# Configurar o tunelamento dividido para clientes VPN no ASA

# Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Diagrama de Rede
Produtos Relacionados
Conventions
Informações de Apoio
Configuração da Separação de Túneis no ASA
Configuração do ASA 7.x com o Adaptive Security Device Manager (ASDM) 5.x
Configurar o ASA 8.x com ASDM6.x
Configurar o ASA 7.x ou posterior via CLI
Configurar o PIX 6.x através do CLI
Verificar
Conexão com o Cliente VPN
Exibir o registro do cliente VPN
Teste o acesso à LAN local com ping
Troubleshooting
Limitação com número de entradas em uma ACL de túnel dividido
Informações Relacionadas

# Introdução

Este documento descreve o processo para permitir que clientes VPN acessem a Internet enquanto fazem o tunelamento em um Cisco ASA 5500 Series Security Appliance.

# Pré-requisitos

## Requisitos

Este documento supõe que já existe uma configuração de VPN de acesso remoto em funcionamento no ASA. Consulte <u>Exemplo de Configuração do PIX/ASA 7.x como Um Servidor</u> <u>Remoto Usando o ASDM se uma configuração não estiver disponível.</u>

**Componentes Utilizados** 

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

- · Cisco ASA 5500 Series Security Appliance Software versão 7.x ou posterior
- Cisco Systems VPN Client versão 4.0.5
- Adaptive Security Device Manager (ASDM)



Observação: este documento também contém a configuração CLI do PIX 6.x que é compatível com o Cisco VPN Client 3.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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Diagrama de Rede

O VPN Client está localizado em uma rede SOHO típica e se conecta pela Internet ao escritório principal.



Diagrama de Rede

## Produtos Relacionados

Essa configuração também pode ser usada com o Cisco PIX 500 Series Security Appliance Software versão 7.x.

### Conventions

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

## Informações de Apoio

Este documento fornece instruções passo a passo sobre como permitir que Clientes VPN acessem a Internet enquanto são enviados pelo túnel para dentro de um Mecanismo de Segurança Cisco Adaptive Security Appliance (ASA) 5500 Series. Esta configuração fornece aos Clientes VPN acesso seguro aos recursos corporativos através do IPsec, ao passo que gera acesso não protegido à Internet.



Observação: o tunelamento completo é considerado a configuração mais segura porque não permite o acesso simultâneo do dispositivo à Internet e à LAN corporativa. Um comprometimento entre o tunelamento completo e o tunelamento dividido permite que os clientes VPN acessem apenas a LAN local. Consulte PIX/ASA 7.x: Exemplo de Configuração de Permissão de Acesso à LAN Local para Clientes VPN para obter mais informações.

Em um cenário básico de VPN Client para ASA, todo o tráfego do VPN Client é criptografado e enviado para o ASA, independentemente de seu destino. Com base na sua configuração e no número de usuários suportados, essa configuração pode consumir muita largura de banda. O tunelamento dividido pode funcionar para aliviar esse problema, pois permite que os usuários enviem apenas o tráfego destinado à rede corporativa pelo túnel. Todo o tráfego restante, como mensagens instantâneas, e-mail ou navegação ocasional, é enviado para a Internet através da LAN local do VPN Client.

# Configuração da Separação de Túneis no ASA

## Configuração do ASA 7.x com o Adaptive Security Device Manager (ASDM) 5.x

Conclua estes passos para configurar seu grupo de túneis para permitir o tunelamento dividido para os usuários no grupo.

1. Escolha Configuration > VPN > General > Group Policy e selecione a Group Policy na qual você deseja habilitar o acesso à LAN local. Em seguida, clique em Editar.



2. Vá até a guia Client Configuration (Configuração do cliente).

General IPSec Client Configuration Client Firewall	Hardware Client NAC WebVPN
Check an Inherit checkbox to let the corresponding	setting take its value from the default group policy.
General Client Parameters Cisco Client Parameters	s Microsoft Client Parameters
Banner:	Minherit Edit Banner
Default Domain:	🔽 Inherit
Colli Tamari DhiChiana (anna dalada D	E http://
Split Tunnel DNS Names (space delimited):	I∕ innent
Split Tunnel Policy:	V Inherit
	_
Split Tunnel Network List:	Manage
Address pools	
🔽 Inherit	
Available Pools	Assigned Pools (up to 6 entries)
	Add≥>
	< <remove< td=""></remove<>

3. Desmarque a caixa Inherit para Split Tunnel Policy e selecione Tunnel Network List Below ..

Name: hillvalleyvpn		
meral IPSec Client Configuration Client Firewall	Hardware Client	
sherai   P360 chera configeration   Citeriu Piretvali	I naroware cienc	
Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
General Client Parameters	L Margarett Clicut	Parameters I
General Client Parameters   Cisco Client Parameters	s   Microsoft Cilerit	Parameters
Banner'	V Inherit	Edit Banner
Danner.	14 In the second	LONG ROMITION ST
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
	_	
Split Tunnel Policy:	I Inherit	Tunnel All Networks
	_	Tunnel All Networks Tunnel Network List Below
Split Tunnel Network List	l⊻ Inherit	Exclude Network List Below
Address pools		
Avaïable Pools		Assigned Pools (up to 6 entries)
		(
	Addee	]
	< <remove< td=""><td></td></remove<>	

Desmarque a caixa Inherit para Split Tunnel Network List e clique em Manage para iniciar o ACL Manager.

iternal Group Policy: hillvalleyvpn		
ame: hillvalleyvpn		
neral IPSen Client Configuration Client Firewal	L Hardware Client	
ierai ( 17360 ) enerri cernigaranen ( cierit Pirevrai	r   naruware cient	
Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
Seneral Client Parameters Cisco Client Parameter	s Microsoft Client	Parameters
Banner:	✓ Inherit	Edit Banner
Default Domain:	🗹 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
	<b>E</b>	-
Split Tunnel Policy:	1 Innent	
Split Tunnel Network List:	inherit;	None Manage
Address pools		
Available Pools		Assigned Pools (up to 6 entries)
	Add≽⊳	
	<-Remove	
	Contracting the	

No ACL Manager, selecione Add > Add ACL... para criar uma nova lista de acesso.

	ACL Manager					( ) I	L I		X
lí	Standard AGL Edender	I AGL							
	◆ Add → 🗐 5dt 🎁	D-Mrr -	F 4   X 4	h 18					
	Add AGL.	dress	.A_6	05	Description				
	· Add ACE. **								
	Topert Atter.								
		-							

Forneça um nome para a ACL e clique em OK.

📫 ACL Manager			X
Standard ACL Extended ACL			
♣ Abi + (() Etc. () DEcc. () # 4	X 陶 略 -		
No Address	Action Description		
			- 1
			- 1
			- 1
			- 1
			- 1
	📫 Axid ACL	X	- 1
	AG, Name: Spit_Turnel_List		- 1
	OV Count	L Hoto	- 1
			- 1
			- 1
			- 1
			- 1
			- 1
Rule Row Diagram			×
	s inside a contract out	side -3	
	deny	···•	
	OK Cancel	Pep	

Depois que a ACL for criada, escolha Add > Add ACE. .para adicionar uma entrada de controle de acesso (ACE).

٠



Defina a ACE que corresponde à LAN por trás do ASA. Nesse caso, a rede é 10.0.1.0/24.

a.

Escolha Permitir.

b.

Escolha o endereço IP 10.0.1.0

c.

Escolha a máscara de rede 255.255.255.0.

#### d.

(Opcional)Forneça uma descrição.

Clique em > OK.

ACL Manager		
Standard ACL Edg	nderil AOL	
◆ Add → 圖(F/R)	Delete 🕈 4 🐰 Ra 🛍 -	
No	Address Action Description	
Spit_Turnet_List		
	St Add ALL	4
	- Artim	
	Action of Lower T	
	Horthedwork	
	P Address  90.1.0	
	Network: 255.253.253.0	
	Description	
	The corporate network behind the ASA.	
	OK Conca Hosp	
		_
Rule Flow Disgram		
	E	

Clique em OK para sair do ACL Manager.

•

e.



Certifique-se de que a ACL que você acabou de criar esteja selecionada para Split Tunnel Network List.

Nerre:       PilvaReyrpn         General       PSac       Clerit Configuration       Clerit Pirewall       Hardware Clerit       NAC       WeivVPil         Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.       General Clerit Parameters       Cloco Clerit Parameters       Microsoft Clerit Parameters         General Clerit Parameters       Cloco Clerit Parameters       Microsoft Clerit Parameters       Elst Elstrongen	Neme:       Neme:         General       IPSic       Clert Configuration       Clert Preveal       Hardware Clert       NAC       WebVPN         Check an inhert checkbox to let the corresponding setting take its value from the default group policy.       General Clert Parameters       Clecc Clert Parameters       Microsoft Clert Parameters         Banner:       IP Innel       IP Innel       Eff Parver.         Default Donveix       IP Innel       IP Innel       IP Parver.         Spit Tunnel DMS Names (space definited):       IP Innel       Ip Innel Network Llet:       IP Innel       IP Innel INT INNEL       Manage         Address pools       Address pools       Address       Address (pools (poils Fiertnes))       Address         Immed       Address       Address       Field Strenge       Innel Inter(In	Edit Internal Group Policy: hillvalleyvpn		
General       PSec       Clert Configuration       Clert Reswall       Hardware Clert       NAC       WebWPN         Check as Inherit checkbox to let the corresponding setting take its value from the default group policy.       General       General       Edr. Borner.         Default       Clert Parameters       Cloco Clert Parameters       Microsoft Clert Parameters       Biorner.         Default       Dowar       Inherit       Edr. Borner.         Default       Dowar       Inherit       Edr. Borner.         Spit Tunnel DNS Nemes (space definited):       Inherit       Turnel Network List Below       Inherit         Spit Tunnel Policy:       Inherit       Spit Turnel Network List Below       Inherit         Addresse pools       Cutsite_cryptional       None -         Addresse pools       Cutsite_cryptional       None -         Addresse pools       Cutsite_cryptional       Cutsite_cryptional         Inherit       Cutsite_cryptional       Cutsite_cryptional         Addresse pools       Cutsite_cryptional       Cutsite_cryptional         Inherit       Cutsite_cryptional       Cutsite_cryptional         Inherit       Cutsite_cryptional       Cutsite_cryptional         Inherit       Cutsite_cryptional       Cutsite_cryption         Inherit </th <th>Operand [PSec] Clerk Configuration       Clerk Firewall Hardware Clerk [NAC] Web/VPN         Check an Inhert checkbox to let the corresponding setting take its value from the default group policy.         Central Clerk Parameters       Claco Clerk Parameters         Banner:       Inhert         Default Domain:       Inhert         Spit Tunnel DNS Names (space definited):       Inhert         Spit Tunnel Policy:       Inhert         Spit Tunnel Network Liet:       Inhert         Address pools       Address pools         Address pools       Address         Address pools       Address         Inhert       Address pools         Inhert       Inhert</th> <th>New New Pillesterre</th> <th></th> <th></th>	Operand [PSec] Clerk Configuration       Clerk Firewall Hardware Clerk [NAC] Web/VPN         Check an Inhert checkbox to let the corresponding setting take its value from the default group policy.         Central Clerk Parameters       Claco Clerk Parameters         Banner:       Inhert         Default Domain:       Inhert         Spit Tunnel DNS Names (space definited):       Inhert         Spit Tunnel Policy:       Inhert         Spit Tunnel Network Liet:       Inhert         Address pools       Address pools         Address pools       Address         Address pools       Address         Inhert       Address pools         Inhert       Inhert	New New Pillesterre		
General       PSec       Clerct Contiguration       Clerct Firewall       Handware Clerct       NAC       WebVPN         Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.       General       Clerct Parameters       Clerct Parameters         General       Clerct Parameters       Clerct Parameters       Microsoft Clerct Parameters       Edit Dorver.         Berner:       Image:       Image:       Image:       Edit Dorver.         Default Dorver.       Image:       Image:       Image:       Image:         Split Tunnel DNS Names (space delimited):       Image:       Image:       Image:       Image:         Split Tunnel Network List:       Image:       Image:       Image:       Image:       Image:         Address pools       Clerct Parameters       Accidese_protos       Clerct Dorver       Image:	General       PSec       Clerct Contiguration       Clerct Firewall       Hardware Clert       NAC       WebVPN         Check an Inhert checkbox to let the corresponding setting take its value from the default group policy.         General       Clerct Parameters       Cloco Clert Parameters       Microsoft Clert Parameters         Banner:       Image:       Image:       Edit Parameters         Default Domain:       Image:       Image:       Image:         Split Tunnel DNS Names (space delimited):       Imment       Tunnel Network List Below       Image:         Split Tunnel Policy:       Imment       Imment       Image:       Image:         Address pools       Imment       Edit Store       Image:       Image:       Image:         Address pools       Address pools       Address       Address pools       Edit Store       Image:       Image	mane. parrancjipri		
Check as Inherit checkbox to let the corresponding setting take its value from the default group policy.   General Client Parameters Cloco Client Parameters   Benner: Image: Edr Borner.   Default Domain: Imherit   Spit Tunnel DNS Names (space delimited): Imherit   Spit Tunnel Policy: Imherit   Spit Tunnel Network List: Imherit   Addresse pools Odd Kinger Pools   Addresse pools Odd Kinger Pools   Addresse pools Control List   Addresse pools Control List   Addresse pools Control List   Control List Control List   Addresse pools Control List   Control List Control List	Check an inherit checkbox to let the corresponding setting take its value from the defauit group policy.  Central Clerit Parameters Cloco Clerit Parameters Microsoft Clerit Parameters Banner:  Defauit Donvein:  Defauit Donvein:  Defauit Donvein:  Split Tunnel DMS Names (space delivited):  Split Tunnel Network List:  Split Tunnel Network List:  None  Address pools  Nordiste Epoils  Addres  Addres  Addres  Cool (op to 5 entres)  Addres  Addres Addres  Addres  Addres  Addres  Addres  Addres  Addres  Addres  Addres  Addres  Addres  Addres  Addres  Addres  Addres  Addres  Addres  Addre	General IPSec Client Configuration Client Firewal	Hardware Client	NAC WebVPN
Ceneral Client Parameters Cisco Client Parameters   Berner: Inherit   Default Domain: Inherit   Spit Tunnel DNS Names (space delimited): Inherit   Spit Tunnel Policy: Inherit   Spit Tunnel Network List: Inherit   Spit Tunnel Network List: Inherit   Address pools Address pools   Address pools Address pools   Address pools Address   Address pools Address   Address pools Address	Central Clert Parameters Disco Clert Parameters   Banner: Inhert   Default Donvain Inhert   Spit Tunnel DNS Names (space delinited): Inhert   Spit Tunnel Policy: Inhert   Spit Tunnel Network List: Inhert   Address pools Stit Tunnel List   Address pools Address	Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
Berner: Inhest   Detaut Domein: Inhest   Spit Tunnel DAS Nenes (space delinited): Inhest   Spit Tunnel Policy: Inhest   Spit Tunnel Network List: Inhest   Spit Tunnel Network List: Inhest   Address pools Inhest   Address pools Address   Address pools Address   Address pools Address   Address pools Address	Berner: Inherit   Detault Donveix Inherit   Spit Tunnel DNS Names (space delimited): Inherit   Spit Tunnel Policy: Inherit   Spit Tunnel Network List: Inherit   Address pools Spit Tunnel List   Address Address   Address Spit Tunnel Network Dist Distributed	General Clent Parameters Cloco Clent Parameter	s Microsoft Client	Parameters
Berner:       Image: Convert         Default Donveix       Image: Convert         Spit Tunnel DNS Names (space delimited):       Immerit         Spit Tunnel Policy:       Immerit         Spit Tunnel Policy:       Immerit         Spit Tunnel Network List:       Immerit         Address pools       Immerit         Address pools       Outside_cryptomax         Address pools       Address         Address       Address         Address       Address         Address       Address         Address       Address         Address       Address	Berner: Image: Edit Edite   Default Donveix Image: Im	,		
Default Domain:     Spit Tunnel DNS Names (space delimited):     Spit Tunnel Policy:     Intent:     Spit Tunnel Network List:     Intent:     Address pools     Address pools     Address     Address <td>Default Domain:     Spit Turnel DNS Names (space delimited):     Spit Turnel Policy:     Inherit     Spit Turnel Network List:     Inherit     Spit Turnel Network     Spit Turnel Network     Inherit     Spit Turnel Network     Inherit     Spit Turnel Network     Spit Tur</td> <td>Banner.</td> <td>🔽 Inhert</td> <td>Edt Borner</td>	Default Domain:     Spit Turnel DNS Names (space delimited):     Spit Turnel Policy:     Inherit     Spit Turnel Network List:     Inherit     Spit Turnel Network     Spit Turnel Network     Inherit     Spit Turnel Network     Inherit     Spit Turnel Network     Spit Tur	Banner.	🔽 Inhert	Edt Borner
Spit Tunnel DNS Names (space delimited):     Spit Tunnel Policy:     Spit Tunnel Network List:     Inherit     Address pools     Address     Address     Inherit     Address     Address     Inherit     Address     Inherit     Inhe	Spit Tunnel DNS Names (space delimited):     Spit Tunnel Policy:     Spit Tunnel Network List:     Inherit     Address pools     Address	Destauit Downein:	E interit	
Spit Tunnel DNS Names (space delimited):     Spit Tunnel Policy:     Spit Tunnel Network List:     Inherit     Spit Tunnel Network List:     Inherit     Address pools     Address po	Spit Tunnel DNS Names (space delimited):     Spit Tunnel Policy:     Spit Tunnel Network List     Inherit     Address pools     Ad	L-C-MARK DAMINGS	1. BERN	
Spit Tunnel Policy:     Spit Tunnel Network List:     Inhert:     Address pools:     Address pools:     Address pools:     Address pools:     Address pool:     Address pool: <tr< td=""><td>Spit Turnel Policy:     Spit Turnel Network List:     Intent     Spit Turnel Network List:     Intent     Address pools     Address     Address</td><td>Split Tunnel DNS Names (space delimited):</td><td>P Inherit</td><td></td></tr<>	Spit Turnel Policy:     Spit Turnel Network List:     Intent     Spit Turnel Network List:     Intent     Address pools     Address	Split Tunnel DNS Names (space delimited):	P Inherit	
Spit Tunnel Network List:     Address pools	Spit Tunnel Network List     Address pools     Address     Address <td>Split Tunnel Policy:</td> <td>[] Interit</td> <td>Turnel Network List Below</td>	Split Tunnel Policy:	[] Interit	Turnel Network List Below
Spit Turnel Network List:     Address pools     Address pools <t< td=""><td>Spit Tunnel Network List:     Address pools     Address     A</td><td></td><td></td><td></td></t<>	Spit Tunnel Network List:     Address pools     Address     A			
Address pools  Address pools  Available Pools  Address  A	Address pade Interit Available Pade Address Address pade Available Pade Address Addre	Spilt Tunnel Network List:	[ Inhert	Splt_TurneU Manage
Available Roots     Accigned Roots (up to 6 ontries)	Image: Sector	-Address pools		Spit_Turnel_List
Available Pools Addree	Available Pools Addree collemove	F interit		outside_cryptomap <sup>5</sup>
Addree	Addive	Avaitable Pools		Assigned Pools (up to 6 entries)
< diemone			Addres	1
			collemone	il l
				1

Clique em OK para retornar à configuração da Política de Grupo.

i 💼 Ei	dit In	ternal Grou	ıp Policy: hillvalleyvpn	1.11				X
	Ne	me. Ja	Ivaleyvpn					
	Ger	eral   IPSec	Client Configuration Client	Firewall Har	rdware Client	NAC WebVPN		
	С	heck an Inhe	nt checkbox to let the corresp	onding settin	g take its valu	e from the default grou	ap policy.	
	G	General Client	Parameters Cisco Client Par	nomotons   M	crosoft Client	Parametera		
		Banner:			🔽 inhert	Edit Bo	mer	
		Default Do	mainc		P Inherit			
		Spilt Tunne	I DNS Names (space delimited	0:	🖂 inherit			
		Split Tunne	i Policy:		Inherit	Tunnel Network List	Below 💌	
		Split Tunne	Network List:		linhert	Spit_Tunnel_L*	Manage	
		-Address p	ools					

Clique em Aplicar e depois em Enviar (se necessário) para enviar os comandos para o ASA.

٠



Configurar o ASA 8.x com o ASDM 6.x

•

Conclua estes passos para configurar seu grupo de túneis para permitir o tunelamento dividido para os usuários no grupo.

Selecione Configuration > Remote Access VPN > Network (Client) Access > Group Policies e escolha a Política de Grupo na qual deseja habilitar o acesso à LAN local. Em seguida, clique em Editar.

Configuration > Remote Access VPN > Net	WORK (Client) Access	> Group Policies					
Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internation is referenced by VPN bunnel groups and user accounts.							
🗣 Add 📼 📝 Edik 📋 Delete	🚸 Add 👻 📝 Edk 📋 Delete						
Name	Туре	Tunneling Protocol	A				
OftGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N/A				
Defaultgroup	Interna	- Inherited	N/A				
(hivalleyvpn	- Internal	svc,IPSec	N/A				

Clique em Split Tunneling.

📫 Edit Internal Group Policy	y: hivalleyvpn	
General Servers Advanced Golt Turneling - IE Browser Proxy B-SSL VPN Client - IPsec Client	Split tunneling network lats distinguish networks that require traffic to go through the tunnel and those require tunneling. The security appliance makes split tunneling decisions on the basis of a network lat, v ACL that consists of list of addresses on the private network. DNS Names: 🖓 Inherit 📃	that do no vhich is an
Clent Access Rule Clent Firewal	Network List: 🖓 Scherit	leniege
100000000000	Intercept DHCP Configuration Message from Micosoft Clients	- e
	Intercept: IV Inherit IC Vice IC No	
	Subnet Mesk (Optional): 0.0.0.0	*
4 · · ·		

Desmarque a caixa Inherit da Split Tunnel Policy e selecione Tunnel Network List Below.

1	Edit Internal Group Policy	y: hivalleyvpn	
	General Gervers Advanced	Split bunneling network lists distinguish networks that require traffic to go through the tunnel and th require tunneling. The security appliance makes split tunneling decisions on the basis of a network list ACL that consists of list of addresses on the private network.	iose that do no st <sub>v</sub> which is an
		DNS Names: 🔽 Inherit Policy: Tunnel Network List Below	
	- Clerit Access Rule - Clerit Prewal - Hardware Clerit	Network List IP Inherit Tunnel Al Network List Below Exclude Network List Below	Managa
		Intercept DHCP Configuration Message from Micosoft Clients	*
		Intercept:  Interc	ws clients

Desmarque a caixa Inherit da Split Tunnel Network List e clique em Manage para iniciar o ACL Manager.

f Edit Internal Group Policy	: hiralleyvpn
Genéral Servins El Advanced	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.
	DNS Names: 🔽 Inherit
B-IPse: Clent	Policy: Dinherit Turnel Network List Below +
- Client Access Rule - Client Firewall	Network List: Street None
·maroware Cienc	Intercept DHCP Configuration Message from Micosoft Clients (*)
	DHCP Intercept lets Microsoft XP clients use split tunneling with the security appliance. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask.
	Intercept: 🔽 Inherit C Yes C No
	Subret Hask (Options): 0.0.0.0

No ACL Manager, selecione Add > Add ACL... para criar uma nova lista de acesso.

i ACL	Manager				
Stani	dard ACL Extend	JOA be			
*	Add 🔹 📓 EdR	💼 Delete 👌	4 🕺 🐚	<b>B</b> . •	
49	Add ACL		Action	Description	
+	Add ACE				
1.20	Insert				
-	Insert After				

Forneça um nome para a ACL e clique em OK.

•

💼 ACL Mana	ger			
Standard AG	3. Extended ACL			
🗣 Add 🔸	🖬 Edit 🏢 Delete 🛉	4 X Pa 🖻	L +	
No	Address	Action	Description	
	Add A	CL e: Split_Tunnel_List OK Cance	Help	
		· · · · · ·		

Após criar a ACL, selecione Adicionar > Adicionar ACE... para adicionar uma entrada de controle de acesso (ACE).

andard ACL Extende	d ACL		
🖡 Add 🕞 📷 Edit	👔 Delete 🛛 🛧	4 % Pa	<b>*</b>
Add ACL	55	Action	Description
Add ACE	9		
Insert			
Insert After			

Defina a ACE que corresponde à LAN por trás do ASA. Nesse caso, a rede é 10.0.1.0/24.

a.

•

Clique no botão de opção Permit.

b.

Selecione o endereço de rede com a máscara 10.0.1.0/24 .

c.

(Opcional) Forneça uma descrição.

d.

Click OK.

📫 ACL Manager					
Standard ACL Extended AC	1				
🗢 Add 👻 🔟 Edt 📋 🕻	Selete 🕈 🗲 👗	Ra Ba -			
No Addr	ess Action		Description		
Split_Turnel_List					
	- A 44 AFT			and the second se	-
	1 HOU HEE				
	Action: (* Permit (	Deny			
	Address: 10.0.1.0/24			17	
	Description:				
	The Corporate natwork b	whind the ASA			
	1				
		OK.	Cancel	Help	
			and 1		

Clique em OK para sair do ACL Manager.

ACL Manager					
Owned wet Area and	a a secol				
scandaro Acc   Exten	ded ACL				
💠 Add 🔹 🧭 Edit	Delete 🕈	4 Å	45 mil -		
No	Address	Action		Description	
Split_Tunnel_List					
1 10.0.	1.0/24	of Permit	The Corporate	e network behind the A	SA
			<u></u>		
			C or C	Canval	Halo

Certifique-se de que a ACL que você acabou de criar esteja selecionada para Split Tunnel Network List.

Clent Access Rule     Clent Pressal     Hardware Clent     Network List:      Defer DHCP Config Solt_Tunnel_List     Manage     None     Intercept DHCP Config Solt_Tunnel_List     DHCP Intercept lets Microsoft XP clents use split tunneling with the security appliance. For Windows clents     prior to XP, DHCP Intercept provides the domain name and subnet mask.	Colic Informal Group Policy: General Servers Advanced IE Browser Proxy (i)-SS, VPN Client Eser Client	hivalleyvpn         Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do nequire tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is at ACL that consists of list of addresses on the private network.         DNS Names:       Image: Ima
antercept: 14 antert 1, http://www.communication.com	-Clent Access Rule -Clent Freeval -Hardware Clent	Network List:       Inherit       Splt_Tunnel_List       Manage         Intercept OHCP Config       Splt_Tunnel_List           DHCP Intercept lets Microsoft XP clients use split tunneling with the security appliance. For Windows clients prior to XP, OHCP Intercept provides the domain name and subnet mask.           Intercept:       Inherit       C 100

Clique em OK para retornar à configuração da Política de Grupo.

٠

Coneral General Servers Advanced	Split tunneling network is require tunneling. The se ACL that consists of list o	ts distinguish networks that require traffic to go through the tu curity appliance makes split tunneling decisions on the basis of 4 if addresses on the private network.	nnel and th a network le	ose that do not it, which is an
IE Browser Proxy	DNS Names: 🗵 Inherit			
B-SSL VPN Clent B-IPsec Clent	Policy: 🕅 Inherit	Tunnel Network List Below	*	
	NetworkList: 🗖 Inherit	Splk_Tunnel_List		Manage
	Intercept DHCP Con DHCP Intercept lets Mi prior to XP, DHCP Inter Intercept: 🔽 Inherit	figuration Message from Micosoft Clients crosoft XP clients use split tunneling with the security appliance cept provides the domain name and subnet mask.	For Windo	(8) es dients

Clique em Aplicar e depois em Enviar (se necessário) para enviar os comandos para o ASA.

#### Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored intermexternally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.

Name	Туре	Tunneling Protocol	
OfItGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpri	N/A
Defaultgroup	Internal	Inherited	N/A
hivalleyvon	Internal	syc. IPSec	N/A -

Acoly Reset

Configurar o ASA 7.x ou posterior via CLI

Em vez de usar o ASDM, você pode concluir estas etapas na CLI do ASA para permitir o tunelamento dividido no ASA:



Nota: A configuração da separação de túneis na CLI é a mesma para o ASA 7.x e 8.x.

Entre no modo de configuração.

<#root>

٠

ciscoasa>

#### enable

Password: \*\*\*\*\*\*\* ciscoasa#

configure terminal

ciscoasa(config)#

Crie a lista de acesso que define a rede por trás do ASA.

<#root>

•

ciscoasa(config)#

access-list Split\_Tunnel\_List remark The corporate network behind the ASA.

ciscoasa(config)#

access-list Split\_Tunnel\_List standard permit 10.0.1.0 255.255.255.0

Entre no modo de configuração de Política de Grupo para a política que você deseja modificar.

<#root>

•

ciscoasa(config)#

group-policy hillvalleyvpn attributes

ciscoasa(config-group-policy)#

Especifique a política de túnel dividido. Neste caso, a política é tunnelspecified.

<#root>

•

ciscoasa(config-group-policy)#

split-tunnel-policy tunnelspecified

Especifique a lista de acesso de túnel dividido. Neste caso, a lista é Split\_Tunnel\_List.

<#root>

٠

ciscoasa(config-group-policy)#

split-tunnel-network-list value Split\_Tunnel\_List

Emita este comando:

<#root>

#### ciscoasa(config)#

tunnel-group hillvalleyvpn general-attributes

Associe a política do grupo ao grupo do túnel.

<#root>

•

ciscoasa(config-tunnel-ipsec)#

default-group-policy hillvalleyvpn

Saia dos dois modos de configuração.

<#root>

٠

ciscoasa(config-group-policy)#

exit

ciscoasa(config)#

exit

ciscoasa#

•

Salve a configuração na RAM não volátil (NVRAM) e pressione Enter quando avisado para especificar o nome de arquivo de origem.

<#root>

ciscoasa#

copy running-config startup-config

Source filename [running-config]? Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a

3847 bytes copied in 3.470 secs (1282 bytes/sec) ciscoasa#

Configurar o PIX 6.x através do CLI

Conclua estes passos:

•

Crie a lista de acesso que define a rede atrás do PIX.

<#root>

PIX(config)#access-list Split\_Tunnel\_List standard permit 10.0.1.0 255.255.255.0

• Crie um vpn group **vpn3000** e especifique a ACL do túnel dividido para ele como mostrado:

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split\_Tunnel\_List



**Observação**: consulte o <u>Cisco Secure PIX Firewall 6.x e o Cisco VPN Client 3.5 para Windows com Autenticação IAS RADIUS do</u> <u>Microsoft Windows 2000 e 2003</u> para obter mais informações sobre a configuração de VPN de acesso remoto para o PIX 6.x.

Verificar

Conclua as etapas nessas seções para verificar a configuração.

Conexão com o Cliente VPN

Exibir o registro do cliente VPN

Teste o acesso à LAN local com ping

Conexão com o Cliente VPN

•

•

•

Conecte seu VPN Client ao VPN Concentrator para verificar sua configuração.

PPN Client - Version 4.0.5 (Rel)		
Connection Entries Status Certificates Log	Options Help	
Connect New Import	Modify Delete	Cisco Systems
Connection Entries Certificates Log		
Connection Entry	Host	Transport .
hilvaleyvpn	172.22.1.160	IPSecAUDP
		_
		- Sec.
		-
4		

Selecione sua entrada de conexão da lista e clique em Connect.

Digite suas credenciais.

👌 VPN Client   User	Authentication	for "hillvalleyvpn"	×
Cisco Systems Us autilitian Ba	sername: marty assword:	OK	Cancel

Escolha Status > Statistics... para exibir a janela Tunnel Details onde você pode inspecionar os detalhes do túnel e ver o tráfego fluindo.

unnel Details	Route Details	Firewal	
Address Info	rmation	Connection Information	i.
Client:	10.0.1.50	Entry:	hillvalley2
Server	172.22.1.160	Time:	0 day(s), 00:00.25
Bytes		Crypto	
Received:	0	Encryption:	168-bit 3-DES
Sent	1494	Authentication:	HMAC-SHA1
Packets		Transport	
Encrypted	9	Transparent Tunneling	Inactive
Decrypted	0	Local LAN:	Disabled
Discarded:	0	Compression:	None
Bypassed:	159		
			Reset

Acesse a guia Route Details para ver as rotas que o VPN Client está protegendo para o ASA.

•

Neste exemplo, o VPN Client está protegendo o acesso a 10.0.1.0/24 enquanto todo o tráfego restante não é criptografado e não é enviado pelo túnel.

ĉ	VPN Client   Statistics						
	Tunnel Details Route Details Frewall						
	Local LAN Routes		Secured Routes				
	Network	Subnet Mask	Network	Subnet Mask			
			10.0.1.0	255.255.255.0			

Exibir o registro do cliente VPN

Ao examinar o log do VPN Client, você pode determinar se o parâmetro que especifica o tunelamento dividido está ou não definido. Para visualizar o registro, vá para a guia Log no VPN Client. Em seguida, clique em **Log Settings** para ajustar o que está registrado. Neste exemplo, o IKE é definido como **3 - High, enquanto que todos os demais elementos são definidos como 1 - Low.** 

VPN Client - Version 4.0.5 (Rel)						
Connection Entries Status Certificates Log Options Help						
Disable Clear Log Settings Log Window						
Connection Entries Certificates Log						
Cisco Systems VPN Client Version 4.0.5 (Ref) Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 5.1.2600 Service Pack 2						
Not connected.						

Cisco Systems VPN Client Version 4.0.5 (Rel) Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 5.1.2600 Service Pack 2

1 14:20:09.532 07/27/06 Sev=Info/6 IKE/0x6300003B Attempting to establish a connection with 172.22.1.160.

!--- Output is supressed

18 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005D Client sending a firewall request to concentrator

19 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy).

20 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion Prevention Security Agent, Capability= (Are you There?).

21 14:20:14.208 07/27/06 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS \*(HASH, ATTR) to 172.22.1.160

22 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.160

23 14:20:14.208 07/27/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ATTR) from 172.22.1.160

24 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010

```
MODE CFG REPLY: Attribute = INTERNAL IPV4 ADDRESS: , value = 10.0.1.50
      14:20:14.208 07/27/06 Sev=Info/5
                                            IKE/0x63000010
25
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0
      14:20:14.208 07/27/06 Sev=Info/5
                                          IKE/0x6300000D
26
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000
      14:20:14.208 07/27/06 Sev=Info/5
                                          IKE/0x6300000D
27
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000
      14:20:14.208 07/27/06 Sev=Info/5
28
                                            IKE/0x6300000E
MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems,
Inc ASA5510 Version 7.2(1) built by root on Wed 31-May-06 14:45
!--- Split tunneling is permitted and the remote LAN is defined.
29
       14:20:14.238 07/27/06 Sev=Info/5
                                            IKE/0x630000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets),
value = 0x0000001
      14:20:14.238 07/27/06 Sev=Info/5
30
                                            IKE/0x6300000F
SPLIT NET #1
   subnet = 10.0.1.0
   mask = 255.255.255.0
   protocol = 0
   src port = 0
   dest port=0
!--- Output is supressed.
```

Teste o acesso à LAN local com ping

Uma maneira adicional de testar se o cliente VPN está configurado para a separação de túneis enquanto permanece encapsulado no ASA é usar o comando ping na linha de comando do Windows. A LAN local do VPN Client é 192.168.0.0/24 e outro host está presente na rede com um endereço IP 192.168.0.3.

<#root>

C:\>

ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

```
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre>
```

Troubleshooting

Limitação com número de entradas em uma ACL de túnel dividido

Há uma restrição com o número de entradas em uma ACL usada para o túnel dividido. Recomenda-se não usar mais de 50 a 60 entradas ACE para uma funcionalidade satisfatória. Você é recomendado implementar o recurso de sub-rede para cobrir um intervalo de endereços IP.

Informações Relacionadas

- <u>PIX/ASA 7.x como servidor VPN remoto, usando o exemplo de configuração do ASDM</u>
- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Suporte técnico e downloads da Cisco

#### 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.