ASA 8.x :VPN访问与使用自签名证书的AnyConnect VPN客户端配置示例

目录

简介

本文档介绍如何使用自签名证书允许从 Cisco AnyConnect 2.0 客户端到 ASA 的远程访问 SSL VPN 连接。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 运行软件版本 8.0 的基本 ASA 配置
- ASDM 6.0(2)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco ASA 8.0(2)、ASDM 6.0 (2)
- Cisco AnyConnect 2.0

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

Cisco AnyConnect 2.0 客户端是一款基于 SSL 的 VPN 客户端。AnyConnect客户端可用于各种操作系统，如Windows 2000、XP、Vista、Linux（多个Distro）和MAC OS X。系统管理员可以在远程PC上手动安装AnyConnect客户端。也可将其加载到安全设备中，以供远程用户下载。下载后，该应用程序可以在连接终止时自动自我卸载，也可以保留在远程 PC 中，以备将来进行 SSL VPN 连接。本示例中的 AnyConnect 客户端在基于浏览器的 SSL 身份验证成功的情况下可供下载。

有关 AnyConnect 2.0 客户端的详细信息，请参阅 AnyConnect 2.0 发行版本注释。

注意：MS终端服务不与AnyConnect客户端一起支持。您不能使用远程桌面协议 (RDP) 连接到计算机然后启动 AnyConnect 会话。您不能使用远程桌面协议 (RDP) 连接到经由 AnyConnect 连接的客户端。

注意：AnyConnect的首次安装要求用户具有管理权限（无论您是使用独立的AnyConnect msi软件包还是从ASA推送pkg文件）。 如果用户没有管理员权限，则系统会弹出对话框说明这一要求。随后的升级将不再要求之前安装了 AnyConnect 的用户拥有管理员权限。

配置

要将 ASA 配置为能够使用 AnyConnect 客户端进行 VPN 访问，请完成以下步骤：

1. 配置自发证书。
2. 上载并标识 SSL VPN 客户端映像。
3. 启用 Anyconnect 访问。
4. 创建新的组策略。
5. 配置 VPN 连接的访问列表绕开选项。
6. 创建 AnyConnect 客户端连接的连接配置文件和隧道组。
7. 配置 AnyConnect 客户端的 NAT 免除。
8. 将用户添加到本地数据库。

步骤 1. 配置自发证书

默认情况下，安全设备拥有自签名证书，该证书在设备每次重新启动时都重新生成。您可以从类似 Verisign 或 EnTrust 这样的供应商处购买自己的证书，也可配置 ASA，让其向自己发出身份证书。这样的证书在设备重新启动后仍会保持不变。完成此步骤可以生成设备重新启动后仍会存留的自发证书。

ASDM 步骤

1. 单击 **Configuration**，然后单击 Remote Access VPN。
2. 展开 **Certificate Management**，然后选择 Identity Certificates。
3. 单击 **Add**，然后单击 Add a new identity certificate 单选按钮。
4. 单击 **New**。
5. 在 Add Key Pair 对话框中单击 **Enter new key pair name 单选按钮。**
6. 输入用于标识密钥对的名称。本示例使用的是 *sslvpnkeypair*。
7. 单击 **Generate Now**。
8. 在 Add Identity Certificate 对话框中，确保新创建的密钥对处于选中状态。
9. 对于 Certificate Subject DN，请输入用于连接到 VPN 终接接口的完全限定域名 (FQDN)。**CN=sslvpn.cisco.com**
10. 单击 **Advanced**，然后在 Certificate Subject DN 字段中输入使用的 FQDN。例如，**FQDN**:sslvpn.cisco.com
11. Click **OK**.
12. 选中 **Generate Self Signed Certificate 复选框，然后单击 Add Certificate。**
13. Click **OK**.
14. 单击 **Configuration**，然后单击 Remote Access VPN。
15. 展开 **Advanced**，然后选择 SSL Settings。
16. 在 Certificates 区域，选择将用于终接 SSL VPN 的接口（外部），然后单击 **Edit**。
17. 在 Certificate 下拉列表中，选择先前生成的自签名证书。
18. 单击 **OK**，然后单击 Apply。

命令行示例

ciscoasa

```
ciscoasa(config)#crypto key generate rsa label
sslvpnkeypair
INFO: The name for the keys will be: sslvpnkeypair
Keypair generation process begin. Please wait...
!--- Generate an RSA key for the certificate. (The name
should be unique. !--- For example, sslvpnkeypair.)
ciscoasa(config)#crypto ca trustpoint localtrust
!--- Create a trustpoint for the self-issued
certificate. ciscoasa(config-ca-trustpoint)#enrollment
self
ciscoasa(config-ca-trustpoint)#fqdn sslvpn.cisco.com
ciscoasa(config-ca-trustpoint)#subject-name
CN=sslvpn.cisco.com
!--- The fully qualified domain name is used for both
fqdn and CN. !--- The name should resolve to the ASA
outside interface IP address. ciscoasa(config-ca-
trustpoint)#keypair sslvpnkeypair
!--- The RSA key is assigned to the trustpoint for
certificate creation. ciscoasa(config-ca-
trustpoint)#crypto ca enroll localtrust noconfirm
% The fully-qualified domain name in the certificate
will be: sslvpn.cisco.com
ciscoasa(config)# ssl trust-point localtrust outside
!--- Assign the trustpoint to be used for SSL
connections on the outside interface.
```

步骤 2. 上载并标识 SSL VPN 客户端映像

本文档使用的是 AnyConnect SSL 2.0 客户端。您可以在 Cisco 软件下载网站获取该客户端。对于远程用户计划使用的操作系统而言，每个操作系统都需要单独的 AnyConnect 映像。有关详细信息

，请参阅 Cisco AnyConnect 2.0 发行版本注释。

获取 AnyConnect 客户端后，请完成以下步骤：

ASDM 步骤

1. 单击 **Configuration**，然后单击 Remote Access VPN。
2. 展开 **Network (Client) Access**，然后展开 Advanced。
3. 展开 **SSL VPN**，然后选择 Client Settings。
4. 在 SSL VPN Client Images 区域，单击 **Add**，然后单击 Upload。
5. 浏览并找到 AnyConnect 客户端下载到的位置。
6. 选择文件，然后单击 **Upload File**。一旦客户端上载完成，您将收到消息提示您文件已成功上载到闪存。
7. Click **OK**.随后会出现一个对话框，要求您确认是否要将新上载的映像用作当前 SSL VPN 客户端映像。
8. Click **OK**.
9. 单击 **OK**，然后单击 Apply。
10. 针对要使用的每个特定于操作系统的 AnyConnect 程序包重复本部分中的这些步骤。

命令行示例

ciscoasa

```
ciscoasa(config)#copy tftp://192.168.50.5/anyconnect-win-2.0.0343-k9.pkg flash

Address or name of remote host [192.168.50.5]?

Source filename [anyconnect-win-2.0.0343-k9.pkg]?

Destination filename [anyconnect-win-2.0.0343-k9.pkg]?

Accessing tftp://192.168.50.5/anyconnect-win-2.0.0343-k9.pkg...!!!!!!!!!!!!!
Writing file disk0:/anyconnect-win-2.0.0343-k9.pkg...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!
2635734 bytes copied in 4.480 secs (658933 bytes/sec)
!--- AnyConnect image is downloaded to ASA via TFTP.
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
!--- Specify the AnyConnect image to be downloaded by users. The image that is !--- downloaded the most should have the lowest number. This image uses 1 for the !--- AnyConnect Windows image.
```

步骤 3. 启用 Anyconnect 访问

要允许 AnyConnect 客户端连接到 ASA，您必须在终止 SSL VPN 连接的接口上启用访问。本示例使用外部接口终止 AnyConnect 连接。

ASDM 步骤

1. 单击 **Configuration**，然后单击 Remote Access VPN。

2. 展开 **Network (Client) Access**，然后选择 SSL VPN Connection Profiles。
3. 选中 **Enable Cisco AnyConnect VPN Client 复选框。**
4. 选中外部接口的 **Allow Access 复选框，然后单击 Apply。**

命令行示例

ciscoasa
ciscoasa(config)#**webvpn** ciscoasa(config-webvpn)#**enable outside** ciscoasa(config-webvpn)#**svc enable** *!--- Enable AnyConnect to be downloaded to remote computers.*

步骤 4. 创建新的组策略

组策略用于指定客户端连接时应该应用于客户端的配置参数。本示例将创建名为 *SSLClientPolicy* 的组策略。

ASDM 步骤

1. 单击 **Configuration**，然后单击 Remote Access VPN。
2. 展开 **Network (Client) Access，然后选择 Group Policies。**
3. 单击 **Add。**
4. 选择 **General**，然后在 Name 字段输入 SSLClientPolicy。
5. 取消选中 Address Pools **Inherit 复选框。**
6. 单击 **Select**，然后单击 Add。此时将出现 Add IP Pool 对话框。
7. 在网络中当前未使用的 IP 范围内配置地址池。本示例使用这些值：**名称：**SSLClientPool**起始 IP 地址**：192.168.25.1**Ending IP Address**：192.168.25.50**子网掩码:**255.255.255.0
8. Click **OK**.
9. 选择新创建的地址池，然后单击 **Assign。**
10. 单击 **OK**，然后单击 More Options。
11. 取消选中 Tunneling Protocols **Inherit 复选框。**
12. 选中 **SSL VPN Client。**
13. 在左窗格中选择 **Servers。**
14. 取消选中 DNS Servers **Inherit 复选框，然后输入 AnyConnect 客户端将使用的内部 DNS 服务器的 IP 地址。**本示例使用 *192.168.50.5*。
15. 单击 **More Options。**
16. 取消选中 Default Domain **Inherit 复选框。**
17. 输入内部网络使用的域。例如，*tsweb.local*。
18. 单击 **OK**，然后单击 Apply。

命令行示例

ciscoasa
ciscoasa(config)#**ip local pool SSLClientPool 192.168.25.1-192.168.25.50 mask 255.255.255.0** *!--- Define the IP pool. The IP pool should be a range of IP addresses !--- not already in use on the internal network.* ciscoasa(config)#**group-policy SSLCLientPolicy internal** ciscoasa(config)#**group-policy SSLCLientPolicy attributes**

```
ciscoasa(config-group-policy)#dns-server value
192.168.50.5
!--- Specify the internal DNS server to be used.
ciscoasa(config-group-policy)#vpn-tunnel-protocol svc
!--- Specify VPN tunnel protocol to be used by the Group
Policy. ciscoasa(config-group-policy)#default-domain
value tsweb.local
!--- Define the default domain assigned to VPN users.
ciscoasa(config-group-policy)#address-pools value
SSLClientPool
!--- Assign the IP pool created to the SSLClientPolicy
group policy.
```

配置 VPN 连接的访问列表绕开选项

启用该选项后，您将允许 SSL/IPsec 客户端绕开接口访问列表。

ASDM 步骤

1. 单击 **Configuration**，然后单击 Remote Access VPN。
2. 展开 **Network (Client) Access**，然后展开 Advanced。
3. 展开 **SSL VPN**，然后选择 Bypass Interface Access List。
4. 确保 **Enable inbound SSL VPN and IPSEC Sessions to bypass interface access lists 复选框处于选中状态，然后单击 Apply。**

命令行示例

ciscoasa

```
ciscoasa(config)#sysopt connection permit-vpn
!--- Enable interface access-list bypass for VPN
connections. !--- This example uses the vpn-filter
command for access control.

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

步骤 6. 创建 AnyConnect 客户端连接的连接配置文件和隧道组

连接到 ASA 时，VPN 客户端将连接到连接配置文件或隧道组。隧道组用于定义特定类型的 VPN 连接（如 IPsec L2L、IPsec 远程访问、无客户端 SSL 和客户端 SSL）的连接参数。

ASDM 步骤

1. 单击 **Configuration**，然后单击 Remote Access VPN。
2. 展开 **Network (Client) Access**，然后展开 SSL VPN。
3. 选择 **Connection Profiles**，然后单击 Add。
4. 选择 **Basic**，然后输入以下值：**名称：**SSLClientProfile**身份验证:**本地**默认组策略**:SSLClientPolicy
5. 确保 **SSL VPN Client Protocol 复选框处于选中状态。**
6. 在左窗格中展开 **Advanced**，然后选择 SSL VPN。
7. 在 Connection Aliases 下单击 **Add**，然后输入用户可以将其 VPN 连接关联到的名称。例如，*SSLVPNClient*。
8. 单击 **OK**，然后再次单击 OK。

9. 在 ASDM 窗口底部，选中 **Allow user to select connection, identified by alias in the table above at login page 复选框，然后单击 Apply。**

命令行示例

ciscoasa

```
ciscoasa(config)#tunnel-group SSLClientProfile type
remote-access
!--- Define tunnel group to be used for VPN remote
access connections. ciscoasa(config)#tunnel-group
SSLClientProfile general-attributes
ciscoasa(config-tunnel-general)#default-group-policy
SSLCLientPolicy
ciscoasa(config-tunnel-general)#tunnel-group
SSLClientProfile webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias SSLVPNClient
enable
!--- Assign alias for tunnel group. ciscoasa(config-
tunnel-webvpn)#webvpn
ciscoasa(config-webvpn)#tunnel-group-list enable
!--- Enable alias/tunnel group selection for SSL VPN
connections.
```

步骤 7. 配置 AnyConnect 客户端的 NAT 免除

对于要允许 SSL VPN 客户端访问的任何 IP 地址或范围，都必须配置 NAT 免除。在本示例中，SSL VPN 客户端仅需要访问内部 IP 192.168.50.5。

注意：如果未启用NAT控制，则不需要此步骤。使用 **show run nat-control 命令进行验证。**要通过 ASDM 进行验证，请单击 **Configuration**，单击 Firewall，然后选择 Nat Rules。如果 **Enable traffic through the firewall without address translation 复选框已选中，则可以跳过此步骤。**

ASDM 步骤

1. 单击 **Configuration**，然后单击 Firewall。
2. 选择 **Nat Rules**，然后单击 Add。
3. 选择 **Add NAT Exempt Rule**，然后输入以下值：**操作：豁免接口:**内部**来源：**192.168.50.5**目的地：**192.168.25.0/24**NAT Exempt Direction**：NAT Exempt outbound traffic from interface 'inside' to lower security interfaces (Default)
4. 单击 **OK**，然后单击 Apply。

命令行示例

ciscoasa

```
ciscoasa(config)#access-list no_nat extended permit
                 ip host 192.168.50.5 192.168.25.0
255.255.255.0
!--- Define access list to be used for NAT exemption.
ciscoasa(config)#nat (inside) 0 access-list no_nat
!--- Allow external connections to untranslated internal
!--- addresses defined by access lisy no_nat.
ciscoasa(config)#
```

步骤 8. 将用户添加到本地数据库

如果要使用本地身份验证（默认选项），则您必须在本地数据库中定义用户名和口令，以便进行用户身份验证。

ASDM 步骤

1. 单击 **Configuration**，然后单击 Remote Access VPN。
2. 展开 **AAA Setup**，然后选择 Local Users。
3. 单击 **Add**，然后输入以下值：**username**：马修**密码**：p@ssw0rd**确认密码：**p@ssw0rd
4. 选择 **No ASDM, SSH, Telnet or Console Access 单选按钮。**
5. 单击 **OK**，然后单击 Apply。
6. 对于其他用户，请重复此步骤，然后点击 **Save**。

命令行示例

ciscoasa

```
ciscoasa(config)#username matthewp password p@ssw0rd
ciscoasa(config)#username matthewp attributes
ciscoasa(config-username)#service-type remote-access
!--- Assign user remote access only. No SSH, Telnet,
ASDM access allowed. ciscoasa(config-username)#write
memory
!--- Save the configuration.
```

验证

使用此部分可以验证 SSL VPN 配置是否成功

使用 AnyConnect 客户端连接到 ASA

直接在 PC 上安装客户端，然后连接到 ASA 外部接口，或者在 Web 浏览器中输入 ASA 的 https 和 FQDN/IP 地址。如果使用 Web 浏览器，客户端会在成功登录后自动安装。

验证 SSL VPN 客户端连接

使用 **show vpn-sessiondb svc 命令验证连接的 SSL VPN 客户端。**

```
ciscoasa(config-group-policy)#show vpn-sessiondb svc

Session Type: SVC

Username     : matthewp               Index        : 6
Assigned IP  : 192.168.25.1           Public IP    : 172.18.12.111
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 35466                  Bytes Rx     : 27543
Group Policy : SSLClientPolicy        Tunnel Group : SSLClientProfile
Login Time   : 20:06:59 UTC Tue Oct 16 2007
Duration     : 0h:00m:12s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

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

vpn-sessiondb logoff name *username* 命令可以根据用户名注销用户。断开时，用户将收到

Administrator Reset 消息。

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

ciscoasa(config)#
```

有关 AnyConnect 2.0 客户端的详细信息，请参阅 Cisco AnyConnect VPN 管理员指南。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令（可选）

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。

注意：在使用debug命令之前，请参阅有关Debug命**令的**重要信息。

- **debug webvpn svc 255** — 显示与通过 WebVPN 连接到 SSL VPN 客户端相关的 debug 消息。

成功的 AnyConnect 登录

```
ciscoasa(config)#debug webvpn svc 255
INFO: debug webvpn svc enabled at level 255.
ciscoasa(config)#ATTR_FILTER_ID: Name:
 SSLVPNClientAccess
, Id: 1, refcnt: 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: 10.10.1.5' - !--- Outside IP of ASA Processing CSTP header line: 'Host:
10.10.1.5'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' - !--- AnyConnect Version
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' Setting
user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343' webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=3338474156@28672@1192565782@EFB9042D72C
63CE02164F790435897AC72EE70AE' Processing CSTP header line: 'Cookie:
webvpn=3338474156@28672@119 2565782@EFB9042D72C63CE02164F790435897AC72EE70AE' Found WebVPN
cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C 63CE02164F790435897AC72EE70AE'
WebVPN Cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C63CE02
164F790435897AC72EE70AE' IPADDR: '3338474156', INDEX: '28672', LOGIN: '1192565782'
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: wkstation1' - !--- Client desktop hostname Processing CSTP header line: 'X-
CSTP-Hostname: wkstation1'
Setting hostname to: 'wkstation1'
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: 'X-CSTP-MTU: 1206'
Processing CSTP header line: 'X-CSTP-MTU: 1206'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv4'
```

```
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451CB0948AFBE98296FD849
                          49EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51'
Processing CSTP header line: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451C
       B0948AFBE98296FD84949EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:
                             DES-CBC3-SHA:DES-CBC-SHA'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.25.1/255.255.255.0 - !--- IP assigned from IP Pool CSTP
state = HAVE_ADDRESS SVC: NP setup np_svc_create_session(0x7000, 0xD41612C8, TRUE)
webvpn_svc_np_setup SVC ACL Name: NULL SVC ACL ID: -1 SVC ACL ID: -1 vpn_put_uauth success!
SVC IPv6 ACL Name: NULL SVC IPv6 ACL ID: -1 SVC: adding to sessmgmt SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy CSTP state = CONNECTED
webvpn_rx_data_cstp webvpn_rx_data_cstp: got internal message Unable to initiate NAC, NAC
might not be enabled or invalid policy
```

失败的 AnyConnect 登录(错误口令)

```
webvpn_portal.c:ewaFormSubmit_webvpn_login[1808]
ewaFormSubmit_webvpn_login: tgCookie = 0
ewaFormSubmit_webvpn_login: cookie = d53d2990
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
webvpn_portal.c:http_webvpn_kill_cookie[627]
webvpn_auth.c:http_webvpn_pre_authentication[1905]
WebVPN: calling AAA with ewsContext (-717386088) and nh (-717388536)!
WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[4380]
WebVPN: AAA status = (REJECT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1808]
ewaFormSubmit_webvpn_login: tgCookie = 0
ewaFormSubmit_webvpn_login: cookie = d53d2990
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
webvpn_auth.c:http_webvpn_post_authentication[1180]
WebVPN: user: (matthewp) rejected.
http_remove_auth_handle(): handle 9 not found!
webvpn_portal.c:ewaFormServe_webvpn_login[1749]
webvpn_portal.c:http_webvpn_kill_cookie[627]
```

相关信息

- Cisco AnyConnect VPN Client 管理员指南，版本 2.0
- AnyConnect VPN 客户端版本 2.0 的发行版本注释
- 技术支持和文档 - Cisco Systems