思科 ASA 系列 VPN CLI 配置指南

软件版本 9.3

发布日期：2014 年 7 月 24 日

思科系统公司
www.cisco.com

思科在全球设有 200 多个办事处。
有关地址、电话号码和传真号码信息，
可查阅思科网站：
www.cisco.com/go/offices。

文本部件号：不适用，仅在线提供

思科 ASA 系列 VPN CLI 配置指南

目 录

关于本指南

文档目的

本指南旨在帮助您使用命令行界面 在自适应安全设备 (ASA) 上配置 VPN。本指南仅介绍最常见的一些配置场景，并未涵盖所有功能。

通过使用自适应安全设备管理器 (ASDM) 这个基于网络的 GUI 应用，您也可以配置和监控 ASA。ASDM 提供配置向导指导您完成一些常见配置场景，并提供联机帮助以使您获得不常见场景的信息。

本指南适用于思科 ASA 系列。本指南中，术语 “ASA”一般适用于所支持的型号，除非另有说明。

相关文档

有关详细信息，请参阅 《*思科 ASA 系列文档导航*》，网址为：http://www.cisco.com/go/asadocs。

约定

本文档使用下列约定：

约定	说明
粗体	命令和关键字及用户输入的文本以**粗体**显示。
斜体	文档标题、新增或强调的术语以及要为其提供值的参数以*斜体*表示。
[ ]	方括号中的元素是可选项。
{x | y | z }	必需的备选关键字集中在大括号内，以竖线分隔。
[x | y | z]	可选的备选关键字集中在方括号内，以竖线分隔。

字符串	不加引号的字符集。请勿将字符串用引号引起来，否则会将字符串和引号视为一个整体。
`courier 字体`	系统显示的终端会话和信息以 `courier 字体`显示。
`courier 粗体`	命令和关键字及用户输入的文本以 **`courier 粗体`**显示。
`courier 斜体`	要提供值的参数以 *`courier 斜体`*显示。
< >	非打印字符 （如密码）括在尖括号中。
[ ]	系统提示的默认回复括在方括号中。
!， #	代码行开头的感叹号 (!) 或井号 (#) 表示注释行。

注 *表示读者需要注意的地方。*

提示 *表示以下信息有助于您解决问题。*

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

获取文档和提交服务请求

有关获取文档、使用思科漏洞搜索工具 (BST)、提交服务请求和收集更多信息的详细信息，请参阅*思科产品文档更新*，网址为：http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html。

通过 RSS 源的方式订阅*思科产品文档更新*（其中包括所有新的和修改过的思科技术文档），并将相关内容通过阅读器应用直接发送至您的桌面。 RSS 源是一种免费服务。

第 1 部分

站点到站点 VPN 和客户端 VPN

IPsec 和 ISAKMP

发布日期：2014 年 7 月 24 日

本章介绍如何配置互联网协议安全 (IPsec) 以及互联网安全关联和密钥管理协议 (ISAKMP) 标准以建立虚拟专用网络 (VPN)。

有关隧道、 IPsec 和 ISAKMP 的信息

隧道让使用互联网等公用 TCP/IP 网络在远程用户和专用企业网络之间创建安全连接成为可能。每个安全连接都叫做一个隧道。

ASA 使用 ISAKMP 和 IPSec 隧道标准建立和管理隧道。 ISAKMP 和 IPSec 将完成以下操作：

- 协商隧道参数
- 建立隧道
- 验证用户和数据
- 管理安全密钥
- 加密和解密数据
- 管理隧道中的数据传输
- 作为隧道终点或路由器管理入站和出站数据传输

ASA 充当双向隧道终点。它可以从专用网络接收明文数据包，将其封装，创建隧道，然后发送到隧道的另一端，随后解封并发送到最终目的地。它也会从公用网络接收封装数据包，将其解封，然后发送给其在专用网络上的最终目标。

IPsec 概述

ASA 会将 IPsec 用于 LAN 对 LAN VPN 连接，并提供将 IPsec 用于客户端对 LAN VPN 连接的选项。在 IPsec 术语中，*对等体*是一个远程访问客户端或另一安全网关。对于这两个连接类型， ASA 仅支持思科对等体。由于我们遵守 VPN 行业标准，ASA 也可以与其他供应商的对等体结合使用；但是，我们不支持这些对等体。

在建立隧道的过程中，两个对等体会协商管理身份验证、加密、封装和密钥管理的安全关联。这些协商涉及两个阶段：第一个阶段，建立隧道 (IKE SA)；第二个阶段，管理该隧道内的流量 (IPsec SA)。

LAN 对 LAN VPN 可连接不同地理位置的网络。在 IPsec LAN 对 LAN 连接中， ASA 可充当发起方或响应方。在 IPsec 客户端对 LAN 连接中，ASA 只能充当响应方。发起方会提议 SA；响应方会接受、拒绝或提出相反提议，所有这一切都根据配置的 SA 参数进行。要建立连接，两个实体都必须同意 SA。

在单情景模式和多情景模式下都可以执行站点对站点任务的配置。

注　多情景模式仅适用于站点对站点的 IKEv2 和 IKEv1，而不适用于 AnyConnect、无客户端 SSL VPN、旧版思科 VPN 客户端、 Apple 本机 VPN 客户端、 Microsoft 本机 VPN 客户端或 IKEv1 IPsec 的 cTCP。

ISAKMP 和 IKE 概述

ISAKMP 是允许两个主机商定如何建立 IPSec 安全关联 (SA) 的协商协议。它提供了商定 SA 属性格式的通用框架。此安全关联包括与对等体协商 SA 以及修改或删除 SA。ISAKMP 将协商分为两个阶段：阶段 1 和阶段 2。阶段 1 创建第一条隧道，其将保护随后的 ISAKMP 协商消息。阶段 2 创建保护数据的隧道。

IKE 使用 ISAKMP 为要使用的 IPsec 设置 SA。 IKE 创建用于对等体身份验证的加密密钥。

ASA 支持对来自旧版思科 VPN 客户端的连接使用 IKEv1，对 AnyConnect VPN 客户端使用 IKEv2。

要设置 ISAKMP 协商条件，请创建 IKE 策略，其包括以下内容：

- IKEv1 对等体要求的身份验证类型，即使用证书的 RSA 签名或预共享密钥 (PSK)。
- 加密方法，用于保护数据并确保隐私。
- 哈希消息认证码 (HMAC) 方法，用于确保发送方身份，以及确保消息在传输过程中未被修改。
- Diffie-Hellman 群，用于确定 encryption-key-determination 算法的强度。ASA 使用此算法派生加密密钥和哈希密钥。
- 对于 IKEv2，使用单独的伪随机函数 (PRF) 作为派生 IKEv2 隧道加密等所要求的密钥内容和哈希运算的算法。
- 对 ASA 替换加密密钥之前使用加密密钥的时间的限制。

利用 IKEv1 策略，您要为每个参数设置一个值。对于 IKEv2，您可以为单个策略配置多个加密和身份验证类型以及多个完整性算法。ASA 按照安全性从高到低的顺序排列这些设置，并按照该排列顺序与对等体协商。这种排列顺序让您可以发送单个提议来传达所有允许的转换，而无须像对 IKEv1 一样发送每个允许的组合。

远程访问 IPsec VPN 的许可要求

下表显示了此功能的许可要求：

注　此功能在无负载加密型号上不可用。

型号	许可证要求[1]
ASA 5505	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证和增强型安全许可证：2 个会话。 *可选永久性或基于时间的许可证：10 或 25 个会话。* *不支持共享许可证。[2]* – AnyConnect 基础版许可证[3]：25 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： – 基础许可证：10 个会话。 – 增强型安全许可证：25 个会话。
ASA 5512-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证和增强型安全许可证：2 个会话。 *可选永久性或基于时间的许可证：10、 25、 50、 100 或 250 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：250 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证和增强型安全许可证：250 个会话。
ASA 5515-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、 25、 50、 100 或 250 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：250 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：250 个会话。

型号	许可证要求[1]
ASA 5525-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、 25、 50、 100、 250、 500 或 750 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：750 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：750 个会话。
ASA 5545-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000 或 2500 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：2500 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：2500 个会话。
ASA 5555-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500 或 5000 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：5000 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：5000 个会话。

型号	许可证要求[1]
ASA 5585-X， 带 SSP-10	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500 或 5000 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：5000 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：5000 个会话。
ASA 5585-X，带 SSP-20、 -40 和 -60	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500、5000 或 10000 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：10000 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：10000 个会话。
ASASM	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500、5000 或 10000 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：10000 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：10000 个会话。

型号	许可证要求[1]
ASAv，带 1 个虚拟 CPU	• 使用 IKEv2 的 IPsec 远程接入 VPN： – 标准版许可证：2 个会话。 – 高级版许可证：250 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 标准和高级版许可证：250 个会话。
ASAv，带 4 个虚拟 CPU	• 使用 IKEv2 的 IPsec 远程接入 VPN： – 标准版许可证：2 个会话。 – 高级版许可证：750 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 标准和高级版许可证：750 个会话。

1. 所有类型的*最大组合 VPN* 会话数量不能超过此表中所示的最大会话数。对于 ASA 5505，基础许可证的最大组合会话数量为 10，增强型安全许可证的最大组合会话数量为 25。
2. 一个共享许可证允许 ASA 用作多个客户端 ASA 的共享许可证服务器。共享许可证池很大，但是，每个 ASA 使用的会话数不能超过永久许可证列出的最大数量。
3. AnyConnect 基础版许可证使 AnyConnect VPN 客户端能够访问 ASA。本许可证并不支持基于浏览器的 SSL VPN 访问或思科安全桌面。对于这些功能，需要激活 AnyConnect 高级许可证，而不是 AnyConnect 基础版许可证。

   注：通过 AnyConnect 基础版许可证， VPN 用户使用网络浏览器登录、下载并启动 （网络启动） AnyConnect 客户端。

   无论是采用本许可证还是 AnyConnect 高级 SSL VPN 版许可证， AnyConnect 客户端软件提供相同的客户端功能集。

   如果在既定的 ASA 上存在以下许可证，则 AnyConnect 基础版许可证无法激活：AnyConnect 高级许可证 （所有类型）或高级终端评估许可证。但是，您可以在同一网络的不同 ASA 上运行 AnyConnect 基础版许可证和 AnyConnect 高级许可证。

   默认情况下，ASA 使用 AnyConnect 基础版许可证；但是，您可以禁用该许可证，使用 **webvpn**，然后使用 **no anyconnect-essentials** 命令来使用其他许可证。

   对于 AnyConnect 基础版许可证和 AnyConnect 高级许可证支持的功能的详细列表，请参阅 *AnyConnect 安全移动客户端功能、许可证和操作系统*：

   http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

准则和限制

此部分包括此功能的准则和限制。

情景模式准则

支持单情景或多情景模式。

防火墙模式准则

仅支持路由防火墙模式。不支持透明防火墙模式。

故障转移准则

仅在主用 / 备用故障转移配置中复制 IPsec VPN 会话。

IPv6 准则

不支持 IPv6。

配置 ISAKMP

本节介绍互联网安全关联以及密钥管理协议 (ISAKMP) 和互联网密钥交换 (IKE) 协议。

配置 IKEv1 和 IKEv2 策略

要创建 IKE 策略，请在单情景或多情景模式下从全局配置模式输入 **crypto *ikev1* | *ikev2* policy** 命令。提示符将显示 IKE 策略配置模式。例如：

```
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
```

创建策略后，您可以为策略指定设置。

表 1-1 和表 1-2 提供有关 IKEv1 和 IKEv2 策略关键字及其值的信息。

表 1-1　用于 CLI 命令的 IKEv1 策略关键字

命令	关键字	含义	说明
authentication	**rsa-sig**	带有使用 RSA 签名算法生成的密钥的数字证书	指定 ASA 用于建立每个 IPSec 对等体的标识的身份验证方法。
	crack	身份验证加密密钥的质询 / 响应	CRACK 在客户端使用 RADIUS 等传统方法进行身份验证且服务器使用公钥身份验证时提供强大的相互身份验证。
	pre-share（默认）	预共享密钥	对于增长型网络，预共享密钥不能很好地进行扩展，但是在小型网络中更容易设置。
encryption	**des** 3des（默认）	56 位 DES-CBC 168 位三重 DES	指定保护两个 IPSec 对等体之间传输的数据的对称加密算法。默认为 168 位三重 DES。
hash	**sha**（默认）	SHA-1（HMAC 变体）	指定用于确保数据完整性的哈希算法。它可以确保数据包来自其所表明的发送方，并且在传输过程中未被修改。
	md5	MD5（HMAC 变体）	默认为 SHA-1。MD5 的摘要较小，被认为速度比 SHA-1 稍快。已发生过针对 MD5 的成功（但非常困难）攻击；然而， IKE 使用的 HMAC 变体可防止此类攻击。
group	**1**	群 1（768 位）	指定 Diffie-Hellman 群标识符，两个 IPsec 对等体会在不相互传输该标识符的情况下，使用该标识符来派生共享密钥。 Diffie-Hellman 群编号越小，其执行所要求的 CPU 时间就越少。 Diffie-Hellman 群编号越大，安全性越高。 AES 只有在支持 VPN-3DES 的安全设备上才可用。要支持 AES 所需要的大密钥长度， ISAKMP 协商应使用 Diffie-Hellman (DH) 群 5。
	2（默认）	群 2（1024 位）	
	5	群 5（1536 位）	
lifetime	**整数值**（86400 = 默认值）	120 至 2147483647 秒	指定 SA 寿命。默认值为 86400 秒或 24 小时。通常，此寿命越短， ISAKMP 协商（在某种程度上）越安全。但是，此寿命越短，ASA 设置将来的 IPSec SA 速度越快。

表 1-2　用于 CLI 命令的 IKEv2 策略关键字

命令	关键字	含义	说明
integrity	**sha** （默认）	SHA-1 （HMAC 变体）	指定用于确保数据完整性的哈希算法。它可以确保数据包来自其所表明的发送方，并且在传输过程中未被修改。
	md5	MD5 （HMAC 变体）	默认为 SHA-1。MD5 的摘要较小，被认为速度比 SHA-1 稍快。已发生过针对 MD5 的成功 （但非常困难）攻击；然而， IKE 使用的 HMAC 变体可防止此类攻击。
	sha256	SHA 2， 256 位摘要	指定具有 256 位摘要的安全哈希算法 SHA 2。
	sha384	SHA 2， 384 位摘要	指定具有 384 位摘要的安全哈希算法 SHA 2。
	sha512	SHA 2， 512 位摘要	指定具有 512 位摘要的安全哈希算法 SHA 2。
	null		指定 AES-GCM 为加密算法时，管理员可以选择 null 作为 IKEv2 完整性算法。
encryption	**des**	56 位 DES-CBC	指定保护两个 IPSec 对等体之间传输的数据的对称加密算法。默认为 168 位三重 DES。
	3des （默认）	168 位三重 DES	
	aes **aes-192** **aes-256**		高级加密标准支持长度为 128、 192、 256 位的密钥。
	aes-gcm **aes-gcm-192** **aes-gcm-256** **null**	用于 IKEv2 加密的 AES-GCM 算法选项	高级加密标准支持长度为 128、 192、 256 位的密钥。
policy_index			访问 IKEv2 策略子模式。
prf	**sha** （默认）	SHA-1 （HMAC 变体）	指定伪随机功能 (PRF)，即用于生成密钥内容的算法。
	md5	MD5 （HMAC 变体）	默认为 SHA-1。MD5 的摘要较小，被认为速度比 SHA-1 稍快。已发生过针对 MD5 的成功 （但非常困难）攻击；然而， IKE 使用的 HMAC 变体可防止此类攻击。
	sha256	SHA 2， 256 位摘要	指定具有 256 位摘要的安全哈希算法 SHA 2。
	sha384	SHA 2， 384 位摘要	指定具有 384 位摘要的安全哈希算法 SHA 2。
	sha512	SHA 2， 512 位摘要	指定具有 512 位摘要的安全哈希算法 SHA 2。
priority			将策略模式扩展为支持其他 IPsec V3 功能并使 AES-GCM 和 ECDH 设置成为 Suite B 支持的一部分。

表 1-2　用于 CLI 命令的 IKEv2 策略关键字 （续）

命令	关键字	含义	说明
group	1	群 1 （768 位）	指定 Diffie-Hellman 群标识符，两个 IPsec 对等体会在不相互传输该标识符的情况下，使用该标识符来派生共享密钥。 Diffie-Hellman 群编号越小，其执行所要求的 CPU 时间就越少。 Diffie-Hellman 群编号越大，安全性越高。 AnyConnect 客户端在非 FIPS 模式下支持 DH 群 1、2 和 5，而在 FIPS 模式下只支持群 2。 AES 只有在支持 VPN-3DES 的安全设备上才可用。要支持 AES 所需要的大密钥长度， ISAKMP 协商应使用 Diffie-Hellman (DH) 群 5。
	2 （默认）	群 2 （1024 位）	
	5	群 5 （1536 位）	
	14		
	19		
	20		
	21		
	24		
lifetime	**整数值** （86400 = 默认值）	120 至 2147483647 秒	指定 SA 寿命。默认值为 86400 秒或 24 小时。通常，此寿命越短， ISAKMP 协商 （在某种程度上）越安全。但是，此寿命越短，ASA 设置将来的 IPSec SA 速度越快。

IKEv1 和 IKEv2 最多分别支持 20 个 IKE 策略，每个都有不同的值集。为您创建的每个策略分别分配一个唯一的优先级。优先级数值越低，优先级越高。

在 IKE 协商开始时，发起协商的对等体将其所有策略发送至远程对等体，然后远程对等体将尝试找到一个匹配项。远程对等体将按照优先级顺序 （优先级最高的优先），将该对等体的所有策略与自身配置的各个策略进行比对，直到发现一个匹配项。

当来自两个对等体的两个策略都包含相同的加密、哈希、身份验证和 Diffie-Hellman 参数值时，就存在匹配项。对于 IKEv1，远程对等体策略还必须指定一个低于或等于发起方发送的策略中寿命的寿命。如果这两个寿命不一样， ASA 将使用较短的寿命。对于 IKEv2，各对等体之间将不协商寿命，而是在本地进行管理，从而可以在每个对等体上单独配置其寿命。如果不存在可接受的匹配项， IKE 将拒绝协商，并且不会建立 IKE SA。

为每个参数选择特定值时，在安全和性能之间就有一个隐式的权衡。默认值提供的安全级别足以达到大多数组织的安全要求。如果与仅支持一个参数值的对等体互通，则只能选择该参数值。

注　新的 ASA 配置没有默认 IKEv1 或 IKEv2 策略。

要配置 IKE 策略，在全局配置模式下，请使用 **crypto *ikev1* | *ikev2* policy** *priority* 命令进入 IKE 策略配置模式。

您必须在每个 ISAKMP 命令中包含优先级。优先级编号仅标识了策略并且决定着策略在 IKE 协商中的优先级。

要启用和配置 IKE，请使用 IKEv1 示例作为指导，完成以下步骤：

注　如果您没有为特定策略参数指定值，则将应用默认值。

步骤 1　进入 IKEv1 策略配置模式：

```
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
```

步骤 2　指定加密算法。默认为三重 DES。本示例将加密算法设置为 DES。

encryption [aes | aes-192 | aes-256 | des | 3des]

例如：

```
hostname(config-ikev1-policy)# encryption des
```

步骤 3　指定哈希算法。默认为 SHA-1。此示例配置 MD5。

hash [md5 | sha]

例如：

```
hostname(config-ikev1-policy)# hash md5
```

步骤 4　指定身份验证方法。默认为预共享密钥。此示例配置 RSA 签名。

authentication [pre-share | crack | rsa-sig]

例如：

```
hostname(config-ikev1-policy)# authentication rsa-sig
```

步骤 5　指定 Diffie-Hellman 群标识符。默认为群 2。此示例配置群 5。

group [**1** | **2** | **5**]

例如：

```
hostname(config-ikev1-policy)# group 5
```

步骤 6　指定 SA 寿命。此示例将其寿命设置为 4 小时 （14400 秒）。默认值为 86400 秒 （24 小时）。

lifetime *seconds*

例如：

```
hostname(config-ikev1-policy)# lifetime 14400
```

在外部接口上启用 IKE

您必须在终止 VPN 隧道的接口上启用 IKE。这通常是外部或公共接口。要启用 IKEv1 或 IKEv2，请在单情景或多情景模式下从全局配置模式使用 **crypto *ikev1*** | ***ikev2*** **enable** *interface-name* 命令。

例如：

```
hostname(config)# crypto ikev1 enable outside
```

禁用 IKEv1 攻击性模式

阶段 1 IKEv1 协商可以使用主模式或攻击性模式。这两个模式提供相同的服务，但是，攻击性模式只需在对等体之间进行总计三条消息的两次交换，而不需要进行总计六条消息的三次交换。攻击性模式速度更快，但是不为通信方提供标识保护。因此，对等体在建立安全 SA 之前必须交换标识信息。默认情况下启用攻击性模式。

- 主模式速度较慢，交换次数较多，但是它会保护通信方的身份。
- 攻击性模式更快，但是，不保护对等体的身份。

要禁用攻击性模式，请在单情景或多情景模式下输入以下命令：

```
crypto ikev1 am-disable
```

例如：

```
hostname(config)# crypto ikev1 am-disable
```

如果禁用了攻击性模式，然后想要恢复它，请使用此命令的 **no** 形式。例如：

```
hostname(config)# no crypto ikev1 am-disable
```

注　禁用攻击性模式可防止思科 VPN 客户端使用预共享密钥身份验证向 ASA 建立隧道。但是，它们可以使用基于证书的身份验证 （也就是 ASA 或 RSA）建立隧道。

确定 IKEv1 和 IKEv2 ISAKMP 对等体的 ID 方法

在 ISAKMP 阶段 I 协商中，对等体必须相互标识自身身份，即 IKEv1 还是 IKEv2。您可以从以下选项中选择标识方法。

地址	使用交换 ISAKMP 标识信息的主机的 IP 地址。
自动	按连接类型确定 ISAKMP 协商： • 预共享密钥的 IP 地址。 • 证书身份验证的证书可分辨名称。
主机名	使用交换 ISAKMP 标识信息的主机的完全限定域名 （默认）。此名称包括主机名和域名。
密钥 ID *key_id_string*	指定远程对等体用于查找预共享密钥的字符串。

ASA 使用发送到对等体的、阶段 I ID。所有 VPN 方案都是如此，但主模式下 LAN 对 LAN IKEv1 连接除外，其使用预共享密钥进行身份验证。

默认设置为自动协商。

要更改对等标识方法，请在单情景或多情景模式下输入以下命令：

```
crypto isakmp identity {address | hostname | key-id id-string | auto}
```

例如，以下命令将对等标识方法设置为使用主机名：

```
hostname(config)# crypto isakmp identity hostname
```

启用经由 NAT-T 的 IPsec

NAT-T 允许 IPsec 对等体通过 NAT 设备建立连接。其方法是使用端口 4500 将 IPsec 流量封装在 UDP 数据报中，从而为 NAT 设备提供端口信息。NAT-T 会自动检测所有 NAT 设备，但只有在必要时才封装 IPSec 流量。此功能默认为已禁用。

注　由于 AnyConnect 客户端的限制，您必须启用 NAT-T，才能让 AnyConnect 客户端使用 IKEv2 成功完成连接。即使客户端不在 NAT-T 设备后面，此要求也适用。

ASA 可同时支持标准 IPsec、经由 TCP 的 IPsec、NAT-T 和经由 UDP 的 IPsec，具体取决于与其交换数据的客户端。

以下细分表格显示启用了各选项的连接。

选项	启用的功能	客户端位置	使用的功能
选项 1	如果已启用 NAT-T	并且客户端位于 NAT 后面，则	使用 NAT-T
		并且没有 NAT，则	使用本地 IPsec (ESP)
选项 2	如果已启用经由 UDP 的 IPsec	并且客户端位于 NAT 后面，则	使用经由 UDP 的 IPsec
		并且没有 NAT，则	使用经由 UDP 的 IPsec
选项 3	如果 NAT-T 和经由 UDP 的 IPsec 都已启用	并且客户端位于 NAT 后面，则	使用 NAT-T
		并且没有 NAT，则	使用经由 UDP 的 IPsec

注　经由 TCP 的 IPsec 启用时，它将优先于所有其他连接方法。

当您启用 NAT-T 时， ASA 将在启用 IPsec 的接口上自动打开端口 4500。

ASA 支持在以下一种网络 （而不是两种网络）中运行的一台 NAT/PAT 设备后面部署多个 IPsec 对等体：

- LAN 对 LAN
- 远程访问

在混合环境中，远程访问隧道将协商失败，因为所有对等体都显示来自相同的公用 IP 地址，即 NAT 设备的地址。此外，远程访问隧道在混合环境中失败的原因还包括它们通常使用和 LAN 对 LAN 隧道组相同的名称（也就是 NAT 设备的 IP 地址）。这种一致性会导致在 NAT 设备后面对等体的 LAN 对 LAN 和远程访问混合网络中多个对等体之间协商失败。

使用 NAT-T

要使用 NAT-T，您必须在单情景或多情景模式下执行以下站点对站点步骤：

步骤 1　输入以下命令，在 ASA 上全局启用经由 NAT-T 的 IPsec：

crypto isakmp nat-traversal *natkeepalive*

其*中 natkeepalive* 参数的范围是 10 至 3600 秒。默认值为 20 秒。

例如，输入以下命令将启用 NAT-T 并将其寿命值设置为一小时。

```
hostname(config)# crypto isakmp nat-traversal 3600
```

步骤 2　通过输入以下命令为 IPsec 分段策略选择加密前选项。

```
hostname(config)# crypto ipsec fragmentation before-encryption
```

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。

启用经由 TCP 的 IKEv1 的 IPsec

对于标准 ESP 或 IKEv1 在其中无法工作，或者仅在修改现有防火墙规则的情况下才能工作的环境，经由 TCP 的 IPsec/IKEv1 使得思科 VPN 客户端可以在此环境中运行。经由 TCP 的 IPSec 将 IKEv1 和 IPSec 协议同时封装在类 TCP 数据包内，并支持同时穿过 NAT 与 PAT 设备和防火墙的安全隧道。此功能默认为已禁用。

注　此功能不可与基于代理的防火墙配合使用。

经由 TCP 的 IPSec 可与远程访问客户端配合使用。在全局启用此功能，则它在所有支持 IKEv1 的接口上都运行。它只是一个客户端到 ASA 功能。它不适用于 LAN 对 LAN 连接。

ASA 可同时支持标准 IPsec、经由 TCP 的 IPsec、 NAT 遍历和经由 UDP 的 IPsec，具体取决于与其交换数据的客户端。经由 TCP 的 IPsec 启用时优先于所有其他连接方法。

一次只支持一个隧道的 VPN 3002 硬件客户端，可使用标准 IPsec、经由 TCP 的 IPsec、NAT 遍历或经由 UDP 的 IPsec 进行连接。

您可以同时在 ASA 及其连接的客户端上启用经由 TCP 的 IPsec。

您可以为您指定的最多 10 个端口启用经由 TCP 的 IPsec。如果您输入一个已知端口，例如端口 80 (HTTP) 或端口 443 (HTTPS)，系统会显示一条警告，指示与该端口关联的协议将不再用于公共接口。其结果是，您无法再使用浏览器通过公共接口管理 ASA。要解决此问题，请将 HTTP/HTTPS 管理重新配置到不同的端口。

默认端口为 10000。

您必须在客户端以及 ASA 上配置 TCP 端口。客户端配置必须包含至少一个您为 ASA 设置的端口。

要在 ASA 上从全局为 IKEv1 启用经由 TCP 的 IPSec，请在单情景或多情景模式下执行以下命令：

```
crypto ikev1 ipsec-over-tcp [port port 1...port0]
```

本示例在端口 45 上启用经由 TCP 的 IPSec：

```
hostname(config)# crypto ikev1 ipsec-over-tcp port 45
```

等待活动会话终止再重新启动

您可以安排 ASA 仅当所有活动会话都已自行终止后，才重新启动。此功能默认为已禁用。

如要启用等待所有活动会话自行终止后 ASA 再重新启动的功能，请在单情景或多情景模式下执行以下站点对站点任务：

```
crypto isakmp reload-wait
```

例如：

```
hostname(config)# crypto isakmp reload-wait
```

使用 **reload** 命令重新启动 ASA。如果设置了 **reload-wait** 命令，则可以使用 **reload quick** 命令覆盖 **reload-wait** 设置。 **reload** 和 **reload-wait** 命令适用于特权执行模式，这两个命令都不包含 **isakmp** 前缀。

断开连接前告警对等体

远程访问或 LAN 对 LAN 会话可能出于某些原因丢失，例如：ASA 关闭或重新启动、会话空闲超时、超过最长连接时间或管理员切断。

ASA 可向合格对等体 （在 LAN 对 LAN 配置中）、思科 VPN 客户端和 VPN 3002 硬件客户端通知会话即将断开。收到此告警的对等体或客户端会对该原因进行解码，并将其显示在事件日志或弹出窗格中。此功能默认为已禁用。

合格客户端和对等体包括以下项：

- 已启用告警的安全设备
- 运行 4.0 或更高版本软件的思科 VPN 客户端 （无需进行配置）
- 运行 4.0 或更高版本软件，并且已启用告警的 VPN 3002 硬件客户端
- 运行 4.0 或更高版本软件，并且已启用告警的 VPN 3000 系列集中器

如要启用用于 IPSec 对等体的断开通知，请在单情景或多情景模式下输入 **crypto isakmp disconnect-notify** 命令。

例如：

```
hostname(config)# crypto isakmp disconnect-notify
```

为 IKEv1 配置证书组匹配

隧道组定义用户连接条件和权限。证书组匹配允许使用用户证书的使用者 DN 或颁发者 DN 的隧道组将用户与隧道组进行匹配。

注　证书组匹配仅适用于 IKEv1 和 IKEv2 LAN 对 LAN 连接。 IKEv2 远程访问连接支持在隧道组的 webvpn 属性中以及在 certificate-group-map 的 webvpn 配置模式下配置的下拉组选择。

如要根据证书的这些字段将用户与隧道组匹配，必须先创建定义匹配标准的规则，然后将每个规则与所需的隧道组匹配。

如要创建证书映射，请使用 **crypto ca certificate map** 命令。要定义隧道组，请使用 **tunnel-group** 命令。

您还必须配置证书组匹配策略，指定从规则或从组织单位 (OU) 字段匹配组，或指定为所有证书用户使用默认组。可以使用其中任意或所有方法。

以下节提供更多信息：

- 第 1-14 页上的创建证书组匹配规则和策略
- 第 1-15 页上的使用 Tunnel-group-map default-group 命令

创建证书组匹配规则和策略

要配置基于证书的 ISAKMP 会话向隧道组映射所遵循的策略和规则并将证书映射条目与隧道组关联，请在单情景或多情景模式下输入 **tunnel-group-map** 映射命令。

其语法如下：

tunnel-group-map enable {*rules* | *ou* | *ike-id* | *peer ip*}

tunnel-group-map [*rule-index*] **enable** *policy*

policy	指定用于从证书派生隧道组名称的策略。 *Policy* 可以是以下某一项： *ike-id* — 指示如果无法根据规则查找确定隧道组或采用来自 OU 的隧道组，则基于证书的 ISAKMP 会话将根据阶段 1 ISAKMP ID 映射到隧道组。 *ou* — 指示如果无法根据规则查找确定隧道组，则使用使用者可分辨名称 (DN) 中 OU 的值。 *peer-ip* — 指示如果无法根据规则查找确定隧道组或采用来自 OU 的隧道组或 ike-id 方法，则使用对等体 IP 地址。 *rules* — 指示根据此命令所配置的证书映射关联，将基于证书的 ISAKMP 会话映射到隧道组。
rule index	（可选）指 **crypto ca certificate map** 命令指定的参数。这些值范围为 1 到 65535。

请注意下列说明：

- 您可以多次调用此命令，只要每次调用是唯一的，并且不引用某个映射超过一次。
- 规则不能超过 255 个字符。
- 您可以将多个规则分配给同一组。为此，您首先要添加规则优先级和组。然后，为每个组定义所需数量的条件语句。当将多个规则分配给同一组时，将为测试为真的第一条规则生成匹配项。
- 通过创建一条规则，您可以要求将用户分配给特定隧道组之前匹配所有条件。要求匹配所有条件等同于逻辑和运算。或者，如果要在将用户分配给特定隧道组之前要求只匹配一个条件，请为每个条件创建一条规则。要求只匹配一个条件等同于逻辑或运算。

以下示例启用根据阶段 1 ISAKMP ID 的内容将基于证书的 ISAKMP 会话映射到隧道组：

```
hostname(config)# tunnel-group-map enable ike-id
hostname(config)#
```

以下示例启用根据对等体的 IP 地址将基于证书的 ISAKMP 会话映射到隧道组：

```
hostname(config)# tunnel-group-map enable peer-ip
hostname(config)#
```

以下示例启用根据使用者可分辨名称 (DN) 中的组织单位 (OU) 映射基于证书的 ISAKMP 会话：

```
hostname(config)# tunnel-group-map enable ou
hostname(config)#
```

以下示例启用根据既定规则映射基于证书的 ISAKMP 会话：

```
hostname(config)# tunnel-group-map enable rules
hostname(config)#
```

使用 Tunnel-group-map default-group 命令

此命令指定在配置未指定隧道组时使用的默认隧道组。

其语法为 **tunnel-group-map** [*rule-index*] **default-group** *tunnel-group-name* ， 其中 *rule-index* 是规则的优先级，并且 *tunnel-group name* 必须用于现有的隧道组。

配置 IPsec

本节提供有关 IPSec 的背景信息并描述使用 IPsec 实施 VPN 时，配置 ASA 所需执行的操作步骤。

了解 IPsec 隧道

IPsec 隧道是 ASA 在对等体之间建立的 SA 集合。SA 指定适用于敏感数据的协议和算法并指定对等体使用的密钥内容。 IPSec SA 控制用户流量的实际传输。 SA 是单向的，但是通常成对建立（入站和出站）。

对等体协商用于每个 SA 的设置。每个 SA 包括以下内容：

- IKEv1 转换集或 IKEv2 提议
- 加密映射
- ACL
- 隧道组
- 预分片策略

了解 IKEv1 转换集和 IKEv2 提议

IKEv1 转换集或 IKEv2 提议是定义 ASA 如何保护数据的安全协议和算法的组合。在 IPsec SA 协商中，对等体必须标识两个对等体都一样的转换集或提议。然后 ASA 应用匹配的转换集或提议为该加密映射创建保护 ACL 中数据流的 SA。

利用 IKEv1 转换集，您要为每个参数设置一个值。对于 IKEv2 提议，您可以为单个提议配置多个加密和身份验证类型以及多个完整性算法。ASA 按照安全性从高到低的顺序排列这些设置，并按照该排列顺序与对等体协商。这让您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

如果您更改用于创建 SA 的转换集或提议的定义， ASA 将撤销隧道。有关详细信息，请参阅第 1-33 页上的清除安全关联。

注　如果您清除或删除转换集或提议中的唯一元素， ASA 将自动取消其加密映射引用。

定义加密映射

*加密映射*定义在 IPsec SA 中协商的 IPSec 策略。其包括以下内容：

- 确定 IPSec 连接允许和保护的数据包的 ACL。
- 对等体标识。
- IPSec 流量的本地地址。（有关详细信息，请参阅第 1-24 页上的将加密映射应用于接口。）
- 最多 11 个 IKEv1 转换集或 IKEv2 提议，用于尝试与对等体安全设置进行匹配。

一个*加密映射集*包括一个或多个具有相同映射名称的加密映射。在创建第一个加密映射时，就要创建加密映射集。以下站点对站点任务将在单情景或多情景模式下创建或添加加密映射：

crypto map *map-name seq-num* **match address** *access-list-name*

使用 access-list-name 指定 ACL ID，即长度最多为 241 个字符的字符串或整数。

提示　使用全部为大写的字母可以更轻松地在您的配置中标识 ACL ID。

您可以继续输入此命令，向加密映射集添加加密映射。在以下示例中， *mymap* 是您可能想要添加加密映射的加密映射集的名称。

```
crypto map mymap 10 match address 101
```

上面语法中显示的*序号* (*seq-num*) 将具有相同名称的加密映射相互区分开。分配给加密映射的序号还决定着同一个加密映射集中该加密映射相较于其他加密映射的优先级。序号越低，优先级越高。在您将加密映射集分配给接口之后， ASA 将按照此映射集中的加密映射评估通过该接口的所有 IP 流量，从序号最小的加密映射开始。

```
[no] crypto map map_name map_index set pfs [group1 | group2 | group5 | group14 | group19 |
group20 | group21 | group24]
```

指定用于加密映射完全向前保密 (FCS) 的 ECDH 组。防止您为加密映射配置组 14 和组 24 选项（使用 IKEv1 策略时）。

```
[no]crypto map name priority set validate-icmp-errors
OR
[no]crypto dynamic-map name priority set validate-icmp-errors
```

指定是否为加密或动态加密映射验证传入的 ICMP 错误消息。

```
[no] crypto map <name> <priority> set df-bit [clear-df | copy-df | set-df}
OR
[no] crypto map dynamic-map <name> <priority> set df-bit [clear-df | copy-df | set-df]
```

为加密或动态加密映射配置现有的不分片 (DF) 策略 （安全关联级别）。

- *clear-df* — 忽略 DF 位。
- *copy-df* — 保持 DF 位。
- *set-df* — 设置和使用 DF 位。

```
[no] crypto map <name> <priority> set tfc-packets [burst <length | auto] [payload-size
<bytes | auto> [timeout <seconds | auto>
OR
[no] crypto dynamic-map <name> <priority> set tfc-packets [burst <length | auto]
[payload-size <bytes | auto> [timeout <seconds | auto>
```

管理员可以按照任意长度和间隔对 IPsec 安全关联启用虚拟流量机密性 (TFC) 数据包。您必须在启用 TFC 之前设置 IKEv2 IPsec 提议。

分配给加密映射的 ACL 包括具有相同 ACL 名称的所有 ACE，如以下命令语法所示：

```
access-list access-list-name {deny | permit} ip source source-netmask destination
destination-netmask
```

每个 ACL 包括具有相同 ACL 名称的一个或多个 ACE。在创建第一个 ACE 时就要创建 ACL。以下命令语法将创建或添加 ACL：

```
access-list access-list-name {deny | permit} ip source source-netmask destination
destination-netmask
```

在以下示例中，ASA 应用将分配给加密映射的 IPSec 保护应用于从 10.0.0.0 子网流向 10.1.1.0 子网的所有流量：

```
access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

匹配数据包的加密映射确定用于 SA 协商的安全设置。如果本地 ASA 发起协商，它将使用静态加密映射中指定的策略创建发送到指定对等体的提议。如果对等体发起协商，ASA 将尝试将策略与静态加密映射匹配，如果匹配失败，其将尝试匹配加密映射集中的动态加密映射，从而决定是接受还是拒绝对等提提议。

要使两个对等体成功建立 SA，它们必须至少有一个兼容的加密映射。要兼容，加密映射必须符合以下条件：

- 加密映射必须包含兼容的加密 ACL （例如，镜像 ACL）。如果响应的对等体使用动态加密映射，则 ASA 还必须包含兼容的加密 ACL 才能应用 IPsec。
- 每个加密映射将标识另一个对等体 （除非响应的对等体使用动态加密映射）。
- 加密映射至少有一个共同的转换集或提议。

一个接口只能应用一个加密映射集。如果存在以下任意情况，则在 ASA 上为特定接口创建一个以上的加密映射：

- 您想让特定对等体处理不同的数据流。
- 您想要将不同的 IPSec 安全应用于不同类型的流量。

例如，创建一个加密映射并分配一个标识两个子网之间流量的 ACL，然后分配一个 IKEv1 转换集或 IKEv2 提议。创建另一个使用不同 ACL 标识另外两个子网之间流量的加密映射，并应用包含不同 VPN 参数的转换集或提议。

如果要为某个接口创建多个加密映射，请为每个映射条目指定一个确定其在加密映射集内优先级的序号 (seq-num)。

每个 ACE 包含一个 permit 或 deny 语句。表 1-3 解释应用于加密映射的 ACL 中 permit 和 deny ACE 的特殊含义。

表 1-3　　应用于出站流量的加密 ACL 中 permit 和 deny 的特殊含义

加密映射评估结果	响应
匹配包含 permit 语句的 ACE 中的条件	停止根据加密映射集中剩余的 ACE 对数据包进行进一步分析，并根据分配给该加密映射的 IKEv1 转换集或 IKEv2 提议中的数据包设置评估数据包安全设置。将这些安全设置与转换集或提议中的设置进行匹配之后， ASA 将应用关联的 IPsec 设置。通常对于出站流量，这意味着对数据包进行解密、身份验证和路由。
匹配包含 deny 语句的 ACE 中的条件	中断对正在评估的加密映射中剩余的 ACE 进行进一步的数据包分析，继续对下一个加密映射中的 ACE 进行评估，具体由分配给它的下一个序号决定。
无法匹配加密映射集中所有受测试的 permit ACE	路由数据包，而不对其进行加密。

包含 deny 语句的 ACE 过滤掉不需要 IPSec 保护的出站流量 （例如，路由协议流量）。因此，请插入初始 deny 语句来过滤不应该按照加密 ACL 中的 permit 语句进行评估的出站流量。

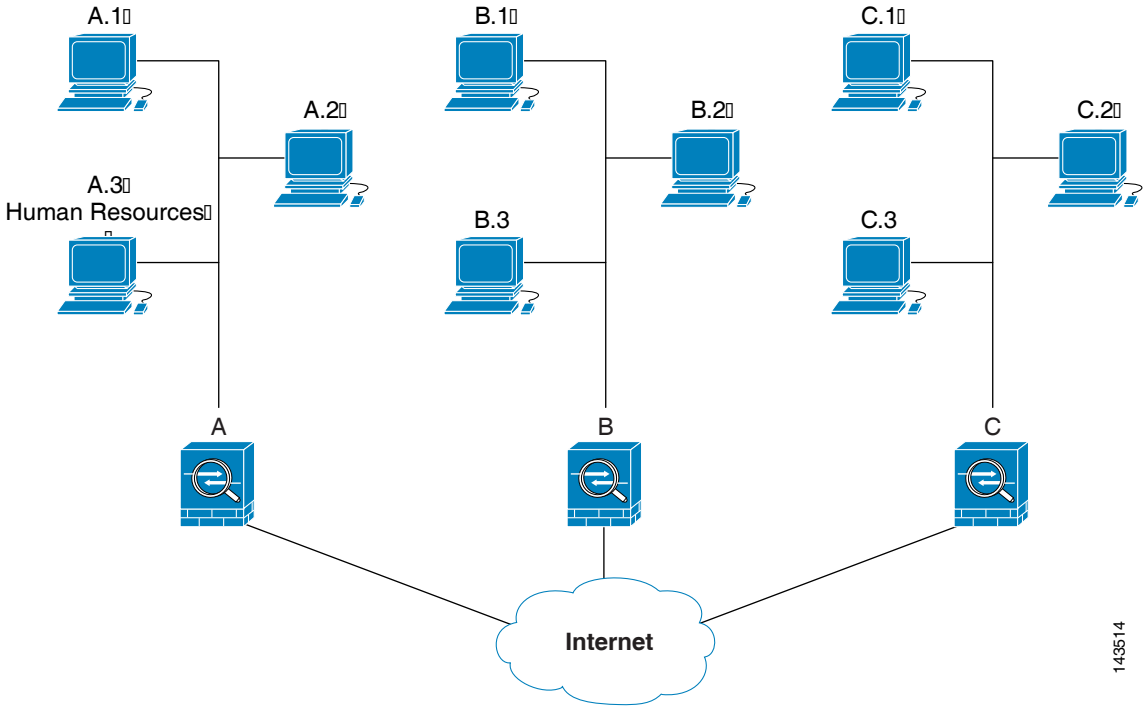
对于入站加密数据包，安全设备使用源地址和 ESP SPI 确定解密参数。解密数据包后，安全设备将会解密的数据包的内部报头与和数据包 SA 关联的 ACL 中的 permit ACE 进行比较。如果内部报头无法与代理匹配，安全设备将丢弃该数据包。如果内部报头与代理匹配，安全设备将路由数据包。

在比较未加密入站数据包的内部报头时，安全设备将忽略所有拒绝规则，因为它们会阻止阶段 2 SA 的建立。

注　要将入站未加密的流量作为明文路由，请在 permit ACE 之前插入 deny ACE。

图 1-1 显示了 ASA 的 LAN 对 LAN 网络示例。

图 1-1　　permit 和 deny ACE 对流量的影响 （概念性地址）



上图中显示的和以下说明中使用的简单地址表示为假想地址。解释后面使用的是带有真实 IP 地址的示例。

本 LAN 对 LAN 网络示例中配置安全设备 A、B 和 C 的目的是允许通过隧道传送来自图 1-1 中所示的一个主机并且以其余主机中另一个主机作为目标的所有流量。但是，因为主机 A.3 的流量包含来自人力资源部门的敏感数据，它要求强大的加密和比其他流量更频繁地重新生成密钥。因此，您会想要为来自主机 A.3 的流量分配一个专用转换集。

要为出站流量配置安全设备 A，您要创建两个加密映射，一个用于来自主机 A.3 的流量，另一个用于来自网络 A 中其他主机的流量，如以下示例所示：

```
Crypto Map Seq_No_1
    deny packets from A.3 to B
    deny packets from A.3 to C
    permit packets from A to B
    permit packets from A to C
Crypto Map Seq_No_2
    permit packets from A.3 to B
    permit packets from A.3 to C
```

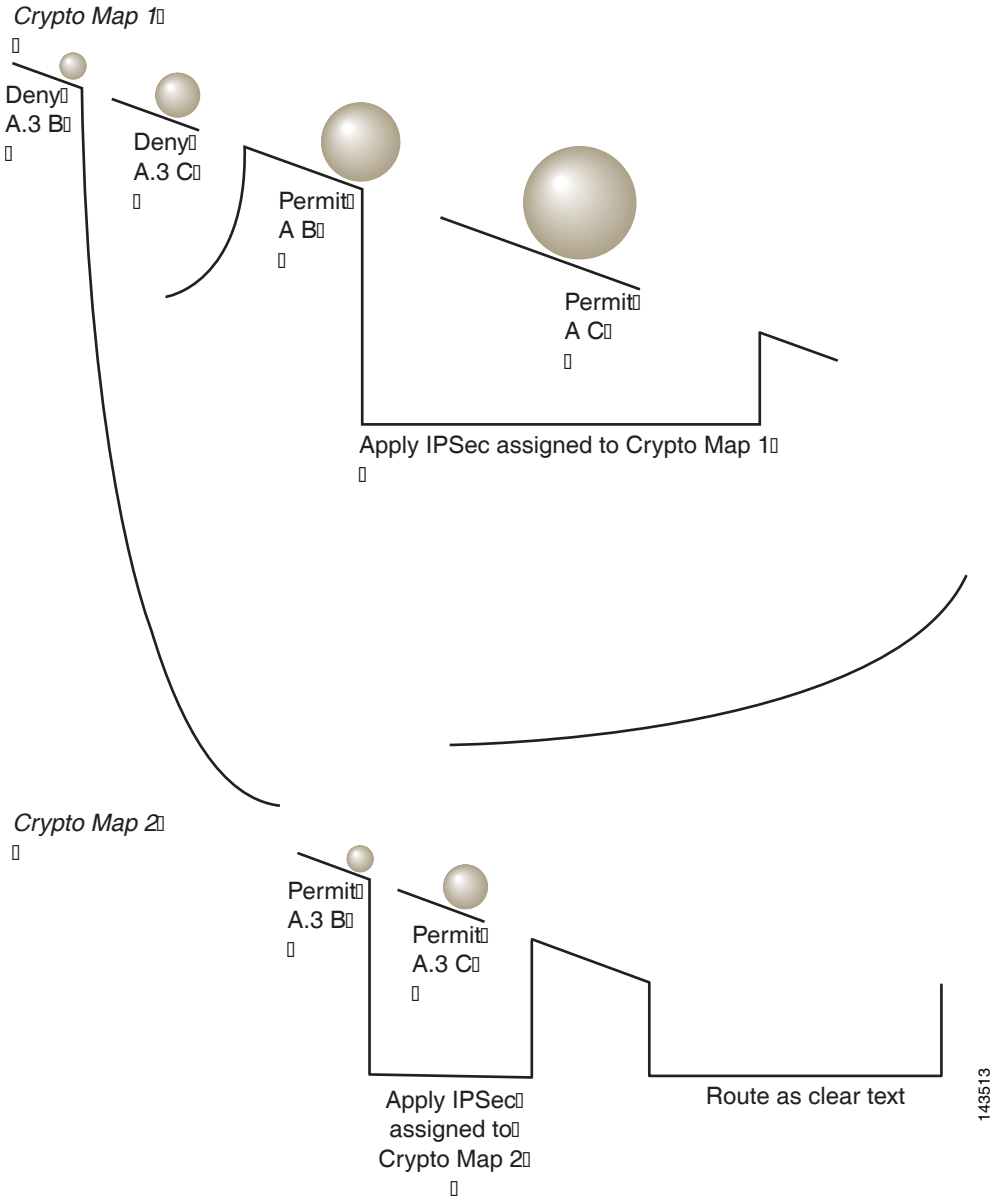
创建 ACL 之后，您要为每个加密映射分配一个转换集，向每个匹配的数据包应用所要求的 IPsec。

级联 ACL 涉及插入 deny ACE 以绕过对 ACL 的评估并继续对加密映射集中的后续 ACL 进行评估。由于您可以将每个加密映射与不同的 IPsec 设置关联，您可以使用 deny ACE 将特定流量从相应加密映射中的进一步评估中排除，并且将特定流量与另一个加密映射中的 permit 语句匹配以提供或要求提供不同的安全保护。分配给加密 ACL 的序号确定其在加密映射集内评估序列中的位置。

图 1-2 显示从本示例中的概念性 ACE 创建的级联 ACL。图中每个符号的含义已在符号后面说明。

	加密映射集中的加密映射。
	（有缺口的直线）当数据包与 ACE 匹配时退出加密映射。
	满足一个 ACE 描述的数据包。各种尺寸的球表示与图中各个 ACE 匹配的不同数据包。尺寸的区别只代表每个数据包的源和目标的差异。
	重定向至加密映射集中的下一个加密映射。
	当数据包与 ACE 匹配或无法匹配加密映射集中的所有 permit ACE 时，做出响应。

图 1-2　　加密映射集中的级联 ACL



安全设备 A 评估源自主机 A.3 的数据包，直到与某个 permit ACE 匹配，并且将尝试分配与加密映射关联的 IPSec 安全。当数据包与某个 deny ACE 匹配时，ASA 将忽略加密映射中剩余的 ACE 并继续评估下一个加密映射，具体由分配给它的序号决定。因此在本示例中，如果安全设备 A 收到来自主机 A.3 的数据包，它会将数据包与第一个加密映射中的 deny ACE 匹配，然后继续评估下一个加密映射中的数据包。当它将数据包与该加密映射中的 deny ACE 匹配时，它将应用关联的 IPSec 安全 （强加密和频繁地重新生成密钥）。

如要在示例网络中完成 ASA 配置，我们要将镜像加密映射分配给 ASA 的 B 和 C。但是，因为在评估入站、加密流量时 ASA 忽略 deny ACE，所以我们可以忽略 deny A.3 B 和 deny A.3 C ACE 的等效镜像，并且因而忽略加密映射 2 的等效镜像。因此，没有必要在 ASA B 和 C 上配置级联 ACL。

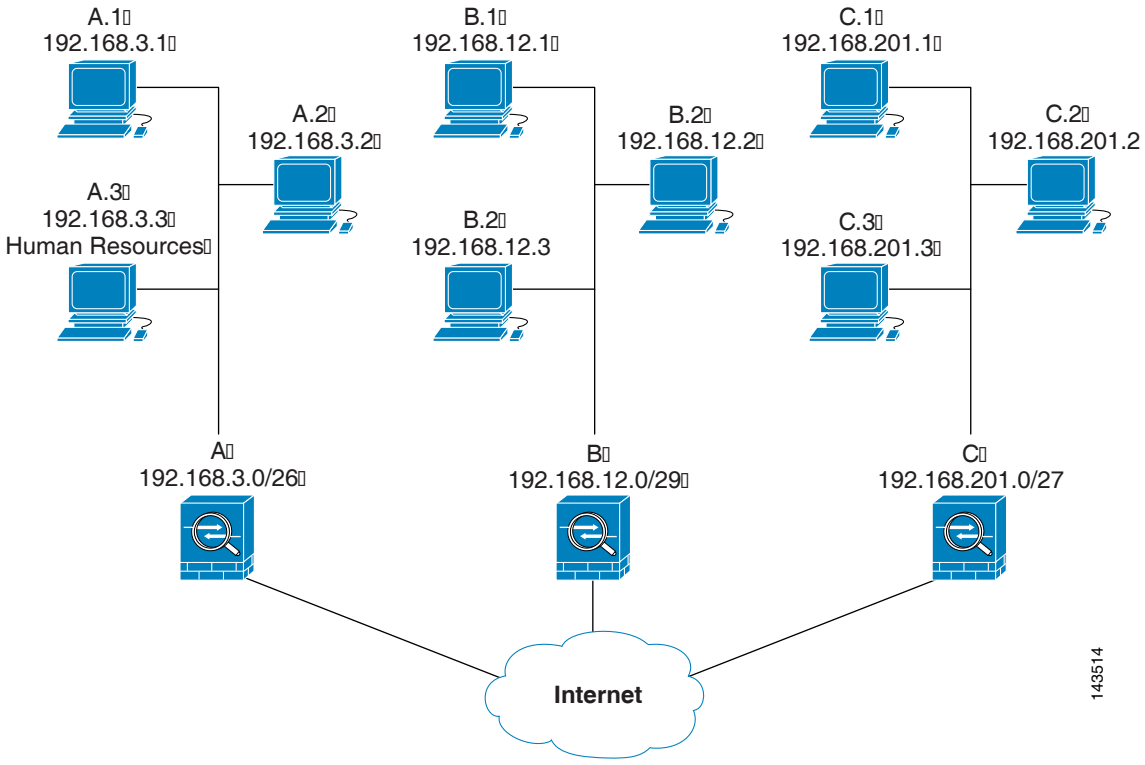
表 1-4 显示向图 1-1 中的所有三个 ASA 配置的加密映射分配的 ACL。

表 1-4　permit 和 deny 语句示例（概念性）

安全设备 A		安全设备 B		安全设备 C	
加密映射序列编号	ACE 模式	加密映射序列编号	ACE 模式	加密映射序列编号	ACE 模式
1	deny A.3 B	1	permit B A	1	permit C A
	deny A.3 C				
	permit A B				
	permit A C		permit B C		permit C B
2	permit A.3 B				
	permit A.3 C				

图 1-3 将图 1-1 中显示的概念性地址映射至真实 IP 地址。

图 1-3　permit 和 deny ACE 对流量的影响（真实地址）



随后的表格将图 1-3 中显示的 IP 地址与表 1-4 中显示的概念相结合。这些表中显示的真实 ACE 确保此网络内接受评估的所有 IPsec 数据包都获得正确的 IPsec 设置

表 1-5　适用于 ASA A 的示例 permit 和 deny 语句

安全设备	加密映射序列编号	ACE 模式	真实 ACE
A	1	deny A.3 B	deny 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		deny A.3 C	deny 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224
		permit A B	permit 192.168.3.0 255.255.255.192 192.168.12.0 255.255.255.248
		permit A C	permit 192.168.3.0 255.255.255.192 192.168.201.0 255.255.255.224
	2	permit A.3 B	permit 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		permit A.3 C	permit 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224
B	不需要	permit B A	permit 192.168.12.0 255.255.255.248 192.168.3.0 255.255.255.192
		permit B C	permit 192.168.12.0 255.255.255.248 192.168.201.0 255.255.255.224
C	不需要	permit C A	permit 192.168.201.0 255.255.255.224 192.168.3.0 255.255.255.192
		permit C B	permit 192.168.201.0 255.255.255.224 192.168.12.0 255.255.255.248

您可以应用示例网络中的推理，通过使用级联 ACL 的推理将不同安全设置分配给受 ASA 保护的不同主机或子网。

注　默认情况下， ASA 不支持目标与其所进入的接口相同的 IPsec 流量。这种类型流量的名称包括 U-turn、hub-and-spoke 和 hairpinning。但是，您可以插入允许流量往返网络的 ACE 将 IPsec 配置为支持 U-turn 流量。例如，要在安全设备 B 上支持 U-turn 流量，请将概念性“permit B B”ACE 添加到 ACL1 中。实际 ACE 如下所示：

```
permit 192.168.12.0 255.255.255.248 192.168.12.0 255.255.255.248
```

管理公钥基础设施 (PKI) 密钥

您必须设置公钥基础结构 (PKI)，管理员才可以在生成或归零密钥对时选择 Suite B ECDSA 算法：

先决条件

如果将加密映射配置为使用 RSA 或 ECDSA 信任点进行身份验证，您首先必须生成密钥集。然后您可以创建信任点并在隧道组配置中引用它。

详细步骤

步骤 1　在生成密钥对时选择 Suite B ECDSA 算法：

```
crypto key generate [rsa [general-keys | label <name> | modules [512 | 768 | 1024 | 2048 | 4096] | noconfirm | usage-keys] | ecdsa [label <name> | elliptic-curve [256 | 384 | 521] | noconfirm]]
```

步骤 2　在归零密钥对时选择 Suite B ECDSA 算法：

```
crypto key zeroize [rsa | ecdsa] [default | label <name> | noconfirm]
```

配置加密核心池

可以在对称多处理 (SMP) 平台上更改加密核心的分配，以提高 AnyConnect TLS/DTLS 流量的吞吐量性能。这些更改可以加速 SSL VPN 数据路径，并在 AnyConnect、智能隧道和端口转发方面提供客户可见的性能提升。如要配置加密核心池，请执行以下步骤。

限制

- 加密核心再平衡在以下平台上可用：
  - 5585-X
  - 5545-X/5555-X
  - ASASM

详细步骤

步骤 1　配置指定三个互相排斥的选项之一的加密核心池：

- balanced — 平均分配加密硬件资源 （Admin/SSL 和 IPsec 核心）。
- ipsec — 将加密硬件资源优先分配给 IPsec （包括 SRTP 加密语音流量）。
- ssl — 将加密硬件资源优先分配给 Admin/SSL。

```
hostname(config)# crypto engine ?

configure mode commands/options:
accelerator-bias
Specify how to allocate crypto accelerator processors

hostname(config)# crypto engine accelerator-bias ?
configure mode commands/options
balanced - Equally distribute crypto hardware resources
ipsec - Allocate crypto hardware resources to favor IPsec/Encrypted Voice (SRTP)
ssl - Allocate crypto hardware resources to favor SSL

hostname(config)# crypto engine accelerator-bias ssl
```

将加密映射应用于接口

您必须为 IPSec 流量经过的每个接口分配加密映射集。 ASA 在所有接口上均支持 IPsec。向接口分配加密映射集将命令 ASA 对所有加密映射集进行所有流量的评估并在连接或 SA 协商期间使用指定的策略。

将加密映射分配给接口还将初始化运行时数据结构，例如 SA 数据库和安全策略数据库。将修改的加密映射重新分配给该接口会将运行时数据结构与加密映射配置重新同步。此外，通过使用新序号添加新的对等体和重新分配加密映射不会中断现有连接。

使用接口 ACL

默认情况下，ASA 允许 IPSec 数据包绕过接口 ACL。如果要将接口 ACL 应用于 IPsec 流量，请使用 **no** 形式的 **sysopt connection permit-vpn** 命令。

与传出接口绑定的加密映射 ACL 将允许或拒绝 IPSec 数据包通过 VPN 隧道。IPsec 对从 IPSec 隧道到达的数据包进行身份验证和解密，并使其按照与隧道关联的 ACL 接受评估。

ACL 定义要保护的 IP 流量。例如，您可以创建 ACL 以保护两个子网或两台主机之间的所有 IP 流量。（这些 ACL 类似于用于 **access-group** 命令的 ACL。但是，用于 **access-group** 命令时， ACL 确定在接口上转发或阻止哪些流量。）

在分配给加密映射之前， ACL 不特定于 IPsec。每个加密映射都引用 ACL，如果某数据包与其中一个 ACL 中的 permit 匹配，则加密映射还确定应用于此数据包的 IPSec 属性。

分配给 IPsec 加密映射的 ACL 有四个主要功能：

- 选择 IPsec 将保护的出站流量 （允许 = 保护）。
- 为在没有建立 SA 的情况下进行的数据传送触发 ISAKMP 协商。
- 处理要过滤掉的入站流量并丢弃原本应受 IPsec 保护的流量。
- 在处理来自对等体的 IKE 协商时，确定是否接受对于 IPSec SA 的请求。（协商只适用于 **ipsec-isakmp crypto map** 条目。）对等体必须允许与 **ipsec-isakmp crypto map** 命令条目关联的数据流，从而确保在协商期间被接受。

不管流量是入站还是出站流量， ASA 都将按照分配给接口的 ACL 评估流量。按照以下步骤将 IPsec 分配到接口上：

步骤 1　创建用于 Ipsec 的 ACL。

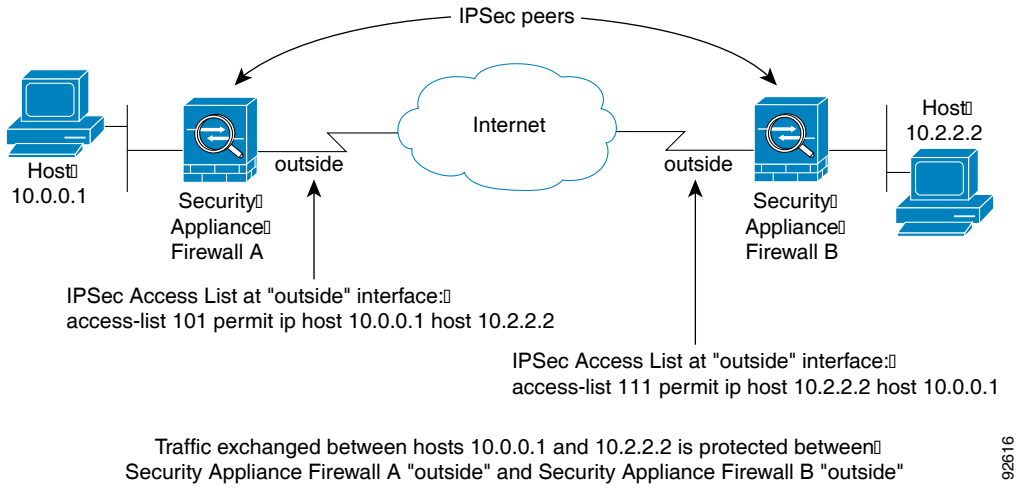
步骤 2　将列表映射到一个或多个使用同一个加密映射名称的加密映射。

步骤 3　将 IKEv1 转换集或 IKEv2 提议映射到加密映射中，从而向数据流应用 IPsec。

步骤 4　通过将加密映射共用的加密映射名称分配到接口上，以加密映射集的形式应用全部加密映射。

在图 1-4 中，数据退出 ASA A 上的外部接口，流向主机 10.2.2.2 时， IPsec 保护将应用于主机 10.0.0.1 和主机 10.2.2.2 之间的流量。

图 1-4　　加密 ACL 如何应用于 IPsec



ASA A 评估从主机 10.0.0.1 到主机 10.2.2.2 的流量，如下所示：

- source = host 10.0.0.1
- dest = host 10.2.2.2

ASA A 也评估从主机 10.2.2.2 到主机 10.0.0.1 的流量，如下所示：

- source = host 10.2.2.2
- dest = host 10.0.0.1

与接受评估的数据包匹配的第一条 permit 语句确定 IPsec SA 的范围。

注　如果删除 ACL 中的唯一元素， ASA 也将删除关联的加密映射。

如果修改一个或多个加密映射当前引用的 ACL，请使 **crypto map interface** 命令重新初始化运行时 SA 数据库。有关详细信息，请参阅 **crypto map** 命令。

对于您在本地对等体上定义的静态加密映射的每个指定加密 ACL，我们建议您在远程对等体上定义一个 “镜像”加密 ACL。加密映射还应支持共同的转换并将对等系统称之为对等体。这将确保两个对等体正确处理 IPsec。

注　每个静态加密映射必须定义一个 ACL 和一个 IPSec 对等体。如果任何一个缺失，加密映射都不完整并且 ASA 将丢弃尚未与之前的完整加密映射匹配的任何流量。使用 **show conf** 命令确保每个加密映射都是完整的。要修复不完整的加密映射，请删除该加密映射，添加缺失的条目，然后将其重新应用。

我们建议不要使用 **any** 关键字来在 ACL 中指定源或目标地址，因为会造成一些问题。我们强烈建议不要使用 **permit any any** 命令语句，因为它会将执行以下操作：

- 保护所有出站流量，包括发送到相应的加密映射中指定对等体的所有受保护流量。
- 要求保护所有入站流量。

  在这种情况下， ASA 将自动丢弃缺少 IPSec 保护的所有入站数据包。

请确保定义要保护哪些数据包。如果将 **any** 关键字用于 **permit** 语句，请在其前面加上一系列 **deny** 语句来过滤掉您不想要保护的流量，否则其将进入 **permit** 语句。

注　配置了 **no sysopt connection permit-vpn** 时，尽管在外部接口上有访问组，客户端将允许解密直通流量，这将调用 deny ip any any access-list。

如果用户想要使用 **no sysopt permit** 命令结合外部接口上的访问控制列表 (ACL) 控制通过站点对站点或远程访问 VPN 对受保护网络的访问，则无法成功进行控制。

在这种情况下，启用管理访问内部接口时，不应用 ACL，用户仍然可以使用 SSH 连接到安全设备。流向内部网络上的主机的流量将被 ACL 正确地阻拦，但是无法阻止流向内部接口的解密直通流量。

ssh 和 **http** 命令具有比 ACL 更高的优先级。换句话说，要拒绝从 VPN 会话流向设备的 SSH、Telnet 或 ICMP 流量，请使用 **ssh**、 **telnet** 和 **icmp** 命令，这些命令将拒绝应该添加的本地 IP 池。

更改 IPsec SA 寿命

协商新的 IPsec SA 时，您可以更改 ASA 使用的全局寿命值。您可以为特定加密映射覆盖这些全局寿命值。

IPSec SA 使用派生的、共享的密钥。密钥是 SA 的组成部分；密钥一起超时就要求刷新密钥。每个 SA 都有两个寿命：计时寿命和流量寿命。 SA 将在各个寿命之后到期，然后对等体将开始协商新的 SA。默认寿命是 28,800 秒 （八小时）和 4,608,000 千字节 （一个小时内每秒钟 10 兆字节）。

如果您更改全局寿命， ASA 将丢弃隧道。它将在随后建立 SA 的协商中使用新值。

如果加密映射没有配置寿命值并且 ASA 请求使用新的 SA，它会将现有 SA 中使用的全局寿命值插入到发送至对等体的请求中。当对等体收到协商请求时，它会使用对等体提议的寿命值和本地配置的寿命值之间较小的值作为新 SA 寿命。

对等体在超出现有 SA 的寿命阈值之前将协商一个新 SA，确保在现有 SA 过期时已经准备好新 SA。现有 SA 剩余寿命只有大约 5% 至 15% 时，对等体将协商一个新的 SA。

创建基本 IPsec 配置

您可以使用静态或动态加密映射创建基本 IPSec 配置。

如要使用静态加密映射创建基本 IPSec 配置，请执行以下步骤：

步骤 1　如要创建 ACL 以定义要保护的流量，请输入以下命令：

```
access-list access-list-name {deny | permit} ip source source-netmask destination
destination-netmask
```

例如：

```
hostname(config)# access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

其中 *access-list-name* 指定 ACL ID，即一个最长为 241 个字符的字符串或整数。 *destination-netmask* 和 *source-netmask* 指定 IPv4 网络地址和子网掩码。在本例中，**permit** 关键字将使匹配指定条件的所有流量受加密保护。

步骤 2　如要配置定义如何保护流量的 IKEv1 转换集，请输入以下命令：

```
crypto ipsec ikev1 transform-set transform-set-name encryption [authentication]
```

Encryption 指定使用哪个加密方法保护 IPsec 数据流：

- esp-aes — 使用带 128 位密钥的 AES。
- esp-aes-192 — 使用带 192 位密钥的 AES。
- esp-aes-256 — 使用带 256 位密钥的 AES。
- esp-des — 使用 56 位 DES-CBC。
- esp-3des — 使用三重 DES 算法。
- esp-null — 不加密。

Authentication 指定使用哪个加密方法保护 IPsec 数据流。

- esp-md5-hmac — 使用 MD5/HMAC-128 作为哈希算法。
- esp-sha-hmac — 使用 SHA/HMAC-160 作为哈希算法。
- esp-none — 不进行 HMAC 身份验证。

例如：

```
hostname(config)# crypto ipsec ikev1 transform-set myset1 esp-des esp-sha-hmac
hostname(config)# crypto ipsec ikev1 transform-set myset2 esp-3des esp-sha-hmac
hostname(config)# crypto ipsec ikev1 transform-set aes_set esp-md5-hmac esp-aes-256
```

在本示例中， myset1 和 myset2 以及 aes_set 是转换集的名称。

要配置也定义如何保护流量的 IKEv2 提议，请输入 **crypto ipsec ikev2 ipsec-proposal** 命令来创建提议，并进入 ipsec 提议配置模式，您可以在此模式下为提议指定多个加密和完整性类型：

crypto ipsec ikev2 ipsec-proposal [*proposal tag*]

Proposal tag 是 IKEv2 IPsec 提议的名称，是一个 1 至 64 个字符的字符串。

例如：

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
```

在本例中， secure 是提议的名称。输入协议和加密类型：

```
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes des
```

相反，以下命令将选择使用哪个 AES-GCM 或 AES-GMAC 算法：

```
hostname(config-ipsec-proposal)# [no] protocol esp encryption [3des | aes | aes-192 |
aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 |
des | null]
```

如果选择 SHA-2 或 null，则必须选择使用哪个算法作为 IPsec 算法。如果将 AES-GCM/GMAC 配置为加密算法，则必须选择 null 完整性算法：

```
hostname(config-ipsec-proposal)# [no] protocol esp integrity [md5 | sha-1 | sha-256 |
sha-384 | sha-512 | null]
```

注　如果 AES-GCM/GMAC 已被配置为加密算法，对于完整性算法您必须选择 null。可以将 SHA-256 用于完整性和 PRF 以建立 IKEv2 隧道，但是也可以将其用于 ESP 完整性保护。

步骤 3　（可选）管理员可以启用路径最大传输单元 (PMTU) 老化并设置将 PMTU 值重置为其原始值的时间间隔。

```
hostname(config-ipsec-proposal)# [no] crypto ipsec security-association pmtu-aging
<reset-interval>
```

步骤 4　要创建加密映射，请使用单情景或多情景模式执行以下站点对站点步骤：

a.　将 ACL 分配到加密映射中：

crypto map *map-name seq-num* **match address** *access-list-name*

加密映射集是一系列加密映射条目，每个条目使用不同的序号 (*seq-num)* ，但使用相同的*映射名称*。使用 *access-list-name* 指定 ACL ID，即长度最多为 241 个字符的字符串或整数。在以下示例中， mymap 是加密映射集的名称。此映射集序号为 10，此序号用于排列一个加密映射集内的多个条目优先级。序号越低，优先级越高。

```
crypto map mymap 10 match address 101
```

在本示例中，名称为 101 的 ACL 将分配给加密映射 mymap。

b. 指定可以向其转发受 IPSec 保护的流量的对等体：

```
crypto map map-name seq-num set peer ip-address
```

例如：

```
crypto map mymap 10 set peer 192.168.1.100
```

ASA 设置 SA，其中对等体分配的 IP 地址为 192.168.1.100。重复此命令指定多个对等体。

c. 指定此加密映射允许哪些 IKEv1 转换集或 IKEv2 提议。按照优先级顺序（优先级高的优先）列出多个转换集或提议。您可以使用以下两个命令之一，在加密映射中最多指定 11 个转换集或提议：

```
crypto map map-name seq-num set ikev1 transform-set transform-set-name1
[transform-set-name2, …transform-set-name11]
```

```
crypto map map-name seq-num set ikev2 ipsec-proposal proposal-name1
[proposal-name2, … proposal-name11]
```

Proposal-name1 和 *proposal-name11* 指定用于 IKEv2 的一个或多个 IPsec 提议名称。每个加密映射条目最多支持 11 个提议。

例如 （对于 IKEv1）：

```
crypto map mymap 10 set ikev1 transform-set myset1 myset2
```

在本示例中，流量与 ACL 101 匹配时， SA 可以使用 myset1（第一优先级）或 myset2（第二优先级），具体取决于哪个转换集与对等体的转换集匹配。

d. （可选）如果想要覆盖全局寿命，请为加密映射指定 SA 寿命。

```
crypto map map-name seq-num set security-association lifetime {seconds seconds |
kilobytes kilobytes}
```

Map-name 指定加密映射集的名称。 *Seq-num* 指定您分配给加密映射条目的序号。

例如：

```
crypto map mymap 10 set security-association lifetime seconds 2700
```

此示例将加密映射集 mymap 10 的计时寿命缩短至 2700 秒（45 分钟）。基于流量的寿命未更改。

e. （可选）指定当此加密映射请求新的 SA 时 IPsec 需要完全向前保密，或要求在从对等体接收的请求中应用 PFS：

```
crypto map map-name seq-num set pfs [group1 | group2 | group5]
```

例如：

```
crypto map mymap 10 set pfs group2
```

此示例要求在为加密映射 mymap 10 协商新 SA 时提供 PFS。 ASA 在新 SA 中使用 1024 位 Diffie-Hellman 素数模数群。

步骤 5　将加密映射集应用于评估 IPSec 流量的接口：

```
crypto map map-name interface interface-name
```

Map-name 指定加密映射集的名称。*Interface-name* 指定启用或禁用 ISAKMP IKEv1 协商的接口的名称。

例如：

```
crypto map mymap interface outside
```

在本示例中， ASA 按照加密映射 mymap 评估通过外部接口的流量，确定其是否需要保护。

使用动态加密映射

动态加密映射是未配置所有参数的加密映射。该映射可作为一个策略模板，其中缺失的参数将在以后根据 IPsec 协商的结果动态获取，以匹配对等体要求。如果对等体尚未在静态加密映射中确定 IP 地址， ASA 将对其应用动态加密映射，允许对等体协商隧道。这种情况发生于以下类型的对等体中：

- 具有动态分配的公用 IP 地址的对等体。

  LAN 对 LAN 和远程访问对等体都可以使用 DHCP 获取公用 IP 地址。ASA 只使用此地址启动隧道。

- 具有动态分配的专用 IP 地址的对等体。

  请求远程访问隧道的对等体通常具有由头端分配的专用 IP 地址。通常， LAN 对 LAN 隧道具有预定的专用网络集，此网络集用于配置静态映射，从而用于建立 IPsec SA。

作为配置静态加密映射的管理员，您可能不知道动态分配的 IP 地址 （通过 DHCP 或其它方法分配），而且您可能不知道其他客户端的专用 IP 地址（无论分配方法如何）。 VPN 客户端通常没有静态 IP 地址；它们要求使用动态加密映射，以允许进行 IPsec 协商。例如，头端在 IKE 协商期间向思科 VPN 客户端分配 IP 地址，然后客户端使用该 IP 地址来协商 IPSec SA。

注　动态加密映射只需要 **transform-set** 参数。

动态加密映射可以简化 IPSec 配置，我们建议在并非总是能够预先确定对等体的网络中使用动态加密映射。对于思科 VPN 客户端 （例如移动用户）和获取动态分配 IP 地址的路由器，请使用动态加密映射。

提示　在动态加密映射中将 **any** 关键字用于 **permit** 条目时，请小心。如果此 **permit** 条目包含的流量可能包含多播或广播流量，请将适用于相应地址范围的 **deny** 条目插入 ACL 中。记住为网络和子网广播流量以及 IPsec 不应保护的任何其他流量插入 **deny** 条目。

动态加密映射只适用于和发起连接的远程对等体协商 SA。 ASA 不能使用动态加密映射向远程对等体发起连接。使用动态加密映射时，如果出站流量匹配 ACL 中的 permit 条目并且对应的 SA 尚不存在，则 ASA 将丢弃该流量。

加密映射集可以包括动态加密映射。动态加密映射集应该是加密映射集中具有最低优先级的加密映射 （也就是说，它们应该具有最高值的序号），从而使 ASA 可以先评估其他加密映射。只有在其他 （静态）映射条目不匹配时它才会检查动态加密映射集。

类似于静态加密映射集，动态加密映射集包括具有相同动态映射名称的所有动态加密映射。动态序号将区分动态映射集中的动态加密映射。如果您配置动态加密映射，请插入 permit ACL 以为加密 ACL 标识 IPSec 对等体的数据流。否则， ASA 将接受对等体提议的所有数据流标识。

注意事项　对于要通过隧道传送到使用静态加密映射集配置的 ASA 接口的流量，请勿对其分配模块默认路由。要确定应该通过隧道传送的流量，请将 ACL 添加到动态加密映射中。配置与远程访问隧道关联的 ACL 时，请注意确定正确的地址池。只有在隧道运行后，才可以使用反向路由注入安装路由。

除了您要创建动态加密映射条目，而不是创建静态加密映射之外，使用动态加密映射条目的操作步骤与 “创建基本 IPsec 配置”中描述的基本配置一样。您也可以在一个加密映射集中组合静态和动态映射条目。

按照以下步骤，使用单情景或多情景模式创建一个动态加密映射条目：

步骤 1　（可选）将 ACL 分配给动态加密映射：

```
crypto dynamic-map dynamic-map-name dynamic-seq-num match address access-list-name
```

这将确定要保护和不保护哪些流量。 *Dynamic-map-name* 指定引用已有动态加密映射的加密映射条目的名称。 *Dynamic-seq-num* 指定与动态加密映射条目对应的序号。

例如：

```
crypto dynamic-map dyn1 10 match address 101
```

在本示例中， ACL 101 已分配给动态加密映射 dyn1。映射序号为 10。

步骤 2　指定此动态加密映射允许哪些 IKEv1 转换集或 IKEv2 提议。使用该命令为 IKEv1 转换集或 IKEv2 提议按照优先级顺序列出多个转换集或提议 （优先级高的优先）：

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set ikev1 transform-set
transform-set-name1, [transform-set-name2, …transform-set-name9]

crypto dynamic-map dynamic-map-name dynamic-seq-num set ikev2 ipsec-proposal
proposal-name1
[proposal-name2, … proposal-name11]
```

Dynamic-map-name 指定引用已有动态加密映射的加密映射条目的名称。*Dynamic-seq-num* 指定与动态加密映射条目对应的序号。 *transform-set-name* 是当前创建或修改的转换集的名称。 *proposal-name* 为 IKEv2 指定一个或多个 IPsec 提议的名称。

例如 （对于 IKEv1）：

```
crypto dynamic-map dyn 10 set ikev1 transform-set myset1 myset2
```

在本示例中，当流量匹配 ACL 101 时， SA 可以使用 myset1 （第一优先级）或 myset2 （第二优先级），具体取决于哪个转换集与对等体的转换集匹配。

步骤 3　（可选）如果您想要覆盖全局寿命值，请指定动态加密映射条目的 SA 寿命：

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set security-association lifetime
{seconds seconds | kilobytes kilobytes}
```

Dynamic-map-name 指定引用已有动态加密映射的加密映射条目的名称。*Dynamic-seq-num* 指定与动态加密映射条目对应的序号。

例如：

```
crypto dynamic-map dyn1 10 set security-association lifetime seconds 2700
```

此示例将动态加密映射集 dyn1 10 的计时寿命缩短至 2700 秒 （45 分钟）。流量寿命未更改。

步骤 4　（可选）指定当为此动态加密映射请求新 SA 时， IPsec 要求提供 PFS，或应该要求从对等体接收的请求中的 PFS：

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set pfs [group1 | group2 | group5 |
group7]
```

Dynamic-map-name 指定引用已有动态加密映射的加密映射条目的名称。*Dynamic-seq-num* 指定与动态加密映射条目对应的序号。

例如：

```
crypto dynamic-map dyn1 10 set pfs group5
```

步骤 5　将动态加密映射集添加到静态加密映射集中。

请确保在加密映射集中将引用动态映射的加密映射设置为优先级最低的条目 （序号最高）。

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

Map-name 指定加密映射集的名称。*Dynamic-map-name* 指定引用已有动态加密映射的加密映射条目的名称。

例如：

```
crypto map mymap 200 ipsec-isakmp dynamic dyn1
```

提供站点对站点冗余

您可以使用加密映射定义多个 IKEv1 对等体，以提供冗余。此配置对于站点对站点 VPN 非常有用。 KEv2 不支持此功能。

如果一个对等体失败， ASA 将与下一个和加密映射关联的对等体建立隧道。它会将数据发送到已与其协商成功的对等体，并且该对等体将成为活动对等体。活动对等体是 ASA 始终首先尝试后续协商的对等体，直到协商失败。此时 ASA 将继续与下一个对等体协商。当与加密映射关联的所有对等体都失败时， ASA 将循环返回第一个对等体。

查看 IPsec 配置

表 1-6 列出您可以在单情景或多情景模式下输入以查看关于您的 IPSec 配置的信息的命令。

表 1-6　用于查看 IPSec 配置信息的命令

命令	目的
show running-configuration crypto	显示整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。
show running-config crypto ipsec	显示完整的 IPsec 配置。
show running-config crypto isakmp	显示完整的 ISAKMP 配置。
show running-config crypto map	显示完整的加密映射配置。
show running-config crypto dynamic-map	显示动态加密映射配置。
show all crypto map	显示所有配置参数，包括使用默认值的那些配置参数。
show crypto ikev2 sa detail	在加密统计信息中显示 Suite B 算法支持。
show crypto ipsec sa	在单情景或多情景模式下显示 Suite B 算法支持和 ESPv3 IPsec 输出。
show ipsec stats	在单情景或多情景模式下显示有关 IPsec 子系统的信息。TFC 数据包以及受到的有效和无效 ICMP 错误中都会显示 ESPv3 统计信息。

清除安全关联

有一些配置更改只有在随后的 SA 的协商过程中才生效。如果要让新的设置立即生效，请清除现有 SA 以使用已更改的配置重新建立它们。如果 ASA 正在处理 IPSec 流量，请清除配置更改所影响的那部分 SA 数据库。对于大规模更改，或 ASA 正在处理少量 IPSec 流量时，请推迟执行清除整个 SA 数据库的时间。

表 1-7 列出了可以在单情景或多情景模式下输入以清除和重新初始化 IPsec SA 的命令。

表 1-7　清除和重新初始化 IPSec SA 的命令

命令	目的
clear configure crypto	删除整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。
clear configure crypto ca trustpoint	删除所有信任点。
clear configure crypto dynamic-map	删除所有动态加密映射。包括让您删除特定动态加密映射的关键字。
clear configure crypto map	删除所有加密映射。包括让您删除特定加密映射的关键字。
clear configure crypto isakmp	删除整个 ISAKMP 配置。
clear configure crypto isakmp policy	删除所有 ISAKMP 策略或特定策略。
clear crypto isakmp sa	删除整个 ISAKMP SA 数据库。

清除加密映射配置

clear configure crypto 命令包括可删除加密配置的元素的参数，包括 IPsec、加密映射、动态加密映射、 CA 信任点、所有证书、证书映射配置和 ISAKMP。

请注意，如果输入不带参数的 **clear configure crypto** 命令，则将删除整个加密配置，包括所有证书。

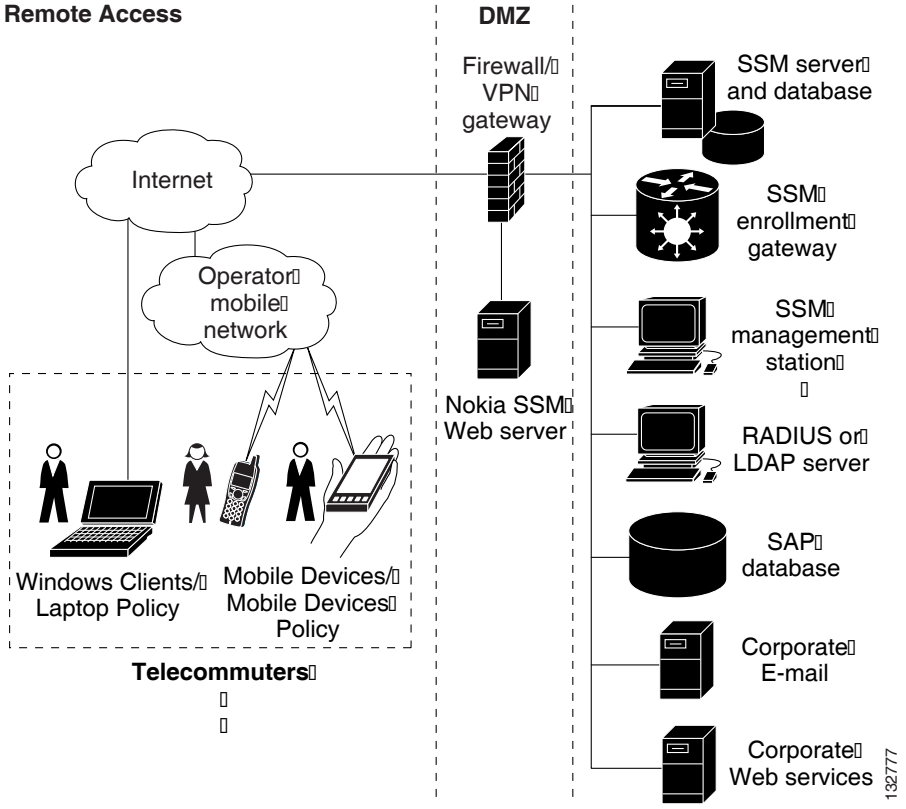
有关详细信息，请参阅*思科 ASA 系列命令参考*中的 **clear configure crypto** 命令。

支持 Nokia VPN 客户端

ASA 使用身份验证加密密钥的质询 / 响应 (CRACK) 协议支持来自 Nokia 92xx Communicator 系列手机上 Nokia VPN 客户端的链接。对于使用旧版身份验证技术而不是数字证书的支持 IPsec 的移动客户端， CRACK 是理想之选。当客户端使用 RADIUS 等基于旧版的密钥身份验证技术并且网关使用公钥身份验证时，它可以提供相互身份验证。

必须具备 Nokia 后端服务才能同时支持 Nokia 客户端和 CRACK 协议。此要求包括图 1-5 中所示的 Nokia 安全服务管理器 (NSSM) 和 Nokia 数据库。

图 1-5　Nokia 92xx Communicator 服务要求



要支持 Nokia VPN 客户端，请在 ASA 上执行以下步骤：

- 在全局配置模式下使用 **crypto isakmp policy** *priority* **authentication** 命令和 **crack** 关键字启用 CRACK 身份验证。例如：

```
hostname(config)# crypto isakmp policy 2
hostname(config-isakmp-policy)# authentication crack
```

如果使用数字证书进行客户端身份验证，请执行以下附加步骤：

步骤 1　配置信任点并删除对完全限定域名的要求。信任点可能是 NSSM 或其它 CA。在本示例中，信任点命名为 CompanyVPNCA：

```
hostname(config)# crypto ca trustpoint CompanyVPNCA
hostname(config-ca-trustpoint)# fqdn none
```

步骤 2　要配置 ISAKMP 对等体的标识，请执行以下步骤之一：

- 使用 **crypto isakmp identity** 命令和 **hostname** 关键字。例如：

```
hostname(config)# crypto isakmp identity hostname
```

- 使用 **crypto isakmp identity** 命令和 **auto** 关键字配置标识从连接类型自动确定。例如：

```
hostname(config)# crypto isakmp identity auto
```

注　如果使用 **crypto isakmp identity auto** 命令，您必须确保客户端证书中的 DN 属性顺序为 CN、OU、O、C、St、L。

有关在 Nokia 客户端上支持 CRACK 协议所需的 Nokia 服务以及确保正确安装和配置这些服务的详细信息，请联系当地 Nokia 代表。

经由 IPsec 的 L2TP

本章介绍如何在 ASA 上配置经由 IPsec/IKEv1 的 L2TP。本章包含以下主题：

有关经由 IPsec/IKEv1 的 L2TP 的信息

第 2 层隧道协议 (L2TP) 是允许远程客户端使用公用 IP 网络安全地与专用企业网络服务器通信的 VPN 隧道协议。 L2TP 使用经由 UDP 的 PPP （端口 1701）来通过隧道传送数据。

L2TP 协议基于客户端 / 服务器型号。此功能在 L2TP 网络服务器 (LNS) 和 L2TP 访问集中器 (LAC) 之间分配。 LNS 通常在路由器等网络网关上运行，而 LAC 可以是拨号网络接入服务器 (NAS) 或有一个捆绑的 L2TP 客户端的终端设备 （如 Microsoft Windows、 Apple iPhone 或 Android）。

在远程访问方案中，使用 IPsec/IKEv1 配置 L2TP 的主要优点在于远程用户可以通过公用 IP 网络访问 VPN，而无需使用网关或专线，实际上就可以利用 POTS 从任何位置启用远程访问。另一个优势是无需思科 VPN 客户端软件等任何其他客户端软件。

注 经由 IPsec 的 L2TP 仅支持 IKEv1。不支持 IKEv2。

利用 IPsec/IKEv1 的 L2TP 的配置支持使用预共享密钥或 RSA 签名方法的证书，并且支持使用动态 （相对于静态）加密映射。此任务摘要假设已经完成 IKEv1 以及预共享密钥或 RSA 签名配置。有关配置预共享密钥、 RSA 和动态加密映射的步骤，请参阅常规操作配置指南中第 41 章 “数字证书”。

注 在 ASA 上使用 IPsec 的 L2TP 允许 LNS 与 Windows、Mac OS X、Android 和思科 IOS 等操作系统中集成的本地 VPN 客户端互通。仅支持使用 IPsec 的 L2TP，在 ASA 上不支持本地 L2TP 本身。Windows 客户端支持的最小 IPsec 安全关联寿命是 300 秒。如果 ASA 上该寿命设置低于 300 秒，Windows 客户端会忽略此设置并将其替换为 300 秒的寿命。

IPsec 传输和隧道模式

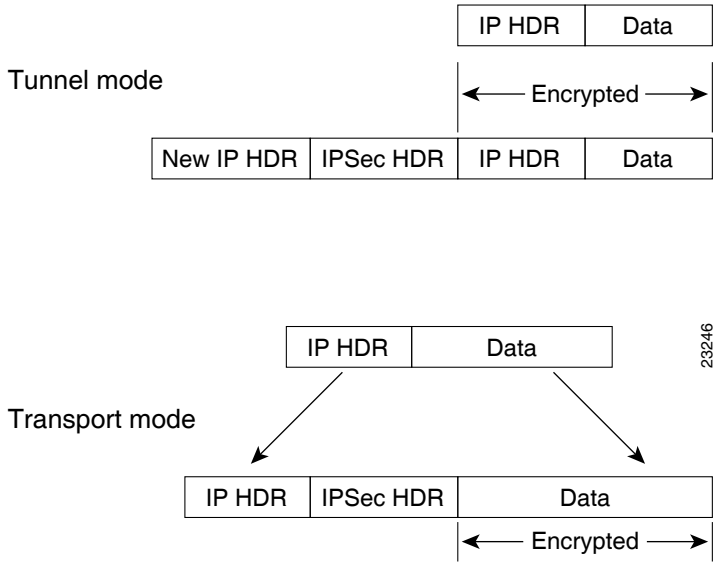
默认情况下，ASA 使用 IPsec 隧道模式 — 整个原始 IP 数据报都将加密并且其将成为新 IP 数据包的负载。此模式允许路由器等网络设备用做 IPsec 代理。也就是说，路由器代表主机进行加密。源路由器将加密数据包并将其沿 IPsec 隧道转发。目标路由器解密原始 IP 数据报并将其转发到目标系统。隧道模式的主要优点是不需要修改终端系统即可获得 IPsec 的优势。隧道模式还可以防止流量分析；利用隧道模式，攻击者只能确定隧道终点，而无法确定通过隧道传送的数据包的源和目标，即使其与隧道终点一样也无法确定。

但是，Windows L2TP/IPsec 客户端使用 IPsec 传输模式 — 只加密 IP 负载，而原始 IP 报头保留原封不动。此模式的优势是每个数据包只需增加少数字节并且允许公用网络上的设备查看数据包的最终源和目标。图 2-1 说明 IPsec 隧道和传输模式之间的差异。

要使 Windows L2TP 和 IPsec 客户端连接到 ASA，必须使用 **crypto ipsec transform-set trans_name mode transport** 命令为转换集配置 IPsec 传输模式。此命令用于配置操作步骤中。

通过此传输功能，可以根据 IP 报头中的信息在中间网络上启用特殊处理（例如 QoS）。然而，第 4 层报头将被加密，这就限制了对数据包的检查。遗憾的是，如果 IP 报头以明文传输，传输模式就会允许攻击者执行某些流量分析。

图 2-1　　隧道和传输模式下的 IPsec



经由 IPsec 的 L2TP 的许可要求

下表显示了此功能的许可要求：

注　此功能在无负载加密型号上不可用。

型号	许可证要求[1]
ASA 5505	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证和增强型安全许可证：2 个会话。 *可选永久性或基于时间的许可证：10 或 25 个会话。* *不支持共享许可证。[2]* – AnyConnect 基础版许可证[3]：25 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： – 基础许可证：10 个会话。 – 增强型安全许可证：25 个会话。
ASA 5512-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证和增强型安全许可证：2 个会话。 *可选永久性或基于时间的许可证：10、 25、 50、 100 或 250 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证 [3]：250 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证和增强型安全许可证：250 个会话。
ASA 5515-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、 25、 50、 100 或 250 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证 [3]：250 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：250 个会话。
ASA 5525-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、 25、 50、 100、 250、 500 或 750 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证 [3]：750 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：750 个会话。

型号	许可证要求[1]
ASA 5545-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000 或 2500 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：2500 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：2500 个会话。
ASA 5555-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500 或 5000 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：5000 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：5000 个会话。
ASA 5585-X， 带 SSP-10	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500 或 5000 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：5000 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：5000 个会话。

型号	许可证要求[1]
ASA 5585-X，带 SSP-20、 -40 和 -60	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500、5000 或 10000 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：10000 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：10000 个会话。
ASASM	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500、5000 或 10000 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：10000 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：10000 个会话。
ASAv，带 1 个虚拟 CPU	• 使用 IKEv2 的 IPsec 远程接入 VPN： – 标准版许可证：2 个会话。 – 高级版许可证：250 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 标准和高级版许可证：250 个会话。
ASAv，带 4 个虚拟 CPU	• 使用 IKEv2 的 IPsec 远程接入 VPN： – 标准版许可证：2 个会话。 – 高级版许可证：750 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 标准和高级版许可证：750 个会话。

1. 所有类型的*最大组合 VPN* 会话数量不能超过此表中所示的最大会话数。对于 ASA 5505，基础许可证的最大组合会话数量为 10，增强型安全许可证的最大组合会话数量为 25。
2. 一个共享许可证允许 ASA 用作多个客户端 ASA 的共享许可证服务器。共享许可证池很大，但是，每个 ASA 使用的会话数不能超过永久许可证列出的最大数量。

3. AnyConnect 基础版许可证使 AnyConnect VPN 客户端能够访问 ASA。本许可证并不支持基于浏览器的 SSL VPN 访问或思科安全桌面。对于这些功能，需要激活 AnyConnect 高级许可证，而不是 AnyConnect 基础版许可证。

   注：通过 AnyConnect 基础版许可证， VPN 用户使用网络浏览器登录、下载并启动 （网络启动） AnyConnect 客户端。

   无论是采用本许可证还是 AnyConnect 高级 SSL VPN 版许可证， AnyConnect 客户端软件提供相同的客户端功能集。

   如果在既定的 ASA 上存在以下许可证，则 AnyConnect 基础版许可证无法激活：AnyConnect 高级许可证 （所有类型）或高级终端评估许可证。但是，您可以在同一网络的不同 ASA 上运行 AnyConnect 基础版许可证和 AnyConnect 高级许可证。

   默认情况下，ASA 使用 AnyConnect 基础版许可证；但是，您可以禁用该许可证，使用 **webvpn**，然后使用 **no anyconnect-essentials** 命令来使用其他许可证。

   对于 AnyConnect 基础版许可证和 AnyConnect 高级许可证支持的功能的详细列表，请参阅 *AnyConnect 安全移动客户端功能、许可证和操作系统*：

   http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

配置经由 IPsec 的 L2TP 的先决条件

配置经由 IPsec 的 L2TP 有以下先决条件：

- 您可以为 L2TP/IPSec 连接配置默认组策略 (DfltGrpPolicy) 或用户定义的组策略。无论如何，必须将组策略配置为使用 L2TP/IPsec 隧道协议。如果没有为用户定义的组策略配置 L2TP/IPsec 隧道协议，请为 L2TP/IPsec 隧道协议配置 DfltGrpPolicy 并允许用户定义的组策略继承此属性。
- 如果您执行的是 “预共享密钥”身份验证，您需要配置默认连接配置文件 （隧道组） DefaultRAGroup。如果执行的是基于证书的身份验证，您可以使用用户定义的连接配置文件，可以根据证书标识符选择该配置文件。
- 需要在对等体之间建立 IP 连接。要测试连接、请尝试从您的终端 ping ASA 的 IP 地址并尝试从 ASA ping 您的终端的 IP 地址。
- 确保连接路径上任何位置 UDP 端口 1701 都未被阻止。
- 如果 Windows 7 终端设备使用指定 SHA 签名类型的证书进行身份验证，签名类型必须与 ASA 的签名类型，即 SHA1 或 SHA2 匹配。

准则和限制

此部分包括此功能的准则和限制。

情景模式准则

支持单情景模式。不支持多情景模式。

防火墙模式准则

仅支持路由防火墙模式。不支持透明模式。

故障转移准则

状态故障转移不支持经由 IPsec 的 L2TP 会话。

IPv6 准则

对于经由 IPsec 的 L2TP，没有本机 IPv6 隧道设置支持。

身份验证准则

ASA 在本地数据库上只支持 PPP 身份验证 PAP 和 Microsoft CHAP 版本 1 和 2。EAP 和 CHAP 由代理身份验证服务器执行。因此，如果远程用户属于用 **authentication eap-proxy** 或 **authentication chap** 命令配置的隧道组，并且 ASA 被配置为使用本地数据库，则该用户将无法连接。

支持的 PPP 身份验证类型

在 ASA 上经由 IPsec 的 L2TP 只支持 PPP 身份验证类型，如表 2-1 所示。

表 2-1　　AAA 服务器支持和 PPP 身份验证类型

AAA 服务器类型	支持的 PPP 身份验证类型
LOCAL	PAP、 MSCHAPv1、 MSCHAPv2
RADIUS	PAP、 CHAP、 MSCHAPv1、 MSCHAPv2、 EAP-Proxy
TACACS+	PAP、 CHAP、 MSCHAPv1
LDAP	PAP
NT	PAP
Kerberos	PAP
SDI	SDI

表 2-1　　PPP 身份验证类型特征

关键字	身份验证类型	特征
`chap`	CHAP	为了响应服务器质询，客户端将返回使用明文用户名的加密 [质询以及密码]。此协议比 PAP 更安全，但不加密数据。
`eap-proxy`	EAP	启用 EAP，它允许安全设备代理面向外部 RADIUS 身份验证服务器的 PPP 身份验证过程。
`ms-chap-v1` `ms-chap-v2`	Microsoft CHAP 版本 1 Microsoft CHAP 版本 2	与 CHAP 类似，但更安全，原因是服务器仅存储和比较加密密码，而不是像 CHAP 中存储和比较明文密码。此协议还为 MPPE 加密的数据生成密钥。
`pap`	PAP	在身份验证期间传递明文用户名和密码，并且不安全。

配置经由 IPsec 的 L2TP

本节提供必要的 ASA IKEv1 (ISAKMP) 策略设置，这些设置允许终端上操作系统集成的本机 VPN 客户端使用经由 IPsec 的 L2TP 协议与 ASA 进行 VPN 连接。

- IKEv1 阶段 1 — 使用 SHA1 哈希方法的 3DES 加密。
- IPSec 阶段 2 — 使用 MD5 或 SHA 哈希方法的 3DES 或 AES 加密。
- PPP 身份验证 — PAP、 MS-CHAPv1 或 MSCHAPv2 （首选）。
- 预共享密钥 （仅适用于 iPhone）。

详细 CLI 配置步骤

	命令	目的
步骤 1	`crypto ipsec transform-set` *`transform_name ESP_Encryption_Type ESP_Authentication_Type`* **示例：** `hostname(config)# crypto ipsec transform-set my-transform-set esp-des esp-sha-hmac`	使用特定 ESP 加密类型和身份验证类型创建转换集。

步骤 2	`crypto ipsec transform-set` *`trans_name`* `mode transport`
	
	示例：
	`hostname(config)# crypto ipsec transform-set my-transform-set mode transport`
		指示 IPsec 使用传输模式而不是隧道模式。

步骤 3	**vpn-tunnel-protocol** *tunneling_protocol*
	
	示例：
	`hostname(config)# group-policy DfltGrpPolicy attributes`
	`hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec`
		将 L2TP/IPsec 指定为 vpn 隧道协议。

步骤 4	**dns value** [**none** | *IP_primary* [*IP_secondary*]	（可选）指示自适应安全设备向组策略客户端发送 DNS 服务器 IP 地址。

	示例：
	`hostname(config)# group-policy DfltGrpPolicy attributes`
	`hostname(config-group-policy)# dns value 209.165.201.1 209.165.201.2`	

步骤 5	**wins-server value** [**none** | *IP_primary* [*IP_secondary*]]	（可选）指示自适应安全设备向组策略客户端发送 WINS 服务器 IP 地址。

	示例：
	`hostname(config)# group-policy DfltGrpPolicy attributes`
	`hostname (config-group-policy)# wins-server value 209.165.201.3 209.165.201.4`	

步骤 6	**tunnel-group** *name* **type remote-access** **示例：** `hostname(config)# tunnel-group sales-tunnel type remote-access`	创建连接配置文件 （隧道组）。

步骤 7	**default-group-policy** *name*
	
	示例：
	`hostname(config)# tunnel-group DefaultRAGroup general-attributes`
	`hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy`
		将组策略的名称与连接配置文件 （隧道组）关联。

	命令	目的
步骤 8	**ip local pool** *pool_name starting_address-ending_address* **mask** *subnet_mask* **示例：** hostname(config)# ip local pool sales_addresses 10.4.5.10-10.4.5.20 mask 255.255.255.0	（可选）创建 IP 地址池。
步骤 9	**address-pool** *pool_name* **示例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# address-pool sales_addresses	（可选）将 IP 地址池与连接配置文件（隧道组）关联。
步骤 10	**authentication-server-group** *server_group* **示例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL	为连接配置文件 （隧道组）指定对尝试经由 IPsec 的 L2TP 连接的用户进行身份验证的方法。如果不是使用 ASA 执行本地身份验证，并且您想要回退到本地身份验证，请在命令末尾添加 LOCAL。
步骤 11	authentication *auth_type* **示例：** hostname(config)# tunnel-group name ppp-attributes hostname(config-ppp)# authentication ms-chap-v1	为隧道组指定 PPP 身份验证协议。有关 PPP 身份验证的类型及其特征的详细信息，请参阅表 2-1。
步骤 12	**tunnel-group** *tunnel group name* **ipsec-attributes** **示例：** hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes hostname(config-tunnel-ipsec)# pre-shared-key *cisco123*	为您的连接配置文件 （隧道组）设置预共享密钥。
步骤 13	**accounting-server-group** *aaa_server_group* **示例：** hostname(config)# tunnel-group sales_tunnel general-attributes hostname(config-tunnel-general)# accounting-server-group sales_aaa_server	（可选）为连接配置文件 （隧道组）生成 L2TP 会话的 AAA 记帐开始和停止记录。
步骤 14	**l2tp tunnel hello** *seconds* **示例：** hostname(config)# l2tp tunnel hello 100	配置 hello 消息之间的间隔 （单位：秒）。范围是 10 到 300 秒。默认值为 60 秒。

	命令	目的
步骤 15	**crypto isakmp nat-traversal** *seconds* **示例：** hostname(config)# crypto isakmp enable hostname(config)# crypto isakmp nat-traversal 1500	（可选）启用 NAT 遍历，从而使 ESP 数据包可以传递通过一个或多个 NAT 设备。 如果您预计 NAT 设备后面会有多个 L2TP 客户端尝试与自适应安全设备进行经由 IPsec 的 L2TP 连接，则必须启用 NAT 遍历。 要在全局启用 NAT 遍历，请检查并确保在全局配置模式下启用 ISAKMP（您可以使用 **crypto isakmp enable** 命令进行启用），然后使用 **crypto isakmp nat-traversal** 命令。
步骤 16	strip-group strip-realm **示例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# strip-group hostname(config-tunnel-general)# strip-realm	（可选）配置隧道组切换。隧道组切换的目的是在用户使用代理身份验证服务器进行身份验证时为用户提供更好的建立 VPN 连接的机会。隧道组与连接配置文件同义。
步骤 17	**username** *name* **password** *password* **mschap** **示例：** hostname(config)# username xxxx password j!doe1 mschap	此示例显示使用用户名 xxxx 和密码 j!doe1 创建用户。mschap 选项指定在您输入密码后，会将密码转换为 Unicode，并使用 MD4 进行哈希处理。 只有在使用本地用户数据库时才需要使用此步骤。
步骤 18	**crypto isakmp policy** *priority* **示例：** hostname(config)# crypto isakmp policy 5	crypto isakmp policy 命令创建阶段 1 的 IKE 策略并为其分配一个编号。您可以为 IKE 策略配置几种不同的可配置参数。 需要 isakamp 策略才能让 ASA 可以完成 IKE 协商。 有关 Windows 7 本机 VPN 客户端的配置示例，请参阅第 2-11 页上的创建响应 Windows 7 提议的 IKE 策略。

创建响应 Windows 7 提议的 IKE 策略

Windows 7 L2TP/IPsec 客户端发送多个 IKE 策略提议来与 ASA 建立 VPN 连接。请定义一个以下 IKE 策略，以便从 Windows 7 VPN 本地客户端建立连接。

	命令	目的
步骤 1	第 2-8 页上的详细 CLI 配置步骤	执行截至步骤步骤 18 的详细 CLI 配置步骤操作步骤。增加此表中的其他步骤，为 Windows 7 本地 VPN 客户端配置 IKE 策略。
步骤 2	**show run crypto isakmp** **示例：** `hostname(config)# show run crypto isakmp`	显示属性和所有现有 IKE 策略的数量。
步骤 3	**crypto isakmp policy** number **示例：** `hostname(config)# crypto isakmp policy` *number* `hostname(config-isakmp-policy)#`	允许您配置 IKE 策略。该编号参数指定您配置的 IKE 策略的编号。此编号已列于 `show run crypto isakmp` 命令的输出中。
步骤 4	**authentication** **示例：** `hostname(config-isakmp-policy)# authentication pre-share`	设置 ASA 用于为每个 IPSec 对等体使用预共享密钥确定身份的身份验证方法。
步骤 5	**encryption** *type* **示例：** `hostname(config-isakmp-policy)# encryption {3des|aes|aes-256}`	选择保护两个 IPSec 对等体之间传输的数据的对称加密方法。对于 Windows 7，请选择 **3des**、 **aes**，对于 128 位 AES，也可选择 **aes-256**。
步骤 6	**hash** **示例：** `hostname(config-isakmp-policy)# hash sha`	选择确保数据完整性的哈希算法。对于 Windows 7，请为 SHA-1 算法指定 **sha**。
步骤 7	group **示例：** `hostname(config-isakmp-policy)# group 5`	选择 Diffie-Hellman 群标识符。对于 Windows 7，请为 1536 位 Diffie-Hellman 群指定 5。
步骤 8	lifetime **示例：** `hostname(config-isakmp-policy)# lifetime 86400`	以秒为单位指定 SA 寿命。对于 Windows 7，请指定 86400 秒，表示 24 小时。

详细 CLI 配置步骤

	命令	目的
步骤 1	`crypto ipsec` *ike_version* `transform-set` *transform_name ESP_Encryption_Type ESP_Authentication_Type* **示例：** `crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-des esp-sha-hmac`	使用特定 ESP 加密类型和身份验证类型创建转换集。

步骤 2	`crypto ipsec` *ike_version* `transform-set` *trans_name* `mode transport`
	
	示例：
	`crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport`
		指示 IPsec 使用传输模式而不是隧道模式。

步骤 3	**vpn-tunnel-protocol** *tunneling_protocol*
	
	示例：
	`hostname(config)# group-policy DfltGrpPolicy attributes`
	`hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec`
		将 L2TP/IPsec 指定为 vpn 隧道协议。

步骤 4	**dns value** [**none** | *IP_primary* [*IP_secondary*]
	
	示例：
	`hostname(config)# group-policy DfltGrpPolicy attributes`
	`hostname(config-group-policy)# dns value 209.165.201.1 209.165.201.2`
		（可选）指示自适应安全设备向组策略客户端发送 DNS 服务器 IP 地址。

步骤 5	**wins-server value** [**none** | *IP_primary* [*IP_secondary*]]
	
	示例：
	`hostname(config)# group-policy DfltGrpPolicy attributes`
	`hostname (config-group-policy)# wins-server value 209.165.201.3 209.165.201.4`
		（可选）指示自适应安全设备向组策略客户端发送 WINS 服务器 IP 地址。

步骤 6	**ip local pool** *pool_name starting_address-ending_address* **mask** *subnet_mask* **示例：** `hostname(config)# ip local pool sales_addresses 10.4.5.10-10.4.5.20 mask 255.255.255.0`	（可选）创建 IP 地址池。

步骤 7	**address-pool** *pool_name*
	
	示例：
	`hostname(config)# tunnel-group DefaultRAGroup general-attributes`
	`hostname(config-tunnel-general)# address-pool sales_addresses`
		（可选）将 IP 地址池与连接配置文件（隧道组）关联。

	命令	目的
步骤 8	**tunnel-group** *name* **type remote-access** **示例：** hostname(config)# tunnel-group sales-tunnel type remote-access	创建连接配置文件 （隧道组）。
步骤 9	**default-group-policy** *name* **示例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy	将组策略的名称与连接配置文件 （隧道组）关联。
步骤 10	**authentication-server-group** *server_group* [local] **示例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL	为连接配置文件 （隧道组）指定对尝试经由 IPsec 的 L2TP 连接的用户进行身份验证的方法。如果不是使用 ASA 执行本地身份验证，并且您想要回退到本地身份验证，请在命令末尾添加 LOCAL。
步骤 11	**authentication** *auth_type* **示例：** hostname(config)# tunnel-group *name* ppp-attributes hostname(config-ppp)# authentication ms-chap-v1	为隧道组指定 PPP 身份验证协议。有关 PPP 身份验证的类型及其特征的详细信息，请参阅表 2-1。
步骤 12	**tunnel-group** *tunnel group name* **ipsec-attributes** **示例：** hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes hostname(config-tunnel-ipsec)# ikev1 pre-shared-key *cisco123*	为您的连接配置文件 （隧道组）设置预共享密钥。
步骤 13	**accounting-server-group** *aaa_server_group* **示例：** hostname(config)# tunnel-group sales_tunnel general-attributes hostname(config-tunnel-general)# accounting-server-group sales_aaa_server	（可选）为连接配置文件 （隧道组）生成 L2TP 会话的 AAA 记帐开始和停止记录。
步骤 14	**l2tp tunnel hello** *seconds* **示例：** hostname(config)# l2tp tunnel hello 100	配置 hello 消息之间的间隔 （单位：秒）。范围是 10 到 300 秒。默认间隔为 60 秒。

	命令	目的
步骤 15	**crypto isakmp nat-traversal** *seconds* **示例：** hostname(config)# crypto isakmp enable hostname(config)# crypto isakmp nat-traversal 1500	（可选）启用 NAT 遍历，从而使 ESP 数据包可以传递通过一个或多个 NAT 设备。 如果您预计 NAT 设备后面会有多个 L2TP 客户端尝试与自适应安全设备进行经由 IPsec 的 L2TP 连接，则必须启用 NAT 遍历。 要在全局启用 NAT 遍历，请检查并确保在全局配置模式下启用 ISAKMP （您可以使用 **crypto isakmp enable** 命令进行启用），然后使用 **crypto isakmp nat-traversal** 命令。
步骤 16	strip-group strip-realm **示例：** hostname(config)# tunnel-group DefaultRAGroup general-attributes hostname(config-tunnel-general)# strip-group hostname(config-tunnel-general)# strip-realm	（可选）配置隧道组切换。隧道组切换的目的是在用户使用代理身份验证服务器进行身份验证时为用户提供更好的建立 VPN 连接的机会。隧道组与连接配置文件同义。
步骤 17	**username** *name* **password** *password* **mschap** **示例：** asa2(config)# username jdoe password j!doe1 mschap	此示例显示使用用户名 jdoe 和密码 j!doe1 创建用户。 mschap 选项指定在您输入密码后，会将密码转换为 Unicode，并使用 MD4 进行哈希处理。 只有在使用本地用户数据库时才需要使用此步骤。
步骤 18	**crypto ikev1 policy** *priority* **group** *Diffie-Hellman Group* **示例：** hostname(config)# crypto ikev1 policy 5 hostname(config-ikev1-policy)# group 5	crypto isakmp policy 命令创建阶段 1 的 IKE 策略并为其分配一个编号。您可以为 IKE 策略配置几种不同的可配置参数。 您还可以为该策略指定一个 Diffie-Hellman 群。 需要 isakamp 策略才能让 ASA 可以完成 IKE 协商。 有关 Windows 7 本机 VPN 客户端的配置示例，请参阅第 2-15 页上的创建响应 Windows 7 提议的 IKE 策略。

创建响应 Windows 7 提议的 IKE 策略

Windows 7 L2TP/IPsec 客户端发送多个 IKE 策略提议来与 ASA 建立 VPN 连接。请定义一个以下 IKE 策略，以便从 Windows 7 VPN 本地客户端建立连接。

	命令	目的
步骤 1	第 2-12 页上的详细 CLI 配置步骤	执行截至步骤步骤 18 的详细 CLI 配置步骤操作步骤。增加此表中的其他步骤，为 Windows 7 本地 VPN 客户端配置 IKE 策略。
步骤 2	**show run crypto ikev1** **示例：** `hostname(config)# show run crypto ikev1`	显示属性和所有现有 IKE 策略的数量。
步骤 3	**crypto ikev1 policy** number **示例：** `hostname(config)# crypto ikev1 policy` *number* `hostname(config-ikev1-policy)#`	允许您配置 IKE 策略。该编号参数指定您配置的 IKE 策略的编号。此编号已列于 `show run crypto ikev1` 命令的输出中。
步骤 4	**authentication** **示例：** `hostname(config-ikev1-policy)# authentication pre-share`	设置 ASA 用于为每个 IPSec 对等体使用预共享密钥确定身份的身份验证方法。
步骤 5	**encryption** *type* **示例：** `hostname(config-ikev1-policy)# encryption {3des|aes|aes-256}`	选择保护两个 IPSec 对等体之间传输的数据的对称加密方法。对于 Windows 7，请选择 **3des**、**aes**，对于 128 位 AES，也可选择 **aes-256**。
步骤 6	**hash** **示例：** `hostname(config-ikev1-policy)# hash sha`	选择确保数据完整性的哈希算法。对于 Windows 7，请为 SHA-1 算法指定 **sha**。

步骤 7	`group`
	
	示例：
	`hostname(config-ikev1-policy)# group 5`
		选择 Diffie-Hellman 群标识符。您可以为 aes、aes-256 或 3des 加密类型指定 5。您只可以为 3des 加密类型指定 2。

步骤 8	`lifetime`
	
	示例：
	`hostname(config-ikev1-policy)# lifetime 86400`
		以秒为单位指定 SA 寿命。对于 Windows 7，请指定 86400 秒，表示 24 小时。

使用 ASA 8.2.5 的经由 IPsec 的 L2TP 配置示例

以下示例显示了确保 ASA 与任意操作系统上的本地 VPN 客户端兼容的配置文件命令。

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
group-policy sales_policy internal
group-policy sales_policy attributes
    wins-server value 209.165.201.3 209.165.201.4
    dns-server value 209.165.201.1 209.165.201.2
    vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
    default-group-policy sales_policy
    address-pool sales_addresses
tunnel-group DefaultRAGroup ipsec-attributes
    pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
    no authentication pap
    authentication chap
    authentication ms-chap-v1
    authentication ms-chap-v2
crypto ipsec transform-set trans esp-3des esp-sha-hmac
crypto ipsec transform-set trans mode transport
crypto dynamic-map dyno 10 set transform-set set trans
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto isakmp enable outside
crypto isakmp policy 10
    authentication pre-share
    encryption 3des
    hash sha
    group 2
    lifetime 86400
```

使用 ASA 8.4.1 及更高版本的经由 IPsec 的 L2TP 配置示例

以下示例显示了确保 ASA 与任意操作系统上的本地 VPN 客户端兼容的配置文件命令。

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
group-policy sales_policy internal
group-policy sales_policy attributes
    wins-server value 209.165.201.3 209.165.201.4
    dns-server value 209.165.201.1 209.165.201.2
    vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
    default-group-policy sales_policy
    address-pool sales_addresses
tunnel-group DefaultRAGroup ipsec-attributes
    pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
    no authentication pap
    authentication chap
    authentication ms-chap-v1
    authentication ms-chap-v2
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set trans
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
```

```
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
```

经由 IPsec 的 L2TP 功能历史记录

表 2-2 列出了此功能的版本历史记录。

表 2-2　　经由 IPsec 的 L2TP 功能历史记录

功能名称	版本	功能信息
经由 IPsec 的 L2TP	7.2(1)	经由 IPsec 的 L2TP 在单一平台上提供部署和管理 L2TP VPN 解决方案以及 IPsec VPN 和防火墙服务的功能。 在远程访问方案中，配置经由 IPsec 的 L2TP 的主要优点在于远程用户可以通过公用 IP 网络访问 VPN，而无需使用网关或专线，实际上就可以利用 POTS 从任何位置启用远程访问。另一个优势是 VPN 访问的唯一客户端要求是使用带 Microsoft 拨号网络 (DUN) 的 Windows。不需要思科 VPN 客户端软件等任何其他客户端软件。 已引入或修改以下命令：**authentication eap-proxy**、**authentication ms-chap-v1**、**authentication ms-chap-v2**、**authentication pap**、**l2tp tunnel hello**、**vpn-tunnel-protocol l2tp-ipsec**。

第 3 章

通用 VPN 参数

虚拟专用网络的 ASA 实施包含不能简单归类的有用功能。本章会对这些功能中的部分功能进行介绍。其中包含以下各节：

配置 IPsec 以绕过 ACL

除非指定是无客户端 （基于浏览器）的 SSL VPN，否则本章中的 SSL VPN 指 SSL VPN 客户端（AnyConnect 2.x 或其前身 SVC 1.x）。要在不检查用于源和目标接口的 ACL 的情况下，允许来自 IPsec 隧道的任意数据包，可以在全局配置模式下输入 **sysopt connection permit-vpn** 命令。

如果您使用位于 ASA 之后的单独 VPN 集中器，并且想要最大限度地提高 ASA 的性能，您可能想要绕过用于 IPsec 流量的接口 ACL。通常，您会通过使用 **access-list** 命令创建允许 IPsec 数据包的 ACL，并将其应用至源接口。使用 ACL 更为安全，因为您可以指定想要允许其通过 ASA 的确切流量。

语法为 **sysopt connection permit-vpn**。该命令没有关键字或参数。

以下示例在不检查 ACL 的情况下，允许 IPsec 流量通过 ASA：

```
hostname(config)# sysopt connection permit-vpn
```

注 配置 **no sysopt connection permit-vpn** 时，尽管客户端在外部接口上有调用 **deny ip any any** ACL 的访问组，也会允许来自该客户端的经过解密的直通流量。

想要结合使用 **no sysopt permit-vpn** 命令和外部接口上的访问控制列表 (ACL)，从而控制经由站点对站点或远程访问 VPN 对受保护网络进行访问的用户，将不会成功。

在这种情况下，当启用了内部管理访问时，则不会应用该 ACL，用户仍然可以使用 SSH 连接至 ASA。流向内部网络中主机的流量会被该 ACL 正确地阻止，但流向内部接口的经过解密的直通流量不会被阻止。

ssh 和 **http** 命令具有比 ACL 更高的优先级。也就是说，要拒绝来自 VPN 会话的流向设备的 SSH、 Telnet 或 ICMP 流量，可以使用 **ssh**、 **telnet** 和 **icmp** 命令。

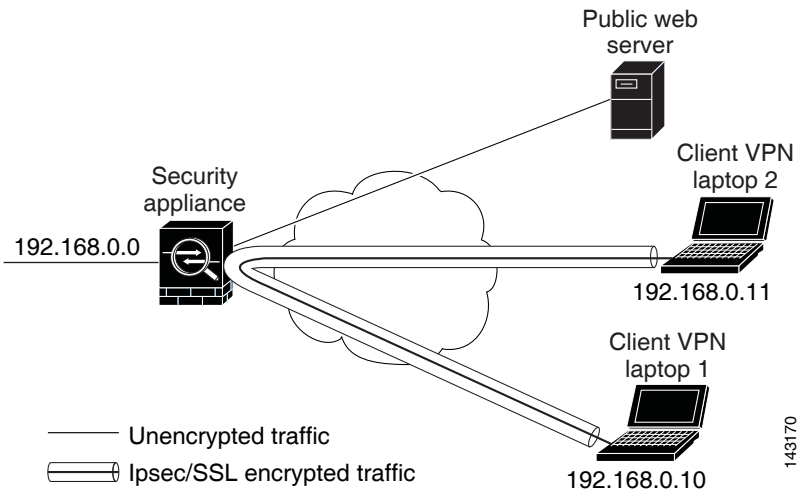
允许接口内流量 (Hairpinning)

ASA 包含一个功能，该功能允许受 IPsec 保护的流量出入相同接口，从而使得 VPN 客户端可以向另一个 VPN 用户发送此类流量。该功能也称为 “hairpinning”，可以将其视为通过 VPN 集线器 (ASA) 连接的 VPN 轮辐 （客户端）。

在另一个应用中， Hairpinning 可以将传入 VPN 流量通过与未加密流量相同的接口重定向回来。例如，对于没有分割隧道，但需要同时访问 VPN 和浏览网络的 VPN 客户端来说，这非常有用。

图 3-1 显示了 VPN 客户端 1 发送安全 IPsec 流量至 VPN 客户端 2，同时还将未加密流量发送至公用网络服务器。

图 3-1　　使用 Hairpinning 的接口内功能的 VPN 客户端



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

该命令的语法为 **same-security-traffic permit** {**inter-interface** | **intra-interface**}。

以下示例展示了如何启用接口内流量：

```
hostname(config)# same-security-traffic permit intra-interface
hostname(config)#
```

注　您可以使用 **same-security-traffic** 命令，但使用 **inter-interface** 参数，以便允许拥有相同安全级别的接口之间进行通信。该功能不是特定于 IPsec 连接的功能。有关详细信息，请参阅本指南的 “配置接口参数” 一章。

要使用 Hairpinning，正如下一节所讨论的，您必须将适当的 NAT 规则应用至 ASA 接口。

接口内流量的 NAT 注意事项

要使 ASA 能够将未加密的流量通过接口回送，您必须为该接口启用 NAT，以便公用可路由地址替代您的专用 IP 地址（除非您已在本地 IP 地址池中使用公用 IP 地址）。以下示例将接口 PAT 规则应用至来自客户端 IP 池的流量：

```
hostname(config)# ip local pool clientpool 192.168.0.10-192.168.0.100
hostname(config)# object network vpn_nat
hostname(config-network-object)# subnet 192.168.0.0 255.255.255.0
hostname(config-network-object)# nat (outside,outside) interface
```

然而，当 ASA 将加密 VPN 流量通过此相同接口回送时，NAT 是可选的。在使用或不使用 NAT 的情况下，VPN 对 VPN Hairpinning 均可正常工作。要将 NAT 应用至所有传出流量，请仅实施以上命令。要使 VPN 对 VPN 流量免于 NAT，请添加为 VPN 对 VPN 流量实施 NAT 免除的命令 （至以上示例），例如：

```
hostname(config)# nat (outside,outside) source static vpn_nat vpn_nat destination static
vpn_nat vpn_nat
```

有关 NAT 规则的详细信息，请参阅本指南的 “应用 NAT”一章。

设置活动 IPsec 或 SSL VPN 会话的最大数量

要将 VPN 会话数限制为低于 ASA 允许的值，可以在全局配置模式下输入 **vpn-sessiondb** 命令：

vpn-sessiondb {**max-anyconnect-premium-or-essentials-limit** <*number*> |
max-other-vpn-limit <*number*>}

max-anyconnect-premium-or-essentials-limit 关键字指定 AnyConnect 会话的最大数量，取值范围为 1 至许可证允许的最大会话数。

max-other-vpn-limit 关键字指定 AnyConnect 客户端会话之外的其他 VPN 会话的最大数量，取值范围为 1 至许可证允许的最大会话数。这包括思科 VPN 客户端 (IPsec IKEv1)、LAN 对 LAN VPN 和无客户端 SSL VPN 会话。

该限制会影响计算得出的 VPN 负载平衡的负载百分比。

以下示例显示如何设置值为 450 的最大 Anyconnect VPN 会话数限制：

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 450
hostname(config)#
```

使用客户端更新确保可接受的 IPsec 客户端修订级别

注　本节中的信息仅适用于 IPsec 连接。

客户端更新功能使得处于中央位置的管理员能够自动通知 VPN 客户端用户，是时候更新 VPN 客户端软件和 VPN 3002 硬件客户端映像。

远程用户可能正在使用已过时的 VPN 软件或硬件客户端版本。您可以随时使用 **client-update** 命令来启用更新客户端修订版本的功能；指定更新适用的客户端类型和修订版本号；提供可以从中获得更新的 URL 或 IP 地址；对于 Windows 客户端，可以可选地通知用户，他们应更新其 VPN 客户端版本。对于 Windows 客户端，您可以为用户提供一种机制来完成该更新。对于 VPN 3002 硬件客户端用户，更新将会在不进行通知的情况下自动进行。该命令仅适用于 IPsec 远程访问隧道组类型。

要执行客户端更新，可以在通用配置模式或隧道组 IPsec 属性配置模式下输入 **client-update** 命令。如果客户端已在运行修订版本号列表上的软件版本，则不需要更新其软件。如果客户端未运行列表上的软件版本，则应进行更新。以下操作步骤说明如何执行客户端更新：

步骤 1　在全局配置模式下，输入此命令以启用客户端更新：

```
hostname(config)# client-update enable
hostname(config)#
```

步骤 2　在全局配置模式下，指定您想要应用至特定类型的所有客户端的客户端更新参数。也就是说，可以指定客户端的类型，可从中获得经过更新的映像的 URL 或 IP 地址，以及该客户端的可接受的修订版本号。您可以指定最多四个用逗号分隔的修订版本号。

如果用户的客户端修订版本号与某个指定的修订版本号匹配，则不需要更新客户端。该命令跨整个 ASA，为所有指定类型的客户端指定客户端更新值。

请使用此语法：

```
hostname(config)# client-update type type url url-string rev-nums rev-numbers
hostname(config)#
```

可用的客户端类型为 **win9X**（包括 Windows 95、Windows 98 和 Windows ME 平台）、**winnt**（包括 Windows NT 4.0、Windows 2000 和 Windows XP 平台）、**windows**（包括所有基于 Windows 的平台），以及 **vpn3002**（VPN 3002 硬件客户端）。

如果客户端已在运行修订版本号列表上的软件版本，则不需要更新其软件。如果客户端未运行列表上的软件版本，则应进行更新。您可以指定这些客户端更新条目中的最多三个条目。关键字 **windows** 涵盖了所有允许的 Windows 平台。如果您指定了 **windows**，则不要指定单个 Windows 客户端类型。

注　对于所有的 Windows 客户端，您必须使用协议 http:// 或 https:// 作为 URL 的前缀。对于 VPN 3002 硬件客户端，您必须指定协议 tftp:// 来进行代替。

以下示例为远程访问隧道组配置客户端更新参数。它指定了修订版本号 4.6.1 以及用于检索更新的 URL，该 URL 为 https://support/updates。

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.6.1
hostname(config)#
```

另外，您可以仅为单个隧道组，而不是特定类型的所有客户端配置客户端更新。（请参阅步骤 3）。

VPN 3002 客户端无需用户介入即可进行更新，并且用户不会收到任何通知消息。以下示例仅适用于 VPN 3002 硬件客户端。在隧道组 IPsec 属性配置模式下输入的命令为 IPsec 远程访问隧道组 **salesgrp** 配置了客户端更新参数。该示例指定了修订版本号 4.7，并使用 TFTP 协议来从采用 IP 地址 192.168.1.1 的站点检索经过更新的软件：

```
hostname(config)# tunnel-group salesgrp type ipsec-ra
hostname(config)# tunnel-group salesgrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type vpn3002 url tftp:192.168.1.1 rev-nums
4.7
hostname(config-tunnel-ipsec)#
```

注　您可以通过在 URL 末尾包含应用名称，来让浏览器自动启动应用；例如：**https://support/updates/vpnclient.exe。**

步骤 3　为特定 ipsec-ra 隧道组定义客户端更新参数集。

在隧道组 IPsec 属性模式下，指定隧道组名称及其类型、从中获取经过更新的映像的 URL 或 IP 地址，以及修订版本号。如果用户的客户端修订版本号与某个指定的修订版本号匹配，则不需要更新该客户端，例如，对于 Windows 客户端，输入此命令：

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type windows url https://support/updates/
rev-nums 4.6.1
hostname(config-tunnel-ipsec)#
```

步骤 4　（可选）向拥有已过时 Windows 客户端的活动用户发送通知，其客户端需要更新。对于这些用户，系统将会显示一个弹出窗口，让他们有机会启动浏览器，并从您在 URL 中指定的站点下载经过更新的软件。此消息中您可以配置的唯一部分是 URL。（请参阅步骤 2 或 3）。不处于活动状态的用户将在他们下一次登录时获得通知消息。您可以将此通知发送至所有隧道组上的所有活动客户端，也可以将其发送至特定隧道组上的客户端。例如，要通知所有隧道组上的所有活动客户端，可以在 Privileged EXEC 模式下输入以下命令：

```
hostname# client-update all
hostname#
```

如果用户的客户端修订版本号与某个指定的修订版本号匹配，则不需要更新客户端，并且不向用户发送通知消息。 VPN 3002 客户端无需用户介入即可进行更新，并且用户不会收到任何通知消息。

注　如果您将客户端更新类型指定为 **windows**（指定所有基于 Windows 的平台），而且随后想要为相同实体输入客户端更新类型 **win9x** 或 **winnt**，您必须先使用此命令的 **no** 形式，移除 Windows 客户端类型，然后使用新的客户端更新命令来指定新的客户端类型。

将 NAT 分配的 IP 实施至公用 IP 连接

在极少数情况下，您可能想要使用 VPN 对等设备在内部网络上的真实 IP 地址，而非已分配的本地 IP 地址。通常在使用 VPN 的情况下，会给定对等体分配的本地 IP 地址来访问内部网络。但是，在例如内部服务器和网络安全基于对等体的真实 IP 地址的情况下，可能要将本地 IP 地址重新转换为对等体的真实公用地址。

思科 ASA 55xx 引入了一种方法，可以将内部 / 受保护网络上的 VPN 客户端的已分配 IP 地址转换为其公用 （源） IP 地址。该功能支持内部网络上的目标服务器 / 服务和网络安全策略要求使用 VPN 客户端的公用 / 源 IP，而不是内部企业网络上的已分配 IP 进行通信的场景。

可以在每个隧道组一个接口的基础上启用此功能。当 VPN 会话已建立或断开连接时，动态添加或删除对象 NAT 规则。

限制

因为路由问题，除非您知道您需要此功能，否则我们不建议使用此功能。

- 仅支持旧版思科 VPN 客户端 (IKEv1) 和 AnyConnect 客户端。
- 流向公用 IP 地址的返回流量必须路由回 ASA，以便可以应用 NAT 策略和 VPN 策略。
- 仅支持 IPv4 的已分配地址和公用地址。
- 不支持 NAT/PAT 设备之后的多个对等体。
- 不支持负载平衡 （因为路由问题）。
- 不支持漫游。

详细步骤

步骤 1　在全局配置模式下，输入 **tunnel general**。

步骤 2　使用此语法来启用地址转换：

```
hostname(config-tunnel-general)# nat-assigned-to-public-ip interface
```

此命令将已分配 IP 地址的 NAT 策略动态安装至源的公用 IP 地址。*interface* 用于确定应用 NAT 的位置。

步骤 3　使用此语法来禁用地址转换：

```
hostname(config-tunnel-general)# no nat-assigned-to-public-ip
```

显示 VPN NAT 策略

地址转换使用基础对象 NAT 机制；因此，VPN NAT 策略会如同手动配置的对象 NAT 策略一样显示。此示例将 95.1.226.4 用作已分配的 IP，将 75.1.224.21 用作对等体的公用 IP：

```
hostname# show nat
Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
    translate_hits = 315, untranslate_hits = 315

prompt# show nat detail

Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
    translate_hits = 315, untranslate_hits = 315
    Source - Origin: 95.1.226.4/32, Translated: 75.1.224.21/32
```

Outside 是 AnyConnect 客户端连接至的接口，而 *inside* 是特定于新隧道组的接口。

注　因为 VPN NAT 策略是动态的，并且不会被添加至配置，所以在 show run 对象和 show run nat 报告中， VPN NAT 对象和 NAT 策略会被隐藏。

了解负载平衡

如果您拥有一个远程访问配置，并且将在其中使用相同网络上连接的两台或更多 ASA 或者 VPN 集中器，则可以将这些设备配置为共享其会话负载。此功能称为*负载平衡*。要实施负载平衡，您可以将相同专用 LAN 对 LAN 网络、专用子网和公用子网上的两台或更多设备逻辑分组为*虚拟集群*。

虚拟集群中的所有设备都可以承载会话负载。负载平衡可以将会话流量定向至集群中负载最低的设备，该集群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。

虚拟集群中的一台设备，即*虚拟集群主用设备*，会将传入流量定向至称为*备用设备*的其他设备。虚拟集群主用设备会监控集群中的所有设备、跟踪其忙碌程度，然后相应地分配会话负载。虚拟集群主用设备这一角色没有与某台物理设备绑定；它可以在设备之间切换。例如，如果当前的虚拟集群主用设备发生故障，该集群的一台备用设备会接管该角色，立即成为新的虚拟集群主用设备。

对于外部客户端，虚拟集群显示为单一*虚拟集群 IP 地址*。此 IP 地址不与特定物理设备绑定。此地址属于当前的虚拟集群主用设备，这使得其成为虚拟地址。VPN 客户端会尝试建立连接，先与此虚拟集群 IP 地址连接。随后，虚拟集群主用设备会将集群中负载最低的可用主机的公用 IP 地址，发送回客户端。在第二个事务 （对用户透明）中，客户端会直接连接至该主机。这样，虚拟集群主用设备就能在资源之间均匀、高效地定向流量。

注　思科 VPN 客户端或思科 3002 硬件客户端之外的所有客户端应如常直接连接至 ASA ；它们不使用虚拟集群 IP 地址。

如果集群中的一台设备发生故障，终止的会话可以立即重新连接到虚拟集群 IP 地址。随后，虚拟集群主用设备会将这些连接，定向至集群中的另一活动设备。如果虚拟集群主用设备自身发生故障，该集群中的一台备用设备会作为新的虚拟会话主用设备，立即自动进行接管。即便该集群中的多台设备发生故障，只要该集群中的任一设备正常运行，并且可用，用户仍然可以继续与该集群连接。

比较负载平衡和故障转移

负载平衡和故障转移功能都是高可用性功能，但是它们的工作方式不同，并且具有不同的要求。在某些情况下，您可以同时使用负载平衡和故障转移。以下部分介绍这些功能之间的差异。

负载平衡

负载平衡是在虚拟集群中的设备之间，合理分配远程访问 VPN 流量的机制。它基于流量的简单分配，而不考虑吞吐量或其他因素。负载平衡集群由两台或更多的设备组成，一台设备是虚拟主用设备，其他设备为备用设备。这些设备不需要是完全相同的类型，也不需要具有相同的软件版本和配置。

虚拟集群中的所有活动设备都可以承载会话负载。负载平衡会将流量定向至集群中负载最低的设备，从而在所有设备之间分配负载。这样可以高效地利用系统资源，提供更高的性能和高可用性。

故障转移

故障转移配置需要两台一致的 ASA，并且它们通过专用故障转移链路，或有状态故障转移链路相互连接。主用接口和设备的运行状况会受到监控，以便确定满足特定故障转移条件的时刻。如果这些条件得到满足，则会进行故障转移。故障转移同时支持 VPN 和防火墙配置。

ASA 支持两种故障转移配置：主用 / 主用故障转移和主用 / 备用故障转移。

使用主用 / 主用故障转移时，两台设备都可以传送网络流量。这不是真正的负载平衡，尽管看似具有相同的效果。发生故障转移时，剩余的主用设备会根据配置的参数接管整合流量的传送。因此，配置主用 / 主用故障转移时，您必须确保两台设备的合并流量在每台设备的容量之内。

使用主用 / 备用故障转移时，只有一台设备会传送流量，而另一台设备会在备用状态下进行等待，不会传送流量。主用 / 备用故障转移允许您用第二台 ASA 来沿用发生故障的设备的功能。当主用设备发生故障时，它将变为备用状态，而备用设备会变为主用状态。变为活动状态的设备会采用发生故障的设备的 IP 地址 （或者，对于透明防火墙，管理 IP 地址）和 MAC 地址，并开始传送流量。此时，处于备用状态的设备会接管主用设备的备用 IP 地址。如果主用设备发生故障，则由备用设备接管，而且不会给客户端 VPN 隧道带来任何干扰。

实施负载平衡

说明　启用负载平衡涉及以下操作：

- 建立集群的公用虚拟集群 IP 地址、UDP 端口（如需要）和 IPsec 共享密钥，从而配置负载平衡集群。您可以为集群中的每台设备配置这些相同的值。
- 在设备上启用负载平衡，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。

注　VPN 负载平衡需要一个活动的 3DES/AES 许可证。在启用负载平衡之前， ASA 将检查此加密许可证是否存在。如果没有检测到活动的 3DES 或 AES 许可证，ASA 会阻止启用负载平衡，也会阻止负载平衡系统进行 3DES 的内部配置，除非许可证允许此使用。

先决条件

负载平衡默认为已禁用。您必须显式地启用负载平衡。

您必须先配置公用 （外部）和专用 （内部）接口，并事先配置虚拟集群 IP 地址所引用的接口。您可以使用 **interface** 和 **nameif** 命令，来为这些接口配置不同的名称。本节中的后续引用使用内部和外部名称。

加入集群的所有设备都必须共享同一个集群特定值：IP 地址、加密设置、加密密钥和端口。

合格平台

负载平衡集群可以包含 ASA 型号 ASA 5512-X （带安全增强型许可证）以及 5515-X 型号和更高型号。您还可以在集群中包含思科 VPN 3000 系列集中器。虽然混合配置是可行的，但如果集群是同构的，管理通常更为简单。

合格客户端

负载平衡仅在使用以下客户端发起的远程会话上有效：

- 思科 AnyConnect VPN 客户端 （2.0 版本及更高版本）
- 思科 VPN 客户端 （3.0 版本及更高版本）
- 思科 ASA 5505 ASA （充当 Easy VPN 客户端时）
- 思科 VPN 3002 硬件客户端 （3.5 版本或更高版本）
- 思科 PIX 501/506E，充当 Easy VPN 客户端时

- 支持 IKE 重定向的思科 IOS EZVPN 客户端设备 (IOS 831/871)
- 无客户端 SSL VPN （不是客户端）

负载平衡可与 IPsec 客户端和 SSL VPN 客户端与无客户端会话配合使用。所有其他 VPN 连接类型 （L2TP、 PPTP、 L2TP/IPsec），包括 LAN 对 LAN，都可以连接至在其上启用了负载平衡的 ASA，但是它们不能参与负载平衡。

VPN 负载平衡算法

主用设备会以 IP 地址的升序维持备用集群成员的已排序列表。每个备用集群成员的负载会计算为整数百分比 （活动会话的数量）。 AnyConnect 非活动会话不会计入负载平衡的 SSL VPN 负载。主用设备将 IPsec 和 SSL VPN 隧道重定向至负载最低的设备，直到其百分比值比其余设备高出 1%。当所有备用集群成员的百分比值都比主用设备高出 1% 时，主用设备会将负载重定向至自身。

例如，如果您有一个主用和两个备用集群成员，则以下循环适用：

注　所有节点的百分比值都从 0% 开始，而且所有百分比值都会四舍五入。

1. 如果所有成员的负载都比主用设备高出 1%，则主用设备会接受连接。
2. 如果主用设备没有接受连接，负载百分比值最低的任一备用设备会接受会话。
3. 如果所有的成员都拥有相同百分比的负载，会话数量最少的备用设备会获得会话。
4. 如果所有的成员都拥有相同百分比的负载，以及相同数量的会话，则 IP 地址最少的设备会获得会话。

VPN 负载平衡集群配置

负载平衡集群由受到以下限制的相同版本、混合版本的 ASA 以及 VPN 3000 集中器，或者这些设备的混合体组成：

- 包含相同版本 ASA 或所有 VPN 3000 集中器的负载平衡集群，可以为混合的 IPsec、AnyConnect 和无客户端 SSL VPN 会话进行负载平衡。
- 包含两个相同版本 ASA 和 VPN 3000 集中器的负载平衡集群，可以为混合的 IPsec、AnyConnect 和无客户端 SSL VPN 的客户端会话与无客户端会话进行负载平衡。
- 包含混合版本 ASA 或相同版本 ASA 以及 VPN 3000 集中器或二者的负载平衡集群，仅可以支持 IPsec 会话。然而，在这样的配置中， ASA 可能无法到达其全部的 IPsec 容量。方案 1：无 SSL VPN 连接的混合集群对该状况进行了说明。

从 7.1(1) 版本起，在确定集群中的每台设备所承载的负载方面， IPsec 和 SSL VPN 会话的数量和权重意义相当。这与 ASA 7.0(x) 版本软件和 VPN 3000 集中器的负载平衡计算不同。这两种平台都使用加权算法，在某些硬件平台上，会以不同于 IPsec 会话负载的方式计算 SSL VPN 会话。

该集群的虚拟主用设备会将会话请求分配至该集群的成员。 ASA 会同等地对待所有会话 （SSL VPN 或 IPsec 会话），并相应地分配它们。您可以将允许的 IPsec 和 SSL VPN 会话的数量配置为您的配置和许可证允许的最大数量。有关如何设置这些限制的描述，请参阅配置 VPN 会话限制。

我们已测试过负载平衡集群中的最多十个节点。更大的集群可能能够正常工作，但是我们不正式支持此类拓扑。

部分典型的混合集群方案

如果您拥有混合的配置 — 也就是说，如果您的负载平衡集群包含运行混合的 ASA 软件版本的设备，或者至少一台运行 ASA 7.1(1) 版本或更高版本的 ASA 以及 VPN 3000 集中器 — 如果初始的集群主用设备发生故障，另一设备作为主用设备进行接管，则加权算法之间的差异将会成为问题。

对于在包含运行混合的 ASA 7.1(1) 版本和 ASA 7.0(x) 版本软件的 ASA 以及 VPN 3000 系列集中器的集群中使用 VPN 负载平衡，以下方案进行了说明。

方案 1：无 SSL VPN 连接的混合集群

在此方案中，集群由 ASA 和 VPN 3000 集中器混合组成。部分 ASA 集群对等体在运行 ASA 7.0(x) 版本软件，部分对等体在运行 7.1(1) 版本软件。7.1(1) 版本之前的版本和 VPN 3000 对等体没有任何 SSL VPN 连接， 7.1(1) 版本集群对等体仅拥有基本 SSL VPN 许可证，该许可证允许两个 SSL VPN 会话，但没有 SSL VPN 连接。在这种情况下，所有连接均为 IPsec 连接，负载平衡可以正常工作。

两个 SSL VPN 许可证对正在利用最大 IPsec 会话限制的用户的影响极小，仅在 VPN 3000 集中器是集群主用设备时，才会有较大的影响。通常，在混合集群中， ASA 上的 SSL VPN 许可证的数量越少，对 ASA 7.1(1) 能够在仅有 IPsec 会话的场景中达到其 IPsec 会话限制，造成的影响就越小。

场景 2：处理 SSL VPN 连接的混合集群

假设，例如，正在运行 ASA 7.1(1) 版本软件的 ASA 是初始的集群主用设备，然后该设备发生故障。集群中的另一设备作为主用设备自动进行接管，并应用其自身的负载平衡算法，来确定集群内的处理器负载。运行 ASA 7.1(1) 版本软件的集群主用设备，不能以该软件提供的方式之外的任何其他方式确定会话负载的权重。因此，它不能正确地向运行早期版本软件的 ASA 设备以及 VPN 3000 集中器分配 IPsec 和 SSL VPN 会话负载的组合。相反地，充当集群主用设备的 VPN 3000 集中器也不能向 ASA 7.1(1) 版本的 ASA 正确地分配负载。以下场景对此困境进行了说明。

此场景与上一场景类似，在上一场景中，集群由 ASA 和 VPN 3000 集中器混合组成。部分 ASA 集群对等体在运行 ASA 7.0(x) 版本软件，部分对等体在运行 7.1(1) 版本软件。然而，在此情况下，集群将会处理 SSL VPN 连接以及 IPsec 连接。

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

如果集群主用设备是运行 ASA 7.0(x) 版本软件的设备，旧版会话加权算法仅会应用至集群中的 7.1(1) 之前版本的对等体。在这种情况下，用户的访问都不会被拒绝。因为 7.1(1) 之前版本的对等体使用该会话加权算法，它们的负载将会较低。

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

配置负载平衡

要使用负载平衡，请为参与集群的每台设备配置以下要素：

- 公用和专用接口
- VPN 负载平衡集群属性

注　集群中的所有参与者都必须具有一致的集群配置，但集群内的设备优先级除外。

注　如果您使用主用 / 主用状态故障转移或 VPN 负载平衡，则本地 CA 功能不受支持。本地 CA 不能从属于另一 CA ；它只能充当根 CA。

为负载平衡配置公用和专用接口

要为负载平衡集群设备配置公用 （外部）和专用 （内部）接口，请执行以下步骤：

步骤 1　在 vpn-load-balancing 配置模式下，输入 **interface** 命令与 **lbpublic** 关键字，从而在 ASA 上配置公用接口。该命令为此设备的负载平衡功能指定公用接口的名称或 IP 地址：

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic outside
hostname(config-load-balancing)#
```

步骤 2　在 vpn-load-balancing 配置模式下，输入 **interface** 命令与 **lbprivate** 关键字，从而在 ASA 上配置专用接口。该命令为此设备的负载平衡功能指定专用接口的名称或 IP 地址：

```
hostname(config-load-balancing)# interface lbprivate inside
hostname(config-load-balancing)#
```

步骤 3　设置在集群内分配给此设备的优先级。取值范围从 1 至 10。该优先级指示，此设备在启动或现有主用设备发生故障时，成为虚拟集群主用设备的可能性。您设置的优先级越高 （例如 10），此设备成为虚拟集群主用设备的可能性就越高。

```
hostname(config-load-balancing)# priority number
hostname(config-load-balancing)#
```

例如，要在集群内为此设备分配值为 6 的优先级，可以输入以下命令：

```
hostname(config-load-balancing)# priority 6
hostname(config-load-balancing)#
```

步骤 4　如果您想要为此设备应用网络地址转换，可以输入 **nat** 命令和此设备的 NAT 分配地址。您可以定义 IPv4 和 IPv6 地址，或者指定此设备的主机名。

```
hostname(config-load-balancing)# nat ipv4_address ipv_address
hostname(config-load-balancing)#
```

例如，要给此设备分配 NAT 地址 192.168.30.3 和 2001:DB8::1，可以输入以下命令：

```
hostname(config-load-balancing)# nat 192.168.30.3 2001:DB8::1
hostname(config-load-balancing)#
```

配置负载平衡集群属性

要为集群中的每台设备配置负载平衡集群属性，请执行以下步骤：

步骤 1　在全局配置模式下，输入 **vpn load-balancing** 命令，从而设置 VPN 负载平衡：

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)#
```

这将会进入 vpn-load-balancing 配置模式，您可以在其中配置剩余的负载平衡属性。

步骤 2　配置此设备所属集群的 IP 地址或完全限定域名。该命令可以指定代表整个虚拟集群的单一 IP 地址或 FQDN。选择在公用子网地址范围内、由虚拟集群中的所有 ASA 共享的 IP 地址。您可以指定 IPv4 或 IPv6 地址。

```
hostname(config-load-balancing)# cluster ip address ip_address
hostname(config-load-balancing)#
```

例如，要将集群 IP 地址设置为 IPv6 地址 2001:DB8::1，请输入以下命令：

```
hostname(config-load-balancing)# cluster ip address 2001:DB8::1
hostname(config-load-balancing)#
```

步骤 3　配置集群端口。该命令指定此设备要参与的虚拟集群的 UDP 端口。默认值为 9023。如果另一应用正使用此端口，输入您想要用于负载平衡的 UDP 目标端口号。

```
hostname(config-load-balancing)# cluster port port_number
hostname(config-load-balancing)#
```

例如，如要将集群端口设置为 4444，请输入以下命令：

```
hostname(config-load-balancing)# cluster port 4444
hostname(config-load-balancing)#
```

步骤 4　（可选）为集群启用 IPsec 加密。默认设置为无加密。该命令可以启用或禁用 IPsec 加密。如果您配置此复选属性，必须先指定和验证共享密钥。虚拟集群中的 ASA 通过使用 IPsec 的 LAN 对 LAN 隧道进行通信。要确保设备之间通信的所有负载平衡信息会被加密，请启用此属性。

```
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)#
```

注　使用加密时，您必须事先配置负载平衡内部接口。如果该接口未在负载平衡内部接口上启用，则在尝试配置集群加密时，会获得一条错误消息。

如果在配置集群加密时启用了负载平衡内部接口，但在配置设备参与虚拟集群之前禁用了该接口，则在您输入 **participate** 命令（或者，在 ASDM 中选中 **Participate in Load Balancing Cluster** 复选框）时，会获得一条错误消息，并且系统不会为该集群启用加密。

要使用集群加密，您必须指定内部接口的情况下，使用 **crypto isakmp enable** 命令在内部接口上启用 ISAKMP。

步骤 5　如果您启用集群加密，还必须输入 **cluster key** 命令，从而指定 IPsec 共享密钥。当您启用了 IPsec 加密时，该命令可以指定 IPsec 对等体之间的共享密钥。您在框中输入的值，会显示为连续的星号字符

```
hostname(config-load-balancing)# cluster key shared_secret
hostname(config-load-balancing)#
```

例如，要将共享密钥设置为 123456789，请输入以下命令：

```
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)#
```

步骤 6　输入 participate 命令，从而在集群中启用此设备的参与：

```
hostname(config-load-balancing)# participate
hostname(config-load-balancing)#
```

使用完全限定域名启用重定向

如要在 VPN 负载平衡模式下使用完全限定域名启用或禁用重定向，请在全局配置模式下使用 **redirect-fqdn enable** 命令。默认情况下禁用此行为。

默认情况下， ASA 仅将负载平衡重定向中的 IP 地址发给客户端。如果使用的证书基于 DNS 名称，证书将在重定向至备用设备时变得无效。

作为 VPN 集群主用设备，该 ASA 在将 VPN 客户端连接重定向至一个集群设备 （集群中的另一 ASA）时，可以通过反向 DNS 查找，发送此集群设备的完全限定域名 (FQDN)，而不是其外部 IP 地址。

集群中的负载平衡设备上的所有外部和内部网络接口，都必须位于相同 IP 网络之上。

要使用 FQDN 而不是 IP 地址为 SSL 或 IPsec/IKEv2 连接进行 VPN 负载平衡，请执行以下配置步骤：

步骤 1　使用 **redirect-fqdn enable** 命令为负载平衡启用 FQDN 的使用：

redirect-fqdn {enable | disable}
no redirect-fqdn {enable | disable}

例如：

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)#
```

步骤 2　如果这些条目不存在，则为您的 ASA 的每个外部接口，向 DNS 服务器添加一个条目。每个 ASA 外部 IP 地址都应具有一个与其关联的 DNS 条目，以供查找。对于反向查找，也必须启用这些 DNS 条目。

步骤 3　使用 **dns domain-lookup inside** 命令或拥有通向 DNS 服务器的路由的任一接口，在您的 ASA 上启用 DNS 查找。

步骤 4　在 ASA 上定义您的 DNS 服务器 IP 地址；例如：**dns name-server 10.2.3.4** （您的 DNS 服务器的 IP 地址）。

以下内容为 VPN 负载平衡命令序列的示例，该命令序列包含一条启用完全限定域名重定向的接口命令，并将集群的公用接口指定为 **test**，将集群的专用接口指定为 **foo**。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
```

```
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)# participate
```

有关负载平衡的常见问题

IP 地址池耗尽

Q. ASA 是否会将 IP 地址池耗尽视为其 VPN 负载平衡方法的一部分？

A. 否。如果远程访问 VPN 会话被定向至已耗尽其 IP 地址池的设备，则会话不会建立。负载平衡算法基于负载，会计算为每个备用集群成员提供的整数百分比 （活动会话和最大会话的数量）。

唯一 IP 地址池

Q. 要实施 VPN 负载平衡，不同 ASA 上的 AnyConnect 客户端或 IPsec 客户端的 IP 地址池必须是唯一的？

A. 是。 IP 地址池对于每台设备必须是唯一的。

在相同设备上使用负载平衡和故障转移

Q. 单一设备是否可以同时使用负载平衡和故障转移？

A. 是。在此配置中，客户端连接至集群的 IP 地址，而客户端负载被重定向至集群中负载最低的 ASA。如果该设备发生故障，备用设备立即接管，不会对 VPN 隧道产生任何影响。

多个接口上的负载平衡

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

A. 您可以仅定义一个接口来作为公用接口参与集群。这个想法是要均衡 CPU 负载。多个接口会在相同 CPU 上融合，因此负载平衡的概念在多个接口上没有意义。

负载平衡集群的最大并行会话数

Q. 请考虑有两台 ASA 5525-X 的部署，每台设备均有一个 100 位用户的 SSL VPN 许可证。在负载平衡集群中，用户的最大总数量是允许 200 个并行会话，还是仅允许 100 个并行会话？如果我们随后添加第三台设备，该设备有一个 100 位用户的许可证，我们此时是否能够支持 300 个并行会话？

A. 使用 VPN 负载平衡的情况下，所有设备均处于活动状态，因此您的集群可以支持的最大会话数量为集群中每台设备的会话数量的总和，在这种情况下为 300。

查看负载平衡

负载平衡集群主用设备从集群中的每台 ASA 收到定期消息，该消息包含活动 AnyConnect 和无客户端会话的数量，以及基于配置限制或许可证限制的最大允许会话数量。如果集群中的 ASA 显示 100% 的全部容量，集群主用设备不会向其重定向更多的连接。尽管 ASA 可能显示为全部容量，但部分用户可能处于非活动 / 等待继续状态，从而浪费许可。作为应急方案，每台 ASA 都提供会话总数量减去非活动状态会话数量之后的数量，而不是会话总数量。（请参阅命令参考中的 **-sessiondb summary** 命令。也就是说，非活动会话不会报告至集群主用设备。即便 ASA 的容量已满 （有部分非活动会话），集群主用设备仍会视需要向其重定向连接。 ASA 收到新的连接时，处于非活动状态最长时间的会话会被注销，从而允许新的连接使用其许可。

以下示例展示了 100 个 SSL 会话 （仅活动会话）和 2% 的 SSL 负载。这些数值不包含非活动会话。也就是说，非活动会话不会计入负载平衡的负载。

```
hostname# load-balancing
    Status :        enabled
    Role :          Master
    Failover :      Active
    Encryption :    enabled
    Cluster IP :    192.168.1.100
    Peers :         1

                                                Load %
Sessions
    Public IP       Role    Pri     Model           IPsec   SSL     IPsec SSL
    192.168.1.9     Master  7       ASA-5540        4       2       216     100
    192.168.1.19    Backup  9       ASA-5520        0       0       0       0
```

配置 VPN 会话限制

您可以运行的 IPsec 和 SSL VPN 会话的数量，与您的平台和 ASA 许可证支持的数量相同。要查看包含您的 ASA 最大会话数的许可信息，可以在全局配置模式下输入 **show version** 命令。以下示例展示了该命令和该命令输出中的许可信息：

```
hostname(config)# show version

Cisco Adaptive Security Appliance Software Version 8.4(1)
Device Manager Version 6.4(1)

Compiled on Sun 02-Jan-11 03:45 by builders
System image file is "disk0:/cdisk.bin"
Config file at boot was "startup-config"
asa4 up 9 days 3 hours

Hardware:   ASA5510, 256 MB RAM, CPU Pentium 4 Celeron 1600 MHz
Internal ATA Compact Flash, 256MB
BIOS Flash M50FW080 @ 0xfff00000, 1024KB

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                             Boot microcode        : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode     : CNLite-MC-SSLm-PLUS-2.03
                             IPsec microcode       : CNlite-MC-IPSECm-MAIN-2.06
                             Number of accelerators: 1

 0: Ext: Ethernet0/0         : address is 001e.f75e.8b84, irq 9
 1: Ext: Ethernet0/1         : address is 001e.f75e.8b85, irq 9
 2: Ext: Ethernet0/2         : address is 001e.f75e.8b86, irq 9
 3: Ext: Ethernet0/3         : address is 001e.f75e.8b87, irq 9
```

```
 4: Ext: Management0/0       : address is 001e.f75e.8b83, irq 11
 5: Int: Internal-Data0/0    : address is 0000.0001.0002, irq 11
 6: Int: Internal-Control0/0 : address is 0000.0001.0001, irq 5

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 100            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 2              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 250            perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Disabled       perpetual
Intercompany Media Engine         : Disabled       perpetual

This platform has an ASA 5510 Security Plus license.

hostname#
```

要将 AnyConnect VPN 会话 （IPsec/IKEv2 或 SSL）数限制为低于 ASA 允许的值，可以在全局配置模式下使用 **vpn-sessiondb max-anyconnect-premium-or-essentials-limit** 命令。要移除会话限制，请使用此命令的 **no** 版本。

例如，如果 ASA 许可证允许 500 个 SSL VPN 会话，而您想要将 AnyConnect VPN 会话数量限制为 250，请输入以下命令：

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

要移除会话限制，请使用此命令的 **no** 版本：

```
hostname(config)# no vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

要将思科 VPN 客户端 (IPsec IKEv1)、LAN 对 LAN VPN 和无客户端 SSL VPN 会话数限制为低于 ASA 允许的值，请在全局配置模式下输入 **vpn-sessiondb max-other-vpn-limit** 命令：

例如，如果 ASA 许可证允许 750 个 IPsec 会话，而您想要将 IPsec 会话数量限制为 500，请输入以下命令：

```
hostname(config)# vpn-sessiondb max-other-vpn-limit 500
hostname(config)#
```

要移除会话限制，请使用此命令的 **no** 版本：

```
hostname(config)# no vpn-sessiondb max-other-vpn-limit 500
hostname(config)#
```

协商时使用身份证书

ASA 与 AnyConnect 客户端协商 IKEv2 隧道时，需要使用身份证书。对于 IKEv2 远程访问信任点配置，请使用以下命令

```
crypto ikev2 remote-access trustpoint <name> [line<number>]
```

使用此命令允许 AnyConnect 客户端支持最终用户的组选择。您可以同时配置两个信任点：两个 RSA、两个 ECDSA，或每种一个。 ASA 扫描已配置的信任点列表并选择客户端支持的第一个信任点。如果首选 ECDSA，则应该在 RSA 信任点之前配置该信任点。

行号选项指定您想要插入信任点的行号。通常，此选项用于在不移除和重新添加另一行的情况下，在顶部插入信任点。如果没有指定行， ASA 会在列表的末尾添加信任点。

如果您尝试添加已经存在的信任点，将会收到一个错误。如果您在没有指定要移除的信任点名称的情况下使用 *no crypto ikev2 remote-access trustpoint* 命令，所有信任点配置都会被移除。

配置加密核心池

可以在对称多处理 (SMP) 平台上更改加密核心的分配，以提高 AnyConnect TLS/DTLS 流量的吞吐量性能。这些更改可以加速 SSL VPN 数据路径，并在 AnyConnect、智能隧道和端口转发方面提供客户可见的性能提升。以下步骤描述在单一情景或多情景模式下配置加密核心池：

注　多情景模式仅适用于 IKEv2 和 IKEv1 站点对站点，但不适用于 AnyConnect、无客户端 SSL VPN、旧版思科 VPN 客户端、Apple 本机 VPN 客户端、Microsoft 本机 VPN 客户端或用于 IKEv1 IPsec 的 cTCP。

限制

- 加密核心再平衡在以下平台上可用：
  - 5585-X
  - 5545-X
  - 5555-X
  - ASASM

详细步骤

	命令	目的
步骤 1	`hostname(config)# crypto engine ?` `hostname(config)# crypto engine accelerator-bias ?`	指定如何分配密码加速器处理器： • **balanced** — 平均分配加密硬件资源 • **ipsec** — 将加密硬件资源优先分配给 IPsec/加密语音 (SRTP) • **ssl** — 将加密硬件资源优先分配给 SSL

查看活动 VPN 会话

按 IP 地址类型查看活动 AnyConnect 会话

要使用命令行界面查看活动 AnyConnect 会话，可以在 Privileged EXEC 模式下输入 **show vpn-sessiondb anyconnect filter p-ipversion** 或 **show vpn-sessiondb anyconnect filter a-ipversion** 命令。

命令	目的
show vpn-sessiondb anyconnect filter p-ipversion {v4 | v6}	该命令显示按终端的公用 IPv4 或 IPv6 地址过滤的活动 AnyConnect 会话。 公用地址是由企业分配给终端的地址。
show vpn-sessiondb anyconnect filter a-ipversion {v4 | v6}	该命令显示按终端的已分配 IPv4 或 IPv6 地址过滤的活动 AnyConnect 会话。 已分配地址是由 ASA 分配给 AnyConnect 安全移动客户端的地址。

示例

示例 3-1　show vpn-sessiondb anyconnect filter p-ipversion [v4 | v6] 命令的输出

```
hostname(config)# show vpn-sessiondb anyconnect filter p-ipversion v4

Session Type: AnyConnect

Username     : user1                  Index        : 40
Assigned IP  : 192.168.17.10          Public IP    : 198.51.100.1
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
Bytes Tx     : 10570                  Bytes Rx     : 8085
Group Policy : GroupPolicy_SSLACCLIENT
Tunnel Group : SSLACCLIENT
Login Time   : 15:17:12 UTC Mon Oct 22 2012
Duration     : 0h:00m:09s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

示例 3-2　show vpn-sessiondb anyconnect filter a-ipversion [v4 | v6] 命令的输出

```
hostname(config)# show vpn-sessiondb anyconnect filter a-ipversion v6

Session Type: AnyConnect

Username     : user1                  Index        : 45
Assigned IP  : 192.168.17.10
Public IP    : 2001:DB8:8:1:90eb:3fe5:9eea:fb29
Assigned IPv6: 2001:DB8:9:1::24
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
```

```
Bytes Tx     : 10662                  Bytes Rx     : 17248
Group Policy : GroupPolicy_SSL_IPv6   Tunnel Group : SSL_IPv6
Login Time   : 17:42:42 UTC Mon Oct 22 2012
Duration     : 0h:00m:33s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

按 IP 地址类型查看活动的无客户端 SSL VPN 会话

如要使用命令行界面查看活动的无客户端 SSL VPN 会话，请在 Privileged EXEC 模式下输入 **show vpn-sessiondb webvpn filter ipversion** 命令。

命令	目的
show vpn-sessiondb webvpn filter ipversion {v4 | v6}	该命令显示按终端的公用 IPv4 或 IPv6 地址过滤的活动无客户端 SSL VPN 会话。 公用地址是由企业分配给终端的地址。

示例

示例 3-3　show vpn-sessiondb webvpn filter ipversion [v4 \| v6] 命令的输出

```
hostname# sh vpn-sessiondb webvpn filter ipversion v4

Session Type: WebVPN

Username     : user1                  Index        : 63
Public IP    : 171.16.17.6
Protocol     : Clientless
License      : AnyConnect Premium
Encryption   : Clientless: (1)RC4     Hashing      : Clientless: (1)SHA1
Bytes Tx     : 62454                  Bytes Rx     : 13082
Group Policy : SSLv6                  Tunnel Group : SSL_IPv6
Login Time   : 18:07:48 UTC Mon Oct 22 2012
Duration     : 0h:00m:16s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

按 IP 地址类型查看活动的 LAN 对 LAN VPN 会话

如要使用命令行界面查看活动的无客户端 SSL VPN 会话，请在 Privileged EXEC 模式下输入 **show vpn-sessiondb l2l filter ipversion** 命令。

命令	目的
show vpn-sessiondb l2l filter ipversion {v4 | v6}	该命令显示按连接的公用 IPv4 或 IPv6 地址过滤的活动 LAN 对 LAN VPN 会话。 公用地址是由企业分配给终端的地址。

配置 ISE 策略实施

思科身份服务引擎 (ISE) 是一个安全策略管理和控制平台。它可自动化并简化有线连接、无线连接和 VPN 连接的访问控制和安全合规性。思科 ISE 主要用于与 Cisco TrustSec 结合提供安全访问和来宾访问，支持自带设备计划和实施使用策略。

ISE 授权变更 (CoA) 功能提供一种机制，以在建立身份验证、授权和记帐 (AAA) 会话后更改其属性。当 AAA 中的用户或用户组的策略发生更改时，可以将 CoA 数据包从 ISE 直接发送到 ASA，以重新初始化身份验证并应用新策略。不再需要内联安全状态实施点 (IPEP) 来为与 ASA 建立的每个 VPN 会话应用访问控制列表 (ACL)。

在以下 VPN 客户端上支持 ISE 策略实施：

- IPSec
- AnyConnect
- L2TP/IPSec

系统流程如下：

1. 最终用户请求 VPN 连接。
2. ASA 向 ISE 对用户进行身份验证，并且接收提供有限网络访问的用户 ACL。
3. 系统向 ISE 发送记帐启动消息以注册会话。
4. 直接在 NAC 代理和 ISE 之间进行安全状态评估。此过程对于 ASA 是透明的。
5. ISE 通过 CoA“策略推送”向 ASA 发送策略更新。这将标识提供提高的网络访问特权的新用户 ACL。

注　在连接的生存期内，可能会通过后续 CoA 更新进行对于 ASA 而言透明的其他策略评估。

配置 RADIUS 服务器组

如要将外部 RADIUS 服务器用于身份验证、授权或记帐，每个 AAA 协议必须先创建至少一个 RADIUS 服务器组，然后向每个服务器组添加一台或多台服务器。您可以按名称标识 AAA 服务器组。

如要添加 RADIUS 服务器组，请执行以下步骤：

详细步骤

	命令	目的

步骤 1	**aaa-server** *server_tag* **protocol radius**
	
	示例：
	`hostname(config)# aaa-server servergroup1 protocol radius`
	`hostname(config-aaa-server-group)#`
		确定服务器组名称和协议。
		
		当您输入 **aaa-server protocol** 命令时，将会进入 AAA 服务器组配置模式。

	命令	目的
步骤 2	**merge-dacl** {**before-avpair** | **after-avpair**} **示例：** hostname(config)# aaa-server servergroup1 protocol radius hostname(config-aaa-server-group)# merge-dacl before-avpair	可以将可下载的 ACL 与来自 RADIUS 数据包的思科 AV 对中收到的 ACL 进行合并。默认设置为 **no merge dacl**，其指定可下载的 ACL 不会与思科 AV 对 ACL 合并。如果同时收到了 AV 对和可下载的 ACL， AV 对将会被优先使用。 **before-avpair** 选项指定可下载的 ACL 条目应放置在思科 AV 对条目之前。 **after-avpair** 选项指定可下载的 ACL 条目应放置在思科 AV 对条目之后。此选项仅适用于 VPN 连接。对于 VPN 用户， ACL 的形式可以是思科 AV 对 ACL、可下载 ACL 和在 ASA 上配置的 ACL。此选项确定可下载 ACL 和 AV 对 ACL 是否会被合并，并且不适用于在 ASA 上配置的任意 ACL。
步骤 3	**max-failed-attempts** *number* **示例：** hostname(config-aaa-server-group)# max-failed-attempts 2	指定在尝试下一服务器前，向组中 RADIUS 服务器发送的请求的最大数量。 *number* 参数的取值范围为 1 至 5。默认值为 3。 如果您配置了使用本地数据库的回退方法 （仅用于管理访问），并且组中的所有服务器都未能响应，则该服务器组会被视为无响应，系统将会尝试回退方法。该服务器组仍然标记为 10 分钟 （默认值）内无响应，因此该时段内其他的 AAA 请求不会尝试联系该服务器组，而是会立即使用回退方法。要将无响应时段从默认值改为其他值，请参阅下一步中的 **reactivation-mode** 命令。 如果没有回退方法， ASA 继续重试该服务器组中的服务器。
步骤 4	**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**} **示例：** hostname(config-aaa-server-group)# reactivation-mode deadtime 20	指定用于重新激活组中的已失败服务器的方法 （重新激活策略）。 **depletion** 关键字仅在组中的所有服务器均处于非活动状态后，才重新激活已失败的服务器。 **deadtime** *minutes* 关键字参数对指定介于 0 至 1440 （单位：分钟）之间的时长，该时长是禁用组中的最后一台服务器到后续重启所有服务器之间会经过的一段时间。默认值为 10 分钟。 **timed** 关键字在 30 秒的停止运行时间之后，重新激活已失败的服务器。
步骤 5	**accounting-mode simultaneous** **示例：** hostname(config-aaa-server-group)# accounting-mode simultaneous	向组中的所有服务器发送记帐消息。 要还原仅向活动服务器发送消息的默认设置，请输入 **accounting-mode single** 命令。
步骤 6	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **示例：** hostname(config)# aaa-server servergroup1 outside host 10.10.1.1	确定 AAA 服务器以及其所属的服务器组。 当您输入 **aaa-server host** 命令时，将会进入 AAA 服务器主机配置模式。

	命令	目的
步骤 7	**dynamic-authorization** {port *port-number*} **示例：** hostname(config-aaa-server-group)# dynamic-authorization port 1700	为 AAA 服务器组启用 RADIUS 动态授权 (CoA) 服务。 一旦定义，则会将相应的 RADIUS 服务器组注册为用于 CoA 通知，而 ASA 会侦听该端口，以获取来自 ISE 的 CoA 策略更新。 CoA 侦听 *port-number* 的有效范围为 1 至 65535。 如果该命令的 “no” 形式中指定的端口号或接口与当前配置中的行不匹配，将会显示一条错误消息。
步骤 8	**authorize-only** **示例：** hostname(config-aaa-server-group)# authorize-only	为 RADIUS 服务器组启用仅授权模式 该命令指定，当此服务器组用于授权时，RADIUS 访问请求消息将会构建为 “仅授权” 请求，而不是现在可用的已配置的密码方法。仅授权请求包含带有仅授权值 (17) 的服务类型属性以及访问请求内的消息身份验证器。 支持仅授权模式可以消除在访问请求中包含 RADIUS 公用密码的需求。因此，不需要在 aaa-server-host 模式下使用 radius-common-pw CLI 配置公用密码。 **注**　为服务器组配置仅授权模式，而公用密码是主机特定的。因此，一旦配置了仅授权模式，为单个 AAA 服务器配置的公用密码会被忽略。
步骤 9	**without-csd** {**anyconnect**} **示例：** hostname(config-tunnel-webvpn)# without-csd anyconnect	可以为通向特定隧道组的连接关闭主机扫描处理。此设置目前适用于无客户端和 L3 连接。该命令已被修改为可以将此设置仅应用于 AnyConnect 连接。
步骤 10	**interim-accounting-update** {periodic *interval*} **示例：** hostname(config-aaa-server-group)# interim-accounting-update periodic 12	启用 RADIUS interim-accounting-update 消息的生成。目前，仅当 VPN 隧道连接添加至无客户端 VPN 会话时，才会生成这些消息。发生此状况时，将会生成记帐更新，以便将新分配的 IP 地址通知给 RADIUS 服务器。已向该命令添加了关键字，以便将该命令配置为支持当前功能，或者可以为所有会话生成定期的临时记帐更新，这些会话被配置为向指定的服务器组发送记帐消息。 *periodic* — 此可选关键字允许为每一个 VPN 会话定期生成和传输记帐记录，这些会话被配置为向所述服务器组发送记帐记录。 *interval* — 该值为代表时长的数值 （单位：小时），是定期记帐更新之间的间隔。该值的有效范围为 1 至 120，默认值为 24。

示例配置

以下示例显示如何添加一个具有单一服务器的 RADIUS 组：

```
hostname(config)# aaa-server AuthOutbound protocol radius
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key RadUauthKey
hostname(config-aaa-server-host)# exit
```

以下示例显示如何配置用于仅授权的 ISE 服务器对象、动态授权 (CoA) 更新，以及每小时定期进行的记帐：

```
hostname(config)# aaa-server ise protocol radius
hostname(config-aaa-server-group)# authorize-only
hostname(config-aaa-server-group)# interim-accounting-update periodic 1
hostname(config-aaa-server-group)# dynamic-authorization
hostname(config-aaa-server-group)# exit
hostname(config-aaa-server-group)# authorize-only
hostname(config)# aaa-server ise (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key sharedsecret
hostname(config-aaa-server-host)# exit
```

以下示例显示如何为采用 ISE 的密码身份验证配置隧道组：

```
hostname(config)# tunnel-group aaa-coa general-attributes
hostname(config-tunnel-general)# address-pool vpn
hostname(config-tunnel-general)# authentication-server-group ise
hostname(config-tunnel-general)# accounting-server-group ise
hostname(config-tunnel-general)# exit
```

以下示例显示如何为采用 ISE 的本地证书验证和授权配置隧道组：

```
hostname(config)# tunnel-group aaa-coa general-attributes
hostname(config-tunnel-general)# address-pool vpn
hostname(config-tunnel-general)# authentication certificate
hostname(config-tunnel-general)# authorization-server-group ise
hostname(config-tunnel-general)# accounting-server-group ise
hostname(config-tunnel-general)# exit
```

有关如何启用 CoA 的更多详细信息，请参阅 《*思科 ASA 系列常规操作 CLI 配置指南*》中的 “*配置用于 AAA 的 RADIUS 服务器*”一章。

命令摘要

命令	目的
hostname(config-aaa-server-group)# **dynamic-authorization {port *port-number*}**	为 AAA 服务器组启用 RADIUS 动态授权 (CoA) 服务。 一旦定义，则会将相应的 RADIUS 服务器组注册为用于 CoA 通知，而 ASA 会侦听该端口，以获取来自 ISE 的 CoA 策略更新。 CoA 侦听 *port-number* 的有效范围为 1 至 65535。 如果该命令的 “no” 形式中指定的端口号或接口与当前配置中的行不匹配，将会显示一条错误消息。
hostname(config-aaa-server-group)# **authorize-only**	为 RADIUS 服务器组启用仅授权模式 该命令指定，当此服务器组用于授权时，RADIUS 访问请求消息将会构建为 “仅授权” 请求，而不是现在可用的已配置的密码方法。仅授权请求包含带有仅授权值 (17) 的服务类型属性以及访问请求内的消息身份验证器。 支持仅授权模式可以消除在访问请求中包含 RADIUS 公用密码的需求。因此，不需要在 aaa-server-host 模式下使用 radius-common-pw CLI 配置公用密码。 **注** 为服务器组配置仅授权模式，而公用密码是主机特定的。因此，一旦配置了仅授权模式，为单个 AAA 服务器配置的公用密码会被忽略。
hostname(config-tunnel-webvpn)# **without-csd {anyconnect}**	可以为通向特定隧道组的连接关闭主机扫描处理。此设置目前适用于无客户端和 L3 连接。该命令已被修改为可以将此设置仅应用于 AnyConnect 连接。
hostname(config-aaa-server-group)# **interim-accounting-update {periodic *interval*}**	启用 RADIUS interim-accounting-update 消息的生成。目前，仅当 VPN 隧道连接添加至无客户端 VPN 会话时，才会生成这些消息。发生此状况时，将会生成记帐更新，以便将新分配的 IP 地址通知给 RADIUS 服务器。已向该命令添加了关键字，以便将该命令配置为支持当前功能，或者可以为所有会话生成定期的临时记帐更新，这些会话被配置为向指定的服务器组发送记帐消息。 *periodic* — 此可选关键字允许为每一个 VPN 会话定期生成和传输记帐记录，这些会话被配置为向所述服务器组发送记帐记录。 *interval* — 该值为代表时长的数值 （单位：小时），是定期记帐更新之间的间隔。该值的有效范围为 1 至 120，默认值为 24。

故障排除

以下命令可用于调试。

要跟踪 CoA 活动：

```
debug radius dynamic-authorization
```

要跟踪重定向 URL 功能：

```
debug aaa url-redirect
```

要查看 URL 重定向功能对应的 NP 分类规则：

```
show asp table classify domain url-redirect
```

连接配置文件、组策略和用户

本章描述如何配置 VPN 连接配置文件 （以前称为 “隧道组”）、组策略和用户。本章包含以下各节：

总之，您首先配置连接配置文件来为连接设置值。然后，配置组策略。这些组策略为汇聚中的用户设置值。然后，配置用户，从而可以从组继承值并在个人用户基础上配置某些值。本章描述配置这些实体的方式和原因。

连接配置文件、组策略和用户概述

组和用户是管理虚拟专用网络 (VPN) 的安全性以及配置 ASA 方面的核心概念。它们指定用于确定对 VPN 的用户访问及使用的属性。*组*是被视为单个实体的用户的集合。*用户*从*组策略*获取其属性。*连接配置文件*标识特定连接的组策略。如果没有向用户分配特定组策略，则应用连接的默认组策略。

注 您使用 **tunnel-group** 命令来配置连接配置文件。在本章中，术语 “连接配置文件”和 “隧道组”往往交换使用。

连接配置文件和组策略简化系统管理。为精简配置任务，ASA 提供默认 LAN 对 LAN 连接配置文件、默认远程访问连接配置文件、默认 SSL/IKEv2 VPN 连接配置文件和默认组策略 (DfltGrpPolicy)。默认连接配置文件和组策略提供对于许多用户而言可能常见的设置。添加用户时，可以指定其从组策略 “继承”参数。因此，可以快速为大量用户配置 VPN 连接。

如果您决定向所有 VPN 用户授予相同权限，则无需配置特定连接配置文件或组策略，但是 VPN 很少以该方式工作。例如，您可能会允许财务组访问专用网络的一部分，允许客户支持组访问另一部分，并允许 MIS 组访问其他部分。此外，您还可能允许 MIS 中的特定用户访问其他 MIS 用户无法访问的系统。连接配置文件和组策略提供安全执行此任务的灵活性。

注 ASA 还包括对象组的概念，对象组是网络列表的超集。通过对象组，可以定义对端口及网络的 VPN 访问。对象组与 ACL 而非与组策略和连接配置文件相关。有关使用对象组的详细信息，请参阅常规操作配置指南 中的第 20 章 “对象”。

安全设备可以应用各种来源的属性值。它根据以下层次结构应用这些属性值：

1. 动态访问策略 (DAP) 记录
2. 用户名
3. 组策略
4. 连接配置文件的组策略
5. 默认组策略

因此，属性的 DAP 值比为用户、组策略或连接配置文件配置的 DAP 值具有更高的优先级。

当启用或禁用 DAP 记录的属性时，ASA 会应用该值并对其进行实施。例如，当在 dap webvpn 配置模式下禁用 HTTP 代理时，ASA 不会进一步查找值。当对 **http-proxy** 命令改用 **no** 值时，DAP 记录中不存在属性，因此安全设备会下移到用户名中的 AAA 属性，并且如有必要，会移至组策略以查找要应用的值。 ASA 无客户端 SSL VPN 配置仅分别支持一个 **http-proxy** 命令和一个 **https-proxy** 命令。建议使用 ASDM 来配置 DAP。

连接配置文件

连接配置文件由用于确定隧道连接策略的记录集组成。这些记录标识对隧道用户进行身份验证的服务器，以及连接信息发送到的记帐服务器 （如果有）。它们还标识连接的默认组策略，并且包含特定于协议的连接参数。连接配置文件包含与创建隧道本身有关的少量属性。连接配置文件包含指向用于定义面向用户的属性的组策略的指针。

ASA 提供以下默认连接配置文件：用于 LAN 对 LAN 连接的 DefaultL2Lgroup、用于远程访问连接的 DefaultRAgroup 以及用于 SSL VPN （基于浏览器）连接的 DefaultWEBVPNGroup。可以修改这些默认连接配置文件，但是无法将其删除。您还可以创建一个或多个特定于您的环境的连接配置文件。连接配置文件对于 ASA 而言为本地配置文件，并且无法在外部服务器上进行配置。

连接配置文件指定以下属性：

- 第 4-2 页上的常规连接配置文件连接参数
- 第 4-3 页上的 IPsec 隧道组连接参数
- 第 4-4 页上的 SSL VPN 会话的连接配置文件连接参数

常规连接配置文件连接参数

常规参数对于所有 VPN 连接都通用。常规参数包括：

- 连接配置文件名称 — 在添加或编辑连接配置文件时指定连接配置文件名称。请注意以下事项：
  - 对于使用预共享密钥进行身份验证的客户端，连接配置文件名称与客户端传递给 ASA 的组名相同。
  - 使用证书进行身份验证的客户端将此名称作为证书的一部分来传递，而 ASA 从证书提取名称。
- 连接类型 — 连接类型包括 IKEv1 远程访问、IPsec LAN 对 LAN 和 Anyconnect (SSL/IKEv2)。连接配置文件只能有一种连接类型。
- 身份验证、授权和记帐服务器 — 这些参数标识 ASA 用于以下目的的服务器组或列表：
  - 对用户进行身份验证
  - 获取有关用户经授权访问的服务的信息
  - 存储记帐记录

  服务器组可由一个或多个服务器组成。

- 连接的默认组策略 — 组策略是面向用户的属性集。默认组策略是 ASA 在对隧道用户进行身份验证或授权时将其属性用作默认值的组策略。
- 客户端地址分配方法 — 此方法包括 ASA 分配给客户端的一个或多个 DHCP 服务器或地址池的值。
- 禁用覆盖帐户 — 通过此参数可覆盖从 AAA 服务器接收到的 “account-disabled” 指示器。
- 密码管理 — 通过此参数可警告用户当前密码在指定的天数内即将到期 （默认为 14 天），然后为用户提供机会更改密码。
- 剥除组和剥除领域 — 这些参数指导 ASA 处理其接收的用户名的方式。它们仅适用于接收到的 user@realm 形式的用户名。

  领域是使用 @ 定界符附加到用户名的管理域 (user@abc)。如果剥除领域，则 ASA 使用用户名和组 （如果存在）进行身份验证。如果剥除组，则 ASA 使用用户名和领域 （如果存在）进行身份验证。

  输入 strip-realm 命令可移除领域限定符，输入 strip-group 命令可在身份验证期间从用户名中移除组限定符。如果将两个限定符均移除，则身份验证仅基于*用户名*。否则，身份验证基于完整的 *username@realm* 或 *username<delimiter> group* 字符串。如果服务器无法解析定界符，则必须指定 strip-realm。

  此外，（仅适用于 L2TP/IPsec 客户端）当指定 strip-group 命令时，ASA 通过从 VPN 客户端提供的用户名获取组名来为用户连接选择连接配置文件 （隧道组）。
- 要求授权 — 通过此参数可要求在授权后用户才能连接，或者关闭该要求。
- 授权 DN 属性 — 此参数指定执行授权时要使用的可分辨名称属性。

IPsec 隧道组连接参数

IPsec 参数包括：

- 客户端身份验证方法预共享密钥和 / 或证书。
  - 对于基于预共享密钥的 IKE 连接，这是与连接策略关联的字母数字密钥本身 （长度最多为 128 个字符）。
  - 对等 ID 验证要求 — 此参数指定是否要求使用对等体的证书来验证对等体的身份。
  - 如果指定证书或证书与密钥作为身份验证方法，则最终用户必须提供有效证书以便进行身份验证。
- 扩展混合身份验证方法：XAUTH 和混合 XAUTH。

  当需要使用数字证书进行 ASA 身份验证并使用其他传统方法 （如 RADIUS、 TACACS+ 或 SecurID）进行远程 VPN 用户身份验证时，请使用 **isakmp ikev1-user-authentication** 命令来实施混合 XAUTH 身份验证。
- ISAKMP (IKE) 保活设置。通过此功能可使 ASA 监控远程对等体的持续状态并向该对等体报告其自己的状态。如果对等体变为无响应，则 ASA 会移除连接。启用 IKE 保活可防止在 IKE 对等体失去连接时连接挂起。

  IKE 保活有各种形式。为使此功能工作， ASA 及其远程对等体均必须支持通用形式。此功能适用于以下对等体：
  - Cisco AnyConnect VPN 客户端
  - Cisco VPN 客户端 （版本 3.0 及以上）
  - Cisco VPN 3000 客户端 （版本 2.x）
  - Cisco VPN 3002 硬件客户端

- Cisco VPN 3000 系列集中器
- Cisco IOS 软件
- Cisco Secure PIX 防火墙

非 Cisco VPN 客户端不支持 IKE 保活。

如果配置的是一组混合对等体，并且其中一些对等体支持 IKE 保活而其他对等体不支持 IKE 保活，请对整个组启用 IKE 保活。该功能不会影响不支持此功能的对等体。

如果禁用 IKE 保活，则具有无响应对等体的连接保持活动状态，直到其超时为止，因此建议缩短空闲超时。要更改空闲超时，请参阅第 4-35 页上的配置组策略。

注　要减少连接成本，请在该组包含通过 ISDN 线路进行连接的任何客户端的情况下禁用 IKE 保活。 ISDN 连接在空闲情况下通常会断开连接，但是， IKE 保活机制可防止连接空闲，从而避免断开连接。

如果禁用 IKE 保活，则仅当其 IKE 或 IPsec 密钥到期时客户端才会断开连接。失败的流量不会如同在启用 IKE 保活时一样，将隧道与 “对等体超时配置文件” 断开连接。

注　如果 LAN 对 LAN 配置使用的是 IKE 主模式，请确保两个对等体具有同一 IKE 保活配置。两个对等项均必须启用 IKE 保活，或者均必须禁用 IKE 保活。

- 如果使用数字证书来配置身份验证，则可以指定是发送整条证书链 （向对等体发送身份证书和所有签发证书）还是仅发送签发证书 （包括根证书和任何从属 CA 证书）。
- 可以通知使用过时版本的 Windows 客户端软件的用户需要更新其客户端，并可为其提供机制来获取已更新的客户端版本。对于 VPN 3002 硬件客户端用户，可以触发自动更新。可以为所有连接配置文件或为特定连接配置文件配置和更改客户端更新。
- 如果使用数字证书来配置身份验证，则可以指定用于标识要发送到 IKE 对等体的证书的信任点的名称。

SSL VPN 会话的连接配置文件连接参数

表 4-1 提供特定于 SSL VPN（AnyConnect 客户端和无客户端）连接的连接配置文件属性的列表。除这些属性外，还会配置对于所有 VPN 连接通用的常规连接配置文件属性。有关配置连接配置文件的分步信息，请参阅第 4-18 页上的配置无客户端 SSL VPN 会话的连接配置文件。

注　在早期版本中，“连接配置文件” 称为 “隧道组”。可通过 tunnel-group 命令来配置连接配置文件。本章往往交换使用这些术语。

表 4-1　SSL VPN 的连接配置文件属性

命令	功能
authentication	设置身份验证方法：AAA 或证书。
customization	标识要应用的以前定义的定制的名称。定制确定用户在登录时看到的窗口的外观。可在配置无客户端 SSL VPN 过程中配置定制参数。
nbns-server	标识要用于 CIFS 名称解析的 NetBIOS 名称服务服务器 (nbns-server) 的名称。
group-alias	指定可供服务器引用连接配置文件的一个或多个备用名称。在登录时，用户从下拉菜单中选择组名。
group-url	标识一个或多个组 URL。如果配置此属性，则访问指定 URL 的用户在登录时无需选择组。
dns-group	标识 DNS 服务器组，该服务器组指定要用于连接配置文件的 DNS 服务器的 DNS 服务器名称、域名、名称服务器、重试次数和超时值。
hic-fail-group-policy	如果使用思科安全桌面管理器将 Group-Based Policy 属性设置为“Use Failure Group-Policy”或“Use Success Group-Policy, if criteria match”，请指定 VPN 功能策略。
override-svc-download	覆盖下载配置用于将 AnyConnect VPN 客户端下载到远程用户的 group-policy 或 username 属性。
radius-reject-message	当拒绝身份验证时，在登录屏幕上启用 RADIUS 拒绝消息的显示。

配置连接配置文件

本节描述单情景模式或多情景模式下连接配置文件的内容和配置。

注　多情景模式仅适用于 IKEv2 和 IKEv1 站点间连接，不适用于 AnyConnect、无客户端 SSL VPN，传统 Cisco VPN 客户端、Apple 本机 VPN 客户端、Microsoft 本机 VPN 客户端或 cTCP for IKEv1 IPsec。

- 第 4-6 页上的最大连接配置文件数
- 第 4-6 页上的默认 IPsec 远程访问连接配置文件配置
- 第 4-7 页上的指定远程访问连接配置文件的名称和类型
- 第 4-7 页上的配置远程访问连接配置文件
- 第 4-15 页上的配置 LAN 对 LAN 连接配置文件
- 第 4-18 页上的配置无客户端 SSL VPN 会话的连接配置文件
- 第 4-24 页上的定制无客户端 SSL VPN 会话用户的登录窗口
- 第 4-31 页上的配置连接配置文件以对 AnyConnect 客户端进行 RADIUS/SDI 消息支持

可以修改默认连接配置文件，并且可以将新连接配置文件配置为三种隧道组类型的任意一种。如果未在连接配置文件中显式配置某个属性，则该属性从默认连接配置文件获取其值。默认连接配置文件类型为远程访问。后续参数取决于选择的隧道类型。要查看所有连接配置文件的当前配置和默认配置，包括默认连接配置文件，请输入 **show running-config all tunnel-group** 命令。

最大连接配置文件数

ASA 可以支持的连接配置文件 （隧道组）的最大数量是一个平台的并发 VPN 会话的最大数量 + 5 的函数。尝试添加超过限制的其他隧道组会产生以下消息：“ERROR: The limit of 30 configured tunnel groups has been reached”。

默认 IPsec 远程访问连接配置文件配置

默认远程访问连接配置文件的内容如下：

```
tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
 no address-pool
 no ipv6-address-pool
 authentication-server-group LOCAL
 accounting-server-group RADIUS
 default-group-policy DfltGrpPolicy
 no dhcp-server
 no strip-realm
 no password-management
 no override-account-disable
 no strip-group
 no authorization-required
 authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup webvpn-attributes
 hic-fail-group-policy DfltGrpPolicy
 customization DfltCustomization
 authentication aaa
 no override-svc-download
 no radius-reject-message
 dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 1500 retry 2
 no radius-sdi-xauth
 isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
 no authentication pap
 authentication chap
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy
```

配置 IPsec 隧道组常规属性

常规属性跨多个隧道组类型通用。 IPsec 远程访问和无客户端 SSL VPN 隧道共享大多数相同的常规属性。 IPsec LAN 对 LAN 隧道使用子集。有关所有命令的完整描述，请参阅 《*Cisco ASA 系列命令参考*》。本节按顺序描述如何配置远程访问连接配置文件和 LAN 对 LAN 连接配置文件。

配置远程访问连接配置文件

在以下远程客户端和中心站点 ASA 之间建立连接时，请使用远程访问连接配置文件：

- 传统 Cisco VPN 客户端 （与 IPsec/IKEv1 连接）
- AnyConnect 安全移动客户端 （与 SSL 或 IPsec/IKEv2 连接）
- 无客户端 SSL VPN （基于浏览器，与 SSL 连接）
- Cisco ASA 5500 Easy VPN 硬件客户端 （与 IPsec/IKEv1 连接）
- Cisco VPM 3002 硬件客户端 （与 IPsec/IKEv1 连接）

我们还提供名为 *DfltGrpPolicy* 的默认组策略。

要配置远程访问连接配置文件，请先配置隧道组常规属性，然后配置远程访问属性。请参阅以下各节：

指定远程访问连接配置文件的名称和类型

通过输入 **tunnel-group** 命令创建连接配置文件，指定其名称和类型。对于远程访问隧道，类型为 **remote-access**：

```
hostname(config)# tunnel-group tunnel_group_name type remote-access
hostname(config)#
```

例如，要创建名为 TunnelGroup1 的远程访问连接配置文件，请输入以下命令：

```
hostname(config)# tunnel-group TunnelGroup1 type remote-access
hostname(config)#
```

配置远程访问连接配置文件常规属性

要配置或更改连接配置文件常规属性，请在以下步骤中指定参数：

步骤 1　要配置常规属性，请在单情景或多情景模式下输入 **tunnel-group general-attributes** 任务，从而进入 tunnel-group general-attributes 模式。提示符会更改以指示模式发生更改。

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

步骤 2　指定要使用的身份验证服务器组的名称 （如果有）。如果要在指定服务器组失败的情况下使用 LOCAL 数据库进行身份验证，请附加关键字 **LOCAL**：

```
hostname(config-tunnel-general)# authentication-server-group [(interface_name)] groupname
[LOCAL]
hostname(config-tunnel-general)#
```

身份验证服务器组的名称最长可为 16 个字符。

可以通过在组名之后包含接口的名称来选择性配置特定于接口的身份验证。用于指定隧道终止位置的接口名称必须用括号括起来。以下命令使用名为 servergroup1 的服务器进行身份验证来为名为 test 的接口配置特定于接口的身份验证：

```
hostname(config-tunnel-general)# authentication-server-group (test) servergroup1
hostname(config-tunnel-general)#
```

步骤 3　指定要使用的授权服务器组的名称 （如果有）。配置该值时，用户必须存在于要连接的授权数据库中：

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

授权服务器组的名称最长可为 16 个字符。例如，以下命令指定使用授权服务器组 FinGroup：

```
hostname(config-tunnel-general)# authorization-server-group FinGroup
hostname(config-tunnel-general)#
```

步骤 4　指定要使用的记帐服务器组的名称 （如果有）。

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

记帐服务器组的名称最长可为 16 个字符。例如，以下命令指定使用名为 comptroller 的记帐服务器组：

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

步骤 5　指定默认组策略的名称：

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

组策略的名称最长可为 64 个字符。以下示例将 DfltGrpPolicy 设置为默认组策略的名称。

```
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
hostname(config-tunnel-general)#
```

步骤 6　指定 DHCP 服务器（最多 10 台服务器）的名称或 IP 地址，以及 DHCP 地址池（最多 6 个池）的名称。默认为无 DHCP 服务器且无地址池。 **dhcp-server** 命令将允许配置 ASA，以在其尝试获取 VPN 客户端的 IP 地址时向指定的 DHCP 服务器发送其他选项。有关详细信息，请参阅 《*思科 ASA 系列命令参考*》指南中的 **dhcp-server** 命令。

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```

注　如果指定接口名称，则必须用括号将其括起来。

在全局配置模式下可使用 **ip local pool** 命令来配置地址池。

步骤 7　指定 NAC 身份验证服务器组的名称 （如果使用的是网络准入控制），以标识要用于网络准入控制状态验证的身份验证服务器组。将至少一个访问控制服务器配置为支持 NAC。使用 **aaa-server** 命令命名 ACS 组。然后，使用 **nac-authentication-server-group** 命令 （对服务器组使用同一名称）。

以下示例将 acs-group1 标识为要用于 NAC 状态验证的身份验证服务器组：

```
hostname(config-group-policy)# nac-authentication-server-group acs-group1
hostname(config-group-policy)
```

以下示例从默认远程访问组继承身份验证服务器组：

```
hostname(config-group-policy)# no nac-authentication-server-group
hostname(config-group-policy)
```

注　NAC 在远程主机上需要思科信任代理。

步骤 8　指定在将用户名传递到 AAA 服务器之前从中剥除组还是领域。默认是既不剥除组名也不剥除领域：

```
hostname(config-tunnel-general)# strip-group
hostname(config-tunnel-general)# strip-realm
hostname(config-tunnel-general)#
```

领域是管理域。如果剥除领域，则 ASA 使用用户名和组 （如果存在）进行身份验证。如果剥除组，则 ASA 使用用户名和领域 （如果存在）进行身份验证。输入 **strip-realm** 命令可移除领域限定符，使用 strip-group 命令可在身份验证期间从用户名中移除组限定符。如果将两个限定符均移除，则身份验证仅基于*用户名*。否则，身份验证基于完整的 *username@realm* 或 *username<delimiter> group* 字符串。如果服务器无法解析定界符，则必须指定 **strip-realm**。

步骤 9　或者，如果服务器是 RADIUS、使用 NT 的 RADIUS 或 LDAP 服务器，则可以启用密码管理。

注　如果是使用 LDAP 目录服务器进行身份验证，则通过 Sun Microsystems JAVA 系统目录服务器 （以前称为 Sun ONE 目录服务器）和 Microsoft Active Directory 来支持密码管理。

DN — 在 ASA 上配置用于访问 Sun 目录服务器的 DN 必须能够访问该服务器上的默认密码策略。建议使用目录管理员或具有目录管理员特权的用户作为 DN。或者，可以在默认密码策略上放置 ACI。

Microsoft — 必须配置基于 SSL 的 LDAP 以对 Microsoft Active Directory 启用密码管理。

此功能 （默认情况下禁用）在当前密码即将到期时警告用户。默认是在到期前 14 天开始警告用户：

```
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

如果服务器是 LDAP 服务器，则可以指定开始警告用户即将到期的截止天数 （0 to 180）：

```
hostname(config-tunnel-general)# password-management [password-expire in days n]
hostname(config-tunnel-general)#
```

注　在 tunnel-group general-attributes 配置模式下输入的 **password-management** 命令会替换以前在 tunnel-group ipsec-attributes 模式下输入的已弃用的 **radius-with-expiry** 命令。

配置 **password-management** 命令时， ASA 会在远程用户登录时通知其当前密码即将到期或已到期。然后， ASA 为用户提供机会更改密码。如果当前密码尚未到期，则用户仍可使用该密码进行登录。如果尚未配置 RADIUS 或 LDAP 身份验证，则 ASA 会忽略此命令。

请注意，这不会更改密码到期之前的天数，而是更改 ASA 开始警告用户密码即将到期的提前天数。

如果确实指定 **password-expire-in-days** 关键字，则还必须指定天数。

指定此命令且天数设置为 0 会禁用此命令。ASA 不通知用户即将到期，但是用户可以在密码到期后对其进行更改。

有关详细信息，请参阅第 4-25 页上的配置 Microsoft Active Directory 设置以进行密码管理。

注　ASA 版本 7.1 及更高版本在使用 LDAP 或使用任何支持 MS-CHAPv2 的 RADIUS 连接进行身份验证时，通常支持 AnyConnect VPN 客户端、 Cisco IPsec VPN 客户端、 SSL VPN 全隧道客户端和无客户端连接的密码管理。对于 Kerberos/AD （Windows 密码）或 NT 4.0 域，所有这些连接类型都*不*支持密码管理。

某些支持 MS-CHAP 的 RADIUS 服务器当前不支持 MS-CHAPv2。**password-management** 命令需要 MS-CHAPv2，因此请咨询您的供应商。

RADIUS 服务器 （例如 Cisco ACS）可能代理发送到另一个身份验证服务器的身份验证请求。但是，从 ASA 的角度而言，它仅与 RADIUS 服务器通信。

对于 LDAP，更改密码的方法为市场上不同 LDAP 服务器所专有。目前， ASA 仅对 Microsoft Active Directory 和 Sun LDAP 服务器实施专有密码管理逻辑。本机 LDAP 需要 SSL 连接。尝试对 LDAP 进行密码管理之前，必须启用基于 SSL 的 LDAP。默认情况下，LDAP 使用端口 636。

步骤 10　或者，通过输入 **override-account-disable** 命令，配置覆盖来自 AAA 服务器的 account-disabled 指示器的能力：

```
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

注　允许 override-account-disable 是一项潜在安全风险。

步骤 11　指定要在从证书派生授权查询的名称过程中使用的一个或多个属性。此属性指定要用作授权的用户名的主题 DN 字段部分：

```
hostname(config-tunnel-general)# authorization-dn-attributes {primary-attribute
[secondary-attribute] | use-entire-name}
```

例如，以下命令指定使用 CN 属性作为授权的用户名：

```
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

authorization-dn-attributes 包括 **C**（国家 / 地区）、 **CN** （公用名称）、 **DNQ** （DN 限定符）、 **EA**（邮件地址）、 **GENQ** （世代限定符）、 **GN** （名）、 **I** （首字母）、 **L** （区域）、 **N** （名称）、 **O**（组织）、 **OU** （组织单位）、 **SER** （序列号）、 **SN** （姓）、 **SP** （州 / 省）、 **T** （职位）、 **UID**（用户 ID）和 **UPN** （用户主体名称）。

步骤 12　指定是否要求成功授权后才允许用户进行连接。默认是不要求授权。

```
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

配置双重身份验证

双重身份验证是一项可选功能，该功能要求用户在登录屏幕上输入其他身份验证凭证，如第二个用户名和密码。指定以下命令来配置双重身份验证。

步骤 1　指定辅助身份验证服务器组。此命令指定要用作辅助 AAA 服务器的 AAA 服务器组。

注　此命令仅适用于 AnyConnect 客户端 VPN 连接。

辅助服务器组无法指定 SDI 服务器组。默认情况下，无需辅助身份验证。

```
hostname(config-tunnel-general)# secondary-authentication-server-group [interface_name]
{none | LOCAL | groupname [LOCAL]} [use-primary-name]
```

如果使用 none 关键字，则无需辅助身份验证。*groupname* 值指定 AAA 服务器组名。LOCAL 指定使用内部服务器数据库，在与 groupname 值配合使用时， LOCAL 指定回退。例如，要将主身份验证服务器组设置为 sdi_group 并将辅助身份验证服务器组设置为 ldap_server，输入以下命令：

```
hostname(config-tunnel-general)# authentication-server-group
hostname(config-tunnel-general)# secondary-authentication-server-group
```

注　如果使用 **use-primary-name** 关键字，则登录对话框仅请求一个用户名。此外，如果用户名提取自数字证书，则仅使用主要用户名进行身份验证。

步骤 2　如果从证书获取次要用户名，请输入 **secondary-username-from-certificate**：

```
hostname(config-tunnel-general)# secondary-username-from-certificate C | CN | ... |
use-script
```

至于主要 **username-from-certificate** 命令，要从证书提取以用作次要用户名的 DN 字段值相同。或者，可以使用 use-script 关键字，该关键字指导 ASA 使用 ASDM 生成的脚本文件。

例如，要指定 “公用名称”作为主要用户名字段并指定 “组织单位”作为次要用户名字段，请输入以下命令：

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# username-from-certificate cn
hostname(config-tunnel-general)# secondary-username-from-certificate ou
```

步骤 3　在 tunnel-group webvpn-attributes 模式下使用 **secondary-pre-fill-username** 命令来实现从客户端证书提取次要用户名以在身份验证中使用。使用关键字指定此命令适用于无客户端连接还是 SSL VPN (AnyConnect) 客户端连接，以及是否要对最终用户隐藏提取的用户名。此功能默认为已禁用。无客户端和 SSL 客户端选项可同时存在，但是必须在不同命令中对其进行配置。

```
hostname(config-tunnel-general)# secondary-pre-fill-username-from-certificate {clientless
| ssl-client} [hide]
```

例如，要指定使用 pre-fill-username 对连接进行主身份验证和辅助身份验证，请输入以下命令：

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# pre-fill-username ssl-client
hostname(config-tunnel-general)# secondary-pre-fill-username ssl-client
```

步骤 4　指定要使用哪些身份验证服务器来获取适用于连接的授权属性。默认选择是主身份验证服务器。此命令仅对双重身份验证有意义。

```
hostname(config-tunnel-general)# authentication-attr-from-server {primary | secondary}
```

例如，要指定使用辅助身份验证服务器，请输入以下命令：

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authentication-attr-from-server secondary
```

步骤 5　指定要与会话关联的身份验证用户名 （primary 或 secondary）。默认值为 primary。在启用双重身份验证的情况下，会话可能会对两个不同用户名进行身份验证。管理员必须将其中一个已进行身份验证的用户名指定为会话用户名。会话用户名是为记帐、会话数据库、系统日志和调试输出提供的用户名。

```
hostname(config-tunnel-general)# authenticated-session-username {primary | secondary}
```

例如，要指定与会话关联的身份验证用户名必须来自辅助身份验证服务器，请输入以下命令：

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authenticated-session-username secondary
```

配置远程访问连接配置文件 IPsec IKEv1 属性

要为远程访问连接配置文件配置 IPsec IKEv1 属性，请执行以下步骤。以下描述假设您已经创建远程访问连接配置文件。远程访问连接配置文件比 LAN 对 LAN 连接配置文件具有更多属性。

步骤 1　要指定远程访问隧道组的 IPsec 属性，请通过在单情景或多情景模式下输入以下命令来进入 tunnel-group ipsec-attributes 模式。提示符会更改以指示模式发生更改。

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

此命令进入 tunnel-group ipsec-attributes 配置模式，在此模式下可在单情景或多情景模式下配置 remote-access tunnel-group IPsec 属性。

例如，以下命令指定后面的 tunnel-group ipsec-attributes 模式命令与名为 TG1 的连接配置文件相关。请注意，提示符会更改以指示您处于 tunnel-group ipsec-attributes 模式：

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

步骤 2　指定预共享密钥以基于预共享密钥来支持 IKEv1 连接。例如，以下命令指定预共享密钥 xyzx 以支持 IPsec IKEv1 远程访问连接配置文件的 IKEv1 连接：

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-ipsec)#
```

步骤 3　指定是否使用对等体的证书来验证对等体的身份：

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

可能的 *option* 值为 **req** （必需）、 **cert** （如果受证书支持）和 **nocheck** （不检查）。默认值为 **req**。

例如，以下命令指定必需 peer-id 验证：

```
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

步骤 4　指定是否启用证书链的发送。以下命令在传输中包含根证书和任何从属 CA 证书：

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

此属性适用于所有 IPsec 隧道组类型。

步骤 5　指定用于标识要发送到 IKE 对等体的证书的信任点的名称：

```
hostname(config-tunnel-ipsec)# ikev1 trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

以下命令指定 mytrustpoint 作为要发送到 IKE 对等体的证书的名称：

```
hostname(config-ipsec)# ikev1 trust-point mytrustpoint
```

步骤 6　指定 ISAKMP 保活阈值和允许的重试次数：

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

threshold 参数指定在开始保活监控之前允许对等体空闲的秒数（10 至 3600）。**retry** 参数是尚未接收到保活响应后前后两次重试之间的间隔（2 至 10 秒）。默认情况下会启用 IKE 保活。要禁用 ISAKMP 保活，请输入 **isakmp keepalive disable**。

例如，以下命令将 IKE 保活阈值设置为 15 秒，并将重试间隔设置为 10 秒：

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

threshold 参数的默认值对于远程访问为 300，对于 LAN 对 LAN 为 10，并且 retry 参数的默认值为 2。

要指定中心站点 （安全网关）绝不应启动 ISAKMP 监控，请输入以下命令：

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

步骤 7　指定 ISAKMP 混合身份验证方法 （XAUTH 或混合 XAUTH）。

当需要使用数字证书进行 ASA 身份验证并使用其他传统方法 （如 RADIUS、 TACACS+ 或 SecurID）进行远程 VPN 用户身份验证时，请使用 **isakmp ikev1-user-authentication** 命令来实施混合 XAUTH 身份验证。混合 XAUTH 将 IKE 的阶段 1 分为以下两个步骤，统称为混合身份验证：

a. ASA 使用标准公钥方法对远程 VPN 用户进行身份验证。这将建立进行单向身份验证的 IKE 安全关联。

b. 然后， XAUTH 交换对远程 VPN 用户进行身份验证。此扩展身份验证可以使用其中一种受支持的传统身份验证方法。

注　必须配置身份验证服务器，创建预共享密钥并配置信任点，然后才能将身份验证类型设置为混合。

可以将 **isakmp ikev1-user-authentication** 命令与可选的 **interface** 参数配合使用来指定特定接口。当省略 **interface** 参数时，该命令适用于所有接口，并且在未指定 per-interface 命令时充当备份。如果为连接配置文件中指定了两个 **isakmp ikev1-user-authentication** 命令，并且一个使用 **interface** 参数而另一个不使用该参数，则指定 interface 的命令对于该特定接口而言优先。

例如，以下命令在名为 example-group 的连接配置文件的内部接口上启用混合 XAUTH：

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication (inside) hybrid
hostname(config-tunnel-ipsec)#
```

配置 IPsec 远程访问连接配置文件 PPP 属性

要为远程访问连接配置文件配置 Point-to-Point Protocol 属性，请执行以下步骤。 PPP 属性*仅*适用于 IPsec 远程访问连接配置文件。以下描述假设您已经创建 IPsec 远程访问连接配置文件。

步骤 1　进入 tunnel-group ppp-attributes 配置模式，在此模式下可通过输入以下命令来配置 remote-access tunnel-group PPP 属性。提示符会更改以指示模式发生更改：

```
hostname(config)# tunnel-group tunnel-group-name type remote-access
hostname(config)# tunnel-group tunnel-group-name ppp-attributes
hostname(config-tunnel-ppp)#
```

例如，以下命令指定后面的 tunnel-group ppp-attributes 模式命令与名为 TG1 的连接配置文件相关。请注意，提示符会更改以指示您现在处于 tunnel-group ppp-attributes 模式：

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ppp-attributes
hostname(config-tunnel-ppp)#
```

步骤 2　指定是否对 PPP 连接使用特定协议来启用身份验证。协议值可以是以下任何一项：

- pap — 对 PPP 连接启用密码身份验证协议。
- chap — 对 PPP 连接启用质询握手身份验证协议。
- ms-chap-v1 或 ms-chap-v2 — 对 PPP 连接启用 Microsoft 质询握手身份验证协议版本 1 或版本 2。
- eap — 对 PPP 连接启用可扩展身份验证协议。

默认情况下会启用 CHAP 和 MSCHAPv1。

此命令的语法为：

```
hostname(config-tunnel-ppp)# authentication protocol
hostname(config-tunnel-ppp)#
```

要对特定协议禁用身份验证，请使用该命令的 **no** 形式：

```
hostname(config-tunnel-ppp)# no authentication protocol
hostname(config-tunnel-ppp)#
```

例如，以下命令对 PPP 连接启用 PAP 协议：

```
hostname(config-tunnel-ppp)# authentication pap
hostname(config-tunnel-ppp)#
```

以下命令对 PPP 连接启用 MS-CHAP 版本 2 协议：

```
hostname(config-tunnel-ppp)# authentication ms-chap-v2
hostname(config-tunnel-ppp)#
```

以下命令对 PPP 连接启用 EAP-PROXY 协议：

```
hostname(config-tunnel-ppp)# authentication pap
hostname(config-tunnel-ppp)#
```

以下命令对 PPP 连接禁用 MS-CHAP 版本 1 协议：

```
hostname(config-tunnel-ppp)# no authentication ms-chap-v1
hostname(config-tunnel-ppp)#
```

配置 LAN 对 LAN 连接配置文件

IPsec LAN 对 LAN VPN 连接配置文件仅适用于 LAN 对 LAN IPsec 客户端连接。虽然您配置的许多参数就 IPsec 远程访问连接配置文件而言相同，但是 LAN 对 LAN 隧道具有更少的参数。以下各节说明如何配置 LAN 对 LAN 连接配置文件。

默认 LAN 对 LAN 连接配置文件配置

默认 LAN 对 LAN 连接配置文件的内容如下：

```
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
 no accounting-server-group
 default-group-policy DfltGrpPolicy
tunnel-group DefaultL2LGroup ipsec-attributes
 no ikev1 pre-shared-key
 peer-id-validate req
 no chain
 no ikev1 trust-point
 isakmp keepalive threshold 10 retry 2
```

LAN 对 LAN 连接配置文件具有比远程访问连接配置文件更少的参数，并且其中大多数参数对于两个组均相同。为便于配置连接，此处将其单独列出。未显式配置的所有参数从默认连接配置文件继承其值。

指定 LAN 对 LAN 连接配置文件的名称和类型

要指定连接配置文件的名称和类型，请输入 **tunnel-group** 命令，如下所示：

```
hostname(config)# tunnel-group tunnel_group_name type tunnel_type
```

对于 LAN 对 LAN 隧道，类型为 **ipsec-l2l**；例如，要创建名为 docs 的 LAN 对 LAN 连接配置文件，请输入以下命令：

```
hostname(config)# tunnel-group docs type ipsec-l2l
hostname(config)#
```

配置 LAN 对 LAN 连接配置文件常规属性

要配置连接配置文件常规属性，请执行以下步骤：

步骤 1　通过在单情景或多情景模式下指定 general-attributes 关键字来进入 tunnel-group general-attributes 模式：

```
hostname(config)# tunnel-group_tunnel-group-name general-attributes
hostname(config-tunnel-general)#
```

提示符会更改以指示您现在处于 config-general 模式，在此模式下可配置隧道组常规属性。

例如，对于名为 docs 的连接配置文件，请输入以下命令：

```
hostname(config)# tunnel-group_docs general-attributes
hostname(config-tunnel-general)#
```

步骤 2　指定要使用的记帐服务器组的名称 （如果有）。

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

例如，以下命令指定使用记帐服务器组 acctgserv1：

```
hostname(config-tunnel-general)# accounting-server-group acctgserv1
hostname(config-tunnel-general)#
```

步骤 3　指定默认组策略的名称：

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

例如，以下命令指定默认组策略的名称为 MyPolicy：

```
hostname(config-tunnel-general)# default-group-policy MyPolicy
hostname(config-tunnel-general)#
```

配置 LAN 对 LAN IPsec IKEv1 属性

要配置 IPsec IKEv1 属性，请执行以下步骤：

步骤 1　要配置隧道组 IPsec IKEv1 属性，请通过在单情景或多情景模式下输入具有 IPsec-attributes 关键字的 tunnel-group 命令来进入 tunnel-group ipsec-attributes 配置模式。

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

例如，以下命令进入 config-ipsec 模式，以便您可以配置名为 TG1 的连接配置文件的参数。

```
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

提示符会更改以指示您现在处于 tunnel-group ipsec-attributes 配置模式。

步骤 2　指定预共享密钥以基于预共享密钥来支持 IKEv1 连接。

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key key
hostname(config-tunnel-ipsec)#
```

例如，以下命令指定预共享密钥 XYZX 以支持 LAN 对 LAN 连接配置文件的 IKEv1 连接：

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-general)#
```

步骤 3　指定是否使用对等体的证书来验证对等体的身份：

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

可用选项为 **req** （必需）、 **cert** （如果受证书支持）和 **nocheck** （不检查）。默认值为 **req**。例如，以下命令将 peer-id-validate 选项设置为 **nocheck**：

```
hostname(config-tunnel-ipsec)# peer-id-validate nocheck
hostname(config-tunnel-ipsec)#
```

步骤 4　指定是否启用证书链的发送。此操作在传输中包含根证书和任何从属 CA 证书：

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

您可以将此属性应用于所有隧道组类型。

步骤 5　指定用于标识要发送到 IKE 对等体的证书的信任点的名称：

```
hostname(config-tunnel-ipsec)# trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

例如，以下命令将信任点名称设置为 mytrustpoint：

```
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
hostname(config-tunnel-ipsec)#
```

您可以将此属性应用于所有隧道组类型。

步骤 6　指定 ISAKMP (IKE) 保活阈值和允许的重试次数。**threshold** 参数指定在开始保活监控之前允许对等体空闲的秒数 （10 至 3600）。 **retry** 参数是尚未接收到保活响应后前后两次重试之间的间隔（2 至 10 秒）。默认情况下会启用 IKE 保活。要禁用 IKE 保活，请输入 **no** 形式的 **isakmp** 命令：

```
hostname(config)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

例如，以下命令将 ISAKMP 保活阈值设置为 15 秒，并将重试间隔设置为 10 秒：

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

LAN 对 LAN 的 **threshold** 参数的默认值为 10， retry 参数的默认值为 2。

要指定中心站点 （安全网关）绝不应启动 ISAKMP 监控，请输入以下命令：

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

步骤 7　指定 ISAKMP 混合身份验证方法 （XAUTH 或混合 XAUTH）。

当需要使用数字证书进行 ASA 身份验证并使用其他传统方法 （如 RADIUS、 TACACS+ 或 SecurID）进行远程 VPN 用户身份验证时，请使用 **isakmp ikev1-user-authentication** 命令来实施混合 XAUTH 身份验证。混合 XAUTH 将 IKE 的阶段 1 分为以下两个步骤，统称为混合身份验证：

a. ASA 使用标准公钥方法对远程 VPN 用户进行身份验证。这将建立进行单向身份验证的 IKE 安全关联。

b. 然后， XAUTH 交换对远程 VPN 用户进行身份验证。此扩展身份验证可以使用其中一种受支持的传统身份验证方法。

注　必须配置身份验证服务器，创建预共享密钥并配置信任点，然后才能将身份验证类型设置为混合。

例如，以下命令对名为 example-group 的连接配置文件启用混合 XAUTH：

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication hybrid
hostname(config-tunnel-ipsec)#
```

配置无客户端 SSL VPN 会话的连接配置文件

无客户端 SSL VPN 连接配置文件的隧道组常规属性是与 IPsec 远程访问连接配置文件的隧道组常规属性相同，不同在于隧道组类型为但隧道组类型为 webvpn，并且 **strip-group** 和 **strip-realm** 命令不适用。可单独定义特定于无客户端 SSL VPN 的属性。以下各节描述如何配置无客户端 SSL VPN 连接配置文件：

配置无客户端 SSL VPN 会话的常规隧道组属性

要配置或更改连接配置文件常规属性，请在以下步骤中指定参数。

步骤 1　要配置常规属性，请输入 **tunnel-group general-attributes** 命令，该命令在单情景或多情景模式下进入 tunnel-group general-attributes 配置模式。请注意，提示符会更改：

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

要配置上一节中创建的 TunnelGroup3 的常规属性，请输入以下命令：

```
hostname(config)# tunnel-group TunnelGroup3 general-attributes
hostname(config-tunnel-general)#
```

步骤 2　指定要使用的身份验证服务器组的名称 （如果有）。如果要在指定服务器组失败的情况下使用 LOCAL 数据库进行身份验证，请附加关键字 LOCAL：

```
hostname(config-tunnel-general)# authentication-server-group groupname [LOCAL]
hostname(config-tunnel-general)#
```

例如，要配置名为 test 的身份验证服务器组，并且要在身份验证服务器组失败的情况下提供到 LOCAL 服务器的回退，请输入以下命令：

```
hostname(config-tunnel-general)# authentication-server-group test LOCAL
hostname(config-tunnel-general)#
```

authentication-server-group 名称标识以前配置的身份验证服务器或服务器组。使用 **aaa-server** 命令配置身份验证服务器。组标记的最大长度为 16 个字符。

您也可以通过在组名之后包含括号中接口的名称来配置特定于接口的身份验证。默认情况下，以下接口可用：

- inside — 接口 GigabitEthernet0/1 的名称
- outside — 接口 GigabitEthernet0/0 的名称

注　ASA 的外部接口地址 （对于 IPv4/IPv6 均适用）不能与专用侧地址空间重叠。

您已配置的其他接口 （使用 **interface** 命令）也可用。以下命令使用服务器 servergroup1 进行身份验证来为名为 outside 的接口配置特定于接口的身份验证：

```
hostname(config-tunnel-general)# authentication-server-group (outside) servergroup1
hostname(config-tunnel-general)#
```

步骤 3　或者，指定要使用的授权服务器组的名称（如果有）。如果未在使用授权，请转至步骤 6。配置该值时，用户必须存在于要连接的授权数据库中：

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

使用 **aaa-server** 命令配置授权服务器。组标记的最大长度为 16 个字符。

例如，以下命令指定使用授权服务器组 FinGroup：

```
hostname(config-tunnel-general)# authorization-server-group FinGroup
hostname(config-tunnel-general)#
```

步骤 4　指定是否要求成功授权后才允许用户进行连接。默认是不要求授权。

```
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

步骤 5　指定要在从证书派生授权查询的名称过程中使用的一个或多个属性。此属性指定要用作授权的用户名的主题 DN 字段部分：

```
hostname(config-tunnel-general)# authorization-dn-attributes {primary-attribute
[secondary-attribute] | use-entire-name}
```

例如，以下命令指定使用 CN 属性作为授权的用户名：

```
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

authorization-dn-attributes 包括 **C**（国家 / 地区）、**CN**（公用名称）、**DNQ**（DN 限定符）、**EA**（邮件地址）、**GENQ**（世代限定符）、**GN**（名）、**I**（首字母）、**L**（区域）、**N**（名称）、**O**（组织）、**OU**（组织单位）、**SER**（序列号）、**SN**（姓）、**SP**（州 / 省）、**T**（职位）、**UID**（用户 ID）和 **UPN**（用户主体名称）。

步骤 6　或者，指定要使用的记帐服务器组的名称（如果有）。如果未在使用记帐，请转至步骤 7。使用 **aaa-server** 命令配置记帐服务器。组标记的最大长度为 16 个字符。

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

例如，以下命令指定使用记帐服务器组 comptroller：

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

步骤 7　或者，指定默认组策略的名称。默认值为 DfltGrpPolicy：

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

以下示例将 MyDfltGrpPolicy 设置为默认组策略的名称：

```
hostname(config-tunnel-general)# default-group-policy MyDfltGrpPolicy
hostname(config-tunnel-general)#
```

步骤 8　或者，指定 DHCP 服务器（最多 10 台服务器）的名称或 IP 地址，以及 DHCP 地址池（最多 6 个池）的名称。以逗号分隔列表项。默认为无 DHCP 服务器且无地址池。

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```

注　接口名称必须用括号括起来。

在全局配置模式下可使用 **ip local pool** 命令来配置地址池。有关配置地址池的信息，请参阅第 5 章，“VPN 的 IP 地址”。

步骤 9　或者，如果服务器是 RADIUS、使用 NT 的 RADIUS 或 LDAP 服务器，则可以启用密码管理。

注　如果是使用 LDAP 目录服务器进行身份验证，则通过 Sun Microsystems JAVA 系统目录服务器（以前称为 Sun ONE 目录服务器）和 Microsoft Active Directory 来支持密码管理。

- DN — 在 ASA 上配置用于访问 Sun 目录服务器的 DN 必须能够访问该服务器上的默认密码策略。建议使用目录管理员或具有目录管理员特权的用户作为 DN。或者，可以在默认密码策略上放置 ACI。
- Microsoft — 必须配置基于 SSL 的 LDAP 以对 Microsoft Active Directory 启用密码管理。

此功能 （默认情况下会启用）在当前密码即将到期时警告用户。默认是在到期前 14 天开始警告用户：

```
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

如果服务器是 LDAP 服务器，则可以指定开始警告用户即将到期的截止天数 （0 to 180）：

```
hostname(config-tunnel-general)# password-management [password-expire in days n]
hostname(config-tunnel-general)#
```

注　在 tunnel-group general-attributes 配置模式下输入的 **password-management** 命令会替换以前在 tunnel-group ipsec-attributes 模式下输入的已弃用的 **radius-with-expiry** 命令。

配置此命令时， ASA 会在远程用户登录时通知其当前密码即将到期或已到期。然后， ASA 为用户提供机会更改密码。如果当前密码尚未到期，则用户仍可使用该密码进行登录。如果尚未配置 RADIUS 或 LDAP 身份验证，则 ASA 会忽略此命令。

请注意，这不会更改密码到期之前的天数，而是更改 ASA 开始警告用户密码即将到期的提前天数。

如果确实指定 **password-expire-in-days** 关键字，则还必须指定天数。

有关详细信息，请参阅第 4-25 页上的配置 Microsoft Active Directory 设置以进行密码管理。

步骤 10　指定此命令且天数设置为 0 会禁用此命令。ASA 不通知用户即将到期，但是用户可以在密码到期后对其进行更改。或者，通过输入 **override-account-disable** 命令来配置覆盖来自 AAA 服务器的 account-disabled 指示器的能力。

```
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

注　允许覆盖 account-disabled 是一项潜在安全风险。

配置无客户端 SSL VPN 会话的隧道组属性

要配置特定于无客户端 SSL VPN 连接配置文件的参数，请遵循本节中的步骤。无客户端 SSL VPN 以前称为 WebVPN，并且您在 tunnel-group webvpn-attributes 模式下配置这些属性。

步骤 1　要指定无客户端 SSL VPN 隧道组的属性，请通过输入以下命令来进入 tunnel-group webvpn-attributes 模式。提示符会更改以指示模式发生更改：

```
hostname(config)# tunnel-group tunnel-group-name webvpn-attributes
hostname(config-tunnel-ipsec)#
```

例如，要为名为 sales 的无客户端 SSL VPN 隧道组指定 webvpn-attributes，请输入以下命令：

```
hostname(config)# tunnel-group sales webvpn-attributes
hostname(config-tunnel-webvpn)#
```

步骤 2　要指定将使用的身份验证方法 （AAA 和 / 或数字证书），请输入 **authentication** 命令。可以按任意顺序指定 aaa 和 / 或证书。

```
hostname(config-tunnel-webvpn)# authentication authentication_method
hostname(config-tunnel-webvpn)#
```

例如，以下命令同时允许 AAA 和证书身份验证：

```
hostname(config-tunnel-webvpn)# authentication aaa certificate
hostname(config-tunnel-webvpn)#
```

应用定制

定制确定用户在登录时看到的窗口的外观。可在配置无客户端 SSL VPN 过程中配置定制参数。

要应用以前定义的网页定制来更改用户在登录时看到的网页外观，请在 username webvpn 配置模式下输入定制命令：

```
hostname(config-username-webvpn)# customization {none | value customization_name}
hostname(config-username-webvpn)#
```

例如，要使用名为 blueborder 的定制，请输入以下命令：

```
hostname(config-username-webvpn)# customization value blueborder
hostname(config-username-webvpn)#
```

可通过在 webvpn 模式下输入 **customization** 命令来配置定制本身。

以下示例显示一个命令序列，它首先建立名为 “123” 的定制来定义密码提示。然后，该示例定义名为 “test” 的无客户端 SSL VPN 隧道组，并使用 **customization** 命令指定使用名为 “123” 的定制：

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# customization value 123
hostname(config-tunnel-webvpn)#
```

步骤 3　ASA 查询 NetBIOS 名称服务器以将 NetBIOS 名称映射到 IP 地址。无客户端 SSL VPN 要求 NetBIOS 访问或共享远程系统上的文件。无客户端 SSL VPN 使用 NetBIOS 和 CIFS 协议来访问或共享远程系统上的文件。当尝试使用 Windows 计算机的计算机名称来与其建立文件共享连接时，指定的文件服务器与标识网络上的资源的特定 NetBIOS 名称对应。

要使 NBNS 功能可运行，必须配置至少一个 NetBIOS 服务器（主机）。可以配置最多三个 NBNS 服务器来实现冗余。 ASA 使用列表中的第一个服务器进行 NetBIOS/CIFS 域名解析。如果查询失败，则使用下一个服务器。

要指定用于 CIFS 名称解析的 NBNS（NetBIOS 名称服务）服务器的名称，请使用 **nbns-server** 命令。可以输入最多三个服务器条目。您配置的第一个服务器是主服务器，其他是备份，用于实现冗余。您还可以指定这是否为主浏览器 （而不只是 WINS 服务器）、超时间隔和重试次数。WINS 服务器或主浏览器通常与 ASA 位于同一网络上，或者可从该网络进行访问。必须在重试次数之前指定超时间隔：

```
hostname(config-tunnel-webvpn)# nbns-server {host-name | IP_address} [master]
[timeout seconds] [retry number]
hostname(config-tunnel-webvpn)#
```

例如，要将名为 nbnsprimary 的服务器配置为主服务器并将服务器 192.168.2.2 配置为辅助服务器，每个服务器允许重试三次且超时为 5 秒，请输入以下命令：

```
hostname(config)# name 192.168.2.1 nbnsprimary
hostname(config-tunnel-webvpn)# nbns-server nbnsprimary master timeout 5 retry 3
hostname(config-tunnel-webvpn)# nbns-server 192.168.2.2 timeout 5 retry 3
hostname(config-tunnel-webvpn)#
```

超时间隔范围为 1 至 30 秒 （默认值为 2），重试次数的范围可为 0 至 10 （默认值为 2）。

tunnel-group webvpn-attributes 配置模式下的 **nbns-server** 命令会替换 webvpn 模式下已弃用的 **nbns-server** 命令。

步骤 4　要指定组的备用名称，请使用 **group-alias** 命令。指定组别名会创建可供用户引用隧道组的一个或多个备用名称。此处指定的组别名显示在用户登录页面上的下拉列表中。每个组可具有多个别名或没有别名，在不同命令中分别进行指定。此功能在同一个组具有多个常见名称 （如 “Devtest” 和 “QA”）时有用。

对于每个组别名，请输入 **group-alias** 命令。默认情况下会启用每个别名。可以选择性显式启用或禁用每个别名：

```
hostname(config-tunnel-webvpn)# group-alias alias [enable | disable]
hostname(config-tunnel-webvpn)#
```

例如，要对名为 QA 的隧道组启用别名 QA 和 Devtest，请输入以下命令：

```
hostname(config-tunnel-webvpn)# group-alias QA enable
hostname(config-tunnel-webvpn)# group-alias Devtest enable
hostname(config-tunnel-webvpn)#
```

注　必须启用 webvpn tunnel-group-list 才会显示 （下拉）组列表。

步骤 5　要指定组的传入 URL 或 IP 地址，请使用 **group-url** 命令。指定组 URL 或 IP 地址可使用户在登录时无需选择组。当用户登录时，ASA 在 tunnel-group-policy 表中查找用户的传入 URL 或地址。如果它找到 URL 或地址，并且如果在连接配置文件中启用了 group-url，则 ASA 将自动选择关联的连接配置文件，并在登录窗口中仅向用户呈现用户名和密码字段。这可简化用户界面，并且新增一个优点，即绝不向用户暴露组列表。用户看到的登录窗口使用为该连接配置文件配置的定制。

如果禁用了 URL 或地址并配置了别名，则还会显示组下拉列表，并且用户必须进行选择。

可以为组配置多个 URL 或地址（或不匹配任何 URL 或地址）。可以单独启用或禁用每个 URL 或地址。必须为指定的每个 URL 或地址使用单独的 **group-url** 命令。必须指定整个 URL 或地址，包括 http 或 https 协议。

不能将同一 URL 或地址与多个组关联。ASA 在接受连接配置文件的 URL 或地址之前会验证 URL 或地址的唯一性。

对于每个组 URL 或地址，请输入 **group-url** 命令。可以选择性显式启用 （默认）或禁用每个 URL 或别名：

```
hostname(config-tunnel-webvpn)# group-url url [enable | disable]
hostname(config-tunnel-webvpn)#
```

Url 指定此隧道组的 URL 或 IP 地址。

例如，要对名为 RadiusServer 的隧道组启用组 URL http://www.example.com 和 http://192.168.10.10，请输入以下命令：

```
hostname(config)# tunnel-group RadiusServer type webvpn
hostname(config)# tunnel-group RadiusServer general-attributes
hostname(config-tunnel-general)# authentication server-group RADIUS
hostname(config-tunnel-general)# accounting-server-group RADIUS
hostname(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias “Cisco Remote Access” enable
hostname(config-tunnel-webvpn)# group-url http://www.example.com enable
hostname(config-tunnel-webvpn)# group-url http://192.168.10.10 enable
hostname(config-tunnel-webvpn)#
```

有关更广泛的示例，请参阅第 4-24 页上的定制无客户端 SSL VPN 会话用户的登录窗口。

步骤 6　要在某些用户输入其中一个 group-url 的情况下免除其逐个连接配置文件运行思科安全桌面，请输入以下命令：

```
hostname(config-tunnel-webvpn)# without-csd
hostname(config-tunnel-webvpn)#
```

注　输入此命令会阻止检测这些会话的终端条件，因此您可能需要调整动态访问策略 (DAP) 配置。

步骤 7　要指定用于无客户端 SSL VPN 会话的连接配置文件的 DNS 服务器组，请使用 **dns-group** 命令。您指定的组必须是已在全局配置模式下配置的组（使用 **dns server-group** 和 **name-server** 命令）。

默认情况下，连接配置文件使用 DNS 服务器组 *DefaultDNS*。但是，必须先配置该组，然后安全设备才能解析 DNS 请求。

以下示例配置名为 *corp_dns* 的新 DNS 服务器组并指定连接配置文件 *telecommuters* 的服务器组：

```
hostname(config)# dns server-group corp_dns
hostname(config-dns-server-group)# domain-name cisco.com
hostname(config-dns-server-group)# name-server 209.165.200.224

hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# dns-group corp_dns
hostname(config-tunnel-webvpn)#
```

步骤 8　（可选）要启用从客户端证书提取用户名以用于身份验证和授权用，请在 tunnel-group webvpn-attributes 模式下使用 **pre-fill-username** 命令。没有默认值。

```
hostname(config)# pre-fill-username {ssl-client | clientless}
```

pre-fill-username 命令支持将从 **username-from-certificate** 命令中 （在 tunnel-group general-attributes 模式下）指定的证书字段中提取的用户名用作用户名 / 密码身份验证和授权的用户名。要使用证书功能中的此预填充用户名，必须配置这两个命令。

注　在版本 8.0.4 中，用户名未预填充；相反，会忽略在用户名字段中发送的任何数据略。

以下示例 （在全局配置模式下输入）创建名为 remotegrp 的 IPsec 远程访问隧道组，支持从证书获取用户名，并且指定 SSL VPN 客户端的身份验证或授权查询的名称必须派生自数字证书：

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# username-from-certificate CN OU
hostname(config)# tunnel-group remotegrp webvpn-attributes
hostname(config-tunnel-webvpn)# pre-fill-username ssl-client
hostname(config-tunnel-webvpn)#
```

步骤 9　（可选）要指定覆盖组策略还是用户名属性配置来下载 AnyConnect 或 SSL VPN 客户端，请使用 **override-svc-download** 命令。默认情况下会禁用此功能。

安全设备根据是否使用 **vpn-tunnel-protocol** 命令在组策略或用户名属性中启用了无客户端和 / 或 SSL VPN 来允许远程用户的无客户端连接或 AnyConnect 客户端连接。 **anyconnect ask** 命令通过提示用户下载客户端或返回到 WebVPN 主页来进一步修改客户端用户体验。

但是，您可能希望在向特定隧道组下登录的无客户端用户呈现无客户端 SSL VPN 主页之前，这些用户在等待下载提示到期时不会遇到延迟。可以使用 **override-svc-download** 命令在连接配置文件级别防止这些用户遇到延迟。此命令导致立即向通过连接配置文件登录的用户呈现无客户端 SSL VPN 主页，而无论 **vpn-tunnel-protocol** or **anyconnect ask** 命令设置如何。

在以下示例中，您进入连接配置文件 *engineering* 的 tunnel-group webvpn attributes 配置模式，并使该连接配置文件能够覆盖客户端下载提示的组策略和用户名属性设置：

```
hostname(config)# tunnel-group engineering webvpn-attributes
hostname(config-tunnel-webvpn)# override-svc-download
```

步骤 10　（可选）要在拒绝身份验证后在登录屏幕上启用 RADIUS 拒绝消息的显示，请使用 **radius-eject-message** 命令。

以下示例对名为 engineering 的连接配置文件启用 RADIUS 拒绝消息的显示：

```
hostname(config)# tunnel-group engineering webvpn-attributes
hostname(config-tunnel-webvpn)# radius-reject-message
```

定制无客户端 SSL VPN 会话用户的登录窗口

可以通过使用定制配置文件和连接配置文件的组合来为不同的组设置不同的登录窗口。例如，假设您已创建名为 salesgui 的定制配置文件，则可为无客户端 SSL VPN 会话创建名为 sales 的使用该定制配置文件的连接配置文件，如下例所示：

步骤 1　在 webvpn 模式下，定义无客户端 SSL VPN 访问的定制 （在本例中名为 salesgui），并将默认徽标更改为 mycompanylogo.gif。必须已在先前将 mycompanylogo.gif 加载到 ASA 的闪存上并保存配置。有关详细信息，请参阅第 13 章，“无客户端 SSL VPN 简介”。

```
hostname# webvpn
hostname (config-webvpn)# customization value salesgui
hostname(config-webvpn-custom)# logo file disk0:\mycompanylogo.gif
hostname(config-webvpn-custom)#
```

步骤 2　在全局配置模式下，设置用户名并将其与刚定义的无客户端的 SSL VPN 的定制关联。

```
hostname# username seller attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# customization value salesgui
hostname(config-username-webvpn)# exit
hostname(config-username)# exit
hostname#
```

步骤 3　在全局配置模式下，为无客户端 SSL VPN 会话创建名为 sales 的隧道组：

```
hostname# tunnel-group sales type webvpn
hostname(config-tunnel-webvpn)#
```

步骤 4　指定要对此连接配置文件使用 salesgui 定制：

```
hostname# tunnel-group sales webvpn-attributes
hostname(config-tunnel-webvpn)# customization salesgui
```

步骤 5　将组 URL 设置为用户输入到浏览器中以登录到 ASA 的地址；例如，如果 ASA 的 IP 地址为 192.168.3.3，请将组 URL 设置为 https://192.168.3.3：

```
hostname(config-tunnel-webvpn)# group-url https://192.168.3.3.
hostname(config-tunnel-webvpn)#
```

如果成功登录必需端口号，请在冒号后包含端口号。 ASA 将此 URL 映射到 sales 连接配置文件，并将 salesgui 定制配置文件应用于用户在登录到 https://192.168.3.3 时看到的登录屏幕。

配置 Microsoft Active Directory 设置以进行密码管理

注　如果是使用 LDAP 目录服务器进行身份验证，则通过 Sun Microsystems JAVA 系统目录服务器（以前称为 Sun ONE 目录服务器）和 Microsoft Active Directory 来支持密码管理。

- DN — 在 ASA 上配置用于访问 Sun 目录服务器的 DN 必须能够访问该服务器上的默认密码策略。建议使用目录管理员或具有目录管理员特权的用户作为 DN。或者，可以在默认密码策略上放置 ACI。
- Microsoft — 必须配置基于 SSL 的 LDAP 以对 Microsoft Active Directory 启用密码管理。

要将密码管理与 Microsoft Active Directory 配合使用，必须设置某些 Active Directory 参数以及在 ASA 上配置密码管理。本节描述与各种密码管理操作关联的 Active Directory 设置。这些描述假设您已在 ASA 上启用密码管理并配置对应的密码管理属性。本节中的特定步骤引用 Windows 2000 下的 Active Directory 术语并包含以下主题：

- 第 4-26 页上的使用 Active Directory 强制用户在下次登录时更改密码
- 第 4-27 页上的使用 Active Directory 指定最长密码期限
- 第 4-28 页上的使用 Active Directory 覆盖 Account Disabled AAA 指示器
- 第 4-30 页上的使用 Active Directory 实施密码复杂性

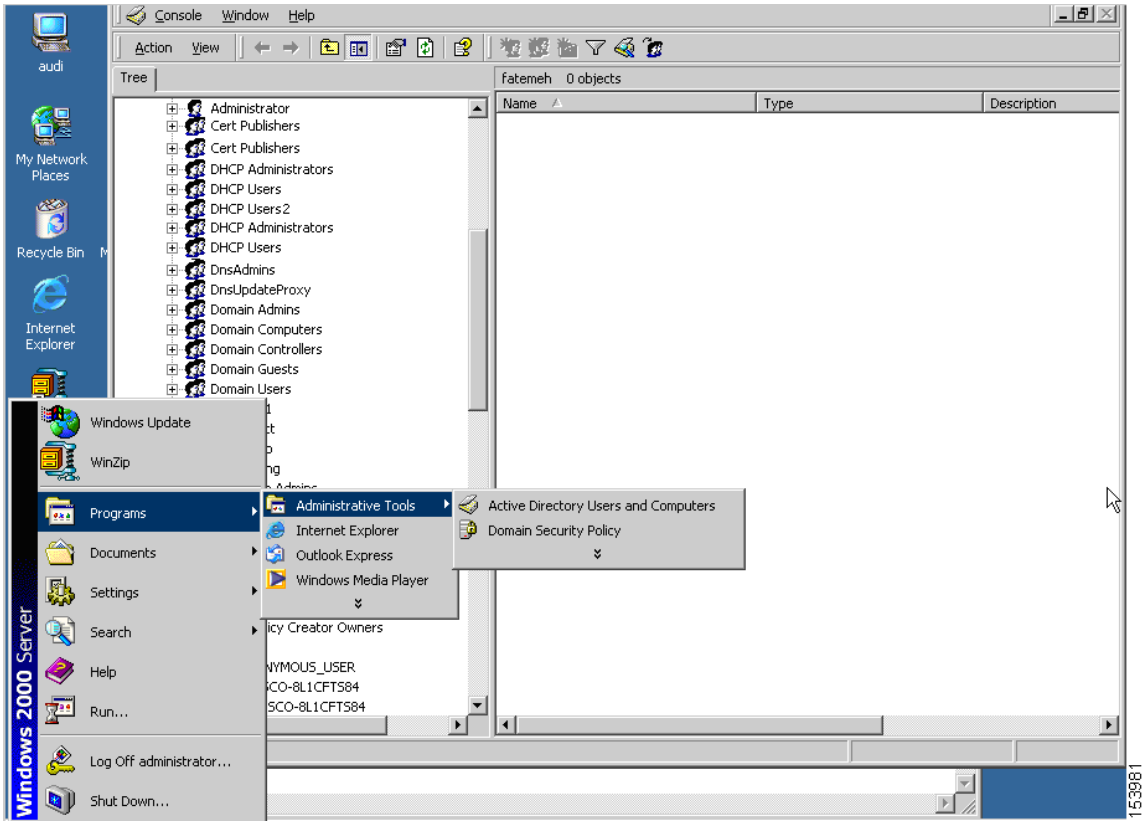
本节假设您是使用 LDAP 目录服务器进行身份验证。

使用 Active Directory 强制用户在下次登录时更改密码

要强制用户在下次登录时更改用户密码，请在 ASA 上的 tunnel-group general-attributes 配置模式下指定 **password-management** 命令，并在 Active Directory 下执行以下步骤：

步骤 1　选择 **Start > Programs > Administrative Tools > Active Directory Users and Computers** (图 4-1)。

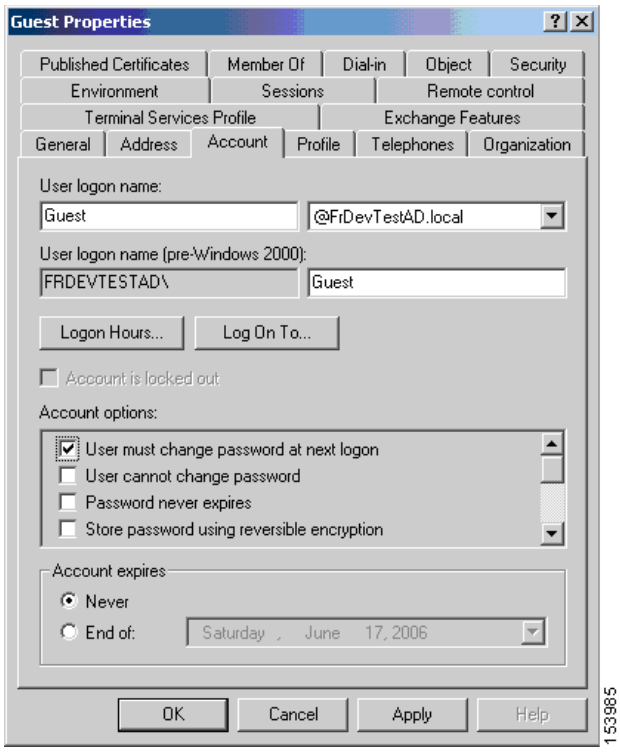
图 4-1　　Active Directory — Administrative Tools 菜单



步骤 2　右键单击选择 **Username > Properties > Account**。

步骤 3　选中 **User must change password at next logon** (图 4-2) 复选框。

图 4-2　　Active Directory — 用户在下次登录时必须更改密码



下次此用户登录时，ASA 会显示以下提示：“New password required.Password change required.You must enter a new password with a minimum length *n* to continue.”您可以在 Active Directory 配置过程中设置最小必需密码长度 *n*（Start > Programs > Administrative Tools > Domain Security Policy > Windows Settings > Security Settings > Account Policies > Password Policy）。选择 **Minimum password length**。

使用 Active Directory 指定最长密码期限

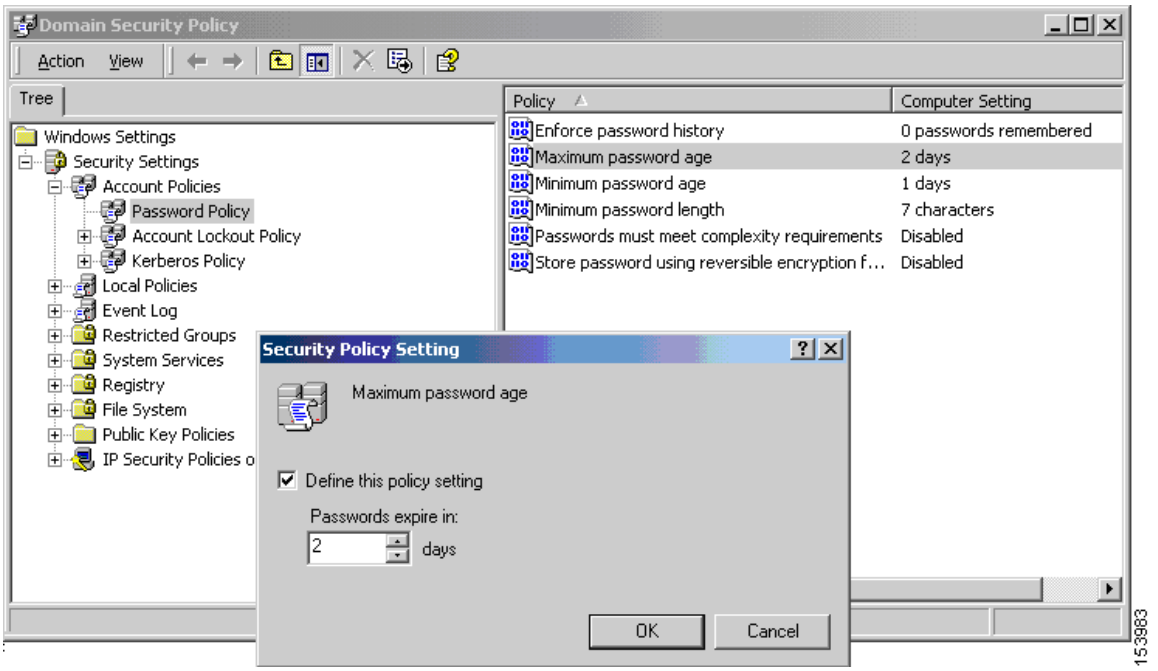
要增强安全性，可以指定密码在经过一定天数后到期。要指定用户密码的最长密码期限，请在 ASA 上的 tunnel-group general-attributes 配置模式下指定 **password-management** 命令，并在 Active Directory 下执行以下步骤：

步骤 1　选择 **Start > Programs > Administrative Tools > Domain Security Policy > Windows Settings > Security Settings > Account Policies > Password Policy**。

步骤 2　双击 Maximum password age。系统将显示 Security Policy Setting 对话框。

步骤 3　选中 **Define this policy setting** 复选框并指定要允许的最长密码期限 （以天为单位）。

图 4-3　　Active Directory — 最长密码期限



注　已弃用 **radius-with-expiry** 命令（以前配置为 tunnel-group remote-access 配置的一部分以执行密码期限功能）。在 tunnel-group general-attributes 模式下输入的 **password-management** 命令会将其替换。

使用 Active Directory 覆盖 Account Disabled AAA 指示器

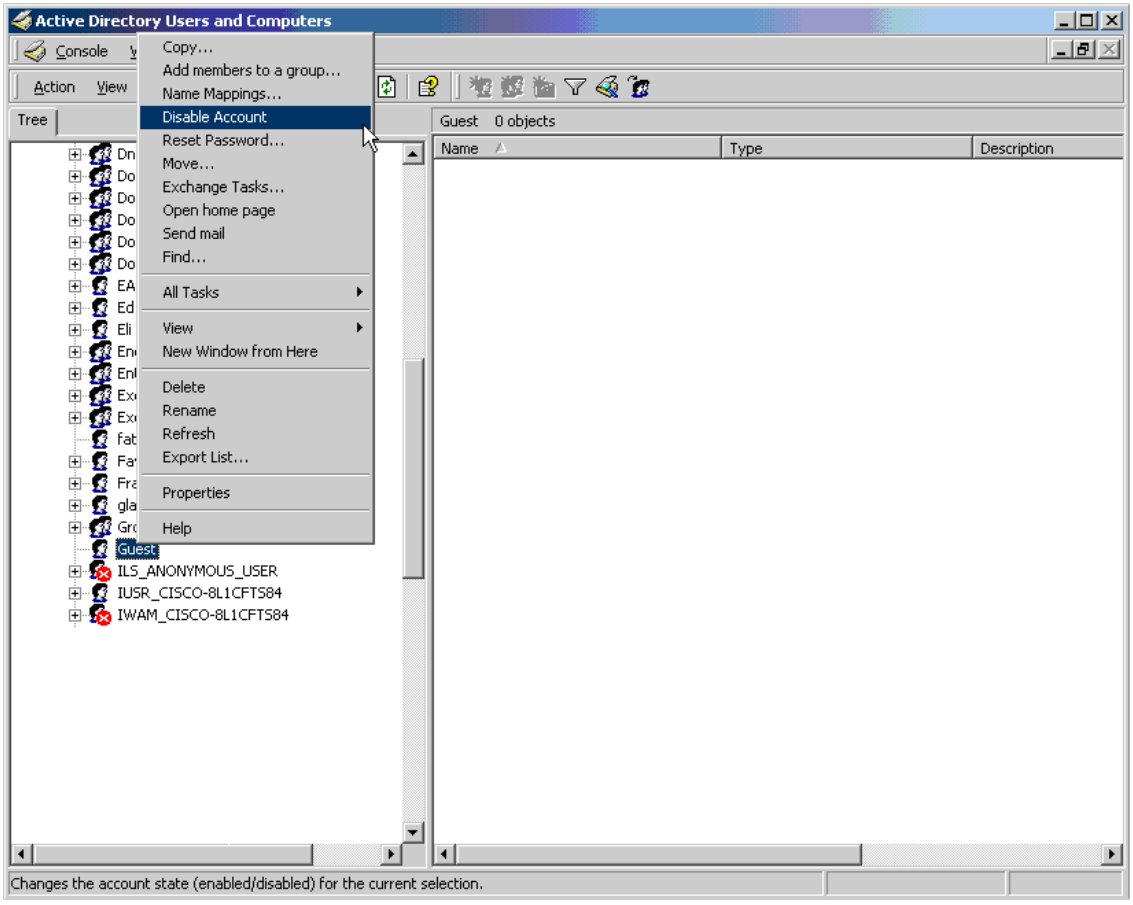
要覆盖来自 AAA 服务器的 account-disabled 指示，请在 ASA 上的 tunnel-group general-attributes 配置模式下使用 **override-account-disable** 命令，并在 Active Directory 下执行以下步骤。

注　允许覆盖 account-disabled 是一项潜在安全风险。

步骤 1　选择 Start > Programs > Administrative Tools > Active Directory Users and Computers。

步骤 2　右键单击 Username > Properties > Account，然后从菜单中选择 Disable Account。

图 4-4　Active Directory — 覆盖已禁用帐户



即使 AAA 服务器提供 account-disabled 指示器，用户也应该能够成功登录。

使用 Active Directory 实施最小密码长度

要实施密码的最小长度，请在 ASA 上的 tunnel-group general-attributes 配置模式下指定 **password-management** 命令，并在 Active Directory 下执行以下步骤：

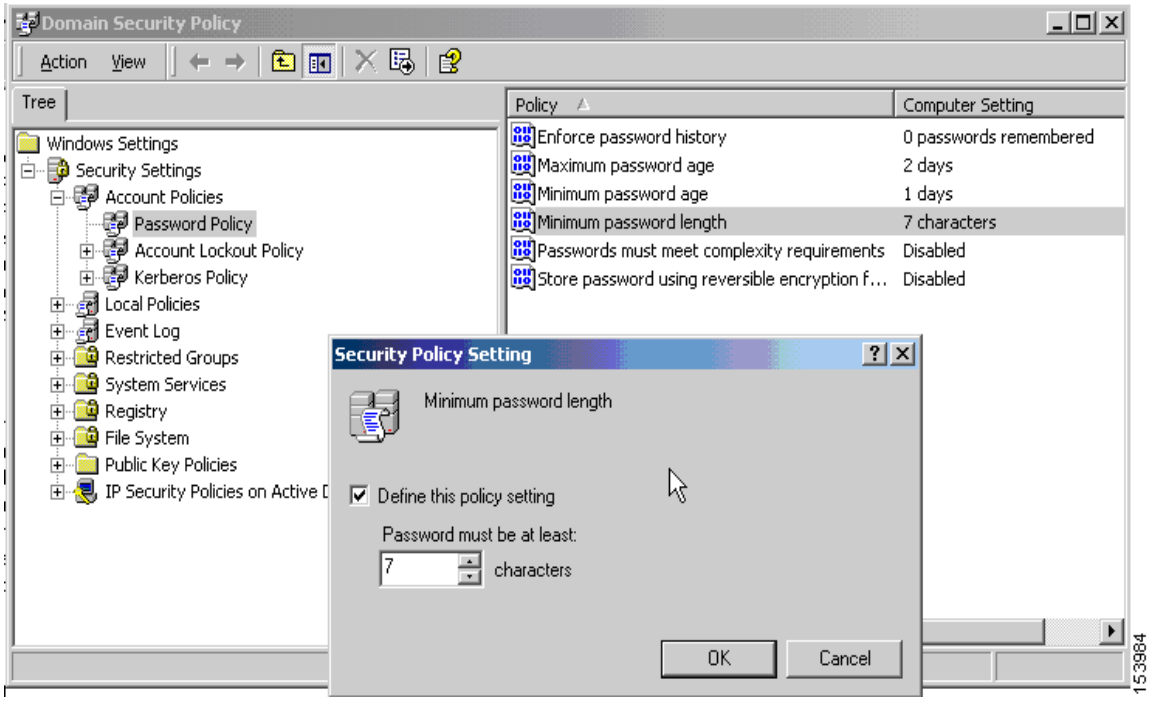
步骤 1　选择 Start > Programs > Administrative Tools > Domain Security Policy。

步骤 2　选择 Windows Settings > Security Settings > Account Policies > Password Policy。

步骤 3　双击 Minimum Password Length。系统将显示 Security Policy Setting 对话框。

步骤 4　选中 Define this policy setting 复选框并指定密码必须包含的最小字符数。

图 4-5　Active Directory — 最小密码长度



使用 Active Directory 实施密码复杂性

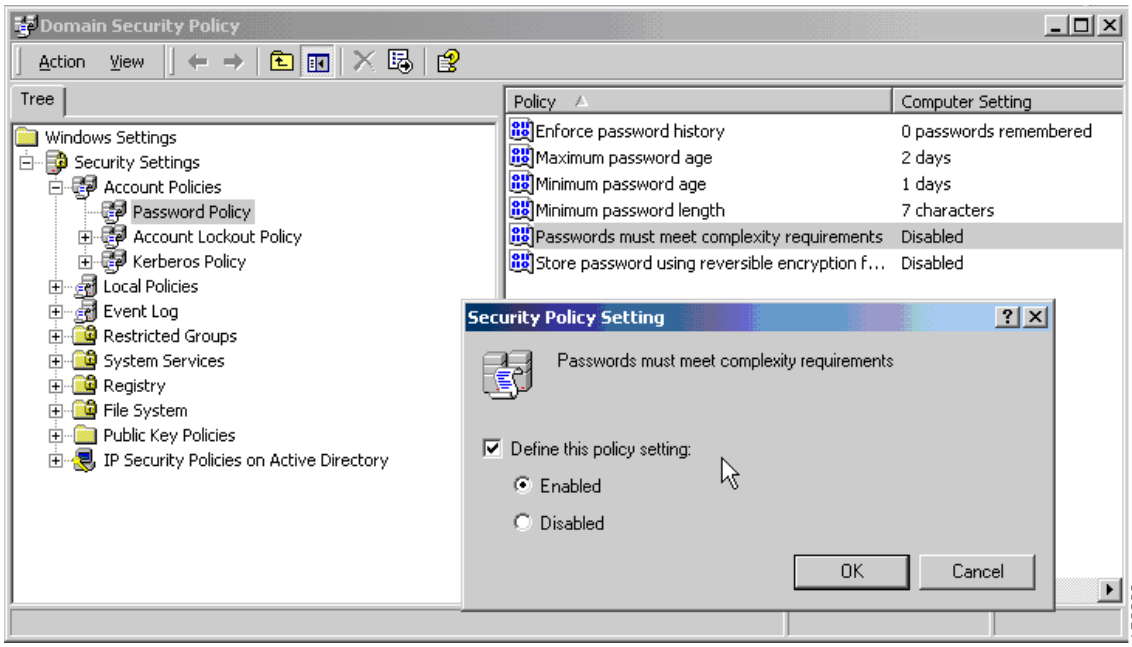
要实施复杂密码（例如，要求密码包含大写和小写字母、数字及特殊字符），请在 ASA 上的 tunnel-group general-attributes 配置模式下输入 **password-management** 命令，并在 Active Directory 下执行以下步骤：

步骤 1　选择 Start > Programs > Administrative Tools > Domain Security Policy。选择 Windows Settings > Security Settings > Account Policies > Password Policy。

步骤 2　双击 Password must meet complexity requirements 以打开 Security Policy Setting 对话框。

步骤 3　选中 Define this policy setting 复选框并选择 **Enable**。

图 4-6　Active Directory — 实施密码复杂性



仅当用户更改密码时，实施密码复杂性才会生效；例如，在配置 Enforce password change at next login 或 Password expires in *n* days 之后。在登录时，用户接收到要求输入新密码的提示，并且系统将仅接受复杂密码。

配置连接配置文件以对 AnyConnect 客户端进行 RADIUS/SDI 消息支持

本节描述相应的操作步骤来确保使用 RSA SecureID 软件令牌的 AnyConnect VPN 客户端能够正确响应通过 RADIUS 服务器（代理到 SDI 服务器）传递到客户端的用户提示。本节包含以下主题：

- AnyConnect 客户端和 RADIUS/SDI 服务器交互
- 配置安全设备以支持 RADIUS/SDI 消息

注　如果已配置双重身份验证功能，则仅在主身份验证服务器上支持 SDI 身份验证。

AnyConnect 客户端和 RADIUS/SDI 服务器交互

当远程用户通过 AnyConnect VPN 客户端连接到 ASA 并尝试使用 RSA SecurID 令牌进行身份验证时， ASA 与 RADIUS 服务器进行通信，后者反过来与 SDI 服务器就身份验证进行通信。

在身份验证期间，RADIUS 服务器向 ASA 呈现访问质询消息。在这些质询消息中是包含来自 SDI 服务器的应答消息文本。 ASA 直接与 SDI 服务器进行通信时和通过 RADIUS 代理进行通信时的消息文本不同。因此，为显示为 AnyConnect 客户端的本机 SDI 服务器， ASA 必须解释来自 RADIUS 服务器的消息。

此外，由于 SDI 消息在 SDI 服务器上可配置，因此 ASA 上的消息文本必须与 SDI 服务器上的消息文本匹配 （全部或部分）。否则，向远程客户端用户显示的提示可能不适用于身份验证期间所需的操作。 AnyConnect 客户端可能无法响应，并且身份验证可能会失败。

第 4-32 页上的配置安全设备以支持 RADIUS/SDI 消息描述如何配置 ASA 以确保在客户端和 SDI 服务器之间成功进行身份验证。

配置安全设备以支持 RADIUS/SDI 消息

要配置 ASA 以解释特定于 SDI 的 RADIUS 应答消息并提示 AnyConnect 用户执行相应的操作，请执行以下步骤：

步骤 1　在 tunnel-group webvpn 配置模式下使用 **proxy-auth sdi** 命令将连接配置文件 （隧道组）配置为通过模拟与 SDI 服务器的直接通信的方式转发 RADIUS 应答消息。向 SDI 服务器进行身份验证的用户必须通过此连接配置文件进行连接。

例如：

```
hostname(config)# tunnel-group sales webvpn attributes
hostname(tunnel-group-webvpn)# proxy-auth sdi
```

步骤 2　在 tunnel-group webvpn 配置模式下使用 **proxy-auth_map sdi** 命令将 ASA 上的 RADIUS 应答消息文本配置为与 RADIUS 服务器发送的消息文本匹配 （全部或部分）。

ASA 使用的默认消息文本是思科安全访问控制服务器 (ACS) 使用的默认消息文本。如果使用的是思科安全 ACS，并且其使用的是默认消息文本，则无需配置 ASA 上的消息文本。否则，请使用 **proxy-auth_map sdi** 命令确保消息文本匹配。

表 4-2 显示消息代码、默认 RADIUS 应答消息文本和各消息的功能。由于安全设备按照字符串在表中的显示顺序对其进行搜索，因此必须确保用于消息文本的字符串不是其他字符串的子集。

例如，对于 new-pin-sup 和 next-ccode-and-reauth，“new PIN”均是默认消息文本的子集。如果将 new-pin-sup 配置为“new PIN”，则在安全设备从 RADIUS 服务器接收到“new PIN with the next card code”时，它会将文本与 new-pin-sup 代码而非 next-ccode-and-reauth 代码匹配。

表 4-2　SDI 操作代码、默认消息文本和消息功能

消息代码	默认 RADIUS 应答消息文本	功能
next-code	Enter Next PASSCODE	指示用户必须输入不含 PIN 的 NEXT 令牌代码。
new-pin-sup	Please remember your new PIN	指示是否已提供新的系统 PIN 并为用户显示该 PIN。
new-pin-meth	Do you want to enter your own pin	来自用户的请求，表明要使用哪种新的 PIN 方法创建新的 PIN。
new-pin-req	Enter your new Alpha-Numerical PIN	指示用户生成的 PIN 并请求用户输入 PIN。
new-pin-reenter	Reenter PIN:	供 ASA 在内部使用以确认用户提供的 PIN。客户端确认 PIN 而不提示用户。
new-pin-sys-ok	New PIN Accepted	指示已接受用户提供的 PIN。
next-ccode-and-reauth	new PIN with the next card code	遵循 PIN 操作并指示用户必须等待下一个令牌代码且输入新的 PIN 和下一个令牌代码才能进行身份验证。
ready-for-sys-pin	ACCEPT A SYSTEM GENERATED PIN	供 ASA 在内部使用以指示用户准备好使用系统生成的 PIN。

以下示例进入 aaa-server-host 模式并更改 RADIUS 应答消息 new-pin-sup 的文本：

```
hostname(config)# aaa-server radius_sales host 10.10.10.1
hostname(config-aaa-server-host)# proxy-auth_map sdi new-pin-sup  “This is your new PIN”
```

组策略

本节描述组策略及其配置方式。

组策略是在设备上以内部方式 （本地）存储或在 RADIUS 服务器上以外部方式存储的 IPsec 连接的面向用户的属性 / 值对的集合。连接配置文件使用组策略在建立隧道后设置用户连接的条款。通过组策略可将整个属性集应用于用户或用户组，而不必为每个用户单独指定每个属性。

在全局配置模式下输入 **group-policy** 命令以向用户分配组策略或修改特定用户的组策略。

ASA 包含默认组策略。除默认组策略 （可以修改但不能删除）以外，您还可以创建特定于您环境的一个或多个组策略。

可以配置内部和外部组策略。内部组在 ASA 的内部数据库上进行配置。外部组在外部身份验证服务器 （如 RADIUS）上进行配置。组策略包含以下属性：

- 身份
- 服务器定义
- 客户端防火墙设置
- 隧道协议
- IPsec 设置
- 硬件客户端设置
- 过滤器
- 客户端配置设置
- 连接设置

默认组策略

ASA 提供默认组策略。您可以修改此默认组策略，但是无法将其删除。名为 DfltGrpPolicy 的默认组策略始终存在于 ASA 上，但是除非将 ASA 配置为使用此组策略，否则其不会生效。当配置其他组策略时，没有显式指定的任何属性都从默认组策略获取其值。如要查看默认组策略，请输入以下命令：

```
hostname(config)# show running-config all group-policy DfltGrpPolicy
hostname(config)#
```

如要配置默认组策略，请输入以下命令：

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

注　默认组策略始终为 internal。尽管实际上命令语法为 hostname(config)# group-policy DfltGrpPolicy {internal | external}，但是无法将其类型更改为 external。

如要更改默认组策略的任何属性，请使用 **group-policy attributes** 命令进入 attributes 模式，然后指定命令更改要修改的任意属性：

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

注　attributes 模式仅适用于内部组策略。

ASA 提供的默认组策略 DfltGrpPolicy 如下：

```
hostname# show run all group-policy DfltGrpPolicy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
 dns-server value 10.10.10.1.1
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
 password-storage disable
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 ipsec-udp disable
 ipsec-udp-port 10000
 split-tunnel-policy tunnelall
 ipv6-split-tunnel-policy tunnelall
 split-tunnel-network-list none
 default-domain value cisco.com
 split-dns none
 split-tunnel-all-dns disable
 intercept-dhcp 255.255.255.255 disable
 secure-unit-authentication disable
 user-authentication disable
 user-authentication-idle-timeout 30
 ip-phone-bypass disable
 client-bypass-protocol disable
 gateway-fqdn none
 leap-bypass disable
 nem disable
 backup-servers keep-client-config
 msie-proxy server none
 msie-proxy method no-modify
 msie-proxy except-list none
 msie-proxy local-bypass disable
 msie-proxy pac-url none
 msie-proxy lockdown enable
 vlan none
 nac-settings none
 address-pools none
 ipv6-address-pools none
 smartcard-removal-disconnect enable
 scep-forwarding-url none
 client-firewall none
 client-access-rule none
 webvpn
```

```
  url-list none
  filter none
  homepage none
  html-content-filter none
  port-forward name Application Access
  port-forward disable
  http-proxy disable
  sso-server none
  anyconnect ssl dtls enable
  anyconnect mtu 1406
  anyconnect firewall-rule client-interface private none
  anyconnect firewall-rule client-interface public none
  anyconnect keep-installer installed
  anyconnect ssl keepalive 20
  anyconnect ssl rekey time none
  anyconnect ssl rekey method none
  anyconnect dpd-interval client 30
  anyconnect dpd-interval gateway 30
  anyconnect ssl compression none
  anyconnect dtls compression lzs
  anyconnect modules none
  anyconnect profiles none
  anyconnect ask none
  customization none
  keep-alive-ignore 4
  http-comp gzip
  download-max-size 2147483647
  upload-max-size 2147483647
  post-max-size 2147483647
  user-storage none
  storage-objects value cookies,credentials
  storage-key none
  hidden-shares none
  smart-tunnel disable
  activex-relay enable
  unix-auth-uid 65534
  unix-auth-gid 65534
  file-entry enable
  file-browsing enable
  url-entry enable
  deny-message value Login was successful, but because certain criteria have not been met
or due to some specific group policy, you do not have permission to use any of the VPN
features.Contact your IT administrator for more information
  smart-tunnel auto-signon disable
  anyconnect ssl df-bit-ignore disable
  anyconnect routing-filtering-ignore disable
  smart-tunnel tunnel-policy tunnelall
  always-on-vpn profile-setting
```

您可以修改默认组策略，也可以创建特定于您的环境的一个或多个组策略。

配置组策略

组策略可以应用于任何类型的隧道。在每个案例中，如果没有显式定义参数，则组从默认组策略获取值。

您可以在单情景模式或多情景模式下执行这些配置任务：

注　多情景模式仅适用于 IKEv2 和 IKEv1 站点间连接，不适用于 AnyConnect、无客户端 SSL VPN，传统 Cisco VPN 客户端、Apple 本机 VPN 客户端、Microsoft 本机 VPN 客户端或 cTCP for IKEv1 IPsec。

配置外部组策略

外部组策略从指定的外部服务器获取其属性值。对于外部组策略，必须标识 ASA 可查询参数的 AAA 服务器组，并指定在从外部 AAA 服务器组检索属性时要使用的密码。如果使用的是外部身份验证服务器，并且如果外部组策略属性与计划进行身份验证的用户存在于同一 RADIUS 服务器中，则必须确保其之间没有名称重复。

注　ASA 上的外部组名引用 RADIUS 服务器上的用户名。换句话说，如果在 ASA 上配置外部组 X，则 RADIUS 服务器将查询视为用户 X 的身份验证请求。因此，外部组实际只是 RADIUS 服务器上对于 ASA 有特殊意义的用户帐户。如果外部组属性与计划进行身份验证用户存在于同一 RADIUS 服务器中，则其之间不得有名称重复。

ASA 在外部 LDAP 或 RADIUS 服务器上支持用户授权。在配置 ASA 以使用外部服务器之前，必须使用正确的 ASA 授权属性来配置服务器，并且从这些属性的子集向个人用户分配特定权限。按照附录 12，“用于授权和身份验证的外部服务器”中的说明配置外部服务器。

要配置外部组策略，请执行以下步骤来指定组策略的名称和类型以及服务器组名和密码：

```
hostname(config)# group-policy group_policy_name type server-group server_group_name
password server_password
hostname(config)#
```

注　对于外部组策略， RADIUS 是唯一受支持的 AAA 服务器类型。

例如，以下命令创建名为 ExtGroup 的外部组策略，该组策略从名为 ExtRAD 的外部 RADIUS 服务器获取其属性并指定在检索属性时要使用的的密码为 newpassword：

```
hostname(config)# group-policy ExtGroup external server-group ExtRAD password newpassword
hostname(config)#
```

注　可以配置多个特定于供应商的属性 (VSA)，如附录 12，“用于授权和身份验证的外部服务器”中所述。如果 RADIUS 服务器配置为返回类属性 (#25)，则 ASA 使用该属性对组名进行身份验证。在 RADIUS 服务器上，该属性必须格式化为：OU=*groupname*；其中 *groupname* 与 ASA 上配置的组名 （例如 OU=Finance）相同。

创建内部组策略

如要配置内部组策略，请进入配置模式，使用组策略命令，指定名称以及组策略的 **internal** 类型：

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

例如，以下命令创建名为 GroupPolicy1 的内部组策略：

```
hostname(config)# group-policy GroupPolicy1 internal
hostname(config)#
```

注　创建组策略后，无法更改其名称。

可以通过复制预先存在的组策略的值来配置内部组策略的属性，方法是附加关键字 **from** 并指定现有策略的名称：

```
hostname(config)# group-policy group_policy_name internal from group_policy_name
hostname(config-group-policy)#
```

例如，以下命令通过复制 GroupPolicy1 的属性来创建名为 GroupPolicy2 的内部组策略：

```
hostname(config)# group-policy GroupPolicy2 internal from GroupPolicy1
hostname(config-group-policy)#
```

配置常规内部组策略属性

组策略名称

创建内部组策略时会选择组策略名称。一旦创建组策略，便无法更改其名称。有关详细信息，请参阅第 4-36 页上的创建内部组策略。

配置组策略横幅消息

指定要显示的横幅或欢迎消息。默认为无横幅。当远程客户端连接时，在其之上会显示您指定的消息。要指定横幅，请在 group-policy 配置模式下指定 **banner** 命令。横幅文本长度最多可以为 510 个字符。输入 “\n” 序列以插入回车符。

注　条幅中包含的回车符和换行符计作两个字符。

如要删除条幅，请输入此命令的 **no** 形式。请注意，使用 **no** 版本的该命令会删除组策略的所有条幅。

一个组策略可以从另一个组策略继承该值。要防止继承值，请输入 **none** 关键字而不是指定条幅字符串的值，如下所示：

```
hostname(config-group-policy)# banner {value banner_string | none}
```

以下示例显示如何为名为 FirstGroup 的组策略创建条幅：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems ASA 9.0.
```

指定远程访问连接的地址池

当远程访问客户端连接到 ASA 时， ASA 可以根据为连接指定的组策略来为客户端分配 IPv4 或 IPv6 地址。

可以指定包含最多六个用于本地地址分配的本地地址池的列表。池的指定顺序至关重要。 ASA 按照池在此命令中的显示顺序从这些池分配地址。

向内部组策略分配 IPv4 地址池

先决条件

创建 IPv4 地址池。请参阅第 5 章，“VPN 的 IP 地址”。

详细步骤

	命令	目的

步骤 1	`group-policy value attributes`
	
	示例：
	`hostname> en`
	`hostname# config t`
	`hostname(config)# group-policy FirstGroup attributes`
	`hostname(config-group-policy)#`
		进入组策略配置模式。

步骤 2	**address-pools value** *pool-name1 pool-name2 pool-name6*
	
	示例：
	`asa4(config-group-policy)# address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3`
	`asa4(config-group-policy)#`
		向 FirstGroup 组策略分配名为 ipv4-pool1、ipv4-pool2 和 ipv4pool3 的地址池。
		允许为组策略指定最多 6 个地址池。

步骤 3	（可选）
	no address-pools value pool-name1 pool-name2 pool-name6
	
	示例：
	`hostname(config-group-policy)# no address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3`
	`hostname(config-group-policy)#`
		使用 **no address-pools value pool-name** 命令从组策略配置中移除地址池，并返回地址池设置来从其他源（例如 DefltGroupPolicy）继承地址池信息。

步骤 4	（可选）
	address-pools none
	
	示例：
	`hostname(config-group-policy)# address-pools none`
	`hostname(config-group-policy)#`
		address-pools none 命令禁止从其他策略源（例如 DefltGrpPolicy）继承此属性：

步骤 5	（可选）
	no address-pools none
	
	示例：
	`hostname(config-group-policy)# no address-pools none`
	`hostname(config-group-policy)#`
		no address pools none 命令从组策略中移除 **address-pools none** 命令，从而还原默认值，即允许继承。

向内部组策略分配 IPv6 地址池

先决条件

创建 IPv6 地址池。请参阅第 5 章，“VPN 的 IP 地址”。

详细步骤

	命令	目的

步骤 1	`group-policy value attributes`
	
	示例：
	`hostname> en`
	`hostname# config t`
	`hostname(config)# group-policy FirstGroup attributes`
	`hostname(config-group-policy)#`
		进入组策略配置模式。

步骤 2	**ipv6-address-pools value** *pool-name1 pool-name2 pool-name6* **示例：** hostname(config-group-policy)# **ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3** hostname(config-group-policy)#	向 FirstGroup 组策略分配名为 ipv6-pool 的地址池。 可以向组策略分配最多六个 ipv6 地址池。 此示例显示 ipv6-pool1、 ipv6-pool2 和 ipv6-pool3 分配到 FirstGroup 组策略。

步骤 3	（可选）
	no ipv6-address-pools value pool-name1 pool-name2 pool-name6
	
	示例：
	`hostname(config-group-policy)# no ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3`
	`hostname(config-group-policy)#`
		使用 **no ipv6-address-pools value pool-name** 命令从组策略配置中移除地址池，并返回地址池设置来从其他源 （例如 DfltGroupPolicy）继承地址池信息。

步骤 4	（可选）
	ipv6-address-pools none
	
	示例：
	`hostname(config-group-policy)# ipv6-address-pools none`
	`hostname(config-group-policy)#`
		ipv6-address-pools none 命令禁止从其他策略源 （例如 DfltGrpPolicy）继承此属性：

步骤 5	（可选）
	no ipv6-address-pools none
	
	示例：
	`hostname(config-group-policy)# no ipv6-address-pools none`
	`hostname(config-group-policy)#`
		no ipv6-address pools none 命令从组策略中移除 **ipv6-address-pools none** 命令，从而还原默认值，即允许继承。

指定组策略的隧道协议

通过在 group-policy 配置模式下输入 **vpn-tunnel-protocol {ikev1 | ikev2 | l2tp-ipsec | ssl-client | ssl-clientless}** 命令来指定此组策略的 VPN 隧道类型。

默认值是继承默认组策略的属性。要从运行配置中移除属性，请输入此命令的 **no** 形式。

此命令的参数值如下：

- **ikev1** — 在两个对等体 （Cisco VPN 客户端或其他安全网关）之间协商 IPsec IKEv1 隧道。创建监管身份验证、加密、封装和密钥管理的安全关联。
- **ikev2** — 在两个对等体 （AnyConnect 安全移动客户端或其他安全网关）之间协商 IPsec IKEv2 隧道。创建监管身份验证、加密、封装和密钥管理的安全关联。
- **l2tp-ipsec** — 为 L2TP 连接协商 IPsec 隧道。
- **ssl-client** — 使用 TLS 或 DTLS 与 AnyConnect 安全移动客户端协商 SSL 隧道。
- **ssl-clientless** — 通过已启用 HTTPS 的 Web 浏览器向远程用户提供 VPN 服务，并且无需客户端。

输入此命令以配置一个或多个隧道模式。必须配置至少一个隧道模式以使用户通过 VPN 隧道进行连接。

以下示例显示如何为名为 FirstGroup 的组策略配置 IPsec IKEv1 隧道模式：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev1
hostname(config-group-policy)#
```

为远程访问指定 VLAN 或对组策略应用统一访问控制规则

过滤器包含根据诸如源地址、目标地址和协议之类的条件来确定允许还是拒绝通过 ASA 的隧道化数据包的规则。可以为组策略指定 IPv4 或 IPv6 统一访问控制列表，或者允许其继承默认组策略中指定的 ACL。

选择以下选项之一来为远程访问指定出口 VLAN （也称为 “VLAN 映射”），或者指定 ACL 以过滤流量：

- 在 group-policy 配置模式下输入以下命令来为分配到此组策略或分配到继承此组策略的组策略的远程访问 VPN 会话指定出口 VLAN：

  ```
  hostname(config-group-policy)# [no] vlan {vlan_id |none}
  ```

  no vlan 从组策略中移除 *vlan_id*。组策略从默认组策略继承 vlan 值。

  none 从组策略中移除 *vlan_id* 并对此组策略禁用 VLAN 映射。组策略不从默认组策略继承 vlan 值。

  vlan_id 是要分配给使用此组策略的远程访问 VPN 会话的 VLAN 的编号 （十进制格式）。必须按照常规操作配置指南中“配置 VLAN 子接口和 802.1Q 中继”中的说明在此 ASA 上配置 VLAN。

  注　出口 VLAN 功能适用于 HTTP 连接，但不适用于 FTP 和 CIFS。

- 在组策略模式下使用 **vpn-filter** 命令指定要应用于 VPN 会话的访问控制规则 (ACL) 的名称。使用 vpn-filter 命令指定 IPv4 或 IPv6 ACL。

注　在以前的版本中，如果 vpn-filter 未指定 IPv6 条目，则可以使用已弃用的 ipv6-vpn-filter 命令来指定 IPv6 ACL。截至 ASA 9.1(4)，已禁用 ipv6-vpn-filter，并且必须使用 vpn-filter 命令指定 IPv6 ACL 条目必须。如果设置 ipv6-vpn-filter，则将终止 VPN 连接。

注　您也可以在用户名模式下配置此属性，在此情况下用户名下配置的值会取代组策略值。

```
hostname(config-group-policy)# vpn-filter {value ACL name | none}
hostname(config-group-policy)#
```

可将 ACL 配置为允许或拒绝此组策略的各种类型的流量。然后，输入 **vpn-filter** 命令以应用这些 ACL。

要移除 ACL，从而包含通过输入 **vpn-filter none** 命令创建的空值，请输入此命令的 **no** 形式。**no** 选项允许从其他组策略继承值。

一个组策略可以从另一个组策略继承该值。要防止继承值，请输入 **none** 关键字而不是指定 ACL 名称。 **none** 关键字指示没有 ACL 并设置空值，从而不允许使用 ACL。

以下示例显示如何为名为 FirstGroup 的组策略设置调用名为 acl_vpn 的 ACL 的过滤器：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter acl_vpn
hostname(config-group-policy)#
```

vpn-filter 命令在其退出隧道后应用于解密后流量，在其进入隧道之前应用于解密前流量。用于 vpn-filter 的 ACL 不应也用于接口访问组。当 **vpn-filter** 命令应用于监管远程访问 VPN 客户端连接的组策略时，应使用客户端分配的 IP 地址 （位于 ACL 的 **src_ip** 位置中）和本地网络 （位于 ACL 的 **dest_ip** 位置中）配置 ACL。

当 **vpn-filter** 命令应用于监管 LAN 对 LAN VPN 连接的组策略时，应使用远程网络（位于 ACL 的 **src_ip** 位置中）和本地网络 （位于 ACL 的 **dest_ip** 位置中）配置 ACL。

构造与 vpn-filter 功能配合使用的 ACL 时应谨慎。构造 ACL 时考虑了解密后流量。但是，ACL 还应用于相反方向的流量。对于以隧道为目标的此加密前流量，在构造 ACL 时 **src_ip** 和 **dest_ip** 位置进行了交换。

在以下示例中， vpn-filter 与远程访问 VPN 客户端配合使用。
此示例假设客户端分配的 IP 地址为 10.10.10.1/24，并且本地网络为 192.168.1.0/24。

以下 ACE 将允许远程访问 VPN 客户端通过 telnet 连接到本地网络：

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255
192.168.1.0 255.255.255.0 eq 23
```

以下 ACE 将允许本地网络通过 telnet 连接到远程访问客户端：

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq
23 192.168.1.0 255.255.255.0
```

注　ACE **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23** 允许本地网络在使用源端口 23 的情况下在任意 TCP 端口上启动与远程访问客户端的连接。ACE **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq 23 192.168.1.0 255.255.255.0** 允许远程访问客户端在使用源端口 23 的情况下在任意 TCP 端口上启动与本地网络的连接。

在下一个示例中， vpn-filter 与 LAN 对 LAN VPN 连接配合使用。此示例假设远程网络为 10.0.0.0/24，并且本地网络为 192.168.1.0/24。
以下 ACE 将允许远程网络通过 telnet 连接到本地网络：

```
hostname(config-group-policy)# access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0
192.168.1.0 255.255.255.0 eq 23
```

以下 ACE 将允许本地网络通过 telnet 连接到远程网络：

```
hostname(config-group-policy)# access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 eq 23
192.168.1.0 255.255.255.0
```

注 ACE **access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 eq 23** 允许本地网络在使用源端口 23 的情况下在任意 TCP 端口上启动与远程网络的连接。 ACE **access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0** 允许远程网络在使用源端口 23 的情况下在任意 TCP 端口上启动与本地网络的连接。

指定组策略的 NAC 策略

此命令选择要应用于此组策略的网络准入控制策略的名称。可以向每个组策略分配可选 NAC 策略。默认值为 --None--。

先决条件

创建 NAC 策略。请参阅第 7-1 页上的网络准入控制。

详细步骤

	命令	目的

步骤 1	`group-policy value attributes`
	
	示例：
	`hostname> en`
	`hostname# config t`
	`hostname(config)# group-policy FirstGroup attributes`
	`hostname(config-group-policy)#`
		进入组策略配置模式。

步骤 2	**nac-settings value** *nac-policy-name* **示例：** hostname(config-group-policy)# **nac-settings value nac-policy-1** hostname(config-group-policy)#	向 FirstGroup 组策略分配名为 nac-policy-1 的组策略。

指定组策略的 VPN 访问时间

先决条件

创建时间范围。请参阅常规操作配置指南中的 “配置时间范围”。

详细步骤

	命令	目的

步骤 1	`group-policy value attributes`
	
	示例：
	`hostname> en`
	`hostname# config t`
	`hostname(config)# group-policy FirstGroup attributes`
	`hostname(config-group-policy)#`
		进入组策略配置模式。

步骤 2	`hostname(config-group-policy)# vpn-access-hours value {time-range-name | none}`
	
	示例：
	`hostname(config-group-policy)# vpn-access-hours value business-hours`
	hostname(config-group-policy)#
		可以通过在 group-policy 配置模式下使用 **vpn-access-hours** 命令将时间范围策略与组策略关联来设置 VPN 访问时间。
		此命令向名为 FirstGroup 的组策略分配名为 business-hours 的 VPN 访问时间范围。
		组策略可以从默认或指定的组策略继承时间范围值。要防止此继承，请在此命令中输入 **none** 关键字而不是时间范围的名称。此关键字将 VPN 访问时间设置为空值，即允许 no time-range 策略。

为组策略指定同时 VPN 登录

在 group-policy 配置模式下使用 **vpn-simultaneous-logins** 命令指定对任何用户允许的同时登录数。

```
hostname(config-group-policy)# vpn-simultaneous-logins integer
```

默认值为 3。范围是介于 0 至 2147483647 之间的整数。一个组策略可以从另一个组策略继承该值。输入 0 以禁用登录并阻止用户访问。以下示例显示如何对名为 FirstGroup 的组策略允许最多 4 个同时登录：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-simultaneous-logins 4
hostname(config-group-policy)#
```

注　尽管同时登录数的最大限制非常大，但是允许若干同时登录可能会危害安全并影响性能。

即使已使用同一用户名建立“新”会话，停滞的 AnyConnect 会话、IPsec 客户端会话或无客户端会话 （异常终止的会话）仍然可能保留在会话数据库中。

如果 vpn-simultaneous-logins 的值为 1，并且同一用户在异常终止后再次登录，则会从数据库中移除停滞的会话并建立新会话。但是，如果现有会话仍然是活动连接并且同一用户再次登录 （可能从其他 PC），则会注销且从数据库中移除第一个会话并建立新会话。

如果同时登录数的值大于 1，则在您已达到该最大数并尝试再次登录时，会注销具有最长空闲时间的会话。如果所有当前会话都已空闲等长的时间，则会注销最旧的会话。此操作释放会话并允许新登录。

将访问限于特定连接配置文件

在 group-policy 配置模式下使用 **group-lock** 命令指定是否限制远程用户仅通过连接配置文件进行访问。

```
hostname(config-group-policy)# group-lock {value tunnel-grp-name | none}
hostname(config-group-policy)# no group-lock
hostname(config-group-policy)#
```

tunnel-grp-name 变量指定 ASA 为使用户进行连接所需的现有连接配置文件的名称。组锁定通过检查在 VPN 客户端中配置的组是否与用户分配到的连接配置文件相同来限制用户。如果不相同，则 ASA 会阻止用户进行连接。如果不配置组锁定，则 ASA 在不考虑分配的组的情况下对用户进行身份验证。默认情况下会禁用组锁定。

要从运行配置中移除 **group-lock** 属性，请输入此命令的 **no** 形式。此选项允许从其他组策略继承值。

要禁用组锁定，请输入带有 **none** 关键字的 **group-lock** 命令。 none 关键字将 group-lock 设置为空值，从而允许 no group-lock 限制。它还防止从默认或指定的组策略继承 group-lock 值

在组策略中指定最长 VPN 连接时间

步骤 1　在 group-policy 配置模式或 username 配置模式下使用 **vpn-session-timeout** 命令配置 VPN 连接的最长时间。

```
hostname(config-group-policy)# vpn-session-timeout {minutes | none}
hostname(config-group-policy)#
```

最短时间为 1 分钟，最长时间为 35791394 分钟。没有默认值。此时间段结束时，ASA 终止连接。

一个组策略可以从另一个组策略继承该值。要防止继承值，请输入 **none** 关键字而不是使用此命令指定分钟数。指定 **none** 关键字将允许会话超时期不受限制并使用空值来设置会话超时，即不允许会话超时。

以下示例显示如何为名为 FirstGroup 的组策略设置 180 分钟的 VPN 会话超时：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

步骤 2　使用 **vpn-session-timeout alert-interval** {minutes | none} 命令配置向用户显示 session-timeout 警报消息时的时间。此警报消息告诉用户在其 VPN 会话自动断开连接之前剩余的分钟数。

以下示例显示如何设置 **vpn-session-timeout alert-interval**，以便在用户的 VPN 会话断开连接之前 20 分钟对其进行通知。可以指定范围为 1 至 30 分钟。

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

none 参数指示用户将不会接收到警报。

使用该命令的 no 形式可指示将从默认组策略继承 VPN 会话超时 alert-interval 属性：

```
no vpn-session-timeout alert-interval
```

指定组策略的 VPN 会话空闲超时

步骤 1　通过在 group-policy 配置模式或 username 配置模式下输入 **vpn-idle-timeout** 命令来配置用户超时期：

```
hostname(config-group-policy)# vpn-idle-timeout {minutes | none}
hostname(config-group-policy)#
```

AnyConnect (SSL IPsec/IKEv2)：从以下命令使用全局 WebVPN default-idle-timeout 值 （秒）：
hostname(config-webvpn)# default-idle-timeout

WebVPN **default-idle-timeout** 命令中该值的范围为 60 至 86400 秒；默认全局 WebVPN 空闲超时（以秒为单位） - 默认值为 1800 秒 （30 分钟）。

注　对于所有 AnyConnect 连接， ASA 需要非零空闲超时值。

对于 WebVPN 用户，仅当在组策略 / 用户名属性中设置了 vpn-idle-timeout none 时，才会实施 **default-idle-timeout** 值。

站点间 （IKEv1 和 IKEv2）和 IKEv1 远程访问：禁用超时并允许无限制的超时期。

以下示例显示如何为名为 FirstGroup 的组策略设置 15 分钟的 VPN 空闲超时：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

步骤 2　使用 **vpn-idle-timeout alert-interval {minutes | none}** 命令配置向用户显示 idle-timeout 警报消息时的时间。此警报消息告诉用户在其 VPN 会话因不活动而断开连接之前剩余的分钟数。

以下示例显示如何设置 vpn-idle-timeout alert-interval，以便在用户的 VPN 会话因不活动而断开连接之前 20 分钟对其进行通知。可以指定范围为 1 至 30 分钟。

```
hostname(config-webvpn)# vpn-idle-timeout alert-interval 20
```

none 参数指示用户将不会接收到警报。

使用该命令的 no 形式可指示将从默认组策略继承 VPN 空闲超时 alert-interval 属性：

```
no vpn-idle-timeout alert-interval
```

为组策略配置 WINS 和 DNS 服务器

可以指定主要和次要 WINS 服务器和 DNS 服务器。在每种情况下的默认值为 none。要指定这些服务器，请执行以下步骤：

步骤 1　指定主要和次要 WINS 服务器：

```
hostname(config-group-policy)# wins-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

指定的第一个 IP 地址是主要 WINS 服务器的 IP 地址。第二个（可选）IP 地址是次要 WINS 服务器的 IP 地址。指定 **none** 关键字而非 IP 地址会将 WINS 服务器设置为空值，这将不允许使用 WINS 服务器并防止从默认或指定的组策略继承值。

每次输入 **wins-server** 命令后，会覆盖现有设置。例如，如果配置 WINS 服务器 x.x.x.x，然后配置 WINS 服务器 y.y.y.y，则第二个命令会覆盖第一个命令，并且 y.y.y.y 成为唯一的 WINS 服务器。对于多台服务器情况也如此。要添加 WINS 服务器而不是覆盖以前配置的服务器，请在输入此命令时包含所有 WINS 服务器的 IP 地址。

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

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

步骤 2　指定主要和次要 DNS 服务器：

```
hostname(config-group-policy)# dns-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

指定的第一个 IP 地址是主要 DNS 服务器的 IP 地址。第二个（可选）IP 地址是次要 DNS 服务器的 IP 地址。指定 **none** 关键字而非 IP 地址会将 DNS 服务器设置为空值，这将不允许使用 DNS 服务器并防止从默认或指定的组策略继承值。可以指定最多四个 DNS 服务器地址：最多两个 IPv4 地址和两个 IPv6 地址。

每次输入 **dns-server** 命令后，会覆盖现有设置。例如，如果配置 DNS 服务器 x.x.x.x，然后配置 DNS 服务器 y.y.y.y，则第二个命令会覆盖第一个命令，并且 y.y.y.y 成为唯一的 DNS 服务器。对于多台服务器情况也如此。要添加 DNS 服务器而不是覆盖以前配置的服务器，请在输入此命令时包含所有 DNS 服务器的 IP 地址。

以下示例显示如何为名为 FirstGroup 的组策略配置 IP 地址为 10.10.10.15、 10.10.10.30、2001:DB8::1 和 2001:DB8::2 的 DNS 服务器：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dns-server value 10.10.10.15 10.10.10.30 2001:DB8::1
2001:DB8::2
hostname(config-group-policy)#
```

步骤 3　如果在 **DeafultDNS DNS server group** 中未指定默认域名，则必须指定默认域。使用域名和顶级域，例如 **example.com**。

```
asa4(config)# group-policy FirstGroup attributes
asa4(config-group-policy)# default-domain value example.com
asa4(config-group-policy)#
```

步骤 4　配置 DHCP 网络范围：

```
hostname(config-group-policy)# dhcp-network-scope {ip_address | none}
hostname(config-group-policy)#
```

DHCP 范围指定 ASA DHCP 服务器应该用于向此组策略的用户分配地址的 IP 地址范围（即子网）。

以下示例显示如何为名为 FirstGroup 的组策略设置 IP 子网 10.10.85.0 （指定 10.10.85.0 至 10.10.85.255 的地址范围）：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.10.85.0
```

配置 AnyConnect 流量的拆分隧道

拆分隧道将一些 AnyConnect 网络流量定向通过 VPN 隧道 （加密），将另一些网络流量定向到 VPN 隧道外部 （未加密或 “无保护”）。

通过创建拆分隧道策略，为该策略配置访问控制列表，然后将拆分隧道策略添加到组策略，可以配置拆分隧道。当组策略发送到客户端时，该客户端将使用拆分隧道策略中的 ACL 来决定要将网络流量定向到的位置。

创建访问列表时：

- 可以在访问控制列表中同时指定 IPv4 和 IPv6 地址。
- 如果使用标准 ACL，则仅使用一个地址或网络。
- 如果使用扩展 ACL，则源网络是拆分隧道网络。目标网络会被忽略。
- 使用 any 或者使用拆分 - 包含 / 排除 0.0.0.0/0.0.0.0 或 ::/0 配置的访问列表将不会发送到客户端。要通过隧道发送所有流量，请在创建拆分隧道策略时指定 “tunnelall”。
- 仅当拆分隧道策略为 **excludespecified** 时，才会将地址 0.0.0.0/255.255.255.255 或 ::/128 发送到客户端。此配置指示客户端不要通过隧道传送以任意本地子网为目标的流量。
- AnyConnect 将流量传递到在拆分隧道策略中指定的所有站点**和**与 ASA 分配的 IP 地址属于同一子网的所有站点。例如，如果 ASA 分配的 IP 地址为 10.1.1.1 且掩码为 255.0.0.0，则无论拆分隧道策略如何，终端设备都会传递所有目标为 10.0.0.0/8 的流量。因此，请为正确引用预期本地子网的分配的 IP 地址使用网络掩码。

您还可以指定域列表来定向拆分隧道流量。客户端将流量定向到 split-dns 列表中的域，进而定向到 VPN，并且所有其他流量都处于无保护状态。

先决条件

- 必须使用 ACL 和 ACE 创建访问列表。
- 如果为 IPv4 网络创建一个拆分隧道策略并为 IPv6 网络创建另一个拆分隧道策略，则在 split-tunnel-network-list 中指定的网络列表同时用于两种协议。因此，网络列表应同时包含 IPv4 和 IPv6 流量的访问控制项 (ACE)。

设置拆分隧道策略

通过指定 IPv4 流量的拆分隧道策略来设置隧道流量的规则：

```
hostname(config-group-policy)# split-tunnel-policy {tunnelall | tunnelspecified |
excludespecified}
hostname(config-group-policy)# no split-tunnel-policy
```

通过指定 IPv6 流量的拆分隧道策略来设置隧道流量的规则：

```
hostname(config-group-policy)# ipv6-split-tunnel-policy {tunnelall | tunnelspecified |
excludespecified}
hostname(config-group-policy)# no ipv6-split-tunnel-policy
```

策略选项包括：

- **tunnelspecified** — 通过隧道在 Network List 中指定的网络上传入或传出所有流量。面向所有其他地址的数据在无保护情况下传播，并由远程用户的 Internet 服务提供商进行路由。

  对于 ASA V9.1.4 及更高版本，在指定包含列表时，还可以为包含范围内的子网指定排除列表。已排除的子网中的地址将不进行隧道传送，而包含列表的其余地址将进行隧道传送。排除列表中的网络将不通过隧道进行发送。可以使用拒绝条目指定排除列表，使用允许条目指定包含列表。

注　客户端将忽略排除列表中的并非包含列表的子集的网络。

- **excludespecified** — 不在 Network List 中指定的网络上通过隧道传入或传出流量。在所有其他地址上进出的流量通过隧道进行传送。在客户端上处于活动状态的 VPN 客户端配置文件必须启用本地 LAN 访问。
- **tunnelall** — 指定所有流量都通过隧道。此策略禁用拆分隧道。远程用户能够访问公司网络，但是其无法访问本地网络。这是默认选项。

注　拆分隧道是一项流量管理功能而非安全功能。为实现最佳安全性，建议不启用拆分隧道。

以下示例显示如何为 IPv4 和 IPv6 设置一个仅通过隧道传送名为 FirstGroup 的组策略的指定网络的拆分隧道策略：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
```

指定拆分隧道的网络列表

在拆分隧道中，网络列表确定通过隧道传播的网络流量内容。 AnyConnect 根据网络列表 （它是 ACL）制定拆分隧道决策。

操作步骤

```
hostname(config-group-policy)# split-tunnel-network-list {value access-list_name | none}
hostname(config-group-policy)# no split-tunnel-network-list value [access-list_name]
```

- **value** *access-list name* — 标识枚举要通过隧道传送或不通过隧道传送的网络的 ACL。 ACL 可以是包含同时指定 IPv4 和 IPv6 地址的 ACE 的统一 ACL。
- **none** — 指示拆分隧道没有网络列表， ASA 通过隧道传送所有流量。指定 **none** 关键字会使用空值来设置拆分隧道网络列表，从而不允许使用拆分隧道。它还防止从默认或指定的组策略继承默认拆分隧道网络列表。

要删除网络列表，请输入此命令的 **no** 形式。要删除所有拆分隧道网络列表，请输入不带参数的 **no split-tunnel-network-list** 命令。此命令删除所有已配置的网络列表，包括空列表 （如果通过输入 **none** 关键字进行了创建）。

当没有拆分隧道网络列表时，用户继承默认或指定的组策略中存在的任何网络列表。要防止用户继承此类网络列表，请输入 **split-tunnel-network-list none** 命令。

示例

以下示例显示如何创建名为 FirstList 的网络列表，并将其添加到名为 FirstGroup 的组策略。FistList 是排除列表，并且是作为该排除列表子集的包含列表：

```
hostname(config)# split-tunnel-policy tunnelspecified
hostname(config)# access-list FirstList deny ip 10.10.10.0 255.255.255.0 any
hostname(config)# access-list FirstList permit ip 10.0.0.0 255.0.0.0 any

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list value FirstList
```

以下示例显示如何创建名为 v6 的网络列表，并将 v6 拆分隧道策略添加到名为 GroupPolicy_ipv6-ikev2 的组策略。 v6 是排除列表，并且是作为该排除列表子集的包含列表：

```
hostname(config)# access-list v6 extended permit ip fd90:5000::/32 any6
hostname(config)# access-list v6 extended deny ip fd90:5000:3000:2880::/64 any6

hostname(config)# group-policy GroupPolicy_ipv6-ikev2 internal
hostname(config)# group-policy GroupPolicy_ipv6-ikev2 attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev2 ssl-client
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
hostname(config-group-policy)# split-tunnel-network-list value v6
```

验证拆分隧道配置

运行 **show runn group-policy attributes** 命令以验证配置。本示例显示管理员已同时设置 IPv4 和 IPv6 网络策略并对两种策略使用网络列表 （统一 ACL） **FirstList**。

```
hostname(config-group-policy)# show runn group-policy FirstGroup attributes
group-policy FirstGroup attributes
 split-tunnel-policy tunnelspecified
 ipv6-split-tunnel-policy tunnelspecified
 split-tunnel-network-list value FirstList
```

配置拆分隧道的域属性

可以指定要通过拆分隧道 （称之为拆分 DNS）解析的默认域名或域列表。

AnyConnect 3.1 对于 Windows 和 Mac OS X 平台支持真拆分 DNS 功能。如果安全设备上的组策略启用拆分 - 包含隧道，并且如果其指定要通过隧道传送 DNS 名称，则 AnyConnect 隧道会将与这些名称匹配的任何 DNS 查询都通过隧道传送到专用 DNS 服务器。真拆分 DNS 允许仅对与 ASA 推送到客户端的域匹配的 DNS 请求进行隧道访问。这些请求不是以无保护形式发送。另一方面，如果 DNS 请求与 ASA 向下推送的域不匹配，则 AnyConnect 会使客户端操作系统上的 DNS 解析器以无保护形式提交主机名来进行 DNS 解析。

请注意，拆分 DNS 支持标准和更新查询 （包括 A、 AAAA、 NS、 TXT、 MX、 SOA、 ANY、 SRV、 PTR 和 CNAME）。允许与任何隧道网络匹配的 PRT 查询通过隧道。

对于 Mac OS X，仅当满足以下条件之一时， AnyConnect 才能对特定 IP 协议使用真拆分 DNS：

- 为一种 IP 协议（例如 IPv4）配置拆分 DNS，为组策略中的另一种 IP 协议（例如 IPv6）配置客户端旁路协议 （没有为后一种 IP 协议配置地址池）。
- 为两种 IP 协议均配置拆分 DNS。

定义默认域名

ASA 将默认域名传递到 AnyConnect 客户端。客户端将域名附加到会省略域字段的 DNS 查询。此域名仅适用于通过隧道发送的数据包。当没有默认域名时，用户继承默认组策略中的默认域名。

要指定组策略的用户的默认域名，请在 group-policy 配置模式下输入 **default-domain** 命令。要删除域名，请输入此命令的 **no** 形式。

```
hostname(config-group-policy)# default-domain {value domain-name | none}
hostname(config-group-policy)# no default-domain [domain-name]
```

value *domain-name* 参数标识组的默认域名。要指定没有默认域名，请输入 **none** 关键字。此命令使用空值来设置默认域名，这将不允许使用默认域名并防止从默认或指定的组策略继承默认域名。

要删除所有默认域名，请输入不带参数的 **no default-domain** 命令。此命令删除所有已配置的默认域名，包括空列表（如果通过输入带有 **none** 关键字的 **default-domain** 命令进行了创建）。 **no** 形式允许继承域名。

以下示例显示如何为名为 FirstGroup 的组策略设置默认域名 FirstDomain：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

定义拆分隧道的域列表

除默认域以外，输入要通过拆分隧道解析的域列表。在 group-policy 配置模式下输入 **split-dns** 命令。要删除列表，请输入此命令的 **no** 形式。

当没有拆分隧道域列表时，用户继承默认组策略中存在的任何内容。要防止用户继承此类拆分隧道域列表，请输入带有 **none** 关键字的 **split-dns** 命令。

要删除所有拆分隧道域列表，请输入不带参数的 **no split-dns** 命令。这会删除删除所有已配置的拆分隧道域列表，包括通过发出不带 **none** 关键字的 **split-dns** 命令创建的空列表。

参数 **value** *domain-name* 提供 ASA 通过拆分隧道解析的域名。 **none** 关键字指示没有任何拆分 DNS 列表。它还使用空值来设置拆分 DNS 列表，从而不允许使用拆分 DNS 列表，并防止从默认或指定的组策略继承拆分 DNS 列表。此命令的语法如下：

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2...
domain-nameN] | none}
hostname(config-group-policy)# no split-dns [domain-name domain-name2 domain-nameN]
```

输入单个空格以分隔域列表中的每个条目。条目的数量没有限制，但是，整个字符串的长度不能超过 255 个字符。只能使用字母数字字符、连字符 (-) 和句点 (.)。如果要通过隧道解析默认域名，则必须在此列表中显式包含该名称。

以下示例显示如何为名为 FirstGroup 的组策略配置要通过拆分隧道解析的域 Domain1、Domain2、 Domain3 和 Domain4：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

注　当配置拆分 DNS 时，请确保指定的专用 DNS 服务器与为客户端平台配置的 DNS 服务器不重叠。如果重叠，则域名解析无法正常工作，并且查询可能会丢失。

为 Windows XP 和拆分隧道配置 DHCP 拦截

如果拆分隧道选项超过 255 个字节，则 Microsoft XP 会异常导致域名的损坏。为避免此问题，ASA 将其发送的路由数显示为 27 至 40 条路由，并且路由数取决于路由的类别。

通过 DHCP 截取，Microsoft Windows XP 客户端可将拆分隧道与 ASA 配合使用。ASA 直接回复 Microsoft Windows XP 客户端 DHCP Inform 消息，为该客户端提供隧道 IP 地址的子网掩码，域名和无类别静态路由。对于 Windows XP 之前的 Windows 客户端， DHCP 拦截提供域名和子网掩码。这在使用 DHCP 服务器无益的环境中有用。

intercept-dhcp 命令启用或禁用 DHCP 拦截。

```
hostname(config-group-policy)# intercept-dhcp netmask {enable | disable}
hostname(config-group-policy)#
```

netmask 变量提供隧道 IP 地址的子网掩码。此命令的 **no** 形式会从配置中移除 DHCP 拦截：

```
[no] intercept-dhcp
```

以下示例显示如何为名为 FirstGroup 的组策略设置 DHCP 拦截：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

为网络安全设置拆分排除策略

关于云网络安全的信息

AnyConnect 网络安全模块是一个终端组件，用于将 HTTP 流量路由到思科云网络安全扫描代理，在此思科云网络安全会对其进行评估。思科云网络安全会解构网页的元素，以便其可以同时分析每个元素。它会阻止可能有害的内容并允许良性内容通过。

由于全球遍布许多思科云网络安全扫描代理，利用 AnyConnect 网络安全的用户可以最快的响应时间将其流量路由到思科云网络安全扫描代理，从而最小化延迟。

用户建立 VPN 会话后，所有网络流量都通过 VPN 隧道发送。但是，当 AnyConnect 用户使用网络安全时，需要将起源于终端的 HTTP 流量从隧道中排除并将其直接发送到云网络安全扫描代理。

要为旨在以云网络安全扫描代理为目标的流量设置拆分隧道排除，请在组策略中使用 **Set up split exclusion for Web Security** 按钮。

先决条件

- 您需要能够使用 ASDM 来访问 ASA。不能使用命令行界面执行此操作步骤。
- 需要配置网络安全以供与 AnyConnect 客户端配合使用。请参阅 《*AnyConnect 安全移动客户端管理员指南*》中的配置网络安全。
- 您已创建组策略并为其分配使用网络安全配置的 AnyConnect 客户端的连接配置文件。

详细步骤

步骤 1　为要配置的前端启动 ASDM 会话并选择 **Remote Access VPN > Configuration > Group Policies**。

步骤 2　选择要配置的组策略，然后点击 **Edit**。

步骤 3　选择 **Advanced > Split Tunneling**。

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

步骤 5　输入用于网络安全拆分排除的新 ACL 或现有 ACL。ASDM 将设置 ACL 以供在网络列表中使用。

步骤 6　对于新列表点击 **Create Access List**，对于现有列表点击 **Update Access List**。

步骤 7　点击 **OK**。

后续步骤

添加其他扫描代理后，使用新信息来更新在此操作步骤中创建的统一 ACL。

配置供与远程访问客户端配合使用的浏览器代理设置

按照以下步骤配置客户端的代理服务器参数。

步骤 1　通过在 group-policy 配置模式下输入 **msie-proxy server** 命令来配置客户端设备的浏览器代理服务器和端口：

```
hostname(config-group-policy)# msie-proxy server {value server[:port] | none}
hostname(config-group-policy)#
```

默认值为 **none**。要从配置中移除属性，请使用该命令的 **no** 形式。

```
hostname(config-group-policy)# no msie-proxy server
hostname(config-group-policy)#
```

包含代理服务器 IP 地址或主机名和端口号的行的长度必须小于 100 个字符。

以下示例显示如何为名为 FirstGroup 的组策略将 IP 地址 192.168.10.1 配置为使用端口 880 的浏览器代理服务器：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server value 192.168.21.1:880
hostname(config-group-policy)#
```

步骤 2　通过在 group-policy 配置模式下输入 **msie-proxy method** 命令来为客户端设备配置浏览器代理操作 （“方法”）。

```
hostname(config-group-policy)# msie-proxy method [auto-detect | no-modify | no-proxy |
use-server]
hostname(config-group-policy)#
```

默认值为 **use-server**。要从配置中移除属性，请使用该命令的 **no** 形式。

```
hostname(config-group-policy)# no msie-proxy method [auto-detect |no-modify | no-proxy |
use-server]
hostname(config-group-policy)#
```

可用的方法如下：

- **auto-detect** — 在客户端设备的浏览器中启用自动代理服务器检测。
- **no-modify** — 对于此客户端设备保持浏览器中的 HTTP 浏览器代理服务器设置不变。
- **no-proxy** — 在客户端设备的浏览器中禁用 HTTP 代理设置。
- **use-server** — 设置浏览器中的 HTTP 代理服务器设置以使用 **msie-proxy server** 命令中配置的值。

包含代理服务器 IP 地址或主机名和端口号的行的长度必须小于 100 个字符。

以下示例显示如何将 auto-detect 配置为名为 FirstGroup 的组策略的浏览器代理设置。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy method auto-detect
hostname(config-group-policy)#
```

以下示例将名为 FirstGroup 的组策略的浏览器代理设置配置为使用服务器 QAserver 和端口 1001 作为客户端设备的服务器。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server QAserver:port 1001
hostname(config-group-policy)# msie-proxy method use-server
hostname(config-group-policy)#
```

步骤 3　通过在 group-policy 配置模式下输入 **msie-proxy except-list** 命令来为客户端设备上的本地旁路配置浏览器代理异常列表设置。这些地址不是通过代理服务器进行访问。此列表对应于 Proxy Settings 对话框中的 Exceptions 框。

```
hostname(config-group-policy)# msie-proxy except-list {value server[:port] | none}
hostname(config-group-policy)#
```

要从配置中移除属性，请使用该命令的 **no** 形式：

```
hostname(config-group-policy)# no msie-proxy except-list
hostname(config-group-policy)#
```

- **value** *server:port* — 指定 MSIE 服务器的 IP 地址或名称以及为此客户端设备应用的端口。端口号是可选的。
- **none** — 指示没有任何 IP 地址 / 主机名或端口并防止继承异常列表。

默认情况下，会禁用 msie-proxy except-list。

包含代理服务器 IP 地址或主机名和端口号的行的长度必须小于 100 个字符。

以下示例显示如何为名为 FirstGroup 的组策略设置浏览器代理异常列表，其中包含 IP 地址为 192.168.20.1 的使用端口 880 的服务器：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
hostname(config-group-policy)#
```

步骤 4　通过在 group-policy 配置模式下输入 **msie-proxy local-bypass** 命令来为客户端设备启用或禁用浏览器代理本地旁路设置。

```
hostname(config-group-policy)# msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

要从配置中移除属性，请使用该命令的 **no** 形式。

```
hostname(config-group-policy)# no msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

默认情况下，会禁用 msie-proxy local-bypass。

以下示例显示如何为名为 FirstGroup 的组策略启用浏览器代理本地旁路：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy local-bypass enable
hostname(config-group-policy)#
```

配置 AnyConnect 安全移动客户端连接的组策略属性

按照第 10 章，“AnyConnect VPN 客户端连接”中所述启用 AnyConnect 客户端连接后，可以启用或要求组策略的 AnyConnect 功能。在 group-policy webvpn 配置模式下按照以下步骤进行操作：

步骤 1　进入 group-policy webvpn 配置模式。例如：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
```

步骤 2　要禁用终端计算机上 AnyConnect 客户端的永久安装，请使用带有 **none** 关键字的 **anyconnect keep-installer** 命令。例如：

```
hostname(config-group-webvpn)# anyconnect keep-installer none
hostname(config-group-webvpn)#
```

默认是启用客户端的永久安装。在 AnyConnect 会话结束时，客户端保持安装在终端上。

步骤 3　要启用通过组策略的 AnyConnect SSL 连接进行 HTTP 数据压缩，请输入 **anyconnect ssl compression** 命令。默认情况下，压缩设置为 **none** （禁用）。启用压缩，请使用 **deflate** 关键字。例如：

```
hostname(config-group-webvpn)# anyconnect compression deflate
hostname(config-group-webvpn)#
```

步骤 4　要在 ASA 上启用失效对等体检测 (DPD) 和设置 AnyConnect 客户端或 ASA 执行 DPD 的频率，请使用 **anyconnect dpd-interval** 命令：

anyconnect dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

默认情况下， ASA 和 AnyConnect 客户端均会每 30 秒执行 DPD。

网关是指 ASA。可以将 ASA 执行 DPD 测试的频率指定为从 30 秒至 3600 秒 （1 小时）的范围。指定 **none** 会禁用 ASA 执行的 DPD 测试。建议使用值 300。

客户端是指 AnyConnect 客户端。可以将客户端执行 DPD 测试的频率指定为从 30 秒至 3600 秒（1 小时）的范围。指定 **none** 会禁用客户端执行的 DPD 测试。建议使用值 30。

以下示例将 ASA（网关）执行的 DPD 频率配置为 300 秒，将客户端执行的 DPD 频率配置为 30 秒。

```
hostname(config-group-webvpn)# anyconnect dpd-interval gateway 300
hostname(config-group-webvpn)# anyconnect dpd-interval client 30
hostname(config-group-webvpn)#
```

步骤 5　可以确保通过代理、防火墙或 NAT 设备进行的 AnyConnect 连接保持打开，即使设备通过使用 **anyconnect ssl keepalive 命令**调整保活消息的频率来限制连接可以空闲的时间也如此：

anyconnect ssl keepalive {none | *seconds***}**

调整保活还确保当远程用户未在主动运行基于套接字的应用 （例如 Microsoft Outlook 或 Microsoft Internet Explorer）时， AnyConnect 客户端不会断开连接并重新连接。

以下示例配置安全设备以使 AnyConnect 客户端能够以 300 秒 （5 分钟）的频率发送保活信息：

```
hostname(config-group-webvpn)# anyconnect ssl keepalive 300
hostname(config-group-webvpn)#
```

步骤 6　要使 AnyConnect 客户端能够对 SSL 会话的执行重新生成密钥操作，请使用 **anyconnect ssl rekey** 命令：

anyconnect ssl rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}}

默认情况下，会禁用重新生成密钥。

将方法指定为 new-tunnel 即指定 AnyConnect 客户端在 SSL 重新生成密钥期间建立新隧道。将方法指定为 **none** 会禁用重新生成密钥。将方法指定为 **ssl** 即指定在重新生成密钥期间进行 SSL 重新协商。可以指定从 1 至 10080 （1 周）的时间 （即从会话开始直到重新生成密钥的分钟数），而不是指定方法。

以下示例将 AnyConnect 客户端配置为在重新生成密钥期间与 SSL 重新协商，并将重新生成密钥配置为在会话开始后 30 分钟发生：

```
hostname(config-group-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
hostname(config-group-webvpn)#
```

步骤 7　客户端协议旁路功能允许配置 ASA 在其只希望 IPv6 流量时如何管理 IPv4 流量，或者在其只希望 IPv4 流量时如何管理 IPv6 流量。

当 AnyConnect 客户端与 ASA 进行 VPN 连接时，ASA 可能会为其分配 IPv4 和 / 或 IPv6 地址。如果 ASA 为 AnyConnect 连接仅分配 IPv4 地址或仅分配 IPv6 地址，则现在可以配置客户端旁路协议来丢弃 ASA 没有为其分配 IP 地址的网络流量，或者允许流量绕过 ASA 并从客户端以未加密或“无保护”的形式发送。

例如，假设 ASA 仅向 AnyConnect 连接分配 IPv4 地址并且终端进行双重堆叠。当终端尝试访问 IPv6 地址时，如果禁用客户端旁路协议，则会丢弃 IPv6 流量；但是，如果启用客户端旁路协议，则会从客户端以无保护形式发送 IPv6 流量。

使用 client-bypass-protocol 命令启用或禁用客户端旁路协议功能。以下是命令语法：

```
client-bypass-protocol {enable | disable}
```

The following example enables client bypass protocol:

```
hostname(config-group-policy)# client-bypass-protocol enable
hostname(config-group-policy)#
```

以下示例启用客户端旁路协议：

```
hostname(config-group-policy)# client-bypass-protocol disable
hostname(config-group-policy)#
```

以下示例移除已启用或已禁用的客户端旁路协议设置：

```
hostname(config-group-policy)# no client-bypass-protocol enable
hostname(config-group-policy)#
```

步骤 8　如果已在 ASA 之间配置负载平衡，请指定 ASA 的 FQDN，以便解析用于重新建立 VPN 会话的 ASA IP 地址。此设置对于支持不同 IP 协议的网络之间 （例如 IPv4 到 IPv6）的客户端漫游至关重要。

漫游后，不能使用 AnyConnect 配置文件中存在的 ASA FQDN 来派生 ASA IP 地址。地址可能与负载平衡方案中的正确设备 （与之建立隧道的设备）不匹配。

如果未将设备 FQDN 推送到客户端，则客户端将尝试重新连接到隧道以前建立的任意 IP 地址。为支持不同 IP 协议的网络之间 （从 IPv4 到 IPv6 ）的漫游， AnyConnect 必须在漫游后执行设备 FQDN 的名称解析，以便其可以确定要使用哪个 ASA 地址重新建立隧道。客户端在初始连接期间使用其配置文件中存在的 ASA FQDN。在后续会话重新连接期间，它在适用时始终使用由 ASA 推送 （并由组策略中的管理员配置）的设备 FQDN。如果未配置 FQDN，则 ASA 从 Device Setup > Device Name/Password and Domain Name 下设置的任意内容派生设备 FQDN（并将其发送到客户端）。

如果设备 FQDN 未由 ASA 推送，则客户端在不同 IP 协议的网络之间漫游后无法重新建立 VPN 会话。

使用 gateway-fqdn 命令配置 ASA 的 FQDN。以下是命令语法：

```
gateway-fqdn value {FQDN_Name | none}
no gateway-fqdn
```

以下示例将 ASA 的 FQDN 定义为 ASAName.example.cisco.com

```
hostname(config-group-policy)# gateway-fqdn value ASAName.example.cisco.com
hostname(config-group-policy)#
```

以下示例从组策略中移除 ASA 的 FQDN。然后，组策略从默认组策略继承该值。

```
hostname(config-group-policy)# no gateway-fqdn
hostname(config-group-policy)#
```

以下示例将 FQDN 定义为空值。如果适用，将使用通过 hostname 和 domain-name 命令配置的全局 FQDN。

```
hostname(config-group-policy)# gateway-fqdn none
hostname(config-group-policy)#
```

配置 IPsec (IKEv1) 客户端的组策略属性

配置 IPsec (IKEv1) 客户端的安全属性

要指定组的安全设置，请执行以下步骤：

步骤 1　在 group-policy 配置模式下使用带有 **enable** 关键字的 **password-storage** 命令指定是否允许用户在客户端系统上存储其登录密码。要禁用密码存储，请使用带有 **disable** 关键字的 **password-storage** 命令。

```
hostname(config-group-policy)# password-storage {enable | disable}
hostname(config-group-policy)#
```

出于安全原因，默认情况下会禁用密码存储。仅在已知处于安全站点中的系统上启用密码存储。

如要从运行配置中移除 password-storage 属性，请输入此命令的 **no** 形式：

```
hostname(config-group-policy)# no password-storage
hostname(config-group-policy)#
```

指定 **no** 形式允许从其他组策略继承 password-storage 的值。

此命令不适用于交互式硬件客户端身份验证或硬件客户端的个人用户身份验证。

以下示例显示如何为名为 FirstGroup 的组策略启用密码存储：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
hostname(config-group-policy)#
```

步骤 2　指定是否启用 IP 压缩 （默认情况下已禁用）。

注　IPsec IKEv2 连接不支持 IP 压缩。

```
hostname(config-group-policy)# ip-comp {enable | disable}
hostname(config-group-policy)#
```

如要启用 LZS IP 压缩，请在 group-policy 配置模式下输入带有 **enable** 关键字的 **ip-comp** 命令。要禁用 IP 压缩，请输入带有 **disable** 关键字的 **ip-comp** 命令。

如要从运行配置中移除 **ip-comp** 属性，请输入此命令的 **no** 形式。这允许从其他组策略继承值。

```
hostname(config-group-policy)# no ip-comp
hostname(config-group-policy)#
```

启用数据压缩可能会加快与调制解调器连接的远程拨入用户的数据传输速率。

注意事项　数据压缩会增加每个用户会话的内存要求和 CPU 使用率，并因此降低 ASA 的整体吞吐量。为此，建议仅对与调制解调器连接的远程用户启用数据压缩。设计特定于调制解调器用户的组策略并仅对其启用压缩。

步骤 3　通过在 group-policy 配置模式下使用带有 **enable** 关键字的 **re-xauth** 命令指定是否要求用户在 IKE 重新生成密钥时重新进行身份验证。

注　IKEv2 连接不支持 IKE 重新生成密钥。

如果在 IKE 重新生成密钥时启用重新身份验证，则 ASA 会提示用户在初始阶段 1 IKE 协商期间输入用户名和密码，此外只要发生 IKE 重新生成密钥便提示进行用户身份验证。重新身份验证提供额外的安全性。

如果配置的重新生成密钥间隔非常短，则用户可能会发现重复的授权请求不便。要避免重复的授权请求，请禁用重新身份验证。要检查配置的重新生成密钥间隔，请在监控模式下，输入 **show crypto ipsec sa** 命令以查看安全关联生存期 （以秒为单位）和生存期 （以数据的千字节数为单位）。要在 IKE 重新生成密钥时禁用用户重新身份验证，请输入 **disable** 关键字。默认情况下，会禁用在 IKE 重新生成密钥时进行重新身份验证。

```
hostname(config-group-policy)# re-xauth {enable | disable}
hostname(config-group-policy)#
```

如要允许从其他组策略继承用于在 IKE 重新生成密钥时进行重新身份验证的值，请通过输入此命令的 **no** 形式来从运行配置中移除 re-xauth 属性：

```
hostname(config-group-policy)# no re-xauth
hostname(config-group-policy)#
```

注　如果在连接的另一端没有任何用户，则重新身份验证会失败。

步骤 4　指定是否启用完全前向保密。在 IPsec 协商过程中，完全前向保密确保每个新的加密密钥与任何先前密钥不相关。一个组策略可以从另一个组策略继承完全前向保密的值。默认情况下会禁用完全前向保密。要启用完全前向保密，请在 group-policy 配置模式下使用带有 **enable** 关键字的 **pfs** 命令。

```
hostname(config-group-policy)# pfs {enable | disable}
hostname(config-group-policy)#
```

要禁用完全前向保密，请输入带有 **disable** 关键字的 **pfs** 命令。

要从运行配置中移除完全前向保密属性并防止继承值，请输入此命令的 **no** 形式。

```
hostname(config-group-policy)# no pfs
hostname(config-group-policy)#
```

配置 IKEv1 客户端的 IPsec-UDP 属性

凭借 IPsec over UDP（有时称为通过 NAT 的 IPSec），Cisco VPN 客户端或硬件客户端通过 UDP 连接到运行 NAT 的 ASA。默认情况下会将其禁用。IPsec over UDP 是专有的；它仅适用于远程访问连接，并且需要模式配置。 ASA 在协商 SA 时与客户端交换配置参数。使用 IPsec over UDP 可能会略微降低系统性能。

要启用 IPsec over UDP，请在 group-policy 配置模式下配置带有 **enable** 关键字的 **ipsec-udp** 命令，如下所示：

```
hostname(config-group-policy)# ipsec-udp {enable | disable}
hostname(config-group-policy)# no ipsec-udp
```

如要使用 IPsec over UDP，还必须配置 **ipsec-udp-port** 命令，如本节中所述。

如要禁用 IPsec over UDP，请输入 **disable** 关键字。要从运行配置中移除 IPsec over UDP 属性，请输入此命令的 **no** 形式。这允许从其他组策略继承 IPsec over UDP 的值。

此外，还必须将 Cisco VPN 客户端配置为使用 IPsec over UDP （默认情况下它配置为使用该属性）。 VPN 3002 无需配置即可使用 IPsec over UDP。

以下示例显示如何为名为 FirstGroup 的组策略设置 IPsec over UDP：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

如果已启用 IPsec over UDP，则还必须在 group-policy 配置模式下配置 **ipsec-udp-port** 命令。此命令设置 IPsec over UDP 的 UDP 端口号。在 IPsec 协商过程中，ASA 侦听已配置的端口并转发该端口的 UDP 流量，即使其他过滤规则丢弃 UDP 流量也如此。端口号的范围可以从 4001 至 49151。默认端口值为 10000。

如要禁用 UDP 端口，请输入此命令的 **no** 形式。这允许从其他组策略继承 IPsec over UDP 端口的值。

```
hostname(config-group-policy)# ipsec-udp-port port
```

以下示例显示如何为名为 FirstGroup 的组策略将 IPsec UDP 端口设置为端口 4025：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

配置 VPN 硬件客户端的属性

本节描述如何为 VPN 硬件客户端启用或禁用安全设备身份验证和用户身份验证或设置用户身份验证超时值。它们还允许思科 IP 电话和 LEAP 数据包绕过个人用户身份验证并允许使用网络扩展模式的硬件客户端进行连接。

配置安全设备身份验证

安全设备身份验证通过要求 VPN 硬件客户端在客户端每次启动隧道时使用用户名和密码进行身份验证来提供额外的安全性。在启用此功能的情况下，硬件客户端不保存用户名和密码。默认情况下会禁用安全设备身份验证。

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

安全设备身份验证要求您具有为硬件客户端使用的连接配置文件配置的身份验证服务器组。如果要求在主 ASA 上进行安全设备身份验证，请确保也在任何备份服务器上对其进行配置。

通过在 group-policy 配置模式下输入带有 **enable** 关键字的 **secure-unit-authentication** 命令来指定是否启用安全设备身份验证。

```
hostname(config-group-policy)# secure-unit-authentication {enable | disable}
hostname(config-group-policy)# no secure-unit-authentication
```

如要禁用安全设备身份验证，请输入 **disable** 关键字。要从运行配置中移除安全设备身份验证属性，请输入此命令的 **no** 形式。此选项允许从其他组策略继承安全设备身份验证的值。

以下示例显示如何为名为 FirstGroup 的组策略启用安全设备身份验证：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

配置用户身份验证

默认情况下会禁用用户身份验证。启用时，用户身份验证要求硬件客户端背后的个人用户进行身份验证以跨隧道获取对网络的访问。个人用户根据配置的身份验证服务器的顺序进行身份验证。

通过在 group-policy 配置模式下输入带有 **enable** 关键字的 **user-authentication** 命令来指定是否启用用户身份验证。

```
hostname(config-group-policy)# user-authentication {enable | disable}
hostname(config-group-policy)# no user-authentication
```

如要禁用用户身份验证，请输入 **disable** 关键字。要从运行配置中移除用户身份验证属性，请输入此命令的 **no** 形式。此选项允许从其他组策略继承用户身份验证的值。

如果要求在主 ASA 上进行用户身份验证，请确保也在任何备份服务器上对其进行配置。

以下示例显示如何为名为 FirstGroup 的组策略启用用户身份验证：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
```

配置空闲超时

通过在 group-policy 配置模式下输入 **user-authentication-idle-timeout** 命令来为硬件客户端背后的个人用户设置空闲超时。如果硬件客户端背后的用户在空闲超时期内没有通信活动，则 ASA 会终止客户端的访问：

```
hostname(config-group-policy)# user-authentication-idle-timeout {minutes | none}
hostname(config-group-policy)# no user-authentication-idle-timeout
```

注　此计时器仅终止客户端通过 VPN 隧道进行的访问，而非终止 VPN 隧道本身。

为响应 **show uauth** 命令而指示的空闲超时始终是已在 Cisco Easy VPN 远程设备上对隧道进行身份验证的用户的空闲超时值。

minutes 参数指定空闲超时期内的分钟数。最小值为 1 分钟，默认值为 30 秒，最大值为 35791394 分钟。

如要删除空闲超时值，请输入此命令的 **no** 形式。此选项允许从其他组策略继承空闲超时值。

如要防止继承空闲超时值，请输入带有 **none** 关键字的 **user-authentication-idle-timeout** 命令。此命令使用空值来设置空闲超时，这将禁止空闲超时并防止从默认或指定的组策略继承用户身份验证空闲超时值。

以下示例显示如何为名为 FirstGroup 的组策略设置 45 分钟的空闲超时值：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication-idle-timeout 45
```

配置 IP 电话旁路

可以允许思科 IP 电话绕过硬件客户端背后的个人用户身份验证。如要启用 IP 电话旁路，请在 group-policy 配置模式下输入带有 **enable** 关键字的 **ip-phone-bypass**。通过 IP 电话旁路，硬件客户端背后的 IP 电话可以在不执行用户身份验证过程的情况下进行连接。默认情况下会禁用 IP 电话旁路。如果启用，则安全设备身份验证保持生效。

如要禁用 IP 电话旁路，请输入 **disable** 关键字。如要从运行配置中移除 IP 电话旁路属性，请输入此命令的 **no** 形式。此选项允许从其他组策略继承 IP 电话旁路的值。

```
hostname(config-group-policy)# ip-phone-bypass {enable | disable}
hostname(config-group-policy)# no ip-phone-bypass
```

注　您必须配置 mac-exempt 来免除客户端进行身份验证。

配置 LEAP 旁路

当启用 LEAP 旁路时，来自 VPN 3002 硬件客户端背后的无线设备的 LEAP 数据包通过 VPN 隧道进行传播，然后再进行用户身份验证。通过此操作，使用思科无线接入点设备的工作站可建立 LEAP 身份验证，然后在每次用户身份认证后再次进行身份验证。默认情况下会禁用 LEAP 旁路。

如要允许来自思科无线接入点的 LEAP 数据包绕过个人用户身份验证，请在 group-policy 配置模式下输入带有 **enable** 关键字的 **leap-bypass** 命令。要禁用 LEAP 旁路，请输入 **disable** 关键字。要从运行配置中移除 LEAP 旁路属性，请输入此命令的 **no** 形式。此选项允许从其他组策略继承 LEAP 旁路的值。

```
hostname(config-group-policy)# leap-bypass {enable | disable}
hostname(config-group-policy)# no leap-bypass
```

注　IEEE 802.1X 是在有线和无线网络上进行身份验证的标准。它在客户端和身份验证服务器之间为无限 LAN 提供强相互身份验证，这可提供动态的每用户、每会话无线加密隐私 (WEP) 密钥，从而移除随静态 WEP 密钥出现的管理负担和安全问题。

Cisco Systems 已开发一种 802.1X 无线身份验证类型，称为 Cisco LEAP。 LEAP （轻量级可扩展身份认证协议）在连接的一端的无线客户端和另一端的 RADIUS 服务器之间实施相互身份验证。用于身份验证的凭据 （包括密码）在通过无线介质传输之前始终加密。

Cisco LEAP 向 RADIUS 服务器进行无线客户端身份验证。它不包括 RADIUS 记帐服务。

如果启用交互式硬件客户端身份验证，则此功能无法按计划工作。

注意事项　允许任何未经身份验证的流量遍历隧道可能会对网络产生安全风险。

以下示例显示如何为名为 FirstGroup 的组策略设置 LEAP 旁路：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# leap-bypass enable
```

启用网络扩展模式

通过网络扩展模式，硬件客户端可通过 VPN 隧道向远程专用网络提供单个可路由的网络。 IPsec 封装从硬件客户端背后的专用网络到 ASA 背后的网络的所有流量。 PAT 不适用。因此， ASA 背后的设备可以通过隧道且仅通过隧道访问硬件客户端背后的专用网络上的设备，反之亦然。硬件客户端必须启动隧道，但是在建立隧道之后，任一端都可启动数据交换。

通过在 group-policy 配置模式下输入带有 **enable** 关键字的 **nem** 命令来为硬件客户端启用网络扩展模式：

```
hostname(config-group-policy)# nem {enable | disable}
hostname(config-group-policy)# no nem
```

如要禁用 NEM，请输入 **disable** 关键字。要从运行配置中移除 NEM 属性，请输入此命令的 **no** 形式。此选项允许从其他组策略继承值。

以下示例显示如何为名为 FirstGroup 的组策略设置 NEM：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
```

配置备份服务器属性

如果计划使用备份服务器，请对其进行配置。通过 IPsec 备用服务器，VPN 客户端可在主 ASA 不可用时连接到中心站点。配置备份服务器时，由于建立了 IPsec 隧道， ASA 会将服务器列表推送到客户端。备份服务器不存在，直到在客户端或主 ASA 上对其进行配置为止。

在客户端或主 ASA 上配置备份服务器。如果在 ASA 上配置备份服务器，则它会将备份服务器策略推送到组中的客户端，从而替换客户端上的备份服务器列表 （如果已配置）。

注　如果使用的是主机名，则明智的方法是将备份 DNS 和 WINS 服务器与主 DNS 和 WINS 服务器放在不同网络上。否则，如果硬件客户端背后的客户端通过 DHCP 从硬件客户端获取 DNS 和 WINS 信息，与主服务器的连接丢失，并且备份服务器具有不同的 DNS 和 WINS 信息，则客户端无法更新，直到 DHCP 租用到期为止。此外，如果使用主机名且 DNS 服务器不可用，则可能发生重大延迟。

如要配置备份服务器，请在 group-policy 配置模式下输入 **backup-servers** 命令：

```
hostname(config-group-policy)# backup-servers {server1 server2... server10 |
clear-client-config | keep-client-config}
```

如要移除备份服务器，请在指定备份服务器的情况下输入此命令的 **no** 形式。如要从运行配置中移除 backup-servers 属性并允许从其他组策略继承 backup-servers 的值，请输入不带参数的此命令的 **no** 形式。

```
hostname(config-group-policy)# no backup-servers [server1 server2... server10 |
clear-client-config | keep-client-config]
```

clear-client-config 关键字指定客户端不使用备份服务器。 ASA 推送空服务器列表。

keep-client-config 关键字指定 ASA 不将备份服务器信息发送到客户端。客户端使用其自己的备份服务器列表 （如果已配置）。这是默认值。

server1 server 2....server10 参数列表是在主 ASA 不可用时要使用的 VPN 客户端的服务器的空格分隔、优先级排序的列表。此列表按 IP 地址或主机名来标识服务器。列表长度可为 500 个字符，并且可以包含最多 10 个条目。

以下示例显示如何为名为 FirstGroup 的组策略配置 IP 地址为 10.10.10.1 和 192.168.10.14 的备份服务器：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

配置网络准入控制参数

本节中的 group-policy NAC 命令全都具有默认值。除非有充分的理由对其进行更改，否则请接受这些参数的默认值。

ASA 使用基于 UDP 的可扩展身份验证协议 (EAP) (EAPoUDP) 消息传递验证远程主机的状态。状态身份验证涉及在分配网络访问策略之前检查远程主机是否符合安全要求。在安全设备上配置 NAC 之前，必须为网络准入控制配置访问控制服务器。

访问控制服务器将状态标记 （可在 ACS 上配置的信息文本字符串）下载到安全设备来协助系统监控、报告、调试和日志记录。典型的状态标记为 Healthy、 Checkup、 Quarantine、 Infected 或 Unknown。在状态验证或无客户端身份验证后， ACS 将会话的访问策略下载到安全设备。

要配置默认组策略或备用组策略的网络准入控制设置，请执行以下步骤：

步骤 1　（可选）配置状态查询计时器周期。安全设备在每次成功的状态验证和状态查询响应后启动状态查询计时器。此计时器到期会触发对于主机状态中的更改的查询，称为状态查询。输入范围在 30 至 1800 内的秒数。默认设置为 300。

要指定网络准入控制会话中每次成功状态验证与对主机状态中的更改的下一次查询之间的间隔，请在 group-policy 配置模式下使用 **nac-sq-period** 命令：

```
hostname(config-group-policy)# nac-sq-period seconds
hostname(config-group-policy)#
```

如要从默认组策略继承状态查询计时器的值，请访问该值继承自的备用组策略，然后使用此命令的 **no** 形式：

```
hostname(config-group-policy)# no nac-sq-period [seconds]
hostname(config-group-policy)#
```

以下示例将状态查询计时器的值更改为 1800 秒：

```
hostname(config-group-policy)# nac-sq-period 1800
hostname(config-group-policy)
```

以下示例从默认组策略继承状态查询计时器的值：

```
hostname(config-group-policy)# no nac-sq-period
hostname(config-group-policy)#
```

步骤 2　（*可选*）配置 NAC 重新验证周期。安全设备在每次成功状态验证后启动重新验证计时器。此计时器到期，会触发下一次无条件状态验证。安全设备在重新验证期间维护状态验证。如果访问控制服务器在状态验证或重新验证期间不可用，则默认组策略会生效。输入每次成功状态验证之间的间隔 （以秒为单位）。范围为 300 至 86400。默认设置为 36000。

如要在网络准入控制会话中指定每次成功状态验证之间的间隔，请在 group-policy 配置模式下使用 **nac-reval-period** 命令：

```
hostname(config-group-policy)# nac-reval-period seconds
hostname(config-group-policy)#
```

如要从默认组策略继承重新验证计时器的值，请访问该值继承自的备用组策略，然后使用此命令的 **no** 形式：

```
hostname(config-group-policy)# no nac-reval-period [seconds]
hostname(config-group-policy)#
```

以下示例将重新验证计时器更改为 86400 秒：

```
hostname(config-group-policy)# nac-reval-period 86400
hostname(config-group-policy)
```

以下示例从默认组策略继承重新验证计时器的值：

```
hostname(config-group-policy)# no nac-reval-period
hostname(config-group-policy)#
```

步骤 3　（*可选*）配置 NAC 的默认 ACL。如果状态验证失败，则安全设备将应用与所选 ACL 关联的安全策略。指定 **none** 或扩展 ACL。默认设置为 **none**。如果设置为 **none** 并且状态验证失败，则安全设备将应用默认组策略。

要指定将用作状态验证失败的网络准入控制会话的默认 ACL，请在 group-policy 配置模式下使用 **nac-default-acl** 命令：

```
hostname(config-group-policy)# nac-default-acl {acl-name | none}
hostname(config-group-policy)#
```

要从默认组策略继承 ACL，请访问该 ACL 继承自的备用组策略，然后使用此命令的 **no** 形式：

```
hostname(config-group-policy)# no nac-default-acl [acl-name | none]
hostname(config-group-policy)#
```

此命令的元素如下：

- *acl-name* — 指定使用 **aaa-server host** 命令在 ASA 上配置的状态验证服务器组的名称。名称必须与该命令中指定的 server-tag 变量匹配。
- **none** — 禁用从默认组策略继承 ACL，并且不将 ACL 应用于状态验证失败的 NAC 会话。

由于默认情况下会禁用 NAC，因此遍历 ASA 的 VPN 流量不受 NAC 默认 ACL 限制，直到启用 NAC 为止。

以下示例将 acl-1 标识为状态验证失败时要应用的 ACL：

```
hostname(config-group-policy)# nac-default-acl acl-1
hostname(config-group-policy)
```

以下示例从默认组策略继承 ACL：

```
hostname(config-group-policy)# no nac-default-acl
hostname(config-group-policy)
```

以下示例禁用从默认组策略继承 ACL，并且不将 ACL 应用于状态验证失败的 NAC 会话：

```
hostname(config-group-policy)# nac-default-acl none
hostname(config-group-policy)#
```

步骤 4　配置 VPN 的 NAC 免除。默认情况下，免除列表为空。过滤器属性的默认值为 **none**。为每个要匹配以免除远程主机进行状态验证的各操作系统 （和 ACL）输入一次 **vpn-nac-exempt 命令**。

如要向免除进状态验证的远程计算机类型的列表中添加条目，请在 group-policy 配置模式下使用 **vpn-nac-exempt** 命令：

```
hostname(config-group-policy)# vpn-nac-exempt os "os name" [filter {acl-name | none}]
[disable]
hostname(config-group-policy)#
```

要禁用继承并指定所有主机都要进行状态验证，请在 **vpn-nac-exempt** 之后随即使用 **none** 关键字：

```
hostname(config-group-policy)# vpn-nac-exempt none
hostname(config-group-policy)#
```

要从免除列表中移除条目，请使用此命令的 **no** 形式并命名要移除的该条目中的操作系统（和 ACL）。

```
hostname(config-group-policy)# no vpn-nac-exempt [os "os name"] [filter {acl-name | none}]
[disable]
hostname(config-group-policy)#
```

要从与此组策略关联的免除列表中移除所有条目并从默认组策略继承该列表，请使用此命令的 **no** 形式而不指定其他关键字：

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)#
```

这些命令的语法元素如下：

- *acl-name* — ASA 配置中存在的 ACL 的名称。
- **disable** — 禁用免除列表中的条目而不将其从列表中移除。
- **filter** —（可选）用于在计算机与操作系统名称匹配的情况下应用 ACL 以过滤流量的过滤器。
- **none** — 紧接在 **vpn-nac-exempt** 之后输入时，此关键字禁用继承并指定所有流量都将进行状态验证。紧接在 **filter** 之后输入时，此关键字指示条目不指定 ACL。
- **OS** — 免除操作系统进行状态验证。
- *os name* — 操作系统名称。仅当名称包含空格时 （例如，“Windows XP”），才必需引号。

以下示例将运行 Windows XP 的所有主机添加到免除状态验证的计算机的列表。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows XP"
hostname(config-group-policy)
```

以下示例免除运行 Windows 98 的所有主机，这些主机与名为 acl-1 的 ACL 中的 ACE 匹配：

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

以下示例将同一条目添加到免除列表，但是将其禁用：

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1 disable
hostname(config-group-policy)
```

以下示例从免除列表中移除同一条目，无论其是否已禁用：

```
hostname(config-group-policy)# no vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

以下示例禁用继承并指定所有主机都将进行状态验证：

```
hostname(config-group-policy)# no vpn-nac-exempt none
hostname(config-group-policy)
```

以下示例从免除列表中移除所有条目：

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)
```

步骤 5　通过输入以下命令启用或禁用网络准入控制：

```
hostname(config-group-policy)# nac {enable | disable}
hostname(config-group-policy)#
```

如要从默认组策略继承 NAC 设置，请访问该 NAC 设置 继承自的备用组策略，然后使用此命令的 **no** 形式：

```
hostname(config-group-policy)# no nac [enable | disable]
hostname(config-group-policy)#
```

默认情况下，会禁用 NAC。启用 NAC 要求对远程访问进行状态验证。如果远程计算机通过验证检查，则 ACS 服务器会下载访问策略以供 ASA 实施。默认情况下会禁用 NAC。

网络上必须存在访问控制服务器。

以下示例为组策略启用 NAC：

```
hostname(config-group-policy)# nac enable
hostname(config-group-policy)#
```

配置 VPN 客户端防火墙策略

*防火墙*通过检查每个入站和出站数据包以确定允许其通过防火墙还是将其丢弃来将计算机与 Internet 隔离并进行保护。如果组中的远程用户配置了拆分隧道，则防火墙可提供额外的安全性。在此情况下，防火墙保护用户的计算机，从而保护公司网络抵御通过 Internet 或用户的本地 LAN 进行的入侵。使用 VPN 客户端连接到 ASA 的远程用户可以选择相应的防火墙选项。

通过在 group-policy 配置模式下输入 **client-firewall** 命令来设置 IKE 隧道协商期间 ASA 推送到 VPN 客户端的个人防火墙策略。要删除防火墙策略，请输入此命令的 **no** 形式。

要删除所有防火墙策略，请输入不带参数的 **no client-firewall** 命令。此命令删除所有已配置的防火墙策略，包括空策略 （此如果通过输入带有 **none** 关键字的 **client-firewall** 命令进行了创建）。

当没有防火墙策略时，用户将继承默认或其他组策略中存在的任何内容。要防止用户继承此类防火墙策略，请输入带有 **none** 关键字的 **client-firewall** 命令。

通过 Client Firewall 选项卡上的 Add or Edit Group Policy 对话框，可以为进行添加或修改的组策略配置 VPN 客户端的防火墙设置。

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

在第一个场景中，远程用户在 PC 上安装了个人防火墙。 VPN 客户端实施在本地防火墙上定义的防火墙策略，并监控该防火墙以确保其正在运行。如果防火墙停止运行，则 VPN 客户端会断开与 ASA 的连接。（此防火墙实施机制称为 *Are You There (AYT)*，因为 VPN 客户端通过向防火墙发送周期性 “are you there?”消息对其进行监控；如果没有应答，则 VPN 客户端知道防火墙关闭并会终止其与 ASA. 的连接）。网络管理员可能按原来配置这些 PC 防火墙，但是通过此方法，每个用户可以定制各自的配置。

在第二个场景中，您可能首选为 VPN 客户端 PC 上的个人防火墙实施集中式防火墙策略。一个常见的示例是阻止 Internet 流量使用拆分隧道传送到组中的远程 PC。在已建立隧道的情况下，此方法保护 PC 并因此保护中心站点抵御从 Internet 进行的入侵。此防火墙场景称为*推送策略*或*中心保护策略 (CPP)*。在 ASA 上，可创建要在 VPN 客户端上实施的流量管理规则集，将这些规则与过滤器关联，并将该过滤器指定为防火墙策略。 ASA 将此策略向下推送到 VPN 客户端。然后，VPN 客户端反过来将策略传递到实施该策略的本地防火墙。

配置 AnyConnect 客户端防火墙策略

AnyConnect 客户端的防火墙规则可以指定 IPv4 和 IPv6 地址。

先决条件

您已创建指定 IPv6 地址的统一访问规则。

表 4-1

	命令	说明
步骤 1	**webvpn** **示例：** hostname(config)# **group-policy ac-client-group attributes** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)#	进入 webvpn 组策略配置模式。
步骤 2	**anyconnect firewall-rule client-interface {private | public} value** *[RuleName]* **示例：** hostname(config-group-webvpn)# **anyconnect fireall-rule client-iterface private value** *ClientFWRule*	指定专用或公用网络规则的访问控制规则。专用网络规则是应用于客户端上的 VPN 虚拟适配器接口的规则。
步骤 3	**show runn group-policy** [value] **示例：** hostname(config-group-webvpn)# **show runn group-policy FirstGroup** group-policy FirstGroup internal group-policy FirstGroup attributes webvpn anyconnect firewall-rule client-interface private value ClientFWRule	显示组策略属性以及组策略的 webvpn 策略属性。
步骤 4	（可选） **no anyconnect firewall-rule client-ineterface private value [***RuleName***]** **示例：** hostname(config-group-webvpn)#**no anyconnect firewall-rule client-ineterface private value** hostname(config-group-webvpn)#	从专用网络规则中移除客户端防火墙规则。

支持 Zone Labs Integrity Server 服务器

本节介绍 Zone Labs Integrity Server 服务器 （也称为 Check Point Integrity 服务器），并提供用于将 ASA 配置为支持 Zone Labs Integrity 服务器的示例操作步骤。Integrity 服务器是用于在远程 PC 上配置和实施安全策略的中央管理站。如果远程 PC 不符合 Integrity 服务器规定的安全策略，则不会授予其对受 Integrity 服务器和 ASA 保护的专用网络的访问。

本节包含以下主题：

Integrity 服务器和 ASA 交互的概述

VPN 客户端软件和 Integrity 客户端软件在远程 PC 上共存。以下步骤汇总远程 PC、 ASA 和 Integrity 服务器在 PC 与企业专用网络之间建立会话过程中的操作：

1. VPN 客户端软件 （与 Integrity 客户端软件驻留在相同的远程 PC 上）连接到 ASA 并告知 ASA 其防火墙客户端的类型。
2. 在 ASA 批准客户端防火墙类型后，ASA 将 Integrity 服务器地址信息传回到 Integrity 客户端。
3. 在 ASA 充当代理的情况下，Integrity 客户端与 Integrity 服务器建立受限连接。受限连接仅在 Integrity 客户端和 Integrity 服务器之间。
4. Integrity 服务器确定 Integrity 客户端是否符合规定的安全策略。如果 Integrity 客户端符合安全策略，则 Integrity 服务器会指示 ASA 打开连接并为 Integrity 客户端提供连接详细信息。
5. 在远程 PC 上， VPN 客户端将连接详细信息传递到 Integrity 客户端，并表明策略实施应立即开始且 Integrity 客户端可以进入专用网络。
6. 建立 VPN 连接后， Integrity 服务器使用客户端检测信号消息继续监控 Integrity 客户端的状态。

注　ASA 的当前版本一次支持一台 Integrity 服务器，即使用户界面支持最多五台 Integrity 服务器的配置也如此。如果活动的 Integrity 服务器发生故障，请在 ASA 上配置另一台 Integrity 服务器，然后重新建立 VPN 客户端会话。

配置 Integrity 服务器支持

本节描述用于将 ASA 配置为支持 Zone Labs Integrity 服务器的示例操作步骤。该操作步骤涉及配置地址、端口、连接失败超时和失败状态以及 SSL 证书参数。

如要配置 Integrity 服务器，请执行以下步骤：

	命令	目的
步骤 1	**zonelabs-Integrity server-address** {*hostname1* | *ip-address1*} **示例：** `hostname(config)# zonelabs-Integrity server-address 10.0.0.5`	使用 IP 地址 10.0.0.5 配置 Integrity 服务器。
步骤 2	**zonelabs-integrity port** *port-number* **示例：** `hostname(config)# zonelabs-integrity port 300`	指定端口 300 （默认端口为 5054）。
步骤 3	**zonelabs-integrity interface** *interface* **示例：** `hostname(config)# zonelabs-integrity interface inside`	指定用于与 Integrity 服务器进行通信的内部接口。
步骤 4	**zonelabs-integrity fail-timeout** *timeout* **示例：** `hostname(config)# zonelabs-integrity fail-timeout 12`	在将 Integrity 服务器声明为已发生故障并关闭 VPN 客户端连接之前，请确保 ASA 等待 12 秒以获取来自活动或备用 Integrity 服务器的响应。 **注**　如果 ASA 和 Integrity 服务器之间的连接失败，则默认情况下 VPN 客户端连接保持打开，以便企业 VPN 不因 Integrity 服务器故障而中断。但是，如果 Zone Labs Integrity 服务器发生故障，则可能要关闭 VPN 连接。
步骤 5	**zonelabs-integrity fail-close** **示例：** `hostname(config)# zonelabs-integrity fail-close`	配置 ASA，以便在 ASA 和 Zone Labs Integrity 服务器之间的连接失败时关闭与 VPN 客户端的连接。
步骤 6	**zonelabs-integrity fail-open** **示例：** `hostname(config)# zonelabs-integrity fail-open`	将已配置的 VPN 客户端连接失败状态恢复为默认值并确保客户端连接保持打开。

	命令	目的
步骤 7	**zonelabs-integrity ssl-certificate-port** *cert-port-number* **示例：** hostname(config)# zonelabs-integrity ssl-certificate-port 300	指定 Integrity 服务器连接到 ASA 上的端口 300（默认值为端口 80）以请求服务器 SSL 证书。
步骤 8	**zonelabs-integrity ssl-client-authentication {enable | disable}** **示例：** hostname(config)# zonelabs-integrity ssl-client-authentication enable	尽管始终会对服务器 SSL 证书进行身份验证，但是另请指定对 Integrity 服务器的客户端 SSL 证书进行身份验证。

要将防火墙客户端类型设置为 Zone Labs Integrity 类型，请输入以下命令：

命令	目的
client-firewall {opt | req} zonelabs-integrity **示例：** hostname(config)# client-firewall req zonelabs-integrity	有关详细信息，请参阅第 4-65 页上的配置 VPN 客户端防火墙策略。当防火墙类型为 **zonelabs-integrity** 时，未使用指定防火墙策略的命令参数，因为 Integrity 服务器会确定这些策略。

设置客户端防火墙参数

输入以下命令以设置相应的客户端防火墙参数。只能配置每个命令的一个实例。有关详细信息，请参阅第 4-65 页上的配置 VPN 客户端防火墙策略。

思科集成防火墙

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-integrated acl-in ACL
acl-out ACL
```

思科安全代理

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-security-agent
```

无防火墙

```
hostname(config-group-policy)# client-firewall none
```

自定义防火墙

```
hostname(config-group-policy)# client-firewall {opt | req} custom vendor-id num product-id
num policy {AYT | CPP acl-in ACL acl-out ACL} [description string]
```

Zone Labs 防火墙

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-integrity
```

注　当防火墙类型为 **zonelabs-integrity** 时，请勿包含参数。 Zone Labs Integrity 服务器确定策略。

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarm policy {AYT
| CPP acl-in ACL acl-out ACL}

hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarmorpro policy
{AYT | CPP acl-in ACL acl-out ACL}

client-firewall {opt | req} zonelabs-zonealarmpro policy {AYT | CPP acl-in ACL acl-out
ACL}
```

Sygate 个人防火墙

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal

hostname(config-group-policy)# client-firewall {opt | req} sygate-personal-pro

hostname(config-group-policy)# client-firewall {opt | req} sygate-security-agent
```

Network Ice Black Ice 防火墙：

```
hostname(config-group-policy)# client-firewall {opt | req} networkice-blackice
```

表 4-3　client-firewall 命令关键字和变量

参数	说明
acl-in *ACL*	提供客户端对入站流量使用的策略。
acl-out *ACL*	提供客户端对出站流量使用的策略。
AYT	指定客户端 PC 防火墙应用控制防火墙策略。ASA 会检查以确保防火墙正在运行。它询问 “Are You There?”，如果没有响应，则 ASA 会拆除隧道。
cisco-integrated	指定 Cisco Integrated 防火墙类型。
cisco-security-agent	指定 Cisco Intrusion Prevention Security Agent 防火墙类型。
CPP	指定 Policy Pushed 作为 VPN 客户端防火墙策略源。
custom	指定 Custom 防火墙类型。
description *string*	描述防火墙。
networkice-blackice	指定 Network ICE Black ICE 防火墙类型。
none	指示没有客户端防火墙策略。使用空值设置防火墙策略，从而禁止防火墙策略。防止从默认或指定的组策略继承防火墙策略。
opt	指示可选防火墙类型。
product-id	标识防火墙产品。
req	指示必需防火墙类型。
sygate-personal	指定 Sygate Personal 防火墙类型。

表 4-3　client-firewall 命令关键字和变量 （续）

sygate-personal-pro	指定 Sygate Personal Pro 防火墙类型。
sygate-security-agent	指定 Sygate Security Agent 防火墙类型。
vendor-id	标识防火墙供应商。
zonelabs-integrity	指定 Zone Labs Integrity Server 防火墙类型。
zonelabs-zonealarm	指定 Zone Labs Zone Alarm 防火墙类型。
zonelabs-zonealarmorpro policy	指定 Zone Labs Zone Alarm 或 Pro 防火墙类型。
zonelabs-zonealarmpro policy	指定 Zone Labs Zone Alarm Pro 防火墙类型。

以下示例显示如何为名为 FirstGroup 的组策略设置需要 Cisco Intrusion Prevention Security Agent 的客户端防火墙策略：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
hostname(config-group-policy)#
```

配置客户端访问规则

通过在 group-policy 配置模式下使用 **client-access-rule** 命令来配置用于限制可通过 IPsec 连接至 ASA 的远程访问客户端类型和版本的规则。根据以下准则来制定规则：

- 如果不定义任何规则，则 ASA 将允许所有连接类型。
- 当客户端不与任何规则匹配时， ASA 拒绝连接。如果定义拒绝规则，则还必须定义至少一个允许规则；否则， ASA 将拒绝所有连接。
- 对于软件和硬件客户端，类型和版本必须与其在 **show vpn-sessiondb remote** 显示中的外观完全匹配。
- ***** 字符是通配符，可以在每条规则中多次输入。例如，**client-access rule 3 deny type * version 3.*** 创建会拒绝所有运行版本 3.x 软件的客户端类型的优先级 3 客户端访问规则。
- 每个组策略可以构造最多 25 条规则。
- 整个规则集的字符数限制为 255。
- 对于不发送客户端类型和 / 或版本的客户端可以输入 n/a。

如要删除规则，请输入此命令的 **no** 形式。此命令与以下命令等效：

```
hostname(config-group-policy)# client-access-rule 1 deny type "Cisco VPN Client" version
4.0
```

如要删除所有规则，请输入不带参数的 **no client-access-rule 命令**。这会删除所有已配置的规则，包括空规则 （如果通过输入带有 **none** 关键字的 **client-access-rule** 命令进行了创建）。

默认情况下，没有访问规则。当没有客户端访问规则时，用户将继承默认组策略中存在的任何规则。

如要防止用户继承客户端访问规则，请输入带有 **none** 关键字的 **client-access-rule** 命令。此命令的结果是所有客户端类型和版本都可以进行连接。

```
hostname(config-group-policy)# client-access rule priority {permit | deny} type type
version {version | none}

hostname(config-group-policy)# no client-access rule [priority {permit | deny} type type
version version]
```

表 4-4 说明这些命令中的关键字和参数的含义。

表 4-4　client-access rule 命令关键字和参数

参数	说明
deny	拒绝特定类型和 / 或版本的设备的连接。
none	允许 no client 访问规则。将 client-access-rule 设置为空值，从而允许无限制。防止从默认或指定的组策略继承值。
permit	允许特定类型和 / 或版本的设备的连接。
priority	确定规则的优先级。具有最小整数的规则具有最高优先级。因此，应用的规则是与客户端类型和 / 或版本匹配的具有最低整数的规则。如果较低优先级的规则发生矛盾，则 ASA 会将其忽略。
type *type*	通过自由格式字符串来标识设备，例如 VPN 3002。字符串必须与其在 **show vpn-sessiondb remote** 显示中的外观完全匹配，不同在于可以输入 * 字符作为通配符。
version *version*	通过自由格式字符串来标识设备，例如 7.0。字符串必须与其在 **show vpn-sessiondb remote** 显示中的外观完全匹配，不同在于可以输入 * 字符作为通配符。

以下示例显示如何为名为 FirstGroup 的组策略创建客户端访问规则。这些规则允许运行软件版本 4.x 的 Cisco VPN 客户端，同时拒绝所有 Windows NT 客户端：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 deny type WinNT version *
hostname(config-group-policy)# client-access-rule 2 permit "Cisco VPN Client" version 4.*
```

注　“type”字段是允许任意值的自由格式字符串，但是该值必须与客户端在连接时发送到 ASA 的固定值匹配。

配置无客户端 SSL VPN 会话的组策略属性

通过无客户端 SSL VPN，用户可以使用 Web 浏览器与 ASA 建立安全的远程访问 VPN 隧道。无需软件或硬件客户端。无客户端 SSL VPN 从几乎任何可以访问 HTTPS Internet 站点的计算机提供对范围广泛的 Web 资源和已启用 Web 的应用的轻松访问。无客户端 SSL VPN 使用 SSL 及其后代 TLS1 在远程用户与在中心站点配置的特定受支持内部资源之间提供安全连接。 ASA 识别需要代理的连接，并且 HTTP 服务器会与身份验证子系统交互来对用户进行身份验证。默认情况下，会禁用无客户端 SSL VPN。

可以定制特定内部组策略的无客户端 SSL VPN 的配置。

注　通过从全局配置模式进入的 webvpn 模式，可以配置无客户端 SSL VPN 会话的全局设置。通过本节中描述的 webvpn 模式 （从 group-policy 配置模式进入），可以专门为无客户端 SSL VPN 会话定制组策略的配置。

在 group-policy webvpn 配置模式下，可以指定继承还是定制以下参数，在后续部分中对其中每种情况进行了描述：

- customizations
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- sso server （单点登录服务器）
- auto-signon
- deny message
- AnyConnect Secure Mobility Client
- keep-alive ignore
- HTTP compression

在许多情况下，可在配置无客户端 SSL VPN 的过程中定义 webvpn 属性，然后在配置 group-policy webvpn 属性时将这些定义应用于特定组。通过在 group-policy 配置模式下使用 **webvpn** 命令来进入 group-policy webvpn 配置模式。组策略的 webvpn 命令定义通过无客户端 SSL VPN 会话对文件、 URL 和 TCP 应用的访问。它们还标识 ACL 和要过滤的流量类型。默认情况下会禁用无客户端 SSL VPN。有关配置无客户端 SSL VPN 会话的属性的详细信息，请参阅*第 13 章，“无客户端 SSL VPN 简介”*的描述。

要移除在 group-policy webvpn 配置模式下输入的所有命令，请输入此命令的 **no** 形式。这些 webvpn 命令适用于从其配置这些命令的用户名或组策略。

```
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# no webvpn
```

以下示例显示如何为名为 FirstGroup 的组策略进入 group-policy webvpn 配置模式：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#
```

应用定制

定制确定用户在登录时看到的窗口的外观。可在配置无客户端 SSL VPN 过程中配置定制参数。要应用以前定义的网页定制来更改用户在登录时看到的网页外观，请在 group-policy webvpn 配置模式下输入 customization 命令：

```
hostname(config-group-webvpn)# customization customization_name
hostname(config-group-webvpn)#
```

例如，如要使用名为 blueborder 的定制，请输入以下命令：

```
hostname(config-group-webvpn)# customization blueborder
hostname(config-group-webvpn)#
```

可通过在 webvpn 模式下输入 **customization** 命令来配置定制本身。

以下示例显示一个命令序列，它首先建立名为 123 的定制来定义密码提示。然后，该示例定义名为 testpolicy 的组策略并使用 **customization** 命令指定对无客户端 SSL VPN 会话使用名为 123 的定制：

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# group-policy testpolicy nopassword
hostname(config)# group-policy testpolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# customization value 123
hostname(config-group-webvpn)#
```

指定 “拒绝”消息

可以通过在 group-policy webvpn 配置模式下输入 **deny-message** 命令来指定传递给成功登录到无客户端 SSL VPN 会话中但没有 VPN 特权的远程用户的消息：

```
hostname(config-group-webvpn)# deny-message value "message"
hostname(config-group-webvpn)# no deny-message value "message"
hostname(config-group-webvpn)# deny-message none
```

no deny-message value 命令移除消息字符串，以便远程用户不会接收消息。

no deny-message none 命令从连接配置文件策略配置中移除属性。策略继承属性值。

消息长度可以是最多 491 个字母数字字符，包括特殊字符、空格和标点符号，但是不计入附带的引号。文本在远程用户登录时显示在其浏览器上。在 **deny-message value** 命令中键入字符串时，即使命令换行也请继续键入。

默认拒绝消息为：“Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features.Contact your IT administrator for more information.”

以下示例中的第一个命令创建名为 group2 的内部组策略。后续命令修改属性，包括与该策略关联的 webvpn 拒绝消息。

```
hostname(config)# group-policy group2 internal
hostname(config)# group-policy group2 attributes
hostname(config-group)# webvpn
hostname(config-group-webvpn)# deny-message value "Your login credentials are OK.However,
you have not been granted rights to use the VPN features.Contact your administrator for
more information."
hostname(config-group-webvpn)
```

配置无客户端 SSL VPN 会话的组策略过滤器属性

通过在 webvpn 模式下使用 **html-content-filter** 命令来指定是否从此组策略的无客户端 SSL VPN 会话中过滤 Java、 ActiveX、图像、脚本和 cookie。默认情况下会禁用 HTML 过滤。

要移除内容过滤器，请输入此命令的 **no** 形式。要移除所有内容过滤器，包括通过发出带有 **none** 关键字的 **html-content-filter** 命令创建的空值，请输入不带参数的此命令的 **no** 形式。**no** 选项允许从其他组策略继承值。要防止继承 html 内容过滤器，请输入带有 **none** 关键字的 **html-content-filter** 命令。

再次使用该命令会覆盖以前的设置。

```
hostname(config-group-webvpn)# html-content-filter {java | images | scripts | cookies |
none}

hostname(config-group-webvpn)# no html-content-filter [java | images | scripts | cookies |
none]
```

表 4-5 描述此命令中使用的关键字的含义。

表 4-5　filter 命令关键字

关键字	含义
cookie	从图像中移除 cookie，从而提供有限的广告过滤和隐私。
images	移除对图像的引用 （移除 <IMG> 标记）。
java	移除对 Java 和 ActiveX 的引用 （移除 <EMBED>、 <APPLET> 和 <OBJECT> 标记）。
none	指示没有过滤。设置空值，从而禁止过滤。防止继承过滤值。
scripts	移除对脚本的引用 （移除 <SCRIPT> 标记）

以下示例显示如何为名为 FirstGroup 的组策略设置 Java、 ActiveX、 cookie 和图像的过滤：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# html-content-filter java cookies images
hostname(config-group-webvpn)#
```

指定用户主页

通过在 group-policy webvpn 配置模式下使用 **homepage** 命令来指定当该组中的用户登录时显示的网页的 URL。没有默认主页。

要移除已配置的主页，包括通过发出 **homepage none** 命令创建的空值，请输入此命令的 **no** 形式。**no** 选项允许从其他组策略继承值。要防止继承主页，请输入 **homepage none** 命令。

none 关键字指示无客户端 SSL VPN 会话没有主页。它设置空值，从而禁止主页并防止继承主页。

关键字 **value** 后面的 *url-string* 变量提供主页的 URL。字符串必须以 http:// 或 https:// 开头。

```
hostname(config-group-webvpn)# homepage {value url-string | none}
hostname(config-group-webvpn)# no homepage
hostname(config-group-webvpn)#
```

配置自动登录

auto-signon 命令是无客户端 SSL VPN 会话的用户的单点登录方法。它将登录凭据 （用户名和密码）传递到内部服务器以使用 NTLM 身份验证和 / 或基本身份验证进行身份验证。可以根据输入顺序 （早期命令优先）来输入和处理多个 auto-signon 命令。

可以在三种模式下使用自动登录功能：webvpn 配置、webvpn 组配置或 webvpn 用户名配置模式。典型的优先顺序行为适用，其中用户名取代组，而组取代全局。选择的模式取决于所需的身份验证范围。

要禁用特定用户对特定服务器进行的自动登录，请使用该命令的 **no** 形式及 IP 块或 URI 的原始规范。要禁用身份验证到所有服务器，请使用不带参数的 **no** 形式。 **no** 选项允许从组策略继承值。

在 group-policy webvpn 配置模式下输入的以下示例使用基本身份验证为名为 anyuser 的用户配置对 IP 地址范围为 10.1.1.0 到 10.1.1.255 的服务器的自动登录：

以下示例命令使用基本或 NTLM 身份验证为无客户端 SSL VPN 会话的用户配置对 URI 掩码 https://*.example.com/* 所定义的服务器的自动登录：

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type all
hostname(config-group-webvpn)#
```

以下示例命令使用基本或 NTLM 身份验证为无客户端 SSL VPN 会话的用户配置对 IP 地址为 10.1.1.0 的服务器 （使用子网掩码 255.255.255.0）的自动登录：

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type all
hostname(config-group-webvpn)#
```

指定无客户端 SSL VPN 会话的 ACL

通过在 webvpn 模式下使用 **filter** 命令来指定要用于此组策略或用户名的无客户端 SSL VPN 会话的 ACL。无客户端 SSL VPN ACL 不适用，直到输入 **filter** 命令将其指定为止。

如要移除 ACL，包括通过发出 **filter none** 命令创建的空值，请输入此命令的 **no** 形式。 **no** 选项允许从其他组策略继承值。要防止继承过滤器值，请输入 **filter value none** 命令。

无客户端 SSL VPN 会话的 ACL 不适用，直到输入 **filter** 命令将其指定为止。

可将 ACL 配置为允许或拒绝此组策略的各种类型的流量。然后，输入 **filter** 命令以对无客户端 SSL VPN 流量应用这些 ACL。

```
hostname(config-group-webvpn)# filter {value ACLname | none}
hostname(config-group-webvpn)# no filter
```

none 关键字指示没有 **webvpntype** ACL。它设置空值，从而禁止 ACL 并防止从其他组策略继承 ACL。

关键字 **value** 后面的 *ACLname* 字符串提供以前配置的 ACL 的名称。

注　无客户端 SSL VPN 会话不使用 **vpn-filter** 命令中定义的 ACL。

以下示例显示如何为名为 FirstGroup 的组策略设置调用名为 *acl_in* 的 ACL 的过滤器：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# filter acl_in
hostname(config-group-webvpn)#
```

应用 URL 列表

可以为组策略指定要在无客户端 SSL VPN 主页上显示的 URL 列表。首先，必须通过在全局配置模式下输入 **url-list** 命令来创建一个或多个指定列表。要将无客户端 SSL VPN 会话的服务器和 URL 的列表应用于特定组策略，从而允许访问特定组策略列表中的 URL，请使用在 group-policy webvpn 配置模式下通过 **url-list** 命令创建的一个或多个列表的名称。没有默认 URL 列表。

如要移除列表，包括通过使用 **url-list none** 命令创建的空值，请使用此命令的 **no** 形式。 **no** 选项允许从其他组策略继承值。如要防止继承 URL 列表，请使用 **url-list none** 命令。再次使用该命令会覆盖以前的设置：

```
hostname(config-group-webvpn)# url-list {value name | none} [index]
hostname(config-group-webvpn)# no url-list
```

表 4-6 显示 **url-list** 命令参数及其含义。

表 4-6　url-list 命令关键字和变量

参数	含义
index	指示主页上的显示优先级。
none	为 URL 列表中设置空值。防止从默认或指定的组策略继承列表。
value *name*	指定以前配置的 URL 列表的名称。要配置此类列表，请在全局配置模式下使用 **url-list** 命令。

以下示例为名为 FirstGroup 的组策略设置名为 FirstGroupURLs 的 URL，并指定这应是主页上显示的第一个 URL 列表：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# url-list value FirstGroupURLs 1
hostname(config-group-webvpn)#
```

启用组策略的 ActiveX 中继

通过 ActiveX 中继，已建立无客户端 SSL VPN 会话的用户可以使用浏览器来启动 Microsoft Office 应用。应用使用会话下载和上传 Microsoft Office 文档。 ActiveX 中继保持生效，直到无客户端 SSL VPN 会话关闭为止。

如要在无客户端 SSL VPN 会话上启用或禁用 ActiveX 控件，请在 group-policy webvpn 配置模式下输入以下命令：

activex-relay {**enable** | **disable**}

如要从默认组策略继承 **activex-relay** 命令，请输入以下命令：

no activex-relay

以下命令在与给定组策略关联的无客户端 SSL VPN 会话上启用 ActiveX 控件：

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# activex-relay enable
hostname(config-group-webvpn)
```

在组策略的无客户端 SSL VPN 会话上启用应用访问

如要为此组策略启用应用访问，请在 group-policy webvpn 配置模式下输入 **port-forward** 命令。默认情况下会禁用端口转发。

必须先定义希望用户能够在无客户端 SSL VPN 会话中使用的应用列表，然后才能在 group-policy webvpn 配置模式下输入 **port-forward** 命令来启用应用访问。在全局配置模式下输入 **port-forward** 命令以定义此列表。

如要从 group-policy 配置中移除端口转发属性，包括通过发出 **port-forward none** 命令创建的空值，请输入此命令的 **no** 形式。 **no** 选项允许从其他组策略继承列表。如要防止继承端口转发列表，请输入带有 **none** 关键字的 **port-forward** 命令。 **none** 关键字指示没有过滤。它设置空值，从而禁止过滤，并防止继承过滤值。

此命令的语法如下：

```
hostname(config-group-webvpn)# port-forward {value listname | none}
hostname(config-group-webvpn)# no port-forward
```

关键字 **value** 后面的 *listname* 字符串标识无客户端 SSL VPN 会话的用户可访问的应用列表。在 webvpn 配置模式下输入 port-forward 命令以定义该列表。

再次使用该命令会覆盖以前的设置。

以下示例显示如何为名为 FirstGroup 的内部组策略设置名为 *ports1* 的端口转发列表：

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward value ports1
hostname(config-group-webvpn)#
```

配置端口转发显示名称

通过在 group-policy webvpn 配置模式下使用 **port-forward-name** 命令来为特定用户或组策略配置用于向最终用户标识 TCP 端口转发的显示名称。如要删除显示名称，包括通过使用 **port-forward-name none** 命令创建的空值，请输入该命令的 **no** 形式。 **no** 选项还原默认名称 Application Access。如要防止使用显示名称，请输入 **port-forward none** 命令。此命令的语法如下：

```
hostname(config-group-webvpn)# port-forward-name {value name | none}
hostname(config-group-webvpn)# no port-forward-name
```

以下示例显示如何为名为 *FirstGroup* 的内部组策略设置名称 Remote Access TCP Applications：

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
hostname(config-group-webvpn)#
```

配置为更新会话计时器而要忽略的最大对象大小

网络设备交换简短保活消息以确保其之间的虚拟回路仍然处于活动状态。这些消息的长度各异。通过 **keep-alive-ignore** 命令，可以指示 ASA 在更新会话计时器时将小于或等于指定大小的所有消息都视为保活消息而非流量。范围为 0 至 900 KB。默认值为 4 KB。

如要指定每个事务的将忽略的 HTTP/HTTPS 流量的上限，请在 group-policy attributes webvpn 配置模式下使用 **keep-alive-ignore** 命令：

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#
```

```
该命令的 no 形式会从配置中移除此规范：
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

以下示例将要忽略的最大对象大小设置为 5 KB：

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

指定 HTTP 压缩

通过在 group-policy webvpn 配置模式下输入 **http-comp** 命令来通过特定组或用户的无客户端 SSL VPN 会话启用 http 数据压缩。

```
hostname(config-group-webvpn)# http-comp {gzip | none}
hostname(config-group-webvpn)#
```

如要从配置中移除该命令并导致继承值，请使用该命令的 **no** 形式：

```
hostname(config-group-webvpn)# no http-comp {gzip | none}
hostname(config-group-webvpn)#
```

此命令的语法如下：

- **gzip** — 指定对组或用户启用压缩。这是默认值。
- **none** — 指定对组或用户禁用压缩。

对于无客户端 SSL VPN 会话，从全局配置模式配置的 **compression** 命令会覆盖在 group-policy 和 username webvpn 模式下配置的 **http-comp** 命令。

在以下示例中，为组策略 sales 禁用了压缩：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# http-comp none
hostname(config-group-webvpn)#
```

指定 SSO 服务器

通过仅适用于无客户端 SSL VPN 会话的单点登录支持，用户可以访问不同服务器上的不同安全服务，而不必多次重新输入用户名和密码。通过在 group-policy-webvpn 模式下输入的 **sso-server value** 命令，可以向组策略分配 SSO 服务器。

如要向组策略分配 SSO 服务器，请在 group-policy-webvpn 配置模式下使用 **sso-server value** 命令。此命令要求配置包含 CA SiteMinder 命令。

```
hostname(config-group-webvpn)# sso-server value server_name
hostname(config-group-webvpn)#
```

如要移除分配并使用默认策略，请使用此命令的 **no** 形式。要防止继承默认策略，请使用 **sso-server none** 命令。

```
hostname(config-group-webvpn)# sso-server {value server_name | none}
hostname(config-group-webvpn)# [no] sso-server value server_name
```

分配给 SSO 服务器的默认策略为 DfltGrpPolicy。

以下示例创建组策略 “my-sso-grp-pol”并将其分配给名为 “example”的 SSO 服务器：

```
hostname(config)# group-policy my-sso-grp-pol internal
hostname(config)# group-policy my-sso-grp-pol attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# sso-server value example
hostname(config-group-webvpn)#
```

配置用户属性

本节描述用户属性及其配置方式。其中包含以下各节：

默认情况下，用户从分配的组策略继承所有用户属性。 ASA 还允许在用户级别分配单独属性，从而覆盖应用于该用户的组策略中的值。例如，可以指定在业务时间提供所有用户访问的组策略，但是为特定用户提供 24 小时的访问。

查看用户名配置

如要显示所有用户名的配置，包括从组策略继承的默认值，请输入 **all** 关键字以及 **show running-config username** 命令，如下所示：

```
hostname# show running-config all username
hostname#
```

这显示所有用户或 （如果提供用户名）该特定用户的。加密密码和特权级别。如果省略 **all** 关键字，则此列表中仅显示显式配置的值。以下示例为名为 testuser 的用户显示此命令的输出：

```
hostname# show running-config all username testuser
username testuser password 12RsxXQnphyr/I9Z encrypted privilege 15
```

配置个人用户的属性

如要配置特定用户，可以使用 **username** 命令 （进入 username 模式）向用户分配密码 （或无密码）和属性。没有指定的任何属性都继承自组策略。

内部用户身份验证数据库由使用 **username** 命令输入的用户的组成。 **login** 命令使用此数据库进行身份验证。要向 ASA 数据库中添加用户，请在全局配置模式下输入 **username** 命令。要移除用户，请使用带有要移除的用户名的此命令的 **no** 版本。要移除所有用户名，请使用 **clear configure username** 命令而不附加用户名。

设置用户密码和特权级别

输入 **username** 命令来为用户分配密码和特权级别。可以输入 **nopassword** 关键字以指定此用户不需要密码。如果确实指定密码，则可以指定该密码是否以加密形式存储。

通过可选的 **privilege** 关键字可设置此用户的特权级别。特权级别的范围为 0 （最低）至 15。系统管理员通常具有最高特权级别。默认级别为 2。

```
hostname(config)# username name {nopassword | password password [encrypted]} [privilege priv_level]}

hostname(config)# no username [name]
```

表 4-7 描述此命令中使用的关键字和变量的含义。

表 4-7　username 命令关键字和变量

关键字 / 变量	含义
encrypted	指示密码已加密。
name	提供用户的名称。
nopassword	指示此用户无需密码。
password *password*	指示此用户具有密码，并提供该密码。
privilege *priv_level*	设置此用户的特权级别。范围为 0 至 15，其中最低的数字使用命令和管理 ASA 的能力最小。默认特权级别为 2。系统管理员的典型特权级别为 15。

默认情况下，使用此命令添加的 VPN 用户没有属性或组策略关联。必须显式配置所有值。

以下示例显示如何使用加密密码 pw_12345678 和特权级别 12 来配置名为 anyuser 的用户：

```
hostname(config)# username anyuser password pw_12345678 encrypted privilege 12
hostname(config)#
```

配置用户属性

配置用户的密码 （如果有）和特权级别后，可设置其他属性。这些属性可以为任何顺序。要移除任何属性 / 值对，请输入该命令的 **no** 形式。

通过输入带有 **attributes** 关键字的 **username** 命令来进入 username 模式：

```
hostname(config)# username name attributes
hostname(config-username)#
```

提示符会更改以指示新模式。现在可以配置属性。

配置 VPN 用户属性

VPN 用户属性设置特定于 VPN 连接的值，如以下各节中所述。

配置继承

可以使用户从组策略继承尚未在用户名级别配置的属性值。要指定此用户从其继承属性的组策略的名称，请输入 **vpn-group-policy** 命令。默认情况下， VPN 用户没有 group-policy 关联：

```
hostname(config-username)# vpn-group-policy group-policy-name
hostname(config-username)# no vpn-group-policy group-policy-name
```

对于在 username 模式下可用的属性，可以通过在 username 模式下配置该属性来覆盖特定用户的组策略中的属性值。

以下示例显示如何配置名为 anyuser 的用户以使用名为 FirstGroup 的组策略中的属性：

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
hostname(config-username)#
```

配置访问时间

通过指定已配置的时间范围策略的名称来关联允许此用户访问系统的时间。

如要从运行配置中移除属性，请输入此命令的 **no** 形式。此选项允许从其他组策略继承时间范围值。如要防止继承值，请输入 **vpn-access-hours none** 命令。默认值为不受限制的访问。

```
hostname(config-username)# vpn-access-hours value {time-range | none}
hostname(config-username)# vpn-access-hours value none
hostname(config)#
```

以下示例显示如何将名为 anyuser 的用户与名为 824 的时间范围策略关联：

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-access-hours 824
hostname(config-username)#
```

配置最大同时登录数

指定为此用户允许的最大同时登录数。范围为 0 至 2147483647。默认为 3 个同时登录。要从运行配置中移除属性，请输入此命令的 **no** 形式。输入 0 以禁用登录并阻止用户访问。

```
hostname(config-username)# vpn-simultaneous-logins integer
hostname(config-username)# no vpn-simultaneous-logins
hostname(config-username)# vpn-session-timeout alert-interval none
```

注　尽管同时登录数的最大限制非常大，但是允许若干同时登录可能会危害安全并影响性能。

以下示例显示如何对名为 anyuser 的用户允许最多 4 个同时登录：

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-simultaneous-logins 4
hostname(config-username)#
```

配置空闲超时

指定空闲超时期 （以分钟为单位），或者输入 **none** 以禁用空闲超时。如果在此期间连接上没有通信活动，则 ASA 会终止连接。可以选择性设置警报间隔，或者保持默认值为一分钟。

范围为 1 至 35791394 分钟。默认值为 30 分钟。如要允许无限超时期，并因此防止继承超时值，请输入带有 **none** 关键字的 **vpn-idle-timeout** 命令。要从运行配置中移除属性，请输入此命令的 **no** 形式。

```
hostname(config-username)# vpn-idle-timeout {minutes | none} alert-interval {minutes}
hostname(config-username)# no vpn-idle-timeout alert-interval
hostname(config-username)# vpn-idle-timeout alert-interval none
```

以下示例显示如何为名为 anyuser 的用户设置 15 分钟的 VPN 空闲超时和 3 分钟的警报间隔：

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout 30 alert-interval 3
hostname(config-username)#
```

设置最长连接时间

指定最长用户连接时间 （以分钟为单位），或者输入 **none** 以允许无限连接时间并防止继承此属性的值。此时间段结束时， ASA 终止连接。可以选择性设置警报间隔，或者保持默认值为一分钟。

范围为 1 至 35791394 分钟。没有默认超时。如要允许无限超时期，并因此防止继承超时值，请输入带有 **none** 关键字的 **vpn-session-timeout** 命令。如要从运行配置中移除属性，请输入此命令的 **no** 形式。

```
hostname(config-username)# vpn-session-timeout {minutes | none} alert-interval {minutes}
hostname(config-username)# no vpn-session-timeout alert-interval
hostname(config-username)#
```

以下示例显示如何为名为 anyuser 的用户设置 180 分钟的 VPN 会话超时：

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180 alert-interval {minutes}
hostname(config-username)#
```

应用 ACL 过滤器

指定要用作 VPN 连接过滤器的以前配置的特定于用户的 ACL 的名称。要禁止 ACL 并防止从组策略继承 ACL，请输入带有 none 关键字的 **vpn-filter** 命令。要移除 ACL，包括通过发出 **vpn-filter none** 命令创建的空值，请输入此命令的 **no** 形式。 **no** 选项允许从组策略继承值。此命令没有默认行为或值。

可将 ACL 配置为允许或拒绝此用户的各种类型的流量。然后，使用 **vpn-filter** 命令以应用这些 ACL。

```
hostname(config-username)# vpn-filter {value ACL_name | none}
hostname(config-username)# no vpn-filter
hostname(config-username)#
```

注　无客户端 SSL VPN 不使用 **vpn-filter** 命令中定义的 ACL。

以下示例显示如何为名为 anyuser 的用户设置调用名为 acl_vpn 的 ACL 的过滤器：

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-filter value acl_vpn
hostname(config-username)#
```

指定 IPv4 地址和网络掩码

指定要分配给特定用户的 IP 地址和网络掩码。要移除 IP 地址，请输入此命令的 **no** 形式。

```
hostname(config-username)# vpn-framed-ip-address {ip_address}
hostname(config-username)# no vpn-framed-ip-address
hostname(config-username)
```

以下示例显示如何为名为 anyuser 的用户设置 IP 地址 10.92.166.7：

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
hostname(config-username)
```

指定要与上一步中指定的 IP 地址配合使用的网络掩码。如果使用了 **no vpn-framed-ip-address** 命令，请勿指定网络掩码。要移除子网掩码，请输入此命令的 **no** 形式。没有默认行为或值。

```
hostname(config-username)# vpn-framed-ip-netmask {netmask}
hostname(config-username)# no vpn-framed-ip-netmask
hostname(config-username)
```

以下示例显示如何为名为 anyuser 的用户设置 子网掩码 255.255.255.254：

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
hostname(config-username)
```

指定 IPv6 地址和网络掩码

指定要分配给特定用户的 IPv6 地址和网络掩码。要移除 IP 地址，请输入此命令的 **no** 形式。

```
hostname(config-username)# vpn-framed-ipv6-address {ip_address}
hostname(config-username)# no vpn-framed-ipv6-address
hostname(config-username)
```

以下示例显示如何为名为 anyuser 的用户设置 IP 地址和网络掩码 2001::3000:1000:2000:1/64。此地址指示前缀值 2001:0000:0000:0000 和接口 ID 3000:1000:2000:1。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ipv6-address 2001::3000:1000:2000:1/64
hostname(config-username)
```

指定隧道协议

指定此用户可以使用的 VPN 隧道类型 （IPsec 或无客户端 SSL VPN）。默认值获取自默认组策略，其默认值为 IPsec。要从运行配置中移除属性，请输入此命令的 **no** 形式。

```
hostname(config-username)# vpn-tunnel-protocol {webvpn | IPsec}
hostname(config-username)# no vpn-tunnel-protocol [webvpn | IPsec]
hostname(config-username)
```

此命令的参数值如下：

- **IPsec** — 在两个对等体 （远程访问客户端或其他安全网关）之间协商 IPsec 隧道。创建监管身份验证、加密、封装和密钥管理的安全关联。
- **webvpn** — 通过已启用 HTTPS 的 Web 浏览器向远程用户提供无客户端 SSL VPN 访问，并且无需客户端。

输入此命令以配置一个或多个隧道模式。必须配置至少一个隧道模式以使用户通过 VPN 隧道进行连接。

以下示例显示如何为名为 anyuser 的用户配置无客户端 SSL VPN 和 IPsec 隧道模式：

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-tunnel-protocol webvpn
hostname(config-username)# vpn-tunnel-protocol IPsec
hostname(config-username)
```

限制远程用户访问

使用 **value** 关键字配置 **group-lock** 属性以限制远程用户仅通过指定的预先存在的连接配置文件进行访问。组锁定通过检查在 VPN 客户端中配置的组是否与用户分配到的连接配置文件相同来限制用户。如果不相同，则 ASA 会阻止用户进行连接。如果不配置组锁定，则 ASA 在不考虑分配的组的情况下对用户进行身份验证。

如要从运行配置中移除 **group-lock** 属性，请输入此命令的 no 形式。此选项允许从组策略继承值。要禁用 group-lock 并防止从默认或指定的组策略继承 group-lock 值，请输入带有 **none** 关键字的 **group-lock** 命令。

```
hostname(config-username)# group-lock {value tunnel-grp-name | none}
hostname(config-username)# no group-lock
hostname(config-username)
```

以下示例显示如何为名为 anyuser 的用户设置组锁定：

```
hostname(config)# username anyuser attributes
hostname(config-username)# group-lock value tunnel-group-name
hostname(config-username)
```

为软件客户端用户启用密码存储

指定是否允许用户在客户端系统上存储其登录密码。默认情况下会禁用密码存储。仅在已知处于安全站点中的系统上启用密码存储。如要禁用密码存储，请输入带有 **disable** 关键字的 **password-storage** 命令。如要从运行配置中移除 password-storage 属性，请输入此命令的 **no** 形式。这允许从组策略继承 password-storage 的值。

```
hostname(config-username)# password-storage {enable | disable}
hostname(config-username)# no password-storage
hostname(config-username)
```

此命令不适用于交互式硬件客户端身份验证或硬件客户端的个人用户身份验证。

以下示例显示如何为名为 anyuser 的用户启用密码存储：

```
hostname(config)# username anyuser attributes
hostname(config-username)# password-storage enable
hostname(config-username)
```

配置特定用户的无客户端 SSL VPN 访问

以下各节描述如何定制无客户端 SSL VPN 会话的特定用户的配置。通过在 username 配置模式下使用 **webvpn** 命令来进入 username webvpn 配置模式。通过无客户端 SSL VPN，用户可以使用 Web 浏览器与 ASA 建立安全的远程访问 VPN 隧道。无需软件或硬件客户端。无客户端 SSL VPN 从几乎任何可以访问 HTTPS Internet 站点的计算机提供对范围广泛的 Web 资源和已启用 Web 的应用的轻松访问。无客户端 SSL VPN 使用 SSL 及其后代 TLS1 在远程用户与在中心站点配置的特定受支持内部资源之间提供安全连接。ASA 识别需要代理的连接，并且 HTTP 服务器会与身份验证子系统交互来对用户进行身份验证。

username webvpn 配置模式命令定义通过无客户端 SSL VPN 会话对文件、 URL 和 TCP 应用的访问。它们还标识 ACL 和要过滤的流量类型。默认情况下会禁用无客户端 SSL VPN。这些 webvpn 命令仅适用于从其配置这些命令的用户名。请注意，提示符会更改，指示您现在处于 username webvpn 配置模式。

```
hostname(config-username)# webvpn
hostname(config-username-webvpn)#
```

如要移除在 username webvpn 配置模式下输入的所有命令，请输入此命令的 **no** 形式。

```
hostname(config-username)# no webvpn
hostname(config-username)#
```

无需将无客户端 SSL VPN 配置为使用邮件代理。

注　通过从全局配置模式进入的 webvpn 模式，可以配置无客户端 SSL VPN 会话的全局设置。通过本节中描述的 username webvpn 配置模式（从 username 模式进入），可以专门为无客户端 SSL VPN 会话定制特定用户的配置。

在 username webvpn 配置模式下，可以定制以下参数，后续步骤中对其中每个参数进行了描述：

- customizations
- deny message
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- sso server （单点登录服务器）
- auto-signon
- AnyConnect Secure Mobility Client
- keep-alive ignore
- HTTP compression

以下示例显示如何进入 username anyuser attributes 的 username webvpn 配置模式：

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)#
```

指定要从 HTML 过滤的内容 / 对象

如要过滤此用户的无客户端 SSL VPN 会话的 Java、 ActiveX、图像、脚本和 cookie，请在 username webvpn 配置模式下输入 **html-content-filter** 命令。如要移除内容过滤器，请输入此命令的 **no** 形式。如要移除所有内容过滤器，包括通过发出 **html-content-filter none** 命令创建的空值，请输入不带参数的此命令的 **no** 形式。 **no** 选项允许从组策略继承值。如要防止继承 HTML 内容过滤器，请输入 **html-content-filter none** 命令。默认情况下会禁用 HTML 过滤。

再次使用该命令会覆盖以前的设置。

```
hostname(config-username-webvpn)# html-content-filter {java | images | scripts | cookies |
none}

hostname(config-username-webvpn)# no html-content-filter [java | images | scripts |
cookies | none]
```

此命令中使用的关键字如下：

- **cookies** — 从图像中移除 cookie，从而提供有限的广告过滤和隐私。
- **images** — 移除对图像的引用 （移除 <IMG> 标记）。
- **java** — 移除对 Java 和 ActiveX 的引用（移除 <EMBED>、<APPLET> 和 <OBJECT> 标记）。
- **none** — 指示没有过滤。设置空值，从而禁止过滤。防止继承过滤值。
- **scripts** — 移除对脚本的引用 （移除 <SCRIPT> 标记）。

以下示例显示如何为名为 anyuser 的用户设置 Java、 ActiveX、 cookie 和图像的过滤：

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# html-content-filter java cookies images
hostname(config-username-webvpn)#
```

指定用户主页

如要指定在此用户登录到无客户端 SSL VPN 会话中时显示的网页的 URL，请在 username webvpn 配置模式下输入 **homepage** 命令。如要移除已配置的主页，包括通过发出 **homepage none** 命令创建的空值，请输入此命令的 **no** 形式。 **no** 选项允许从组策略继承值。要防止继承主页，请输入 **homepage none** 命令。

none 关键字指示没有无客户端 SSL VPN 主页。它设置空值，从而禁止主页并防止继承主页。

关键字 **value** 后面的 *url-string* 变量提供主页的 URL。字符串必须以 http:// 或 https:// 开头。

没有默认主页。

```
hostname(config-username-webvpn)# homepage {value url-string | none}
hostname(config-username-webvpn)# no homepage
hostname(config-username-webvpn)#
```

以下示例显示如何将 www.example.com 指定为名为 anyuser 的用户的主页：

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# homepage value www.example.com
hostname(config-username-webvpn)#
```

应用定制

定制确定用户在登录时看到的窗口的外观。可在配置无客户端 SSL VPN 过程中配置定制参数。如要应用以前定义的网页定制来更改用户在登录时看到的网页外观，请在 username webvpn 配置模式下输入定制命令：

```
hostname(config-username-webvpn)# customization {none | value customization_name}
hostname(config-username-webvpn)#
```

例如，如要使用名为 blueborder 的定制，请输入以下命令：

```
hostname(config-username-webvpn)# customization value blueborder
hostname(config-username-webvpn)#
```

可通过在 webvpn 模式下输入 **customization** 命令来配置定制本身。

以下示例显示一个命令序列，它首先建立名为 123 的定制来定义密码提示。然后，该示例定义名为 test 的隧道组，并使用 **customization** 命令指定使用名为 123 的定制：

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# username testuser nopassword
hostname(config)# username testuser attributes
hostname(config-username-webvpn)# webvpn
hostname(config-username-webvpn)# customization value 123
hostname(config-username-webvpn)#
```

指定 “拒绝”消息

可以通过在 username webvpn 配置模式下输入 **deny-message** 命令来指定传递给成功登录到无客户端 SSL VPN 会话中但没有 VPN 特权的远程用户的消息：

```
hostname(config-username-webvpn)# deny-message value "message"
hostname(config-username-webvpn)# no deny-message value "message"
hostname(config-username-webvpn)# deny-message none
```

no deny-message value 命令移除消息字符串，以便远程用户不会接收消息。

no deny-message none 命令从连接配置文件策略配置中移除属性。策略继承属性值。

消息长度可以是最多 491 个字母数字字符，包括特殊字符、空格和标点符号，但是不计入附带的引号。文本在远程用户登录时显示在其浏览器上。在 **deny-message value** 命令中键入字符串时，即使命令换行也请继续键入。

默认拒绝消息为：“Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features.Contact your IT administrator for more information.”

以下示例中的第一个命令进入 username 模式并配置名为 anyuser 的用户的属性。后续命令进入 username webvpn 配置模式并修改与该用户关联的拒绝消息。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# deny-message value "Your login credentials are
OK.However, you have not been granted rights to use the VPN features.Contact your
administrator for more information."
hostname(config-username-webvpn)
```

指定无客户端 SSL VPN 会话的 ACL

如要指定将用于此用户的无客户端 SSL VPN 会话的 ACL 的名称，请在 username webvpn 配置模式下输入 **filter** 命令。如要移除 ACL，包括通过发出 **filter none** 命令创建的空值，请输入此命令的 **no** 形式。 **no** 选项允许从组策略继承值。要防止继承过滤器值，请输入 **filter value none** 命令。

无客户端 SSL VPN ACL 不适用，直到输入 **filter** 命令将其指定为止。

可将 ACL 配置为允许或拒绝此用户的各种类型的流量。然后，输入 **filter** 命令以对无客户端 SSL VPN 流量应用这些 ACL。

```
hostname(config-username-webvpn)# filter {value ACLname | none}
hostname(config-username-webvpn)# no filter
hostname(config-username-webvpn)#
```

none 关键字指示没有 **webvpntype** ACL。它设置空值，从而禁止 ACL 并防止从其他组策略继承 ACL。

关键字 **value** 后面的 *ACLname* 字符串提供以前配置的 ACL 的名称。

注　无客户端 SSL VPN 不使用 **vpn-filter** 命令中定义的 ACL。

以下示例显示如何为名为 anyuser 的用户设置调用名为 *acl_in* 的 ACL 的过滤器：

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# filter acl_in
hostname(config-username-webvpn)#
```

应用 URL 列表

可以为已建立无客户端 SSL VPN 会话的用户指定要在主页上显示的 URL 的列表。首先，必须通过在全局配置模式下输入 **url-list** 命令来创建一个或多个指定列表。如要将服务器和 URL 的列表应用于无客户端 SSL VPN 的特定用户，请在 username webvpn 配置模式下输入 **url-list** 命令。

如要移除列表，包括通过使用 **url-list none** 命令创建的空值，请输入此命令的 **no** 形式。 **no** 选项允许从组策略继承值。如要防止继承 URL 列表，请使用 **url-list none** 命令。

```
hostname(config-username-webvpn)# url-list {listname displayname url | none}
hostname(config-username-webvpn)# no url-list
```

此命令中使用的关键字和变量如下：

- *displayname* — 指定 URL 的名称。此名称显示在无客户端 SSL VPN 会话中的门户页上。
- *listname* — 标识要按其对 URL 进行分组的名称。
- **none** — 指示没有 URL 列表。设置空值，从而禁止 URL 列表。防止继承 URL 列表值。
- *url* — 指定无客户端 SSL VPN 的用户可访问的 URL。

没有默认 URL 列表。

再次使用该命令会覆盖以前的设置。

以下示例显示如何为名为 anyuser 的用户设置名为 AnyuserURLs 的 URL 列表：

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# url-list value AnyuserURLs
hostname(config-username-webvpn)#
```

为用户启用 ActiveX 中继

通过 ActiveX 中继，已建立无客户端 SSL VPN 会话的用户可以使用浏览器来启动 Microsoft Office 应用。应用使用会话下载和上传 Microsoft Office 文档。 ActiveX 中继保持生效，直到无客户端 SSL VPN 会话关闭为止。

要在无客户端 SSL VPN 会话上启用或禁用 ActiveX 控件，请在 username webvpn 配置模式下输入以下命令：

activex-relay {**enable** | **disable**}

要从组策略继承 **activex-relay** 命令，请输入以下命令：

no activex-relay

以下命令在与给定用户名关联的无客户端 SSL VPN 会话上启用 ActiveX 控件：

```
hostname(config-username-policy)# webvpn
hostname(config-username-webvpn)# activex-relay enable
hostname(config-username-webvpn)
```

启用无客户端 SSL VPN 会话的应用访问

如要为此用户启用应用访问，请在 username webvpn 配置模式下输入 **port-forward** 命令。默认情况下会禁用端口转发。

如要从配置中移除端口转发属性，包括通过发出 **port-forward none** 命令创建的空值，请输入此命令的 **no** 形式。 **no** 选项允许从组策略继承列表。如要禁止过滤并防止继承端口转发列表，请输入带有 **none** 关键字的 **port-forward** 命令。

```
hostname(config-username-webvpn)# port-forward {value listname | none}
hostname(config-username-webvpn)# no port-forward
hostname(config-username-webvpn)#
```

关键字 **value** 后面的 *listname* 字符串标识无客户端 SSL VPN 的用户可访问的应用列表。在配置模式下输入 **port-forward** 命令以定义该列表。

再次使用该命令会覆盖以前的设置。

必须先定义希望用户能够在无客户端 SSL VPN 会话中使用的应用列表，然后才能在 username webvpn 配置模式下输入 **port-forward** 命令来启用应用访问。在全局配置模式下输入 **port-forward** 命令以定义此列表。

以下示例显示如何配置名为 ports1 的端口转发列表：

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward value ports1
hostname(config-username-webvpn)#
```

配置端口转发显示名称

通过在 username webvpn 配置模式下使用 **port-forward-name** 命令来为特定用户配置用于向最终用户标识 TCP 端口转发的显示名称。如要删除显示名称，包括通过使用 **port-forward-name none** 命令创建的空值，请输入该命令的 **no** 形式。 **no** 选项还原默认名称 Application Access。要防止使用显示名称，请输入 **port-forward none** 命令。

```
hostname(config-username-webvpn)# port-forward-name {value name | none}
hostname(config-username-webvpn)# no port-forward-name
```

以下示例显示如何配置端口转发名称 test：

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward-name value test
hostname(config-username-webvpn)#
```

配置为更新会话计时器而要忽略的最大对象大小

网络设备交换简短保活消息以确保其之间的虚拟回路仍然处于活动状态。这些消息的长度各异。通过 **keep-alive-ignore** 命令，可以指示 ASA 在更新会话计时器时将小于或等于指定大小的所有消息都视为保活消息而非流量。范围为 0 至 900 KB。默认值为 4 KB。

如要指定每个事务的将忽略的 HTTP/HTTPS 流量的上限，请在 group-policy attributes webvpn 配置模式下使用 **keep-alive-ignore** 命令：

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#
```

该命令的 no 形式会从配置中移除此规范：

```
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

以下示例将要忽略的最大对象大小设置为 5 KB：

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

配置自动登录

要使用 NTLM 和 / 或基本 HTTP 身份验证自动将无客户端 SSL VPN 的特定用户的登录凭据提交到内部服务器，请在 username webvpn 配置模式下使用 **auto-signon** 命令。

auto-signon 命令是无客户端 SSL VPN 会话的用户的单点登录方法。它将登录凭据 （用户名和密码）传递到内部服务器以使用 NTLM 身份验证和 / 或基本身份验证进行身份验证。可以根据输入顺序 （早期命令优先）来输入和处理多个 auto-signon 命令。

可以在三种模式下使用自动登录功能：webvpn 配置、webvpn 组配置或 webvpn 用户名配置模式。典型的优先顺序行为适用，其中用户名取代组，而组取代全局。选择的模式将取决于所需的身份验证范围。

如要禁用特定用户对特定服务器进行的自动登录，请使用该命令的 **no** 形式及 IP 块或 URI 的原始规范。要禁用身份验证到所有服务器，请使用不带参数的 **no** 形式。 **no** 选项允许从组策略继承值。

以下示例命令使用基本或 NTLM 身份验证为名为 anyuser 的无客户端 SSL VPN 会话用户配置对 URI 掩码 https://*.example.com/* 所定义的服务器的自动登录：

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow uri https://*.example.com/* auth-type
all
```

以下示例命令使用基本或 NTLM 身份验证为名为 anyuser 的无客户端 SSL VPN 会话用户配置对 IP 地址为 10.1.1.0 的服务器 （使用子网掩码 255.255.255.0）的自动登录：

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type
all
hostname(config-username-webvpn)#
```

指定 HTTP 压缩

通过在 username webvpn 配置模式下输入 **http-comp** 命令来通过特定用户的无客户端 SSL VPN 会话启用 http 数据压缩。

```
hostname(config-username-webvpn)# http-comp {gzip | none}
hostname(config-username-webvpn)#
```

如要从配置中移除该命令并导致继承值，请使用该命令的 **no** 形式：

```
hostname(config-username-webvpn)# no http-comp {gzip | none}
hostname(config-username-webvpn)#
```

此命令的语法如下：

- **gzip** — 指定对组或用户启用压缩。这是默认值。
- **none** — 指定对组或用户禁用压缩。

对于无客户端 SSL VPN 会话，从全局配置模式配置的 **compression** 命令会覆盖在 group-policy 和 username webvpn 模式下配置的 **http-comp** 命令。

在以下示例中，对用户名 testuser 禁用了压缩：

```
hostname(config)# username testuser internal
hostname(config)# username testuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# http-comp none
hostname(config-username-webvpn)#
```

指定 SSO 服务器

通过仅适用于无客户端 SSL VPN 会话的单点登录支持，用户可以访问不同服务器上的不同安全服务，而不必多次重新输入用户名和密码。通过在 username-webvpn 模式下输入的 **sso-server value** 命令，可以向用户分配 SSO 服务器。

如要向用户分配 SSO 服务器，请在 username-webvpn 配置模式下使用 **sso-server value** 命令。此命令要求配置包含 CA SiteMinder 命令。

```
hostname(config-username-webvpn)# sso-server value server_name
hostname(config-username-webvpn)#
```

如要移除分配并使用默认策略，请使用此命令的 **no** 形式。如要防止继承默认策略，请使用 **sso-server none** 命令。

```
hostname(config-username-webvpn)# sso-server {value server_name | none}
hostname(config-username-webvpn)# [no] sso-server value server_name
```

分配给 SSO 服务器的默认策略为 DfltGrpPolicy。

以下示例将名为 example 的 SSO 服务器分配给名为 anyuser 的用户：

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# sso-server value example
hostname(config-username-webvpn)#
```

VPN 的 IP 地址

本章介绍 IP 地址分配方法。

IP 地址使互联网络连接成为可能。它们就像电话号码：发送方和接收方必须具有要连接的分配号码。但是，对于 VPN，实际上存在两组地址：第一组连接公用网络的客户端和服务器。连接建立后，第二组通过 VPN 隧道连接客户端和服务器。

在 ASA 地址管理方面，我们处理第二组的 IP 地址：这些专用 IP 地址通过隧道与具有专用网络资源的客户端连接，并且让客户端的运行看起来像直接连接至专用网络一样。此外，我们仅处理分配给客户端的专用 IP 地址。分配给专用网络上其他资源的 IP 地址是您的网络管理职责而非 VPN 管理的一部分。因此，当我们在这里讨论 IP 地址时，我们是指让客户端用作隧道终端的专用网络寻址方案中可用的 IP 地址。

配置 IP 地址分配策略

ASA 可使用以下一种或多种方法将 IP 地址分配给远程访问客户端。如已配置多个地址分配方法，则 ASA 将搜索每一个选项，直到找到一个 IP 地址为止。默认情况下，所有方法均已启用。

- aaa — 从外部身份验证、授权和记帐服务器逐个用户检索 IP 地址。如在使用已配置 IP 地址的身份验证服务器，我们建议使用此方法。此方法适用于 IPv4 和 IPv6 分配策略。
- dhcp — 从 DHCP 服务器获取 IP 地址。如要使用 DHCP，则必须配置 DHCP 服务器。还必须定义 DHCP 服务器可使用的 IP 地址范围。此方法适用于 IPv4 分配策略。
- **local** — 内部配置的地址池是配置地址池分配的最简单方法。如果选择 Local，也必须使用 **ip local - pool** 命令定义要使用的 IP 地址范围。此方法适用于 IPv4 和 IPv6 分配策略。
  - 在 IP 地址释放的一段时间之后允许重新使用 IP 地址，在 IP 地址返回到地址池之后会延迟重新使用它。添加延迟有助于在 IP 地址快速重新分配后防止防火墙可能遇到的问题。默认情况下 ASA 将不强制执行延迟。此可配置元素适用于 IPv4 分配策略。

使用以下方法之一指定将 IP 地址分配给远程访问客户端的方法。

在命令行配置 IPv4 地址分配

命令	用途
vpn-addr-assign {aaa | dhcp | local [reuse-delay *minutes*]**}** **示例：** hostname(config)# **vpn-addr-assign aaa** **示例：** hostname(config)# **vpn-addr-assign local reuse-delay 180** **示例：** hostname(config)# **no vpn-addr-assign dhcp**	在将 IPv4 地址分配给 VPN 连接时，启用要供 ASA 使用的地址分配方法。可用的方法是从 AAA 服务器、DHCP 服务器或本地地址池获取 IP 地址。默认情况下，所有这些方法均已启用。 对于本地 IP 地址池，可配置在 IP 地址释放后的 0 与 480 分钟之间重新使用 IP 地址。 使用此命令的 no 形式禁用地址分配方法。

在命令行配置 IPv6 地址分配

命令	用途
ipv6-vpn-addr-assign {aaa | local} **示例：** hostname(config)# **ipv6-vpn-addr-assign aaa** **示例：** hostname(config)# **no ipv6-vpn-addr-assign local**	在将 IPv6 地址分配给 VPN 连接时，启用要供 ASA 使用的地址分配方法。可用的方法是从 AAA 服务器或本地地址池获取 IP 地址。默认情况下，这两种方法均已启用。 使用此命令的 no 形式禁用地址分配方法。

模式

下表显示了此功能可用的模式：

防火墙模式		安全情景		
			多个	
路由	透明	单个	情景	系统
•	-	•	-	-

查看地址分配方法

使用以下方法之一查看在 ASA 上配置的地址分配方法：

从命令行查看 IPv4 地址分配

命令	用途
show running-config all vpn-addr-assign **示例：** hostname(config)# show running-config all vpn-addr-assign	显示已配置的地址分配方法。已配置的地址方法可能为 aaa、 dhcp 或 local。 vpn-addr-assign aaa vpn-addr-assign dhcp vpn-addr-assign local

从命令行查看 IPv6 地址分配

命令	用途
show running-config all ipv6-vpn-addr-assign **示例：** hostname(config)# show running-config all ipv6-vpn-addr-assign	显示已配置的地址分配方法。已配置的地址方法可能为 aaa 或 local。 ipv6-vpn-addr-assign aaa ipv6-vpn-addr-assign local reuse-delay 0

配置本地 IP 地址池

如要配置用于 VPN 远程访问隧道的 IPv4 地址池，请在全局配置模式下输入 **ip local pool** 命令。要删除地址池，请输入此命令的 **no** 形式。

如要配置用于 VPN 远程访问隧道的 IPv6 地址池，请在全局配置模式下输入 **ipv6 local pool** 命令。要删除地址池，请输入此命令的 **no** 形式。

ASA 根据连接配置文件或连接的组策略使用地址池。池的指定顺序非常重要。如已为连接配置文件或组策略配置多个地址池，则 ASA 将按您向 ASA 添加地址池的顺序使用地址池。

如果从非本地子网分配地址，我们建议添加位于子网边界的池，从而可更轻松地添加这些网络的路由。

使用下列方法之一配置本地 IP 地址池：

- 第 5-4 页上的使用 CLI 配置本地 IPv4 地址池
- 第 5-4 页上的使用 CLI 配置本地 IPv6 地址池

使用 CLI 配置本地 IPv4 地址池

	命令	用途
步骤 1	**vpn-addr-assign local** **示例：** hostname(config)# **vpn-addr-assign local**	将 IP 地址池配置为地址分配方法，输入参数为 **local** 的命令 **vpn-addr-assign**。另请参阅第 5-2 页上的在命令行配置 IPv4 地址分配。
步骤 2	**ip local pool** *poolname first_address-last_address* **mask** *mask* **示例：** hostname(config)# ip local pool **firstpool** **10.20.30.40-10.20.30.50** mask **255.255.255.0** **示例：** hostname(config)# no ip local pool **firstpool**	配置地址池。此命令为池命名，并指定 IPv4 地址范围和子网掩码。 第一个示例配置名为 **firstpool** 的 IP 地址池。起始地址为 **10.20.30.40**，结束地址为 **10.20.30.50**。网络掩码为 **255.255.255.0**。 第二个示例删除名为 **firstpool** 的 IP 地址池。

使用 CLI 配置本地 IPv6 地址池

	命令	用途
步骤 1	**ipv6-vpn-addr-assign local** **示例：** hostname(config)# **ipv6-vpn-addr-assign local**	将 IP 地址池配置为地址分配方法，输入参数为 **local** 的命令 ipv6-**vpn-addr-assign**。另请参阅第 5-2 页上的在命令行配置 IPv6 地址分配。
步骤 2	**ipv6 local pool** *pool_name starting_address prefix_length number_of_addresses* **示例：** hostname(config)# **ipv6 local pool** *ipv6pool 2001:DB8::1/32 100* **示例：** hostname(config)# **no ipv6 local pool** *ipv6pool*	配置地址池。此命令为池命名，并确定起始 IPv6 地址、前缀长度 （位数）和要在范围中使用的地址数量。 第一个示例配置名为 **ipv6pool** 的 IP 地址池。起始地址为 **2001:DB8::1**，前缀长度为 **32** 位，要在池中使用的地址数量为 **100**。 第二个示例删除名为 **ipv6pool** 的 IP 地址池。

将内部地址池分配给 ASDM 中的组策略

在 Add or Edit Group Policy 对话框中，可为正在添加或修改的内部网络 （客户端）访问组策略指定地址池、隧道协议、过滤器、连接设置和服务器。对于此对话框中的每一个字段，如果选中 Inherit 复选框，则相应的设置将从默认组策略获取其值。 Inherit 是此对话框中所有属性的默认值。

可为同一组策略配置 IPv4 和 IPv6 地址池。如已在同一组策略中配置 IP 地址的两个版本，则为 IPv4 配置的客户端将获取 IPv4 地址，为 IPv6 配置的客户端将获取 IPv6 地址，为 IPv4 和 IPv6 地址配置的客户端将获取 IPv4 和 IPv6 地址。

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

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

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

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

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

步骤 5　点击 **OK**。

步骤 6　点击 **Apply**。

配置 AAA 寻址

如要使用 AAA 服务器为 VPN 远程访问客户端分配地址，必须首先配置 AAA 服务器或服务器组。请参阅命令参考中的 **aaa-server protocol** 命令。

此外，用户必须匹配为 RADIUS 身份验证配置的连接配置文件。

以下示例说明了如何为名为 firstgroup 的隧道组定义名为 RAD2 的 AAA 服务器组。它包括一个绝对需要执行的步骤，在该步骤中，您曾命名隧道组并定义隧道组类型、该步骤在以下示例中显示为一则提醒，提示您只有设置这些值，然后才有权访问后续 tunnel-group 命令。

这些示例创建的配置概述如下：

```
hostname(config)# vpn-addr-assign aaa
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)# authentication-server-group RAD2
```

如要配置用于 IP 寻址的 AAA，请执行以下步骤：

步骤 1　**要将 AAA 配置为地址分配方法，请输入参数为 aaa 的命令 vpn-addr-assign。**

```
hostname(config)# vpn-addr-assign aaa
hostname(config)#
```

步骤 2　如要建立名为 firstgroup 的隧道组作为远程访问或建立 LAN 对 LAN 隧道组，请输入关键字为 **type** 命令 **tunnel-group** 与关键字。以下示例配置远程访问隧道组。

```
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)#
```

步骤 3　如要进入通用属性配置模式，在该模式下可为名为 firstgroup 的隧道组定义 AAA 服务器组，请输入参数为 **general-attributes** 的命令 **tunnel-group**。

```
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)#
```

步骤 4　如要指定用于身份验证的 AAA 服务器组，请输入命令 **authentication-server-group**。

```
hostname(config-general)# authentication-server-group RAD2
hostname(config-general)#
```

此命令包含的参数比此示例中的参数要多。有关详细信息，请参阅命令参考。

配置 DHCP 寻址

如要使用 DHCP 为 VPN 客户端分配地址，必须首先配置 DHCP 服务器和 DHCP 服务器可使用的 IP 地址范围。然后根据连接配置文件定义 DHCP 服务器。或者，也可在与连接配置文件或用户名相关的组策略中定义 DHCP 网络范围。它可能是 IP 网络编号，也可能是 IP 地址，用于向 DHCP 服务器标识要使用的 IP 地址池。

以下示例为名为 **firstgroup** 的连接配置文件定义 IP 地址为 172.33.44.19 的 DHCP 服务器。它们还为名为 **remotegroup** 的组策略将 DHCP 网络范围定义为 192.86.0.0。（名为 remotegroup 的组策略与名为 firstgroup 的连接配置文件关联）。如不定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将经过各个池，直到其发现未分配的地址为止。

以下配置包括多个绝对需要执行的步骤，在这些步骤中，您可能已将连接配置文件类型命名和定义为远程访问，并将组策略命名和标识为内部或外部。这些步骤会在以下示例中作为一则提醒显示，提示您只有先设置这些值，然后才有权访问后续命令 tunnel-group 和 group-policy。

准则和限制

您只能使用 IPv4 地址标识要分配客户端地址的 DHCP 服务器。

使用 CLI 配置 DHCP 寻址

	命令	用途
步骤 1	`vpn-addr-assign` **`dhcp`**	将 IP 地址池配置为地址分配方法。输入参数为 **dhcp** 的命令 **vpn-addr-assign**。另请参阅第 5-2 页上的在命令行配置 IPv4 地址分配。
步骤 2	`tunnel-group` **`firstgroup`** `type` **`remote-access`**	建立名为 firstgroup 的连接配置文件作为远程访问连接配置文件。 输入关键字为 **type** 和参数为 **remote-access** 的命令 **tunnel-group**。
步骤 3	`tunnel-group firstgroup` **`general-attributes`**	进入连接配置文件的通用属性配置模式，以便配置 DHCP 服务器。 输入参数为 **general-attributes** 的命令 **tunnel-group**。
步骤 4	`dhcp-server` *`IPv4_address_of_DHCP_server`* **示例：** `hostname(config-general)# dhcp-server` **`172.33.44.19`** `hostname(config-general)#`	按 IPv4 地址定义 DHCP 服务器。无法按 IPv6 地址定义 DHCP 服务器。可为连接配置文件指定多个 DHCP 服务器地址。 输入命令 **dhcp - server**。借助于此命令，可将 ASA 配置为在其尝试获取 VPN 客户端的 IP 地址时向指定的 DHCP 服务器发送附加选项。有关详细信息，请参阅 *《思科安全设备命令参考》* 指南中的命令 **dhcp-server**。 该示例配置 IP 地址为 172.33.44.19 的 DHCP 服务器。
步骤 5	`hostname(config-general)#` **`exit`** `hostname(config)#`	退出隧道组模式。

	命令	用途
步骤 6	`hostname(config)# group-policy remotegroup` **`internal`**	创建名为 **remotegroup** 的内部组策略。 输入参数为 **internal** 的命令 **group-policy**，以制定内部组策略。 该示例配置一个内部组。
步骤 7	`hostname(config)# group-policy remotegroup` **`attributes`** **示例：** `hostname(config)# group-policy remotegroup` **`attributes`** `hostname(config-group-policy)#`	（可选）进入组策略属性配置模式，在其中，可为要使用的 DHCP 服务器配置 IP 地址的子网。 输入关键字为 **attributes** 的命令 **group-policy**。 该示例为 **remotegroup** 组策略进入组策略属性配置模式。
步骤 8	`hostname(config-group-policy)#` **`dhcp-network-scope 192.86.0.0`** `hostname(config-group-policy)#`	（可选）要指定 DHCP 服务器在将地址分配给名为 **remotegroup** 的组策略用户时要使用的 IP 地址范围，请输入命令 **dhcp-network-scope**。 此示例配置网络范围 192.86.0.0。 **注**　dhcp-network-scope 必须是可路由 IP 地址，而非 DHCP 池的子集。 DHCP 服务器确定此 IP 地址所属的子网并从该池分配 IP 地址。出于路由原因，我们建议您使用 ASA 的接口作为 dhcp-network-scope。可使用任何 IP 地址作为 dhcp-network-scope，但它可以要求将静态路由添加至网络。

示例

这些示例创建的配置摘要如下：

```
hostname(config)# vpn-addr-assign dhcp
hostname(config)# tunnel-group firstgroup type remote-access
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)# group-policy remotegroup internal
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 192.86.0.0
```

将 IP 地址分配给本地用户

可将本地用户帐户配置为使用组策略，且可配置某些 AnyConnect 属性。当 IP 地址的其他源出现故障时，这些用户帐户将提供回退，以便管理员仍有访问权限。

本小节介绍如何为本地用户配置所有属性。

先决条件

此操作步骤描述如何编辑现有用户。要添加用户，请选择 **Configuration > Remote Access VPN > AAA/Local Users**，然后点击 **Add**。有关详细信息，请参阅常规操作配置指南。

用户编辑

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

如要覆盖每项设置，请取消选中 **Inherit** 复选框，并输入新值。下面的详细步骤介绍 Edit User Account 屏幕上的每项设置。

详细步骤

步骤 1　**启动 ASDM 并选择 Configuration > Remote Access VPN > AAA/Local Users > Local Users。**

步骤 2　选择要配置的用户，然后点击 **Edit**。

系统将打开 Edit User Account 屏幕。

步骤 3　在左侧窗格中，点击 **VPN Policy**。

步骤 4　为该用户指定一个组策略。用户策略将继承该组策略的属性。如果此屏幕中的其他字段设置为从 Default Group Policy **继承**配置，则此组策略中指定的属性优先于 Default Group Policy 中的属性。

步骤 5　指定可供用户使用的隧道协议，或是否从组策略继承值。选中所需的 **Tunneling Protocols** 复选框，以选择可供使用的 VPN 隧道协议。仅所选协议可供使用。选项如下：

- 无客户端 SSL VPN（通过 SSL/TLS 的 VPN）使用网络浏览器建立与 VPN 集中器连接的安全远程访问隧道；不需要软件和硬件客户端。无客户端 SSL VPN 可提供广泛企业资源的便捷访问，包括企业网站、支持网络的应用程序、 NT/AD 文件共享 （支持网络）、邮件和几乎任何计算机中的可访问 HTTPS 互联网网站的其他基于 TCP 的应用程序。
- SSL VPN 客户端允许用户在下载思科 AnyConnect 客户端应用程序后进行连接。第一次，用户可以使用无客户端 SSL VPN 连接来下载此应用程序。随后，每当用户连接时，都会视需要进行客户端更新。
- IPsec IKEv1 — IP 安全协议。 IPsec 被视为最安全的协议，为 VPN 隧道提供最完整的架构。站点间 （对等）连接和思科 VPN 客户端到 LAN 连接均可使用 IPsec IKEv1。
- IPsec IKEv2 — AnyConnect 安全移动客户端支持的 IPsec IKEv2。组合使用 IPsec 与 IKEv2 的 AnyConnect 连接能够利用向 SSL VPN 连接提供的相同功能集。
- 采用互联网协议安全的第二层隧道协议允许具有若干公共 PC 和移动 PC 操作系统的随附的 VPN 客户端远程用户通过公用 IP 网络与 ASA 和专用企业网络建立安全连接。

注　如未选择协议，系统会显示错误消息。

步骤 6　指定要使用的过滤器 （IPv4 或 IPv6），或者是否从组策略继承值。过滤器由规则组成，这些规则根据诸如源地址、目标地址和协议之类的条件来确定允许还是拒绝隧道数据包通过 ASA。要配置过滤器和规则，请选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > General > More Options > Filter**。

点击 **Manage** 以显示 ACL Manager 窗格，可以在其中添加、编辑及删除 ACL 和 ACE。

步骤 7　指定继承连接配置文件 （隧道组）锁定还是使用所选隧道组锁定 （如果有）。选择特定锁定会限定用户只能通过此组进行远程访问。隧道组锁定通过检查在 VPN 客户端上配置的组是否与用户分配的组相同来限制用户。如果不相同， ASA 将阻止用户进行连接。如果未选中 Inherit 复选框，则默认值为 None。

步骤 8　指定是否从该组继承 Store Password on Client System 设置。取消选中 **Inherit** 复选框以激活 Yes 和 No 单选按钮。点击 **Yes**，将登录密码存储在客户端系统上 （可能是不太安全的选项）。点击 **No**（默认）以要求用户输入每个连接的密码。为确保最高安全性，我们建议您*不允许*密码存储。

步骤 9　指定要应用于此用户的访问时长策略，为用户创建新的访问时长策略，或者保持选中 Inherit 框。默认值为 Inherit，或者，如果未选中 Inherit 复选框，则默认值为 Unrestricted。

点击 **Manage** 以打开 Add Time Range 对话框，可以在其中指定一组新的访问时长。

步骤 10　按用户指定同时登录数。 Simultaneous Logons 参数指定允许该用户执行的最多同时登录数。默认值为 3。最小值为 0，表示禁止登录并阻止用户访问。

注　在没有最大限制时，允许多个同时连接可能会降低安全性并影响性能。

步骤 11　为用户连接时间指定**最大连接时间** （以分钟为单位）。此时间结束时，系统会终止连接。最小值为 1 分钟，最大值为 2147483647 分钟 （4000 多年）。要允许无限连接时间，请选中 **Unlimited** 复选框 （默认）。

步骤 12　指定用户的空闲超时 （以分钟为单位）。如果在此期间，用户在连接上没有通信活动，系统会终止连接。最短时间为 1 分钟，最长时间为 10080 分钟。该值不适用于无客户端 SSL VPN 连接的用户。

步骤 13　配置会话警报间隔。如果取消选中 Inherit 复选框，则自动选中 Default 复选框。这将会话警报间隔设置为 30 分钟。如果您要指定新值，可以取消选中 Default 复选框，并在分钟框中指定 1 至 30 分钟的会话警报间隔。

步骤 14　配置空闲警报间隔。如果取消选中 Inherit 复选框，则自动选中 Default 复选框。这会将空闲警报间隔设置为 30 分钟。如果您要指定新值，可以取消选中 Default 复选框，并在分钟框中指定 1 至 30 分钟的会话警报间隔。

步骤 15　要为此用户设置专用 IPv4 地址，请在 Dedicated IPv4 Address (Optional) 区域中输入 IPv4 地址和子网掩码。

步骤 16　要为此用户设置专用 IPv6 地址，请在 Dedicated IPv6 Address (Optional) 区域中输入一个带 IPv6 前缀的 IPv6 地址。 IPv6 前缀表示 IPv6 地址所驻留的子网。

步骤 17　要配置无客户端 SSL 设置，请在左侧格中点击 **Clientless SSL VPN**。要覆盖每项设置，请取消选中 **Inherit** 复选框，并输入新值。

步骤 18　点击 **Apply**。

更改会保存到运行配置。

远程访问 IPsec VPN

本章介绍如何配置远程访问 IPsec VPN，包括以下各节：

有关远程访问 IPsec VPN 的信息

远程访问 VPN 使用户可以通过安全的 TCP/IP 网络连接 （例如互联网）连接到中心站点。互联网安全关联和密钥管理协议 （又称为 IKE）是一种协商协议，让远程 PC 上的 IPsec 客户端和 ASA 可以协商如何构建 IPSec 安全关联。每个 ISAKMP 协商分为两个部分，分别称为第 1 阶段和第 2 阶段。

第 1 阶段创建第一条隧道，用于保护后来的 ISAKMP 协商消息。第 2 阶段创建的隧道用于保护通过安全连接传输的数据。

要设置 ISAKMP 协商条款，您可以创建 ISAKMP 策略。 ISAKMP 策略包括以下部分：

- 身份验证方法，用于确保对等体的身份。
- 加密方法，用于保护数据并确保隐私。
- 哈希消息认证码 (HMAC) 方法，用于确保发送方身份，以及确保消息在传输过程中未被修改。
- Diffie-Hellman 群，用于设置加密密钥的大小。
- ASA 在更换加密密钥前可使用该加密密钥的时长限制。

转换集由加密方法和身份验证方法组成。在使用 ISAKMP 进行 IPsec 安全关联协商过程中，对等体同意使用特定转换集来保护特定数据流。该转换集对于两个对等体必须是相同的。

转换集保护在关联加密映射条目中指定的 ACL 的数据流。您可以在 ASA 配置中创建转换集，然后在加密映射条目或动态加密映射条目中指定最大转换集数量 11。有关更多概述信息 （包括列出有效加密方法和身份验证方法的表），请参阅本指南的第 9 章，“LAN 对 LAN IPsec VPN”中的第 9-6 页上的创建 IKEv1 转换集。

您可以将 ASA 配置为向 AnyConnect 客户端分配 IPv4 或 IPv6 地址或者同时分配 IPv4 和 IPv6 地址，方法是，在 ASA 上创建内部地址池，或者向 ASA 上的本地用户分配专用地址。

终端必须已在其操作系统中实现双栈协议，才有资格分配得到这两种地址。在上述两种方法中，如果没有 IPv6 地址池但有 IPv4 地址可用，或者没有 IPv4 地址池但有 IPv6 地址可用，仍会发生连接。但是，不会通知客户端；因此，管理员必须查看 ASA 日志才能了解详细信息。

SSL 协议支持向客户端分配 IPv6 地址。 IKEv2/IPsec 协议不支持此功能。

远程访问 IPsec VPN 的许可要求

下表显示此功能的许可要求：

注　此功能在无负载加密型号上不可用。

型号	许可证要求[1]
ASA 5505	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证和增强型安全许可证：2 个会话。 *可选永久性或基于时间的许可证：10 或 25 个会话。* *不支持共享许可证。*[2] – AnyConnect 基础版许可证[3]：25 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： – 基础许可证：10 个会话。 – 增强型安全许可证：25 个会话。
ASA 5512-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证和增强型安全许可证：2 个会话。 *可选永久性或基于时间的许可证：10、 25、 50、 100 或 250 个会话。* *可选共享许可证*[2]*：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证 [3]：250 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证和增强型安全许可证：250 个会话。

型号	许可证要求[1]
ASA 5515-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、 25、 50、 100 或 250 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：250 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：250 个会话。
ASA 5525-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、 25、 50、 100、 250、 500 或 750 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：750 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：750 个会话。
ASA 5545-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000 或 2500 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：2500 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：2500 个会话。
ASA 5555-X	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500 或 5000 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证[3]：5000 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：5000 个会话。

型号	许可证要求[1]
ASA 5585-X， 带 SSP-10	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500 或 5000 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证 [3]：5000 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：5000 个会话。
ASA 5585-X，带 SSP-20、 -40 和 -60	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500、5000 或 10000 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证 [3]：10000 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：10000 个会话。
ASASM	• 使用 IKEv2 的 IPsec 远程接入 VPN （使用以下任何一个）： – AnyConnect 高级版许可证： 基础许可证：2 个会话。 *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500、5000 或 10000 个会话。* *可选共享许可证[2]：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* – AnyConnect 基础版许可证 [3]：10000 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 基础许可证：10000 个会话。

型号	许可证要求[1]
ASAv，带 1 个虚拟 CPU	• 使用 IKEv2 的 IPsec 远程接入 VPN： – 标准版许可证：2 个会话。 – 高级版许可证：250 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 标准和高级版许可证：250 个会话。
ASAv，带 4 个虚拟 CPU	• 使用 IKEv2 的 IPsec 远程接入 VPN： – 标准版许可证：2 个会话。 – 高级版许可证：750 个会话。 • 使用 IKEv1 的 IPsec 远程接入 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点到站点 VPN： 标准和高级版许可证：750 个会话。

1. 所有类型的*最大组合 VPN* 会话数量不能超过此表中所示的最大会话数。对于 ASA 5505，基础许可证的最大组合会话数量为 10，增强型安全许可证的最大组合会话数量为 25。
2. 一个共享许可证允许 ASA 用作多个客户端 ASA 的共享许可证服务器。共享许可证池很大，但是，每个 ASA 使用的会话数不能超过永久许可证列出的最大数量。
3. AnyConnect 基础版许可证使 AnyConnect VPN 客户端能够访问 ASA。本许可证并不支持基于浏览器的 SSL VPN 访问或思科安全桌面。对于这些功能，需要激活 AnyConnect 高级许可证，而不是 AnyConnect 基础版许可证。

   注：通过 AnyConnect 基础版许可证， VPN 用户使用网络浏览器登录、下载并启动 （网络启动） AnyConnect 客户端。

   无论是采用本许可证还是 AnyConnect 高级 SSL VPN 版许可证， AnyConnect 客户端软件提供相同的客户端功能集。

   如果在既定的 ASA 上存在以下许可证，则 AnyConnect 基础版许可证无法激活：AnyConnect 高级许可证 （所有类型）或高级终端评估许可证。但是，您可以在同一网络的不同 ASA 上运行 AnyConnect 基础版许可证和 AnyConnect 高级许可证。

   默认情况下，ASA 使用 AnyConnect 基础版许可证；但是，您可以禁用该许可证，使用 **webvpn**，然后使用 **no anyconnect-essentials** 命令来使用其他许可证。

   对于 AnyConnect 基础版许可证和 AnyConnect 高级许可证支持的功能的详细列表，请参阅 *AnyConnect 安全移动客户端功能、许可证和操作系统*：

   http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

准则和限制

此节包括该功能的指导原则和限制。

情景模式准则

仅支持单一情景模式。不支持多情景模式。

防火墙模式准则

仅支持路由防火墙模式。不支持透明模式。

故障转移准则

IPsec VPN 会话仅可在主用 / 备用故障转移配置中复制。不支持主用 / 主用故障转移。

配置远程访问 IPsec VPN

本章介绍如何配置远程访问 VPN，包括以下主题：

配置接口

一个 ASA 至少有两个接口，在本指南中分别将它们称为外部接口和内部接口。通常，外部接口连接到公共互联网，内部接口连接到专用网络且不接受公共访问。

首先，在 ASA 上配置并启用两个接口。然后，为接口分配名称、 IP 地址和子网掩码。或者，在安全设备上配置接口的安全级别、速度和双工操作。

如要配置接口，请使用示例中所示的命令语法执行以下步骤：

详细步骤

	命令	用途

步骤 1	**interface** {*interface*}
	
	示例：
	`hostname(config)# interface ethernet0`
	`hostname(config-if)#`
		从全局配置模式进入接口配置模式。

步骤 2	**ip address** *ip_address* [*mask*] [**standby** *ip_address*]
	
	示例：
	`hostname(config)# interface ethernet0`
	`hostname(config-if)#`
	`hostname(config-if)# ip address 10.10.4.200 255.255.0.0`
		设置接口的 IP 地址和子网掩码。

步骤 3	**nameif** *name*
	
	示例：
	`hostname(config-if)# nameif outside`
	`hostname(config-if)#`
		为接口指定名称 （最多包含 48 个字符）。接口名称一旦设置便不可更改。

步骤 4	`shutdown`
	
	示例：
	`hostname(config-if)# no shutdown`
	`hostname(config-if)#`
		启用接口。默认情况下，接口被禁用。

在外部接口上配置 ISAKMP 策略和启用 ISAKMP

本节介绍在外部接口上配置和启用 ISAKMP 策略的操作步骤。

详细步骤

执行以下命令：

	命令	用途

步骤 1	`crypto ikev1 policy` *priority* `authentication {crack | pre-share | rsa-sig}`
	
	示例：
	`hostname(config)# crypto ikev1 policy 1 authentication pre-share`
	`hostname(config)#`
		指定要在 IKEv1 协商过程中使用的身份验证方法和参数集。
		Priority 唯一标识互联网密钥交换 (IKE) 策略并向该策略分配优先级。使用 1 到 65,534 之间的整数，其中， 1 是最高优先级， 65,534 是最低优先级。
		在本示例及后续步骤中，我们将优先级设置为 1。

步骤 2	**crypto ikev1** policy *priority* encryption {aes | aes-192 | aes-256 | des | 3des}
	
	示例：
	`hostname(config)# crypto ikev1 policy 1 encryption 3des`
	`hostname(config)#`
		指定要在 IKE 策略中使用的加密方法。

步骤 3	**crypto ikev1** policy *priority* hash {md5 | sha}
	
	示例：
	`hostname(config)# crypto ikev1 policy 1 hash sha`
	`hostname(config)#`
		为 IKE 策略指定哈希算法 （又称为 HMAC 变体）。

步骤 4	**crypto ikev1** policy *priority* group {1 | 2 | 5}
	
	示例：
	`hostname(config)# crypto ikev1 policy 1 group 2`
	`hostname(config)#`
		为 IKE 策略指定 Diffie-Hellman 群 — 允许 IPsec 客户端和 ASA 建立共享密钥的加密协议。

步骤 5	**crypto ikev1** policy *priority* lifetime {*seconds*}
	
	示例：
	`hostname(config)# crypto ikev1 policy 1 lifetime 43200`
	`hostname(config)#`
		指定加密密钥生存期 — 每个安全关联的存续时长，以秒为单位。
		有效生存期为 120 到 2147483647 秒。
		0 表示无限生存期。

	命令	用途
步骤 6	**crypto ikev1** enable *interface-name* **示例：** hostname(config)# **crypto ikev1** enable outside hostname(config)#	在名为 *outside* 的接口上启用 ISAKMP。
步骤 7	write memory **示例：** hostname(config-if)# write memory Building configuration... Cryptochecksum: 0f80bf71 1623a231 63f27ccf 8700ca6d 11679 bytes copied in 3.390 secs (3893 bytes/sec) [OK] hostname(config-if)#	保存配置更改。

配置地址池

ASA 需要有用于向用户分配 IP 地址的方法。本节以地址池为例。可将以下示例中所示的命令语法作为指导。

命令	用途
ip local pool *poolname first-address—last-address* [mask *mask*] **示例：** hostname(config)# **ip local pool testpool 192.168.0.10-192.168.0.15** hostname(config)#	使用一系列 IP 地址创建地址池， ASA 会从该地址池向客户端分配地址。 地址掩码是可选的。但是，如果 IP 地址分配给属于非标准网络的 VPN 客户端，您必须提供掩码值；如果使用默认掩码，数据路由可能会出错。这种情况的一个典型示例是，本地 IP 地址池包含 10.10.10.0/255.255.255.0 地址，因为默认情况下这是 A 类网络。当 VPN 客户端需要通过不同接口访问该网络中的不同子网时，可能会导致路由问题。

添加用户

本节介绍如何配置用户名和密码。可将以下示例中所示的命令语法作为指导。

命令	用途
username *name* {nopassword | password *password* [mschap | encrypted | nt-encrypted]} [privilege *priv_level*] **示例：** hostname(config)# **username testuser password 12345678** hostname(config)#	创建用户、密码和权限级别。

创建 IKEv1 转换集或 IKEv2 方案

本节介绍如何配置转换集 (IKEv1) 或方案 (IKEv2) （由加密方法和身份验证方法组成）。

执行以下任务：

命令	用途

配置 IKEv1 转换集：
`crypto ipsec ikev1 transform-set` *transform-set-name encryption-method* [*authentication*]
 	
示例：
`hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac`
`hostname(config)#`
	配置 IKEv1 转换集，用于指定要用于确保数据完整性的 IPsec IKEv1 加密和哈希算法。
	对 *encryption* 使用以下其中一个值：
	• **esp-aes** — 将 AES 和 128 位密钥结合使用。
	• **esp-aes-192** — 将 AES 和 192 位密钥结合使用。
	• **esp-aes-256** — 将 AES 和 256 位密钥结合使用。
	• **esp-des** — 使用 56 位 DES-CBC。
	• **esp-3des** — 使用三重 DES 算法。
	• **esp-null** — 不使用加密。
	对 *authentication* 使用以下其中一个值：
	• **esp-md5-hmac** — 将 MD5/HMAC-128 用作哈希算法。
	• **esp-sha-hmac** — 将 SHA/HMAC-160 用作哈希算法。
	• **esp-none** — 不使用 HMAC 身份验证。

配置 IKEv2 方案：
crypto ipsec ikev2 ipsec-proposal *proposal_name*
 	
然后：
protocol {**esp**} {**encryption** {**des** | **3des** | **aes** | **aes-192** | **aes-256** | **null**} | **integrity** {**md5** | **sha-1**}
 	
示例：
`hostname(config)# crypto ipsec ikev2 ipsec-proposal secure_proposal`
`hostname(config-ipsec-proposal)# protocol esp encryption des integrity md5`
	配置 IKEv2 方案集，用于指定要使用的 IPsec IKEv2 协议、加密和完整性算法。
	esp 指定封装安全负载 (ESP) IPsec 协议 （是目前唯一受支持的 IPsec 协议）。
	对 *encryption* 使用以下其中一个值：
	• **des** — 对 ESP 使用 56 位 DES-CBC 加密。
	• **3des** -（默认值）对 ESP 使用三重 DES 加密算法。
	• **aes —** 对 ESP 结合使用 AES 和 128 位密钥加密。
	• **aes-192 —** 对 ESP 结合使用 AES 和 192 位密钥加密。
	• **aes-256 —** 对 ESP 结合使用 AES 和 256 位密钥加密。
	• **null** — 不对 ESP 使用加密。
	对 *integrity* 使用以下其中一个值：
	• **md5** — 为 ESP 完整性保护指定 md5 算法。
	• **sha-1** -（默认值）为 ESP 完整性保护指定安全哈希算法 (SHA) SHA-1 （在美国联邦信息处理标准 [FIPS] 中定义）。

定义隧道组

本节介绍如何配置隧道组 （隧道组是包含隧道连接策略的记录集）。您可以配置隧道组来标识 AAA 服务器，指定连接参数，以及定义默认组策略。 ASA 会在内部存储隧道组。

ASA 系统中有两个默认隧道组：DefaultRAGroup 和 DefaultL2Lgroup，前者是默认的远程访问隧道组，后者是默认的 LAN 到 LAN 隧道组。您可以更改默认隧道组，但不能删除它们。如果在隧道协商过程中没有标识特定隧道组， ASA 将会使用使用这两个隧道组来配置远程访问隧道组和 LAN 到 LAN 隧道组的默认隧道参数。

执行以下任务：

详细步骤

	命令	用途

步骤 1	`tunnel-group` *name* `type` *type*
	
	示例：
	`hostname(config)# tunnel-group testgroup type ipsec-ra`
	`hostname(config)#`
		创建 IPsec 远程访问隧道组 （又称为连接配置文件）。

步骤 2	**tunnel-group** *name* **general-attributes**
	
	示例：
	`hostname(config)# tunnel-group testgroup general-attributes`
	`hostname(config-tunnel-general)#`
		进入隧道组常规属性模式 （在该模式下可输入身份验证方法）。

步骤 3	**address-pool** [(*interface name*)] **address_pool1** [...address_pool6] **示例：** `hostname(config-general)# address-pool testpool`	指定要用于隧道组的地址池。

步骤 4	**tunnel-group** *name* **ipsec-attributes**
	
	示例：
	`hostname(config)# tunnel-group testgroup ipsec-attributes`
	`hostname(config-tunnel-ipsec)#`
		进入隧道组 IPsec 属性模式 （在该模式下可输入用于 IKEv1 连接的 IPsec 特定属性）。

步骤 5	**ikev1 pre-shared-key** *key* **示例：** `hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfx`	（可选）配置预共享密钥（仅限 IKEv1）。该密钥可以是包含 1 到 128 个字符的字母数字字符串。 用于自适应安全设备和客户端的密钥必须相同。如果具有不同预共享密钥大小的思科 VPN 客户端尝试连接，该客户端将会记录错误消息，指明它无法对对等体进行身份验证。 **注**　在隧道组 webvpn 属性中使用证书为 IKEv2 配置 AAA 身份验证。

创建动态加密映射

本节介绍如何配置动态加密映射 （动态加密映射定义策略模板，其中的所有参数都不需要进行配置）。动态加密映射使 ASA 可以接收来自使用未知 IP 地址的对等体的连接。远程访问客户端属于此类别。

动态加密映射条目标识用于连接的转换集。您还可以启用反向路由，这样， ASA 可以获悉所连接客户端的路由信息，并通过 RIP 或 OSPF 通告这些信息。

执行以下任务：

详细步骤

	命令	用途

步骤 1	对于 IKEv1，请使用以下命令：
	`crypto dynamic-map` *`dynamic-map-name seq-num`* `set ikev1 transform-set` *`transform-set-name`*
	
	示例：
	`hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet`
	`hostname(config)#`
	
	对于 IKEv2，请使用以下命令：
	`crypto dynamic-map` *`dynamic-map-name seq-num`* `set ikev2 ipsec-proposal` *`proposal-name`*
	
	示例：
	`hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal FirstSet`
	`hostname(config)#`
		创建动态加密映射并为其指定 IKEv1 转换集或 IKEv2 方案。

步骤 2	**`crypto dynamic-map`** ***`dynamic-map-name dynamic-seq-num`*** **`set reverse-route`**
	
	示例：
	`hostname(config)# crypto dynamic-map dyn1 1 set reverse route`
	`hostname(config)#`
		（可选）根据加密映射条目为任何连接启用反向路由注入。

创建加密映射条目以使用动态加密映射

本节介绍如何创建加密映射条目，以使 ASA 可以使用动态加密映射来设置 IPsec 安全关联的参数。

在以下命令示例中，加密映射的名称是 *mymap*，序列号是 1，动态加密映射的名称是 *dyn1* （是在上一节 “创建动态加密映射”中创建的）。

执行以下任务：

详细步骤

	命令	用途

步骤 1	`crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name`
	
	示例：
	`hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1`
	`hostname(config)#`
		创建使用动态加密映射的加密映射条目。

步骤 2	**crypto map** *map-name* **interface** *interface-name*
	
	示例：
	`hostname(config)# crypto map mymap interface outside`
	`hostname(config)#`
		将加密映射应用于外部接口。

保存安全设备配置

执行上述配置任务后，请务必保存配置更改，如本示例中所示：

命令	用途

`write memory`
 	
示例：
`hostname(config-if)# write memory`
`Building configuration...`
`Cryptochecksum: 0f80bf71 1623a231 63f27ccf 8700ca6d`
 	
`11679 bytes copied in 3.390 secs (3893 bytes/sec)`
`[OK]`
`hostname(config-if)#`
	保存配置更改。

远程访问 IPsec VPN 配置示例

以下示例展示如何配置远程访问 IPsec/IKEv1 VPN：

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption 3des
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)# lifetime 43200
hostname(config)# crypto ikev1 outside
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev1 transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# tunnel-group testgroup type remote-access
```

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# ikev1 pre-shared-key 44kkaol59636jnfx
hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)# crypto map mymap interface outside
hostname(config)# write memory
```

以下示例展示如何配置远程访问 IPsec/IKEv2 VPN：

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)# integrity sha
hostname(config-ikev2-policy)# lifetime 43200
hostname(config-ikev2-policy)# prf sha
hostname(config)# crypto ikev2 outside
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev2 ipsec-proposal FirstSet
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes
hostname(config)# tunnel-group testgroup type remote-access
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup webvpn-attributes
hostname(config-webvpn)# authentication aaa certificate
hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal FirstSet
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)# crypto map mymap interface outside
hostname(config)# write memory
```

远程访问 VPN 的功能历史记录

表 6-1 列出了此功能的版本历史记录。

表 6-1　　功能 1 的功能历史记录

功能名称	版本	功能信息
用于 IPsec IKEv1 和 SSL 的远程访问 VPN。	7.0	远程访问 VPN 使用户可以通过安全的 TCP/IP 网络连接（例如互联网）连接到中心站点。
用于 IPsec IKEv2 的远程访问 VPN	8.4(1)	增加了对 AnyConnect 安全移动客户端的 IPsec IKEv2 支持。

网络准入控制

本章包含以下小节：

有关网络准入控制的信息

网络准入控制会执行终端合规性和漏洞检查，并以此作为网络生产访问的条件，从而防止企业网络遭受蠕虫、病毒和欺诈应用程序的入侵和感染。我们将这些检查称为*状态验证*。您可以配置状态验证来确保拥有 IPsec 或 WebVPN VPN 会话的主机上的防病毒文件、个人防火墙规则或入侵防御软件均为最新，然后再向内联网上的易受攻击主机提供访问权限。状态验证可以包括，对远程主机上运行的应用程序是否使用最新修补程序进行更新的验证。NAC 仅在用户身份验证和隧道设置之后进行。 NAC 对于防止不受自动网络策略实施约束的主机 （家用 PC）访问企业网络，特别有用。

终端和 ASA 之间的隧道建立会触发状态验证。

您可以将 ASA 配置为，如果客户端不响应状态验证请求，则将客户端的 IP 地址传送到可选的审核服务器。审核服务器 （例如 Trend 服务器）使用主机地址直接质询主机，以评估其运行状态。例如，它可能会质询主机确定它的病毒检查软件是否处于活动和最新状态。审核服务器完成与远程主机后的交互后，它会将标记传送给状态验证服务器，指示远程主机的运行状况。

验证状态成功或收到指示远程主机运行状况良好的标记后，状态验证服务器会将一个网络访问策略发送到 ASA，以便应用于隧道上的流量。

在涉及 ASA 的 *NAC Framework* 配置中，只有在客户端上运行的 Cisco Trust Agent 可以履行状态代理角色，而且只有思科访问控制服务器 (ACS) 可以履行状态验证服务器角色。ACS 可使用动态 ACL 确定每个客户端的访问策略。

作为 RADIUS 服务器，除了作为状态验证服务器履行其角色，ACS 可以对建立隧道所需的登录凭证进行身份验证。

注　只有在 ASA 上配置的 NAC 框架策略可支持审核服务器的使用。

在它作为状态验证服务器的角色中， ACS 使用访问控制列表。如果状态验证成功，且 ACS 指定一个重定向 URL 作为它发到 ASA 的访问策略的一部分， ASA 将所有 HTTP 和 HTTPS 请求从远程主机重定向至重定向 URL。一旦状态验证服务器将访问策略上传到 ASA，所有关联流量必须通过安全设备和 ACS （反之亦然）才能到达其目标。

如果 NAC 框架策略被分配给组策略， IPsec 或 WebVPN 客户端和 ASA 之间的隧道建立会触发状态验证。但是， NAC 策略框架可以确定免除状况验证的操作系统和指定筛选这些流量的可选 ACL。

许可要求

下表显示了此功能的许可要求：

注　此功能在无负载加密型号上不可用。

型号	许可证要求
ASA 5512-X	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、 25、 50、 100 或 250 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5515-X	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、 25、 50、 100 或 250 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5525-X	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、 25、 50、 100、 250、 500 或 750 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5545-X	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000 或 2500 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*

型号	许可证要求
ASA 5555-X	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、 25、 50、 100、 250、 500、 750、 1000、 2500 或 5000 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5585-X，带 SSP-10	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、 25、 50、 100、 250、 500、 750、 1000、 2500 或 5000 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5585-X，带 SSP-20、 -40 和 -60	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500、5000 或 10000 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASASM	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500、5000 或 10000 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASAv，带 1 个虚拟 CPU	• 标准版许可证：2 个会话。 • 高级版许可证：250 个会话。
ASAv，带 4 个虚拟 CPU	• 标准版许可证：2 个会话。 • 高级版许可证：750 个会话。

注　如果您启动无客户端 SSL VPN 会话，然后从门户启动 AnyConnect 客户端会话，总计使用的是 1 个会话。但是，如果先启动 AnyConnect 客户端（例如从独立客户端启动），然后登录无客户端 SSL VPN 门户，则使用的是 2 个会话。

*所有*类型的最大组合 VPN 会话数量不能超过此表中所示的最大会话数。

一个共享许可证允许 ASA 用作多个客户端 ASA 的共享许可证服务器。共享许可证池很大，但是，每个 ASA 使用的会话数不能超过永久许可证列出的最大数量。

NAC 先决条件

当 ASA 配置为支持 NAC 时，它作为 Cisco 安全访问控制服务器的一个客户端，要求至您在网络中必须安装至少一个访问控制服务器来提供 NAC 身份验证服务。

准则和限制

在网络上配置一个或多个访问控制服务器后，您必须使用 **aaa-server** 命令来命名访问控制服务器组。然后，请遵循第 7-6 页上的 “配置 NAC 策略”过程中的说明。

NAC 框架的 ASA 支持只限于远程访问 IPsec 和 WebVPN VPN 客户端会话。NAC 框架配置只支持单一模式。

ASA 上的 NAC 不支持第 3 层 （非 VPN）流量和 IPv6 流量。

查看安全设备上的 NAC 策略

在配置要分配给组策略的 NAC 策略之前，我们建议您查看 ASA 上可能已经设置的任何 NAC 策略。由于默认配置不包含 NAC 策略，因此输入此命令是确定是否已添加任何此策略的一种非常有用的方法。否则，您可以确定已配置的策略是适当的并忽略有关配置 NAC 策略的部分。

详细步骤。

	命令	目的

步骤 1	**show running-config nac-policy**
	
	示例：
	`hostname# show running-config nac-policy`
	`nac-policy nacframework1 nac-framework`
	`default-acl acl-1`
	`reval-period 36000`
	`sq-period 300`
	`exempt-list os "Windows XP" filter acl-2`
	`hostname#`
		查看已在 ASA 上设置的所有 NAC 策略。
		显示名为 nac-framework1 的 NAC 策略的配置

步骤 2	• default-acl — 状态验证之前应用的 NAC 默认 ACL。在状态验证后，安全设备使用从远程主机的访问控制服务器获得的 ACL 替换默认 ACL。如果状态验证失败， ASA 将保留默认 ACL。 • reval-period — NAC 框架会话中每次成功的状态验证之间间隔的秒数。 • sq-period — NAC 框架会话中每次成功的状态验证和终端安全评估中下一个更改查询之间间隔的秒数。 • exempt-list — 被免除状态验证的操作系统名称。此外，如果远程计算机操作系统与该名称匹配，则会显示过滤流量的可选 ACL。 • authentication-server-group — 要用于 NAC 状态验证的身份验证服务器组的名称。	显示 NAC 框架属性。

	命令	目的

步骤 3	`show nac-policy`
	
	示例：
	`asa2(config)# show nac-policy`
	`nac-policy framework1 nac-framework`
	`  applied session count = 0`
	`  applied group-policy count = 2`
	`  group-policy list:  GroupPolicy2  GroupPolicy1`
	`nac-policy framework2 nac-framework is not in use.`
	`asa2(config)#`
		显示 NAC 策略向组策略的分配。
		
		显示了哪些 NAC 策略未被分配以及每个 NAC 策略的使用计数。

步骤 4	• applied session count — 此 ASA 向其应用 NAC 策略的 VPN 会话的累计数量。 • applied group-policy count — 此 ASA 向其应用 NAC 策略的组策略的累计数量。 • group-policy list — 向其分配此 NAC 策略的组策略的列表。在这种情况下，组策略的使用不决定其是否显示在该列表中；如果 NAC 策略被分配给一个正在运行的配置中的组策略，则该组策略将显示在此列表中。	解释 show nac-policy 命令中的字段。 **注**　策略未被分配给任何组策略时，策略类型旁边将显示 “is not in use”。

请参考以下节，创建 NAC 策略或修改现有的策略。

添加、访问或删除 NAC 策略

输入以下命令添加或修改 NAC 策略：

详细步骤

	命令	目的
步骤 1	**`global`**	切换成全局配置模式。

步骤 2	**`nac-policy`** *nac-policy-name* **`nac-framework`**
	
	示例：
	`hostname(config)# nac-policy nac-framework1 nac-framework`
	`hostname(config-nac-policy-nac-framework)`
		添加或修改 NAC 策略。
		
		nac-policy-name 是新的或或现有的 NAC 策略的名称。该名称为最多 64 个字符的字符串。
		
		`nac-framework` 指定 NAC 框架配置将为远程主机提供网络访问策略。该网络上必须有思科访问控制服务器才能为 ASA 提供 NAC 框架服务。指定此类型时，提示符将表明您处于 `nac-policy-nac-framework` 配置模式下。此模式允许配置 NAC 框架策略。
		
		注　您可以创建不止一个 NAC 框架策略，但是一个组策略所分配的 NAC 框架策略不能超过一个。
		
		创建并访问名称为 NAC framework1 的 NAC 框架策略。

	命令	目的
步骤 3	（可选） [no] **nac-policy** *nac-policy-name* **nac-framework**	从配置中删除 NAC 策略。您必须同时指定策略的名称和类型。
步骤 4	（可选） **clear configure nac-policy**	从配置中删除所有 NAC 策略，但已分配给组策略的 那些除外。
步骤 5	**show running-config nac-policy**	显示安全设备上已有的每个 NAC 策略的名称和配置。

配置 NAC 策略

使用 **nac-policy** 命令命名 NAC 框架策略之后，请根据以下节来给其属性赋值，再将其分配给组策略。

指定访问控制服务器组

您必须至少配置一个思科访问控制服务器来支持 NAC。

详细步骤

	命令	目的
步骤 1	**aaa-server host**	命名访问控制服务器组，即使该组只包含一个服务器。
步骤 2	（可选） **show running-config aaa-server** **示例：** hostname(config)# **show running-config aaa-server** aaa-server acs-group1 protocol radius aaa-server acs-group1 (outside) host 192.168.22.44 key secret radius-common-pw secret hostname(config)#	显示 AAA 服务器配置。
步骤 3	**nac-policy-nac-framework**	切换为 nac-policy-nac-framework 配置模式。
步骤 4	**authentication-server-group** *server-group* **示例：** hostname(config-nac-policy-nac-framework)# **authentication-server-group acs-group1** hostname(config-nac-policy-nac-framework)	指定用于 NAC 状态验证的组。 *server-group* 必须与 **aaa-server host** 命令中指定的 server-tag 变量匹配。如果使用的是该命令的 **no** 版本，则此要求是可选的。 将 acs-group1 指定为用于 NAC 状态验证的身份验证服务器组。
步骤 5	（可选） [no] **authentication-server-group** *server-group*	从 NAC 策略删除该命令。

设置状态更改查询计时器

每次状态验证成功之后，ASA 将启动状态查询计时器。此计时器到期会触发向远程主机查询最近一次状态验证之后状态中的变更。如果响应指示没有变更，则会重置状态查询计时器。如果响应指示状态有变更，则会触发无条件状态重新验证。 ASA 在重新验证期间保持当前的访问策略。

默认情况下，每次成功的状态验证和状态查询以及每个后续状态查询之间的间隔是 300 秒（5 分钟）。按照以下步骤更改状态查询间隔：

详细步骤

	命令	目的
步骤 1	**nac-policy-nac-framework**	切换为 nac-policy-nac-framework 配置模式。
步骤 2	**sq-period seconds** **示例：** hostname(config-group-policy)# **sq-period 1800** hostname(config-group-policy)	更改状态查询间隔。 *seconds* 必须在 30 至 1800 秒范围内（5 至 30 分钟）。 将查询计时器改为 1800 秒。
步骤 3	（可选） [**no**] **sq-period** *seconds*	关闭状态查询计时器。
步骤 4	**show running-config nac-policy**	在 sq-period 属性旁边显示 0，表示计时器已关闭。

设置重新验证计时器

每次状态验证成功之后，ASA 将启动重新验证计时器。此计时器到期，会触发下一次无条件状态验证。 ASA 在重新验证期间保持当前的访问策略。

默认情况下，每次成功的状态验证之间的间隔为 36000 秒 （10 小时）。要更改此间隔，请在 nac-policy-nac-framework 配置模式下输入以下命令：

详细步骤

	命令	目的
步骤 1	**nac-policy-nac-framework**	切换为 nac-policy-nac-framework。
步骤 2	**reval-period** *seconds* **示例：** hostname(config-nac-policy-nac-framework)# **reval-period 86400** hostname(config-nac-policy-nac-framework)	更改每次成功的状态验证之间的间隔。 *seconds* 必须在 300 至 86400 秒 （5 分钟至 24 小时）范围内。
步骤 3	（可选） [**no**] **reval-period** *seconds*	关闭状态查询计时器。
步骤 4	**show running-config nac-policy**	在 sq-period 属性旁边显示 0，表示计时器已关闭。

配置 NAC 的默认 ACL

每个组策略都指向要应用于匹配该策略并且符合 NAC 资格的主机的默认 ACL。在状况验证之前 ASA 应用 NAC 默认 ACL。在状态验证后， ASA 使用从远程主机的访问控制服务器获得的 ACL 替换默认 ACL。如果状态验证失败， ASA 将保留默认 ACL。

如果已启用无客户端身份验证 （这是默认设置）， ASA 也会应用 NAC 默认 ACL。

详细步骤

	命令	目的
步骤 1	**nac-policy-nac-framework**	切换为 nac-policy-nac-framework 配置模式。
步骤 2	**default-acl** *acl-name* **示例：** hostname(config-nac-policy-nac-framework)# **default-acl acl-2** hostname(config-nac-policy-nac-framework)	指定使用哪个 ACL 作为用于 NAC 会话的默认 ACL。 *acl-name* 是要应用于会话的访问控制列表的名称。 将 ac1-2 标识为在状态验证成功之前应用的那个 ACL。
步骤 3	（可选） [**no**] **default-acl** *acl-name*	从 NAC 框架策略删除该命令。指定 *acl-name* 是可选的。

配置 NAC 免除

ASA 配置存储免除 NAC 状态验证的列表。您可以指定被免除的操作系统。如果指定 ACL，运行该指定操作系统的客户端将被免除进行状态验证并且客户端流量将接受 ACL。

要向免除 NAC 状态验证的远程计算机类型列表中添加条目，请在 nac-policy-nac-framework 配置模式下输入以下命令：

详细步骤

	命令	目的
步骤 1	`nac-policy-nac-framework`	切换为 nac-policy-nac-framework 配置模式。
步骤 2	**exempt-list os** "*os-name*" [**disable** | **filter** *acl-name* [**disable**]	向免除 NAC 状态验证的远程计算机类型列表添加条目。 • *os-name* 是操作系统名称。如果该名称包含空格，请使用引号（例如“Windows XP”）。 • 如果计算机操作系统与 *os name* 名称匹配，**filter** 将应用 ACL 来过滤流量。该 **filter**/*acl-name* 对是可选的。 • **disable** 执行如下两个功能之一： – 如果您在“os-name”后面输入它，ASA 将忽略免除，并向运行该操作系统的远程主机应用 NAC 状态验证。 – 如果您在 *acl-name* 后面输入它， ASA 将免除该操作系统，但是不会向相关流量应用 ACL。 • *acl-name* 是 ASA 配置中显示的 ACL 的名称。指定该名称时，其必须跟在 **filter** 关键字后面。

	示例：
	`hostname(config-group-policy)# exempt-list os "Windows XP"`
	`hostname(config-group-policy)`
		向被免除状态验证的计算机列表中添加运行 Windows XP 的所有主机。

	`hostname(config-nac-policy-nac-framework)# exempt-list os "Windows XP" filter acl-2` `hostname(config-nac-policy-nac-framework)`	免除运行 Windows XP 的所有主机并向来自这些主机的流量应用 ACL acl-2
	`hostname(config-nac-policy-nac-framework)# no exempt-list os "Windows XP" filter acl-2` `hostname(config-nac-policy-nac-framework)`	从免除列表中删除相同条目。
步骤 3	（可选） [**no**] **exempt-list os** "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]	从 NAC 框架策略删除所有免除。在发出 no 版本的该命令时指定一个条目会将此条目从免除列表中删除。

	示例：
	`hostname(config-nac-policy-nac-framework)# no exempt-list`
	`hostname(config-nac-policy-nac-framework)`
		从免除列表中删除所有条目。

注　当该命令指定一个操作系统时，它不会覆盖之前添加到异常列表中的条目；为您想要免除的每个操作系统和 ACL 分别输入一次该命令。

将 NAC 策略分配给组策略

完成每个隧道设置后，如果已向组策略、会话分配 NAC 策略，则 ASA 将应用此策略。默认情况下，在每个组策略的配置中不显示 **nac-settings** 命令。当您将 NAC 策略分配给组策略时， ASA 将自动为该组策略启用 NAC。

详细步骤

	命令	目的
步骤 1	**group-policy**	切换为 group-policy 配置模式。
步骤 2	**nac-settings** { **value** *nac-policy-name* | **none** } **示例：** hostname(config-group-policy)# **nac-settings value framework1** hostname(config-group-policy)	将 NAC 策略分配给组策略。 • **nac-settings none** 将从组策略中删除 *nac-policy-name* 并为该组策略禁用 NAC 策略。组策略不继承默认组策略的 nac-settings 值。 • **nac-settings value** 将您命名的 NAC 策略分配给组策略。 将名称为 framework1 的 NAC 策略分配给组策略。
步骤 3	（可选） [**no**] **nac-settings** { **value** *nac-policy-name* | **none** }	从组策略删除 nac-policy-name。组策略继承默认组策略的 nac-settings 值。
步骤 4	（可选） **show running-config nac-policy**	显示每个 NAC 策略的名称和配置

变更全局 NAC 框架设置

ASA 为 NAC 框架配置提供默认设置。使用本节的说明调整这些设置，以便遵守您的网络中有效的策略。

更改无客户端身份验证设置

可以为无客户端身份验证配置 NAC 框架支持。其适用于不具备 Cisco Trust Agent 的主机，履行状态代理角色。 ASA 应用默认访问策略，为状态验证发送经由 UDP 的 EAP 请求，然后请求超时。如果没有将 ASA 配置为向访问控制服务器请求无客户端主机的策略，它将保持无客户端主机中已经在用的默认访问策略。如果已将 ASA 配置为向访问控制服务器请求无客户端主机的策略，它将执行此请求并且访问控制服务器将下载要由 ASA 执行的访问策略。

启用和禁用无客户端身份验证

无客户端身份验证在默认情况下处于启用状态。默认配置包含 **eou allow clientless** 配置。

限制

eou 命令*只*适用于 NAC 框架会话。

详细步骤

按照以下步骤启用 NAC 框架配置的无客户端身份验证：

	命令	目的
步骤 1	`global`	切换成全局配置模式。

步骤 2	`eou allow {audit | clientless | none}`
	
	示例：
	`hostname(config)# eou allow audit`
	`hostname(config)#`
		为 NAC 框架配置启用无客户端身份验证。
		• **audit** 使用审核服务器进行无客户端身份验证。
		• **clientless** 使用思科访问控制服务器进行无客户端身份验证。
		• **none** 禁用无客户端身份验证。
		
		显示如何配置 ASA 以使用审核服务器进行无客户端身份验证。

步骤 3	`[no] eou allow {audit | clientless | none}`
	
	示例：
	`hostname(config)# no eou allow audit`
	`hostname(config)#`
		从配置中删除命令。
		
		禁用审核服务器的使用。

更改用于无客户端身份验证的登录凭证

启用无客户端身份验证，并且 ASA 无法从远程主机接收到对验证请求的响应时，其将代表远程主机向访问控制服务器发送无客户端身份验证请求。该请求包括与访问控制服务器上为无客户端身份验证配置的那些凭证匹配的登录凭证。在 ASA 上的无客户端身份验证的默认用户名和密码与访问控制服务器上的默认用户名和密码匹配；默认用户名和密码均为 “clientless”。

先决条件

如果在访问控制服务器更改了这些值，则必须在 ASA 上也执行这些更改。

详细步骤

输入以下命令更改用于无客户端身份验证的用户名：

	命令	目的
步骤 1	**global**	切换成全局配置模式。
步骤 2	**eou clientless username** *username* **示例：** hostname(config)# **eou clientless username sherlock** hostname(config)# **eou clientless password 221B-baker** hostname(config)#	更改用于无客户端身份验证的用户名。 *username* 必须与访问控制服务器上配置的用户名匹配才能支持无客户端主机。输入 1 至 64 个 ASCII 字符，不包括前导和尾部空格、井号 (#)、问号 (?)、引号 (")、星号 (*) 以及尖括号 （< 和 >）。 将无客户端身份验证的用户名和密码分别改为 sherlock 和 221B-baker。您可以仅指定用户名、仅指定密码和同时指定二者。
步骤 3	**eou clientless password** *password*	更改用于无客户端身份验证的密码。 *password* 必须与访问控制服务器上配置的密码匹配才能支持无客户端主机。请输入 4 至 32 个 ASCII 字符。
步骤 4	（可选） **no eou clientless username** **示例：** hostname(config)# **no eou clientless username** hostname(config)#	将用户名改为其默认值。
步骤 5	（可选） **no eou clientless password** **示例：** hostname(config)# **no eou clientless password** hostname(config)#	将密码改为其默认值。

更改 NAC 框架会话属性

ASA 为指定 ASA 和远程主机之间通信的属性提供默认设置。这些属性指定 与远程主机上的状态代理通信的端口号以及对与状态代理的通信进行限制的到期计数器。这些属性、默认设置以及您可以输入以对其进行修改的命令如下：

详细步骤

	命令	目的
步骤 1	`global`	切换成全局配置模式。

步骤 2	**eou port** *port_number*
	
	示例：
	`hostname(config)# eou port 62445`
	`hostname(config)#`
		默认端口号为 21862。该命令将更改用于与状态代理的经由 UDP 的 EAP 通信的端口号 （在客户端终端上）。
		port_number 必须与 CTA 上配置的端口号匹配。输入 1024 至 65535 范围内的值。
		
		将经由 UDP 的 EAP 通信的端口号改为 62445。

步骤 3	（可选）
	no eou port
	
	示例：
	`hostname(config)# no eou port`
	`hostname(config)#`
		将端口号改为其默认值。

步骤 4	**eou timeout retransmit** *seconds*
	
	示例：
	`hostname(config)# eou timeout retransmit 6`
	`hostname(config)#`
		更换重新传输重试计时器。当 ASA 向远程主机发送经由 UDP 的 EAP 消息时，它将等待响应。如果在 *n* 秒内未收到响应，它将重新发送经由 UDP 的 EAP 消息。默认情况下，重新传输计时器为 3 秒。
		seconds 是 1 至 60 范围内的一个值。
		将重新传输计时器改为 6 秒。

步骤 5	（可选）
	no eou timeout **retransmit**
	
	示例：
	`hostname(config)# no eou timeout retransmit`
	`hostname(config)#`
		将重新传输重试计时器改为其默认值。

步骤 6	**eou max-retry** *retries*
	
	示例：
	`hostname(config)# eou max-retry 1`
	`hostname(config)#`
		更改重新传输重试次数。当 ASA 向远程主机发送经由 UDP 的 EAP 消息时，它将等待响应。如果未收到响应，它将重新发送经由 UDP 的 EAP 消息。默认情况下，它可重试最多 3 次。
		retries 是 1 至 3 范围内的一个值。
		将经由 UDP 的 EAP 重新传输的次数限制为 1 次。

步骤 7	（可选）
	no eou max-retry
	
	示例：
	`hostname(config)# no eou max-retry`
	`hostname(config)#`
		将最大重新传输重试次数改为其默认值。

	命令	目的
步骤 8	**eou timeout hold-period** *seconds* **示例：** hostname(config)# **eou timeout hold-period 120** hostname(config)#	更改会话重新初始化计时器。重新传输重试次数计数器与最大重试次数值匹配时，ASA 将终止与远程主机的经由 UDP 的 EAP 会话并启动保持计时器。当保持计时器等于 *n* 秒时，ASA 将与远程主机建立新的经由 UDP 的 EAP 会话。默认情况下，建立新会话之前等待的最长时间为 180 秒。 *seconds* 是 60 至 86400 范围内的一个值。 将发起新的经由 UDP 的 EAP 关联之前的等待时间改为 120 秒
步骤 9	（可选） **no** eou timeout hold-period **示例：** hostname(config)# **no eou timeout hold-period** hostname(config)#	将会话重新初始化改为其默认值。

PPPoE 客户端

本节介绍如何配置 ASA 随附的 PPPoE 客户端。包括下列主题：

PPPoE 客户端概述

PPPoE 结合两种被广泛接受的标准：以太网和 PPP，为向客户端系统分配 IP 地址提供一种经过验证的方法。 PPPoE 客户端通常是通过 DSL 或电缆服务等远程宽带连接与 ISP 连接的个人电脑。ISP 会部署 PPPoE，因为 PPPoE 支持使用 ISP 的现有远程访问基础设施进行高速宽带接入并且客户使用起来更加简单。

PPPoE 提供在以太网网络上使用点对点协议 (PPP) 身份验证方法的标准方法。 PPPoE 用于 ISP 时，允许对 IP 地址进行经过身份验证的分配。在这种实施方案中，PPPoE 客户端和服务器通过在 DSL 或其他宽带连接上运行的第 2 层网桥协议互联。

PPPoE 由以下两个主要阶段组成：

- 主动发现阶段 — 在此阶段， PPPoE 客户端将查找叫做访问集中器的 PPPoE 服务器。在此阶段将分配会话 ID 并建立 PPPoE 层。
- PPP 会话阶段 — 在此阶段，将协商 PPP 选项并执行身份验证。一旦链路建立完成，PPPoE 将用作第 2 层封装方法，允许数据通过 PPPoE 报头中的 PPP 链路传输。

在系统初始化时， PPPoE 客户端通过交换一系列数据包与访问集中器建立会话。建立会话后，将建立 PPP 链路，此链路包括使用密码身份验证协议 (PAP) 的身份验证。建立了 PPP 会话后，每个数据包都将封装在 PPPoE 和 PPP 报头中。

注 在 ASA 上配置了故障转移时，或在多情景或透明模式下，不支持 PPPoE。只有在单一路由模式下且没有配置故障转移时才支持 PPPoE。

配置 PPPoE 客户端用户名和密码

要配置用于为访问集中器对 ASA 进行身份验证的用户名和密码，请使用 **vpdn** 命令。要使用 **vpdn** 命令，请首先定义一个 VPDN 组，然后在组内创建各个用户。

要配置 PPPoE 用户名和密码，请执行以下步骤：

步骤 1　使用以下命令定义用于 PPPoE 的 VPDN 组：

```
hostname(config)# vpdn group group_name request dialout pppoe
```

在此命令中，请使用该组的描述性名称替换 *group_name*，例如 “pppoe-sbc”。

步骤 2　如果您的 ISP 要求进行身份验证，请通过输入以下命令选择身份验证协议：

```
hostname(config)# vpdn group group_name ppp authentication {chap | mschap | pap}
```

使用您在上一步骤中定义的同一组名称替换 *group_name*。针对您的 ISP 所使用的身份验证类型，输入相应的关键字：

- CHAP — 质询握手身份验证协议
- MS-CHAP — Microsoft 质询握手身份验证协议版本 1
- PAP — 密码身份验证协议

注　使用 CHAP 或 MS-CHAP 时，用户名可以称为远程系统名称，而密码可以称为 CHAP 密钥。

步骤 3　通过输入以下命令将 ISP 分配的用户名与 VPDN 组关联：

```
hostname(config)# vpdn group group_name localname username
```

使用 VPDN 组名称替换 *group_name* 并且用 ISP 分配的用户名替换 *username*。

步骤 4　通过输入下列命令为 PPPoE 连接创建用户名和密码对。

```
hostname(config)# vpdn username username password password [store-local]
```

用用户名替换 *username* 并且用 ISP 分配的密码替换 *password*。

注　**store-locaAuto Update Serverl** 选项将用户名和密码存储于 ASA 上 NVRAM 的特定位置。如果自动更新服务器向 ASA 发送 **clear config** 命令，然后连接中断，则 ASA 可以从 NVRAM 读取用户名和密码并为访问集中器重新进行身份验证。

启用 PPPoE

注　启用 PPPoE 之前，必须使用 **vpdn** 命令完成配置，如 “配置 PPPoE 客户端用户名和密码”所述。

默认情况下， PPPoE 客户端功能处于关闭状态。要启用 PPPoE，请执行以下步骤：

步骤 1　通过在接口配置模式下输入以下命令启用 PPPoE 客户端：

```
hostname(config-if)# ip address pppoe [setroute]
```

其中 **setroute** 选项设置 PPPoE 客户端尚未建立连接时的默认路由。使用 **setroute** 选项时，在配置中就不能有静态定义的路由。

无法同时支持 PPPoE 与 DHCP，因为使用 PPPoE 时， IP 地址由 PPP 分配。如果没有默认路由，**setroute** 选项将促使创建默认路由。默认路由器是访问集中器的地址。最大传输单位 (MTU) 大小自动设置为 1492 字节，这是一个以太网帧内允许 PPPoE 传输的正确值。

重新输入该命令，重置 DHCP 租用和请求新的租用。

注　如果在两个接口 （例如主要接口和备用接口）上启用 PPPoE，而且您未配置双 ISP 支持（请参阅常规操作配置指南中的 “监控静态或默认路由”），则 ASA 只能通过第一个接口发送流量，获取 IP 地址。

例如：

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ip address pppoe
```

步骤 2　在接口配置模式下使用以下命令为 PPPoE 客户端指定 VPDN 组 （可选）：

```
hostname(config-if)# pppoe client vpdn group grpname
```

grpname 是指 VPDN *组的名称。*

注　如果您配置了多个 VPDN 组，并且未使用 **pppoe client vpdn group** 命令指定组，则 ASA 可能会随机选择一个 VPDN 组。要避免这种情况，请指定 VPDN 组。

使用带固定 IP 地址的 PPPoE

您也可以按照以下形式在接口配置模式下使用 ip address 命令通过手动输入 IP 地址启用 PPPoE：

```
hostname(config-if)# ip address ipaddress mask pppoe
```

此命令会导致 ASA 使用指定的地址，而不与 PPPoE 服务器协商来动态分配地址。用分配给您的 ASA 的 IP 地址和子网掩码替换 *ipaddress* 和 *mask*。

例如：

```
hostname(config-if)# ip address outside 201.n.n.n 255.255.255.0 pppoe
```

注　**setroute** 选项是 **ip address** 命令的一个选项，可以用于允许访问集中器在 PPPoE 客户端尚未建立连接时设置默认路由。使用 **setroute** 选项时，在配置中就不能有静态定义的路由。

监控和调试 PPPoE 客户端

使用以下命令显示当前 PPPoE 客户端配置信息：

```
hostname# show ip address outside pppoe
```

使用以下命令启用或禁用 PPPoE 客户端的调试：

```
hostname# [no] debug pppoe {event | error | packet}
```

以下是每个关键字的功能总结：

- **event** — 显示协议事件信息
- **error** — 显示错误消息
- **packet** — 显示数据包信息

使用以下命令查看 PPPoE 会话的状态：

```
hostname# show vpdn session [l2tp | pppoe] [id sess_id | packets | state | window]
```

以下示例显示了该命令提供的信息样本：

```
hostname# show vpdn

Tunnel id 0, 1 active sessions
     time since change 65862 secs
     Remote Internet Address 10.0.0.1
    Local Internet Address 199.99.99.3
     6 packets sent, 6 received, 84 bytes sent, 0 received
Remote Internet Address is 10.0.0.1
     Session state is SESSION_UP
       Time since event change 65865 secs, interface outside
       PPP interface id is 1
       6 packets sent, 6 received, 84 bytes sent, 0 received
hostname#
hostname# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
hostname#
hostname# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
   6 packets sent, 6 received, 84 bytes sent, 0 received
hostname#
```

清除配置

如要从配置中删除所有 **vpdn group** 命令，请在全局配置模式下使用 **clear configure vpdn group** 命令：

```
hostname(config)# clear configure vpdn group
```

如要删除所有 **vpdn username** 命令，请使用 **clear configure vpdn username** 命令：

```
hostname(config)# clear configure vpdn username
```

输入以下任一命令不会影响活动的 PPPoE 连接。

使用相关命令

使用以下命令使 DHCP 服务器在 PPP/IPCP 协商过程中使用访问集中器提供的 WINA 和 DNS 地址：

```
hostname(config)# dhcpd auto_config [client_ifx_name]
```

只有在运营商提供此信息时，才需要使用此命令，如 RFC 1877 中所述。 *client_ifx_name* 参数标识 DHCP **auto_config** 选项支持的接口。此时，因为 PPPoE 客户端只在在单个外部接口上受支持，所以不需要此关键字。

LAN 对 LAN IPsec VPN

LAN 对 LAN VPN 可连接不同地理位置的网络。

当两个思科或第三方对等体具有 IPv4 内部和外部网络 （IPv4 地址位于内部和外部接口上）时，ASA 支持与这些对等体的 LAN 到 LAN VPN 连接。

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

具体而言，当两个对等体均是 ASA 时，支持以下拓扑：

- ASA 具有 IPv4 内部网络且外部网络是 IPv6（IPv4 地址位于内部接口上且 IPv6 地址位于外部接口上）。
- ASA 具有 IPv6 内部网络且外部网络是 IPv4（IPv6 地址位于内部接口上且 IPv4 地址位于外部接口上）。
- ASA 具有 IPv6 内部网络且外部网络是 IPv6 （IPv6 地址位于内部和外部接口上）。

注 ASA 支持与思科对等体以及与符合所有相关标准的第三方对等体的 LAN 对 LAN IPsec 连接。

本章描述如何构建 LAN 对 LAN VPN 连接。其中包括以下各节：

配置摘要

本节提供本章描述的示例 LAN 对 LAN 配置的摘要。后面各节提供分步说明。

```
hostname(config)# interface ethernet0/0
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption 3des
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)# lifetime 43200
hostname(config)# crypto ikev1 enable outside
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# encryption 3des
hostname(config-ikev2-policy)# group 2
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)# lifetime 43200
hostname(config)# crypto ikev2 enable outside
hostname(config)# crypto ipsec ikev1 transform-set FirstSet esp-3des esp-md5-hmac
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes des
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key 44kkaol59636jnfx
hostname(config)# crypto map abcmap 1 match address l2l_list
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)# crypto map abcmap 1 set ikev1 transform-set FirstSet
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)# crypto map abcmap interface outside
hostname(config)# write memory
```

在多情景模式下配置站点间 VPN

按照以下步骤在多情景模式下允许站点间支持。通过执行这些步骤，可以了解资源分配如何划分。

步骤 1　如要在多情景模式下配置 VPN，请配置资源类，然后选择 VPN 许可证作为允许的资源的一部分。“为资源管理配置类”提供这些配置步骤。以下是示例配置：

```
class ctx1
    limit-resource VPN Burst Other 100
    limit-resource VPN Other 1000
```

步骤 2　配置情景并使其成为已配置的允许 VPN 许可证的类的成员。“配置安全情景”提供这些配置步骤。以下是示例配置：

```
context context1
    member ctx1
    allocate-interface GigabitEthernet3/0.2
    allocate-interface GigabitEthernet3/1.2
    allocate-interface Management0/0
    config-url disk0:/sm_s2s_ik1_ip4_no_webvpn.txt
    join-failover-group 1
```

步骤 3　配置连接配置文件、策略、加密映射等，如同使用站点间 VPN 的单情景 VPN 配置进行配置一样。

配置接口

ASA 具有至少两个接口，此处称为外部和内部。通常，外部接口连接到公共 Internet，而内部接口则连接到专用网络并防止公共访问。

如要开始配置，请在 ASA 上配置并启用两个接口。然后，分配名称、IP 地址和子网掩码。或者，在安全设备上配置其安全级别、速度和双工操作。

注　ASA 的外部接口地址 （适用于 IPv4/IPv6）不能与专用端地址空间重叠。

如要配置接口，请使用示例中的命令语法执行以下步骤：

步骤 1　如要进入接口配置模式，请在全局配置模式下输入含有要配置的接口的默认名称的 **interface** 命令。在以下示例中，该接口为 ethernet0。

```
hostname(config)# interface ethernet0/0
hostname(config-if)#
```

步骤 2　如要设置接口的 IP 地址和子网掩码，请输入 **ip address** 命令。在以下示例中， IP 地址为 10.10.4.100，子网掩码为 255.255.0.0。

```
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)#
```

步骤 3　如要对接口进行命名，请输入 **nameif** 命令，最多 48 个字符。设置此名称后，不能对其进行更改。在以下示例中， ethernet0 接口的名称为 outside。

```
hostname(config-if)# nameif outside
hostname(config-if)##
```

步骤 4　如要启用接口，请输入 **shutdown** 命令的 **no** 版本。默认情况下，接口处于禁用状态。

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

步骤 5　如要保存更改，请输入 **write memory** 命令：

```
hostname(config-if)# write memory
hostname(config-if)#
```

步骤 6　如要配置其他接口，请使用同一操作步骤。

在外部接口上配置 ISAKMP 策略并启用 ISAKMP

ISAKMP 是使两台主机商定如何构建 IPsec 安全关联 (SA) 的协商协议。它提供用于商定 SA 属性的格式的公共框架。这包括与对等体协商 SA，以及修改或删除 SA。ISAKMP 将协商分为两个阶段：第 1 阶段和第 2 阶段。第 1 阶段创建第一条隧道，该隧道保护后续 ISAKMP 协商消息。第 2 阶段创建用于保护数据的隧道。

IKE 使用 ISAKMP 为要使用的 IPsec 设置 SA。IKE 创建用于对对等体进行身份验证的加密密钥。

ASA 对于来自传统 Cisco VPN 客户端的连接支持 IKEv1，对于 AnyConnect VPN 客户端支持 IKEv2。

如要设置 ISAKMP 协商的条款，请创建 IKE 策略，其中包含以下内容：

- IKEv1 对等体必需的身份验证类型：使用证书的 RSA 签名或预共享密钥 (PSK)。
- 加密方法，用于保护数据并确保隐私。
- 哈希消息身份验证代码 (HMAC) 方法，用于确保发送方的身份，以及确保消息在传输过程中尚未修改。
- Diffie-Hellman 组，用于确定加密密钥确定算法的强度。 ASA 使用此算法派生加密密钥和哈希密钥。
- 对于 IKEv2，用作派生 IKEv2 隧道加密所需的密钥内容和哈希操作的算法的伪随机功能 (PRF)。
- ASA 在替换加密密钥之前对其使用的时间的限制。

通过 IKEv1 策略，可以为每个参数设置一个值。对于 IKEv2，可以配置多个加密和身份验证类型，并为单个策略配置多个完整性算法。 ASA 将设置从最安全到最不安全进行排序，并使用该顺序与对等体进行协商。借此可以潜在发送单个建议来传达允许的所有转换，而无需与 IKEv1 一样发送允许的每个组合。

以下各节提供在接口上创建 IKEv1 和 IKEv2 策略并将其启用的操作步骤：

- 第 9-4 页上的为 IKEv1 连接配置 ISAKMP 策略
- 第 9-5 页上的为 IKEv2 连接配置 ISAKMP 策略

为 IKEv1 连接配置 ISAKMP 策略

如要为 IKEv1 连接配置 ISAKMP 策略，请使用 **crypto ikev1 policy** *priority* 命令进入 IKEv1 策略配置模式，在此模式下可以配置 IKEv1 参数。

执行以下步骤并使用以下示例中的命令语法作为指南。

步骤 1　进入 IPsec IKEv1 策略配置模式。例如：

```
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
```

步骤 2　设置身份验证方法。以下示例配置预共享密钥：

```
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)#
```

步骤 3　设置加密方法。以下示例配置 3DES：

```
hostname(config-ikev1-policy)# encryption 3des
hostname(config-ikev1-policy)#
```

步骤 4　设置 HMAC 方法。以下示例配置 SHA-1：

```
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)#
```

步骤 5　设置 Diffie-Hellman 组。以下示例配置组 2：

```
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)#
```

步骤 6　设置加密密钥生存期。以下示例配置 43,200 秒 （12 小时）：

```
hostname(config-ikev1-policy)# lifetime 43200
hostname(config-ikev1-policy)#
```

步骤 7　在单情景或多情景模式下于名为 outside 的接口上启用 IKEv1：

```
hostname(config)# crypto ikev1 enable outside
hostname(config)#
```

步骤 8　要保存更改，请输入 **write memory** 命令：

```
hostname(config)# write memory
hostname(config)#
```

为 IKEv2 连接配置 ISAKMP 策略

如要为 IKEv2 连接配置 ISAKMP 策略，请使用 **crypto ikev2 policy** *priority* 命令进入 IKEv2 策略配置模式，在此模式下可以配置 IKEv2 参数。

执行以下步骤：

步骤 1　进入 IPsec IKEv2 策略配置模式。例如：

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)#
```

步骤 2　设置加密方法。以下示例配置 3DES：

```
hostname(config-ikev2-policy)# encryption 3des
hostname(config-ikev2-policy)#
```

步骤 3　设置 Diffie-Hellman 组。以下示例配置组 2：

```
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)#
```

步骤 4　设置用作派生 IKEv2 隧道加密所需的密钥内容和哈希操作的算法的伪随机功能 (PRF)。以下示例配置 SHA-1 （HMAC 变体）：

```
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)#
```

步骤 5　设置加密密钥生存期。以下示例配置 43,200 秒 （12 小时）：

```
hostname(config-ikev2-policy)# lifetime seconds 43200
hostname(config-ikev2-policy)#
```

步骤 6　在名为 outside 的接口上启用 IKEv2：

```
hostname(config)# crypto ikev2 enable outside
hostname(config)#
```

步骤 7　如要保存更改，请输入 **write memory** 命令：

```
hostname(config)# write memory
hostname(config)#
```

创建 IKEv1 转换集

IKEv1 转换集将加密方法与身份验证方法相结合。在 IPsec 与 ISAKMP 进行安全关联协商期间，对等体同意使用特定转换集来保护特定数据流。转换集对于两个对等体必须相同。

转换集保护关联加密映射条目中指定的 ACL 的数据流。您可以在 ASA 配置中创建转换集，然后在加密映射或动态加密映射条目中指定最多 11 个转换集。

表 9-1 列出有效的加密和身份验证方法。

表 9-1　　有效的加密和身份验证方法

有效加密方法	有效身份验证方法
esp-des	esp-md5-hmac
esp-3des （默认）	esp-sha-hmac （默认）
esp-aes （128 位加密）	
esp-aes-192	
esp-aes-256	
esp-null	

隧道模式是在通过不可信网络 （例如公共 Internet）连接的两个 ASA 之间实施 IPsec 的通常方式。隧道模式是默认模式，无需配置。

如要配置转换集，请在单情景或多情景模式下执行以下站点间任务：

步骤 1　在全局配置模式下，输入 **crypto ipsec ikev1 transform-set** 命令。以下示例使用名称 FirstSet、esp-3des 加密和 esp-md5-hmac 身份验证配置转换集。语法如下：

crypto ipsec ikev1 transform-set *transform-set-name* ***encryption-method authentication-method***

```
hostname(config)# crypto ipsec transform-set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

步骤 2　保存更改。

```
hostname(config)# write memory
hostname(config)#
```

创建 IKEv2 建议

对于 IKEv2，可以配置多个加密和身份验证类型，并为单个策略配置多个完整性算法。 ASA 将设置从最安全到最不安全进行排序，并使用该顺序与对等体进行协商。借此可以潜在发送单个建议来传达允许的所有转换，而无需与 IKEv1 一样发送允许的每个组合。

表 9-2 列出有效的 IKEv2 加密和身份验证方法。

表 9-2　　有效的 IKEv2 加密和完整性方法

有效加密方法	有效完整性方法
des	sha （默认）
3des （默认）	md5
aes	
aes-192	
aes-256	

如要配置 IKEv2 建议，请在单情景或多情景模式下执行以下任务：

步骤 1　在全局配置模式下，使用 **crypto ipsec ikev2 ipsec-proposal** 命令进入 ipsec 建议配置模式，在此模式下可以为建议指定多个加密和完整性类型。在以下示例中， *secure* 是建议的名称：

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)#
```

步骤 2　然后，输入建议和加密类型。 ESP 是唯一受支持的类型。例如：

```
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes des
hostname(config-ipsec-proposal)#
```

步骤 3　输入完整性类型。例如：

```
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config-ipsec-proposal)#
```

步骤 4　保存更改。

配置 ACL

ASA 使用访问控制列表来控制网络访问。默认情况下，自适应安全设备拒绝所有流量。您需要配置允许流量的 ACL。有关详细信息，请参阅常规操作配置指南中的 “有关访问控制列表的信息”。

为此 LAN 对 LAN VPN 控制连接配置的 ACL 基于源 IP 地址和已转换的目标 IP 地址。配置在连接两端相互镜像的 ACL。

VPN 流量的 ACL 使用已转换的地址。

如要配置 ACL，请执行以下步骤：

步骤 1　输入 **access-list extended** 命令。以下示例配置一个名为 l2l_list 的 ACL，通过它可使来自 192.168.0.0 网络中 IP 地址的流量传播到 150.150.0.0 网络。语法为 **access-list** *listname* **extended permit ip** *source-ipaddress source-netmask destination-ipaddress destination-netmask*。

```
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)#
```

步骤 2　在连接的另一端 （对 ACL 进行镜像）为 ASA 配置该 ACL。在以下示例中，对等体的提示符为 hostname2。

```
hostname2(config)# access-list l2l_list extended permit ip 150.150.0.0 255.255.0.0
192.168.0.0 255.255.0.0
hostname(config)#
```

注　有关使用 VPN 过滤器配置 ACL 的详细信息，请参阅第 4-40 页上的为远程访问指定 VLAN 或对组策略应用统一访问控制规则。

定义隧道组

隧道组是包含年隧道连接策略的记录的集合。您可以配置隧道组来标识 AAA 服务器，指定连接参数，以及定义默认组策略。 ASA 在内部存储隧道组。

ASA 中有两个默认隧道组：DefaultRAGroup （默认 IPsec 远程访问隧道组）和 DefaultL2Lgroup （默认 IPsec LAN 对 LAN 隧道组）。可以修改它们，但不能对其删除。

IKE 版本 1 和 2 之间的主要差异在于其允许的身份验证方法。IKEv1 在 VPN 两端仅允许一种类型的身份验证 （即，预共享密钥或证书）。但是， IKEv2 允许分别使用本地和远程身份验证 CLI 配置不对称身份验证方法 （即，对发起方使用预共享密钥身份验证，但对响应方使用证书身份验证）。因此，通过 IKEv2 可使用不对称身份验证，其中一端对一个凭据进行身份验证，另一端使用其他凭据 （预共享密钥、证书）。

您也可以根据环境创建一个或多个新隧道组。当在隧道协商期间未标识任何特定隧道组时， ASA 使用这些组为远程访问和 LAN 对 LAN 隧道组配置默认隧道参数。

如要建立基本 LAN 对 LAN 连接，必须为隧道组设置两个属性：

- 将连接类型设置为 IPsec LAN 对 LAN。
- 配置 IP 地址的身份验证方法 — 在以下示例中，为 IKEv1 和 IKEv2 配置预共享密钥。

注　如要使用 VPN，包括隧道组， ASA 必须处于单路由模式。用于配置隧道组参数的命令不会出现在任何其他模式中。

步骤 1　如要将连接类型设置为 IPsec LAN 对 LAN，请输入 **tunnel-group** 命令。语法为 **tunnel-group** *name* **type** *type*，其中 *name* 是分配给隧道组的名称， *type* 是隧道的类型。在 CLI 中输入的隧道类型为：

- **remote-access** （IPsec、 SSL 和无客户端 SSL 远程访问）
- **ipsec-l2l** （IPsec LAN 对 LAN）

在以下示例中，隧道组的名称是 LAN 对 LAN 对等体的 IP 地址 10.10.4.108。

```
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)#
```

注　仅当隧道身份验证方法为数字证书和 / 或对等体配置为使用攻击性模式时，才能使用名称非 IP 地址的 LAN 对 LAN 隧道组。

步骤 2　如要将身份验证方法设置为使用预共享密钥，请进入 ipsec-attributes 模式，然后输入 **ikev1 pre-shared-key** 命令以创建预共享密钥。需要在此 LAN 对 LAN 连接的两个 ASA 上均使用同一预共享密钥。

密钥是 1 至 128 个字符的字母数字字符串。

在以下示例中， IKEv1 预共享密钥是 44kkaol59636jnfx：

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfx
```

在以下示例中， IKEv2 预共享密钥也配置为 44kkaol59636jnfx：

```
hostname(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 44kkaol59636jnfx
```

注　必须配置 **ikev2 remote-authentication pre-shared-key** 命令或 **ikev2 remote-authentication certificate** 命令以完成身份验证。

步骤 3　保存更改。

```
hostname(config)# write memory
hostname(config)#
```

如要验证隧道是否启动并正常运行，请使用 **show vpn-sessiondb summary**、 **show vpn-sessiondb detail l2l** 或 **show cry ipsec sa** 命令。

创建加密映射并将其应用于接口

加密映射条目组合 IPsec 安全关联的各种元素，包括以下元素：

- IPsec 应保护的流量 （在 ACL 中定义）。
- 将 IPsec 保护的流量发送到的位置 （通过标识对等体）。
- 对此流量应用的 IPsec 安全性 （由转换集指定）。
- IPsec 流量的本地地址 （通过对接口应用加密映射进行标识）。

为使 IPsec 成功，两个对等体均必须包含具有兼容配置的加密映射条目。为使两个加密映射条目兼容，它们必须至少满足以下条件：

- 加密映射条目必须包含兼容的加密 ACL （例如，镜像映像 ACL）。如果对应的对等体使用动态加密映射，则对等体的加密 ACL 必须 “允许” ASA 加密 ACL 中的条目。
- 加密映射条目必须各自标识另一个对等体 （除非对应的对等体使用的是动态加密映射）。
- 加密映射条目必须共同具有至少一个转换集。

如果为给定接口创建多个加密映射条目，请使用每个条目的序号 (seq-num) 将其排名：seq-num 越低，优先级越高。在设置有加密映射的接口上， ASA 首先对优先级较高的条目评估流量。

如果以下任一条件存在，请为给定接口创建多个加密映射条目：

- 不同对等体处理不同数据流。
- 您希望对不同类型的流量 （面向相同或不同的对等体）应用不同的 IPsec 安全性，例如，如果希望对一组子网之间的流量进行身份验证，对另一组子网之间的流量同时进行身份验证和加密。在此情况下，请在两个单独 ACL 中定义不同类型的流量，并为每个加密 ACL 创建单独的加密映射条目。

如要在全局配置模式下创建加密映射并将其应用于外部接口，请在单情景或多情景模式下执行以下步骤：

步骤 1　如要将 ACL 分配给加密映射条目，请输入 **crypto map match address** 命令。

语法为 **crypto map** *map-name seq-num* **match address** *aclname*。在以下示例中，映射名称为 abcmap，序号为 1， ACL 名称为 `l2l_list`。

```
hostname(config)# crypto map abcmap 1 match address l2l_list
hostname(config)#
```

步骤 2　如要标识 IPsec 连接的对等体，请输入 **crypto map set peer** 命令。

语法为 **crypto map** *map-name seq-num* **set peer** {*ip_address1* | `hostname`*1*}[*... ip_address10* | `hostname`*10*]。在以下示例中，对等体名称为 10.10.4.108。

```
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)#
```

步骤 3　如要为加密映射条目指定 IKEv1 转换集，请输入 **crypto map ikev1 set transform-set** 命令。

语法为 **crypto map** *map-name seq-num* **ikev1 set transform-set** *transform-set-name*。
在以下示例中，转换集名称为 *FirstSet*。

```
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
hostname(config)#
```

步骤 4　如要为加密映射条目指定 IKEv2 建议，请输入 **crypto map ikev2 set ipsec-proposal** 命令：

语法为 **crypto map** *map-name seq-num set* **ikev2 ipsec-proposal** ***proposal-name***。
在以下示例中，建议名称为 *secure*。

通过 **crypto map** 命令，可以为单个映射索引指定多个 IPsec 建议。在该情况下，多个建议会在协商过程中传输到 IKEv2 对等体，并且建议的顺序由管理员在加密映射条目排序时确定。

注　如果 IPsec 建议中存在组合模式 (AES-GCM/GMAC) 和普通模式 （所有其他类型）算法，则无法将单个建议发送到对等体。在此情况下您必须具有至少两个建议，一个用于组合模式算法，另一个用于普通模式算法。

```
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)#
```

对接口应用加密映射

您必须将加密映射集应用于 IPsec 流量传播所通过的每个接口。ASA 在所有接口上都支持 IPsec。对接口应用加密映射集将指导 ASA 对加密映射集评估所有接口流量，并在连接或安全关联协商期间使用指定的策略。

将加密映射绑定到接口还会初始化运行时数据结构，例如安全关联数据库和安全策略数据库。今后以任何方式修改加密映射时， ASA 都会自动将更改应用于运行配置。它将断开任何现有连接，并在应用新的加密映射后重新建立这些连接。

如要将已配置的加密映射应用于外部接口，请执行以下步骤：

步骤 1　输入 **crypto map interface** 命令。语法为 **crypto map** *map-name* **interface** *interface-name*。

```
hostname(config)# crypto map abcmap interface outside
hostname(config)#
```

步骤 2　保存更改。

```
hostname(config)# write memory
hostname(config)#
```

AnyConnect VPN 客户端连接

本节描述如何配置 AnyConnect VPN 客户端连接，涵盖了以下主题：

有关 AnyConnect VPN 客户端连接的信息

思科 AnyConnect 安全移动客户端为远程用户提供了通向 ASA 的安全的 SSL 和 IPsec/IKEv2 连接。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 ASA 已配置为将 http:// 请求重定向至 https://，否则用户必须以 https://<*address*> 的形式输入 URL。

输入 URL 后，浏览器连接至该接口，并显示登录屏幕。如果用户满足登录和身份验证要求，并且 ASA 将用户确定为需要客户端，则它会下载与远程计算机的操作系统匹配的客户端。下载后，客户端进行安装并自行配置，建立安全的 SSL 或 IPsec/IKEv2 连接，连接终止时，客户端会保留或自行卸载 （取决于配置）。

如果先前已安装客户端，当用户进行身份验证时， ASA 将检查客户端的修订版本并在必要情况下升级客户端。

客户端与 ASA 协商 SSL VPN 连接时，会使用传输层安全 (TLS) 和 （可选）数据报传输层安全 (DTLS) 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。

AnyConnect 客户端可从 ASA 下载，也可以由系统管理员在远程 PC 上手动安装。有关手动安装客户端的详细信息，请参阅 《*思科 AnyConnect VPN 客户端管理员指南*》。

ASA 基于建立连接的用户的组策略或用户名属性下载客户端。您可以将 ASA 配置为自动下载客户端，也可以将其配置为提示远程用户是否下载客户端。对于后一种情况，如果用户不响应，您可以将 ASA 配置为在超时时段过后下载客户端，或显示登录页面。

AnyConnect 连接的许可要求

注　此功能在无负载加密型号上不可用。

型号	许可要求
ASA 5512-X	使用以下任一许可证： • AnyConnect 高级版许可证： – 基础许可证：2 个会话。 – *可选永久性或基于时间的许可证：10、 25、 50、 100 或 250 个会话。* – *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* • AnyConnect 基础版许可证：250 个会话。
ASA 5515-X	使用以下任一许可证： • AnyConnect 高级版许可证： – 基础许可证：2 个会话。 – *可选永久性或基于时间的许可证：10、 25、 50、 100 或 250 个会话。* – *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* • AnyConnect 基础版许可证：250 个会话。
ASA 5525-X	使用以下任一许可证： • AnyConnect 高级版许可证： – 基础许可证：2 个会话。 – *可选永久性或基于时间的许可证：10、 25、 50、 100、 250、 500 或 750 个会话。* – *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* • AnyConnect 基础版许可证：750 个会话。
ASA 5545-X	使用以下任一许可证： • AnyConnect 高级版许可证： – 基础许可证：2 个会话。 – *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000 或 2500 个会话。* – *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* • AnyConnect 基础版许可证：2500 个会话。

型号	许可要求
ASA 5555-X	使用以下任一许可证： • AnyConnect 高级版许可证： – 基础许可证：2 个会话。 – *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500 或 5000 个会话。* – *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* • AnyConnect 基础版许可证：5000 个会话。
ASA 5585-X，带 SSP-10	使用以下任一许可证： • AnyConnect 高级版许可证： – 基础许可证：2 个会话。 – *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500 或 5000 个会话。* – *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* • AnyConnect 基础版许可证：5000 个会话。
ASA 5585-X，带 SSP-20、 -40 和 -60	使用以下任一许可证： • AnyConnect 高级版许可证： – 基础许可证：2 个会话。 – *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500、5000 或 10000 个会话。* – *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* • AnyConnect 基础版许可证：10000 个会话。
ASASM	使用以下任一许可证： • AnyConnect 高级版许可证： – 基础许可证：2 个会话。 – *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500、5000 或 10000 个会话。* – *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。* • AnyConnect 基础版许可证：10000 个会话。
带 1 个虚拟 CPU 的 ASAv	• 标准版许可证：2 个会话。 • 高级版许可证：250 个会话。
带 4 个虚拟 CPU 的 ASAv	• 标准版许可证：2 个会话。 • 高级版许可证：750 个会话。

注　如果您启动无客户端 SSL VPN 会话，然后从门户启动 AnyConnect 客户端会话，总计使用的是 1 个会话。但是，如果先启动 AnyConnect 客户端（例如从独立客户端启动），然后登录无客户端 SSL VPN 门户，则使用的是 2 个会话。

*所有*类型的最大组合 VPN 会话数量不能超过此表中所示的最大会话数。对于 ASA 5505，基础许可证的最大组合会话数量为 10 个、安全增强型许可证的最大组合会话数量为 25 个。

一个共享许可证允许 ASA 用作多个客户端 ASA 的共享许可证服务器。共享许可证池很大，但是，每个 ASA 使用的会话数不能超过针对永久许可证列出的最大数量。

AnyConnect 基础版许可证允许 AnyConnect VPN 客户端访问 ASA。此许可证不支持基于浏览器的 SSL VPN 访问或思科安全桌面。对于这些功能，请激活 AnyConnect 高级版许可证而不是 AnyConnect 基础版许可证。利用 AnyConnect 基础版许可证， VPN 用户可以使用网络浏览器登录，并下载和启动 （网络启动） AnyConnect 客户端。 AnyConnect 客户端软件提供相同的客户端功能，无论是使用这个许可证还是 AnyConnect 高级版 SSL VPN 版本许可证启用此软件。在特定 ASA 上， AnyConnect 基础版许可证不能和以下许可证同时处于活动状态：AnyConnect 高级版许可证 （所有类型）或高级终端评估许可证。但是，您可以在同一网络中的不同 ASA 上运行 AnyConnect 基础版和 AnyConnect 高级版许可证。默认情况下， ASA 使用 AnyConnect 基础版许可证 （如有），但是您可以使用 **no anyconnect-essentials** 命令。有关 AnyConnect 基础版许可证和 AnyConnect 高级版许可证支持的功能的详细列表，请参阅 *AnyConnect 安全移动客户端功能、许可证和操作系统*：
http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

准则和限制

此部分包括此功能的准则和限制。

远程 PC 系统要求

有关对运行 AnyConnect 安全移动客户端的终端计算机的要求，请参阅您将使用 ASA 部署的 AnyConnect 客户端版本的版本说明。

远程 HTTPS 证书限制

ASA 不会验证远程 HTTPS 证书。

配置 AnyConnect 连接

本节描述将 ASA 配置为接受 AnyConnect VPN 客户端连接的先决条件、限制和详细任务。

将 ASA 配置为以网络方式部署客户端

本节描述将 ASA 配置为以网络方式部署 AnyConnect 客户端的步骤。

先决条件

使用 TFTP 或其他方法将客户端映像包复制到 ASA。

详细步骤

	命令	用途

步骤 1	`anyconnect image filename order`
	
	示例：
	`hostname(config-webvpn)#anyconnect image anyconnect-win-2.3.0254-k9.pkg 1`
	`hostname(config-webvpn)#anyconnect image anyconnect-macosx-i386-2.3.0254-k9.pkg 2`
	`hostname(config-webvpn)#anyconnect image anyconnect-linux-2.3.0254-k9.pkg 3`
		将闪存上的文件标识为 AnyConnect 客户端包文件。
		
		ASA 在缓存中展开文件，以便下载至远程 PC。如果您有多个客户端，使用 order 参数给客户端映像分配顺序。
		
		ASA 以您指定的顺序下载每个客户端的各个部分，直到其与远程 PC 的操作系统相匹配。因此，请给最常见的操作系统使用的映像分配最小的数值。
		
		注　使用 **anyconnect image xyz** 命令配置 AnyConnect 映像后，您必须发出 **anyconnect enable** 命令。如果您没有启用 **anyconnect enable** 命令， AnyConnect 不会如预期操作， **show webvpn anyconnect** 会将 SSL VPN 客户端视为未启用，而不是列出已安装的 AnyConnect 包。

步骤 2	**enable** *interface*
	
	示例：
	`hostname(config)# webvpn`
	`hostname(config-webvpn)# enable outside`
		在接口上启用 SSL，以便进行无客户端或 AnyConnect SSL 连接。

步骤 3	**anyconnect enable**	在没有发出此命令的情况下， AnyConnect 不会如预期工作，而且 **show webvpn anyconnect** 命令会返回 “SSL VPN is not enabled”，而不是列出已安装的 AnyConnect 包。
步骤 4	**ip local pool** *poolname startaddr-endaddr* **mask** *mask* **示例：** `hostname(config)# ip local pool vpn_users 209.165.200.225-209.165.200.254 mask 255.255.255.224`	（可选）创建地址池。您可以使用其他地址分配方法，如 DHCP 和 / 或用户分配的寻址。

步骤 5	**address-pool** *poolname*
	
	示例：
	`hostname(config)# tunnel-group telecommuters general-attributes`
	`hostname(config-tunnel-general)# address-pool vpn_users`
		将地址池分配至隧道组。

步骤 6	**default-group-policy** *name* **示例：** `hostname(config-tunnel-general)# default-group-policy sales`	将默认组策略分配至隧道组。

	命令	用途
步骤 7	**group-alias** *name* **enable** **示例：** hostname(config)# **tunnel-group telecommuters webvpn-attributes** hostname(config-tunnel-webvpn)# **group-alias sales_department enable**	启用隧道组列表在无客户端门户和 AnyConnect GUI 登录页面上的显示。该别名列表由 *group-alias name enable* 命令定义。
步骤 8	**tunnel-group-list enable** **示例：** hostname(config)# **webvpn** hostname(config-webvpn)# **tunnel-group-list enable**	将 AnyConnect 客户端指定为组或用户的允许的 VPN 隧道协议。
步骤 9	**vpn-tunnel-protocol** **示例：** hostname(config)# **group-policy sales attributes** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **vpn-tunnel-protocol**	将 SSL 指定为组或用户的允许的 VPN 隧道协议。您还可以指定其他协议。有关详细信息，请参阅 《命令参考》中的 **vpn-tunnel-protocol** 命令。 有关将用户分配至组策略的详细信息，请参阅第 6 章 “配置连接配置文件、组策略和用户”。

启用永久性客户端安装

启用永久性客户端安装将会禁用客户端的自动卸载功能。客户端仍保持安装在远程计算机上以进行后续连接，从而缩短远程用户的连接时间。

如要为特定组或用户启用永久性客户端安装，可以在组策略或用户名 webvpn 模式下，使用 **anyconnect keep-installer** 命令：

anyconnect keep-installer installer

默认是启用客户端的永久性安装。会话结束时，客户端仍位于远程计算机上。以下示例将现有组策略 *sales* 配置为在会话结束时在远程计算机上移除客户端。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# anyconnect keep-installer installed none
```

配置 DTLS

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

默认情况下，在接口上启用 SSL VPN 访问时，则会启用 DTLS。如果您禁用 DTLS，SSL VPN 连接仅会与 SSL VPN 隧道连接。

注　为使 DTLS 能够回退至 TLS 连接，必须启用失效对等体检测 (DPD)。如果您没有启用 DPD，DTLS 连接会遭遇问题，该连接会终止而不是回退至 TLS。有关启用 DPD 的详细信息，请参阅第 10-14 页上的启用和调整失效对等体检测。

您可以在 webvpn 配置模式下使用 **enable** 命令 **tls-only** 选项，为所有 AnyConnect 客户端用户禁用 DTLS：

enable <*interface*> **tls-only**

例如：

hostname(config-webvpn)# **enable outside tls-only**

默认情况下，在组策略 webvpn 或用户名 webvpn 配置模式下，使用 **anyconnect ssl dtls** 命令为特定组或用户启用 DTLS：

[**no**] **anyconnect ssl dtls {enable interface | none}**

如果您需要禁用 DTLS，请使用该命令的 **no** 形式。例如：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no anyconnect ssl dtls none
```

提示远程用户

您可以在组策略 webvpn 或用户名 webvpn 配置模式下，使用 **anyconnect ask** 命令来允许 ASA 提示远程 SSL VPN 客户端的用户下载客户端。

[**no**] **anyconnect ask** {**none** | **enable** [**default** {**webvpn** | } **timeout** *value*]}

anyconnect enable 提示远程用户下载客户端或转至无客户端门户页面，并且无限期等待用户响应。

anyconnect ask enable default 立即下载客户端。

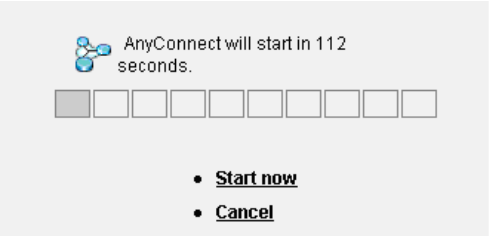
anyconnect ask enable default webvpn 立即转至门户页面。

anyconnect ask enable default timeout *value* 提示远程用户下载客户端或转至无客户端门户页面，并且在采取默认操作 （显示无客户端门户页面）前等待长度为 *value* 的一段时间。

anyconnect ask enable default clientless timeout *value* 提示远程用户下载客户端或转至无客户端门户页面，并且在采取默认操作 （下载客户端）前等待长度为 *value* 的一段时间。

图 10-1 显示已配置 **default anyconnect timeout** *value 或* **default webvpn timeout** *value 时，向远程用户显示的提示：*

图 10-1　　向远程用户显示的用于 SSL VPN 客户端下载的提示



以下示例将 ASA 配置为提示用户下载客户端或转至无客户端门户页面，并且在下载客户端前等待 *10 秒*供客户作出响应：

```
hostname(config-group-webvpn)# anyconnect ask enable default anyconnect timeout 10
```

启用 AnyConnect 客户端配置文件下载

您可以在 AnyConnect 配置文件中启用 Cisco AnyConnect 安全移动客户端 包含核心客户端及其 VPN 功能以及可选客户端模块网络访问管理器 (NAM)、状态、遥感勘测和网络安全的配置设置的 XML 文件。 ASA 在 AnyConnect 的安装和更新期间部署配置文件。用户无法管理或修改配置文件。

ASDM 中的配置文件编辑器

您可以使用 AnyConnect 配置文件编辑器对配置文件进行配置，该编辑器是一款从 ASDM 启动的基于 GUI 的便捷配置工具。 2.5 版及更高版本的适用于 Windows 的 AnyConnect 软件包提供了该编辑器，在您于 ASA 上加载 AnyConnect 包并将其指定为 AnyConnect 客户端映像时，该编辑器会激活。

独立配置文件编辑器

我们还提供了该配置文件编辑器的适用于 Windows 的独立版本，您可以将其用作与 ASDM 集成的配置文件编辑器的备选编辑器。如果您要预先部署客户端，可以使用独立配置文件编辑器为您可使用软件管理系统部署至计算机的 VPN 服务和其他模块创建配置文件。有关使用配置文件编辑器的详细信息，请参阅 《思科 AnyConnect 安全移动客户端管理员指南》。

注　AnyConnect 客户端协议默认设置为 SSL。要启用 IPsec IKEv2，您必须在 ASA 上配置 IKEv2 设置，并且还要在客户端配置文件中将 IKEv2 配置为主协议。必须将 IKEv2enabled 配置文件部署至终端计算机，否则客户端会尝试使用 SSL 进行连接。有关详细信息，请参阅 《思科 AnyConnect 安全移动客户端管理员指南》。

请遵循以下步骤来编辑配置文件，并使 ASA 能够将其下载至远程客户端：

步骤 1　使用 ASDM 中的配置文件编辑器或独立配置文件编辑器来创建配置文件。有关详细信息，请参阅《思科 AnyConnect 安全移动客户端管理员指南》。

步骤 2　使用 TFTP 或其他方法将配置文件加载至 ASA 上的闪存。

步骤 3　在 webvpn 配置模式下，使用 **anyconnect profiles** 命令将文件确定为要加载至缓存的客户端配置文件。

以下示例将文件 *sales_hosts.xml* 和 *engineering_hosts.xml* 指定为配置文件：

```
asa1(config-webvpn)# anyconnect profiles sales disk0:/sales_hosts.xml
asa1(config-webvpn)# anyconnect profiles engineering disk0:/engineering_hosts.xml
```

这些配置文件此时对于组策略可用。

您可以使用 **dir cache:stc/profiles** 命令查看已在缓存中加载的配置文件：

```
hostname(config-webvpn)# dir cache:/stc/profiles

Directory of cache:stc/profiles/

0      ----  774         11:54:41 Nov 22 2006  engineering.xml
0      ----  774         11:54:29 Nov 22 2006  sales.xml

2428928 bytes total (18219008 bytes free)
hostname(config-webvpn)#
```

步骤 4　进入组策略 webvpn 配置模式，并使用 **anyconnect profiles** 命令为组策略指定客户端配置文件：

您可以输入后面带有问号 (**?**) 的 **anyconnect profiles value** 命令，以便查看可用的配置文件。例如：

```
asa1(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  saless
```

下一示例将组策略配置将配置文件 *sales* 与客户端配置文件类型 *vpn* 配合使用：

```
asa1(config-group-webvpn)# anyconnect profiles value sales type vpn
asa1(config-group-webvpn)#
```

启用 AnyConnect 客户端延迟升级

延迟升级允许 AnyConnect 用户延迟客户端升级的下载。客户端更新可用时， AnyConnect 打开一个对话框，询问用户是想要进行更新，还是想要延迟升级。

通过将自定义属性类型和命名值添加至 ASA，然后在组策略中引用和配置这些属性，可以启用延迟升级。

以下自定义属性支持延迟升级：

表 10-1　适用于延迟升级的自定义属性

自定义属性类型	有效值	默认值	说明
DeferredUpdateAllowed	true false	false	True 可以启用延迟更新。如果延迟更新被禁用 (false)，以下设置会被忽略。
DeferredUpdateMinimumVersion	x.y.z	0.0.0	实现更新可延迟所必须要安装的最低 AnyConnect 版本。 最低版本检查适用于数据头端上启用的所有模块。如果启用的任一模块 （包括 VPN）均未安装或不符合最低版本要求，则连接不符合延迟更新条件。 如果未指定此属性，无论在终端上安装的版本如何，系统都会显示 （或自动关闭）延迟提示。
DeferredUpdateDismissTimeout	0-300 （秒）	none （禁用）	延迟升级提示在自动关闭之前显示的秒数。仅当会显示延迟更新提示时才应用此属性 （先评估最低版本属性）。 如果此属性缺失，则禁用自动关闭功能，对话框会一直显示 （如需要），直到用户作出响应。 将此属性设置为零，允许基于以下条件强制进行自动延迟或升级： • 已安装的版本和 DeferredUpdateMinimumVersion 的值。 • DeferredUpdateDismissResponse 的值。
DeferredUpdateDismissResponse	defer update	update	发生 DeferredUpdateDismissTimeout 时采取的操作。

步骤 1　在 webvpn 配置模式下，使用 **anyconnnect-custom-attr** 命令创建自定义属性类型：

[no] anyconnect-custom-attr *attr-type* **[description** *description*]

以下示例显示如何添加自定义属性类型 DeferredUpdateAllowed 和 DeferredUpdateDismissTimeout：

```
hostame(config)# anyconnect-custom-attr DeferredUpdateAllowed description Indicates if the
deferred update feature is enabled or not
hostame(config)# anyconnect-custom-attr DeferredUpdateDismissTimout
```

步骤 2　在全局配置模式下，使用 **anyconnect-custom-data** 命令为自定义属性添加命名值：

[no] anyconnect-custom-data *attr-type attr-name attr-value*

以下示例显示如何为自定义属性类型 DeferredUpdateDismissTimout 和启用的 DeferredUpdateAllowed 添加命名值。

```
hostname(config)# anyconnect-custom-data DeferredUpdateDismissTimout def-timeout 150
hostname(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
```

步骤 3　使用 **anyconnect-custom** 命令向组策略添加名为 value 的自定义属性，或将其从组策略中移除：

anyconnect-custom *attr-type* **value** *attr-name*

anyconnect-custom *attr-type* **none**

no anyconnect-custom *attr-type*

以下示例显示如何为名为 sales 的组策略启用延迟更新，并将超时时间设置为 150 秒：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# anyconnect-custom DeferredUpdateAllowed value def-allowed
hostname(config-group-policy)# anyconnect-custom DeferredUpdateDismissTimeout value
def-timout
```

启用其他 AnyConnect 客户端功能

如要最大限度缩短下载时间，客户端可以仅请求下载 （从 ASA）其需要的核心模块。当附加功能对于 AnyConnect 客户端可用时，您需要更新远程客户端，以便它们能够使用这些功能。

要启用新功能，您必须在组策略 webvpn 或用户名 webvpn 配置模式下，使用 **anyconnect modules** 命令指定新模块的名称：

[no] anyconnect modules {**none** | **value** *string*}

使用逗号分隔多个字符串。

有关要为每个客户端功能输入的值列表，请参阅思科 AnyConnect VPN 客户端的版本说明。

启用登录前开始

登录前开始 (SBL) 支持适用于安装在 Windows PC 上的 AnyConnect 客户端的登录脚本、密码缓存、驱动器映射等。对于 SBL，您必须允许 ASA 下载可为 AnyConnect 客户端启用图形标识和身份验证 (GINA) 的模块。以下操作步骤显示如何启用 SBL：

步骤 1　在组策略 webvpn 或用户名 webvpn 配置模式下，可以使用 **anyconnect modules** *vpngina* 命令允许 ASA 将用于 VPN 连接的 GINA 模块下载至特定组或用户。

在以下示例中，用户先进入组策略 *telecommuters* 的组策略属性模式，然后进入组策略的 webvpn 配置模式，最后指定字符串 *vpngina*：

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)#anyconnect modules value vpngina
```

步骤 2　检索客户端配置文件 (AnyConnectProfile.tmpl) 的副本。

步骤 3　编辑配置文件，以便指定启用 SBL。以下示例显示适用于 Windows 的配置文件 (AnyConnectProfile.tmpl) 的相关部分：

```
<Configuration>
    <ClientInitialization>
        <UseStartBeforeLogon>false</UseStartBeforeLogon>
    </ClientInitialization>
```

<UseStartBeforeLogon> 标记确定客户端是否使用 SBL。要打开 SBL，请用 *true* 替换 *false*。以下示例显示打开 SBL 的标记：

```
    <ClientInitialization>
        <UseStartBeforeLogon>true</UseStartBeforeLogon>
    </ClientInitialization>
```

步骤 4　在 webvpn 配置模式下，使用 **profile** 命令保存对 AnyConnectProfile.tmpl 的更改，并为 ASA 上的组或用户更新配置文件。例如：

```
asa1(config-webvpn)#anyconnect profiles sales disk0:/sales_hosts.xml
```

转换 AnyConnect 用户消息的语言

ASA 为向发起基于浏览器的无客户端 SSL VPN 连接的用户显示的门户和屏幕，以及向思科 AnyConnect VPN 客户端用户显示的界面，提供了语言转换功能。

本节描述如何配置 ASA 以便转换这些用户消息，其中包括以下部分：

- 第 10-11 页上的了解语言转换
- 第 10-12 页上的创建转换表

了解语言转换

向远程用户显示的功能区域及其消息归入转换域。在思科 AnyConnect VPN 客户端的用户界面上显示的所有*消息都位于 AnyConnect 域中*。

ASA 的软件映像包包括用于 AnyConnect 域的转换表模板。您可以导出此模板，这会在您提供的 URL 创建此模板的一个 XML 文件。此文件中的消息字段为空。您可以编辑消息并导入模板，以创建位于闪存中的新转换表对象。

您还可以导出现有转换表。创建的 XML 文件将显示您之前编辑的消息。重新导入具有相同语言名称的此 XML 文件将创建一个新版的转换表对象，同时覆盖以前的消息。对 AnyConnect 域的转换表的更改会立即向 AnyConnect 客户端用户显示。

创建转换表

以下操作步骤描述如何创建 AnyConnect 域的转换表：

步骤 1　在特权 EXEC 模式下，使用 **export webvpn translation-table** 命令将转换表模板导出到计算机中。

在以下示例中， **show webvpn translation-table** 命令显示可用的转换表模板和转换表。

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect
CSD
PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
```

接着，用户可以导出 AnyConnect 转换域的转换表。创建的 XML 文件的文件名为 *client*，该文件包含有空白的消息字段：

```
hostname# export webvpn translation-table AnyConnect template
tftp://209.165.200.225/client
```

在下一示例中，用户导出名为 *zh* 的转换表，该转换表是先前通过模板导入的。 zh 是 Microsoft Internet Explorer 使用的中文缩写。

```
hostname# export webvpn translation-table customization language zh
tftp://209.165.200.225/chinese_client
```

步骤 2　编辑转换表 XML 文件。以下示例显示 AnyConnect 模板的部分内容。此输出的末尾包含消息 *Connected* 的消息 ID 字段 (msgid) 和消息字符串字段 (msgstr)，客户端建立 VPN 连接时，该消息会在 AnyConnect 客户端 GUI 上显示。完整的模板包含许多的消息字段对：

```
# SOME DESCRIPTIVE TITLE.
# Copyright (C) YEAR THE PACKAGE'S COPYRIGHT HOLDER
# This file is distributed under the same license as the PACKAGE package.
# FIRST AUTHOR <EMAIL@ADDRESS>, YEAR.
#
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: PACKAGE VERSION\n"
"Report-Msgid-Bugs-To: \n"
"POT-Creation-Date: 2006-11-01 16:39-0700\n"
"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"
"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"
"Language-Team: LANGUAGE <LL@li.org>\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=CHARSET\n"
"Content-Transfer-Encoding: 8bit\n"
```

```
#: C:\cygwin\home\<user>\cvc\main\Api\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\check\AgentIfc.cpp:22
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp~:20
#: C:\cygwin\home\<user>\cvc\main\Api\save\older\AgentIfc.cpp:22
msgid "Connected"
msgstr ""
```

msgid 包含默认转换。 msgid 之后的 msgstr 提供转换。如要创建转换，请在 msgstr 字符串的引号内输入转换的文本。例如，如要使用西班牙语转换选项转换消息 “Connected”，请在引号内插入西班牙语文本：

```
msgid "Connected"
msgstr "Conectado"
```

请确保已保存文件。

步骤 3　在 Privileged EXEC 模式下，使用 **import webvpn translation-table** 命令导入转换表。请确保使用与浏览器兼容的语言缩写来指定新转换表的名称。

在以下示例中，导入了 XML 文件，*es-us* - Microsoft Internet Explorer 面向在美国讲西班牙语的用户所用的缩写。

```
hostname# import webvpn translation-table AnyConnect language es-us
tftp://209.165.200.225/client
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# show import webvpn translation-table
Translation Tables' Templates:
AnyConnect
PortForwarder
csd
customization
keepout
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
es-us AnyConnect
```

配置高级 AnyConnect SSL 功能

下一节描述可微调 AnyConnect SSL VPN 连接的高级功能，包括以下部分：

启用重新生成密钥

ASA 与 AnyConnect 客户端在 SSL VPN 连接上重新生成密钥时，它们会重新协商加密密钥和初始化向量，从而提高连接的安全性。

如要允许客户端为特定组或用户在 SSL VPN 连接上重新生成密钥，请在组策略或用户名 webvpn 模式下使用 **anyconnect ssl rekey** 命令。

[no]anyconnect ssl rekey {**method** {**new-tunnel** | **none** | **ssl**} | **time** *minutes*}

method new-tunnel 用于指定客户端在重新生成密钥的过程中建立新的隧道。

method ssl 用于指定客户端在重新生成密钥的过程中建立新的隧道。

method none 用于禁用重新生成密钥。

注　将重新生成密钥的方法配置为 **ssl** 或 **new-tunnel**，用于指定客户端在重新生成密钥的过程中建立新的隧道，而不会在重新生成密钥的过程中进行 SSL 重新协商。有关 **anyconnect ssl rekey** 命令的历史记录，请参阅 《命令参考》。

time *minutes* 用于指定从会话开始或上一次重新生成密钥直到重新生成密钥所需经过的分钟数，取值范围从 1 至 10080 （1 周）。

在以下示例中，对于现有组策略 *sales* 来说，客户端被配置为在重新生成密钥的过程中使用 SSL 进行重新协商，重新生成密钥在会话开始 30 分钟后进行：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
```

启用和调整失效对等体检测

失效对等体检测 (DPD) 确保 ASA （网关）或客户端可以快速检测到对等体无响应且连接已失败的状况。

如要在 ASA 或客户端上为特定组或用户启用 DPD，并设置 ASA 或客户端执行 DPD 的频率，请在组策略或用户名 webvpn 模式下使用 **anyconnect dpd-interval** 命令：

anyconnect dpd-interval {[**gateway** {*seconds* | **none***}*] | [**client** {*seconds* | **none***}*]}

其中：

gateway seconds 用于启用由 ASA （网关）执行的 DPD，并指定 ASA （网关）执行 DPD 的频率，取值范围从 5 至 3600 秒。

gateway none 用于禁用由 ASA 执行的 DPD。

client *seconds* 用于启用客户端执行的 DPD，并指定客户端执行 DPD 的频率，取值范围从 5 至 3600 秒。

client none 用于禁用由客户端执行的 DPD。

如要从配置中移除 **anyconnect dpd-interval** 命令，请使用该命令的 **no** 形式：

no anyconnect dpd-interval {[**gateway** {*seconds* | **none***}*] | [**client** {*seconds* | **none***}*]}

注　如果您启用 DTLS，也会启用失效对等体检测 (DPD)。 DPD 允许已失败的 DTLS 连接回退至 TLS。否则，该连接会终止。

以下示例面向现有组策略 *sales*，将 ASA 执行的 DPD 的频率设置为 30 秒，将客户端执行的 DPD 的频率设置为 10 秒：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect dpd-interval gateway 30
hostname(config-group-webvpn)# anyconnect dpd-interval client 10
```

启用保持连接

您可以调整保持连接消息的频率，以确保经由代理、防火墙或 NAT 设备的 SSL VPN 连接保持打开状态，即使该设备限制了连接可处于空闲状态的时间也是如此。调整该频率还确保当远程用户未在积极运行诸如 Microsoft Outlook 或 Microsoft Internet Explorer 的基于套接字的应用时，客户端不会断开连接并重新连接。

注　默认情况下启用保持连接功能。如果您禁用保持连接功能，发生故障转移事件时， SSL VPN 客户端会话不会被转换到备用设备。

如要设置保持连接消息的频率，请在组策略 webvpn 或用户名 webvpn 配置模式下使用 **keepalive** 命令：

[no] anyconnect ssl keepalive {none | *seconds*}

none 用于禁用客户端保持连接消息。

seconds 使客户端可以发送保持连接消息，并指定发送消息的频率，取值范围为 15 至 600 秒。

默认设置为启用保持连接消息。

使用该命令的 **no** 形式可以将该命令从配置中移除，并导致该值被继承：

在以下示例中，对于现有组策略 *sales*， ASA 被配置为使客户端可以 300 秒 （5 分钟）的频率发送保持连接消息：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#anyconnect ssl keepalive 300
```

使用压缩

对于低带宽连接，压缩可以减小正被传输的数据包的大小，从而提高 ASA 和客户端之间的通信性能。默认情况下，在 ASA 上为全局级别和针对特定组或用户的所有 SSL VPN 连接启用压缩。

注　在宽带连接上实施压缩时，您必须谨慎考虑压缩依赖于低损连接的这一事实。该事实是默认情况下没有在宽带连接上启用压缩的主要原因。

压缩必须在全局配置模式下使用 **anyconnect ssl compression** 命令全局性地打开，然后在组策略和用户名 webvpn 模式下，针对特定组或用户，使用 **anyconnect ssl compression** 命令进行设置。

全局性地更改压缩

如要更改全局压缩设置，请在全局配置模式下使用 **anyconnect ssl compression** 命令：

compression

no compression

如要从配置中移除该命令，请使用该命令的 **no** 形式。

在以下示例中，为所有 SSL VPN 连接全局性地禁用了压缩：

```
hostname(config)# no compression
```

更改组和用户的压缩

如要更改特定组或用户的压缩，请在组策略和用户名 webvpn 模式下使用 **anyconnect ssl compression** 命令：

anyconnect ssl compression {**deflate** | **none**}

no anyconnect ssl compression {**deflate** | **none**}

默认情况下，对于组和用户而言， SSL 压缩被设置为 *deflate* （启用）。

如要从配置中移除 **anyconnect ssl compression** 命令，并致使该值从全局设置中继承，可以使用该命令的 **no** 形式：

在以下示例中，为组策略 sales 禁用了压缩：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no anyconnect ssl compression none
```

调整 MTU 大小

在组策略 webvpn 或用户名 webvpn 配置模式下，您可以使用 **anyconnect mtu** 命令调整客户端建立的 SSL VPN 连接的 MTU 大小 （从 256 至 1406 个字节）：

[no]anyconnect mtu *size*

该命令仅影响 AnyConnect 客户端。旧版思科 SSL VPN 客户端 () 不能调整为不同的 MTU 大小。

在默认组策略中，该命令的默认设置为 **no anyconnect mtu**。 MTU 大小基于连接使用的接口的 MTU 减去 IP/UDP/DTLS 开销自动进行调整。

该命令影响在 SSL 中建立的客户端连接以及在 SSL 中通过 DTLS 建立的客户端连接。

示例

以下示例将组策略 *telecommuters* 的 MTU 大小配置为 1200 个字节：

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#anyconnect mtu 1200
```

更新 AnyConnect 客户端映像

您可以使用以下操作步骤随时更新 ASA 上的客户端映像：

步骤 1　在 Privileged EXEC 模式下使用 **copy** 命令或者使用其他方法，将新的客户端映像复制至 ASA。

步骤 2　如果新的客户端映像文件与已加载的文件拥有相同的文件名，请重新输入在配置中的 **anyconnect image** 命令。如果新文件名不同，请使用 **noanyconnect image** 命令卸载旧文件。然后使用 **anyconnect image** 命令为映像分配顺序，并使 ASA 加载新的映像。

启用 IPv6 VPN 访问

如果您想要配置 IPv6 访问，则必须使用命令行界面。9.0(x) 版本的 ASA 为使用 SSL 和 IKEv2/IPsec 协议的其外部接口添加了 IPv6 VPN 连接支持。

在启用 SSL VPN 连接的过程中，您可以使用 **ipv6 enable** 命令启用 IPv6 访问。以下内容为在外部接口上启用 IPv6 的 IPv6 连接示例：

```
hostname(config)# interface GigabitEthernet0/0
hostname(config-if)# ipv6 enable
```

如要启用 IPV6 SSL VPN，请执行以下通用操作：

1. 在外部接口上启用 IPv6。
2. 在内部接口上启用 IPv6 和 IPv6 地址。
3. 为客户端分配的 IP 地址配置 IPv6 地址本地池。
4. 配置 IPv6 隧道默认网关。

要实施此操作步骤，请执行以下步骤：

步骤 1　配置接口：

```
interface GigabitEthernet0/0
     nameif outside
     security-level 0
     ip address 192.168.0.1 255.255.255.0
     ipv6 enable           ; Needed for IPv6.
    !
interface GigabitEthernet0/1
     nameif inside
     security-level 100
     ip address 10.10.0.1 255.255.0.0
     ipv6 address 2001:DB8::1/32        ; Needed for IPv6.
    ipv6 enable            ; Needed for IPv6.
```

步骤 2　配置 “ipv6 local pool”（用于 IPv6 地址分配）：

```
ipv6 local pool ipv6pool 2001:DB8:1:1::5/32 100     ; Use your IPv6 prefix here
```

注　通过在 ASA 上创建内部地址池，或者通过向 ASA 上的本地用户分配专用地址，您可以将 ASA 配置为向 AnyConnect 客户端分配 IPv4 地址和 / 或 IPv6 地址。

步骤 3　将 IPv6 地址池添加至您的隧道组策略 （或组策略）：

```
tunnel-group YourTunGrp1 general-attributes  ipv6-address-pool ipv6pool
```

注　您也必须在此处配置 IPv4 地址池 （使用 “address-pool”命令）。

步骤 4　配置 IPv6 隧道默认网关：

```
ipv6 route inside ::/0 X:X:X:X::X tunneled
```

监控 AnyConnect 连接

如要查看有关活动会话的信息，请使用 **show vpn-sessiondb**：

命令	用途
show vpn-sessiondb	显示有关活动会话的信息。
vpn-sessiondb logoff	注销 VPN 会话。
show vpn-sessiondb anyconnect	扩充 VPN 会话摘要，以显示 OSPFv3 会话信息。
show vpn-sessiondb ratio encryption	显示隧道数量和 Suite B 算法 （如 AES-GCM-128、 AES-GCM-192、AES-GCM-256、 AES-GMAC-128 等）的百分比。

示例

Inactivity 字段显示自 AnyConnect 会话断开连接以来所经过的时间。如果会话处于活动状态，会在该字段中显示 00:00m:00s。

```
hostname# show vpn-sessiondb

Session Type: SSL VPN Client

Username     : lee
Index        : 1                      IP Addr      : 209.165.200.232
Protocol     : SSL VPN Client         Encryption   : 3DES
Hashing      : SHA1                   Auth Mode    : userPassword
TCP Dst Port : 443                    TCP Src Port : 54230
Bytes Tx     : 20178                  Bytes Rx     : 8662
Pkts Tx      : 27                     Pkts Rx      : 19
Client Ver   : Cisco STC 1.1.0.117
Client Type  : Internet Explorer
Group        : DfltGrpPolicy
Login Time   : 14:32:03 UTC Wed Mar 20 2007
Duration     : 0h:00m:04s
Inactivity   : 0h:00m:04s
Filter Name  :

hostname# vpn-sessiondb logoff
INFO: Number of sessions of type "" logged off : 1

hostname# vpn-sessiondb logoff name tester
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "tester" logged off : 1
```

注销 AnyConnect VPN 会话

如要注销所有的 VPN 会话，请在全局配置模式下使用 **vpn-sessiondb logoff** 命令：

vpn-sessiondb logoff

以下示例注销了所有的 VPN 会话：

```
hostname# vpn-sessiondb logoff
INFO: Number of sessions of type  “” logged off : 1
```

您可以使用 name 参数或 index 参数注销单个会话：

vpn-session-db logoff name *name*

vpn-session-db logoff index *index*

处于非活动状态时间最长的会话会被标记为空闲 （并自动注销），以便不会达到许可证容量，并且新用户可以登录。如果会话稍后恢复活动状态，将会从非活动列表中移除该会话。

您可以在 **show vpn-sessiondb anyconnect** 命令的输出中找到用户名和索引号（按客户端映像的顺序建立）。以下示例显示用户名 *lee* 和索引号 *1*。

```
hostname# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : lee                    Index        : 1
Assigned IP  : 192.168.246.1           Public IP    : 10.139.1.2
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 11079                  Bytes Rx     : 4942
Group Policy : EngPolicy            Tunnel Group : EngGroup
Login Time   : 15:25:13 EST Fri Jan 28 2011
Duration     : 0h:00m:15s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

以下示例使用 **vpn-session-db logoff** 命令的 **name** 选项终止会话：

```
hostname# vpn-sessiondb logoff name lee
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name  “lee” logged off : 1

hostname#
```

启用 AnyConnect 连接的配置示例

以下示例显示如何配置基于 IPsec 的 L2TP：

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
aaa-server sales_server protocol radius
crypto ipsec transform-set sales_l2tp_transform esp-3des esp-sha-hmac
crypto ipsec transform-set sales_l2tp_transform mode transport
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
l2tp tunnel hello 100

group-policy sales_policy internal
group-policy sales_policy attributes
```

```
 wins-server value 209.165.201.3 209.165.201.4
 dns-server value 209.165.201.1 209.165.201.2
 vpn-tunnel-protocol l2tp-ipsec
tunnel-group sales_tunnel type remote-access
tunnel-group sales_tunnel general-attributes
 address-pool sales_addresses
 authentication-server-group none
 accounting-server-group sales_server
 default-group-policy sales_policy
tunnel-group sales_tunnel ppp-attributes
 authentication pap
```

AnyConnect 连接的功能历史记录

表 10-2 列出了此功能的版本历史记录。

表 10-2　AnyConnect 连接的功能历史记录

功能名称	版本	功能信息
AnyConnect 连接	7.2(1)	已引入或修改以下命令：**authentication eap-proxy**、**authentication ms-chap-v1**、 **authentication ms-chap-v2**、 **authentication pap**、**l2tp tunnel hello**、 **vpn-tunnel-protocol l2tp-ipsec**。
IPsec IKEv2	8.4(1)	添加了 IKEv2，以支持用于 AnyConnect 和 LAN 对 LAN 的 IPsec IKEv2 连接。

AnyConnect 主机扫描

Configuration > Remote Access VPN > Host Scan Image

AnyConnect 状态模块为 AnyConnect 安全移动客户端提供标识主机上安装的操作系统、防病毒软件、防间谍软件和防火墙软件的能力。主机扫描应用会收集此信息。

使用自适应安全设备管理器 (ASDM) 中的安全桌面管理器工具，您可以创建评估主机扫描标识的操作系统、防病毒软件、防间谍软件和防火墙软件的预登录策略。根据预登录策略的评估结果，您可以控制允许哪些主机创建与安全设备的远程访问连接。

主机扫描支持图表包含您在预登录策略中使用的防病毒应用、防间谍软件应用和防火墙应用的产品信息及版本信息。我们在主机扫描软件包中提供主机扫描和主机扫描支持图表以及其他组件。

从 3.0 版本 AnyConnect 安全移动客户端开始，主机扫描可与 CSD 分开使用。这意味着您无须安装 CSD 即可部署主机扫描功能，而且您可以通过升级最新主机扫描数据包更新您的主机扫描支持图表。

状态评估和 AnyConnect 遥测模块要求在主机上安装主机扫描。

本章包含以下各节：

主机扫描依赖关系和系统要求

依赖关系

具有安全状态模块的 AnyConnect 安全移动客户端至少需要以下版本 ASA 组件：

- ASA 8.4
- ASDM 6.4

这些 AnyConnect 功能要求安装安全状态模块。

- SCEP 身份验证
- AnyConnect 遥测模块

系统要求

安全状态模块可以安装在以下任何平台上：

- Windows XP （x86 和在 x64 上运行的 x86）
- Windows Vista （x86 和在 x64 上运行的 x86）
- Windows 7 （x86 和在 x64 上运行的 x86）
- Mac OS X 10.5 和 10.6 （32 位和在 64 位上运行的 32 位）
- Linux （32 位和在 64 位上运行的 32 位）
- Windows Mobile

许可

以下是安全状态模块的 AnyConnect 许可要求：

- 用于基本主机扫描的 AnyConnect 高级版。
- 以下功能需要高级终端评估许可证
  - 补救
  - 移动设备管理

主机扫描包装

您可以通过以下方式之一将主机扫描软件包加载到 ASA 上：

- 可以将其作为独立软件包上载：**hostscan-*version*.pkg**
- 可以通过上载 AnyConnect 安全移动软件包来将其上载：**anyconnect-NGC-win-*version*-k9.pkg**
- 可以通过上载思科安全桌面软件包来将其上载：**csd_version-k9.pkg**

文件	说明
hostscan-*version*.pkg	此文件包含主机扫描软件以及主机扫描库和支持图表。
anyconnect-NGC-win-*version*-k9.pkg	此软件包包含所有 Cisco AnyConnect 安全移动客户端功能，包括 hostscan-*version*.pkg 文件。
csd_*version*-k9.pkg	此文件包含所有思科安全桌面功能，包括主机扫描软件以及主机扫描库和支持图表。 此方法需要单独的适用于思科安全桌面的许可证。

在 ASA 上安装并启用主机扫描

以下任务描述在 ASA 上安装和启用主机扫描：

- 安装或升级主机扫描
- 启用或禁用主机扫描
- 查看 ASA 上启用的主机扫描版本
- 卸载主机扫描
- 将 AnyConnect 功能模块分配到组策略

安装或升级主机扫描

使用此操作步骤安装或升级主机扫描软件包并使用 ASA 命令行界面进行启用。

先决条件

- 登录 ASA 并进入全局配置模式。在全局配置模式下， ASA 将显示以下提示符：hostname(config)#
- 将 hostscan_version-k9.pkg 文件或 anyconnect-NGC-win-version-k9.pkg 文件上载到 ASA。

详细步骤

	命令	目的
步骤 1	**webvpn** **示例：** `hostname(config)# webvpn`	进入 webvpn 配置模式。

步骤 2	**csd hostscan image** path
	
	示例：
	`ASAName(webvpn)#csd hostscan image disk0:/hostscan-3.6.0-k9.pkg`
	`ASAName(webvpn)#csd hostscan image disk0:/anyconnect-NGC-win-3.0.0327-k9.pkg`
		指定指向要指定为主机扫描映像的软件包的路径。可以将独立的主机扫描软件包或 AnyConnect 安全移动客户端软件包指定为主机扫描软件包。
		注　对任何操作系统， Windows、 Linux 和 Mac OS X，客户都需要上载 anyconnect-NGC-win-*version*-k9.pkg 文件，才能让终端可以安装主机扫描。

步骤 3	**csd enable** **示例：** `ASAName(webvpn)#csd enable`	启用在上一步中指定的主机扫描映像。
步骤 4	write memory **示例：** `hostname(webvpn)# write memory`	将运行配置保存到闪存中。 成功地将新配置保存到闪存中后，您将收到消息 [OK]。

启用或禁用主机扫描

这些命令使用 ASA 的命令行界面启用或禁用已安装的主机扫描映像。

先决条件

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

启用主机扫描的详细步骤

	命令	目的
步骤 1	**webvpn** **示例：** `hostname(config)# webvpn`	进入 webvpn 配置模式。
步骤 2	**csd enable** **示例：** hostname(config)# **csd enable**	如果尚未从您的 ASA 中卸载独立主机扫描映像或 AnyConnect 安全移动客户端软件包中的主机扫描映像，则启用这些映像。如果没有安装任何这些类型的软件包，但是安装了 CSD 软件包，这将启用 CSD 软件包中的主机扫描功能。

禁用主机扫描的详细步骤

	命令	目的
步骤 1	**webvpn** **示例：** `hostname(config)# webvpn`	进入 webvpn 配置模式。
步骤 2	**no csd enable** **示例：** hostname(config)# **no csd enable**	为所有已安装的主机扫描软件包禁用主机扫描。 **注**　必须使用此命令禁用主机扫描，然后才能卸载已启用的主机扫描映像。

查看 ASA 上启用的主机扫描版本

使用 ASA 的命令行界面，按照以下操作步骤确定已启用的主机扫描版本。

先决条件

登录 ASA 并进入特权执行模式。在特权执行模式下， ASA 将显示以下提示符：**hostname#**

命令	目的

`show webvpn csd hostscan`
 	
示例：
`hostname# show webvpn csd hostscan`
	显示 ASA 上启用的主机扫描版本。

卸载主机扫描

卸载主机扫描软件包会在 ASDM 界面上将其隐藏并防止 ASA 对其进行部署，即使启用主机扫描或 CSD 也如此。卸载主机扫描不会从闪存驱动器中删除主机扫描软件包。

先决条件

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

详细步骤

	命令	目的
步骤 1	**webvpn** **示例：** `hostname(config)# webvpn`	进入 webvpn 配置模式。
步骤 2	**no csd enable** **示例：** `ASAName(webvpn)#no csd enable`	禁用想要卸载的主机扫描映像。
步骤 3	**no csd hostscan image** path **示例：** hostname(webvpn)#no csd hostscan image disk0:/hostscan-3.6.0-k9.pkg `hostname(webvpn)#no csd hostscan image disk0:/anyconnect-NGC-win-3.0.0327-k9.pkg`	指定指向想要卸载的主机扫描映像的路径。您可能已将独立主机扫描软件包或 AnyConnect 安全移动客户端软件包指定为主机扫描软件包。

步骤 4	`write memory`
	
	示例：
	`hostname(webvpn)# write memory`
		将运行配置保存到闪存中。
		成功地将新配置保存到闪存中后，您将收到消息 [OK]。

将 AnyConnect 功能模块分配到组策略

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

先决条件

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

详细步骤

	命令	目的
步骤 1	**group-policy** *name* **internal** **示例：** `hostname(config)# group-policy PostureModuleGroup internal`	为网络客户端访问添加内部组策略
步骤 2	**group-policy** *name* **attributes** **示例：** `hostname(config)# group-policy PostureModuleGroup attributes`	编辑新的组策略。输入该命令后，您会收到组策略配置模式的提示符：**hostname(config-group-policy)#**。

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

步骤 4	`hostname(config-group-webvpn)#` **anyconnect modules value** AnyConnect Module N*ame* **示例：** `hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture`	配置组策略以为组中的所有用户下载 AnyConnect 功能模块。 anyconnect 模块命令的值可能包含下列一个或多个值。当指定多个模块时，请用逗号将这些值隔开。 **值** — **AnyConnect 模块名称** **dart** — AnyConnect DART （诊断和报告工具） **nam** — AnyConnect 网络访问管理器 **vpngina** — AnyConnect SBL (Start Before Logon) **websecurity** — AnyConnect 网络安全模块 **telemetry** — AnyConnect 遥测模块 **posture** — AnyConnect 安全状态模块 **none** — 单独用于从组策略删除所有 AnyConnect 模块。 要删除某个模块，请重新发送指定仅要保留的模块值的命令。例如，这个命令将**删除**网络安全模块： `hostname(config-group-webvpn)# anyconnect modules value telemetry,posture`

步骤 5	`write memory`
	
	示例：
	`hostname(config-group-webvpn)# write memory`
		将运行配置保存到闪存中。
		成功地将新配置保存到闪存中后，您将收到消息 [OK]，并且 ASA 将向您返回以下提示符：
		hostname(config-group-webvpn)#

其他重要文档寻址主机扫描

一旦主机扫描从终端计算机收集安全状态凭证，您就将需要了解诸如配置预登录策略、配置动态访问策略以及使用 Lua 表达式利用信息之类的主题。

以下文档中详细涵盖这些主题：

- 《思科安全桌面配置指南》
- 《思科自适应安全设备管理器配置指南》

另请参阅 《*Cisco AnyConnect 安全移动客户端管理员指南，发行版 3.0*》以获取有关主机扫描如何与 AnyConnect 客户端配合工作的详细信息。

第 12 章

用于授权和身份验证的外部服务器

本章介绍如何配置外部 LDAP、RADIUS 或 TACACS+ 服务器来支持 ASA 的 AAA。在您配置 ASA 以便使用外部服务器之前，必须使用正确的 ASA 授权属性配置 AAA 服务器，并且从这些属性子集中，将特定权限分配给个别用户。

了解授权属性的策略实施

ASA 支持将用户授权属性 （也称为用户授权或权限）应用到 VPN 连接的多种方法。您可以配置 ASA，以便通过以下任意组合获取用户属性：

- ASA 上的动态访问策略 (DAP)
- 外部 RADIUS 或 LDAP 身份验证和 / 或授权服务器
- ASA 上的组策略

如果 ASA 收到来自所有来源的属性，将会对这些属性进行评估、合并，并将其应用至用户策略。如果属性之间有冲突， DAP 属性优先。

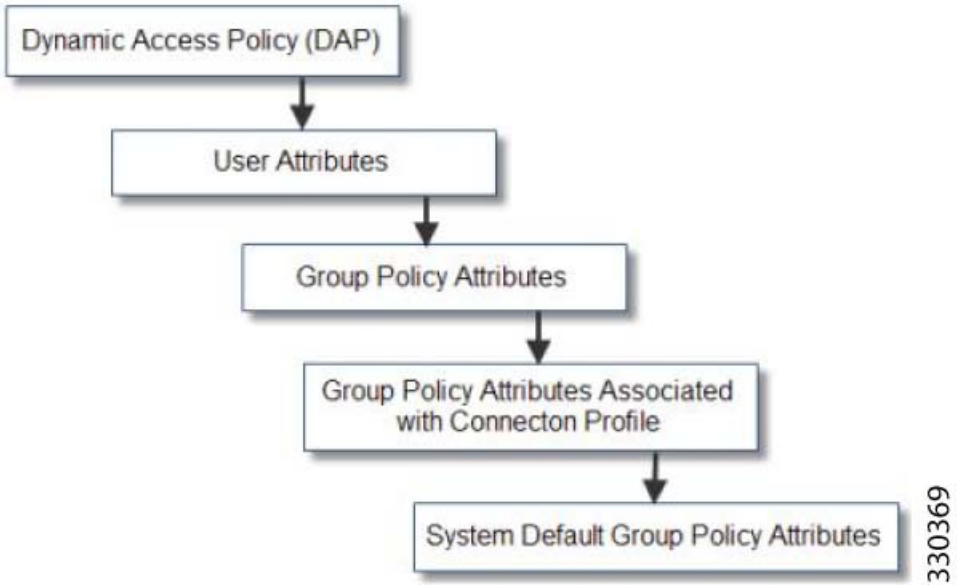
ASA 按照以下顺序应用属性 （请参阅图 12-1）。

1. ASA 上的 DAP 属性 — 在 8.0(2) 版本中引入，这些属性优先于所有其他的属性。如果您在 DAP 中设置书签或 URL 列表，它会覆盖组策略中设置的书签或 URL 列表。
2. AAA 服务器上的用户属性 — 该服务器在用户身份验证和 / 或授权成功后返回这些属性。请不要将这些属性与为 ASA 本地 AAA 数据库中的个别用户 （ASDM 中的用户帐户）设置的属性混淆。
3. 在 ASA 上配置的组策略 — 如果 RADIUS 服务器为该用户返回 RADIUS CLASS 属性 IETF-Class-25 (OU=*group-policy*) 值， ASA 会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。

   对于 LDAP 服务器，任何属性名称都可用于设置该会话的组策略。您在 ASA 上配置的 LDAP 属性映射会将该 LDAP 属性映射至思科属性 IETF-Radius-Class。
4. 连接配置文件分配的组策略（在 CLI 中称为隧道组）- 连接配置文件具有该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。连接至 ASA 的所有用户最初都属于此组，这可以提供 DAP 缺失的所有属性、服务器返回的用户属性或分配给用户的组策略。
5. ASA 分配的默认组策略 (DfltGrpPolicy) — 系统默认属性提供 DAP、用户属性、组策略或连接配置文件中缺失的所有值。

定义 ASA LDAP 配置

图 12-1　　策略实施流程



授权是指实施权限或属性的过程。 LDAP 服务器的定义是实施权限或属性的身份验证或授权服务器 （如已配置）。

准则

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

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

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

Active Directory/LDAP VPN 远程访问授权示例

本部分提供在 ASA 上使用 Microsoft Active Directory 服务器配置身份验证和授权的示例操作步骤。包括下列主题：

Cisco.com 提供的其他配置示例包括以下技术说明。

- 处于以下 URL 的 *《ASA/PIX：通过 LDAP 配置将 VPN 客户端映射至 VPN 组策略的示例》*：
  http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008089149d.shtml
- 处于以下 URL 的 *《PIX/ASA 8.0：登录时使用 LDAP 身份验证来分配组策略》*：
  http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00808d1a7c.shtml

基于用户的属性策略实施

您可以将任意标准 LDAP 属性映射至一个已知的供应商特定属性 (VSA)，也可以将一个或多个 LDAP 属性映射至一个或多个思科 LDAP 属性。

以下示例展示如何配置 ASA，以便为在 AD LDAP 服务器上配置的用户实施简单欢迎信息。在服务器上，使用 General 选项卡中的 Office 字段输入欢迎信息文本。此字段使用名为 physicalDeliveryOfficeName 的属性。在 ASA 中，创建将 physicalDeliveryOfficeName 映射至 Cisco 属性 Banner1 的属性映射。在身份验证过程中， ASA 从该服务器检索 physicalDeliveryOfficeName 的值，将该值映射至 Cisco 属性 Banner1，然后向用户显示该欢迎信息。

此示例适用于任意连接类型，包括 IPSec VPN 客户端、 AnyConnect SSL VPN 客户端或无客户端 SSL VPN。在此示例中， User1 通过无客户端 SSL VPN 连接进行连接。

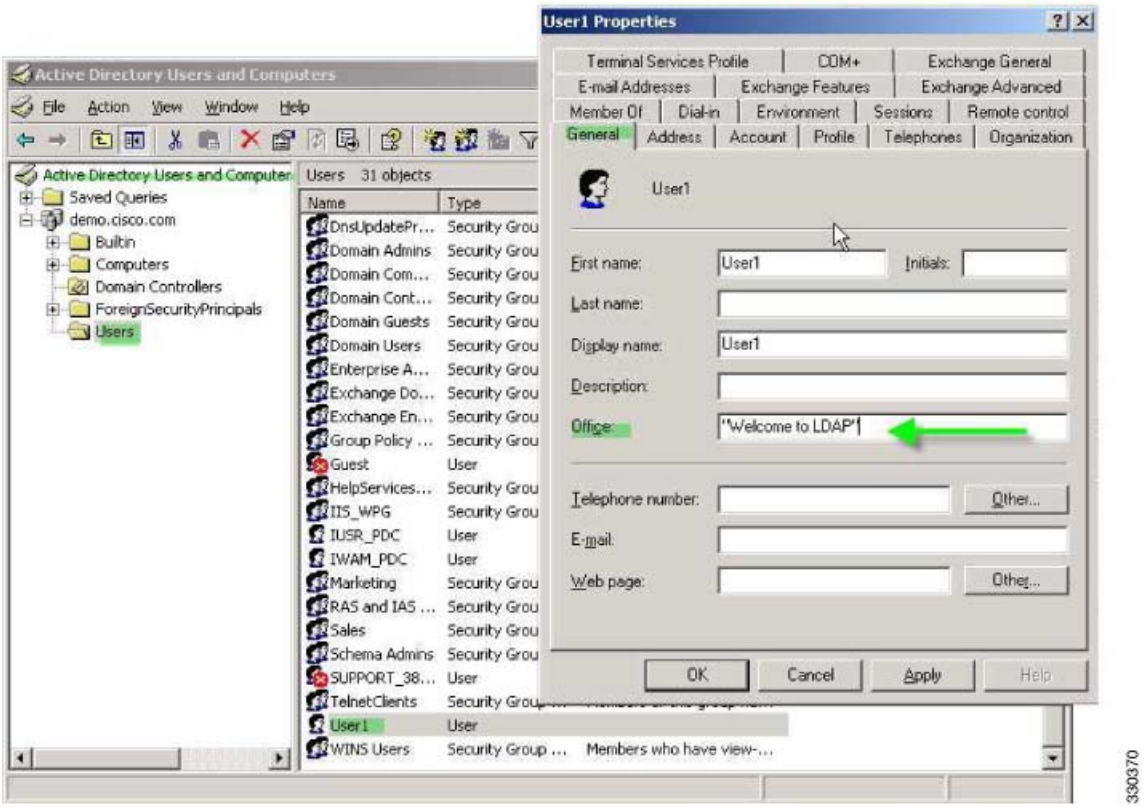
如要在 AD 或 LDAP 服务器上为用户配置属性，请执行以下步骤：

步骤 1　右键单击用户。

系统将显示 Properties 对话框 （请参阅图 12-2）。

步骤 2　点击 **General** 选项卡，在 Office 字段中输入欢迎信息文本，这会使用 AD/LDAP 属性 physicalDeliveryOfficeName。

图 12-2　　LDAP 用户配置



步骤 3　在 ASA 上创建一个 LDAP 属性映射。

以下示例创建映射 Banner，并将 AD/LDAP 属性 physicalDeliveryOfficeName 映射至 Cisco 属性 Banner1：

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

步骤 4　将 LDAP 属性映射关联到 AAA 服务器。

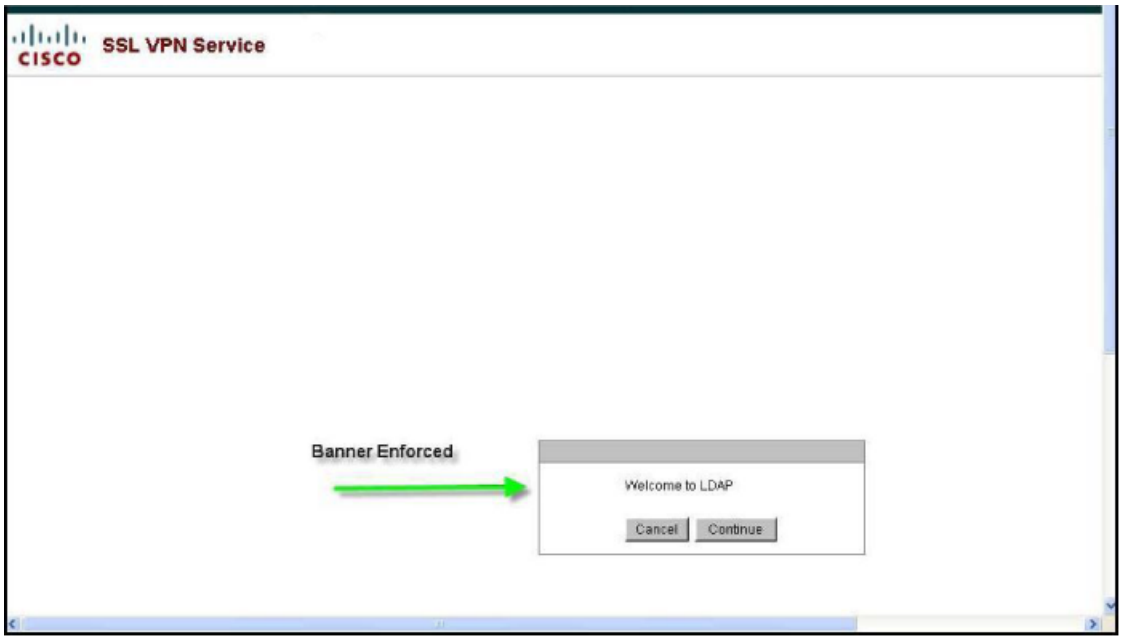
以下示例进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您在步骤 3 中创建的属性映射 Banner：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

步骤 5　测试此欢迎信息的实施。

以下示例展示无客户端 SSL 连接，以及用户完成身份验证后通过属性映射实施的欢迎信息（请参阅图 12-3）。

图 12-3　显示的欢迎信息



将 LDAP 用户置于特定组策略中

以下示例展示如何在 AD LDAP 服务器上对 User1 进行身份验证，以便将其置于 ASA 上的特定组策略。在服务器上，使用 Organization 选项卡的 Department 字段输入组策略的名称。然后创建一个属性映射，将 Department 映射到思科属性 IETF-Radius-Class。在身份验证过程中， ASA 从服务器检索 Department 的值，将此值映射到 IETF-Radius-Class，然后将 User1 置于该组策略中。

此示例适用于任意连接类型，包括 IPSec VPN 客户端、 AnyConnect SSL VPN 客户端或无客户端 SSL VPN。在此示例中， User1 通过无客户端 SSL VPN 连接进行连接。

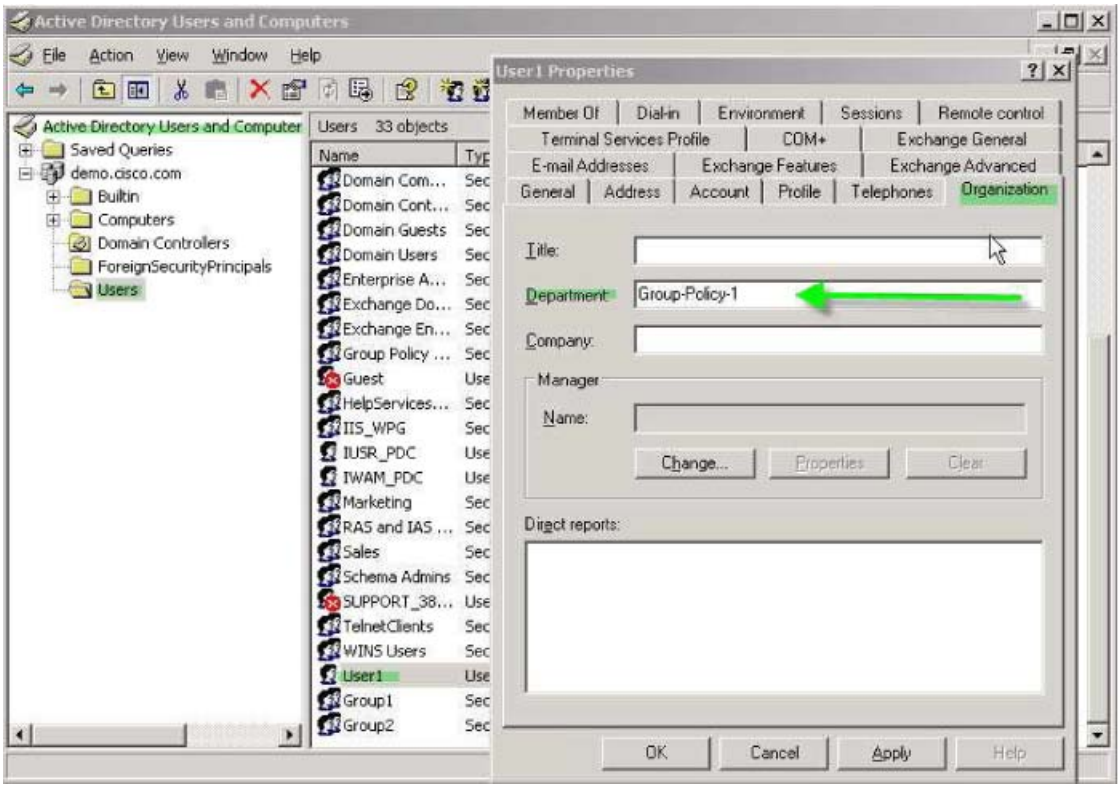
要在 AD LDAP 服务器上为用户配置属性，请执行以下步骤：

步骤 1　右键点击该用户。

系统将显示 Properties 对话框 （请参阅图 12-4）。

步骤 2　点击 **Organization** 选项卡，在 Department 字段中输入 **Group-Policy-1**。

图 12-4　AD/LDAP 部门属性



步骤 3　为步骤 1 中显示的 LDAP 配置定义一个属性映射。

以下示例展示如何将 AD 属性 Department 映射到思科属性 IETF-Radius-Class。

```
hostname(config)# ldap attribute-map group_policy
hostname(config-ldap-attribute-map)# map-name Department IETF-Radius-Class
```

步骤 4　将 LDAP 属性映射关联到 AAA 服务器。

以下示例进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您在步骤 3 中创建的属性映射 group_policy：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map group_policy
```

步骤 5　在 ASA 上添加新的组策略，配置将分配给该用户的所需策略属性。以下示例创建 Group-policy-1，即在服务器的 Department 字段中输入的名称。

```
hostname(config)# group-policy Group-policy-1 external server-group LDAP_demo
hostname(config-aaa-server-group)#
```

步骤 6　像用户一样建立 VPN 连接，并验证会话是否会继承 Group-Policy1 中的属性 （以及默认组策略中的任何其他适用属性）。

步骤 7　通过从特权 EXEC 模式启用 **debug ldap 255** 命令，监控 ASA 和该服务器之间的通信。以下是此命令的示例输出，此输出已经过编辑，以便提供关键信息。

```
[29] Authentication successful for user1 to 10.1.1.2
[29] Retrieving user attributes from server 10.1.1.2
[29] Retrieved Attributes:
[29] department: value = Group-Policy-1
[29] mapped to IETF-Radius-Class: value = Group-Policy-1
```

为 AnyConnect 隧道实施静态 IP 地址分配

在此示例中，将会配置 AnyConnect 客户端用户 Web1，以便接收静态 IP 地址。然后在 AD LDAP 服务器上的 Dialin 选项卡的 Assign Static IP Address 字段中输入地址。此字段使用 msRADIUSFramedIPAddress 属性。创建将此属性映射到 Cisco 属性 IETF-Radius-Framed-IP-Address 的属性映射。

在身份验证过程中，ASA 从服务器检索 physicalDeliveryOfficeName 的值，将该值映射到 Cisco 属性 IETF-Radius-Framed-IP-Address，并向 User1 提供静态地址。

以下示例适用于全隧道客户端，包括 IPSec 客户端和 SSL VPN 客户端 （AnyConnect 客户端 2.x 和 SSL VPN 客户端）。

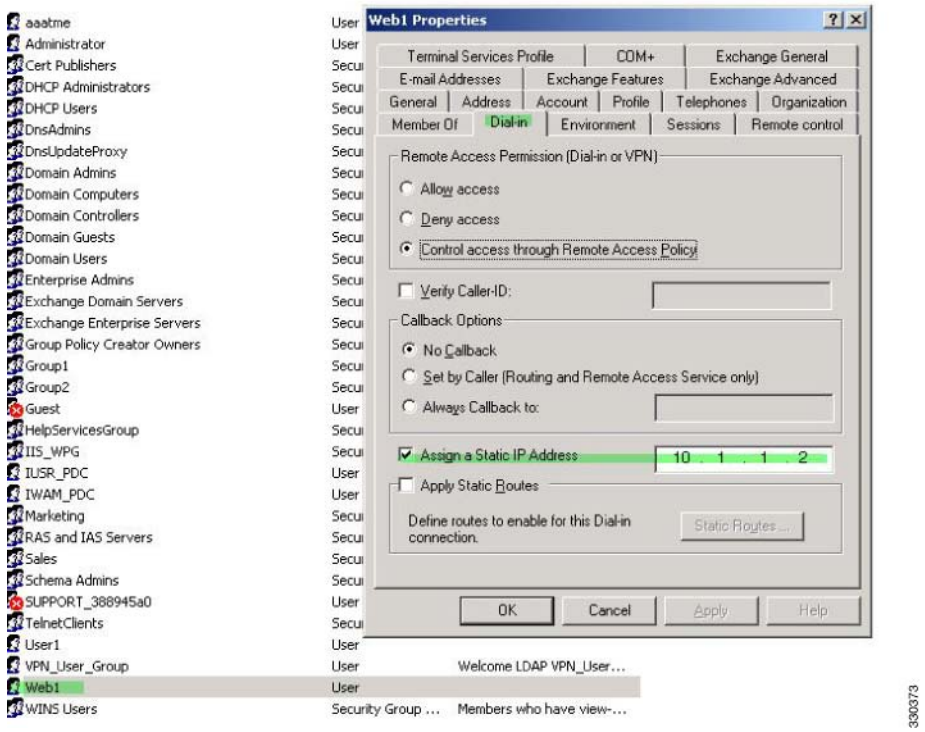
要在 AD/LDAP 服务器上配置用户属性，请执行以下步骤：

步骤 1　右键单击该用户名。

系统将显示 Properties 对话框 （请参阅图 12-5）。

步骤 2　点击 **Dialin** 选项卡，选择 **Assign Static IP Address** 复选框，然后输入 IP 地址 10.1.1.2。

图 12-5　　分配静态 IP 地址



步骤 3　为步骤 1 中显示的 LDAP 配置创建一个属性映射。

以下示例展示如何将 Static Address 字段使用的 AD 属性 msRADIUSFramedIPAddress 映射至 Cisco 属性 IETF-Radius-Framed-IP-Address：

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

步骤 4　将 LDAP 属性映射关联到 AAA 服务器。

以下示例进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您在步骤 3 中创建的属性映射 static_address：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

步骤 5　通过使用 **show run all vpn-addr-assign** 命令查看此部分的配置，验证是否已配置 **vpn-address-assignment** 命令来指定 AAA：

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa    << 确保配置此项 >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

步骤 6　使用 AnyConnect 客户端建立与 ASA 的连接。请观察以下内容：

- 欢迎信息以与无客户端连接相同顺序接收（请参阅图 12-6）。
- 用户会收到在服务器上配置并映射至 ASA 的 IP 地址（请参阅图 12-7）。

图 12-6　验证 AnyConnect 会话的欢迎信息

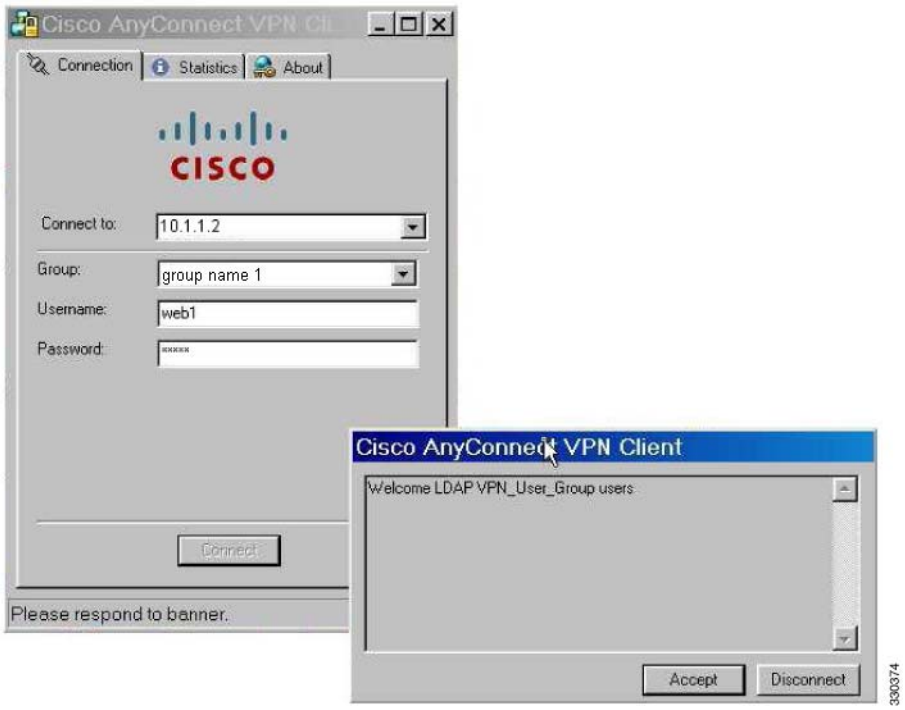


图 12-7　　建立的 AnyConnect 会话

步骤 7　使用 **show vpn-sessiondb svc** 命令来查看会话详细信息，并验证分配的地址：

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                    Index        : 31
Assigned IP  : 10.1.1.2               Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128              Hashing      : SHA1
Bytes Tx     : 304140                  Bytes Rx     : 470506
Group Policy : VPN_User_Group          Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                     VLAN         : none
```

实施拨入允许或拒绝访问

以下示例创建指定用户允许的隧道协议的 LDAP 属性映射。您可以将 Dialin 选项卡上的允许访问和拒绝访问设置映射至思科属性 Tunneling-Protocol，该属性支持表 12-1 中显示的映射值。

表 12-1　　思科 Tunneling-Protocol 属性的位映射值

值	隧道协议
1	PPTP
2	L2TP
4[1]	IPsec (IKEv1)
8[2]	L2TP/IPsec
16	无客户端 SSL

表 12-1　思科 Tunneling-Protocol 属性的位映射值 （续）

值	隧道协议
32	SSL 客户端 — AnyConnect 或 SSL VPN 客户端
64	IPsec (IKEv2)

1. 不同时支持 IPsec 和经由 IPsec 的 L2TP。因此，值 4 和 8 是互相排斥的。
2. 请参阅注释 1。

使用此属性创建协议的允许访问 (TRUE) 或拒绝访问 (FALSE) 条件，并实施允许用户访问的方法。

对于此简化示例，通过映射隧道协议 IPsec/IKEv1 (4)，您可以为该思科 VPN 客户端创建允许 (true) 条件。您还可以映射 WebVPN (16) 和 SVC/AC (32)，它们会被映射为值 48 (16+32)，以及创建拒绝 (false) 条件。这允许用户使用 IPsec 连接到 ASA，但是任何使用无客户端 SSL 或 AnyConnect 客户端的连接尝试会被拒绝。

位于以下 URL 的技术说明 *《ASA/PIX：通过 LDAP 配置将 VPN 客户端映射至 VPN 组策略的示例》*中提供了实施拨入允许访问或拒绝访问的另一示例：

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008089149d.shtml

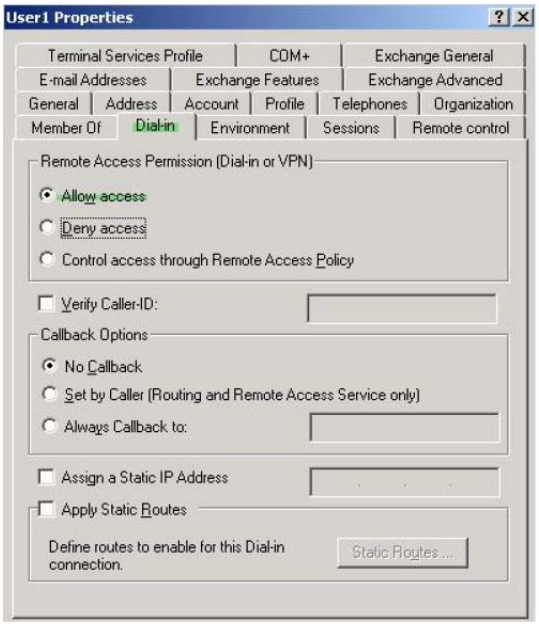
要在 AD/LDAP 服务器上配置用户属性，请执行以下步骤：

步骤 1　右键点击该用户。

系统将显示 Properties 对话框。

步骤 2　点击 **Dial-in** 选项卡，然后点击 **Allow Access** 单选按钮 （图 12-8）。

图 12-8　AD/LDAP User1 — 允许访问



注　如果您通过 Remote Access Policy 选项选择控制访问，则服务器不会返回值，实施的权限会基于 ASA 的内部组策略设置。

步骤 3　创建一个属性映射允许 IPsec 和 AnyConnect 连接，但是拒绝无客户端 SSL 连接。

以下示例展示如何创建映射 tunneling_protocols，使用 **map-name** 命令将 Allow Access 设置使用的 AD 属性 msNPAllowDialin 映射到思科属性 Tunneling-Protocols，以及使用 **map-value** 命令添加映射值：

```
hostname(config)# ldap attribute-map tunneling_protocols
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

步骤 4　将 LDAP 属性映射关联到 AAA 服务器。

以下示例进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您在步骤 2 中创建的属性映射 tunneling_protocols：

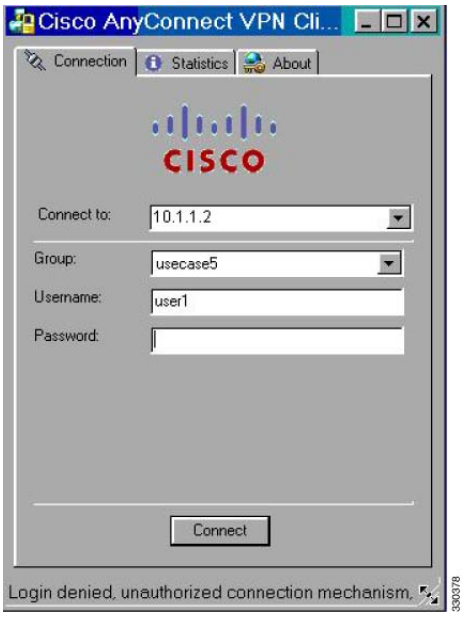
```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

步骤 5　验证属性映射是否如配置工作。

步骤 6　使用无客户端 SSL、 AnyConnect 客户端和 IPSec 客户端尝试连接。无客户端和 AnyConnect 连接应该会失败，并且应该会通知用户，未经授权的连接机制是连接失败的原因。 IPSec 客户端应进行连接，因为根据属性映射， IPsec 是允许的隧道协议 （请参阅图 12-9 和图 12-10）。

图 12-9　　无客户端用户的登录被拒绝消息

图 12-10　AnyConnect 客户端用户的登录被拒绝消息



实施登录时段和时间规则

以下示例展示如何配置和实施允许无客户端 SSL 用户 （例如业务合作伙伴）访问网络的时段。

在 AD 服务器上，使用 Office 字段输入合作伙伴的名称，该字段使用 physicalDeliveryOfficeName 属性。然后我们在 ASA 上创建一个属性映射，以便将该属性映射到思科属性 Access-Hours。在身份验证过程中， ASA 会检索 physicalDeliveryOfficeName 的值，并将其映射到 Access-Hours。

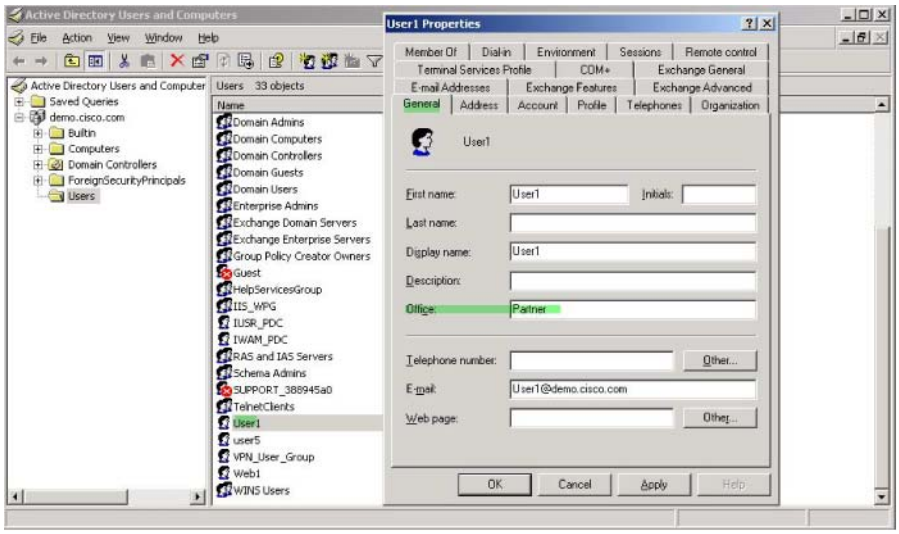
要在 AD/LDAP 服务器上配置用户属性，请执行以下步骤：

步骤 1　选择该用户，然后右键单击 **Properties**。

系统将显示 Properties 对话框 （请参阅图 12-11）。

步骤 2　点击 **Search** 选项卡。

图 12-11　Active Directory Properties 对话框



步骤 3　创建属性映射。

以下示例展示如何创建属性映射 access_hours，并将 Office 字段使用的 AD 属性 physicalDeliveryOfficeName 映射到思科属性 Access-Hours。

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

步骤 4　将 LDAP 属性映射关联到 AAA 服务器。

以下示例进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您在步骤 3 中创建的属性映射 access_hours：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

步骤 5　为服务器上允许的每个值配置时间范围。

以下示例将合作伙伴访问时段配置为周一至周五上午 9 点到下午 5 点：

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

使用 LDAP 为 VPN 配置授权

在 VPN 访问的 LDAP 身份验证成功后，ASA 将查询 LDAP 服务器，这会返回 LDAP 属性。这些属性通常包括应用到 VPN 会话的授权数据。

您可能需要来自 LDAP 目录服务器的授权，此授权与身份验证机制不同。例如，如果您使用 SDI 或证书服务器进行身份验证，系统不会传回任何授权信息。对于这种情况下的用户授权，您可在身份验证成功后查询 LDAP 目录，两步完成身份验证和授权。

如要使用 LDAP 设置 VPN 用户授权，请执行以下步骤。

详细步骤

	命令	用途

步骤 1	**aaa-server** *server_group* **protocol** {**kerberos** | **ldap** | **nt** | **radius** | **sdi** | **tacacs+**}
	
	示例：
	`hostname(config)# aaa-server servergroup1 protocol ldap`
	`hostname(config-aaa-server-group)`
		创建 AAA 服务器组。

步骤 2	**tunnel-group** *groupname* **示例：** `hostname(config)# tunnel-group remotegrp`	创建一个名为 remotegrp 的 IPsec 远程访问隧道组。
步骤 3	**tunnel-group** *groupname* **general-attributes** **示例：** `hostname(config)# tunnel-group remotegrp general-attributes`	将服务器组和隧道组关联。
步骤 4	**authorization-server-group** *group-tag* **示例：** `hostname(config-general)# authorization-server-group ldap_dir_1`	将新隧道组分配到先前创建的 AAA 服务器组进行授权。

示例

虽然有可用于特定要求的其他授权相关命令和选项，以下示例展示启用使用 LDAP 的用户授权的命令。然后示例将创建一个名为 remote-1 的 IPsec 远程访问隧道组，将新隧道组分配到先前创建的 ldap_dir_1 AAA 服务器组进行授权：

```
hostname(config)# tunnel-group remote-1 type ipsec-ra
hostname(config)# tunnel-group remote-1 general-attributes
hostname(config-general)# authorization-server-group ldap_dir_1
hostname(config-general)#
```

在完成此配置工作后，接着您可以通过输入以下命令，配置其他的 LDAP 授权参数，如目录密码、搜索目录的起点和目录搜索的范围：

```
hostname(config)# aaa-server ldap_dir_1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
hostname(config-aaa-server-host)# ldap-login-dn obscurepassword
hostname(config-aaa-server-host)# ldap-base-dn starthere
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)#
```

第 2 部分

无客户端 SSL VPN

第 13 章

无客户端 SSL VPN 简介

2014 年 4 月 14 日

无客户端 SSL VPN 简介

无客户端 SSL VPN 让最终用户可以使用支持 SSL 的网络浏览器随时随地安全地访问公司网络上的资源。用户首先利用无客户端 SSL VPN 网关进行身份验证，然后允许用户访问预配置的网络资源。

注 启用无客户端 SSL VPN 时，不支持安全情景 （也称为多模防火墙）和主动 / 主动状态故障切换。

无客户端 SSL VPN 使用网络浏览器创建访问 ASA 的安全远程访问隧道，而不要求使用软件或硬件客户端。通过它可以从无法通过 HTTP 连接互联网的几乎任何设备安全和便捷地访问各种网络资源以及支持网络的和旧版的应用。具体包括：

- 内部网站。
- 支持网络的应用。
- NT/Active Directory 文件共享。
- 邮件代理，包括 POP3S、 IMAP4S 和 SMTPS。
- Microsoft Outlook Web Access Exchange Server 2000、 2003 和 2007。
- 8.4(2) 和更低版本中适用于 Exchange Server 2010 的 Microsoft Web App
- 应用访问 （对其他基于 TCP 的应用的智能隧道或端口转发访问）

无客户端 SSL VPN 使用安全套接字层协议及其后继传输层安全性协议 (SSL/TLS1) 在远程用户与您在内部服务器上配置的特定受支持的内部资源之间提供安全连接。 ASA 将识别必须代理的连接，并且 HTTP 服务器会与身份验证子系统交互以对用户进行身份验证。

网络管理员以组为基础为无客户端 SSL VPN 的用户提供对资源的访问。用户无权直接访问内部网络上的资源。

先决条件

关于 9.0 版本 ASA 支持的平台和浏览器，请参阅*支持的 VPN 平台、思科 ASA 系列*。

准则和限制

- ActiveX 页面要求您启用 ActiveX 中继或为关联的组策略输入 **activex-relay**。如果您这么做或给策略分配一个智能隧道列表，并且终端上的浏览器代理特例列表指定了一个代理，则用户必须向该列表添加一个 “shutdown.webvpn.relay.” 条目。
- ASA 不支持从 Windows 7、Vista、Internet Explorer 8 至 10、Mac OS X 或 Linux 对 Windows Shares (CIFS) Web Folders 进行无客户端访问。
- 证书身份验证，包括美国国防部通用存取卡和智能卡，仅适用于 Safari 钥匙串。
- ASA 不支持无客户端 SSL VPN 连接的 DSA 或 RSA 证书。
- 一些基于域的安全产品要求可能高于源自 ASA 的这些请求。
- 不支持在模块化策略框架下配置控件检查和其他检查功能。
- 组策略下的 *vpn-filter* 命令适用于基于客户端的访问，因此不受支持。组策略中无客户端 SSL VPN 模式下的*过滤器*只适用于基于无客户端的访问。
- NAT 或 PAT 都不适用于客户端。
- ASA 不支持使用 QoS rate-limiting 命令，例如 **police** 或 **priority-queue**。
- ASA 不支持使用连接限制，其通过静态或模块化策略框架 **set connection** 命令进行检查。
- 无客户端 SSL VPN 某些组件需要在 Mac OS X v10.7 和更高版本中运行的 Java Runtime Environment (JRE)。默认情况下不安装 Java。有关如何在 Mac OS X 上安装 Java 的详细信息，请参阅 http://java.com/en/download/faq/java_mac.xml。

当您为无客户端门户配置了几个组策略时，它们将显示在登录页面上的下拉列表中。当列表中的第一个组策略要求提供证书时，用户必须具有匹配的证书。如果某些组策略不使用证书，则必须将列表配置为首先显示非证书策略。或者，您可能希望创建一个名称为 “0-Select-a-group” 的虚拟组策略。

提示　您可以通过按照字母顺序给组策略命名或在其名称前面加上数字前缀，从而控制首先显示哪个策略。例如 1-AAA, 2-Certificate。

第 14 章

基本无客户端 SSL VPN 配置

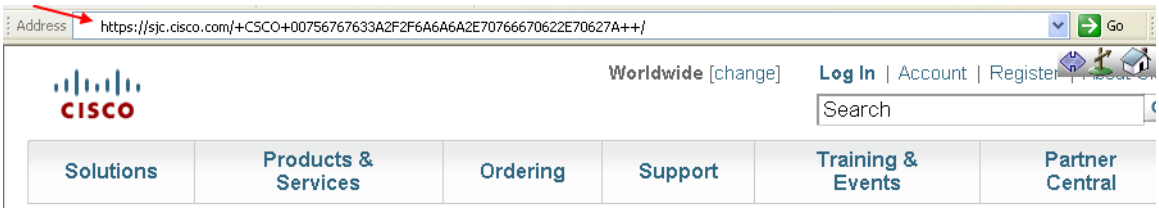
修订日期：2014 年 3 月 12 日

无客户端 SSL VPN 安全预防措施

默认情况下， ASA 允许所有门户网站流量流向所有网络资源 （例如 HTTPS、 CIFS、 RDP 和插件）。无客户端 SSL VPN 将每个 URL 重写入仅对 ASA 有意义的 URL。用户无法使用此 URL 确认其已连接至其所请求的网站。为了避免用户遭受钓鱼网站所带来的风险，请将网络 ACL 分配给为无客户端访问配置的策略 （如组策略和 / 或动态访问策略），以控制源自门户网站的流量。我们建议关闭这些策略上的 URL Entry，以防止用户弄不清哪些内容才是可访问的。

图 14-1　　用户输入的 URL 示例

图 14-2　　安全设备重写以及浏览器窗口中显示的相同 URL



关闭门户网站网页上的 URL Entry

此门户网站网页在用户建立基于浏览器的连接时打开。

先决条件

为需要无客户端 SSL VPN 访问权限的所有用户配置组策略，并仅为该组策略启用无客户端 SSL VPN。

详细步骤

	命令	用途
步骤 1	`webvpn`	切换至组策略无客户端 SSL VPN 配置模式。
步骤 2	`url-entry`	控制用户输入任意 HTTP/HTTPS URL 的权限。
步骤 3	（可选）`url-entry disable`	关闭 URL Entry。

验证无客户端 SSL VPN 服务器证书

在通过无客户端 SSL VPN 连接至支持 SSL 的远程服务器时，务必知悉您可信任该远程服务器，且该服务器实际上就是您在尝试连接的服务器。 ASA 9.0 引入了以下支持功能：根据无客服端 SSL VPN 的受信任证书颁发机构 (CA) 证书的列表执行 SSL 服务器证书验证。

在使用 HTTPS 协议连接至带有网络浏览器的远程服务器时，该服务器提供证书颁发机构 (CA) 签署的数字证书进行自我标识。网络浏览器包括用于验证服务器证书有效性的 CA 证书集合。这是一种形式的公共密钥基础结构 (PKI)。

ASA 提供 trustpool 形式的受信任池证书管理设施。这可视为表示多个已知 CA 证书的信任点的特殊案例。 ASA 包括一个默认的证书捆绑包，与随网络浏览器提供的证书捆绑包相似。只有管理员发出 **`crypto ca import default`** 命令后才会激活它。

注　ASA trustpool 与 Cisco IOS trustpool 类似，但不完全相同。

配置浏览器对插件的访问

以下各节介绍如何为无客户端 SSL VPN 浏览器访问集成浏览器插件：

浏览器插件是网络浏览器在执行专用功能时 （例如，将客户端连接至浏览器窗口中的服务器）调用的一个单独程序。借助于 ASA，可在无客户端 SSL VPN 会话中导入要下载至远程浏览器的插件。当然，思科将测试其重新分发的插件，在某些情况下，将测试其无法重新分发的插件的连接性。但是，我们建议不要导入目前支持流媒体的插件。

在闪存设备上安装插件时， ASA 将执行以下操作：

- （仅限思科分发的插件）解压缩 URL 中指定的 jar 文件。
- 将文件写入 ASA 文件系统。
- 填充 ASDM 中 URL 属性旁边的下拉列表。
- 为所有未来无客户端 SSL VPN 会话启用插件，然后将主菜单选项和选项添加至门户网站网页 Address 字段旁边的下拉列表。

表 14-1 显示在添加以下各节中描述的插件时对门户网站网页的主菜单和 Address 字段做出的更改。

表 14-1　　无客户端 SSL VPN 门户网站网页上插件的效果

插件	已添加至门户网站网页的主菜单选项	已添加至门户网站网页的 Address 字段选项
ica	Citrix MetaFrame Services	ica://
rdp	Terminal Servers	rdp://
rdp2*	Terminal Servers Vista	rdp2://
ssh,telnet	Secure Shell	ssh://
	Telnet Services (supporting v1 and v2)	telnet://
vnc	Virtual Network Computing services	vnc://

* 不是推荐的插件。

当用户在无客户端 SSL VPN 会话中点击门户网站网页上的关联菜单选项时，门户网站网页显示界面窗口和帮助窗格。用户可选择下拉列表中显示的协议，并在 Address 字段中输入 URL，以建立连接。

插件支持单点登录 (SSO)。请参阅第 18-11 页上的使用 HTTP 表单协议配置 SSO，了解实施详细信息。

先决条件

- 无客户端 SSL VPN 只有在 ASA 上启用才能提供对插件的远程访问。
- 要为插件配置 SSO 支持，需安装插件，添加书签条目以显示服务器链接，并在添加书签时指定 SSO 支持。
- 远程使用所需的最低访问权限属于宾客特权模式。
- 使用插件需要安装 ActiveX 或 Oracle Java Runtime Environment (JRE)；请参阅兼容性矩阵了解版本要求。

限制

注　远程桌面协议插件不支持用会话代理程序进行负载平衡。由于协议处理源自会话代理程序的重定向的方法不当，连接失败。如未使用会话代理程序，插件将发挥正常作用。

- 插件支持单点登录 (SSO)。它们使用所输入的*相同凭据*打开无客户端 SSL VPN 会话。因为插件不支持宏替换，所以，您无法选择对不同的字段（如内部域密码）或 RADIUS 或 LDAP 服务器上的属性执行 SSO。
- 有状态故障转移不保留使用插件建立的会话。出现故障转移后，用户必须重新连接。
- 如果使用无状态故障转移替代有状态故障转移，则无客户端功能（例如书签、自定义和动态访问策略）不会在故障转移 ASA 对之间同步。在发生故障转移时，这些功能不起作用。

为安装插件准备安全设备

在安装插件之前，请按以下所示准备 ASA：

先决条件

确保在 ASA 界面上已启用无客户端 SSL VPN。

限制

请勿将 IP 地址指定为 SSL 证书的通用名称 (CN)。远程用户尝试使用 FQDN 与 ASA 进行通信。远程 PC 必须能够使用 DNS 或 System32\drivers\etc\hosts 文件中的条目解析 FQDN。

详细步骤

	命令	用途
步骤 1	`show running-config`	显示无客户端 SSL VPN 是否已在 ASA 上启用。
步骤 2	Install an SSL certificate onto the ASA interface	为远程用户连接提供完全限定域名 (FQDN)。

转至与标识要为无客户端 SSL VPN 访问提供的插件类型相对应的那部分。

- 第 14-4 页上的安装思科重新分发的插件
- 第 14-6 页上的提供对 Citrix XenApp 服务器的访问

安装思科重新分发的插件

思科重新分发以下基于 Java 的开源组件，作为无客户端 SSL VPN 会话中网络浏览器的插件来访问。

先决条件

确保无客户端 SSL VPN 已在 ASA 的界面上启用。为此，请输入 **show running - config** 命令。

表 14-2　思科重新分发的插件

协议	说明	重新分布的插件的来源 *
RDP	访问 Windows Vista 和 Windows 2003 R2 托管的 Microsoft 终端服务。 支持远程桌面 ActiveX 控件。 我们建议使用支持 RDP 和 RDP2 的此插件。仅支持最高版本为 5.1 的 RDP 和 RDP2 协议。不支持版本 5.2 及更高版本。	http://properjavardp.sourceforge.net/
RDP2	访问 Windows Vista 和 Windows 2003 R2 托管的 Microsoft 终端服务。 支持远程桌面 ActiveX 控件。 **注**　此旧版插件仅支持 RDP2。我们不建议使用此插件；请换用上述 RDP 插件。	http://properjavardp.sourceforge.net/
SSH	安全外壳 Telnet 插件可供远程用户建立到远程计算机的安全外壳 （v1 或 v2）或 Telnet 连接。 **注**　由于 JavaSSH 不支持键盘交互身份验证，它不受 SSH 插件 （用于实施不同的身份验证机制）支持。	http://javassh.org/
VNC	虚拟网络计算插件可供远程用户使用显示器、键盘和鼠标查看和控制已打开远程桌面共享 （也称为 VNC 服务器或服务）的计算机。此版本更改文本的默认颜色并包含更新的法语和日语帮助文件。	http://www.tightvnc.com/

* 有关部署配置和限制的信息，请参阅插件文档。

这些插件可从思科自适应安全设备软件下载站点下载。

详细步骤

注　ASA 不会在配置中保留命令 **import webvpn plug-in protocol**。相反，它会自动加载 csco-config/97/plugin 目录的内容。辅助 ASA 会从主 ASA 获取插件。

<table>
<tr><th></th><th>命令</th><th>用途</th></tr>
<tr><td>步骤 1</td><td>import webvpn plug-in protocol [rdp | rdp2 | [ssh | telnet] | vnc] URL

示例：
hostname# import webvpn plug-in protocol ssh,telnet tftp://local_tftp_server/plugins/ssh-plugin.jar

Accessing
tftp://local_tftp_server/plugins/ssh-plugin.jar...!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/ssh...
!!
!!!!!!!
238510 bytes copied in 3.650 secs (79503 bytes/sec)</td><td>将插件安装到 ASA 的闪存设备上。protocol 是以下值之一：ssh,telnet 提供对安全外壳和 Telnet 服务的插件访问。

注　请不要分别为 SSH 和 Telnet 输入一次此命令。在键入 telnet 字符串 ssh 时，请不要插入空格。

URL 是插件 .jar 文件的远程路径。输入 TFTP 或 FTP 服务器的主机名或地址以及插件路径。</td></tr>
<tr><td>步骤 2</td><td>（可选）
revert webvpn plug-in protocol protocol

示例：
hostname# revert webvpn plug-in protocol rdp</td><td>关闭和移除无客户端 SSL VPN 对插件的支持，并从 ASA 的闪存驱动器中将其移除。</td></tr>
</table>

提供对 Citrix XenApp 服务器的访问

作为如何提供无客户端 SSL VPN 浏览器对第三方插件的访问的示例，本节介绍如何添加无客户端 SSL VPN 对 Citrix XenApp 服务器客户端的支持。

借助于 ASA 上安装的 Citrix 插件，无客户端 SSL VPN 用户可以使用 ASA 的连接访问 Citrix XenApp 服务。

有状态故障转移不保留使用 Citrix 插件建立的会话。 Citrix 用户必须在故障转移后重新进行身份验证。

要提供对 Citrix 插件的访问，请遵循以下各节中的操作步骤。

- 为无客户端 SSL VPN 访问准备 Citrix XenApp 服务器
- 创建和安装 Citrix 插件

为无客户端 SSL VPN 访问准备 Citrix XenApp 服务器

必须将 Citrix Web Interface 软件配置为在不使用 (Citrix) “安全网关”的模式下运行。否则，Citrix 客户端无法连接至 Citrix XenApp 服务器。

注　如果尚未提供对插件的支持，则必须遵守第 14-4 页上的为安装插件准备安全设备中的说明，才可使用本节内容。

创建和安装 Citrix 插件

详细步骤

步骤 1　从思科软件下载网站下载文件 ica-plugin.zip。

此文件包含思科自定义的可与 Citrix 插件配合使用的文件。

步骤 2　从 Citrix 站点下载 Citrix Java 客户端。

在 Citrix 网站的下载区域，选择 **Citrix Receiver** 和 **Receiver for Other Platforms** 并点击 **Find**。点击 **Receiver for Java** 超链接并下载存档文件。

步骤 3　从存档文件中提取以下文件，然后将它们添加到 ica plugin.zip 文件：

- JICA-configN.jar
- JICAEngN.jar

步骤 4　确保 Citrix Java 客户端随附的 EULA 授予您在网络服务器上部署客户端的权利和权限。

步骤 5　通过使用 ASDM 或在特权 EXEC 模式中输入以下 CLI 命令来安装插件：

import webvpn plug-in protocol ica *URL*

URL 是主机名或 IP 地址以及 ica plugin.zip 文件的路径。

注　提供对 Citrix 会话的 SSO 支持需要添加书签。我们建议您在书签中使用 URL 参数，以方便查看，例如：

ica://10.56.1.114/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

步骤 6　建立 SSL VPN 无客户端会话并点击书签或输入 Citrix 服务器的 URL。

使用 《适用于 Java 的客户端的管理员指南》（根据需要）。

查看在安全设备上安装的插件

详细步骤

	命令	用途
步骤 1	**show import webvpn plug** **示例：** hostname# **show import webvpn plug** ssh rdp vnc ica	列出可供无客户端 SSL VPN 用户使用的基于 Java 的客户应用。
步骤 2	**show import webvpn plug detail** **示例：** hostname **show import webvpn plug** post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tues, 29 Apr 2008 19:57:03 GMT rdp fHeyReIOUwDCgAL9HdTs PnjdBoo= Tues, 15 Sep 2009 23:23:56 GMT rdp2 shw8c22T2SsILLk6zyCd6H6VOz8= Wed, 11 Feb 2009 21:17:54 GMT	纳入插件的哈希值和日期。

配置端口转发

以下各节介绍端口转发以及如何配置它：

有关端口转发的信息

借助于端口转发，用户可通过无客户端 SSL VPN 连接访问基于 TCP 的应用。此类应用包括：

- Lotus Notes
- Microsoft Outlook
- Microsoft Outlook Express
- Perforce
- Sametime
- Secure FTP (FTP over SSH)
- SSH
- Telnet
- Windows Terminal Service
- XDDTS

其他基于 TCP 的应用也可能起作用，但是，我们尚未对其进行测试。使用 UDP 的协议不起作用。

端口转发是通过无客户端 SSL VPN 连接支持基于 TCP 的应用的传统技术。可以选择使用端口转发，因为您已构建支持此技术的早期配置。

考虑端口转发的以下替代项：

- 智能隧道接入为用户提供以下优势：
  - 智能隧道性能比插件更好。
  - 不同于端口转发，智能隧道不要求用户将本地应用连接至本地本地端口，简化了用户体验。
  - 不同于端口转发，智能隧道不要求用户拥有管理员权限。
- 与端口转发和智能隧道接入不同，插件不需要将客户端应用安装在远程计算机上。

在 ASA 上配置端口转发时，指定应用使用的端口。在配置智能隧道接入时，指定可执行文件的名称或其路径。

先决条件

- 远程主机必须运行以下操作系统的 32 位版本：
  - Microsoft Windows Vista、 Windows XP SP2 或 SP3 ；或 Windows 2000 SP4。
  - 安装了 Safari 2.0.4(419.3) 的 Apple Mac OS X 10.4 或 10.5。
  - Fedora Core 4
- 远程主机还必须运行 Oracle Java Runtime Environment (JRE) 5 或更高版本。
- Mac OS X 10.5.3 上基于浏览器的 Safari 用户必须标识与 ASA URL 配合使用的客户端证书，由于 Safari 解释 URL 的方法，此 URL 一次用反斜杠，一次不用。例如，
  - https://example.com/
  - https://example.com

  有关详细信息，请转至 Safari, Mac OS X 10.5.3：客户端证书身份验的变更。
- 使用端口转发或智能隧道的 Microsoft Windows Vista 或更高版本的用户必须将 ASA 的 URL 添加至 Trusted Site 区域。要访问 Trusted Site 区域，它们必须启动 Internet Explorer 并选择 **Tools > Internet Options > Security** 选项卡。 Vista （或更高版本）用户还可关闭保护模式以简化智能隧道接入；但是，由于此方法会使计算机更易于遭受攻击，我们建议不要使用此方法。
- 确保 Oracle Java Runtime Environment (JRE) 1.5.x 或更高版本已安装在远程计算机上，以支持端口转发 （应用接入）和数字证书。如在运行 JRE 1.4.x 且用户使用数字证书进行身份验证，则应用未能启动，因为 JRE 无法访问网络浏览器证书存储区。

限制

- 端口转发仅支持使用静态 TCP 端口的 TCP 应用。使用动态端口或多个 TCP 端口的应用不受支持。例如，使用端口 22 的 SecureFTP 通过无客户端 SSL VPN 端口转发进行工作，但是使用端口 20 和 21 的标准 FTP 却不是这样。
- 端口转发不支持使用 UDP 的协议。
- 端口转发不支持 Microsoft Outlook Exchange (MAPI) 代理。但是，可为 Microsoft Office Outlook 和 Microsoft Outlook Exchange Server 一起配置智能隧道支持。
- 有状态故障转移不保留使用 Application Access （端口转发或智能隧道接入）建立的会话。出现故障转移后，用户必须重新连接。
- 端口转发不支持与个人数字助理的连接。

- 由于端口转发需要下载 Java 小程序和配置本地客户端，并且，由于这样做需要本地系统的管理员权限，因此，在用户从公共远程系统进行连接时可能无法使用应用。

  Java 小程序显示在其自带窗口中的最终用户 HTML 界面上。它显示可向用户提供的已转发端口列表的内容，以及活动的端口和收发的流量 （以字节为单位）。

- 在使用本地 IP 地址 127.0.0.1 时，端口转发小程序会将本地端口和远程端口显示为同一端口，并且无法由源自 ASA 的无客户端 SSL VPN 连接进行更新。因此，ASA 为本地代理 ID 创建新的 IP 地址 127.0.0.2、127.0.0.3 等等。由于可以修改主机文件并使用不同的环回，因此远程端口用作小程序中的本地端口。要连接，可使用含主机名的 Telnet，无需指定端口。本地主机文件中提供正确的本地 IP 地址。

为端口转发配置 DNS

端口转发会将远程服务器的域名或其 IP 地址转发至 ASA 以进行解析和连接。换句话说，端口转发小程序接受来自应用的请求并将其转发至 ASA。 ASA 执行适当的 DNS 查询并代表端口转发小程序建立连接。端口转发小程序只对 ASA 执行 DNS 查询。它更新主机文件，以便在端口转发应用尝试执行 DNS 查询时，查询重定向至环回地址。按以下方式配置 ASA，使其接受来自端口转发小程序的 DNS 请求：

	命令	用途
步骤 1	**dns server-group**	进入 dns server-group 模式。 配置名为 example.com 的 DNS 服务器组。
步骤 2	**domain-name** **示例：** hostname(config)# **dns server-group example.com** hostname(config-dns-server-group)# **domain-name example.com**	指定域名。默认 domain-name 设置为 DefaultDNS。
步骤 3	**name-server** **示例：** hostname(config-dns-server-group)# **name-server 192.168.10.10**	将域名解析为 IP 地址。
步骤 4	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 5	**tunnel-group webvpn**	切换至 tunnel-group 无客户端 SSL VPN 配置模式。
步骤 6	（仅在使用非默认域名 [DefaultDNS] 时才需要。） **dns-group** **示例：** asa2(config-dns-server-group)# **exit** asa2(config)# **tunnel-group DefaultWEBVPNGroup webvpn-attributes** asa2(config-tunnel-webvpn)# **dns-group example.com**	指定隧道组将使用的域名。默认情况下，安全设备将默认无客户端 SSL VPN 组分配为无客户端连接的默认隧道组。如果 ASA 使用该隧道组将设置分配给无客户端连接，请遵循此说明。否则，对于为无客户端连接配置的每个隧道，请遵循此步骤。

使应用符合端口转发条件

每个 ASA 的无客户端 SSL VPN 配置均支持*端口转发列表*，每一个列表均指定为其提供访问的应用所使用的本地和远程端口。由于每个组策略或用户名仅支持一个端口转发列表，因此，必须将每个受支持的 ca 集分组到列表中。要显示 ASA 配置中已存在的端口转发列表条目，输入以下命令：

详细步骤

	命令	用途
步骤 1	`show run webvpn port-forward`	显示 ASA 配置中已存在的端口转发列表条目。
步骤 2	`webvpn`	切换至无客户端 SSL VPN 配置模式。

步骤 3	**port-forward {<list name> <local port> <remote server> <remote port> <description>}**
	
	示例：
	`hostname(config)# webvpn`
	`hostname(config-webvpn)# port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail`
	`hostname(config-webvpn)# port-forward SalesGroupPorts 20025 SMTPSserver 25 Send Mail`
	`hostname(config-webvpn)# port-forward SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH`
	`hostname(config-webvpn)# port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet`
		将端口转发条目添加至列表。
		• *list_name* — 供无客户端 SSL VPN 会话用户访问的一组应用的名称 （从技术上讲，指一组已转发的 TCP 端口）。 ASA 使用输入的名称创建列表 （如果 ASA 未识别该名称）。否则，它将端口转发条目添加至列表。最多 64 个字符。
		• *local_port* — 侦听用户计算机上运行的应用的 TCP 流量的端口。对于每个端口转发列表，本地端口号只能使用一次。输入介于 1 和 65535 之间的端口号或端口名称。为了避免与现有服务冲突，请使用大于 1024 的端口号。
		• *remote_server* — 应用的远程服务器的 DNS 名称或 IP 地址。 IP 地址可以采用 IPv4 或 IPv6 格式。我们建议使用 DNS 名称，这样就无需为特定 IP 地址配置客户端应用。
		注　DNS 名称必须与一个已分配给隧道组的名称匹配，只有这样，才能根据上一节中的说明建立隧道并解析为 IP 地址。该节中介绍的 **domain-name group** 和 **dns-group** 命令的默认设置为 DefaultDNS。
		• *remote_port* — 要为远程服务器上的此应用连接的端口。这是应用使用的实际端口。输入介于 1 和 65535 之间的端口号或端口名称。
		• *description* — 在最终用户的 Port Forwarding Java applet 屏幕上显示的应用名称或短描述。最多 64 个字符。
		
		显示如何创建名为 SalesGroupPorts 的端口转发列表，以提供对这些应用的访问。

步骤 4	（可选） **no port-forward <list name> <local port>**	从列表中移除条目，从而指定列表和本地端口。

如下一节中所述，遵循端口转发列表的配置，将列表分配给组策略或用户名。

分配端口转发列表

可添加或编辑要与通过无客户端 SSL VPN 连接接入的用户或组策略关联的已命名 TCP 列表。对于每个组策略和用户名，可以配置无客户端 SSL VPN 执行以下任一操作：

- 在用户登录时自动启动端口转发访问。

注　对于每个组策略和用户名，这些选项相互排斥。只能使用一个。

先决条件

在启动 **port-forward enable <list name>** 命令之前，用户需要使用无客户端 SSL VPN 门户网站网页上的 **Application Access** > **Start Applications** 手动启动端口转发。

详细步骤

这些命令可用于每个组策略和用户名。每个组策略和用户名的配置一次仅支持其中一个这些命令，因此，输入一个命令时， ASA 均将用新命令替换相关组策略或用户名的配置中存在的命令，或者，如果是最后一个命令，只需从组策略或用户名配置中移除 **port - forward** 命令。

	命令	用途
步骤 1	`port-forward auto-start` **<list name>**	用户登录时自动启动端口转发。
	`port-forward enable` **<list name>**	用户登录时启用端口转发。
	`port-forward disable`	防止端口转发。
	`no port-forward [auto-start` **<list name>** `| enable` **<list name>** `| disable]`	从组策略或用户名配置中移除 **port - forward** 命令，该配置然后从默认组策略继承 **[no] port - forward** 命令。**port - forward** 命令之后的关键字为可选；然而，他们限定于只能移除名为 **port - forward** 的命令。

自动端口转发

要在用户登录时自动启动端口转发，请输入以下命令：

详细步骤

	命令	用途
步骤 1	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 2	**group-policy webvpn** **username webvpn**	切换至组策略无客户端 SSL VPN 配置模式。 切换至用户名无客户端 SSL VPN 配置模式。
步骤 3	**port-forward auto-start <list name>** **示例：** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **port-forward auto-start apps1**	用户登录时自动启动端口转发。 *list_name* 命名 ASA 无客户端 SSL VPN 配置中已存在的端口转发列表。无法将多个端口转发列表分配给一个组策略或用户名。 将名为 apps1 的端口转发列表分配给组策略。
步骤 4	**show run webvpn port-forward**	显示 ASA 配置中已存在的端口转发列表条目。
步骤 5	（可选） **no port-forward**	从组策略或用户名中移除 **port - forward** 命令并恢复默认设置。

启用和关闭端口转发

默认情况下，端口转发已关闭。

详细步骤

	命令	用途
步骤 1	**port-forward [enable <list name> | disable]** **示例：** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **port-forward enable apps1**	启用端口转发。如果输入上一个表中的 **port-forward auto-start** *list_name*，则无需手动启动端口转发。 *list_name* 是 ASA 无客户端 SSL VPN 配置中已存在的端口转发列表的名称。无法将多个端口转发列表分配给一个组策略或用户名。 将名为 apps1 的端口转发列表分配给组策略。
步骤 2	**show running-config port-forward**	显示端口转发列表条目。
步骤 3	（可选） **no port-forward**	从组策略或用户名中移除 **port - forward** 命令并恢复默认设置。
步骤 4	（可选） **port-forward disable**	关闭端口转发。

配置文件访问

无客户端 SSL VPN 为远程用户提供与 ASA 上运行的代理 CIFS 和 / 或 FTP 客户端连接的 HTTPS 门户网站网页。通过使用 CIFS 或 FTP，无客户端 SSL VPN 向用户提供网络文件的网络访问，在某种程度上，用户需满足身份验证需求并且文件属性不会限制访问。 CIFS 和 FTP 客户端是透明的；无客户端 SSL VPN 所交付的门户网站网页提供直接访问文件系统的外观。

在用户请求文件列表时，无客户端 SSL VPN 将查询为包含列表的服务器 IP 地址指定为主浏览器的服务器。 ASA 获取列表并将其交付给门户网站网页的远程用户。

借助于无客户端 SSL VPN，用户可根据用户身份验证需求和文件属性调用以下 CIFS 和 FTP 功能。

- 导航并列出域和工作组、域或工作组中的服务器、服务器内的共享以及共享或目录内的文件。
- 创建目录。
- 下载、上传、重命名、移动和删除文件。

当远程用户点击门户网站网页的菜单中或在无客户端 SSL VPN 会话期间显示的工具栏上的 **Browse Networks** 时， ASA 使用通常与 ASA 处于同一网络或从该网络访问的主浏览器、 WINS 服务器或 DNS 服务器在该网络中查询服务器列表。

主浏览器或 DNS 服务器向 ASA 上的 CIFS/FTP 客户端提供网络资源的列表，无客户端 SSL VPN 向远程用户提供该列表。

注　在配置文件访问之前，必须在服务器上配置共享供用户访问。

CIFS 文件访问要求和限制

要访问*文件夹* `\\server\share\subfolder\personal`，用户必须具有所有父文件夹 （包括共享本身）的最低读取权限。

使用 **Download** 或 **Upload**，在 CIFS 目录和本地桌面之间复制和粘贴文件。 Copy and Paste 按钮仅适用于远程到远程操作，不适用于本地到远程或远程到本地操作。

CIFS 浏览服务器功能不支持双字节字符共享名称 （长度超过 13 个字符的共享名称）。这仅影响显示的文件夹的列表，不影响用户对文件夹的访问。作为解决方法，可为使用双字节共享名称的 CIFS 文件夹预配置书签，用户也可输入 URL 或用 cifs://server/<long-folder-name> 格式为文件夹添加书签。例如：

```
cifs://server/Do you remember?
cifs://server/Do%20you%20remember%3F
```

添加对文件访问的支持

按以下所示配置文件访问：

注　此操作步骤说明如何指定主浏览器和 WINS 服务器。或者，可使用 ASDM 配置 URL 列表和条目以提供文件共享访问。

在 ASDM 中添加共享不需要主浏览器或 WINS 服务器。但是，它不提供对浏览网络链接的支持。在输入 **nbns - server** 命令时，可使用主机名或 IP 地址指代 ServerA。如使用主机名， ASA 需要 DNS 服务器将其解析为 IP 地址。

详细步骤

	命令	用途
步骤 1	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 2	**tunnel-group webvpn**	切换至 tunnel-group 无客户端 SSL VPN 配置模式。
步骤 3	**nbns-server** {IPaddress | hostname} **[master] [timeout** *timeout*] **[retry** *retries*] **示例：** hostname(config-tunnel-webvpn)# **nbns-server 192.168.1.20 master** hostname(config-tunnel-webvpn)# **nbns-server 192.168.1.41** hostname(config-tunnel-webvpn)# **nbns-server 192.168.1.47**	浏览每个 NetBIOS 名称服务器的 (NBNS) 的网络或域。 • **master** 是指定为主浏览器的计算机。主浏览器保留计算机和共享资源的列表。通过此命令标识但未输入该命令的主要部分的任何 NBNS 服务器均必须为 Windows Internet 命名服务器 (WINS)。首先指定主浏览器，然后指定 WINS 服务器。最多可为连接配置指定三台服务器，包括主浏览器。 • *timeout* 是在向相同服务器 （若只有一台）或其他服务器 （若有多台）再次发送查询之前 ASA 等待的秒数。默认超时是 2 秒，范围是 1 至 30 秒。 • *retries* 是向 NBNS 服务器重试查询的次数。ASA 在发送错误消息之前按此次数循环服务器列表。默认值为 2；范围为 1 至 10。
步骤 4	**hostname# show tunnel-group webvpn-attributes**	显示连接配置文件配置中已存在的 NBNS 服务器。
步骤 5	（可选） **character-encoding** ***charset*** **示例：** hostname(config)# **webvpn** hostname(config-webvpn)# **character-encoding shift_jis** hostname(config-webvpn)# **customization DfltCustomization** hostname(config-webvpn-custom)# **page style background-color:white**	指定要在交付给远程用户的无客户端 SSL VPN 门户网站网页中编码的字符集。默认情况下，远程浏览器上的编码类型集确定无客户端 SSL VPN 门户网站网页的字符集，因此，只有需要确保在浏览器上正确编码的情况下才需要设置字符编码。 *charset* 是最多包含 40 个字符的字符串，并且与在 http://www.iana.org/assignments/character-sets 中标识的其中一个有效字符集相同 . 您可以使用该页列出的字符集的名称或别名。示例包括 iso-8859-1、 shift_jis 和 ibm850。 **注**　character-encoding 和 file-encoding 值不排除浏览器将使用的字体系列。如果使用日语 Shift_JIS 字符编码，则需要使用 webvpn 自定义命令模式中的命令 **page style** 补充这些值之一的设置，以替换字体系列，如以下示例所示，或输入 webvpn 自定义命令模式中的命令 **no page style**，以移除字体系列。 设置字符编码属性以支持 Shift_JIS 字符、删除字体系列并保留默认背景颜色。
步骤 6	（可选） **file-encoding {server-name | server-ip-address}** ***charset*** **示例：** hostname(config-webvpn)# **file-encoding 10.86.5.174 cp860**	从特定 CIFS 服务器为无客户端 SSL VPN 门户网站网页指定编码。因此，可将不同的 file-encoding 值用于需要不同字符编码的 CIFS 服务器。 设置 CIFS 服务器 10.86.5.174 的 file-encoding 属性以支持 IBM860 （别名 “CP860”）字符。

有关这些命令的完整说明，请参阅命令参考。

确保 SharePoint 访问的时钟准确性

ASA 上的无客户端 SSL VPN 服务器使用 cookie 与应用 （如终端上的 Microsoft Word）交互。如果 ASA 上的时间不正确，在访问 SharePoint 服务器上的文档时， ASA 设置的 cookie 过期时间可导致 Word 出现故障。为防止此故障，请正确设置 ASA 时钟。我们建议将 ASA 配置为与 NTP 服务器动态同步时间。有关说明，请参阅常规操作配置指南中关于设置日期和时间的小节。

虚拟桌面基础设施 (VDI)

ASA 支持与 Citrix 和 VMWare VDI 服务器的连接。

- 对于 Citrix， ASA 允许通过无客户端门户网站访问用户运行的 Citrix Receiver。
- VMWare 已配置为 （智能隧道）应用。

与其他服务器应用一样，还可通过无客户端门户网站上的书签访问 VDI 服务器。

限制

- 由于这些形式的身份验证不允许中间的 ASA，因此，不支持在自动登录时使用证书或智能卡进行的身份验证。
- XML 服务必须在 XenApp 和 XenDesktop 服务器上安装和配置。
- 在使用独立移动客户端时，不支持客户端证书验证、双重身份验证、内部密码和 CSD （全部 CSD，不只是 Vault）。

Citrix 移动支持

运行 Citrix Receiver 的移动用户可按以下方式连接至 Citrix 服务器：

- 使用 AnyConnect 连接至 ASA，然后连接至 Citrix 服务器。
- 通过 ASA 连接至 Citrix 服务器，无需使用 AnyConnect 客户端。登录凭据可能包括：
  - Citrix 登录屏幕中的连接配置文件别名 （也称为隧道组别名）。 VDI 服务器可能有多个组策略，每个都具有不同的授权和连接设置。
  - 配置 RSA 服务器时的 RSA SecureID 令牌值。 RSA 支持包括无效条目的下一个令牌，还包括用于为初始或过期 PIN 输入新 PIN 的下一个令牌。

受支持的移动设备

- iPad-Citrix Receiver 版本 4.x 或更高版本
- iPhone/iTouch-Citrix Receiver 版本 4.x 或更高版本
- Android 2.x/3.x/4.0/4.1 phone-Citrix Receiver 版本 2.x 或更高版本
- Android 4.0 phone-Citrix Receiver 版本 2.x 或更高版本

限制

证书限制

- 不支持将证书 / 智能卡身份验证作为自动登录方式。
- 客户端证书验证和 CSD 不受支持
- 由于安全问题，证书中的 Md5 签名无效，此问题为 iOS 中的已知问题，网址为 http://support.citrix.com/article/CTX132798
- 只有 Windows 支持 SHA2 签名，如 Citrix 网站上所述，网址为 http://www.citrix.com/
- 超过 1024 的密钥大小不受支持

其他限制

- 不支持 HTTP 重定向； Citrix Receiver 应用不适用于重定向。
- XML 服务必须在 XenApp 和 XenDesktop 服务器上安装和配置。

关于 Citrix Mobile Receiver 用户登录

连接 Citrix 服务器的移动用户登录取决于 ASA 是将 Citrix 服务器配置为 VDI 服务器，还是配置为 VDI 代理服务器。

当 Citrix 服务器配置为 VDI 服务器时：

1. 通过使用 AnyConnect 安全移动客户端，连接至具有 VPN 凭证的 ASA。
2. 通过使用 Citrix Mobile Receiver，连接至具有 Citrix 服务器凭据的 Citrix 服务器（如已配置单点登录，则不需要 Citrix 凭据）。

当 ASA 配置为 VDI 代理服务器时：

1. 通过使用 Citrix Mobile Receiver 并输入 VPN 和 Citrix 服务器的凭据，连接至 ASA。在第一次连接后，如果配置正确，后续连接只需要 VPN 凭据。

已将 ASA 配置为代理 Citrix 服务器

可将 ASA 配置为充当 Citrix 服务器的代理，因此，对于用户而言，ASA 的连接看起来与 Citrix 服务器的连接相似。在 ASDM 中启用 VDI 代理时，不需要 AnyConnect 客户端。以下高级别步骤显示最终用户如何连接至 Citrix。

1. 移动用户打开 Citrix Receiver 并连接至 ASA 的 URL。
2. 用户为 XenApp 服务器提供凭据和 Citrix 登录屏幕上的 VPN 凭据。
3. 对于 Citrix 服务器的每个后续连接，用户只需输入 VPN 凭据。

如将 ASA 用作 XenApp 和 XenDesktop 的代理，则会移除 Citrix 访问网关的要求。XenApp 服务器信息记录在 ASA 上并显示在 ASDM 中。

配置 Citrix 服务器的地址和登录凭据，并将该 VDI 服务器分配给组策略或用户名。如已配置用户名和组策略，则用户名设置将覆盖组策略设置。

其他信息

http://www.youtube.com/watch?v=JMM2RzppaG8 — 此视频介绍将 ASA 用作 Citrix 代理的优势。

将 VDI 服务器分配给组策略

已按以下方式配置 VDI 服务器并将其分配给组策略：

- 在 VDI Access 窗格上添加 VDI 服务器，并将组策略分配给该服务器。
- 将 VDI 服务器添加至组策略。

如已配置用户名和组策略，则用户名设置优先于组策略。输入以下命令：

```
configure terminal
    group-policy DfltGrpPolicy attributes
        webvpn
            vdi type <citrix> url <url> domain <domain> username <username> password
            <password>
configure terminal
    username <username> attributes
        webvpn
            vdi type <citrix> url <url> domain <domain> username <username> password
            <password>]
```

语法选项定义如下：

- type — VDI 的类型。对 Citrix Receiver 类型，该值必须为 *citrix*。
- url — XenApp 或 XenDesktop 服务器的完整 URL，包括 http 或 https、主机名和端口号，以及 XML 服务的路径。
- username — 用于登录虚拟化基础设施服务器的用户名。该值可能是无客户端宏。
- password — 用于登录虚拟化基础设施服务器的密码。该值可能是无客户端宏。
- domain — 用于登录虚拟化基础设施服务器的域。该值可能是无客户端宏。

使用 SSL 访问内部服务器

	命令	用途
步骤 1	`webvpn`	切换至组策略无客户端 SSL VPN 配置模式。
步骤 2	`url-entry disable`	关闭 URL Entry。

无客户端 SSL VPN 使用 SSL 及其后继者 TLS1 在远程用户与内部服务器上受支持的特定内部资源之间提供安全连接。

- 第 14-19 页上的将 HTTPS 用于无客户端 SSL VPN 会话
- 第 14-19 页上的配置无客户端 SSL VPN 和 ASDM 端口
- 第 14-20 页上的配置对代理服务器的支持
- 第 14-22 页上的配置 SSL/TLS 加密协议

将 HTTPS 用于无客户端 SSL VPN 会话

先决条件

在网络浏览器中，用户输入 https://*address* 格式的 ASA 地址，其中 *address* 是 ASA 接口的 IP 地址或 DNS 主机名。

限制

- 必须在用户连接至的 ASA 界面上启用无客户端 SSL VPN 会话。
- 必须使用 HTTPS 访问 ASA 或负载平衡集群。

	命令	用途
步骤 1	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 2	**enable** <name of interface to use for Clientless SSL VPN sessions> **示例：** hostname(config)# **webvpn** hostname(config-webvpn)# **enable outside**	在外部调用的界面上启用无客户端 SSL VPN 会话。

配置无客户端 SSL VPN 和 ASDM 端口

从版本 8.0(2) 开始，ASA 同时支持外部接口的端口 443 上的无客户端 SSL VPN 会话和 ASDM 管理会话。可在不同的界面上配置这些应用。

	命令	用途
步骤 1	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 2	**port** *port_number* **示例：** hostname(config)# **http server enable** hostname(config)# **http 192.168.3.0 255.255.255.0 outside** hostname(config)# **webvpn** hostname(config-webvpn)# **port 444** hostname(config-webvpn)# **enable outside**	为无客户端 SSL VPN 更改 SSL 侦听端口。 在外部接口的端口 444 上启用无客户端 SSL VPN。借助于此配置，初始化无客户端 SSL VPN 会话的远程用户在浏览器中输入 https://<outside_ip>:444。
步骤 3	**http 服务器启用** **示例：** hostname(config)# **http server enable** hostname(config)# **http 192.168.3.0 255.255.255.0 outside** hostname(config)# **webvpn** hostname(config-webvpn)# **enable outside**	（特权模式）为 ASDM 更改侦听端口。 指定 HTTPS ASDM 会话使用外部接口上的端口 444。无客户端 SSL VPN 也在外部接口上启用并使用默认端口 (443)。借助于此配置，远程用户通过输入 https://<outside_ip>:444 初始化 ASDM 会话

配置对代理服务器的支持

ASA 可终止 HTTPS 连接并将 HTTP 和 HTTPS 请求转发至代理服务器。这些服务器在用户与公共或专用网络之间充当中介。如果要求通过组织控制的代理服务器进行网络访问，则可提供其他过滤机会，以确保安全的网络访问和管理控制。

在配置对 HTTP 和 HTTPS 代理服务的支持时，可分配将随每个基本身份验证请求一起发送的预设凭据。还可指定要从 HTTP 和 HTTPS 请求中排除的 URL。

限制

可指定要从 HTTP 代理服务器下载的代理自动配置 (PAC) 文件，然而，在指定 PAC 文件时不能使用代理身份验证。

	命令	用途
步骤 1	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 2	**http-proxy 和 https-proxy**	配置 ASA，使其使用外部代理服务器处理 HTTP 和 HTTPS 请求。 **注**　**http-proxy** 中不支持代理 NTLM 身份验证。只支持无身份验证的代理和基本身份验证。
步骤 3	**http-proxy** *host* [*port*] [**exclude** *url*] [**username** *username* {**password** *password*}]	配置 HTTP 代理。
步骤 4	**https-proxy** *host* [*port*] [**exclude** *url*] [**username** *username* {**password** *password*}]	配置 HTTPS 代理。
步骤 5	**http-proxy pac** *url*	设置 PAC 文件 URL。
步骤 6	（可选） exclude	从可发送至代理服务器的请求中排除 URL。
步骤 7	*host*	提供外部代理服务器的主机名或 IP 地址。
步骤 8	pac	下载至 ASA 的代理自动配置文件，该文件使用 JavaScript 函数标识每个 URL 的代理。
步骤 9	（可选，仅在指定用户名的情况下可用） password	每个代理请求均附有一个密码，以提供基本代理身份验证。
步骤 10	*password*	随每个 HTTP 或 HTTPS 请求发送至代理服务器的密码。
步骤 11	（可选） *port*	提供代理服务器使用的端口号。默认 HTTP 端口为 80。默认 HTTPS 端口为 443。如未指定替代值，则 ASA 使用每一这些端口。范围为 1-65535。

	命令	用途
步骤 12	*url*	如已输入 **exclude**，则请输入一个 URL 或多个 URL 的逗号分隔列表，以从可发送至代理服务器的请求中排除这些 URL。字符串没有字符限制，但是整个命令不能超过 512 个字符。您可以指定文本 URL 或使用以下通配符： – ***** 匹配任意字符串，包括斜线 (/) 和句点 (.)。必须将此通配符与字母数字字符串结合使用。 – **?** 匹配任意单个字符，包括斜线和句点。 – [*x*-*y*] 匹配 *x* 至 *y* 的范围内的任意单个字符，其中 *x* 代表一个字符，*y* 代表 ANSI 字符集中的另一个字符。 – [**!***x*-*y*] 匹配不属于该范围的任意单个字符。
步骤 13	如已输入 **http-proxy pac**，请在其后输入 **http://** 并键入代理自动配置文件的 URL。（如果省略 **http://** 部分，则 CLI 将忽略命令。）	-
步骤 14	（可选） `username`	随每个 HTTP 代理请求附上用于基本代理身份验证的用户名。仅 **http-proxy** *host* 命令支持该关键字。
步骤 15	*username*	随每个 HTTP 或 HTTPS 请求一起发送至代理服务器的用户名。

步骤 16	**示例：**
	`hostname(config-webvpn)# http-proxy 209.165.201.1 user jsmith password mysecretdonttell`
	
	`hostname(config-webvpn)`
		显示如何配置借助默认端口将 HTTP 代理服务器与 IP 地址 209.165.201.1 一起使用，从而随每个 HTTP 请求发送用户名和密码。

步骤 17	**示例：**
	`hostname(config-webvpn)# http-proxy 209.165.201.1 exclude www.example.com username jsmith password mysecretdonttell`
	`hostname(config-webvpn)`
		显示相同的命令，但在 ASA 接收 HTTP 请求中的特定 URL www.example.com 时除外，在此时，它解析请求而不是将请求传递给代理服务器。

步骤 18	**示例：**
	`hostname(config-webvpn)# http-proxy pac http://www.example.com/pac`
	`hostname(config-webvpn)`
		显示如何指定 URL，以便为浏览器提供代理自动配置文件。

ASA 无客户端 SSL VPN 配置仅支持一个 **http-proxy** 和一个 **https-proxy** 命令。例如，如果 **http-proxy** 命令的一个实例已存在于正在运行的配置中，并且您输入了另一个实例，则 CLI 将覆盖上一个实例。

注　**http-proxy** 中不支持代理 NTLM 身份验证。仅支持无身份验证和基本身份验证的代理。

配置 SSL/TLS 加密协议

端口转发需要 Oracle Java Runtime Environment (JRE)。当无客户端 SSL VPN 的用户使用某些 SSL 版本进行连接时，端口转发不起作用。有关受支持的 JRE 版本，请参阅兼容性矩阵。

使用数字证书进行身份验证

SSL 使用数字证书进行身份验证。 ASA 在启动时创建自签名 SSL 服务器证书；或者您可在 ASA 中安装 PKI 情景中已发行的 SSL 证书。对于 HTTPS，必须将此证书安装在客户端上。

限制

MS Outlook、 MS Outlook Express 和 Eudora 等邮件客户端无法访问证书存储。

有关使用数字证书进行身份验证和授权的详细信息，请参阅常规操作配置指南中关于使用证书和用户登录凭据的小节。

配置客户端服务器插件的浏览器访问

客户端服务器插件表显示 ASA 向无客户端 SSL VPN 会话中浏览器提供的插件。

如要添加、更改或移除插件，请执行以下操作之一：

- 如要添加插件，点击 **Import**。 Import Plug-ins 对话框将打开。
- 如要移除插件，选定它并点击 **Delete**。

以下各节介绍如何为无客户端 SSL VPN 浏览器访问集成浏览器插件：

- 关于安装浏览器插件
- 为安装插件准备安全设备
- 安装思科重新分发的插件

关于安装浏览器插件

浏览器插件是网络浏览器在执行专用功能时 （例如，将客户端连接至浏览器窗口中的服务器）调用的一个单独程序。借助于 ASA，可在无客户端 SSL VPN 会话中导入要下载至远程浏览器的插件。当然，思科将测试其重新分发的插件，在某些情况下，将测试其无法重新分发的插件的连接性。但是，我们建议不要导入目前支持流媒体的插件。

在闪存设备上安装插件时， ASA 将执行以下操作：

- （仅限思科分发的插件）解压缩 *URL* 中指定的 jar 文件。
- 将文件写入 ASA 文件系统上的 csco-config/97/plugin 目录。
- 填充 ASDM 中 URL 属性旁边的下拉列表。
- 为所有未来无客户端 SSL VPN 会话启用插件，然后将主菜单选项和选项添加至门户网站网页 Address 字段旁边的下拉列表。

表 14-3 显示在添加以下各节中描述的插件时对门户网站网页的主菜单和 Address 字段做出的更改。

表 14-3　无客户端 SSL VPN 门户网站网页上插件的效果

插件	已添加至门户网站网页的主菜单选项	已添加至门户网站网页的 Address 字段选项
ica	Citrix Client	citrix://
rdp	Terminal Servers	rdp://
rdp2	Terminal Servers Vista	rdp2://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

注　辅助 ASA 从主 ASA 获取插件。

当用户在无客户端 SSL VPN 会话中点击门户网站网页上的关联菜单选项时，门户网站网页显示界面窗口和帮助窗格。用户可选择下拉列表中显示的协议，并在 Address 字段中输入 URL，以建立连接。

注　即使目标服务的会话未建立，某些 Java 插件也可能报告已连接或联机状态。开源插件报告状态，而不是 ASA。

在安装第一个插件之前，必须遵循下一节中的说明。

先决条件

- 如果安全设备配置要使用代理服务器的无客户端会话，则插件不起作用。

注　远程桌面协议插件不支持用会话代理程序进行负载平衡。由于协议处理源自会话代理程序的重定向的方法不当，连接失败。如未使用会话代理程序，插件将发挥正常作用。

- 插件支持单点登录 (SSO)。它们使用所输入的*相同凭据*打开无客户端 SSL VPN 会话。因为插件不支持宏替换，所以，您无法选择对不同的字段（如内部域密码）或 RADIUS 或 LDAP 服务器上的属性执行 SSO。
- 如要为插件配置 SSO 支持，需安装插件，添加书签条目以显示服务器链接，并在添加书签时指定 SSO 支持。
- 远程使用所需的最低访问权限属于宾客特权模式。

要求

- 根据 GNU 通用公共许可证 (GPL)，思科重新分发插件，但未对其做出任何更改。根据 GPL，思科无法直接增强这些插件的功能。
- 无客户端 SSL VPN 只有在 ASA 上启用才能提供对插件的远程访问。
- 有状态故障转移不保留使用插件建立的会话。出现故障转移后，用户必须重新连接。
- 插件要求在浏览器上启用 ActiveX 或 Oracle Java Runtime Environment (JRE) 1.4.2（或更高版本）。对于 64 位浏览器， RDP 插件没有 ActiveX 版本。

RDP 插件 ActiveX 调试快速参考

如要设置和使用 RDP 插件，必须添加新的环境变量。

步骤 1　右键单击 **My Computer** 以访问 System Properties，并选择 **Advanced** 选项卡。

步骤 2　在 Advanced 选项卡上，选择环境变量按钮。

步骤 3　在 New User Variable 对话框中，输入变量 RF_DEBUG。

步骤 4　验证用户变量部分中的新环境变量。

步骤 5　如将客户端计算机与低于版本 8.3 版本的无客户端 SSL VPN 使用，则必须移除旧版 Cisco Portforwarder Control。转至目录 C:/WINDOWS/Downloaded Program Files，右键单击 portforwarder 控件，然后选择 **Remove**。

步骤 6　清除 Internet Explorer 浏览器的所有缓存。

步骤 7　启动无客户端 SSL VPN 会话并用 RDP ActiveX 插件建立 RDP 会话。

现可查看 Windows 应用事件查看器中的事件。

为安装插件准备安全设备

步骤 1　确保在 ASA 界面上已启用无客户端 SSL VPN。

步骤 2　在远程用户使用完全限定域名 (FQDN) 连接到的 ASA 界面上安装 SSL 证书。

注　请勿将 IP 地址指定为 SSL 证书的通用名称 (CN)。远程用户尝试使用 FQDN 与 ASA 进行通信。远程 PC 必须能够使用 DNS 或 System32\drivers\etc\hosts 文件中的条目解析 FQDN。

配置 ASA 以使用新的 HTML 文件

详细步骤

	命令	用途
步骤 1	**import webvpn webcontent <file> <url>** **示例：** hostname# **import webvpn webcontent /+CSCOU+/login.inc tftp://209.165.200.225/login.inc** !!!!* Web resource `+CSCOU+/login.inc' was successfully initialized hostname#	将文件和图像作为网络内容导入。
步骤 2	**export webvpn customization <file> <URL>** **示例：** hostname2# **export webvpn customization template tftp://209.165.200.225/sales_vpn_login** !! %INFO: Customization object 'Template' was exported to tftp://10.21.50.120/sales _vpn_login	导出自定义模板。
步骤 3	在文件中更改要启用的完全自定义模式标记。 **示例：** <full-customization> <mode>**enable**</mode> <url>/**+CSCOU+/login.inc**</url> </full-customization>	提供 ASA 内存中已存储的登录文件的 URL。
步骤 4	导入文件作为新自定义对象 **示例：** hostname# **import webvpn customization sales_vpn_login tftp://10.21.50.120/sales_vpn_login**$!! %INFO: customization object 'sales_vpn_login' was successfully imported	-
步骤 5	将自定义对象应用于连接配置文件 （隧道组） **示例：** hostname(config)# **tunnel-group Sales webvpn-attributes** hostname(config-tunnel-webvpn)#**customization sales_vpn_login**	-

第 15 章

高级无客户端 SSL VPN 配置

2013 年 9 月 13 日

Microsoft Kerberos 约束委派解决方案

很多组织都想要对其无客户端 VPN 用户进行身份验证并使用超出现在 ASA 可以提供的身份验证方法将身份验证凭据无缝扩展至基于网络的资源。随着对使用智能卡和一次性密码 (OTP) 的远程访问用户进行身份验证的需求日益增长， SSO 功能无法满足这种需求，因为当需要进行身份验证时，它只是向基于网络的无客户端资源转发静态用户名和密码等传统用户凭据。

例如，证书和基于 OTP 的身份验证方法都不包含 ASA 对基于网络的资源无缝地进行 SSO 访问所需的传统用户名和密码。利用证书进行身份验证时， ASA 不需要用户名和密码即可扩展至基于网络的资源，使其成为 SSO 不支持的一种身份验证方法。另一方面，虽然 OTP 确实包括静态用户名，但密码是动态的，并且随后在整个 VPN 会话期间也会发生改变。一般来说，基于网络的资源都配置为接受静态用户名和密码，因此也使 OTP 成为 SSO 不支持的一种身份验证方法。

Microsoft 的 Kerberos 约束委派 (KCD) 是 ASA 的 8.4 版本软件中引入的一个新功能，可提供对专用网络中受 Kerberos 保护的网络应用的访问。利用此优势，您可以无缝地将基于证书和 OTP 的身份验证方法扩展至网络应用。因此，通过同时但独立地使用 SSO 和 KCD，现在很多组织都可以对无客户端 VPN 用户进行身份验证，并将他们的身份验证凭据无缝扩展至使用 ASA 支持的所有身份验证方法的网络应用。

要求

为了让 **kcd-server** 命令正常运行， ASA 必须在*源*域（即 ASA 所在的域）和*目标*或*资源*域（即网络服务所在的域）之间建立信任关系。 ASA 使用其独特的格式，跨越从源到目标域的证书路径并代表远程访问用户获取访问服务所需的票证。

这种跨越证书路径的操作叫做跨域身份验证。在跨域身份验证的每个阶段， ASA 依赖于特定域上的凭据和与后续域的信任关系。

了解 KCD 的工作方式

Kerberos 依赖受信任的第三方来验证网络中实体的数字身份。这些实体 （例如用户、主机和主机上运行的服务）称为主体，并且必须位于同一个域内。 Kerberos 使用票证，而不是使用密钥，来验证访问服务器的客户端。票证源于密钥，由客户端的身份、加密的会话密钥和标志组成。每个票证由密钥发行中心发行并具有设定的生命期。

Kerberos 安全系统是一种身份验证协议，用于验证实体 （用户、计算机或应用）并通过打乱数据从而使只有指定接收该信息的设备可以解密这些数据保护网络传输。您可以配置 KCD，向无客户端 SSL VPN 用户提供对任何受 Kerberos 保护的网络服务的 SSO 访问。这类网络服务或应用示例包括 Outlook Web Access (OWA)、 Sharepoint 和互联网信息服务器 (IIS)。

Kerberos 协议实施了两项扩展：*协议转换*和*约束委派*。这两项扩展允许无客户端 SSL VPN 远程访问用户访问专用网络中通过 Kerberos 身份验证的应用。

*协议转换*在用户身份验证层面支持不同的身份验证机制，而且会在随后的应用层中切换至 Kerberos 协议以获得更多安全功能 （例如相互身份验证和约束委派），从而为您提供了更高的灵活性和安全性。*约束委派*为域管理员提供了一种通过限制应用服务可以代表用户的情况指定并执行应用信任边界的方法。这种灵活性减少了受不信任服务危害的几率，改善了应用安全设计。

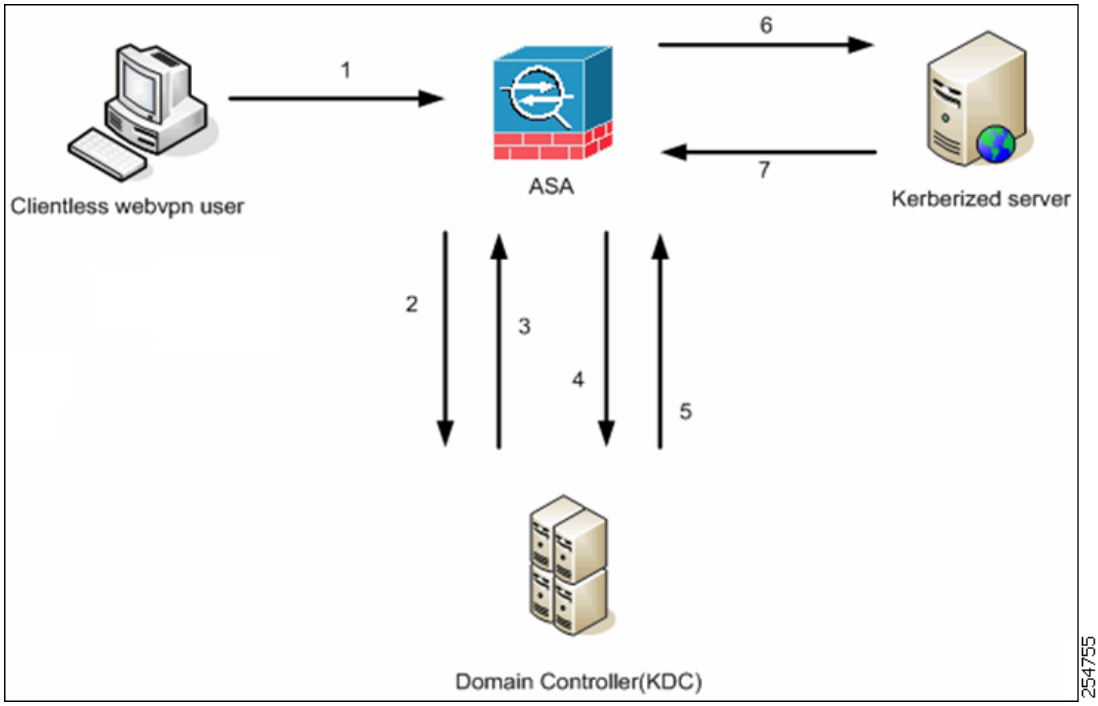
有关约束委派的详细信息，请通过 IETF 网站参阅 RFC 1510 (http://www.ietf.org)。

使用 KCD 的身份验证流程

图 15-1 描述了用户通过无客户端门户访问被信任进行委派的资源时直接和间接体验的数据包和流程。此流程假设已完成以下任务：

- 已在 ASA 上配置 KCD
- 已加入 Windows Active Directory，并已确保服务被信任进行委派
- 已委派 ASA 作为 Windows Active Directory 域的成员

图 15-1　　KCD 流程



注　无客户端用户会话由 ASA 使用为用户配置的身份验证机制进行身份验证。（在使用智能卡凭据的情况下， ASA 使用数字证书的 userPrincipalName 对 Windows Active Directory 执行 LDAP 授权）。

1. 身份验证成功后，用户登录进入 ASA 无客户端门户页面。用户可以通过在门户页面中输入 URL 或点击书签访问网络服务。如果网络服务要求进行身份验证，服务器将请求 ASA 提供凭据并发送一份受服务器支持的身份验证方法列表。

   注　适用于无客户端 SSL VPN 的 KCD 支持所有身份验证方法 （RADIUS、 RSA/SDI、LDAP、数字证书等等）。请参阅 AAA 支持表格，网址为 http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_aaa.html#wp1069492。

2. 根据请求中的 HTTP 报头， ASA 确定服务器是否要求进行 Kerberos 身份验证。（这是 SPNEGO 机制的一部分。）如果连接到后端服务器要求进行 Kerberos 身份验证， ASA 将代表密钥发行中心为自身请求获取服务票证。
3. 密钥发行中心将向 ASA 返回所请求的票证。即使这些票证传递到 ASA，它们仍包含用户的授权数据。 ASA 就用户想要访问的特定服务向 KDC 请求获取服务票证。

   注　第 1 步至第 3 步包含协议转换。完成这些步骤后，任何使用非 Kerberos 身份验证协议进行身份验证访问 ASA 的用户都显然已使用 Kerberos 向密钥发行中心完成身份验证。

4. ASA 为用户想要访问的特定服务向密钥发行中心请求获取服务票证。
5. 密钥发行中心将特定服务的服务票证返回至 ASA。
6. ASA 使用此服务票证请求访问网络服务。
7. 网络服务器对 Kerberos 服务票证进行身份验证并授权访问此服务。如果身份验证失败，系统将显示相应的错误消息并要求确认。如果 Kerberos 身份验证失败，预期行为是退回到基本身份验证。

配置 KCD 之前

如要为跨域身份验证配置 ASA，您必须使用以下命令。

	命令	用途
步骤 1	**ntp** hostname **示例：** hostname(config)# **configure terminal** # 为域控制器创建别名 hostname(config)# **name 10.1.1.10 DC** # 配置名称服务器	加入 Active Directory 域。 10.1.1.10 域控制器 （可在接口内接触到）。
步骤 2	**dns domain-lookup** **dns server-group** **示例：** hostname(config)# **ntp server DC** # 通过配置 DNS 服务器和域名启用 DNS 查找 hostname(config)# **dns domain-lookup inside** hostname(config)# **dns server-group DefaultDNS** hostname(config-dns-server-group)# **name-server DC** hostname(config-dns-server-group)# **domain-name private.net** # 利用服务器和领域配置 AAA 服务器组 hostname(config)# **aaa-server KerberosGroup protocol Kerberos** hostname(config-asa-server-group)# **aaa-server KerberosGroup (inside) host DC** hostname(config-asa-server-group)# **Kerberos-realm PRIVATE.NET** # 配置域加入 hostname(config)# **webvpn** hostname(config-webvpn)# **kcd-server KerberosGroup username dcuser password dcuser123!** hostname(config)#	执行查找。 本示例显示 private.net 的域名以及使用 dcuser 作为用户名并使用 dcuser123！作为密码的域控制器上的一个服务帐户。

配置 KCD

如要使 ASA 加入 Windows Active Directory 域并返回成功或失败状态，请执行以下步骤。

详细步骤

	命令	用途
步骤 1	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 2	**kcd-server**	配置 KCD。

	命令	用途
步骤 3	**kcd-server** ***aaa-server-group*** **示例：** ASA(config)# **aaa-server KG protocol kerberos** ASA(config)# **aaa-server KG (inside) host DC** ASA(config-aaa-server-host)# k**erberos-realm test.edu** ASA(webvpn-config)# k**cd-server KG username user1 password abc123** ASA(webvpn-config)# **no kcd-server**	指定域控制器名称和领域。 AAA 服务器组必须是 Kerberos 类型。
步骤 4	（可选） **no kcd-server**	为 ASA 移除指定行为。
步骤 5	（可选） **kcd-server reset**	重置为内部状态。
步骤 6	**kcd domain-join username** *<user>* **password** *<pass>* user — 不对应特定管理用户，只是具有在 Windows 域控制器上添加设备的服务级别权限的用户。 pass — 密码不对应特定密码，只是具有在 Windows 域控制器上添加设备的服务级别密码权限的用户。	检查是否存在 KCD 服务器并启动域加入进程。 Active Directory 用户名和密码只用于 EXEC 模式下并且不保存在配置中。 **注**　首次加入需要具备管理权限。域控制器上具有服务级别权限的用户不会获得访问权限。
步骤 7	kcd domain-leave	验证 KCD 服务器命令是否具有有效的域加入状态，然后发起离开域。

显示 KCD 状态信息

要显示域控制器信息和域加入状态，请执行本步骤。

	命令	用途
步骤 8	**show webvpn kcd** **示例：** ASA# show webvpn kcd KCD-Server Name: DC User : user1 Password : **** KCD State : Joined	显示域控制器信息和域加入状态。

显示缓存的 Kerberos 票证

如要显示 ASA 上缓存的所有 Kerberos 票证，请输入以下命令：

	命令	用途
步骤 9	**show aaa kerberos**	显示 ASA 上缓存的所有 Kerberos 票证。
步骤 10	**show aaa kerberos [username** ***user*** **| host** ***ip*** **|** ***hostname***] **示例：** ASA# **show aaa kerberos** Default Principal Valid Starting Expires Service Principal asa@example.COM 06/29/10 18:33:00 06/30/10 18:33:00 krbtgt/example.COM@example.COM kcduser@example.COM06/29/10 17:33:00 06/30/10 17:33:00 asa$/example.COM@example.COM kcduser@example.COM06/29/10 17:33:00 06/30/10 17:33:00 http/owa.example.com@example.COM ASA# show aaa kerberos username kcduser Default Principal Valid Starting Expires Service Principal kcduser@example.COM06/29/10 17:33:00 06/30/10 17:33:00 asa$/example.COM@example.COM kcduser@example.COM06/29/10 17:33:00 06/30/10 17:33:00 http/owa.example.com@example.COM ASA# show aaa kerberos host owa.example.com Default Principal Valid Starting Expires Service Principal kcduser@example.COM10-6-2910-6-30 17:33:00 http/owa.example.com@example.COM ASA# show aaa kerberos username kcduser Default Principal Valid Starting Expires Service Principal kcduser@example.COM06/29/10 17:33:00 06/30/10 17:33:00 asa$/example.COM@example.COM kcduser@example.COM06/29/10 17:33:00 06/30/10 17:33:00 http/owa.example.com@example.COM ASA# show aaa kerberos host owa.example.com Default Principal Valid Starting Expires Service Principal kcduser@example.COM10-6-29 10-6-30 17:33:00 http/owa.example.com@example.COM	• user — 用于查看特定用户的 Kerberos 票证 • hostname — 用于查看授予特定主机的 Kerberos 票证

清除缓存的 Kerberos 票证

要清除 ASA 上的所有 Kerberos 票证信息，请执行这些步骤。

	命令	用途
步骤 11	**clear aaa kerberos**	清除 ASA 上的所有 Kerberos 票证信息。
步骤 12	**clear aaa kerberos [username** *user* **| host** *ip* **|** *hostname***]**	• *user* — 用于清除特定用户的 Kerberos 票证 • *hostname* — 用于清除特定主机的 Kerberos 票证

限制

为使用 Kerberos 约束委派 (KCD) 的应用创建书签时，请勿选中 Enable Smart Tunnel。

配置应用配置文件自定义框架

无客户端 SSL VPN 包含一个 Application Profile Customization Framework (APCF) 选项，其允许 ASA 处理非标准应用和网络资源，以便通过 SSL VPN 连接正确显示它们。APCF 配置文件包含为特定应用指定何时 （之前、之后）、在何处 （报头、正文、请求、响应）转换什么内容 （数据）的脚本。脚本在 XML 中并使用 sed （数据流编辑器）语法转换字符串 / 文本。

您可以同时在 ASA 上配置和运行多个 APCF 配置文件。在 APCF 配置文件脚本中，可应用多个 APCF 规则。 ASA 根据配置历史记录首先处理最早的规则，接下来处理下一个最早的规则。

您可以将 APCF 配置文件存储在 ASA 闪存上，或者存储在 HTTP、 HTTPS 或 TFTP 服务器上。

限制

我们建议您只有在思科人员的帮助下方可配置 APCF 配置文件。

管理 APCF 数据包

详细步骤

	命令	用途
步骤 1	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 2	**apcf** **示例：** hostname(config)# **webvpn** hostname(config-webvpn)# **apcf flash:/apcf/apcf1.xml** hostname(config)# **webvpn** hostname(config-webvpn)# **apcf** **https://myserver:1440/apcf/apcf2.xml**	确定并找到要加载到 ASA 上的 APCF 配置文件。 显示如何启用位于闪存上的 APCF 配置文件 apcf1.xml。 显示如何启用位于 HTTPS 服务器 myserver 端口 1440 上的 APCF 配置文件 apcf2.xml，其中路径为 /apcf。

APCF 语法

APCF 配置文件采用 XML 格式和 sed 脚本语法，同时采用表 15-1 中的 XML 标签。

准则

APCF 配置文件使用错误可能导致性能下降和出现内容呈现意外。在大多数情况下，思科工程部供应 APCF 配置文件来解决特定应用呈现问题。

表 15-1　APCF XML 标签

标签	使用
<APCF>...</APCF>	打开任何 APCF XML 文件的强制性根元素。
<version>1.0</version>	指定 APCF 实施版本的强制性标签。目前唯一的版本是 1.0。
<application>...</application>	包围 XML 说明的正文的强制性标签。
<id> 文本 </id>	描述这个特定 APCF 功能的强制性标签。
<apcf-entities>...</apcf-entities>	包围一个或多个 APCF 实体的强制性标签。
<js-object>…</js-object> <html-object>…</html-object> <process-request-header>...</process-request-header> <process-response-header>...</process-response-header> <preprocess-response-body>...</preprocess-response-body> <postprocess-response-body>...</postprocess-response-body>	这些标签之一指定内容的类型或应该发生 APCF 处理的阶段。
<conditions>… </conditions>	指定处理标准的处理前 / 后标签的子元素，例如： • http-version （例如 1.1、 1.0、 0.9） • http-method （get、 put、 post、 webdav） • http-scheme （“http/”、“https/”、其他） • server-regexp regular expression containing ("a".."z" | "A".."Z" | "0".."9" | ".-_*[]?") • server-fnmatch （正则表达式，包含 ("a".."z" | "A".."Z" | "0".."9" | ".-_*[]?+()\{},"）， • user-agent-regexp • user-agent-fnmatch • request-uri-regexp • request-uri-fnmatch • 如果存在不止一个条件标签， ASA 将对所有标签执行逻辑 AND 运算。

表 15-1　APCF XML 标签（续）

标签	使用
<action> … </action>	包围在特定条件下对内容执行的一项或多项操作；您可以使用以下标签来定义这些操作（如下所示）： • <do> • <sed-script> • <rewrite-header> • <add-header> • <delete-header>
<do>…</do>	用于定义一个以下操作的操作标签子元素： • <no-rewrite/> — 请勿改变从远程服务器接收的内容。 • <no-toolbar/> — 请勿插入工具栏。 • <no-gzip/> — 请勿压缩内容。 • <force-cache/> — 保留原始缓存说明。 • <force-no-cache/> — 使对象不可缓存。 • < downgrade-http-version-on-backend> — 向远程服务器发送请求时使用 HTTP/1.0。
<sed-script> 文本 </sed-script>	用于更改基于文本的对象内容的操作标签子元素。文本必须是有效的 Sed 脚本。<sed-script> 适用于之前定义的 <conditions> 标签。
<rewrite-header></rewrite-header>	操作标签的子元素。更改如下所示子元素 <header> 标签中指定的 HTTP 报头的值。
<add-header></add-header>	用于添加在如下所示子元素 <header> 标签中指定的新 HTTP 报头的操作标签的子元素。
<delete-header></delete-header>	用于删除如下所示子元素 <header> 标签指定的 HTTP 报头的操作标签子元素。
<header></header>	指定要重写、添加或删除的名称 HTTP 报头。例如，以下标签将更改名为 Connection 的 HTTP 报头的值： <rewrite-header> <header>Connection</header> <value>close</value> </rewrite-header>

APCF 的配置示例

示例：

```
<APCF>
<version>1.0</version>
<application>
  <id>Do not compress content from example.com</id>
  <apcf-entities>
      <process-request-header>
         <conditions>
           <server-fnmatch>*.example.com</server-fnmatch>
         </conditions>
           <action>
```

```
            <do><no-gzip/></do>
          </action>
      </process-request-header>
  </apcf-entities>
</application>
</APCF>
```

示例：

```
<APCF>
<version>1.0</version>
<application>
 <id>Change MIME type for all .xyz objects</id>
 <apcf-entities>
      <process-response-header>
        <conditions>
            <request-uri-fnmatch>*.xyz</request-uri-fnmatch>
        </conditions>
         <action>
           <rewrite-header>
                <header>Content-Type</header>
                <value>text/html</value>
           </rewrite-header>
         </action>
      </process-response-header>
 </apcf-entities>
</application>
</APCF>
```

编码

通过编码，您可查看或指定无客户端 SSL VPN 门户页面的字符编码。

字符编码，又称为“字符代码”和“字符集”，是指使用字符来表示数据对原始数据进行配对（例如 0s 和 1s）。语言决定着要使用的字符编码方法。有些语言使用单一方法，有些语言则不是的。通常，地理区域决定着浏览器使用的默认编码方法，但是远程用户可以进行更改。浏览器也可检测页面上指定的编码，并相应地呈现文档。

编码属性允许指定在门户页面上使用的字符编码方法的值，从而确保正确呈现此页面，无论用户是在什么区域使用该浏览器，也无论对浏览器进行了任何更改。

默认情况下， ASA 将对来自通用互联网文件系统 (CIFS) 服务器的页面应用 “Global Encoding Type”。在正确呈现文件名或目录路径以及页面方面遇到问题时，在全局使用 “Global Encoding Type”属性并且对个别页面使用表格中显示的文件编码特例，将 CIFS 服务器映射为对应的字符编码，提供对 CISF 页面的正确处理和显示。

详细步骤

步骤 1　Global Encoding Type 决定着所有无客户端 SSL VPN 门户页面继承的字符编码，表中列出来自 CIFS 服务器的字符编码除外。您可以键入字符串或从下拉列表中选择以下选项之一，此下拉列表包含大多数常用值，如下所示：

- big5
- gb2312

- ibm-850
- iso-8859-1
- shift_jis

注　如果使用的是日文 Shift_jis 字符编码，请在关联的 Select Page Font 窗格的 Font Family 区域点击 **Do Not Specify** 以删除该字体系列。

- unicode
- windows-1252
- none

注　如果您点击 **none** 或指定无客户端 SSL VPN 会话上的浏览器不支持的值，它将使用自己的默认编码。

您可以键入最多包含 40 个字符并且等于 http://www.iana.org/assignments/character-sets 中确定的一个有效字符集的字符串。您可以使用该页列出的字符集的名称或别名。字符串不区分大小写。当保存 ASA 配置时，命令解释程序会将大写转换为小写。

步骤 2　输入编码要求与 “Global Encoding Type”属性设置不同的 CIFS 服务器的名称或 IP 地址。 ASA 将保留您指定的大小写，不过，它在将名称与服务器匹配时将忽略大小写。

步骤 3　选择 CIFS 服务器应该为无客户端 SSL VPN 门户页面提供的字符编码。您可以键入字符串或从下拉列表中选择以下选项之一，此下拉列表只包含大多数常用值，如下所示：

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis

注　如果使用的是日文 Shift_jis 字符编码，请在关联的 Select Page Font 窗格的 Font Family 区域点击 **Do Not Specify** 以删除该字体系列。

- unicode
- windows-1252
- none

如果您点击 **none** 或指定无客户端 SSL VPN 会话上的浏览器不支持的值，它将使用自己的默认编码。

您可以键入最多包含 40 个字符并且等于 http://www.iana.org/assignments/character-sets 中确定的一个有效字符集的字符串。您可以使用该页列出的字符集的名称或别名。字符串不区分大小写。当保存 ASA 配置时，命令解释程序会将大写转换为小写。

在无客户端 SSL VPN 上使用邮件

无客户端 SSL VPN 支持多种邮件访问方式。本节包括以下方法：

- 配置邮件代理
- 配置网络邮件：MS Outlook Web App

配置邮件代理

无客户端 SSL VPN 支持 IMAP、 POP3 和 SMTP 邮件代理。以下属性在全局适用于邮件代理用户。

限制

MS Outlook、 MS Outlook Express 和 Eudora 等邮件客户端无法访问证书存储。

详细步骤

	命令	用途
步骤 1	**accounting-server-group**	指定用于邮件代理的以前配置的记帐服务器。
步骤 2	**身份验证**	指定邮件代理用户的身份验证方法。默认值如下： • IMAP：邮件主机 （必填） • POP3 邮件主机 （必填） • SMTP：AAA
步骤 3	**authentication-server-group**	指定用于邮件代理的以前配置的身份验证服务器。默认值为 LOCAL。
步骤 4	**authorization-server-group**	指定用于无客户端 SSL VPN 的以前配置的授权服务器。
步骤 5	**authorization-required**	要求用户成功授权后才能连接。默认设置为关闭。
步骤 6	**authorization-dn-attributes**	确定用做授权用户名的对等证书的 DN。默认设置如下： • 主要属性：CN • 辅助属性：OU
步骤 7	**default-group-policy**	指定要使用的组策略的名称。默认值为 DfltGrpPolicy。
步骤 8	**enable**	启用指定接口上的邮件代理。默认设置为关闭。
步骤 9	**name-separator**	定义邮件和 VPN 用户名与密码之间的分隔符。默认为冒号 (:)。
步骤 10	**outstanding**	配置未完成的未经身份验证的会话的最大数量。默认值为 20。

	命令	用途
步骤 11	**port**	设置邮件代理侦听的端口。默认如下： • IMAP：143 • POP3：110 • SMTP：25
步骤 12	**server**	指定默认邮件服务器。
步骤 13	**server-separator**	定义在邮件和服务器名称之间的分隔符。默认为 @。

配置网络邮件：MS Outlook Web App

ASA 支持 Microsoft Outlook Web App 对 Exchange Server 2010 以及 Microsoft Outlook Web Access 对 Exchange Server 2007、 2003 和 2000。

详细步骤

步骤 1　在地址字段输入邮件服务的 URL 或点击无客户端 SSL VPN 会话中的关联书签。

步骤 2　系统提示时，按照*域**用户名*的格式输入邮件服务器用户名。

步骤 3　输入邮件密码。

第 16 章 策略组

2014 年 4 月 14 日

为访问资源创建和应用无客户端 SSL VPN 策略

为无客户端 SSL VPN 创建和应用管理访问内部服务器上资源的策略包括以下任务：

- 向组策略分配用户

向组策略分配用户

向组策略分配用户可以通过允许您将策略应用于很多用户而简化配置。您可以使用 ASA 上的内部身份验证服务器或外部 RADIUS 或 LDAP 服务器向组策略分配用户。有关利用组策略简化配置的方法的详细说明，请参阅第 4 章 “连接配置文件、组策略和用户”。

为无客户端 SSL VPN 配置连接配置文件属性

表 16-1 提供了专用于无客户端 SSL VPN 的连接配置文件属性列表。除了这些属性之外，您还可以配置所有 VPN 连接共用的通用连接配置文件属性。有关配置连接配置文件的分步信息，请参阅第 4 章 “连接配置文件、组策略和用户”。

注 在较早版本中，“连接配置文件”被称为 “隧道组”。您要使用 **tunnel-group** 命令配置连接配置文件。本章经常互换使用这两个术语。

表 16-1 无客户端 SSL VPN 的连接配置文件属性

命令	功能
身份验证	设置身份验证方法。
`customization`	确定要应用的以前定义的自定义名称。
`exit`	退出隧道组无客户端 SSL VPN 属性配置模式。
`nbns-server`	确定要用于 CIFS 名称解析的 NetBIOS 名称服务服务器 (nbns-server) 的名称。
`group-alias`	指定服务器可以用于引用连接配置文件的备用名称。
`group-url`	确定一个或多个组 URL。如果您使用此属性建立 URL，当用户使用这些 URL 访问时，将自动选择此组。

表 16-1　无客户端 SSL VPN 的连接配置文件属性 （续）

命令	功能
dns-group	确定指定 DNS 服务器名称、域名、名称服务器、重试次数和超时值的 DNS 服务器组。
help	为隧道组配置命令提供帮助。
hic-fail-group-policy	如果您使用思科安全桌面管理器将 Group-Based Policy 属性设置为 “Use Failure Group-Policy” 或 “Use Success Group-Policy, if criteria match”，则指定 VPN 功能策略。
no	删除属性值对。
override-svc-download	覆盖为向远程用户下载 AnyConnect VPN 客户端配置的下载组策略或用户名属性。
pre-fill-username	在此隧道组上配置用户名 - 证书绑定。
proxy-auth	确定此隧道组作为特定代理身份验证隧道组。
radius-reject-message	身份验证被拒绝时，启用在登录屏幕上显示 RADIUS 拒绝消息。
secondary-pre-fill-username	在此隧道组上配置二次用户名 - 证书绑定。
without-csd	关闭隧道组的 CSD。

为无客户端 SSL VPN 配置组策略和用户属性

表 16-2 提供了无客户端 SSL VPN 组策略和用户属性列表。有关配置组策略、用户属性的逐步说明，请参阅 *《思科 ASA 系列 VPN CLI 配置指南》* 中的 “配置组策略和配置各个用户的属性” 或 “连接配置文件、组策略和用户”。

表 16-2　无客户端 SSL VPN 的组策略和用户属性

命令	功能
activex-relay	允许已建立无客户端 SSL VPN 会话的用户使用浏览器启动 Microsoft Office 应用。这些应用将使用此会话下载和上传 ActiveX。 ActiveX 中继一直有效，直到无客户端 SSL VPN 会话关闭。
auto-sign-on	设置自动登录的值，这样用户只需要输入一次无客户端 SSL VPN 连接的用户名和密码凭据。
customization	向组策略或用户分配自定义对象。
deny-message	指定向成功登录无客户端 SSL VPN，但是没有 VPN 权限的远程用户传输的消息。
file-browsing	启用文件服务器和共享的 CIFS 文件浏览。浏览要求使用 NBNS（Master Browser 或 WINS）。
file-entry	允许用户输入要访问的文件服务器名称。
filter	设置 webtype 访问列表的名称。
hidden-shares	控制 CIFS 文件的隐藏共享的可视性。
homepage	设置在登录时显示的网页的 URL。
html-content-filter	配置该组策略要从 HTML 过滤的内容和对象。
http-comp	配置压缩。

表 16-2　无客户端 SSL VPN 的组策略和用户属性 （续）

命令	功能
`http-proxy`	配置 ASA 使用外部代理服务器处理 HTTP 请求。 **注**　**http-proxy** 中不支持代理 NTLM 身份验证。只支持无身份验证的代理和基本身份验证。
`keep-alive-ignore`	设置更新会话计时器要忽略的最大对象大小。
`port-forward`	将无客户端 SSL VPN TCP 端口列表应用于转发。用户界面显示此列表中的应用。
`post-max-size`	设置要发布的最大对象大小。
`smart-tunnel`	配置要使用智能隧道的程序列表和多个智能隧道参数。
`sso-server`	设置 SSO 服务器的名称。
`storage-objects`	配置会话之间存储的数据的存储对象。
`svc`	配置 SSL VPN 客户端属性。
`unix-auth-gid`	设置 UNIX 组 ID。
`unix-auth-uid`	设置 UNIX 用户 ID。
`upload-max-size`	设置要上载的最大对象大小。
`url-entry`	控制用户输入任意 HTTP/HTTPS URL 的权限。
`url-list`	应用无客户端 SSL VPN 门户网页为最终用户访问显示的 URL 和服务器列表。
`user-storage`	配置存储会话之间的用户数据的位置。

配置智能隧道访问

下节将说明如何使用无客户端 SSL VPN 会话启用智能隧道访问，指定此访问提供的应用，并提供其使用说明。

配置智能隧道访问

要配置智能隧道访问，您要创建一份包含一个或多个可以执行智能隧道访问的智能隧道列表以及与此列表关联的终端操作系统。由于每个组策略或本地用户策略都支持一个智能隧道列表，您必须将要支持的基于非浏览器的应用归类到智能隧道列表中。创建此列表后，请将其分配给一个或多个组策略或本地用户策略。

以下节将介绍智能隧道以及如何配置智能隧道：

关于智能隧道

智能隧道是基于 TCP 的应用与专用站点之间的一种连接，其使用无客户端（基于浏览器的）SSL VPN 会话，以安全设备作为通道并以 ASA 作为代理服务器。您可以确定要授权智能隧道访问的应用并指定每个应用的本地路径。对于 Microsoft Windows 上运行的应用，您还可以要求匹配校验和的 SHA-1 哈希值，作为授权智能隧道访问的条件。

Lotus Sametime 和 Microsoft Outlook 是您可能要授权智能隧道访问的应用示例。

配置智能隧道需要执行以下步骤之一，具体取决于应用是客户端还是支持网络的应用：

- 创建客户端应用的一个或多个智能隧道列表，然后将列表分配给需要智能隧道访问的组策略或本地用户策略。
- 创建一个或多个书签列表条目来指定符合智能隧道访问条件、支持网络的应用的 URL，然后将列表分配给需要智能隧道访问的组策略或本地用户策略。

您还可以列出通过无客户端 SSL VPN 会话在智能隧道连接中自动提交登录凭据的支持网络的应用。

为什么选择智能隧道？

智能隧道访问让客户端基于 TCP 的应用可以使用基于浏览器的 VPN 连接访问服务。与插件和端口转发传统技术相比，它可给用户提供以下优势：

- 智能隧道性能比插件更好。
- 不同于端口转发，智能隧道不要求用户将本地应用连接至本地本地端口，简化了用户体验。
- 不同于端口转发，智能隧道不要求用户拥有管理员权限。

插件的优点在于它不要求在远程计算机上安装客户端应用。

先决条件

有关 ASA 9.0 版本智能隧道支持的平台和浏览器，请参阅*受支持的 VPN 平台、思科 ASA 系列*。

下列要求和限制适用于 Windows 上的智能隧道访问：

- 在 Windows 中必须在浏览器上启用 ActiveX 或 Oracle Java Runtime Environment (JRE) 4 更新 15 或更高版本 （推荐 JRE 6 或更高版本）。

  ActiveX 页面要求在关联组策略上输入 **activex-relay** 命令。如果这么做或将智能隧道列表分配给此策略，并且终端上的浏览器代理异常列表指定了一个代理，则用户必须向此列表添加“shutdown.webvpn.relay.”条目。
- 仅 Winsock 2、基于 TCP 的应用符合智能隧道访问条件。
- 仅适用于 Mac OS X，必须在浏览器上启用 Java Web Start。

限制

- 智能隧道仅支持放在运行 Microsoft Windows 的计算机和安全设备之间的代理。智能隧道使用 Internet Explorer 配置，其设置 Windows 中的全系统参数。此配置可能包括代理信息：
  - 如果 Windows 计算机需要代理才能访问 ASA，则客户端浏览器中必须有一个静态代理条目，并且要连接的主机必须在客户端的代理异常列表上。
  - 如果 Windows 计算机不需要代理就能访问 ASA，但是，需要代理才能访问主机应用，则 ASA 必须在客户端的代理异常列表上。

代理系统可以由静态代理条目的客户端配置或自动配置定义，或者由 PAC 文件定义。目前智能隧道仅支持静态代理配置。

- 智能隧道不支持 Kerberos 约束委派 (KCD)。
- 对于 Windows，要向从命令提示符启动的应用添加智能隧道访问，您必须在智能隧道列表一个条目的 Process Name 中指定 “cmd.exe”，然后在另一个条目中指定指向该应用本身的路径，因为 “cmd.exe”是该应用的父级。
- 对于基于 HTTP 的远程访问，某些子网可能会阻止用户访问 VPN 网关。要解决此问题，请在 ASA 前面放一个代理，路由网络和最终用户之间的流量。该代理必须支持此连接方法。对于需要身份验证的代理，智能隧道仅支持基本摘要式身份验证类型。
- 智能隧道启动时，默认情况下，如果浏览器进程相同， ASA 会将所有浏览器流量传递通过 VPN 会话。只有在应用全隧道策略 （默认配置）的情况下， ASA 才会也这么做。如果用户启动浏览器进程的另一个实例，它会将所有流量传递通过 VPN 会话。如果浏览器进程相同，但安全设备不提供对 URL 的访问，用户将无法打开它。作为应急方案，请分配不属于全隧道的隧道策略。
- 状态故障转移不保留智能隧道连接。出现故障转移后，用户必须重新连接。
- Mac 版本的智能隧道不支持 POST 书签、基于表单的自动登录或 POST 宏替换。
- 对于 Mac OS X 用户，只有从门户页面启动的那些应用才可以建立智能隧道连接。此要求包括对 Firefox 的智能隧道支持。在首次使用智能隧道期间使用 Firefox 启动 Firefox 的另一个实例要求使用名称为 csco_st 的用户配置文件。如果没有此用户配置文件，会话将提示用户创建一个此配置文件。
- 在 Mac OS X 中，使用与 SSL 库动态链接的 TCP 的应用可通过智能隧道运行。
- 智能隧道在 Mac OS X 上不提供以下支持：
  - 代理服务。
  - 自动登录。
  - 使用两层名称空间的应用。
  - 基于控制台的应用，如 Telnet、 SSH 和 cURL。
  - 使用 dlopen 或 dlsym 来查找 libsocket 调用的应用。
  - 静态链接的应用查找 libsocket 调用。
- Mac OS X 需要指定进程的完整路径并区分大小写。为避免指定每个用户名的路径，请在部分路径前面插入波形符 (~) （例如 ~/bin/vnc）。

添加符合智能隧道访问条件的应用

每个 ASA 的无客户端 SSL VPN 配置都支持 *智能隧道列表*，每个列表都会确定一个或多个符合智能隧道访问条件的应用。由于每个组策略或用户名都只支持一个智能隧道列表，您必须将每组要支持的应用分别归类为一个智能隧道列表。

有关智能隧道列表

对于每个组策略和用户名，可以配置无客户端 SSL VPN 执行以下任一操作：

- 在用户登录时自动启动智能隧道访问。
- 在用户登录时启动智能隧道访问，但是要求用户手动启动，即使用无客户端 SSL VPN 门户页面上的 **Application Access > Start Smart Tunnels** 按钮。

限制

对于每个组策略和用户名，智能隧道登录选项是互相排斥的。只能使用一个。

详细步骤

以下智能隧道命令可用于每个组策略和用户名。每个组策略和用户名的配置每次都只支持这其中一个命令，因此，当您输入一个命令时， ASA 会将当前的组策略或用户名中现有的命令替换为此新命令，对于上一个命令，只是将组策略或用户名中已经存在的 **smart-tunnel** 命令删除。

	命令	用途
步骤 1	**smart-tunnel auto-start** *list* 或 **smart-tunnel enable** *list* 或 **smart-tunnel disable** 或 **no smart-tunnel [auto-start list | enable list | disable]**	在用户登录时自动启动智能隧道访问。 在用户登录时启动智能隧道访问，但是要求用户手动启动智能隧道访问，即使用无客户端 SSL VPN 门户页面上的 **Application Access > Start Smart Tunnels** 按钮。 阻止智能隧道访问。 从组策略或用户名配置中取消 **smart-tunnel** 命令，它将从默认组策略继承 **[no] smart-tunnel** 命令。在 **no smart-tunnel** 命令后面的关键字是可选的，但是它们可以限制取消指定的 **smart-tunnel** 命令。
步骤 2	有关必要选项，请参阅自动智能隧道访问。	

配置和应用智能隧道策略

智能隧道策略要求为每个组策略 / 用户名进行配置。每个组策略 / 用户名都引用一个全局配置的网络列表。智能隧道打开时，您可以使用以下 2 个 CLI 允许隧道外的流量流过：其中一个配置网络 （一组主机），另一个使用指定的智能隧道网络对用户执行策略。以下命令将创建一个用于配置智能隧道策略的主机列表：

详细步骤

	命令	用途
步骤 1	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 2	**[no] smart-tunnel network** *network name* **ip** *ip netmask*	创建一个用于配置智能隧道策略的主机列表。*network name* 是要应用于隧道策略的名称。 *ip* 是网络的 IP 地址。 *netmask* 是网络的网络掩码。
步骤 3	**[no] smart-tunnel network** *network name* **host** *host mask*	确定主机名掩码，例如 *.cisco.com。
步骤 4	**[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified}** *network name* **| tunnelall]** 或 **[no] smart-tunnel tunnel-policy {excludespecified | tunnelspecified}** *network* **name | tunnelall]**	将智能隧道策略应用于特定组或用户策略。*network name* 是要用隧道访问的网络的列表。*tunnelall* 设置全部进行隧道访问 （加密）。*tunnelspecified* 只对按照网络名称指定的网络进行隧道访问。 *excludespecified* 只对网络名称指定网络之外的网络进行隧道访问。

配置和应用智能隧道策略

与 SSL VPN 客户端的分离隧道配置一样，智能隧道策略是按组策略 / 用户名配置的。每个组策略 / 用户名都引用一个全局配置的网络列表：

命令	用途
[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified} *network name* **| tunnelall]** 或 **[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified}** *network name* **| tunnelall]**	引用一个全局配置的网络列表。 *network name* 是要用隧道访问的网络的列表。 *tunnelall* 设置全部进行隧道访问 （加密）。 tunnelspecified 只对按照网络名称指定的网络进行隧道访问。 excludespecified 只对网络名称指定网络之外的网络进行隧道访问。
ciscoasa(config-webvpn)# [no] smart-tunnel network *network name* **ip** *ip netmask* **ciscoasa(config-webvpn)# [no] smart-tunnel network** *network name* **host** *host mask*	将隧道策略应用于组策略 / 用户策略。一个命令指定主机，另一个命令指定网络 IP ；只能使用一个。 *network name* — 要应用于隧道策略的网络的名称 *ip address* — 网络的 IP 地址 *netmask* — 网络的网络掩码 *host mask* — 主机名掩码，例如 *.cisco.com
示例： ciscoasa(config-webvpn)# **smart-tunnel network inventory ip 10.5.2.2** ciscoasa(config-webvpn)# **smart-tunnel network inventory host www.example.com**	当供应商希望让合作伙伴无需首先进入无客户端门户即可对内部库存服务器页面进行无客户端访问时，智能隧道策略配置是一个很好的选择。创建只包含一个主机的隧道策略 （假设库存页面托管于 www.example.com (10.5.2.2) 上，并且您想要为主机配置 IP 地址和名称）。
ciscoasa(config-group-webvpn)# **smart-tunnel tunnel-policy tunnelspecified inventory**	将隧道指定的隧道策略应用于合作伙伴的组策略。
（可选） ciscoasa(config-group-webvpn)# **homepage value http://www.example.com** ciscoasa(config-group-webvpn)# h**omepage use-smart-tunnel**	指定组策略主页并在此主页上启用智能隧道。无需写入脚本或上载任何内容，管理员可以指定通过智能隧道连接哪个主页。
（可选） ciscoasa(config-webvpn)# **smart-tunnel notification-icon**	因为在启用智能隧道的情况下由浏览器发起的所有进程都具有隧道访问权限，所以默认情况下，没有必要配置智能隧道应用。但是，因为门户不可见，您可能想要启用注销通知图标。

创建智能隧道自动登录服务器列表

命令	用途
webvpn	切换至无客户端 SSL VPN 配置模式。
smart-tunnel auto-sign-on *list* [*use-domain*] [**realm** *realm-string*] [**port** *port-num*]{**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}	用于将每个服务器添加到服务器列表上 • *list* — 给远程服务器的列表命名。如果此名称包含空格，则将此名称放在引号内。此字符串最多可以包含 64 个字符。如果配置中没有此列表，则 ASA 将创建此列表。否则，它会向此列表添加条目。指定一个可帮助您区分的名称。 • use-domain （可选） — 如果身份验证需要，则向用户名中添加 Windows 域。如果您输入此关键字，请确保在将智能隧道列表分配到一个或多个组策略或用户名时指定域名。 • *realm* — 为身份验证配置领域。领域与网站的受保护区域关联，并且在身份验证期间在身份验证提示中或 HTTP 报头中回传至浏览器。配置了自动登录并且指定了领域字符串之后，用户可以配置网络应用 （例如 Outlook Web Access）的领域字符串，然后无需登录即可访问网络应用 • *port* — 指定哪个端口执行自动登录。对于 Firefox，如果没有指定端口号，则在 HTTP 和 HTTPS 上执行自动登录，分别用默认端口号 80 和 443 访问。 • *ip — 按照服务器 IP 地址和网络掩码指定服务器*。 • *ip-address*[*netmask*] — 确定要执行自动身份验证的主机的子网。 • *host* — 按照服务器主机名或通配符掩码指定服务器。使用此选项避免配置出现 IP 地址动态变化。 • *hostname-mask* — 指定执行自动身份验证的主机名或通配符掩码。
（可选） [**no**] **smart-tunnel auto-sign-on** *list* [**use-domain**] [**realm** *realm-string*] [**port** *port-num*] {**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}	按照在 ASA 配置中的显示指定列表和 IP 地址或主机名，从服务器列表中删除某个条目。
show running-config webvpn smart-tunnel	显示智能隧道自动登录列表条目。
config-webvpn	切换至 config-webvpn 配置模式。
smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0	添加子网上的所有主机，并且如果身份验证需要，还可将 Windows 域添加到用户名中。

命令	用途
（可选） `no smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0`	从列表中删除该条目，并且如果删除的条目是列表中的唯一条目，则还将删除列表命名的 HR。
`no smart-tunnel auto-sign-on HR`	从 ASA 配置删除整个列表。
`smart-tunnel auto-sign-on intranet host *.example.com`	将域中的所有主机添加到名为 intranet 的智能隧道自动登录列表中。
`no smart-tunnel auto-sign-on intranet host *.example.com`	从列表中删除该条目。

配置智能隧道自动登录服务器列表后，您必须将其分配给组策略或本地用户策略才能使它激活，如下节所述。

下一步是将服务器添加到服务器列表中。

将服务器添加到智能隧道自动登录服务器列表中

以下步骤说明了如何将服务器添加到要在智能隧道连接中提供自动登录的服务器列表中以及如何将该列表分配给组策略或本地用户。

先决条件

首先，您必须使用 **smart-tunnel auto-sign-on** *list* 命令创建服务器列表。您只能向组策略或用户名分配一个列表。

限制

- 智能隧道自动登录功能只支持使用 Internet Explorer 和 Firefox 进行 HTTP 和 HTTPS 通信的应用。
- Firefox 要求管理员使用完全匹配的主机名或 IP 地址指定主机 （而不能使用带有通配符的主机掩码，使用 IP 地址的子网或网络掩码）。例如，在 Firefox 中，您不能输入 *.cisco.com 并期望自动登录主机 email.cisco.com。

详细步骤

要在无客户端 （基于浏览器的） SSL VPN 会话中启用智能隧道自动登录，请使用以下命令：

	命令	用途
步骤 1	`webvpn`	切换至无客户端 SSL VPN 配置模式。

步骤 2	`group-policy webvpn`
	或
	`username webvpn`
		切换至组策略无客户端 SSL VPN 配置模式。
		切换至用户名无客户端 SSL VPN 配置模式。

步骤 3	`smart-tunnel auto-sign-on enable`	启用智能隧道自动登录无客户端 SSL VPN 会话。

	命令	用途
步骤 4	（可选） **[no] smart-tunnel auto-sign-on enable** *list* **[domain** *domain*]	关闭智能隧道自动登录无客户端 SSL VPN 会话，从组策略或用户名中删除它，并使用默认值。 • *list* — ASA 无客户端 SSL VPN 配置中已经存在的智能隧道自动登录列表的名称。 • （可选）*domain* — 在身份验证期间要向用户名添加的域的名称。如果您输入域名，请在列表条目中输入 **use-domain** 关键字。
步骤 5	**show running-config webvpn smart-tunnel**	查看 SSL VPN 配置中的智能隧道自动登录列表条目。
步骤 6	**smart-tunnel auto-sign-on enable HR**	启用名为 HR 的智能隧道自动登录列表。
步骤 7	**smart-tunnel auto-sign-on enable HR domain CISCO**	启用名为 HR 的智能隧道自动登录列表并且在身份验证期间将名为 CISCO 的域添加到用户名中。
步骤 8	**（可选）** **no smart-tunnel auto-sign-on enable HR**	从组策略删除名为 HR 的智能隧道自动登录列表并且从默认组策略继承智能隧道自动登录列表命令。

自动智能隧道访问

如要在用户登录时自动启动智能隧道访问，请输入以下命令：

要求

对于 Mac OS X，您必须在门户的 Application Access 面板中点击应用的链接，无论是否配置了自动启动功能。

详细步骤

	命令	用途
步骤 1	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 2	**group-policy webvpn** 或 **username webvpn**	切换至组策略无客户端 SSL VPN 配置模式。 切换至用户名无客户端 SSL VPN 配置模式。
步骤 3	**smart-tunnel auto-start** *list* **示例：** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **smart-tunnel auto-start apps1**	在用户登录时自动启动智能隧道访问。*list* 是已经存在的智能隧道列表的名称。 将名为 apps1 的智能隧道列表分配给组策略。
步骤 4	**show running-config webvpn smart-tunnel**	显示 SSL VPN 配置中的智能隧道列表条目。
步骤 5	（可选） **no smart-tunnel**	从组策略或用户名中删除 **smart-tunnel** 命令并恢复默认设置。

启用和关闭智能隧道访问

默认情况下，智能隧道处于关闭状态。

详细步骤

	命令	用途
步骤 1	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 2	**group-policy webvpn** 或 **username webvpn**	切换至组策略无客户端 SSL VPN 配置模式。 切换至用户名无客户端 SSL VPN 配置模式。
步骤 3	**smart-tunnel [enable** *list* **| disable]** **示例：** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **smart-tunnel enable apps1**	启用智能隧道访问。*list* 是已经存在的智能隧道列表的名称。如果您输入上一表格的 **smart-tunnel auto-start list**，您无需手动启动智能隧道访问。 将名为 apps1 的智能隧道列表分配给组策略。
步骤 4	**show running-config webvpn smart-tunnel**	显示 SSL VPN 配置中的智能隧道列表条目。
步骤 5	（可选） **no smart-tunnel**	从组策略或本地用户策略删除 **smart-tunnel** 命令并恢复默认组策略。
步骤 6	（可选） **smart-tunnel disable**	关闭智能隧道访问。

配置智能隧道注销

本节介绍如何确保正确注销智能隧道。当所有浏览器窗口都已关闭时可以注销智能隧道，也可以右键单击通知图标并确认注销。

注　我们强烈建议使用门户上的注销按钮。此方法适合于无客户端 SSL VPN 和不管是否使用智能隧道都要注销的情况。只有在使用独立应用而不使用服务器的时候才可以使用通知图标。

当父进程终止时

这种做法要求所有浏览器都关闭才表示注销。目前智能隧道生命期与启动进程生命期关联。例如，如果您从 Internet Explorer 启动智能隧道，无 iexplore.exe 运行时智能隧道就会关闭。即使用户关闭了所有浏览器而不注销，智能隧道仍可确定 VPN 会话已经结束。

注　有些情况下，浏览器进程会延迟，那属于意外情况，并且严格地讲应该是错误导致的。此外，使用安全桌面时，即使用户在安全桌面中关闭所有浏览器，浏览器进程仍然可以在另一个桌面上运行。因此，在当前桌面中再也没有可见窗口时，智能隧道即宣布所有浏览器实例都已关闭。

详细步骤

	命令	用途
步骤 1	`[no] smart-tunnel notification-icon`	允许管理员在全局范围打开通知图标。此命令配置将注销属性和控制是否向用户显示用于注销的注销图标，否则就要通过关闭浏览器窗口触发注销。此命令还控制父进程终止时的注销，其将在通知图标打开或关闭时自动打开或关闭。 **notification-icon** 是指定何时使用此图标来注销的关键字。 **注**　默认情况下不使用此命令，在这种情况下将通过关闭所有浏览器窗口注销 SSL VPN 会话。 **注**　门户注销仍然有效并且不受影响。
步骤 2	`*.webvpn。`	当使用代理和添加到代理列表异常时，确保在您注销时智能隧道正确关闭，无论是否使用图标。

使用通知图标

您还可以选择关闭在父进程终止时注销，这样当您关闭浏览器时会话将继续。对于这个做法，您要使用系统托盘中的通知图标注销。此图标将一直显示，直到用户点击该图标注销。如果会话在用户注销之前到期，该图标仍继续显示，直到下一次尝试连接。您可能需要等待系统托盘中更新会话状态。

注　此图标是 SSL VPN 注销的备选方法。它不指示 VPN 会话状态。

配置内容转换

默认情况下， ASA 处理通过内容转换 / 重写引擎的所有无客户端 SSL VPN 流量，此引擎包括 JavaScript 和 Java 等高级元素，以便代理根据用户是从 SSL VPN 设备内部还是独立于此设备来访问应用，采用不同语义和访问控制规则的 HTTP 流量。

某些网络资源需要高度个性化的处理。以下节将介绍提供这类处理的功能：

- 为签发重写的 Java 内容配置证书
- 关闭内容重写
- 使用代理旁路

根据您的组织的要求和涉及的网络内容，您可以使用以下一种功能。

为签发重写的 Java 内容配置证书

通过 SSL VPN 转换的 Java 对象随后可以使用与信任点关联的 PKCS12 数字证书签发。

详细步骤

	命令	用途
步骤 1	**crypto ca import**	导入证书。
步骤 2	**ava-trustpoint** **示例：t** hostname(config)# **crypto ca import mytrustpoint pkcs12 mypassphrase** 输入 base 64 编码的 PKCS12。 以关键字 “quit”结束一行。 [PKCS12 data omitted] **quit** 重要信息：导入 PKCS12 操作成功完成。 hostname(config)# **webvpn** hostname(config)# **java-trustpoint mytrustpoint**	使用证书。 显示创建名为 mytrustpoint 的信任点以及将其分配给签发的 Java 对象。

关闭内容重写

您可能不想让某些应用和公共网站等网络资源进入 ASA。因此， ASA 允许您创建允许用户浏览某些网站和应用程序，而不通过 ASA 的重写规则。这类似于 IPSec VPN 连接中的分离隧道。

	命令	用途
步骤 1	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 2	**rewrite**	指定在无客户端 SSLN VPN 隧道外部访问的应用和资源。您可以多次使用此命令。
步骤 3	**disable**	与 **rewrite** 命令结合使用。规则序号很重要，因为安全设备将按照序号搜索重写规则，从最低序号开始，并应用匹配的第一个规则。

使用代理旁路

当应用和网络资源利用此功能提供的特殊内容重写效果更好时，您可以配置 ASA 使用代理旁路。代理旁路是对原始内容更改最少的一种内容重写备选方法。通常适用于自定义网络应用。

您可以多次使用 **proxy-bypass** 命令。您配置条目的顺序并不重要。接口和路径掩码或接口和端口将唯一标识代理旁路规则。

如果使用端口而不是路径掩码配置代理旁路，根据您的网络配置，您可能需要更改您的防火墙配置以允许这些端口访问 ASA。使用路径掩码可避免此限制。但是，请注意，路径掩码可能会改变，因此您可能需要使用多个 pathmask 语句来穷尽各种可能性。

路径是 URL 中 .com 或 .org 或其他类型域名之后的任何内容。例如，在 URL www.example.com/hrbenefits 中， *hrbenefits* 就是路径。同样，对于 URL www.example.com/hrinsurance， *hrinsurance* 就是路径。要为所有 hr 站点使用代理旁路，您可以通过使用 * 通配符避免多次使用此命令，如下所示：/hr*。

详细步骤

	命令	用途
步骤 1	`webvpn`	切换至无客户端 SSL VPN 配置模式。
步骤 2	`proxy-bypass`	配置代理旁路。

配置门户访问规则

此增强功能让客户可以配置全局无客户端 SSL VPN 访问策略以根据 HTTP 报头中的数据允许或拒绝无客户端 SSL VPN 会话。如果 ASA 拒绝无客户端 SSL VPN 会话，它将立即向终端返回错误代码。

ASA 在终端向 ASA 进行身份验证之前，评估此访问策略。因此，一旦访问被拒绝，终端的其他连接尝试消耗的 ASA 处理资源会更少。

先决条件

登录 ASA 并进入全局配置模式。在全局配置模式下， ASA 显示以下提示符：

```
hostname(config)#
```

详细步骤

	命令	用途
步骤 1	**webvpn** **示例：** `hostname(config)# webvpn`	进入无客户端 SSL VPN 配置模式。

步骤 2	**portal-access-rule** *priority* [{**permit** | **deny** [**code** *code*]} {**any** | **user-agent match** *string*}
	
	示例：
	`hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match *Thunderbird*`
	
	`hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match “*my agent*”`
		根据 HTTP 报头代码或 HTTP 报头中的字符串允许或拒绝创建无客户端 SSL VPN 会话。
		
		第二个示例显示了指定带空格的字符串的正确语法。在字符串前后加上通配符 (*)，然后将其放入引号内 (“ ”)。

优化无客户端 SSL VPN 性能

ASA 提供多种优化 SSL VPN 性能和功能的方法。性能改进包括缓存和压缩网络对象。功能调整包括对内容转换和**代理旁路**设置限制。 APCF 提供调整内容转换的另一种方法。以下节将说明这些功能：

- 配置缓存
- 配置内容转换

配置缓存

缓存可增强无客户端 SSL VPN 性能。它将经常重复使用的对象存储在系统缓存中，这会减少对内容执行重复重写和压缩的需要。它减少了无客户端 SSL VPN 和远程服务器之间的流量，结果让很多应用运行效率更高。

默认情况下会启用缓存。您可以在缓存模式下使用缓存命令自定义您的环境中的缓存运行方式。

无客户端 SSL VPN 远程用户

2013 年 9 月 13 日

此节适用于为最终用户设置无客户端 （基于浏览器的） SSL VPN 的系统管理员。本节总结了用户远程系统的配置要求和任务。此节还详细说明了要让用户开始使用无客户端 SSL VPN 需要向他们传递的信息。

注 我们假定，您已经为无客户端 SSL VPN 配置了 ASA。

需要用户名和密码

根据您的网络，在远程会话期间，可能需要登录以下任一项或所有项：计算机、互联网服务提供程序、无客户端 SSL VPN、邮件或文件服务器或企业应用。用户可能必须在许多不同情景下进行身份验证，这要求提供不同的信息，例如唯一用户名、密码或 PIN。确保用户具备所需的访问权限。

表 17-1 列出了无客户端 SSL VPN 用户可能需要知道的用户名和密码的类型。

表 17-1 要向无客户端 SSL VPN 用户提供的用户名和密码

登录用户名 / 密码类型	用途	输入时间
计算机	访问计算机	启动计算机
互联网服务提供商	访问互联网	连接互联网服务提供商
无客户端 SSL VPN	访问远程网络	启动无客户端 SSL VPN 会话
文件服务器	访问远程文件服务器	使用无客户端 SSL VPN 文件浏览功能访问远程文件服务器

表 17-1　要向无客户端 SSL VPN 用户提供的用户名和密码 （续）

登录用户名 / 密码类型	用途	输入时间
企业应用登录	访问受防火墙保护的内部服务器	使用无客户端 SSL VPN 网络浏览功能访问受保护的内部网站
邮件服务器	通过无客户端 SSL VPN 访问远程邮件服务器	发送或接收邮件信息

传达安全提示

建议用户始终从会话中注销。要注销无客户端 SSL VPN，请点击无客户端 SSL VPN 工具栏上的注销图标或关闭浏览器。

告知用户使用无客户端 SSL VPN 并不能保证与每个站点的通信都是安全的。无客户端 SSL VPN 将确保远程计算机或工作站与公司网络上的 ASA 之间数据传输的安全性。然后，如果用户访问非 HTTPS 网络资源 （位于互联网或内部网络上），从公司 ASA 到目标网络服务器之间的通信就不安全。

配置远程系统以使用无客户端 SSL VPN 功能

表 17-2 包括有关设置远程系统使用无客户端 SSL VPN 的下列信息：

- 启动无客户端 SSL VPN
- 使用无客户端 SSL VPN 浮动工具栏
- 网络浏览
- 网络扫描和文件管理
- 使用应用 （端口转发）
- 通过端口转发、网络访问或电子邮件代理使用邮件

表 17-2 也提供以下信息：

- 按功能列出的无客户端 SSL VPN 要求
- 无客户端 SSL VPN 支持的应用
- 客户端应用安装和配置要求
- 可能需要向最终用户提供的信息
- 对最终用户的提示和使用建议

很有可能的是，您对用户帐户的配置不同，每个无客户端 SSL VPN 用户可用的功能不同。表 17-2 按照用户活动组织信息，因此您可以跳过与不可用功能相关的信息。

表 17-2　　无客户端 SSL VPN 远程系统配置和最终用户要求

任务	远程系统或最终用户要求	规范或使用建议
启动无客户端 SSL VPN	连接到互联网	支持各种互联网连接，包括： • 家庭数字用户线、电缆或拨号 • 公共终端机 • 酒店联结线路 • 机场无线节点 • 网吧
	支持无客户端 SSL VPN 的浏览器	我们推荐适用于无客户端 SSL VPN 的以下浏览器。其他浏览器可能不完全支持无客户端 SSL VPN 功能。 在 Microsoft Windows 上： • Internet Explorer 8 • Firefox 8 在 Linux 上： • Firefox 8 在 Mac OS X 上： • Safari 5 • Firefox 8
	在浏览器上启用 Cookie	要通过端口转发访问应用，必须在浏览器上启用 Cookie。
	适用于无客户端 SSL VPN 的 URL	以下形式的一个 HTTPS 地址： https:// *地址* 其中*地址*是启用无客户端 SSL VPN 的 ASA（或负载平衡集群）的接口的 IP 地址或 DNS 主机名。例如：https://10.89.192.163 或 https://cisco.example.com。
	无客户端 SSL VPN 用户名和密码	
	[可选] 本地打印机	无客户端 SSL VPN 不支持从网络浏览器打印到网络打印机。不支持打印到本地打印机。

表 17-2　无客户端 SSL VPN 远程系统配置和最终用户要求 （续）

任务	远程系统或最终用户要求	规范或使用建议
在无客户端 SSL VPN 连接中使用浮动工具栏		浮动工具栏可简化无客户端 SSL VPN 的使用。此工具栏允许您输入 URL、浏览文件位置以及选择预配置的网络连接，而不会干扰主浏览器窗口。 如果将浏览器配置为阻止弹出窗口，则无法显示浮动工具栏。 浮动工具栏显示当前无客户端 SSL VPN 会话。如果点击 **Close** 按钮， ASA 会提示您关闭无客户端 SSL VPN 会话。 **提示**　要将文本粘贴到文本字段，请使用 **Ctrl-V**。（无客户端 SSL VPN 工具栏上不支持右键单击。）
网络浏览	受保护网站的用户名和密码	使用无客户端 SSL VPN 并不能保证与每个站点的通信都是安全的。请参阅 “传达安全提示”。
		使用无客户端 SSL VPN 进行网络浏览时，用户可能会体验到不同于以往的外观和感受。例如： • 无客户端 SSL VPN 标题栏显示在每个网页上方。 • 您可以通过以下方式访问网站： – 在无客户端 SSL VPN 主页 Enter Web Address 字段输入 URL。 – 点击无客户端 SSL VPN 主页上预配置的网站链接。 – 单击通过前两个方法之一访问的网页的链接。 此外，根据您配置特定帐户的方式，可能存在以下情况： • 某些网站会被拦截。 • 只有在无客户端 SSL VPN 主页上显示为链接的网站才可用。
网络扫描和文件管理	为共享远程访问配置的文件权限	仅共享文件夹和文件可通过无客户端 SSL VPN 进行访问。
	受保护的文件服务器的服务器名称和密码	-
	文件夹和文件所在的域、工作组和服务器名称	用户可能并不熟悉如何在您的组织网络中查找他们的文件。
	-	在复制过程中，请勿中断 **Copy File to Server** 命令或导航至其他屏幕。中断操作可能会导致在服务器上保存的文件不完整。

表 17-2　无客户端 SSL VPN 远程系统配置和最终用户要求 （续）

任务	远程系统或最终用户要求	规范或使用建议
使用应用 （称为端口转发或应用访问）	**注**　在 Mac OS X 上，仅 Safari 浏览器支持此功能。	
	注　由于此功能需要安装 Oracle Java Runtime Environment (JRE) 和配置本地客户端，并且因为这样做需要具备本地系统的管理员权限，因此用户在通过公共远程系统连接时可能无法使用应用。	
	⚠ **注意事项**　当用户结束使用应用时，始终应该通过点击 **Close** 图标关闭 Application Access 窗口。不正确关闭此窗口可能会导致无法访问 Application Access 或应用本身。	
	安装的客户端应用	-
	在浏览器上启用 Cookie	-
	管理员权限	如果您使用 DNS 名称来指定服务器，则必须具备计算机上的管理员访问权限，因为修改主机要求具有此权限。
	已安装 Oracle Java Runtime Environment (JRE) 1.4.x 和 1.5.x 版本 必须在浏览器上启用 JavaScript。默认情况下， JavaScript 已启用。	如果未安装 JRE，系统将显示弹出窗口，指导用户浏览至提供此 JRE 的站点。 极少数情况下，端口转发小程序将出现故障，显示 Java 异常错误。如果出现这种情况，请执行以下操作： 1. 清除浏览器缓存并关闭浏览器。 2. 确认计算机任务栏上没有任何 Java 图标。结束 Java 的所有实例。 3. 建立一个无客户端 SSL VPN 会话并启动端口转发 Java 小程序。
	必要时，要配置客户端应用。 **注**　Microsoft Outlook 客户端不需要执行此配置步骤。 所有非 Windows 客户端应用都要求此配置。 如要查看 Windows 是否要求执行此配置，请检查 Remote Server 字段的值。 • 如果 Remote Server 字段包含服务器主机名，则不需要配置客户端应用。 • 如果 Remote Server 字段包含 IP 地址，则必须配置客户端应用。	如要配置客户端应用，请使用服务器的本地映射 IP 地址和端口号。要查找此信息，请执行以下操作： 1. 在远程系统上启动无客户端 SSL VPN 并点击无客户端 SSL VPN 主页上的 Application Access 链接。系统将显示 Application Access 窗口。 2. 在 Name 列，找到要使用的服务器名称，然后确定其相应的客户端 IP 地址和端口号（在 Local 列）。 3. 使用该 IP 地址和端口号来配置客户端应用。配置步骤因各客户端应用而异。
	注　在通过无客户端 SSL VPN 运行的应用中点击 URL（例如邮件信息中的一个 URL）不会通过无客户端 SSL VPN 打开站点。如要通过无客户端 SSL VPN 打开站点，请剪切此 URL 并将其粘贴到 Enter (URL) Address 字段。	

表 17-2　无客户端 SSL VPN 远程系统配置和最终用户要求 （续）

任务	远程系统或最终用户要求	规范或使用建议
使用邮件（通过 Application Access）	满足 Application Access 的要求 （请参阅“使用应用”）	如要使用邮件，请从无客户端 SSL VPN 主页启动 Application Access。这样即可使用邮件客户端。
	注　如果在使用 IMAP 客户端时失去与邮件服务器之间的连接或者无法建立新的连接，请关闭 IMAP 应用并重新启动无客户端 SSL VPN。	
	其他邮件客户端	我们测试了 Microsoft Outlook Express 5.5 和 6.0 版本。 无客户端 SSL VPN 应该支持通过端口转发的其他 SMTPS、POP3S 或 IMAP4S 邮件程序，例如 Lotus Notes 和 Eudora，但我们未进行验证。
通过电子邮件代理使用邮件	已安装基于网络的邮件产品	支持的产品包括： • Outlook Web Access 为了获得最佳效果，请在 Internet Explorer 8.x 或更高版本或 Firefox 8.x 上使用 OWA。 • Lotus Notes 其他基于网络的邮件产品应该也可以使用，但我们未进行验证。
通过电子邮件代理使用邮件	已安装支持 SSL 的邮件应用 请勿将 ASA SSL 版本设置为仅 TLSv1。Outlook 和 Outlook Express 不支持 TLS。	支持的邮件应用： • Microsoft Outlook • Microsoft Outlook Express 5.5 和 6.0 版本 其他支持 SSL 的邮件客户端应该也可以使用，但我们未进行验证。
	已配置邮件应用	

捕获无客户端 SSL VPN 数据

CLI capture 命令允许您记录无法通过无客户端 SSL VPN 连接正常显示的网站的信息。此数据可帮助您的思科客户支持工程师对问题进行故障排除。以下节介绍了如何使用 capture 命令：

- 创建捕获文件
- 使用浏览器显示捕获数据

注　启用无客户端 SSL VPN 捕获会影响 ASA 的性能。在生成用于故障排除的捕获文件后，请务必关闭捕获功能。

创建捕获文件

详细步骤

步骤 1　如要启动无客户端 SSL VPN 捕获实用程序，请在特权 EXEC 模式中使用 **capture** 命令。

capture *capture-name* **type webvpn user** *csslvpn-username*

其中：

- *capture-name* 是您分配给捕获的名称，也是捕获文件名称的前缀。
- *csslvpn-username* 是要与捕获匹配的用户名。

捕获实用程序启动。

步骤 2　用户登录并开始了无客户端 SSL VPN 会话。捕获实用程序开始捕获数据包。

使用命令的 **no** 版本来停止捕获。

no capture *capture-name*

捕获实用程序将创建一个 *capture-name*.zip 文件，这个文件将用密码 **koleso** 加密。

步骤 3　将该 .zip 文件发送给思科或将其添加在思科技术支持中心服务请求中。

步骤 4　如要查看该 .zip 文件的内容，请使用密码 **koleso** 解压该文件。

以下示例创建名称为 *hr* 的捕获，它将把 user2 的无客户端 SSL VPN 流量捕获到文件中：

```
hostname# capture hr type webvpn user user2
WebVPN WebVPN capture started.
   capture name   hr
   user name      user2
hostname# no capture hr
```

使用浏览器显示捕获数据

详细步骤。

步骤 1　如要启动无客户端 SSL VPN 捕获实用程序，请在特权 EXEC 模式中使用 **capture** 命令。

capture *capture-name* **type webvpn user** *csslvpn-username*

其中：

- *capture-name* 是您分配给捕获的名称，也是捕获文件名称的前缀。
- *csslvpn-username* 是要与捕获匹配的用户名。

捕获实用程序启动。

步骤 2　用户登录并开始了无客户端 SSL VPN 会话。捕获实用程序开始捕获数据包。

使用命令的 **no** 版本来停止捕获。

步骤 3　打开浏览器并在地址栏输入：

https://*ASA 的 IP 地址或主机名***/webvpn_capture.html**

被捕获的内容以探查器的格式显示。

步骤 4　当您检查完捕获内容后，使用命令的 **no** 版本来停止捕获。

无客户端 SSL VPN 用户

2014 年 4 月 14 日

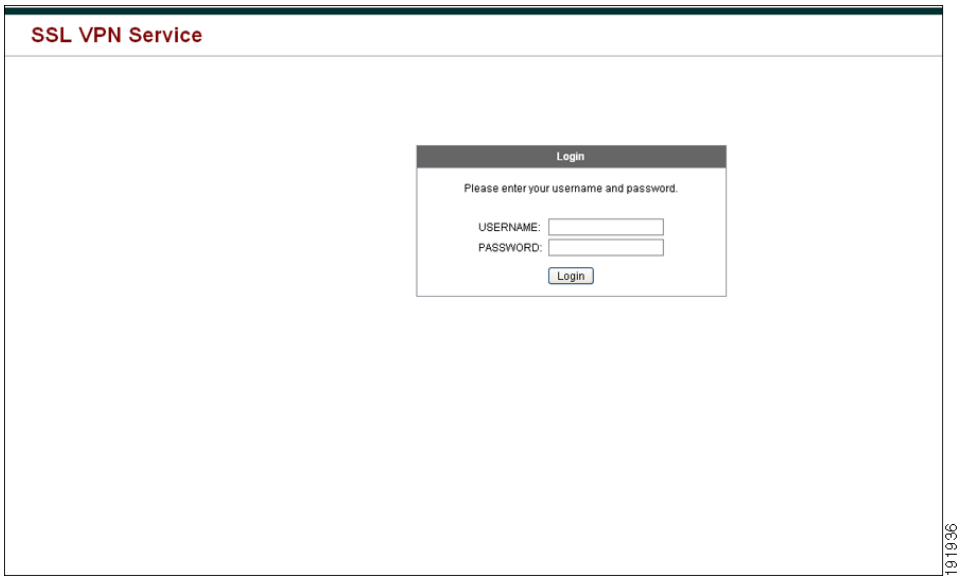
概述

本节向用户提供有关无客户端 SSL VPN 的使用入门的信息。包括下列主题：

定义最终用户界面

无客户端 SSL VPN 最终用户界面包括一系列 HTML 面板。用户按照 https:// *地址*的形式输入 ASA 接口的 IP 地址即可登录无客户端 SSL VPN。显示的第一个面板是登录屏幕 （图 18-1）。

图 18-1　　无客户端 SSL VPN 登录屏幕



查看无客户端 SSL VPN 主页

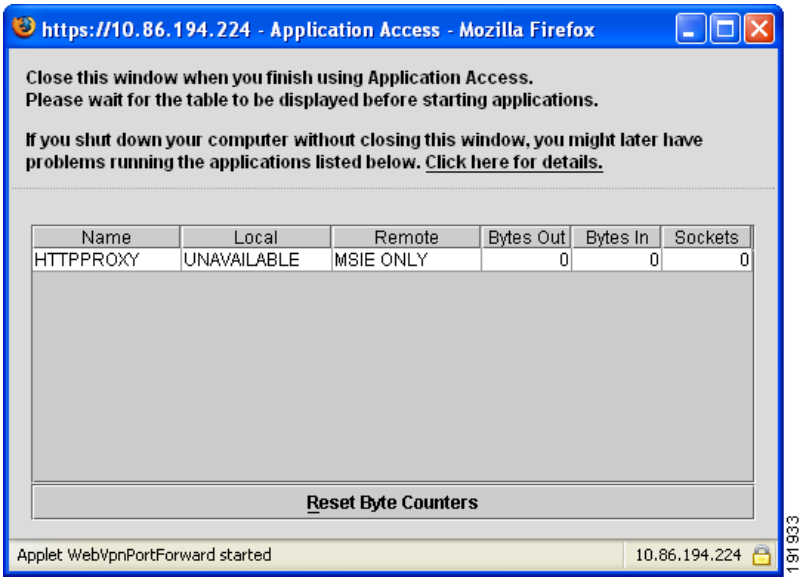
用户登录后，门户页面将会打开。

主页显示已配置的所有无客户端 SSL VPN 功能，其外观反映所选的徽标、文本和颜色。除了不能标识特定文件共享，此示例主页包括所有可用的无客户端 SSL VPN 功能。用户可以通过此主页浏览网络，输入 URL，访问特定网站，以及使用应用访问 （端口转发和智能隧道）来访问 TCP 应用。

查看无客户端 SSL VPN 应用访问面板

如要启动端口转发或智能隧道，用户可点击 Application Access 框中的 **Go** 按钮。 Application Access 窗口将会打开 （图 18-2）。

图 18-2　　无客户端 SSL VPN Application Access 窗口



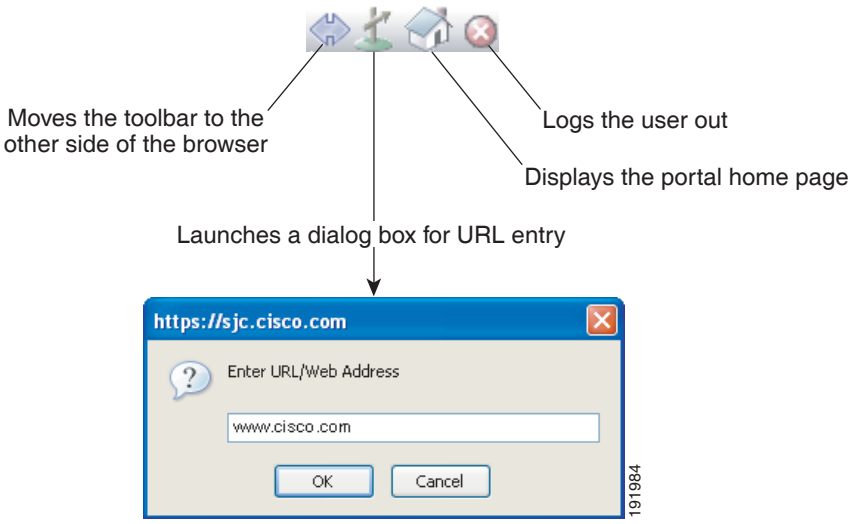
此窗口显示为此无客户端 SSL VPN 连接配置的 TCP 应用。如要在此面板打开的情况下使用某应用，用户可以按照正常方式启动该应用。

注　状态故障转移将不保留使用 Application Access 建立的会话。出现故障转移后，用户必须重新连接。

查看浮动工具栏

图 18-3 中显示的浮动工具栏显示当前无客户端 SSL VPN 会话。

图 18-3　　无客户端 SSL VPN 浮动工具栏



请注意浮动工具栏的以下特征：

- 此工具栏允许您输入 URL、浏览文件位置以及选择预配置的网络连接，而不会干扰主浏览器窗口。
- 如果将浏览器配置为阻止弹出窗口，则无法显示浮动工具栏。
- 如果关闭此工具栏， ASA 会提示您结束无客户端 SSL VPN 会话。

有关使用无客户端 SSL VPN 的详细信息，请参阅第 18-20 页上的表 18-2。

管理密码

如有需要，可以将 ASA 配置为会在最终用户的密码即将到期时向他们发出警告。

ASA 支持 RADIUS 和 LDAP 协议的密码管理。对于 LDAP，它仅支持“password-expire-in-days”选项。

可以为 IPsec 远程访问和 SSL VPN 隧道组配置密码管理。

配置密码管理时， ASA 会在远程用户登录时通知其当前密码即将到期或已到期。然后， ASA 允许用户更改密码。如果当前密码未到期，用户仍可使用该密码登录。

此命令对于支持此类通知的 AAA 服务器有效。

使用 LDAP 或支持 MS-CHAPv2 的任何 RADIUS 配置进行身份验证时，ASA 版本 7.1 及更高版本通常支持以下连接类型的密码管理：

- AnyConnect VPN 客户端
- IPsec VPN 客户端
- 无客户端 SSL VPN

RADIUS 服务器（例如，思科 ACS）可能会将身份验证请求以代理方式发送到另一个身份验证服务器。但是， ASA 仅与 RADIUS 服务器进行通信。

先决条件

- 本机 LDAP 需要 SSL 连接。在尝试执行 LDAP 密码管理之前，必须先启用基于 SSL 的 LDAP。默认情况下， LDAP 使用端口 636。
- 如果将 LDAP 目录服务器用于身份验证，Sun Java 系统目录服务器（原称为 SunONE 目录服务器）和 Microsoft Active Directory 支持密码管理。

  Sun — 在 ASA 上配置的用于访问 Sun 目录服务器的 DN 必须能够访问该服务器上的默认密码策略。我们建议将目录管理员或具有目录管理员权限的用户用作 DN。或者，可以在默认密码策略中创建 ACI。

  Microsoft — 要启用 Microsoft Active Directory 的密码管理，必须配置基于 SSL 的 LDAP。

  限制

- 支持 MSCHAP 的某些 RADIUS 服务器目前不支持 MSCHAPv2。此命令需要 MSCHAPv2，因此，请与供应商联系。
- Kerberos/Active Directory （Windows 密码）或 NT 4.0 域的任何连接类型都*不*支持密码管理。
- 对于 LDAP，市场上不同的 LDAP 服务器有专有的密码更改方法。目前，ASA 仅对 Microsoft Active Directory 和 Sun LDAP 服务器实施专有密码管理逻辑。
- 如果尚未配置 RADIUS 或 LDAP 身份验证， ASA 将忽略此命令。

详细步骤

注　**password - management** 命令不会更改密码有效天数，而是更改 ASA 提前多少天警告用户密码即将到期。

	命令	用途
步骤 1	`tunnel-group general-attributes`	切换至 general-attributes 模式。
步骤 2	`password-management`	通知远程用户密码即将到期。
步骤 3	`password-expire-in-days`	指定密码到期时间。

步骤 4	输入天数
	
	示例：
	`hostname(config)# tunnel-group testgroup type webvpn`
	`hostname(config)# tunnel-group testgroup general-attributes`
	`hostname(config-general)# password-management password-expire-in-days 90`
		如果指定关键字，还必须指定天数。如果将天数设置为 0，此命令将关闭。
		注　ASA 不会通知用户密码即将到期，但是用户可以在密码到期后更改密码。
		
		将连接配置文件 “testgroup” 的密码到期警告提前天数设置为 90。

对无客户端 SSL VPN 使用单点登录

借助单点登录 (SSO) 支持，无客户端 SSL VPN 的用户一次只需输入一个用户名和密码，就可以访问多个受保护的服务和网络服务器。一般来说， SSO 机制作为 AAA 流程的一部分启动，或者在成功执行 AAA 服务器的用户身份验证后启动。ASA 上运行的无客户端 SSL VPN 服务器充当身份验证服务器的用户的代理。当有用户登录时，无客户端 SSL VPN 服务器会向身份验证服务器发送 SSO 身份验证请求 （包括用户名和密码）。如果服务器批准身份验证请求，服务器会将 SSO 身份验证 Cookie 返回到无客户端 SSL VPN 服务器。ASA 会代表用户保留此 Cookie 并将其用于对用户进行身份验证，以确保受 SSO 服务器保护的域内的网站的安全。

本节介绍无客户端 SSL VPN 支持的 SSO 身份验证方法：HTTP 基本身份验证和 NTLMv1 (NT LAN Manager) 身份验证、 Computer Associates eTrust SiteMinder SSO 服务器 （原称为 Netegrity SiteMinder）、安全断言标记语言 (SAML) 1.1 （POST 类型 SSO 服务器身份验证）。

本节包括：

使用 HTTP 基本身份验证或 NTLM 身份验证来配置 SSO

本节介绍使用 HTTP 基本身份验证或 NTLM 身份验证的单点登录。可以使用这两种方法之一或结合使用这两种方法来配置 ASA，以实现 SSO。**auto-sign-on** 命令将 ASA 配置为会自动将无客户端 SSL VPN 用户登录凭证 （用户名和密码）传递到内部服务器。可以输入多个 **auto-sign-on** 命令。ASA 根据输入顺序处理命令 （先输入的命令优先）。可以使用 IP 地址和 IP 掩码或 URI 掩码指定要接收登录凭证的服务器。

可以在如下三种模式之一下使用 **auto-sign-on** 命令：无客户端 SSL VPN 配置模式、无客户端组策略模式或无客户端 SSL VPN 用户名模式。用户名取代组，组取代全局。选择具有所需身份验证范围的模式：

模式	范围
`webvpn configuration`	所有全局无客户端 SSL VPN 用户。
`webvpn group-policy configuration`	组策略定义的无客户端 SSL VPN 用户的子集。
`webvpn username configuration`	无客户端 SSL VPN 的单个用户。

详细步骤

以下示例命令显示模式和参数的各种可用组合。

	命令	用途

步骤 1	示例：
	`hostname(config)# webvpn`
	
	`hostname(config-webvpn)# auto-sign-on allow ip 10.1.1.1 255.255.255.0 auth-type ntlm`
		使用 NTLM 身份验证将所有无客户端 SSL VPN 用户配置为可自动登录到 IP 地址介于 10.1.1.0 和 10.1.1.255 之间的服务器。

步骤 2	示例：
	`hostname(config)# webvpn`
	`hostname(config-webvpn)# auto-sign-on allow uri https://*.example.com/* auth-type basic`
		使用 HTTP 基本身份验证将所有无客户端 SSL VPN 用户配置为可自动登录到 URI 掩码 https://*.example.com/* 定义的服务器。

步骤 3	示例：
	`hostname(config)# group-policy ExamplePolicy attributes`
	`hostname(config-group-policy)# webvpn`
	`hostname(config-group-webvpn)# auto-sign-on allow uri https://*.example.com/* auth-type all`
		使用基本身份验证或 NTLM 身份验证将与 ExamplePolicy 组策略相关的无客户端 SSL VPN 会话配置为可自动登录到 URI 掩码定义的服务器。

步骤 4	示例：
	`hostname(config)# username Anyuser attributes`
	`hostname(config-username)# webvpn`
	`hostname(config-username-webvpn)# auto-sign-on allow ip 10.1.1.1 255.255.255.0 auth-type basic`
		使用 HTTP 身份验证将名为 Anyuser 用户配置为可自动登录到 IP 地址介于 10.1.1.0 和 10.1.1.255 之间的服务器。

步骤 5	`(config-webvpn)# smart-tunnel auto-sign-on` *host-list* `[use-domain] [realm` *realm string*`] [port` *port num*`] [host` *host mask* `|` `ip` *address subnet mask*`]`	配置使用特定端口和领域的自动登录以便进行身份验证。

使用 SiteMinder 配置 SSO 身份验证

本节介绍使用 SiteMinder 将 ASA 配置为支持 SSO。但是，如果网站安全基础设施中已纳入了 SiteMinder，通常会选择使用 SiteMinder 来实现 SSO。使用此方法时，SSO 身份验证与 AAA 流程分开执行，在 AAA 流程完成后立即执行 SSO 身份验证。

先决条件

- 指定 SSO 服务器。
- 指定 ASA 向其发出 SSO 身份验证请求的 SSO 服务器的 URL。
- 指定密钥，以保护 ASA 与 SSO 服务器之间的通信。此密钥与密码类似：可根据思科 Java 插件身份验证方案，创建、保存并在 ASA 和 SiteMinder 策略服务器上输入密钥。

除了必要的任务外，还可以执行以下配置任务：

- 配置身份验证请求超时。
- 配置身份验证请求重试次数。

限制

要为用户或组配置用于访问无客户端 SSL VPN 的 SSO，必须首先配置 AAA 服务器 （例如 RADIUS 或 LDAP 服务器）。可以设置对于无客户端 SSL VPN 的 SSO 支持。

详细步骤

本节介绍使用 CA SiteMinder 将 ASA 配置为支持 SSO 身份验证的具体步骤。

	命令	用途
步骤 1	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 2	**sso-server type** *type* **示例：** hostname(config)# **webvpn** hostname(config-webvpn)# **sso-server Example type siteminder** hostname(config-webvpn-sso-siteminder)#	创建 SSO 服务器。 创建类型为 siteminder 且名为 Example 的 SSO 服务器。
步骤 3	**config-webvpn-sso-siteminder**	切换至 siteminder 配置模式。
步骤 4	**web-agent-url** **示例：** hostname(config-webvpn-sso-siteminder)# **web-agent-url http://www.Example.com/webvpn** hostname(config-webvpn-sso-siteminder)#	指定 SSO 服务器的身份验证 URL。 将身份验证请求发送到 URL http://www.Example.com/webvpn。
步骤 5	**policy-server-secret** *secret* **示例：** hostname(config-webvpn-sso-siteminder)# **policy-server-secret AtaL8rD8!** hostname(config-webvpn-sso-siteminder)#	指定密钥，以保护 ASA 与 SiteMinder 之间的身份验证通信。 创建密钥 AtaL8rD8!。可以使用任何常规或经过转换的字母数字字符来创建任意长度的密钥，但必须在 ASA 和 SSO 服务器上输入相同的密钥。
步骤 6	**request-timeout** *seconds* **示例：** hostname(config-webvpn-sso-siteminder)# **request-timeout 8** hostname(config-webvpn-sso-siteminder)#	配置失败的 SSO 身份验证尝试超时之前的秒数。默认值是 5 秒，允许的范围是 1 至 30。 将请求超时之前的秒数更改为 8。
步骤 7	**max-retry-attempts** **示例：** hostname(config-webvpn-sso-siteminder)# **max-retry-attempts 4** hostname(config-webvpn-sso-siteminder)#	配置 ASA 在身份验证超时之前尝试进行 SSO 身份验证的重试次数。默认值是 3 次，允许的范围是 1 到 5 次。 将重试次数配置为 4。
步骤 8	**username-webvpn** **group-policy-webvpn**	为用户指定身份验证。 为组指定身份验证。

	命令	用途
步骤 9	**sso-server value** *value* **示例：** hostname(config)# **username Anyuser attributes** hostname(config-username)# **webvpn** hostname(config-username-webvpn)# **sso-server value** *value* hostname(config-username-webvpn)#	为组或用户指定 SSO 身份验证。 将名为 Example 的 SSO 服务器分配给名为 Anyuser 的用户。
步骤 10	**test sso-server** *server* **username** *username* **示例：** hostname# **test sso-server Example username Anyuser** INFO: Attempting authentication request to sso-server Example for user Anyuser INFO: STATUS: Success hostname#	测试 SSO 服务器配置。 使用用户名 Anyuser 测试名为 Example 的 SSO 服务器。

将思科身份验证方案添加到 SiteMinder

除了使用 SiteMinder 配置 ASA 来实现 SSO 之外，还必须使用思科身份验证方案 （一个可从思科网站下载的 Java 插件）配置 CA SiteMinder 策略服务器。

先决条件

配置 SiteMinder 策略服务器要求具备使用 SiteMinder 的经验。

详细步骤

本节介绍一般任务，而非完整的操作步骤。

步骤 1　如果使用 SiteMinder Administration 实用程序创建自定义身份验证方案，请务必使用以下特定参数：

- 在 Library 字段中，输入 **smjavaapi**。
- 在 Secret 字段中，输入在 ASA 上配置的那个密钥。

  通过在命令行界面上使用 **policy-server-secret** 命令可以在 ASA 上配置密钥。
- 在 Parameter 字段中，输入 **CiscoAuthApi**。

步骤 2　使用 Cisco.com 登录名，从 http://www.cisco.com/cisco/software/navigator.html 下载文件 **cisco_vpn_auth.jar**，并将其复制到 SiteMinder 服务器的默认库目录。思科 ASA CD 中也提供了此 .jar 文件。

使用 SAML 浏览器 Post 配置文件配置 SSO 身份验证

本节介绍将 ASA 配置为对授权用户支持安全断言标记语言 (SAML) 1.1 POST 配置文件单点登录 (SSO)。

会话发起后，ASA 会按照配置的 AAA 方法对用户进行身份验证。接着，ASA（断言方）会为信赖方（SAML 服务器提供的使用者 URL 服务）生成断言。如果 SAML 交换成功，用户可以访问受保护的资源。

先决条件

如要使用 SAML 浏览器 Post 配置文件配置 SSO，必须执行以下任务：

- 使用 **sso-server** 命令指定 SSO 服务器
- 为身份验证请求指定 SSO 服务器的 URL（**assertion-consumer-ur** 命令）
- 将 ASA 主机名指定为发出身份验证请求的组件（**issuer** 命令）
- 指定用于对 SAML Post 配置文件断言进行签名的信任点证书（**trustpoint** 命令）

除了这些必要的任务外，还可以执行以下配置任务：

- 配置身份验证请求超时（**request-timeout** 命令）
- 配置身份验证请求重试次数（**max-retry-attempts** 命令）

限制

- 仅无客户端 SSL VPN 会话支持 SAML SSO。
- ASA 目前仅支持浏览器 Post 配置文件类型的 SAML SSO 服务器。
- 不支持用于交换断言的 SAML 浏览器 Artifact 方法。

详细步骤

本节介绍使用 SAML-V1.1-POST 配置文件将 ASA 配置为支持 SSO 身份验证的具体步骤。

	命令	用途
步骤 1	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 2	**sso-server type** *type* **示例：** hostname(config)# **webvpn** hostname(config-webvpn)# **sso-server sample type SAML-V1.1-post** hostname(config-webvpn-sso-saml)#	创建 SSO 服务器。 创建类型为 SAML-V1.1-POST 且名为 Sample 的 SSO 服务器。
步骤 3	**sso saml**	切换至无客户端 SSL VPN sso-saml 配置模式。
步骤 4	**assertion-consumer-url** *url* **示例：** hostname(config-webvpn-sso-saml)# **assertion-consumer-url http://www.example.com/webvpn** hostname(config-webvpn-sso-saml)#	指定 SSO 服务器的身份验证 URL。 将身份验证请求发送到 URL http://www.Example.com/webvpn。

	命令	用途
步骤 5	**issuer** *string* **示例：** hostname(config-webvpn-sso-saml)# **issuer myasa** hostname(config-webvpn-sso-saml)#	在 ASA 生成断言时对 ASA 进行标识。通常，此颁发者名称是 ASA 的主机名。
步骤 6	**trust-point** hostname(config-webvpn-sso-saml)# **trust-point mytrustpoint**	指定用于对断言进行签名的身份证书。
步骤 7	（可选） **request-timeout** **示例：** hostname(config-webvpn-sso-saml)# **request-timeout 8** hostname(config-webvpn-sso-saml)#	配置失败的 SSO 身份验证尝试超时之前的秒数。 将请求超时之前的秒数设置为 8。默认值是 5 秒，允许的范围是 1 至 30。
步骤 8	（可选） **max-retry-attempts** **示例：** hostname(config-webvpn-sso-saml)# **max-retry-attempts 4** hostname(config-webvpn-sso-saml)#	配置 ASA 在身份验证超时之前尝试进行 SSO 身份验证的重试次数。 将重试次数设置为 4。默认值是 3 次，允许的范围是 1 到 5 次。
步骤 9	webvpn	切换至无客户端 SSL VPN 配置模式。
步骤 10	**group-policy-webvpn** **username-webvpn**	将 SSO 服务器分配给组策略。 将 SSO 服务器分配给用户策略。
步骤 11	**sso-server value** **示例：** hostname(config)# **username Anyuser attributes** hostname(config-username)# **webvpn** hostname(config-username-webvpn)# **sso-server value sample** hostname(config-username-webvpn)#	为组或用户指定 SSO 身份验证。 将名为 Example 的 SSO 服务器分配给名为 Anyuser 的用户。
步骤 12	**test sso-server** **示例：** hostname# **test sso-server Example username Anyuser** INFO: Attempting authentication request to sso-server sample for user Anyuser INFO: STATUS: Success	（特权执行模式）测试 SSO 服务器配置。 使用用户名 Anyuser 测试名为 Example 的 SSO 服务器。

配置 SAML POST SSO 服务器

使用服务器软件供应商提供的 SAML 服务器文档在信赖方模式下配置 SAML 服务器。

详细步骤

步骤 1　配置 SAML 服务器参数来代表断言方 (ASA)：

- 接收使用者 URL （与 ASA 上配置的断言使用者 URL 相同）
- 颁发者 ID （字符串，通常是设备的主机名）
- 配置文件类型 — 浏览器 Post 配置文件

步骤 2　配置证书。

步骤 3　指明必须对断言方的断言进行签名。

步骤 4　选择 SAML 服务器如何标识用户：

- 使用者名称类型为 DN
- 使用者名称格式为 uid=<user>

使用 HTTP 表单协议配置 SSO

本节介绍使用 HTTP 表单协议来配置 SSO。 HTTP 表单协议是一种 SSO 身份验证方法，也可用作 AAA 方法。它提供了一种安全的方法用于在无客户端 SSL VPN 用户与身份验证网络服务器之间交换身份验证信息。此协议可以与其他 AAA 服务器 （例如 RADIUS 或 LDAP 服务器）配合使用。**先决条件**

如要使用 HTTP 协议正确配置 SSO，必须全面了解 SSO 身份验证和 HTTP 协议交换的工作原理。

限制

HTTP 表单协议是一种常见协议，仅在用于进行身份验证的网络服务器应用符合以下条件时才适用：

- 必须为成功的请求设置身份验证 Cookie，但不为未授权的登录设置身份验证 Cookie。在这种情况下， ASA 无法区分成功和失败的身份验证。

详细步骤

ASA 同样充当身份验证网络服务器的无客户端 SSL VPN 用户的代理，但在这种情况下，它使用 HTTP 表单协议和 POST 请求方法。必须将 ASA 配置为可发送和接收表单数据。图 18-4 介绍以下 SSO 身份验证步骤：

步骤 1　无客户端 SSL VPN 用户首先输入用户名和密码，以登录到 ASA 上的无客户端 SSL VPN 服务器。

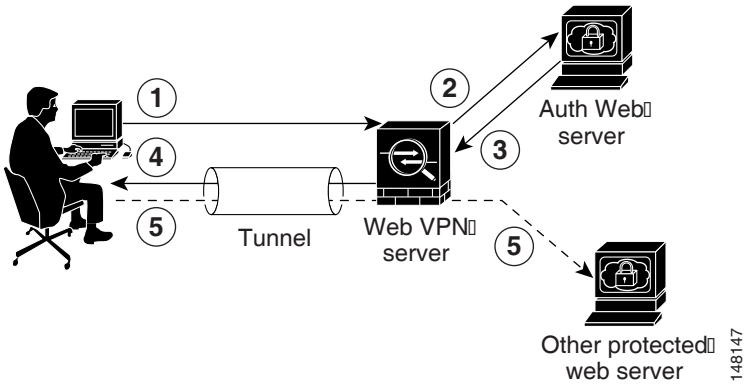
步骤 2　无客户端 SSL VPN 服务器充当用户的代理，并使用 POST 身份验证请求将表单数据 （用户名和密码）转发到身份验证网络服务器。

步骤 3　如果身份验证网络服务器批准用户数据，它会将身份验证 Cookie 返回到无客户端 SSL VPN 服务器 （该服务器会代表用户存储该 Cookie）。

步骤 4　无客户端 SSL VPN 服务器建立通向用户的隧道。

步骤 5　这样，用户无需重新输入用户名和密码即可访问受保护 SSO 环境中的其他网站。

图 18-4　使用 HTTP 表单的 SSO 身份验证



虽然您通常会配置允许 ASA 包含 POST 数据 （例如用户名和密码）的表单参数，但是，您最初可能不会注意到网络服务器需要的其他隐藏参数。某些身份验证应用会遇到一些既不向用户显示也不是由用户输入的隐藏数据。但是，可以通过以下方法发现身份验证网络服务器会遇到的隐藏参数：从浏览器向身份验证网络服务器发送直接身份验证请求，而不使用 ASA 作为中间代理。使用 HTTP 报头分析器分析网络服务器响应能够以类似于以下的格式显示隐藏参数：

```
<param name>=<URL encoded value>&<param name>=<URL encoded>
```

有些隐藏参数是必填的，有些是可选的。如果网络服务器需要隐藏参数的数据，它将拒绝忽略这些数据的任何身份验证 POST 请求。由于报头分析器不会指出隐藏参数是否为必填的，因此，我们建议将所有隐藏参数包括在内，直至确定哪些是必填的。

要使用 HTTP 表单协议配置 SSO，必须执行以下操作：

- 在身份验证网络服务器上配置统一资源标识符，用以接收和处理表单数据 (**action-uri**)。
- 配置用户名参数 (**user-parameter**)。
- 配置用户密码参数 (**password-parameter**)。

可能还需要执行以下任务，具体取决于身份验证网络服务器的要求：

- 如果身份验证网络服务器要求登录前 Cookie 交换，请配置启动 URL (**start-url**)。
- 配置身份验证网络服务器所需的任何隐藏身份验证参数 (**hidden-parameter**)。
- 配置身份验证网络服务器设置的身份验证 Cookie 的名称 (**auth-cookie-name**)。

	命令	用途
步骤 1	**aaa-server-host**	切换至 aaa-server-host 配置模式。
步骤 2	**start-url** **示例：** hostname(config)# **aaa-server testgrp1 protocol http-form** hostname(config)# **aaa-server testgrp1 host 10.0.0.2** hostname(config-aaa-server-host)# **start-url http://example.com/east/Area.do?Page-Grp1** hostname(config-aaa-server-host)#	如果身份验证网络服务器有要求，请指定用于从身份验证网络服务器检索登录前 Cookie 的 URL。 指定 IP 地址为 10.0.0.2 的 testgrp1 服务器组中的身份验证网络服务器 URL http://example.com/east/Area.do?Page-Grp1。

	命令	用途
步骤 3	**action-uri** **示例：** http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SM5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth.example.com 要指定此操作 URI，请输入以下命令： hostname(config-aaa-server-host)# **action-uri http://www.example.com/auth/index.htm** hostname(config-aaa-server-host)# **action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP** hostname(config-aaa-server-host)# **action-uri 554433&REALMOID=06-000a1311-a828-1185** hostname(config-aaa-server-host)# **action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON** hostname(config-aaa-server-host)# **action-uri =0&METHOD=GET&SMAGENTNAME=SM5FZmjnk** hostname(config-aaa-server-host)# **action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r** hostname(config-aaa-server-host)# **action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F** hostname(config-aaa-server-host)# **action-uri %2Fauth.example.com** hostname(config-aaa-server-host)#	指定身份验证网络服务器上的身份验证计划的 URI。 可以在多个顺序行上输入同一个 URI。每行的最大字符数是 255。完整 URI 的最大字符数是 2048。 必须在操作 URI 中包含主机名和协议。在本示例中，主机名和协议显示在 http://www.example.com 中 URI 的开头。
步骤 4	**user-parameter** **示例：** hostname(config-aaa-server-host)# **user-parameter userid** hostname(config-aaa-server-host)#	为 HTTP POST 请求配置 **userid** 用户名参数。
步骤 5	**password-parameter** **示例：** hostname(config-aaa-server-host)# **password-parameter user_password** hostname(config-aaa-server-host)#	为 HTTP POST 请求配置 **user_password** 用户密码参数。

	命令	用途
步骤 6	**hidden-parameter** **示例：** SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0 要指定此隐藏参数，请输入以下命令： hostname(config)# **aaa-server testgrp1 host example.com** hostname(config-aaa-server-host)# **hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe** hostname(config-aaa-server-host)# **hidden-parameter t=https%3A%2F%2Fwww.example.com%2Femc** hostname(config-aaa-server-host)# **hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo** hostname(config-aaa-server-host)# **hidden-parameter de%3DENG&smauthreason=0** hostname(config-aaa-server-host)#	指定用以与身份验证网络服务器进行交换的隐藏参数。 显示摘录自 POST 请求的隐藏参数示例。此隐藏参数包含四个表单条目及其值，条目之间用 & 分隔。这些条目及其值如下： • SMENC，值为 ISO-8859-1。 • SMLOCALE，值为 US-EN。 • 值为 https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do 的目标。 • %3FEMCOPageCode%3DENG。 • 值为 0 的 smauthreason。
步骤 7	（可选） **auth-cookie-name** *cookie-name* **示例：** hostname(config-aaa-server-host)# **auth-cookie-name SsoAuthCookie** hostname(config-aaa-server-host)#	指定身份验证 Cookie 的名称。 指定 SsoAuthCookie 的身份验证 Cookie 名称。
步骤 8	**tunnel-group general-attributes**	切换至 tunnel-group general-attributes 配置模式。
步骤 9	**authentication-server-group** **示例：** hostname(config)# **tunnel-group testgroup general-attributes** hostname(config-tunnel-general)**#authentication-server-group testgrp1**	配置隧道组，以使用在上述步骤中配置的 SSO 服务器。 配置名为 /testgrp/ 的隧道组，以使用名为 /testgrp1/ 的 SSO 服务器。
步骤 10	**aaa-server-host**	切换至 AAA 服务器主机配置模式。

	命令	用途
步骤 11	**hidden-parameter** **示例：** SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0 要指定此隐藏参数，请输入以下命令： hostname(config)# **aaa-server testgrp1 host example.com** hostname(config-aaa-server-host)# **hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe** hostname(config-aaa-server-host)# **hidden-parameter t=https%3A%2F%2Fwww.example.com%2Femc** hostname(config-aaa-server-host)# **hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo** hostname(config-aaa-server-host)# **hidden-parameter de%3DENG&smauthreason=0** hostname(config-aaa-server-host)#	指定用以与身份验证网络服务器进行交换的隐藏参数。 显示摘录自 POST 请求的隐藏参数示例。此隐藏参数包含四个表单条目及其值，条目之间用 & 分隔。这些条目及其值如下： • SMENC，值为 ISO-8859-1。 • SMLOCALE，值为 US-EN。 • 值为 https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do 的目标。 • %3FEMCOPageCode%3DENG。 • 值为 0 的 smauthreason。
步骤 12	（可选） **auth-cookie-name** *cookie-name* **示例：** hostname(config-aaa-server-host)# **auth-cookie-name SsoAuthCookie** hostname(config-aaa-server-host)#	指定身份验证 Cookie 的名称。 指定 SsoAuthCookie 的身份验证 Cookie 名称。
步骤 13	**tunnel-group general-attributes**	切换至 tunnel-group general-attributes 模式。
步骤 14	**authentication-server-group** *group* **示例：** hostname(config)# **tunnel-group testgroup general-attributes** hostname(config-tunnel-general)**#authentication-server-group testgrp1**	配置隧道组，以使用在上述步骤中配置的 SSO 服务器。 配置名为 /testgroup/ 的隧道组，以使用名为 /testgrp1/ 的 SSO 服务器。

收集 HTTP 表单数据

本节介绍发现和收集必要的 HTTP 表单数据的步骤。如果不知道身份验证网络服务器需要哪些参数，可以通过分析身份验证交换来收集参数数据。

先决条件

这些步骤需要使用浏览器和 HTTP 报头分析器。

详细步骤

步骤 1　启动浏览器和 HTTP 报头分析器，并直接连接到网络服务器登录页面 （而不是通过 ASA 连接）。

步骤 2　在浏览器中加载网络服务器登录页面后，检查登录序列以确定是否已在交换过程中设置了 Cookie。如果网络服务器已使用登录页面加载了 Cookie，请将该登录页面 URL 配置为 *start-URL*。

步骤 3　输入用户名和密码以登录到网络服务器，然后按 **Enter**。此操作会生成使用身份验证 POST 请求（可使用 HTTP 报头分析器检查该请求）。

包含主机 HTTP 报头和正文的 POST 请求示例如下：

```
POST
/emco/myemco/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000430e1-7443-125c-ac05
-83846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk2KcqVCFbIr
NT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.com%2Femco%2Fmye
mco%2FHTTP/1.1

Host: www.example.com

(BODY)

SMENC=ISO-8859-1&SMLOCALE=US-EN&USERID=Anyuser&USER_PASSWORD=XXXXXX&target=https%3A%2F%
2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0
```

步骤 4　检查 POST 请求并复制协议、主机和完整的 URL，以配置操作 URI 参数。

步骤 5　检查 POST 请求正文并复制以下内容：

a. 用户名参数。在上一个示例中，此参数是 *USERID*，而不是值 *anyuser*。

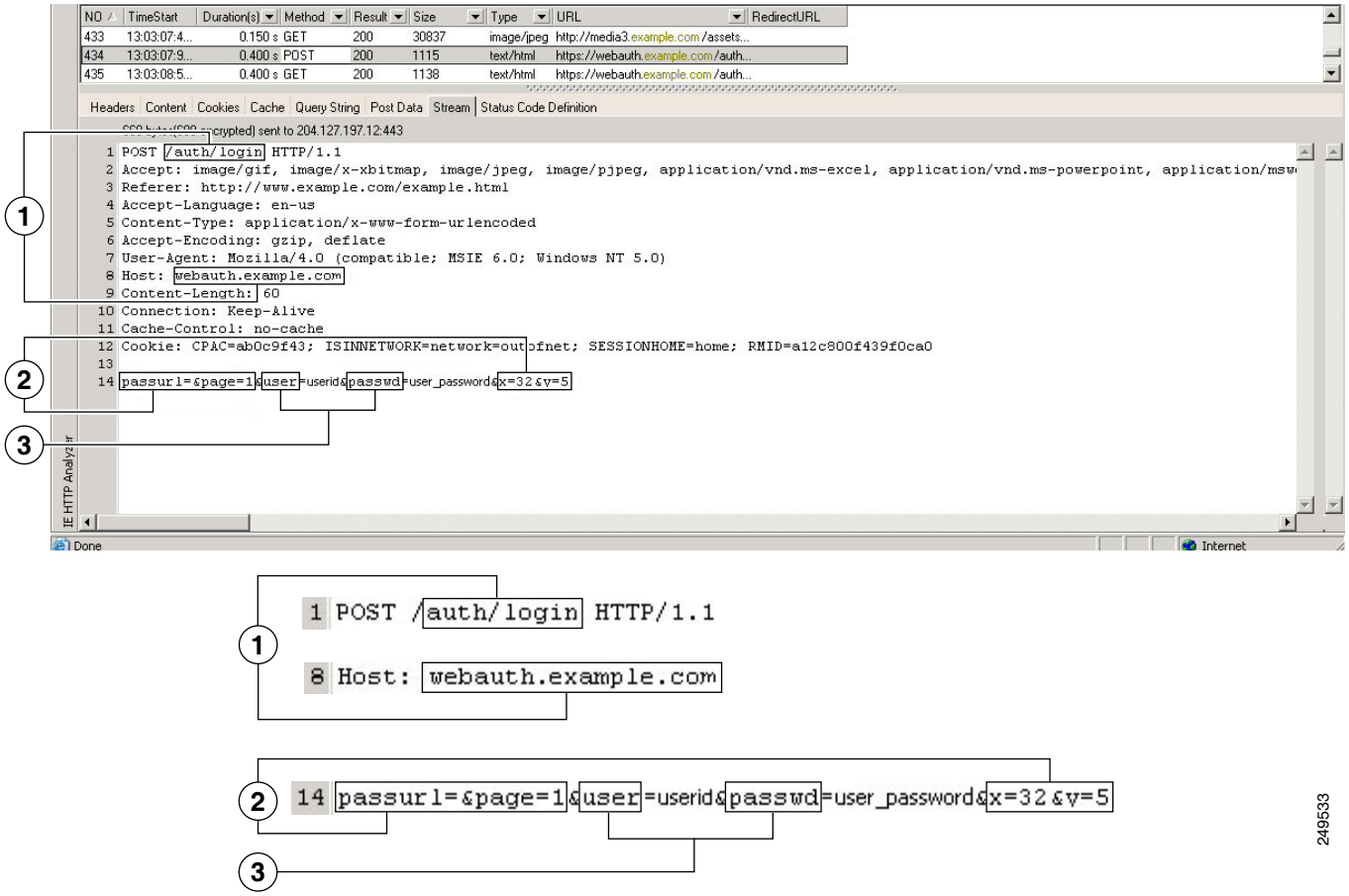
b. 密码参数。在上一个示例中，此参数是 *USER_PASSWORD*。

c. 隐藏参数。此参数是 POST 正文中除用户名和密码参数之外的一切内容。在上一个示例中，隐藏参数如下所示：

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0

图 18-5 突出显示了 HTTP 分析器的输出示例中的操作 URI 参数、隐藏参数、用户名参数和密码参数。这只是一个示例；不同网站的输出会有所不同。

图 18-5　　操作 URI 参数、隐藏参数、用户名参数和密码参数



1	操作 URI 参数
2	隐藏参数
3	用户名和密码参数

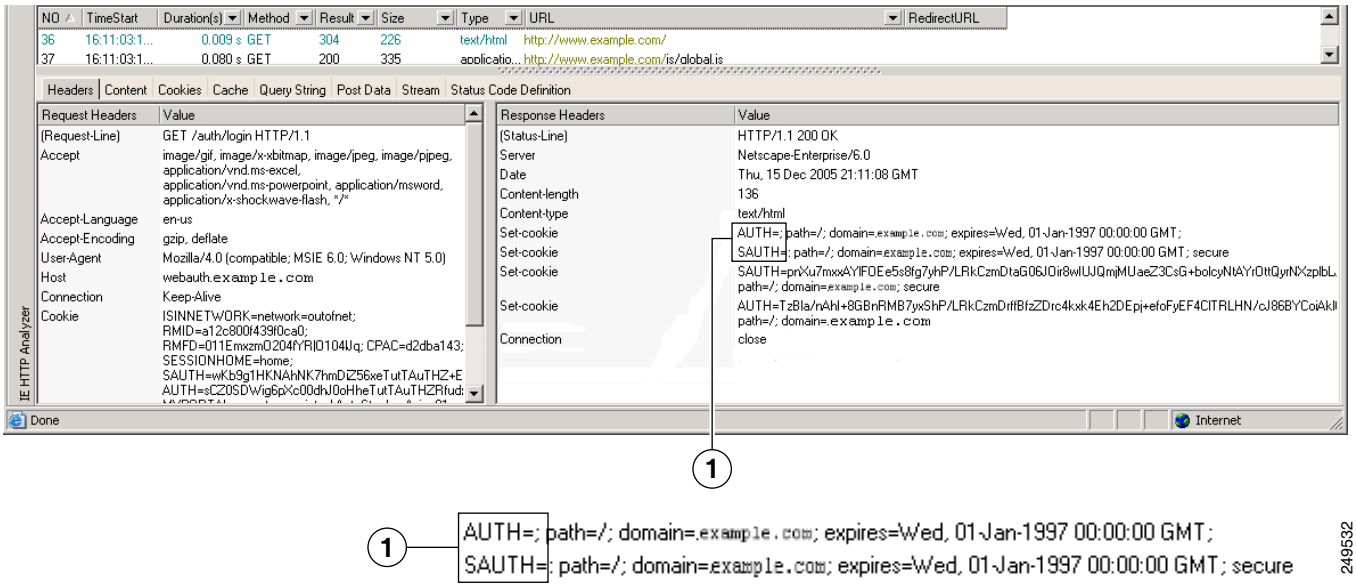
步骤 6　如果成功登录到网络服务器，请使用 HTTP 报头分析器检查服务器响应，以查找浏览器中服务器设置的会话 Cookie 名称。这是 **auth-cookie-name** 参数。

在以下服务器响应报头中，会话 Cookie 名称是 SMSESSION。只需要名称，不需要值。

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZP
bHIHtWLDKTa8ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSS
OSepWvnsCb7IFxCw+MGiw0o88uHa2t4l+SillqfJvcpuXfiIAO06D/gtDF40Ow5YKHEl2KhDEvv+yQ
zxwfEz2cl7Ef5iMr8LgGcDK7qvMcvrgUqx68JQOK2+RSwtHQ15bCZmsDU5vQVCvSQWC8OMHNGwpS25
3XwRLvd/h6S/tM0k98QMv+i3N8oOdj1V7flBqecH7+kVrU01F6oFzr0zM1kMyLr5HhlVDh7B0k9wp0
dUFZiAzaf43jupD5f6CEkuLeudYW1xgNzsR8eqtPK6t1gFJyOn0s7QdNQ7q9knsPJsekRAH9hrLBhW
BLTU/3B1QS94wEGD2YTuiW36TiP14hYwOlCAYRj2/bY3+lYzVu7EmzMQ+UefYxh4cF2gYD8RZL2Rwm
P9JV5l48I3XBFPNUw/3V5jf7nRuLr/CdfK3OO8+Pa3V6/nNhokErSgyxjzMd88DVzM41LxxaUDhbcm
koHT9ImzBvKzJX0J+o7FoUDFOxEdIqlAN4GNqk49cpi2sXDbIarALp6Bl3+tbB4MlHGH+0CPscZXqo
i/kon9YmGauHyRs+0m6wthdlAmCnvlJCDfDoXtn8DpabgiW6VDTrvl3SGPyQtUv7Wdahuq5SxbUzjY
2JxQnrUtwB977NCzYu2sOtN+dsEReWJ6ueyJBbMzKyzUB4L3i5uSYN50B4PCv1w5KdRKa5p3N0Nfq6
RM6dfipMEJw0Ny1sZ7ohz3fbvQ/YZ7lw/k7ods/8VbaR15ivkE8dSCzuf/AInHtCzuQ6wApzEp9CUo
G8/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma5dc/emWor9vWr0HnT
QaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.example.com;Path=
/
```

图 18-6 显示了 HTTP 分析器输出中授权 Cookie 的示例。这只是一个示例；不同网站的输出会有所不同。

图 18-6　　HTTP 分析器输出示例中的授权 Cookie



1	授权 Cookie

步骤 7　在某些情况下，不管身份验证是否成功，服务器都可能会设置相同的 Cookie，且该 Cookie 不可用于 SSO。要确认 Cookie 是否不同，请使用无效的登录凭证重复步骤 1 到步骤 6，并将“失败”Cookie 与“成功”Cookie 作比较。到此，已具备使用 HTTP 表单协议将 ASA 配置为支持 SSO 所需的参数数据。

为插件配置 SSO

插件支持单点登录 (SSO)。插件使用输入的相同凭据 （用户名和密码）对无客户端 SSL VPN 会话进行身份验证。由于插件不支持宏替换，因此，用户不能对不同的字段 （例如，内部域密码或者 RADIUS 或 LDAP 服务器上的属性）执行 SSO。

要将插件配置为支持 SSO，请安装插件并添加书签条目以显示服务器链接，同时使用 csco_sso=1 参数指定 SSO 支持。以下示例显示了为 SSO 启用的插件书签：

```
ssh://ssh-server/?cisco_sso=1
rdp://rdp-server/?Parameter1=value&Parameter2=value&csco_sso=1
```

使用宏替换配置 SSO

本节介绍将宏替换用于 SSO。使用宏替换配置 SSO 可以将某些变量插入到书签以替换动态值。

注 智能隧道书签支持自动登录，但不支持变量替换。例如，为智能隧道配置的 SharePoint 书签使用与用于登录无客户端 SSL VPN 的凭证相同的用户名和密码凭证登录到应用。可以同时或单独使用变量替换和自动登录。

您现在可以利用宏替换使用书签自动登录某些网页。之前创建的 POST 插件方法使管理员可以指定带登录宏的 POST 书签和接收发布 POST 请求之前要加载的启动页面。这种 POST 插件方法消除了需要有 cookie 或其他标头项的那些请求。现在管理员要确定预加载页面和 URL，其指定向何处发送 POST 登录请求。预加载页面使终端浏览器可以获取一起发送至网络服务器或网络应用的特定信息，而不仅仅是使用包含凭据的 POST 请求。

以下变量 （或宏）允许在书签和基于表单的 HTTP POST 操作中执行替换：

- CSCO_WEBVPN_USERNAME — 用户登录 ID
- CSCO_WEBVPN_PASSWORD — 用户登录密码
- CSCO_WEBVPN_INTERNAL_PASSWORD — 用户内部 （或域）密码。此缓存凭证未通过 AAA 服务器进行身份验证。输入此值后，安全设备会将其用作自动登录密码，而不是用作密码 / 主密码值。

  注 不能在基于 GET 的 HTTP 书签中使用这三个变量当中的任何一个。只有基于 POST 的 HTTP 和 CIFS 书签可以使用这些变量。

- CSCO_WEBVPN_CONNECTION_PROFILE — 用户登录组下拉列表 （连接配置文件别名）
- CSCO_WEBVPN_MACRO1 — 使用 RADIUS-LDAP 供应商特定属性 (VSA) 进行设置。如果要从包含 ldap-attribute-map 命令的 LDAP 进行映射，请将 WebVPN-Macro-Substitution-Value1 思科属性用于该宏。有关 Active Directory ldap-attribute-mapping 示例，请访问 http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/ref_extserver.html#wp1572118。

  VSA#223 执行对于 RADIUS 的 CSCO_WEBVPN_MACRO1 宏替换 （请参阅表 18-1）。

表 18-1　VSA#223

WebVPN-Macro-Value1	Y	223	字符串	单个	无限
WebVPN-Macro-Value2	Y	224	字符串	单个	无限

值 （例如 www.cisco.com/email）将会动态填充无客户端 SSL VPN 门户上的书签 （例如，特定 DAP 或组策略的 https://CSCO_WEBVPN_MACRO1 或 https://CSCO_WEBVPN_MACRO2）。

- CSCO_WEBVPN_MACRO2 — 使用 RADIUS-LDAP 供应商特定属性 (VSA) 进行设置。如果要从包含 ldap-attribute-map 命令的 LDAP 进行映射，请将 WebVPN-Macro-Substitution-Value2 思科属性用于该宏。有关 Active Directory ldap-attribute-mapping 示例，请访问 http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/ref_extserver.html#wp1572118。

  VSA#224 执行对于 RADIUS 的 CSCO_WEBVPN_MACRO2 宏替换 （请参阅表 18-1）。

每次无客户端 SSL VPN 识别出最终用户请求 （以书签或 Post 形式）中的六个字符串之一时，它都会将该字符串替换为用户指定的值，然后将请求传递到远程服务器。

如果未能在 ASA 上找到用户名和密码，将会替换空字符串，且行为将会恢复为如同没有自动登录可用时一样。

需要用户名和密码

根据您的网络，在远程会话期间，可能需要登录以下任一项或所有项：计算机、互联网服务提供程序、无客户端 SSL VPN、邮件或文件服务器或企业应用。用户可能必须在许多不同情景下进行身份验证，这要求提供不同的信息，例如唯一用户名、密码或 PIN。

表 18-2 列出了无客户端 SSL VPN 用户可能需要知道的用户名和密码的类型。

表 18-2　　要向无客户端 SSL VPN 会话用户提供的用户名和密码

登录用户名 / 密码类型	用途	输入时间
计算机	访问计算机	启动计算机
互联网服务提供商	访问互联网	连接互联网服务提供商
无客户端 SSL VPN	访问远程网络	启动无客户端 SSL VPN
文件服务器	访问远程文件服务器	使用无客户端 SSL VPN 文件浏览功能访问远程文件服务器
企业应用登录	访问受防火墙保护的内部服务器	使用无客户端 SSL VPN 网络浏览功能访问受保护的内部网站
邮件服务器	通过无客户端 SSL VPN 访问远程邮件服务器	发送或接收邮件信息

传达安全提示

建议用户在关闭无客户端 SSL VPN 会话时始终点击工具栏上的注销图标。（关闭浏览器窗口不会关闭会话。）

无客户端 SSL VPN 将确保远程计算机或工作站与公司网络上的 ASA 之间数据传输的安全性。告知用户使用无客户端 SSL VPN 并不能保证与每个站点的通信都是安全的。如果用户在收到该提醒后访问非 HTTPS 网络资源 （位于互联网或内部网络上），公司 ASA 与目标网络服务器之间的通信不是专用的，因为它未加密。

第 1 页上的 “无客户端 SSL VPN 安全预防措施”中根据在该节中执行的步骤提供了有关与用户进行通信的其他提示。

配置远程系统以使用无客户端 SSL VPN 功能

本节介绍如何设置远程系统以使用无客户端 SSL VPN。

可采用不同的方式配置各个用户帐户，以使每个用户可以使用不同的无客户端 SSL VPN 功能。

启动无客户端 SSL VPN

可以使用任何受支持的连接方法连接到互联网，这些方法包括：

- 家庭 DSL、电缆或拨号。
- 公共信息亭。
- 酒店热点。
- 机场无线节点。
- 网吧。

注　有关无客户端 SSL VPN 支持的网络浏览器的列表，请参阅 《*支持的 VPN 平台 （思科 ASA 系列）*》。

先决条件

- 要通过端口转发访问应用，必须在浏览器上启用 Cookie。
- 必须有无客户端 SSL VPN 的 URL。 URL 必须是采用以下格式的 https 地址：*//address*，其中， *address* 是启用了 SSL VPN 的 ASA （或负载平衡集群）的接口的 IP 地址或 DNS 主机名。例如， https://cisco.example.com。
- 必须有无客户端 SSL VPN 用户名和密码。

限制

- 无客户端 SSL VPN 支持本地打印，但不支持通过 VPN 连接到公司网络上的打印机进行打印。

使用无客户端 SSL VPN 浮动工具栏

浮动工具栏可简化无客户端 SSL VPN 的使用。此工具栏允许您输入 URL、浏览文件位置以及选择预配置的网络连接，而不会干扰主浏览器窗口。

浮动工具栏显示当前无客户端 SSL VPN 会话。如果点击 **Close** 按钮， ASA 会提示您关闭无客户端 SSL VPN 会话。

提示　要将文本粘贴到文本字段，请使用 **Ctrl-V**。（对于在无客户端 SSL VPN 会话期间显示的工具栏，右键单击操作不可用。）

限制

如果将浏览器配置为阻止弹出窗口，则无法显示浮动工具栏。

浏览网络

使用无客户端 SSL VPN 并不能保证与每个站点的通信都是安全的。请参阅传达安全提示。

使用无客户端 SSL VPN 进行网络浏览时，用户可能会体验到不同于以往的外观和感受。例如：

- 无客户端 SSL VPN 的标题栏显示在每个网页的上方。
- 您可以通过以下方式访问网站：
  - 在无客户端 SSL VPN 主页的 **Enter Web Address** 字段中输入 URL
  - 点击无客户端 SSL VPN 主页上的预配置网站链接
  - 点击通过上述两种方法之一访问的网页上的链接

此外，根据您配置特定帐户的方式，可能存在以下情况：

- 某些网站被阻止
- 只有在无客户端 SSL VPN 主页上显示为链接的网站可用

先决条件

需要有受保护网站的用户名和密码。

限制

此外，根据您配置特定帐户的方式，可能存在以下情况：

- 某些网站被阻止
- 只有在无客户端 SSL VPN 主页上显示为链接的网站可用

浏览网络 （文件管理）

用户可能并不熟悉如何在您的组织网络中查找他们的文件。

注　在复制过程中，请勿中断 **Copy File to Server** 命令或导航至其他屏幕。中断操作可能会导致在服务器上保存的文件不完整。

先决条件

- 必须配置共享远程访问的文件权限。
- 必须有受保护文件服务器的服务器名称和密码。
- 必须有文件夹和文件所在的域、工作组和服务器的名称。

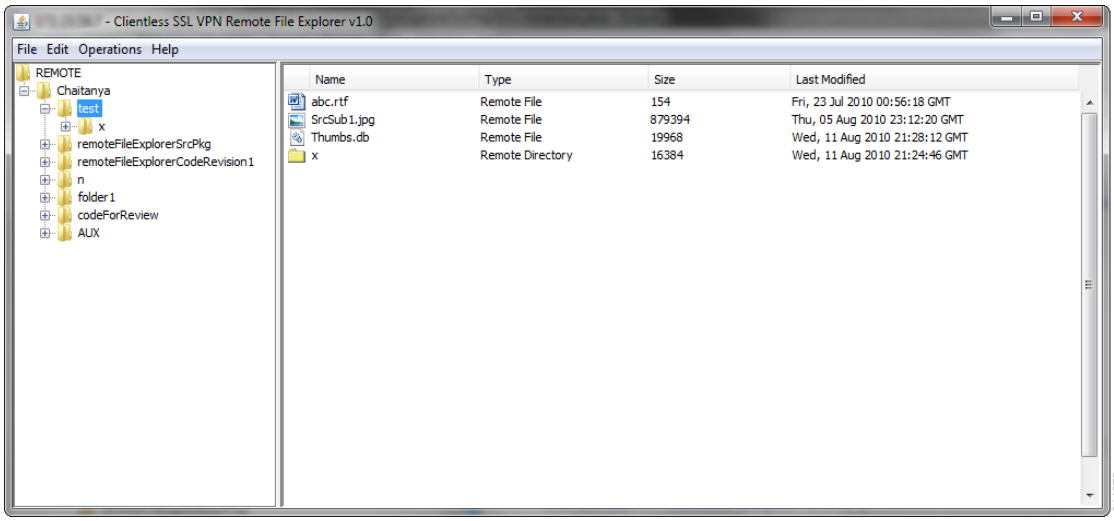
限制

仅共享文件夹和文件可通过无客户端 SSL VPN 进行访问。

使用 Remote File Explorer

有了 Remote File Explorer，用户可以从网络浏览器浏览公司网络。用户点击思科 SSL VPN 门户页面上的 Remote File System 图标时，用户系统上会启动一个小程序，在文件夹树视图中显示远程文件系统。

图 18-7　　无客户端 SSL VPN Remote File Explorer



此浏览器使用户可以：

- 浏览远程文件系统。
- 重命名文件。
- 移动或复制远程文件系统中以及远程文件系统与本地文件系统之间的文件。
- 执行文件批量上传和下载。

注　要使用此功能，用户计算机上需要安装 Oracle Java Runtime Environment (JRE) 1.4 或更高版本，还需要在网络浏览器中启用 Java。启动远程文件需要 JRE 1.6 或更高版本。

重命名文件或文件夹

要重命名文件或文件夹，请执行以下操作：

步骤 1　点击要重命名的文件或文件夹。

步骤 2　选择 **Edit > Rename**。

步骤 3　出现提示时，在对话框中输入新名称。

步骤 4　点击 **OK** 重命名文件或文件夹。或者，点击 **Cancel** 保留原来的名称。

移动或复制远程服务器上的文件或文件夹

要移动或复制远程服务器上的文件或文件夹，请执行以下操作：

步骤 1　导航至包含要移动或复制的文件或文件夹的源文件夹。

步骤 2　点击所需的文件或文件夹。

步骤 3　如要复制文件，请选择 **Edit > Copy**。要移动文件，请选择 **Edit > Cut**。

步骤 4　导航至目标文件夹。

步骤 5　选择 **Edit > Paste**。

将文件从本地系统驱动器复制到远程文件夹

可以在本地文件系统与远程文件系统之间复制文件，方法是，在远程文件浏览器的右侧窗格与本地文件管理器应用之间拖放文件。

上传和下载文件

下载文件的具体操作如下：在浏览器中点击要下载的文件，选择 **Operations > Download**，然后在 **Save** 对话框中提供用于保存该文件的位置和名称。

上传文件的具体操作如下：在目标文件夹中点击要上传的文件，选择 **Operations > Upload**，然后在 **Open** 对话框中提供该文件的位置的名称。

此功能有以下限制：

- 用户不能查看他们无权访问的子文件夹。
- 不能移动或复制用户无权访问的文件，即使这些文件显示在浏览器中。
- 嵌套文件夹的最大深度为 32 级。
- 树视图不支持拖放复制。
- 在 Remote File Explorer 的多个实例之间移动文件时，所有实例必须浏览同一台服务器（根目录共享）。
- Remote File Explorer 在一个文件夹中最多可显示 1500 个文件和文件夹。如果文件夹数量超过这个限制，文件夹将无法显示。

使用端口转发

注　当用户结束使用应用时，始终应该通过点击 **Close** 图标关闭 Application Access 窗口。未能正确退出窗口可能会导致应用访问或应用本身关闭。有关详细信息，请参阅第 21-1 页上的使用 Application Access 时从 hosts 文件错误中恢复。

先决条件

- 在 Mac OS X 上，仅 Safari 浏览器支持此功能。
- 必须已安装客户端应用。
- 必须已在浏览器上启用了 Cookie。
- 如果使用 DNS 名称指定服务器，必须具有管理员权限，因为修改主机文件需要这一权限。
- 必须已安装 Oracle Java Runtime Environment (JRE) 1.4.x 和 1.5.x。

  如果未安装 JRE，系统将显示弹出窗口，指导用户浏览至提供此 JRE 的站点。极少数情况下，端口转发小程序将出现故障，显示 Java 异常错误。如果出现这种情况，请执行以下操作：

  a. 清除浏览器缓存并关闭浏览器。
  b. 确认计算机任务栏上没有任何 Java 图标。
  c. 结束 Java 的所有实例。
  d. 建立一个无客户端 SSL VPN 会话并启动端口转发 Java 小程序。
- 必须在浏览器上启用 JavaScript。默认情况下， JavaScript 已启用。
- 如有需要，必须配置客户端应用。

注　Microsoft Outlook 客户端不需要执行此配置步骤。所有非 Windows 客户端应用都要求此配置。要确定 Windows 应用是否需要进行配置，请检查 Remote Server 字段的值。如果 Remote Server 字段包含服务器主机名，不需要配置客户端应用。如果 Remote Server 字段包含 IP 地址，则必须配置客户端应用。

限制

由于此功能要求安装 Oracle Java Runtime Environment (JRE) 并配置配置本地客户端，而且，这样做需要具有本地系统的管理员权限或者对 C:\windows\System32\drivers\etc 的完全控制权，因此，用户从公共远程系统连接时将无法使用应用。

详细步骤

要配置客户端应用，请使用服务器的本地映射 IP 地址和端口号。要查找此信息，请执行以下操作：

1. 启动无客户端 SSL VPN 会话，并点击主页上的 **Application Access** 链接。系统将显示 Application Access 窗口。
2. 在 Name 列，找到要使用的服务器名称，然后确定其相应的客户端 IP 地址和端口号（在 Local 列）。
3. 使用该 IP 地址和端口号来配置客户端应用。配置步骤因各客户端应用而异。

注　点击通过无客户端 SSL VPN 会话运行的应用中的 URL（例如，邮件中的 URL）不会打开会话站点。要打开会话站点，请将 URL 粘贴到 Enter Clientless SSL VPN (URL) Address 字段中。

通过端口转发使用邮件

如要使用邮件，请从无客户端 SSL VPN 主页启动应用访问。这样即可使用邮件客户端。

注　如果在使用 IMAP 客户端时失去与邮件服务器之间的连接或者无法建立新的连接，请关闭 IMAP 应用并重新启动无客户端 SSL VPN。

先决条件

必须满足应用访问及其他邮件客户端的要求。

限制

我们测试了 Microsoft Outlook Express 5.5 和 6.0 版本。

无客户端 SSL VPN 应能够通过端口转发支持其他 SMTPS、 POP3S 或 IMAP4S 邮件程序 （例如 Lotus Notes 和 Eudora），但是我们尚未验证这一点。

通过网络访问使用邮件

支持以下邮件应用：

- 在 Exchange Server 2010 上运行的 Microsoft Outlook Web App。
  OWA 要求使用 Internet Explorer 7 或更高版本，或者 Firefox 3.01 或更高版本。
- Exchange Server 2007、 2003 和 2000 上运行的 Microsoft Outlook Web Access。
  为了获得最佳效果，请在 Internet Explorer 8.x 或更高版本或者 Firefox 8.x 上使用 OWA。
- Lotus iNotes

先决条件

必须已安装基于网络的邮件产品。

限制

应该也支持其他基于网络的邮件应用，但我们尚未验证这一点。

通过邮件代理使用邮件

支持以下旧版邮件应用：

- Microsoft Outlook 2000 和 2002
- Microsoft Outlook Express 5.5 和 6.0

有关邮件应用的说明和示例，请参阅第 15-12 页上的在无客户端 SSL VPN 上使用邮件。

先决条件

- 必须已安装支持 SSL 的邮件应用。
- 请勿将 ASA SSL 版本设置为仅 TLSv1。 Outlook 和 Outlook Express 不支持 TLS。
- 必须已正确配置邮件应用。

限制

应该也支持其他支持 SSL 的客户端，但我们尚未验证这一点。

使用智能隧道

使用智能隧道不需要具有管理权限。

注　与使用端口转发程序时不同，使用智能隧道时不会自动下载 Java。

先决条件

- 智能隧道要求 Windows 上必须安装 ActiveX 或 JRE （1.4x 和 1.5x），要求 Mac OS X 上必须安装 Java Web Start。
- 必须确保浏览器上已启用 Cookie。
- 必须确保浏览器上已启用 JavaScript。

限制

- Mac OS X 不支持前端代理。
- 仅支持第 16-3 页上的配置智能隧道访问中指定的操作系统和浏览器。
- 仅支持基于 TCP 套接字的应用。

第 19 章

将无客户端 SSL VPN 用于移动设备

2013 年 9 月 13 日

将无客户端 SSL VPN 用于移动设备

您可以从 Pocket PC 或其他已获认证的移动设备访问无客户端 SSL VPN。ASA 管理员和无客户端 SSL VPN 用户无需任何特殊操作即可将无客户端 SSL VPN 用于已获认证的移动设备。

思科已认证以下移动设备平台：

HP iPaq H4150

Pocket PC 2003

Windows CE 4.20.0，内部版本 14053

Pocket Internet Explorer (PIE)

ROM 版本 1.10.03ENG

ROM 日期：7/16/2004

移动设备版本的无客户端 SSL VPN 存在一些不同之处：

- 横幅网页代替了无客户端 SSL VPN 弹出窗口。
- 图标栏代替了标准无客户端 SSL VPN 浮动工具栏。此栏显示 Go、 Home 和 Logout 按钮。
- 无客户端 SSL VPN 门户主页上不包含 Show Toolbar 图标。
- 注销 SSL VPN 时，系统将显示警告消息，提供关于正确关闭 PIE 浏览器的说明。如果您不遵循这些说明并按照常规方式关闭浏览器窗口，PIE 将不断开无客户端 SSL VPN 或使用 HTTPS 的任何安全网站。

限制

- 无客户端 SSL VPN 支持 OWA 2000 和 OWA 2003 基本身份验证。如果在 OWA 服务器上未配置基本身份验证并且无客户端 SSL VPN 用户尝试访问该服务器，访问将被拒绝。
- 不支持的无客户端 SSL VPN 功能：
  - Application Access 和其他 Java 相关功能。
  - HTTP 代理。
  - Citrix Metaframe 功能 （如果 PDA 没有对应的 Citrix ICA 客户端软件）。

自定义无客户端 SSL VPN

无客户端 SSL VPN 最终用户设置

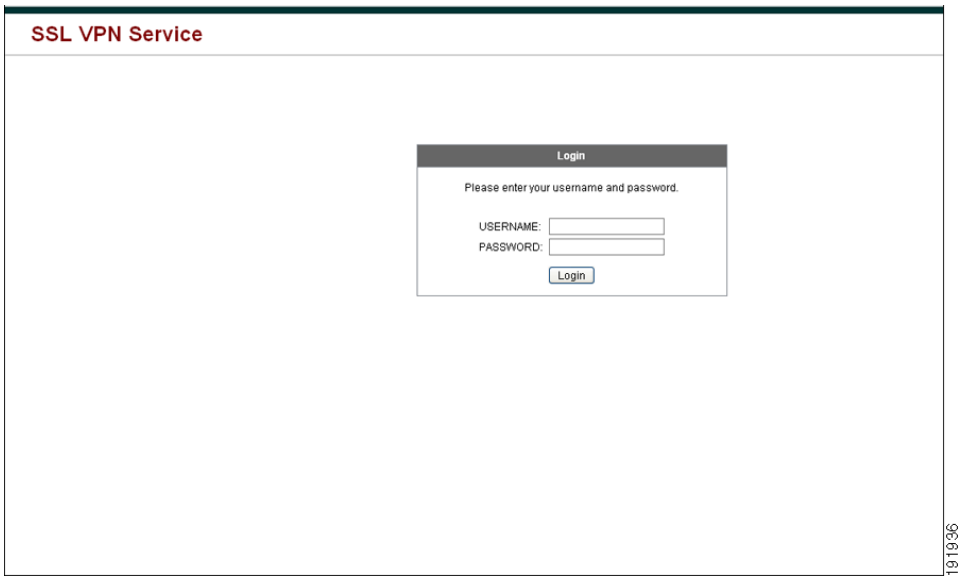
本节适用于为最终用户设置无客户端 SSL VPN 的系统管理员。它介绍了如何自定义最终用户界面。并总结了远程系统的配置要求和任务。此节将详细说明要让用户开始使用无客户端 SSL VPN 需要向他们传递的信息。包括下列主题：

- 定义最终用户界面
- 自定义无客户端 SSL VPN 页面
- 有关自定义的信息
- 导出自定义模板
- 编辑自定义模板

定义最终用户界面

无客户端 SSL VPN 最终用户界面包括一系列 HTML 面板。用户按照 https:// *地址*的形式输入 ASA 接口的 IP 地址即可登录无客户端 SSL VPN。显示的第一个面板是登录屏幕 （图 20-1）。

图 20-1　　无客户端 SSL VPN 登录屏幕



查看无客户端 SSL VPN 主页

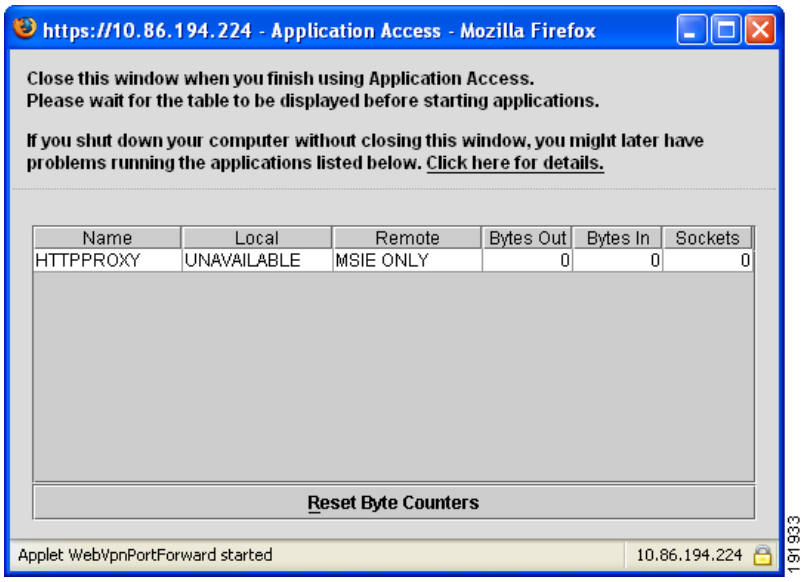
用户登录后，门户页面将会打开。

主页显示已配置的所有无客户端 SSL VPN 功能，其外观反映所选的徽标、文本和颜色。除了不能标识特定文件共享，此示例主页包括所有可用的无客户端 SSL VPN 功能。用户可以通过此主页浏览网络，输入 URL，访问特定网站，以及使用应用访问 （端口转发和智能隧道）来访问 TCP 应用。

查看无客户端 SSL VPN 应用访问面板

如要启动端口转发或智能隧道，用户可点击 Application Access 框中的 **Go** 按钮。 Application Access 窗口将会打开 （图 20-2）。

图 20-2　　无客户端 SSL VPN Application Access 窗口



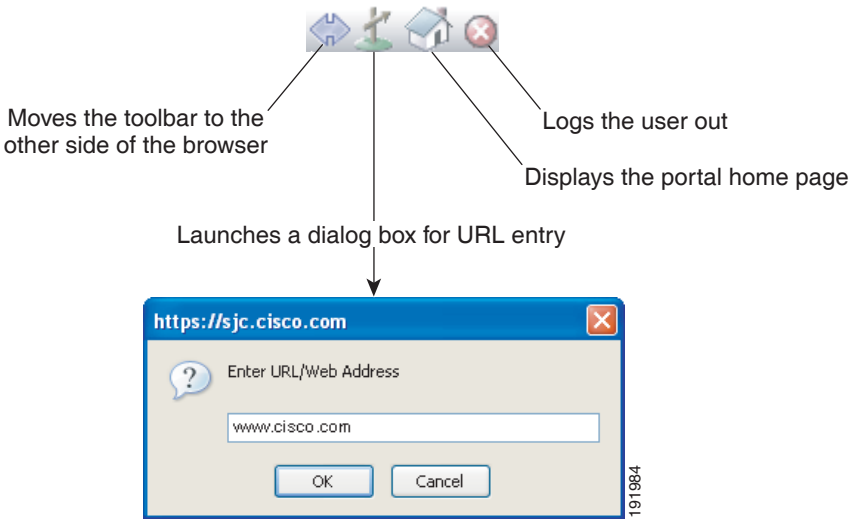
此窗口显示为此无客户端 SSL VPN 连接配置的 TCP 应用。如要在此面板打开的情况下使用某应用，用户可以按照正常方式启动该应用。

注　状态故障转移将不保留使用 Application Access 建立的会话。出现故障转移后，用户必须重新连接。

查看浮动工具栏

图 20-3 中显示的浮动工具栏显示当前无客户端 SSL VPN 会话。

图 20-3　　无客户端 SSL VPN 浮动工具栏



请注意浮动工具栏的以下特征：

- 此工具栏允许您输入 URL、浏览文件位置以及选择预配置的网络连接，而不会干扰主浏览器窗口。
- 如果将浏览器配置为阻止弹出窗口，则无法显示浮动工具栏。
- 如果关闭此工具栏， ASA 会提示您结束无客户端 SSL VPN 会话。

自定义无客户端 SSL VPN 页面

您可以更改向无客户端 SSL VPN 用户显示的门户页面的外观。这包括当用户连接至安全设备时向用户显示的登录页面、安全设备对用户进行身份验证之后向用户显示的主页、用户启动某个应用时显示的 Application Access 窗口以及用户注销无客户端 SSL VPN 会话时显示的注销页面。

自定义门户页面后，可以保存您的自定义配置并将其应用于特定连接配置文件、组策略或用户。直到您重新加载 ASA，或者关闭再重新启用无客户端 SSL 之后，更改才会生效。

您可以创建和保存很多自定义对象，让安全设备可以更改单个用户或用户组的门户页面的外观。

- 第 20-4 页上的有关自定义的信息
- 第 20-5 页上的导出自定义模板
- 第 20-5 页上的编辑自定义模板
- 第 20-11 页上的导入自定义对象
- 第 20-11 页上的将自定义配置应用于连接配置文件、组策略和用户
- 第 20-12 页上的登录屏幕高级自定义

有关自定义的信息

ASA 使用自定义对象定义用户屏幕的外观。自定义对象从包含 XML 标签的 XML 文件进行编译，其中 XML 标签适用于向远程用户显示的所有可自定义屏幕项。ASA 软件包含您可以导出到远程 PC 的自定义模板。您可以编辑此模板，然后将此模板重新导入 ASA，用做新的自定义对象。

导出自定义对象时，将在您指定的 URL 位置创建包含 XML 标签的 XML 文件。名称为 *Template* 的自定义对象创建的 XML 文件包含空 XML 标签，为创建新的自定义对象提供基础。无法从缓存中更改或删除此对象，但可以将其导出、编辑并重新导入回到 ASA 中，作为新的自定义对象。

自定义对象、连接配置文件和组策略

首先，当用户首次连接时，连接配置文件 （隧道组）中标识的默认自定义对象 （名称为 *DfltCustomization*）将确定登录屏幕的显示方式。如果已启用连接配置文件列表，并且用户选择有自己的不同自定义配置的组，此屏幕会改为反映该新组的自定义对象。

远程用户进行身份验证之后，屏幕外观取决于是否给组策略分配了自定义对象。

导出自定义模板

导出自定义对象时，将在您指定的 URL 位置创建一份 XML 文件。自定义模板 （名称为 *Template*）包含空 XML 标签，为创建新的自定义对象提供基础。无法从缓存中更改或删除此对象，但可以将其导出、编辑并重新导入回到 ASA 中，作为新的自定义对象。

详细步骤

	命令	用途
步骤 1	**export webvpn customization**	导出自定义对象并允许您对 XML 标签进行更改。
步骤 2	**import webvpn customization** **示例：** hostname# **export webvpn customization DfltCustomization tftp://209.165.200.225/dflt_custom** !!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to tftp://10.86.240.197/dflt_custom hostname#	导入文件，用做新的对象。 导出默认自定义对 (DfltCustomization) 并创建名称为 *dflt_custom* 的 XML 文件。

编辑自定义模板

本节显示自定义模板的内容并提供方便的图示，帮助您快速选择正确的 XML 标签和进行影响屏幕的更改。

您可以使用文本编辑器或 XML 编辑器编辑此 XML 文件。以下示例显示了自定义模板的 XML 标签。为了便于查看，某些冗余标签已删除。

示例：

```
<custom>
   <localization>
      <languages>en,ja,zh,ru,ua</languages>
      <default-language>en</default-language>
   </localization>
    <auth-page>
      <window>
          <title-text l10n="yes"><![CDATA[SSL VPN Service]]></title-text>
      </window>
      <full-customization>
          <mode>disable</mode>
          <url></url>
      </full-customization>
      <language-selector>
        <mode>disable</mode>
        <title l10n="yes">Language:</title>
        <language>
          <code>en</code>
          <text>English</text>
        </language>
        <language>
          <code>zh</code>
          <text>ä¸-å›½ (Chinese)</text>
        </language>
```

```
        <language>
          <code>ja</code>
          <text>æ-¥æœ¬ (Japanese)</text>
        </language>
        <language>
          <code>ru</code>
          <text>Ð ÑƒÑÑкий (Russian)</text>
        </language>
        <language>
          <code>ua</code>
          <text>Ð£ÐºÑ?ÐºÑ-Ð½ÑÑкий (Ukrainian)</text>
        </language>
      </language-selector>
      <logon-form>
          <title-text l10n="yes"><![CDATA[Login]]></title-text>
          <title-background-color><![CDATA[#666666]]></title-background-color>
          <title-font-color><![CDATA[#ffffff]]></title-font-color>
          <message-text l10n="yes"><![CDATA[Please enter your username and
password.]]></message-text>
          <username-prompt-text l10n="yes"><![CDATA[USERNAME:]]></username-prompt-text>
          <password-prompt-text l10n="yes"><![CDATA[PASSWORD:]]></password-prompt-text>
          <internal-password-prompt-text l10n="yes">Internal
Password:</internal-password-prompt-text>
          <internal-password-first>no</internal-password-first>
          <group-prompt-text l10n="yes"><![CDATA[GROUP:]]></group-prompt-text>
          <submit-button-text l10n="yes"><![CDATA[Login]]></submit-button-text>
          <title-font-color><![CDATA[#ffffff]]></title-font-color>
          <title-background-color><![CDATA[#666666]]></title-background-color>
          <font-color>#000000</font-color>
          <background-color>#ffffff</background-color>
          <border-color>#858A91</border-color>
      </logon-form>
      <logout-form>
          <title-text l10n="yes"><![CDATA[Logout]]></title-text>
          <message-text l10n="yes"><![CDATA[Goodbye.<br>

For your own security, please:<br>

<li>Clear the browser's cache

<li>Delete any downloaded files

<li>Close the browser's window]]></message-text>
          <login-button-text l10n="yes">Logon</login-button-text>
          <hide-login-button>no</hide-login-button>
          <title-background-color><![CDATA[#666666]]></title-background-color>
          <title-font-color><![CDATA[#ffffff]]></title-font-color>
          <title-font-color><![CDATA[#ffffff]]></title-font-color>
          <title-background-color><![CDATA[#666666]]></title-background-color>
          <font-color>#000000</font-color>
          <background-color>#ffffff</background-color>
          <border-color>#858A91</border-color>
      </logout-form>
      <title-panel>
         <mode>enable</mode>
         <text l10n="yes"><![CDATA[SSL VPN Service]]></text>
         <logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
         <gradient>yes</gradient>
         <style></style>
         <background-color><![CDATA[#ffffff]]></background-color>
         <font-size><![CDATA[larger]]></font-size>
         <font-color><![CDATA[#800000]]></font-color>
         <font-weight><![CDATA[bold]]></font-weight>
      </title-panel>
```

```
  <info-panel>
    <mode>disable</mode>
    <image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
    <image-position>above</image-position>
    <text l10n="yes"></text>
  </info-panel>
  <copyright-panel>
     <mode>disable</mode>
     <text l10n="yes"></text>
  </copyright-panel>
</auth-page>
<portal>
  <title-panel>
     <mode>enable</mode>
     <text l10n="yes"><![CDATA[SSL VPN Service]]></text>
     <logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
     <gradient>yes</gradient>
     <style></style>
     <background-color><![CDATA[#ffffff]]></background-color>
     <font-size><![CDATA[larger]]></font-size>
     <font-color><![CDATA[#800000]]></font-color>
     <font-weight><![CDATA[bold]]></font-weight>
  </title-panel>
  <browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
  <access-network-title l10n="yes">Start AnyConnect</access-network-title>
  <application>
     <mode>enable</mode>
     <id>home</id>
     <tab-title l10n="yes">Home</tab-title>
     <order>1</order>
  </application>
  <application>
     <mode>enable</mode>
     <id>web-access</id>
     <tab-title l10n="yes"><![CDATA[Web Applications]]></tab-title>
     <url-list-title l10n="yes"><![CDATA[Web Bookmarks]]></url-list-title>
     <order>2</order>
  </application>
  <application>
     <mode>enable</mode>
     <id>file-access</id>
     <tab-title l10n="yes"><![CDATA[Browse Networks]]></tab-title>
     <url-list-title l10n="yes"><![CDATA[File Folder Bookmarks]]></url-list-title>
     <order>3</order>
  </application>
  <application>
     <mode>enable</mode>
     <id>app-access</id>
     <tab-title l10n="yes"><![CDATA[Application Access]]></tab-title>
     <order>4</order>
  </application>
  <application>
     <mode>enable</mode>
     <id>net-access</id>
     <tab-title l10n="yes">AnyConnect</tab-title>
     <order>4</order>
  </application>
  <application>
     <mode>enable</mode>
     <id>help</id>
     <tab-title l10n="yes">Help</tab-title>
     <order>1000000</order>
  </application>
  <toolbar>
```

```
            <mode>enable</mode>
            <logout-prompt-text l10n="yes">Logout</logout-prompt-text>
            <prompt-box-title l10n="yes">Address</prompt-box-title>
            <browse-button-text l10n="yes">Browse</browse-button-text>
         </toolbar>
         <column>
            <width>100%</width>
            <order>1</order>
         </column>
         <pane>
            <type>TEXT</type>
            <mode>disable</mode>
            <title></title>
            <text></text>
            <notitle></notitle>
            <column></column>
            <row></row>
            <height></height>
         </pane>
         <pane>
            <type>IMAGE</type>
            <mode>disable</mode>
            <title></title>
            <url l10n="yes"></url>
            <notitle></notitle>
            <column></column>
            <row></row>
            <height></height>
         </pane>
         <pane>
            <type>HTML</type>
            <mode>disable</mode>
            <title></title>
            <url l10n="yes"></url>
            <notitle></notitle>
            <column></column>
            <row></row>
            <height></height>
         </pane>
         <pane>
            <type>RSS</type>
            <mode>disable</mode>
            <title></title>
            <url l10n="yes"></url>
            <notitle></notitle>
            <column></column>
            <row></row>
            <height></height>
         </pane>
         <url-lists>
            <mode>group</mode>
         </url-lists>
         <home-page>
            <mode>standard</mode>
            <url></url>
         </home-page>
      </portal>
   </custom>
```

图 20-4 显示了登录页面及其自定义 XML 标签。所有这些标签都嵌套于更高级别的标签 <auth-page> 中。

图 20-4　　登录页面和关联的 XML 标签

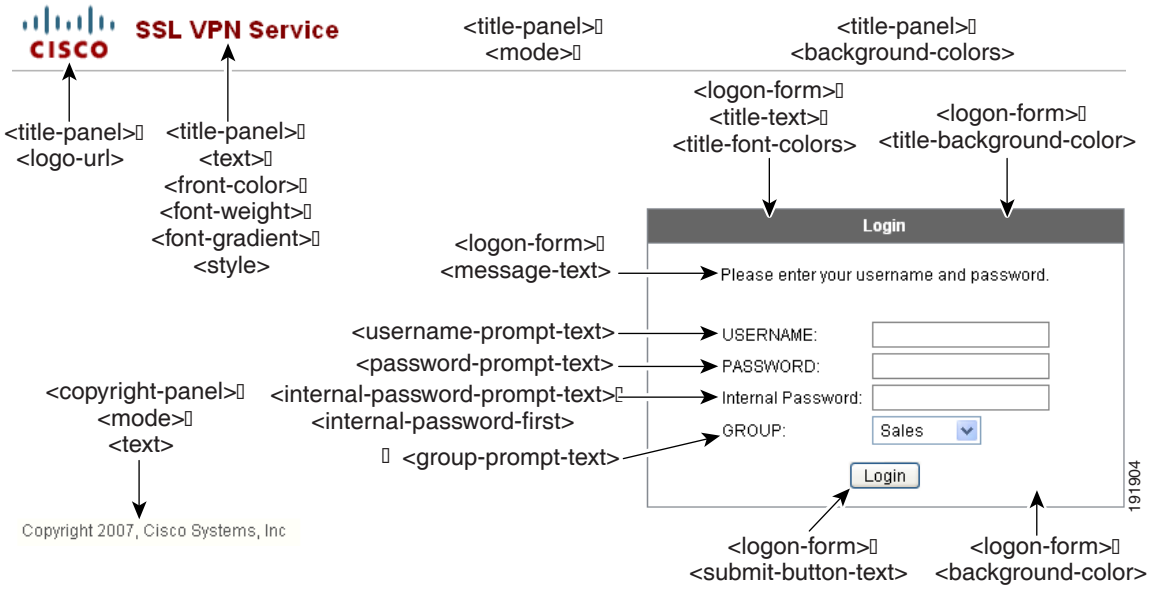


图 20-5 显示了在登录页面上可用的语言选择器下拉列表以及用于自定义此功能的 XML 标签。所有这些标签都嵌套于更高级别的 <auth-page> 标签中。

图 20-5　　登录屏幕上的语言选择器和关联的 XML 标签

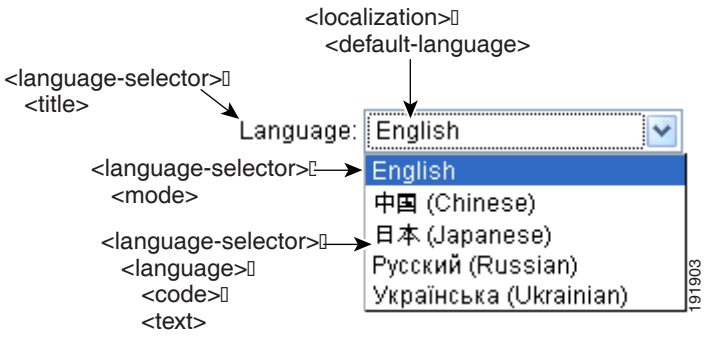


图 20-6 显示了在登录页面上可用的信息面板以及用于自定义此功能的 XML 标签。此信息可显示在登录框的左侧或右侧。这些标签都嵌套于更高级别的 <auth-page> 标签中。

图 20-6　　登录屏幕上的信息面板和关联的 XML 标签

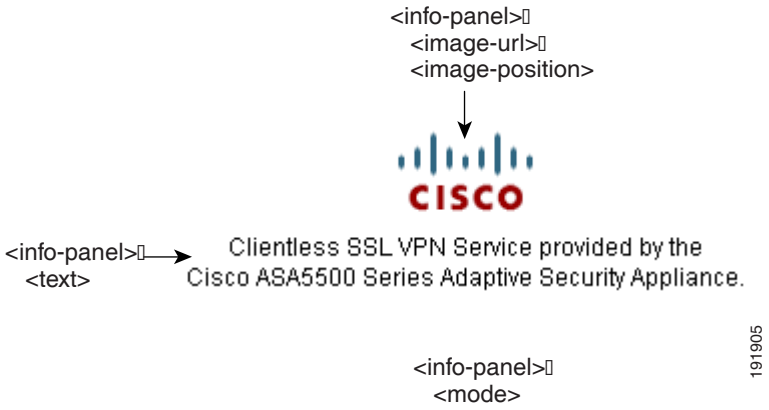
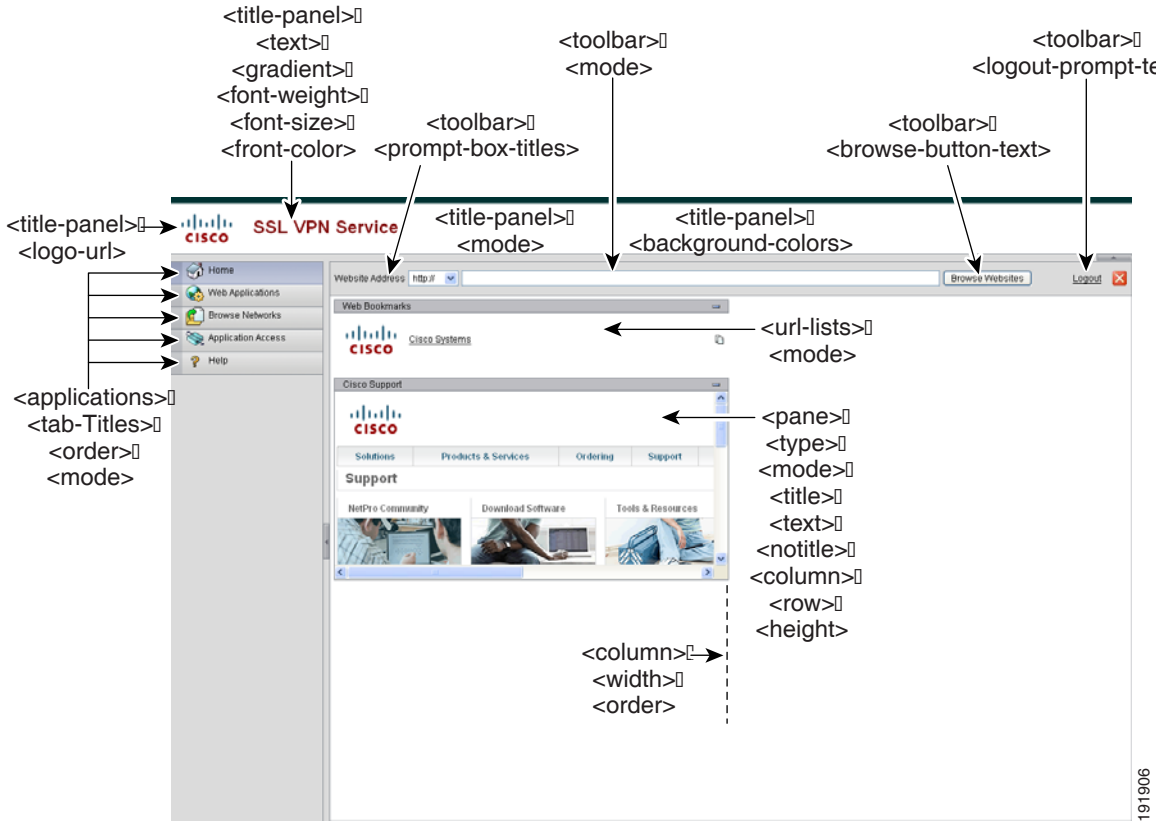


图 20-7 显示了门户页面以及自定义此功能的 XML 标签。这些标签都嵌套于更高级别的 <auth-page> 标签中。

图 20-7　　门户页面和关联的 XML 标签



导入自定义对象

编辑和保存 XML 文件后，使用以下命令将其导入到 ASA 的缓存中：

详细步骤

	命令	用途
步骤 1	`import webvpn customization`	将 XML 文件导入到 ASA 的缓存中。当您导入自定义对象时， ASA 将检查 XML 代码的有效性。如果代码有效，则 ASA 会将此对象存储在缓存中的某个隐藏位置。

	示例：
	`hostname# import webvpn customization custom1 tftp://209.165.201.22/customization /General.xml`
	`Accessing tftp://209.165.201.22/customization/General.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`Writing file disk0:/csco_config/97/custom1...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`329994 bytes copied in 5.350 secs (65998 bytes/sec)`
		从 URL 209.165.201.22/customization 导入自定义对象 *General.xml*，并将其命名为 *custom1*。

将自定义配置应用于连接配置文件、组策略和用户

创建自定义配置后，可以使用 **Customization** 命令将此自定义配置应用于连接配置文件 （隧道组）、一个组或用户。此命令显示的选项根据所处的模式而不同。

注 自定义门户页面后，直到您重新加载 ASA 或者禁用然后再启用无客户端 SSL，更改才生效。

有关配置连接配置文件、组策略和用户的详细信息，请参阅 《思科 ASA 系列 VPN CLI 配置指南》中的 “连接配置文件组、策略和用户”章节。

详细步骤

	命令	用途
步骤 1	`webvpn`	切换至无客户端 SSL VPN 配置模式。

步骤 2	`tunnel-group webvpn`
	或
	`group-policy webvpn`
	或
	`username webvpn`
		切换至 tunnel-group 无客户端 SSL VPN 配置模式。
		切换至组策略无客户端 SSL VPN 配置。
		切换至用户名无客户端 SSL VPN 配置。

	命令	用途

步骤 3	**自定义*名称***
	
	示例：
	`hostname(config)# tunnel-group cisco_telecommuters webvpn-attributes`
	`hostname(tunnel-group-webvpn)# customization cisco`
	
	或
	
	customization {none | value *name*}
	
	示例：
	`hostname(config)# group-policy cisco_sales attributes`
	`hostname(config-group-policy)# webvpn`
	`hostname(config-username-webvpn)# customization value ?`
	`config-username-webvpn 模式命令 / 选项：`
	`可用的已配置自定义配置文件：`
	`DfltCustomization`
	`cisco`
	`hostname(config-group-webvpn)# customization value cisco`
	
	示例：
	`hostname(config)# username cisco_employee attributes`
	`hostname(config-username)# webvpn`
	`hostname(config-username-webvpn)# customization value cisco`
		将自定义配置应用于连接配置文件。名称和要应用到连接配置文件上的自定义配置的名称相同。
		
		进入隧道组无客户端 SSL VPN 配置模式并为连接配置文件 *cisco_telecommutes* 启用自定义 *cisco*。
		
		将自定义配置应用于组或用户。可提供以下选项：
		• **none** 禁用组或用户的自定义，以防值被继承，并显示默认的无客户端 SSL VPN 页面。
		• **value** *name* 是 cu 的名称
		
		进入组策略无客户端 SSL VPN 配置模式，查询安全设备是否有一份自定义列表并为该组策略 *cisco_sales* 启用自定义 *cisco*。
		
		进入用户名无客户端 SSL VPN 配置模式并为用户 *cisco_employee* 启用自定义配置 *cisco*。

步骤 4	（可选）
	`[no] customization name`
	
	或
	`[no] customization {none | value name}`
		从配置中删除命令并从连接配置文件中删除某自定义配置。
		
		从配置中删除命令并还原为默认配置。

步骤 5	**customization** command followed by a question mark (?)	显示现有自定义配置列表。

登录屏幕高级自定义

如果您希望使用自己的自定义登录屏幕，而不是更改我们所提供的登录页面的特定屏幕元素，您可以使用 “*完全自定义*”功能执行这种高级自定义。

利用 “完全自定义”功能，您可以为您自己的登录屏幕提供 HTML 并插入调用 ASA 上创建登录表单和语言选择器下拉列表的函数的思科 HTML 代码。

本节描述您需要对您的 HTML 代码所做的修改和配置 ASA 使用您的代码所需完成的任务。

图 20-8 显示了向无客户端 SSL VPN 用户显示的标准思科登录屏幕。登录表单由 HTML 代码调用的函数显示。

图 20-8　　标准思科登录页面

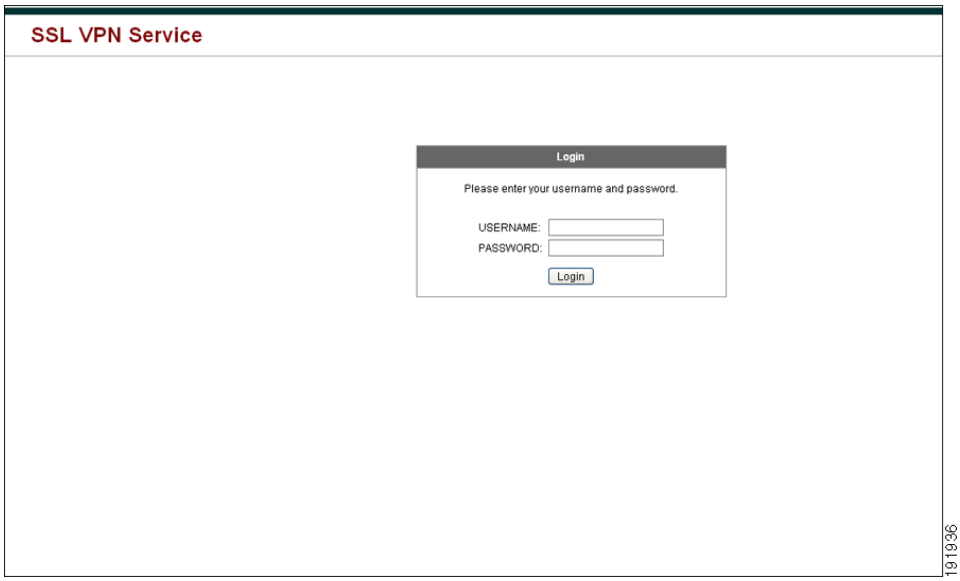
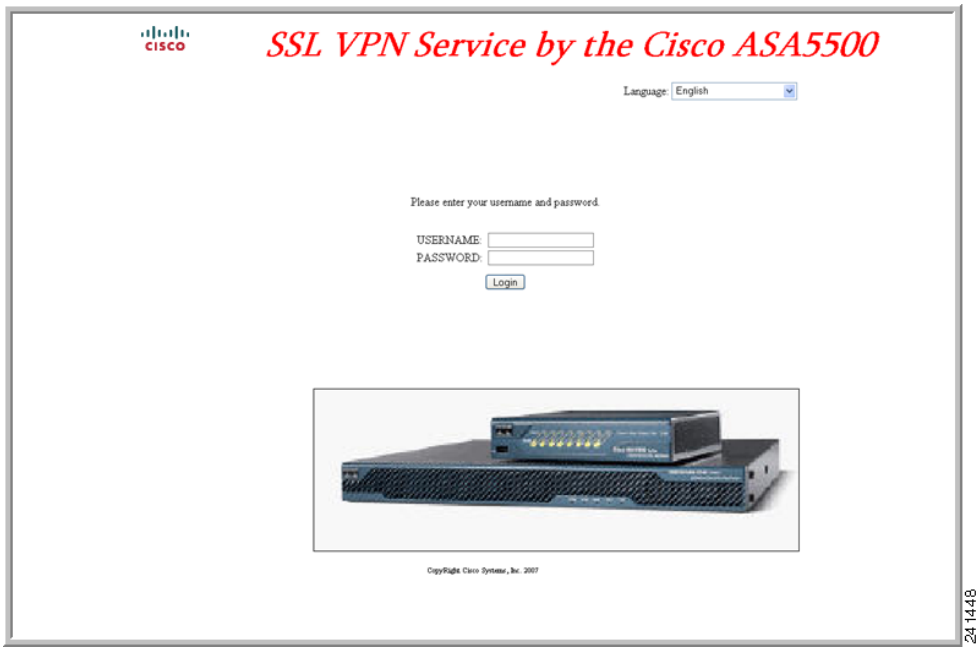


图 20-9 显示了语言选择器下拉列表。此功能是无客户端 SSL VPN 用户的一个选项，也是由登录屏幕的 HTML 代码中的函数调用。

图 20-9　　语言选择器下拉列表

图 20-10 显示了 “完全自定义”功能启用的一个简单的自定义登录屏幕示例。

图 20-10　　登录屏幕的完全自定义示例



以下 HTML 代码是一个示例，也是系统显示的代码：

示例：

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>New Page 3</title>
<base target="_self">
</head>

<p align="center">
<img border="0" src="/+CSCOU+/cisco_logo.jpg" width="188" height="48"><font face="Snap
ITC" size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7"> </font><i><b><font
color="#FF0000" size="7" face="Sylfaen"> SSL VPN Service by the Cisco
ASA5500</font></b></i></p>

    <body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

    <table>

    <tr><td colspan=3 height=20 align=right><div id="selector" style="width:
    300px"></div></td></tr>
    <tr><td></td><td></td><td></td></tr>
    <tr>
    <td height="379"></td>
    <td height="379"></td>
    <td align=middle valign=middle>
    <div id=lform >
    <p> </p>
    <p> </p>
```

```
<p> </p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>

</table>
```

这种缩进的代码将在屏幕上注入登录表单和语言选择器。函数 **csco_ShowLoginForm('lform')** 注入登录表单。 **csco_ShowLanguageSelector('selector')** 注入语言选择器。

修改您的 HTML 文件

详细步骤

步骤 1　将您的文件命名为 **logon.inc**。当您导入文件时， ASA 将此文件名识别为登录屏幕。

步骤 2　修改该文件使用的映像的路径以包含 **/+CSCOU+/**。

在身份验证之前向远程用户显示的文件必须放在 ASA 缓存的特定区域，以路径 /+CSCOU+/ 表示。因此，该文件中每个映像的源都必须包含此路径。例如：

```
src=" /+CSCOU+/asa5520.gif"
```

步骤 3　插入下面的特殊 HTML 代码。此代码包含之前描述的在屏幕上注入登录表单和语言选择器的思科函数。

```
<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>

</table>
```

自定义书签帮助

ASA 为选择的每个书签在应用面板上显示帮助内容。您可以自定义这些帮助文件或创建其他语言的帮助文件。然后将其导入到闪存中，以便在后续会话期间显示这些帮助文件。您还可以检索之前导入的帮助内容文件、修改这些文件，然后将其重新导入到闪存中。

每个应用面板都用预定的文件名显示其自己的帮助文件内容。每个文件的预期位置在 ASA 的闪存内的 /+CSCOE+/help/*language*/ URL 中。表 20-1 显示了您可以为 VPN 会话保留的每个帮助文件的详细信息。

表 20-1　　VPN 应用帮助文件

应用类型	面板	安全设备闪存中帮助文件的 URL	思科是否提供了英文版的帮助文件？
标准	Application Access	/+CSCOE+/help/*language*/app-access-hlp.inc	是
标准	Browse Networks	/+CSCOE+/help/*language*/file-access-hlp.inc	是
标准	AnyConnect Client	/+CSCOE+/help/*language*/net-access-hlp.inc	是
标准	使用邮件	/+CSCOE+/help/*language*/web-access-hlp.inc	是
插件	MetaFrame Access	/+CSCOE+/help/*language*/ica-hlp.inc	否
插件	Terminal Servers	/+CSCOE+/help/*language*/rdp-hlp.inc	是
插件	Telnet/SSH Servers	/+CSCOE+/help/*language*/ssh,telnet-hlp.inc	是
插件	VNC Connections	/+CSCOE+/help/*language*/vnc-hlp.inc	是

language 指浏览器呈现的语言的缩写。此字段*不*是用于文件转换，而是指示文件中使用的语言。要指定特定语言代码，请从您的浏览器呈现的语言列表复制语言缩写。例如，当您使用下列步骤之一时，对话框窗口将显示语言和相关语言代码：

- 打开 Internet Explorer，选择**工具 > Internet 选项 > 语言 > 添加**。
- 打开 Mozilla Firefox，选择**工具 > 选项 > 高级 > 常规**，点击语言旁边的**选择**，然后点击**选择要添加的语言**。

以下各节介绍了如何自定义帮助内容：

- 第 20-16 页上的自定义思科提供的帮助文件
- 第 20-17 页上的为思科未提供的语言创建帮助文件
- 第 20-18 页上的将帮助文件导入到闪存
- 第 20-18 页上的从闪存中导出以前导入的帮助文件

自定义思科提供的帮助文件

如要自定义思科提供的帮助文件，您首先需要从闪存卡上获取该文件的副本。获取副本并按照如下步骤进行自定义：

详细步骤

步骤 1　使用浏览器与 ASA 建立一个无客户端 SSL VPN 会话。

步骤 2　通过将表 20-1 中 “安全设备闪存中的帮助文件的 URL”中的字符串追加到 ASA 的地址中，然后按 Enter，以显示帮助文件。

注　输入 **en** 替换 *language*，获取英文版帮助文件。

以下地址示例显示了 Terminal Servers 帮助的英文版本：

https://*address_of_security_appliance***/+CSCOE+/help/en/rdp-hlp.inc**

步骤 3　选择 **File > Save (Page) As**。

注　请勿更改 File name 框中的内容。

步骤 4　将 Save as 类型选项改为 **Web Page, HTML only**，然后点击 **Save**。

步骤 5　用您的首选 HTML 编辑器修改此文件。

注　您可以使用大多数 HTML 标签，但是 *请勿* 使用定义文件及其结构的标签。例如，请勿使用 <html>、 <title>、 <body>、 <head>、 <h1> 或 <h2>。您可以使用 <b> 等字符标签和 <p>、 、 以及 <li> 标签来构造内容。

步骤 6　使用原始文件名和扩展名，将文件保存为仅 HTML。

步骤 7　确保文件名与表 20-1 中的文件名匹配并且没有多余的文件名扩展名。

为思科未提供的语言创建帮助文件

使用 HTML 以其他语言创建帮助文件。

建议为支持的每个语言创建单独的文件夹。

将文件另存为仅 HTML。使用表 20-1 中 “安全设备闪存中帮助文件的 URL”最后一个斜线后面的文件名。

请参阅下一节，导入要在 VPN 会话期间显示的文件。

限制

您可以使用大多数 HTML 标签，但是 *请勿* 使用定义文件及其结构的标签，例如，请勿使用 <html>、 <title>、 <body>、 <head>、 <h1> 或 <h2>。您可以使用 <b> 等字符标签和 <p>、 、 以及 <li> 标签来构造内容。

将帮助文件导入到闪存

详细步骤

	命令	用途
步骤 1	**import webvpn webcontent** *destination_url source_url* **示例：** hostname# **import webvpn webcontent** **/+CSCOE+/help/en/app-access-hlp.inc** **tftp://209.165.200.225/app-access-hlp.inc**	将帮助文件导入到闪存中，以便在无客户端 SSL VPN 会话期间显示此帮助文件。 • destination_url 是表 20-1VPN 应用帮助文件中“安全设备闪存中帮助文件的 URL”列中的字符串。 • *source_url* 是要导入的文件的 URL。有效前缀是 ftp://、 http:// 和 tftp://。 将帮助文件 *app-access-hlp.inc* 从地址为 209.165.200.225 的 TFTP 服务器复制到闪存中。此 URL 包含英语的缩写 *en*。

从闪存中导出以前导入的帮助文件

详细步骤

	命令	用途
步骤 1	**export webvpn webcontent** *source_url destination_url* **示例：** hostname# **export webvpn webcontent** **/+CSCOE+/help/en/file-access-hlp.inc** **tftp://209.165.200.225/file-access-hlp.inc**	检索以前导入的帮助内容文件，随后进行编辑。 • *source_url* 是表 20-1 中“安全设备闪存中帮助文件的 URL”中的字符串。 • *destination_url* 是**目标 URL**。有效前缀是 ftp:// 和 tftp://。最大字符数为 255。 将 Browser Networks 面板上显示的英语帮助文件 *file-access-hlp.inc* 复制到 TFTP 服务器 209.165.200.225。

用户消息的语言转换

ASA 为整个无客户端 SSL VPN 会话提供语言转换。这包括登录、注销横幅以及在身份验证之后显示的插件和 AnyConnect 等门户页面。

本节介绍了如何配置 ASA 以对这些用户消息进行语言转换。

了解语言转换

向远程用户显示的功能区域及其消息归入转换域。表 20-2 显示了转换域和转换的功能区域。

表 20-2　语言转换域选项

转换域	转换的功能区域
AnyConnect	在思科 AnyConnect VPN 客户端的用户界面上显示的消息。
banners	无客户端连接的 VPN 访问被拒绝时显示的消息。
CSD	思科安全桌面 (CSD) 的消息。
customization	登录和注销页面与门户页面上显示的消息以及用户可自定义的所有消息。
plugin-ica	Citrix 插件的消息。
plugin-rdp	远程桌面协议插件的消息。
plugin-rdp2	Java 远程桌面协议插件的消息。
plugin-telnet,ssh	Telnet 和 SSH 插件的消息。
plugin-vnc	VNC 插件的消息。
PortForwarder	向端口转发用户显示的消息。
url-list	用户为门户页面上的 URL 书签指定的文本。
webvpn	不可自定义的所有第 7 层、 AAA 和门户消息。

ASA 包括每个域属于标准功能组成部分的转换表模板。插件的模板随附于插件中并定义其自己的转换域。

您可以导出转换域的模板，在您提供的 URL 位置创建模板的 XML 文件。此文件中该消息字段为空。您可以编辑消息并导入模板，创建位于闪存中的新转换表对象。

您还可以导出现有转换表。创建的 XML 文件将显示您之前编辑的消息。重新导入具有相同语言名称的此 XML 文件将创建一个新版的转换表对象，并覆盖以前的消息。

有些模板是静态的，而有些模板则根据 ASA 的配置而变化。因为您可以自定义无客户端用户的 *登录与注销页面，门户页面和 URL 书签*，**ASA 将动态生成 customization** 和 **url-list** 转换域模板，并且此模板将动态地反映您对这些功能区域的更改。

创建转换表后，就可用于您创建并应用于组策略或用户属性的自定义对象。除 AnyConnect 转换域外，转换表没有任何影响，消息不会在用户屏幕上转换，直到您创建自定义对象，确定该对象要使用的转换表，并指定将该自定义对象应用于组策略或用户。对 AnyConnect 域的转换表的更改会立即向 AnyConnect 客户端用户显示。

创建转换表

在单情景模式和多情景模式下您都可以创建转换表：

详细步骤

	命令	用途
步骤 1	**导出 webvpn 转换表** **示例：** hostname# **show import webvpn translation-table** 转换表的模板： customization AnyConnect CSD PortForwarder url-list webvpn Citrix-plugin RPC-plugin Telnet-SSH-plugin VNC-plugin 转换表： **示例：** hostname# **export webvpn translation-table customization template tftp://209.165.200.225/portal**	将转换表模板导出到计算机上。 显示可用的转换表模板和表。 为自定义域导出转换表模板，这会影响向无客户端 SSL VPN 会话中为用户显示的消息。创建的 XML 文件的文件名为 *portal*（用户指定）并包含空消息字段。

	命令	用途

步骤 2	编辑转换表 XML 文件
	
	示例：
	`# Copyright (C) 2006 by Cisco Systems, Inc.`
	`#`
	`#, fuzzy`
	`msgid ""`
	`msgstr ""`
	`"Project-Id-Version: ASA\n"`
	`"Report-Msgid-Bugs-To: vkamyshe@cisco.com\n"`
	`"POT-Creation-Date: 2007-03-12 18:57 GMT\n"`
	`"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"`
	`"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"`
	`"Language-Team: LANGUAGE <LL@li.org>\n"`
	`"MIME-Version: 1.0\n"`
	`"Content-Type: text/plain; charset=UTF-8\n"`
	`"Content-Transfer-Encoding: 8bit\n"`
	
	`#: DfltCustomization:24 DfltCustomization:64`
	`msgid "Clientless SSL VPN Service"`
	`msgstr ""`
		显示一个导出为 *portal* 的模板的一部分。此输出内容的末尾包含用户建立无客户端 SSL VPN 会话时在门户页面上显示的消息的消息 ID 字段 (msgid) 和消息字符串字段 (msgstr)。完整的模板包含多对消息字段。

步骤 3	**import webvpn translation-table**
	
	示例：
	`hostname# import webvpn translation-table customization language es-us tftp://209.165.200.225/portal`
	`hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`hostname# show import webvpn translation-table`
	转换表的模板：
	`AnyConnect`
	`PortForwarder`
	`csd`
	`customization`
	`keepout`
	`url-list`
	`webvpn`
	`Citrix-plugin`
	`RPC-plugin`
	`Telnet-SSH-plugin`
	`VNC-plugin`
	
	转换表：
	`es-us customization`
		导入转换表。
		
		导入 XML 文件。 *es-us* 是美式西班牙语的缩写。

如果您导入 AnyConnect 域的转换表，您的更改会立即生效。如果您导入任何其他域的转换表，您必须创建自定义对象、确定在该对象中使用该转化表并为组策略或用户指定该自定义对象。

在自定义对象中引用语言

本节介绍如何导出自定义模板、编辑并将其导入为自定义对象，使您可以引用它。

先决条件

为了让自定义对象正确调用转换表，必须先使用相同的名称导入转换表。这些名称必须与浏览器的语言选项兼容。

详细步骤

	命令	功能
步骤 1	**export webvpn customization template** **示例：** hostname# **export webvpn customization template tftp://209.165.200.225/sales**	将自定义模板导出至您可以编辑它的 URL。 导出模板并在指定的 URL 位置创建 *sales* 的副本。
步骤 2	编辑自定义模板并引用以前导入的转换表 **示例：** <localization> <languages>en,ja,zh,ru,ua</languages> <default-language>en</default-language> </localization> **示例：** <auth-page> .... <language-selector> <mode>enable</mode> <title l10n="yes">Language:</title> <language> <code>en</code> <text>English</text> </language> <language> <code>es-us</code> <text>Spanish</text> </language> </language-selector>	自定义模板中 XML 代码的两个区域与转换表相关。 指定要使用的转换表。 • XML 代码中的 <languages> 标签后面紧接转换表的名称。在本例中，它们是 en、 ja、 zh、 ru 和 ua。 • <default-language> 标签指定远程用户连接至 ASA 时首次看到的语言。在以上示例代码中，语言为英文。 影响语言选择器的显示并且包含启用和自定义语言选择器的 <language selector> 标签和关联的 <language> 标签： • <language-selector> 标签组包含启用和禁用语言选择器的显示的 <mode> 标签以及指定列示语言的下拉框标题的 <title> 标签。 • <language> 标签组包括将语言选择器下拉框中显示的语言名称映射到指定转换表的 <code> 和 <text> 标签中。
步骤 3	做出更改后，请保存文件。	

	命令	功能
步骤 4	**import webvpn customization** **示例：** hostname# **import webvpn customization sales tftp://209.165.200.225/sales** hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!	导入自定义模板，用做新的对象。
步骤 5	**show import webvpn customization** **示例：** hostname# **import webvpn customization sales tftp://209.165.200.225/sales** hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!	显示新的自定义对象 *sales*。

更改组策略或用户属性以使用自定义对象

本节介绍如何为特定组或用户激活您的更改。

详细步骤

	命令	用途
步骤 1	**webvpn**	切换至无客户端 SSL VPN 配置模式。
步骤 2	**group-policy webvpn**	切换至组策略无客户端 SSL VPN 配置模式。
步骤 3	**customization** **示例：** hostname(config)# **group-policy sales attributes** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **customization value sales**	启用自定义对象。 显示在组策略 *sales* 中启用的自定义对象 *sales*。

无客户端 SSL VPN 故障排除

2014 年 4 月 14 日

关闭 Application Access 以防 hosts 文件错误

为防止出现可能会干扰 Application Access 的 hosts 文件错误，使用完 Application Access 之后请正确关闭 Application Access 窗口。为此，请点击关闭图标。

使用 Application Access 时从 hosts 文件错误中恢复

如未正确关闭 Application Access 窗口，可能会出现以下错误：

- 您下一次尝试启动 Application Access 时，它可能会关闭；您会收到 `Backup HOSTS File Found` 错误消息。
- 即使您在本地位置运行应用程序，这些应用程序也可能会关闭或出现故障。

不正确停止 Application Access 可能会导致这些错误。例如：

- 当您使用 Application Access 时，您的浏览器会崩溃。
- 当您使用 Application Access 时，电源会中断或系统会关闭。
- 您在工作时可以将 Application Access 窗口最小化，然后在此窗口处于活动状态（但是已最小化）的情况下关闭您的计算机。

- 了解 hosts 文件
- 错误停止 Application Access
- 使用无客户端 SSL VPN 自动重新配置主机的文件
- 手动重新配置 hosts 文件

了解 hosts 文件

您本地系统上的 hosts 文件会将 IP 地址映射到主机名上。当您启动 Application Access 时，无客户端 SSL VPN 将修改 hosts 文件，增加无客户端 SSL VPN 特定条目。通过正确关闭 Application Access 来停止 Application Access 可以让文件恢复其原始状态。

激活 Application Access 之前 ……	hosts 文件处于原始状态。
当 Application Access 启动时 ……	• 无客户端 SSL VPN 将 hosts 文件复制到 hosts.webvpn，从而创建备份。 • 无客户端 SSL VPN 然后编辑 hosts 文件，插入无客户端 SSL VPN 的特定信息。
当 Application Access 停止时 ……	• 无客户端 SSL VPN 将备份文件复制到 `hosts` 文件，从而将 hosts 文件恢复到其原始状态。 • 无客户端 SSL VPN 删除 hosts.webvpn。
完成 Application Access 后 ……	hosts 文件处于原始状态。

注　Microsoft 反间谍软件将拦截端口转发 Java 小程序对 hosts 文件的更改。有关使用反间谍软件时如何允许更改 hots 文件，请参阅 www.microsoft.com。

错误停止 Application Access

当 Application Access 异常停止时，`hosts` 文件将保持处于无客户端 SSL VPN 自定义的状态。下次您启动 Application Access 时，无客户端 SSL VPN 将通过搜索 hosts.webvpn 文件检查此状态。如果发现了一个，系统将显示 `Backup HOSTS File Found` 错误消息，并且 Application Access 将暂时关闭。

如果您错误地关闭 Application Access，您的远程访问客户端 / 服务器应用将处于不稳定状态。如果您尝试启动这些应用，而不使用无客户端 SSL VPN，它们可能会发生故障。您会发现自己通常连接的主机不可用。如果在家远程运行应用，并且在关闭计算机前未退出 Application Access 窗口，然后再尝试从办公室运行这些应用，通常会发生这种情况。

使用无客户端 SSL VPN 自动重新配置主机的文件

如果能够连接到远程访问服务器，请执行以下步骤以重新配置主机的文件并重新启用 Application Access 和应用。

详细步骤

步骤 1　启动无客户端 SSL VPN 并登录。系统将打开主页。

步骤 2　点击 **Applications Access** 链接。系统将显示 `Backup HOSTS File Found` 消息。

步骤 3　选择以下一个选项：

- **Restore from backup** — 无客户端 SSL VPN 强制执行正确的关闭操作。它会将 hosts.webvpn 备份文件复制到 `hosts` 文件，将其恢复原始状态，然后删除 hosts.webvpn。然后，您必须重新启动 Application Access。
- **Do nothing** — Application Access 不启动。系统重新显示远程访问主页。

- **Delete backup** — 无客户端 SSL VPN 删除 hosts.webvpn 文件，使 hosts 文件处于无客户端 SSL VPN 自定义状态。原始 hosts 文件设置将丢失。然后 Application Access 将启动，将无客户端 SSL VPN 自定义的 hosts 文件作为新的原始状态。只有在您不担心丢失 hotst 文件设置时，才可以选择此选项。如果您或您使用的程序在 Application Access 不正确关闭之后编辑了 hosts 文件，请选择一个其他选项或手动编辑 hosts 文件。（请参阅 “手动重新配置 hosts 文件”。）

手动重新配置 hosts 文件

如果您无法从当前位置连接到远程访问服务器，或者您已自定义 hosts 文件并且不想丢失您的编辑，请按照以下步骤重新配置 hosts 文件并重新启用 Application Access 和应用。

详细步骤

步骤 1　查找并编辑您的 hosts 文件。最常见的位置是 c:\windows\sysem32\drivers\etc\hosts。

步骤 2　检查是否有些行包含字符串：`# added by WebVpnPortForward` 如果任何行包含此字符串，则您的 hosts 文件是无客户端 SSL VPN 自定义的。如果您的 hosts 文件是无客户端 SSL VPN 自定义的，则它会类似于以下示例：

```
server1 # added by WebVpnPortForward
server1.example.com invalid.cisco.com # added by WebVpnPortForward
server2 # added by WebVpnPortForward
server2.example.com invalid.cisco.com # added by WebVpnPortForward
server3 # added by WebVpnPortForward
server3.example.com invalid.cisco.com # added by WebVpnPortForward

# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to hostnames.Each
# entry should be kept on an individual line.The IP address should
# be placed in the first column followed by the corresponding hostname.
# The IP address and the hostname should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     cisco.example.com          # source server
#       38.25.63.10     x.example.com              # x client host

123.0.0.1       localhost
```

步骤 3　删除包含此字符串的行：`# added by WebVpnPortForward`

步骤 4　保存并关闭文件。

步骤 5　启动无客户端 SSL VPN 并登录。

系统将显示主页。

步骤 6　点击 **Application Access** 链接。

系统将显示 Application Access 窗口。 Application Access 现已启动成功。

捕获数据

CLI **capture** 命令允许您记录无法在无客户端 SSL VPN 会话上正确显示的网站相关信息。此数据可帮助您的思科客户支持工程师对问题进行故障排除。以下各节将介绍如何捕获和查看无客户端 SSL VPN 会话数据：

先决条件

- 启用无客户端 SSL VPN 捕获会影响安全设备的性能。在生成用于故障排除的捕获文件后，请务必关闭捕获功能。

创建捕获文件

详细步骤

	命令	用途

步骤 1	**capture *capture_name* type webvpn user *webvpn_username***
	
	示例：
	`hostname# capture hr type webvpn user user2`
	`WebVPN 捕获已开始。`
	`   capture name   hr`
	`   user name      user2`
	`hostname# no capture hr`
		启动无客户端 SSL VPN 捕获实用程序。
		• *capture_name* 是分配给捕获的名称，此名称也将加在捕获文件的名称前面。
		• *webvpn_user* 是要与捕获匹配的用户名。
		创建名称为 hr 的捕获，它将把 user2 的流量捕获到文件中。

步骤 2	（可选） **no capture capture_name**	用户登录并开始了无客户端 SSL VPN 会话之后，使捕获实用程序停止捕获数据包。捕获实用程序将创建 *capture_name*.zip 文件，此文件使用密码 **koleso** 加密。
步骤 3	将此 .zip 文件发送至 Cisco Systems 或添加到思科 TAC 服务请求中。	
步骤 4	使用 *koleso* 密码解压此文件的内容。	

使用浏览器显示捕获数据

详细步骤

	命令	用途
步骤 1	**capture** *capture_name* **type webvpn user** ***webvpn_username***	启动无客户端 SSL VPN 捕获实用程序。 • *capture_name* 是分配给捕获的名称，此名称也将加在捕获文件的名称前面。 • *webvpn_user* 是要与捕获匹配的用户名。
步骤 2	（可选） **no capture capture_name**	用户登录并开始了无客户端 SSL VPN 会话之后，使捕获实用程序停止捕获数据包。
步骤 3	打开浏览器并输入以下信息： **https://***asdm_enabled_interface_of_the_security_appliance*:*port*/**admin/capture/***capture_name*/pcap **示例：** **https://192.0.2.1:60000/admin/capture/hr/pcap**	以探查器的格式显示名为 hr 的捕获。
步骤 4	重复第 2 步。	

第 22 章

无客户端 SSL VPN 许可

2013 年 9 月 13 日

许可

注 此功能在无负载加密型号上不可用。

型号	许可证要求
ASA 5512-X	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、 25、 50、 100 或 250 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5515-X	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、 25、 50、 100 或 250 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5525-X	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、 25、 50、 100、 250、 500 或 750 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5545-X	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000 或 2500 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*

型号	许可证要求
ASA 5555-X	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500 或 5000 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5585-X，带 SSP-10	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500 或 5000 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASA 5585-X，带 SSP-20、-40 和 -60	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500、5000 或 10000 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASASM	AnyConnect 高级版许可证： • 基础许可证：2 个会话。 • *可选永久性或基于时间的许可证：10、25、50、100、250、500、750、1000、2500、5000 或 10000 个会话。* • *可选共享许可证：参与者或服务器。对于服务器许可证，以 500 为增量，会话数量为 500-50,000 个；以 1000 为增量，会话数量为 50,000-545,000。*
ASAv，带 1 个虚拟 CPU	• 标准版许可证：2 个会话。 • 高级版许可证：250 个会话。
ASAv，带 4 个虚拟 CPU	• 标准版许可证：2 个会话。 • 高级版许可证：750 个会话。

注　如果您启动无客户端 SSL VPN 会话，然后从门户启动 AnyConnect 客户端会话，总计使用的是 1 个会话。但是，如果先启动 AnyConnect 客户端（例如从独立客户端启动），然后登录无客户端 SSL VPN 门户，则使用的是 2 个会话。

*所有*类型的最大组合 VPN 会话数量不能超过此表中所示的最大会话数。

一个共享许可证允许 ASA 用作多个客户端 ASA 的共享许可证服务器。共享许可证池很大，但是，每个 ASA 使用的会话数不能超过永久许可证列出的最大数量。