ASA 7.2(2)：SSL VPN客户端(SVC)单臂公共互联网的VPN配置示例

目录

简介

本文档介绍了如何设置自适应安全设备 (ASA) 7.2.2 以执行单臂 SSL VPN。此设置适用于 ASA 不允许分割隧道并且用户必须先直接连接到 ASA 然后才能访问 Internet 的特定案例。

注意： 在 ASA 版本 7.2.2 中，same-security-traffic permit 配置模式命令中的 **intra-interface** 关键字将允许所有数据流出入相同接口（不仅 IPsec 数据流）。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 集线器 ASA 安全设备需要运行版本 7.2.2
- Cisco SSL VPN客户端(SVC) 1.x**注意：** 请从 Cisco 软件下载中下载 SSL VPN Client 程序包 (sslclient-win*.pkg)（仅限仅限注册用户）。将 SVC 复制到 ASA 上的闪存中。SVC 将被下载到远程用户计算机中，以建立与 ASA 的 SSL VPN 连接。有关详细信息，请参阅 *Cisco 安全设备命令行配置指南 7.2 版* 的安装 SVC 软件部分。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本 7.2(2) 的 Cisco 5500 系列自适应安全设备 (ASA)
- 适用于 Windows 1.1.4.179 的 Cisco SSL VPN Client 版本
- 运行 Windows 2000 Professional 或 Windows XP 的 PC
- Cisco 自适应安全设备管理器 (ASDM) 版本 5.2(2)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

SSL VPN 客户端 (SVC) 是一种 VPN 隧道技术，这种技术让远程用户可以利用 IPsec VPN 客户端的优势，而无需网络管理员在远程计算机上安装和配置 IPsec VPN 客户端。SVC 使用远程计算机上已经具有的 SSL 加密以及安全设备的 WebVPN 登录和身份验证。

要建立 SVC 会话，远程用户在浏览器中输入安全设备的 Webvpn 接口的 IP 地址，然后浏览器即会连接到此接口并显示 Webvpn 登录屏幕。如果用户完成登录并通过身份验证，并且安全设备将用户识别为要求 SVC，则它会将 SVC 下载到远程计算机。如果安全设备将用户识别为可以选择使用 SVC，安全设备会将 SVC 下载到远程计算机，同时在用户屏幕上显示一个用于跳过 SVC 安装的链接。

下载完成以后，SVC 将自行安装和配置，然后当连接终止时，SVC 会在远程计算机中保留或卸载自己（根据配置）。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

使用 ASDM 5.2(2) 配置 ASA 7.2(2)

本文档假设基本配置（例如接口配置）已完成并且可以正常工作。

注意： 要使 ASDM 可配置 ASA，请参阅允许 ASDM 进行 HTTPS 访问。

注意： 除非更换端口号，否则无法在同一 ASA 接口上启用 WebVPN 和 ASDM。有关详细信息，请参阅在相同 ASA 接口上同时启用 Webvpn 和 ASDM。

要在 ASA 的单接口上配置 SSL VPN，请执行以下步骤：

1. 选择 **Configuration > Interfaces**，并选中 Enable traffic between two or more hosts connected to the same interface 复选框以允许 SSL VPN 数据流出入相同接口。
2. 单击 **Apply**。**注意：** 以下是等效的 CLI 配置命令：
3. 选择 **Configuration > VPN > IP Address Management > IP Pools > Add** 以创建名为 *vpnpool* 的 IP 地址池。
4. 单击 **Apply**。**注意：** 以下是等效的 CLI 配置命令：
5. 启用 Webvpn：选择 **Configuration > VPN > WebVPN > WebVPN Access**，然后选择外部接口。单击 **Enable**。选中 **Enable Tunnel Group Drop-down List on WebVPN Login Page** 复选框以允许用户从登录页中选择其相应用户组。单击 **Apply**。选择 **Configuration > VPN > WebVPN > SSL VPN Client > Add** 以便从 ASA 闪存中添加 SSL VPN 客户端镜像。单击 **Ok**。单击 **Ok**。单击 **SSL VPN Client** 复选框。**注意：** 以下是等效的 CLI 配置命令：
6. 配置组策略：选择 **Configuration > VPN > General > Group Policy > Add (Internal Group Policy)** 以创建名为 *clientgroup* 的内部组策略。单击 **General** 选项卡，然后选中 WebVPN 复选框以启用 WebVPN 作为隧道协议。单击 **Client Configuration** 选项卡，然后单击 General Client Parameters 选项卡。从 Split Tunnel Policy 下拉列表中选择 **Tunnel All Networks** 以允许远程 PC 的所有数据包通过安全隧道。单击 **WebVPN > SSLVPN Client** 选项卡，然后选择以下选项：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。通过此选项，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 单选按钮使用此选项，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。**注意：** 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。**注意：** 重新协商可以使用当前的 SSL 隧道或专为重新协商创建的新隧道。此时 SSL VPN Client 属性的配置应如下图所示：单击 **OK**，然后单击 Apply。**注意：** 以下是等效的 CLI 配置命令：
7. 选择 **Configuration> VPN >General > Users >Add** 以创建新用户帐户 *ssluser1*。
8. 单击 **OK**，然后单击 Apply。**注意：** 以下是等效的 CLI 命令：
9. 选择 **Configuration > Properties > AAA Setup > AAA Servers Groups > Edit**。
10. 选择默认服务器组 *LOCAL*，然后单击 **Edit**。
11. 在 Edit LOCAL Server Group 对话框中，单击 **Enable Local User Lockout** 复选框，然后在 Maximum Attempts 文本框中输入 16。
12. 单击 **Ok**。**注意：** 以下是等效的 CLI 命令：
13. 配置隧道组：选择 **Configuration > VPN > General > Tunnel Group > Add(WebVPN access)** 以创建名为 *sslgroup* 的新隧道组。单击 **General** 选项卡，然后单击 Basic 选项卡。从 Group Policy 下拉列表中选择 **clientgroup** 。单击 **Client Address Assignment** 选项卡，然后单击 Add 以分配可用地址池 *vpnpool*。单击 **WebVPN** 选项卡，然后单击 Group Aliases and URLs 选项卡。在参数框中键入别名，然后单击 **Add** 以将其添加到登录页的组名列表中。单击 **OK**，然后单击 Apply。**注意：** 以下是等效的 CLI 配置命令：
14. 配置 NAT：选择 **Configuration > NAT > Add > Add Dynamic NAT Rule** 以允许将来自内部网络的数据流转换为外部 IP 地址 172.16.1.5 的数据流。单击 **Ok**。选择 **Configuration > NAT > Add > Add Dynamic NAT Rule** 以允许将来自外部网络 192.168.10.0 的数据流转换为外部 IP 地址 172.16.1.5 的数据流。单击 **Ok**。单击 **Apply**。**注意：** 以下是等效的 CLI 配置命令：

ASA 7.2(2) CLI 配置

Cisco ASA 7.2(2)

```
ciscoasa#show running-config : Saved : ASA Version
7.2(2) ! hostname ciscoasa enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0
nameif inside security-level 100 ip address
10.77.241.142 255.255.255.192 ! interface Ethernet0/1
nameif outside security-level 0 ip address 172.16.1.1
255.255.255.0 ! interface Ethernet0/2 shutdown no nameif
no security-level no ip address ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive same-security-traffic permit intra-
interface !--- Command that permits the SSL VPN traffic
to enter !--- and exit the same interface. access-list
100 extended permit icmp any any pager lines 24 mtu
inside 1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254 !--- The address pool for
the SSL VPN Clients. no failover icmp unreachable rate-
limit 1 burst-size 1 asdm image disk0:/asdm-522.bin no
asdm history enable arp timeout 14400 global (outside) 1
172.16.1.5 !--- The global address for Internet access
used by VPN Clients. !--- Note: Uses an RFC 1918 range
for lab setup. !--- Apply an address from your public
range provided by your ISP. nat (inside) 1 0.0.0.0
0.0.0.0 !--- The NAT statement to define what to encrypt
!--- (the addresses from vpn-pool). nat (outside) 1
192.168.10.0 255.255.255.0 access-group 100 in interface
outside route outside 0.0.0.0 0.0.0.0 172.16.1.2 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 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02: timeout uauth 0:05:00 absolute
group-policy clientgroup internal !--- Create an
internal group policy "clientgroup." group-policy
clientgroup attributes vpn-tunnel-protocol webvpn !---
Enable webvpn as tunneling protocol. split-tunnel-policy
tunnelall !--- Encrypt all the traffic coming from the
SSL VPN Clients. webvpn svc required !--- Activate the
SVC under webvpn mode svc keep-installer installed !---
When the security appliance and the SVC perform a rekey,
they renegotiate !--- the crypto keys and initialization
vectors, increasing the security of !--- the connection.
svc rekey time 30 --- Command that specifies the number
of minutes from the start of the !--- session until the
rekey takes place, from 1 to 10080 (1 week). svc rekey
method ssl !--- Command that specifies that SSL
renegotiation takes place during SVC rekey. username
ssluser1 password ZRhW85jZqEaVd5P. encrypted !--- Create
an user account "ssluser1." aaa local authentication
attempts max-fail 16 !--- Enable the AAA local
authentication. http server enable http 0.0.0.0 0.0.0.0
inside no snmp-server location no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart tunnel-group sslgroup type webvpn !--
- Create a tunnel group "sslgroup" with type as WebVPN.
tunnel-group sslgroup general-attributes address-pool
vpnpool !--- Associate the address pool vpnpool created.
default-group-policy clientgroup !--- Associate the
group policy "clientgroup" created. tunnel-group
sslgroup webvpn-attributes group-alias sslgroup_users
enable !--- Configure the group alias as sslgroup-users.
```

```
telnet timeout 5 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 netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global webvpn enable outside !---
Enable WebVPN on the outside interface. svc image
disk0:/sslclient-win-1.1.4.179.pkg 1 !--- Assign an
order to the SVC image. svc enable !--- Enable the
security appliance to download SVC images to remote
computers. tunnel-group-list enable !--- Enable the
display of the tunnel-group list on the WebVPN Login
page. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa#
```

使用 SVC 建立 SSL VPN 连接

要建立与 ASA 的 SSL VPN 连接，请执行以下步骤。

1. 在 Web 浏览器的 Address 字段中键入 ASA 的 Webvpn 接口的 URL 或 IP 地址。例如：`https://<IP address of the ASA WebVPN interface>`
2. 输入用户名和密码，然后从 Group 下拉列表中选择相应的组。**注意：** 在下载 SSL VPN Client 之前，您的计算机上必须已安装 ActiveX 软件。当连接建立时，将出现以下对话框：当连接建立后，即会出现以下消息：
3. 当连接建立后，双击出现在计算机任务栏中的黄色密钥图标。即会出现 Cisco Systems SSL VPN Client 对话框，并显示有关 SSL 连接的信息。

验证

使用本部分可确认配置能否正常运行。

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。

- **show webvpn svc** — 显示存储在 ASA 闪存中的 SVC 映像。`ciscoasa#show webvpn svc 1. disk0:/sslclient-win-1.1.4.179.pkg 1 CISCO STC win2k+ 1.0.0 1,1,4,179 Fri 01/18/2008 15:19:49.43 1 SSL VPN Client(s) installed`
- **show vpn-sessiondb svc** — 显示有关当前 SSL 连接的信息。`ciscoasa#show vpn-sessiondb svc Session Type: SVC Username : ssluser1 Index : 1 Assigned IP : 192.168.10.1 Public IP : 192.168.1.1 Protocol : SVC Encryption : 3DES Hashing : SHA1 Bytes Tx : 131813 Bytes Rx : 5082 Client Type : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) Client Ver : Cisco Systems SSL VPN Client 1, 1, 4, 179 Group Policy : clientgroup Tunnel Group : sslgroup Login Time : 12:38:47 UTC Mon Mar 17 2008 Duration : 0h:00m:53s Filter Name :`
- **show webvpn group-alias** — 显示为各组配置的别名。`ciscoasa#show webvpn group-alias Tunnel Group: sslgroup Group Alias: sslgroup_users enabled`
- 在 ASDM 中，选择 **Monitoring > VPN > VPN Statistics > Sessions** 以查看有关 ASA 中的当前 Webvpn 会话的信息。

故障排除

本部分提供的信息可用于对配置进行故障排除。

- **vpn-sessiondb logoff name <用户名>** — 允许您注销指定用户名的 SSL VPN 会话。
  ciscoasa#**vpn-sessiondb logoff name ssluser1 Called vpn_remove_uauIth: success! webvpn_svc_np_tear_down: no ACL NFO: Number of sessions with name "ssluser1" logged off : 1**
  同样地，您也可以使用 **vpn-sessiondb logoff svc** 命令终止所有 SVC 会话。**注意：** 如果 PC 转入待机或休眠模式，则可以终止 SSL VPN 连接。
  webvpn_rx_data_cstp webvpn_rx_data_cstp: got message SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, etc) Called vpn_remove_uauth: success! webvpn_svc_np_tear_down: no ACL ciscoasa#**show vpn-sessiondb svc** INFO: There are presently no active sessions
- **Debug webvpn svc <1-255>** — 提供实时 webvpn 事件以建立会话。Ciscoasa#**debug webvpn svc 7** ATTR_CISCO_AV_PAIR: got SVC ACL: -1 webvpn_rx_data_tunnel_connect CSTP state = HEADER_PROCESSING http_parse_cstp_method() ...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1' webvpn_cstp_parse_request_field() ...input: 'Host: 172.16.1.1' Processing CSTP header line: 'Host: 172.16.1.1' webvpn_cstp_parse_request_field() ...input: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4, 179' Processing CSTP header line: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4, 179' Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Version: 1' Processing CSTP header line: 'X-CSTP-Version: 1' Setting version to '1' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Hostname: tacweb' Processing CSTP header line: 'X-CSTP-Hostname: tacweb' Setting hostname to: 'tacweb' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0' Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0' webvpn_cstp_parse_request_field() ...input: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486 D5BC554D2' Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1 CF236DB5E8BE70B1486D5BC554D2' Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1 486D5BC554D2' WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B C554D2' Validating address: 0.0.0.0 CSTP state = WAIT_FOR_ADDRESS webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0 CSTP state = HAVE_ADDRESS No subnetmask... must calculate it SVC: NP setup webvpn_svc_np_setup SVC ACL Name: NULL SVC ACL ID: -1 SVC ACL ID: -1 vpn_put_uauth success! SVC: adding to sessmgmt SVC: Sending response CSTP state = **CONNECTED**
- 在 ASDM 中，选择 **Monitoring > Logging > Real-time Log Viewer > View** 以查看实时事件。以下示例显示 SVC 192.168.10.1 和 Internet 中的 Web 服务器 10.2.2.2 之间通过 172.16.1.5 的会话信息。

相关信息

- Cisco 5500 系列自适应安全设备支持页
- PIX/ASA 7.x 以及用于公共 Internet VPN 的单接口 VPN Client 的配置示例
- 在 ASA 上用 ASDM 配置 SSL VPN Client (SVC) 的示例
- 技术支持和文档 - Cisco Systems