ASA 8.x:使用AnyConnect VPN客戶端使用自簽名證書的VPN訪問配置示例

目錄

簡介

本文檔介紹如何使用自簽名證書允許從Cisco AnyConnect 2.0客戶端遠端訪問SSL VPN連線到ASA。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 運行軟體版本8.0的基本ASA配置
- ASDM 6.0(2)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

Cisco AnyConnect 2.0客戶端是基於SSL的VPN客戶端。AnyConnect客戶端可用於和安裝在各種作業系統上，例如Windows 2000、XP、Vista、Linux（多個總代理商）和MAC OS X。系統管理員可以手動將AnyConnect客戶端安裝在遠端PC上。還可以將其載入到安全裝置上，並準備下載到遠端使用者。下載應用程式後，連線終止後，該應用程式會自動解除安裝，或者保留在遠端PC上用於將來的SSL VPN連線。此示例使AnyConnect客戶端在成功進行基於瀏覽器的SSL身份驗證後即可下載。

有關AnyConnect 2.0客戶端的詳細資訊，請參閱AnyConnect 2.0發行說明。

注意：MS終端服務不支援與AnyConnect客戶端結合使用。您不能對電腦執行RDP，然後啟動AnyConnect會話。無法通過RDP連線到通過AnyConnect連線的客戶端。

注意：AnyConnect的首次安裝要求使用者具有管理員許可權（無論您是使用獨立AnyConnect msi軟體包還是從ASA推送軟體包檔案）。 如果使用者沒有管理員許可權，則會出現一個對話方塊，說明此要求。後續升級將不需要以前安裝AnyConnect的使用者具有管理員許可權。

設定

要使用AnyConnect客戶端配置ASA以進行VPN訪問，請完成以下步驟：

1. 配置自行頒發的證書。
2. 上傳和標識SSL VPN客戶端映像。
3. 啟用Anyconnect訪問。
4. 建立新的組策略。
5. 為VPN連線配置訪問清單旁路。
6. 為AnyConnect客戶端連線建立連線配置檔案和隧道組。
7. 為AnyConnect客戶端配置NAT免除。
8. 向本地資料庫新增使用者。

步驟1.配置自行頒發的證書

預設情況下，安全裝置具有自簽名證書，每次重新啟動裝置時都會重新生成該證書。您可以從Verisign或EnTrust等供應商購買自己的證書，也可以將ASA配置為向自身頒發身份證書。即使重新引導裝置，此證書也會保持不變。完成此步驟可生成自頒發的證書，該證書在裝置重新啟動時仍然存在。

ASDM過程

1. 按一下**Configuration**，然後按一下**Remote Access VPN**。
2. 展開**Certificate Management**，然後選擇**Identity Certificates**。
3. 按一下**Add**，然後按一下**Add a new identity certificate**單選按鈕。
4. 按一下「**New**」。
5. 在「新增金鑰對」對話方塊中，按一下**輸入新金鑰對名稱**單選按鈕。
6. 輸入用於標識金鑰對的名稱。此範例使用*sslvpnkeypair*。
7. 按一下「**Generate Now**」。
8. 在新增身份證書對話方塊中，確保選中新建立的金鑰對。
9. 對於證書使用者DN，輸入將用於連線到VPN終端介面的完全限定域名(FQDN)。
   CN=sslvpn.cisco.com
10. 按一下**Advanced**，然後輸入用於Certificate Subject DN欄位的FQDN。例如，**FQDN**:sslvpn.cisco.com
11. 按一下「**OK**」（確定）。
12. 選中**Generate Self Signed Certificate**覈取方塊，然後按一下**Add Certificate**。
13. 按一下「**OK**」（確定）。
14. 按一下**Configuration**，然後按一下**Remote Access VPN**。
15. 展開**Advanced**，然後選擇**SSL Settings**。
16. 在Certificates區域中，選擇將用於終止SSL VPN的介面（外部），然後按一下**Edit**。
17. 在「Certificate」下拉選單中，選擇您之前生成的自簽名證書。
18. 按一下「**OK**」，然後按一下「**Apply**」。

命令列示例

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.
```

步驟2.上傳和識別SSL VPN客戶端映像

本檔案使用AnyConnect SSL 2.0使用者端。您可以從思科軟體下載網站取得此使用者端。遠端使用者計畫使用的每個作業系統都需要一個單獨的Anyconnect映像。如需詳細資訊，請參閱Cisco

AnyConnect 2.0版本說明。

獲得AnyConnect客戶端後，請完成以下步驟：

ASDM過程

1. 按一下**Configuration**，然後按一下**Remote Access VPN**。
2. 展開**網路（客戶端）訪問**，然後展開**高級**。
3. 展開**SSL VPN**，然後選擇**Client Settings**。
4. 在SSL VPN Client Images區域中，按一下**Add**，然後按一下**Upload**。
5. 瀏覽至下載AnyConnect客戶端的位置。
6. 選擇檔案，然後按一下**Upload File**。使用者端上傳後，您會收到一則訊息，說明檔案已成功上傳到快閃記憶體。
7. 按一下「**OK**」（確定）。將出現一個對話方塊，確認要將新上傳的映像用作當前SSL VPN客戶端映像。
8. 按一下「**OK**」（確定）。
9. 按一下「**OK**」，然後按一下「**Apply**」。
10. 對要使用的每個作業系統特定的Anyconnect軟體包重複本節中的步驟。

命令列示例

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.
```

步驟3.啟用Anyconnect訪問

要允許AnyConnect客戶端連線到ASA，必須在終止SSL VPN連線的介面上啟用訪問。此示例使用外部介面來終止Anyconnect連線。

ASDM過程

1. 按一下**Configuration**，然後按一下**Remote Access VPN**。

2. 展開**網路（客戶端）訪問**，然後選擇**SSL VPN連線配置檔案**。
3. 選中**Enable Cisco AnyConnect VPN Client**覈取方塊。
4. 選中外部介面的**Allow Access**覈取方塊，然後按一下**Apply**。

命令列示例

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

步驟4.建立新的組策略

組策略指定連線客戶端時應應用的配置引數。此示例建立名為*SSLClientPolicy*的組策略。

ASDM過程

1. 按一下**Configuration**，然後按一下**Remote Access VPN**。
2. 展開**網路（客戶端）訪問**，然後選擇**組策略**。
3. 按一下「**Add**」。
4. 選擇**General**，然後在Name欄位中輸入**SSLClientPolicy**。
5. 取消選中Address Pools **Inherit**覈取方塊。
6. 按一下「**Select**」，然後按一下「**Add**」。系統將顯示Add IP Pool對話方塊。
7. 從網路上當前未使用的IP範圍配置地址池。此示例使用以下值：**名稱:**SSLClientPool**起始IP地址**:192.168.25.1**結束IP地址**:192.168.25.50**子網路遮罩**:255.255.255.0
8. 按一下「**OK**」（確定）。
9. 選擇新建立的池，然後按一下**Assign**。
10. 按一下**OK**，然後按一下**More Options**。
11. 取消選中Tunneling Protocols **Inherit**覈取方塊。
12. 檢查**SSL VPN Client**。
13. 在左窗格中，選擇**Servers**。
14. 取消選中DNS Servers **Inherit**覈取方塊，並輸入AnyConnect客戶端將使用的內部DNS伺服器的IP地址。本示例使用*192.168.50.5*。
15. 按一下「**More Options**」。
16. 取消選中Default Domain **Inherit**覈取方塊。
17. 輸入您的內部網路使用的域。例如，*tsweb.local*。
18. 按一下「**OK**」，然後按一下「**Apply**」。

命令列示例

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.
```

為VPN連線配置訪問清單繞行

啟用此選項時，將允許SSL/IPsec客戶端繞過介面訪問清單。

ASDM過程

1. 按一下**Configuration**，然後按一下**Remote Access VPN**。
2. 展開**網路（客戶端）訪問**，然後展開**高級**。
3. 展開**SSL VPN**，然後選擇**Bypass Interface Access List**。
4. 確保選中**Enable inbound SSL VPN and IPSEC Sessions to bypass interface access lists**覈取方塊，然後按一下**Apply**。

命令列示例

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)#
```

步驟6.為AnyConnect客戶端連線建立連線配置檔案和隧道組

當VPN客戶端連線到ASA時，它們連線到連線配置檔案或隧道組。隧道組用於定義特定型別VPN連線的連線引數，例如IPsec L2L、IPsec遠端訪問、無客戶端SSL和客戶端SSL。

ASDM過程

1. 按一下**Configuration**，然後按一下**Remote Access VPN**。
2. 展開**網路（客戶端）訪問**，然後展開**SSL VPN**。
3. 選擇**Connection Profiles**，然後按一下**Add**。
4. 選擇**Basic**，然後輸入以下值：**名稱**:SSLClientProfile**驗證**:本地**預設組策略**:SSLClientPolicy
5. 確保選中**SSL VPN Client Protocol**覈取方塊。
6. 在左窗格中，展開**Advanced**，然後選擇**SSL VPN**。
7. 在Connection Aliases下，按一下**Add**，然後輸入使用者可以將VPN連線關聯到的名稱。例如*SSLVPNClient*。
8. 按一下「**OK**」，然後再次按一下「**OK**」。
9. 在ASDM視窗的底部，選中**Allow user to select connection， identified by alias in the table above at login page**覈取方塊，然後按一下**Apply**。

命令列示例

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.*

步驟7.為AnyConnect客戶端配置NAT免除

應該為要允許SSL VPN客戶端訪問的任何IP地址或範圍配置NAT免除。在本示例中，SSL VPN客戶端只需要訪問內部IP 192.168.50.5。

注意：如果未啟用NAT控制，則不需要此步驟。使用**show run nat-control**命令進行驗證。若要通過ASDM進行驗證，請按一下**Configuration**，然後按一下**Firewall**，然後選擇**Nat Rules**。如果選中**Enable traffic through the firewall without address translation**覈取方塊，則可以跳過此步驟。

ASDM過程

1. 按一下**Configuration**，然後按一下**Firewall**。
2. 選擇**Nat Rules**，然後按一下**Add**。
3. 選擇**Add NAT Exempt Rule**，然後輸入以下值：**Action:**免稅**Interface:**inside**來源**:192.168.50.5**目標**:192.168.25.0/24**NAT豁免方向**:NAT將出站流量從介面「內部」豁免到安全性較低的介面（預設）
4. 按一下「**OK**」，然後按一下「**Apply**」。

命令列示例

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)#

步驟8.將使用者新增到本地資料庫

如果使用本地身份驗證（預設），則必須在本地資料庫中定義使用者名稱和密碼以進行使用者身份

驗證。

ASDM過程

1. 按一下**Configuration**，然後按一下**Remote Access VPN**。
2. 展開**AAA Setup**，然後選擇**Local Users**。
3. 按一下**Add**，然後輸入以下值：**使用者名稱**:matthewp**密碼**:p@ssw0rd**確認密碼**:p@ssw0rd
4. 選擇**No ASDM， SSH， Telnet or Console Access**單選按鈕。
5. 按一下「**OK**」，然後按一下「**Apply**」。
6. 對其他使用者重複此步驟，然後按一下**儲存**。

命令列示例

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.
```

驗證

使用本節內容，確認SSL VPN組態是否成功

使用AnyConnect客戶端連線到ASA

直接在PC上安裝客戶端，然後連線到ASA外部介面，或在Web瀏覽器中輸入https和ASA的FQDN/IP地址。如果使用Web瀏覽器，客戶端會在成功登入後自行安裝。

驗證SSL VPN客戶端連線

使用**show vpn-sessiondb svc**命令驗證連線的SSL VPN客戶端。

```
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 命令按使用者名稱註銷使用者。斷開連線時，將向使用者傳送*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)#
```

有關AnyConnect 2.0客戶端的詳細資訊，請參閱Cisco AnyConnect VPN管理員指南。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

故障排除命令（可選）

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **debug webvpn svc 255** — 顯示有關通過WebVPN連線到SSL VPN客戶端的調試消息。**成功AnyConnect登入**

```
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
```

AnyConnect登入失敗（密碼錯誤）

```
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]
```

相關資訊

- Cisco AnyConnect VPN客戶端管理員指南2.0版
- AnyConnect VPN客戶端2.0版發行說明
- 技術支援與文件 - Cisco Systems