# AnyConnect SSL over IPv4+IPv6到ASA配置

### 目錄

<u>簡介</u> <u>必要條件</u> <u>累明例態證</u> 關 資訊

# <u>簡介</u>

本文檔提供了思科自適應安全裝置(ASA)的配置示例,以允許Cisco AnyConnect安全移動客戶端 (本文檔的其餘部分中稱為「AnyConnect」)通過IPv4或IPv6網路建立SSL VPN隧道。

此外,此配置允許客戶端通過隧道傳遞IPv4和IPv6流量。

# <u>必要條件</u>

#### <u>需求</u>

為了成功建立通過IPv6的SSLVPN隧道,請滿足以下要求:

- 需要端到端IPv6連線
- AnyConnect版本必須是3.1或更高版本
- ASA軟體版本必須是9.0或更高版本

但是,如果其中任一要求未滿足,則本文檔中討論的配置仍將允許客戶端通過IPv4連線。

#### <u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- ASA-5505與軟體版本9.0(1)
- Microsoft Windows XP Professional上的AnyConnect安全移動客戶端3.1.00495(不支援IPv6)
- Microsoft Windows 7 Enterprise 32位版上的AnyConnect安全移動客戶端3.1.00495

#### <u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。



首先,定義一個IP地址池,您將從該池為連線的每個客戶端分配一個IP地址。

如果您希望客戶端也通過隧道傳輸IPv6流量,則需要一個IPv6地址池。這兩個池稍後將在組策略中 引用。

ip local pool pool4 172.16.2.100-172.16.2.199 mask 255.255.255.0 ipv6 local pool pool6 fcfe:2222::64/64 128 要通過IPv6連線到ASA,您需要在客戶端要連線的介面(通常是外部介面)上獲得IPv6地址。

要通過隧道連線到內部主機的IPv6連線,您還需要內部介面上的IPv6。

interface Vlan90
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0
ipv6 address 2001:db8:90::2/64
!
interface Vlan102
nameif inside
security-level 100
ip address 192.168.102.2 255.255.255.0
ipv6 address fcfe:102::2/64
對於IPv6,您還需要一條指向下一跳路由器指向Internet的預設路由。

ipv6 route outside ::/0 2001:db8:90::5
route outside 0.0.0.0 0.0.0.0 203.0.113.5 1

為了對客戶端進行身份驗證,ASA需要具有身份證書。有關如何建立或匯入此類證書的說明,不在 本檔案的範圍之內,但可以在其他文檔(例如

/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/98596-asa-8-x-3rdpartyvendorcert.html

生成的配置應類似於以下內容:

crypto ca trustpoint testCA keypair testCA crl configure ... crypto ca certificate chain testCA certificate ca 00 30820312 308201fa a0030201 02020100 300d0609 2a864886 f70d0101 05050030 ... quit certificate 04 3082032c 30820214 a0030201 02020104 300d0609 2a864886 f70d0101 05050030 ... quit

然後,指示ASA將此證書用於SSL:

接下來是在外部介面上啟用該功能的基本的webvpn(SSLVPN)配置。定義可供下載的客戶端軟體包 ,並定義配置檔案(稍後詳述):

webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.1.00495-k9.pkg 1
anyconnect profiles asa9-ssl-ipv4v6 disk0:/asa9-ssl-ipv4v6.xml
anyconnect enable

在此基本示例中,配置IPv4和IPv6地址池、DNS伺服器資訊(將推送到客戶端)以及預設組策略 (DfltGrpPolicy)中的配置檔案。 此處可以配置更多屬性,而且您可以根據需要為不同的使用者集定 義不同的組策略。

**注意:**「gateway-fqdn」屬性是9.0版中的新屬性,它定義了DNS中已知的ASA的FQDN。客戶端從 ASA獲取此FQDN,並將在從IPv4漫遊到IPv6網路或反向漫遊時使用此FQDN。

group-policy DfltGrpPolicy attributes dns-server value 10.48.66.195 vpn-tunnel-protocol ssl-client gateway-fqdn value asa9.example.net address-pools value pool4 ipv6-address-pools value pool6 webvpn

anyconnect profiles value asa9-ssl-ipv4v6 type user

接下來,配置一個或多個隧道組。本示例使用預設組(DefaultWEBVPNGroup),並將其配置為要求 使用者使用證書進行身份驗證:

tunnel-group DefaultWEBVPNGroup webvpn-attributes

authentication certificate

預設情況下,AnyConnect客戶端會嘗試通過IPv4進行連線,並且僅當連線失敗時,才會嘗試通過 IPv6進行連線。但是,此行為可以通過XML配置檔案中的設定進行更改。上述配置中引用的 AnyConnect配置檔案「asa9-ssl-ipv4v6.xml」是使用ASDM(配置 — 遠端訪問VPN — 網路(客戶 端)訪問 — AnyConnect客戶端配置檔案)中的配置檔案編輯器生成的。

00	Add AnyConnect Client Profile	
Profile Name Profile Usage	asa9-ssl-ipv4v6 Enteronomotorthoprofile	
Enter a device fil created if it does	e path for an xml file, ie. disk0:/ac_profile. The file will be automatically not exist.	
Profile Location	disk0:/asa9-ssl-ipv4v6.xml	Browse Flash
Group Policy	<unassigned></unassigned>	Upload
	Enable 'Always On VPN' for selected group	
	Help Cancel OK	

00	AnyConnect Client Profile Editor - asa9-ssl-ipv4v6	
Profile: asa9-ssl-ipv4v6		About
V2N Preferences (Part 1) Forfinance (Part 2) Backup Servers Certificate Matching Certificate Enrolment Mobile Policy Preferences Server List	Preferences (Part 1) Windows Logon Enforcement SingleLocalLo Windows VPN Establishment LocalUsersOnly Clear SmartCard PIN IP Protocol Supported IPv6,IPv4	
	Help Cancel OK	
888	AnyConnect Client Profile Editor – asa9-ssl-ipv4v6	
Profile: asa9-ssl-ipv4v6		About
VPN Preferences (Part 1) Preferences (Part 2) Rescription	Server List	ñ
Certificate Matching	Hostname Host Address User G., Backup, Autom, CA URL Mobile (Add)	

Note: it is highly recommended that at least one server be defined in a profile.

Cancel OK

-- Inh...

Edit... Delete

Details

4 Ŧ

Certificate Enrollment

🛛 🔐 Server List

SSL to ASA9 (IPv4,IPv6) asa9.example.net

Help )

00	Server List	Entry
Host Display Name (requir. SSL to ASA9 (IPv4 FODN or IP Addr asa9.example.net Group URL asa9.example.net	l,IPv6) User group	Additional mobile-only setti
Backup Server List Host Address	Add Move Up Move Down Delete	Load Balancing Server List "Always On" is disabled. Load Balancing Fields have been disabled. Host Address Add Delete
Primary Protocol Standard Authentication Only (IOS ga Auth Method During IKE Negotiation IKE Identity	SSL	Automatic SCEP Host CA URL Prompt For Challenge Password CA Thumbprint
	ОК	Cancel

生成的XML配置檔案(為簡潔起見省略大部分預設部件):

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
...
</clientInitialization>
```

</HostEntry> </ServerList>

</AnyConnectProfile>

在上述配置檔案中還定義了HostName(可以是任何型別,不需要匹配ASA的實際主機名)和 HostAddress(通常是ASA的FQDN)。

**注意:**HostAddress欄位可以為空,但HostName欄位必須包含ASA的FQDN。

**注意:**除非預先部署配置檔案,否則第一個連線要求使用者鍵入ASA的FQDN。此初始連線將優先 使用IPv4。連線成功後,將下載配置檔案。從這裡將應用配置檔案設定。

# <u>驗證</u>

:

要驗證客戶端是通過IPv4還是IPv6連線,請檢查ASA上的客戶端GUI或VPN會話DB:

• 在客戶端上,開啟Advanced視窗,轉到Statistics頁籤並驗證「Server」的IP地址。第一個使用 者從不支援IPv6的Windows XP系統連線

Cit	sco AnyConnect Secure I I I I I I I AnyCon CISCO	Mobility Client	oility Client	
	Virtual Private Netwo	rk (VPN)	Diagnostics	1.3
	Preferences Statistics Ro	te Details   Firewall   Message Hist	ory	
	Connection Informat	on	^	200
	State: Tunnel Mode (IPv4): Tunnel Mode (IPv6): Duration:	Connected Tunnel All Traffic Drop All Traffic 00:10:01		
	Address Information Client (IPv4): Client (IPv6):	172.16.2.101 Not Available		er-
	Bytes	203.0.113.2		
	Senk: Received:	8644 19831	<b>•</b>	
			Reset Export Stats	
		O Cisco Any	Connect Secure Mobility Client	
			VPN: Connected to asa9.example.net, asa9.example.net	Disconnect
		¢ ()		

第二個使用者通過IPv6連線從Windows 7主機連線到 ASA:

0	Cis	co AnyConnect Secure Mobility	Client	- • -
	،، د	lulu AnyConn	ect Secure Mobility Clien	t
		Virtual Private Network	(VPN) Details Firewall Message History	Diagnostics
	•	Connection Information State: Tunnel Mode (IPv4): Tunnel Mode (IPv6): Duration: Address Information Client (IPv4): Client (IPv4): Server: Bytes Sent: Received: Frames	Connected Tunnel All Traffic Tunnel All Traffic 00: 10:24 172. 16.2. 100 5555-2222-0:0:0:0:0:64 2001:DB8:90:0:0:0:0:2 14427 19940	
ļ			Reset	Export Stats
			Cisco AnyConnect Secure Mobility Client VPN: Connected to asa9.example.net 00:10:24	et. Disconnect

• 在ASA上,從CLI檢查「show vpn-sessiondb anyconnect」輸出中的「Public IP」。在此示例 中,您可以看到與上面相同的兩個連線:一個來自XP over IPv4,一個來自Windows 7 over IPv6:

asa9# show vpn-sessiondb anyconnect Session Type: AnyConnect Username : Nanashi no Gombei Index : 45 Assigned IP : 172.16.2.101 Public IP : 192.0.2.95 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Bytes Tx : 13138 Bytes Rx : 22656 Group Policy : DfltGrpPolicy Tunnel Group : DefaultWEBVPNGroup Login Time : 11:14:29 UTC Fri Oct 12 2012 Duration : 1h:45m:14s

```
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
Username : Uno Who Index : 48
Assigned IP : 172.16.2.100 Public IP : 2001:db8:91::7
Assigned IPv6: fcfe:2222::64
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11068 Bytes Rx : 10355
Group Policy : DfltGrpPolicy Tunnel Group : DefaultWEBVPNGroup
Login Time : 12:55:45 UTC Fri Oct 12 2012
Duration : 0h:03m:58s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

## 相關資訊

• 技術支援與文件 - Cisco Systems