CLI 手册 3：Cisco Secure Firewall ASA VPN CLI 配置指南，9.20

上次修改日期: 2026 年 1 月 13 日

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. 保留所有权利。

目录

关于本指南

以下主题介绍如何使用本指南。

文档目标

本指南旨在帮助您使用命令行界面在 Cisco Secure Firewall 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。

您也可以使用自适应安全设备管理器 (ASDM) 这一基于 Web 的 GUI 应用来配置和监控 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 ASA 系列。在本指南中，除非有专门指定，否则术语“ASA”一般适用于受支持的模型。

相关文档

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

文档约定

本文档遵循以下文本、显示和警报约定。

关于本指南

文本约定

约定	指示
boldface	命令、关键字、按钮标签、字段名称及用户输入的文本以**boldface**字体显示。对于基于菜单的命令，显示指向该命令的完整路径。
斜体	为其赋值的变量以斜体字体显示。 斜体字体还用于文档标题和一般强调。
等宽字体	系统显示的终端会话和信息以等宽字体格式显示。
{x | y | z}	必需的备选关键字集中在大括号内，以竖线分隔。
[ ]	方括号中的元素是可选项。
[x | y | z]	可选的备选关键字集中在方括号内，以竖线分隔。
[]	对于系统提示符的默认响应也位于方括号内。
< >	非打印字符（例如密码）位于尖括号内。
!、#	一行代码开头带有叹号 (!) 或星号 (#) 表示这是注释行。

读者提示

本文档采用以下格式的读者提示：

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

提示 表示以下信息可帮助您解决问题。

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

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

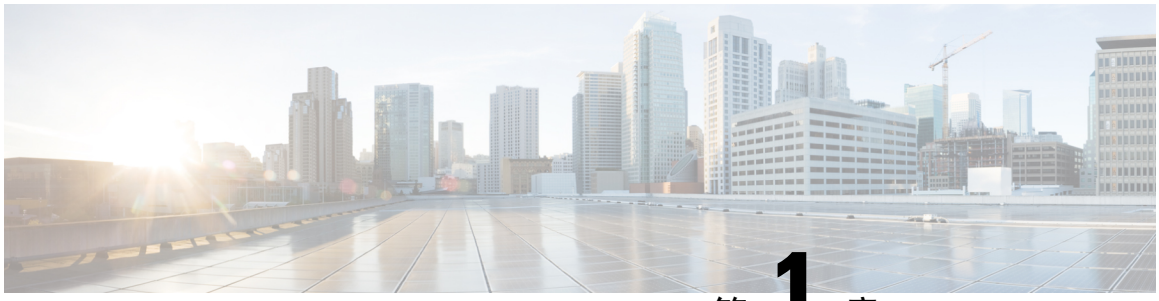
警告 表示读者需要注意。在这种情况下，操作可能会造成人身伤害。

通信、服务和其他信息

- 要及时从思科收到相关信息，请注册思科配置文件管理器。
- 要使用重要技术实现您期望实现的业务结果，请访问思科服务。
- 要提交服务请求，请访问思科支持。
- 要了解并浏览安全且经过验证的企业级应用、产品、解决方案和服务，请访问思科 DevNet。
- 要获取一般网络、培训和认证主题相关的信息，请访问 Cisco Press。
- 要查找有关特定产品或产品系列的保修信息，请访问思科保修服务查找工具。

思科漏洞搜索工具

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



第 1 章

IPsec 和 ISAKMP

有关隧道、IPsec 和 ISAKMP

本主题介绍用于建立虚拟专用网络 (VPN) 的互联网协议安全 (IPsec) 以及互联网安全关联和密钥管理协议 (ISAKMP) 标准。

借助隧道，可以使用互联网等公共TCP/IP网络在远程用户与企业专用网络之间创建安全连接。每个安全连接都称为一个隧道。

ASA 使用 ISAKMP 和 IPSec 隧道标准来建立和管理隧道。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
- 作为隧道终端或路由器管理入站和出站数据传输

ASA 可用作双向隧道终端。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标。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 间 VPN 连接，并提供将 IPsec 用于客户端到 LAN VPN 连接的选项。在 IPsec 术语中，对等体是一个远程访问客户端或其他安全网关。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 (SA)。这些协商包括两个阶段：第一个阶段，建立隧道 (IKE SA)；第二个阶段，管理该隧道内的流量 (IPsec SA)。

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

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

ISAKMP 和 IKE 概述

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 创建用于对对等体进行身份验证的加密密钥。

ASA 支持为旧版思科 VPN 客户端连接使用 IKEv1，还支持为 AnyConnect VPN 客户端使用 IKEv2。

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。
- 散列消息身份验证代码 (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未发生修改。

- 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散列密钥。
- 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散列运算的算法。
- 在更换加密密钥前，ASA 可使用该加密密钥的时间限制。

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 将按照安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。利用这种排序，您可以发送单个提议来传达所有允许的转换，而无需像对 IKEv1 一样发送每个允许的组合。

ASA 不支持 IKEv2 多安全关联 (SA)。ASA 当前仅接受找到的第一个 SA 上的入站 IPsec 流量。如果在任何其他 SA 上收到 IPsec 流量，则该流量将由于 `vpn-overlap-conflict` 而被丢弃。多个 IPsec SA 可能来自两个对等体之间的重复隧道，也可能来自非对称隧道。

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，您可以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 将按照安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。利用这种排序，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其 SA 的转换集或提议的定义，ASA 将撤销隧道。有关详细信息，请参阅清除安全关联，第 39 页。

注释 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。

关于 IKEv2 多对等体加密映射

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

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

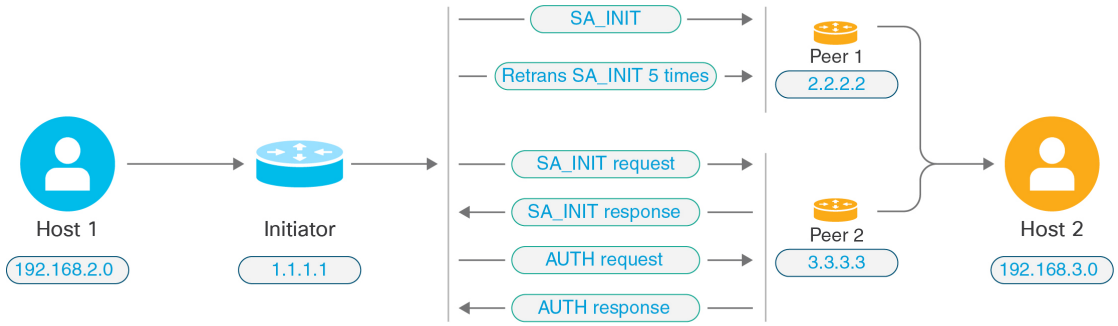
IKEv2 发起方行为

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

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

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

图 *1:* 发起方流程



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

IKEv2 响应方行为

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

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

注释 IKEv2 多对等体拓扑的响应方侧不支持对等体遍历。

加密映射更改时重置对等体索引

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

表 *1: SA* 之前的多对等体索引转换

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

表 *2: SA* 之后的多对等体索引转换

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

IKEv2 多对等体的准则

IKEv1 和 IKEv2 协议

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

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

高可用性

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

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

集中式集群

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

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

分布式集群

如果配置了 IKEv2 多对等体加密映射，则不支持分布式集群。

多情景模式

在多情景模式下，多对等体行为将特定于每个情景。

调试命令

如果隧道建立失败，请启用这些命令以对问题作进一步分析。

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

以下示例是特定于 IKEv2 多对等体的调试日志，显示了对等体的转换。

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

IPsec VPN 的许可

注释 此功能不适用于无负载加密型号。

使用 IKEv2 的 IPsec 远程访问 VPN 需要 AnyConnect Plus 或 Apex 许可证，可单独购买。使用 IKEv1 的 IPsec 远程访问 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点间 VPN 使用 基础 许可证随附的其他 VPN 许可证。有关每个型号的最大值，请参阅思科 ASA 系列功能许可证。

IPsec VPN 准则

情景模式准则

支持单情景或多情景模式。在多情景模式下，远程访问 VPN 需要 AnyConnect Apex 许可证。尽管 ASA 未明确认可 AnyConnect Apex 许可证，但它实施 Apex 许可证的特征，例如获得平台限制许可的 AnyConnect 高级版、Secure Client 移动版、适用于思科 VPN 电话的 Secure Client 和高级终端评估。

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。
- 当发生故障转移时，ESP 序列号会增加 2500 万，以防止错误的反重放。

其他准则

在配置 IKE 时，系统会自动保留 RADIUS UDP 端口 1645 和 1646。系统日志 713903 中记录了此预留，其中端口号显示为 27910 和 28166。该预留可确保端口不会被用于 PAT 转换。

配置 ISAKMP

配置 IKEv1 和 IKEv2 策略

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，优先级就越高。

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包含相同的加密、散列、身份验证和 Diffie-Hellman 参数值时，表明存在匹配项。对于 IKEv1，远程对等体策略还必须指定一个生命周期，其值应低于或等于发起方发送的策略中的生命周期。如果生命周期不相同，ASA 将使用较短的生命周期。对于 IKEv2，各对等体之间将不协商生命周期，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生命周期。如果不存在可接受的匹配项，IKE 将拒绝协商，并且不会建立 SA。

毫无疑问，为每个参数选择具体值时，需要在安全和性能之间进行权衡。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进行互操作，则只能选择该参数值。

您必须在每个 ISAKMP 命令中包含优先级。优先级数值唯一标识了策略并且决定着策略在 IKE 协商中的优先级。

过程

步骤 1 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。

示例：

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

注释
新的 ASA 配置没有默认 IKEv1 或 IKEv2 策略。

步骤 2 指定加密算法。 默认值为 AES-128。

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

示例：

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

步骤 3 指定散列算法。默认值为 SHA-1。

hash[sha]

示例：

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

步骤 4 指定身份验证方法。默认设置为预共享密钥。

authentication[**pre-shared**]**rsa-sig**]

示例：

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

步骤 5 指定 Diffie-Hellman 群标识符。默认值是组 14。

group [14]

示例：

```
hostname(config-ikev1-policy)#
group 14
```

步骤 6 指定 SA 生命周期。默认值为 86400 秒（24 小时）。

lifetime *seconds*

示例：

此示例将其生命周期设置为 4 小时（14400 秒）：

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

步骤 7 使用 IKE 策略关键字和值，第 9 页中提供的 IKEv1 和 IKEv2 策略关键字及其值来指定其他设置。如果您没有为特定策略参数指定值，则将应用默认值。

IKE 策略关键字和值

	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 对等体身份的身份验证方法。
	pre-share（默认）	预共享密钥	预共享密钥不能在增长型网络中很好地进行扩展，但是在小型网络中更容易设置。
encryption	**aes**（默认）	使用 128 位密钥的 AES	指定保护两个 IPSec 对等体之间传输的数据的对称加密算法。 默认值为 128 位密钥。
hash	**sha**（默认）	SHA-1（HMAC 变体）	指定用于确保数据完整性的散列算法。它可以确保数据包来自其所声明的发送方，并且在传输过程中未被修改。
group	**14**（默认）	组 14（2048 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，则安全性越高。 默认组是 DH 组 14
lifetime	**整数值** （86400＝默认值）	120 至 2147483647 秒	指定 SA 生命周期。默认值为 86400 秒或 24 小时。通常，此生命周期越短，ISAKMP 协商（在某种程度上）越安全。但是，此生命周期越短，ASA 设置后续 IPSec SA 的速度越快。

	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散列算法。它可以确保数据包来自其所声明的发送方，并且在传输过程中未被修改。
	sha256	SHA 2，256 位摘要	指定具有 256 位摘要的安全散列算法 SHA 2。

	关键字	含义	说明
	sha384	SHA 2，384 位摘要	指定具有 384 位摘要的安全散列算法 SHA 2。
	sha512	SHA 2，512 位摘要	指定具有 512 位摘要的安全散列算法 SHA 2。
	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	aes（默认）	AES	指定保护两个 IPSec 对等体之间传输的数据的对称加密算法。 默认值为 128 位 AES。
	aesaes-192aes-256		高级加密标准支持长度为 128、192、256 位的密钥。
	aesgmaesgm-192aesgm-256	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）	指定伪随机函数 (PRF)，即用于生成密钥内容的算法。
	sha256	SHA 2，256 位摘要	指定具有 256 位摘要的安全散列算法 SHA 2。
	sha384	SHA 2，384 位摘要	指定具有 384 位摘要的安全散列算法 SHA 2。
	sha512	SHA 2，512 位摘要	指定具有 512 位摘要的安全散列算法 SHA 2。
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。
group	**1419202124**	组 14（2048 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，则安全性越高。 默认值为 (DH) 组 14
lifetime	整数值 （86400＝默认值）	120 至 2147483647 秒	指定 SA 生命周期。默认值为 86400 秒或 24 小时。通常，此生命周期越短，ISAKMP 协商（在某种程度上）越安全。但是，此生命周期越短，ASA 设置后续 IPSec SA 的速度越快。

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
```

启用或禁用 IKEv1 积极模式

阶段 1 IKEv1 协商可以使用主模式或积极模式。这两个模式提供相同的服务，但是积极模式只需在对等体之间进行两次消息交换，交换总计三条消息；而不需要进行三次消息交换，交换总计六条消息。积极模式速度更快，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。默认情况下启用积极模式。

注释 禁用积极模式可防止思科 VPN 客户端使用预共享密钥身份验证建立通向 ASA 的隧道。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。

要为第 1 阶段 IKEv1 协商启用积极模式，请在单情景或多情景模式下输入以下命令：

```
hostname(config)# crypto map <map-name> seq-num set ikev1 phase1-mode aggressive <group-name>
```

要禁用积极模式，请在单情景或多情景模式下输入以下命令：

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

如果禁用了积极模式，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
```

配置 IKEv1 和 IKEv2 ISAKMP 对等体的 ID 方法

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

Address	使用交换 ISAKMP 标识信息的主机的 IP 地址。
Automatic （默认）	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。

Hostname	使用交换 ISAKMP 标识信息的主机的完全限定域名（默认）。此名称包含主机名和域名。
Key ID *key_id_string*	指定远程对等体用于查找预共享密钥的字符串。

ASA 使用要向对等体发送的阶段 I ID。所有 VPN 场景都是如此，但主模式下 LAN 间 IKEv1 连接除外，它使用预共享密钥进行身份验证。

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
```

INVALID_SELECTORS 通知

如果 IPsec 系统在某个 SA 上收到入站数据包，但该数据包的报头字段与该 SA 的选择符不一致，则 IPsec 系统必须丢弃该数据包。此事件的审核日志条目包括当前日期/时间、SPI、IPsec 协议、数据包的源和目标、该数据包的任何其他可用向量值，以及来自相关SA条目的选择符值。系统会生成IKE通知 INVALID_SELECTORS 并发送到发送方（IPsec 对等体），表明收到的数据包因未能通过选择符检查而丢弃。

ASA 已在 CTM 中使用如下所示的现有系统日志对此事件进行日志记录：

```
%ASA-4-751027: IKEv2 Received INVALID_SELECTORS Notification from peer: <peer IP>. Peer
received a packet (SPI=<spi>) from <local_IP>. The decapsulated inner packet didn't match
 the negotiated policy in the SA. Packet destination <pkt_daddr>, port <pkt_dest_port>,
source <pkt_saddr>, port <pkt_src_port>, protocol <pkt_prot>
```

管理员现在可以启用或禁用在SA上收到与该SA的流量选择符不匹配的入站数据包时向对等体发送IKEv2 通知。如果启用，IKEv2 通知消息的速率限制为每个 SA 每 5 秒发送一条通知消息。IKEv2 通知在 IKEv2 信息交换中发送到对等体。

配置十六进制 IKEv2 预共享密钥

您可以在本地和远程预共享密钥命令中添加关键字 *hex*，配置十六进制的 IKEv2 预共享密钥。

```
ikev2 local-authentication pre-shared-key [ 0 | 8 | hex ] <string>
ikev2 remote-authentication pre-shared-key [ 0 | 8 | hex ] <string>
```

启用或禁用发送 IKE 通知

管理员可以启用或禁用在 IKEv2 IPsec VPN 连接上收到与该连接的流量选择符不匹配的入站数据包时向对等体发送 IKE 通知。默认情况下禁用发送此通知。使用以下 CLI 命令启用或禁用在对 ASDM 证书中的用户名授权时发送 IKE INVALID_SELECTORS 通知：

[**no**] **crypto ikev2 notify invalid-selectors**

执行证书身份验证时，证书中的 CN 就是用户名，并且将对本地服务器执行授权。如果检索“service-type”属性，则按前文所述进行处理。

配置 IKEv2 分片选项

在 ASA 上，可以启用或禁用 IKEv2 分片，可以指定对 IKEv2 数据包分片时的 MTU（最大传输单位），还可以由管理员使用以下命令配置首选分片方法：

[**no**] **crypto ikev2 fragmentation** [**mtu** <*mtu-size*>] | [**preferred-method** [**ietf** | **cisco**]]

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

在考虑以下注意事项的情况下，指定 [**mtu** <*mtu-size*>]：

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

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

可将以下支持的分片方法之一配置为 IKEv2 [**preferred-method** [**ietf** | **cisco**]] 的首选分片方法：

- 基于 IETF RFC-7383 标准的 IKEv2 分片。
  - 当两个对等体都指定了协商期间的支持和首选项时，系统将使用此方法。
  - 使用此方法时，系统将在分片后执行加密，为每个 IKEv2 分片消息提供单独的保护。
- 思科专有分片。
  - 如果此方法是对等体（例如 Secure Client）提供的唯一方法，或者两个对等体都指定了协商期间的支持和首选项，则系统将使用此方法。
  - 使用此方法时，系统将在加密后执行分片。接收方对等体在收到所有分片之前，无法对消息进行解密或身份验证。
  - 此方法不能与非思科对等体实现互操作。

命令 **show running-config crypto ikev2** 将显示当前配置，**show crypto ikev2 sa detail** 将显示将分片用于 SA 时所实施的 MTU。

开始之前

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

示例

- 要禁用 IKEv2 分片，请执行以下操作：

```
no crypto ikev2 fragmentation
```

- 要恢复默认操作，请执行以下操作：

```
crypto ikev2 fragmentation
```

或

```
crypto ikev2 fragmentation mtu 576
preferred-method ietf
```

- 要将 MTU 值更改为 600，请执行以下操作：

```
crypto ikev2 fragmentation mtu 600
```

- 要恢复默认 MTU 值，请执行以下操作：

```
 no crypto ikev2 fragmentation mtu 576
```

- 要将首选分片方法更改为“思科”，请执行以下操作：

```
crypto ikev2 fragmentation preferred-method cisco
```

- 要将首选分片方法恢复为“IETF”，请执行以下操作：

```
no crypto ikev2 fragmentation preferred-method cisco
```

或

```
 crypto ikev2 fragmentation preferred-method ietf
```

AAA 身份验证和授权

```
aaa authentication http console LOCAL
aaa authorization http console radius
```

使用用户输入的用户名/密码，对本地服务器执行 AAA 身份验证。使用同一用户名，对 *radius* 服务器执行其他授权。如果检索 *service-type* 属性，则按前文所述进行处理。

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。

注释 由于 Secure Client的限制，您必须启用 NAT-T，才能让 Secure Client使用 IKEv2 成功建立连接。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、IPsec over TCP、NAT-T 和 IPsecover UDP，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
		并且如果没有 NAT，则	使用本地 IPsec (ESP)
选项 2	如果已启用 IPsec over UDP	并且客户端位于 NAT 后面，则	使用 IPsec over UDP
		并且如果没有 NAT，则	使用 IPsec over UDP
选项 3	如果 NAT-T 和 IPsec over UDP 都已启用	并且客户端位于 NAT 后面，则	使用 NAT-T
		并且如果没有 NAT，则	使用 IPsec over UDP

注释 IPsec over TCP 启用时，它将优先于所有其他连接方法。

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

ASA 支持在 LAN 间访问网络或远程访问网络中运行（但不能同时在这两种网络中运行）的一台 NAT/PAT 设备后面部署多个 IPsec 对等体。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 间隧道组相同的名称（也就是 NAT 设备的 IP 地址）。这种一致性会导致在 NAT 设备后面的 LAN 间和远程访问混合网络中多个对等体之间协商失败。

如要使用 NAT-T，请在单情景或多情景模式下执行以下站点间步骤：

过程

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

crypto isakmp nat-traversal *natkeepalive*

其中 natkeepalive 参数的取值范围是 10 至 3600 秒。默认值为 20 秒。

示例：

输入以下命令将启用 NAT-T 并将其生命周期值设置为一小时：

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

步骤 2 通过输入以下命令为 IPsec 分片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 IPsec with IKEv1 over TCP

IPsec over TCP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。默认情况下会禁用此功能。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，IPsec/IKEv1 over TCP 使得思科 VPN 客户端可以在此环境中运行。

注释 此功能不能与基于代理的防火墙配合使用。

IPsec over TCP 可与远程访问客户端配合使用。您可以同时在 ASA 及其连接的客户端上启用 IPsec over TCP。它在 ASA 上全局启用，用于所有启用 IKEv1 的接口。它不适用于 LAN 间连接。

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

您可以为您指定的最多 10 个端口启用 IPsec over TCP。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 上为 IKEv1 全局启用 IPsec over TCP，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 IPsec over TCP：

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

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 将用户与隧道组进行匹配。

注释 证书组匹配仅适用于 IKEv1 和 IKEv2 LAN 间连接。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。

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条件的规则，然后将每个规则与所需的隧道组匹配。

要创建证书映射，请使用 **use the 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。

过程

步骤 1 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 命令。

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

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

policy	指定用于从证书获取隧道组名称的策略。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 的内容映射到隧道组。 *ou* - 指示如果无法根据规则查找确定隧道组，则使用主题可分辨名称 (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。有效值为 1 到 65535。

请注意下列说明：

- 您可以多次调用此命令，前提是每次调用都是唯一的，并且不多次引用映射索引。
- 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。

步骤 2 指定当配置未指定隧道组时要使用的默认隧道组。

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。

示例

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
```

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
```

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
```

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
```

配置 IPsec

本节介绍使用 IPsec 实施 VPN 时配置 ASA 所需执行的程序。

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，请参阅将加密映射应用于接口，第 27 页。）
- 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。以下站点间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。序号越小，优先级就越高。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 [group14 | group15 | group16 | group19 | group20 | group21]**

指定用于加密映射完全向前保密 (PFS) 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 *map_name seq-num* **set reverse-route** [**dynamic**]

根据此加密映射条目为任何连接启用反向路由注入 (RRI)。如果未指定为动态，则 RRI 在配置时完成并被视为静态，在配置更改或被删除之前保持不变。此外，只要为 RRI 路由配置了已存在静态路由的相同目标，现有的静态路由就会被丢弃并安装 RRI 路由。ASA 可自动将静态路由添加到路由表中，并向其使用 OSPF 的专用网络或边界路由器通告这些路由。如果将任何源/目标 (0.0.0.0/0.0.0.0) 指定为受保护网络，请勿启用 RRI，否则会影响使用默认路由的流量。

注释 请对 RRI 使用特定网络，因为如果您选择“任何”作为受保护网络，那么 RRI 将不起作用。

如果指定为动态，则在成功建立 IPsec 安全关联 (SA) 时创建 RRI 并在删除 IPsec SA 后删除路由。

不能使用与静态加密映射相同的名称来配置动态加密映射，反之亦然，即使其中一个加密映射实际上并未被使用。

注释 动态 RRI 仅适用于基于 IKEv2 的静态加密映射。

[no] crypto map *name priority* **set validate-icmp-errors**

或

[**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}

或

[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*—Ignores the DF bit.
- *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>

或

[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。

注释 启用流量保密性数据包可防止 VPN 空闲超时。

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*

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 对从 10.0.0.0 子网流向 10.1.1.0 子网的所有流量应用分配给加密映射的 IPSec 保护：

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 会尝试将策略与静态加密映射匹配，如果匹配失败，则尝试匹配加密映射集中的任意动态加密映射，从而决定是接受还是拒绝对等体提议。

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）。如果对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（除非对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上为特定接口创建多个加密映射：

- 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。下表解释应用于加密映射的 ACL 中 permit 和 deny ACE 的特殊含义。

加密映射评估结果	解决方案
匹配 ACE 中包含 permit 语句的条件	停止按照加密映射集中剩余的ACE对数据包进行进一步分析，而按照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 ACE 中包含 deny 语句的条件	中断按照正在评估的加密映射中剩余的 ACE 对数据包进行进一步分析，而按照下一个加密映射（具体由分配给它的下一个序号决定）中的 ACE 继续进行评估。
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。

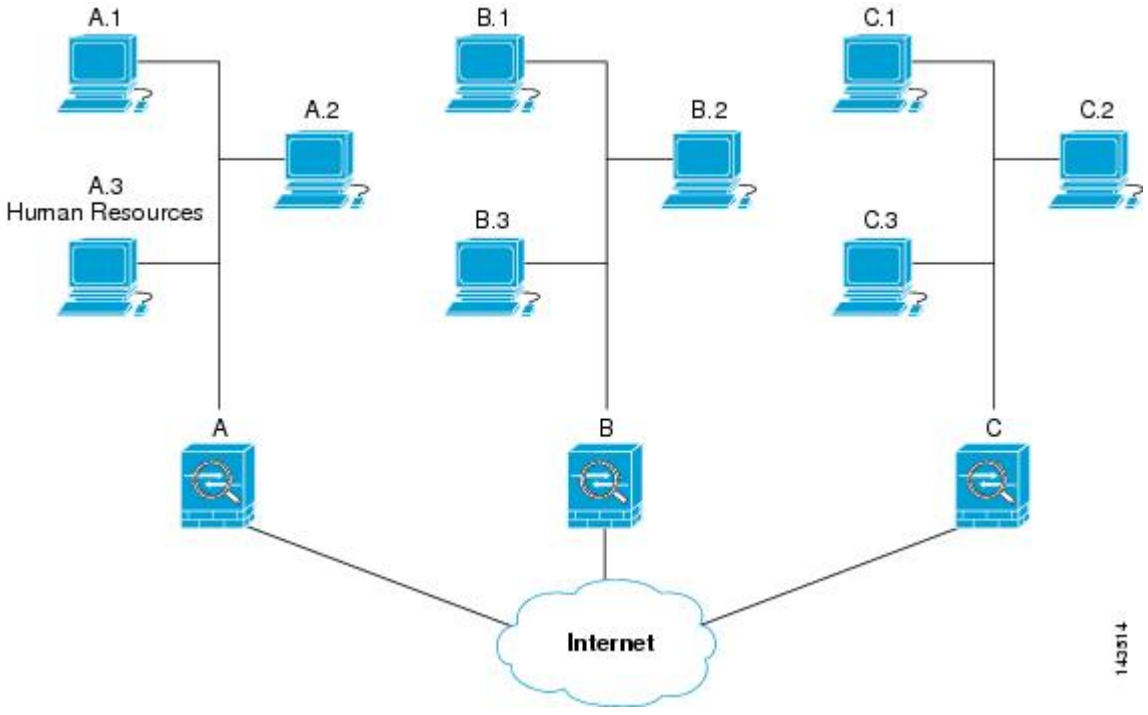
对于入站加密数据包，安全设备使用源地址和 ESP SPI 确定解密参数。安全设备解密数据包后，会将解密的数据包的内部报头与和数据包 SA 关联的 ACL 中的 permit ACE 进行比较。如果内部报头无法与代理匹配，安全设备将丢弃该数据包。如果内部报头与代理匹配，安全设备则会路由该数据包。

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。

注释 要将未加密的入站流量作为明文路由，请在 permit ACE 之前插入 deny ACE。ASA 在分割隧道访问列表中推送的 ACE 不能超过 28 个。

LAN 间加密映射示例

以下LAN 间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其中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，所以这些流量要求采用强加密并比其他流量更频繁地重新生成密钥。因此，您需要为来自主机 A.3 的流量分配一个专用转换集。



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。说明后面使用的是带有真实 IP 地址的示例。

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
```

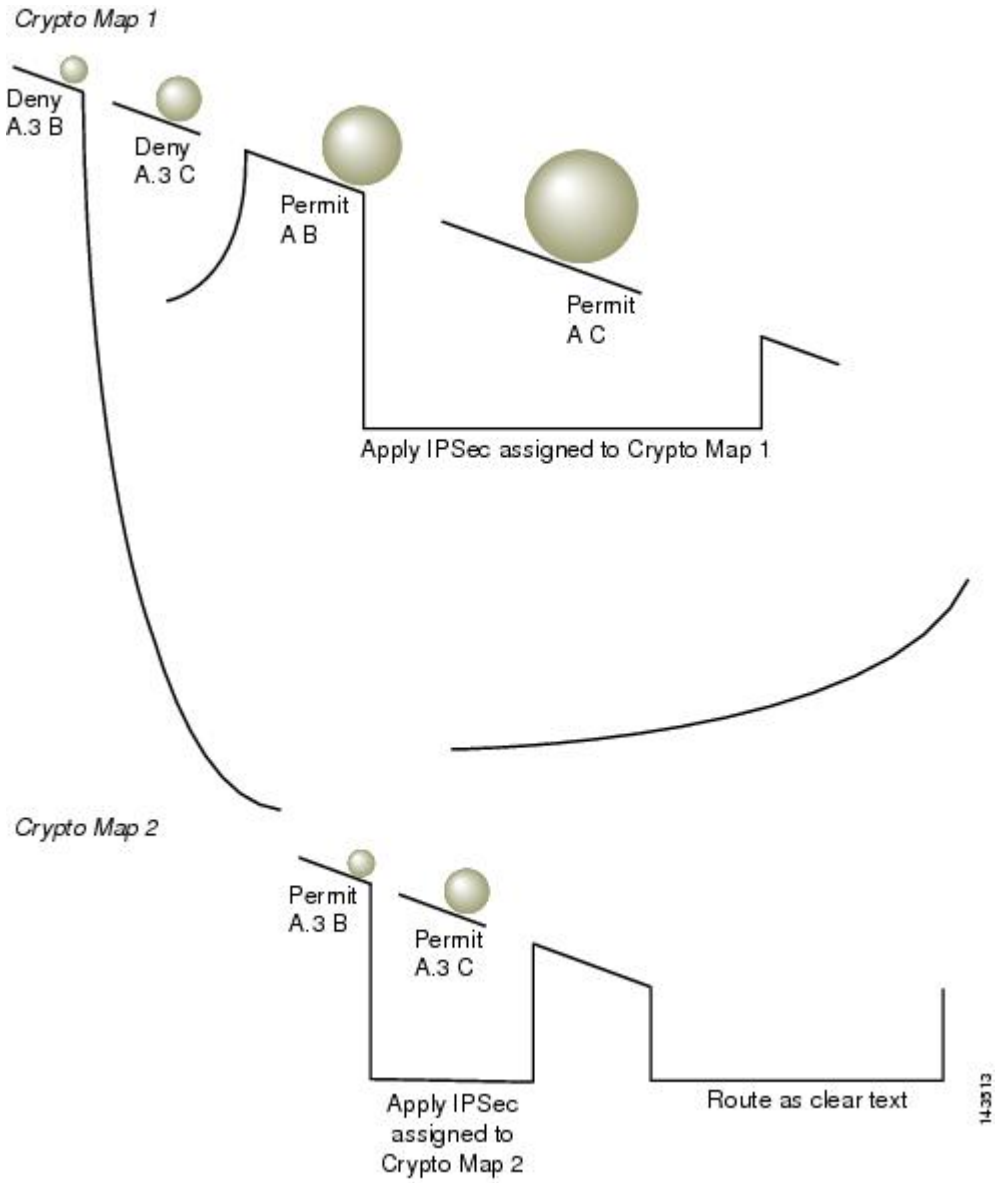
创建 ACL 之后，您要为每个加密映射分配一个转换集，向每个匹配的数据包应用所要求的 IPsec。

级联 ACL 涉及插入 deny ACE 以绕过按照某个 ACL 进行的评估，而按照加密映射集中的后续 ACL 继续进行评估。由于您可以将每个加密映射与不同的 IPsec 设置关联，因此您可以使用 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。

下图显示从本示例中的概念性 ACE 创建的级联 ACL。每个符号的含义定义如下：

	加密映射集中的加密映射。
	（直线上的缺口）当数据包与 ACE 匹配时退出加密映射。
	符合一个 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 *2:* 加密映射集中的级联 ***ACL***



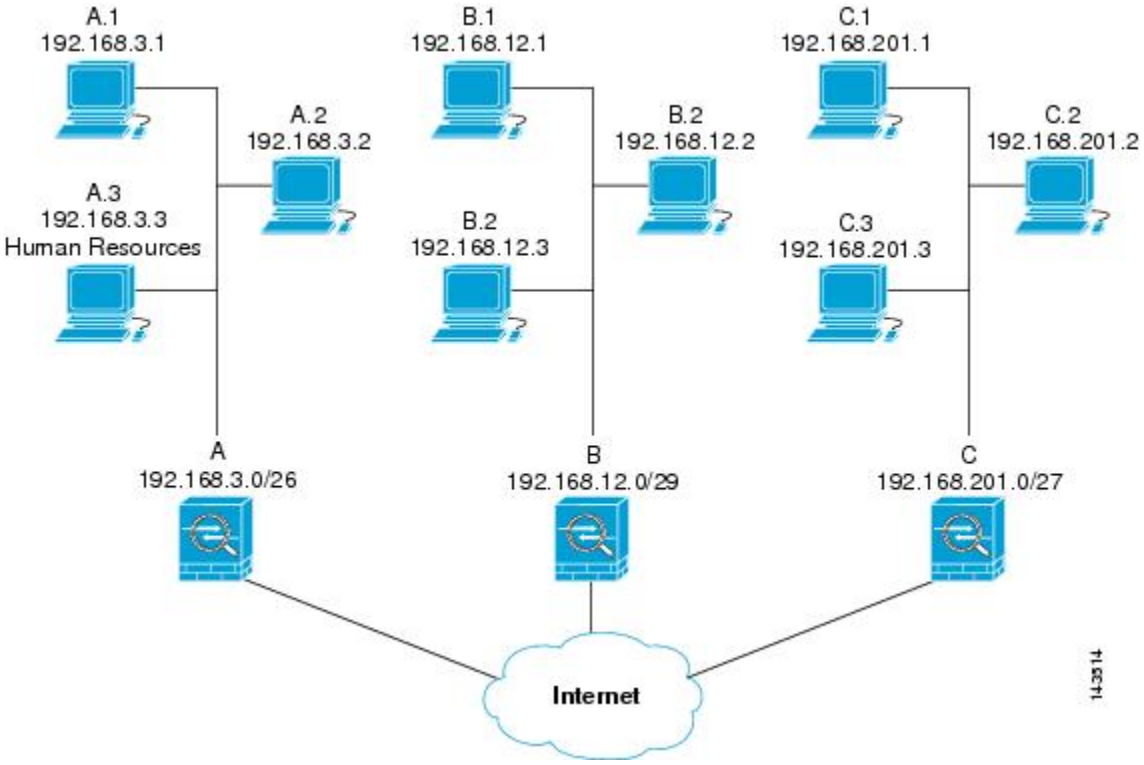
安全设备 A 评估源自主机 A.3 的数据包，直到与某个 permit ACE 匹配，然后尝试分配与加密映射关联的 IPSec 安全。但凡数据包与某个 deny ACE 匹配，ASA 将忽略加密映射中剩余的 ACE，然后按照下一个加密映射（具体由分配给它的序号决定）继续进行评估。因此在本示例中，如果安全设备 A 收到来自主机 A.3 的数据包，它会将数据包与第一个加密映射中的 deny ACE 匹配，然后按照下一个加密映射继续评估数据包。当它将数据包与该加密映射中的 permit ACE 匹配时，它会应用关联的 IPSec 安全（强加密和频繁地重新生成密钥）。

为了完成示例网络中的 ASA 配置，我们将镜像加密映射分配到 ASA B 和 C。但是，因为 ASA 在评估加密的入站流量时会忽略 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。

下表显示分配给为所有三个 ASA（A、B 和 C）配置的加密映射的 ACL：

安全设备 **A**		安全设备 **B**		安全设备 **C**	
加密映射序号	**ACE** 模式	加密映射序号	**ACE** 模式	加密映射序号	**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				

下图将此前显示的概念性地址映射至真实 IP 地址。



下表中显示的真实 ACE 可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

安全设备	加密映射序号	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所示的推理，通过使用级联 ACL 将不同安全设置分配给受 ASA 保护的不同主机或子网。

注释 默认情况下，ASA 不支持目的地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，从而将 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**

设置公钥基础设施 (PKI) 密钥

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

开始之前

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。

过程

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]

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 在所有接口上都支持 IPsec。向接口分配加密映射集将命令 ASA 按照该加密映射集评估所有流量并在连接或 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。将修改过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。
- 处理入站流量，以便过滤出并丢弃原本应受 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。（协商仅适用于 **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，才能确保在协商期间被接受。

注释 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，请使用 **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其他系统称为对等体。这将确保两个对等体正确处理 IPsec。

注释 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。要修复某个不完整的加密映射，请删除该加密映射，添加缺少的条目，然后重新应用它。

加密 ACL 不支持重复或重叠的条目。

我们建议不要使用 **any** 关键字在加密 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。

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。

注释 配置了 **no sysopt connection permit-vpn** 时，尽管在外部接口上有访问组（调用 deny ip any any access-list），系统仍会允许来自客户端的解密直通流量。

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) 来控制通过站点间或远程访问 VPN 对受保护网络进行的访问，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，应使用 **ssh**、**telnet** 和 **icmp** 命令，这些命令将拒绝应该添加的本地 IP 池。

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：

过程

步骤 1 创建用于 Ipsec 的 ACL。

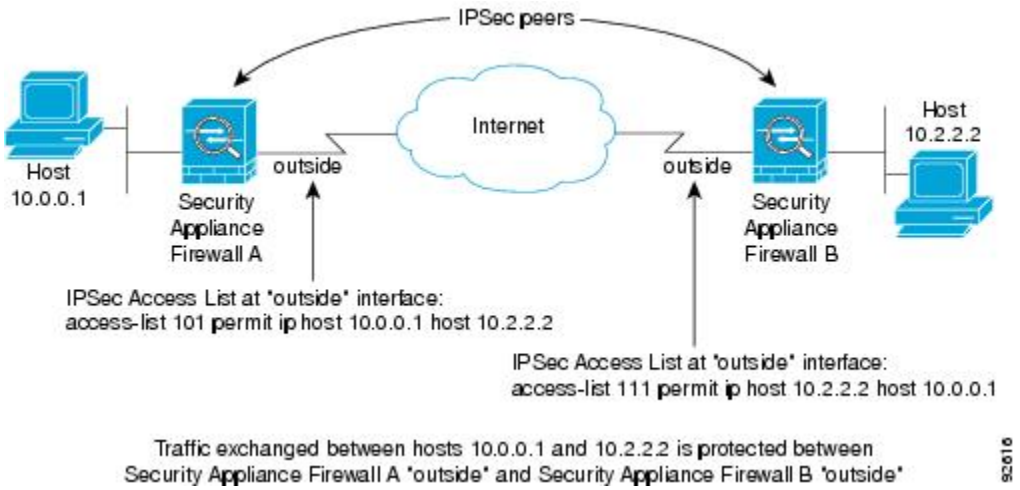
步骤 2 将列表映射到一个或多个使用同一个加密映射名称的加密映射。

步骤 3 将 IKEv1 转换集或 IKEv2 提议映射到加密映射，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，以加密映射集的形式应用全部加密映射。

示例

在本示例中，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。



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：

- 源 = 主机 10.0.0.1
- 目标 = 主机 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：

- 源 = 主机 10.2.2.2
- 目标 = 主机 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。

更改 IPsec SA 生命周期

协商新的 IPsec SA 时，您可以更改 ASA 使用的全局生命周期值。您可以为特定加密映射覆盖这些全局生命周期值。

IPSec SA 使用派生的共享密钥。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 都有两个生命周期：计时生命周期和流量生命周期。SA 将在各个生命周期之后到期，然后对等体将开始协商新的 SA。默认生命周期是 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）。

如果您更改全局生命周期，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生命周期值并且 ASA 请求使用新的 SA，它会将现有 SA 中使用的全局生命周期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生命周期值和本地配置的生命周期值这二者中较小的值作为新 SA 的生命周期。

对等体将在超出现有 SA 的生命周期阈值之前协商一个新 SA，确保在现有 SA 过期时已经准备好新 SA。当现有 SA 剩余生命周期只有大约 5% 至 15% 时，对等体将协商一个新的 SA。

注释 我们建议您在站点间 IKEv2 隧道的任一端配置不同的安全关联计时器，以避免重新生成密钥冲突。

更改 VPN 路由

默认情况下，按数据包邻接关系查找针对外部 ESP 数据包执行；不会对通过 IPsec 隧道发送的数据包执行查找。

在某些网络拓扑中，路由更新更改了内部数据包的路径，但本地 IPsec 隧道仍正常运行时，通过隧道的数据包可能无法正确路由，且无法到达其目的地。

要避免此情况，请对 IPsec 内部数据包启用按数据包路由查找功能。

开始之前

为避免这些查找产生任何性能影响，默认情况下禁用此功能。此功能仅在需要时启用。

过程

请对 IPsec 内部数据包启用按数据包路由查找功能。

[no] [crypto] ipsec inner-routing-lookup

注释
此命令在配置后仅适用于非 VTI 隧道。

示例

```
ciscoasa(config)# crypto ipsec inner-routing-lookup
ciscoasa(config)# show run crypto ipsec
 crypto ipsec ikev2 ipsec-proposal GCM
 protocol esp encryption aes-gcm
 protocol esp integrity null
 crypto ipsec inner-routing-lookup
```

创建静态加密映射

要使用静态加密映射创建基本 IPSec 配置，请执行以下步骤：

过程

步骤 1 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*

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。

示例：

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

步骤 2 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-null — 不加密。

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

- esp-sha-hmac — 使用 SHA/HMAC-160 作为散列算法。
- esp-none — 不进行 HMAC 身份验证。

示例：

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

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

步骤 3 要配置同时定义如何保护流量的 IKEv2 提议，请输入以下命令：

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

proposal tag 是 IKEv2 IPsec 提议的名称，即一个 1 至 64 个字符的字符串。

创建提议，然后进入 ipsec 提议配置模式，在此模式下可以为提议指定多个加密和完整性类型。

示例：

```
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 aes
```

示例：

此命令用于选择是使用 AES-GCM 算法还是 AES-GMAC 算法：

[no] protocol esp encryption [aes| aes-192 | aes-256 | aes-gcm| aes-gcm-192 | aes-gcm-256| null]

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

[no] protocol esp integrity [sha-1 | sha-256 | sha-384 | sha-512 | null]

注释
如果已将 AES-GCM/GMAC 配置为加密算法，则必须选择 null 完整性算法：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 4 （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。

[no] crypto ipsec security-association pmtu-aging *reset-interval*

步骤 5 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间步骤：

a) 将 ACL 分配到加密映射：

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多个条目的优先级。序号越小，优先级就越高。

示例：

在本示例中，名称为 101 的 ACL 将分配给加密映射 mymap。

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

b) 指定可以向其转发受 IPSec 保护的流量的对等体：

crypto map *map_name sequence number***set peer** *ip_address1 [ip_address2] [...]*

示例：

```
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。

注释

从 9.14(1) 开始，ASA 支持 IKEv2 加密映射中的多个对等体。您最多可以向列表中添加 10 个对等体。

c) 指定此加密映射允许哪些 IKEv1 转换集或 IKEv2 提议。按照优先级顺序列出多个转换集或提议（优先级高的优先）。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*]

或

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。每个加密映射条目支持最多 11 个提议。

示例：

在 IKEv1 的本示例中，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。

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

d) （可选）对于 IKEv2，请指定将 ESP 加密和身份验证应用于隧道的**mode**。此字段确定原始 IP 数据包的哪个部分已应用 ESP。

crypto map *map-name seq-num* **set ikev2 mode** [**transport | tunnel | transport-require**]

- **隧道模式** -（默认）封装模式将为隧道模式。隧道模式将 ESP 加密和身份验证应用至整个原始 IP 数据包（IP 报头和数据），从而隐藏最终的源地址和目的地址。整个原始 IP 数据报经过加密，成为新 IP 数据包中的负载。

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

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

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

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

- **传输必要** - 封装模式将为仅传输模式，不允许回退到隧道模式。

其中，**tunnel**封装模式是默认模式；**transport**封装模式是传输模式，如果对等体不支持，可以回退到隧道模式；**transport-require**封装模式仅实施传输模式。

注释
不建议将传输模式用于远程访问 VPN。

例如，封装模式的协商如下所示：

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

e) （可选）如果想要覆盖全局生命周期，请为加密映射指定 SA 生命周期。

crypto map *map-name seq-num* **set security-association lifetime** { **seconds** *number* | **kilobytes** {*number* | **unlimited**}}

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。您可以基于时间或传输的数据设置两个生命周期。但是，所传输数据的生命周期仅适用于站点间 VPN，不适用于远程访问 VPN。

示例：

此示例将加密映射 mymap 10 的计时生命周期缩短至 2700 秒（45 分钟）。基于流量的生命周期未更改。

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

f) （可选）指定在为此加密映射请求新的 SA 时 IPsec 要求完全向前保密，或在从对等体接收的请求中要求 PFS：

crypto map *map_name seq-num* **set pfs** [**group14** | **group15** | **group16** | **group19** | **group20** | **group21**]

示例：

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 2048 位 Diffie-Hellman 素数模数群。

```
crypto map mymap 10 set pfs group14
```

g) （可选）根据此加密映射条目为任何连接启用反向路由注入 (RRI)。

crypto map *map_name seq-num* **set reverse-route** [**dynamic**]

如果未指定为动态，则 RRI 在配置时完成并被视为静态，在配置更改或被删除之前保持不变。ASA 可自动将静态路由添加到路由表中，并向其使用 OSPF 的专用网络或边界路由器通告这些路由。如果将任何源/目标 (0.0.0.0/0.0.0.0) 指定为受保护网络，请勿启用 RRI，否则会影响使用默认路由的流量。

如果指定为动态，则在成功建立 IPsec 安全关联 (SA) 时创建 RRI 并在删除 IPsec SA 后删除路由。

注释
动态 RRI 仅适用于基于 IKEv2 的静态加密映射。

示例：

```
crypto map mymap 10 set reverse-route dynamic
```

步骤 6 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* 指定要在其上启用或禁用 ISAKMP IKEv1 协商的接口的名称。

示例：

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。

```
crypto map mymap interface outside
```

创建动态加密映射

动态加密映射是未配置任何参数的加密映射。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。如果尚未在静态加密映射中确定对等体的 IP 地址，ASA 将应用动态加密映射以便对等体协商隧道。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 间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间隧道具有预定的专用网络集，用于配置静态映射，进而用于建立 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或其他方法），而且您可能不知道其他客户端的专用 IP 地址（无论它们如何分配）。VPN 客户端通常没有静态 IP 地址；这些客户端需要动态加密映射来支持 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。

注释 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）和获取动态分配的 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组播或广播流量，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 条目并且尚不存在对应的 SA，则 ASA 将丢弃该流量。

加密映射集可以包括动态加密映射。动态加密映射集应是加密映射集中优先级最低的加密映射（即它们应该具有最高序列号），以便ASA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。

与静态加密映射集类似，动态加密映射集也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加密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，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 对于要通过隧道传送到使用动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。要标识应通过隧道传送的流量，请将 ACL 添加到动态加密映射。配置与远程访问隧道关联的 ACL 时，请小心标识合适的地址池。仅在隧道启用后使用反向路由注入安装路由。

使用单情景或多情景模式创建一个动态映射条目。您可以在一个加密映射集中同时包含静态和动态映射条目。

过程

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*

这将确定应保护和不应保护哪些流量。*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。

示例：

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

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

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。

示例：

在 IKEv1 的本示例中，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。

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

步骤 3 （可选） 如果您想要覆盖全局生命周期值，请为动态加密映射条目指定 SA 生命周期：

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

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。您可以基于时间或传输的数据设置两个生命周期。但是，所传输数据的生命周期仅适用于站点间 VPN，不适用于远程访问 VPN。

示例：

此示例将动态加密映射 dyn1 10 的计时生命周期缩短至 2700 秒（45 分钟）。基于时间的生命周期未更改。

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

步骤 4 （可选） 指定在为此动态加密映射请求新的 SA 时 IPsec 要求 PFS，或应该在从对等体接收的请求中要求 PFS：

crypto dynamic-map *dynamic-map-name dynamic-seq-num***set pfs**[**group14**|**group15**|**group16**|**group19**|**group20**|**group21**]

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。

示例：

```
crypto dynamic-map dyn1 10 set pfs group14
```

步骤 5 将动态加密映射集添加到静态加密映射集中。

请确保将引用动态映射的加密映射设置为加密映射集中优先级最低的条目（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。

示例：

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

提供站点间冗余

您可以使用加密映射定义多个IKEv1对等体，以提供冗余。此配置对于站点间VPN非常有用。IKEv2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，直到协商失败为止。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。

管理 IPsec VPN

查看 IPsec 配置

您可以在单情景或多情景模式下输入这些命令，用于查看有关 IPSec 配置的信息。

表 *3:* 用于查看 *IPSec* 配置信息的命令

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数据包以及收到的有效和无效ICMP错误中都会显示 ESPv3 统计信息。

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。默认情况下会禁用此功能。

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 EXEC 模式，这两个命令都不包含 **isakmp** 前缀。

过程

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间任务：

crypto isakmp reload-wait

示例：

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

断开连接前向对等体发出警报

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

ASA 可以通知合格的对等体（在 LAN 间配置或 VPN 客户端中）会话即将断开。收到此警报的对等体或客户端会对该原因进行解码，并将其显示在事件日志或弹出窗格中。默认情况下会禁用此功能。

合格客户端和对等体包括以下项：

- 已启用警报的安全设备
- 运行 4.0 或更高版本软件的思科 VPN 客户端（无需进行配置）

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。

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，请只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。

下表列出了可以在单情景或多情景模式下输入用以清除和重新初始化 IPsec SA 的命令。

表 *4:* 清除和重新初始化 ***IPSec SA*** 的命令

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。

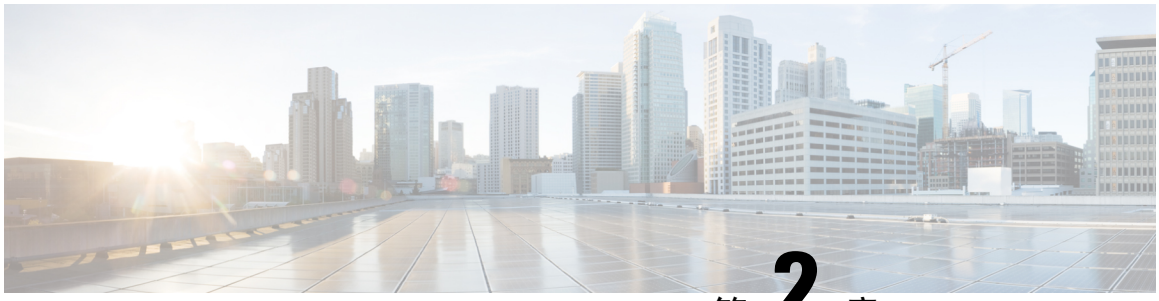
clear configure crypto ca trustpoint	删除所有信任点。
clear configure crypto dynamic-map	删除所有动态加密映射。包括用于删除特定动态加密映射的关键字。
clear configure crypto map	删除所有加密映射。包括用于删除特定加密映射的关键字。
clear configure crypto isakmp	删除整个 ISAKMP 配置。
clear configure crypto isakmp policy	删除所有 ISAKMP 策略或特定策略。
clear crypto isakmp sa	删除整个 ISAKMP SA 数据库。

清除加密映射配置

clear configure crypto 命令包括可用于删除加密配置的元素的参数，这些配置包括 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《*Cisco Secure Firewall ASA* 系列命令参考》中的 **clear configure crypto** 命令。



第 2 章

L2TP over IPsec

本章介绍如何在 ASA 上配置 L2TP over IPsec/IKEv1。

关于 L2TP over IPsec/IKEv1 VPN

第 2 层隧道协议 (L2TP) 是允许远程客户端使用公共 IP 网络安全地与企业专用网络服务器通信的 VPN 隧道协议。L2TP 使用 PPP over UDP（端口 1701）来通过隧道传送数据。

L2TP 协议基于客户端/服务器模式。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）。

在远程访问场景中，使用 IPsec/IKEv1 配置 L2TP 的主要优势在于远程用户可以通过公共 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 从任何位置实现远程访问。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。

注释 L2TP over IPsec TP 仅支持 IKEv1。不支持 IKEv2。

使用 IPsec/IKEv1 的 L2TP 配置支持使用预共享密钥或 RSA 签名方法的证书，也支持使用动态（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的第 41 章“数字证书”。

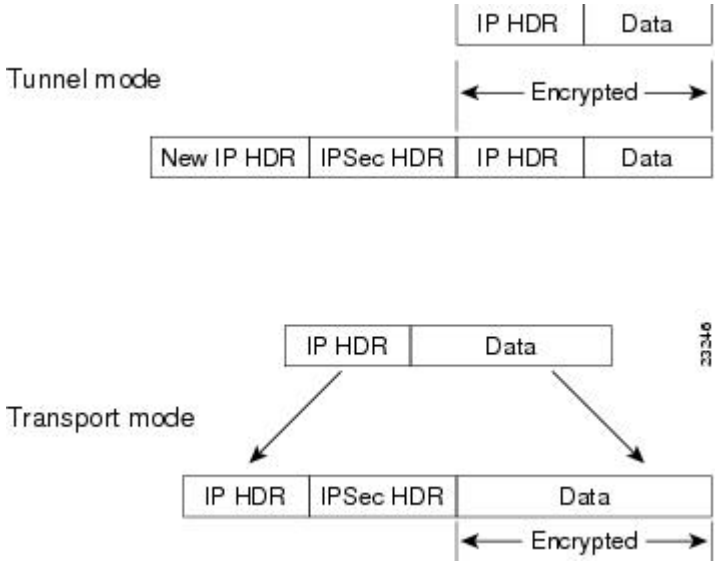
注释 在 ASA 上，使用 IPsec 的 L2TP 允许 LNS 与 Windows、Mac OS X、Android 和思科 IOS 等操作系统中集成的本地 VPN 客户端进行互操作。ASA 上仅支持使用 IPsec 的 L2TP，不支持单独使用本地 L2TP。Windows 客户端支持的最小 IPsec 安全关联生命周期是 300 秒。如果 ASA 上的生命周期设置低于 300 秒，Windows 客户端会忽略此设置并将其替换为 300 秒的生命周期。

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作 IPsec 代理。也就是说，路由器代表主机执行加密。源路由器加密数据包并将其沿 IPsec 隧道转发。目标路由器解密原始 IP 数据报并将其转发到目标系统。隧道模式的主要优势是不需要修改终端系统即可获得 IPsec 的优势。隧道模式还可以防止流量分析；利用隧道模式，攻击者只能确定隧道终端，而无法确定通过隧道传送的数据包的真正源和目标，即使其与隧道终点一样也无法确定。

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几个字节并且允许公共网络上的设备查看数据包的最终源和目标。下图说明了 IPsec 隧道和传输模式之间的差异。

图 *3:* 隧道和传输模式下的 ***IPsec***



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。此命令用于配置程序。**.**

注释 ASA 在分割隧道访问列表中推送的 ACE 不能超过 28 个。

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。

L2TP over IPsec 的许可要求

注释　此功能不适用于无负载加密型号。

使用 IKEv2 的 IPsec 远程访问 VPN 需要 AnyConnect Plus 或 Apex 许可证，可单独购买。使用 IKEv1 的 IPsec 远程访问 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点间 VPN 使用 基础 许可证随附的其他 VPN 许可证。有关每个型号的最大值，请参阅思科 ASA 系列功能许可证。

配置 L2TP over IPsec 的前提条件

配置 L2TP over IPsec 有以下前提条件：

- 组策略 - 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。不论是哪种情况，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。
- 连接配置文件 - 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。
- 确保连接路径上的任何位置都未阻止 UDP 端口 1701。
- 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

本节包括此功能的准则和限制。

情景模式准则

在单情景模式中受支持。

防火墙模式准则

仅在路由防火墙模式下受支持。不支持透明模式。

故障转移准则

状态故障转移不支持 L2TP over IPsec 会话。

IPv6 准则

对于 L2TP over IPsec，没有本机 IPv6 隧道设置支持。

所有平台上的软件限制

我们目前仅支持 4096 L2TP over IPsec 隧道。

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，而 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，L2TP over IPsec 连接只支持 PPP 身份验证类型，如下所示：

表 *5: 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
本地	PAP、MSCHAPv1、MSCHAPv2
RADIUS	PAP、CHAP、MSCHAPv1、MSCHAPv2、EAP-Proxy
TACACS+	PAP、CHAP、MSCHAPv1
LDAP	PAP
NT	PAP
Kerberos	PAP
SDI	SDI

表 *6: PPP* 身份验证类型特征

关键字	身份验证类型	特征
chap	CHAP	客户端响应服务器质询，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。

关键字	身份验证类型	特征
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，因为服务器仅存储和比较加密密码，而不是像 CHAP 中那样存储和比较明文密码。此协议还通过 MPPE 生成用于数据加密的密钥。
pap	PAP	在身份验证期间传递明文用户名和密码，因此并不安全。

使用 CLI 配置 L2TP over Eclipse

您必须配置 IKEv1 (ISAKMP) 策略设置来允许本地 VPN 客户端使用 L2TP over Eclipse 协议与 ASA 进行 VPN 连接。

- IKEv1 阶段 1 - 使用 SHA1 散列方法的 AES 加密。
- Eclipse 阶段 1 - 使用 SHA 散列方法的 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）。

过程

步骤 1 使用特定 ESP 加密类型和身份验证类型创建转换集。

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-aes esp-sha-hmac
```

步骤 2 指示 Eclipse 使用传输模式而不是隧道模式。

crypto ipsec ike_version transform-set *trans_name* **mode transport**

示例：

```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
```

步骤 3 将 L2TP/Eclipse 指定为 VPN 隧道协议。

vpn-tunnel-protocol *tunneling_protocol*

示例：

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec
```

步骤 4 （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。

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
```

步骤 5 （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。

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
```

步骤 6 （可选） 创建 IP 地址池。

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
```

步骤 7 （可选） 将 IP 地址池与连接配置文件（隧道组）关联。

address-pool *pool_name*

示例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# address-pool sales_addresses
```

步骤 8 将组策略的名称与连接配置文件（隧道组）关联。

default-group-policyname

示例：

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

步骤 9 指定一个身份验证服务器，以验证尝试通过 IPsec 连接的 L2TP 的用户。如果想在服务器不可用时将身份验证退回到本地身份验证，请在命令末尾添加 LOCAL。

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
```

步骤 10 为连接配置文件（隧道组）指定对尝试 L2TP over Eclipse 连接的用户进行身份验证的方法。如果目前不是使用 ASA 执行本地身份验证而您想要回退到本地身份验证，请在命令末尾添加 LOCAL。

authentication *auth_type*

示例：

```
hostname(config)# tunnel-group DefaultRAGroup ppp-attributes
hostname(config-ppp)# authentication ms-chap-v1
```

步骤 11 为您的连接配置文件（隧道组）设置预共享密钥。

tunnel-group 隧道组名称 **ipsec-attributes**

示例：

```
hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key cisco123
```

步骤 12 （可选） 为连接配置文件（隧道组）生成 L2TP 会话的 AAA 审计开始和停止记录。

accounting-server-group *aaa_server_group*

示例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# accounting-server-group sales_aaa_server
```

步骤 13 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。

l2tp tunnel hello *seconds*

示例：

```
hostname(config)# l2tp tunnel hello 100
```

步骤 14 （可选） 启用 NAT 遍历，从而使 ESP 数据包可以通过一个或多个 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 L2TP over Eclipse 连接，则必须启用 NAT 遍历。

crypto isakmp nat-traversal *seconds*

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（可以使用 **crypto isakmp enable** 命令启用），然后使用 **crypto isakmp nat-traversal** 命令。

示例：

```
hostname(config)# crypto ikev1 enable
hostname(config)# crypto isakmp nat-traversal 1500
```

步骤 15 （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。

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
```

步骤 16 （可选） 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 进行散列处理。

只有在使用本地用户数据库时才需要使用此步骤。

username *name* **password** *password* **mschap**

示例：

```
asa2(config)# username jdoe password j!doe1 mschap
```

步骤 17 为阶段 1 创建 IKE 策略，并为其分配编号。

crypto ikev1 policy *priority*

group *Diffie-Hellman Group*

您可以为 IKE 策略配置几种不同的参数。您还可以为该策略指定一个 Diffie-Hellman 群。ASA 使用 isakamp 策略来完成 IKE 协商。

示例：

```
hostname(config)# crypto ikev1 policy 14
hostname(config-ikev1-policy)# group14
```

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。请定义以下任意一个 IKE 策略，以便从 Windows 7 VPN 本地客户端建立连接。

请按照为 ASA 配置 L2TP over IPsec 的程序进行操作。如要为 Windows 7 本地 VPN 客户端配置 IKE 策略，需在本任务中增加其他步骤。

过程

步骤 1 显示属性和所有现有 IKE 策略的数量。

示例：

```
hostname(config)# show run crypto ikev1
```

步骤 2 配置 IKE 策略number 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。

crypto ikev1 policy *number*

步骤 3 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。

示例：

```
hostname(config-ikev1-policy)# authentication pre-share
```

步骤 4 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，请选择适用于 128 位 AES 的 **aes**，或者选择 **aes-256**。

encryption {|**aes**|**aes-256**}

步骤 5 选择确保数据完整性的散列算法。对于 Windows 7，请为 SHA-1 算法指定 **sha**。

示例：

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

步骤 6 选择 Diffie-Hellman 群标识符。您可以为 aes,aes-256 加密类型指定 14 。

示例：

```
hostname(config-ikev1-policy)# group 14
```

步骤 7 指定 SA 生命周期（以秒为单位）。对于 Windows 7，请指定 86400 秒（即 24 小时）。

示例：

```
hostname(config-ikev1-policy)# lifetime 86400
```

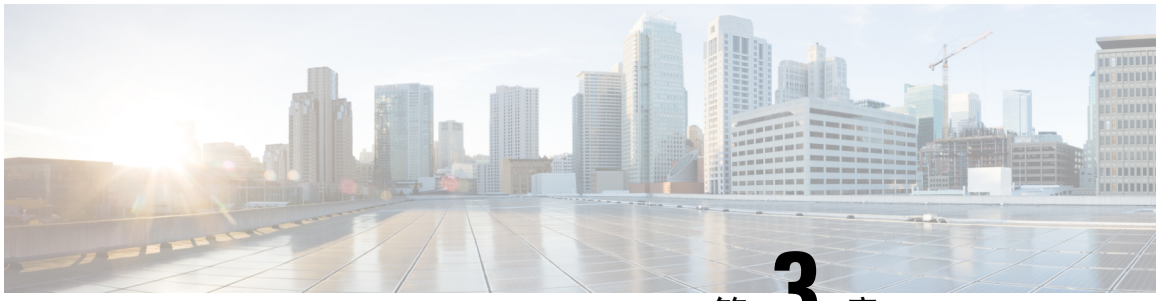
L2TP over IPsec 的配置示例

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 trans esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set trans 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 aes
 hash sha

 group 14
 lifetime 86400
```

L2TP over IPsec 功能历史记录

功能名称	版本	功能信息
L2TP over IPsec	7.2(1)	L2TP over IPsec 在单一平台上提供部署和管理 L2TP VPN 解决方案以 VPN 和防火墙服务的功能。 在远程访问场景中，配置 L2TP over IPsec 的主要优势在于远程用户 过公共 IP 网络访问 VPN，而无需使用网关或专线，实际上就可以利 从任何位置实现远程访问。另一个优势是 VPN 访问的唯一客户端 用带 Microsoft 拨号网络 (DUN) 的 Windows。不需要思科 VPN 客户 等任何其他客户端软件。 引入或修改了以下命令：authentication eap-proxy、authentication ms-c authentication ms-chap-v2、authentication pap、l2tp tunnel hello、 vpn-tunnel-protocol l2tp-ipsec。
弃用 IKE/IPsec 加密和完整性/PRF 密码 对 IKEv1 的 DH 组 14 支持	9.13(1)	以下加密/完整性/PRF 密码已弃用，并将在后续版本 - 9.14(1) 中删 • 3DES 加密 • DES 加密 • MD5 完整性 添加了对 IKEv1 的 DH 组 14（默认）支持。group 2 和 group 5 命令 弃用，并将在后续版本 9.14(1) 中删除。



第 3 章

高可用性选项

高可用性选项

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

Cisco Secure Firewall eXtensible 操作系统 (FXOS) 机箱上的 VPN 和集群

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

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

  VPN 功能仅限控制设备使用，且不能利用集群的高可用性功能。如果控制设备发生故障，所有现有的 VPN 连接都将断开，通过 VPN 连接的用户将遇到服务中断。选择新的控制设备后，必须重新建立 VPN 连接。

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

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

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

分布式 VPN 集群模式仅支持站点间 IKEv2。

仅在 Firepower 9300 上支持分布式 VPN 集群模式。

集中式和分布式集群模式均不支持远程访问 VPN。

VPN 负载均衡

VPN 负载均衡是在 VPN 负载均衡组中的设备之间合理分配远程访问 VPN 流量的机制。它基于简单的流量分配，而不考虑吞吐量或其他因素。VPN 负载均衡组由两台或更多设备组成。一台设备是导向器，而其他设备是成员设备。组设备不需要是完全相同的类型，也不需要具有相同的软件版本和配置。

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

故障转移

故障转移配置需要通过专用故障转移链路和状态故障转移链路（后者可选）相互连接的两台相同 ASA。主用接口和设备的运行状况会受到监控，以便确定满足特定故障转移条件的时刻。如果这些条件得到满足，则会进行故障转移。故障转移同时支持 VPN 和防火墙配置。

ASA 支持两种故障转移配置：主用/主用故障转移和主用/备用故障转移。

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

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

VPN 负载均衡

关于 VPN 负载均衡

如果您拥有一个远程客户端配置，在该配置中使用连接至相同网络的两个或更多 ASA 来处理远程会话，则可以通过创建 VPN 负载均衡组来将这些设备配置为共享其会话负载。VPN 负载均衡会将会

话流量定向至负载最低的设备，从而在所有设备之间分配负载。这样可以高效地利用系统资源，并提高性能和可用性。

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

VPN 负载均衡组会对外部客户端显示为单个虚拟 IP 地址。此 IP 地址不与特定物理设备绑定。它属于当前导向器。VPN 客户端会尝试建立连接，先与虚拟 IP 地址连接。随后，导向器会将组中负载最低的可用主机的公用 IP 地址，发送回客户端。在第二个事务（对用户透明）中，客户端会直接连接至该主机。这样，VPN 负载均衡组导向器就能在资源之间均匀、高效地定向流量。

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

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

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

VPN 负载均衡算法

VPN 负载均衡组导向器会维护一个按 IP 地址升序排列的组成员列表。每个成员的负载计算为整数百分比（活动会话数）。Secure Client 非活动会话不会被计入 VPN 负载均衡的 SSL VPN 负载。导向器会将 IPsec 和 SSL VPN 隧道重定向至负载最低的设备，直到其百分比值比其余设备高出 1%。当所有成员都比导向器高 1% 时，导向器就会将流量重定向到自身。

例如，如果您有一个导向器和两个成员，则以下循环适用：

注释 所有节点的百分比值都从 0% 开始，而且所有百分比值都会四舍五入。

1. 如果所有成员的负载都比导向器高出 1%，则导向器会接受连接。
2. 如果导向器没有接受连接，则哪台成员设备负载百分比值最低就由哪台备用设备接受会话。
3. 如果所有成员的负载百分比值相同，则由会话数最少的成员获得会话。
4. 如果所有成员的负载百分比值和会话数都相同，则由 IP 地址最少的成员获得会话。

VPN 负载均衡组配置

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

- 包含两个相同版本 ASA 的 VPN 负载均衡组，可以为混合的 IPsec、Secure Client 和无客户端 SSL VPN 客户端会话进行 VPN 负载均衡。
- 包含混合版本 ASA 的 VPN 负载均衡组可支持 IPsec 会话。不过，在这样的配置中，ASA 可能无法达到其最高 IPsec 容量。

组的主管会将会话请求分配给组的成员。ASA 会同等地对待所有会话（SSL VPN 或 IPsec 会话），并相应地分配它们。您可以配置允许的 IPsec 和 SSL VPN 会话的数量，可配置的数量最多为您的配置以及许可证允许的最大数量。

我们已测试过 VPN 负载均衡组中的最多 10 个节点。更大的组可能能够正常工作，但是我们不正式支持此类拓扑。

VPN 负载均衡导向器选举

导向器选举过程

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

成员在导向器选举期间执行以下功能：

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

Hello 握手

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

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

Keepalive 消息

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

保持连接超时的工作原理如下：

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

有关 VPN 负载均衡的常见问题

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

多情景模式

问: 在多情景模式下是否支持 VPN 负载均衡？

答: 在多情景模式下，既不支持 VPN 负载均衡也不支持状态故障转移。

IP 地址池耗尽

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

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

唯一 IP 地址池

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

答: 是的。IP 地址池对于每台设备必须是唯一的。

在相同设备上使用 VPN 负载均衡和故障转移

问: 一台设备可以同时使用 VPN 负载均衡和故障转移吗？

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

多个接口上的 VPN 负载均衡

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

答: 只能定义一个接口作为公共接口加入 VPN 负载平衡组。这个想法是为了均衡 CPU 负载，多个接口会在相同 CPU 上融合，因此多个接口上的 VPN 负载均衡这个概念不会改善性能。

VPN 负载均衡集群的最大并行会话数

问: 请考虑有两台 Firepower 1150 的部署，每台设备均有一个 100 位用户的 SSL VPN 许可证。在 VPN 负载均衡组中，最大用户总数是允许 200 个并行会话还是仅允许 100 个并行会话？如果我们随后添加第三台设备，该设备有一个 100 位用户的许可证，我们此时能够支持 300 个并行会话吗？

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

VPN 负载均衡的许可

VPN 负载均衡有以下许可要求：

- 有效的 3DES/AES 许可证。

ASA 会在启用 VPN 负载均衡前检查是否存在此加密许可证。如果没有检测到有效的 3DES 或 AES 许可证，ASA 会阻止启用 VPN 负载均衡，也会阻止 VPN 负载均衡系统进行 3DES 的内部配置，除非许可证允许此使用。

- 防火墙上已激活此功能的有效增强型安全许可证。
- 您的智能账户必须有足够的增强型安全许可证才能符合要求。

VPN 负载均衡的前提条件

另请参阅VPN 负载均衡准则和限制，第 57 页。

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

  可以使用 **interface** 和 **nameif** 命令为这些接口配置不同的名称。
- 您必须事先配置虚拟 IP 地址所引用的接口。建立组通用的虚拟 IP 地址、UDP 端口（如需要）和 IPsec 共享密钥。
- 加入组的所有设备都必须共享同一个集群特定值：IP 地址、加密设置、加密密钥和端口。
- 要使用 VPN 负载均衡组加密，请先使用 **crypto ikev1 enable** 命令在内部接口上启用 IKEv1，同时指定内部接口；否则，在尝试配置 VPN 负载均衡组加密时，您将收到错误消息。
- 如果使用主用/主用状态故障转移或 VPN 负载均衡，则不支持本地 CA 功能。本地 CA 不能从属于另一 CA；它只能用作根 CA。

VPN 负载均衡准则和限制

符合条件的客户端

VPN 负载均衡仅在使用以下客户端发起的远程会话上有效：

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

客户端注意事项

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

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

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

负载均衡组

- ASA 支持每个 VPN 负载均衡组包含 10 台设备。
- UCAPL 模式不支持 VPN 负载均衡，即使禁用加密也是如此。在 UCAPL 模式下，使用 IKEv2 建立安全隧道。

情景模式

多情景模式下不支持 VPN 负载均衡。

FIPS

FIPS 不支持集群加密。

证书验证

使用 Secure Client 为 VPN 负载均衡执行证书验证，并且该连接通过某个 IP 地址重定向时，该客户端通过此 IP 地址进行其所有的名称检查。请确保重定向 IP 地址已在证书公用名或主题备用名称中列出。如果 IP 地址没有出现在这些字段中，则该证书会被视为不可信。

遵循RFC 2818中定义的准则，如果证书中包含有**主题备用名称**，我们会仅将**主题备用名称**用于名称检查，并忽略公用名。请确保已在证书的**主题备用名称**中，定义提供证书的服务器的 IP 地址。

对于独立 ASA，IP 地址为该 ASA 的 IP。在 VPN 负载均衡组情况下，该地址取决于证书配置。如果该组使用一个证书，则该证书应该具有包含虚拟 IP 地址和组 FQDN 的 SAN 扩展，并应包含带每个 ASA 的 IP 和 FQDN 的使用者备用名称扩展。如果该组使用多个证书，则每个 ASA 的证书均应具有包含虚拟 IP、组 FQDN 和各 ASA 的 IP 地址和 FQDN 的 SAN 扩展。

地理 VPN 负载均衡

在定期更改 DNS 解析的 VPN 负载均衡环境中，必须谨慎考虑如何设置生存时间 (TTL) 值。要使 DNS 负载均衡配置与 Secure Client 成功配合使用，从选定 ASA 到隧道完全建立，ASA 的名称到地址映射都必须保持相同。如果在输入凭证前，经过的时间过长，查找将会重新启动，不同的 IP 地址可能会成为解析后的地址。如果在输入凭证前，DNS 映射变更至不同的 ASA，VPN 隧道会失效。

VPN 的地理负载均衡通常使用 Cisco Global Site Selector (GSS)。GSS 使用 DNS 进行负载均衡，并且 DNS 解析的生存时间 (TTL) 值默认为 20 秒。如果您提高 GSS 上的 TTL 值，则可以显著降低连接发送故障的可能性。当用户输入凭证并建立隧道时，增加为更高的值可以为身份验证阶段提供充足的时间。

要增加输入凭证的时间，您还可以考虑禁用 Connect on Start Up。

IKE/IPSec 安全关联

集群加密会话不会同步到 VPN 负载均衡器拓扑中的备用设备。

配置 VPN 负载均衡

如果您拥有一个远程客户端配置，在该配置中使用连接至相同网络的两个或更多ASA来处理远程会话，则可以将这些设备配置为共享其会话负载。此功能称为VPN负载均衡，它会将会话流量定向至负载最低的设备，从而在所有设备之间分配负载。VPN 负载均衡可以高效地利用系统资源，提供更高的性能和系统可用性。

要使用 VPN 负载均衡，请在组中的每台设备上执行以下操作：

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

为 VPN 负载均衡配置公共和专用接口

要为 VPN 负载均衡组设备配置公共（外部）和专用（内部）接口，请执行以下步骤。

过程

步骤 1 在 vpn-load-balancing 配置模式下输入带有 **lbpublic** 关键字的 **interface** 命令，在 ASA 上配置公共接口。该命令为此设备的 VPN 负载均衡功能指定公共接口的名称或 IP 地址：

示例：

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

步骤 2 在 vpn-load-balancing 配置模式下输入带有 **lbprivate** 关键字的 **interface** 命令，在 ASA 上配置专用接口。该命令为此设备的 VPN 负载均衡功能指定专用接口的名称或 IP 地址：

示例：

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

步骤 3 设置要在组内分配给此设备的优先级。范围是从 1 到 10。该优先级指示，此设备在启动或现有导向器发生故障时，成为组导向器设备的可能性。设置的优先级越高（例如 10），此设备成为组导向器设备的可能性就越高。

示例：

例如，如要在组内为此设备分配值为 6 的优先级，请输入以下命令：

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

步骤 4 如果要对此设备应用网络地址转换，请输入 **nat** 命令和此设备的 NAT 分配地址。可以定义 IPv4 和 IPv6 地址，也可以指定此设备的主机名。

示例：

例如，如要为此设备分配 NAT 地址 192.168.30.3 和 2001:DB8::1，请输入以下命令：

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

配置 VPN 负载均衡组属性

如要为组中的每台设备配置 VPN 负载均衡组属性，请执行以下步骤：

过程

步骤 1 在全局配置模式下输入 **vpn load-balancing** 命令，设置 VPN 负载均衡：

示例：

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

此命令将进入 vpn-load-balancing 配置模式，可以在其中配置其余负载均衡属性。

步骤 2 配置此设备所属组的 IP 地址或完全限定域名。该命令指定代表整个 VPN 负载均衡组的单一 IP 地址或 FQDN。在公共子网地址范围内，选择由组中所有 ASA 共享的 IP 地址。必须指定 IPv4（强制）。您可以选择提供 IPv6 地址。

示例：

要配置虚拟 IPv4 和 IPv6 地址，请输入以下命令：

```
hostname(config-load-balancing)# cluster ip address 192.168.10.1 1000::2
hostname(config-load-balancing)#show running-config vpn load-balancing
vpn load-balancing
redirect-fqdn enable
cluster key *****
cluster ip address 192.168.10.1 1000::2
cluster encryption
```

要为 VPN 负载均衡集群配置 IPv6 地址，必须进行 IPv4 地址配置。如果仅配置虚拟 IPv6 地址，则会显示错误消息。

```
hostname(config-load-balancing)#show running-config vpn load-balancing
vpn load-balancing
redirect-fqdn enable
cluster key *****
cluster encryption
participate
hostname(config-load-balancing)# cluster ip address 1000::2
ERROR: Virtual IPv4 address is not set
```

步骤 3 配置组端口。该命令可为此设备要参与的 VPN 负载均衡组指定 UDP 端口。默认值为 9023。如果另一应用正使用此端口，输入您想要用于负载均衡的 UDP 目标端口号。

示例：

例如，如要将组端口设置为 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 VPN 负载均衡组启用 IPsec 加密。

默认设置为无加密。该命令可以启用或禁用 IPsec 加密。如果配置此复选属性，必须先指定和验证共享密钥。VPN 负载均衡组中的 ASA 通过使用 IPsec 的 LAN 间隧道进行通信。如要确保加密设备之间通信的所有负载均衡信息，请启用此属性。

注释
要使用 VPN 负载均衡组加密，请先使用 **crypto ikev1 enable** 命令在内部接口上启用 IKEv1，同时指定内部接口；否则，在尝试配置 VPN 负载均衡组加密时，您将收到错误消息。

如果在配置组加密时启用了 IKEv1，但在配置设备加入组之前已被禁用，则在输入 **participate** 命令时，您会收到一条错误消息，并且也不会为该组启用加密。

示例：

```
hostname(config)# crypto ikev1 enable inside
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)#
```

步骤 5 如果启用组加密，还必须输入 **cluster key** 命令指定 IPsec 共享密钥。在启用 IPsec 加密后，该命令指定 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。如果需要输入已加密的密钥（例如，从其他配置中复制），请输入 **cluster key 8** *key* 命令。

示例：

例如，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，让此设备加入组：

示例：

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

下一步做什么

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

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

使用 **tunnel-group**、**general-attributes**、**group-url** 命令配置这些组 URL。

启用使用完全限定域名的重定向

默认情况下，ASA 只会将 VPN 负载均衡重定向中的 IP 地址发给客户端。如果使用的证书基于 DNS 名称，证书将在重定向至成员设备时变得无效。

作为 VPN 负载均衡导向器，该 ASA 在将 VPN 客户端连接重定向至一个成员设备（组中的另一 ASA）时，可以通过反向 DNS 查找发送此成员设备的完全限定域名 (FQDN)，而不是其外部 IP 地址。

要在 vpn load-balancing 模式下启用或禁用使用完全限定域名的重定向，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。

开始之前

组中的 VPN 负载均衡设备上的所有外部和内部网络接口，都必须位于相同 IP 网络之上。

过程

步骤 1 为 VPN 负载均衡启用 FQDN。

redirect-fqdn {**enable** | **disable**}

示例：

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

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

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

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

VPN 负载均衡配置示例

基本 VPN 负载均衡 CLI 配置

以下 VPN 负载均衡命令序列示例包含一条启用完全限定域名重定向的接口命令，将组的公共接口指定为 **test**，将组的专用接口指定为 **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
```

查看 VPN 负载均衡信息

VPN 负载均衡组导向器从组中的每台 ASA 接收定期消息，其中包含活动 Secure Client 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。如果组中的 ASA 显示 100% 的容量已满，则组导向器无法向其重定向更多的连接。尽管 ASA 可能显示为容量已满，但有些用户可能处于非活动/等待继续状态，造成了许可证的浪费。作为应急方案，每台 ASA 都提供会话总数减去非活动状态会话数之后的数量，而不是会话总数量。请参阅 ASA 命令参考中的 **-sessiondb summary** 命令。也就是说，非活动会话不会报告至组导向器。即便 ASA 的容量已满（有部分非活动会话），组导向器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证。

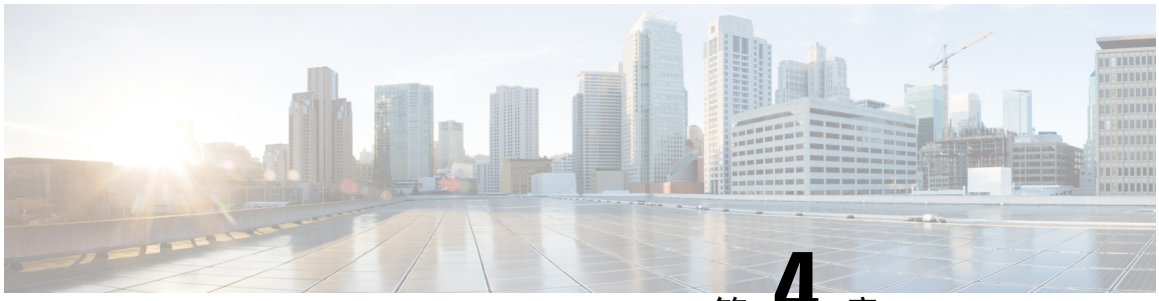
以下示例显示了 100 个 SSL 会话（仅活动会话）和 2% 的 SSL 负载。这些数值不包含非活动会话。也就是说，非活动会话不会计入 VPN 负载均衡的负载。

```
hostname# show vpn 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
```

VPN 负载均衡的功能历史记录

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



第 4 章

常规 VPN 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。本章将介绍其中一些功能。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

同时支持单情景和多情景模式。在相应版本的《ASA 常规操作 CLI 配置指南》中，有关在多情景模式下不支持内容的列表以及提供这些版本中新增内容细分信息的新功能，请参阅多情景模式准则。

防火墙模式准则

仅在路由防火墙模式下受支持。不支持透明模式。

网络地址转换 (NAT)

有关 NAT 配置的准则和信息，请参阅《*Cisco Secure Firewall ASA* 系列防火墙 *CLI* 配置指南》的适用于 *VPN* 的 *NAT* 部分。

配置 IPsec 以绕过 ACL

如要在不检查源和目标接口的 ACL 的情况下允许来自 IPsec 隧道的所有数据包，请在全局配置模式下输入 **sysopt connection permit-vpn** 命令。

如果使用位于 ASA 之后单独的 VPN 集中器并且想要最大限度提高 ASA 性能，则可能需要绕过用于 IPsec 流量的接口 ACL。通常，需要使用 **access-list** 命令创建允许 IPsec 数据包的 ACL，并将其应用于源接口。使用 ACL 可以指定想要允许其通过 ASA 的确切流量。

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
```

注释 配置了 **no sysopt connection permit-vpn** 时，尽管在外部接口上有访问组（调用 **deny ip any any** ACL），系统仍会允许来自客户端的解密直通流量。

如果尝试使用 **no sysopt permit-vpn** 命令结合外部接口上的访问控制列表 (ACL) 来控制通过站点间或远程访问 VPN 对受保护网络进行的访问，则无法成功进行控制。

sysopt connection permit-vpn 将在为需要关注的流量启用了加密映射的接口上绕过 ACL（入口和出口），连同所有其他接口的出口 (out) ACL 一起，但不包括入口 (in) ACL。

在这种情况下，启用管理访问内部接口时，系统不应用ACL，用户仍然可以使用SSH连接到ASA。流向内部网络中主机的流量会被 ACL 正确地阻止，但流向内部接口的解密直通流量不会被阻止。

ssh 和 **http** 命令具有比 ACL 更高的优先级。如要拒绝从 VPN 会话流向设备的 SSH、Telnet 或 ICMP 流量，应使用 **ssh**、**telnet** 和 **icmp** 命令。

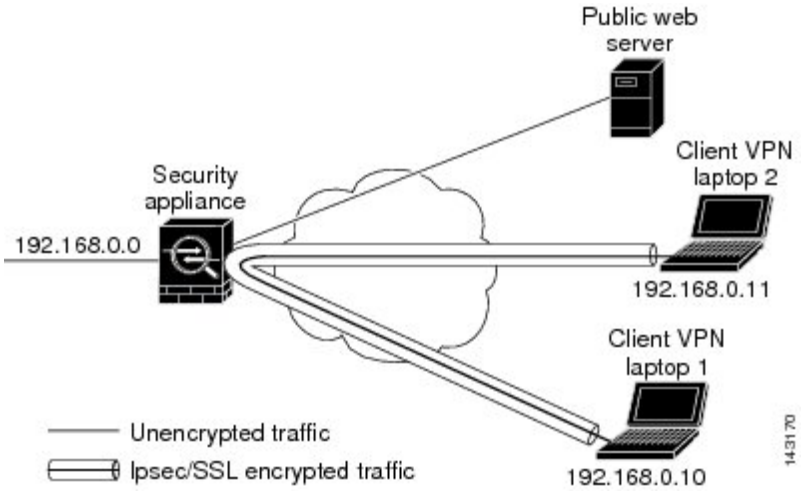
允许接口内流量 (Hairpinning)

ASA 提供一项功能，允许受 IPsec 保护的流量出入同一个接口，从而使得 VPN 客户端可以向其他 VPN 用户发送这些流量。该功能也称为“hairpinning”，可以将其视为通过 VPN 集线器 (ASA) 连接的 VPN 分支（客户端）。

Hairpinning还可以将传入VPN流量通过与未加密流量相同的接口重新向外传出去。例如，对于没有分割隧道但需要同时访问 VPN 和浏览 Web 的 VPN 客户端来说，此功能非常有用。

下图显示了 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共 Web 服务器。

图 *4:* 使用 ***Hairpinning*** 的接口内功能的 ***VPN*** 客户端



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

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

以下示例显示如何启用接口内流量：

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

注释 如果使用 **same-security-traffic** 命令和 **inter-interface** 参数，则可允许安全级别相同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，必须按照接口内流量的 NAT 注意事项中所述，对 ASA 接口应用适当的 NAT 规则。

接口内流量的 NAT 注意事项

要使 ASA 能够通过该接口退送未加密的流量，必须为该接口启用 NAT，以便公用可路由地址替换专用 IP 地址（除非已在本地 IP 地址池中使用公用 IP 地址）。以下示例对来自客户端 IP 池的流量应用接口 PAT 规则：

```
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 通过同一接口退送加密的 VPN 流量时，NAT 是可选的。无论是否使用 NAT，VPN 到 VPN Hairpinning 均可正常工作。要对所有传出流量应用 NAT，请仅实施以上命令。要使 VPN 到 VPN 流量豁免 NAT，请添加为 VPN 到 VPN 流量实施 NAT 豁免的命令（添加到以上示例命令中），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。

设置最大活动 IPsec 或 SSL VPN 会话数

要将 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** 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 Secure Client 的最大会话数，从 1 到许可证允许的最大会话数。

注释 正确的许可期限、级别和用户计数不再使用这些命令来确定。请参阅Secure Client订购指南：http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf

max-other-vpn-limit 关键字用于指定除 Secure Client会话之外的其他 VPN 的最大会话数，范围为从 1 到许可证允许的最大会话数。这包括思科 VPN 客户端 (IPsec IKEv1) 和 LAN 间 VPN 会话。

该限制会影响计算得出的 VPN 负载均衡的负载百分比。

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达到可接受的 IPsec 客户端修订级别

注释 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 客户端用户更新 VPN 客户端软件。

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，可以选择性地通知用户应更新其 VPN 客户端版本。对于 Windows 客户端，您可以为用户提供一种完成该更新的机制。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，请在常规配置模式或 tunnel-group ipsec-attributes 配置模式下输入 **client-update** 命令。如果客户端已经在运行修订号列表中包含的软件版本，则无需更新其软件。如果客户端未运行列表中包含的软件版本，则应进行更新。以下程序说明如何执行客户端更新：

过程

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，指定要对所有特定类型客户端应用的客户端更新参数。也就是说，指定客户端类型、可从中获取更新映像的 URL 或 IP 地址，以及该客户端的可接受的修订版本号。最多可以指定四个修订版本号，以逗号分隔。

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。该命令用于为整个 ASA 中所有指定类型的客户端指定客户端更新值。

使用以下语法：

```
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）。

如果客户端已经在运行修订号列表中包含的软件版本，则无需更新其软件。如果客户端未运行列表中包含的软件版本，则应进行更新。最多可以指定这些客户端更新条目中的三个条目。关键字**windows** 涵盖了所有允许的 Windows 平台。如果指定了 **windows**，则不要指定单个 Windows 客户端类型。

注释
对于所有的 Windows 客户端，必须使用协议 http:// 或 https:// 作为 URL 的前缀。

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

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

或者，也可以只为单个隧道组配置客户端更新，而不是为特定类型的所有客户端配置更新。（请参阅步骤 3。）

注释
在 URL 末尾包含应用的名称可以让浏览器自动启动该应用；例如：
https://support/updates/vpnclient.exe。

步骤 3 为特定的 ipsec-ra 隧道组定义一组客户端更新参数。

在 tunnel-group ipsec-attributes 模式下，指定隧道组名称及其类型、可从中获取更新映像的 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，则不需要更新客户端。例如，对于 Windows 客户端，请输入此命令：

```
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） 向安装过时 Windows 客户端的活动用户发送通知，指出其客户端需要更新。对于这些用户，系统将显示一个弹出窗口，让他们可以启动浏览器，并从您在URL中指定的站点下载经新的软件。此消息中唯一可配置的部分是 URL。（请参阅步骤 2 或 3。）非活动用户将在下次登录时收到通知消息。您可以向所有隧道组上的所有活动客户端发送此通知，也可以将其发送到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，则在特权 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，并且不会向该用户发送通知消息。

下一步做什么

注释 如果指定客户端更新类型为 **windows**（指定所有基于 Windows 的平台），然后要对同一实体输入 **win9x** 或 **winnt** 的客户端更新类型，必须先使用此命令的 **no** 形式删除 windows 客户端类型，然后使用新的客户端更新命令指定新客户端类型。

对公共 IP 连接实施 NAT 分配的 IP

在极少数情况下，您可能要在内部网络上使用 VPN 对等体的实际 IP 地址，而非已分配的本地 IP 地址。通常在使用 VPN 的情况下，对等体会获得分配的本地 IP 地址以访问内部网络。但是，在有些情况下，例如当内部服务器和网络安全基于对等体的真实 IP 地址时，可能就需要将本地 IP 地址重新转换为对等体的真实公共地址。

ASA 引入了一种方法，可以将 VPN 客户端在内部/受保护网络中分配的 IP 地址转换为其公共（源）IP 地址。该功能支持以下场景：内部网络中的目标服务器/服务和网络安全策略要求使用 VPN 客户端的公共/源 IP 而非其在内部企业网络中分配的 IP 进行通信。

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。

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 (IKEv1) 和 Secure Client。
- 流向公共 IP 地址的返回流量必须路由回 ASA，以便应用 NAT 策略和 VPN 策略。
- 仅支持 IPv4 的已分配地址和公共地址。
- 不支持 NAT/PAT 设备之后的多个对等体。
- 不支持负载均衡（因为路由问题）。
- 不支持漫游。

过程

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
```

此命令动态安装将已分配 IP 地址转换为源的公共 IP 地址的 NAT 策略。*interface* 用于确定要应用 NAT 的接口。

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 用作分配的 IP，将 75.1.224.21 用作对等体的公共 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 Secure Client连接至的接口，而 *inside* 是特定于新隧道组的接口。

注释 因为 VPN NAT 策略是动态的且不会添加到配置中，所以在 show run 对象和 show run nat 报告中，VPN NAT 对象和 NAT 策略会隐藏。

配置 VPN 会话限制

您可以运行的 IPsec 和 SSL VPN 会话数量与您的平台和 ASA 许可证支持的数量相同。要查看 ASA 的许可信息（包括最大会话数），请在全局配置模式下输入 **show version** 命令，并查找许可部分。以下示例显示该命令和该命令输出中的许可信息；为明确期间，其中还编入了其他输出内容。

```
hostname(config)# show version
...
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 500            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 100            perpetual
Carrier                           : Enabled        perpetual
AnyConnect Premium Peers          : 5000           perpetual
AnyConnect Essentials             : 5000           perpetual
Other VPN Peers                   : 5000           perpetual
Total VPN Peers                   : 5000           perpetual
AnyConnect for Mobile             : Enabled        perpetual
AnyConnect for Cisco VPN Phone    : Enabled        perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
Shared License                    : Disabled       perpetual
Total TLS Proxy Sessions          : 3000           perpetual
Botnet Traffic Filter             : Disabled       perpetual
IPS Module                        : Disabled       perpetual
Cluster                           : Enabled        perpetual
Cluster Members                   : 2              perpetual

This platform has an ASA5555 VPN Premium license.
```

显示许可证资源分配

使用以下命令显示资源分配：

```
asa2(config)# sh resource allocation
Resource       Total    % of Avail
Conns[rate]    100(U)      0.00%
Inspects[rate] unlimited
Syslogs[rate]  unlimited
Conns          unlimited
Hosts          unlimited
IPsec          unlimited
Mac-addresses  unlimited
ASDM           10          5.00%
SSH            10          10.00%
Telnet         10          10.0%
```

```
Xlates          unlimited
AnyConnect      1000        10%
AnyConnectBurst 200         2%
OtherVPN        2000        20%
OtherVPNBurst   1000        10%
```

显示许可证资源使用情况

使用以下命令显示资源使用情况：

注释 还可以使用 **sh resource usage system controller all 0** 命令显示系统级别使用情况，其限制为平台限制。

```
ASA(config-ca-trustpoint)# sh resource usage
Resource        Current  Peak  Limit  Denied  Context
Conns           1        16    280000 0       System
Hosts           2        10    N/A    0       System
AnyConnect      2        25    1000   0       cust1
AnyConnectBurst 0        0     200    0       cust1
OtherVPN        1        1     2000   0       cust2
OtherVPNBurst   0        0     1000   0       cust2
```

限制 VPN 会话

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。要删除会话限制，请使用此命令的 **no** 版本。

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

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

要删除会话限制，请使用此命令的 **no** 版本：

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

协商时使用身份证书

ASA 在与Secure Client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>]
```

使用此命令可以让 Secure Client支持最终用户的组选择。可以同时配置两个信任点：两个 RSA、两个 ECDSA 或各一个。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，则应先配置 ECDSA 信任点，再配置 RSA 信任点。

行号选项指定您想要插入信任点的行号。通常，此选项用于在不删除和重新添加另一行的情况下，在顶部插入信任点。如果未指定行，ASA 将在列表末尾添加信任点。

如果尝试添加已存在的信任点，将收到一条错误消息。如果使用 *no crypto ikev2 remote-access trustpoint* 命令而不指定要删除哪个信任点名称，则会删除所有信任点配置。

配置加密核心池

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

过程

指定如何分配密码加速器处理器：

crypto engine accelerator-bias

- **balanced** - 平均分配加密硬件资源（Admin/SSL 和 IPsec 核心）。
- **ipsec** - 将加密硬件资源优先分配给 IPsec（包括 SRTP 加密语音流量）。
- **ssl** - 将加密硬件资源优先分配给 Admin/SSL。当您支持基于 SSL 的 Secure Client 远程访问 VPN 会话时，请使用此偏差。

示例：

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

配置动态分割隧道

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

开始之前

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

过程

步骤 1 在 WebVPN 上下文中可使用以下命令定义自定义属性：`anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains`

步骤 2 定义客户端需要访问的VPN隧道外的每个云/Web服务的自定义属性名称。例如，添加Google_domains以表示有关 Google Web 服务的 DNS 域名的列表。属性值包含要从 VPN 隧道中排除的域名列表，且必须为逗号分隔值(CSV)格式，如下所示：`anyconnect-custom-data dynamic-split-exclude-domains webex.com, webexconnect.com, tags.tiqcdn.com`

步骤 3 使用以下命令将之前定义的自定义属性附加到特定策略组中，该命令在组策略属性上下文中执行：`anyconnect-custom dynamic-split-exclude-domains value webex_service_domains`

下一步做什么

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

配置管理 VPN 隧道

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

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

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

开始之前

需要 AnyConnect 版本 4.7（或更高版本）。

过程

步骤 1 将已上传的配置文件 (profileMgmt) 添加到映射到管理隧道连接所用隧道组的组策略 (MgmtTunGrpPolicy)：

要指示配置文件是 AnyConnect 管理 VPN 配置文件，请在 **anyconnect profiles** 命令中包含 **type vpn-mgmt**。常规 AnyConnect VPN 配置文件的类型为 user。

```
group-policy MgmtTunGrpPolicy attributes
```

```
  webvpn
     anyconnect profiles value profileMgmt type vpn-mgmt
```

步骤 2 要通过用户隧道连接部署管理 VPN 配置文件，请将上传的配置文件 *(profileMgmt)* 添加到映射到用户隧道连接所用隧道组的组策略 *(DfltGrpPolicy)*：

```
group-policy DfltGrpPolicy attributes
  webvpn
     anyconnect profiles value profileMgmt type vpn-mgmt
```

查看活动 VPN 会话

以下主题介绍如何查看 VPN 会话信息。

按 IP 地址类型查看活动 Secure Client 会话

要使用命令行界面查看活动的 Secure Client 会话，请在特权 EXEC 模式下输入 **show vpn-sessiondb anyconnect filter p-ipversion** 或 **show vpn-sessiondb anyconnect filter a-ipversion** 命令。

- 显示按终端的公共 IPv4 或 IPv6 地址过滤的活动 Secure Client 会话。公共地址是由企业分配给终端的地址。

  show vpn-sessiondb anyconnect filter p-ipversion {v4 | v6}

- 显示按终端的已分配 IPv4 或 IPv6 地址过滤的活动 Secure Client 会话。已分配地址是由 ASA 分配给 Secure Client的地址。

  show vpn-sessiondb anyconnect filter a-ipversion {v4 | v6}

示例 Output from show vpn-sessiondb anyconnect filter p-ipversion [v4 | v6] command

```
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
```

Output from show vpn-sessiondb anyconnect filter a-ipversion [v4 | v6] command

```
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 LAN 到 LAN VPN 会话

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

该命令显示按连接的公共 IPv4 或 IPv6 地址过滤的活动 LAN 到 LAN VPN 会话。

公共地址是由企业分配给终端的地址。

show vpn-sessiondb l2l filter ipversion {v4 | v6}

关于 ISE 策略实施

思科身份服务引擎 (ISE) 是一个安全策略管理和控制平台。可自动化并简化有线连接、无线连接和 VPN 连接的接入控制和安全合规性管理。思科 ISE 主要用于与思科 TrustSec 结合提供安全接入和访客接入、支持自带设备 (BYOD) 计划和执行使用策略。

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

在以下 VPN 客户端上支持 ISE 策略实施：

- IPSec
- Secure Client
- L2TP/IPSec

注释 系统支持某些策略元素，例如动态 ACL (dACL) 和安全组标记 (SGT)，而不支持诸如 VLAN 分配和 IP 地址分配之类的策略元素。

系统流程如下：

1. 最终用户请求 VPN 连接。
2. ASA 向 ISE 对用户进行身份验证，并且接收提供有限网络访问的用户 ACL。
3. 系统向 ISE 发送记帐启动消息以注册会话。
4. 直接在 NAC 代理和 ISE 之间进行安全状态评估。此过程对 ASA 透明。
5. ISE 通过 CoA“policy push”向 ASA 发送策略更新。这样可以识别提供更多网络访问权限的新用户 ACL。

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

这种流模型与使用 RADIUS CoA 的大多数场景不同。对于有线/无线 802.1x 身份验证，RADIUS CoA 不包含任何属性。它只会触发第二次身份验证，而在第二次身份验证中会附加所有属性，如 DACL。对于 ASA VPN 终端安全评估，没有第二次身份验证。所有属性都会在 RADIUS CoA 中返回。VPN 会话处于活动状态，无法更改大部分 VPN 用户设置。CoA 激活后可更改的唯一设置是重定向 URL、重定向 ACL 和安全组标记 (SGT)。

为 ISE 策略实施配置 RADIUS 服务器组

要启用 ISE 策略评估和实施，请针对 ISE 服务器配置 RADIUS AAA 服务器组并将服务器添加到该组。为 VPN 配置隧道组时，可以为该组中的 AAA 服务指定此服务器组。

过程

步骤 1 创建 RADIUS AAA 服务器组。

aaa-server *group_name* **protocol radius**

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)#
```

步骤 2 为 AAA 服务器组启用 RADIUS 动态授权 (CoA) 服务。

dynamic-authorization [**port** *number*]

可以选择是否指定端口。默认值为 1700，范围为 1024 至 65535。

当您在 VPN 隧道中使用服务器组时，RADIUS 服务器组将注册接收 CoA 通知，并且 ASA 会侦听用于从 ISE 获取 CoA 策略更新的端口

```
hostname(config-aaa-server-group)# dynamic-authorization
```

步骤 3 如果您不想将 ISE 用于授权，则请为 RADIUS 服务器组启用仅授权模式。

authorize-only

这表示当此服务器组用于授权时，RADIUS 访问请求消息将会构建为“仅授权”请求，而不是为 AAA 服务器定义的已配置的密码方法。如果您使用 **radius-common-pw** 命令为 RADIUS 服务器配置公用密码，则它将被忽略。

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

```
hostname(config-aaa-server-group)# authorize-only
```

步骤 4 启用 RADIUS 临时记帐更新消息的定期生成。

interim-accounting-update [**periodic** [*hours*]]

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

- **periodic**[*hours*] 允许为每个被配置为向有关服务器组发送审计记录的 VPN 会话定期生成和传输审计记录。可以选择包括发送这些更新的间隔（以小时为单位）。默认值为 24 小时，范围为 1 至 120。
- （无参数。）如果使用不带 **periodic** 关键字的此命令，则 ASA 仅会在将 VPN 隧道连接添加到无客户端VPN会话时发送临时审计更新消息。发生此情况时，将生成记帐更新，以便将新分配的 IP 地址通知给 RADIUS 服务器。

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

步骤 5 （可选。）将可下载 ACL 与来自 RADIUS 数据包的思科 AV 对中收到的 ACL 进行合并。

merge-dacl {**before-avpair** | **after-avpair**}

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 是否会合并，并且不适用于在 ASA 上配置的任何 ACL。

默认设置为 **no merge dacl**，此值指定可下载 ACL 将不与思科 AV 对 ACL 合并。如果同时收到 AV 对和可下载 ACL，则优先使用 AV 对。

before-avpair 选项指定可下载 ACL 条目应放置在思科 AV 对条目之前。

after-avpair 选项指定可下载 ACL 条目应放置在思科 AV 对条目之后。

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)# merge-dacl before-avpair
```

步骤 6 （可选。）指定在尝试下一服务器前，向组中的 RADIUS 服务器发送的最大请求数。

max-failed-attempts *number*

范围为 1 至 5。默认值为 3。

如果您使用本地数据库（仅用于管理访问）配置了回退方法，并且组中的所有服务器都无法响应，则会将该组视为无响应，并将尝试回退方法。该服务器组会在10分钟（默认值）内保持标记为无响应，以确保该时段内其他AAA请求不会尝试联系该服务器组，而是立即使用回退方法。要更改默认的无响应期间，请参阅下一步中的 **reactivation-mode** 命令。

如果没有回退方法，则 ASA 将继续重试该组中的服务器。

```
hostname(config-aaa-server-group)# max-failed-attempts 2
```

步骤 7 （可选。）指定用于重新激活组中的故障服务器的方法（重新激活策略）。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

其中：

- **depletion** [**deadtime** *minutes*] 仅在组中的所有服务器都处于非活动状态后才重新激活故障服务器。这是默认重新激活模式。可以指定从禁用组内最后一个服务器到随后重新启用所有服务器所经过的时长（0 到 1440 分钟之间）。默认值为 10 分钟。
- **timed** 在 30 秒钟的停机时间后重新激活出现故障的服务器。

```
hostname(config-aaa-server-group)# reactivation-mode deadtime 20
```

步骤 8 （可选。）向组中的所有服务器发送记帐消息。

accounting-mode simultaneous

如要恢复仅向活动服务器发送消息的默认设置，请输入 **accounting-mode single** 命令。

```
hostname(config-aaa-server-group)# accounting-mode simultaneous
```

步骤 9 将 ISE RADIUS 服务器添加至该组。

aaa-server *group_name* [(*interface_name*)] **host** {*server_ip* | *name*} [*key*]

其中：

- *group_name* 是 RADIUS 服务器组的名称。
- (*interface_name*) 是可以通过其访问服务器的接口的名称。默认值为 （内部）。需要使用圆括号。
- **host** {*server_ip* | *name*} 是 ISE RADIUS 服务器的 IP 地址或主机名。

- *key* 是用于加密连接的可选密钥。进入 aaa-server-host 模式后，您可以更轻松地在 **key** 命令中输入此密钥。如果不配置密钥，则不对连接加密（明文）。该密钥是一个区分大小写的字母数字字符串，最多 127 个字符，其值与 RADIUS 服务器上的密钥相同。

可以向该组添加多个服务器。

```
hostname(config)# aaa-server servergroup1 (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key sharedsecret
hostname(config-aaa-server-host)# exit
```

ISE 策略实施的示例配置

使用密码针对 ISE 动态身份验证配置 VPN 隧道

以下示例显示如何为动态授权 (CoA) 更新和每小时定期记帐配置 ISE 服务器组。其中包括使用 ISE 配置密码身份验证的隧道组配置。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

针对 ISE 仅授权配置 VPN 隧道

以下示例显示如何使用ISE为本地证书验证和授权配置隧道组。包括服务器组配置中的仅授权命令，因为不会将服务器组用于身份验证。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

故障排除策略实施

以下命令可用于调试。

如要跟踪 CoA 活动，请输入以下命令：

```
debug radius dynamic-authorization
```

如要跟踪重定向 URL 功能，请输入以下命令：

```
debug aaa url-redirect
```

如要查看 URL 重定向功能对应的 NP 分类规则，请输入以下命令：

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

配置高级 SSL 设置

ASA 使用安全套接字层 (SSL) 协议和传输层安全 (TLS) 为 ASDM、无客户端 SSL VPN、VPN 和基于浏览器的会话提供安全消息传输支持。ASA 支持用于基于 SSL 的 VPN 和管理连接的 SSLv3、TLSv1、TLv1.1 TLSv1.2 以及 TLSv1.3 协议。此外，DTLS 还被用于 Cisco Secure 客户端的 AnyConnect VPN 模块连接。

支持以下密码（如下表所述）：

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

密码	TLSv1.1/DTLSV1	TLSV1.2/DTLSV1.2	TLSv1.3
DHE-RSA-AES128-SHA	是	是	否
DHE-RSA-AES128-SHA256	否	是	否
DHE-RSA-AES256-GCM-SHA384	否	l	否
DHE-RSA-AES256-SHA	是	是	否
ECDHE-ECDSA-AES128-GCM-SHA256	否	是	否
ECDHE-ECDSA-AES128-SHA256	否	是	否
ECDHE-ECDSA-AES256-GCM-SHA384	否	是	否
ECDHE-ECDSA-AES256-SHA384	否	是	否
ECDHE-RSA-AES128-GCM-SHA256	是	是	否
ECDHE-RSA-AES128-SHA256	否	是	否
ECDHE-RSA-AES256-GCM-SHA384	否	是	否
ECDHE-RSA-AES256-SHA384	否	是	否
NULL-SHA	否	否	否
RC4-MD5	否	否	否
RC4-SHA	否	否	否

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

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

要指定 ASA 协商 SSL/TLS 和 DTLS 连接的最低协议版本，请执行以下步骤：

过程

步骤 1 设置 ASA 将协商连接的最低协议版本。

ssl server-version ［**tlsv1** | **tlsv1.1** | **tlsv1.2** | **tlsv1.3**］ ［**dtlsv1** | **dtlsv1.2**］

其中：

- **tlsv1**- 输入此关键字则接受 SSLv2 ClientHello 消息并协商 TLSv1（或更高版本）
- **tlsv1.1**- 输入此关键字则接受 SSLv2 ClientHello 消息并协商 TLSv1.1（或更高版本）
- **tlsv1.2**- 输入此关键字则接受 SSLv2 ClientHello 消息并协商 TLSv1.2（或更高版本）
- **tlsv1.3** - 输入此关键字则接受 SSLv2 ClientHello 消息并协商 TLSv1.3（或更高版本）
- **dtlsv1**- 输入此关键字则接受 DTLSv1 ClientHello 消息并协商 DTLSv1（或更高版本）
- **dtlsv1.2**- 输入此关键字则接受 DTLSv1.2 ClientHello 消息并协商 DTLSv1.2（或更高版本）

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

请使用与 DTLS 版本相等或更高版本的 TLS，确保 TLS 会话与 DTLS 会话同样安全或更安全。鉴于此点，tlsv1.2 是选择 dtls1.2 时唯一可接受的 TLS 版本；而任何 TLS 版本均可与 dtls1 配合使用，因为其版本均等于或高于 DTLS 1.0。

示例：

示例：

```
hostname(config)# ssl server-version tlsv1.1

hostname(config)# ssl server-version tlsv1.2 dtlsv1.2
```

步骤 2 指定 ASA 作为服务器时使用的 SSL/TLS 协议的最高版本。

ssl server-max-version ［**tlsv1** | **tlsv1.1** | **tlsv1.2** | **tlsv1.3**］

如果服务器最高版本配置为 TLSV1.2，则无法将 TLSV1.3 配置为服务器版本。

步骤 3 指定 ASA 用作客户端时所使用的 SSL/TLS 协议版本。

ssl client-version ［**tlsv1** | **tlsv1.1** | **tlsv1.2** | **tlsv1.3**］

其中：

- **tlsv1** - 输入此关键字以指定 ASA 可以传输 TLSv1 客户端 Hello 消息并协商 TLSv1（或更高版本）。
- **tlsv1.1** - 输入此关键字以指定 ASA 可以传输 TLSv1.1 客户端 Hello 消息并协商 TLSv1.1（或更高版本）。
- **tlsv1.2** - 输入此关键字以指定 ASA 可以传输 TLSv1.2 客户端 Hello 消息并协商 TLSv1.2（或更高版本）。
- **tlsv1.3** - 输入此关键字以指定 ASA 可以传输 TLSv1.3 客户端 Hello 消息并协商 TLSv1.3（或更高版本）。

DTLS 不可用于 SSL 客户端角色。

示例：

示例：

```
hostname(config)# ssl client-version tlsv1
```

步骤 4 指定 ASA 作为客户端时使用的 SSL/TLS 协议的最高版本。

ssl client-max-version ［**tlsv1** | **tlsv1.1** | **tlsv1.2** | **tlsv1.3**］

如果客户端最高版本配置为 TLSV1.2，则无法将 TLSV1.3 配置为客户端版本。

步骤 5 指定 SSL、DTLS 和 TLS 协议的加密算法。

ssl cipher *version* ［ *level* | **custom** *string*］

其中：

- *version* 参数指定 SSL、DTLS 或 TLS 协议版本。支持的版本包括：
  - default - 用于出站连接的密码集。
  - dtlsv1 - 用于 DTLSv1 入站连接的密码。
  - dtlsv1.2 - 用于 DTLSv1.2 入站连接的密码。
  - tlsv1 - 用于 TLSv1 入站连接的密码。
  - tlsv1.1 - 用于 TLSv1.1 入站连接的密码。
  - tlsv1.2 - 用于 TLSv1.2 入站连接的密码。
  - tlsv1.3 - 用于 TLSv1.3 入站连接的密码。
- *level* 参数指定密码的强度并表示已配置的最低级别密码。有效值（按强度的升序排列）如下：
  - all - 包括所有密码。
  - low - 包括除 NULL-SHA 以外的所有密码。
  - medium（这是所有协议版本的默认值）- 包括所有密码（NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA 和 DES-CBC3-SHA 除外）。
  - fips - 包括所有符合 FIPS 的密码（NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA 和 DES-CBC3-SHA 除外）。
  - high（仅适用于 TLSv1.2 和 TLSv1.3）- 仅包括 TLSv1.2 使用 SHA-2 密码的 AES-256。所有 TLSv1.3 密码的强度都很高。
- 通过指定 **custom** *string* 选项，您可以使用 OpenSSL 密码定义字符串对密码套件进行全面控制。有关详细信息，请参阅 https://www.openssl.org/docs/apps/ciphers.html。

推荐设置为 **medium**。使用 **high** 可能会限制连接。如果仅配置了几个密码，使用 custom 可能会限制功能。限制默认自定义值会限制出站连接，包括集群。

ASA 指定了支持的密码的优先级顺序。有关更多信息，请参阅命令参考。

此命令取代了从版本 9.3(2) 开始弃用的 ssl encryption 命令。

步骤 6 允许一个接口上有多个信任点。

ssl trust-point *name* [[**interface** *vpnlb-ip*] | [**domain** *domain-name*]

```
hostname(config)# ssl trust-point www-cert domain www.example.com
```

name 参数指定信任点的名称。**interface** 参数指定在其上配置信任点的接口的名称。vpnlb-ip 关键字仅适用于接口，并将此信任点与该接口上的 VPN 负载均衡集群 IP 地址关联。**domain***domain-name* 关键字-参数对指定与访问该接口所用的特定域名相关联的信任点。

最多可为每个接口配置 16 个信任点。

如果不指定接口或域，则此命令将为所有未配置信任点的接口创建回退信任点。

如果输入 **ssl trustpoint ?** 命令，则会显示可用的已配置信任点。如果输入 **ssl trust-point** *name***?** 命令（例如，**ssl trust-point mysslcert ?**），则会显示信任点 SSL 证书关联的可用已配置接口。

使用此命令时请遵守以下准则：

- trustpoint 的值必须是 **crypto ca trustpoint name** 命令中配置的 CA 信任点的名称。
- interface 的值必须是之前配置的接口的 nameif 名称。
- 删除信任点也会删除引用该信任点的任何 **ssl trust-point** 条目。
- 您可以为每个接口指定一个 ssl trust-point 条目，还可以指定一个不指定接口的条目。
- 可以将同一信任点重复用于多个条目。
- 一个配置了 domain 关键字的信任点可应用于多个接口（取决于连接方式）。
- 每个 *domain-name* 值只能有一个 **ssl trust-point**。
- 如果在输入此命令后显示以下错误：

  ```
  error:0B080074:x509 certificate routines:X509_check_private_key:key values
  mismatch@x509_cmp.c:339
  ```

  表示用户已配置新证书来替换先前配置的证书。无需任何操作。

- 证书按以下顺序选择：
  - 如果连接与 **domain** 关键字的值匹配，则首选该证书。（**ssl trust-point***name***domain***domain-name* 命令）
  - 如果与负载均衡地址建立连接，则选择 vpnlb-ip 证书。（**ssl trust-point** *name* **interface** *vpnlb-ip* 命令）
  - 为接口配置的证书。（**ssl trust-point** *name* interface 命令）
  - 未与接口关联的默认证书。(**ssl trust-point** *name*)
  - ASA 的自签名、自生成证书。

步骤 7 指定将与 TLS 所使用的 DHE-RSA 密码一起使用的 DH 群。

```
ssl dh-group [group14 | group15]

hostname(config)# ssl dh-group group14
```

group14 和 15 关键字配置 DH 群 14（2048 位模数，224 位素数阶子组）。

组 14 与 Java 7 不兼容。所有群均与 Java 8 兼容。组 14 符合 FIPS。默认值为 ssl dh-group group14。

步骤 8 指定将与 TLS 所使用的 ECDHE-ECDSA 密码一起使用的群。

```
ssl ecdh-group [group19 | group20 | group21]

hostname(config)# ssl ecdh-group group20
```

group19 关键字配置群 19（256 位 EC）。group20 关键字配置群 20（384 位 EC）。group21 关键字配置群 21（521 位 EC）。

默认值为 ssl ecdh-group group19。

注释
ECDSA 和 DHE 密码具有最高优先级。

下一步做什么

您可以使用以下命令来查看 TLS/DTLS 配置：

- 如果不是默认的 TLS/DTLS 版本，则输入**show run ssl** 。
- 如果是默认的 TLS/DTLS 版本，则输入**show run ssl all** 。

持续 IPsec 隧道流量

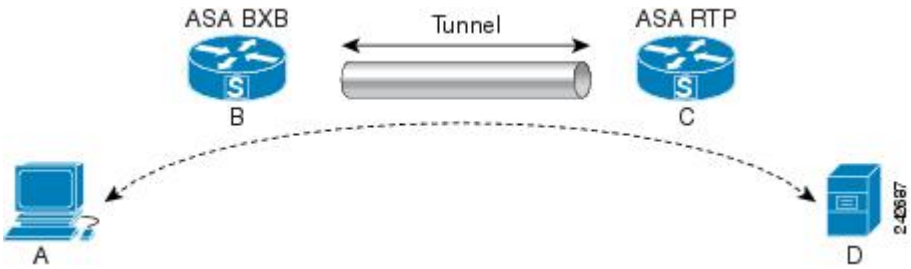
在运行版本低于 8.0.4 版的 ASA 软件的网络中，IPSec 隧道丢弃时，通过该隧道的现有 IPsec LAN 间或远程访问 TCP 流量会被丢弃。如果该隧道恢复，这些流量会按需重建。从资源管理和安全性角度来看，此策略非常不错。然而，对于用户，尤其是从 PIX 迁移至纯 ASA 环境的用户，以及无法轻松重启的旧版 TCP 应用，或者在包含常会频繁丢弃隧道的网关的网络中，在有些情况下，这一行为会带来问题。（有关详细信息，请参阅 CSCsj40681 和 CSCsi47630。）

持续 IPsec 隧道流量功能可以解决这一问题。启用此功能时，ASA 会保留和恢复状态 (TCP) 隧道流量。隧道丢弃时，所有其他流量都会被丢弃，并且必须在新隧道出现时重建。

注释　该功能支持在网络扩展模式下运行的 IPsec LAN 间隧道和 IPsec 远程访问隧道。它不支持 IPSec 或 AnyConnect/SSL VPN 远程访问隧道。

以下示例显示持续 IPsec 隧道流量功能的工作方式。

图 5: 网络场景



在此示例中，BXB 和 RTP 网络通过一对安全设备，经由安全的 LAN 间隧道进行连接。BXB 网络中的 PC 正经由安全隧道，通过 RTP 网络中的服务器执行 FTP 传输。在此场景中，假设在 PC 登录至服务器并开始传输后，出于某些原因，隧道丢弃。尽管隧道会因为数据仍在尝试流动而重建，FTP 传输却不会完成。用户必须终止传输，并通过重新登录至服务器来重新开始传输。然而，如果启用了持续 IPsec 隧道，一旦隧道在超时间隔内被重建，数据会继续成功流过新的隧道，因为安全设备会保留该流量的历史记录（状态信息）。

场景

以下各节说明隧道丢弃和隧道恢复时的数据流量状况，首先说明禁用持续 IPsec 隧道流量功能时的情况，然后说明启用该功能时的情况。有关这两种情况下的网络图解，请参阅上图。在此图中：

- 流量 B-C 定义隧道并承载加密 ESP 数据。
- 流量 A-D 是用于 FTP 传输的 TCP 连接并通过由流量 B-C 定义的隧道。此流量还包括防火墙用于检查 TCP/FTP 流量的状态信息。该状态信息至关重要，在传输过程中，防火墙会不断更新该状态信息。

注释 为简单起见，每个方向上的反向流量已被忽略。

已禁用持续 IPsec 隧道流量

LAN 到 LAN 隧道丢弃时，流量 A-D 和流量 B-C 以及属于它们的所有状态信息都会被删除。随后，隧道被重建，流量 B-C 被重建，并且能够继续承载隧道数据。但是 TCP/FTP 流量 A-D 出现故障。因为描述 FTP 传输中到目前为止的流量状况的状态信息已被删除，状态防火墙阻止未送达的 FTP 数据，并拒绝创建流量 A-D。已丢失此流量的历史记录的状况会一直存在，防火墙将 FTP 传输视为离群的 TCP 数据包，并将其丢弃。此为默认行为。

已启用持续 IPsec 隧道流量

在启用持续 IPsec 隧道流量功能的情况下，一旦隧道在超时时段内被重建，数据会继续成功流过，因为 ASA 仍然可以访问流量 A-D 中的状态信息。

在启用该功能的情况下，ASA 会单独对待该流量。这意味着，流量 B-C 定义的隧道被丢弃时，流量 A-D 不会被删除。ASA 保留和恢复状态 (TCP) 隧道流量。所有其他流量都被丢弃，并且必须在新隧

道上重建。这不会削弱隧道流量的安全策略，因为在隧道发生故障时，ASA 会丢弃流量 A-D 上抵达的所有数据包。

未丢弃隧道 TCP 流量，因此其依靠 TCP 超时进行清除。但是，如果为特定隧道流量禁用了超时，则该流量会保留在系统中，直到手动或通过其他方法（例如，通过来自对等体的 TCP RST）清除为止。

使用 CLI 配置持续 IPsec 隧道流量

配置示例

持续 IPsec 隧道流量故障排除

对持续 IPsec 隧道流量存在的问题进行故障排除时，**show asp table** 和 **show conn** 命令都十分有用。

持续 IPsec 隧道流量功能是否已启用？

要查看特定隧道是否已启用此功能，请使用 **show asp table** 命令查看与该隧道关联的 VPN 情景。show asp table vpn-context 命令对隧道丢弃后维持状态流量的每个情景显示“+PRESERVE”标志，如以下示例所示（为方便辨认，添加了粗体效果）：

```
hostname(config)# show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0

------------------------------------------------------------------------------

hostname(config)# show asp table vpn-context detail

VPN CTX  = 0x0005FF54

Peer IP  = ASA_Private
Pointer  = 0x6DE62DA0
State    = UP
Flags    = DECR+ESP+PRESERVE
SA       = 0x001659BF
SPI      = 0xB326496C
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN CTX  = 0x0005B234

Peer IP  = ASA_Private
Pointer  = 0x6DE635E0
State    = UP
Flags    = ENCR+ESP+PRESERVE
SA       = 0x0017988D
SPI      = 0x9AA50F43
Group    = 0
```

```
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
hostname(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.
```

定位孤立流量

如果 LAN 间/网络扩展模式隧道丢弃，并且没有在超时之前恢复，则可能存在许多孤立隧道流量。这些流量不会因为隧道发生故障而被拆解，但是试图从中流过的所有数据都会被丢弃。要查看这些流量，请使用 **show conn** 命令，如以下示例所示（出于强调和显示用户输入的目的，添加了粗体效果）：

```
asa2(config)# show conn detail
9 in use, 14 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
```

以下示例显示存在孤立流量时 **show conn** 命令的示例输出，孤立流量以 **V** 标志表示：

```
hostname# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00 bytes 1048 flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle bytes 1048 flags UIOB
```

要将报告内容限定为具有孤立流量的连接，请将 **vpn_orphan** 选项添加至 **show conn state** 命令，如以下示例所示：

```
hostname# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013 idle 0:00:00 bytes 2841019 flags UOVB
```

使用加密存档进行故障排除

关于加密存档

加密问题难以分类。而加密存档可帮助您解决这些问题。加密存档包含有关加密请求的加密会话信息、对等体信息、发送加密请求的组件以及超时的加密会话信息。ASA 不会保存会话的密钥和初始化向量 (IV)。对于 SSL 和 IPsec，您还可以查看以下信息：

- 对于 SSL：会话 SSL 版本、源、目的 IP 地址和端口。
- 对于 IPsec：IPsec 安全关联信息。

一个环可以容纳 2000 个加密命令条目。ASA 会在其中一个环中推送 crypto 命令，并在完成加密请求后提取结果。加密存档文件现在包含超时加密请求的环和条目索引。环及其条目索引有助于对有问题的加密命令进行故障排除。

加密存档有两种格式：文本文件和二进制文件。您可以使用 **debug menu ctm 103** 命令来解码二进制文件。

例如：

```
ASA# debug menu ctm 103 crypto_eng0_arch_4.bin
[Nitrox V Archive Header v1.0 Info]
ASA Image Version: PIX (9.20) #0: Tue Mar 29 16:20:30 GMT 2022
...
SE SSL microcode: CNN5x-MC-SE-SSL-0011
AE microcode: CNN5x-MC-AE-MAIN-0002
Crypto Engine 0
Crash type: SE Ring Timeout
...
Core Soft Resets: 11
...
Timeout Ring (SE): 12
Timeout Entry: 642
SE TIMEOUT:
Core SE 6 Touts: 2
Core SE 8 Touts: 2
Core SE 12 Touts: 4
Core SE 32 Touts: 2
Core SE 37 Touts: 1
.....
[Timeout Session Info]
Active: TRUE
Sync: FALSE
Callback: TRUE
Saved Callback: FALSE
Commands in progress: 1
Engine : hardware
Device : n5 (Nitrox V)
Session : ssl
Priority: normal
NP VPN context handle : 0x00000000
Flag : 0
vcid : 0
Block size : 2050
async cb ring index: 0
tls offload rsa: FALSE
```

```
Session context:
SSL Version : dtls1.2
SSL Context Type : handshake
Encryption Mode : gcm
Auth Algorithm : null
Hash Algorithm : none
Key Size : 32
SSL V : dtls1.2
Source IP : 82.1.2.2
Source Port : 51915
Dest IP : 82.29.155.32
Dest Port : 443
```

在上例中，突出显示的信息显示了超时环、崩溃时间（超时条目）和 SSL 会话信息。

加密存档支持的设备

以下配备 Nitrox V 加密加速器的设备可支持加密存档：

- Cisco Firepower 3105、3110、3120、3130、3140
- Cisco Firepower 4112、4115、4125、4145
- Cisco Firepower 9300 SM-40、SM-48 和 SM-56

使用 SSL 计数器

您可以使用 SSL 计数器来查看 SSL 隧道信息和日志。有关围绕连接建立的状态机转换、其他状态和详细信息可用于帮助进行调试。

debug ssl state 命令提供以下信息：

- 具有关联 IP、端口和协议的远程设备和接口。
- 用于 SSL 连接建立错误的调试。
- 用于验证解密数据填充长度的调试。

使用 **show counters** 命令来查看 SSL 计数器。从版本 9.20.1 开始，有更多的 SSL 计数器可用于调试，例如：

- CNT_SSL_NP_CP_EVENT_NULL
- CNT_SSL_NP_CP_EVENT_ENQUEUE_ERR
- CNT_SSL_NP_CP_EVENT_RELEASE
- CNT_SSL_NP_SNP_FLOW_HNDSHK_FAIL
- CNT_SSL_NP_HDL_LOCK_RELEASE
- CNT_SSL_NP_VERIFY_PADDING
- CNT_SSL_NP_MAX_PAD_LEN_EXCEEDED

- CNT_SSL_NP_NO_CIPHERS_COMPATIBLE
- CNT_SSL_NP_CIPHER_LIC_NOT_GOOD

如何删除停滞的 ASP 表条目

在版本 9.19.1 及更早版本中，如果存在卡住的 ASP 加密规则，则您必须重新启动设备。在版本 9.20.1 及更高版本中，您可以使用 **debug menu asp 100 <encrypt_rule_id>** 命令从 ASP 表中删除停滞的加密规则，而无需重新启动设备。使用 **show asp table classify domain encrypt** 命令查找 *encrypt_rule_id*。

准则

- 由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。我们建议您仅在与思科 TAC 的故障排除会话期间使用此 debug 命令。
- 不会验证检查规则是否停滞。如果系统尝试删除的规则之前已使用此命令删除，则设备将会崩溃。
- 命令 ID 参数必须与 ASP 表中的实际 ID 完全匹配。

示例

在下面的示例中，当流量达到停滞规则 **0x7f039846aaaa** 时，流量会被丢弃，而不是达到良好规则 **0x7f039846bbbb**。您可以从命中计数中识别停滞的规则。停滞规则的命中计数为 9999，而良好规则的命中计数为 0。

1. 使用 **show asp table classify domain encrypt** 命令来查看 ASP 规则。

```
ASAv(config)# show asp table classify domain encrypt
...
out id=0x7f039846aaaa, priority=70, domain=encrypt, deny=false
hits=9999, user_data=0xaaaa, cs_id=0x7f03941866e0, reverse, flags=0x0, protocol=0
src ip/id=1.0.0.0, mask=255.0.0.0, port=0, tag=any
dst ip/id=2.0.0.0, mask=255.0.0.0, port=0, tag=any
src nsg_id=none, dst nsg_id=none
dscp=0x0, input_ifc=any, output_ifc=outside
out id=0x7f039846bbbb, priority=70, domain=encrypt, deny=false //this is a good rule
hits=0, user_data=0xbbbb, cs_id=0x7f03941866e0, reverse, flags=0x0, protocol=0
src ip/id=1.0.0.0, mask=255.0.0.0, port=0, tag=any
dst ip/id=2.0.0.0, mask=255.0.0.0, port=0, tag=any
src nsg_id=none, dst nsg_id=none
dscp=0x0, input_ifc=any, output_ifc=outside
...
```

2. 使用 **debug menu asp 100 <encrypt_rule_id>** 命令从 ASP 表中删除停滞的加密规则

```
ASAv(config)# debug menu asp 100 id=0x7f039846aaaa
Encrypt rule 0x7f0398469510 was successfully deleted.
```

3. 使用 **show asp table classify domain encrypt** 命令来验证 ASA 是否已删除停滞的 ASP 规则。

```
ASAv(config)# show asp table classify domain encrypt
...
out id=0x7f039846bbbb, priority=70, domain=encrypt, deny=false //now this rule has hits
hits=10, user_data=0xbbbb, cs_id=0x7f03941866e0, reverse, flags=0x0, protocol=0
```

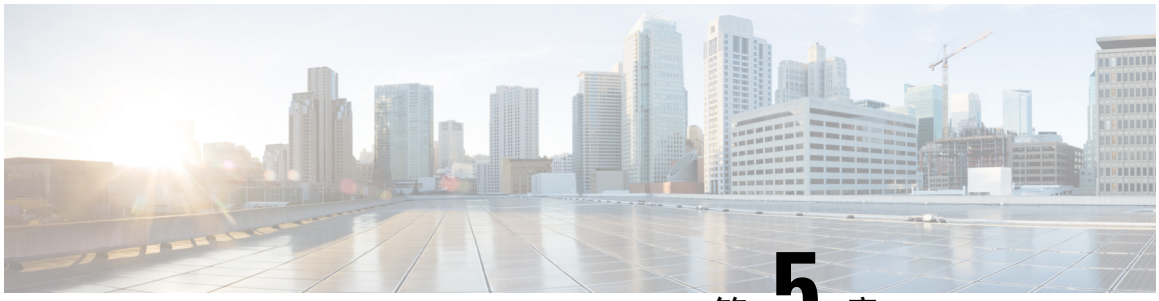
```
src ip/id=1.0.0.0, mask=255.0.0.0, port=0, tag=any
dst ip/id=2.0.0.0, mask=255.0.0.0, port=0, tag=any
src nsg_id=none, dst nsg_id=none
dscp=0x0, input_ifc=any, output_ifc=outside
```

从 ASA 清除 WebVPN 配置

使用 **no webvpn** 和 **clear configure webvpn** 命令时，不会删除默认 WebVPN 配置。会保留 **http_in** 和 **http_out** 计数器以整理压缩统计信息。

要从 ASA 中清除 WebVPN 配置，请执行以下操作之一：

- 启动后使用 **no compression all** 命令禁用压缩统计信息。
- 使用 **clear compression all** 命令清除压缩统计信息计数器。



第 5 章

连接配置文件、组策略和用户

本章介绍如何配置 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。

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。

总之，首先要配置连接配置文件来为连接设置值。然后，配置组策略。这些组策略将用户作为总体为其设置值。然后再配置用户，可以从组继承值并逐一为个别用户配置某些值。本章将介绍配置这些实体的方式和原因。

注释 可使用 **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”经常交替使用。

连接配置文件和组策略可以简化系统管理。为精简配置任务，ASA 提供 LAN 间连接配置文件 (DefaultL2Lgroup)、IKEv2 VPN 的默认远程访问连接配置文件 (DefaultRAgroup)、无客户端 SSL 和 Secure Client SSL 连接的默认连接配置文件 (DefaultWEBVPNgroup) 和默认组策略 (DfltGrpPolicy)。默认连接配置文件和组策略提供对许多用户可能都相同的设置。添加用户时，可以指定其从组策略“继承”参数。这样就可以快速为大量用户配置 VPN 访问。

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，您可能还要允许 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。

注释 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相关，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。

当您启用或禁用 DAP 记录的某个属性时，ASA 会应用并实施该值。例如，在 dap webvpn 配置模式下禁用 HTTP 代理时，ASA 不会进一步查找值。当您对 http-proxy 命令改用 no 值时，DAP 记录中就没有该属性，因此安全设备会下移到用户名中的AAA属性，并且如有必要，再下移到组策略查找要应用的值。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

连接配置文件由一组用于确定隧道连接策略的记录组成。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。连接配置文件包含少量与创建隧道本身有关的属性。连接配置文件还包含一个指针，指向用于定义面向用户的属性的组策略。

ASA 提供以下默认连接配置文件：用于 LAN 间连接的 DefaultL2Lgroup、用于 IPSEC 远程访问连接的 DefaultRAgroup 以及用于 SSL VPN（基于浏览器和 Secure Client）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。

注释 某些配置文件（例如阶段 1 的 IKEv1）可能无法确定终端是远程访问还是 LAN 间。如果它无法确定隧道组，则默认为

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

（默认值为 *DefaultRAGroup*）。

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 间和 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：
  - 用户身份验证
  - 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 - 组策略是一组面向用户的属性。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。
- 密码管理 - 通过此参数可向用户发出当前密码即将在指定天数（默认设置为 14 天）内到期的警告，然后为用户提供机会更改密码。
- 剥除组和剥除领域 - 这些参数向 ASA 指示处理其接收的用户名的方式。这些参数仅适用于收到的 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（如果有）进行身份验证。如果剥除组，则ASA 使用用户名和领域（如果有）进行身份验证。

  输入 strip-realm 命令将在身份验证期间从用户名中删除领域限定符，而输入 strip-group 命令则删除组限定符。如果同时删除两个限定符，身份验证将仅基于用户名。否则，身份验证将基于

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加密钥作为身份验证方法，则最终用户必须提供有效证书才能进行身份验证。
- 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（例如 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) 保持连接设置。通过此功能可使 ASA 监控远程对等体的持续在网状态并向该对等体报告其自己的在网状态。如果对等体变为无响应，则 ASA 会删除该连接。启用 IKE 保持连接可防止在 IKE 对等体失去连接时连接挂起。

  IKE 保持连接有各种形式。为使此功能正常工作，ASA 及其远程对等体必须支持共同的形式。此功能适用于以下对等体：
  - Cisco AnyConnect VPN 客户端
  - 思科 IOS 软件
  - Cisco Secure PIX Firewall

    非思科 VPN 客户端不支持 IKE 保持连接。

    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 保持连接而其他对等体不支持 IKE 保持连接，请对整个组启用 IKE 保持连接。该功能不会影响不支持此功能的对等体。

    如果禁用 IKE 保持连接，则具有无响应对等体的连接会保持活动状态直到其超时为止，因此建议缩短空闲超时。如要更改空闲超时，请参阅配置组策略，第 128 页。

注释 如要减少连接成本，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 保持连接。ISDN 连接通常会在空闲情况下断开连接，但是 IKE 保持连接机制可防止连接空闲，从而避免断开连接。

如果禁用 IKE 保持连接，则客户端仅在其 IKE 或 IPsec 密钥到期时才会断开连接。失败的流量不会如同在启用 IKE 保持连接时一样，使用对等体超时配置文件值断开隧道连接。

如果 LAN 间配置使用的是 IKE 主模式，请确保两个对等体的 IKE 保持连接配置相同。两个对等项均必须启用 IKE 保持连接，或者均必须禁用 IKE 保持连接。

- 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。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

下表提供了特定于 SSL VPN（Secure Client和无客户端）连接的连接配置文件属性的列表。除了这些属性之外，还要配置对于所有 VPN 连接通用的常规连接配置文件属性。

注释 在早期版本中，“连接配置文件”称为“隧道组”。连接配置文件需要使用 tunnel-group 命令进行配置。本章经常交替使用这两个术语。

表 *7: SSL VPN* 的连接配置文件属性

	功能
authentication	设置身份验证方法：AAA 或证书。
customization	确定要应用的以前定义的自定义配置名称。自定义配置用于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 的过程中配置自定义参数。
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。

	功能
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	确定一个或多个组 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。 负载均衡部署将组 URL 用于 Secure Client连接，要求集群中的每个 ASA 节点配置适用于虚拟集群地址的组 URL 以及适用于该节点负载均衡公共地址的组 URL。
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”，则指定 VPN 功能策略。
override-svc-download	覆盖为给远程用户下载 AnyConnect VPN 客户端而配置的下载组策略或用户名属性。
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。

配置连接配置文件

本节介绍单情景模式或多情景模式下连接配置文件的内容和配置。

注释 多情景模式仅适用于站点间的 IKEv2 和 IKEv1，而不适用于 Secure Client、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。

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（包括默认连接配置文件）的当前配置和默认配置，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最大并发 VPN 会话数 + 5 的函数。尝试添加超过限制的其他隧道组会引发以下消息：“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


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 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
```

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 间隧道使用其中一部分属性。有关所有命令的完整说明，请参阅《*Cisco Secure FIrewall ASA* 系列命令参考》。本节按顺序介绍如何配置远程访问连接配置文件和 LAN 间连接配置文件。

配置远程访问连接配置文件

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

- 安全客户端（通过 SSL 或 IPsec/IKEv2 连接）
- 无客户端 SSL VPN（基于浏览器，通过 SSL 连接）
- 思科 ASA 5500 简易 VPN 硬件客户端（通过 IPsec/IKEv1 连接）

我们还提供名为 DfltGrpPolicy 的默认组策略。

如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，第 102 页。
- 配置远程访问连接配置文件常规属性，第 103 页。
- 配置双重身份验证，第 107 页
- 配置远程访问连接配置文件 IPsec IKEv1 属性，第 108 页。
- 配置 IPsec 远程访问连接配置文件 PPP 属性，第 111 页

指定远程访问连接配置文件的名称和类型

过程

输入 **tunnel-group**命令，创建连接配置文件，并指定该连接配置文件的名称和类型。

对于远程访问隧道，类型为 **remote-access**。

tunnel-group *tunnel_group_name* **type remote-access**

示例：

例如，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

如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：

过程

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 配置模式。提示符会更改以表示模式发生更改。

```
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（如果有）的名称。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。以下命令为名为 test 的接口配置特定于接口的身份验证，使用名为 servergroup1 的服务器进行身份验证：

```
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（如果有）的名称。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-groupFinGroup
hostname(config-tunnel-general)#
```

步骤 4 指定要使用的记帐服务器组（如果有）的名称：

```
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。默认设置为无DHCP服务器且无地址池。dhcp-server 命令可用于将 ASA 配置为在尝试获取 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《Cisco Secure Firewall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)#
```

注释
如果指定接口名称，则必须用括号将其括起来。

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

步骤 7 如果使用网络准入控制，请指定NAC身份验证服务器组的名称，用于标识要用于网络准入控制安全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 安全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)
```

注释
NAC 需要远程主机上安装思科信任代理。

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。默认设置为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（如果有）进行身份验证。如果剥除组，则ASA使用用户名和领域（如果有）进行身份验证。输入**strip-realm**命令将在身份验证期间从用户名中删除领域限定符，而使用 strip-group 命令则删除组限定符。如果同时删除两个限定符，身份验证将仅基于用户名。否则，身份验证将基于完整的 *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。

注释
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。

Sun - 在 ASA 上配置的用于访问 Sun 目录服务器的 DN 必须能够访问该服务器上的默认密码策略。建议使用目录管理员或具有目录管理员权限的用户作为 DN。也可以将 ACI 放入默认密码策略。

Microsoft - 必须配置基于 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。默认设置为到期前 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，则可以指定在到期之前多少天（0 到 180）开始警告用户即将到期：

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

注释
在 tunnel-group general-attributes 配置模式下输入的 **password-management** 命令取代了以前在 tunnel-group ipsec-attributes 模式下输入的已弃用的 **radius-with-expiry** 命令。

配置此 **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，用户仍可使用该密码登录。如果尚未配置 RADIUS 或 LDAP 身份验证，ASA 将忽略此命令。

请注意，这不会更改距离密码到期的天数，而是更改ASA在到期之前多少天开始警告用户密码即将到期。

如果指定 **password-expire-in-days** 关键字，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。

有关详细信息，请参阅配置 Microsoft Active Directory 设置以进行密码管理，第 121 页。

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、思科 IPsec VPN 客户端、SSL VPN 完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** 命令需要使用 MS-CHAPv2，因此请咨询您的供应商。

注释
RADIUS 服务器（例如，思科 ACS）可能会将身份验证请求以代理方式发送到另一个身份验证服务器。但是， ASA 仅与 RADIUS 服务器通信。

对于 LDAP，市场上不同的 LDAP 服务器有专有的密码更改方法。目前，ASA 仅对 Microsoft Active Directory 和 Sun LDAP 服务器实施专有密码管理逻辑。本机 LDAP 需要 SSL 连接。在尝试执行 LDAP 密码管理之前，必须先启用基于 SSL 的 LDAP。默认情况下，LDAP 使用端口 636。

步骤 10

步骤 11 指定在从证书派生用于授权查询的名称时要使用的一个或多个属性。此属性指定要将使用者 DN 字段的哪个部分用作授权的用户名：

```
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**（省/自治区/直辖市）、**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。默认设置为不要求授权。

```
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。

过程

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。

注释
此命令仅适用于 AnyConnect 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，请输入以下命令：

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

注释
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
```

要从证书提取以用作次要用户名的DN字段值与主要**username-from-certificate**命令相同。或者，也可以指定 use-script 关键字，该关键字指示 ASA 使用 ASDM 生成的脚本文件。

例如，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 客户端 (AnyConnect) 连接，以及是否要对最终用户隐藏提取的用户名。默认情况下会禁用此功能。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 | client} [hide]
```

例如，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 client
hostname(config-tunnel-general)# secondary-pre-fill-username 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，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，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

如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。以下说明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 间连接配置文件具有更多属性。

过程

步骤 1 如要指定远程访问隧道组的 IPsec 属性，请在单情景或多情景模式下输入以下命令进入 tunnel-group ipsec-attributes 模式。提示符会更改以表示模式发生更改。

```
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，提示符会更改以表示目前处于 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 根据预共享密钥，指定用于支持 IKEv1 连接的预共享密钥。例如，以下命令为 IPsec IKEv1 远程访问连接配置文件指定预共享密钥 xyzx 来支持 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 保持连接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 参数指定在开始保持连接监控之前允许对等体空闲的秒数（10 至 3600）。**retry** 参数是没有收到保持连接响应后的重试间隔（2 至 10 秒）。默认情况下会启用 IKE 保持连接。如要禁用 ISAKMP 保持连接，请输入 **isakmp keepalive disable**。

例如，以下命令将 IKE 保持连接阈值设置为 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 间连接为 10，而 retry 参数的默认值为 2。

如要指定中心站点（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（例如 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。

注释
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 命令时备用。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，以下命令为名为 example-group 的连接配置文件在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

如要为远程访问连接配置文件配置点对点协议属性，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。以下说明假设您已经创建 IPsec 远程访问连接配置文件。

过程

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。提示符会更改以表示模式发生更改：

```
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，提示符会更改以表示目前处于 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，请使用此命令的 **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 间连接配置文件

IPsec LAN 间 VPN 连接配置文件仅适用于 LAN 间 IPsec 客户端连接。虽然您配置的许多参数与 IPsec 远程访问连接配置文件的参数相同，但是 LAN 间隧道的参数更少。以下各节介绍如何配置 LAN 间连接配置文件：

默认 LAN 间连接配置文件配置

默认 LAN 间连接配置文件的内容如下：

```
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
 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 间连接配置文件的参数比远程访问连接配置文件少，并且其中大多数参数对于两个组相同。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 间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 间隧道，类型为 **ipsec-l2l**；例如，如要创建名为 docs 的 LAN 间连接配置文件，请输入以下命令：

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

配置 LAN 间连接配置文件常规属性

如要配置连接配置文件常规属性，请执行以下步骤：

过程

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：

tunnel-group *tunnel-group-name* **general-attributes**

示例：

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)#
```

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

步骤 2 指定默认组策略的名称：

default-group-policy *policyname*

示例：

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 间 IPsec IKEv1 属性

如要配置 IPsec IKEv1 属性，请执行以下步骤：

过程

步骤 1 如要配置隧道组 IPsec IKEv1 属性，请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，以便您为名为 TG1 的连接配置文件的配置参数：

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

提示符会更改以表示现在处于 tunnel-group ipsec-attributes 配置模式。

步骤 2 根据预共享密钥，指定用于支持 IKEv1 连接的预共享密钥。

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

例如，以下命令为 LAN 间连接配置文件指定预共享密钥 XYZX 来支持 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到所有隧道组类型。

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到所有隧道组类型。

步骤 6 指定 ISAKMP (IKE) 保持连接阈值和允许的重试次数。**threshold** 参数指定在开始保持连接监控之前允许对等体空闲的秒数（10 至 3600）。**retry** 参数是没有收到保持连接响应后的重试间隔（2 至 10 秒）。默认情况下会启用 IKE 保持连接。要禁用 IKE 保持连接，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 保持连接阈值设置为 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 间的 **threshold** 参数的默认值为 10，retry 参数的默认值为 2。

如要指定中心站点（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（例如 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。

注释
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)#
```

关于基于标准的 IKEv2 客户端的隧道组

隧道组是包含隧道连接策略的一组记录。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。

IPsec 远程访问的默认隧道组为 DefaultRAGroup。默认隧道组可以修改，但不能删除。

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或EAP身份验证）。因此，通过IKEv2可使用不对称身份验证，其中一端对一个凭证进行身份验证，另一端使用其他凭证（预共享密钥、证书或EAP）。

应该为EAP身份验证配置DefaultRAGroup，因为这些客户端连接无法映射到特定隧道组，除非同时使用证书身份验证和证书 DN 匹配。

基于标准的 IKEv2 属性支持

ASA 支持以下 IKEv2 属性：

- INTERNAL_IP4_ADDRESS/INTERNAL_IP6_ADDRESS - IPv4 或 IPv6 地址

注释 IKEv2 不支持双协议栈（同时分配 IPv4 和 IPv6 地址）。如果同时请求 IPv4 和 IPv6 地址，并且这两种地址都可以分配，则只分配 IPv4 地址。

- INTERNAL_IP4_NETMASK - IPv4 网络掩码
- INTERNAL_IP4_DNS/INTERNAL_IP6_DNS - 主要/辅助 DNS 地址
- INTERNAL_IP4_NBNS - 主要/辅助 WINS 地址
- INTERNAL_IP4_SUBNET/INTERNAL_IP6_SUBNET - 分割隧道列表
- APPLICATION_VERSION - 忽略。出于安全原因，为避免传递任何有关 ASA 的版本信息，不会发送任何响应。但是，客户端配置负载请求可能包括此属性，并且该字符串将显示于ASA上的 **vpn - sessiondb** 命令输出和系统日志中。

DAP 支持

要确保能够按连接类型执行 DAP 策略配置，可使用新的客户端类型 IPsec-IKEv2-Generic-RA 对此连接类型应用特定策略。

远程访问客户端的隧道组选择

下表提供了远程访问客户端及其可用隧道组选项的列表：

远程访问客户端	隧道组列表	组 URL	证书 DN 匹配	默认组 (DefaultRAGroup)	其他
AnyConnect VPN 客户端	支持	支持	支持	支持	不适用
Windows L2TP/IPsec （主模式 IKEv1）	否	否	• 是（使用本地计算机证书时） • 否（使用 PSK 时）	兼容	不适用
基于标准的 IKEv2	否	否	• 是（使用本地计算机证书时） • 否（使用 EAP 身份验证时）	是 **注释** 必须使用 DefaultRAGroup 隧道组。	不适用

基于标准的 IKEv2 客户端的身份验证支持

下表提供了基于标准的 IKEv2 客户端及其支持的身份验证方法的列表：

注释 身份验证方法的限制根据客户端上缺乏支持而定，而非根据 ASA 上缺乏支持而定。所有 EAP 方法身份验证都由 ASA 在客户端与 EAP 服务器之间代理。EAP 方法的支持根据客户端和 EAP 服务器对 EAP 方法的支持而定。

客户端类型/身份验证方法	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	仅证书	PSK
Linux 上的 StrongSwan	N/A	• ISE - 是 • ACS - 是 • FreeRadius - 是 • 通过 FreeRadius 的 AD - 是	• ISE - 是 • ACS - 是 • FreeRadius - 是 • 通过 FreeRadius 的 AD - 是	支持	支持

客户端类型/身份验证方法	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	仅证书	PSK
Android 上的 StrongSwan	N/A	• ISE - 是 • ACS - 是 • FreeRadius - 是 • 通过 FreeRadius 的 AD - 是	否	是	不适用
Windows 7/8/8.1	• ISE - 是 • ACS - 是 • FreeRadius - 是 • 通过 FreeRadius 的 AD - 是	• ISE - 是 • ACS - 是 • FreeRadius - 是 • 通过 FreeRadius 的 AD - 是	不适用	兼容	不适用
Windows Phone	• ISE - 是 • ACS - 是 • FreeRadius - 是 • 通过 FreeRadius 的 AD - 是	• ISE - 是 • ACS - 是 • FreeRadius - 是 • 通过 FreeRadius 的 AD - 是	不适用	不适用	不适用
Samsung Knox	N/A	• ISE - 是 • ACS - 是 • FreeRadius - 是 • 通过 FreeRadius 的 AD - 是	• ISE - 是 • ACS - 是 • FreeRadius - 是 • 通过 FreeRadius 的 AD - 是	兼容	不适用

客户端类型/身份验证方法	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	仅证书	PSK
iOS 8	• ISE - 是 • ACS - 是 • FreeRadius - 是 • 通过 FreeRadius 的 AD - 是	• ISE - 是 • ACS - 是 • FreeRadius - 是 • 通过 FreeRadius 的 AD - 是	不适用	是	是
Android 本机客户端	N/A	• ISE - 是 • ACS - 是 • FreeRadius - 是 • 通过 FreeRadius 的 AD - 是	不适用	支持	支持

添加多证书身份验证

我们对汇聚身份验证协议进行了扩展，以便定义用于多证书身份验证的协议交换并将此功能用于两种会话类型。客户端建立SSL连接并进入聚合身份验证后，系统将建立另一个SSL连接，ASA会发现客户端需要进行证书身份验证并请求客户端证书。

ASA 针对远程访问类型隧道组的 Secure Client 连接配置所需身份验证。系统使用现有方法（例如证书规则映射、组 URL 等）执行隧道组映射，但是稍后将就所需身份验证方法与客户端进行协商。

示例

tunnel-group <name> webvpn-attributes

authentication {aaa [certificate | multiple-certificate] | multiple-certificate [aaa | saml] | saml [certificate | multiple-certificate]}

身份验证选项包括：仅AAA、仅证书、仅多证书、AAA和证书、AAA和多证书以及SAML、SAML、SAML 和证书或多重证书和 SAML。

```
ASA(config)# tunnel-group AnyConnect webvpn-attributes
ASA(config-tunnel-webvpn)# authentication?
tunnel-group-webvpn mode commands/options:
aaa         Use username and password for authentication
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
saml   Use SAML for authentication
ASA(config-tunnel-webvpn)# authentication multiple-certificate?

tunnel-group-webvpn mode commands/options:
aaa  Use username and password for authentication
```

```
saml  Use SAML for authentication
<cr>

ASA(config-tunnel-webvpn)# authentication aaa?

tunnel-group-webvpn mode commands/options:
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
<cr>ASA(config-tunnel-webvpn)# authentication aaa?

ASA(config-tunnel-webvpn)# authentication saml?
tunnel-group-webvpn mode commands/options:
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
<cr>
```

为 EAP 身份检索配置 query-identity 选项

Microsoft Windows 7 IKEv2 客户端发送一个 IP 地址作为互联网密钥交换 (IKE) 身份，它可阻止思科 ASA 服务器使用其有效地进行隧道组查找。ASA 必须使用 EAP 身份验证的 **query-identity** 选项进行配置，才能允许 ASA 从该客户端检索有效的 EPA 身份。

对于基于证书的身份验证，ASA 服务器和 Microsoft Windows 7 客户端证书必须如下配置扩展密钥用法 (EKU) 字段：

- 对于客户端证书，EKU 字段 = 客户端身份验证证书。
- 对于服务器证书，EKU 字段 = 服务器身份验证证书。

可以从 Microsoft 证书服务器或其他 CA 服务器获取证书。

对于 EAP 身份验证，Microsoft Windows 7 IKEv2 客户端需要先收到 EAP 身份请求，然后才能接收任何其他 EAP 请求。请务必在 IKEv2 ASA 服务器上的隧道组配置文件中配置 **query-identity** 关键字，以便向客户端发送 EAP 身份请求。

注释 IKEv2 支持 DHCP 拦截，以允许 Windows 分割隧道。此功能只适用于 IPv4 分割隧道属性。

过程

步骤 1 要将连接类型设置为 IPsec 远程访问，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：

在以下示例中，IKEv2 预共享密钥配置为 44kkaol59636jnfx：

```
hostname(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 44kkaol59636jnfx
```

注释
必须配置 **ikev2 remote-authentication pre-shared-key** 命令或 **ikev2 remote-authentication certificate** 命令来完成身份验证。

步骤 2 要指定可扩展身份验证协议 (EAP) 作为通过基于标准的第三方 IKEv2 远程访问客户端支持用户身份验证的方法，请使用 **ikev2 remote-authentication eap** [**query-identity**] 命令。

注释
必须先使用证书配置本地身份验证，并使用 **ikev2 local-authentication** {**certificate** *trustpoint*} 命令配置有效信任点，然后才能对远程身份验证启用 EAP。否则，会拒绝 EAP 身份验证请求。

可以配置多个选项，使客户端能够使用配置的任何（但不是全部）选项进行远程身份验证。

对于 IKEv2 连接，隧道组映射必须知道哪些身份验证方法允许远程身份验证（PSK、证书和 EAP）和本地身份验证（PSK 和证书），以及哪个信任点用于本地身份验证。当前，使用从对等体或对等体证书字段值（使用证书映射）获取的 IKE ID 执行映射。如果这两个选项失效，则传入的连接将映射到默认远程访问隧道组 DefaultRAGroup。仅当远程对等体通过证书进行身份验证时，证书映射选项才适用。此映射允许映射到不同的隧道组。仅对证书身份验证使用规则或默认设置执行隧道组查找。对于 EAP 和 PSK 身份验证，使用客户端上的 IKE ID（与隧道组名称匹配）或使用默认设置执行隧道组查找。

对于 EAP 身份验证，除非客户端允许独立配置 IKE ID 和用户名，否则必须使用 DefaultRAGroup 隧道组。

以下示例显示遭到拒绝的身份验证的 EAP 请求：

```
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 12345678
ERROR: The local-authentication method is required to be certificate based
if remote-authentication allows EAP
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

步骤 3 保存更改。

```
hostname(config)# write memory
hostname(config)#
```

要验证隧道是否启动并正常运行，请使用 **show vpn-sessiondb summary** 或 **show crypto ipsec sa** 命令。

配置 Microsoft Active Directory 设置以进行密码管理

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。

- Sun - 在 ASA 上配置的用于访问 Sun 目录服务器的 DN 必须能够访问该服务器上的默认密码策略。建议使用目录管理员或具有目录管理员权限的用户作为 DN。也可以将 ACI 放入默认密码策略。
- Microsoft - 必须配置基于 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。本节介绍与各种密码管理操作关联的 Active Directory 设置。这些说明假设您已在 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。本节假设您使用 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：

过程

步骤 1 依次选择**开始 (Start)** > **程序 (Programs)** > **管理工具 (Administrative Tools)** > **Active Directory 用户和计算机 (Active Directory Users and Computers)**。

步骤 2 右键点击并依次选择**用户名 (Username)** > **属性 (Properties)** > **账户 (Account)**。

步骤 3 选中**用户必须在下一次登录时更改密码 (User must change password at next logon)** 复选框。

此用户下次登录时，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**最小密码长度 (Minimum password length)**。

使用 Active Directory 指定最长密码期限

如要增强安全性，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：

注释 已弃用 **radius-with-expiry** 命令，该命令以前配置为 tunnel-group remote-access 配置的一部分以执行密码期限功能。取而代之的是在 tunnel-group general-attributes 模式下输入的 **password-management** 命令。

过程

步骤 1 依次选择**开始 (Start)** > **程序 (Programs)** > **管理工具 (Administrative Tools)** > **域安全策略 (Domain Security Policy)** > **Windows 设置 (Windows Settings)** > **安全设置 (Security Settings)** > **账户策略 (Account Policies)** > **密码策略 (Password Policy)**。

步骤 2 双击“密码最长期限”。

步骤 3 选中**定义此策略设置 (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）。

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：

过程

步骤 1 依次选择**开始 (Start)** > **程序 (Programs)** > **管理工具 (Administrative Tools)** > **域安全策略 (Domain Security Policy)**。

步骤 2 依次选择**Windows 设置 (Windows Settings)** > **安全设置 (Security Settings)** > **账户策略 (Account Policies)** > **密码策略 (Password Policy)**。

步骤 3 双击**最小密码长度**。

步骤 4 选中**定义此策略设置 (Define this policy setting)** 复选框并指定密码必须包含的最小字符数。

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：

过程

步骤 1 依次选择**开始 (Start)** > **程序 (Programs)** > **管理工具 (Administrative Tools)** > **域安全策略 (Domain Security Policy)**。依次选择 **Windows 设置 (Windows Settings)** > **安全设置 (Security Settings)** > **账户策略 (Account Policies)** > **密码策略 (Password Policy)**。

步骤 2 双击“密码必须满足复杂性要求”以打开“安全策略设置”对话框。

步骤 3 选中“定义此策略设置”(Define this policy setting) 复选框并选择**启用 (Enable)**。

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支持 Secure Client的 RADIUS/SDI 消息

本节介绍相应程序来确保使用 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。

注释 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。

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。

在身份验证过程中，RADIUS 服务器向 ASA 显示访问质询消息。这些质询消息中有包含来自 SDI 服务器的文本的应答消息。ASA 直接与某 SDI 服务器通信时的消息文本与通过 RADIUS 代理通信时的消息文本不同。因此，为了向 Secure Client 显示为本地 SDI 服务器，ASA 必须解析来自 RADIUS 服务器的消息。

此外，由于 SDI 消息在 SDI 服务器上可配置，ASA 的消息文本必须与 SDI 服务器的消息文本（全部或部分）匹配。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。Secure Client可能无法响应，并且身份验证可能会失败。

配置安全设备以支持 RADIUS/SDI 消息，第 124 页 介绍如何配置 ASA 以确保在客户端与 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 Secure Client 用户执行相应的操作，请执行以下步骤：

过程

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。

示例：

```
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** 命令配置 ASA 上的 RADIUS 应答消息文本，使其与 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。如果您使用思科安全ACS，且它使用默认消息文本，则您无需在ASA上配置消息文本。否则，请使用**proxy-auth_map sdi** 命令确保消息文本匹配。

下表显示消息代码、默认 RADIUS 回复消息文本和每个消息的功能。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，必须确保用于消息文本的字符串不是其他字符串的一部分。

例如，对于 new-pin-sup 和 next-ccode-and-reauth，“new PIN”均是默认消息文本的一部分。如果您将 new-pin-sup 配置为“new PIN”，则当安全设备从 RADIUS 服务器收到“new PIN with the next card code”时，它将此文本与 new-pin-sup 代码（而不是 next-ccode-and-reauth 代码）匹配。

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	表示用户必须输入不含 PIN 的 NEXT 令牌代码。
new-pin-sup	Please remember your new PIN	表示已提供新的系统 PIN 并向用户显示该 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	表示用户生成的 PIN 并请求用户输入此 PIN。
new-pin-reenter	Reenter PIN:	在内部由 ASA 用于确认用户提供的 PIN。客户端确认 PIN 而不提示用户。
new-pin-sys-ok	New PIN Accepted	表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，表示用户必须等待下一个令牌代码并输入新 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	在内部由 ASA 用于表示用户已为系统生成的 PIN 做好准备。

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

本节介绍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 连接的一组面向用户的属性/值对。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。通过组策略可将整组属性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
- 筛选条件
- 客户端配置设置
- 连接设置

修改默认组策略

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继承其值。

注释 在 DfltGrpPolicy 上配置（然后分配到）的Secure Client配置文件，包括任何或所有Secure Client配置文件类型（例如网络访问管理器、Umbrella 等），除非其他组策略明确配置为从 DfltGrpPolicy 继承。换而言之，在组策略上配置特定Secure Client配置文件时，不会继承与 DfltGrpPolicy 关联的Secure Client配置文件。

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)#
```

注释 默认组策略始终为 internal。尽管命令语法为 hostname(config)# group-policy DfltGrpPolicy {internal | external}，但是无法将其类型更改为 external。

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
```

注释 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

 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

  http-proxy disable

  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

  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

  anyconnect ssl df-bit-ignore disable
  anyconnect routing-filtering-ignore disable

  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。在每种情况下，如果没有显式定义参数，则组从默认组策略获取值。

可以在单情景模式或多情景模式下执行这些配置任务：

注释 多情景模式仅适用于站点间 IKEv2 和 IKEv1，而不适用于 AnyConnect、无客户端 SSL VPN、Apple 本机 VPN 客户端、Microsoft 本机 VPN 客户端或 IKEv1 IPsec 的 cTCP。

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，则必须确保二者之间没有名称重复。

注释 ASA 上的外部组名引用 RADIUS 服务器上的用户名。换句话说，如果在 ASA 上配置外部组 X，则 RADIUS 服务器将查询视为用户 X 的身份验证请求。因此，外部组其实只是 RADIUS 服务器上对 ASA 具有特殊意义的用户账户。如果外部组属性与计划进行身份验证的用户存在于同一RADIUS服务器中，则其之间不得有任何名称重复。

ASA 在外部 LDAP 或 RADIUS 服务器上支持用户授权。将 ASA 配置为使用外部服务器之前，必须使用正确的ASA授权属性来配置该服务器，并从其中一部分属性向个人用户分配特定权限。按照为 VPN 配置外部 AAA 服务器，第 283 页中的说明配置外部服务器。

过程

要配置外部组策略，请执行以下步骤并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)#
```

注释
对于外部组策略，RADIUS 是唯一支持的 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)#
```

注释
可以配置多个特定于供应商的属性 (VSA)，如为 VPN 配置外部 AAA 服务器，第 283 页中所述。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

要配置内部组策略，请进入配置模式，使用 group-policy 命令为组策略指定名称和 **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)#
```

注释 创建组策略后，无法更改其名称。

通过附加关键字 **from** 并指定现有策略的名称，可以复制原本已有的组策略的值来配置内部组策略的属性：

```
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)#
```

配置内部组策略常规属性

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，请参阅创建内部组策略，第 130 页。

配置组策略横幅消息

指定要显示的横幅或欢迎消息（如果有）。默认无横幅。当远程客户端连接时，在其之上会显示指定的消息。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 500 个字符。

注释 确保在横幅对话框中使用正常的换行符，而不是“\n”。

在 ASA 版本 9.5.1 中，登录后在 VPN 远程客户端上显示的整体标志长度已从 510 个字符增至 4000 个字符。

注释 横幅中包含的回车符和换行符计作两个字符。

要删除横幅，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横幅。

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** 关键字而不要指定横幅字符串的值，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 的组策略创建横幅：

```
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。

可以指定最多包含六个本地地址池的列表用于本地地址分配。地址池的指定顺序非常重要。ASA 按照这些地址池在此命令中出现的顺序分配这些地址池中的地址。

将 IPv4 地址池分配给内部组策略

开始之前

创建 IPv4 地址池。

过程

步骤 1 进入组策略配置模式。

group-policy *value* **attributes**

示例：

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
```

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

步骤 2 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。

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)#
```

步骤 3 （可选） 使用 **no address-pools value pool-name** 命令从组策略配置中删除地址池，并返回地址池设置来从其他源（例如 DefltGroupPolicy）继承地址池信息。

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)#
```

步骤 4 （可选） **address-pools none** 命令禁止从其他策略源（例如 DefltGrpPolicy）继承此属性：

```
hostname(config-group-policy)# address-pools none
hostname(config-group-policy)#
```

步骤 5 （可选） **no address pools none** 命令从组策略中删除 **address-pools none** 命令，从而恢复默认值，即允许继承。

```
hostname(config-group-policy)# no address-pools none
hostname(config-group-policy)#
```

将 IPv6 地址池分配给内部组策略

开始之前

创建 IPv6 地址池。请参阅VPN 的 IP 地址，第 179 页。

过程

步骤 1 进入组策略配置模式。

group-policy *value* **attributes**

示例：

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

步骤 2 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。

示例：

此示例显示向 FirstGroup 组策略分配 ipv6-pool1、ipv6-pool2 和 ipv6-pool3。

```
hostname(config-group-policy)# ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3
hostname(config-group-policy)#
```

步骤 3 （可选） 使用 **no ipv6-address-pools value pool-name** 命令从组策略配置中删除地址池，并返回地址池设置来从其他源（例如 DfltGroupPolicy）继承地址池信息。

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)#
```

步骤 4 （可选） 使用 **ipv6-address-pools none** 命令禁止从其他策略源（例如 DfltGrpPolicy）继承此属性。

```
hostname(config-group-policy)# ipv6-address-pools none
hostname(config-group-policy)#
```

步骤 5 （可选） 使用 **no ipv6-address pools none** 命令从组策略中删除 **ipv6-address-pools none** 命令，从而恢复默认值，即允许继承。

```
hostname(config-group-policy)# no ipv6-address-pools none
hostname(config-group-policy)#
```

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} 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。要从运行配置中删除属性，请输入此命令的 **no** 形式。

此命令的参数值包括：

- ikev1 - 在两个对等体（思科 VPN 客户端或其他安全网关）之间协商 IPsec IKEv1 隧道。创建管理身份验证、加密、封装和密钥管理的安全关联。

- ikev1 - 在两个对等体（Secure Client或其他安全网关）之间协商 IPsec IKEv2 隧道。创建管理身份验证、加密、封装和密钥管理的安全关联。
- **l2tp-ipsec**- 协商 L2TP 连接的 IPsec 隧道。
- ssl-client - 使用 TLS 或 DTLS 与 Secure Client协商 SSL 隧道。

输入此命令以配置一个或多个隧道模式。至少必须配置一个隧道模式供用户通过 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

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

注释 使用 IPv6 执行 VLAN 映射时，对于每个 VLAN 而言，外部 （目标） 地址必须是唯一地址，以便解密流量路由至内部网络。同一目标网络的 VLAN 和路由指标必须相同。

- 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：

  [**no**] **vlan** {*vlan_id* |**none**}

  no vlan 从组策略中删除 *vlan_id*。组策略从默认组策略继承 vlan 值。

  none 从组策略中删除 *vlan_id* 并对此组策略禁用 VLAN 映射。组策略不会从默认组策略继承 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。

注释 对于无客户端 VPN 连接，出口 VLAN 功能仅适用于 HTTP 协议。

- 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。可以使用 vpn-filter 命令指定 IPv4 或 IPv6 ACL。

注释 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。

要删除 ACL，包括通过输入 **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** 关键字而不要指定 ACL 名称。**none** 关键字表示没有 ACL 并设置空值，从而禁止使用 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 命令应用于解密后流量（在其退出隧道后）和解密前流量（在其进入隧道前）。不得将用于 vpn-filter 的 ACL 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 到 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** 位置交换。

另请注意，VPN 过滤器仅适用于初始连接。它不适用于因应用检查操作而打开的辅助连接，例如 SIP 媒体连接。

在以下示例中，vpn-filter 用于远程访问 VPN 客户端。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 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 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
```

注释 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 端口上发起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 端口上发起与本地网络的连接。

在下一个示例中，vpn-filter 用于 LAN 到 LAN VPN 连接。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 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 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
```

注释 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 端口上发起与远程网络的连接。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 端口上发起与本地网络的连接。

指定组策略的 VPN 访问时长

开始之前

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”。

过程

步骤 1 进入组策略配置模式。

group-policy *value* **attributes**

示例：

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
```

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

步骤 2 可以通过在 group-policy 配置模式下使用 **vpn-access-hours** 命令将配置的时间范围策略与组策略关联来设置 VPN 访问时长。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 访问时长设置为空值，即允许 no time-range 策略。

vpn-access-hours value {*time-range-name* | **none**}

示例：

```
hostname(config-group-policy)# vpn-access-hours value business-hours
hostname(config-group-policy)#
```

指定组策略的 VPN 同时登录数

您可以为组策略设置一个特定用户可维持的同时会话数限制。默认值为 3 个同时会话。

即使已使用同一用户名建立“新”会话，停滞的 Secure Client 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。

如果允许的同时会话数为 1，并且同一用户在异常终止后再次登录，则会从数据库中删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删除第一个会话并建立新会话。

如果允许的同时会话数大于 1，则当用户达到该最大数量并尝试再次登录时，会注销空闲时间最长的会话。如果所有当前会话的空闲时间同样长，则会注销最早的会话。此操作会释放一个会话并允许新用户登录。

一旦达到最大会话限制，系统需要一些时间才能删除最早的会话。因此，用户可能无法立即登录，并且可能必须在成功完成新的连接之前重试新连接。如果用户按预期注销会话，应该就不会出现此问题。您可以将系统配置为不等待删除完成并立即允许新用户连接，从而删除延迟。

过程

	命令或操作	目的
步骤 1	在 group-policy 配置模式下使用 **vpn-simultaneous-logins** *integer* 命令指定对任何用户允许的同时登录数。	**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 则禁用登录并阻止用户访问。以下示例显示如何为名为 FirstGroup 的组策略设置最大同时登录数 4： `hostname(config)# group-policy FirstGroup attributes`

	命令或操作	目的
		hostname(config-group-policy)# **vpn-simultaneous-logins 4** 注释 • 尽管同时登录数的上限非常大，但允许多个用户同时登录可能会降低安全性并影响性能。 • 当连接到使用不同组策略的不同隧道组时， **vpn-simultaneous-logins** 会删除用户会话，即使现有会话使用不同的组策略。
步骤 2	（可选。）在达到同时登录限制时，将系统配置为建立新会话，而不等待删除最早的会话。	**vpn-simultaneous-login-delete-no-delay** 默认情况下该选项处于禁用状态。 hostname(config)# **group-policy FirstGroup attributes** hostname(config-group-policy)# **vpn-simultaneous-login-delete-no-delay**

限制对特定连接配置文件的访问

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 要求用户连接的现有连接配置文件的名称。组锁定通过检查在 VPN 客户端中配置的组与用户分配的连接配置文件是否相同来限制用户。如果不一样，ASA 会阻止用户进行连接。如果不配置组锁定，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。

要从运行配置中删除 **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。它还可防止从默认或指定的组策略继承 group-lock 值

指定组策略中的最长 VPN 连接时间

过程

步骤 1 （可选） 在 group-policy 配置模式或 username 配置模式下使用 **vpn-session-timeout** {*minutes* 命令配置 VPN 连接的最长时间。

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 将终止连接。

以下示例显示如何将名为 FirstGroup 的组策略的 VPN 会话超时设置为 180 分钟：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

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
hostname(config-username)#
```

其他 [**no**] **vpn-session-timeout** {*minutes* | **none**} 命令的其他操作：

- 要从此策略中删除属性并允许继承，请输入此命令的 **no vpn-session-timeout** 形式。
- 要允许无限超时期，并因此防止继承超时值，请输入 **vpn-session-timeout none**。

步骤 2 使用 **vpn-session-timeout alert-interval** {*minutes*|} 命令，配置向用户显示会话超时警报消息的时间。

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。以下示例显示如何指定用户在其 VPN 会话断开连接之前 20 分钟收到通知。可以指定的范围为 1 至 30 分钟。

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

其他 [**no**] **vpn-session-timeout alert-interval** {*minutes* | **none**} 命令的其他操作：

- 使用该命令的 no 形式表示将从默认组策略继承 VPN 会话超时 alert-interval 属性：

  ```
  hostname(config-webvpn)# no vpn-session-timeout alert-interval
  ```

- **vpn-session-timeout alert-interval none** 表示用户将不会收到警报。

指定组策略的 VPN 会话空闲超时

过程

步骤 1 （可选） 要配置 VPN 空闲超时期限，请在 group-policy 配置模式或 username 配置模式下使用 **vpn-idle-timeout** *minutes* 命令。

如果在此期间连接上没有通信活动，则 ASA 将终止此连接。最小值为 1 分钟，最大值为 35791394 分钟，默认值为 30 分钟。

以下示例展示如何将名为 FirstGroup 的组策略的 VPN 空闲超时设置为 15 分钟：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

其他 [**no**] **vpn-idle-timeout** {*minutes* | **none**} 命令的其他操作：

- 输入 **vpn-idle-timeout none** 以禁用 VPN 空闲超时并防止继承超时值。

  ```
  hostname(config)# group-policy FirstGroup attributes
  hostname(config-group-policy)# vpn-idle-timeout none
  hostname(config-group-policy)#
  ```

  这将致使 Secure Client（SSL 和 IPsec/IKEv2）和无客户端 VPN 使用全局 webvpn **default-idle-timeout** *seconds* 值。在 webvpn-config 模式下输入此命令，例如：`hostnamee(config-webvpn)# default-idle-timeout 300`。默认值为 1800 秒（30 分钟），范围为 60 至 86400 秒。

  对于所有 webvon 连接，仅当系统在组策略/用户名属性中设置 **vpn-idle-timeout none** 时，才会实施 **default-idle-timeout** 值。对于所有 Secure Client 连接，ASA 需要一个非零的空闲超时值。

  对于站点间（IKEv1、IKEv2）和 IKEv1 远程访问 VPN，我们建议禁用超时并允许无限制的空闲期。

- 要禁用此组策略或用户策略的空闲超时，请输入 **no vpn-idle-timeout**。系统将继承该值。
- 如果未设置 **vpn-idle-timeout**，那么系统无论如何都会继承该值，默认值为 30 分钟。

注释
vpn-idle-timeout 只能控制父会话的最长时间。子会话 (SSL/DTLS) 会因硬编码的 5 分钟 TCP 非活动超时或未能通过 3 次对等体存活检测 (DPD) 检查而提前终止。有关详细信息，请参阅 配置对等体存活检测中的说明。有关 DPD、保持连接和超时属性的更多详细信息，请参阅 AnyConnect 常见问题解答 - 隧道、DPD 和非活动计时器 (AnyConnect FAQ - Tunnels, DPDs, and Inactivity Timer)。

步骤 2 （可选） 使用 **vpn-idle-timeout alert-interval** {*minutes*} 命令，可以选择性地配置向用户显示空闲超时警报消息的时间。

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。默认警报间隔为一分钟。

以下示例显示如何为名为 anyuser 的用户设置 3 分钟的 VPN 空闲超时警报间隔：

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout alert-interval 3
hostname(config-username)#
```

其他 [**no**] **vpn-idle-timeout alert-interval** {*minutes* | **none**} 命令的其他操作：

- **none** 参数表示用户将不会收到警报。

  ```
  hostname(config)# username anyuser attributes
  hostname(config-username)# vpn-idle-timeout none
  hostname(config-username)#
  ```

- 要删除此组或用户策略的警报间隔，请输入 **no vpn-idle-timeout alert-interval**。系统将继承该值。
- 如果未设置此参数，则默认警报间隔为一分钟。

为组策略配置 WINS 和 DNS 服务器

可以指定主要和辅助 WINS 服务器和 DNS 服务器。每种情况下的默认值为 none。如要指定这些服务器，请执行以下步骤：

过程

步骤 1 指定主要和辅助 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 地址是辅助 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，这将禁止使用 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，第二条命令会覆盖第一条，并且 y.y.y.y 会成为唯一 WINS 服务器。对于多台服务器情况也如此。如要添加 WINS 服务器而不覆盖以前配置的服务器，请在输入此命令时包含所有 WINS 服务器的 IP 地址。

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 指定主要和辅助 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 地址是辅助 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，这将禁止使用 DNS 服务器并防止从默认或指定的组策略继承值。最多可以指定四个 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，第二条命令将覆盖第一条，并且 y.y.y.y 成为唯一 DNS 服务器。对于多台服务器情况也如此。如要添加 DNS 服务器而不覆盖以前配置的服务器，请在输入此命令时包含所有 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 **DefaultDNS DNS** 服务器组中未指定默认域名，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 （可选。）配置 DHCP 网络范围：

dhcp-network-scope {*ip_address* | **none**}

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

如未定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将检查各个池，直到发现未分配的地址为止。

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

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

指定 **none** 可阻止 DHCP 地址分配，例如从默认或继承的组策略进行分配。

示例：

以下是进入 FirstGroup 的属性配置模式，并将 DHCP 范围设置为 10.100.10.1 的示例。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```

设置分割隧道策略

通过指定分割隧道策略为 IPv4 流量设置通过隧道传送流量的规则：

split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

no split-tunnel-policy

通过指定分割隧道策略为 IPv6 流量设置通过隧道传送流量的规则：

ipv6-split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

no ipv6-split-tunnel-policy

策略选项包括：

- **tunnelspecified** - 通过隧道在网络列表中指定的网络上传入或传出所有流量。发往所有其他地址的数据则明文传送，并由远程用户的互联网运营商路由。

  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。

- **excludespecified** - 不在网络列表中指定的网络上通过隧道传入或传出流量。进出所有其他地址的流量通过隧道传送。。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。此选项仅适用于 Secure Client。

注释 客户端会忽略排除列表中的并非包含列表的子集的网络。

- **tunnelall** —指定所有流量都通过隧道。此策略禁用分割隧道。远程用户能够访问企业网络，但无法访问本地网络。这是默认选项。

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

示例

以下示例显示如何为 IPv4 和 IPv6 设置一个分割隧道策略，仅通过隧道传送名为 FirstGroup 的组策略的指定网络：

```
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
```

指定分割隧道的网络列表

在分割隧道中，网络列表确定通过隧道传送的网络流量。Secure Client 根据网络列表（即 ACL）制定分割隧道决策。

```
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** - 表示分割隧道没有网络列表，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分割隧道网络列表，从而禁止分割隧道。它还可防止从默认或指定的组策略继承默认分割隧道网络列表。

要删除网络列表，请输入此命令的 **no** 形式。要删除所有分割隧道网络列表，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）。

当没有分割隧道网络列表时，用户将继承默认或指定组策略中存在的任意网络列表。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 是一个排除列表和一个属于该排除列表一部分的包含列表：

```
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 分割隧道策略添加到名为 GroupPolicy_ipv6-ikev2 的组策略。v6 是一个排除列表和一个属于该排除列表一部分的包含列表：

```
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
```

验证分割隧道配置

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
```

配置分割隧道的域属性

可以指定要通过分割隧道解析的默认域名或域列表，我们称之为分割 DNS。

AnyConnect 3.1 对于 Windows 和 Mac OS X 平台支持真分割 DNS 功能。如果安全设备上的组策略启用分割-包含隧道，并且如果其指定要通过隧道传送的 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。真分割 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。这些请求并非明文发送。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 解析器以明文提交主机名来进行 DNS 解析。

注释 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 协议使用真分割 DNS：

- 为组策略中的一种 IP 协议（例如 IPv4）配置分割 DNS 并为另一种 IP 协议（例如 IPv6）配置客户端绕行协议（对后一种 IP 协议不配置地址池）。
- 为两个 IP 协议都配置分离 DNS。

定义默认域名

ASA 将默认域名传递到 Secure Client。客户端将域名附加到省略域字段的 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。

要为组策略的用户指定默认域名，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，这将禁止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
```

定义分割隧道的域列表

除默认域以外，输入要通过分割隧道解析的域列表。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。

当没有分割隧道域列表时，用户将继承默认组策略中存在的任意域列表。要防止用户继承此类分割隧道域列表，请输入带有 **none** 关键字的 **split-dns** 命令。

要删除所有分割隧道域列表，请输入不带参数的 **no split-dns** 命令。这会删除所有已配置的分割隧道域列表，包括通过发出带 **none** 关键字的 **split-dns** 命令创建的空列表。

参数 **value** domain-name 提供 ASA 通过分割隧道解析的域名。**none** 关键字表示没有任何分割 DNS 列表。它还使用空值来设置分割 DNS 列表，从而禁止使用分割 DNS 列表，并防止从默认或指定的组策略继承分割 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，但整个字符串不能超过 492 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分割隧道解析的域 Domain1、Domain2、Domain3 和 Domain4：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

注释 当配置分割 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 和分割隧道配置 DHCP 拦截

如果分割隧道选项超过 255 个字节，则 Microsoft XP 会异常导致域名的损坏。为避免此问题，ASA 将其发送的路由数限制为 27 至 40 条路由，并且路由数取决于路由类。

通过 DHCP 拦截，Microsoft Windows XP 客户端可将分割隧道与 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。这对于不适合使用 DHCP 服务器的环境很有用。

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** 形式会从配置中删除 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
```

配置用于远程访问客户端的浏览器代理设置

按照以下步骤配置客户端的代理服务器参数。

过程

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)#
```

默认值是 **none**，这并不指定客户端设备浏览器上的任何代理服务器设置。要从配置中删除该属性，请使用此命令的 **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 **no-modify**。要从配置中删除该属性，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**—禁用客户端设备浏览器中的 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绕行配置浏览器代理例外列表设置。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)#
```

要从配置中删除该属性，请使用此命令的 **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 地址或名称以及适用于此客户端设备的端口。端口号可选。
- **none**- 表示没有任何 IP 地址/主机名或端口并防止继承例外列表。

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例外列表，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绕行设置。

```
hostname(config-group-policy)# msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

要从配置中删除该属性，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绕行：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy local-bypass enable
hostname(config-group-policy)#
```

为 IPsec (IKEv1) 客户端配置安全属性

如要指定组的安全设置，请执行以下步骤。

过程

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。

要从运行配置中删除 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）。

注释
IPsec IKEv2 连接不支持 IP 压缩。

```
hostname(config-group-policy)# ip-comp {enable | disable}
hostname(config-group-policy)#
```

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。

要从运行配置中删除 **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使用调制解调器连接的远程拨入用户的数据传输速率。

提示
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，建议仅对使用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。

注释
IKEv2 连接不支持 IKE 重新生成密钥。

如果启用在 IKE 重新生成密钥时重新进行身份验证，则 ASA 会在初始阶段 1 IKE 协商期间提示用户输入用户名和密码，此外只要 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，用户可能会发现重复的授权请求十分不便。如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** 命令查看以秒为单位和以千字节数据为单位的安全关联生命周期。要禁用在 IKE 重新生成密钥时重新进行用户身份验证，请输入 **disable** 关键字。默认情况下，会禁用在 IKE 重新生成密钥时重新进行身份验证。

```
hostname(config-group-policy)# re-xauth {enable | disable}
hostname(config-group-policy)#
```

要允许从其他组策略继承用于在 IKE 重新生成密钥时重新进行身份验证的值，请输入此命令的 **no** 形式从运行配置中删除 re-xauth 属性：

```
hostname(config-group-policy)# no re-xauth
hostname(config-group-policy)#
```

注释
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 指定是否启用完全向前保密。在 IPsec 协商过程中，完全向前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向前保密的值。默认情况下会禁用完全向前保密。要启用完全向前保密，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)#
```

要禁用完全向前保密，请输入带有 **disable** 关键字的 **pfs** 命令。

要从运行配置中删除完全向前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)#
```

为 IKEv1 客户端配置 IPsec-UDP 属性

借助 IPsec over UDP（有时称为通过 NAT 的 IPSec），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
```

要使用 IPsec over UDP，还必须配置 **ipsec-udp-port** 命令，如本节中所述。

要禁用 IPsec over UDP，请输入 **disable** 关键字。要从运行配置中删除 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。

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。

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 的端口值。

```
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

过程

步骤 1 （可选） 使用以下命令配置网络扩展模式：

[**no**] **nem** [**enable** | **disable**]

网络扩展模式可让硬件客户端通过 VPN 隧道为远程专用网络提供单一、可路由的网络。PAT 不适用。因此，Easy VPN 服务器背后的设备可以通过隧道而且只能通过隧道直接访问 Easy VPN Remote 背后的专用网络中的设备，反之亦然。硬件客户端必须启动隧道，但是在建立隧道之后，任一端都可发起数据交换。

示例：

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
```

要禁用 NEM，请输入 **disable** 关键字。要从运行配置中删除 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。

步骤 2 （可选） 使用以下命令配置安全设备身份验证：

[**no**] **secure-unit-authentication** [**enable** | **disable**]

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。启用此功能后，硬件客户端不会使用保存的用户名和密码（如果已配置）。默认情况下会禁用安全设备身份验证。

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

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

示例：

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
```

要禁用安全设备身份验证，请输入 **disable** 关键字。要从运行配置中删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。

步骤 3 （可选） 使用以下命令配置用户身份验证：

[**no**] **user-authentication** [**enable** | **disable**]

启用后，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，以获取通过隧道访问网络的权限。个人用户按照身份验证服务器的配置顺序进行身份验证。默认情况下会禁用用户身份验证。

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

示例：

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
```

要禁用用户身份验证，请输入 **disable** 关键字。要从运行配置中删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。

步骤 4 使用以下命令为通过身份验证的个人用户设置空闲超时：

[**no**] **user-authentication-idle-timeout** *minutes* | **none**]

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。

如果在空闲超时期限内硬件客户端背后的用户没有通信活动，则ASA会终止该客户端的访问。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。

示例：

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 enable
hostname(config-group-policy)#user-authentication-idle-timeout 45
```

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。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 null 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。

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

步骤 5 使用以下命令配置 IP 电话绕行：

ip-phone-bypass enable

通过 IP 电话绕行，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 电话绕行。此选项仅当启用 IUA 时应用。

注释
您还必须在客户端上配置 MAC 地址豁免来豁免这些客户端的身份验证。

要禁用 IP 电话绕行，请输入 **disable** 关键字。要从运行配置中删除 IP 电话绕行属性，请输入此命令的 **no** 形式。此选项允许从其他组策略继承 IP 电话绕行的值。

步骤 6 使用以下命令配置 LEAP 绕行：

leap-bypass enable

LEAP 绕行仅当启用 **user-authentication** 时应用。此命令可以让来自思科无线接入点设备的 LEAP 数据包建立 LEAP 身份验证，然后在每次用户身份验证时再次进行身份验证。默认情况下会禁用 LEAP 绕行。

硬件客户端背后的 LEAP 用户面临着一个循环困境：他们无法协商 LEAP 身份验证，因为他们无法通过隧道将自己的凭证发送到中心站点设备背后的 RADIUS 服务器。而他们无法通过隧道发送凭证的原因是他们尚未在无线网络中进行身份验证。为解决此问题，LEAP 绕行让 LEAP 数据包（并且仅限 LEAP 数据包）穿过隧道，在个人用户进行身份验证之前，向 RADIUS 服务器进行无线连接身份验证。然后，用户继续进行个人用户身份验证。

在以下情况下，LEAP 绕行可以正确运行：

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

示例：

以下示例显示如何为名为 FirstGroup 的组策略设置 LEAP 绕行：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
hostname(config-group-policy)# leap-bypass enable
```

要禁用 LEAP 绕行，请输入 **disable** 关键字。要从运行配置中删除 LEAP 绕行属性，请输入此命令的 **no** 形式。此选项允许从其他组策略继承 LEAP 绕行的值：

为 Secure Client连接配置组策略属性

按照AnyConnect VPN 客户端连接，第 229 页中所述启用 Secure Client连接后，可以启用或要求组策略的 Secure Client 功能。在组策略 webvpn 配置模式下按照以下步骤进行操作：

过程

步骤 1 进入组策略 webvpn 配置模式。例如：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
```

步骤 2 要禁用在终端计算机上永久性安装 Secure Client，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)#
```

默认设置为启用客户端的永久性安装。在 Secure Client 会话结束时，客户端仍安装在终端上。

步骤 3 如要为组策略的 Secure Client SSL 连接上的 HTTP 数据启用压缩，请输入 anyconnect ssl compression 命令。默认情况下，压缩设置为 **none**（禁用）。要启用压缩，请使用 **deflate** 关键字。例如：

```
hostname(config-group-webvpn)# anyconnect compression deflate
hostname(config-group-webvpn)#
```

步骤 4 配置对等体存活检测，第 244 页

步骤 5 可以使用 调整保持消息的频率，以确保经由代理、防火墙或 NAT 设备的 Secure Client 连接保持打开状态，即使设备限制了连接可处于空闲状态的时间也是如此： **anyconnect ssl keepalive command:**

anyconnect ssl keepalive {none | *seconds***}**

调整保持连接还可确保当远程用户未主动运行基于套接字的应用（例如 Microsoft Outlook 或 Microsoft Internet Explorer）时，Secure Client不会断开连接并重新连接。

以下示例配置安全设备以使 Secure Client能够以 300 秒（5 分钟）的频率发送保持连接信息：

```
hostname(config-group-webvpn)# anyconnect ssl keepalive 300
hostname(config-group-webvpn)#
```

步骤 6 如要使 Secure Client能够对 SSL 会话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 Secure Client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），而不指定方法。

以下示例将 Secure Client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 通过客户端绕行协议功能，可以配置 Secure Client 在应该只有 IPv6 流量时如何管理 IPv4 流量，或者在应该只有 IPv4 流量时如何管理 IPv6 流量。

当 Secure Client对 ASA 进行 VPN 连接时，ASA 可以为客户端分配一个 IPv4、IPv6 或 IPv4 和 IPv6 两个地址。如果 ASA 对 Secure Client 连接仅分配一个 IPv4 地址或一个 IPv6 地址，则您可以配置客户端旁路协议以丢弃 ASA 尚未分配 IP 地址的网络流量，或允许该流量绕过 ASA 并从客户端以未加密或“明文形式”发送。

例如，假设 ASA 只将一个 IPv4 地址分配到 Secure Client 连接，且终端为双协议栈。当终端尝试访问 IPv6 地址时，如果禁用客户端旁路协议，则会丢弃 IPv6 流量；但是，如果启用客户端旁路协议，则会从客户端以明文形式发送 IPv6 流量。

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

使用 client-bypass-protocol 命令启用或禁用客户端绕行协议功能。以下是命令语法：

client-bypass-protocol {enable | disable}

以下示例启用客户端绕行协议：

```
hostname(config-group-policy)# client-bypass-protocol enable
hostname(config-group-policy)#
```

以下示例禁用客户端绕行协议：

```
hostname(config-group-policy)# client-bypass-protocol disable
hostname(config-group-policy)#
```

以下示例删除已启用或已禁用的客户端绕行协议设置：

```
hostname(config-group-policy)# no client-bypass-protocol enable
hostname(config-group-policy)#
```

步骤 8 如果已在 ASA 之间配置负载均衡，请指定 ASA 的 FQDN，以解析用于重新建立 VPN 会话的 ASA IP 地址。此设置对于支持不同 IP 协议（例如 IPv4 到 IPv6）的网络之间的客户端漫游非常关键。

在漫游之后，您无法使用 Secure Client 配置文件中的 ASA FQDN 来获取 ASA IP 地址。在负载均衡场景中，地址可能与正确的设备（与之建立隧道的设备）不匹配。

如果未将设备 FQDN 推送到客户端，则客户端将尝试重新连接到隧道以前建立的任意 IP 地址。为了支持不同 IP 协议（从 IPv4 到 IPv6）的网络之间的漫游，Secure Client 必须在漫游之后执行设备 FQDN 的名称解析，以便为重新建立隧道确定使用哪个 ASA 地址。在初始连接中，客户端使用其配置文件中的 ASA FQDN。如果可用，在后续会话重新连接期间，它总是使用由 ASA 推送（并由管理员在组策略中配置）的设备 FQDN。如果未配置 FQDN，则 ASA 从 Device Setup > Device Name/Password and Domain Name 下设置的任意内容派生设备 FQDN（并将其发送到客户端）。

如果 ASA 未推送设备 FQDN，则客户端在不同 IP 协议的网络之间漫游后无法重新建立 VPN 会话。

使用 gateway-fqdn 命令配置 ASA 的 FQDN。以下是命令语法：

gateway-fqdn { **value** *FQDN_Name* | **none**} 或 **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删除 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。如果可用，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)#
```

配置备份服务器属性

如果计划使用备用服务器，请对其进行配置。通过 IPsec 备份服务器，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，ASA 会在建立 IPsec 隧道时将服务器列表推送到客户端。如果不在客户端或主 ASA 上配置备份服务器，则没有备份服务器。

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，它会将备份服务器策略推送到组中的客户端，从而取代客户端上的备份服务器列表（如果已配置）。

注释 如果使用主机名，最好将备用 DNS 和 WINS 服务器置于与主要 DNS 和 WINS 服务器不同的网络。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，并且备用服务器具有不同的 DNS 和 WINS 信息，则客户端在 DHCP 租用到期之前无法更新。此外，如果使用主机名且 DNS 服务器不可用，则可能出现显著延迟。

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}
```

要删除备份服务器，请在指定备份服务器的情况下输入此命令的 **no** 形式。要从运行配置中删除 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 将推送空服务器列表。

keep-client-config 关键字指定 ASA 不将备份服务器信息发送到客户端。客户端使用自己的备用服务器列表（如果已配置）。这是默认值。

*server1 server 2.... server10*参数列表是 VPN 客户端在主 ASA 不可用时要使用的服务器列表，以空格分隔并按优先级排序。此列表以 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 的备用服务器：

```
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 命令全部都有默认值。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 使用经由 UDP 的可扩展身份验证协议 (EAP) (EAPoUDP) 消息传递验证远程主机的安全状态。安全状态验证包括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。

访问控制服务器将安全状态标记（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。典型的安全状态标记为正常、检查、隔离、感染或未知。在安全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。

如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：

过程

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安全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安全状态更改的查询，称为状态查询。输入范围在 30 至 1800 内的秒数。默认设置为 300。

如要指定网络准入控制会话中每次成功的安全状态验证与下一次主机安全状态更改查询之间的间隔，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，请访问要从中继承该值的备用组策略，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的安全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的安全状态验证。安全设备在重新验证期间维护安全状态验证。如果访问控制服务器在安全状态验证或重新验证期间不可用，则默认组策略会生效。输入每次成功的安全状态验证之间的间隔（以秒为单位）。范围为 300 到 86400。默认设置为 36000。

如要指定网络准入控制会话中每次成功的安全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，请访问要从中继承该值的备用组策略，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。如果安全状态验证失败，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** 并且安全状态验证失败，安全设备将应用默认组策略。

如要指定将用作安全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)#
```

如要从默认组策略继承 ACL，请访问要从中继承该 ACL 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 上配置的安全状态验证服务器组的名称。该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，并且不对安全状态验证失败的 NAC 会话应用 ACL。

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 标识为安全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，并且不对安全状态验证失败的 NAC 会话应用 ACL：

```
hostname(config-group-policy)# nac-default-acl none
hostname(config-group-policy)#
```

步骤 4 配置 VPN 的 NAC 豁免。默认情况下，豁免列表为空。过滤器属性的默认值为 **none**。为每个要匹配以豁免远程主机安全状态验证的操作系统（和 ACL）输入一次 **vpn-nac-exempt 命令**。

如要向豁免安全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)#
```

如要禁用继承并指定所有主机都要进行安全状态验证，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)#
```

如要从豁免列表中删除条目，请使用此命令的 **no** 形式并命名要删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)#
```

如要从与此组策略关联的豁免列表中删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 配置中已有的 ACL 的名称。
- disable - 禁用豁免列表中的条目而不将其从列表中删除。
- **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 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主机都要进行安全状态验证。紧接在 **filter** 之后输入时，此关键字表示该条目不指定 ACL。
- **OS** - 豁免操作系统的安全状态验证。
- *os name* - 操作系统名称。仅当名称包含空格时才需要引号（例如“Windows XP”）。

以下示例禁用继承并指定所有主机都要进行安全状态验证：

```
hostname(config-group-policy)# no vpn-nac-exempt none
hostname(config-group-policy)
```

以下示例从豁免列表删除所有条目：

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)
```

步骤 5 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，请访问要从中继承该 NAC 设置的备用组策略，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安全状态验证。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互联网隔离并进行保护。如果组中的远程用户配置了分割隧道，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，从而帮助企业网络抵御通过互联网或用户的本地 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。

在 group-policy 配置模式下使用 **client-firewall** 命令，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（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的任何策略。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“添加或编辑组策略”对话框，可以为 VPN 客户端正在添加或修改的组策略配置防火墙设置。

注释 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 客户端通过定期向防火墙发送“are you there?”消息对其进行监控；如果没有响应，则 VPN 客户端知道防火墙关闭并会终止其与 ASA 的连接）。网络管理员可以在最初配置这些 PC 防火墙，但是如果采用此方法，每个用户就可以自定义自己的配置。

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

配置 Secure Client 防火墙策略

Secure Client 的防火墙规则可以指定 IPv4 和 IPv6 地址。

开始之前

您已创建指定 IPv6 地址的统一访问规则。

过程

步骤 1 进入 webvpn 组策略配置模式。

webvpn

示例：

```
hostname(config)# group-policy ac-client-group attributes
hostname(config-group-policy)# webvpn
```

步骤 2 指定专用或公共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。

anyconnect firewall-rule client-interface {private | public} value *[RuleName]*

```
hostname(config-group-webvpn)# anyconnect firewall-rule client-interface private value
ClientFWRule
```

步骤 3 显示组策略属性以及组策略的 webvpn 策略属性。

show runn group-policy [value]

示例：

```
hostname(config-group-webvpn)# show run group-policy FirstGroup
group-policy FirstGroup internal
group-policy FirstGroup attributes
```

```
webvpn
  anyconnect firewall-rule client-interface private value ClientFWRule
```

步骤 4 从专用网络规则中删除客户端防火墙规则。

no anyconnect firewall-rule client-interface private value [*RuleName*]

示例：

```
hostname(config-group-webvpn)# no anyconnect firewall-rule client-interface private value
hostname(config-group-webvpn)#
```

使用 Zone Labs Integrity 服务器

本节介绍 Zone Labs Integrity 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 服务器的示例程序。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，则不会获准访问受到 Integrity 服务器和 ASA 保护的专用网络。

VPN 客户端软件和 Integrity 客户端软件在远程 PC 上共存。以下步骤汇总了远程 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 用作代理的情况下，Integrity 客户端与 Integrity 服务器建立受限连接。受限连接仅在 Integrity 客户端与 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。

注释 ASA 的当前版本每次只支持一个 Integrity 服务器，即使用户接口支持多达五个 Integrity 服务器的配置也一样。如果活动的 Integrity 服务器发生故障，请在 ASA 上配置另一台 Integrity 服务器，然后重新建立 VPN 客户端会话。

如要配置 Integrity 服务器，请执行以下步骤：

过程

步骤 1 使用 IP 地址 10.0.0.5 配置 Integrity 服务器。

```
zonelabs-Integrity server-address {hostname1 | ip-address1}
```

示例：

```
hostname(config)# zonelabs-Integrity server-address 10.0.0.5
```

步骤 2 指定端口 300（默认端口为 5054）。

```
zonelabs-integrity port port-number
```

示例：

```
hostname(config)# zonelabs-integrity port 300
```

步骤 3 指定用于与 Integrity 服务器进行通信的内部接口。

```
zonelabs-integrity interface interface
```

示例：

```
hostname(config)# zonelabs-integrity interface inside
```

步骤 4 确保 ASA 在声明 Integrity 服务器发生故障并关闭 VPN 客户端连接之前，会等 12 秒待活动或备用 Integrity 服务器响应。

注释
如果 ASA 与 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。

```
zonelabs-integrity fail-timeout timeout
```

示例：

```
hostname(config)# zonelabs-integrity fail-timeout 12
```

步骤 5 配置 ASA，以便在 ASA 与 Zone Labs Integrity 服务器之间的连接失败时关闭与 VPN 客户端的连接。

```
zonelabs-integrity fail-close
```

示例：

```
hostname(config)# zonelabs-integrity fail-close
```

步骤 6 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。

```
zonelabs-integrity fail-open
```

示例：

```
hostname(config)# zonelabs-integrity fail-open
```

步骤 7 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。

```
zonelabs-integrity ssl-certificate-port cert-port-number
```

示例：

```
hostname(config)# zonelabs-integrity ssl-certificate-port 300
```

步骤 8 尽管始终会对服务器 SSL 证书进行身份验证，但是仍会指定对 Integrity 服务器的客户端 SSL 证书进行身份验证。

```
zonelabs-integrity ssl-client-authentication {enable | disable}
```

示例：

```
hostname(config)# zonelabs-integrity ssl-client-authentication enable
```

将防火墙客户端类型设置为 Zone Labs

过程

	命令或操作	目的
步骤 1	如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： 示例： `hostname(config)# client-firewall req zonelabs-integrity`	**client-firewall {opt | req} zonelabs-integrity**

下一步做什么

有关详细信息，请参阅配置 VPN 客户端防火墙策略，第 162 页。当防火墙类型为 **zonelabs-integrity** 时，不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，请参阅配置 VPN 客户端防火墙策略，第 162 页。

- 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
```

注释 当防火墙类型为 **zonelabs-integrity** 时，请不要包含参数。Zone Labs Integrity 服务器会确定策略。

```
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 *8: 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。将询问：“Are You There?” 如果没有响应，ASA将拆解隧道。

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	说明防火墙。
networkice-blackice	指定 Network ICE Black ICE 防火墙类型。
none	表示无客户端防火墙策略。使用空值设置防火墙策略，从而禁止使用防火墙策略。防止从默认或指定的组策略继承防火墙策略。
opt	表示可选的防火墙类型。
product-id	标识防火墙产品。
req	表示必需的防火墙类型。
sygate-personal	指定 Sygate Personal 防火墙类型。
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 服务器防火墙类型。
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

在 group-policy 配置模式下使用 **client-access-rule** 命令通过 ASA 配置可通过 IPsec 连接的远程访问客户端类型和版本的限制规则。根据以下准则来制定规则：

- 如果不定义任何规则，ASA 将允许所有连接类型。

- 如果一个客户端与所有规则均不匹配，ASA 将拒绝此连接。如果定义拒绝规则，则还必须定义至少一个允许规则；否则，ASA 将拒绝所有连接。
- 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.*** 会创建一条优先级为 3 的客户端访问规则，拒绝所有运行版本 3.x 软件的客户端类型。
- 您可以为每个组策略最多构建 25 个规则。
- 对整组规则的限制为 255 个字符。
- 对于不发送客户端类型和/或版本的客户端可以输入 n/a。

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
```

要删除所有规则，请输入不带参数的 **no client-access-rule command**。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，无访问规则。当没有客户端访问规则时，用户将继承默认组策略中的任何规则。

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]
```

下表说明了这些命令中的关键字和参数的含义。

表 *9: client-access rule* 命令关键字和参数

参数	说明
deny	拒绝特定类型和/或版本设备的连接。
none	允许无客户端访问规则。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，与客户端类型和/或版本匹配的具有最小整数的规则是应用的规则。如果一个较低优先级的规则与之冲突，ASA 会忽略它。

参数	说明
type *type*	通过任意形式的字符串标识设备类型。字符串必须与其在 **show vpn-sessiondb remote** 显示中的外观完全匹配，但可以输入 * 字符作为通配符。
version version	通过任意形式的字符串标识设备版本，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，但可以输入 * 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 的思科 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.*
```

注释 “类型”字段是允许任意值的任意形式字符串，但是该值必须与客户端在连接时发送到ASA的固定值匹配。

配置用户属性

本节介绍用户属性及其配置方式。

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，可以指定一个组策略为所有用户授予办公时间的访问权限，但授予特定用户 24 小时访问权限。

查看用户名配置

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#
```

这将显示所有用户（如果提供了用户名，则为特定用户）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 testuse
username testuser password 12RsxXQnphyr/I9Z encrypted privilege 15
```

配置个人用户属性

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包含使用 **username** 命令输入的用户。**login** 命令使用此数据库进行身份验证。要将用户添加到 ASA 数据库，请在全局配置模式下输入 **username** 命令。要删除用户，请使用此命令（带有要删除的用户名）的 **no** 版本。要删除所有用户名，请使用 **clear configure username** 命令而不附加用户名。

设置用户密码和权限级别

输入 **username** 命令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。如果确实指定了密码，则可以指定是否以加密形式存储该密码。

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]
```

下表说明了此命令中使用的关键字和变量的含义。

username 命令关键字和变量

关键字/变量	含义
encrypted	表示密码已加密。
name	提供用户的名称。
nopassword	表示此用户无需密码。
password password	表示此用户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，越低的数字使用命令和管理 ASA 的能力越小。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。这些属性可为任意顺序。要删除任何属性/值对，请输入此命令的 **no** 形式。

输入带有 **attributes** 关键字的 **username** 命令进入 username 模式：

```
hostname(config)# username name attributes
hostname(config-username)#
```

提示符会更改以表示进入新模式。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

可以让用户从组策略继承尚未在用户名级别配置的属性值。要指定此用户从中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)#
```

配置访问时长

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长：

要从运行配置中删除属性，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。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 到 2147483647。默认值为 3 个同时登录。要从运行配置中删除属性，请输入此命令的 **no** 形式。输入 0 则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
```

注释 尽管同时登录数的上限非常大，但允许多个用户同时登录可能会降低安全性并影响性能。

以下示例显示如何为名为 anyuser 的用户设置最大同时登录数 4：

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-simultaneous-logins 4
hostname(config-username)#
```

配置空闲超时

过程

步骤 1 （可选） 要配置 VPN 空闲超时期限，请在 group-policy 配置模式或 username 配置模式下使用 **vpn-idle-timeout** *minutes* 命令。

如果在此期间连接上没有通信活动，则 ASA 将终止此连接。最小值为 1 分钟，最大值为 35791394 分钟，默认值为 30 分钟。

以下示例展示如何将名为 FirstGroup 的组策略的 VPN 空闲超时设置为 15 分钟：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

其他 [**no**] **vpn-idle-timeout** {*minutes* | **none**} 命令的其他操作：

- 输入 **vpn-idle-timeout none** 以禁用 VPN 空闲超时并防止继承超时值。

  ```
  hostname(config)# group-policy FirstGroup attributes
  hostname(config-group-policy)# vpn-idle-timeout none
  hostname(config-group-policy)#
  ```

  这将致使 Secure Client（SSL 和 IPsec/IKEv2）和无客户端 VPN 使用全局 webvpn **default-idle-timeout** *seconds* 值。在 webvpn-config 模式下输入此命令，例如：`hostnamee(config-webvpn)# default-idle-timeout 300`。默认值为 1800 秒（30 分钟），范围为 60 至 86400 秒。

  对于所有 webvon 连接，仅当系统在组策略/用户名属性中设置 **vpn-idle-timeout none** 时，才会实施 **default-idle-timeout** 值。对于所有 Secure Client 连接，ASA 需要一个非零的空闲超时值。

对于站点间（IKEv1、IKEv2）和 IKEv1 远程访问 VPN，我们建议禁用超时并允许无限制的空闲期。

- 要禁用此组策略或用户策略的空闲超时，请输入 **no vpn-idle-timeout**。系统将继承该值。
- 如果未设置 **vpn-idle-timeout**，那么系统无论如何都会继承该值，默认值为 30 分钟。

注释
vpn-idle-timeout 只能控制父会话的最长时间。子会话 (SSL/DTLS) 会因硬编码的 5 分钟 TCP 非活动超时或未能通过 3 次对等体存活检测 (DPD) 检查而提前终止。有关详细信息，请参阅 配置对等体存活检测中的说明。有关 DPD、保持连接和超时属性的更多详细信息，请参阅 AnyConnect 常见问题解答 - 隧道、DPD 和非活动计时器 (AnyConnect FAQ - Tunnels, DPDs, and Inactivity Timer)。

步骤 2 （可选） 使用 **vpn-idle-timeout alert-interval** {*minutes*} 命令，可以选择性地配置向用户显示空闲超时警报消息的时间。

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。默认警报间隔为一分钟。

以下示例显示如何为名为 anyuser 的用户设置 3 分钟的 VPN 空闲超时警报间隔：

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout alert-interval 3
hostname(config-username)#
```

其他 [**no**] **vpn-idle-timeout alert-interval** {*minutes* | **none**} 命令的其他操作：

- **none** 参数表示用户将不会收到警报。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout none
hostname(config-username)#
```

- 要删除此组或用户策略的警报间隔，请输入 **no vpn-idle-timeout alert-interval**。系统将继承该值。
- 如果未设置此参数，则默认警报间隔为一分钟。

配置最长连接时间

过程

步骤 1 （可选） 在 group-policy 配置模式或 username 配置模式下使用 **vpn-session-timeout** {*minutes* 命令配置 VPN 连接的最长时间。

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 将终止连接。

以下示例显示如何将名为 FirstGroup 的组策略的 VPN 会话超时设置为 180 分钟：

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
```

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

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
hostname(config-username)#
```

其他 [**no**] **vpn-session-timeout** {*minutes* | **none**} 命令的其他操作：

- 要从此策略中删除属性并允许继承，请输入此命令的 **no vpn-session-timeout** 形式。
- 要允许无限超时期，并因此防止继承超时值，请输入 **vpn-session-timeout none**。

步骤 2 使用 **vpn-session-timeout alert-interval** {*minutes* | } 命令，配置向用户显示会话超时警报消息的时间。

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。以下示例显示如何指定用户在其 VPN 会话断开连接之前 20 分钟收到通知。可以指定的范围为 1 至 30 分钟。

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

其他 [**no**] **vpn-session-timeout alert-interval** {*minutes* | **none**} 命令的其他操作：

- 使用该命令的 no 形式表示将从默认组策略继承 VPN 会话超时 alert-interval 属性：

  ```
  hostname(config-webvpn)# no vpn-session-timeout alert-interval
  ```

- **vpn-session-timeout alert-interval none** 表示用户将不会收到警报。

应用 ACL 过滤器

指定要用作 VPN 连接过滤器的以前配置的用户特定 ACL 名称。要禁止使用 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。要删除 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。请注意，VPN 过滤器仅适用于初始连接。它不适用于因应用检查操作而打开的辅助连接，例如 SIP 媒体连接。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)#
```

注释 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。要删除 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。要删除子网掩码，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。要删除 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。此地址表示前缀值为 2001:0000:0000:0000，接口 ID 为 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。要从运行配置中删除属性，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。创建管理身份验证、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。至少必须配置一个隧道模式供用户通过 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原本已有的指定连接配置文件进行访问。组锁定通过检查在VPN客户端中配置的组与用户分配的连接配置文件是否相同来限制用户。如果不一样，ASA 会阻止用户进行连接。如果不配置组锁定，则 ASA 在不考虑分配的组的情况下对用户进行身份验证。

要从运行配置中删除 **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。要禁用密码存储，请输入带有 **disable** 关键字的 **password-storage**

命令。要从运行配置中删除 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)
```

此命令与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无关。

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)
```

配置和调整 VPN 过滤器 ACL 的最佳实践

本节介绍在不中断流量的情况下更新现有 VPN 过滤器 ACL 时应遵循的最佳实践。

更新现有 VPN 过滤器 ACL

当要更新在 ASA 设备上应用的 vpn-filter ACL 时，请执行以下步骤：

1. 在系统上创建新的 vpn-filter ACL（示例：*new_acl.txt*）。
2. 从设备下载当前的 vpn-filter ACL（示例：*old_acl.txt*）。
3. 为 ACL 创建修改说明：

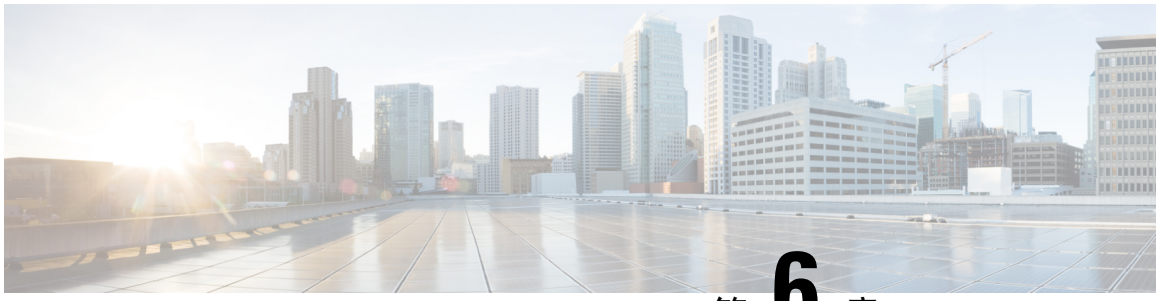
```
* Add update in-progress to ACL remark
echo ?access-list <name> line 1 ACL update in-progress? > push.txt
* Delete old rules
sed ?s/^/no /g? old.acl >> push.txt
 * Add new rules
cat new.acl >> push.txt
 * Remove update in-progress to ACL remark
echo ?no access-list <name> ACL update in-progress? >> push.txt
```

4. 将 push.txt 上传到设备。

使用新的 VPN 过滤器 ACL 替换现有的 VPN 过滤器 ACL

按照以下步骤替换 ASA 设备上应用的 vpn-filter ACL：

1. 每次要替换现有 vpn-filter ACL 时都会创建一个新的 vpn-filter ACL。
2. 使用 vpn-filter ACL 来更新组策略。
3. 删除设备上应用的旧 vpn-filter ACL。



第 6 章

VPN 的 IP 地址

配置 IP 地址分配策略

ASA 可使用以下一种或多种方法将 IP 地址分配给远程访问客户端。如已配置多种地址分配方法，则 ASA 将搜索每一个选项，直到找到一个 IP 地址为止。默认情况下，所有方法均已启用。

- aaa 从外部身份验证、授权和记账服务器逐个用户检索 IP 地址。如果使用已配置 IP 地址的身份验证服务器，建议使用此方法。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分配地址池以进行配置的最简单方法。如果选择 local，还必须使用 **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。
  - 允许释放 IP 地址一段时间之后对其重新使用 - 在 IP 地址返回到地址池之后，延迟一段时间方可重新使用。增加延迟有助于防止防火墙在快速重新分配 IP 地址时遇到的问题。默认情况下 ASA 不会强制执行延迟。此配置元素适用于 IPv4 分配策略。

使用以下方法之一指定将 IP 地址分配给远程访问客户端的方法。

配置 IPv4 地址分配

过程

启用要供 ASA 在将 IPv4 地址分配给 VPN 连接时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，这些方法均已启用。

vpn-addr-assign {**aaa** | **dhcp** | **local** [**reuse-delay** *minutes*]}

示例：

例如，您可以将 IP 地址释放之后重新开始使用的时间配置为 0 至 480 分钟。

```
hostname(config)#vpn-addr-assign aaa
hostname(config)#vpn-addr-assign local reuse-delay 180
```

以下示例使用此命令的 no 形式禁用地址分配方法。

```
hostname(config)# no vpn-addr-assign dhcp
```

配置 IPv6 地址分配

过程

启用要供 ASA 在将 IPv6 地址分配给 VPN 连接时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。

ipv6-vpn-addr-assign {**aaa** | local}

示例：

```
hostname(config)# ipv6-vpn-addr-assign aaa
```

以下示例使用此命令的 no 形式禁用地址分配方法。

```
hostname(config)# no ipv6-vpn-addr-assign local
```

查看地址分配方法

过程

使用以下方法之一查看在 ASA 上配置的地址分配方法：

- 查看 IPv4 地址分配

  显示已配置的地址分配方法。已配置的地址分配方法可能为 aaa、dhcp 或 local。

  ```
  show running-config all vpn-addr-assign
  vpn-addr-assign aaa
  vpn-addr-assign dhcp
  vpn-addr-assign local
  ```

- 查看 IPv6 地址分配

显示已配置的地址分配方法。已配置的地址分配方法可能为 aaa 或 local。

```
show running-config all ipv6-vpn-addr-assign
ipv6-vpn-addr-assign aaa
ipv6-vpn-addr-assign local reuse-delay 0
```

配置本地 IP 地址池

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。如要删除地址池，请输入此命令的 **no** 形式。

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。如要删除地址池，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。地址池的指定顺序非常重要。如果为连接配置文件或组策略配置了多个地址池，则 ASA 将按您向 ASA 添加地址池的顺序使用地址池。

如果从非本地子网分配地址，我们建议添加位于子网边界的地址池，从而可更轻松地添加这些网络的路由。

注释 在修改活动隧道组中当前正在使用的现有地址池（即，向最终用户开放连接）时，您必须在更改窗口中执行更改，并确保满足以下条件：

- 连接的用户已注销。
- 地址池将从隧道组中删除，并根据需要进行修改。
- 然后，修改后的地址池将被重新添加到隧道组下。

如果不以这种方式修改地址池，则可能会导致 ASA 的行为不一致。

配置本地 IPv4 地址池

注释 如果要在 CLI 上修改活动隧道组中当前正在使用的现有地址池（即向最终用户开放连接），则建议在更改窗口中执行此更改。应注销连接的用户，从隧道组中删除地址池，根据需要进行修改，然后重新添加到隧道组下。如果不以这种方式完成，则可能会导致 ASA 的行为不一致。

过程

步骤 1 将 IP 地址池配置为地址分配方法。输入参数为 **local** 的 **vpn-addr-assign** 命令。

示例：

```
hostname(config)# vpn-addr-assign local
```

步骤 2 配置地址池。此命令为地址池命名，并指定 IPv4 地址范围和子网掩码。

ip local pool*poolname first_address-last_address***mask***mask*

示例：

此示例配置名为 *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。

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

此示例删除名为 **firstpool** 的 IP 地址池。

```
hostname(config)# no ip local pool firstpool
```

配置本地 IPv6 地址池

过程

步骤 1 将 IP 地址池配置为地址分配方法，输入参数为 **local** 的 ipv6-**vpn-addr-assign** 命令。

示例：

```
hostname(config)# ipv6-vpn-addr-assign local
```

步骤 2 配置地址池。此命令为地址池命名，并确定起始 IPv6 地址、前缀长度（位数）和要在相应地址范围中使用的地址数量。

ipv6 local pool *pool_name starting_address prefix_length number_of_addresses*

示例：

此示例配置名为 *ipv6pool* 的 IP 地址池。起始地址为 2001:DB8::1，前缀长度为 32 位，要在地址池中使用的地址数量为 100。

```
hostname(config)# ipv6 local pool ipv6pool 2001:DB8::1/32 100
```

此示例删除名为 *ipv6pool* 的 IP 地址池。

```
hostname(config)# no ipv6 local pool ipv6pool
```

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。

以下示例说明如何为名为 firstgroup 的隧道组定义名为 RAD2 的 AAA 服务器组。此过程还包括一个必须执行的步骤，在该步骤中，您可能已经为隧道组命名并定义隧道组类型。该步骤在以下示例中显示为一则提醒，提示您只有先设置这些值，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)# authentication-server-group RAD2
```

如要配置用于 IP 寻址的 AAA，请执行以下步骤：

过程

步骤 1 如要将 AAA 配置为地址分配方法，请输入参数为 **aaa** 的 **vpn-addr-assign** 命令：

```
hostname(config)# vpn-addr-assign aaa
hostname(config)#
```

步骤 2 如要建立用作远程访问的名为 firstgroup 的隧道组或 LAN 间隧道组，请输入关键字为 **type** 的 **tunnel-group** 命令。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 **tunnel-group** 命令。

```
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 **authentication-server-group** 命令。

```
hostname(config-general)# authentication-server-group RAD2
hostname(config-general)#
```

下一步做什么

此命令包含的参数比此示例中的参数要多。有关详情，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关联的组策略中定义 DHCP 网络范围。

以下示例为名为 **firstgroup** 的连接配置文件定义为 172.33.44.19 的 DHCP 服务器。该示例还为名为 **remotegroup** 的组策略将 DHCP 网络范围定义为 10.100.10.1。（名为 remotegroup 的组策略与名为 firstgroup 的连接配置文件关联）。如未定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将检查各个池，直到发现未分配的地址为止。

开始之前

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

过程

步骤 1 将 IP 地址池配置为地址分配方法。

vpn-addr-assign dhcp

步骤 2 建立名为 **firstgroup** 的连接配置文件作为远程访问连接配置文件。

tunnel-group firstgroup type remote-access

步骤 3 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。

tunnel-group firstgroup general-attributes

步骤 4 按 IPv4 地址定义 DHCP 服务器，然后退出隧道组配置模式。

dhcp-server *IPv4_address_of_DHCP_server*

不能用 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 dhcp-server 命令。您可通过此命令将 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。

示例：

以下示例配置 IP 地址为 172.33.44.19 的 DHCP 服务器。然后，退出隧道组配置模式。

```
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)#
```

步骤 5 如果该组尚不存在，请创建一个名为 **remotegroup** 的内部组策略。

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

步骤 6 （可选。）进入 group-policy attributes 配置模式并定义 DHCP 网络范围。

dhcp-network-scope *ip_address*

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

如未定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将检查各个池，直到发现未分配的地址为止。

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

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

示例：

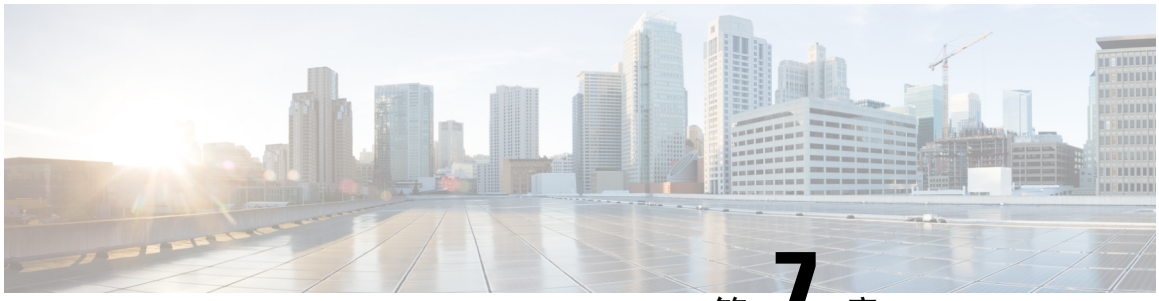
以下是进入 remotegroup 的属性配置模式，并将 DHCP 范围设置为 10.100.10.1 的示例。

```
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```

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 10.100.10.1
```



第 7 章

远程访问 IPsec VPN

远程访问 IPsec VPN 概述

远程访问 VPN 使用户可以通过安全的 TCP/IP 网络连接与中心站点相连接。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，分别称为阶段 1 和阶段 2。

阶段 1 创建第一条隧道，用于保护随后的 ISAKMP 协商消息。阶段 2 创建的隧道用于保护通过安全连接传输的数据。

如要设置 ISAKMP 协商条款，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。
- 散列消息身份验证代码 (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未发生修改。
- 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。在与 ISAKMP 进行 IPsec 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。

转换集保护关联的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多 11 个转换集。有关更多概述信息（包括有效的加密方法和身份验证方法的列表），请参阅本指南创建 IKEv1 转换集或 IKEv2 提议，第 192 页。

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 Secure Client分配 IPv4 地址和/或 IPv6 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。在上述两种场景中，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，仍会进行连接。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。

关于 Mobike 和远程访问 VPN

移动 IKEv2 (mobike) 将扩展 ASA RA VPN 以支持移动设备漫游。此支持意味着移动设备 IKE/IPSEC 安全关联 (SA) 的终端 IP 地址在该设备从其当前连接点移至其他连接点时可以更新而不是直接删除。

默认情况下，Mobike 可在 ASA 版本 9.8(1) 以及更高版本中使用，这意味着 Mobike“始终可用”。只有当客户端提议且 ASA 接受 Mobike 时，才可针对每个 SA 启用 Mobike。此协商作为 IKE_AUTH 交换的一部分予以执行。

在系统启用 mobike 支持的情况下建立 SA 后，客户端可以随时更改其地址，并使用 INFORMATIONAL 交换通知 ASA， 以 UPDATE_SA_ADDRESS 负载指示新地址。ASA 将处理此消息，然后使用新的客户端 IP 地址更新 SA。

注释 您可以使用 `show crypto ikev2 sa detail` 命令确定是否针对当前所有 SA 启用了 mobike。

当前 Mobike 实施在以下方面提供支持：

- 仅限 IPv4 地址
- NAT 映射更改
- 路径连接和故障检测，通过可选的返回路由能力检查来执行
- 主用/备用故障转移
- VPN 负载均衡

如果返回路由能力检查 (RRC) 功能已启用，则系统会在更新 SA 之前，向移动客户端发送 RRC 消息确认新的 IP 地址。

Cisco Secure 客户端的 AnyConnect VPN 模块的许可要求

注释 此功能不适用于无负载加密型号。

如果要从 Cisco Secure Firewall ASA 前端部署 Cisco Secure 客户端（包括 AnyConnect）并使用 VPN 和 Cisco Secure Firewall Posture 或 HostScan 模块，则需要 Advantage 或 Premier 许可证。提供试用许可证。请参阅《Cisco Secure 客户端订购指南》。有关每个型号的最大值，请参阅思科 ASA 系列功能许可证。

远程访问 IPsec VPN 的限制

- 防火墙模式准则 - 仅在路由防火墙模式中受支持。不支持透明模式。
- 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。不支持主用/主用故障转移配置。
- 在 HA 同步期间，配置更改会被阻止。如果用户在此期间尝试登录，防火墙中的 DACL 规则安装可能会失败。完成 HA 同步后，用户即可成功登录。
- 如果第三方客户端发送空用户代理，ASA 不接受远程访问 VPN 会话。
- 对解析到多个频繁变化的 IP 地址的域使用完全限定域名 (FQDN) 访问控制列表 (ACL)，会影响远程访问 VPN 环境中 DHCP 地址的解析。如果配置了外部 DHCP 服务器并启用了网络地址转换 (NAT) 事务提交，则可能会出现此问题。
- 使用高级终端评估进行终端安全评估可能会生成 SSL 连接系统日志消息，并且 不会与 VPN 登录或注销事件相关联。
- 由于 ASA 不会终止任何 EAP 方法，因此无法进行本地身份验证。

  ASA 仅支持 EAP 作为传递，并要求对 VPN 客户端进行证书身份验证以进行客户端的 EAP 身份验证。将 EAP 配置为远程身份验证方法时，请确保为 VPN 客户端配置证书身份验证。即使同时配置了 EAP、PSK 或证书等多个远程身份验证方法，也会显示错误。

配置远程访问 IPsec VPN

本章介绍如何配置远程访问 VPN。

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，请在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。

过程

步骤 1 从全局配置模式进入接口配置模式：

interface {*interface*}

示例：

```
hostname(config)# interface ethernet0
hostname(config-if)#
```

步骤 2 设置接口的 IP 地址和子网掩码：

ip address *ip_address* [*mask*] [*standby ip_address*]

示例：

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
```

步骤 3 为接口指定名称（最多包含 48 个字符）。设置此名称后，不能对其进行更改。

nameif *name*

示例：

```
hostname(config-if)# nameif outside
hostname(config-if)#
```

步骤 4 启用接口。默认情况下，接口处于禁用状态。

示例：

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

在外部接口上配置 ISAKMP 策略和启用 ISAKMP

过程

步骤 1 指定要在 IKEv1 协商过程中使用的身份验证方法和一组参数。

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。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。

在后续步骤中，我们将优先级设置为 1。

步骤 2 指定要在 IKE 策略中使用的加密方法：

crypto ikev1 policy *priority* **encryption** {**aes-192** | **aes-256** | | }

示例：

步骤 3 为 IKE 策略指定散列算法（又称为 HMAC 变体）：

crypto ikev1 policy *priority* **hash** { | **sha**}

示例：

```
hostname(config)# crypto ikev1 policy 1 hash sha
hostname(config)#
```

步骤 4 为 IKE 策略指定 Diffie-Hellman 群 - 支持 IPsec 客户端与 ASA 建立共享密钥的加密协议：

crypto ikev1 policy *priority* **group** {**14** | | | **19** | **20** | 21}

示例：

```
hostname(config)#crypto ikev1 policy 1 group 14
hostname(config)#
```

步骤 5 指定加密密钥生命周期 - 每个安全关联在到期之前应存在的时长，以秒为单位：

crypto ikev1 policy *priority* **lifetime** {*seconds*}

有限生命周期为 120 到 2147483647 秒。要设置无限生命周期，请使用 0 秒。

示例：

```
hostname(config)# crypto ikev1 policy 1 lifetime 43200
hostname(config)#
```

步骤 6 在名为 outside 的接口上启用 ISAKMP：

crypto ikev1 enable *interface-name*

示例：

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

步骤 7 保存对配置的更改：

write memory

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。

过程

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。

ip local pool *poolname first-address—last-address* [**mask** *mask*]

地址掩码是可选的。但是，如果将 IP 地址分配给属于非标准网络的 VPN 客户端，则必须提供掩码值；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例子是本地 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 10 网络中的不同子网时，可能会导致路由问题。

示例：

```
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)#
```

添加用户

过程

为用户创建用户、密码和权限级别：

username *name* {**nopassword** | **password** *password* [**mschap** | **encrypted** | **nt-encrypted**]} [**privilege** *priv_level*]

示例：

```
Hostname(config)# username testuser password 12345678
```

创建 IKEv1 转换集或 IKEv2 提议

本节介绍如何配置转换集(IKEv1) 或提议 (IKEv2)（由加密方法和身份验证方法组成）。

以下步骤显示如何创建 IKEv1 和 IKEv2 提议。

过程

步骤 1 配置 IKEv1 转换集，用于指定为确保数据完整性而要使用的 IPsec IKEv1 加密和散列算法。

crypto ipsec ikev1 transform-set *transform-set-name encryption-method* [*authentication*]

对 encryption 使用以下其中一个值：

- 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-null 不使用加密。

对 authentication 使用以下其中一个值：

- esp-md5-hmac 使用 MD5/HMAC-128 作为散列算法。
- esp-sha-hmac 使用 SHA/HMAC-160 作为散列算法。
- esp-none 不使用 HMAC 身份验证。

示例：

要使用 AES 配置 IKEv1 转换集：

```
hostname(config)# crypto ipsec transform set FirstSet esp-aes esp-sha-hmac
```

步骤 2 配置 IKEv2 提议集，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（目前唯一支持的 IPsec 协议）。

crypto ipsec ikev2 ipsec-proposal *proposal_name*

protocol {**esp**} {**encryption** { | | **aes** | **aes-192** | **aes-256** | } | **integrity** { | **sha-1**}

对 encryption 使用以下其中一个值：

- aes - 对 ESP 结合使用 AES（默认）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。

对 integrity 使用以下其中一个值：

- sha-1 （默认）为 ESP 完整性保护指定美国联邦信息处理标准 (FIPS) 中定义的安全散列算法 (SHA) SHA-1。

如要配置 IKEv2 提议，请使用以下命令：

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

hostname(config-ipsec-proposal)# protocol esp encryption aes intergrity sha-1
```

定义隧道组

隧道组是一组隧道连接策略。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间隧道组。可以更改这些组，但不能将其删除。如果在隧道协商过程中没有标识特定隧道组，ASA 将会使用这两个隧道组来配置远程访问隧道组和 LAN 间隧道组的默认隧道参数。

过程

步骤 1 创建 IPsec 远程访问隧道组（又称为连接配置文件）：

tunnel-group *name* **type** *type*

示例：

```
hostname(config)# tunnel-group testgroup type ipsec-ra
hostname(config)#
```

步骤 2 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）：

tunnel-group *name* **general-attributes**

示例：

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

步骤 3 指定要用于隧道组的地址池：

address-pool [*(interface name)*] *address_pool1* [*...address_pool6*]

示例：

```
hostname(config-general)# address-pool testpool
```

步骤 4 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）：

tunnel-group *name* **ipsec-attributes**

示例：

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

步骤 5 （可选） 配置预共享密钥（仅适用于 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，表明其无法对对等体进行身份验证。

ikev1 pre-shared-key *key*

示例：

```
hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfx
```

创建动态加密映射

动态加密映射定义的策略模板并未配置所有参数。这样，ASA 就可以接受来自 IP 地址未知的对等体（例如远程访问客户端）的连接。

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，让 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。

过程

步骤 1 创建动态加密映射并为其指定 IKEv1 转换集或 IKEv2 提议：

- 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*

- 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 ikev1 transform-set FirstSet
hostname(config)#

hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal secure_proposal
hostname(config)#
```

步骤 2 （可选）根据此加密映射条目为任何连接启用反向路由注入：

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)#
```

创建加密映射条目以使用动态加密映射

创建加密映射条目，确保 ASA 能够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，序号是 1，动态加密映射的名称是 dyn1（是在创建动态加密映射主体中创建的）。

过程

步骤 1 创建使用动态加密映射的加密映射条目：

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

示例：

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
```

步骤 2 将加密映射应用于外部接口：

crypto map *map-name* **interface** *interface-name*

示例：

```
hostname(config)# crypto map mymap interface outside
```

步骤 3 保存对配置的更改：

write memory

在多情景模式下配置 IPSec IKEv2 远程访问 VPN

有关远程访问 IPsec VPN 配置的详细信息，请参阅以下各节：

- 配置接口，第 189 页
- 配置地址池，第 191 页
- 添加用户，第 192 页
- 创建 IKEv1 转换集或 IKEv2 提议，第 192 页
- 定义隧道组，第 193 页
- 创建动态加密映射，第 195 页
- 创建加密映射条目以使用动态加密映射，第 195 页

使用后量子预共享密钥进行 VPN 身份验证

您可以使用新密钥（后量子预共享密钥(PPK)）和预共享密钥(PSK)配置IKEv2，以确保安全客户端和ASA之间的IPsec通信免受量子计算机攻击。您必须在客户端和ASA上配置匹配的PPK和PSK，以实现安全的IPsec连接。安全客户端和ASA使用PPK和PSK获取网络流量的加密和解密密钥。

PPK以二进制格式加密生成。对于ASA和安全客户端配置，必须将二进制PPK转换为256位64个字符的十六进制字符串。

使用后量子预共享密钥进行 VPN 身份验证的前提条件

- 许可证：ASA必须拥有强加密许可证。
- 支持的版本

- ASA 9.18.1 及更高版本。
- 安全客户端 5.1.8 及更高版本。

- 在 ASA 上配置远程访问 IPsec/IKEv2 VPN 连接的所有其他参数，如地址池、IKEv2 提议和加密映射。
- 生成二进制 PPK。
- 将二进制 PPK 转换为 256 位 64 个字符的十六进制字符串。
- 在客户端计算机的 Windows 凭证管理器 (WCM) 中为安全客户端配置 PPK 和两个 PSK。请参阅在 Windows 凭证管理器上配置后量子预共享密钥和预共享密钥，第 198 页。
- 在安全客户端的 VPN 配置文件中配置 PPK 属性。请参阅使用后量子预共享密钥属性为安全客户端配置 VPN 配置文件，第 199 页。
- 确保 ASA 和安全客户端上的 PPK 和 PPK ID 值相同。

在 VPN 身份验证中使用后量子预共享密钥的准则和限制

准则

- 管理员必须确保 PPK 和 PSK 的生成、质量以及向每个客户端设备的分发。

限制

- 仅支持带有 PSK 和 PPK 的 IKEv2。
- 安全客户端仅支持 Windows。
- 客户端只能在 WCM 中为一个 ASA 存储凭证。

使用后量子预共享密钥进行 VPN 验证的工作流程

表 *10:* 使用后量子预共享密钥进行 *VPN* 验证的工作流程

步骤	操作	更多信息
1	生成二进制 PPK 并将其转换为 256 位 64 个字符的十六进制字符串。	-
2	在 Windows 凭证管理器 (WCM) 中配置 PPK 和 PSK。	在 Windows 凭证管理器上配置后量子预共享密钥和预共享密钥，第 198 页

步骤	操作	更多信息
3	使用 PPK 参数配置安全客户端 VPN 配置文件。	使用后量子预共享密钥属性为安全客户端配置 VPN 配置文件，第 199 页
4	配置 ASA 隧道组。	使用后量子预共享密钥在 ASA 上配置 VPN 身份验证，第 199 页
5	用户登录安全客户端以连接 ASA。	-
6	安全客户端使用 VPN 配置文件中的 PPK_ID 从 WCM 获取 PPK 和两个 PSK。	-
7	安全客户端使用 ASA 隧道组参数验证 WCM 中的 PPK 和 PSK 参数。	-
8	如果安全客户端和 ASA 的 PPK 和 PSK 匹配，则安全客户端会与 ASA 建立 VPN 连接。 如果 PPK 和 PSK 不匹配，则与 ASA 的 VPN 连接会失败。	-

在 Windows 凭证管理器上配置后量子预共享密钥和预共享密钥

您必须为 PPK、本地 PSK 和远程 PSK 配置单独的凭证条目。

开始之前

确保您查看 使用后量子预共享密钥进行 VPN 身份验证的前提条件，第 196 页 和 在 VPN 身份验证中使用后量子预共享密钥的准则和限制，第 197 页。

过程

步骤 1 在 Windows 客户端设备中，依次选择**控制面板 (Control Panel)** > **用户账户 (User Accounts)** > **凭证管理器 (Credential Manager)**。

步骤 2 点击 **Windows 凭证 (Windows Credentials)** 选项卡。

步骤 3 点击**添加通用凭证 (Add a Generic Credential)**。

步骤 4 在 **Internet 或网络地址 (Internet or network address)** 字段中，指定以下值之一：

- 对于 PPK，请将值指定为 **AC/PPK/**<HostAddress：后量子预共享密钥。它在 WCM 中存储为 64 个十六进制字符，客户端将其转换为二进制，然后在 IKEv2 的加密和解密密钥派生中包含该密钥。
- 对于本地 PSK，请将值指定为 **AC/PSK_Local/<HostAddress以表示**客户端的 PSK 配置。

- 对于远程 PSK，请将值指定为 **AC/PSK_Remote/<HostAddress**，以表示 ASA 的 PSK 配置。

步骤 5 在**用户名 (User name)** 字段中，请将值指定为**不适用**，因为安全客户端不使用该值。

步骤 6 在**密码 (Password)** 字段中，指定以下值之一：

- 对于 PPK，请指定 256 位 64 个字符的十六进制字符串。
- 对于本地和远程 PSK，请指定一个字符串来指定隧道组别名。

步骤 7 点击**确定 (OK)**。

安全客户端使用 VPN 配置文件中的 PPK_ID 从 WCM 获取 PPK 和两个 PSK。安全客户端使用上述 PPK 和 PSK 值，将 PPK 转换为二进制，将 PPK 和 PSK 值与 ASA 配置相匹配，并执行 VPN 身份验证。建立 VPN 连接不需要其他输入，因为这三个密钥就是身份验证凭证。

使用后量子预共享密钥属性为安全客户端配置 VPN 配置文件

VPN 配置文件中的 **HostEntry** 参数具有以下新字段，用于配置安全客户端的 PPK 参数：

- **IKEIdentity** - 指定用于标识对等体 ASA 的字符串。此字符串必须与 ASA 中的隧道组名称匹配。
- **PPK_ID** - 指定用于标识 PPK 的唯一字符串。该值必须与 ASA 中的 PPK ID 一致。
- **PPK_mandatory** - 如果 PPK 对于 VPN 连接为强制，则将值指定为 true。如果不配置该值，则 PPK 配置将是可选的。

示例

以下给出了 VPN 配置文件中的 HostEntry 的示例：

```
<HostEntry>
<HostName> ASAv_PPK</HostName>
<HostAddress>192.168.1.2</HostAddress>
<UserGroup>IPSec_Profile</UserGroup>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true</StandardAuthenticationOnly>
 <IKEIdentity>secure_client_PPK</IKEIdentity>
 <PPK_ID>PPKID_test</PPK_ID>
</PrimaryProtocol>
</HostEntry>
```

使用后量子预共享密钥在 ASA 上配置 VPN 身份验证

ASA 中的隧道组用于标识 VPN 连接的组策略。您可以配置隧道组策略，使用 PPK 和 PSK 启用 VPN 身份验证。

开始之前

确保您查看 使用后量子预共享密钥进行 VPN 身份验证的前提条件，第 196 页 和 在 VPN 身份验证中使用后量子预共享密钥的准则和限制，第 197 页。

过程

步骤 1 配置隧道组的 IPsec 属性。

tunnel-group *name* **ipsec-attributes**

示例：

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

步骤 2 配置客户端的 PSK。

ikev2 remote-authentication pre-shared-key *key*

示例：

```
hostname(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key *****
```

步骤 3 配置 ASA 的 PSK。

ikev2 local-authentication pre-shared-key *key*

示例：

```
hostname(config-tunnel-ipsec)#ikev2 local-authentication pre-shared-key *****
```

步骤 4 配置客户端的 PPK。

ikev2 remote-authentication post-quantum-key *key* **identifier** *id* mandatory

- key：指定 PPK 密钥。
- ID：指定用于标识 PPK 的唯一字符串。此值必须与安全客户端的 VPN 配置文件中的 PPK ID 匹配。
- mandatory：指定 PPK 对于 VPN 连接是否为强制。如果未指定为强制，则 PPK 配置为可选。

示例：

```
hostname(config-tunnel-ipsec)#ikev2 remote-authentication post-quantum-key  *****
 identifier PPKID_test mandatory
```

以下示例显示了 ASA 使用 PPK 和 PSK 进行隧道组配置的片段：

示例

```
tunnel-group secure_client_PPK ipsec-attributes
       ikev2 remote-authentication pre-shared-key *****
       ikev2 local-authentication pre-shared-key *****
       ikev2 remote-authentication post-quantum-key ***** identity PPKID_test mandatory
```

请注意以下提示：

- 隧道组名称必须与 VPN 配置文件的 IKEIdentity 字符串匹配。
- 隧道组配置中的 PPK ID 必须与 VPN 配置文件的 PPK_ID 相匹配。

其他参考资料

- RFC 8784
- Cisco Secure 客户端（包括 AnyConnect）管理员指南，5 版

远程访问 IPsec VPN 配置示例

以下示例显示如何配置远程访问 IPsec/IKEv1 VPN：

```
hostname(config)# crypto ikev1 policy 10
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption aes-256
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config)# crypto ikev1 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev1 transform set AES256-SHA
esp-aes-256 esp-sha-hmac
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-ipsec)# ikev1 pre-shared-key ravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev1
transform-set AES256-SHA
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

以下示例显示如何配置远程访问 IPsec/IKEv2 VPN：

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)# integrity sha512
hostname(config-ikev2-policy)# prf sha512
hostname(config)# crypto ikev2 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev2 ipsec-proposal  AES256-SHA512
hostname(config-ipsec-proposal)# protocol esp encryption  aes-256
hostname(config-ipsec-proposal)# protocol esp integrity sha-512
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-tunnel-ipsec)# ikev2 local-authentication
```

```
pre-shared-key localravpnkey
hostname(config-tunnel-ipsec)# ikev2 remote-authentication
pre-shared-key remoteravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev2
ipsec-proposal AES256-SHA512
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

多情景模式下基于标准的IPSec IKEv2远程访问VPN的配置示例

以下示例显示如何为多情景模式下基于标准的远程访问 IPsec/IKEv2 VPN 配置 ASA。示例分别提供有关系统情景配置和用户情景配置的信息。

对于系统情景配置：

```
class default
  limit-resource All 0
  limit-resource Mac-addresses 65536
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource VPN AnyConnect 4.0%

hostname(config)#context CTX2
hostname(config-ctx)#member default   ===============> License allotment for contexts using
 class
hostname(config-ctx)#allocate-interface Ethernet1/1.200
hostname(config-ctx)#allocate-interface Ethernet1/3.100
hostname(config-ctx)#config-url disk0:/CTX2.cfg
```

对于用户情景配置：

```
hostname/CTX2(config)#ip local pool CTX2-pool 1.1.2.1-1.1.2.250 mask 255.255.255.0
hostname/CTX2(config)#aaa-server ISE protocol radius
hostname/CTX2(config)#aaa-server ISE (inside) host 10.10.190.100
hostname/CTX2(config-aaa-server-host)#key *****
hostname/CTX2(config-aaa-server-host)#exit
hostname/CTX2(config)#

hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 internal
hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 attributes
hostname/CTX2(config-group-policy)#vpn-tunnel-protocol ikev2
hostname/CTX2(config-group-policy)#exit
hostname/CTX2(config)#

hostname/CTX2(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX2(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
```

```
hostname/CTX2(config)#crypto map outside_map interface outside
```

默认情况下，从基于标准的客户端的 IPSec/IKEv2 远程访问连接位于隧道组 DefaultRAGroup 中。

```
hostname/CTX2(config)#tunnel-group DefaultRAGroup type remote-access
hostname/CTX2(config)#tunnel-group DefaultRAGroup general-attributes
hostname/CTX2(config-tunnel-general)#default-group-policy GroupPolicy_CTX2-IKEv2
hostname/CTX2(config-tunnel-general)#address-pool CTX2-pool
hostname/CTX2(config-tunnel-general)#authentication-server-group ISE
hostname/CTX2(config-tunnel-general)#exit
hostname/CTX2(config)#
```

```
hostname/CTX2(config)#tunnel-group DefaultRAGroup ipsec-attributes
hostname/CTX2(config-tunnel-ipsec)#ikev2 remote-authentication eap query-identity
hostname/CTX2(config-tunnel-ipsec)#ikev2 local-authentication certificate ASDM_TrustPoint0
hostname/CTX2(config-tunnel-ipsec)#exit
hostname/CTX2(config)#
```

多情景模式下 Secure Client IPSec IKEv2 远程访问 VPN 的配置示例

以下示例显示如何为多情景模式下 Secure Client 远程访问 IPsec/IKEv2 VPN 配置 ASA。示例分别提供有关系统情景配置和用户情景配置的信息。

对于系统情景配置：

```
class default
    limit-resource All 0
    limit-resource Mac-addresses 65536
    limit-resource ASDM 5
    limit-resource SSH 5
    limit-resource Telnet 5
    limit-resource VPN AnyConnect 4.0%
```

```
hostname(config)#context CTX3
hostname(config-ctx)#member default   ===============> License allotment for contexts using
 class
hostname(config-ctx)#allocate-interface Ethernet1/1.200
hostname(config-ctx)#allocate-interface Ethernet1/3.100
hostname(config-ctx)#config-url disk0:/CTX3.cfg
```

每种情景的虚拟文件系统创建都会包含 Secure Client 文件，例如映像和配置文件。

```
hostname(config-ctx)#storage-url shared disk0:/shared disk0
```

对于用户情景配置：

```
hostname/CTX3(config)#ip local pool ctx3-pool 1.1.3.1-1.1.3.250 mask 255.255.255.0
hostname/CTX3(config)#webvpn
hostname/CTX3(config-webvpn)#enable outside
hostname/CTX3(config-webvpn)# anyconnect image
disk0:/anyconnect-win-4.6.00010-webdeploy-k9.pkg 1
hostname/CTX3(config-webvpn)#anyconnect profiles IKEv2-ctx1 disk0:/ikev2-ctx1.xml
hostname/CTX3(config-webvpn)#anyconnect enable
```

```
hostname/CTX3(config-webvpn)#tunnel-group-list enable


hostname/CTX3(config)#username cisco password *****
hostname/CTX3(config)#ssl trust-point ASDM_TrustPoint0 outside
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 internal
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 attributes


hostname/CTX3(config-group-policy)#vpn-tunnel-protocol ikev2 ssl-client
hostname/CTX3(config-group-policy)#dns-server value 10.3.5.6
hostname/CTX3(config-group-policy)#wins-server none
hostname/CTX3(config-group-policy)#default-domain none
hostname/CTX3(config-group-policy)#webvpn
hostname/CTX3(config-group-webvpn)#anyconnect profiles value IKEv2-ctx1 type user
```

在以下示例中，要启用客户端服务，请使用 **crypto ikev2 enable outside client-services** 命令。

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

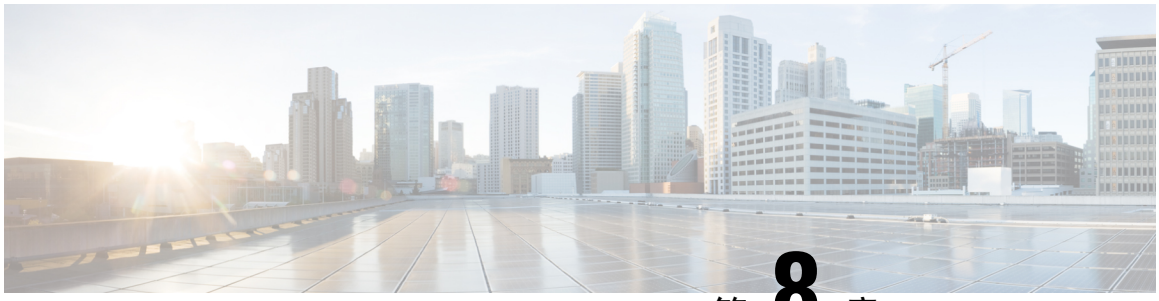
注释 您可以使用与在同一设备上运行的 SSL VPN 相同的端口。即使配置了 SSL VPN，您也必须选择此选项，以便通过 SSL 为 IPsec-IKEv2 客户端启用文件下载。

```
hostname/CTX3(config)#crypto ikev2 enable outside client-services port 443
hostname/CTX3(config)#crypto ikev2 remote-access trustpoint ASDM_TrustPoint0
hostname/CTX3(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX3(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
hostname/CTX3(config)#crypto map outside_map interface outside


hostname/CTX3(config)#tunnel-group CTX3-IKEv2 type remote-access
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 general-attributes
hostname/CTX3(config-tunnel-general)#default-group-policy GroupPolicy_CTX3-IKEv2
hostname/CTX3(config-tunnel-general)#address-pool ctx3-pool
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 webvpn-attributes
hostname/CTX3(config-tunnel-webvpn)#group-alias CTX3-IKEv2 enable
```

远程访问 VPN 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)	添加了对 Secure Client 的 IPsec IKEv2 支持。

功能名称	版本	功能信息
远程访问 VPN 的 mobike 自动支持。	9.8(1)	添加了 IPsec IKEv2 RA VPN 的移动 IKE (mobike) 支持。Mobike 始终开启。 添加了 `ikev2 mobike rrc` 命令以在 IKEv2 RA VPN 连接的 mobike 通信期间启用返回路由能力检查。
多情景模式下 IPsec IKEv2 的远程访问 VPN	9.9(2)	支持配置 ASA，以允许 Secure Client 和基于标准的第三方 IPSec IKEv2 VPN 客户端建立远程访问 VPN 会话，连接到以多情景模式运行的 ASA。 添加了 `ikev2 rsa-sig-hash sha1` 命令，以便对身份验证负载进行签名。
使用 SHA-1 散列算法的 RSA，用于对身份验证负载签名	9.12(1)	在使用第三方基于标准的 IPSec IKEv2 VPN 客户端与 ASA 建立远程访问 VPN 会话时，支持使用 SHA-1 散列算法来对身份验证负载进行签名。
弃用 IKE/IPsec 加密和完整性/PRF 密码 对 IKEv1 的 DH 组 14 支持	9.13(1)	以下加密/完整性/PRF 密码已弃用，并将在后续版本 - 9.14(1) 中删除： • 3DES 加密 • DES 加密 • MD5 完整性 添加了对 IKEv1 的 DH 组 14（默认）支持。group 2 和 group 5 命令选项已弃用，并将在后续版本 9.14(1) 中删除。



第 8 章

LAN 间 IPsec VPN

LAN 间 VPN 可连接不同地理位置的网络。

可以创建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 间 IPsec 连接。这些对等体可以采用内部和外部地址（使用 IPv4 和 IPv6 选址）的任意组合。

ASA 不允许通过 VPN 隧道传输 ping 以外的本地源流量。

本章介绍如何构建 LAN 间 VPN 连接。

配置摘要

本节提供本章介绍的示例 LAN 间配置的摘要。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 aes
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 aes
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-aes esp-sha-hmac
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)# protocol esp encryption aes
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。

过程

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。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，如同对使用站点间VPN的单情景VPN配置进行配置一样。

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，请在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。

注释 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。

过程

步骤 1 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 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 要命名接口，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 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 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，请使用相同程序。

在外部接口上配置 ISAKMP 策略和启用 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 属性的格式的通用框架。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：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 创建用于对对等体进行身份验证的加密密钥。

ASA 支持为旧版思科 VPN 客户端连接使用 IKEv1，还支持为 AnyConnect VPN 客户端使用 IKEv2。

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。
- 散列消息身份验证代码 (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未发生修改。
- 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散列密钥。
- 对于 IKEv2，使用单独的伪随机函数 (PRF) 作为派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法。
- 在更换加密密钥前，ASA 可使用该加密密钥的时间限制。

通过 IKEv1 策略，可以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 将按照安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。利用这种排序，您可以发送单个提议来传达所有允许的转换，而无需像对 IKEv1 一样发送每个允许的组合。

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：

- 为 IKEv1 连接配置 ISAKMP 策略，第 210 页
- 为 IKEv2 连接配置 ISAKMP 策略，第 211 页

为 IKEv1 连接配置 ISAKMP 策略

要为 IKEv1 连接配置 ISAKMP 策略，请使用 **crypto ikev1 policy** 命令进入 IKEv1 策略配置模式，在此模式下可以配置 IKEv1 参数。

过程

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：

```
hostname(config-ikev1-policy)# encryption aes
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 群。以下示例配置组 14：

```
hostname(config-ikev1-policy)# group 14
hostname(config-ikev1-policy)#
```

步骤 6 设置加密密钥生命周期。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 如要保存更改，请输入 **write memory** 命令：

```
hostname(config)# write memory
hostname(config)#
```

为 IKEv2 连接配置 ISAKMP 策略

要为 IKEv2 连接配置 ISAKMP 策略，请使用 **crypto ikev2 policy** 命令进入 IKEv2 策略配置模式，在此模式下可以配置 IKEv2 参数。

过程

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。以下是配置 AES 的示例：

```
hostname(config-ikev2-policy)# encryption aes
hostname(config-ikev2-policy)#
```

步骤 3 设置 Diffie-Hellman 群。以下是配置组 15 的示例：

```
hostname(config-ikev2-policy)# group 15
hostname(config-ikev2-policy)#
```

步骤 4 设置用作派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法的伪随机函数 (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 设置加密密钥生命周期。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)#
```

IKEv2 的多密钥交换

IKEv2 使用 Diffie-Hellman (DH) 组在发起方和响应方之间建立共享密钥。IKEv2 支持额外的密钥交换，以保护 IPsec 通信免受量子计算机的攻击。每个交换都会使用不同的 DH 组。为 SA 设置计算出的共享密钥是从每次交换派生的所有密钥的组合。IKE SA 是在 IKE 对等体之间交换多个密钥后建立的。

ASA 对多密钥交换使用七种新的转换类型：

- 额外密钥交换 1（IANA 值 6）
- 额外密钥交换 2（IANA 值 7）
- 额外密钥交换 3（IANA 值 8）
- 额外密钥交换 4（IANA 值 9）
- 额外密钥交换 5（IANA 值 10）
- 额外密钥交换 6（IANA 值 11）
- 额外密钥交换 7（IANA 值 12）

您最多可以配置七个多密钥交换。对于配置的每个额外密钥交换，您必须指定 DH 组。ASA 使用从先前交换派生的密钥来对中间密钥交换进行加密。如果发起方和响应方对等体未就DH组达成一致，则协商失败，并会向发起方发送 **NO_PROPOSAL_CHOSEN** 错误通知。您还可以将转换配置为 none。如果选择 none，则不会进行密钥交换。

对于发起方，如果为额外密钥交换 *n* 将密钥交换方法配置为 **none**：

- 响应方可以为额外密钥交换 *n* 选择 **none** 作为密钥交换方法。
- 额外密钥交换为可选。

要让提议协商成功，发起方提议中的所有转换都必须与响应方中的转换相匹配。

在以下发起方示例中：

```
crypto ikev2 policy 1
encryption aes
integrity sha256
group 14
prf sha256
lifetime seconds 120
additional-key-exchange 5
key-exchange-method none
```

响应方必须具有 additional-key-exchange 5 才能匹配提议。

如果对等体不支持额外密钥交换，则会发生以下情况：

- 如果发起方有另一个与响应方提议匹配的 IKEv2 提议，则会建立 IKEv2 SA。
- 对等体将IKE_SA_INIT交换消息中的任何额外密钥交换转换类型视为未知转换类型，并跳过这些提议。协商失败，并会向发起方发送 **NO_PROPOSAL_CHOSEN** 错误通知。

有关此功能的详细信息，请参阅 RFC 9242。

IKEv2 多密钥交换的准则和限制

- 您最多可以有七个多密钥交换。
- 您无法在后续密钥交换中使用相同的 DH 组。

对于此功能，ASA 不支持：

- IKEv1
- 传统密钥交换和基于后量子算法的密钥交换组合。
- 远程访问 VPN。只有站点间 VPN 支持 IKEv2 多密钥交换。
- 集群

为 IKEv2 配置多密钥交换

此配置为可选，如果要保护 IPsec 通信免受量子计算机攻击，则可以执行此配置。

开始之前

- 查看准则和限制。有关详细信息，请参阅IKEv2 多密钥交换的准则和限制，第 213 页。
- 配置 IKEv2 策略的加密算法、散列算法、身份验证方法和 SA 生命周期。有关详细信息，请参阅配置 IKEv1 和 IKEv2 策略，第 7 页。

过程

步骤 1 创建 IKEv2 策略。

crypto ikev2 policy *policy_index*

提示符将显示 IKEv2 策略配置模式。

示例：

```
hostname(config)# crypto ikev2 policy 1
```

步骤 2 为 IKEv2 策略配置额外的密钥交换转换。

additional-key-exchange <*1-7*>

提示符将显示 IKEv2 策略额外密钥交换配置模式。一个策略最多可以配置七个密钥交换转换。

示例：

```
hostname(config-ikev2-policy)# additional-key-exchange 1
```

步骤 3 通过为额外密钥交换转换定义一个或多个 DH 组来配置密钥交换方法。

key-exchange-method <*DH_group*>

将 DH 组指定为 14、15、16、19、20、21 或 31。您还可以将转换配置为 none。如果选择 none，则不会进行密钥交换。

示例：

```
hostname(config-ikev2-policy-ake)# key-exchange-method 21 31
```

步骤 4 重复步骤 2 和 3，为 IKEv2 策略配置多个密钥交换。

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# additional-key-exchange 1
hostname(config-ikev2-policy-ake)# key-exchange-method 21 31
hostname(config-ikev2-policy)# additional-key-exchange 2
hostname(config-ikev2-policy-ake)# key-exchange-method 20 21
hostname(config-ikev2-policy)# additional-key-exchange 3
hostname(config-ikev2-policy-ake)# key-exchange-method 19 20 none
...
```

下一步做什么

确认配置。有关详细信息，请参阅验证 IKEv2 多密钥交换配置 ， 第 215 页。

验证 IKEv2 多密钥交换配置

使用以下显示命令来查看或验证 IKEv2 多密钥交换配置：

- **show running-config crypto ikev2**

```
crypto ikev2 policy 1
encryption aes
integrity sha256
group 14
prf sha256
lifetime seconds 120
additional-key-exchange 1
key-exchange-method 21 31
additional-key-exchange 2
key-exchange-method 20 21
...
```

- **show crypto ikev2 sa detail**

```
IKEv2 SAs:
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local Remote fvrf/ivrf Status Role
41567725 192.168.15.1/500 192.168.15.2/500 READY INITIATOR
Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Additional Key Exchange Group: AKE1: 31 AKE2: 21 AKE3: 20 AKE4: 19 AKE5: 16 AKE6: 15
AKE7: 14
Life/Active Time: 120/5 sec
Session-id: 4
Status Description: Negotiation done
Local spi: 6BB6B7BFA0BAADF4 Remote spi: 7030C7xxx xxxxxxE9DBDE77EB
Local id: 192.168.15.1
Remote id: 192.168.15.2
Local req mess id: 9 Remote req mess id: 0
Local next mess id: 9 Remote next mess id: 0
Local req queued: 9 Remote req queued: 0
Local window: 1 Remote window: 1
DPD configured for 10 seconds, retry 2
NAT-T is not detected
IKEv2 Fragmentation Configured MTU: 576 bytes, Overhead: 28 bytes, Effective MTU: 548
bytes
Parent SA Extended Status:
Delete in progress: FALSE
```

```
Marked for delete: FALSE
Child sa: local selector 20.0.0.0/0 - 20.0.0.255/65535
remote selector 30.0.0.0/0 - 30.0.0.255/65535
ESP spi in/out: 0x4a7d5da2/0x56a28fa8
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

创建 IKEv1 转换集

IKEv1 转换集由加密方法和身份验证方法组成。在与 ISAKMP 进行 IPsec 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。

转换集保护关联的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多 11 个转换集。

下表列出了有效的加密和身份验证方法。

表 *11*: 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-sha-hmac（默认）
esp-aes（128 位加密）（默认）	
esp-aes-192	
esp-aes-256	
esp-null	

在通过不可信网络（例如公共互联网）连接的两个 ASA 之间，通常采用隧道模式实施 IPsec。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：

过程

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-aes 加密 和 esp-sha-hmac 身份验证来配置转换集。语法如下：

esp-sha-hmac（默认）

crypto ipsec ikev1 transform-set *transform-set-nameencryption-method authentication-method*

```
hostname(config)#
crypto ipsec transform-set FirstSet esp-aes esp-sha-hmac
hostname(config)#
```

步骤 2 保存更改。

```
hostname(config)# write memory
hostname(config)#
```

创建 IKEv2 提议

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 将按照安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。利用这种排序，您可以发送单个提议来传达所有允许的转换，而无需像对 IKEv1 一样发送每个允许的组合。

下表列出了有效的 IKEv2 加密和身份验证方法。

表 *12:* 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
	sha（默认）
aes（默认）- 使用 128 位密钥的 AES。	
aes-192	
aes-256	

如要配置 IKEv2 提议，请在单情景或多情景模式下执行以下任务：

过程

步骤 1 在全局配置模式下，使用 **crypto ipsec ikev2 ipsec-proposal** 命令进入 ipsec 提议配置模式，在此模式下可以为提议指定多个加密和完整性类型。在以下示例中，secure 是提议的名称：

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

步骤 2 然后，输入协议和加密类型。ESP 是唯一支持的协议。例如：

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

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 间 VPN 控制连接配置的 ACL 基于源 IP 地址和转换的目标 IP 地址以及（可选）端口。配置在连接两端相互镜像的 ACL。

VPN 流量的 ACL 使用转换的地址。

注释 有关使用 VPN 过滤器配置 ACL 的详细信息，请参阅为远程访问指定 VLAN 或对组策略应用统一访问控制规则，第 134 页。

过程

步骤 1 输入 **access-list extended** 命令。

access-list *listname* **extended permit ip** *source-ipaddress source-netmask destination-ipaddress destination-netmask*

以下示例配置名为 l2l_list 的 ACL，允许来自 192.168.0.0 网络中 IP 地址的流量传送到 150.150.0.0 网络。

```
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 在连接的另一端为 ASA 配置一个 ACL，对该 ACL 进行镜像。

加密映射中的 ACL 或附加到同一加密映射的两个不同加密 ACL 中定义的子网不得重叠。

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)#
```

定义隧道组

隧道组是包含隧道连接策略的一组记录。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 中有两个默认隧道组：DefaultRAGroup 和 DefaultL2Lgroup，前者是默认的 IPsec 远程访问隧道组，后者是默认的 IPsec LAN 间隧道组。可以修改这些隧道组，但不能将其删除。

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，其中一端对一个凭证进行身份验证，另一端使用其他凭证（预共享密钥或证书）。

您也可以根据环境创建一个或多个新隧道组。如果在隧道协商过程中没有标识特定隧道组，ASA 将会使用这两个隧道组来配置远程访问隧道组和 LAN 间隧道组的默认隧道参数。

要建立基本 LAN 间连接，必须为隧道组设置两个属性：

- 将连接类型设置为 IPsec LAN 间。
- 配置 IP 地址的身份验证方法（即用于 IKEv1 和 IKEv2 的预共享密钥）。

过程

步骤 1 要将连接类型设置为 IPsec LAN 间，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 间）

在以下示例中，隧道组的名称是 LAN 间对等体的 IP 地址 10.10.4.108。

```
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)#
```

注释
仅当隧道身份验证方法为数字证书和/或对等体配置为使用积极模式时，才能使用名称非 IP 地址的 LAN 间隧道组。

步骤 2 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 **ikev1pre-shared-key** 命令以创建预共享密钥。需要在此 LAN 间连接的两个 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)# ikev1-pre-shared-key 44kkaol59636jnfx
```

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 crypto 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，它们必须至少符合以下条件：

- 加密映射条目必须包含兼容的加密 ACL（例如，镜像 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动态加密映射）。
- 加密映射条目必须至少有一个共同的转换集。

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 先按照优先级较高的映射条目评估流量。

如果反向路由注入 (RRI) 被应用于加密映射，则该映射对于 ASA 上的一个接口必须是唯一的。换而言之，同一加密映射不能被应用于多个接口。如果将多个加密映射应用于多个接口，则可能无法正确清除路由。如果多个接口需要加密映射，则每个路由都必须使用唯一定义的映射。

如果存在以下任意情况，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。
- 您想要将不同的 IPSec 安全应用于不同类型的流量（面向相同或不同的对等体），例如您希望对一组子网之间的流量进行身份验证，而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，请在两个单独的 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。

在多个接口上应用加密映射

对于双 ISP，您可以将加密映射应用于 ASA 上的外部接口和备份接口。在使用此配置时，仅发起选项不可用。如果需要此冗余，则您必须使用 Virtual Tunnel Interface (VTI)。

在多个接口上使用加密映射时：

- 您必须有路由协议或路由跟踪。
- 确保远程端也使用路由协议。
- 您必须为同一个加密映射谨慎选择多个接口，因为ASA允许来自具有较低首选路由的接口上的远程站点的连接。

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：

过程

步骤 1 要将 ACL 分配到加密映射条目，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 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 | hostname1}[... ip_address10 | hostname10]。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 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 提议，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，提议名称为 secure。

通过 **crypto map** 命令，可以为单个映射索引指定多个 IPsec 提议。在该情况下，多个提议会在协商过程中传输到 IKEv2 对等体，并且提议的顺序由管理员在加密映射条目排序时确定。

注释
如果 IPsec 提议中存在组合模式 (AES-GCM/GMAC) 和普通模式（所有其他类型）算法，则无法将单个提议发送到对等体。在此情况下必须具有至少两个提议，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)#
```

将加密映射应用于接口

您必须对 IPsec 流量经过的每个接口应用加密映射集。ASA 在所有接口上都支持 IPsec。对接口应用加密映射集将命令 ASA 按照该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：

过程

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)#
```

动态站点间 VPN 概述

在动态站点间 VPN 中，环回接口用作 VPN 隧道的源和目标。您可以使用这些接口在安全网关之间移动站点到站点对等体，而无需更新对等体。当环回地址通过路由协议传播时，ASA 会将流量从远程对等体无缝重定向到新的安全网关集群，而无需更改对等体上的配置。

注释 此功能不适用于评估许可证。

在动态站点间 VPN 中使用环回接口的优势

- 冗余：在物理链路或接口发生故障期间，由于环回接口仍可通过多个物理接口访问，因此 VPN 连接保持存在。在集群中，如果具有环回接口的节点发生故障，则接口和会话将转移到备用节点。
- 动态环回地址重新分配：将环回地址重新分配给其他安全网关集群期间会保留 VPN 连接，而无需更改远程对等体。
- 动态路径选择 (Dynamic Path Selection)：当路由协议动态选择站点之间的最佳路径时，VPN 连接会得到优化，从而提高性能和可靠性。

使用具有环回接口的动态 VPN 的前提条件

一般前提条件

此功能受以下支持：

- Cisco Secure Firewall 4200 系列版本 9.24.1
- 第 2 层集群
- 与动态加密映射附加的静态加密映射。

许可证前提条件

此功能需要许可证：

- 具有强加密的基础许可证。
- 分布式 VPN 模式的运营商许可证。

使用环回接口配置动态站点间 VPN

开始之前

确保您查看 使用具有环回接口的动态 VPN 的前提条件，第 223 页。

过程

步骤 1 使用 **interface** 命令配置外部接口：

a) 使用 **nameif** 命令配置环回接口的名称。
b) 使用 security-level 命令配置 **安全级别** 。
c) 使用 **ip address** 命令来配置接口的 IP 地址。

示例：

```
hostname(config)# interface ethernet0/0
hostname(config-if)#nameif outside
hostname(config-if)#security-level 0
hostname(config-if)#ip address 192.0.2.17 255.255.255.0
```

步骤 2 使用 **interface** 命令配置第 2 层环回接口：

a) 使用 **description** 命令配置说明。
b) 使用 **nameif** 命令配置环回接口的名称。
c) 使用 **ip address** 命令来配置环回接口的 IP 地址。

示例：

```
hostname(config)# interface Loopback2
hostname(config-if)#description Loopback to terminate Group 2
hostname(config-if)#nameif LB2
hostname(config-if)#ip address 209.165.201.1 255.255.255.252
```

步骤 3 使用 **crypto ipsec ikev2 ipsec-proposal** *proposal tag* 命令配置 IKEv2 IPsec 提议：

a) 使用 **description** 命令配置说明。
b) 使用 **protocol esp encryption** 命令配置加密协议。
c) 使用 **protocol esp integrity** 命令配置加密和完整性协议。

示例：

```
hostname(config)#crypto ipsec ikev2 ipsec-proposal ESP-AES-SHA
hostname(config-ipsec-proposal)#protocol esp encryption aes
hostname(config-ipsec-proposal)#protocol esp integrity sha-256
```

步骤 4 使用 **crypto ikev2 policy** *policy_index*命令配置 IKEv2 策略：

a) 使用 **protocol esp encryption** 命令配置加密协议。
b) 使用 **protocol esp integrity** 命令配置加密和完整性协议。
c) 使用 **group** 命令来配置 Diffie-Hellman 群。
d) 使用 **prf** 命令配置伪随机函数 (PRF) 该伪随机函数用作导出密钥材料和 IKEv2 隧道加密所需的哈希操作的算法。
e) 使用 **生命周期** 命令配置加密钥的生命周期。

示例：

```
hostname(config)#crypto ikev2 policy 1
hostname(config-ikev2-policy)#protocol esp encryption aes-256
hostname(config-ikev2-policy)#protocol esp integrity sha
hostname(config-ikev2-policy)#group 5
hostname(config-ikev2-policy)#prf sha
hostname(config-ikev2-policy)#lifetime seconds 86400
```

步骤 5 创建动态加密映射

a) 使用 **crypto dynamic-map** *dynamic-map-name dynamic-sequence-num* **set ikev2 ipsec-proposal** *transform-set-name1* 命令配置动态加密映射并为该映射指定 IKEv2 转换集。

b) 使用 **crypto dynamic-map** *dynamic-map-name dynamic-sequence-num* **set reverse-route** 命令根据此加密映射条目为任何连接启用反向路由注入。

示例：

```
hostname(config)#crypto dynamic-map dmap 1 set ikev2 ipsec-proposal ESP-AES-SHA
hostname(config)#crypto dynamic-map dmap 1 set reverse-route
```

步骤 6 配置静态加密映射：

a) 使用 **crypto map** *map-name sequence-num* **ipsec-isakmp dynamic** *dynamic-map-name* 命令将动态加密映射集添加到静态加密映射集中。

b) 使用 **crypto map** *map-name* **interface** *loopback_interface* 命令将静态加密映射应用到环回接口。

示例：

```
hostname(config)#crypto map vpn 1 ipsec-isakmp dynamic dmap
hostname(config)#crypto map vpn interface LB2
```

步骤 7 配置默认 LAN 间隧道组：

a) 使用 **tunnel-group DefaultL2LGroup ipsec-attributes** 命令配置默认 LAN 到 LAN 隧道组的 IPsec IKEv2 属性。

b) 使用 **ikev2 remote-authentication pre-shared-key** *key* 命令配置用于对远程对等体进行身份验证的预共享密钥 (PSK)。

c) 使用 **ikev2 local-authentication pre-shared-key** *key* 命令配置用于对本地设备进行身份验证的预共享密钥。

示例：

```
hostname(config)#tunnel-group DefaultL2LGroup ipsec-attributes
hostname(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key ****
hostname(config-tunnel-ipsec)#ikev2 local-authentication pre-shared-key ****
```

步骤 8 在环回接口上使用 **crypto ikev2 enable** *loopback_interface* 命令启用 IKEv2：

示例：

```
hostname(config)#crypto ikev2 enable LB2
```

步骤 9 配置路由协议以通告环回接口。

示例：

配置 OSPF 示例:

```
hostname(config)#router ospf 1
hostname(config-router)#network 203.0.113.0 255.255.255.0 area 0
hostname(config-router)#network 209.165.201.1 255.255.255.252 area 0
hostname(config-router)#log-adj-changes
hostname(config-router)#redistribute connected

hostname(config)#interface outside
hostname(config-interface)#ospf cost 1
hostname(config-interface)#ospf message-digest-key 1 md5 *****
hostname(config-interface)#ospf authentication message-digest
```

验证动态站点间 IPsec VPN 配置。

使用以下显示命令来验证动态站点间 VPN（使用环回接口）配置：

显示 vpn-sessiondb

```
asa-node2/data-node# show vpn-sessiondb det l2l

Session Type: LAN-to-LAN Detailed

Connection   : DefaultL2LGroup
Index        : 399                    IP Addr      : <Peer-IP>
Protocol     : IKEv2 IPsec
Encryption   : IKEv2: (1)AES128  IPsec: (1)AES128
Hashing      : IKEv2: (1)SHA256  IPsec: (1)SHA256
Bytes Tx     : 58680                  Bytes Rx     : 86152
Login Time   : 09:59:41 EDT Tue Apr 8 2025
Duration     : 0h:01m:21s
Session State: Cluster Owner (backup is asa-node1)

IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
  Tunnel ID    : 399.1
  UDP Src Port : 500                    UDP Dst Port : 500
  Rem Auth Mode: preSharedKeys
  Loc Auth Mode: preSharedKeys
  Encryption   : AES128                 Hashing      : SHA256
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86319 Seconds
  PRF          : SHA256                 D/H Group    : 14
  Filter Name  : trace

IPsec:
  Tunnel ID    : 399.2
  Local Addr   : 209.165.201.1 255.255.255.0/0/0
  Remote Addr  : 192.0.2.20 255.255.255.0/0/0
  Encryption   : AES128                 Hashing      : SHA256
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28715 Seconds
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Bytes Tx     : 58680                  Bytes Rx     : 86152
  Pkts Tx      : 978
```

显示 crypto ikev2

```
asa-node2/data-node# show crypto ikev2 sa
IKEv2 SAs:
Session-id:399, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local                         Remote
fvrf/ivrf     Status         Role
   724781 209.165.201.1/500           192.0.2.20/500
Global/Global      READY    RESPONDER

   ...
```

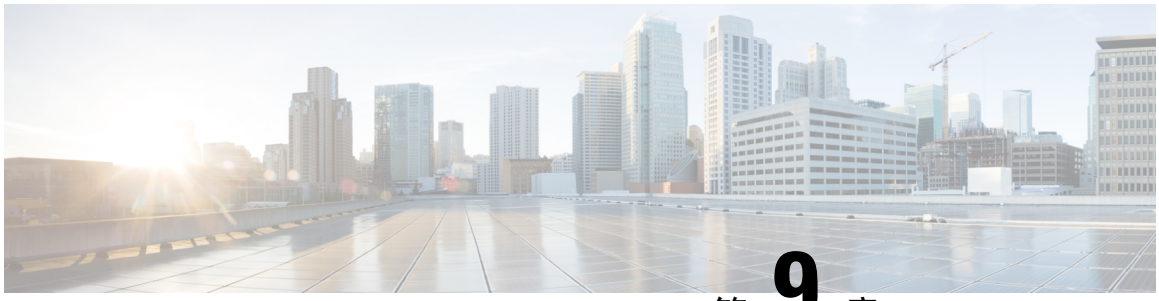
show crypto ipsec sa

```
asa-node2/data-node# show crypto ipsec sa

interface: LB2
```

验证动态站点间 IPsec VPN 配置。

```
 Crypto map tag: dyn-loop1, seq num: 65535, local addr: 209.165.201.1
...
```

验证动态站点间 IPsec VPN 配置。



第 9 章

AnyConnect VPN 客户端连接

本节介绍如何配置 AnyConnect VPN 客户端连接。

关于 Secure Client VPN 客户端

Secure Client为远程用户提供了与 ASA 的安全 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:// 请求重定向到 https://，否则用户必须以 https://<*address*> 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。

当客户端与 ASA 协商 SSL VPN 连接时，实际上会使用传输层安全 (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。

Secure Client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，请参阅相应版本的《思科 AnyConnect 安全移动配置指南》。

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 配置为在超时期限结束后下载客户端，或显示登录页面。

要求 Secure Client

有关运行 Secure Client的终端计算机的要求，请参阅 相应版本的《思科 AnyConnect 安全移动版本说明》。

准则和限制 Secure Client

- ASA 不会验证远程 HTTPS 证书。
- 支持单情景或多情景模式。在多情景模式下，远程访问 VPN 需要 AnyConnect Apex 许可证。尽管 ASA 未明确认可 AnyConnect Apex 许可证，但它实施 Apex 许可证的特征，例如获得平台限制许可的 AnyConnect 高级版、Secure Client 移动版、适用于思科 VPN 电话的 Secure Client 和高级终端评估。系统不支持共享许可、AnyConnect 基础版、故障转移许可证聚合以及 Flex/基于时间的许可证。
- 不直接支持对 RA VPN 前端发出命令（例如 **curl** ），并且可能不会产生所需的结果。例如，前端不响应 HTTP HEAD 请求。
- 当硬件 VPN 电话（例如思科 88xx 系列）使用 Secure Client 时，尽管启用了 DTLS 并配置了对等体存活检测 (DPD)，但它们也可能会重新连接。
- 当客户端连接到 Secure Client 时，连接前后客户端的 IP 地址会更改。ASA 支持此行为。

Secure Client的许可要求

注释 此功能不适用于无负载加密型号。

VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。有关每个型号的最大值，请参阅思科 ASA 系列功能许可证。

如果启动无客户端 SSL VPN 会话，然后从门户启动 Secure Client 会话，则总共会使用 1 个会话。但是，如果先启动 Secure Client（例如，通过独立客户端），然后登录无客户端 SSL VPN 门户，则会使用 2 个会话。

配置 Secure Client 连接

本节介绍将 ASA 配置为接受 AnyConnect VPN 客户端连接的前提条件、限制和详细任务。

将 ASA 配置为以 Web 方式部署客户端

本节介绍将 ASA 配置为以 Web 方式部署 Secure Client的步骤。

开始之前

使用 TFTP 或其他方法将客户端映像包复制到 ASA。

注释 即使在 ASA 上禁用了无客户端 VPN 功能，当您使用 Web 浏览器访问 AnyConnect webdeploy (https://x.x.x.x<ASA IP address> 时，ASA 上的 VPN 会话将被算作无客户端会话。

过程

步骤 1 将闪存上的文件标识为 Secure Client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，请使用 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。

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
```

注释
使用 **anyconnect image** 命令配置 Secure Client 映像后，必须发出 **anyconnect enable** 命令。如果没有启用 Secure Client，则其不会执行预期操作，并且 **show webvpn anyconnect** 会将 SSL VPN 客户端视为未启用，而不是列出已安装的 Secure Client 包。

步骤 2 在接口上启用 SSL，以便进行无客户端或 Secure Client SSL 连接。

enable *interface*

示例：

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

步骤 3 在没有发出此命令的情况下，Secure Client 不会执行预期操作，而且 **show webvpn anyconnect** 命令会返回“SSL VPN is not enabled”，而不是列出已安装的 Secure Client 包。

anyconnect enable

步骤 4 （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。

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
```

步骤 5 将地址池分配至隧道组。

address-pool *poolname*

示例：

```
hostname(config)# tunnel-group telecommuters general-attributes
hostname(config-tunnel-general)# address-pool vpn_users
```

步骤 6 将默认组策略分配至隧道组。

default-group-policy *name*

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

步骤 7 启用在无客户端门户和 Secure Client GUI 登录页面上显示隧道组列表。该别名列表由 *group-alias name enable* 命令定义。

group-alias *name* **enable**

示例：

```
hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias sales_department enable
```

步骤 8 将 Secure Client 指定为组或用户的允许的 VPN 隧道协议。

tunnel-group-list enable

示例：

```
hostname(config)# webvpn
hostname(config-webvpn)# tunnel-group-list enable
```

步骤 9 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。

vpn-tunnel-protocol

示例：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# vpn-tunnel-protocol
```

下一步做什么

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。

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：

默认设置为启用客户端的永久性安装。客户端在会话结束时仍安装在远程计算机上。以下示例将现有组策略 *sales* 配置为在会话结束时从远程计算机上删除客户端。

```
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 Secure Client建立 SSL VPN 连接，以便使用两个并行隧道 - SSL 隧道和 DTLS 隧道。使用 DTLS 可避免与 SSL 连接关联的延迟和带宽问题，并且提高对于数据包延迟敏感的实时应用的性能。

开始之前

请参阅 配置高级 SSL 设置，第 82 页 在此头端上配置 DTLS 和使用的 DTLS 版本。

为使DTLS能够回退至TLS连接，必须启用对等体存活检测(DPD)。如果没有启用DPD，则当DTLS连接遇到问题时，连接会终止而不是回退至TLS。有关DPD的详细信息，请参阅配置对等体存活检测，第 244 页。

过程

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

a) 在 webvpn 模式下，在接口上启用 SSL 和 DTLS。

默认情况下，在接口上启用 SSL VPN 访问时，则会启用 DTLS。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

在 webvpn 配置模式下，使用 **enable** *interface* **tls-only** 命令为所有 Secure Client 用户禁用 DTLS。

如果禁用 DTLS，则 SSL VPN 连接只会与 SSL VPN 隧道连接。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside tls-only
```

b) 使用 **port** 和 **dtls port** 命令配置 SSL 和 DTLS 的端口。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
hostname(config-webvpn)# port 555
hostname(config-webvpn)# dtls port 556
```

步骤 2 为特定组策略指定 DTLS 选项。

a) 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。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl dtls enable
```

b) 如果需要，使用 anyconnect dtls compression 命令启用 DTLS 压缩。

```
hostname(config-group-webvpn)# anyconnect dtls compression lzs
```

提示远程用户

过程

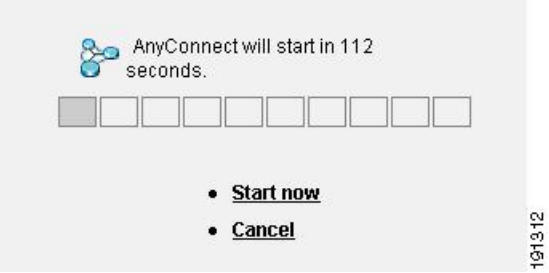
您可以在组策略 webvpn 或用户名 webvpn 配置模式下，使用 **anyconnect ask** 命令来允许 ASA 提示远程 SSL VPN 客户端用户下载客户端：

[**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（下载客户端）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（显示无客户端门户页面）前等待长度为 *value* 的一段时间。

下图显示配置 **default anyconnect timeout** *value* 或**default webvpn timeout** *value* 时向远程用户显示的提示：

图 *6:* 向远程用户显示提示，提示其下载 ***SSL VPN*** 客户端



示例

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* 秒以便用户作出响应：

```
hostname(config-group-webvpn)# anyconnect ask enable default anyconnect timeout
 10
```

启用 Secure Client配置文件下载

您可以在 Secure Client 配置文件中启用 Secure Client 功能，这些配置文件是 XML 文件，包含核心客户端及其 VPN 功能以及可选客户端模块的配置设置。ASA 会在 Secure Client 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。

下载到客户端的文件格式如下：<*profile_name*>.xml。

您可以使用 Secure Client 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 或 ISE 启动的基于 GUI 的便捷配置工具。适用于 Windows 的 Secure Client 软件包提供了该编辑器，在您于选定的头端设备上加载 AnyConnect 包并将其指定为 Secure Client映像时，该编辑器会激活。

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 或 ISE 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 Secure Client及其配置文件编辑器的详细信息，请参阅相应版本的《思科 AnyConnect 安全移动配置指南》。

注释 Secure Client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。

过程

步骤 1 使用 ASDM/ISE 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。

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。

示例：

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
```

此时，这些配置文件可供组策略使用。

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：

示例：

您可以输入后面带有问号的 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 sales
```

下一示例将组策略配置为使用客户端配置文件类型为 *vpn* 的配置文件 *sales*：

```
asa1(config-group-webvpn)# anyconnect profiles value sales type vpn
asa1(config-group-webvpn)#
```

启用 Secure Client 延迟升级

延迟升级允许 Secure Client 用户延迟客户端升级的下载。当客户端更新可用时，Secure Client 会打开一个对话框，询问用户是想要进行更新，还是想要延迟升级。除非您已在 Secure Client 配置文件设置中将“自动更新”(AutoUpdate) 设置为已启用 *(Enabled)*，否则系统不会显示此升级对话框。

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 13: 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	备注
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 Secure Client 版本。 最低版本检查适用于头端上启用的所有模块。如果启用的任意模块（包括 VPN）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）	无（已禁用）	延迟升级提示在自动关闭之前显示的秒数。仅当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，则允许根据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	延迟更新	更新	发生 DeferredUpdateDismissTimeout 时采取的操作。

过程

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*]

示例：

以下示例显示如何添加自定义属性类型 DeferredUpdateAllowed 和 DeferredUpdateDismissTimeout：

```
hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed
description Indicates if the deferred update feature is enabled or not
```

```
hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateDismissTimeout
```

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：对于长值属性，您可以提供重复条目以允许连接。然而，在具备重复配置条目的情况下，系统将不会显示“延迟更新”对话框，并且用户不能延迟升级；相反，系统将会自动升级。

[**no**] **anyconnect-custom-data** *attr-type attr-name attr-value*

示例：

以下示例显示如何为自定义属性类型 DeferredUpdateDismissTimeout 和启用的 DeferredUpdateAllowed 添加命名值：

```
hostname(config)# anyconnect-custom-data DeferredUpdateDismissTimeout
def-timeout 150
hostname(config)# anyconnect-custom-data DeferredUpdateAllowed
def-allowed true
```

步骤 3 使用 **anyconnect-custom** 命令在组策略中添加或删除自定义属性命名值：

- **anyconnect-custom** *attr-type* **value** *attr-name*
- **anyconnect-custom** *attr-type* **none**
- **no anyconnect-custom** *attr-type*

示例：

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)# anyconnect-custom DeferredUpdateAllowed
value def-allowed
hostname(config-group-policy)# anyconnect-custom DeferredUpdateDismissTimeout
value def-timeout
```

启用 DSCP 预留

通过设置另一个自定义属性，可以仅对 DTLS 连接控制 Windows 或 OS X 平台上的差分服务代码点 (DSCP)。通过启用 DSCP 预留，设备可以优先处理延迟敏感型流量；路由器会考虑是否设置此选项，并且标记优先化的流量以提高出站连接质量。

过程

步骤 1 在 webvpn 配置模式下使用 **anyconnect-custom-attr** 命令创建自定义属性类型：

[no] anyconnect-custom-attr DSCPPreservationAllowed description Set to control Differentiated Services Code Point (DSCP) on Windows or OS X platforms for DTLS connections only.

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 DSCPPreservationAllowed true

注释
默认情况下，Secure Client 会执行 DSCP 预留 (true)。要将其禁用，请在头端将自定义属性设置为 false，然后重新启动连接。

启用其他 Secure Client 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 或 ISE）其需要的核心模块。当附加功能可供 Secure Client使用时，您需要更新远程客户端，以便其能够使用这些功能。

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。

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 Secure Client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 Secure Client启用图形标识和身份验证 (GINA) 的模块。以下程序显示如何启用 SBL：

过程

步骤 1 在组策略 webvpn 或用户名 webvpn 配置模式下，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。

示例：

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 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。以下示例显示配置文件 (AnyConnectProfile.tmpl) 中适用于 Windows 的相关部分：

```
<Configuration>
    <ClientInitialization>
        <UseStartBeforeLogon>false</UseStartBeforeLogon>
```

```
    </ClientInitialization>
```

<UseStartBeforeLogon> 标记确定客户端是否使用 SBL。如要打开 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 Secure Client 用户消息的语言

ASA 提供语言转换功能，此功能适用于向发起基于浏览器的无客户端 SSL VPN 连接的用户所显示的门户和屏幕，以及向 Cisco AnyConnect VPN 客户端用户所显示的界面。

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。在 Cisco AnyConnect VPN 客户端的用户界面上显示的所有消息都位于 Secure Client 域中。

ASA 的软件映像包中含有用于 Secure Client 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，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 Secure Client 域的转换表的更改会立即向 Secure Client用户显示。

创建转换表

以下程序描述如何创建 Secure Client 域的转换表：

过程

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 import 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
```

```
PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
```

接着，用户可以导出 Secure Client 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 对中文的缩写。

```
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 Secure Client 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)，该消息会在客户端建立 VPN 连接时显示在 Secure Client GUI 上。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"
```

请务必保存文件。

步骤 3 在特权 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 对美国所使用的西班牙语的缩写。

```
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

customization
keepout
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
es-us AnyConnect
```

删除转换表

如果不再需要转换表，则可以将其删除。

过程

步骤 1 列出现有转换表。

在以下示例中，**show import webvpn translation-table** 命令显示可用的转换表模板和转换表。各种转换表支持法语 (fr)、日语 (ja) 和俄语 (ru) 版本。

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
```

```
  customization
  url-list
  webvpn
Translation Tables:
  fr                    PortForwarder
  fr                    AnyConnect
  fr                    customization
  fr                    webvpn
  ja                    PortForwarder
  ja                    AnyConnect
  ja                    customization
  ja                    webvpn
  ru                    PortForwarder
  ru                    customization
  ru                    webvpn
```

步骤 2 删除不需要的转换表。

revert webvpn translation-table *translationdomain* **language** *language*

其中，*translationdomain* 为上述转换表列表右侧列出的域，*language* 为语言名称，长度为 2 个字符。

必须逐个删除每个转换表。无法使用一个命令删除给定语言版本的所有转换表。

例如，要删除 Secure Client 的法语版本转换表：

```
ciscoasa# revert webvpn translation-table anyconnect language fr
ciscoasa#
```

配置高级 Secure Client SSL 功能

下一节介绍可精细调整 Secure Client SSL VPN 连接的高级功能。

启用重新生成密钥

ASA 与 Secure Client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。

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** 指定客户端在重新生成密钥的过程中建立新的隧道。
- **method ssl** 指定客户端在重新生成密钥的过程中建立新的隧道。
- **method none** 禁用重新生成密钥。
- **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，取值范围为 1 至 10080（1 周）。

注释 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，而不是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。

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
```

配置对等体存活检测

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

注释 当连接在客户端中断时，ASA 不会由于 DPD 或保持连接而无条件地丢弃 Secure Client 会话。仅当存在从 ASA 到客户端的数据流时，ASA 仅会触发 DPD。一旦触发 DPD，它会先对每个子会话 (SSL/DTLS) 进行三次重试，然后再将其断开。

如果那里没有数据流，则不会触发 DPD，ASA 具有硬编码的 5 分钟 TCP 非活动超时，当恰好 5 分钟没有数据或保持连接数据包流时，该超时会自动关闭 SSL/DTLS 隧道连接，无论配置的 VPN 空闲超时设置如何请参阅。断开子会话后，**vpn-idle-timeout** 命令仅负责控制可父会话的最长时间。有关 DPD、保持连接和超时属性的更多详细信息，请参阅 AnyConnect 常见问题解答 - 隧道、DPD 和非活动计时器 (AnyConnect FAQ - Tunnels, DPDs, and Inactivity Timer 。

开始之前

- 此功能仅适用于 ASA 网关与 Secure Client SSL VPN 客户端之间的连接。它不适用于 IPsec，因为 DPD 基于不允许填充的标准实施。
- 如果启用 DTLS，则也要启用对等体存活检测 (DPD)。DPD 允许已失败的 DTLS 连接回退至 TLS。否则，该连接会终止。
- 在 ASA 上启用 DPD 时，可以使用最佳 MTU (OMTU) 功能查找客户端可以成功传输 DTLS 数据包的最大终端 MTU。通过向最大 MTU 发送填充的 DPD 数据包来实施 OMTU。如果从头端接收到负载的正确回显，则接受 MTU 大小。否则，将减小 MTU 并再次发送探测，直到达到协议允许的最小 MTU 为止。

过程

步骤 1 转到所需的组策略。

进入组策略或用户名 webvpn 模式：

```
hostname(config)# group-policy group-policy-name  attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#
```

或，

```
hostname# username username attributes
hostname(config-username)# webvpn
hostname (config-username-webvpn #
```

步骤 2 设置网关端检测。

使用 [**no**] **anyconnect dpd-interval** {[**gateway** {*seconds* | **none**}] 命令。

网关是指 ASA。启用 DPD 并将 ASA 等待客户端数据包的时间间隔指定为从 30 秒（默认）至 3600 秒（1 小时）的范围。建议使用值 300。如果在该时间间隔内未收到任何数据包，则 ASA 将在相同的时间间隔内执行三次 DPD 测试。如果 ASA 未收到客户端的响应，则会断开 TLS/DTLS 隧道。

注释
指定 **none** 会禁用 ASA 执行的 DPD 测试。使用 **no anyconnect dpd-interval** 从配置中移除该命令。

指定 **none** 会禁用 ASA 执行的 DPD 测试。使用 **no anyconnect dpd-interval** 可从配置中删除此命令。

步骤 3 设置客户端检测。

使用 [**no**] **anyconnect dpd-interval** {[**client** {*seconds* | **none**}]} 命令。

客户端是指 Secure Client。启用 DPD 并将客户端执行 DPD 测试的频率指定为从 30 秒（默认）至 3600 秒（1 小时）的范围。建议的值为 30 秒。

指定 **client none** 会禁用客户端执行的 DPD。使用 **no anyconnect dpd-interval** 可从配置中删除此命令。

示例

以下示例为现有组策略销售将 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，即使设备限制了连接可处于空闲状态的时间也是如此。调整频率还可以确保客户端在远程用户没有主动运行基于套接字的应用（如 Microsoft Outlook 或 Microsoft Internet Explorer）时不会断开并重新连接。

默认情况下启用保持连接功能。如果禁用保持连接功能，发生故障转移事件时，SSL VPN 客户端会话不会被切换到备用设备。

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：要从配置中删除此命令并使值得到继承，请使用此命令的 **no** 形式：

[**no**] **anyconnect ssl keepalive** {**none** | *seconds*}

- **none** 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。

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，压缩可以减小要传输的数据包的大小，从而提高ASA与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。

注释 在宽带连接上实施压缩时，您必须谨慎考虑压缩依赖于无损连接这一事实。这也正是默认情况下没有在宽带连接上启用压缩的主要原因。

首先必须在全局配置模式下使用 **compression** 命令全局性地打开压缩，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** 命令设置压缩。

全局性地更改压缩

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：要从配置中删除此命令，请使用此命令的 **no** 形式：

在以下示例中，对所有 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：

[**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）。

要从配置中删除 **anyconnect ssl compression** 命令，并使该值从全局设置中得到继承，请使用此命令的 **no** 形式：

在以下示例中，对组策略 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

您可以在组策略 webvpn 或用户名 webvpn 配置模式下，使用 **anyconnect mtu** 命令调整客户端建立的 SSL VPN 连接的 MTU 大小（从 576 至 1406 个字节）：

[**no**] **anyconnect mtu** *size*

该命令仅影响 Secure Client。旧版思科 SSL VPN 客户端 () 不能调整为不同的 MTU 大小。同时，该命令还影响在 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。

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。

例如，运行 ISE 安全状态 AnyConnect 模块时，您可能会收到一条消息，内容为“从安全网关发送的 MTU 配置太小”。如果输入 **anyconnect mtu 1200** 和 **anyconnect ssl df-bit-ignore disable**，则可以避免这些系统扫描错误。

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 Secure Client 映像

您可以使用以下程序随时更新 ASA 上的客户端映像。

注释 为了实现 VPN 基础设施的最佳安全性、性能和可管理性，我们建议您定期从防火墙中删除过时的 Secure Client 映像，仅保留最新的所需版本，以防止配置冲突。

过程

步骤 1 在特权 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，请重新输入配置中的 **anyconnect image** 命令。如果新文件名不同，请使用 [**no**]**anyconnect image**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 为其使用 SSL 和 IKEv2/IPsec 协议的外部接口添加了 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。

过程

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
```

注释

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 Secure Client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
```

注释
您还必须在此处配置 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
```

SAML 2.0

ASA 支持 SAML 2.0，因此当 VPN 最终用户在专用网络外部 SAAS 应用之间切换时，只能输入一次凭证。

例如，某企业客户已启用 PingIdentity 作为其 SAML 身份提供程序 (IdP) 并且具有已启用了 SAML 2.0 SSO 的 Rally、Salesforce、Oracle OEM、Microsoft ADFS、onelogin 或 Dropbox 账户。当您将 ASA 配置为支持 SAML 2.0 SSO 作为服务提供程序 (SP) 时，最终用户能够登录一次，并有权访问所有这些服务。

此外，还增加了 AnyConnect SAML 支持，因此 AnyConnect 4.4 客户端可以使用 SAML 2.0 访问基于 SAAS 的应用。AnyConnect 4.6 引入了一个增强版的与嵌入浏览器的 SAML 集成，以替换以前版本中的本机（外部）浏览器集成。具有嵌入式浏览器的全新增强版本要求升级到 AnyConnect 4.6（或更高版本）和 ASA 9.7.1.24（或更高版本）、9.8.2.28（或更高版本）或 9.9.2.1（或更高版本）。

ASA 版本 9.17.1/ASDM 版本 7.17.1 引入了对 AnyConnect 4.10.04065（或更高版本）的 AnyConnect VPN SAML 外部浏览器的支持。当您使用 SAML 作为 AnyConnect VPN 连接配置文件的主身份验证方法时，您可以选择在执行 Web 身份验证让 Secure Client 使用本地浏览器而不是 Secure Client 嵌入式浏览器。借助此功能，Secure Client 可支持 WebAuthN 和任何其他基于 SAML 的 Web 身份验证选项，例如单点登录、生物识别身份验证或嵌入式浏览器不可用的其他增强方法。对于 SAML 外部浏览器，您必须执行此处所述的配置：为 SAML 身份验证配置默认操作系统浏览器，第 254 页。

当 SAML 配置为隧道组、默认隧道组或任何其他项目的身份验证方法时，ASA 将启用 SP 。VPN 用户通过访问启用的 ASA 或 SAML IdP 来启动单点登录。下文介绍了上述每种场景。

SAML SP 发起的 SSO

当最终用户通过访问 ASA 来发起登录时，登录行为的过程如下所示：

1. 当 VPN 用户访问或选择已启用 SAML 的隧道组时，最终用户会被重定向至 SAML IdP 进行身份验证。用户将收到提示，除非用户直接访问组 URL，在那种情况下重定向无提示。

   ASA 将生成一个 SAML 身份验证请求，由浏览器将该请求重定向至 SAML IdP。

2. IdP 向最终用户质询凭证，然后最终用户登录。输入的凭证必须满足 IdP 身份验证配置的要求。

3. IdP 响应被发送回浏览器并发布到 ASA 登录 URL。ASA 验证响应以完成登录。

SAML IdP 发起的 SSL

当用户通过访问 IdP 来发起登录时，登录行为的过程如下所示：

1. 最终用户访问 IdP。IdP 根据 IdP 的身份验证配置向最终用户质询凭证。最终用户提交凭证和登录 IdP。
2. 一般情况下，最终用户会获得 IdP 已配置的启用 SAML 的服务列表。最终用户选择 ASA。
3. SAML 响应被发送回浏览器并发布到 ASA 登录 URL。ASA 验证响应以完成登录。

信任圈

ASA 与 SAML 身份提供程序之间的信任关系通过配置的证书建立（ASA 信任点）。

最终用户与 SAML 身份提供程序之间的信任关系通过 IdP 上配置的身份验证建立。

SAML 超时

SAML 断言中有如下 NotBefore 和 NotOnOrAfter：<saml:Conditions NotBefore="2015-03-10T19:47:41Z" NotOnOrAfter="2015-03-10T20:47:41Z">

如果 NotBefore 与 ASA 上配置的 SAML 超时之和早于 NotOnOrAfter，则 SAML 超时将覆盖 NotOnOrAfter。如果 NotBefore + 超时晚于 NotOnOrAfter，则 NotOnOrAfter 将生效。

超时应该非常短，以防超时后重新使用断言。为了使用 SAML 功能，必须使您的 ASA 网络时间协议 (NTP) 服务器与 IdP NTP 服务器同步。

专用网络中的支持

在专用网络中支持基于 SAML 2.0 的服务提供商 IdP。在私有云中部署 SAML IdP 时，ASA 和其他启用 SAML 的服务处于对等位置，并且都在专用网络中。使用 ASA 作为用户与服务之间的网关，可利用受限的匿名 webvpn 会话来处理 IdP 上的身份验证，并转换 IdP 与用户之间的所有流量。当用户登录时，ASA 会使用相应的属性修改会话并存储 IdP 会话。然后，您可以使用专用网络中的服务提供程序而无需再次输入凭证。

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

注释 您不能在专用网络和公共网络之间交换身份验证信息。如果将相同的 IdP 同时用于内部和外部服务提供程序，必须分别进行身份验证。仅内部 IdP 无法用于外部服务：仅外部 IdP 无法用于专用网络中的服务提供程序。

SAML 2.0 的准则和限制

- ASA 支持以下 SAML 身份验证签名：
  - 包含 RSA 和 HMAC 的 SHA1
  - 包含 RSA 和 HMAC 的 SHA2

- ASA 支持 SAML 2.0 重定向-POST 绑定，所有 SAML IdP 也支持此功能。
- ASA 仅用作 SAML SP。在网关模式或对等模式下，它不能用作身份提供程序。
- 此 SAML SSO SP 功能是互斥的身份验证方法。它不能与 AAA 和证书一起使用。
- 不支持基于用户名/密码身份验证、证书身份验证和 KCD 的功能。例如，用户名/密码预填充功能、基于表单的自动登录、基于宏替换的自动登录、KCD SSO 等。
- ASA 支持使用 AnyConnect SAML 身份验证的 VPN 负载均衡。
- 使用 Safari 进行 SAML 身份验证时，请确保您安装了 Safari 更新 14.1.2 或更高版本。
- ASA 管理员需要确保 ASA 与 SAML IdP 之间的时钟同步，从而正确处理身份验证断言并确保正确的超时行为。
- ASA 管理员有责任在 ASA 和 IdP 上维护有效的签名证书，并考虑以下因素：
  - 在 ASA 上配置 IdP 时，必须配置 IdP 签名证书。
  - ASA 不会对从 IdP 接收的签名证书执行吊销检查。
- SAML 断言中有 NotBefore 和 NotOnOrAfter 条件。ASA SAML 配置的**超时**与这两个条件如下交互：
  - 如果 NotBefore 与超时之和早于 NotOnOrAfter，则超时将覆盖 NotOnOrAfter。
  - 如果 NotBefore + 超时晚于 NotOnOrAfter，则 NotOnOrAfter 生效。
  - 如果不存在 NotBefore 属性，ASA 将拒绝登录请求。如果不存在 NotOnOrAfter 属性且未设置 SAML 超时，ASA 将拒绝登录请求。
- ASA 不适用于使用内部 SAML 的部署中的 Duo，由于在双因素身份验证（推送、代码、密码）的质询/响应期间发生 FQDN 更改，这会强制到客户端代理的 ASA 进行身份验证。
- 在嵌入式浏览器中不允许不受信任的服务器证书。
- CLI 或 SBL 型号中不支持嵌入式浏览器 SAML 集成。
- 在网络浏览器中建立的 SAML 身份验证不会与 AnyConnect 共享，反之亦然。
- 根据具体配置，在使用嵌入式浏览器连接到前端时，会使用各种不同的方法。例如，尽管 AnyConnect 相比于 IPv6 连接更喜欢 IPv4 连接，但嵌入式浏览器可能更喜欢 IPv6，或反之亦然。同样，在尝试代理和收到失败后，AnyConnect 可能会回退到没有代理状态，而嵌入式浏览器在尝试代理并收到失败后可能会停止导航。
- 为了使用 SAML 功能，必须使您的 ASA 网络时间协议 (NTP) 服务器与 IdP NTP 服务器同步。
- ASDM 上的 VPN 向导目前不支持 SAML 配置。
- 使用内部 IdP 登录后，您将无法访问包含 SSO 的内部服务器。
- SAML IdP NameID 属性确定用户的用户名，并且用于授权、记帐和 VPN 会话数据库。
- 多情景模式不支持 SAML。

- 不支持通过 SAML 断言接收多个属性。
- Chromebook 不支持使用外部浏览器身份验证的安全客户端 SAML。
- 确保 IdP 在 SAML 响应中包含相应 SAML 请求中接收的中继状态参数。

配置 SAML 2.0 身份提供程序 (IdP)

开始之前

获取 SAML (IdP) 提供程序的登录和注销 URL。您可以从提供商的网站获取这些 URL，或者，他们可能会在元数据文件中提供该信息。

过程

步骤 1 在 webvpn 配置模式下创建 SAML 身份提供程序并进入 webvpn 下的 saml-idp 子模式。

[**no**] **saml idp** *idp-entityID*

idp-entityID - SAML IdP 实体 ID 必须包含 4 到 128 个字符。

要删除 SAML IdP，请使用此命令的 **no** 形式。

步骤 2 配置 IdP URL。

url [**sign-in** | **sign-out**] *value*

value - 这是用于登录 IdP 的 URL 或注销 IdP 时用于重定向的 URL。**sign-in** URL 为必填项，**sign-out** URL 可选。URL 值必须包含 4 到 500 个字符。

步骤 3 （可选）为 VPN 身份验证配置 SAML 服务提供商的基本 URL。此 URL 在 SAML 元数据中使用（会提供给第三方 IdP），以便 IdP 可以将终端用户重定向回 ASA。

base-url *URL*

向第三方 IdP 提供此 URL，用于将最终用户重定向回 ASA。

如果配置了 base-url，则将其用作 **show saml metadata** 中 AssertionConsumerService 和 SingleLogoutService 属性的基本 URL。

如果未配置 base-url，则由 ASA 的 hostname 和 domain-name 决定 URL。例如，当主机名为 `ssl-vpn` 且域名为 `cisco.com` 时，我们使用 `https://ssl-vpn.cisco.com`。

如果输入 **show saml metadata** 时既未配置 base-url 也未配置 hostname/domain-name，则会出现错误。

步骤 4 配置 IdP 与 SP (ASA) 之间的信任点。

trustpoint [**idp** | **sp**] *trustpoint-name*

idp- 指定包含供 ASA 用于验证 SAML 断言的 IdP 证书的信任点。

sp - 指定包含供 IdP 用于验证 ASA 签名或加密 SAML 断言的 ASA (SP) 证书的信任点。

trustpoint-name - 必须是以前配置的信任点。

步骤 5 （可选） 配置 SAML 超时。

timeout assertion *timeout-in-seconds*

如果指定，则在NotBefore和超时秒数之和早于NotOnOrAfter的情况下，此配置会覆盖NotOnOrAfter。

如果不指定，则断言中的 NotBefore 和 NotOnOrAfter 用于确定有效性。

注释
对于配置了现有 SAML IdP 的隧道组，在 webvpn 下对 saml idp CLI 的任何更改仅在对该特定隧道组重新启用SAML时才会应用于该隧道组。配置了超时后，只有在隧道组webvpn属性中重新发出saml identity-provider CLI 后，更新后的超时才会生效。

步骤 6 （可选） 在 SAML 请求中启用或禁用（默认设置）签名。

signature <value>

注释
升级到 SSO 2.5.1 后，默认签名方法从 SHA1 更改为 SHA256，而且通过输入 *value* rsa-sha1、rsa-sha256、rsa-sha384 或 rsa-sha512，还可以配置首选签名方法。

步骤 7 （可选）要设置确定 IdP　是内部网络的标志，请使用 **internal** 命令。然后，ASA 将在网关模式下工作。

步骤 8 使用 **show webvpn saml idp** 查看配置。

步骤 9 使用 **force re-authentication** 使身份提供程序在收到 SAML 身份验证请求时直接进行身份验证而不依赖于以前的安全情景。此设置为默认值；因此，要将其禁用，请使用 **no force re-authentication**。

示例

以下示例配置名为 salesforce_idp 的 IdP 并使用预配置的信任点：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)#saml idp salesforce_idp

ciscoasa(config-webvpn-saml-idp)#url sign-in
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
ciscoasa(config-webvpn-saml-idp)#url sign-out
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect

ciscoasa(config-webvpn-saml-idp)#trustpoint idp salesforce_trustpoint
ciscoasa(config-webvpn-saml-idp)#trustpoint sp asa_trustpoint

ciscoasa(config)#show webvpn saml idp
saml idp salesforce_idp
url sign-in https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
url sign-out https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
trustpoint idp salesforce_trustpoint
trustpoint  sp asa_trustpoint
```

以下网页显示了如何获取 Onelogin 的 URL 的示例

https://onelogin.zendesk.com/hc/en-us/articles/202767260-Configuring-SAML-for-Clarizen

以下网页是如何使用元数据从 OneLogin 查找 URL 的示例。

http://onlinehelp.tableau.com/current/online/en-us/saml_config_onelogin.htm

下一步做什么

如将 ASA 配置为 SAML 2.0 服务提供程序 (SP)，第 254 页中所述，将 SAML 身份验证应用于连接配置文件。

将 ASA 配置为 SAML 2.0 服务提供程序 (SP)

开始之前

IdP 必须事先已配置。请参阅配置 SAML 2.0 身份提供程序 (IdP)，第 252 页。

过程

步骤 1 在 tunnel-group webvpn 子模式下，使用 saml identity-provider 命令分配 IdP。

saml identity-provider *idp-entityID*

idp-entityID - 必须是以前配置的现有 IdP 之一。

要禁用 SAML SP，请使用此命令的 **no** 形式。

步骤 2 启用 SAML 身份验证方法。

authentication saml

示例

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

为 SAML 身份验证配置默认操作系统浏览器

指定 AnyConnect 应使用平台的本地浏览器（操作系统的默认浏览器），还是使用 AnyConnect 中嵌入的浏览器处理 SSO 身份验证过程。

您必须下载 AnyConnect 外部浏览器软件包（例如，*external-sso-4.10.04065-webdeploy-k9.pkg*）并将其上传到 ASA。然后，您可以选择 SAML 登录方法（AnyConnect 的嵌入式浏览器或操作系统的默认浏览器）进行 SAML 身份验证。此捆绑包是一个脚本，允许 VPN 客户端启动默认操作系统 Web

浏览器进行身份验证，与操作系统、浏览器和 VPN 客户端版本无关。只要启用该功能，VPN 客户端版本和外部浏览器软件包版本文件就不需要匹配。

选择默认操作系统浏览器可在您的 VPN 身份验证和其他企业登录之间启用单点登录 (SSO)。如果您想要支持无法在 VPN 客户端的嵌入式浏览器中执行的 Web 身份验证方法（例如生物特征身份验证），则可选择此选项。在选择操作系统的浏览器之前，您必须上传可在浏览器中运行的软件包，以启用 Web 身份验证。

过程

步骤 1 在 webvpn 子模式下，使用 anyconnect external-browser-pkg 命令通过操作系统的默认浏览器启用 AnyConnect SAML 身份验证。

anyconnect external-browser-pkg *path*

要禁用操作系统的默认浏览器进行 SAML 身份验证，请使用此命令的 **no** 形式。

步骤 2 在 tunnel-group webvpn 子模式下，使用 external-browser 命令通过操作系统的默认浏览器启用 AnyConnect SAML 身份验证。

external-browser enable *idp-entityID*

要禁用操作系统的默认浏览器进行 SAML 身份验证，请使用此命令的 **no** 形式。

示例

此示例选择 AnyConnect 外部浏览器软件包的路径，并为 SAML 身份验证启用外部浏览器（操作系统的默认浏览器）。

```
asa(config-webvpn)# anyconnect external-browser-pkg flashshow :
asa(config)# tunnel-group SAML webvpn-attributes
asa(config-tunnel-webvpn)# external-browser enable
asa(config-tunnel-webvpn)#
```

配置证书和 SAML 身份验证

您可以为基于 SAML 的连接配置文件配置证书和 SAML 身份验证，以便验证客户拥有的资产而无需分析特定文件/注册表密钥。基于 SAML 的身份验证可以绑定到已批准的资产和/或用户。您可以将单个证书或多个证书与 SAML 配合用于身份验证。

当 Secure Client 发起连接时，ASA 或 FTD 将在执行 SAML 身份验证之前从终端请求并验证一个或多个证书。

SAML 身份验证完成后，SAML 和证书用户名可以

SAML 身份验证完成后，可以在进入授权阶段之前比较 SAML 和证书用户名。

开始之前

确保在配置证书和 SAML 身份验证之前配置所需的 SAML 设置：

- 获取 SAML (IdP) 提供程序的登录和注销 URL。您可以从提供商的网站获取这些 URL，或者，他们可能会在元数据文件中提供该信息。
- 配置 SAML 身份提供程序和信任点设置。请参阅 配置证书和 SAML 身份验证，第 255 页

过程

步骤 1 要配置证书和 SAML 身份验证，请输入以下命令进入 tunnel-group webvpn-attributes 模式。提示符会更改以表示模式发生更改：

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

步骤 2 要指定想使用的身份验证方法，请输入以下命令：

```
hostname(config-tunnel-webvpn)#authentication authentication_method
```

例如，以下命令同时允许 SAML 和证书身份验证：

```
hostname(config-tunnel-webvpn)#authentication saml certificate
```

以下命令允许证书和 SAML 身份验证：

```
hostname(config-tunnel-webvpn)#authentication certificate saml
```

以下命令同时允许多证书和 SAML 身份验证：

```
hostname(config-tunnel-webvpn)#authentication multiple-certificate saml
```

步骤 3 添加或编辑连接配置文件，然后选择**基本 (Basic)** 连接配置文件属性设置。

步骤 4 要指定证书和 SAML 身份验证的身份验证方法，请从下拉列表中选择 SAML 和证书或多个证书和 SAML。

示例

以下是为 sales_group 连接配置文件配置多个证书和 SAML 身份验证的示例：

```
ciscoasa(config)# tunnel-group sales_group webvpn
ciscoasa(config-tunnel-webvpn)#authentication multiple-certificate saml
```

以 SAML 2.0 和 Onelogin 为例说明

按照此示例，使用您的第三方 SAML 2.0 IdP 代替 Onelogin 信息和命名。

1. 设置 IdP 与 ASA (SP) 之间的时间同步。

```
ciscoasa(config)# ntp server 209.244.0.4
```

2. 按照您的第三方 IdP 提供的程序从 IdP 获取 IdP SAML 元数据。

3. 将 IdP 的签名证书导入信任点。

```
ciscoasa(config)# crypto ca trustpoint onelogin
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# no ca-check
ciscoasa(config-ca-trustpoint)# crypto ca authenticate onelogin
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
quit
INFO: Certificate has the following attributes:
Fingerprint:     85de3781 07388f5b d92d9d14 1e22a549
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

4. 将 SP (ASA) 签名 PKCS12 导入信任点

```
ciscoasa(config)# crypto ca import asa_saml_sp pkcs12 password
Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
quit
INFO: Import PKCS12 operation completed successfully
```

5. 添加 SAML IdP：

```
ciscoasa(config-webvpn)# saml idp https://app.onelogin.com/saml/metadata/462950
```

6. 在 saml-idp 子模式下配置属性：

   配置 IdP 登录 URL 和注销 URL:

```
ciscoasa(config-webvpn-saml-idp)# url sign-in
https://ross.onelogin.com/trust/saml2/http-post/sso/462950
ciscoasa(config-webvpn-saml-idp)# url sign-out
https://ross.onelogin.com/trust/saml2/http-redirect/slo/462950
```

   配置 IdP 信任点和 SP 信任点

```
ciscoasa(config-webvpn-saml-idp)# trustpoint idp onelogin
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_saml_sp
```

   配置无客户端 VPN 基本 URL、SAML 请求签名和 SAML 断言超时：

```
ciscoasa(config-webvpn-saml-idp)# base-url https://172.23.34.222
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 7200
```

7. 为隧道组配置 IdP 并启用 SAML 身份验证。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

8. 显示 ASA 的 SAML SP 元数据：

您可以从 `https://172.23.34.222/saml/sp/metadata/cloud_idp_onelogin` 获取 ASA 的 SAML SP 元数据。在 URL 中，`cloud_idp_onelogin` 是隧道组名称。

9. 按照您的第三方 IdP 提供的程序在您的第三方 IdP 上配置 SAML SP。

排除 SAML 2.0 故障

使用 **debug webvpn saml***value* 调试 SAML 2.0 行为。根据 *value*，系统将显示以下 SAML 消息：

- 8 - 错误
- 16 - 警告和错误
- 128 或 255 - 调试、警告和错误

监控 Secure Client 连接

如要查看有关活动会话的信息，请使用 **show vpn-sessiondb** 命令：

命令	目的
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 AES-GCM-256、AES-GMAC-128 等）的百分比。

注释 **AnyConnect 父隧道**

AnyConnect 父隧道没有分配的 IP 地址。

这是在协商期间创建的主会话，用于设置因网络连接问题或休眠而需要重新连接的会话令牌。根据连接机制，Cisco Adaptive Security Appliance (ASA) 将会话列为无客户端（通过门户的 WebLaunch）或父项（独立 AnyConnect）。

AnyConnect 父项表示客户端未主动连接时的会话。实际上，它的工作原理类似于 Cookie，因为它是 ASA 上映射到来自特定客户端的连接的数据库条目。如果客户端休眠/休眠，则隧道（IPsec/互联网密钥交换 (IKE)/传输层安全 (TLS)/数据报传输层安全 (DTLS) 协议）将被删除，但父项会保留，直到空闲计时器或最大连接数时间生效。这允许用户重新连接而无需重新进行身份验证。

示例

Inactivity 字段显示自 Secure Client 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：

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-sessiondb logoff name *name*
vpn-sessiondb 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），这样就不会达到许可证容量，而让新用户可以登录。如果该会话稍后恢复，则会从非活动列表中删除。

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#
```

Secure Client 连接的功能历史记录

下表列出了此功能的版本历史记录。

表 *14: Secure Client* 连接的功能历史记录

功能名称	版本	功能信息
Secure Client 连接	7.2(1)	引入或修改了以下命令：authentication eap-proxy、authentication ms-c 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 Secure Client 和 LAN 间 的 IPsec IKEv

第 10 章

Secure Client HostScan

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

HostScan/Cisco Secure Firewall Posture 的前提条件

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

- ASA 8.4
- ASDM 6.4

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

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

HostScan 的许可

以下是 HostScan 的 Secure Client 许可要求：

- AnyConnect Apex
- AnyConnect 仅 VPN

HostScan 程序包

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

安装或升级 HostScan/Cisco Secure Firewall Posture

使用 ASA 的命令行界面，按照以下程序安装或升级 HostScan 或 Cisco Secure Firewall Posture 程序包并启用 HostScan。

开始之前

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

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

- 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 secure-firewall-posture-*version*-k9.pkg 上传到 ASA。如果您使用的是 HostScan 4.x 版本，则应上传 hostscan_*version*-k9.pkg 文件。

过程

步骤 1 进入 webvpn 配置模式。

示例：

```
hostname(config)# webvpn
```

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

步骤 3 指定要指定为 HostScan/Cisco Secure Firewall Posture 映像的程序包的路径。您可以指定独立软件包或 Secure Client 软件包。

hostscan image *path*

示例：

如果您使用的是 HostScan 4.x 版本，

```
ASAName(webvpn)#hostscan image disk0:/hostscan_4.10.06081.pkg
```

如果您使用的是 Cisco Secure Firewall Posture 5.x 版本，

```
ASAName(webvpn)#hostscan image disk0:/secure-firewall-posture5.0.00556.pkg
```

步骤 4 启用在上一步中指定的 HostScan/Cisco Secure Firewall Posture 映像。

示例：

```
ASAName(webvpn)#hostscan enable
```

步骤 5 将运行配置保存到闪存中。成功地将新配置保存到闪存中后，您将收到消息 [OK]。

示例：

```
hostname(webvpn)# write memory
```

步骤 6

启用或禁用 HostScan

这些命令使用 ASA 的命令行界面启用或禁用已安装的 HostScan 映像。

开始之前

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

过程

步骤 1 进入 webvpn 配置模式。

示例：

webvpn

步骤 2 启用独立的 HostScan 映像（如果尚未将其从 ASA 中卸载）。

hostscan enable

步骤 3 为所有已安装的 HostScan 程序包禁用 HostScan。

注释
卸载已启用的 HostScan 映像之前，必须先使用以下命令禁用 HostScan。

no hostscan enable

查看 ASA 上启用的 HostScan/Cisco Secure Firewall Posture 版本

使用 ASA 的命令行界面，按照以下程序确定已启用的 HostScan/Cisco Secure Firewall Posture 版本。

开始之前

登录 ASA 并进入特权 EXEC 模式。在特权 EXEC 模式下，ASA 将显示以下提示符：hostname#

过程

显示 ASA 上启用的 HostScan/Cisco Secure Firewall Posture 版本

show webvpn hostscan

卸载 HostScan/Cisco Secure Firewall Posture

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

开始之前

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

过程

步骤 1 进入 webvpn 配置模式。

webvpn

步骤 2 禁用要卸载的 HostScan/Cisco Secure Firewall Posture 映像。

no hostscanenable

步骤 3 指定要卸载的 HostScan/Cisco Secure Firewall Posture 映像的路径。可能已有一个独立程序包被指定为 HostScan/Cisco Secure Firewall Posture 程序包。

no hostscan image *path*

示例：

如果您使用的是 HostScan 4.x 版本，

```
ASAName(webvpn)#hostscan image disk0:/hostscan_4.10.06081-k9.pkg
```

如果您使用的是 Cisco Secure Firewall Posture 5.x 版本，

```
ASAName(webvpn)#hostscan image disk0:/secure-firewall-posture-5.0.00556-k9.pkg
```

步骤 4 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]。

write memory

将 Secure Client 功能模块分配到组策略

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

开始之前

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

过程

步骤 1 为网络客户端访问添加内部组策略

group-policy *name* **internal**

示例：

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

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

group-policy *name* **attributes**

示例：

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

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

webvpn

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

anyconnect modules value *Cisco Secure Firewall* 模块 *Name*

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

值	Cisco Secure Firewall 模块/功能名称
dart	安全客户端 DART（诊断和报告工具）
vpngina	安全客户端 SBL（登录前开始）
posture	Cisco Secure Firewall Posture/HostScan
nam	安全客户端 网络访问管理器
none	单独使用可从组策略中删除所有 AnyConnect 模块。
profileMgmt	安全客户端 管理隧道 VPN

示例：

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

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

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

步骤 5 将运行配置保存到闪存中。

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

write memory

HostScan/Cisco Secure Firewall Posture 相关文档

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

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

第 11 章

Virtual Tunnel Interface

本章介绍如何配置 VTI 隧道。

关于 Virtual Tunnel Interface

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

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

静态 VTI

您可以使用静态 VTI 配置进行站点间连接，其中两个站点之间的隧道会始终在线。对于静态 VTI 接口，您必须将物理接口定义为隧道源。每个设备最多可以关联 1024 个 VTI。要创建静态 VTI 接口，请参阅添加 VTI 接口，第 274 页。

动态 VTI

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

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

择器。动态 VTI 也支持动态 (DHCP) 分支。要创建动态 VTI 接口，请参阅添加动态 VTI 接口，第 277 页。

ASA 如何为 VPN 会话创建动态 VTI 隧道

1. 在 ASA 上创建虚拟模板 (**interface virtual-Template** *template_number* **type tunnel**)。

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

Virtual Tunnel Interface 准则

情景模式和集群

- 仅支持单一模式。
- 不支持集群。

防火墙模式

仅在路由模式中受支持。

BGP IPv4 和 IPv6 支持

支持 VTI 上的 IPv4 和 IPv6 BGP 路由。

EIGRP 支持

支持 VTI 上的 IPv4 和 IPv6 EIGRP 路由。

OSPF IPv4 和 IPv6 支持

支持 VTI 上的 IPv4 和 IPv6 OSPF 路由。

IPv6 支持

- 可以配置 IPv6 寻址的 VTI。

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

常规配置准则

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

  我们的建议操作如下动作之一：
  - 将 LAN 间 VPN 迁移到动态 VTI。
  - 使用静态加密映射及其自己的隧道组。
- VTI 只有在 IPsec 模式下才可配置。不支持在 ASA 上终止 GRE 隧道。
- 您可以将静态、BGP、OSPF 或 EIGRP IPv4 路由用于使用这种隧道接口的流量。
- 对于静态和动态 VTI，请确保不将借用 IP 接口用作任何 VTI 接口的隧道源 IP 地址。
- VTI 的 MTU 将根据底层物理接口自动设置。但是，如果在启用 VTI 后更改物理接口 MTU，则您必须禁用并重新启用 VTI 才能使用新的 MTU 设置。
- 对于动态 VTI，虚拟接入接口会从配置的隧道源接口继承 MTU。如果不指定隧道源接口，虚拟接入接口将从源接口继承 MTU，而 ASA 会从该接口接受 VPN 会话请求。
- 您最多可以在一台设备上配置 1024 个 VTI。在计算 VTI 计数时，请考虑以下事项：
  - 包括 nameif 子接口，以便得出可在设备上配置的 VTI 总数。
  - 您不能在端口通道的成员接口上配置 nameif。因此，隧道计数只会随实际主端口通道接口的数量减少，而不会随其任何成员接口的数量减少。
  - 即使平台支持超过 1024 个接口，VTI 计数也限于该平台上可配置的 VLAN 数量。例如，如果型号支持 5510 VLAN，则隧道计数为 500 减去配置的物理接口数。

- 对于动态 VTI，动态创建的虚拟接入接口的最大数量可以是 1024 或平台的总接口限制，以较小者为准。
- VTI 支持 IKE 版本 v1 和 v2，并使用 IPsec 在隧道的源地址与目的地址之间收发数据。
- 如果必须应用 NAT，则将 IKE 和 ESP 数据包封装在 UDP 报头中。
- 无论隧道中的数据流量如何，IKE 和 IPsec 安全关联都将不断重新生成密钥。这可确保 VTI 隧道始终处于活动状态。
- 隧道组名称必须与对等体作为其 IKEv1 或 IKEv2 身份发送的内容相符。
- 对于站点间隧道组中的 IKEv1，仅当隧道身份验证方法为数字证书和/或对等体配置为使用积极模式时，才能使用非 IP 地址的名称。
- 只要加密映射中配置的对等体地址与 VTI 的隧道目的地址不同，VTI 和加密映射配置就可以在同一个物理接口上共存。
- 可以在 VTI 接口上应用访问规则来控制通过 VTI 的流量。
- VTI 接口之间支持 ICMP ping。
- 如果 IKEv2 站点间 VPN 隧道的对等设备发送 IKEv2 配置请求负载，则 ASA 无法与该设备建立 IKEv2 隧道。您必须在对等设备上禁用 config-exchange 请求，ASA 才能与对等设备建立 VPN 隧道。
- 动态 VTI 支持 HA 和 IKEv2。

默认设置

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

VTI 的限制

ASA 会在 VTI 解密后丢弃安全组标签 (SGT) 帧和数据包。

动态 VTI 不支持：

- ECMP 和 VRF
- 集群
- IKEv1
- QoS

对于动态 VTI，如果未指定隧道源，IKEv2 将在设备的所有接口上启用，管理专用接口和故障转移接口除外。

创建 VTI 隧道

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

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

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

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

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

hostname(config)# sysopt connection permit-vpn

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

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

有关详细信息，请参阅允许接口内流量 (Hairpinning)，第 66 页。

过程

步骤 1 添加 IPsec 提议（转换集）。

步骤 2 添加 IPsec 配置文件。

步骤 3 添加 VTI 隧道。

添加 IPsec 提议（转换集）

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

开始之前

- 可以使用预共享密钥或证书对与 VTI 关联的 IKE 会话进行身份验证。IKEv2 允许使用不对称身份验证方法和密钥。对于 IKEv1 和 IKEv2，必须在用于 VTI 的隧道组下配置预共享密钥。

- 对于使用 IKEv1 的基于证书的身份验证，必须指定要在发起方使用的信任点。对于响应方，必须在 tunnel-group 命令中配置信任点。对于 IKEv2，必须同时在发起方和响应方的 tunnel-group 命令下配置用于身份验证的信任点。

过程

添加 IKEv1 转换集或 IKEv2 IPsec 提议以建立安全关联。

要添加 IKEv1 转换集，请使用以下命令：

crypto ipsec ikev1 transform-set {*transform-set-name* | *encryption* | *authentication*}

示例：

```
ciscoasa(config)#crypto ipsec ikev1 transform-set SET1 esp-aes esp-sha-hmac
```

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-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 作为散列算法。
- esp-sha-hmac — 使用 SHA/HMAC-160 作为散列算法。
- esp-none — 不进行 HMAC 身份验证。

添加 IKEv2 IPsec 提议。

注释
对于 IOS 平台，请在 IKEv2 配置文件配置模式下使用 **no config-exchange request** 命令来禁用配置交换选项。有关详细信息，请参阅http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c2.html#wp3456426280。

- 指定 IPsec 提议名称：

  crypto ipsec ikev2 ipsec-proposal *IPsec proposal name*

示例：

```
ciscoasa(config)#crypto ipsec ikev2 ipsec-proposal SET1
```

- 在 crypto IPsec ikev2 ipsec-proposal 配置模式下指定安全参数：

  protocol esp {encryption {aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | null} | integrity {sha-1 | sha-256 | sha-384 | sha-512 | null}

示例：

```
ciscoasa(config-ipsec-proposal)#protocol esp encryption aes aes-192
```

添加 IPsec 配置文件

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

过程

步骤 1 设置配置文件名称：

crypto ipsec profile *name*

示例：

```
ciscoasa(config)#crypto ipsec profile PROFILE1
```

步骤 2 设置 IKEv1 或 IKEv2 提议。可以选择 IKEv1 转换集或 IKEv2 IPsec 提议。

a) 设置 IKEv1 转换集。

- 要设置 IKEv1 提议，请在 crypto ipsec profile 命令子模式下输入以下命令：

  set ikev1 transform set *set_name*

  在本示例中，SET1 是先前创建的 IKEv1 提议集。

  ```
  ciscoasa(config-ipsec-profile)#set ikev1 transform-set SET1
  ```

b) 设置 IKEv2 提议。

- 要设置 IKEv2 提议，请在 crypto ipsec profile 命令子模式下输入以下命令：

  set ikev2 ipsec-proposal *IPsec_proposal_name*

  在本示例中，SET1 是先前创建的 IKEv2 IPsec 提议。

  ```
  ciscoasa(config-ipsec-profile)#set ikev2 ipsec-proposal SET1
  ```

步骤 3 （可选）指定安全关联的持续时间：

set security-association lifetime { **seconds** *number* | **kilobytes** {*number* | **unlimited**}}

示例：

```
ciscoasa(config-ipsec-profile)#set security-association lifetime
seconds 120 kilobytes 10000
```

步骤 4 （可选）将 VTI 隧道端部配置为仅用作响应方：

responder-only

- 可以将 VTI 隧道的一端配置为仅用作响应方。仅响应方端不会发起隧道或重新生成密钥。

- 如果使用的是IKEv2，请设置安全关联生命周期的持续时间，此值应大于发起方端的IPsec配置文件中的生命周期值。这是为了方便发起方端成功地重新生成密钥，并确保隧道保持活动状态。
- 如果使用的是IKEv1，IOS应始终处于仅响应方模式，这是因为IOS不支持连续通道模式。ASA将成为会话发起方并重新生成密钥。
- 如果发起方端的重新生成密钥配置未知，请删除仅响应方模式以便双向建立SA，或在仅响应方端配置无限 IPsec 生命周期值以防止到期。

步骤 5 （可选）指定 PFS 组。完美前向保密 (PFS) 为每个加密交换生成唯一会话密钥。此唯一会话密钥可保护交换免于后续解密。要配置 PFS，必须选择在生成 PFS 会话密钥时要使用的 Diffie-Hellman 密钥导出算法。该密钥导出算法将生成 IPsec 安全关联 (SA) 密钥。每组具有不同的长度模数。模数越大，安全性越高，但需要的处理时间更长。两个对等体上的 Diffie-Hellman 组必须匹配。

set pfs { **group14** }

示例：

```
ciscoasa(config-ipsec-profile)# set pfs group14
```

步骤 6 （可选）指定用于定义发起 VTI 隧道连接时要使用的证书的信任点。

set trustpoint *name*

示例：

```
ciscoasa(config-ipsec-profile)#set trustpoint TPVTI
```

步骤 7 （可选）为此 IPsec 配置文件启用反向路由注入 (RRI)，并将反向路由设置为动态。

set reverse-route [dynamic]

示例：

```
ciscoasa(config-ipsec-profile)#set reverse-route dynamic
```

添加 VTI 接口

要创建新 VTI 接口并建立 VTI 隧道，请执行以下步骤：

注释 实施IP SLA，确保当活动隧道中的路由器不可用时，隧道仍保持活动状态。请参阅《ASA常规操作配置指南》(http://www.cisco.com/go/asa-config) 中的“配置静态路由跟踪”。

过程

步骤 1 创建新的隧道接口：

interface tunnel *tunnel_interface_number*

指定 0 到 10413 范围内的隧道 ID。最多可支持 10413 个 VTI 接口。

示例：

```
ciscoasa(config)#interface tunnel 100
```

步骤 2 输入 VTI 接口的名称。

在 **interface tunnel** 命令子模式下输入以下命令：

nameif *interface name*

示例：

```
ciscoasa(config-if)#nameif vti
```

步骤 3 输入 VTI 接口的 IP 地址。

ip address *IP addressmask*

示例：

```
ciscoasa(config-if)#ip address 192.168.1.10 255.255.255.254
```

步骤 4 输入虚拟模板继承的接口的 IPv4 或 IPv6 地址。

您还可以选择物理接口或设备上配置的环回接口。从虚拟模板克隆的所有虚拟访问接口都将具有相同的 IP 地址。

ip unnumbered *interface-name*

ipv6 unnumbered *interface-name*

示例：

```
ciscoasa(config-if)#ip unnumbered loopback1
```

步骤 5 指定隧道源接口。

tunnel source interface *interface_name*

源接口可以是物理接口或环回接口。

示例：

```
ciscoasa(config-if)#tunnel source interface outside
```

步骤 6 指定隧道目标 IP 地址。

tunnel destination *ip_address*

示例：

```
ciscoasa(config-if)#tunnel destination 10.1.1.1
```

步骤 7 使用隧道模式 IPsec IPv4 配置隧道。

tunnel mode ipsec *ipv4*

示例：

```
ciscoasa(config-if)#tunnel mode ipsec ipv4
```

步骤 8 将 IPsec 配置文件分配给隧道。

tunnel protection ipsec *IPsec profile*

示例：

```
ciscoasa(config-if)#tunnel protection ipsec Profile1
```

步骤 9 为静态 VTI 接口分配一个流量选择器。

tunnel protection policy *acl_name*

访问列表可以包含单个或多个列表选择器。如果不配置此命令，静态 VTI 接口将默认建议使用任意到任意选择器。

示例：

```
ciscoasa(config)# access-list Spoke-to-Hub extended permit ip 209.165.200.225 255.255.255.224
 any
ciscoasa(config-if)# tunnel protection ipsec policy Spoke-to-Hub
```

示例

ASA 与 IOS 设备之间的 VTI 隧道（采用 IKEv2）配置示例：

```
ASA□

crypto ikev2 policy 1
 encryption aes-gcm-256
 integrity null
 □ 21
 prf sha512
 lifetime seconds 86400
!
crypto ipsec ikev2 ipsec-proposal gcm256
 protocol esp encryption aes-gcm-256
 protocol esp integrity null
!
crypto ipsec profile asa-vti
 set ikev2 ipsec-proposal gcm256
!
interface Tunnel 100
 nameif vti
 ip address 10.10.10.1 255.255.255.254
 tunnel source interface [asa-source-nameif]
 tunnel destination [router-ip-address]
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile asa-vti
!
tunnel-group [router-ip-address] ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
crypto ikev2 enable [asa-interface-name]
```

```
IOS□

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

添加动态 VTI 接口

要为动态 VTI 创建虚拟模板，请执行以下操作：

注释 实施 IP SLA，确保当活动隧道中的路由器不可用时，隧道仍保持活动状态。请参阅《ASA 常规操作配置指南》中的“配置静态路由跟踪”，地址是：http://www.cisco.com/go/asa-config。

开始之前

确保您已配置 IPsec 配置文件和 IP 未编号接口。

过程

步骤 1 创建新的虚拟模板：

interface virtual-Template *template_number* **type tunnel**

template_number 是虚拟模板的唯一编号。范围为 1 到 10413。

接口模板不得处于关闭状态。以下是虚拟模板的必填参数：

- 接口名称
- 隧道 IPsec 模式
- 隧道 IPsec 配置文件

示例：

```
ciscoasa(config)#interface virtual-Template 101 type tunnel
```

步骤 2 指定动态 VTI 虚拟模板接口的名称。

在 **interface** 配置模式下输入以下命令：

nameif *interface_name*

ASA 会动态创建虚拟访问接口为 <*Virtual_Template_name*>_va<*n*>。例如，如果虚拟模板的名称为 dVTI101，则虚拟访问接口将为 dVTI101_va1、dVTI101_va2，以此类推。如果要修改虚拟模板，必须使用 **shutdown** 命令来关闭虚拟模板。

示例：

```
ciscoasa(config-if)#nameif dVTI101
```

步骤 3 配置虚拟模板继承的接口的 IPv4 或 IPv6 地址。

ip unnumbered *interface-name*

ipv6 unnumbered *interface-name*

虚拟模板可以继承设备上配置的任何物理接口的 IP 地址或环回地址。从虚拟模板克隆的所有虚拟访问接口都将具有相同的 IP 地址。

示例：

```
ciscoasa(config-if)#ip unnumbered loopback1
```

步骤 4 （可选）指定隧道源接口。

tunnel source interface *interface_name*

源接口可以是物理接口或环回接口。

ASA 仅接受来自配置为隧道源 IP 地址的接口的 VPN 会话请求。如果没有指定该接口，ASA 将接受从任何接口接收的 VPN 会话请求。虚拟访问接口会从配置的隧道源接口继承 MTU。如果没有启用上述选项，虚拟访问接口将从源接口继承 MTU，而 ASA 会从该接口接受 VPN 会话请求。

示例：

```
ciscoasa(config-if)#tunnel source interface outside1
```

步骤 5 将隧道保护模式指定为 IPv4 或 IPv6。

tunnel mode ipsec {**ipv4** | **ipv6**}

示例：

```
ciscoasa(config-if)#tunnel mode ipsec ipv4
```

步骤 6 将 IPsec 配置文件分配给隧道。

tunnel protection ipsec profile *ipsec_profile*

此 IPsec 配置文件会配置协商交换所需的 IPSec/IKE 参数。

示例：

```
ciscoasa(config-if)#tunnel protection ipsec profile Profile1
```

步骤 7 将虚拟模板附加到隧道组。

tunnel-group *tunnel_group_name* **type** *type*

tunnel-group *tunnel_group_name* **ipsec-attributes**

virtual-template *template_number*

您可以将同一虚拟模板连接到多个隧道组。ASA 会使用虚拟模板来为每个 VPN 会话创建单独的虚拟访问接口。

示例：

```
ciscoasa(config)#tunnel-group DVTI_spoke1 type ipsec-l2l
ciscoasa(config)#tunnel-group DVTI_spoke1 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#virtual-template 101
```

步骤 8 为隧道组启用动态路由。

tunnel-group *tunnel_group_name* **ipsec-attributes**

ikev2 route accept any

ikev2 route set interface

ikev2 route accept any 命令允许 ASA 接受在 IKEv2 交换期间收到的任何隧道接口 IP 地址。 默认情况下，此选项处于已启用状态。

ikev2 route set interface 命令允许 ASA 在 IKEv2 交换期间发送隧道接口 IP 地址。 此选项可在 VTI 接口之间启用单播可访问性，以便 BGP 通过隧道运行。

使用 BGP/OSPF/EIGRP 为隧道组启用动态路由。在配置虚拟模板后，您必须配置路由策略，以便通过 VTI 隧道来路由设备之间的动态 VTI 流量。您还必须配置访问控制规则以允许已加密的流量。

示例：

```
ciscoasa(config)#tunnel-group DVTI_spoke1 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#ikev2 route set interface
ciscoasa(config-tunnel-ipsec)#ikev2 route accept any
```

Virtual Tunnel Interface 的功能历史记录

功能名称	版本	功能信息
动态 Virtual Tunnel Interface 支持	9.19(1)	您可以创建动态 VTI 并使用它在中心辐射型拓扑配置基于路由的站点间 VPN。动态 VTI 简化了大型企业中心辐射型部署的对等体配置。单个动态 VTI 可以替换中心上的多个静态 VTI 配置。您可以将新的分支添加到中心，而无需更改中心配置。 新增/修改的命令：**interface virtual-Template, ip unnumbered, ipv6 unnumbered, tunnel protection ipsec policy**
OSPF IPv4 和 IPv6 支持	9.19(1)	支持 VTI 上的 OSPF IPv4 和 IPv6 路由协议。
EIGRP 支持	9.19(1)	支持 VTI 上的 EIGRP IPv4 和 IPv6 路由协议。
静态和动态 VTI 的环回接口支持	9.19(1)	现在，您可以将环回接口设置为 VTI 的源接口。还添加了支持以从环回接口继承 IP 地址，而不是静态配置的 IP 地址。环回接口有助于克服路径故障。如果接口发生故障，您可以通过分配给环回接口的 IP 地址来访问所有接口。 新增/修改的命令：**tunnel source interface**、**ip unnumbered**、**ipv6 unnumbered**
本地隧道 ID 支持	9.17(1)	ASA 支持唯一本地隧道 ID，它允许 ASA 在 NAT 后面有多个 IPsec 隧道，以便连接到 Cisco Umbrella 安全互联网网关 (SIG)。本地身份用于为每个 IKEv2 隧道配置唯一身份，而不是为所有隧道配置一个全局身份。 新增/修改的命令： **local-identity-from-cryptomap** 、
在静态 VTI 上支持 IPv6	9.16（1）	ASA 在 Virtual Tunnel Interface (VTI) 配置中支持 IPv6 地址。 VTI 隧道源接口可以具有 IPv6 地址，您可以将其配置为用作隧道终端。如果隧道源接口有多个 IPv6 地址，您可以指定要使用的地址，否则默认使用列表中的第一个 IPv6 全局地址。 隧道模式可以是 IPv4 或 IPv6，但必须与 VTI 上配置的 IP 地址类型相同，隧道才能处于活动状态。IPv6 地址可以分配给 VTI 中的隧道源或隧道目标接口。 新增/修改的命令：**tunnel source interface**、**tunnel destination**、**tunnel mode**
支持每个设备 1024 个 VTI 接口	9.16（1）	要在设备上配置的最大VTI数量已从 100 增加到 1024。 即使平台支持超过 1024 个接口，VTI 计数也限于该平台上可配置的 VLAN 数量。例如，ASA 5510 支持 100 个VLAN，隧道计数为 100 减去配置的物理接口数。 新增/修改的命令：无
VTI 上的 DHCP 中继服务器支持	9.14(1)	ASA 允许将 VTI 接口配置为 DHCP 中继服务器连接接口。 修改了以下命令：**dhcprelay server** *ip_address vti_ifc_name*。

功能名称	版本	功能信息
VTI 中支持 IKEv2、基于证书的身份验证和 ACL	9.8.(1)	Virtual Tunnel Interface (VTI) 现在支持 BGP（静态 VTI）。现在可在独立和高可用性模式下使用 IKEv2。可以通过在 IPsec 配置文件中设置信任点来使用基于证书的身份验证。还可以使用 access-group 命令，将 VTI 上的访问列表应用于过滤进口流量。 在 IPsec 配置文件配置模式下引入了以下命令：**set trustpoint**。
Virtual Tunnel Interface (VTI) 支持	9.7.(1)	使用新的逻辑接口（称为 Virtual Tunnel Interface (VTI)）可增强 ASA，该接口用于向对等体表示 VPN 隧道。这可通过将 IPSec 配置文件连接到隧道的每一端，为基于 VPN 的路由提供支持。使用 VTI 将不再需要配置静态加密映射访问列表并将其映射到接口。 引入了以下命令：**crypto ipsec profile**、**interface tunnel**、**responder-only**、**set ikev1 transform-set**、**set pfs**、**set security-association lifetime**、**tunnel destination**、**tunnel mode ipsec**、**tunnel protection ipsec profile**、**tunnel source interface**。

第 12 章

为 VPN 配置外部 AAA 服务器

关于外部 AAA 服务器

此 ASA 可配置为使用外部 LDAP、RADIUS 或 TACACS+ 服务器来支持 ASA 的认证、授权和审计 (AAA)。外部 AAA 服务器会实施配置的权限和属性。将 ASA 配置为使用外部服务器之前，必须使用正确的 ASA 授权属性来配置外部 AAA 服务器，并从其中一部分属性向个人用户分配特定权限。

了解授权属性的策略实施

ASA 支持将用户授权属性（也称为用户授权或权限）应用到 VPN 连接的多种方法。您可以将 ASA 配置为通过以下任意组合获取用户属性：

- ASA 上的动态访问策略 (DAP)
- 外部 RADIUS 或 LDAP 身份验证和/或授权服务器
- ASA 上的组策略

如果ASA收到来自所有来源的属性，将会对这些属性进行评估、合并，并将其应用至用户策略。如果属性之间有冲突，DAP 属性优先。

ASA 按照以下顺序应用属性：

1. ASA 上的 DAP 属性 - 在 8.0(2) 版本中引入，这些属性优先于所有其他的属性。如果您在 DAP 中设置书签或 URL 列表，它会覆盖组策略中设置的书签或 URL 列表。
2. AAA 服务器上的用户属性 - 该服务器在用户身份验证和/或授权成功后返回这些属性。请不要将这些属性与 ASA 本地 AAA 数据库中为单个用户（ASDM 中的用户账户）设置的属性混淆。

3. 在 ASA 上配置的组策略 - 如果 RADIUS 服务器为用户返回 RADIUS CLASS 属性 IETF-Class-25 (OU=*group-policy*) 值， ASA 会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。

   对于 LDAP 服务器，任何属性名称都可用于设置会话的组策略。您在 ASA 上配置的 LDAP 属性映射会将该 LDAP 属性映射至思科属性 IETF-Radius-Class。

4. 连接配置文件（在 CLI 中称为隧道组）分配的组策略 - 连接配置文件具有该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。连接至 ASA 的所有用户最初都属于此组，这可以提供 DAP、服务器返回的用户属性或分配给用户的组策略中缺失的所有属性。

5. ASA 分配的默认组策略 (DfltGrpPolicy) - 系统默认属性提供 DAP、用户属性、组策略或连接配置文件中缺失的所有值。

外部 AAA 服务器使用准则

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

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

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

配置多证书身份验证

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

通过多证书选项，可以同时通过证书对计算机和用户进行证书身份验证。如果没有此选项，则只能对其中之一执行证书身份验证，但不能二者兼顾。

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

通过预填充用户名字段，可以解析第二个（用户）证书中的字段并将其用于 AAA 和证书身份验证连接中的后续 AAA 身份验证。始终从自客户端收到的第二个（用户）证书检索主用和辅助用户名预填充。

从 9.14(1) 开始，ASA 允许您在配置多证书身份验证并使用“身份验证”或“授权”的预填充用户名选项时指定主用户名和辅助用户名应来自哪个证书。有关信息，请参阅配置多证书用户名，第 285 页

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

您也可以配置通过 SAML 进行多证书身份验证。

修改现有身份验证 webvpn 属性，以包含多证书身份验证选项：

```
tunnel-group <name> webvpn-attributes
authentication {aaa [certificate | multiple-certificate] | multiple-certificate [aaa | saml]
 | saml [certificate | multiple-certificate]}
```

通过多证书身份验证，可以根据证书字段制定策略决策，该证书用于对该连接尝试进行身份验证。将在多证书身份验证期间从客户端收到的用户和计算机证书加载到 DAP，以确保能够根据证书字段配置策略。要使用动态访问策略 (DAP) 添加多证书身份验证，以设置允许或禁止连接尝试的规则，请参阅中向 *DAP* 添加多证书身份验证一节相应版本的《ASA VPN ASDM 配置指南》。

配置多证书用户名

ASA 9.14(1) 中引入了一个新命令，可用于配置 ASA 必须用作身份验证或授权的主要和辅助用户名的证书。您可以指定是使用 SSL 或 IKE 中发送的计算机证书（第一个证书）还是来自客户端的用户证书（第二个证书）来获取身份验证和授权参数。无论身份验证类型如何（**aaa**、**证书**或**多证书**），均可为任何隧道组配置此选项。但是，此配置仅对多证书身份验证（**多证书**或 **aaa 多证书**）有效。当该选项未用于多证书身份验证时，默认情况下会使用第二个证书来进行身份验证或授权。

过程

步骤 1 指定是使用第一个证书还是第二个证书中的主用户名：

username-from-certificate-choice {first-certificate | second-certificate}

步骤 2 指定是使用第一个证书还是第二个证书中的辅助用户名：

secondary-username-from-certificate-choice {first-certificate | second-certificate}

示例：

```
tunnel-group tg1 webvpn-attributes
authentication aaa multiple-certificate
pre-fill-username client
secondary-pre-fill-username client
tunnel-group tg1 type remote-access
tunnel-group tg1 general-attributes
secondary-authentication-server-group LOCAL
username-from-certificate-choice first-certificate
secondary-username-from-certificate-choice first-certificate
```

为 VPN 配置 LDAP 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，此授权是独立的且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，分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。

过程

步骤 1 创建一个 AAA 服务器组。

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)
```

步骤 2 创建一个名为 remotegrp 的 IPsec 远程访问隧道组。

tunnel-group *groupname*

示例：

```
hostname(config)# tunnel-group remotegrp
```

步骤 3 将服务器组和隧道组关联。

tunnel-group *groupname* **general-attributes**

示例：

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

步骤 4 将新隧道组分配到先前创建的 AAA 服务器组进行授权。

authorization-server-group *group-tag*

示例：

```
hostname(config-general)# authorization-server-group ldap_dir_1
```

示例

以下示例显示启用 LDAP 的用户授权的命令。然后，该示例将创建一个名为 RAVPN 的 IPsec 远程访问隧道组，将新隧道组分配到先前创建的 LDAP AAA 服务器组进行授权：

```
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
```

```
hostname(config-general)# authorization-server-group (inside) LDAP
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 protocol ldap
hostname(config-aaa-server-group)# aaa-server LDAP (inside) host 10.0.2.128
hostname(config-aaa-server-host)# ldap-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-group-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-login-dn AD\cisco
hostname(config-aaa-server-host)# ldap-login-password cisco123
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)# server-type microsoft
```

定义 ASA LDAP 配置

本节介绍如何定义 LDAP AV 对属性语法，其中包括以下信息：

- LDAP 授权支持的思科属性，第 287 页
- 思科 AV 对属性语法，第 298 页
- 思科 AV 对 ACL 示例，第 299 页

注释 ASA 会根据属性名称而不是数值 ID 来实施 LDAP 属性。另一方面，RADIUS 属性会按数值 ID 而不是名称来实施。

授权是指执行权限或属性的过程。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）。

对于 ASA 7.0 版本，LDAP 属性包含 cVPN3000 前缀。对于软件 7.1 及更高版本，此前缀已移除。

LDAP 授权支持的思科属性

本节提供 ASA 5500、VPN 3000 集中器和 PIX 500 系列 ASA 的完整属性列表（请参阅）。该表包括 VPN 3000 集中器和 PIX 500 系列 ASA 的属性支持信息，以帮助您配置这些设备的组合。

表 *15: ASA* 支持的思科 *LDAP* 授权属性

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
Access-Hours	是	支持	支持	字符串	单值	时间范围的名称（例如，工作时间）

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
Allow-Network-Extension-Mode	支持	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
Authenticated-User-Idle-Timeout	支持	支持	支持	整数	单值	1 - 35791394 分钟
Authorization-Required	支持			整数	单值	0 = 否 1 = 是
Authorization-Type	是			整数	单值	0 = 无 1 = RADIUS 2 = LDAP
Banner1	是	支持	支持	字符串	单值	无客户端和客户端 SSL VPN 以及 IPsec 客户端的标语字符串。
Banner2	是	支持	支持	字符串	单值	无客户端和客户端 SSL VPN 以及 IPsec 客户端的标语字符串。
Cisco-AV-Pair	支持	支持	支持	字符串	多值	以下格式的八位组字符串： *[Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port]* 有关详细信息，请参阅“思科 AV 对属性语法”部分。
Cisco-IP-Phone-Bypass	是	支持	支持	整数	单值	0 = 已禁用 1 = 已启用
Cisco-LEAP-Bypass	是	支持	支持	整数	单值	0 = 已禁用 1 = 已启用
Client-Intercept-DHCP-Configure-Msg	支持	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
Client-Type-Version-Limiting	是	支持	支持	字符串	单值	IPsec VPN 客户端版本号字符串
Confidence-Interval	支持	支持	支持	整数	单值	10 - 300 秒
DHCP-Network-Scope	是	支持	支持	字符串	单值	IP 地址
DN-Field	支持	支持	支持	字符串	单值	可能的值：UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER 和 use-entire-name

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
Firewall-ACL-In		支持	支持	字符串	单值	访问列表 ID
Firewall-ACL-Out		支持	支持	字符串	单值	访问列表 ID
Group-Policy		是	支持	字符串	单值	为远程访问 VPN 会话设置组策略。对于 8.2 版本及更高版本，请改用此属性而非 IETF-Radius-Class。您可以使用以下三种格式之一： • 组策略名称 • OU= 组策略名称 • OU= 组策略名称：
IE-Proxy-Bypass-Local				布尔值	单值	0 = 已禁用 1 = 已启用
IE-Proxy-Exception-List				字符串	单值	DNS 域列表。条目必须以新的行字符序列 (\n) 分隔。
IE-Proxy-Method	支持	支持	支持	整数	单值	1 = 不修改代理设置 2 = 不使用代理 3 = 自动检测 4 = 使用 ASA 设置
IE-Proxy-Server	支持	支持	支持	整数	单值	IP 地址
IETF-Radius-Class	支持	支持	支持		单值	为远程访问 VPN 会话设置组策略。对于 8.2 版本及更高版本，请改用此属性而非 IETF-Radius-Class。您可以使用以下三种格式之一： • 组策略名称 • OU= 组策略名称 • OU= 组策略名称：
IETF-Radius-Filter-Id	支持	支持	支持	字符串	单值	在 ASA 上定义的访问列表名称。该设置适用于 VPN 远程访问 IPsec 和 SSL VPN 客户端。
IETF-Radius-Framed-IP-Address	支持	支持	支持	字符串	单值	IP 地址。该设置适用于 VPN 远程访问 IPsec 和 SSL VPN 客户端。

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
IETF-Radius-Framed-IP-Netmask	支持	支持	支持	字符串	单值	IP 地址掩码。该设置适用于 VPN 远程访问 IPsec 和 SSL VPN 客户端。
IETF-Radius-Idle-Timeout	支持	支持	支持	整数	单值	秒
IETF-Radius-Service-Type	支持	支持	支持	整数	单值	1 = 登录 2 = 成帧 5 = 远程访问 6 = 管理 7 = NAS 提示符
IETF-Radius-Session-Timeout	支持	支持	支持	整数	单值	秒
IKE-Keep-Alives	是	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Allow-Passwd-Store	是	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Authentication	支持	支持	支持	整数	单值	0 = 无 1 = RADIUS 2 = LDAP（仅限授权） 3 = NT 域 4 = SDI (RSA) 5 = 内部 6 = 具有有效期的 RADIUS 7 = Kerberos 或 Active Directory
IPsec-Auth-On-Rekey	是	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Backup-Server-List	是	支持	支持	字符串	单值	服务器地址（以空格分隔）
IPsec-Backup-Servers	是	支持	支持	字符串	单值	1 = 使用客户端配置的列表 2 = 已禁用并清除客户端列表 3 = 使用备份服务器列表
IPsec-Client-Firewall-Filter-Name	支持			字符串	单值	指定要作为防火墙策略推送到客户端的过滤器的名称。

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
IPsec-Client-Firewall-Filter-Optional	支持	支持	支持	整数	单值	0 = 必需 1 = 可选
IPsec-Default-Domain	是	支持	支持	字符串	单值	指定要发送到客户端的单个默认域名（1 到 255 个字符）。
IPsec-Extended-Auth-On-Rekey		支持	支持	字符串	单值	字符串
IPsec-IKE-Peer-ID-Check	是	支持	支持	整数	单值	1 = 必需 2 = 如果受对等体证书支持 3 = 不检查
IPsec-IP-Compression	是	支持	支持	整数	单值	0 = 已禁用 1 = 已启用
IPsec-Mode-Config	是	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP	是	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP-Port	是	支持	支持	整数	单值	4001 - 49151；默认值为 10000。
IPsec-Required-Client-Firewall-Capability	是	支持	支持	整数	单值	0 = 无 1 = 远程防火墙 Are-You-There (AYT) 定义的策略 2 = 策略推送的 CPP 4 = 来自服务器的策略
IPsec-Sec-Association	支持			字符串	单值	安全关联的名称
IPsec-Split-DNS-Names	是	支持	支持	字符串	单值	指定要发送到客户端的辅助域名列表（1 到 255 个字符）。
IPsec-Split-Tunneling-Policy	是	支持	支持	整数	单值	0 = 全部隧道化 1 = 分割隧道 2 = 允许本地 LAN
IPsec-Split-Tunnel-List	是	支持	支持	字符串	单值	指定用于描述分割隧道包含列表的网络或访问列表的名称。

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
IPsec-Tunnel-Type	是	支持	支持	整数	单值	1 = LAN 对 LAN 2 = 远程访问
L2TP-Encryption	支持			整数	单值	位图： 1 = 要求加密 2 = 40 位 4 = 128 位 8 = 无状态请求 15 = 40/128 位加密/无状态请求
L2IP-MPPC-Compression	支持			整数	单值	0 = 已禁用 1 = 已启用
MS-Client-Subnet-Mask	是	支持	支持	字符串	单值	IP 地址
PFS-Required	支持	支持	支持	布尔值	单值	0 = 否 1 = 是
Port-Forwarding-Name	支持	支持		字符串	单值	名称字符串（例如，“Corporate-Apps”）
PPTP-Encryption	支持			整数	单值	位图： 1 = 要求加密 2 = 40 位 4 = 128 位 8 = 无状态请求 示例： 15 = 40/128 位加密/无状态请求
PPTP-MPPC-Compression	支持			整数	单值	0 = 已禁用 1 = 已启用
Primary-DNS	是	支持	支持	字符串	单值	IP 地址
Primary-WINS	是	支持	支持	字符串	单值	IP 地址
Privilege-Level				整数	单值	对于用户名，0 - 15

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
Required-Client-Firewall-Vendor-Code	是	支持	支持	整数	单值	1 = 思科系统公司（带思科集成客户端） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5=思科系统公司（带思科入侵防御安全代理）
Required-Client-Firewall-Description	支持	支持	支持	字符串	单值	—
Required-Client-Firewall-Product-Code	支持	支持	支持	整数	单值	思科系统公司产品： 1=思科入侵防御安全代理或思科集成客户端 (CIC) Zone Labs 产品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 产品： 1 = BlackIce Defender/代理 Sygate 产品： 1 = 个人防火墙 2 = 个人防火墙专业版 3 = 安全代理
Require-HW-Client-Auth	是	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
Require-Individual-User-Auth	支持	支持	支持	整数	单值	0 = 已禁用 1 = 已启用
Secondary-DNS	是	支持	支持	字符串	单值	IP 地址
Secondary-WINS	是	支持	支持	字符串	单值	IP 地址
SEP-Card-Assignment				整数	单值	未使用
Simultaneous-Logins	是	支持	支持	整数	单值	0-2147483647

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
Strip-Realm	是	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
TACACS-Authtype	支持	支持	支持	整数	单值	—
TACACS-Privilege-Level	支持	支持	支持	整数	单值	—
Tunnel-Group-Lock		是	支持	字符串	单值	隧道组的名称或“none”
Tunneling-Protocols	是	支持	支持	整数	单值	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2TP/IPSec 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 和 4 相互排斥 （合法值为 0-11、16-27、32-43，以及 48-59 ）。
Use-Client-Address	支持			布尔值	单值	0 = 已禁用 1 = 已启用
User-Auth-Server-Name	支持			字符串	单值	IP 地址或主机名
User-Auth-Server-Port	支持	支持	支持	整数	单值	服务器协议的端口号
User-Auth-Server-Secret	支持			字符串	单值	服务器密码
WebVPN-ACL-Filters		支持		字符串	单值	Webtype 访问列表名称
WebVPN-Apply-ACL-Enable	支持	支持		整数	单值	0 = 已禁用 1 = 已启用 对于 8.0 及更高版本，此属性并非必需。
WebVPN-Citrix-Support-Enable	支持	支持		整数	单值	0 = 已禁用 1 = 已启用 对于 8.0 及更高版本，此属性并非必需。

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
WebVPN-Enable-functions				整数	单值	未使用 - 已弃用
WebVPN-Exchange-Server-Address				字符串	单值	未使用 - 已弃用
WebVPN-Exchange-Server-NETBIOS-Name				字符串	单值	未使用 - 已弃用
WebVPN-File-Access-Enable	是	支持		整数	单值	0 = 已禁用 1 = 已启用
WebVPN-File-Server-Browsing-Enable	是	支持		整数	单值	0 = 已禁用 1 = 已启用
WebVPN-File-Server-Entry-Enable	支持	支持		整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Forwarded-Ports		支持		字符串	单值	端口转发列表名称
WebVPN-Homepage	支持	支持		字符串	单值	URL，例如 http://www.example.com
WebVPN-Macro-Substitution-Value1	支持	支持		字符串	单值	例如，请参阅位于以下 URL 的《SSL VPN 部署指南》： http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Macro-Substitution-Value2	支持	支持		字符串	单值	例如，请参阅位于以下 URL 的《SSL VPN 部署指南》： http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Port-Forwarding-Auto-Download-Enable	支持	支持		布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-Enable	支持	支持		布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	支持	支持		布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-HTTP-Proxy-Enable	支持	支持		布尔值	单值	0 = 已禁用 1 = 已启用

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
WebVPN-Single-Sign-On-Server-Name	支持	支持		布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-Client-DPD	支持	支持		布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-Compression	是	支持		布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-Enable	支持	支持		布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-Gateway-DPD	支持	支持		整数	单值	0 = 已禁用 n = 失效对等体检测值，以秒为单位 (30 - 3600)
WebVPN-SVC-Keepalive	支持	支持		整数	单值	0 = 已禁用 n = 保持连接值，以秒为单位 (15 - 600)
WebVPN-SVC-Keep-Enable	支持	支持		整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-Rekey-Method	是	支持		整数	单值	0 = 无 1 = SSL 2 = 新隧道 3 = 任意（设置为 SSL）
WebVPN-SVC-Rekey-Period	支持	支持		整数	单值	0 = 已禁用 n = 重试时间，以分钟为单位 (4 - 10080)
WebVPN-SVC-Required-Enable	支持	支持		整数	单值	0 = 已禁用 1 = 已启用
WebVPN-URL-Entry-Enable	是	支持		整数	单值	0 = 已禁用 1 = 已启用
WebVPN-URL-List		是		字符串	单值	URL 列表名称

ACL 中支持的 URL 类型

URL 可以是部分 URL，包含服务器的通配符或包含端口。

支持以下 URL 类型。

任何 URL	https://	post://	ssh://
cifs://	ica://	rdp://	telnet://
citrix://	imap4://	rdp2://	vnc://
citrixs://	ftp://	smart-tunnel://	
http://	pop3://	smtp://	

使用思科 AV 对 (ACL) 的准则

- 使用带有 ip:inacl# 前缀的思科 AV 对条目来对远程 IPsec 和 SSL VPN 客户端 (SVC) 隧道实施访问列表。
- 使用带有 webvpn:inacl# 前缀的思科 AV 对条目来对 SSL VPN 无客户端（浏览器模式）隧道实施访问列表。
- 对于 Webtype ACL，您不用指定源，因为 ASA 就是源。

表 *16: ASA* 支持的令牌

令牌	语法字段	说明
ip:inacl# *Num* =	不适用（标识符）	（其中 *Num* 是唯一的整数。）启动所有 AV 对访问控制列表。对远程 IPsec 和 SSL VPN (SVC) 隧道实施访问列表。
webvpn:inacl# *Num* =	不适用（标识符）	（其中 *Num* 是唯一的整数。）启动所有无客户端 SSL AV 对访问控制列表。对无客户端（浏览器模式）隧道实施访问列表。
deny	操作	拒绝操作。（默认）
permit	操作	允许操作。
icmp	协议	互联网控制消息协议 (ICMP)
1	协议	互联网控制消息协议 (ICMP)
IP	协议	Internet 协议 (IP)
0	协议	Internet 协议 (IP)
TCP	协议	传输控制协议 (TCP)
6	协议	传输控制协议 (TCP)

令牌	语法字段	说明
UDP	协议	用户数据报协议 (UDP)
17	协议	用户数据报协议 (UDP)
any	主机名	规则适用于任何主机。
host	主机名	表示主机名的任何字母数字字符串。
log	记录	发生该事件时，系统会显示过滤器日志消息。（与 permit 和 log 或 deny 和 log 相同。）
lt	运算符	小于值
gt	运算符	大于值
eq	运算符	等于值
neq	运算符	不等于值
range	运算符	包含范围。应后跟两个值。

思科 AV 对属性语法

思科属性值 (AV) 对（ID 编号 26/9/1）可用于从 RADIUS 服务器（例如思科 ACS）或通过 LDAP 属性映射从 LDAP 服务器来实施访问列表。

每个 Cisco-AV-Pair 规则的语法如下：

[Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port]

表 *17: AV* 对属性语法规则

字段	说明
操作	规则与拒绝或允许匹配时要执行的操作。
目标	接收数据包的网络或主机。将其指定为 IP 地址、主机名或 **any** 关键字。如果使用 IP 地址，则必须遵循源通配符掩码。
目标通配符掩码	适用于目标址的通配符掩码。
记录	生成过滤器日志消息。您必须使用此关键字生成严重性级别为 9 的事件。
运算符	逻辑运算符：大于、小于、等于、不等于。
端口	TCP 或 UDP 端口号，范围为 0 - 65535。

字段	说明
前缀	AV 对的唯一标识符（例如：ip:inacl#1= 表示标准访问列表或 webvpn:inacl# = 无客户端 SSL VPN 访问列表）。仅当过滤器作为 AV 对发送时才会显示此字段。
协议	IP 协议的名称或编号。0-255 范围内的整数或以下关键字之一：**icmp**、**igmp**、**ip**、**tcp**、**udp**。
源	发送数据包的网络或主机。将其指定为 IP 地址、主机名或 **any** 关键字。如果使用 IP 地址，则必须遵循源通配符掩码。此字段不适用于无客户端 SSL VPN，因为 ASA 具有源或代理角色。
源通配符掩码	适用于源地址的通配符掩码。此字段不适用于无客户端 SSL VPN，因为 ASA 具有源或代理角色。

思科 AV 对 ACL 示例

本节显示思科 AV 对的示例，并介绍导致的允许或拒绝操作。

注释 inacl# 中的每个 ACL # 必须是唯一的。但是，它们不需要是连续的（例如，1、2、3、4）。也就是说，它们可能是 5、45、135。

表 *18:* 思科 *AV* 对及其允许或拒绝操作的示例

思科 AV 对示例	允许或拒绝操作
`ip:inacl#1=deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log`	允许使用完整隧道 IPsec 或 SSL VPN 客户端的两台主机之间的 IP 流量。
`ip:inacl#2=permit TCP any host 10.160.0.1 eq 80 log`	仅允许使用完整隧道 IPsec 或 SSL VPN 客户端将 TCP 流量从端口 80 传输到特定主机。
`webvpn:inacl#1=permit url http://www.example.comwebvpn:inacl#2=deny url smtp://serverwebvpn:inacl#3=permit url cifs://server/share`	允许流向指定 URL 的无客户端 SSL VPN 流量，拒绝流向特定服务器的 SMTP 流量，并允许流向指定服务器的文件共享访问 (CIFS)。
`webvpn:inacl#1=permit tcp 10.86.1.2 eq 2222 logwebvpn:inacl#2=deny tcp 10.86.1.2 eq 2323 log`	拒绝 Telnet 访问并允许分别在非默认端口 2323 和 2222 上进行 SSH 访问，或允许使用这些端口的其他应用流量进行无客户端 SSL VPN 访问。
`webvpn:inacl#1=permit url ssh://10.86.1.2webvpn:inacl#35=permit tcp 10.86.1.5 eq 22 logwebvpn:inacl#48=deny url telnet://10.86.1.2webvpn:inacl#100=deny tcp 10.86.1.6 eq 23`	分别允许对默认端口 22 进行无客户端 SSL VPN SSH 访问，并拒绝对端口 23 进行 Telnet 访问。此示例假定您使用的是这些 ACL 实施的 Telnet 或 SSH Java 插件。

Active Directory/LDAP VPN 远程访问授权示例

本节提供在 ASA 上使用 Microsoft Active Directory 服务器配置身份验证和授权的示例程序。包括以下主题：

Cisco.com 提供的其他配置示例包括以下技术说明。

- ASA/PIX：通过 LDAP 配置将 VPN 客户端映射至 VPN 组策略的示例
- PIX/ASA 8.0：登录时使用 LDAP 身份验证来分配组策略

基于用户的属性的策略实施

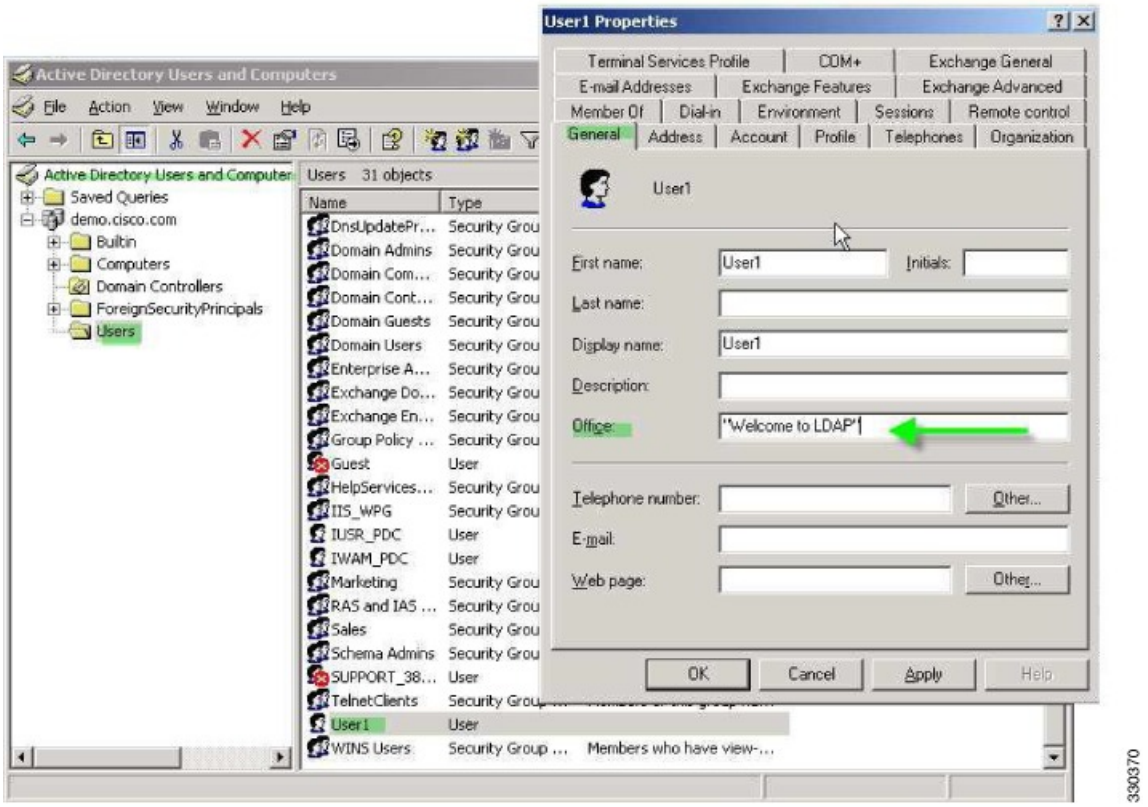
此示例向用户显示一个简单的欢迎信息，说明如何将任意标准 LDAP 属性映射至一个已知的供应商特定属性 (VSA)，或者将一个或多个 LDAP 属性映射至一个或多个思科 LDAP 属性。此示例适用于任意连接类型，包括 IPSec VPN 客户端和 Secure Client。

如要为 AD LDAP 服务器上配置的用户实施简单的欢迎信息，请使用 General 选项卡中的 Office 字段输入欢迎信息文本。此字段使用名为 physicalDeliveryOfficeName 的属性。在 ASA 中，创建将 physicalDeliveryOfficeName 映射至思科属性 Banner1 的属性映射。

在身份验证过程中，ASA 从服务器检索 physicalDeliveryOfficeName 的值，将该值映射至思科属性 Banner1，然后向用户显示该欢迎信息。

过程

步骤 1 右键点击用户名打开“属性”(Properties) 对话框，然后点击**常规 (General)** 选项卡，在“办公室”(Office) 字段中输入欢迎信息文本，该字段使用 AD/LDAP 属性 physicalDeliveryOfficeName。



步骤 2 在 ASA 上创建一个 LDAP 属性映射。

创建映射 Banner，并将 AD/LDAP 属性 physicalDeliveryOfficeName 映射至思科属性 Banner1：

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

步骤 3 将 LDAP 属性映射关联到 AAA 服务器。

进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您先前创建的属性映射 Banner：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

步骤 4 测试此欢迎信息的实施。

为 Secure Client 隧道实施静态 IP 地址分配

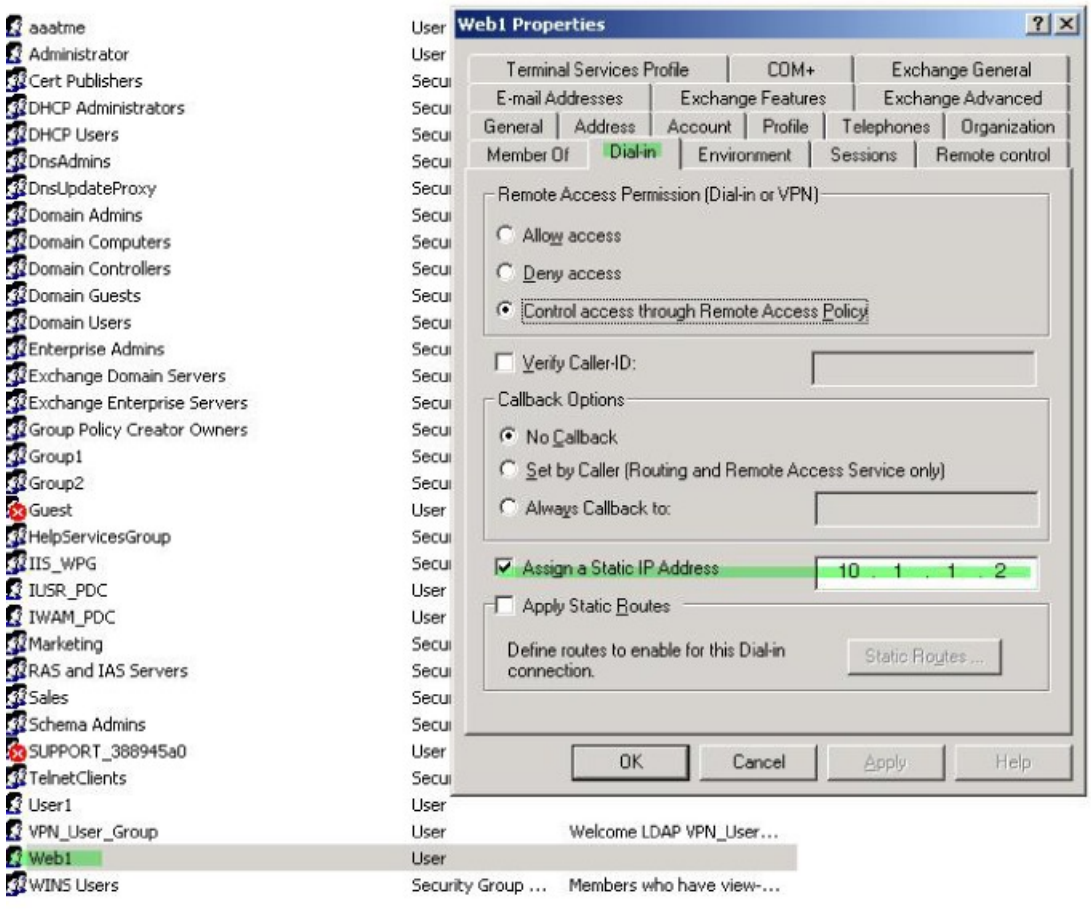
此示例适用于完全隧道客户端，例如 IPsec 客户端和 SSL VPN 客户端。

如要实施静态 Secure Client 静态 IP 分配，请将 Secure Client用户 Web1 配置为接受静态 IP 地址，在 AD LDAP 服务器上的 Dialin 选项卡的 Assign Static IP Address 字段中输入地址（此字段使用 msRADIUSFramedIPAddress 属性），然后创建一个可将该属性映射至思科属性 IETF-Radius-Framed-IP-Address 的属性映射。

在身份验证过程中，ASA 从服务器检索 msRADIUSFramedIPAddress 的值，将该值映射至思科属性 IETF-Radius-Framed-IP-Address，并向 User1 提供静态地址。

过程

步骤 1 右键点击用户名打开“属性”(Properties) 对话框，然后点击**拔入 (Dial-in)** 选项卡，选中**分配静态 IP 地址 (Assign Static IP Address)** 复选框并输入 IP 地址 10.1.1.2。



步骤 2 为显示的 LDAP 配置创建一个属性映射。

将 Static Address 字段使用的 AD 属性 msRADIUSFramedIPAddress 映射至思科属性 IETF-Radius-Framed-IP-Address：

```
hostname(config)# ldap attribute-map static_address
```

```
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

步骤 3 将 LDAP 属性映射关联到 AAA 服务器。

进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您先前创建的属性映射 static_address：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

步骤 4 通过查看此部分的配置，验证是否已配置 **vpn-address-assignment** 命令来指定 AAA：

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa   << Make sure this is configured >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

步骤 5 使用 Secure Client建立与 ASA 的连接。观察用户是否收到在服务器上配置并映射至 ASA 的 IP 地址。

步骤 6 使用 **show vpn-sessiondb svc** 命令来查看会话详细信息，并验证分配的地址：

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

实施拨入允许或拒绝访问

本示例创建指定用户允许的隧道协议的 LDAP 属性映射。您可以将 Dialin 选项卡中的允许访问和拒绝访问设置映射至思科属性 Tunneling-Protocol，该属性支持以下映射值：

值	隧道协议
1	PPTP
2	L2TP
4	IPsec (IKEv1)
8	L2TP/IPsec

值	隧道协议
16	无客户端 SSL
32	SSL 客户端 - Secure Client 或 SSL VPN 客户端
64	IPsec (IKEv2)

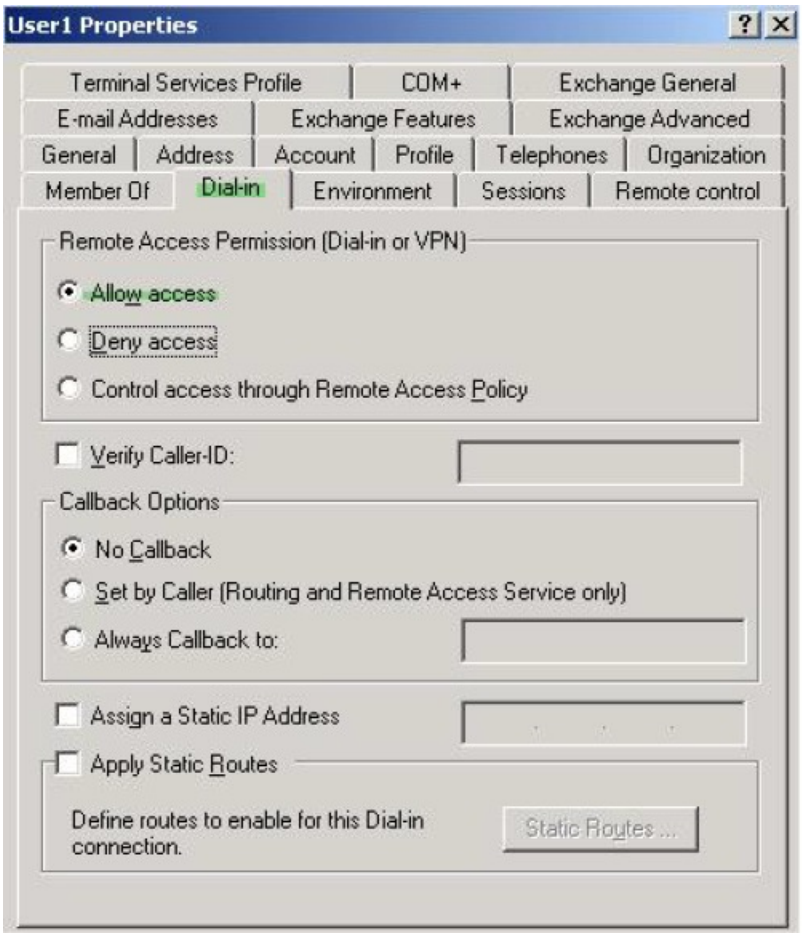
[1] (1) 不能同时支持 IPsec 和 L2TP over IPsec。因此，值 4 和 8 只能二选其一。
[2] (2) 请参阅注释 1。

使用此属性创建协议的允许访问 (TRUE) 或拒绝访问 (FALSE) 条件，并实施允许用户访问的方法。

有关实施拨入允许访问或拒绝访问的其他示例，请参阅以下技术说明：ASA/PIX：通过 LDAP 配置将 VPN 客户端映射至 VPN 组策略的示例。

过程

步骤 1 右键点击用户名打开“属性”(Properties) 对话框，然后点击**拨入 (Dial-in)** 选项卡，再点击“允许访问”(Allow Access) 单选按钮。



注释
如果您通过“远程访问策略”(Remote Access Policy) 选项选择控制访问，则服务器不会返回值，而实施的权限则根据 ASA 的内部组策略设置而定。

步骤 2 创建一个允许 IPsec 和 Secure Client 连接，但是拒绝无客户端 SSL 连接的属性映射。

a) 创建映射 tunneling_protocols：

```
hostname(config)# ldap attribute-map tunneling_protocols
```

b) 将 Allow Access 设置使用的 AD 属性 msNPAllowDialin 映射至思科属性 Tunneling-Protocols：

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) 添加映射值：

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

步骤 3 将 LDAP 属性映射关联到 AAA 服务器。

a) 进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) 关联您创建的属性映射 tunneling_protocols：

```
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

步骤 4 验证属性映射是否按配置工作。

尝试使用无客户端 SSL 的连接，用户应接到通知，告知其未经授权的连接机制是连接失败的原因。IPSec 客户端应该可以连接，因为根据属性映射，IPsec 是允许的隧道协议。

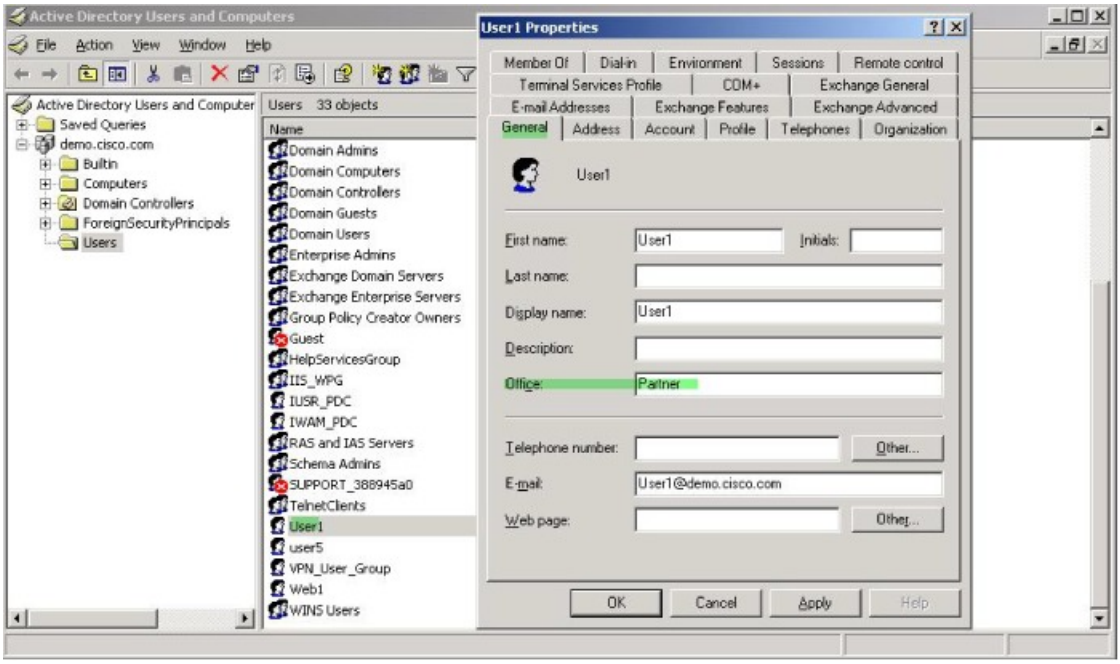
实施登录时长和时间规则

以下示例展示如何配置和实施允许无客户端 SSL 用户（例如业务合作伙伴）访问网络的时长。

在 AD 服务器上，使用 Office 字段输入合作伙伴的名称，该字段使用 physicalDeliveryOfficeName 属性。然后我们在 ASA 上创建一个可将该属性映射至思科属性 Access-Hours 的属性映射。在身份验证过程中，ASA 会检索 physicalDeliveryOfficeName 的值，并将其映射至 Access-Hours。

过程

步骤 1 选择用户，右键点击**属性 (Properties)**，然后打开**常规 (General)** 选项卡：



步骤 2 创建属性映射。

创建属性映射 access_hours，并将 Office 字段使用的 AD 属性 physicalDeliveryOfficeName 映射至思科属性 Access-Hours。

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

步骤 3 将 LDAP 属性映射关联到 AAA 服务器。

进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您创建的属性映射 access_hours：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

步骤 4 为服务器上允许的每个值配置时间范围。

将合作伙伴访问时长配置为周一至周五上午 9 点到下午 5 点：

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

当地语言翻译版本说明

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