用户证书中选择 VPN 会话的用户名。
   - **第一个证书 (First Certificate)** - 映射计算机证书中的用户名。

- **第二个证书 (Second Certificate)** - 映射用户证书中的用户名，以便对 VPN 用户进行身份验证。

7. 配置所需的连接配置文件设置和远程访问 VPN 设置。
8. 保存连接配置文件和远程访问 VPN 策略。在 上部署远程访问 VPN 策略。

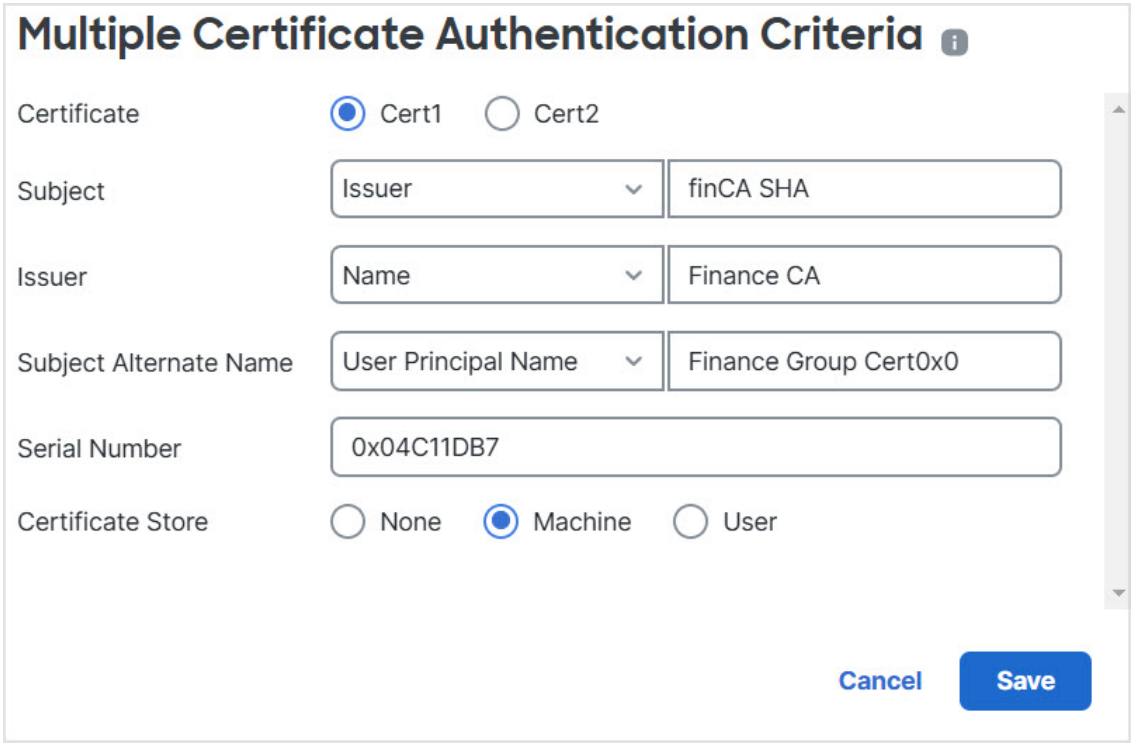
有关远程访问 VPN AAA 设置的信息，请参阅配置远程访问 VPN 的 AAA 设置，第 24 页。

DAP 中的证书配置

您也可以在 DAP 记录中配置证书条件属性。将在多证书身份验证期间从 VPN 客户端收到的用户和计算机证书加载到动态访问策略 (DAP)，以确保能够根据证书字段配置策略。您可以根据证书字段制定策略决策，该证书用于对该连接尝试进行身份验证。

1. 依次选择**设备 (Devices)** > **动态访问策略 (Dynamic Access Policy)**。
2. 编辑现有 DAP 策略或创建新的 DAP 策略，然后编辑该策略。
3. 选择现有的 DAP 记录，或创建新的 DAP 记录并对其进行编辑。
4. 选择**终端条件 (Endpoint Criteria)** > **证书 (Certificate)**。
5. 选择匹配条件**所有 (All)** 或**任何 (Any)**。
6. 点击**添加 (Add)** 以添加证书属性。

图 *4:*



7. 选择证书 **Cert1** 或 **Cert2**。
8. 选择**使用者 (Subject)** 并指定证书使用者值。
9. 选择**颁发机构 (Issuer)** 并指定证书颁发机构名称。
10. 选择**使用者替代名称 (Subject Alternate Name)**，并为使用者指定替代名称。
11. 指定**序列号 (Serial Number)**。
12. 选择**证书存储区 (Certificate Store)**：无、计算机或用户。

    此选项会添加一个条件来检查在终端上要从中挑选证书的存储区。
13. 点击**保存**以完成证书条件设置。

    配置所需的 DAP 记录设置，然后将 DAP 与远程接入 VPN 关联。

有关 DAP 的详细信息，请参阅动态访问策略。

远程接入 VPN 的功能历史记录

功能	防火墙管理中心最低版本	最低版本	详细信息
基于地理位置的 RA VPN	7.7	7.7	现在，您可以根据国家或地区允许或阻止远程访问 VPN 连接。不符合基于位置的条件的连接会在验证前被阻止，并记录在案以备审核。 新增/修改的屏幕： • **对象** > **对象管理** > **访问列表** > **服务访问** • **设备** > **VPN** > **远程访问**
VTI 环回接口上的 IPsec 流分流	7.4	任意	在 Cisco Secure Firewall 3100 和 Cisco Secure Firewall 4200 设备上，会在 VTI 环回接口上自动启用 IPsec 数据流分流。

功能	防火墙管理中心最低版本	最低版本	详细信息
安全客户端自定义	7.4	任意	您可以配置安全客户端自定义并将其部署到 VPN 头端。当用户从安全客户端连接时，威胁防御会将这些自定义分发到终端： • GUI 文本和消息 • 图标和图像 • 脚本 • 二进制文件 • 自定义安装程序转换 • 本地化安装程序转换 新增/修改的屏幕： • **对象 > 对象管理 > VPN > 安全客户端自定义** > > • **设备** > **远程访问** > **高级** > **安全客户端自定义**
WAN 摘要控制面板	7.4	任意	WAN 摘要控制面板提供 WAN 设备及其接口的快照。 新增/修改的屏幕： **概述** > **控制面板** > **WAN 摘要**
支持证书的 SAML	7.2	任意	我们更新了远程接入 VPN 配置向导，以支持通过证书和 SAML 进行用户身份验证。您可以将远程接入 VPN 配置为在发起 SAML 身份验证之前对计算机或用户证书进行身份验证。
IPsec 流分流。	7.2	任意	在 Cisco Secure Firewall 3100上，默认情况下会分流 IPsec 流。初始设置 IPsec 站点间 VPN 或远程访问 VPN 安全关联 (SA) 后，IPsec 连接将被分流到设备中的现场可编程门阵列 (FPGA)，这应该会提高设备性能。 您可以使用 FlexConfig 和 **flow-offload-ipsec** 命令更改配置。
多个 IDP 信任点支持	7.1	任意	Cisco Secure Firewall Management Center 支持使用 Microsoft Azure 的多个身份提供程序信任点，这些信任点可以具有相同实体ID的多个应用，但具有唯一身份证书。

功能	防火墙管理中心最低版本	最低版本	详细信息
AnyConnect VPN SAML 外部浏览器	7.1	任意	您现在可以配置 AnyConnect VPN SAML 外部浏览器，以启用其他身份验证选项，例如无密码身份验证、WebAuthN、FIDO、SSO、U2F 以及由于 Cookie 的持久性而改进的 SAML 体验。当您使用 SAML 作为远程访问 VPN 连接配置文件的主身份验证方法时，可以选择让 AnyConnect 客户端使用客户端的本地浏览器而不是 AnyConnect 嵌入式浏览器来执行 Web 身份验证。此选项可在您的 VPN 身份验证和其他企业登录之间启用单点登录 (SSO)。如果您想要支持无法在嵌入式浏览器中执行的 Web 身份验证方法（例如生物特征身份验证和 Yubikeys），也可选择此选项。 我们更新了远程访问 VPN 连接配置文件向导，现在您可以配置 **SAML 登录体验**。
多证书身份验证	7.0	任意	Cisco Secure Firewall Management Center 现在支持多种基于证书的 身份验证，以验证机器或设备证书，确保设备是企业发放的设备，此外还可以验证用户的身份证书，以便允许使用 AnyConnect 客户端进行 VPN 接入。
VPN 负载均衡	7.0	任意	VPN 负载均衡会在逻辑上对两台或多台设备进行分组，并在分组的设备之间平均分配远程接入 VPN 会话，而不考虑吞吐量和其他流量参数。
AnyConnect 自定义属性	7.0	任意	Cisco Secure Firewall Management Center 现在支持 AnyConnect 自定义属性，同时提供配置 AnyConnect 客户端功能的基础设施，而无需在 上添加对这些功能的硬编码支持。
本地用户身份验证	7.0	任意	您现在可以使用 Cisco Secure Firewall Management Center Web 界面在 上配置和管理用户，并为主要和辅助远程接入 VPN 身份验证配置本地用户。
选择性策略部署	7.0	任意	现在，您可以选择包括或排除在部署期间对远程接入 VPN 和站点间 VPN 配置的更改。
支持 AnyConnect 模块配置	6.7	任意	Cisco Secure Firewall Management Center 现在支持配置 AnyConnect 模块和配置文件以提高安全性。
支持 LDAP 授权	6.7	任意	您可以使用 Cisco Secure Firewall Management Center 为远程接入 VPN 配置 LDAP 授权。
远程接入 VPN 的 SAML 单点登录支持	6.7	任意	您可以为远程接入 VPN 将 SAML 2.0 服务器配置为单点登录身份验证服务器。
AnyConnect 管理 VPN 隧道支持	6.7	任意	远程访问 VPN 支持配置 AnyConnect 管理 VPN 隧道，该隧道允许在企业终端通电时通过 VPN 连接到终端，而无需 VPN 用户连接到 VPN。

功能	防火墙管理中心最低版本	最低版本	详细信息
支持数据报传输层安全 (DTLS) 1.2	6.6	任意	DTLS 1.2 现在是默认 SSL 密码组的一部分，并且它可以与 TLS 1.2 一起配置。

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。