AnyConnect VPN 客户端连接

本节介绍如何配置 AnyConnect VPN 客户端连接。

关于 Secure Client VPN 客户端

Secure Client为远程用户提供了与 ASA 的安全 SSL 和 IPsec/IKEv2 连接。在先前未安装客户端的情况下，远程用户可以在他们的浏览器中输入配置为接受 SSL 或 IPsec/IKEv2 VPN 连接的接口的 IP 地址。除非 ASA 已配置为将 http:// 请求重定向到 https://，否则用户必须以 https://<*address*> 形式输入 URL。

输入 URL 后，浏览器连接至该接口，并显示登录屏幕。如果用户满足登录和身份验证要求，并且 ASA 将用户确定为需要客户端，则它会下载与远程计算机的操作系统匹配的客户端。下载后，客户端进行安装并自行配置，建立安全的 SSL 或 IPsec/IKEv2 连接，连接终止时，客户端会保留或自行卸载（取决于配置）。

如果先前已安装客户端，当用户进行身份验证时，ASA 将检查客户端的修订版本并在必要情况下升级客户端。

当客户端与 ASA 协商 SSL VPN 连接时，实际上会使用传输层安全 (TLS) 和（可选）数据报传输层安全 (DTLS) 进行连接。DTLS 可避免与某些 SSL 连接关联的延迟和带宽问题，并可提高对于数据包延迟敏感的实时应用的性能。

Secure Client可从 ASA 下载，也可以由系统管理员在远程 PC 上手动安装。有关手动安装客户端的详细信息，请参阅相应版本的《思科 AnyConnect 安全移动配置指南》。

ASA 基于建立连接的用户的组策略或用户名属性下载客户端。您可以将 ASA 配置为自动下载客户端，也可以将其配置为提示远程用户是否下载客户端。对于后一种情况，如果用户不响应，您可以将 ASA 配置为在超时期限结束后下载客户端，或显示登录页面。

要求 Secure Client

有关运行 Secure Client的终端计算机的要求，请参阅 相应版本的《思科 AnyConnect 安全移动版本说明》。

准则和限制 Secure Client

- ASA 不会验证远程 HTTPS 证书。
- 支持单情景或多情景模式。在多情景模式下，远程访问 VPN 需要 AnyConnect Apex 许可证。尽管 ASA 未明确认可 AnyConnect Apex 许可证，但它实施 Apex 许可证的特征，例如获得平台限制许可的 AnyConnect 高级版、Secure Client 移动版、适用于思科 VPN 电话的 Secure Client 和高级终端评估。系统不支持共享许可、AnyConnect 基础版、故障转移许可证聚合以及 Flex/基于时间的许可证。
- 不直接支持对 RA VPN 前端发出命令（例如 **curl** ），并且可能不会产生所需的结果。例如，前端不响应 HTTP HEAD 请求。
- 当硬件 VPN 电话（例如思科 88xx 系列）使用 Secure Client 时，尽管启用了 DTLS 并配置了对等体存活检测 (DPD)，但它们也可能会重新连接。
- 当客户端连接到 Secure Client 时，连接前后客户端的 IP 地址会更改。ASA 支持此行为。

Secure Client的许可要求

注释 此功能不适用于无负载加密型号。

VPN 许可证需要 AnyConnect Plus 或 Apex 许可证，可单独购买。有关每个型号的最大值，请参阅思科 ASA 系列功能许可证。

如果启动无客户端 SSL VPN 会话，然后从门户启动 Secure Client 会话，则总共会使用 1 个会话。但是，如果先启动 Secure Client（例如，通过独立客户端），然后登录无客户端 SSL VPN 门户，则会使用 2 个会话。

配置 Secure Client 连接

本节介绍将 ASA 配置为接受 AnyConnect VPN 客户端连接的前提条件、限制和详细任务。

将 ASA 配置为以 Web 方式部署客户端

本节介绍将 ASA 配置为以 Web 方式部署 Secure Client的步骤。

开始之前

使用 TFTP 或其他方法将客户端映像包复制到 ASA。

注释 即使在 ASA 上禁用了无客户端 VPN 功能，当您使用 Web 浏览器访问 AnyConnect webdeploy (https://x.x.x.x<ASA IP address> 时，ASA 上的 VPN 会话将被算作无客户端会话。

过程

步骤 1 将闪存上的文件标识为 Secure Client包文件。

ASA 在缓存中展开文件，以便下载至远程 PC。如果您有多个客户端，请使用 order 参数给客户端映像分配顺序。

ASA 以您指定的顺序下载每个客户端的各个部分，直到其与远程 PC 的操作系统相匹配。因此，请给最常见的操作系统使用的映像分配最小的数值。

anyconnect image *filename order*

示例：

```
hostname(config-webvpn)# anyconnect image
anyconnect-win-2.3.0254-k9.pkg 1
hostname(config-webvpn)# anyconnect image
anyconnect-macosx-i386-2.3.0254-k9.pkg 2
hostname(config-webvpn)# anyconnect image
anyconnect-linux-2.3.0254-k9.pkg 3
```

注释
使用 **anyconnect image** 命令配置 Secure Client 映像后，必须发出 **anyconnect enable** 命令。如果没有启用 Secure Client，则其不会执行预期操作，并且 **show webvpn anyconnect** 会将 SSL VPN 客户端视为未启用，而不是列出已安装的 Secure Client 包。

步骤 2 在接口上启用 SSL，以便进行无客户端或 Secure Client SSL 连接。

enable *interface*

示例：

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

步骤 3 在没有发出此命令的情况下，Secure Client 不会执行预期操作，而且 **show webvpn anyconnect** 命令会返回“SSL VPN is not enabled”，而不是列出已安装的 Secure Client 包。

anyconnect enable

步骤 4 （可选） 创建地址池。您可以使用其他地址分配方法，如 DHCP 和/或用户分配的寻址。

ip local pool *poolname startaddr-endaddr* **mask** *mask*

示例：

```
hostname(config)# ip local pool vpn_users 209.165.200.225-209.165.200.254
mask 255.255.255.224
```

步骤 5 将地址池分配至隧道组。

address-pool *poolname*

示例：

```
hostname(config)# tunnel-group telecommuters general-attributes
hostname(config-tunnel-general)# address-pool vpn_users
```

步骤 6 将默认组策略分配至隧道组。

default-group-policy *name*

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

步骤 7 启用在无客户端门户和 Secure Client GUI 登录页面上显示隧道组列表。该别名列表由 *group-alias name enable* 命令定义。

group-alias *name* **enable**

示例：

```
hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias sales_department enable
```

步骤 8 将 Secure Client 指定为组或用户的允许的 VPN 隧道协议。

tunnel-group-list enable

示例：

```
hostname(config)# webvpn
hostname(config-webvpn)# tunnel-group-list enable
```

步骤 9 将 SSL 指定为组或用户的允许的 VPN 隧道协议。您还可以指定其他协议。有关详细信息，请参阅命令参考中的 vpn-tunnel-protocol 命令。

vpn-tunnel-protocol

示例：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# vpn-tunnel-protocol
```

下一步做什么

有关将用户分配至组策略的详细信息，请参阅第 6 章“配置连接配置文件、组策略和用户”。

启用永久性客户端安装

启用永久性客户端安装将会禁用客户端的自动卸载功能。客户端仍安装在远程计算机上以进行后续连接，从而缩短远程用户的连接时间。

要为特定组或用户启用永久性客户端安装，可以在组策略或用户名 webvpn 模式下，使用 anyconnect keep-installer 命令：

默认设置为启用客户端的永久性安装。客户端在会话结束时仍安装在远程计算机上。以下示例将现有组策略 *sales* 配置为在会话结束时从远程计算机上删除客户端。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# anyconnect keep-installer installed none
```

配置 DTLS

数据报传输层安全 (DTLS) 允许 Secure Client建立 SSL VPN 连接，以便使用两个并行隧道 - SSL 隧道和 DTLS 隧道。使用 DTLS 可避免与 SSL 连接关联的延迟和带宽问题，并且提高对于数据包延迟敏感的实时应用的性能。

开始之前

请参阅 配置高级 SSL 设置 在此头端上配置 DTLS 和使用的 DTLS 版本。

为使DTLS能够回退至TLS连接，必须启用对等体存活检测(DPD)。如果没有启用DPD，则当DTLS连接遇到问题时，连接会终止而不是回退至TLS。有关DPD的详细信息，请参阅配置对等体存活检测，第 16 页。

过程

步骤 1 为 Secure Client VPN 连接指定 DTLS 选项：

a) 在 webvpn 模式下，在接口上启用 SSL 和 DTLS。

默认情况下，在接口上启用 SSL VPN 访问时，则会启用 DTLS。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

在 webvpn 配置模式下，使用 **enable** *interface* **tls-only** 命令为所有 Secure Client 用户禁用 DTLS。

如果禁用 DTLS，则 SSL VPN 连接只会与 SSL VPN 隧道连接。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside tls-only
```

b) 使用 **port** 和 **dtls port** 命令配置 SSL 和 DTLS 的端口。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
hostname(config-webvpn)# port 555
hostname(config-webvpn)# dtls port 556
```

步骤 2 为特定组策略指定 DTLS 选项。

a) 在组策略 webvpn 或用户名 webvpn 配置模式下，使用 **anyconnect ssl dtls** 命令为特定组或用户启用 DTLS。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl dtls enable
```

b) 如果需要，使用 anyconnect dtls compression 命令启用 DTLS 压缩。

```
hostname(config-group-webvpn)# anyconnect dtls compression lzs
```

提示远程用户

过程

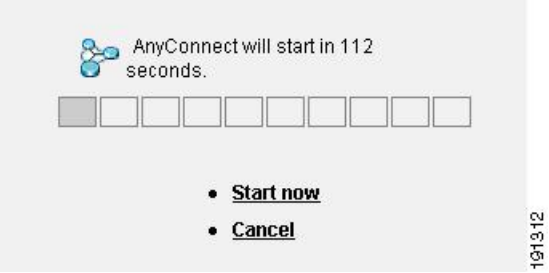
您可以在组策略 webvpn 或用户名 webvpn 配置模式下，使用 **anyconnect ask** 命令来允许 ASA 提示远程 SSL VPN 客户端用户下载客户端：

[**no**] **anyconnect ask** {**none** | **enable** [**default** {**webvpn** | } **timeout** *value*]}

- **anyconnect enable** 提示远程用户下载客户端或转至无客户端门户页面，并且无限期等待用户响应。
- **anyconnect ask enable default** 立即下载客户端。
- **anyconnect ask enable default webvpn** 立即转至门户页面。
- **anyconnect ask enable default timeout** value 提示远程用户下载客户端或转至无客户端门户页面，并且在采取默认操作（下载客户端）前等待长度为 *value* 的一段时间。
- **anyconnect ask enable default clientless timeout** value 提示远程用户下载客户端或转至无客户端门户页面，并且在采取默认操作（显示无客户端门户页面）前等待长度为 *value* 的一段时间。

下图显示配置 **default anyconnect timeout** *value* 或**default webvpn timeout** *value* 时向远程用户显示的提示：

图 *1:* 向远程用户显示提示，提示其下载 ***SSL VPN*** 客户端



示例

以下示例将 ASA 配置为提示用户下载客户端或转至无客户端门户页面，并且在下载客户端前等待 *10* 秒以便用户作出响应：

```
hostname(config-group-webvpn)# anyconnect ask enable default anyconnect timeout
 10
```

启用 Secure Client配置文件下载

您可以在 Secure Client 配置文件中启用 Secure Client 功能，这些配置文件是 XML 文件，包含核心客户端及其 VPN 功能以及可选客户端模块的配置设置。ASA 会在 Secure Client 的安装和更新期间部署配置文件。用户无法管理或修改配置文件。

下载到客户端的文件格式如下：<*profile_name*>.xml。

您可以使用 Secure Client 配置文件编辑器对配置文件进行配置，该编辑器是一款从 ASDM 或 ISE 启动的基于 GUI 的便捷配置工具。适用于 Windows 的 Secure Client 软件包提供了该编辑器，在您于选定的头端设备上加载 AnyConnect 包并将其指定为 Secure Client映像时，该编辑器会激活。

我们还提供了该配置文件编辑器的适用于 Windows 的独立版本，您可以将其用作与 ASDM 或 ISE 集成的配置文件编辑器的备选编辑器。如果您要预先部署客户端，可以使用独立配置文件编辑器为您使用软件管理系统部署至计算机的 VPN 服务和其他模块创建配置文件。

有关 Secure Client及其配置文件编辑器的详细信息，请参阅相应版本的《思科 AnyConnect 安全移动配置指南》。

注释 Secure Client协议默认设置为 SSL。要启用 IPsec IKEv2，您必须在 ASA 上配置 IKEv2 设置，并且还要在客户端配置文件中将 IKEv2 配置为主协议。必须将 IKEv2enabled 配置文件部署至终端计算机，否则客户端会尝试使用 SSL 进行连接。

过程

步骤 1 使用 ASDM/ISE 中的配置文件编辑器或独立配置文件编辑器来创建配置文件。

步骤 2 使用 TFTP 或其他方法将配置文件加载至 ASA 上的闪存。

步骤 3 在 webvpn 配置模式下，使用 **anyconnect profiles** 命令将文件确定为要加载至缓存的客户端配置文件。

示例：

以下示例将文件 sales_hosts.xml 和 engineering_hosts.xml 指定为配置文件：

```
asa1(config-webvpn)# anyconnect profiles sales
disk0:/sales_hosts.xml
asa1(config-webvpn)# anyconnect profiles engineering
disk0:/engineering_hosts.xml
```

此时，这些配置文件可供组策略使用。

可以使用 **dir cache:stc/profiles** 命令查看已在缓存中加载的配置文件：

```
hostname(config-webvpn)# dir cache:/stc/profiles

Directory of cache:stc/profiles/

0      ----  774         11:54:41 Nov 22 2006  engineering.xml
0      ----  774         11:54:29 Nov 22 2006  sales.xml

2428928 bytes total (18219008 bytes free)
hostname(config-webvpn)#
```

步骤 4 进入组策略 webvpn 配置模式，并使用 **anyconnect profiles** 命令为组策略指定客户端配置文件：

示例：

您可以输入后面带有问号的 profiles value 命令 (**?**)，以便查看可用的配置文件。例如：

```
asa1(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages: engineering sales
```

下一示例将组策略配置为使用客户端配置文件类型为 *vpn* 的配置文件 *sales*：

```
asa1(config-group-webvpn)# anyconnect profiles value sales type vpn
asa1(config-group-webvpn)#
```

启用 Secure Client 延迟升级

延迟升级允许 Secure Client 用户延迟客户端升级的下载。当客户端更新可用时，Secure Client 会打开一个对话框，询问用户是想要进行更新，还是想要延迟升级。除非您已在 Secure Client 配置文件设置中将“自动更新”(AutoUpdate) 设置为已启用 *(Enabled)*，否则系统不会显示此升级对话框。

通过将自定义属性类型和命名值添加至 ASA，然后在组策略中引用和配置这些属性，可以启用延迟升级。

以下自定义属性支持延迟升级：

表 *1:* 适用于延迟升级的自定义属性

自定义属性类型	有效值	默认值	备注
DeferredUpdateAllowed	true false	False	True 可以启用延迟更新。如果延迟更新被禁用 (false)，以下设置会被忽略。
DeferredUpdateMinimumVersion	x.y.z	0.0.0	实现更新可延迟所必须要安装的最低 Secure Client 版本。 最低版本检查适用于头端上启用的所有模块。如果启用的任意模块（包括 VPN）未安装或不符合最低版本要求，则连接不符合延迟更新条件。 如果未指定此属性，无论在终端上安装的版本如何，系统都会显示（或自动关闭）延迟提示。
DeferredUpdateDismissTimeout	0-300 （秒）	无（已禁用）	延迟升级提示在自动关闭之前显示的秒数。仅当显示延迟更新提示时才应用此属性（先评估最低版本属性）。 如果此属性缺失，则禁用自动关闭功能，对话框会一直显示（如需要），直到用户作出响应。 将此属性设置为零，则允许根据以下条件强制进行自动延迟或升级： • 已安装的版本和 DeferredUpdateMinimumVersion 的值。 • DeferredUpdateDismissResponse 的值。
DeferredUpdateDismissResponse	延迟更新	更新	发生 DeferredUpdateDismissTimeout 时采取的操作。

过程

步骤 1 在 webvpn 配置模式下使用 **anyconnnect-custom-attr** 命令创建自定义属性类型：

[**no**] **anyconnect-custom-attr** *attr-type* [**description** *description*]

示例：

以下示例显示如何添加自定义属性类型 DeferredUpdateAllowed 和 DeferredUpdateDismissTimeout：

```
hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed
description Indicates if the deferred update feature is enabled or not
```

```
hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateDismissTimeout
```

步骤 2 在全局配置模式下，使用 **anyconnect-custom-data** 命令为自定义属性添加命名值：对于长值属性，您可以提供重复条目以允许连接。然而，在具备重复配置条目的情况下，系统将不会显示“延迟更新”对话框，并且用户不能延迟升级；相反，系统将会自动升级。

[**no**] **anyconnect-custom-data** *attr-type attr-name attr-value*

示例：

以下示例显示如何为自定义属性类型 DeferredUpdateDismissTimeout 和启用的 DeferredUpdateAllowed 添加命名值：

```
hostname(config)# anyconnect-custom-data DeferredUpdateDismissTimeout
def-timeout 150
hostname(config)# anyconnect-custom-data DeferredUpdateAllowed
def-allowed true
```

步骤 3 使用 **anyconnect-custom** 命令在组策略中添加或删除自定义属性命名值：

- **anyconnect-custom** *attr-type* **value** *attr-name*
- **anyconnect-custom** *attr-type* **none**
- **no anyconnect-custom** *attr-type*

示例：

以下示例显示如何为名为 sales 的组策略启用延迟更新，并将超时时间设置为 150 秒：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# anyconnect-custom DeferredUpdateAllowed
value def-allowed
hostname(config-group-policy)# anyconnect-custom DeferredUpdateDismissTimeout
value def-timeout
```

启用 DSCP 预留

通过设置另一个自定义属性，可以仅对 DTLS 连接控制 Windows 或 OS X 平台上的差分服务代码点 (DSCP)。通过启用 DSCP 预留，设备可以优先处理延迟敏感型流量；路由器会考虑是否设置此选项，并且标记优先化的流量以提高出站连接质量。

过程

步骤 1 在 webvpn 配置模式下使用 **anyconnect-custom-attr** 命令创建自定义属性类型：

[no] anyconnect-custom-attr DSCPPreservationAllowed description Set to control Differentiated Services Code Point (DSCP) on Windows or OS X platforms for DTLS connections only.

步骤 2 在全局配置模式下，使用 **anyconnect-custom-data** 命令为自定义属性添加命名值：

[no] anyconnect-custom-data DSCPPreservationAllowed true

注释
默认情况下，Secure Client 会执行 DSCP 预留 (true)。要将其禁用，请在头端将自定义属性设置为 false，然后重新启动连接。

启用其他 Secure Client 功能

如要最大限度缩短下载时间，客户端可以仅请求下载（从 ASA 或 ISE）其需要的核心模块。当附加功能可供 Secure Client使用时，您需要更新远程客户端，以便其能够使用这些功能。

要启用新功能，您必须在组策略 webvpn 或用户名 webvpn 配置模式下，使用 **anyconnect modules** 命令指定新模块的名称：

[**no**]**anyconnect modules** {**none** | **value** *string*}

使用逗号分隔多个字符串。

启用登录前开始

登录前开始 (SBL) 支持适用于安装在 Windows PC 上的 Secure Client的登录脚本、密码缓存、驱动器映射等。对于 SBL，您必须允许 ASA 下载可为 Secure Client启用图形标识和身份验证 (GINA) 的模块。以下程序显示如何启用 SBL：

过程

步骤 1 在组策略 webvpn 或用户名 webvpn 配置模式下，使用 **anyconnect modules** *vpngina* 命令允许 ASA 将用于 VPN 连接的 GINA 模块下载至特定组或用户。

示例：

在以下示例中，用户先进入组策略 *telecommuters* 的组策略属性模式，然后进入组策略 webvpn 配置模式，最后指定字符串 *vpngina*：

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)#anyconnect modules value vpngina
```

步骤 2 检索客户端配置文件 (AnyConnectProfile.tmpl) 的副本。

步骤 3 编辑配置文件，以便指定启用 SBL。以下示例显示配置文件 (AnyConnectProfile.tmpl) 中适用于 Windows 的相关部分：

```
<Configuration>
    <ClientInitialization>
        <UseStartBeforeLogon>false</UseStartBeforeLogon>
```

```
    </ClientInitialization>
```

<UseStartBeforeLogon> 标记确定客户端是否使用 SBL。如要打开 SBL，请用 *true* 替换 *false*。以下示例显示打开 SBL 的标记：

```
<ClientInitialization>
        <UseStartBeforeLogon>true</UseStartBeforeLogon>
    </ClientInitialization>
```

步骤 4 在 webvpn 配置模式下，使用 **profile** 命令保存对 AnyConnectProfile.tmpl 的更改，并为 ASA 上的组或用户更新配置文件。例如：

```
asa1(config-webvpn)#anyconnect profiles sales disk0:/sales_hosts.xml
```

转换 Secure Client 用户消息的语言

ASA 提供语言转换功能，此功能适用于向发起基于浏览器的无客户端 SSL VPN 连接的用户所显示的门户和屏幕，以及向 Cisco AnyConnect VPN 客户端用户所显示的界面。

本节介绍了如何配置 ASA 以对这些用户消息进行语言转换。

了解语言转换

向远程用户显示的功能区域及其消息归入转换域。在 Cisco AnyConnect VPN 客户端的用户界面上显示的所有消息都位于 Secure Client 域中。

ASA 的软件映像包中含有用于 Secure Client 域的转换表模板。您可以导出此模板，这会在您提供的 URL 创建此模板的一个 XML 文件。此文件中的消息字段为空。您可以编辑消息并导入模板，创建位于闪存中的新转换表对象。

您还可以导出现有转换表。创建的 XML 文件将显示您之前编辑的消息。重新导入具有相同语言名称的此 XML 文件将创建一个新版的转换表对象，同时覆盖以前的消息。对 Secure Client 域的转换表的更改会立即向 Secure Client用户显示。

创建转换表

以下程序描述如何创建 Secure Client 域的转换表：

过程

步骤 1 在特权 EXEC 模式下，使用 **export webvpn translation-table** 命令将转换表模板导出到计算机中。

在以下示例中，**show import webvpn translation-table** 命令显示可用的转换表模板和转换表。

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect
```

```
PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
```

接着，用户可以导出 Secure Client 转换域的转换表。创建的 XML 文件的文件名为 *client*，该文件包含有空白的消息字段：

```
hostname# export webvpn translation-table AnyConnect
template tftp://209.165.200.225/client
```

在下一示例中，用户导出名为 *zh* 的转换表，该转换表是先前通过模板导入的。zh 是 Microsoft Internet Explorer 对中文的缩写。

```
hostname# export webvpn translation-table customization
language zh tftp://209.165.200.225/chinese_client
```

步骤 2 编辑转换表 XML 文件。以下示例显示 Secure Client 模板的部分内容。此输出的末尾包含消息 *Connected* 的消息 ID 字段 (msgid) 和消息字符串字段 (msgstr)，该消息会在客户端建立 VPN 连接时显示在 Secure Client GUI 上。完整的模板包含许多的消息字段对：

```
# SOME DESCRIPTIVE TITLE.
# Copyright (C) YEAR THE PACKAGE'S COPYRIGHT HOLDER
# This file is distributed under the same license as the PACKAGE package.
# FIRST AUTHOR <EMAIL@ADDRESS>, YEAR.
#
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: PACKAGE VERSION\n"
"Report-Msgid-Bugs-To: \n"
"POT-Creation-Date: 2006-11-01 16:39-0700\n"
"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"
"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"
"Language-Team: LANGUAGE <LL@li.org>\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=CHARSET\n"
"Content-Transfer-Encoding: 8bit\n"

#: C:\cygwin\home\<user>\cvc\main\Api\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\check\AgentIfc.cpp:22
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp~:20
#: C:\cygwin\home\<user>\cvc\main\Api\save\older\AgentIfc.cpp:22
msgid "Connected"
msgstr ""
```

msgid 包含默认转换。msgid 之后的 msgstr 提供转换。如要创建转换，请在 msgstr 字符串的引号内输入转换的文本。例如，如要使用西班牙语转换选项转换消息“Connected”，请在引号内插入西班牙语文本：

```
msgid "Connected"
msgstr "Conectado"
```

请务必保存文件。

步骤 3 在特权 EXEC 模式下，使用 **import webvpn translation-table** 命令导入转换表。请确保使用与浏览器兼容的语言缩写来指定新转换表的名称。

在以下示例中，导入了 XML 文件 *es-us* - Microsoft Internet Explorer 对美国所使用的西班牙语的缩写。

```
hostname# import webvpn translation-table AnyConnect
language es-us tftp://209.165.200.225/client
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# show import webvpn translation-table
Translation Tables' Templates:
AnyConnect
PortForwarder

customization
keepout
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
es-us AnyConnect
```

删除转换表

如果不再需要转换表，则可以将其删除。

过程

步骤 1 列出现有转换表。

在以下示例中，**show import webvpn translation-table** 命令显示可用的转换表模板和转换表。各种转换表支持法语 (fr)、日语 (ja) 和俄语 (ru) 版本。

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
```

```
  customization
  url-list
  webvpn
Translation Tables:
  fr                    PortForwarder
  fr                    AnyConnect
  fr                    customization
  fr                    webvpn
  ja                    PortForwarder
  ja                    AnyConnect
  ja                    customization
  ja                    webvpn
  ru                    PortForwarder
  ru                    customization
  ru                    webvpn
```

步骤 2 删除不需要的转换表。

revert webvpn translation-table *translationdomain* **language** *language*

其中，*translationdomain* 为上述转换表列表右侧列出的域，*language* 为语言名称，长度为 2 个字符。

必须逐个删除每个转换表。无法使用一个命令删除给定语言版本的所有转换表。

例如，要删除 Secure Client 的法语版本转换表：

```
ciscoasa# revert webvpn translation-table anyconnect language fr
ciscoasa#
```

配置高级 Secure Client SSL 功能

下一节介绍可精细调整 Secure Client SSL VPN 连接的高级功能。

启用重新生成密钥

ASA 与 Secure Client在 SSL VPN 连接上重新生成密钥时，它们会重新协商加密密钥和初始化向量，从而提高连接的安全性。

要允许客户端为特定组或用户在 SSL VPN 连接上重新生成密钥，请在组策略或用户名 webvpn 模式下使用 **anyconnect ssl** rekey 命令。

[no]anyconnect ssl rekey {**method** {**new-tunnel** | **none** | **ssl**} | **time** *minutes*}

- **method new-tunnel** 指定客户端在重新生成密钥的过程中建立新的隧道。
- **method ssl** 指定客户端在重新生成密钥的过程中建立新的隧道。
- **method none** 禁用重新生成密钥。
- **time** *minutes* 用于指定从会话开始或上一次重新生成密钥直到重新生成密钥所需经过的分钟数，取值范围为 1 至 10080（1 周）。

注释 将重新生成密钥的方法配置为 **ssl** 或 **new-tunnel**，用于指定客户端在重新生成密钥的过程中建立新的隧道，而不是在重新生成密钥的过程中进行 SSL 重新协商。有关 **anyconnect ssl rekey** 命令的历史记录，请参阅命令参考。

在以下示例中，对于现有组策略 *sales* 来说，客户端被配置为在重新生成密钥的过程中使用 SSL 进行重新协商，重新生成密钥在会话开始 30 分钟后进行：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
```

配置对等体存活检测

对等体存活检测 (DPD) 可确保 ASA（网关）或客户端可以快速检测到对等体无响应且连接已失败的情况。要启用对等体存活检测 (DPD) 并设置 Secure Client 或 ASA 网关执行 DPD 的频率，请执行以下操作：

注释 当连接在客户端中断时，ASA 不会由于 DPD 或保持连接而无条件地丢弃 Secure Client 会话。仅当存在从 ASA 到客户端的数据流时，ASA 仅会触发 DPD。一旦触发 DPD，它会先对每个子会话 (SSL/DTLS) 进行三次重试，然后再将其断开。

如果那里没有数据流，则不会触发 DPD，ASA 具有硬编码的 5 分钟 TCP 非活动超时，当恰好 5 分钟没有数据或保持连接数据包流时，该超时会自动关闭 SSL/DTLS 隧道连接，无论配置的 VPN 空闲超时设置如何请参阅。断开子会话后，**vpn-idle-timeout** 命令仅负责控制可父会话的最长时间。有关 DPD、保持连接和超时属性的更多详细信息，请参阅 AnyConnect 常见问题解答 - 隧道、DPD 和非活动计时器 (AnyConnect FAQ - Tunnels, DPDs, and Inactivity Timer 。

开始之前

- 此功能仅适用于 ASA 网关与 Secure Client SSL VPN 客户端之间的连接。它不适用于 IPsec，因为 DPD 基于不允许填充的标准实施。
- 如果启用 DTLS，则也要启用对等体存活检测 (DPD)。DPD 允许已失败的 DTLS 连接回退至 TLS。否则，该连接会终止。
- 在 ASA 上启用 DPD 时，可以使用最佳 MTU (OMTU) 功能查找客户端可以成功传输 DTLS 数据包的最大终端 MTU。通过向最大 MTU 发送填充的 DPD 数据包来实施 OMTU。如果从头端接收到负载的正确回显，则接受 MTU 大小。否则，将减小 MTU 并再次发送探测，直到达到协议允许的最小 MTU 为止。

过程

步骤 1 转到所需的组策略。

进入组策略或用户名 webvpn 模式：

```
hostname(config)# group-policy group-policy-name  attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#
```

或，

```
hostname# username username attributes
hostname(config-username)# webvpn
hostname (config-username-webvpn #
```

步骤 2 设置网关端检测。

使用 [**no**] **anyconnect dpd-interval** {[**gateway** {*seconds* | **none**}] 命令。

网关是指 ASA。启用 DPD 并将 ASA 等待客户端数据包的时间间隔指定为从 30 秒（默认）至 3600 秒（1 小时）的范围。建议使用值 300。如果在该时间间隔内未收到任何数据包，则 ASA 将在相同的时间间隔内执行三次 DPD 测试。如果 ASA 未收到客户端的响应，则会断开 TLS/DTLS 隧道。

注释
指定 **none** 会禁用 ASA 执行的 DPD 测试。使用 **no anyconnect dpd-interval** 从配置中移除该命令。

指定 **none** 会禁用 ASA 执行的 DPD 测试。使用 **no anyconnect dpd-interval** 可从配置中删除此命令。

步骤 3 设置客户端检测。

使用 [**no**] **anyconnect dpd-interval** {[**client** {*seconds* | **none**}]} 命令。

客户端是指 Secure Client。启用 DPD 并将客户端执行 DPD 测试的频率指定为从 30 秒（默认）至 3600 秒（1 小时）的范围。建议的值为 30 秒。

指定 **client none** 会禁用客户端执行的 DPD。使用 **no anyconnect dpd-interval** 可从配置中删除此命令。

示例

以下示例为现有组策略销售将 ASA 执行的 DPD 的频率设置为 30 秒，将客户端执行的 DPD 的频率设置为 10 秒：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect dpd-interval gateway 30
hostname(config-group-webvpn)# anyconnect dpd-interval client 10
```

启用保持连接

您可以调整保持连接消息的频率，以确保经由代理、防火墙或 NAT 设备的 SSL VPN 连接保持打开状态，即使设备限制了连接可处于空闲状态的时间也是如此。调整频率还可以确保客户端在远程用户没有主动运行基于套接字的应用（如 Microsoft Outlook 或 Microsoft Internet Explorer）时不会断开并重新连接。

默认情况下启用保持连接功能。如果禁用保持连接功能，发生故障转移事件时，SSL VPN 客户端会话不会被切换到备用设备。

要设置保持连接消息的频率，请在组策略 webvpn 或用户名 webvpn 配置模式下使用 **keepalive** 命令：要从配置中删除此命令并使值得到继承，请使用此命令的 **no** 形式：

[**no**] **anyconnect ssl keepalive** {**none** | *seconds*}

- **none** 禁用客户端保持连接消息。
- *seconds* 使客户端可以发送保持连接消息，并指定发送消息的频率，取值范围为 15 至 600 秒。

在以下示例中，对于现有组策略 *sales*，ASA 被配置为使客户端可以 300 秒（5 分钟）的频率发送保持连接消息：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl keepalive 300
```

使用压缩

对于低带宽连接，压缩可以减小要传输的数据包的大小，从而提高ASA与客户端之间的通信性能。默认情况下，在 ASA 上为全局级别和针对特定组或用户的所有 SSL VPN 连接启用压缩。

注释 在宽带连接上实施压缩时，您必须谨慎考虑压缩依赖于无损连接这一事实。这也正是默认情况下没有在宽带连接上启用压缩的主要原因。

首先必须在全局配置模式下使用 **compression** 命令全局性地打开压缩，然后在组策略和用户名 webvpn 模式下，针对特定组或用户，使用 **anyconnect ssl compression** 命令设置压缩。

全局性地更改压缩

要更改全局压缩设置，请在全局配置模式下使用 anyconnect ssl **compression** 命令：要从配置中删除此命令，请使用此命令的 **no** 形式：

在以下示例中，对所有 SSL VPN 连接全局性地禁用了压缩：

```
hostname(config)# no compression
```

更改组和用户的压缩

如要更改特定组或用户的压缩，请在组策略和用户名 webvpn 模式下使用 anyconnect ssl compression 命令：

[**no**] **anyconnect ssl compression** {**deflate** | **none**}

默认情况下，对于组和用户而言，SSL 压缩被设置为 *deflate*（启用）。

要从配置中删除 **anyconnect ssl compression** 命令，并使该值从全局设置中得到继承，请使用此命令的 **no** 形式：

在以下示例中，对组策略 sales 禁用了压缩：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no anyconnect ssl compression none
```

调整 MTU 大小

您可以在组策略 webvpn 或用户名 webvpn 配置模式下，使用 **anyconnect mtu** 命令调整客户端建立的 SSL VPN 连接的 MTU 大小（从 576 至 1406 个字节）：

[**no**] **anyconnect mtu** *size*

该命令仅影响 Secure Client。旧版思科 SSL VPN 客户端 () 不能调整为不同的 MTU 大小。同时，该命令还影响在 SSL 中建立的客户端连接以及在 SSL 中通过 DTLS 建立的客户端连接。

在默认组策略中，该命令的默认设置为 **no anyconnect mtu**。MTU 大小基于连接使用的接口的 MTU 减去 IP/UDP/DTLS 开销自动进行调整。

例如，运行 ISE 安全状态 AnyConnect 模块时，您可能会收到一条消息，内容为“从安全网关发送的 MTU 配置太小”。如果输入 **anyconnect mtu 1200** 和 **anyconnect ssl df-bit-ignore disable**，则可以避免这些系统扫描错误。

示例

以下示例将组策略 telecommuters 的 MTU 大小配置为 1200 个字节：

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect mtu 1200
```

更新 Secure Client 映像

您可以使用以下程序随时更新 ASA 上的客户端映像。

注释 为了实现 VPN 基础设施的最佳安全性、性能和可管理性，我们建议您定期从防火墙中删除过时的 Secure Client 映像，仅保留最新的所需版本，以防止配置冲突。

过程

步骤 1 在特权 EXEC 模式下使用 **copy** 命令或者使用其他方法，将新的客户端映像复制至 ASA。

步骤 2 如果新的客户端映像文件与已加载的文件拥有相同的文件名，请重新输入配置中的 **anyconnect image** 命令。如果新文件名不同，请使用 [**no**]**anyconnect image**image 命令卸载旧文件。然后使用 **anyconnect image** 命令为映像分配顺序，并使 ASA 加载新的映像。

启用 IPv6 VPN 访问

如果您想要配置 IPv6 访问，则必须使用命令行界面。9.0(x) 版本的 ASA 为其使用 SSL 和 IKEv2/IPsec 协议的外部接口添加了 IPv6 VPN 连接支持。

在启用 SSL VPN 连接的过程中，您可以使用 **ipv6 enable** 命令启用 IPv6 访问。以下内容为在外部接口上启用 IPv6 的 IPv6 连接示例：

```
hostname(config)# interface GigabitEthernet0/0
hostname(config-if)# ipv6 enable
```

如要启用 IPV6 SSL VPN，请执行以下通用操作：

1. 在外部接口上启用 IPv6。
2. 在内部接口上启用 IPv6 和 IPv6 地址。
3. 为客户端分配的 IP 地址配置 IPv6 地址本地池。
4. 配置 IPv6 隧道默认网关。

过程

步骤 1 配置接口：

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 192.168.0.1 255.255.255.0
 ipv6 enable      ; Needed for IPv6.
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.0.1 255.255.0.0
 ipv6 address 2001:DB8::1/32        ; Needed for IPv6.
 ipv6 enable      ; Needed for IPv6.
```

步骤 2 配置“ipv6 local pool”（用于 IPv6 地址分配）：

```
ipv6 local pool ipv6pool 2001:DB8:1:1::5/32 100     ; Use your IPv6 prefix here
```

注释

通过在 ASA 上创建内部地址池，或者通过向 ASA 上的本地用户分配专用地址，您可以将 ASA 配置为向 Secure Client分配 IPv4 地址和/或 IPv6 地址。

步骤 3 将 IPv6 地址池添加至您的隧道组策略（或组策略）：

```
tunnel-group YourTunGrp1 general-attributes  ipv6-address-pool ipv6pool
```

注释
您还必须在此处配置 IPv4 地址池（使用“address-pool”命令）。

步骤 4 配置 IPv6 隧道默认网关：

```
ipv6 route inside ::/0 X:X:X:X::X tunneled
```

SAML 2.0

ASA 支持 SAML 2.0，因此当 VPN 最终用户在专用网络外部 SAAS 应用之间切换时，只能输入一次凭证。

例如，某企业客户已启用 PingIdentity 作为其 SAML 身份提供程序 (IdP) 并且具有已启用了 SAML 2.0 SSO 的 Rally、Salesforce、Oracle OEM、Microsoft ADFS、onelogin 或 Dropbox 账户。当您将 ASA 配置为支持 SAML 2.0 SSO 作为服务提供程序 (SP) 时，最终用户能够登录一次，并有权访问所有这些服务。

此外，还增加了 AnyConnect SAML 支持，因此 AnyConnect 4.4 客户端可以使用 SAML 2.0 访问基于 SAAS 的应用。AnyConnect 4.6 引入了一个增强版的与嵌入浏览器的 SAML 集成，以替换以前版本中的本机（外部）浏览器集成。具有嵌入式浏览器的全新增强版本要求升级到 AnyConnect 4.6（或更高版本）和 ASA 9.7.1.24（或更高版本）、9.8.2.28（或更高版本）或 9.9.2.1（或更高版本）。

ASA 版本 9.17.1/ASDM 版本 7.17.1 引入了对 AnyConnect 4.10.04065（或更高版本）的 AnyConnect VPN SAML 外部浏览器的支持。当您使用 SAML 作为 AnyConnect VPN 连接配置文件的主身份验证方法时，您可以选择在执行 Web 身份验证让 Secure Client 使用本地浏览器而不是 Secure Client 嵌入式浏览器。借助此功能，Secure Client 可支持 WebAuthN 和任何其他基于 SAML 的 Web 身份验证选项，例如单点登录、生物识别身份验证或嵌入式浏览器不可用的其他增强方法。对于 SAML 外部浏览器，您必须执行此处所述的配置：为 SAML 身份验证配置默认操作系统浏览器，第 26 页。

当 SAML 配置为隧道组、默认隧道组或任何其他项目的身份验证方法时，ASA 将启用 SP 。VPN 用户通过访问启用的 ASA 或 SAML IdP 来启动单点登录。下文介绍了上述每种场景。

SAML SP 发起的 SSO

当最终用户通过访问 ASA 来发起登录时，登录行为的过程如下所示：

1. 当 VPN 用户访问或选择已启用 SAML 的隧道组时，最终用户会被重定向至 SAML IdP 进行身份验证。用户将收到提示，除非用户直接访问组 URL，在那种情况下重定向无提示。

   ASA 将生成一个 SAML 身份验证请求，由浏览器将该请求重定向至 SAML IdP。

2. IdP 向最终用户质询凭证，然后最终用户登录。输入的凭证必须满足 IdP 身份验证配置的要求。

3. IdP 响应被发送回浏览器并发布到 ASA 登录 URL。ASA 验证响应以完成登录。

SAML IdP 发起的 SSL

当用户通过访问 IdP 来发起登录时，登录行为的过程如下所示：

1. 最终用户访问 IdP。IdP 根据 IdP 的身份验证配置向最终用户质询凭证。最终用户提交凭证和登录 IdP。
2. 一般情况下，最终用户会获得 IdP 已配置的启用 SAML 的服务列表。最终用户选择 ASA。
3. SAML 响应被发送回浏览器并发布到 ASA 登录 URL。ASA 验证响应以完成登录。

信任圈

ASA 与 SAML 身份提供程序之间的信任关系通过配置的证书建立（ASA 信任点）。

最终用户与 SAML 身份提供程序之间的信任关系通过 IdP 上配置的身份验证建立。

SAML 超时

SAML 断言中有如下 NotBefore 和 NotOnOrAfter：<saml:Conditions NotBefore="2015-03-10T19:47:41Z" NotOnOrAfter="2015-03-10T20:47:41Z">

如果 NotBefore 与 ASA 上配置的 SAML 超时之和早于 NotOnOrAfter，则 SAML 超时将覆盖 NotOnOrAfter。如果 NotBefore + 超时晚于 NotOnOrAfter，则 NotOnOrAfter 将生效。

超时应该非常短，以防超时后重新使用断言。为了使用 SAML 功能，必须使您的 ASA 网络时间协议 (NTP) 服务器与 IdP NTP 服务器同步。

专用网络中的支持

在专用网络中支持基于 SAML 2.0 的服务提供商 IdP。在私有云中部署 SAML IdP 时，ASA 和其他启用 SAML 的服务处于对等位置，并且都在专用网络中。使用 ASA 作为用户与服务之间的网关，可利用受限的匿名 webvpn 会话来处理 IdP 上的身份验证，并转换 IdP 与用户之间的所有流量。当用户登录时，ASA 会使用相应的属性修改会话并存储 IdP 会话。然后，您可以使用专用网络中的服务提供程序而无需再次输入凭证。

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

注释 您不能在专用网络和公共网络之间交换身份验证信息。如果将相同的 IdP 同时用于内部和外部服务提供程序，必须分别进行身份验证。仅内部 IdP 无法用于外部服务：仅外部 IdP 无法用于专用网络中的服务提供程序。

SAML 2.0 的准则和限制

- ASA 支持以下 SAML 身份验证签名：
  - 包含 RSA 和 HMAC 的 SHA1
  - 包含 RSA 和 HMAC 的 SHA2

- ASA 支持 SAML 2.0 重定向-POST 绑定，所有 SAML IdP 也支持此功能。
- ASA 仅用作 SAML SP。在网关模式或对等模式下，它不能用作身份提供程序。
- 此 SAML SSO SP 功能是互斥的身份验证方法。它不能与 AAA 和证书一起使用。
- 不支持基于用户名/密码身份验证、证书身份验证和 KCD 的功能。例如，用户名/密码预填充功能、基于表单的自动登录、基于宏替换的自动登录、KCD SSO 等。
- ASA 支持使用 AnyConnect SAML 身份验证的 VPN 负载均衡。
- 使用 Safari 进行 SAML 身份验证时，请确保您安装了 Safari 更新 14.1.2 或更高版本。
- ASA 管理员需要确保 ASA 与 SAML IdP 之间的时钟同步，从而正确处理身份验证断言并确保正确的超时行为。
- ASA 管理员有责任在 ASA 和 IdP 上维护有效的签名证书，并考虑以下因素：
  - 在 ASA 上配置 IdP 时，必须配置 IdP 签名证书。
  - ASA 不会对从 IdP 接收的签名证书执行吊销检查。
- SAML 断言中有 NotBefore 和 NotOnOrAfter 条件。ASA SAML 配置的**超时**与这两个条件如下交互：
  - 如果 NotBefore 与超时之和早于 NotOnOrAfter，则超时将覆盖 NotOnOrAfter。
  - 如果 NotBefore + 超时晚于 NotOnOrAfter，则 NotOnOrAfter 生效。
  - 如果不存在 NotBefore 属性，ASA 将拒绝登录请求。如果不存在 NotOnOrAfter 属性且未设置 SAML 超时，ASA 将拒绝登录请求。
- ASA 不适用于使用内部 SAML 的部署中的 Duo，由于在双因素身份验证（推送、代码、密码）的质询/响应期间发生 FQDN 更改，这会强制到客户端代理的 ASA 进行身份验证。
- 在嵌入式浏览器中不允许不受信任的服务器证书。
- CLI 或 SBL 型号中不支持嵌入式浏览器 SAML 集成。
- 在网络浏览器中建立的 SAML 身份验证不会与 AnyConnect 共享，反之亦然。
- 根据具体配置，在使用嵌入式浏览器连接到前端时，会使用各种不同的方法。例如，尽管 AnyConnect 相比于 IPv6 连接更喜欢 IPv4 连接，但嵌入式浏览器可能更喜欢 IPv6，或反之亦然。同样，在尝试代理和收到失败后，AnyConnect 可能会回退到没有代理状态，而嵌入式浏览器在尝试代理并收到失败后可能会停止导航。
- 为了使用 SAML 功能，必须使您的 ASA 网络时间协议 (NTP) 服务器与 IdP NTP 服务器同步。
- ASDM 上的 VPN 向导目前不支持 SAML 配置。
- 使用内部 IdP 登录后，您将无法访问包含 SSO 的内部服务器。
- SAML IdP NameID 属性确定用户的用户名，并且用于授权、记帐和 VPN 会话数据库。
- 多情景模式不支持 SAML。

- 不支持通过 SAML 断言接收多个属性。
- Chromebook 不支持使用外部浏览器身份验证的安全客户端 SAML。
- 确保 IdP 在 SAML 响应中包含相应 SAML 请求中接收的中继状态参数。

配置 SAML 2.0 身份提供程序 (IdP)

开始之前

获取 SAML (IdP) 提供程序的登录和注销 URL。您可以从提供商的网站获取这些 URL，或者，他们可能会在元数据文件中提供该信息。

过程

步骤 1 在 webvpn 配置模式下创建 SAML 身份提供程序并进入 webvpn 下的 saml-idp 子模式。

[**no**] **saml idp** *idp-entityID*

idp-entityID - SAML IdP 实体 ID 必须包含 4 到 128 个字符。

要删除 SAML IdP，请使用此命令的 **no** 形式。

步骤 2 配置 IdP URL。

url [**sign-in** | **sign-out**] *value*

value - 这是用于登录 IdP 的 URL 或注销 IdP 时用于重定向的 URL。**sign-in** URL 为必填项，**sign-out** URL 可选。URL 值必须包含 4 到 500 个字符。

步骤 3 （可选）为 VPN 身份验证配置 SAML 服务提供商的基本 URL。此 URL 在 SAML 元数据中使用（会提供给第三方 IdP），以便 IdP 可以将终端用户重定向回 ASA。

base-url *URL*

向第三方 IdP 提供此 URL，用于将最终用户重定向回 ASA。

如果配置了 base-url，则将其用作 **show saml metadata** 中 AssertionConsumerService 和 SingleLogoutService 属性的基本 URL。

如果未配置 base-url，则由 ASA 的 hostname 和 domain-name 决定 URL。例如，当主机名为 `ssl-vpn` 且域名为 `cisco.com` 时，我们使用 `https://ssl-vpn.cisco.com`。

如果输入 **show saml metadata** 时既未配置 base-url 也未配置 hostname/domain-name，则会出现错误。

步骤 4 配置 IdP 与 SP (ASA) 之间的信任点。

trustpoint [**idp** | **sp**] *trustpoint-name*

idp- 指定包含供 ASA 用于验证 SAML 断言的 IdP 证书的信任点。

sp - 指定包含供 IdP 用于验证 ASA 签名或加密 SAML 断言的 ASA (SP) 证书的信任点。

trustpoint-name - 必须是以前配置的信任点。

步骤 5 （可选） 配置 SAML 超时。

timeout assertion *timeout-in-seconds*

如果指定，则在NotBefore和超时秒数之和早于NotOnOrAfter的情况下，此配置会覆盖NotOnOrAfter。

如果不指定，则断言中的 NotBefore 和 NotOnOrAfter 用于确定有效性。

注释
对于配置了现有 SAML IdP 的隧道组，在 webvpn 下对 saml idp CLI 的任何更改仅在对该特定隧道组重新启用SAML时才会应用于该隧道组。配置了超时后，只有在隧道组webvpn属性中重新发出saml identity-provider CLI 后，更新后的超时才会生效。

步骤 6 （可选） 在 SAML 请求中启用或禁用（默认设置）签名。

signature <value>

注释
升级到 SSO 2.5.1 后，默认签名方法从 SHA1 更改为 SHA256，而且通过输入 *value* rsa-sha1、rsa-sha256、rsa-sha384 或 rsa-sha512，还可以配置首选签名方法。

步骤 7 （可选）要设置确定 IdP　是内部网络的标志，请使用 **internal** 命令。然后，ASA 将在网关模式下工作。

步骤 8 使用 **show webvpn saml idp** 查看配置。

步骤 9 使用 **force re-authentication** 使身份提供程序在收到 SAML 身份验证请求时直接进行身份验证而不依赖于以前的安全情景。此设置为默认值；因此，要将其禁用，请使用 **no force re-authentication**。

示例

以下示例配置名为 salesforce_idp 的 IdP 并使用预配置的信任点：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)#saml idp salesforce_idp

ciscoasa(config-webvpn-saml-idp)#url sign-in
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
ciscoasa(config-webvpn-saml-idp)#url sign-out
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect

ciscoasa(config-webvpn-saml-idp)#trustpoint idp salesforce_trustpoint
ciscoasa(config-webvpn-saml-idp)#trustpoint sp asa_trustpoint

ciscoasa(config)#show webvpn saml idp
saml idp salesforce_idp
url sign-in https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
url sign-out https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
trustpoint idp salesforce_trustpoint
trustpoint  sp asa_trustpoint
```

以下网页显示了如何获取 Onelogin 的 URL 的示例

https://onelogin.zendesk.com/hc/en-us/articles/202767260-Configuring-SAML-for-Clarizen

以下网页是如何使用元数据从 OneLogin 查找 URL 的示例。

http://onlinehelp.tableau.com/current/online/en-us/saml_config_onelogin.htm

下一步做什么

如将 ASA 配置为 SAML 2.0 服务提供程序 (SP)，第 26 页中所述，将 SAML 身份验证应用于连接配置文件。

将 ASA 配置为 SAML 2.0 服务提供程序 (SP)

开始之前

IdP 必须事先已配置。请参阅配置 SAML 2.0 身份提供程序 (IdP)，第 24 页。

过程

步骤 1 在 tunnel-group webvpn 子模式下，使用 saml identity-provider 命令分配 IdP。

saml identity-provider *idp-entityID*

idp-entityID - 必须是以前配置的现有 IdP 之一。

要禁用 SAML SP，请使用此命令的 **no** 形式。

步骤 2 启用 SAML 身份验证方法。

authentication saml

示例

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

为 SAML 身份验证配置默认操作系统浏览器

指定 AnyConnect 应使用平台的本地浏览器（操作系统的默认浏览器），还是使用 AnyConnect 中嵌入的浏览器处理 SSO 身份验证过程。

您必须下载 AnyConnect 外部浏览器软件包（例如，*external-sso-4.10.04065-webdeploy-k9.pkg*）并将其上传到 ASA。然后，您可以选择 SAML 登录方法（AnyConnect 的嵌入式浏览器或操作系统的默认浏览器）进行 SAML 身份验证。此捆绑包是一个脚本，允许 VPN 客户端启动默认操作系统 Web

浏览器进行身份验证，与操作系统、浏览器和 VPN 客户端版本无关。只要启用该功能，VPN 客户端版本和外部浏览器软件包版本文件就不需要匹配。

选择默认操作系统浏览器可在您的 VPN 身份验证和其他企业登录之间启用单点登录 (SSO)。如果您想要支持无法在 VPN 客户端的嵌入式浏览器中执行的 Web 身份验证方法（例如生物特征身份验证），则可选择此选项。在选择操作系统的浏览器之前，您必须上传可在浏览器中运行的软件包，以启用 Web 身份验证。

过程

步骤 1 在 webvpn 子模式下，使用 anyconnect external-browser-pkg 命令通过操作系统的默认浏览器启用 AnyConnect SAML 身份验证。

anyconnect external-browser-pkg *path*

要禁用操作系统的默认浏览器进行 SAML 身份验证，请使用此命令的 **no** 形式。

步骤 2 在 tunnel-group webvpn 子模式下，使用 external-browser 命令通过操作系统的默认浏览器启用 AnyConnect SAML 身份验证。

external-browser enable *idp-entityID*

要禁用操作系统的默认浏览器进行 SAML 身份验证，请使用此命令的 **no** 形式。

示例

此示例选择 AnyConnect 外部浏览器软件包的路径，并为 SAML 身份验证启用外部浏览器（操作系统的默认浏览器）。

```
asa(config-webvpn)# anyconnect external-browser-pkg flashshow :
asa(config)# tunnel-group SAML webvpn-attributes
asa(config-tunnel-webvpn)# external-browser enable
asa(config-tunnel-webvpn)#
```

配置证书和 SAML 身份验证

您可以为基于 SAML 的连接配置文件配置证书和 SAML 身份验证，以便验证客户拥有的资产而无需分析特定文件/注册表密钥。基于 SAML 的身份验证可以绑定到已批准的资产和/或用户。您可以将单个证书或多个证书与 SAML 配合用于身份验证。

当 Secure Client 发起连接时，ASA 或 FTD 将在执行 SAML 身份验证之前从终端请求并验证一个或多个证书。

SAML 身份验证完成后，SAML 和证书用户名可以

SAML 身份验证完成后，可以在进入授权阶段之前比较 SAML 和证书用户名。

开始之前

确保在配置证书和 SAML 身份验证之前配置所需的 SAML 设置：

- 获取 SAML (IdP) 提供程序的登录和注销 URL。您可以从提供商的网站获取这些 URL，或者，他们可能会在元数据文件中提供该信息。
- 配置 SAML 身份提供程序和信任点设置。请参阅 配置证书和 SAML 身份验证，第 27 页

过程

步骤 1 要配置证书和 SAML 身份验证，请输入以下命令进入 tunnel-group webvpn-attributes 模式。提示符会更改以表示模式发生更改：

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

步骤 2 要指定想使用的身份验证方法，请输入以下命令：

```
hostname(config-tunnel-webvpn)#authentication authentication_method
```

例如，以下命令同时允许 SAML 和证书身份验证：

```
hostname(config-tunnel-webvpn)#authentication saml certificate
```

以下命令允许证书和 SAML 身份验证：

```
hostname(config-tunnel-webvpn)#authentication certificate saml
```

以下命令同时允许多证书和 SAML 身份验证：

```
hostname(config-tunnel-webvpn)#authentication multiple-certificate saml
```

步骤 3 添加或编辑连接配置文件，然后选择**基本 (Basic)** 连接配置文件属性设置。

步骤 4 要指定证书和 SAML 身份验证的身份验证方法，请从下拉列表中选择 SAML 和证书或多个证书和 SAML。

示例

以下是为 sales_group 连接配置文件配置多个证书和 SAML 身份验证的示例：

```
ciscoasa(config)# tunnel-group sales_group webvpn
ciscoasa(config-tunnel-webvpn)#authentication multiple-certificate saml
```

以 SAML 2.0 和 Onelogin 为例说明

按照此示例，使用您的第三方 SAML 2.0 IdP 代替 Onelogin 信息和命名。

1. 设置 IdP 与 ASA (SP) 之间的时间同步。

```
ciscoasa(config)# ntp server 209.244.0.4
```

2. 按照您的第三方 IdP 提供的程序从 IdP 获取 IdP SAML 元数据。

3. 将 IdP 的签名证书导入信任点。

```
ciscoasa(config)# crypto ca trustpoint onelogin
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# no ca-check
ciscoasa(config-ca-trustpoint)# crypto ca authenticate onelogin
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
quit
INFO: Certificate has the following attributes:
Fingerprint:     85de3781 07388f5b d92d9d14 1e22a549
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

4. 将 SP (ASA) 签名 PKCS12 导入信任点

```
ciscoasa(config)# crypto ca import asa_saml_sp pkcs12 password
Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
quit
INFO: Import PKCS12 operation completed successfully
```

5. 添加 SAML IdP：

```
ciscoasa(config-webvpn)# saml idp https://app.onelogin.com/saml/metadata/462950
```

6. 在 saml-idp 子模式下配置属性：

   配置 IdP 登录 URL 和注销 URL:

```
ciscoasa(config-webvpn-saml-idp)# url sign-in
https://ross.onelogin.com/trust/saml2/http-post/sso/462950
ciscoasa(config-webvpn-saml-idp)# url sign-out
https://ross.onelogin.com/trust/saml2/http-redirect/slo/462950
```

   配置 IdP 信任点和 SP 信任点

```
ciscoasa(config-webvpn-saml-idp)# trustpoint idp onelogin
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_saml_sp
```

   配置无客户端 VPN 基本 URL、SAML 请求签名和 SAML 断言超时：

```
ciscoasa(config-webvpn-saml-idp)# base-url https://172.23.34.222
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 7200
```

7. 为隧道组配置 IdP 并启用 SAML 身份验证。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

8. 显示 ASA 的 SAML SP 元数据：

您可以从 `https://172.23.34.222/saml/sp/metadata/cloud_idp_onelogin` 获取 ASA 的 SAML SP 元数据。在 URL 中，`cloud_idp_onelogin` 是隧道组名称。

9. 按照您的第三方 IdP 提供的程序在您的第三方 IdP 上配置 SAML SP。

排除 SAML 2.0 故障

使用 **debug webvpn saml***value* 调试 SAML 2.0 行为。根据 *value*，系统将显示以下 SAML 消息：

- 8 - 错误
- 16 - 警告和错误
- 128 或 255 - 调试、警告和错误

监控 Secure Client 连接

如要查看有关活动会话的信息，请使用 **show vpn-sessiondb** 命令：

命令	目的
show vpn-sessiondb	显示有关活动会话的信息。
vpn-sessiondb logoff	注销 VPN 会话。
show vpn-sessiondb anyconnect	扩充 VPN 会话摘要，以显示 OSPFv3 会话信息。
show vpn-sessiondb ratio encryption	显示隧道数量和 Suite B 算法（如 AES-GCM-128、AES-GCM AES-GCM-256、AES-GMAC-128 等）的百分比。

注释 **AnyConnect 父隧道**

AnyConnect 父隧道没有分配的 IP 地址。

这是在协商期间创建的主会话，用于设置因网络连接问题或休眠而需要重新连接的会话令牌。根据连接机制，Cisco Adaptive Security Appliance (ASA) 将会话列为无客户端（通过门户的 WebLaunch）或父项（独立 AnyConnect）。

AnyConnect 父项表示客户端未主动连接时的会话。实际上，它的工作原理类似于 Cookie，因为它是 ASA 上映射到来自特定客户端的连接的数据库条目。如果客户端休眠/休眠，则隧道（IPsec/互联网密钥交换 (IKE)/传输层安全 (TLS)/数据报传输层安全 (DTLS) 协议）将被删除，但父项会保留，直到空闲计时器或最大连接数时间生效。这允许用户重新连接而无需重新进行身份验证。

示例

Inactivity 字段显示自 Secure Client 会话断开连接以来所经过的时间。如果会话处于活动状态，会在该字段中显示 00:00m:00s。

```
hostname# show vpn-sessiondb

Session Type: SSL VPN Client

Username     : lee
Index        : 1                        IP Addr      : 209.165.200.232
Protocol     : SSL VPN Client           Encryption   : 3DES
Hashing      : SHA1                     Auth Mode    : userPassword
TCP Dst Port : 443                      TCP Src Port : 54230
Bytes Tx     : 20178                    Bytes Rx     : 8662
Pkts Tx      : 27                       Pkts Rx      : 19
Client Ver   : Cisco STC 1.1.0.117
Client Type  : Internet Explorer
Group        : DfltGrpPolicy
Login Time   : 14:32:03 UTC Wed Mar 20 2007
Duration     : 0h:00m:04s
Inactivity    : 0h:00m:04s
Filter Name  :

hostname# vpn-sessiondb logoff
INFO: Number of sessions of type "" logged off : 1

hostname# vpn-sessiondb logoff name tester
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "tester" logged off : 1
```

注销 AnyConnect VPN 会话

如要注销所有的 VPN 会话，请在全局配置模式下使用 **vpn-sessiondb logoff** 命令：

以下示例注销了所有的 VPN 会话：

```
hostname# vpn-sessiondb logoff
INFO: Number of sessions of type “” logged off : 1
```

您可以使用 name 参数或 index 参数注销单个会话：

vpn-sessiondb logoff name *name*
vpn-sessiondb logoff index *index*

处于非活动状态时间最长的会话会被标记为空闲（并自动注销），这样就不会达到许可证容量，而让新用户可以登录。如果该会话稍后恢复，则会从非活动列表中删除。

您可以在 **show vpn-sessiondb anyconnect** 命令的输出中找到用户名和索引号（按客户端映像的顺序建立）。以下示例显示用户名 *lee* 和索引号 *1*。

```
hostname# show vpn-sessiondb anyconnect

Session Type: AnyConnect
```

```
Username     : lee                    Index        : 1
Assigned IP  : 192.168.246.1           Public IP    : 10.139.1.2
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 11079                  Bytes Rx     : 4942
Group Policy : EngPolicy            Tunnel Group : EngGroup
Login Time   : 15:25:13 EST Fri Jan 28 2011
Duration     : 0h:00m:15s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

以下示例使用 **vpn-session-db logoff** 命令的 **name** 选项终止会话：

```
hostname# vpn-sessiondb logoff name lee
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name “lee” logged off : 1

hostname#
```

Secure Client 连接的功能历史记录

下表列出了此功能的版本历史记录。

表 *2: Secure Client* 连接的功能历史记录

功能名称	版本	功能信息
Secure Client 连接	7.2(1)	引入或修改了以下命令：authentication eap-proxy、authentication ms-c authentication ms-chap-v2、authentication pap、l2tp tunnel hello、vpn-tunnel-protocol l2tp-ipsec。
IPsec IKEv2	8.4(1)	添加了 IKEv2，以支持用于 Secure Client 和 LAN 间 的 IPsec IKEv

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。