ASA/PIX:使用CLI和ASDM配置IPSec VPN客戶端 的靜態IP地址示例

目錄

簡介 必要條件 需求 採用元件 相關產品 慣例 設定 網路圖表 設定遠端存取VPN(IPSec) 使用CLI配置ASA/PIX Cisco VPN客戶端配置 驗證 show命令 疑難排解 清除安全關聯 疑難排解指令 相關資訊

<u>簡介</u>

本文檔介紹如何配置Cisco 5500系列自適應安全裝置(ASA),以便通過自適應安全裝置管理器 (ASDM)或CLI向VPN客戶端提供靜態IP地址。ASDM通過直觀易用的基於Web的管理介面提供世界 一流的安全管理和監控。Cisco ASA配置完成後,即可通過Cisco VPN客戶端進行驗證。

請參閱<u>使用Windows 2003 IAS RADIUS(針對Active Directory)的PIX/ASA 7.x和Cisco VPN客戶 端4.x身份驗證配置示例</u>,以在Cisco VPN客戶端(4.x for Windows)和PIX 500系列安全裝置7.x之間 設定遠端訪問VPN連線。遠端VPN客戶端使用者使用Microsoft Windows 2003 Internet身份驗證服 務(IAS)RADIUS伺服器對Active Directory進行身份驗證。

請參閱<u>PIX/ASA 7.x和Cisco VPN Client 4.x for Cisco Secure ACS身份驗證配置示例</u>,以在思科 VPN客戶端(4.x for Windows)和PIX 500系列安全裝置7.x之間設定遠端訪問VPN連線,該連線具有 用於擴展身份驗證(Xauth)的思科安全訪問控制伺服器(ACS版本3.2)。

<u>必要條件</u>



本文檔假定ASA已完全正常運行並配置為允許Cisco ASDM或CLI進行配置更改。

註:請參閱<u>允許ASDM或PIX/ASA 7.x的HTTPS訪問</u>:<u>內部和外部介面上的SSH配</u>置示例,允許通過 ASDM或安全外殼(SSH)遠端配置裝置。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- •思科自適應安全裝置軟體版本7.x及更高版本
- 自適應安全裝置管理器5.x版及更高版本
- Cisco VPN客戶端4.x版及更高版本

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。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

相關產品

此配置還可以與Cisco PIX安全裝置7.x版及更高版本配合使用。

<u>慣例</u>

如需文件慣例的詳細資訊,請參閱<u>思科技術提示慣例。</u>

設定

本節提供用於設定本文件中所述功能的資訊。

註:使用Command Lookup Tool(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定:



注意:此配置中使用的IP編址方案在Internet上不能合法路由。它們是RFC 1918地址,在實驗室環 境中使用。

ASDM過程

完成以下步驟以配置遠端訪問VPN:

1. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > IKE Policies > Add以建立ISAKMP策略。

	🚰 Cisco ASDM 6.1 for ASA - 10.77.241.111						
	File View Tools Wa	zards Wi	ndow Help				
	Home 🚱 Configur	ation 📝	Monitoring 🛛 🔚	Save 🔇 Refresh	🕒 Back 🔘 Forward	🦻 Help	
2.	Remote Access Production Network (Client) Acc AnyConnect Conr IPsec Connection Group Policies Dynamic Access R Address Assignm Address Assignm Address Assignm Address Assignm SSL VPN SSL VPN SSL VPN SSL VPN Fisec Connto Ma IPsec Trar IPsec Trar IPsec Trar IPsec Trar	ess ectior Profile ent rity	Configuration Configure s Add	n > Remote Access pecific Internet Key Ex Edit î Delete	<u>VPN > Network (Clin</u> change (IKE) algorithms Encryption	ent) Access > Adva s and parameters, with Hash	ance hin t
	🖆 Add IKE Polic	у					<
	Priority:	2		Authentication:	pre-share 🔽		
	Encryption:	des	~	D-H Group:	2 😽		
	Hash:	sha	~	Lifetime:	Unlimited86400	seconds 💌	
		C	<u> </u>	Cancel	Help		

按一下「OK」和「Apply」。

3. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > IKE Parameters以在外部介面上啟用IKE。

🚰 Cisco ASDM 6.1 for ASA - 10.77.241.111								
File View Tools Wizards Wi	ndow Help							
🚯 Home 🔒 Configuration 📴 I	🔥 Home 🚜 Configuration 📴 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦓 Help							
Remote Access d P ×	Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Parameters							
Introduction Network (Client) Access AnyConnect Connection Presc Connection Profil Presc Connection Profil Crypto Maps Presc Presc	Enable IKE NAT Transparency Interface IKE Enable Inside No Disable Disable Inside No Outside Yes Enable IPsec over NAT-T NAT Keepalive: 20 seconds Enable IPsec over TCP Enter up to 10 comma-separated TCP port values (1- 65535): 10000							
INCLPARAMETERS INCLPARAMETERS Insec Transform Insec Transform Insec Prefragms Certificate to Co Insec Voload Software Voload Software	Identity to Be Sent to Peer Identity: Automa V Key Id String:							
System Options	Disable inbound aggressive mode connections							
AAA/Local Users	Alert peers before disconnecting Wait for all active sessions to voluntarily terminate before rebooting							

4. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > IPSec Transform Sets > Add以建立ESP-DES-SHA轉換集,如圖所示。

🕵 Add	Transform Set				×
	Set Name:	ESP-DES-SHA]	
	Properties			-	
	Mode:	💽 Tunnel	יד 🚫	ansport	
	ESP Encryption	1:	DES	~	
	ESP Authentica	ation:	SHA	~	
	Ĺ	Ca		Help	按-

「OK」和「Apply」。

5. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > Crypto Maps > Add,以便使用優先順序為1的動態策略建立加密對映,如下所示。

🖆 Create IPsec Rule	
Tunnel Policy (Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection	
Interface: outside 💙 Policy Type: dynamic 💙	Priority: 1
Transform Sets	
Transform Set to Be Added:	Move Up
Remove	Move Down
Peer Settings - Optional for Dynamic Crypto Map Entries	
The Connection Type is applicable to static tunnel policies only. Uni-directional connection for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may	type policies are used specify up to 10
redundant peers.	
OK Cancel Help	

按一下「OK」和「Apply」。

6. 選擇Configuration > Remote Access VPN > AAA Setup > Local Users > Add,以便為VPN客 戶端訪問建立使用者帳戶(例如,使用者名稱 — cisco123和密碼 — cisco123)。

Username: discol23 Password:	AUG OSET ACCOUNT				
Cill login prompt for SSH, Telnet and console (no ASDM access) This setting is effective only if AAA authenticate console command is configured. No ASDM, SSH, Telnet or Console access This setting is effective only if AAA authenticate console command is configured. Find: Find: Find	Es Allo Oser Account	Username: ci: Password: * Confirm Password: * User authenticated Access Restriction	sco123 ****** ****** using MSCHAP tions below to restrict ASDM, SSH, 7 network access, regardless of thes N, SSH, Telnet and Console) is used with command authorization 2	Telnet and e settings	I Console access.
請轉到VPN Policy並為使用者「cisco123」新增靜態/專用IP地址,如下所示。 Gisco ASDA 6.1 for ASA - 10.77.241.111 Fie View Tools Wizards Window Hetp Configuration ② Monitoring ③ Save ③ Refresh ③ Back ③ Forward ② Hetp Remote Access … ④ ♥ × Introduction Network (Client) Access Add User Account Corr Add User Account Corr Add User Account Corr Add User Account Corr Add User Sassyment AAA Clientless SSL VPN Access AddAsces Pools AddAsces Pools Acces Pools AddAsces Pool	Find:	CLI login prompt This setting is No ASDM, SSH, T This setting is	for SSH, Telnet and console (no AS effective only if AAA authenticate of Telnet or Console access effective only if AAA authenticate of Next O Previous	iDM acces: console co console co Help	s) mmand is configured. mmand is configured.
Cisco ASDA 6.1 for ASA - 10.77.241.111 File View Tools Wizards Window Heb Home Configuration Monitoring Save Refresh Back Provend Help Remote Access P × Configuration > Remote Access VPN > AAAAlocal Users > Local Users Introduction Network (Client) Access Add User Account Introduction Configuration > Remote Access VPN > AAAAlocal Users > Local Users Introduction Configuration > Remote Access VPN > AAAAlocal Users > Local Users Introduction Configuration > Remote Access VPN > AAAAlocal Users > Local Users Introduction Configuration > Remote Access VPN > AAAAlocal Users > Local Users Introduction Configuration > Remote Access VPN > AAAAlocal Users > Local Users Introduction Configuration > Remote Access VPN > AAAAlocal Users Address Pools Configuration > Remote Access VPN > AAAAlocal Users Address Pools Configuration > Remote Access VPN > AAAAlocal Users AAAAlocal Users Inherit AAAalocal Users	青轉到VPN Policy並為	使用者「cisco123」	新增 靜態/專用IP地址 ,	如下列	f示。
Home Configuration Monitoring Save Refresh Refresh Refresh Home Home Home Refresh <	Cisco ASDM 6.1 for ASA - 1	0.77.241.111			
Remote Access Introduction Introduction Address Introduction Process Introt Process	Home Configuration M	nitoring 🔲 Save 💽 Refres	h 🙆 Back 🔘 Forward 🦻 Help		
Introduction Cree Add User Account Cree Add User Account Correct Connection Profiles AAA Correct Connection Profiles AAA Coup Policies AAA Coup Policies AAA Coup Policies AAA Coup Policies AAA Coup Policy Check an Inherit checkbox to let the corresponding setting take its value from Coup Policy Coup Policies AAA Coup Policy Check an Inherit checkbox to let the corresponding setting take its value from Coup Policy Coup Pol	Remote Access a + × (onfiguration > Remote Accr	ess VPN > AAAAlocal Users > Local	Users	
Idle Timeout:	Introduction Network (Client) Access AnyConnect Connection P Prec Connection Profiles Group Policies Dynamic Access Policies Address Assignment Assignment Policy Address Pools Address SL VPN Access AAA/Local Users AAA/Local Users AAA Server Groups AAA	Cree Corr Corr AAA Use Enst	Check an Inherit checkbox to let t Group Policy: Tunneling Protocols: Filter: Tunnel Group Lock: Store Password on Client System Connection Settings Access Hours:	he correspo Inheri Inheri Inheri Inheri Inheri Inheri	t t t t t t t t t t

8. 選擇Configuration > Remote Access VPN > Network(Client)Access > Address Assignment > Address Pools,然後按一下Add為VPN客戶端使用者新增VPN客戶端。

🚰 Cisco ASDM 6.1 for ASA	- 10.77.241.111
File View Tools Wizards Wir	ndow Help
🔥 Home 🚱 Configuration 🛐 I	Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help
Remote Access 🗗 🕈 ×	Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools
Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Connection Profiles Group Policies Dynamic Access Policies Address Assignment Address Pools Ad	Configure named IP Address pools. This parameter is enforced in either a VPN IPsec Connection Profiles, AnyConnect Connection Profiles or Group Policis Add IP Pool Pool Name Pool Name Star Name: vpnclient1 Starting IP Address: 192.168.5.10 Ending IP Address: 192.168.5.100 Subnet Mask: SSSSSSSS
	OK Cancel Help

9. 選擇Configuration > Remote Access VPN > Network(Client)Access > IPSec Connection Profiles > Add以新增隧道組(例如,TunnelGroup1和Preshared key as cisco123),如下所

示。					
File View Tools Wizards Window He	Þ			Look For:	
Home 🦓 Configuration 🔯 Monitorin	ng 🔚 Save 🔇 Refresh 🔇 Br	ok 🔘 Forward 🤗 H	lelp		
Remote Access VPN	Configuration > Remote Access A Access Interfaces Enable interfaces for IPsec access. Interface outside dmz	PH > Network (Client) A Allow A	ccess	ection Profiles	
Address Assignment Advanced Advanced Advanced Advanced Advanced Advanced Advanced Clentless SSL VPN Access Advanced Clentless SSL VPN Access Advanced Clentless SSL VPN Access Language Localization Certificate Management Language Localization Clentless Balancing DHCP Server DNS	inside Connection Profiles Connection profile (tunnel group) s Add	pecifies how user is authen	icated and other para	mebers.	
E Advanced	Name	IPsec Enabled	L2TP/IPse	c Enabled	Autentication
~	DefaultWEBVPNGroup			1	LOCAL
	DefaultRAGroup	N	5	2	LOCAL
Remote Access VPN					
*		[Apply R	eset	

在**Basic**頁籤下,為User Authentication欄位選擇伺服器組作為LOCAL。選擇vpnclient1作為 VPN客戶端使用者的客戶端地址池。

Home & Configuration	Monitoring 🔚 Save 🤇	🕨 Refresh 🚱 Back	Forward 🦓 Help	
Remote Access 🗗 🔍 🗡	Configuration > Rem	ote Access VPN > Net	work (Client) Access > IPsec Connection	Profiles
	-			
Network (Client) Access	🚰 Add IPsec Remote	Access Connection	n Profile	
AnyConnect Connection				
Installation control works	Basic	Name:	TunnelGroup1	
Group Policies	Advanced		·	-
- Address Assignment		IKE Peer Authentication		
Accircoment Policy		De de du		1
Address Projs		Pre-shared key:	******	
B-B Advanced		Identify Certificate:	None	Managa
Clientless SSL VPN Access		toerrory ceruncere.	140110	I manage
AAA/Local Users		Channel As allowed in a binnel		
AAA Server Groups		Oser Autorentication		
		Server Group:	LOCAL	Manage
- 🕼 Local Users				
🕂 🚮 Secure Desktop Manager		Fallback:	Use LOCAL it Server Group fails	
P-100 Language Localization		Client Address Assignme	ent	
		DHCP Servers:		1
f DHCP Server			<u> </u>	·
DNS		Client Address Pools	vpnclient1	Select.
P-123 Advanced			<	,
		Default Group Policy		
		Croup Policy:	DifficerPalicy	Managa
		a oup roncy.	once proncy .	
			(Following fields are attributed of the group po	licy selected a
			Enable IPser protocol	
			- en recerción a core prioritados	
			Enable L2TP over IPsec protocol	

按一下「OK」(確定)。

10. 選擇Advanced > Client Addressing,然後選中Use address pool覈取方塊以將IP地址分配給 VPN客戶端。**注意:**確保取消選中Use authentication server和Use DHCP的**覈取方塊。**

Add IPsec Remote	ccess Connection Profile
Advanced General General Authentication Authorization Accounting IPsec PPP	obal Client Address Assignment Policy This policy affects all Network (Client) Access connections. The following are tried in order until an address is found. Use authentication server Use DHCP Use address pool terface-Specific Address Pools Add C Edit Delete Interface
Find:	💿 Next 💿 Previous
	OK Cancel Help

按一下「OK」(確定)。

	11.	為IPSec訪問啟用Outside介面	。按一	下Apply繼續。
--	-----	---------------------	-----	-----------

🚰 Cisco ASDM 6.1 for ASA - 10.77.241.111					
File View Tools Wizards Wind	dow Help				
🔥 Home 🦓 Configuration 📴 M	fonitoring 🔚 Save 🔇 Refresh 🔇 Bad	k 🚫 Forward 💡 Help			
Remote Access D A X Throduction Network (Client) Access AnyConnect Connection Profiles Group Policies Dynamic Access Policies Address Assignment Policy Address Pools Address Pools Address Pools Address SSL VPN Access AAA/Local Users AAA Server Groups LOAP Attribute Map Local Users Secure Desktop Manager Certificate Management Language Localization Coad Balancing DHCP Server DNS Advanced	Configuration > Remote Access VPN > Access Interfaces Enable interfaces for IPsec access. Interface Allow / outside	Network (Client) Access > IPsec Conne			

<u>使用CLI配置ASA/PIX</u>

完成這些步驟,以便配置DHCP伺服器從命令列為VPN客戶端提供IP地址。有關所使用的每個命令的詳細資訊,請參閱<u>配置遠端訪問VPN</u>或<u>Cisco ASA 5500系列自適應安全裝置 — 命令參考</u>。

在ASA裝置上運行配置
ASA# sh run
ASA Version 8.0(2)
!
! Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! ! Configure the outside and inside
<i>interfaces.</i> interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 ! Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.10-192.168.5.100
mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1

--- Specify the location of the ASDM image for ASA to fetch the image for ASDM access. asdm image disk0:/asdm-613.bin no asdm history enable arp timeout 14400 global (outside) 1 192.168.1.5 nat (inside) 0 access-list 101 nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0 192.168.1.2 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 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policyrecord DfltAccessPolicy 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 crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto dynamic-map outside_dyn_map 1 set transform-set ESP-DES-SHA crypto map outside_map 1 ipsec-isakmp dynamic outside_dyn_map !--- Specifies the interface to be used with !--- the settings defined in this configuration. crypto map outside_map interface outside !--- PHASE 1 CONFIGURATION ---! !--- This configuration uses ISAKMP policy 2. !---The configuration commands here define the Phase !--- 1 policy parameters that are used. crypto isakmp enable outside crypto isakmp policy 2 authentication pre-share encryption des hash sha group 2 lifetime 86400 no crypto isakmp nat-traversal !--- Specifies that the IP address to the vpn clients are assigned by the local and not by AAA or dhcp. The CLI vpn-addr-assign local for VPN address assignment through ASA is hidden in the CLI provided by show run command. no vpn-addr-assign aaa no vpn-addr-assign dhcp telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list 1 class-map inspection_default match default-inspection-traffic 1 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
!
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol IPSec webvpn
group-policy GroupPolicy1 internal
!--- In order to identify remote access users to the
Security Appliance, !--- you can also configure
usernames and passwords on the device. !--- specify the
IP address to assign to a particular user, use the vpn-
framed-ip-address command !--- in username mode
username cisco123 password ffIRPGpDSOJh9YLq encrypted
username cisco123 attributes
 vpn-framed-ip-address 192.168.5.1 255.255.255.0
!--- Create a new tunnel group and set the connection !-
-- type to remote-access. tunnel-group TunnelGroup1 type
remote-access tunnel-group TunnelGroup1 general-
attributes address-pool vpnclient1 !--- Enter the pre-
shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

<u>Cisco VPN客戶端配置</u>

嘗試使用Cisco VPN客戶端連線到Cisco ASA,以驗證ASA配置是否成功。

- 1. 選擇Start > Programs > Cisco Systems VPN Client > VPN Client。
- 2. 按一下New以啟動Create New VPN Connection Entry視窗。



3. 填寫新連線的詳細資訊。輸入連線條目的名稱和說明。在Host框中輸入ASA的外部IP地址。然後輸入ASA中配置的VPN隧道組名稱(TunnelGroup1)和密碼(預共用金鑰—cisco123)。按 一下「Save」。

VPN Client Create New VPN Connect	tion Entry			
Connection Entry: ASA				
Description: vpntunnel		cisco		
Host: 192.168.1.1				
Authentication Transport Backup Servers	Dial-Up			
Group Authentication				
Name: TunnelGroup1				
Password: ******				
Confirm Password: *******				
Certificate Authentication Name: Send CA Certificate Chain				
Erase User Password	Save	Cancel		

4. <u>按一下要使用的連線,然後在VPN客戶端主視窗中按一下**Connect**。</u>

🥔 stati	us: Connected VPN Client - Version	5.0.03.0530	e la se altre e la service e la service e la 💽	
Connect	ion Entries Status Certificates Log Options	Help		
Conn	nect New Import Modify	Delete	्रम् दा	ulu sco
Connec	tion Entries Certificates Log			
	Connection Entry /	Host	Transport	
0	ASA	192.168.1.1	IPSec/UDP	

5. 出現提示時,輸入Username:cisco123和密碼:cisco123如在ASA中為Xauth配置,然後點選 OK以連線到遠端網路。

The	and the fallenting i		
authentication.	sted the following i	nrormation to complete	e the user
Username:	cisco123		
CISCO Password	******		
		OK	Court

6. VPN客戶端與中心站點的ASA連線。

🥔 stat	tus: Connected VPN Client -	Version 5.0.03.0530	
Connec	tion Entries Status Certificates Log	Options Help	
Discor	nnect New Import	lodiy Delete	cisco
Connec	ction Entries Certificates Log		
	Connection Entry	Host	Transport
0	ASA	192.168.1.1	IPSec/UDP
Conner	La Regali		

7. 成功建立連線後,從Status選單中選擇**Statistics**以驗證隧道的詳細資訊。

🥔 status: Cor	nected VPN Client - Version 5	.0.03.0530	
Connection Entrie	es Status Certificates Log Options	Help	
Disconnect Connection Entri	Statistics Ctrl+S Notifications Ctrl+N Reset Stats	Delete	alialia cisco
C	Connection Entry	Host	Transport
<u>۵</u> ۸	SA	192.168.1.1	IPSec/UDP



<u>show命令</u>

使用本節內容,確認您的組態是否正常運作。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>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 。

- show crypto isakmp sa 顯示對等體上的所有當前IKE安全關聯(SA)。
- show crypto ipsec sa 顯示當前SA使用的設定。

<u>疑難排解</u>

本節提供的資訊可用於對組態進行疑難排解。還顯示了調試輸出示例。

註:有關遠端訪問IPSec VPN故障排除的詳細資訊,請參<u>閱最常見的L2L和遠端訪問IPSec VPN故</u> <u>障排除解決方案</u>。

<u>清除安全關聯</u>

進行故障排除時,請確保在進行更改後清除現有的安全關聯。在PIX的特權模式下,使用以下命令 :

- clear [crypto] ipsec sa 刪除活動的IPSec SA。關鍵字crypto是可選的。
- clear [crypto] isakmp sa 刪除活動的IKE SA。關鍵字crypto是可選的。

<u>疑難排解指令</u>

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>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<u>有關 Debug 指令的重要資訊</u>。

- debug crypto ipsec 7 顯示第2階段的IPSec協商。
- debug crypto isakmp 7 顯示第1階段的ISAKMP協商。

相關資訊

- Cisco ASA 5500系列自適應安全裝置支援頁
- Cisco ASA 5500系列自適應安全裝置命令參考
- Cisco PIX 500系列安全裝置支援頁面
- Cisco PIX 500系列安全裝置命令參考
- <u>思科調適型資安裝置管理員</u>
- IPSec協商/IKE通訊協定支援頁面
- Cisco VPN使用者端支援頁面
- Cisco PIX防火牆軟體
- Cisco Secure PIX防火牆命令參考
- 安全產品現場通知(包括PIX)
- <u>要求建議 (RFC)</u>

• 技術支援與文件 - Cisco Systems