# ASA/PIX:带有用于 VPN 客户端流量的入站 NAT 的远程 VPN 服务器(带有 CLI 和 ASDM)配置 示例

### 目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>相关产品</u> <u>规则</u> <u>背景信息</u> 配置 <u>使用 ASDM 将 ASA/PIX 配置为远程 VPN 服务器</u> <u>使用 ASDM 配置从 ASA/PIX 到 NAT 的入站 VPN 客户端流量</u> <u>使用 CLI 将 ASA/PIX 配置为远程 VPN 服务器并使之适用于入站 NAT</u> 验证 <u>ASA/PIX 安全设备 - show 命令</u> <u>故障排除</u> <u>相关信息</u>

## <u>简介</u>

本文档介绍了如何使用自适应安全设备管理器 (ASDM) 或 CLI 将 Cisco 5500 系列自适应安全设备 (ASA) 配置为充当远程 VPN 服务器,以及如何将 NAT 配置为入站 VPN 客户端流量。ASDM 通过 一个直观且易于使用的基于 Web 的管理界面提供一流的安全管理和监控。完成 Cisco ASA 配置后 ,可以使用 Cisco VPN 客户端对其进行验证。

## <u> 先决条件</u>

#### <u>要求</u>

本文档假设 ASA 处于完全运行状态,并配置为允许 Cisco ASDM 或 CLI 进行配置更改。此外,也 假设要对 ASA 进行配置,使之适用于出站 NAT。有关如何配置出站 NAT 的详细信息,请参阅<u>允许</u> <u>内部主机使用 PAT 访问外部网络</u>。

**注意:** 请参阅<u>允许对 ASDM 进行 HTTPS 访问</u>或 <u>PIX/ASA 7.x:内部和外部接口上的 SSH 配置示</u> <u>例</u>以允许通过 ASDM 或Secure Shell (SSH) 远程对设备进行配置。

#### <u>使用的组件</u>

本文档中的信息基于以下软件和硬件版本:

- Cisco可适应安全工具软件版本7.x和以上
- 自适应安全设备管理器版本 5.x 及更高版本
- Cisco VPN 客户端 4.x 及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

#### 相关产品

此配置也可用于 Cisco PIX 安全设备版本 7.x 及更高版本。

#### <u>规则</u>

有关文档规则的详细信息,请参阅 <u>Cisco 技术提示规则</u>。

### <u>背景信息</u>

远程访问配置提供对 Cisco VPN 客户端(如移动用户)的安全远程访问。远程访问 VPN 使远程用 户可以安全地访问集中的网络资源。Cisco VPN 客户端遵守 IPSec 协议并专门设计为可与安全设备 配合使用。但是,安全设备可以与许多协议兼容客户端建立 IPSec 连接。有关 IPSec 的详细信息 ,请参阅 <u>ASA 配置指南</u>。

组和用户是 VPN 安全管理和安全设备配置中的核心概念。它们指定确定用户访问和使用 VPN 的属 性。组是被视为单个实体的用户集合。用户从组策略获得他们的属性。隧道组标识特定连接的组策 略。如果没有为用户分配特定组策略,则应用连接的默认组策略。

隧道组由确定隧道连接策略的一组记录构成。这些记录标识用于对隧道用户进行身份验证的服务器 ,以及向其发送连接信息的记帐服务器(如果有)。它们还标识连接的默认组策略,并且它们包含 协议特定的连接参数。隧道组包括与隧道自身创建相关的少量属性。隧道组包括指向定义面向用户 的属性的组策略的一个指针。

### 配置

#### 使用 ASDM 将 ASA/PIX 配置为远程 VPN 服务器

要使用 ASDM 将 Cisco ASA 配置为远程 VPN Server,请完成以下步骤:

1. 打开浏览器并输入 https://<为访问 ASDM 而配置的 ASA 接口的 IP 地址>,以访问 ASA 上的 ASDM。确保核准浏览器提供的有关 SSL 证书真实性的任何警告。默认的用户名和口令均为 空。ASA 显示此窗口以允许下载 ASDM 应用程序。此示例将应用程序加载到本地计算机,但 不在 Java 小程序中运行。



- 3. 下载 ASDM 启动程序之后,完成提示所指示的步骤,以便安装该软件并运行 Cisco ASDM 启 动程序。
- 4. 输入使用 http 命令配置的接口的 IP 地址,以及用户名和口令(如果已指定)。此示例使用 cisco123 作为用户名,使用 cisco123 作为口令。

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

5. 从主窗口中选择 Wizards > IPsec VPN Wizard。

<b>E</b> 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 <u> I</u> Delete	High Ausilshilitu and Scalahilitu Wisard		
	High Availability and Scalability Wizard		
10.77.241.1	Packet Capture Wizard		

6. 选择 Remote Access VPN 隧道类型,并确保根据需要设置了 VPN Tunnel Interface,然后单击 Next(如图所示)。

🖆 VPN Wizard	
VPN Wizard	A PN Tunnel Type (Step 1 of)
Branch Branch F SP Home	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
	⊖ 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. <u>选择 VPN Client Type(如图所示)。此时选择 Cisco VPN Client。单击 Next。</u>

🖆 VPN Wizard					
VPN Wizard	Remote Access Client (Step 2 of)				
Branch	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:				
Home					
Corporate	<ul> <li>Cisco VPN Client, Release 3.x or higher;</li> </ul>				
and the second s	or other Easy VPN Remote product				
I THE IN	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.				
- I STULL	PAP V CHAP V MS-CHAP-V1 MS-CHAP-V2 EAP-PROXY				
	Specify if the client will send tunnel group name as - username@tunnelgroup.				
- A-	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.				
	< Back Next > Finish Cancel Help				

8. 为Tunnel Group Name输入名称。输入要使用的身份验证信息,在本示例中是预共享密钥。本

示例中使用的预共享密钥是 **cisco123**。此示例中使用的 Tunnel Group Name 为 **cisco**。单击 **Next**。

🖆 VPN Wizard	
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
Branch Horne Horne Horne	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 Pre-Shared Key: cisco123 Certificate Certificate Signing Algorithm: rsa-sig Certificate Name: Challenge/response authentication (CRACK) Tunnel Group Tunnel Group Name: cisco
	< Back Next > Finish Cancel Help

9. 选择是希望使用本地用户数据库对远程用户进行身份验证,还是希望使用外部 AAA 服务器组 对远程用户进行身份验证。注意:您将在步骤 10 中将用户添加到本地用户数据库中。注意: 有关如何通过 ASDM 配置外部 AAA 服务器组的信息,请参阅 <u>PIX/ASA 7.x 的通过 ASDM</u> 为 <u>VPN 用户配置身份验证和授权服务器组的配置示例</u>。

🖆 VPN Wizard		×
VPN Wizard	Client Authentication (Step 4 of)	
Branch Br	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.	
	< Back Next > Finish Cancel He	Þ

10. 提供 Username 和可选的 Password ,然后单击 Add 将新用户添加到用户认证数据库中。单击 Next。注意:请不要从此窗口中删除现有用户。在 ASDM 主窗口中选择 Configuration > Device Management > Users/AAA > User Accounts,以编辑数据库中的现有条目或将其从数据库中删除。

🖆 VPN Wizard			×
VPN Wizard	User Accounts (Step 5 of 11)		
	Add new users into the user aut or to remove them from the data Users/AAA > User Accounts in t	thentication database. To edit existing entries in the database abase, go to Configuration > Device Management > the main ASDM window.	
Home	User to Be Added		
Corporate Network	Username:	dsco123	
The said	cisco	Add >>	
	Password (optional):	Delete	
1 I WILLING	•••••		
THINK	Confirm Password (optional):		
IT AL	•••••		
			5
		< Back Next > Finish Cancel Hel	P

11. 要定义将动态分配给远程 VPN 客户端的本地地址池,请单击 New 创建新的 IP Pool。

🖆 VPN Wizard	
VPN Wizard	Address Pool (Step 6 of 11)
Branch ISP Hornso	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.
Corporate Natwork	Pool Name:
	Pool Settings
THURMAN	Range Start Address:
-I-I-IIIII	Range End Address:
the state of the s	Subnet Mask:
	< Back Next > Finish Cancel Help

12. 在名为 Add IP Pool 的新窗口中,请提供以下信息,然后单击 OK。IP 池的名称起始 IP 地址

	🚰 Add IP Pool	X
	Name:	VDDDool
	Starting IP Address:	192.168.1.1
	Ending IP Address:	192.168.1.254
	Subnet Mask:	255.255.255.0
终止 IP 地址子网掩码	ОКЪ	Cancel Help

13. 定义在远程 VPN 客户端建立连接时将动态分配给这些客户端的本地地址池后,请单击 Next。

					_
🖆 VPN Wizard					$\times$
VPN Wizard	Address Pool (Step	6 of 11)			
Branch Branch Branch Branch Home	Enter a pool of loc clients.	al addresses to be use	ed for assigning dynamic IP a	ddresses to remote VPN	
Corporate Network	Tunn	el Group Name :	cisco		
Trate Ital	Pool f	Name:	vpnpool 🍝	New	
	Poo	ol Settings			
THUM		Range Start Address:	192.168.1.1		
- Cast		Range End Address:	192.168.1.254		
TAT		Subnet Mask:	255.255.255.0		
			< Back Next >	Finish Cancel Hel	Þ

14. **可选:**指定 DNS 和 WINS 服务器信息以及将被推送到远程 VPN 客户端的默认域名。

🖆 VPN Wizard		
VPN Wizard	Attributes Pushed to Client (Optional)	(Step 7 of 11)
Bronch Bronch	Attributes you configure below are push ASA. If you do not want an attribute pu	ned to the VPN client when the client connects to the ished to the client, leave the corresponding field blank.
Corporate	Tunnel Group:	cisco
- T	Primary DNS Server:	
A REAL	Secondary DNS Server:	
TIM	Primary WINS Server:	
	Secondary WINS Server:	
	Default Domain Name:	
		< Back Next > Finish Cancel Help

15. 为 IKE 指定参数,也称为 IKE 第 1 阶段。隧道两端的配置必须完全一致。但 Cisco VPN 客 户端会自动为自己选择正确的配置。因此,无需在客户端 PC 上执行 IKE 配置。

🖆 VPN Wizard		X
VPN Wizard	IKE Policy (Step 8 of 11)	
Branch Pr	Select the encryption algorithm, authentication algorithm, and Diffie-Helman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.	
Notwork	Encryption: DES	
	Authentication:	
1 July	Diffie-Helman Group: 2	
	< Back Next Finish Cancel H	elp

16. 此窗口显示您已执行操作的汇总。如果对配置感到满意,请单击 Finish。



### 使用 ASDM 配置从 ASA/PIX 到 NAT 的入站 VPN 客户端流量

要使用 ASDM 配置从 Cisco ASA 到 NAT 的入站 VPN 客户端流量,请完成以下步骤:

1. 选择 Configuration > Firewall > Nat Rules,然后单击 Add。在下拉列表中选择 Add Dynamic Configuration > Firewall > NAT Rules



NAT Rule。

2. 在 Add Dynamic NAT Rule 窗口中,选择 Outside 作为 Interface,然后单击 Source 框旁边的 浏览按钮。

🕵 Ada	d Dyna	mic NAT Rule		
Origina Inte Sour Transk Sele	al	Outside	ranslation.	
Po (	ool ID 0 0	Interface (outbound) (inbound)	Addresses Pool Same as original address (identity) Same as original address (identity)	Manage
Conr	nection	Settings	OK Cancel Help	*

3. 在 Browse Source 窗口中,选择正确的网络对象,同时选择 Selected Source 部分下的 **source**,然后单击 **OK**。此处选择的网络对象 (Network Object) 为 192.168.1.0。

📬 Browse Source				
💠 Add 🏹 Edit î De	elete Q			
Filter:				Filter Clear
Name	1 IP Address	Netmask	Description	
■ Network Objects				
- 🌑 any	0.0.0.0	0.0.0.0		
📑 과 inside-network	172.16.1.0	255.255.255.0		
- 🛃 Outside-netwo	ork 10.10.10.0	255.255.255.0		
L 192.168.1.0	192.168.1.0	255.255.255.0		
Selected Source				
Source -> 192.	168.1.0/24			
				_
				K Cancel

4. 单击 Manage。

🕵 Add Dyn	amic NAT Rule		
Original — Interface: Source: Translated – Select a gl	Outside 192.168.0.0 obal pool for dynamic tr	ranslation.	
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

5. 在 Manage Global Pool 窗口中,单击 Add。

🕵 Manage Glo	obal Pool		×
Add 🖬 E	dit 💼 Delete		
Pool ID	Interface	Addresses Pool	
	ок	Cancel Help	

6. 在 Add Global Address Pool 窗口中,选择 **Inside** 作为 Interface,选择 2 作为 **Pool ID**。此外 ,请确保选中 **PAT using IP Address of the interface** 旁边的单选按钮。单击 **Add>>**,然后单 击 **OK**。

📧 Add Global Address Pool		×
Interface: inside  Pool ID: 2		
IP Addresses to Add  Range Starting IP Address: Ending IP Address: Netmask (optional):  Port Address Translation (PAT) IP Address: Netmask (optional):  Port Address Translation (PAT) using IP Address of the interface	Add >> << Delete	Addresses Pool
	Cancel	Help

7. 在使用上一步配置的 Pool ID 2 选择全局池后,请单击 OK。

🕵 Add Dyn	amic NAT Rule		
Original			
Interface:	Outside	~	
Source:	192.168.1.0/24		
Translated			
Select a glo	bal pool for dynamic	translation.	
Pool ID	Interface	Addresses Pool	]
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	
2	inside	🚥 inside	Manage
Connectio	n Settings		۲
		OK Cancel Help	

8. 现在请单击 Apply,以便将配置应用到 ASA。配置到此结束。

Configura	Configuration > Firewall > NAT Rules						
💠 Add	🝷 📑 Edit 🎁 Dele	ste   🛧 🗲   🕉 🖿	💼 - 🔍 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	insic	
⊡∙inside	(1 Exempt rules, 1 Dy	ynamic rules)					
1	Exempt	🌍 any	192.168.1.0/24		(outbound)		
2	🔛 Dynamic	🌍 any			Outside	🎫 Out	
💟 Enabl	e traffic through the	firewall without address	translation				
		Apply	Reset	)			

## 使用 CLI 将 ASA/PIX 配置为远程 VPN 服务器并使之适用于入站 NAT

### 在 ASA 设备上运行配置

ciscoasa# <b>show running-config</b> : Saved ASA Version 8.0(3)
! 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 ! ! 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
<b>255.255.255.0</b> 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 sipdisconnect 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-md5-hmac 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 generalattributes 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 \* ! class-map inspection\_default match default-inspection-traffic ! ! 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 ! servicepolicy global\_policy global prompt hostname context Cryptochecksum:f2ad6f9d5bf23810a26f5cb464e1fdf3 : end ciscoasa#

## <u>验证</u>

尝试通过 Cisco VPN 客户端连接到 Cisco ASA,以便验证是否已成功配置 ASA。

#### 1. <u>单击 **New**</u>。

VPN Client - Version 5.0.03.0530			
Connection Entries Status Certificates Log Options	Help		
Connect News Import Modify	) Delete		cisco
Connection Entries Certificates Log		-	
Connection Entry	Host	Transport	
Not connected.			

2. 填写新连接的详细信息。Host 字段必须包含以前配置的 Cisco ASA 的 IP 地址或主机名。组身 份验证 (Group Authentication) 信息必须与**步骤 4** 中使用的组身份验证信息对应。完成后,请 单击 **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. 选择新创建的连接,然后单击 Connect。

Status: Disconnected   VPN Client - Vers	ion 5.0.03.0530		
Connection Entries Status Certificates Log Option	s Help		
Confuct New Import Modify	) Delete		cisco
Connection Entries Certificates Log			
Connection Entry	Host	Transport	
MyVPNClient	10.10.10.2	IPSec/UDP	
Not connected.			

4. 输入用于扩展身份验证的用户名和口令。此信息必须与步骤 5 和步骤 6 中指定的信息一致。

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

5. 成功建立连接后,在 Status 菜单中选择 Statistics 以验证隧道的详细信息。

Status: Connected   V	PN Client - Version 5.0.03.0530		×
Connection Entries Status Ce	artificates Log Options Help		
Disconnect N	tics Ctrl+S tations Ctrl+N Stats	CISC	0 0
Connection Entries			
Connection Entry	A Host	Transport	
MyVPNClient	10.10.10.2	IPSec/UDP	
Connected to "MyVPNClient".		Connected Time: 0 day(s), 00:00.36	• /

此窗口显示数据流和加密信息



#### ASA/PIX 安全设备 - show 命令

• show crypto isakmp sa - 显示对等体上的所有当前 IKE SA。ASA#show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA:

1 1 IKE Peer: 10.10.10.1 Type : user Role : responder Rekey : no State : AM\_ACTIVE

- show crypto ipsec sa 显示对等体上的所有当前 IPsec SA。ASA#show crypto ipsec sa interface: Outside Crypto map tag: SYSTEM DEFAULT CRYPTO MAP, seg 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: ciscol23 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 #prefrag 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 2 !--- 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 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 reply from 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>故障排除</u>

本部分提供的信息可用于对配置进行故障排除。

<u>命令输出解释程序(仅限注册用户</u>)(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输 出的分析。

有关站点到站点 VPN 故障排除的详细信息,请参阅<u>最常见的 L2L 和远程访问 IPsec VPN 故障排除</u> <u>解决方案</u>。

## 相关信息

- Cisco ASA 5500 系列自适应安全设备
- Cisco 自适应安全设备管理器
- Cisco ASA 5500 系列自适应安全设备故障排除和警报
- <u>技术支持和文档 Cisco Systems</u>