PIX/ASA 7.x ASDM: Restringir o acesso à rede de usuários de VPN de acesso remoto

Contents

Introdução Pré-requisitos Requisitos Componentes Utilizados Produtos Relacionados Diagrama de Rede Conventions Configurar Acesso via ASDM Configurar o acesso via CLI Verificar Troubleshooting Informações Relacionadas

Introdução

Este documento fornece uma configuração de exemplo usando o Cisco Adaptive Security Device Manager (ASDM) para restringir quais redes internas os usuários do acesso remoto VPN podem acessar por trás do Mecanismo de Segurança PIX ou do Adaptive Security Appliance (ASA). É possível limitar os usuários do acesso remoto VPN apenas às áreas da rede que deseja que elas acessem quando você:

- 1. Crie listas de acesso.
- 2. Associá-los a políticas de grupo.
- 3. Associe essas políticas de grupo a grupos de túnel.

Consulte <u>Configuring the Cisco VPN 3000 Concentrator for Blocking with Filters and RADIUS</u> <u>Filter Assignment</u> para saber mais sobre o cenário em que o VPN Concentrator bloqueia o acesso de usuários VPN.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

• O PIX pode ser configurado usando o ASDM.

Observação: consulte <u>Permitindo o Acesso HTTPS para o ASDM</u> para permitir que o PIX seja configurado pelo ASDM.

 Você tem pelo menos uma configuração de VPN de acesso remoto em boas condições em vigor.

Observação: Se você não tiver nenhuma dessas configurações, consulte <u>ASA como um</u> <u>Servidor VPN Remoto usando o Exemplo de Configuração do ASDM</u> para obter informações sobre como configurar uma boa configuração de VPN de acesso remoto.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

• Cisco Secure PIX 500 Series Security Appliance versão 7.1(1)

Observação: os PIX 501 e 506E Security Appliances não suportam a versão 7.x.

• Cisco Adaptive Security Device Manager versão 5.1(1)

Observação: O ASDM está disponível apenas no PIX ou no ASA 7.x.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Esta configuração também pode ser utilizada com estas versões de hardware e software:

• Cisco ASA 5500 Series Adaptive Security Appliance versão 7.1(1)

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Neste exemplo de configuração, supõe-se uma rede corporativa pequena com três sub-redes. Este diagrama ilustra a topologia. As três sub-redes são Intranet, Engenharia e Folha de Pagamento. O objetivo deste exemplo de configuração é permitir que o pessoal da folha de pagamento acesse remotamente as sub-redes Intranet e Folha de Pagamento e impedi-los de acessar a sub-rede Engenharia. Além disso, os engenheiros devem ser capazes de acessar remotamente as sub-redes Intranet e Engenharia, mas não a sub-rede Folha de pagamento. O usuário da folha de pagamento neste exemplo é "controller1". O usuário de engenharia neste exemplo é "engenheiro1".

Conventions

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

Configurar Acesso via ASDM

Conclua estas etapas para configurar o PIX Security Appliance usando o ASDM:

1. Selecione Configuration > VPN > General > Group Policy.

🔂 Cisco ASDM 5.1	for PIX - 10.89.129.147					_0×
File Rules Sea	arch Options Tools Wizards	Help				
Home C	onfiguration Monitoring	Back Forward Search	h Refresh	Save Help		CISCO SYSTEMS
Interfaces Interfaces Security Policy MAT Security Policy Properties	Configuration > VPN > General	Group Policy Group Policy Manage VPN group policy Manage VPN group policy Manage VPN group policy mame policy information is reference Name payroll engineering DffGrpPolicy (System D	cies. A VPN gm d internally on the erenced by VPN Type Internal	pup policy is a collection he device or externally o I tunnel groups and use Tunneling Protocol nherited Sec Sec	AAA Server Group • N/A • • • N/A • • • N/A • • • N/A • •	ute/value e group Add • Edit Delete
			cisco	NA (2)	2 🛅 🔰 3/1 3/0	6 3:07:51 PM UTC

2. Com base em quais etapas foram executadas para configurar grupos de túneis no PIX, as Políticas de Grupo podem já existir para os grupos de túneis cujos usuários você deseja restringir. Se já existir uma Diretiva de Grupo adequada, escolha-a e clique em Editar. Caso contrário, clique em Add e escolha Internal Group Policy....



- 3. Se necessário, insira ou altere o nome da Diretiva de Grupo na parte superior da janela que será aberta.
- 4. Na guia Geral, desmarque a caixa Herdar ao lado de Filtro e clique em Gerenciar.

dit Internal Group Policy: pa	yroll		
Name: payroll			
∋eneral IPSec Client Confi	iguration C	lient Firewall Hardware Client	
Check an Inherit checkbox t	o let the corr	responding setting take its value from the default group policy	
Tunneling Protocols:	🔽 Inherit	F IPSec	
Filter:	🗆 İnherif	None Manage	
Connection Settings			
Access Hours:	🔽 Inherit	New	
Simultaneous Logins:	🔽 Inherit		
Maximum Connect Time:	🔽 Inherit	Unlimited minutes	
Idle Timeout:	🗹 Inherit	Unlimited minutes	
Servers			
DNS Servers:	🔽 Inherit	Primany: Secondary:	
WINS Servers:	🔽 Inherit	Primany: Secondary:	
DHCP Scope:	🔽 Inherit		
	OK	Cancel Help	
	UK	Help	

5. Clique em Add ACL para criar uma nova lista de acesso na janela do ACL Manager exibida.

1	ACL Mar	nager							X
	Configure	ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination HostNetwork	Service	Log Level Interval	Time Range	Add ACL
									Add ACE
									EditACE
									Delete
									Move Up
									Move Down
l	🖌 🖌	w traffic	3 C	Deny traffic				•	
				0	Cance	I	Help		

6. Escolha um número para a nova lista de acesso e clique em OK.

付 Add New	ACL				×
ACL ID:	10				
	ОK	R	Cance	el 🛛	

7. Com a nova ACL selecionada à esquerda, clique em Adicionar ACE para adicionar uma nova entrada de controle de acesso à lista.

🕵 ACL M	anager										×
Configu	re ACLs.										
#	Rule Enabled	Action	Source Host/Ne	etwork	Destination Host/Netw	n ork	Service	Log	Level wal	Time Rang	e Add ACL
10											Add ACE
											EditACE
											Delete
											Move Up
											Move Down
-											
🖌 🗸	low traffic	(3 C) eny traffic								
				OK		Cancel		Help			

8. Defina a entrada de controle de acesso (ACE) que deseja adicionar.

Neste exemplo, a primeira ACE na ACL 10 permite acesso IP à sub-rede de folha de pagamento de qualquer origem.

Observação: Por padrão, o ASDM seleciona somente o TCP como o protocolo. Você deve escolher IP se quiser permitir ou negar aos usuários acesso IP completo. Clique em OK quando terminar.

Action		Time Bange	
Action			
		Time Range: Not Applied 💌	New
Permit C De	ny	Syslog	
		Default Syslog More O	ntions
			parenterin
Source Host/Network		Destination Host/Network	
IP Address C Name	C Group	IP Address C Name	C Group
IR address: 0.0.0.0		IR address: 40.0.20.0	-
1 address. [0.0.0.0		10.0.20.0	
Mask: 0.0.0.0	*	Mask: 255.255.255.0 💌]
	_		-
Protocol and Service			
TOP CUDP CIC	MP 🐨 🕑	Manage Service	Groups
IP Protocol			
IP protocol: any			
ease enter the description be	low (optional):		
ermit IP access from ANY sou	rce to the payroll su	onet (10.8.28.0 /24)	
			•

9. O ACE que você acabou de adicionar agora aparece na lista. Escolha Adicionar ACE novamente para adicionar mais linhas à lista de acesso.

¢	ACL Mar	nager							x
	Configure	ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	ID								Add ACE
	1		1	🧠 any	10.8.28.0/24	💌 ip		Not Applied	Edit ACE
									Delete
									Move Up
									Move Down
l	•							•	
	🖌 🎺	w traffic	Q (Denytraffic					
					w				
					Canc		Help		

Neste exemplo, uma segunda ACE é adicionada à ACL 10 para permitir o acesso à subrede da Intranet.

Ration			Time Dense			
Action			- Time Range	Not Appl	ed	▼ Now
Permit	C Denv		nine Kange.	NOLAPPI	ieu j	New
· · · · · · ·	s Delly		-Syslog		Maria	Ontinue
			Default Sysio	g	More	Options
Source Host/N	letwork		Destination Ho	st/Network	<	
IP Address	C Name C G	roup	IP Address	C Na	ame	C Group
IP address:	0.0.0.0		IP address:	10.8.27.0)	_
Mask	0.0.0.0		Mask:	255.255.	255.0	*
Protocol and S	Service					
С ТСР С	UDP CICMP C	IP		Mana	ge Servio	e Groups
- IP Protocol -						
IP protocol	any					
lease enter the	e description below (option	al):				
ermit IP acces	s from ANY source to the s	ubnet used by	all employees (1	0.8.27.0/2	(4)	
						<u>}</u>

10. Clique em OK quando terminar de adicionar ACEs.

1	AC	L Ma	nager							×
С	on	figur	e ACLs.							
Γ		#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	Ξ	10								Add ACE
		1	V	~	🧼 any	A 10.5.28.0/24	😕 ip		Not Applied	EditACE
		2		V	🧇 any	10.8.27.0/24	🗈 ip		Not Applied	<u></u>
										Delete
										Move Up
										Move Down
	1								Þ	
	4	P Allo	ow traffic	(3)	Deny traffic					
					0	K Cance	el	Help		

11. Selecione a ACL que você definiu e preencheu nas últimas etapas para ser o filtro da sua Política de grupo. Clique em OK quando terminar.

oneth an innent thethou	ix to let the com	esponding setting take i	ts value from the default group po	olicy.
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. Clique em Apply para enviar as alterações ao PIX.



13. Se estiver configurado para fazer isso em Options > Preferences, o ASDM visualizará os comandos que está prestes a enviar para o PIX. Clique em Enviar.

🖆 Preview CLI Commands	X
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-filter value 10]
▼ Send Cancel	1

14. Aplique a Diretiva de Grupo que acabou de ser criada ou modificada ao grupo de túneis correto. Clique em Tunnel Group no quadro esquerdo.



15. Escolha o grupo de túneis ao qual deseja aplicar a diretiva de grupo e clique em Edit.

File Rules Se	1 for PIX - 10.89.129.147 arch Options Tools Wizards H	qle			
Home C	Configuration Montoring Ba	ck Forward Search	h Refresh S	ave Help	CISCO SYSTEMS
Hiterfaces Hiterfaces Security Policy NAT Security Policy NAT Security NAT Security NAT Security NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT	Configuration > VFN > General > Tu Configuration > VFN > General > Tu Configuration > VFN > General Configuration > VFN > General Configuration > VFN > General Configuration > VFN > General Configuration > VFN > General > Tu Configuration > VFN > General = Tu Configurat	Annel Group Manage VPN tunnel gro PBec or WebVPN conn Name Payroll engineering DefaultRAGroup DefaultL2LGroup Specify the delimeter to are received when tunne Group Delimiter:	ups: A VPN tunnel gr ection. Type ipsec-ra ipsec-ra ipsec-l2l be used when parsin els are being negotiar None	oup represents a connection Group Policy payroll engineering DftGrpPolicy DftGrpPolicy	specific record for a
			Apply	Reset	
Configuration cha	anges saved successfully.		cisco NA	(2) 📑 🙀	🔒 3/13/06 3:22:31 PM UTC

16. Se a Diretiva de Grupo foi criada automaticamente (consulte a etapa 2), verifique se a Diretiva de Grupo que você acabou de configurar está selecionada na caixa suspensa. Se sua Diretiva de Grupo não foi configurada automaticamente, selecione-a na caixa suspensa. Clique em OK quando terminar.

🞼 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. Clique em Apply e, se solicitado, clique em Send para adicionar a alteração à configuração do PIX.

Se a Diretiva de Grupo já tiver sido selecionada, você poderá receber uma mensagem informando "Nenhuma alteração foi feita". Click OK.

18. Repita as etapas de 2 a 17 para todos os grupos de túnel adicionais aos quais você deseja adicionar restrições.

Neste exemplo de configuração, também é necessário restringir o acesso dos engenheiros. Embora o procedimento seja o mesmo, estas são algumas janelas nas quais as diferenças são notáveis:

Nova lista de acesso 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	Maria I.a.
	2		1	🧇 any	4 10.8.27.0/24	🕑 ip		Not Applied	Move Op
									Move Down
•								F	
•	🖉 Allo	ow traffic	3 (Deny traffic					
				0	Cance	el	Help		

• Escolha Access List 20 como um filtro na Engineering Group Policy.

reaction pergineering				
eneral IPSec Client Conf	iguration Cl	ient Firewall Hardwai	re Client	
Check an Inherit checkbox t	o let the corre	esponding setting take	its value from the default group pol	icy.
Tunneling Protocols:	🗹 Inherit	F IPSec		
Filter:	🗌 Inherit	20	Manage	
Connection Settings				
Access Hours:	🔽 Inherit		▼ New	
Simultaneous Logins:	🔽 Inherit			
Maximum Connect Time:	🔽 Inherit	🗖 Unlimited	minutes	
Idle Timeout:	🔽 Inherit	Unlimited	minutes	
Servers				
DNS Servers:	🔽 Inherit	Primary:	Secondary:	
WINS Servers:	🔽 Inherit	Primary:	Secondary:	
DHCP Scope:	🔽 Inherit			

• Verifique se a diretiva de grupo de engenharia está definida para o grupo de túnel de engenharia.

🚰 Edit Tunnel Group	×
Name: engineering Type: ipsec-ra	
General IPSec	
Configure general access attributes from the following sub-tabe	
Basic AAA Client Address Assignment Advanced	
	l
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	

Configurar o acesso via CLI

Conclua estas etapas para configurar o Security Appliance usando a CLI:

Observação: alguns dos comandos mostrados nesta saída são trazidos para uma segunda linha devido a razões espaciais.

1. Crie duas listas de controle de acesso diferentes (15 e 20) que são aplicadas aos usuários quando eles se conectam à VPN de acesso remoto. Essa lista de acesso é chamada posteriormente na configuração.

<#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
```

 Crie dois pools de endereços VPN diferentes. Crie um para Folha de Pagamento e um para os usuários remotos do Engineering.

<#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. Crie políticas para Folha de Pagamento que se apliquem somente a elas quando se conectarem.

```
<#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)#
vpn-filter value 15
!--- 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. Esta etapa é igual à etapa 3, exceto que é para o grupo Engenharia.

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

```
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.

 Crie usuários locais e designe os atributos recém-criados a esses usuários para restringir seu acesso aos recursos.

```
<#root>
ASAwCSC-CLI(config)#
username engineer password ciscol23
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)#
vpn-group-policy Payroll
ASAwCSC-CLI(config-username)#
vpn-filter value 15
```

6. Crie grupos de túnel que contenham políticas de conexão para os usuários do Payroll.

```
<#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. Crie grupos de túneis que contenham políticas de conexão para os usuários do Engineering.

```
<#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
```

Depois que a configuração for inserida, você poderá ver esta área destacada em sua configuração:

Nome do dispositivo 1
<#root>
ASA-AIP-CLI(config)#
show running-config
ASA Version 7.2(2)
hostname ASAwCSC-ASDM
domain-name corp.com
enable password 9jNtZuG3TC5tCVH0 encrypted
interface Ethernet0/0
nameif Intranet
in address 10.8.27.2 255.255.0
! !
interface Ethernet0/1
nameif Engineer
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/2
nameit Payroll security-level 100
ip address 10.8.28.0
interface Ethernet0/3

```
no nameif
no security-level
no ip address
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 6XmYwQOO9tiYnUDN 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
L
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)#
```

Verificar

Use os recursos de monitoramento do ASDM para verificar sua configuração:

1. Selecione Monitoring > VPN > VPN Statistics > Sessions.

Você vê as sessões de VPN ativas no PIX. Selecione a sessão na qual está interessado e clique em Details.

File Rules Search	PIX - 10.69.129.147 Options Tools Wizards I	Help			
ල්) ග් Hame Config	Monitoring E	CoCoCoCoCoCoCoCoCoCoCoCoCoCoCoCoCoCoCo	Q Q earch Refresh	🔜 🤶 Save Help	CISCO SYSTEMS
Interfaces	toring > VPN > VPN Statistics VPN Connection Grapt IPSec Tunnels VPN Statistics Crypto Statistics Encryption Statistic Global IKE/IPSec 8 Protocol Statistics Sessions	Sessions Remote Access Filter By: Remote A Username controller1 To sort VPN sessions, Logout By: - All Se	LAN-to-LAN 1 CCCESS I All Sess Group Policy Tunnel Group Officy Policy Sayroll ight-click on the above ssions I	Total 0 sions Assigned IP Address Public IP Address 10.8,27,50 172,22.1.165 3 total t	Total Cumulative 1 3 Fitter Protocol Encryption Cogout Essions Ping Sort Order from popup menu. gout Bessions
Data Refreshed Survey	ssfully		icisco in	NA (7) 🛛 🖓 🔜	B 3/13/08 8:36:34 PM UTC

2. Selecione a guia ACL.

O hitchts da ACL reflete o tráfego que flui pelo túnel do cliente para a(s) rede(s) permitida(s).

	Craus Bolley	Registered ID Addresse	Destacol	L ogio Timo	ClientTime
Usemame	Tunnel Group	Public IP Address	Encryption	Duration	Version
ntroller1	DfttGrpPolicy 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
The following	ACL is being appli	ed to this session:			
access-list 10 access-list 10 access-list 10 access-list 10 access-list 10	; 2 elements line 1 remark per line 2 extended p line 3 remark per line 4 extended p	mit IP access from ermit ip any 10.8.2 mit IP access from ermit ip any 10.8.2	ANY source to the 8.0 255.255.255.0 ANY source to the 7.0 255.255.255.0	payroll subnet (10.8.28.0 /2 (hitcnt=8) 0x25954260 subnet used by all employees (hitcnt=4) 0xd52617df	34) 9 (10.8.27.0 /2
access-list 10 access-list 10 access-list 10 access-list 10 access-list 10	; 2 elements line 1 remark per line 2 extended p line 3 remark per line 4 extended p	mit IP access from ermit ip any 10.8.2 mit IP access from ermit ip any 10.8.2	ANY source to the 8.0 255.255.255.0 ANY source to the 7.0 255.255.255.0	payroll subnet (10.8.28.0 /2 (hitcnt=8) 0x25954260 subnet used by all employees (hitcnt=4) 0x452617df	;4) ⊅ (10.8.27.0 /2

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- <u>Exemplo de Configuração do Cisco ASA 5500 Series Adaptive Security Appliances ASA</u> como um Servidor VPN Remoto Usando o ASDM
- <u>Exemplos de Configuração e Notas Técnicas dos Dispositivos de Segurança Cisco PIX 500</u> <u>Series</u>
- <u>Exemplos de configuração e notas técnicas dos dispositivos de segurança adaptáveis Cisco</u> <u>ASA 5500 Series</u>
- Exemplos de configuração e notas técnicas do Cisco VPN Client
- Suporte Técnico e Documentação Cisco Systems

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.