設定 ASA 的 AnyConnect VPN 管理通道

目錄

 簡介

 必要條件

 需求

 採用元件

 背景資訊

 管理隧道的工作

 限制

 設定

 通過ASDM/CLI在ASA上進行配置

 建立AnyConnect管理VPN配置檔案

 AnyConnect管理VPN配置檔案的部署方法

 (可選)配置自定義屬性以支援全隧道配置

 驗證

 疑難排解

 相關資訊

簡介

本文檔介紹如何將ASA配置為VPN網關通過管理VPN隧道接受來自Cisco AnyConnect安全移動客戶端的連線。

必要條件

需求

思科建議您瞭解以下主題:

- 通過自適應安全裝置管理器(ASDM)配置VPN
- •基本自適應安全裝置(ASA)CLI配置
- •X509憑證

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco ASA軟體版本9.12(3)9
- Cisco ASDM軟體版本7.12.2
- Windows 10與Cisco AnyConnect安全移動客戶端版本4.8.03036

注意:下載AnyConnect VPN Web部署包(anyconnect-win*.pkg or anyconnect-macos*.pkg)從Cisco <u>Software Download</u>(僅<u>限註冊</u>客戶)網站下載。將AnyConnect VPN客戶端複製到要下載到遠 端使用者電腦的ASA的快閃記憶體,以與ASA建立SSL VPN連線。有關詳細資訊,請參閱 本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

管理VPN隧道確保無論何時客戶端系統通電時連線到公司網路,而不僅僅是在終端使用者建立 VPN連線時。您可以對辦公室外端點(尤其是使用者通過VPN不經常連線到辦公室網路的裝置)執 行補丁管理。需要企業網路連線的終端作業系統登入指令碼也受益於此功能。

AnyConnect管理隧道允許管理員在使用者登入之前連線AnyConnect,而無需使用者干預。 AnyConnect管理隧道可與受信任網路檢測結合使用,因此僅當終端位於外部並與使用者啟動的 VPN斷開連線時才會觸發。AnyConnect管理隧道對終端使用者是透明的,在使用者發起VPN時自動 斷開。

作業系統/應用程式	最低版本要求
ASA	9.0.1
ASDM	7.10.1
Windows AnyConnect版本	4.7.00136
macOS AnyConnect版本	4.7.01076
Linux	不支援

管理隧道的工作

AnyConnect VPN代理服務在系統啟動時自動啟動。它檢測到管理隧道功能已啟用(通過管理 VPN配置檔案),因此它啟動管理客戶端應用程式以啟動管理隧道連線。管理客戶端應用程式使用 管理VPN配置檔案中的主機條目來啟動連線。然後,VPN隧道按慣例建立,但有一個例外:管理隧 道連線期間不執行軟體更新,因為管理隧道對使用者是透明的。

使用者通過AnyConnect UI啟動VPN隧道,這將觸發管理隧道終止。一旦管理隧道終止,使用者隧 道建立將照常繼續。

使用者斷開VPN隧道的連線,從而觸發管理隧道的自動重建。

限制

- 不支援使用者互動
- 僅支援通過電腦證書儲存區(Windows)進行的基於證書的身份驗證
- 強制實施嚴格的伺服器證書檢查
- 不支援專用代理
- 不支援公共代理(在無法從瀏覽器中檢索本機代理設定的平台上支援ProxyNative值)
- 不支援AnyConnect自定義指令碼

注意:有關詳細資訊,請參閱<mark>關於管理VPN隧道。</mark>

本節介紹如何將Cisco ASA配置為VPN網關,以便通過管理VPN隧道從AnyConnect客戶端接受連線。

通過ASDM/CLI在ASA上進行配置

步驟1.建立AnyConnect組策略。導航至 Configuration > Remote Access VPN > Network (Client) Access > Group Policies.按一下 Add.

注意:建議您建立僅用於AnyConnect管理隧道的新AnyConnect組策略。

1	Home 🦓 Configuration 📴 Monitoring 识 S	Save 🔇 Refresh 🔇 Back 🔘 Fon	ward 💡 Help Type topic Go			diala cisco
	O O Remote Access VPN	Configuration > Remote Ac	cess VPN > Network (Client) Acces	s > Group Policies		
s	? Introduction ▼ ■ Network (Client) Access ■ AnyConnect Connection Profiles > □ AnyConnect Customization/Localizati □ AnyConnect Client Profile	Manage VPN group policies.A VPN g policy information is referenced by To enforce authorization attributes	group is a collection of user-oriented VPN connection profiles and user ac from an LDAP server you must use a ssign	d authorization attribute/value pairs that may be stored in counts. n LDAP attribute map.	nternally on the device or externally on a RADIUS/LDAP server. The group	
4	AnyConnect Client Software				Connection Brofiler Illease	_
- kn	Contraction of the second seco	Name	Туре	Tunneling Protocol	Connection Profiles/Users Assigned To	
8	福田 Group Policies	AnyConnect	Internal	ssl-client	AnyConnect	
	IPsec(IKEv1) Connection Profiles	DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;Defau	IKWE
	IPsec(IKEv2) Connection Profiles					
	Secure Mobility Solution					
	Address Assignment					
	Advanced					
	P Clientess SSL VPN Access					
	MARA Secure Crowns					
	Se I DAP Attribute Man					
	for Local lisers					
	A Secure Desktop Manager					
	Certificate Management					
	Anguage Localization					
	Se Load Balancing					
	P DHCP Server					
	J DNS					
	Advanced					
	A Device Setup					
	🗖 firmell					
	a virewan					
	Remote Access VPN					
	Site-to-Site VPN	Find:	Match Case			
	Device Management					
				Reset Apply		
	-					

步驟2.提供 Name 用於組策略。分配/建立 Address Pool.選擇 Tunneling Protocols 作為 SSL VPN Client 和/或 IPsec IKEv2中,如圖所示。

		Edit Interna	al Group Policy: AnyConnect_MGMT_Tunnel	
General	Name: AnyConnect_MGMT_	Tunnel		
Advanced	Banner: 🗹 Inherit			
	SCEP forwarding URL: 🔽 Inherit			
	Address Pools: Inherit VPN_Po	ool		Select
	IPv6 Address Pools: 🔽 Inherit			Select
	More Options	_		_
	Tunneling Protocols:	Inherit	Clientless SSL VPN 🗹 SSL VPN Client 🗌 IPsec IKEv1 💟 IPsec IKEv2 🗌 L2TP/IPs	ec
	Filter:	🗹 Inherit	0	Manage
	Access Hours:	🗹 Inherit	0	Manage
	Simultaneous Logins:	🗹 Inherit		
	Restrict access to VLAN:	🗹 Inherit	0	
	Connection Profile (Tunnel Group) Lock:	🗹 Inherit	0	
	Maximum Connect Time:	🗹 Inherit	Unlimited minutes	
	Idle Timeout:	🗹 Inherit	None minutes	
	Security Group Tag (SGT):	🗹 Inherit	None (2 – 65519)	
	On smart card removal:	🗹 Inherit	O Disconnect O Keep the connection	
	Timeout Alerts			
	Maximum Connect Time Alert Interval:	🗹 Inherit	Default minutes	
	Periodic Certificate Authentication Interval	: 🗹 Inherit	Unlimited hours	
ind:	Sext Sext	Previous		
		н	elp Cancel OK	

步驟3. 導航至 Advanced > Split Tunneling.配置 Policy 作為 Tunnel Network List Below 並選擇 Network List中,如 圖所示。

• •		Edit Internal G	roup Policy: AnyConnect_MGMT_	[unnel	
General Servers Y Advanced	The VPN client makes split tunneling dee fields.	cisions on the	basis of a network list that can	be specified below by providing the proper parameters to 'Policy' and	i 'Networl
Split Tunneling	DNS Names:	🗹 Inherit			
Browser Proxy ► AnyConnect Client	Send All DNS Lookups Through Tunnel:	Inherit	🔿 Yes 💿 No		
P IPSec(IKEVI) Client	Policy:	Inherit	Tunnel Network List Below	C	
	IPv6 Policy:	🗹 Inherit		0	
	Network List:	Inherit	VPN-Split	•	Manag
c	Pressing this button to set up split exlus Set up Split Exclusion for Web Securi Intercept DHCP Configuration Message	sion for Web S ty	iecurity proxies. oft Clients		_
Find:	Next C	I Previous Help	Cancel OK		<u> </u>

注意:如果未同時為IP協定(IPv4和IPv6)推送客戶端地址, Client Bypass Protocol 設定必須為 enabled 以使對應的流量不會被管理通道中斷。要配置,請參閱<u>步驟4</u>。

步驟4. 導航至 Advanced > AnyConnect Client. 設定 Client Bypass Protocol 成長至 Enable. 按一下 OK 儲存,如 圖所示。

• •		Add Internal Group Policy	
General	Keep Installer on Client System:	☑ Inherit O Yes O No	
Servers	Datagram Transport Layer Security (DTLS):	☑ Inherit	
Split Tunneling	DTLS Compression:	☑ Inherit	
Browser Proxv	SSL Compression:	☑ Inherit O Deflate O LZS O Disable	
▶ IPsec(IKEv1) Client	Ignore Don't Fragment(DF) Bit:	🗹 Inherit 💿 Enable 💿 Disable	
	Client Bypass Protocol:	Inherit O Enable Disable	
	FQDN of This Device:	🗹 FQDN	
	MTU:	🗹 Inherit	
	Keepalive Messages:	☑ Inherit Disable Interval: seconds	
	Optional Client Modules to Download:	🗹 Inherit	٢
0	Always-On VPN:	☑ Inherit O Disable O Use AnyConnect Profile setting 0	
	Client Profiles to Download:	🗹 Inherit	
		Add 1 Delete	
		Profile Name Profile Usage/Type	
			- 1
			- 1
			- 1
Find:	Novt A		
rind.	- Next		
		Help Cancel OK	

步驟5.如圖所示,按一下 Apply 將配置推送到ASA。

🚮 Ho	ome 🍫 Configuration 📴 Monitoring 🔚	Save 🔇 Refresh 🔇 Back 🔘 Forw	ard 💡 Help Type topic Go		cisco
	O O Remote Access VPN	○ ○ ○ Configuration > Remote Acc	ess VPN > Network (Client) Acce	ss > Group Policies	
ks	Introduction Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localizati AnyConnect Client Profile AnyConnect Client Profile	Manage VPN group policies.A VPN g policy information is referenced by To enforce authorization attributes f Add C C C C C C C C C C C C C C C C C C	roup is a collection of user-oriente /PN connection profiles and user a from an LDAP server you must use sign	ed authorization attribute/value pairs that may be stored in ccounts. an <u>LDAP attribute map</u> .	ternally on the device or externally on a RADIUS/LDAP server. The group
m	AnyConnect Client Software	Marrie	T	Turneline Protocol	Connection Profiles/Users
ook	B Group Policies	Name	Type	Tunneling Protocol	Assigned To
	IPsec(IKEv1) Connection Profiles	AnyConnect	Internal	ssl-client	AnyConnect
	IPsec(IKEv2) Connection Profiles	DiltGrpPolicy (System Default)	Internal	ikev1;ikev2;i2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;DefaultWE
	Secure Mobility Solution	AnyConnect_MGM1_Tunnel	internal	ikevz;ssi-client	Anyconnect_MGM1_1unnet
	Address Assignment				
	Advanced				
Þ	Clientless SSL VPN Access				
Ŧ	AAA/Local Users				
	AAA Server Groups				
	Se LDAP Attribute Map				
	g Local Users				
Þ	A Secure Desktop Manager				
Þ	Certificate Management				
	Language Localization				
	Load Balancing				
	DHCP Server				
	A DNS				
P	C Advanced				
	9 a. j. d.				
	B Device Setup				
1	h Firewall				
	Remote Access VPN				
6	💦 Site-to-Site VPN	Find:	Match Case		
3	Device Management				
	*			Reset Apply	

組策略的CLI配置:

```
ip local pool VPN_Pool 192.168.10.1-192.168.10.100 mask 255.255.255.0
! access-list VPN-Split standard permit 172.16.0.0 255.255.0.0
! group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
vpn-tunnel-protocol ikev2 ssl-client
```

split-tunnel-network-list value VPN-Split
client-bypass-protocol enable
address-pools value VPN_Pool

步驟6.建立AnyConnect連線配置檔案。導航至 Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. 按一下 Add.

注意:建議您建立僅用於AnyConnect管理隧道的新AnyConnect連線配置檔案。

• Mende Access VMP • Mende A	Home 🔧 Configuration [Monitoring	Save 🔇 Refresh 🔇 Back 🌘	Forward ? Help Ty	pe topic Go			cise
 Indication <	O O O Remote Access VPN	O O Configuration > Rem	ote Access VPN > Netwo	rk (Client) Access > AnyConne	ct Connection Profiles		
Connection Profiles Connection Profiles Subard Access Subard Client Services Connection Profiles Subard Client Services Connection Profiles Subard Client Services Laguage Localization Connection Profiles Subard Client Services Subard Client Service Subard Client Se	? Introduction ? Network (Client) Access > 3/myConnect Connection Profiles > 3/myConnect Client Profile 3/myConnect Client Software	The security appliance auton VPN Client supports IPsec (Ik Access Interfaces Zenable Cisco AnyConnec SSL access must be enabled	natically deploys the Cisco (Ev2) tunnel as well as SSL t VPN Client access on th if you allow AnyConnect of	AnyConnect VPN Client to rem tunnel with Datagram Transpor	ote users upon connection. The initia : Layer Security (DTLS) tunneling opti below rser (Web Launch) .	al client deployment requires end-use ons.	er administrative rights. The Cisco AnyConnect
	Dynamic Access Policies		IPs	rc (IKEv2) Access			
 Preclatery: Jointe: Coll Profiles Secure Mobility Solution Advanced Port Settings Secure Booking State Compaction profile on the login page. Secure State Compaction profile on the login page. Connection Profiles Connection Profiles Connection profile funnel group specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here. Advanced Port Settings Advanced Port Settings Advanced Port Settings Connection Profiles Connection profile funnel group specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here. Advanced Port Settings Advanced Port Settings Advanced Port Settings Port Settings	Group Policies	Interface Allow Access	Enable DTLS Alle	w Access Enable Client Service	es Device Certificate		
 Security of control of marked and a second second	Psec(KEv2) Connection Profiles	outside 🗹					
 Modifiess Assignment Moduless Assignment Moduless Assignment Moduless SSL VPN Access MAXLocal Users MAXLocal Users Moduless SSL VPN Access Moduless Advanced Moduless SSL VPN Access Moduless SSL VPN Access Moduless SSL VPN Access Moduless Advanced Moduless SSL VPN Access Moduless SSL VPN Access Moduless SSL VPN Access Moduless SSL VPN Access Moduless Advanced Moduless	Secure Mobility Solution	inside			Port Settings		
 S Advanced S Advanced	Address Assignment						
 ▷ Cliencless SSL VPN Access ▲ AAA Server Groups ▲ LAA Server Groups ▲ LAB Server Groups ▲ Journeet > Shutdown portal login page. Connection Profiles Connection profile furnel group specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here. Connection Profiles Connection profile Erind: Connection Profiles Connection Profile Erind: Connection Profile Erind: Match Case Name SSL Enabled Prec Enabled Advanced Advanced Coroup Policy AAALLOCAJ DMGropPolicy AnyConnect AnyConnect AnyConnect AnyConnect 	Advanced	Bypass interface access	lists for inbound VPN sess	ions			
 Advanced Users Advanced Connection profile funnel group specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here. Connection profile funnel group specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here. Connection profile funnel group specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here. Connection profile funnel group specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here. Advanced Advanced Stenabled Phece Inabled Alases Authentication Method Croup Policy DefaultXES/PORGroup Advanced Advance	Clientless SSL VPN Access	Access lists from aroun poli	cy and user policy always	apply to the traffic			
MAX Server Groups ILogin Page Setting ILogin Page Setting Articluk Management Language Localization ILogin Stationing PhiCP Server DNS INS Name Statistication Name Statistication Maximum Advanced Name Statistication Maximum Advanced	T AAA/Local Users	Access lists from group poin	cy and user poincy amays	apply to the frame.			
 ^A LOW-Rains Raip ^B Low livers ^A Low user to select connection profile on the login page. ^A Low user to select connection profile on the login page. ^B Low Load Balancing ^B Load Balancing ^B Low Server ^B DKS ^A Load ^B Edit ^B Delete ^B Ind: ^B Thete Find: ^B Advanced ^A Low and ^B Edit ^B Delete ^B Find: ^B Match Case ^A Low Connection Profile <u>Find: ^B Philory ^A Low Connection ^A Low Connecti ^A Low Connecti ^A Low Connect</u>	AAA Server Groups	Login Page Setting					
 Secure Desktop Manager Gertificate Managernent Land galancing Did Drick Server DNS Advanced In me SSL Enabled Prece Enabled Prece Enabled Prece Enabled Prece Enabled Advanced Advanced	Coral lisers	Allow user to select cont	nection profile on the logi	n page. 💿			
 Certificate Management Language Localization Language Localization Language Localization Language Localization Dick' Server DNS Dis Advanced State Language Localization State Localization State Localization State Localization State Localization State Localization State Localizati	> A Secure Desktop Manager	Shutdown portal login pa	age.				
Connection profiles Connection Connectio	En Certificate Management		-				
Load Balancing Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from Certificate to connection profile here. D DIS Advanced Name SSL Enabled Prece Enabled Alases Advanced OfficripPolicy DefaultWEEVPNGroup Image: Connect AnyConnect AnyConnect	3 Language Localization	Connection Profiles					
Image: Direct server Image: Direct server Image: Direc	Se Load Balancing	Connection profile (tunnel ge	roup) specifies how user i	s authenticated and other param	eters. You can configure the mapping	g from certificate to connection profi	le <u>here</u> .
Name SSL Enabled IPsec Enabled Aliases Authentication Method Group Policy DefaultRAGroup IPsec Enabled Aliases AAALLOCAL) DffGripPolicy DefaultWEBVPNGroup Image: Connect AnyConnect AnyConnect AnyConnect	Pr DHCP Server	Add 🗹 Edit 🎁 Delete	Find:	O O Match Case			
Name SSL Enabled IPsec Enabled Aliases Authentication Method Group Policy DefaultRAGroup Image: SSL Enabled Image: SSL Enabled Aliases Authentication Method DffGroup Policy DefaultWEBVPNGroup Image: SSL Enabled Image: SSL Enabled Image: SSL Enabled Aliases Authentication Method DffGroup Policy AnyConnect Image: SSL Enabled Image: SSL Enabled Image: SSL Enabled Image: SSL Enabled DffGroup Policy AnyConnect Image: SSL Enabled AnyConnect Image: SSL Enabled Image: SSL Enabled <td< td=""><td>Advanced</td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	Advanced						
DefaultikAcroup DefaultikEVPNGroup DefaultikEVPNGroup AnyConnect A		Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultWEBVPKGroup Z AAALCCAU DHKrpPolicy AnyConnect AAALLOCAU AnyConnect AAALLOCAU AnyConnect		DefaultRAGroup				AAA(LOCAL)	DfltGrpPolicy
AnyConnect Adduction AnyConnect		DefaultWEBVPNGroup		<u> </u>		AAA(LOCAL)	DfltGrpPolicy
		AnyConnect			AnyConnect	AAA(LOCAL)	AnyConnect
A Device Setup	A Device Setup						
	Simual						
St income	S rirewan						
Remote Access VPN	Kemote Access VPN						
Site-to-Site VPN	Site-to-Site VPN						
Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.		Let group URL take prece	edence if group URL and c	ertificate map match different co	nnection profiles. Otherwise, the co	nnection profile that matches the cer	tificate map will be used.
E Device Management	Device Management						
» Reset Apply					Reset Apply		

步驟7.提供 Name 連線配置檔案,並設定 Authentication Method 作為 Certificate only.選擇 Group Policy 作為 在<u>步驟1中建立的路徑</u>。

Basic	Name:	AnyConnect_MGMT_Tunnel					
Advanced	Aliases:						
	Authoritation						
	Method:	Certificate only					
	AAA Samar Crown			Managa			
	AAA Server Group:	LOCAL		Manage			
		Use LOCAL if Server Group fails					
	SAML Identity Provider						
	SAML Server :	None		Manage			
	Client Address Assignment						
	DHCP Servers:						
		💿 None 💿 DHCP Link 💿 DHCP Subnet					
	Client Address Pools:			Select			
	Client IPv6 Address Pools	:		Select			
	Default Crown Policy						
	Group Policy:	AnyConnect MCMT Tunnel	•	Manage			
	(Following fields are linke	d to attribute of the group policy selected above)	<u> </u>	managem			
	✓ Enable SSL VPN client protocol						
	Enable IPsec(IKEv2)	client protocol					
	DNS Servers:						
	WINS Servers:						
	Domain Name:						
	bomain Name.						
Find:		Sext Previous					

注意:確保ASA上存在來自本地CA的根證書。 導航至 Configuration > Remote Access VPN > Certificate Management > CA Certificates 以新增/檢視證書。

注意:請確保由同一本地CA頒發的身份證書存在於電腦證書儲存區(Windows)和/或系統金鑰 鏈(MacOS)中。

步驟8.導航至 Advanced > Group Alias/Group URL.按一下 Add 在 Group URLs 並新增 URL.確保 Enabled 已選中。按一下 OK 儲存,如圖所示。

Add AnyConnect Connection Profile

Basic V Advanced General Client Addressing Authentication Secondary Authentication Authorization Accounting Group Alias/Group URL	 Enable the display of Radius Reject-Message on the login screen when authentication is rejected Enable the display of Securid messages on the login screen Connection Aliases This SSL VPN access method will present a list of aliases configured for all connection profiles. You r the Login Page Setting in the main panel to complete the configuration. Add Delete (The table is in-line editable.) Alias
	Croup URLs This SSL VPN access method will automatically select the connection profile, without the need for use Add Delete (The table is in-line editable.) URL Enabled URL: https://asa.example.com/AnyConnect_MGMT_Tunnel © Enabled Help Cancel OK
Find:	Next OPrevious
	Help Cancel OK

如果使用IKEv2,請確保 IPsec (IKEv2) Access 在用於AnyConnect的介面上啟用。

O O Remote Access VPN	O O Confi	guration > Remot	e Access VPN > I	Network (Client)	Access > AnyConnect Con	nection Profiles					
Introduction Network (Client) Access AnyConnect Connection Profiles	The security Client supp	e security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN lent supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.									
AnyConnect Customization/Local AnyConnect Client Profile AnyConnect Client Software	Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below SL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).										
Group Policies	Interface	SSL Access Allow Access	Enable DTLS	IPsec (IKEv2) Acc Allow Access	Enable Client Services	Device Certificate					
Prec(IKEV1) Connection Profiles	outside	S			✓						
Secure Mobility Solution	inside					Port Settings					

步驟9.按一下 Apply 將配置推送到ASA。



連線配置檔案的CLI配置(隧道組):

tunnel-group AnyConnect_MGMT_Tunnel type remote-access tunnel-group AnyConnect_MGMT_Tunnel general-attributes default-group-policy AnyConnect_MGMT_Tunnel tunnel-group AnyConnect_MGMT_Tunnel webvpn-attributes authentication certificate group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable

步驟10.確保在ASA上安裝受信任證書並繫結到用於AnyConnect連線的介面。導航至 Configuration > Remote Access VPN > Advanced > SSL Settings 新增/檢視此設定。

注意:請參閱在ASA上安裝身份證書。

O Remote Access VPN	O O Configuration > Remote Acces	ss VPN > Advanced > SSL Settings				
Introduction						
Network (Client) Access	Configure SSL parameters. These para	meters affect both ASDM and SSL VPN acc	ess.			
AnyConnect Customization AnyConnect Client Profile	The minimum SSL version for the sec	urity appliance to negotiate as a "server":	TLS V1	0	OTLSV1 OTLSV1.2	
AnyConnect Client Softwar	The minimum SSL version for the sec	urity appliance to negotiate as a "client":	TLS V1	0		
Group Policies	Diffie-Hellman group to be used with	SSL:	Group2 - 1024-bit modulus	0		
IPsec(IKEv1) Connection P IPsec(IKEv2) Connection P	ECDH group to be used with SSL:		Group19 - 256-bit EC	0		
Secure Mobility Solution	Encryption					
Standard Address Assignment	Cipher Version	Cinhar Saruribul aud		Cipher Algorithm	e / Custom String	1
3 Advanced	Default	Madium		DES_CRC2_SUA	AFC128_SUA DUE_DCA_AFC128_SUA AFC256_SUA DUE_DCA	Edit
Clientless SSL VPN Access	TISVI	Medium		DHE-PSA-AES2	CE-SUA AECOSE-SUA DUE-DCA-AECIDE-SUA AECIDE-SUA	
AAA/Local Users	TISVI 1	Medium		DHE-RSA-AES2	SG_SHA AES25G_SHA DHE_DCA_AES128_SHA AES128_SHA	
AAA Server Groups	10/1.2	Medium		CONE CODE		
Se LDAP Attribute Map	0710/1	Medium		DUE DEA AFEN	AES230-GUM-SHA304 ECDHE-RSA-AES230-GUM-SHA304 D	
C Local Lisers	010/1	Medium		CODUC CODEA	20-3NA AE3230-3NA DHE-K3A-AE3128-3NA AE3128-3NA	
Secure Deckton Manager	011391.2	Medium		ECDHE-ECDSA-	AES250-GCM-SHA384 ECDHE-KSA-AES250-GCM-SHA384 D	
Secure Desktop Manager						
Certificate Management						
Language Localization						
Load Balancing	Conver Name Indication (CNI)					
DHCP Server	Server wame indication (SNI)					
DNS	Domain		Certificate			Add
Advanced						Edit
SSI Settings						CON
Reference Identity						Delete
D Cartificate to Am Connect						
Certificate to AnyConnect						
HITP Redirect						
Maximum VPN Sessions						
Crypto Engine						
	Certificates					
	Specify which certificates, if any, s	hould be used for SSL authentication on ea	ch interface. The fallback certificate	will be used on interfa	ces not associated with a certificate of their own.	
	Interface	Drimany Castificate	Lond Polyaging Castificate		Key Ture	
Pevice Setup	Interrace	Primary Cercincate	coad balancing Certificate		Key-Type	Edit
	inside					
irewall	management					
	outside	ROOT-CA:hostname=ASA.example	.co		Primary: RSA (2048 bits), Load Balancing: none	
emote Access VPN						
ite-to-Site VPN						
Device Management						
			Deces Control	h.		

SSL信任點的CLI配置:

ssl trust-point ROOT-CA outside

建立AnyConnect管理VPN配置檔案

步驟1. 建立AnyConnect客戶端配置檔案。導航至 Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile.按一下 Add中,如圖所示。

O O Remote Access VPN O O Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile	
Production Prevark (Client) Access AnyConnect Connection Profile AnyConnect Client Software Add Edit C Croup Policy Detect Detect	can select the 'Add'
Profile Isaar Profile Isaar Croup Policy Profile Laar	
Image: Description of the state of the	
経 Reference Identity Sectificate to AnyConnect and で 地打TP Redirect M Maximum VPN Sessions G Crypto Engine	
💑 Device Setup	
Firewall	
C Remote Access VPN	
Z Reset Apply	

步驟2.提供 Profile Name.選擇 Profile Usage 作為 AnyConnect Management VPN profile.選擇 Group Policy 在<u>步驟</u> 1中建立。按一下 Ок 中,如圖所示。

ofile Name		Profile Usage	Group Policy		Profile Location
	• • •	Add AnyConnect Client Pro	ofile		
	Profile Name	AnyConnect_MGMT_Profile			
	Profile Usage	AnyConnect Management VPN Profile	0		
	Enter a device f created if it do	ile path for an xml file, ie. disk0:/ac_profile. The file w es not exist.	ill be automatically		
	Profile Location	disk0:/anyconnect_mgmt_profile.vpnm		Browse Flash	
				Upload	
	Group Policy	AnyConnect_MGMT_Tunnel			
		Enable 'Always On VPN' for selected group			
		Help Cancel	ОК		
			Reset Apply		

步驟3.選擇建立的配置檔案,然後按一下 Edit中,如圖所示。



步驟4.導航至 Server List.按一下 Add 以新增新的伺服器清單條目,如下圖所示。

ine. Anyeenneer_ine					Ab
VPN Preferences (Part 1)	Server List				
Preferences (Part 2)					
Backup Servers	Hostname	Host Address	User Group	Backup Server List	Certificate Pins
Certificate Matching					
Server List					
	Note: at most o	one server can be defined	l in a management VP	N profile. Add.	Delete
				Edit	Details

步驟5.提供 Display Name.新增 FQDN/IP address ASA的。提供 User Group 作為隧道組名稱。 Group URL 自動填入 FQDN 和 User Group.按一下 OK.

Server	Certificate Pinning
Primary Server Display Name (required) AnyConnect_MGMT_Tunnel FQDN or IP Addr User Group (required)	Connection Information Primary Protocol SSL 📀
asa.example.com / AnyConnect_MGMT. Group URL asa.example.com/AnyConnect_MGMT_Tunnel	Auth Method During IKE Negotiation EAP-AnyConnect 🗘
Backup Servers Host Address	Add Move Up Move Down Delete
ОК	Cancel

注意:FQDN/IP地址+使用者組必須與步驟8中配置AnyConnect連線配置檔案時提到的組 URL<u>相同</u>。

注意:將IKEv2作為協定的AnyConnect也可用於建立到ASA的管理VPN。確保 Primary Protocol 設定為 IPsec 在<u>步驟5</u>中。

步驟6.如圖所示,按一下 ок 儲存。

file: AnyConnect_MC	GMT_Profile				Ab
VPN	Server List				
Preferences (Part 1)					
Backup Servers	Hostname	Host Address	User Group	Backup Server List	Certificate Pins
Certificate Pinning	AnyConnect_MGM	T_T asa.example.com	AnyConnect_MGMT	T Inherited	Certificate Fills
Certificate Matching					
Server List					
	Note: at most o	one server can be defined	in a management VPN	I profile Add	Delete
	Note. at most e	she server can be defined	in a management vriv	Add	Delete
				Edit	Details

步驟7.按一下 Apply t將配置推送到ASA,如圖所示。

1	Home 🍕 Configuration 👰 Monito	ing 調 Save 💽 Refresh 🔇 Back 🔘 Forv	vard 💡 Help Type topic Go			cisco
	O O O Remote Access VPN	○ ○ ○ Configuration > Remote Access Vi	PN > Network (Client) Access > AnyConnect Client	nt Profile		
Ĕ	Introduction					
ŝ	V Network (Client) Access					
8	AnyConnect Connection Profil	This panel is used to manage AnyConnect	Client Profiles and perform group assignment for A	nyConnect version 2.5 or later.You can select a profi	le to edit, change group or to delete. You can select the 'Add'	
n.	h AmConnect Customization/L	The profile Usage field is introduced with	he forum Mehility Solution. This field contains diff	or client profiles between local machine and device.		
	Am Connect Client Profile	The prome usage neid is introduced with t	the secure mobility solution. This neid contains unit	erent prome usage in Anyconnect version 5.0 and ia	ter.	
2	Am Connect Client Software	HostScan configuration can be performed	by going to Secure Desktop Manager/HostScan. If '	HostScan' is not visible under 'Secure Desktop Manag	er', you will need to restart ASDM.	
2	Demonsis Assess Balisias					
ð.	Craw Palisias	Add 17 Edit 22 Change Crown Policy	Delete Tilmport 🖡 Export 🖓 Validate			
8	Billion (Kful) Connection Brafil	* Add Care 25 change Group Foncy	Belete a import a cxport gy vandate			
	Psec(KEVI) Connection Profil	Profile Name	Profile Usage	Group Policy	Profile Location	
	Psec(ikev2) Connection Profil	AnyConnect_MGMT_Profile	AnyConnect Management VPN Profile	AnyConnect_MGMT_Tunnel	disk0:/anyconnect_mgmt_profile.vpnm	
	Secure Mobility Solution					
	Address Assignment					
	P W Advanced					
	P Chendess SSL VPN Access					
	REF AAA Correct Correct					
	AAA Server Groups					
	EDAF Attribute Map					
	B Cocura Dachter Manager					
	Gertificate Management					
	Ceronicate Management					
	8.8 Load Palancing					
	Coad balancing					
	B DNS					
	T T Advanted					
	the Connection Category					
	SEL Satting					
	Reference Identify					
	Cartificate to AmConnect and					
	WITTP Redirect					
	Maximum VPN Services					
	Comto Engine					
	Ba Crypto Engine					
	Q Davidas Satura					
	Bevice Setup					
	Firewall					
	Remote Access VPN					
	Site-to-Site VPN					
	Device Management					
	No overce management			Devel Australia		
	2 T			Appry		

新增AnyConnect管理VPN配置檔案後的CLI配置。

webvpn enable outside hsts enable max-age 31536000 include-sub-domains no preload no anyconnect-essentials anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm anyconnect enable tunnel-group-list enable cache disable error-recovery disable 1 group-policy AnyConnect_MGMT_Tunnel internal group-policy AnyConnect_MGMT_Tunnel attributes vpn-tunnel-protocol ikev2 ssl-client split-tunnel-network-list value VPN-Split client-bypass-protocol enable address-pools value VPN_Pool webvpn anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt

AnyConnect客戶端電腦上的AnyConnect管理VPN配置檔案:

```
<?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="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>
```

<ShowPreConnectMessage>false</ShowPreConnectMessage>

```
<ProxySettings>IgnoreProxy</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>30</AuthenticationTimeout>
```

--- Output Omitted ---

```
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>false</AllowManualHostInput> </ClientInitialization>
```

注意:如果使用者AnyConnect VPN配置檔案中使用了受信任網路檢測(TND),則建議匹配管 理VPN配置檔案中的相同設定,以獲得一致的使用者體驗。根據應用到使用者VPN隧道配置 檔案的TND設定觸發管理VPN隧道。此外,管理VPN配置檔案中的TND連線操作(僅在管理 VPN隧道處於活動狀態時實施)始終應用於使用者VPN隧道,以確保管理VPN隧道對終端使 用者透明。

注意:在任何最終用戶PC上,如果管理VPN配置檔案啟用了TND設定,且使用者VPN配置檔 案缺失,則它會考慮TND的預設首選項設定(在AC客戶端應用程式中的預設首選項中禁用了 該設定)來代替缺失的使用者VPN配置檔案。這種不匹配可能會導致意外/未定義的行為。 預設情況下,在預設首選項中禁用TND設定。

要克服AnyConnect客戶端應用程式中的預設首選項硬編碼設定,終端使用者PC必須擁有兩個 VPN配置檔案,一個使用者VPN配置檔案和一個交流管理VPN配置檔案,並且兩者必須具有 相同的TND設定。

管理VPN隧道連線和斷開背後的邏輯是,為了建立管理VPN隧道,AC代理使用使用者VPN配 置檔案TND設定,而對於管理VPN隧道的斷開,它將檢查管理VPN配置檔案TND設定。

AnyConnect管理VPN配置檔案的部署方法

使用ASA連線配置檔案成功完成使用者VPN連線,以便從VPN網關下載AnyConnect管理VPN配置檔案。

注意:如果用於管理VPN隧道的協定是IKEv2,則需要通過SSL建立第一個連線(為了從 ASA下載AnyConnect管理VPN配置檔案)。

 AnyConnect管理VPN配置檔案可以通過GPO推送或手動安裝手動上傳到客戶端電腦(確保配置 檔名稱為 VpnMgmtTunProfile.xml)。

需要新增配置檔案的資料夾位置:

Windows: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun macOS: /opt/cisco/anyconnect/profile/mgmttun/

(可選)配置自定義屬性以支援全隧道配置

預設情況下,管理VPN隧道需要包括隧道配置的拆分,以避免對使用者發起的網路通訊產生影響。 在管理隧道連線使用的組策略中配置自定義屬性時,可以覆蓋此屬性。

步驟1.導航至Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. 按一下 Add中,如圖所示。



步驟2.將自定義屬性Type設定為 ManagementTunnelAllAllowed 並提供 Description. 按一下 OK中,如圖所示。

) <u>Configurat</u>	tion > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes
rations of cu	ustom attribute types and these attributes are enforced in AnyConnect group policy, AnyConnect dynamic access policy and AnyConnect custom attribute names
a al est sous la	
tad 🔤 Edit	
1	Description
	Crasta Custom Attributa Tuna
	Type: ManagementTunnelAllAllowed
	Type: ManagementTunnelAllAllowed ManagementTunnelAllAllowed
	Type: ManagementTunnelAllAllowed ManagementTunnelAllAllowed Description:
	Type: ManagementTunnelAllAllowed ManagementTunnelAllAllowed Description:
	Type: ManagementTunnelAllAllowed ManagementTunnelAllAllowed Description:
	Type: ManagementTunnelAllAllowed ManagementTunnelAllAllowed Description: Help Cancel OK
	Type: ManagementTunnelAllAllowed ManagementTunnelAllAllowed Description: Help Cancel OK
	Type: ManagementTunnelAllAllowed ManagementTunnelAllAllowed Description: Help Cancel OK

步驟3. 導航至 Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. 按一下 Add中,如圖所示。



步驟4.選擇型別作為 ManagementTunnelAllAllowed. 將名稱設定為 true.按一下 Add提供自定義屬性值,如 圖所示。

e Nam	ne Values			
	Type: Name:	ManagementTunnelAllAllowed true Value	Add	Manage
			Edit Delete	
	Configure Value	5:		

步驟5.將值設定為 true.按一下 OK中,如圖所示。

	Create Cu	ustom Attribute Name		
Type:	ManagementTunnelAllAllowed	d	\$	Manage
Name:	true			
	Value		Add	
•		Add Value	E Pr	
true				
alue:				

步驟6.導航至 Configuration > Remote Access VPN > Network (Client) Access > Group Policies.選擇組策略。 按一下 Edit 中,如圖所示。



步驟7.如圖所示,導覽至 Advanced > Split Tunneling.將策略配置為 Tunnel All Networks.

• •		Edit Interr	nal Group Policy: AnyConnect_MGMT_Tunnel		
General Servers	The VPN client makes split tunneling de fields.	cisions on the	e basis of a network list that can be specified below by providing the proper parameters to 'Polic	y' and 'Network L	Ji:
General Servers Advanced Split Tunneling Browser Proxy AnyConnect Client IPsec(IKEv1) Client	The VPN client makes split tunneling de fields. DNS Names: Send All DNS Lookups Through Tunnel: Policy: IPv6 Policy: Network List: Pressing this button to set up split exlu Set up Split Exclusion for Web Securi Intercept DHCP Configuration Message	Cisions on the Cisions on the Inherit Inherit Inherit Inherit Inherit Inherit Inherit Inherit Inherit Inherit	e basis of a network list that can be specified below by providing the proper parameters to 'Polic Yes No Tunnel All Networks Security proxies. oft Clients	y' and 'Network L ○ ○ Manage	
Find:	Next	Previous			
			Help Cancel OK		

步驟8.導航至 Advanced > Anyconnect Client > Custom Attributes.按一下 Add中,如圖所示。

• •	Edit Internal Group Policy: AnyConnect_MGMT_Tunnel
General Servers Advanced Split Tunneling Browser Proxy AnyConnect Client Login Setting Client Firewall Key Regeneration Dead Peer Detection Custom Attributes IPsec(IKEv1) Client	Configuration of custom policy attributes.
Find:	Next Previous Help Cancel OK

步驟9. 選擇屬性型別作為 ManagementTunnelAllAllowed 並選擇值作為 true.按一下 OK中,如圖所示。

pe		Name of Value	
	• • •	Create Custom Attribute	
	Attribute type:	ManagementTunnelAllAllowed	lanage
	Omit the value		
	Select Value:	true 🗘 M	lanage

步驟10.按一下 Apply 將配置推送到ASA,如圖所示。

Non-On-Charles Remote Access VPN Image: Access VPN Access Image: Access VPN Access Image: Access VPN Access Image: Access VPN Second Clambraction (Clambraction) Image: Access VPN Second Clambraction) Image: Accentect Under C	🚳 Home 🍓 Configuration 📴 Monitoring 🎧	Save 🔇 Refresh 🔇 Back 🔘 Forwa	rd 💡 Help Type topic Go		cisco
 Production Production	000 Remote Access VPN	○ ○ ○ Configuration > Remote Acce	ss VPN > Network (Client) Access > 0	Group Policies	
Image: Construction Profiles Users Name Type Tunneling Protocol Connection Profiles Users Image: Construction Profiles Users Sec(IKLS) Connection Profiles Sec(IKLS) Connection Profiles Sec(IKLS) Connection Profiles Image: Construction Profiles Users Sec(IKLS) Connection Profiles Sec(IKLS) Connection Profiles AnyConnect AnyConnect Image: Construction Profiles Users Sec(IKLS) Connection Profiles Sec(IKLS) Connection Profiles Sec(IKLS) Connection Profiles Image: Construction Profiles Users Sec(IKLS) Connection Profiles Sec(IKLS) Connection Profiles Sec(IKLS) Connection Profiles Image: Construction Profiles Users Sec(IKLS) Connection Profiles Sec(IKLS) Connection Profiles AnyConnect Image: Construction Profiles Users Secure Abality Solution Name Name Name Image: Construction Profiles Users Secure Abality Solution Name Name Name Image: Construction Profiles Users Secure Abality Solution Name Name Name Image: Construction Profiles Users Secure Abality Solution Name Name Name Image: Construction Profiles Users Secure Abality Solution Name Name Name Image: Construction Profiles Users Secure Abality Solution Name Name Name <t< th=""><th>Introduction Pretwork (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localizati AnyConnect Client Profile AnyConnect Client Software</th><th>Manage VPN group policies. A VPN group policy information is referenced by VF To enforce authorization attributes fm Add ? @ Edit 1 Delete 2 Assi</th><th>up is a collection of user-oriented aut N connection profiles and user accoun om an LDAP server you must use an LD gn</th><th>orization attribute/value pairs that may be stored in ts. AP attribute map.</th><th>nternally on the device or externally on a RADIUS/LDAP server. The group</th></t<>	Introduction Pretwork (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localizati AnyConnect Client Profile AnyConnect Client Software	Manage VPN group policies. A VPN group policy information is referenced by VF To enforce authorization attributes fm Add ? @ Edit 1 Delete 2 Assi	up is a collection of user-oriented aut N connection profiles and user accoun om an LDAP server you must use an LD gn	orization attribute/value pairs that may be stored in ts. AP attribute map.	nternally on the device or externally on a RADIUS/LDAP server. The group
Image: Product Notice State Assignes to Assigne to Assignes to Assigne to Assignee to Assig	Dynamic Access Policies	Name	Туре	Tunneling Protocol	Connection Profiles/Users
Image: Secure Mobility Solution Psecure Mobility Solution Image: Secure Desking Manager Psecure Desking Manager Image: Local Users Secure Desking Manager Image: Longuage Localization Psecure Desking Manager Image: Desking Psecure Secure Desking Image: Desking Psecure Se	Group Policies	AnyConnect	Internal	ssl-client	Assigned to AnyConnect
Psec(IEX.2) Connection Profiles Secure Mobility Solution > Sp.Address Sts. VPN Access > MAX.Secure Groups @ LDAP Attribute Map Ø LDAP Attribute Map Ø LOAP Attribute Map Ø LOAP Attribute Map Ø LOAP Attribute Map Ø LDAP Attribute Map Ø LOAP Attribute Map Ø LOAP Attribute Map Ø LOAP Attribute Map Ø LOAP Attribute Map Ø DAP Attribute Map Ø LAP Attribute Map Ø DAP Attribute Map Ø DAP Attribute Map Ø DAP Attribute Map Ø DAP Sever Ø DAS > Ø Advanced	IPsec(IKEv1) Connection Profiles	DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;DefaultWE
Secure Mobility Solution Secure Mobility Solution Address Assignment Control Server Control S	Psec(IKEv2) Connection Profiles	AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel
 > 3 Address Assignment > 3 Secure Desktop Manager > 3 Secure Desktop M	Secure Mobility Solution				
 Image: Solution of the solution	Address Assignment				
Image: Controls Source Provides Source Correction Image: Control Source C	Giantiarr SSI VIDN Accorr				
AAA Server Groups Age DAP Attribute Map Go Loal Users Secure Desktop Manager Bo Secure Desktop Manager Destinate Management Destinate Management Destinate Management Destinate Balancing Det Des Server Jons DNS DNS DNS	T AAA/Iocal lisers				
IDAP Attribute Map	AAA Server Groups				
	Mag LDAP Attribute Map				
 A scure Desktop Manager B careve Desktop Ma	🙀 Local Users				
▷ III Certificate Management Stanuage Localization ♥ Locd Balancing ● Def Server	A Secure Desktop Manager				
S Language Localization S Language Localization P DHCP Server P DHCP Server P S Advanced	Certificate Management				
Coto Battorig POHCP Server Jo DKS F S Advanced	Language Localization				
B DNS ► S Advanced	PhiCP Server				
▶ S Advanced	A DNS				
	Advanced				
	~				
2. Device Setup	Device Setup				
S Firewall	Eirewall				
S Remote Access VPN	Kemote Access VPN				
Image: Site-to-Site VPN Find: Image:	Site-to-Site VPN	Find:	Match Case		
Device Management	Device Management				
Reset Apply	*			Reset Apply	

CLI配置 ManagementTunnelAllAllowed 新增自定義屬性:

webvpn

enable outside

anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed hsts enable

max-age 31536000

```
include-sub-domains
 no preload
no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
anyconnect enable
tunnel-group-list enable
cache
 disable
 error-recovery disable
1
anyconnect-custom-data ManagementTunnelAllAllowed true true
1
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelall
client-bypass-protocol enable
address-pools value VPN_Pool
anyconnect-custom ManagementTunnelAllAllowed value true
webvpn
 anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
驗證
```

```
使用CLI驗證管理VPN隧道連線 show vpn-sessiondb detail anyconnect 指令。
```

ASA# show vpn-sessiondb detail anyconnect

```
Session Type: AnyConnect Detailed
Username
           : vpnuser
                                    Index
                                                : 10
                                    Public IP
Assigned IP : 192.168.10.1
                                                : 10.65.84.175
          : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
Protocol
License
          : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-
256
           : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Hashing
           : 17238
                                             : 1988
Bytes Tx
                                    Bytes Rx
         : 12
Pkts Tx
                                    Pkts Rx
                                                 : 13
                                    Pkts Rx Drop : 0
Pkts Tx Drop : 0
Group Policy : AnyConnect_MGMT_Tunnel Tunnel Group : AnyConnect_MGMT_Tunnel
Login Time : 01:23:55 UTC Tue Apr 14 2020
           : 0h:11m:36s
Duration
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                               : none
                                    VLAN
Audt Sess ID : c0a801010000a0005e9510ab
Security Grp : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
--- Output Omitted ---
DTLS-Tunnel:
 Tunnel ID
              : 10.3
 Assigned IP : 192.168.10.1
                                    Public IP : 10.65.84.175
 Encryption : AES-GCM-256
                                     Hashing
                                                 : SHA384
 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
 Encapsulation: DTLSv1.2
                                      UDP Src Port : 57053
```

UDP Dst Port :	443	Auth Mode	: Certificate
Idle Time Out:	30 Minutes	Idle TO Left	: 18 Minutes
Client OS :	Windows		
Client Type :	DTLS VPN Client		
Client Ver :	Cisco AnyConnect VPN	Agent for Windo	ws 4.8.03036
Bytes Tx :	17238	Bytes Rx	: 1988
Pkts Tx :	12	Pkts Rx	: 13
Pkts Tx Drop :	0	Pkts Rx D	prop : 0

驗證ASDM上的管理VPN隧道連線。

導航到Monitoring > VPN > VPN Statistics > Sessions。按AnyConnect Client過濾以檢視客戶端會 話。

🚮 Home 🦓 Configuration [📴 M	onitoring 📊 Save 🄇	🔖 Refresh 🔇 Bac	k 🔘 Forward 🧳	Help Type topi	Go					cisco
Device List Bookmarks	000 Monitoring	> VPN > VPN Statis	stics > <u>Sessions</u>							
O O Device List										
Add 🔟 Delete 🔊 Connect	Туре	Active		Cumulative		Peak Concurrent	nt	Inactive		
Go Go	AnyConnect Client		1			19		1		0
≞ 10.106.39.196	SSL/TIS/DTIS		1			19		1		0
10.106.64.230										
A 10.197.227.47										
10.106.51.99:444										
COO VPN										
VPN Statistics	Filter By AnyCo	nnect Client	All S	essions		Fil	ter			
Sessions	licername	Group Policy	Assigned IP Address	Protocol		Login Time	Bytes Tx	Inactivity	Audit	Details
Crypto Statistics	Osermanie	Connection Profile	Public IP Address	Encryption		Duration	Bytes Rn	inactivity	Audit .	
Compression Statistics	vpnuser	AnyConnect_MGMT AnyConnect_MGMT	.192.168.10.1	AnyConnect-Par AnyConnect-Par	ent: (1)none	0h:01m:31s		Un:00m:00s	cuasu	Logout
Encryption Statistics		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			(_,				_	
Global IKE/IPsec Statistics										Ping
Protocol Statistics										
VLAN Mapping Sessions										
Shared SSL VPN										
VPN Connection Graphs										
WSA Sessions										
_										
Interfaces										
C Y MON										
VP <u>N</u>	To cost VPN cossion	s right slick on the	a above table and c	alact Table Sort O	der from nor					
A Routing	TO SOLE VEN SESSION	is, right-click on th	e above table and s	siect rable sont of	der nom pop	Jup menu.				
S- Properties	Logout By: A	ll Sessio ᅌ		Logout Sessions						

驗證客戶端電腦上的管理VPN隧道連線:

Sisco AnyConnect Secure Mobili	ty Client		×			
cisco AnyCon	nect Secure Mobili	ty Client	(i)			
Virtual Private Network (VPN	۷)	Diagnostics				
Preferences Statistics Route Detail	s Firewall Message History					
Connection Information State:	Disconnected		^			
Tunnel Mode (IPv4):	Not Available	Sisco AnyC	Connect Secure N	Nobility Client		×
Tunnel Mode (IPv6): Dynamic Tunnel Exclusion: Dynamic Tunnel Inclusion: Duration: Session Disconnect: Management Connection State:	Not Available Not Available Not Available 00:00:00 None Connected (asa.example.com)		VPN: Ready to conne	ct.	Connect	
Address Information						
Client (IPv4):	Not Available			Salt - Charles - R		
Client (IPv6):	Not Available	‡ (i)				diadia cisco
Server: Bytes	INOT AVAIIADIE		~ ~			
		Reset Export Stat	s			

疑難排解

新的UI統計資訊行(管理連線狀態)可用於排除管理隧道連線問題。以下是常見的錯誤狀態:

已斷開連線(禁用):

- 功能已禁用。
- 確保通過使用者隧道連線(要求您將管理VPN配置檔案新增到使用者隧道組策略)或通過手動 上傳配置檔案將管理VPN配置檔案部署到客戶端。
- 確保為管理VPN配置檔案配置了一個包含隧道組的單個主機條目。

已斷開連線(受信任網路):

•TND檢測到受信任網路,因此未建立管理隧道。

已斷開連線(使用者隧道處於活動狀態):

• 使用者VPN隧道當前處於活動狀態。

已斷開連線(進程啟動失敗):

•嘗試管理隧道連線時遇到進程啟動失敗。

已斷開連線(連線失敗):

- 建立管理隧道時遇到連線故障。
- 確保在隧道組中配置證書身份驗證, 組策略中不存在標語, 並且伺服器證書必須受信任。

已斷開連線(無效的VPN配置):

- 從VPN伺服器接收到無效的拆分隧道配置。
- 檢查管理隧道組策略中的拆分隧道配置。

已斷開連線(軟體更新掛起):

• AnyConnect軟體更新當前掛起。

已斷開連線:

•管理隧道即將建立或由於其他原因無法建立。

<u>收集DART以進</u>一步進行故障排除。

相關資訊

- <u>管理VPN隧道的配置</u>
- <u>管理VPN隧道故障排除</u>
- <u>技術支援與文件 Cisco Systems</u>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。