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 34 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 *1: 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 8 页。
- 配置远程访问连接配置文件常规属性，第 9 页。
- 配置双重身份验证，第 13 页
- 配置远程访问连接配置文件 IPsec IKEv1 属性，第 14 页。
- 配置 IPsec 远程访问连接配置文件 PPP 属性，第 17 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 27 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 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：

- 指定 LAN 间连接配置文件的名称和类型，第 19 页
- 配置 LAN 间连接配置文件常规属性，第 19 页
- 配置 LAN 间 IPsec IKEv1 属性，第 20 页

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	是	是	是	是	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）	是	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	是	是

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	是	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	是	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	N/A	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	是	是

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 30 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 36 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。输入“\n”序列以插入回车符。

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。

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`
		`hostname(config-group-policy)# vpn-simultaneous-logins 4`

	命令或操作	目的
		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。

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。

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

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 68 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 68 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 *2: 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 *3: 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。
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。

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。

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。