PIX/ASA 7.x ASDM:限制远程访问VPN用户的网络访问

目录

<u>简介</u> <u>先决条件</u> 要求 使用的组件 相关产品 网络图 <u>规则</u> 通过 ASDM 配置访问 通过 CLI 配置访问 验证 故障排除 相关信息

简介

本文档提供了使用 Cisco 自适应安全设备管理器 (ASDM) 限制远程访问 VPN 用户可访问 PIX 安全 工具或自适应安全设备 (ASA) 后的哪些内部网络的示例配置。执行以下任务时,可将远程访问 VPN 用户限制为仅访问您希望他们访问的网络区域:

- 1. 建立访问列表。
- 2. 将这些用户与组策略关联。
- 3. 将上述组策略与隧道组关联。

请参阅配置 Cisco VPN 3000 集中器以通过过滤器和 RADIUS 过滤器分配进行阻止,了解 VPN 集 中器阻止 VPN 用户访问的各种方案的相关信息。

先决条件

要求

尝试进行此配置之前,请确保满足以下要求:

• 可使用 ASDM 配置 PIX。

注意:要允许ASDM配置PIX,请参阅<u>允许ASDM进行HTTPS访问</u>。

• 至少已设置一种运行良好的远程访问 VPN 配置。

注意:如果没有此类配置,请参阅<u>使用ASDM将ASA配置为远程VPN服务器的配置示例</u>,以获 取如何配置一种运行良好的远程访问VPN配置的信息。

使用的组件

本文档中的信息基于以下软件和硬件版本:

• Cisco Secure PIX 500 系列安全设备版本 7.1(1)

注意: PIX 501和506E安全设备不支持版本7.x。

• Cisco 自适应安全设备管理器版本 5.1(1)

注意:ASDM仅在PIX或ASA 7.x中可用。

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

此配置也可用于以下硬件和软件版本:

• Cisco ASA 5500 系列自适应安全设备版本 7.1 (1)

网络图

本文档使用以下网络设置:



在此配置示例中,假定一家小型公司具有三个子网。上图对此拓扑进行了说明。这三个子网分别是 Intranet、工程和薪酬。此配置示例的目标是允许薪酬人员远程访问 Intranet 和薪酬子网,并阻止他 们访问工程子网。同时,工程人员应当能够远程访问 Intranet 和工程子网,但不能访问薪酬子网。

本示例中的薪酬用户是"controller1"。本示例中的工程用户是"engineer1"。

规则

有关文档约定的更多信息,请参考 <u>Cisco 技术提示约定。</u>

通过 ASDM 配置访问

完成以下步骤,以便使用 ASDM 配置 PIX 安全设备:

1. 选择 Configuration > VPN > General > Group Policy。



2. 根据在 PIX 上配置隧道组所采取步骤,对于要限制其用户的那些隧道组,可能已存在相应的 组策略。如果已存在适当的组策略,请选择它并单击 Edit。否则,请单击 Add,然后选择 "Internal Group Policy..."。



- 3. 如果需要,请在打开的窗口顶部输入或更改组策略的名称。
- 4. 在"General"选项卡上,取消选中"Filter"旁边的 Inherit 框,然后单击"Manage"。

Check an Inherit checkbox	to let the corri	esponding setting take i	ts value from the default group policy.
Tunneling Protocols:	🔽 Inherit	🗖 IPSec	
Filter:	🗖 Inherit	None	Manage
Connection Settings Access Hours:	🔽 Inherit		New
Simultaneous Logins:	🔽 Inherit		
Maximum Connect Time	e: 🔽 Inherit	🗖 Unlimited	minutes
Idle Timeout:	🔽 Inherit	Unlimited	minutes
Servers			
DNS Servers:	🔽 Inherit	Primany:	Secondary:
WINS Servers:	🔽 Inherit	Primary:	Secondary:
DHCP Scope:	🔽 Inherit		

5. 单击 Add ACL,以便在显示的"ACL Manager"窗口中创建一个新的访问列表。

K	ACL Mar	nager							×
С	onfigure	ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
Γ									Add ACE
									EditACE
									Delete
									Move Up
									Move Down
Ŀ	🚽 🖉 Allo	wtraffic	1 6	Denv traffic				•	
	•								
				01	Cance		Help		

6. 为新访问列表选择一个编号,然后单击 OK。

付 Add New A	EL	×
ACL ID:	10]
	OK Cancel	

7. 在左侧选中新 ACL,然后单击 Add ACE 在列表中添加新的访问控制条目。

🔂 ACL M	anager							×
Configu	re ACLs.							
#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
10				·				Add ACE
								EditACE
								Delete
								Move Up
								Move Down
🖌 A	low traffic	0	Deny traffic					
			0	Cance		Help		

8. 定义要添加的访问控制条目 (ACE)。

在本示例中,ACL 10 中的第一个 ACE 允许 IP 从任何源访问薪酬子网。

注意:默认情况下,ASDM仅选择TCP作为协议。如果要对用户授予或拒绝完整的 IP 访问权限,则必须选择"IP"。完成后,单击确定。

o extended Access List Rule	
Action	Time Range
	Time Range: Not Applied 💌 New
Permit C Deny	Syslog
	Default Syslog More Options
Source Host/Network	Destination Host/Network
	C D A H H H H H H H H H H H H H H H H H H
IP Address C Name C Group	• IP Address C Name C Group
IP address: 0.0.0.0	IP address: 10.8.28.0
Mask: 0.0.0.0	Mask: 255.255.255.0 -
Protocol and Cassica	
	Manage Service Groups
IP Protocol	interesting and a second secon
IP protocol: any	
ease enter the description below (optional):	
ermit IP access from ANY source to the payroll subn	et (10.8.28.0 /24)
	F

9. 此时,列表中将显示您刚刚添加的 ACE。再次选择 Add ACE,以便在访问列表中添加任何其 他行。

1	ACL Ma	nager							x
0	Configure	e ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	⊟ 10								Add ACE
	1		1	🧇 any	E ² 10.8.28.0/24	💌 ip		Not Applied	Edit ACE
									Delete
									Move Up
									Move Down
L	•							•	
	🖌 Allo	w traffic	Q (Deny traffic					
				0	Canc	el	Help		

在本示例中,在 ACL 10 中添加了另一个 ACE,以便允许访问 Intranet 子网。

Action		Time Panga
Action		Time Range: Not Applied Nev
C Permit C Deny		Syslog Default Syslog More Options
Source Host/Network		Destination Host/Network
IP Address C Name	C Group	
IP address: 0.0.0.0	_	IP address: 10.8.27.0
Mask: 0.0.0.0	-	Mask: 255.255.255.0 💌
IP protocol: any	-	
lease enter the description below (o	ptional):	
lease enter the description below (o ermit IP access from ANY source to	ptional): the subnet used	by all employees (10.8.27.0 /24)

10. 完成添加 ACE 之后,请单击 OK。

🚰 ACL Manager										X
С	on	figure	e ACLs.							
		#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	Ξ	10								Add ACE
		1	N	~	🧼 any	10.5.28.0/24	😕 ip		Not Applied	EditACE
		2		1	🧇 any	10.8.27.0/24	💌 ip		Not Applied	<u></u>
Γ										Delete
										Move Up
										Move Down
Ŀ	1								•	
	۴	2 Allo	rw traffic	(3)	Denytraffic					
							1	1		
					0	Canc	el	Help		

11. 将上一步骤中定义和填充的 ACL 选择为组策略的过滤器。完成后单击 OK。

			no value nom pre delatan group po
Tunneling Protocols:	🔽 Inherit	F IPSec	
Filter:	🗖 Inherit	10	Manage
Connection Settings		None 10	
Access Hours:	🔽 Inherit		New
Simultaneous Logins:	🗹 Inherit		
Maximum Connect Tim	ie: 🗹 Inherit	Unlimited	minutes
Idle Timeout	🔽 Inherit	Unlimited	minutes
Servers			
DNS Servers:	🔽 Inherit	Primary:	Secondary:
WINS Servers:	🔽 Inherit	Primary:	Secondary:
DHCP Scope:	🔽 Inherit		

12. 单击 Apply 将更改发送到 PIX。



13. 如果您在 Options > Preferences 下将 ASDM 配置为执行此操作,ASDM 预览将发送到 PIX 的命令。单击发送。

💼 Preview CLI Commands	×
The following CLI commands are generated based on the changes you made in ASDM. To send the commands to the PIX_click Send. To not send the commands and continue making	
changes in ASDM, click Cancel.	
access-list 10 line 1 remark permit IP access from ANY source to the payroll subnet (10.8.28.0 /24 -	
access-list 10 line 2 extended permit ip any 10.8.28.0 255.255.255.0 access-list 10 line 3 remark permit IP access from ANY source to the subnet used by all employee	
access-list 10 line 4 extended permit ip any 10.8.27.0 255.255.255.0 group-policy payroll attributes	
vpn-intervalue 10	
Send Cancel	

14. 将刚刚创建或修改的组策略应用到正确的隧道组。在左侧框中单击 Tunnel Group。



15. 选择要应用组策略的隧道组,然后单击 Edit。

File Rules Set	1 for PIX - 10.89.129.147 arch Options Tools Wizards H	qle			
Home C	Configuration Montoring Ba	ck Forward Search	h Refresh Save) 🤗 Ныр	CISCO SYSTEMS
Nterfaces	Configuration - VFN - General - Tu Configuration - VFN - General - Tu Configuration - Tu Configuratio -	Innel Group Manage VPN tunnel group IPSec or WebVPN conn Name	ups. A VPN tunnel grou ection. Type	p represents a connection s Group Policy	specific record for a
VPN Routing Global Objects	· 플립VPN System Option 다 NKE 다 아이지 Address Manageme 다 말IPSec	engineering DefaultRAGroup DefaultL2LGroup	ipsec-ra ipsec-ra ipsec-ra ipsec-l2l	psyroll engineering DftOrpPolicy DftGrpPolicy	Edit Delete
Properties	1	Specify the delimeter to are received when tunn Group Delimiter:	be used when parsing t els are being negotiated None 💌	tunnel group names from th t. Reset	ne user name that

16. 如果已自动创建组策略(请参阅第2步),请验证是否已在下拉框中选中您刚刚配置的组策 略。如果未自动配置组策略,请在下拉框中选中它。完成后单击 OK。

🔂 Edit Tunnel Group	×
Name: payroll Type: ipsec-ra	
General IPSec	
Configure general access attributes from the following sub-tabs.	
Basic AAA Client Address Assignment Advanced	
Group Policy: payroll	
Strip the realm from username before passing it on to the AAA server	
Strip the group from username before passing it on to the AAA server	
OK Cancel Help	

17. 单击 Apply,如果提示,请单击"Send"以将更改添加到 PIX 配置中。

如果已选择组策略,您可能会收到"No changes were made"消息。 Click OK.

18. 请对要添加限制的任何其他隧道组重复第 2-17 步。

在此配置示例中,还需要限制工程人员的访问。尽管过程相同,但仍存在一些具有明显区别的 窗口:

• 新建访问列表 20

📬 A	CL Ma	nager							x
Co	nfigure	e ACLs.							
	#	Rule Enabled	Action	Source Hast/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	10								Add ACE
	1	V	~	🧼 any	AD 10.8.28.0/24	😕 ip		Not Applied	EditACE
	2	V	~	🧼 any	A 10.8.27.0/24	😕 ip		Not Applied	
8	20								Delete
	1	V	~	🧇 any	A 192.168.1.0/24	😕 ip		Not Applied	Mauritin
	2		1	🧇 any	4 10.8.27.0/24	🕑 ip		Not Applied	Move Op
									Move Down
•								Þ	
•	🖉 Allo	ow traffic	3 (Deny traffic					
				0	Cance	el	Help		

• 在"Engineering Group Policy"中选择 Access List 20 作为过滤器。

Check an infent checkbo	x to let the com	esponding setting take	rits value from the default group p	лісу.
Tunneling Protocols:	🔽 Inherit	F IPSec		
Filter:	🖵 Inherit	20	Manage	
Connection Settings Access Hours:	Inherit		New	
Simultaneous Logins:	🔽 Inherit			
Maximum Connect Tim	e: 🔽 Inherit	Unlimited	minutes	
Idle Timeout:	🔽 Inherit	Unlimited	minutes	
Servers				
DNS Servers:	🔽 Inherit	Primary:	Secondary:	
WINS Servers:	🔽 Inherit	Primary:	Secondary:	
DHCP Scope:	🔽 Inherit			

• 验证是否已为工程隧道组设置工程组策略。

🚰 Edit Tunnel Group	×
Name: engineering Type: ipsec-ra	
General IPSec	
Configure general access attributes from the following sub-tabs.	
Basic AAA Client Address Assignment Advanced	
Group Policy: engineering	
Strip the realm from username before passing it on to the AAA server	
Strip the group from username before passing it on to the AAA server	
OK Cancel Help	

通过 CLI 配置访问

完成以下步骤,以便使用 CLI 配置安全设备:

注意:由于空间原因,此输出中显示的一些命令分成两行。

建立两个不同的访问控制列表(15 和 20),当用户连接到远程访问 VPN 时将应用这些列表
 。此访问列表将在后续配置中调用。

<#root>

ASAwCSC-CLI(config)#

access-list 15 remark permit IP access from ANY source to the payroll subnet (10.8.28.0/24)

```
ASAwCSC-CLI(config)#
access-list 15 extended permit ip
any 10.8.28.0 255.255.255.0
ASAwCSC-CLI(config)#
access-list 15 remark Permit IP access from ANY
source to the subnet used by all employees (10.8.27.0)
ASAwCSC-CLI(config)#
access-list 15 extended permit ip
any 10.8.27.0 255.255.255.0
ASAwCSC-CLI(config)#
access-list 20 remark Permit IP access from ANY
source to the Engineering subnet (192.168.1.0/24)
ASAwCSC-CLI(config)#
access-list 20 extended permit ip
any 192.168.1.0 255.255.255.0
ASAwCSC-CLI(config)#
access-list 20 remark Permit IP access from ANY
source to the subnet used by all employees (10.8.27.0/24)
ASAwCSC-CLI(config)#
access-list 20 extended permit ip
any 10.8.27.0 255.255.255.0
```

 创建两个不同的 VPN 地址池。创建的其中一个 VPN 地址池用于薪酬远程用户,而另一个 VPN 地址池则用于工程远程用户。

<#root>

ASAwCSC-CLI(config)#

ip local pool Payroll-VPN 172.10.1.100-172.10.1.200 mask 255.255.255.0

ASAwCSC-CLI(config)#

ip local pool Engineer-VPN 172.16.2.1-172.16.2.199 mask 255.255.255.0

3. 创建当薪酬用户连接时仅应用于这些用户的策略。

<#root>

ASAwCSC-CLI(config)#

group-policy Payroll internal

ASAwCSC-CLI(config)#

group-policy Payroll attributes

ASAwCSC-CLI(config-group-policy)#

dns-server value 10.8.27.10

ASAwCSC-CLI(config-group-policy)#

!--- Call the ACL created in step 1 for Payroll.

ASAwCSC-CLI(config-group-policy)# vpn-tunnel-protocol IPSec ASAwCSC-CLI(config-group-policy)# default-domain value payroll.corp.com

ASAwCSC-CLI(config-group-policy)# address-pools value Payroll-VPN

!--- Call the Payroll address space that you created in step 2.

4. 此步骤与第3步相同,但适用于工程组。

<#root> ASAwCSC-CLI(config)# group-policy Engineering internal

ASAwCSC-CLI(config)#

group-policy Engineering attributes

```
ASAwCSC-CLI(config-group-policy)#
dns-server value 10.8.27.10
```

```
ASAwCSC-CLI(config-group-policy)#
```

vpn-filter value 20

!--- Call the ACL that you created in step 1 for Engineering.

ASAwCSC-CLI(config-group-policy)# vpn-tunnel-protocol IPSec ASAwCSC-CLI(config-group-policy)# default-domain value Engineer.corp.com ASAwCSC-CLI(config-group-policy)#

address-pools value Engineer-VPN

!--- Call the Engineering address space that you created in step 2.

5. 创建本地用户,并将刚刚创建的属性分配给这些用户,以便限制他们对资源的访问。

<#root>

```
ASAwCSC-CLI(config)#
```

username engineer password cisco123

ASAwCSC-CLI(config)#

username engineer attributes

ASAwCSC-CLI(config-username)#

vpn-group-policy Engineering

ASAwCSC-CLI(config-username)#

vpn-filter value 20

ASAwCSC-CLI(config)#

username marty password cisco456

ASAwCSC-CLI(config)#

username marty attributes

ASAwCSC-CLI(config-username)#

ASAwCSC-CLI(config-username)#

6. 创建包含薪酬用户的连接策略的隧道组。

<#root>

ASAwCSC-CLI(config)#

tunnel-group Payroll type ipsec-ra

ASAwCSC-CLI(config)#

tunnel-group Payroll general-attributes

ASAwCSC-CLI(config-tunnel-general)#

address-pool Payroll-VPN

ASAwCSC-CLI(config-tunnel-general)#

default-group-policy Payroll

ASAwCSC-CLI(config)#

tunnel-group Payroll ipsec-attributes

ASAwCSC-CLI(config-tunnel-ipsec)# pre-shared-key time1234

7. 创建包含工程用户的连接策略的隧道组。

<#root>

ASAwCSC-CLI(config)# tunnel-group Engineering type ipsec-ra

ASAwCSC-CLI(config)#

tunnel-group Engineering general-attributes

ASAwCSC-CLI(config-tunnel-general)#

address-pool Engineer-VPN

ASAwCSC-CLI(config-tunnel-general)#

default-group-policy Engineering

ASAwCSC-CLI(config)#

tunnel-group Engineering ipsec-attributes

ASAwCSC-CLI(config-tunnel-ipsec)#

pre-shared-key Engine123

输入配置之后,您将在配置中看到以下突出显示区域:

```
设备名称1
<#root>
ASA-AIP-CLI(config)#
show running-config
ASA Version 7.2(2)
L
hostname ASAwCSC-ASDM
domain-name corp.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
I
interface Ethernet0/0
nameif Intranet
security-level 0
ip address 10.8.27.2 255.255.255.0
1
interface Ethernet0/1
nameif Engineer
security-level 100
ip address 192.168.1.1 255.255.255.0
ļ
interface Ethernet0/2
nameif Payroll
security-level 100
ip address 10.8.28.0
1
interface Ethernet0/3
no nameif
no security-level
no ip address
ļ
interface Management0/0
no nameif
```

```
no security-level
no ip address
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name corp.com
access-list Inside_nat0_outbound extended permit ip any 172.10.1.0 255.255.255.0
access-list Inside_nat0_outbound extended permit ip any 172.16.2.0 255.255.255.0
access-list 15 remark permit IP access from ANY source to the
  Payroll subnet (10.8.28.0/24)
access-list 15 extended permit ip any 10.8.28.0 255.255.255.0
access-list 15 remark Permit IP access from ANY source to the subnet
  used by all employees (10.8.27.0)
access-list 15 extended permit ip any 10.8.27.0 255.255.255.0
access-list 20 remark Permit IP access from Any source to the Engineering
  subnet (192.168.1.0/24)
access-list 20 extended permit ip any 192.168.1.0 255.255.255.0
access-list 20 remark Permit IP access from Any source to the subnet used
  by all employees (10.8.27.0/24)
access-list 20 extended permit ip any 10.8.27.0 255.255.255.0
pager lines 24
mtu MAN 1500
mtu Outside 1500
mtu Inside 1500
ip local pool Payroll-VPN 172.10.1.100-172.10.1.200 mask 255.255.255.0
ip local pool Engineer-VPN 172.16.2.1-172.16.2.199 mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-522.bin
no asdm history enable
arp timeout 14400
global (Intranet) 1 interface
nat (Inside) 0 access-list Inside_nat0_outbound
nat (Inside) 1 192.168.1.0 255.255.255.0
nat (Inside) 1 10.8.27.0 255.255.255.0
nat (Inside) 1 10.8.28.0 255.255.255.0
route Intranet 0.0.0.0 0.0.0.0 10.8.27.2
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
group-policy Payroll internal
group-policy Payroll attributes
dns-server value 10.8.27.10
vpn-filter value 15
vpn-tunnel-protocol IPSec
default-domain value payroll.corp.com
address-pools value Payroll-VPN
group-policy Engineering internal
group-policy Engineering attributes
dns-server value 10.8.27.10
vpn-filter value 20
vpn-tunnel-protocol IPSec
default-domain value Engineer.corp.com
 address-pools value Engineer-VPN
```

```
username engineer password LCaPXI.4Xtvclaca encrypted
username engineer attributes
vpn-group-policy Engineering
vpn-filter value 20
username marty password 6XmYwQ009tiYnUDN encrypted privilege 0
username marty attributes
vpn-group-policy Payroll
vpn-filter value 15
no snmp-server location
no snmp-server contact
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto dynamic-map Outside_dyn_map 20 set pfs
crypto dynamic-map Outside_dyn_map 20 set transform-set ESP-3DES-SHA
crypto map Outside_map 65535 ipsec-isakmp dynamic Outside_dyn_map
crypto map Outside_map interface Outside
crypto isakmp enable Outside
crypto isakmp policy 10
authentication pre-share
 encryption 3des
hash sha
 group 2
lifetime 86400
tunnel-group Payroll type ipsec-ra
tunnel-group Payroll general-attributes
address-pool vpnpool
default-group-policy Payroll
tunnel-group Payroll ipsec-attributes
pre-shared-key *
tunnel-group Engineering type ipsec-ra
tunnel-group Engineering general-attributes
address-pool Engineer-VPN
default-group-policy Engineering
tunnel-group Engineering ipsec-attributes
pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
class-map inspection_default
match default-inspection-traffic
1
ļ
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:0e579c85004dcfb4071cb561514a392b
: end
ASA-AIP-CLI(config)#
```

验证

使用 ASDM 的监控功能验证您的配置:

1. 选择 Monitoring > VPN > VPN Statistics > Sessions。

随即会在 PIX 上显示活动 VPN 会话。选择您感兴趣的会话并单击 Details。

🐞 Cisco ASDM 5.1 for PIX - 10.89.129.147						
File Rules Sea	arch Options Tools Wizards	Help				
Home of	Sconfiguration Monitoring	Back Forward	Q Q Search Refresh	G ? Save Help	Cis	CO SYSTEMS
Interfaces	Monitoring > VPN > VPN Statistics VPN Connection Grapt VPN Statistics Crypto Statistics Encryption Statistic Global IKE/IPSec 8 Protocol Statistics Sessions	 Sessions Sessions Remote Access Filter By: Remote Username controller1 To sort VPN sessions Logout By: All S 	LAN-to-LAN 1 Access T All Sess Group Policy Tunnel Group DifforpPolicy eavroll right-click on the above	Total 0 sions Assigned IP Address Public IP Address 10 8:27:50 172:22:1:165	Total Cumulative 1 Protocol Encryption IPSoc 3DES 3DES Soft Order from popup r .ogout Sessions	9 3 Details Logout Ping Nernu.
Data Refreshed S	successfully.		cisco	VA (2)	🖌 🖸 3013/06 8:3	6:34 PM 01C

2. 选择 ACL 选项卡。

ACL hitcnts 反映了流经客户端和允许网络之间的隧道的数据流。

Session Details					2		
Remote Detailed			F orter of	1			
Usemame	Tunnel Group	Public IP Address	Encryption	Duration	Version		
ontroller1	DfltGrpPolicy payroll	10.8.27.50 172.22.1.165	IPSec 3DES	20:35:08 UTC Mon Mar 13 2006 0h:08m:58s	WinNT 4.8.00.0440		
Details ACL							
The following &CL is being applied to this session:							
access-list 10	; 2 elements	de TD concer from	ANT source to the r	amell admet 110 8 22 2 (2			
access-list 10 line 1 remark permit IP access from ANY source to the payroll submet (10.8.28.0 /24) access-list 10 line 2 extended permit ip any 10.8.28.0 255.255.255.0 (hitcht=8) 0x25954260							
access-list 10	line 4 extended pe	rnit ip any 10.8.2	7.0 255.255.255.0 (hitent=4) Oxd52617df	(10.8.27.0 72		
•					× •		
		[[[
		Herresh	Close	нер			
				Last Update	d: 3/13/06 2:47:17 PM		

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- <u>使用 ASDM 将 Cisco ASA 5500 系列自适应安全设备 ASA 配置为远程 VPN 服务器的配置示</u> <u>例</u>
- Cisco PIX 500 系列安全设备配置示例和 TechNotes
- Cisco ASA 5500 系列自适应安全设备配置示例和 TechNotes
- <u>Cisco VPN 客户端配置示例和 TechNotes</u>
- <u>技术支持和文档 Cisco Systems</u>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。