

在 ASA 上用 ASDM 配置 SSL VPN Client (SVC) 的示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[网络图](#)

[配置前的任务](#)

[规则](#)

[在 ASA 上配置 SSL VPN Client](#)

[第 1 步. 在 ASA 上启用 WebVPN 访问](#)

[第 2 步. 在 ASA 上安装并启用 SSL VPN Client](#)

[第 3 步. 在客户端上启用 SVC 安装](#)

[第 4 步. 启用重新生成密钥参数](#)

[结果](#)

[自定义配置](#)

[第 1 步. 创建自定义组策略](#)

[第 2 步. 创建自定义隧道组](#)

[第 3 步. 创建用户并将该用户添加到自定义组策略中](#)

[验证](#)

[验证](#)

[配置](#)

[命令](#)

[故障排除](#)

[SVC 错误](#)

[SVC 是否与 ASA 建立了安全会话？](#)

[是否正在成功地建立和终止安全会话？](#)

[检查 WebVPN 配置文件中的 IP 池](#)

[提示](#)

[命令](#)

[相关信息](#)

简介

通过安全套接字层 (SSL) 虚拟专用网络 (VPN) 技术，可以使用下面这些方法之一从任何位置安全地连接到内部公司网络：

- **无客户端 SSL VPN (WebVPN)** — 提供一个远程客户端，它要求通过启用了 SSL 的 Web 浏览

器才能访问公司局域网 (LAN) 上的 HTTP 或 HTTPS Web 服务器。此外，利用无客户端 SSL VPN 还可以通过公用 Internet 文件系统 (CIFS) 协议浏览 Windows 文件。Outlook Web Access (OWA) 就是 HTTP 访问的一个示例。请参阅 [ASA 上的无客户端 SSL VPN \(WebVPN\) 配置示例](#) 详细了解无客户端 SSL VPN。

- **瘦客户端 SSL VPN (端口转发)** — 提供一个远程客户端，它下载基于 Java 的小程序，并允许以安全方式访问使用静态端口号的传输控制协议 (TCP) 应用程序。安全访问的示例包括邮局协议 (POP3)、简单邮件传输协议 (SMTP)、Internet 邮件访问协议 (IMAP)、安全 Shell (ssh) 和 Telnet。由于本地计算机上的文件发生更改，因此用户必须有本地管理权限才能使用此方法。这种 SSL VPN 方法不能与使用动态端口分配的应用程序 (如某些文件传输协议 (FTP) 应用程序) 配合工作。请参阅 [在 ASA 上用 ASDM 配置瘦客户端 SSL VPN \(WebVPN\) 的示例](#) 以详细了解瘦客户端 SSL VPN。**注意：** 不支持用户数据报协议 (UDP)。
- **SSL VPN Client (隧道模式)** — 向远程工作站下载一个小客户端，并允许以安全方式完全访问公司内部网络中的资源。可以将 SSL VPN Client (SVC) 永久下载到远程工作站，也可以在安全会话关闭后删除该客户端。

本文档介绍如何使用自适应安全管理器 (ASDM) 在自适应安全设备 (ASA) 上配置 SVC。[结果](#) 部分中列出了此配置所产生的命令行。

[先决条件](#)

[要求](#)

尝试进行此配置之前，请确保满足以下要求：

- Cisco 自适应安全设备软件 7.1 版及更高版本支持 SVC
- 在所有远程工作站上都有本地管理权限
- 在远程工作站上有 Java 和 Activex 控件
- 端口 443 在连接路径中的任何位置都不受到阻止

[使用的组件](#)

本文档中的信息基于以下软件和硬件版本：

- Cisco 自适应安全设备软件版本 7.2(1)
- Cisco 自适应安全管理器 5.2(1)
- Cisco 自适应安全设备 5510 系列
- Microsoft Windows XP Professional SP 2

本文档中的信息在实验室环境中形成。本文档中使用的所有设备都重置为其默认配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。此配置中使用的所有 IP 地址都是从实验室环境中的 RFC 1918 地址挑选而出的；这些 IP 地址在 Internet 上不可路由，仅做测试用途。

[网络图](#)

本文档使用此部分所述的网络配置。

远程用户通过启用了 SSL 的 Web 浏览器连接到 ASA 的 IP 地址。身份验证成功后，将 SVC 下载到客户端计算机，随后用户即可使用加密的安全会话完全访问公司网络上允许的所有资源。

[配置前的任务](#)

开始之前，请完成以下这些任务：

- 要使 ASDM 可配置 ASA，请参阅[允许 ASDM 进行 HTTPS 访问](#)。要访问 ASDM 应用程序，请从管理站点上使用启用了 SSL 的 Web 浏览器，并输入 ASA 设备的 IP 地址。例如：https://inside_ip_address，其中 inside_ip_address 是 ASA 的地址。加载 ASDM 后，即可开始配置 SVC。
- 从 [Cisco 软件下载](#) ([仅限注册用户](#)) 网站将 SSL VPN Client 软件包 (sslclient-win*.pkg) 下载到从中访问 ASDM 应用程序的管理站点的本地硬盘驱动器。

除非更换端口号，否则无法在同一 ASA 接口上启用 WebVPN 和 ASDM。如果希望两种技术使用同一设备上的相同端口（端口 443），则可以在 [内部接口](#) 上启用 ASDM，并在外部接口上启用 WebVPN。

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[在 ASA 上配置 SSL VPN Client](#)

要在 ASA 上配置 SSL VPN Client，请完成以下这些步骤：

1. [在 ASA 上启用 WebVPN 访问](#)
2. [在 ASA 上安装并启用 SSL VPN Client](#)
3. [在客户端上启用 SVC 安装](#)
4. [启用重新生成密钥参数](#)

[第 1 步. 在 ASA 上启用 WebVPN 访问](#)

要在 ASA 上启用 WebVPN 访问，请完成以下这些步骤：

1. 在 ASDM 应用程序中，单击 **Configuration**，然后单击 VPN。
2. 展开 **WebVPN**，然后选择 WebVPN Access。
3. 选择要为其启用 WebVPN 的接口，然后单击 **Enable**。

[第 2 步. 在 ASA 上安装并启用 SSL VPN Client](#)

要在 ASA 上安装并启用 SSL VPN Client，请完成以下这些步骤：

1. 单击 **Configuration**，然后单击 VPN。
2. 在导航窗格中，展开 **WebVPN**，然后选择 SSL VPN Client。
3. 单击 **Add**。此时出现 Add SSL VPN Client Image 对话框。
4. 单击 **Upload** 按钮。此时出现 Upload Image 对话框。
5. 单击 **Browse Local Files** 按钮在本地计算机上查找文件，或单击 **Browse Flash** 按钮在闪存文件系统上查找文件。
6. 找到要上载的客户端映像文件，然后单击 **OK**。
7. 单击 **Upload File**，然后单击 **Close**。

8. 客户端映像加载到闪存后，选中 **Enable SSL VPN Client** 复选框，然后单击 Apply。**注意：**如果收到错误消息，则请确认启用了 WebVPN 访问。在导航窗格中，展开 **WebVPN**，然后选择 WebVPN Access。选择要为其配置访问的接口，然后单击 **Enable**。
9. 单击 **Save**，然后单击 **Yes** 接受更改。

第 3 步. 在客户端上启用 SVC 安装

要在客户端上启用 SVC 安装，请完成以下这些步骤：

1. 在导航窗格中，展开 **IP Address Management**，然后选择 IP Pools。
2. 单击 **Add**，在 Name、Starting IP Address、Ending IP Address 和 Subnet Mask 字段中输入值。对 Starting IP Address 和 Ending IP Address 字段输入的 IP 地址必须来自内部网络的子网。
3. 单击 **OK**，然后单击 Apply。
4. 单击 **Save**，然后单击 **Yes** 接受更改。
5. 在导航窗格中，展开 **IP Address Management**，然后选择 Assignment。
6. 选中 **Use internal address pools** 复选框，然后取消选中 Use authentication server 和 Use DHCP 复选框。
7. 单击 **Apply**。
8. 单击 **Save**，然后单击 **Yes** 接受更改。
9. 在导航窗格中，展开 **General**，然后选择 Tunnel Group。
10. 选择要管理的隧道组，然后单击 **Edit**。
11. 单击 **Client Address Assignment** 选项卡，然后从 Available Pools 列表中选择新创建的 IP 地址池。
12. 单击 **Add**，然后单击 **OK**。
13. 在 ASDM 应用程序窗口中，单击 **Apply**。
14. 单击 **Save**，然后单击 **Yes** 接受更改。

第 4 步. 启用重新生成密钥参数

启用重新生成密钥参数：

1. 在导航窗格中，展开 **General**，然后选择 Group Policy。
2. 选择要向此客户端组应用的策略，然后单击 **Edit**。
3. 在 General 选项卡下，取消选中 Tunneling Protocols 的 **Inherit** 复选框，然后选中 WebVPN 复选框。
4. 单击 **WebVPN** 选项卡，单击 SSL VPN Client 选项卡，然后选择以下这些选项：对于 Use SSL VPN Client 选项，取消选中 **Inherit** 复选框，然后单击 Optional 单选按钮。通过此选择，远程客户端可选择是否下载 SVC。Always 选择确保在每个 SSL VPN 连接期间将 SVC 下载到远程工作站。对于 Keep Installer on Client System 选项，取消选中 **Inherit** 复选框，然后单击 Yes 单选按钮。通过此操作，SVC 软件可保留在客户端计算机上；因此，不必在每次进行连接时都要求 ASA 将 SVC 软件下载到客户端。对于经常访问企业网络的远程用户而言，此选项是一个很好的选择。对于 Renegotiation Interval 选项，取消选中 **Inherit** 框，取消选中 Unlimited 复选框，然后输入重新生成密钥之前经过的分钟数。通过设置密钥有效时间限制可增强安全性。对于 Renegotiation Method 选项，取消选中 **Inherit** 复选框，然后单击 SSL 单选按钮。重新协商可以使用当前的 SSL 隧道或为重新协商显式创建的新隧道。此时 SSL VPN Client 属性的配置应如下图所示：
5. 单击 **OK**，然后单击 Apply。

6. 单击 **Save** , 然后单击 **Yes** 接受更改。

结果

ASDM 创建了以下这些命令行配置：

```
ciscoasa
ciscoasa(config)#show run ASA Version 7.2(1) ! hostname
ciscoasa domain-name cisco.com enable password
9jNfZuG3TC5tCVH0 encrypted names dns-guard ! interface
Ethernet0/0 nameif outside security-level 0 ip address
172.22.1.160 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 10.2.2.1
255.255.255.0 passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive dns server-group DefaultDNS domain-name
cisco.com no pager logging enable logging asdm
informational mtu outside 1500 mtu inside 1500 mtu DMZ1
1500 mtu Mgt 1500 ip local pool CorporateNet 10.2.2.50-
10.2.2.60 mask 255.255.255.0 icmp permit any outside
asdm image disk0:/asdm521.bin no asdm history enable arp
timeout 14400 global (outside) 1 interface nat (inside)
1 0 0 route outside 0.0.0.0 0.0.0.0 172.22.1.1 1 timeout
xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323
0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute !
!--- Group Policy Statements group-policy GroupPolicy1
internal group-policy GroupPolicy1 attributes vpn-
tunnel-protocol IPSec l2tp-ipsec webvpn !--- Enable the
SVC for WebVPN webvpn svc enable svc keep-installer
installed svc rekey time 30 svc rekey method ssl !
username cisco password 53QNetqK.Kqqfshe encrypted
privilege 15 ! http server enable http 10.2.2.0
255.255.255.0 inside ! no snmp-server location no snmp-
server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart !--- Tunnel
Group and Group Policy using the defaults here tunnel-
group DefaultWEBVPNGroup general-attributes address-pool
CorporateNet default-group-policy GroupPolicy1 ! no vpn-
addr-assign aaa no vpn-addr-assign dhcp ! telnet timeout
5 ssh 172.22.1.0 255.255.255.0 outside ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect rsh inspect rtsp inspect esmtp
inspect sqlnet inspect skinny inspect sunrpc inspect
xdmcp inspect sip inspect netbios inspect tftp !
service-policy global_policy global !--- Enable webvpn
and the select the SVC client webvpn enable outside svc
image disk0:/sslclient-win-1.1.1.164.pkg 1 svc enable !-
-- Provide list for access to resources url-list
ServerList "E-Commerce Server1" http://10.2.2.2 1 url-
list ServerList "BrowseServer" cifs://10.2.2.2 2 tunnel-
group-list enable prompt hostname context
Cryptochecksum:80a1890a95580dca11e3aee200173f5f : end
```

自定义配置

在 [ASA 上配置 SSL VPN Client](#) 中介绍的过程对于组策略和隧道组都使用 ASA 默认名称，分别为 (*GroupPolicy1*) 和 (*DefaultWebVPNGroup*)，如下图所示：

以下过程介绍如何创建自己的自定义组策略和隧道组，并根据组织的安全策略将其联系在一起。

要自定义配置，请完成以下这些步骤：

1. [创建自定义组策略](#)
2. [创建自定义隧道组](#)
3. [创建用户并将该用户添加到自定义组策略中](#)

[第 1 步. 创建自定义组策略](#)

要创建自定义组策略，请完成以下这些步骤：

1. 单击 **Configuration**，然后单击 VPN。
2. 展开 **General**，然后选择 Group Policy。
3. 单击 **Add**，然后选择 Internal Group Policy。
4. 在 Name 字段中，输入组策略的名称。在本示例中，组策略名称已更改为 *SalesGroupPolicy*。
5. 在 General 选项卡下，取消选中 Tunneling Protocols 的 **Inherit** 复选框，然后选中 WebVPN 复选框。
6. 单击 **WebVPN** 选项卡，然后单击 SSL VPN Client 选项卡。在此对话框中，还可以对 SSL VPN Client 的行为做出选择。
7. 单击 **OK**，然后单击 Apply。
8. 单击 **Save**，然后单击 **Yes** 接受更改。

[第 2 步. 创建自定义隧道组](#)

要创建自定义隧道组，请完成以下这些步骤：

1. 单击 **Configuration** 按钮，然后单击 VPN。
2. 展开 **General**，然后选择 Tunnel Group。
3. 单击 **Add**，然后选择 WebVPN Access。
4. 在 Name 字段中，输入隧道组的名称。在本示例中，隧道组名称已更改为 *SalesForceGroup*。
5. 单击 **Group Policy** 下拉箭头，然后选择新创建的组策略。此时组策略和隧道组即相关联。
6. 单击 **Client Address Assignment** 选项卡，然后输入 DHCP Server 信息，或从本地创建的 IP 池进行选择。
7. 单击 **OK**，然后单击 Apply。
8. 单击 **Save**，然后单击 **Yes** 接受更改。

[第 3 步. 创建用户并将该用户添加到自定义组策略中](#)

要创建用户并将该用户添加到自定义组策略中，请完成以下这些步骤：

1. 单击 **Configuration**，然后单击 VPN。
2. 展开 **General**，然后选择 Users。

3. 单击 **Add**，然后输入用户名和口令信息。
4. 单击 **VPN Policy** 选项卡。确保新创建的组策略显示在 Group Policy 字段中。此用户继承新组策略的所有特性。
5. 单击 **OK**，然后单击 **Apply**。
6. 单击 **Save**，然后单击 **Yes** 接受更改。

验证

使用本部分可确认配置能否正常运行。

验证

使用以下方法之一实现 SSL VPN Client 的身份验证：

- Cisco 安全 ACS 服务器 (Radius)
- NT 域
- Active Directory
- 一次性密码
- 数字证书
- 智能卡
- 本地 AAA 身份验证

本文档使用 ASA 设备上创建的本地帐户。

注意： 如果可适应安全工具有共享同样CA的多个信任点，只有共享这些信任点的之一CA可以用于验证用户证书。

配置

要用远程客户端连接到 ASA，请向启用了 SSL 的 Web 浏览器的地址字段输入 **https://ASA_outside_address**。ASA_outside_address 是 ASA 的外部 IP 地址。如果配置成功，则会出现 Cisco Systems SSL VPN Client 窗口。

注意： 只有在从 ASA 接受证书后以及将 SSL VPN Client 下载到远程站点后，才会出现 Cisco Systems SSL VPN Client 窗口。如果未出现该窗口，请确保未将其最小化。

命令

有若干 **show** 命令与 WebVPN 关联。可以在命令行界面 (CLI) 上执行这些命令以显示统计信息和其他信息。有关 **show** 命令的详细信息，请参阅[验证 WebVPN 配置](#)。

注意： [命令输出解释程序 \(仅限注册用户\)](#) (OIT) 支持某些 **show** 命令。使用 OIT 可查看对 **show** 命令输出的分析。

故障排除

使用本部分可排除配置故障。

SVC 错误

问题

在身份验证期间可能会收到此错误消息：

```
"The SSL VPN connection to the remote peer was disrupted and could not be automatically re-established. A new connection requires re-authentication and must be restarted manually. Close all sensitive networked applications."
```

解决方案

如果计算机上正在运行防火墙服务，则可能会中断身份验证。停止服务，然后重新连接客户端。

SVC 是否与 ASA 建立了安全会话？

确保 SSL VPN Client 与 ASA 建立了安全会话：

1. 单击 **Monitoring**。
2. 展开 **VPN Statistics**，然后选择 **Sessions**。
3. 从 **Filter By** 下拉菜单中，选择 **SSL VPN Client**，然后单击 **Filter** 按钮。此时会话列表中应显示您的配置。

是否正在成功地建立和终止安全会话？

可以查看实时日志以确保正在成功地建立和终止会话。查看会话日志：

1. 单击 **Monitoring**，然后单击 **Logging**。
2. 选择 **Real-time Log Viewer** 或 **Log Buffer**，然后单击 **View**。**注意：**要仅显示来自某个特定地址的会话，请按地址过滤。

检查 WebVPN 配置文件中的 IP 池

```
%ASA-3-722020: Group group User user-name IP IP_address No address available for SVC connection
```

没有地址可供分配给 SVC 连接。因此，请在配置文件中分配 IP 池地址。

如果创建新的连接配置文件，则要配置别名或 `group-url` 以访问此连接配置文件。否则，所有 SSL 尝试都将采用没有 IP 池与其关联的默认 WebVPN 连接配置文件。设置此命令以使用默认的连接配置文件，并在其上放置 IP 池。

提示

- 请确保通过分配给远程客户端的 IP 地址池实现正确路由。此 IP 地址池应来自 LAN 上的子网。还可以使用 DHCP 服务器或身份验证服务器分配 IP 地址。
- ASA 创建默认隧道组 (*DefaultWebVPNGroup*) 和默认组策略 (*GroupPolicy1*)。如果创建新组和策略，请确保根据网络的安全策略应用这些值。
- 如果要允许通过 CIFS 浏览 Windows 文件，则在 **Configuration > VPN > WebVPN > Servers and URLs** 下输入 WINS (NBNS) 服务器。此技术使用 CIFS 选择。

命令

有若干 **debug** 命令与 WebVPN 关联。有关这些命令的详细信息，请参阅[使用 WebVPN Debug 命令](#)。

注意：使用 **debug** 命令可能会对 Cisco 设备造成负面影响。使用 **debug** 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

[相关信息](#)

- [ASA 上的无客户端 SSL VPN \(WebVPN\) 配置示例](#)
- [在 ASA 上用 ASDM 配置瘦客户端 SSL VPN \(WebVPN\) 的示例](#)
- [使用 ASDM 和 NTLMv1 配置具有 WebVPN 和单点登录的 ASA 示例](#)
- [Cisco ASA 5500 系列自适应安全设备](#)
- [技术支持和文档 - Cisco Systems](#)