ASA/PIX:使用CLI和ASDM配置VPN客戶端流量的 帶入站NAT的遠端VPN伺服器示例

目錄

 簡介

 必要條件

 需求

 採用元件

 相關產品

 慣例

 背景資訊

 組態

 使用ASDM將ASA/PIX配置為遠端VPN伺服器

 使用CLI將ASA/PIX配置為遠端VPN伺服器和入站NAT

 驗證

 ASA/PIX安全裝置 — show命令

 疑難排解

 相關資訊

<u>簡介</u>

本文檔介紹如何使用自適應安全裝置管理器(ASDM)或CLI和NAT將思科5500系列自適應安全裝置 (ASA)配置為遠端VPN伺服器(入站VPN客戶端流量)。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,可通過Cisco VPN客戶端進行驗證。

<u>必要條件</u>

<u>需求</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。還假定ASA配置為 出站NAT。有關如何配置出站NAT的詳細資訊,請參閱<u>允許內部主機使用PAT訪問外部網路</u>。

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。

<u>相關產品</u>

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,請參閱思科技術提示慣例。

<u>背景資訊</u>

遠端訪問配置為Cisco VPN客戶端(例如移動使用者)提供安全的遠端訪問。遠端訪問VPN使遠端 使用者能夠安全地訪問集中式網路資源。Cisco VPN Client符合IPSec協定,專門設計用於與安全裝 置配合使用。但是,安全裝置可以與許多符合協定的客戶端建立IPSec連線。有關IPSec的詳細資訊 ,請參閱<u>ASA配置指南</u>。

組和使用者是VPN安全管理和安全裝置配置中的核心概念。它們指定用於確定使用者對VPN的訪問 許可權和使用的屬性。組是被視為單個實體的使用者集合。使用者從組策略獲取其屬性。隧道組標 識特定連線的組策略。如果未向使用者分配特定組策略,則應用連線的預設組策略。

隧道組由確定隧道連線策略的一組記錄組成。這些記錄標識隧道使用者被驗證到的伺服器,以及連 線資訊被傳送到其上的記帳伺服器(如果有)。它們還標識連線的預設組策略,並且它們包含特定 於協定的連線引數。通道組包含與建立通道本身相關的少量屬性。隧道組包括指向定義面向使用者 的屬性的組策略的指標。

<u> 組態</u>

使用ASDM將ASA/PIX配置為遠端VPN伺服器

完成以下步驟,以便使用ASDM將Cisco ASA配置為遠端VPN伺服器:

 開啟瀏覽器並輸入https://<IP_Address of the interface of ASA that has configured for ASDM Access>以訪問ASA上的ASDM。確保授權瀏覽器提供的與SSL證書真實性相關的任何警告。 預設使用者名稱和密碼均為空。ASA顯示此視窗以允許下載ASDM應用程式。此示例將應用程 式載入到本地電腦上,並且不在Java小程式中運行。



3. 下載ASDM啟動程式後,請完成提示指導的步驟,以便安裝軟體並運行Cisco ASDM啟動程式

0

4. 輸入您使用http -命令配置的介面的IP地址,以及使用者名稱和密碼(如果已指定)。此範例使用cisco123作為使用者名稱,cisco123作為密碼。

🖆 Cisco ASDM Launcher v1.5(30)		
		cisco
Device IP Address / Name:	10.77.241.111	T
Username:	cisco123	
Password:	****	
🔄 Run in Demo Mode		
	0	1 🕯 🖆

5. <u>從主視窗中選擇Wizards > IPsec VPN Wizard。</u>

🖆 Cisco ASDM 6.1 for ASA - 10.77.241.111					
File View Tools Wizards Window Help					
Home 🖧 Cor Startup Wizard					
IPsec VPN Wizard					
Device List	SSL VPN Wizard				
🖶 Add 📋 Delete	High Availability and Scalability Wizard				
🖳 10.77.241.10	right Availability and Scalability wizard				
10.77.241.1	Packet Capture Wizard				

6. 選擇Remote Access VPN隧道型別並確保已根據需要設定VPN隧道介面,然後按一下 Next(如下所示)。

📫 VPN Wizard	
VPN Wizard	VPN Tunnel Type (Step 1 of)
Branch Branch ISP Homo	Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.
Corporate	VPN Tunnel Type: Site-to-Site VPN
	O Site-to-Site
	Remote Access
	VPN Tunnel Interface: Outside
	Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.
	< Back Next > Finish Cancel Help
7. 選擇VPN客戶端型別,該	如下所示。 此處選擇了 Cisco VPN Client。按「 Next 」(下一步)。
🖆 VPN Wizard	
VPN Wizard	Remote Access Client (Step 2 of)
Brand	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.
	VPN Client Type:
Corporate	⊙ Cisco VPN Client, Release 3.x or higher,
Notwork	or other Easy VPN Remote product
E E	Microsoft Windows client using L2TP over IPsec
	Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it.
1 THE FEEL	PAP CHAP MS-CHAP-V1 MS-CHAP-V2 EAP-PROXY
TIT	Specify if the client will send tunnel group name as - username@tunnelgroup.
6	Client will send tunnel group name as username@tunnelgroup.
	If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.
	C Back Next > Finish Cancel Hab

8. 輸入隧道組名**稱的名稱**。輸入要使用的身份驗證資訊,即本示例**中的預共**享金鑰。本示例中使

用的預共用金鑰是cisco123。本示例中使用的隧道組名稱為cisco。按「Next」(下一步)。

🖆 VPN Wizard	
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch	The ASA allows you to group remote access tunnel users based on common connection parameters and clent attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote clent. Authentication Method Pre-Shared Key: clsco123 Certificate Certificate Signing Algorithm: rsa-sig Certificate Name: Certificate Name: Certificate Name: Certificate Signing Algorithm: clack() Tunnel Group Tunnel Group Name: clsco
	< Back Next > Finish Cancel Help
ᇔᇣᆸᅖᄥᅷᆇᆄᇥᇛᆇ	

9. 選擇是要對本地使用者資料庫還是外部AAA伺服器組驗證遠端使用者。注意:您可以在步驟 10中將使用者新增到本地使用者資料庫。注意:有關如何使用ASDM配置外部AAA伺服器組的 資訊,請參閱通過ASDM為VPN使用者配置PIX/ASA 7.x身份驗證和授權伺服器組配置示例。

🖆 VPN Wizard		×
VPN Wizard	Client Authentication (Step 4 of)	
Branch Branch Desete ISP Desete ISP Home Home Network	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.	
Casta In	 Authenticate using the local user database 	
The states	Authenticate using an AAA server group	
	AAA Server Group Name: New	
	< Back Next > Finish Cancel He	Þ

10. 提供**使用者名稱**和可選的**密碼**,然後按一下Add以向使用者身份驗證資料庫新增新使用者。 按「Next」(下一步)。**注意:**不要從此視窗中刪除現有使用者。在ASDM主視窗中選擇 Configuration > Device Management > Users/AAA > User Accounts,以編輯資料庫中的現 有條目或將其從資料庫中刪除。

🖆 VPN Wizard		
VPN Wizard	User Accounts (Step 5 of 11)	
	Add new users into the user auth or to remove them from the data Users/AAA > User Accounts in th	nentication database. To edit existing entries in the database base, go to Configuration > Device Management > we main ASDM window.
Horne	User to Be Added	1
Corporate Network	Username:	dsco123
THE THE	cisco	Add >>
	Password (optional):	Delete
1 I I I I I I I I I I I I I I I I I I I	•••••	
THINK	Confirm Password (optional):	
TAT	•••••	
		< Back Next > Finish Cancel Help

11. 要定義要動態分配給遠端VPN客戶端的本地地址池,請按一下New以建立新的IP池。

🖆 VPN Wizard		
VPN Wizard	Address Pool	(Step 6 of 11)
Branch Branch Fisp Branch Horne Corporate Horne	Enter a po clients.	ol of local addresses to be used for assigning dynamic IP addresses to remote VPN Tunnel Group Name : cisco
Note		Pool Name: New
		Range End Address:
		Subnet Mask:
		< Back Next > Finish Cancel Help

12. 在標題為Add IP Pool的新視窗中,提供此資訊,然後按一下OK。IP池的名稱起始IP地址結束

1	dd IP Pool		×
			_
	Name:	vpnpool	
	Starting IP Address:	192.168.1.1	
	Ending IP Address:	192.168.1.254	
	Subnet Mask:	255.255.255.0	~
	ОКЪС	Cancel Help]
地址子網路遮置			

13. <u>定</u>義連線時動態分配給遠端VPN客戶端的本地地址池後,按一下**下一步。**

🖆 VPN Wizard		×
VPN Wizard	Address Pool (Step 6 of 11)	
Branch Branch	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.	
Corporate Natwork	Tunnel Group Name : cisco	
THE IN	Pool Name: vpnpool 🖌 New	
	Pool Settings	
THUM	Range Start Address: 192.168.1.1	
- Carlon	Range End Address: 192.168.1.254	
The state	Subnet Mask: 255.255.255.0	
		J
	< Back Next > Finish Cancel Help	ן

14. 可選:指定要推送到遠端VPN客戶端的DNS和WINS伺服器資訊以及預設域名。

🛋 VPN Wizard		
VPN Wizard	Attributes Pushed to Client (Optional)(Step 7 of 11)
Bronch Bronch Discourse Bronch Bronch Bronch Bronch	Attributes you configure below are push ASA. If you do not want an attribute pus	ed to the VPN client when the client connects to the shed to the client, leave the corresponding field blank.
Corporate Network	Tunnel Group:	cisco
	Primary DNS Server:	
A REAL	Secondary DNS Server:	
TIM	Primary WINS Server:	
	Secondary WINS Server:	
	Default Domain Name:	
		<back next=""> Finish Cancel Help</back>

15. 指定IKE的引數,也稱為IKE階段1。通道兩端的設定必須完全相符。但是,Cisco VPN客戶端 會自動為自己選擇正確的配置。因此,客戶端PC上無需進行IKE配置。

🖆 VPN Wizard						×
VPN Wizard	IKE Policy (Step 8 of	11)				
Branch Branch Designed (SP) Home Corroorate	Select the encrypti devices to use to n them. Configuration	on algorithm, aut egotiate an Inter ns on both sides (hentication algorith net Key Exchange of the connection r	nm, and Diffi (IKE) securi nust match (ie-Hellman group for the ty association between exactly.	
Network	Encryp	tion:	DES	~		
	Auther	ntication:	MDS	~		
	Diffie-I	Helman Group:	2 🗸			
			< Back	Next 2	Finish Cancel H	telp

16. 此視窗顯示您已採取的操作的摘要。如果對配置滿意,請按一下Finish。



使用ASDM配置ASA/PIX到NAT入站VPN客戶端流量

完成以下步驟,以便使用ASDM配置Cisco ASA到NAT入站VPN客戶端流量:

1. 選擇Configuration > Firewall > Nat Rules,然後按一下Add。在下拉選單中,選擇Add



Dynamic NAT Rule。

2. 在Add Dynamic NAT Rule視窗中,選擇Outside作為介面,然後按一下Source框旁的瀏覽按鈕

🕵 Add Dyn	amic NAT Rule		
Original — Interface: Source: Translated – Select a di	Outside	anslation.	
Pool ID 0 0	Interface (outbound) (inbound)	Addresses Pool Same as original address (identity) Same as original address (identity)	Manage
Connectio	on Settings	OK Cancel Help	8

3. 在Browse Source視窗中,選擇適當的網路對象,並在Selected Source部分下選擇**source**,然 後按一下**OK**。此處選擇了192.168.1.0網路對象。

🕵 Browse Source	e			
🗣 Add 🏼 Edit	<u>î</u> Delete 🔍			
Filter:				Filter Clear
Name	^1 IP Address	Netmask	Description	
Network Objects	s			
👋 any	0.0.0	0.0.0		
inside-ne	stwork 172.16.1.0	255.255.255.0		
🚮 Outside-	network 10.10.10.0	255.255.255.0		
i- 192.168	.1.0 192.168.1.0	255.255.255.0		
Selected Source —				
Source ->	192.168.1.0/24			
				K Cancel

4. 按一下「Manage」。

🖆 Add Dyn	amic NAT Rule		
Original — Interface: Source: Translated — Select a glo	Outside 192.168.0.0 obal pool for dynamic t	ranslation.	
0	(outbound) (inbound)	Same as original address (identity) Same as original address (identity)	Manage
Connectio	n Settings	OK Cancel Help	*

5. 在「管理全域性池」視窗中,按一下**新增**。

<table-cell-rows> Mana</table-cell-rows>	ge Glo	bal Pool		
4 Ada	📑 Ed	it 💼 Delete		
Pool ID		Interface	Addresses Pool	
		ОК	Cancel Help	

6. 在Add Global Address Pool視窗中,選擇**Inside**作為Interface,選擇2作為**Pool ID**。此外,請 確保已選中**PAT using IP Address of the interface**(使用**介面的IP地址的PAT)旁邊的**單選按鈕。 按一下**Add>>**,然後按一下**OK**。

🖆 Add Global Address Pool		X
Interface: inside Pool ID: 2		
IP Addresses to Add Range Starting IP Address: Ending IP Address: Netmask (optional): IP Address: Netmask (optional): Dert Address: Netmask (optional):	Add >> << Delete	Addresses Pool
Address of the interface	Cancel	Help

7. 選擇全域性池ID為2(在上一步中配置)後,按一下**OK**。

🖾 A (dd Dyna	mic NAT Rule		
Origi	inal —			
Int	terface:	Outside	~	
So	urce:	192.168.1.0/24		
Trans	slated			
Se	elect a glo	bal pool for dynamic	translation.	
F	Pool ID	Interface	Addresses Pool	
	0	(outbound)	Same as original address (identity)	
	0	(inbound)	Same as original address (identity)	
	2	inside	🔤 inside	Manage
Cor	nnectio	Settings		*
			OK Cancel Help	

8. 現在,按一下Apply,將配置應用到ASA。這樣即可完成配置。

Configuration > Firewall > NAT Rules						
💠 Add	🝷 📝 Edit 🏢 Dele	te 🛧 🗲 🕉 🖿	💼 - 🛛 🔍 Find 🖥	🔁 Diagram 🗐	Packet Trace	
		Original			Translated	
#	Туре	Source	Destination	Service	Interface	Addre:
🗏 Outsid	le (1 Dynamic rules)					
1	Dynamic	🛃 192.168.1.0/24			inside	🛲 insit
⊡∙inside	(1 Exempt rules, 1 D)	mamic rules)				
1	🞫 Exempt	🌍 any	192.168.1.0/24		(outbound)	
2	Dynamic	🌍 any			Outside	🔤 Out
<						>
🔄 Enabl	e traffic through the	firewall without address t	ranslation			
_		Apply	Reset			

使用CLI將ASA/PIX配置為遠端VPN伺服器和入站NAT

在ASA裝置上運行配置
ciscoasa# show running-config
: Saved
ASA Version 8.0(3)
1
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif Outside
security-level 0
ip address 10.10.10.2 255.255.255.0
interface Ethernet0/1

nameif inside security-level 100 ip address 172.16.1.2 255.255.255.0 1 1 passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa803-k8.bin ftp mode passive access-list inside_nat0_outbound extended permit ip any 192.168.1.0 255.255.255 0 pager lines 24 logging enable mtu Outside 1500 mtu inside 1500 ip local pool vpnpool 192.168.1.1-192.168.1.254 mask 255.255.255.0 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-615.bin asdm history enable arp timeout 14400 nat-control global (Outside) 1 interface global (inside) 2 interface nat (Outside) 2 192.168.1.0 255.255.255.0 outside nat (inside) 0 access-list inside_nat0_outbound nat (inside) 1 0.0.0.0 0.0.0.0 route Outside 0.0.0.0 0.0.0.0 10.10.10.3 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-policy-record DfltAccessPolicy http server enable no snmp-server location no snmp-server contact !--- Configuration for IPsec policies. !--- Enables the crypto transform configuration mode, !--- where you can specify the transform sets that are used !--- during an IPsec negotiation. crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5hmac crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs group1 crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set transform-set ESP-DES-SH ESP-DES-MD5 crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP crypto map Outside_map interface Outside crypto isakmp enable Outside !--- Configuration for IKE policies. !--- Enables the IKE policy configuration (config-isakmp) !--- command mode, where you can specify the parameters that !--- are used during an IKE negotiation. Encryption and !---

Policy details are hidden as the default values are

```
chosen. crypto isakmp policy 10
authentication pre-share
 encryption des
hash sha
group 2
lifetime 86400
crypto isakmp policy 30
authentication pre-share
encryption des
hash md5
group 2
lifetime 86400
telnet timeout 5
ssh timeout 60
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
group-policy cisco internal
group-policy cisco attributes
vpn-tunnel-protocol IPSec
!--- Specifies the username and password with their !---
respective privilege levels username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15
username cisco password ffIRPGpDSOJh9YLq encrypted
privilege 0
username cisco attributes
vpn-group-policy cisco
tunnel-group cisco type remote-access
tunnel-group cisco general-attributes
address-pool vpnpool
default-group-policy cisco
!--- Specifies the pre-shared key "cisco123" which must
!--- be identical at both peers. This is a global !---
configuration mode command. tunnel-group cisco ipsec-
attributes
pre-shared-key *
1
class-map inspection_default
match default-inspection-traffic
1
policy-map type inspect dns migrated_dns_map_1
parameters
 message-length maximum 512
policy-map global_policy
class inspection_default
 inspect dns migrated_dns_map_1
 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
prompt hostname context
Cryptochecksum:f2ad6f9d5bf23810a26f5cb464e1fdf3
: end
ciscoasa#



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

. <mark>按一下「New」。</mark>			
VPN Client - Version 5.0.03.0530			
Connection Entries Status Certificates Log Option	is Help		
Connect News Import Modify	Delete		linin Isco
Connection Entries Certificates Log			
Connection Entry	Host	Transport	
Not connected.			

2. 填寫新連線的詳細資訊。Host欄位必須包含先前配置的Cisco ASA的IP地址或主機名。組身份 驗證資訊必須與**步驟4**中使用的資訊相對應。完成後按一下**Save**。

VPN Client Create New VPN Connection Entry	×
Connection Entry: MyVPNClient	
Description:	
Host: 10.10.10.2	
Authentication Transport Backup Servers Dial-Up	
Group Authentication	
Name: cisco	
Password: ******	
Confirm Password: *******	
 Certificate Authentication Name: Send CA Certificate Chain 	
Erase User Password Cancel	

3. <u>選擇新建立的連線,然後按一下**Connect**。</u>

🥔 status: Disconnected VPN Client - Ver	rsion 5.0.03.0530		
Connection Entries Status Certificates Log Optic	ons Help		
Confuct New Import Modify) Delete		cisco
Connection Entry	Host	Transport	
MyVPNClient	10.10.10.2	IPSec/UDP	
Not connected.			

4. 輸入用於擴展身份驗證的使用者名稱和密碼。此資訊必須與步驟5和6中指定的資訊匹配。

VPN Client User Authentication for "MyVPNC	Client" 🛛 🔀		
The server has requested the following information to complete t authentication.	he user		
Lisco Password: *******			
ОК	Cancel		

5. 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: Connected VP	N Client - Version 5.0.03.0530	
Connection Entries Status Cer	tificates Log Options Help	
Disconnect N	cs Ctrl+S ations Ctrl+N Delete	cisco
Connection Entries Reset S	stats	
Connection Entry /	Host	Transport
MyVPNClient	10.10.10.2	IPSec/UDP
Connected to "MyVPNClient".	Cor	nected Time: 0 day(s), 00:00.36 🛛 🔻

此視窗顯示流量和加密資訊



<u>ASA/PIX安全裝置 — show命令</u>

• show crypto isakmp sa — 顯示對等體上的所有當前IKE SA。 ASA#show crypto isakmp sa

```
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
 Total IKE SA: 1
    IKE Peer: 10.10.10.1
 1
     Type
          : user
                              Role
                                       : responder
                                     : AM_ACTIVE
     Rekey
             : no
                               State
• show crypto ipsec sa — 顯示對等體上的所有當前IPsec SA。
 ASA#show crypto ipsec sa
 interface: Outside
     Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10
 .10.2
       local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
       remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
       current_peer: 10.10.10.1, username: cisco123
       dynamic allocated peer ip: 192.168.1.1
       #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
       #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0
       #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
       #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
       #send errors: 0, #recv errors: 0
       local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1
       path mtu 1500, ipsec overhead 58, media mtu 1500
       current outbound spi: F49F954C
     inbound esp sas:
       spi: 0x3C10F9DD (1007745501)
          transform: esp-des esp-md5-hmac none
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
          sa timing: remaining key lifetime (sec): 27255
          IV size: 8 bytes
          replay detection support: Y
     outbound esp sas:
       spi: 0xF49F954C (4104099148)
          transform: esp-des esp-md5-hmac none
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
          sa timing: remaining key lifetime (sec): 27255
          IV size: 8 bytes
          replay detection support: Y
 ciscoasa(config)#debug icmp trace
 !--- Inbound Nat Translation is shown below for Outside to Inside ICMP echo request
 translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
 ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3
 !--- Inbound Nat Translation is shown below for Inside to Outside ICMP echo reply
 untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
 ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192
 len=32
 ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
 ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3
 2
 ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32
```

Active SA: 1

ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8960 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8960 len=32

<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。

<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 。

有關如何對站點站點VPN進行故障排除的詳細資訊,請參閱<u>最常見的L2L和遠端訪問IPSec VPN故</u> <u>障排除解決方案</u>。

相關資訊

- Cisco ASA 5500系列調適型安全裝置
- 思科調適型資安裝置管理員
- Cisco ASA 5500系列自適應安全裝置故障排除和警報
- 技術支援與文件 Cisco Systems