在ASA上为VPN客户端配置分割隧道

目录 简介 <u>先决条件</u> 要求 使用的组件 <u>网络图</u> <u>相关产品</u> <u>规则</u> 背景信息 在 ASA 上配置分割隧道 使用自适应安全设备管理器 (ASDM) 5.x 配置 ASA 7.x 使用ASDM6.x配置ASA 8.x 通过 CLI 配置 ASA 7.x 及更高版本 通过 CLI 配置 PIX 6.x 验证 <u>连接 VPN 客户端</u> 查看 VPN 客户端日志 通过 Ping 测试本地 LAN 访问 故障排除 <u>分割隧道ACL中的条目数量限制</u> 相关信息

简介

本文档介绍允许VPN客户端在通过隧道连接到Cisco ASA 5500系列安全设备时访问互联网的过程。

先决条件

要求

本文档假定 ASA 上已存在有效的远程访问 VPN 配置。如果尚未配置此配置,请参阅<u>使用ASDM将</u> <u>PIX/ASA 7.x配置为远程VPN服务器的配置示例</u>。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- Cisco ASA 5500 系列安全设备软件版本 7.x 及更高版本
- Cisco Systems VPN 客户端 4.0.5 版

• 自适应安全设备管理器 (ASDM)



注意:本文档还包含与Cisco VPN客户端3.x兼容的PIX 6.x CLI配置。

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。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

网络图

VPN 客户端位于典型的 SOHO 网络中,并通过 Internet 连接到总部。



网络图

相关产品

此配置还可用于 Cisco PIX 500 系列安全设备软件版本 7.x。

规则

有关文档约定的更多信息,请参考 Cisco 技术提示约定。

背景信息

本文档提供在 VPN 客户端通过隧道连接到 Cisco 自适应安全设备 (ASA) 5500 系列安全设备时如何 允许 VPN 客户端访问 Internet 的分步说明。此配置允许 VPN 客户端在无法安全访问 Internet 时通 过 IPsec 安全地访问公司资源。



注意:全隧道配置被视为最安全的配置,因为它不允许设备同时访问互联网和公司LAN。全 隧道和分割隧道之间的折衷方案仅允许VPN Client本地LAN访问。有关详细信息,请参阅 <u>PIX/ASA 7.x:允许VPN Client访问本地LAN的配置示例</u>。

在 VPN 客户端到 ASA 的基本方案中,不管流量目标如何,将对来自 VPN 客户端的所有流量进行 加密并将其发送到 ASA。根据您的配置和支持的用户数,此设置可能会占用大量带宽。运行分割隧 道可以缓解此问题,这是因为它允许用户通过隧道只发送要发送到公司网络的流量。即时消息、电 子邮件或临时浏览等所有其他流量将通过 VPN 客户端的本地 LAN 向外发送到 Internet。

在 ASA 上配置分割隧道

使用自适应安全设备管理器 (ASDM) 5.x 配置 ASA 7.x

完成以下步骤以便将隧道组配置为允许该组中的用户使用分割隧道。

1. 依次选择 Configuration > VPN > General > Group Policy,并选择您希望在其中启用本地 LAN 访问的组策略。然后单击 Edit。



2. 转至 Client Configuration 选项卡。

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 P	arameters
Banner:	🔽 Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	🔽 inherit	¥.
Split Tunnel Network List:	🔽 Inherit	Manage
Address pools		
🗹 Inherit		
Available Pools		Assigned Poors (up to 6 entries)
	Add>>	
	< <remove< td=""><td></td></remove<>	

3. 取消选中Split Tunnel Policy所对应的Inherit框,然后选择Tunnel Network List Below...

Iame: Initialleyopn Ineral IPSec Client Contiguration 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 Clicco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Benner Default Domain: Inherit Edit Benner Split Tunnel DNS Names (space delimited): Inherit Tunnel All Networks Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List Inherit Tunnel All Network List Below Address pools Address pools Address Imherit Address Address Address pools Address Address			
neral PSec Client Configuration Client Firewall Hardware Client NAC VVebVPN Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. General Client Parameters Clisco Client Parameters Microsoft Client Parameters Banner: Image: Client Configuration Microsoft Client Parameters Banner: Image: Client Parameters Microsoft Client Parameters Banner: Image: Client Parameters Microsoft Client Parameters Default Domain: Immerit Edit Banner Spit Tunnel DNS Names (space definited): Immerit Tunnel All Networks Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Immerit Tunnel All Network List Below Address pools Address pools Address Immerit Address Address Address pools Address	Name: hillvalleyvpn		
Inherit Edit Banner: Default Domain: Inherit Split Tunnel DNS Names (space definited): Inherit Split Tunnel Policy: Inherit Split Tunnel Network List: Inherit Address pools Address pools Address pools Address	unit Down Client Configuration Client Success	Lundowe cont	
Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. General Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Banner Default Domain: Inherit Edit Banner Split Tunnel DNS Names (space delimited): Inherit Tunnel All Networks Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List: Inherit Exclude Network List Below Address pools Address Assigned Pools (up to 6 entries) Address Address Assigned Pools (up to 6 entries)	eneral IPSec Client Configuration Client Firewall	Hardware Client	NAC WebYPN
General Client Parameters Cisco Client Parameters Banner: Inherit Default Domain: Inherit Split Tunnel DNS Names (space delimited): Inherit Split Tunnel Policy: Inherit Split Tunnel Network List: Inherit Address pools Inherit Varieble Pools Address Address pools Inherit	Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
General Client Parameters Clisco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Banner Default Domain: Inherit Edit Banner Split Tunnel DNS Names (space delimited): Inherit Inherit Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List: Inherit Tunnel Network List Below Address pools Address pools Address Inherit Avaïebre Pools Address Address Address Assigned Pools (up to 6 entries)		1	
Banner: Inherit Edit Banner Default Domain: Inherit Inherit Spit Tunnel DNS Names (space delimited): Inherit Tunnel All Networks Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Tunnel Network List Below Address pools Address Pools (up to 6 entries) Address pools Address Assigned Pools (up to 6 entries)	General Client Parameters Cisco Client Parameter:	s Microsoft Client	Parameters
Banner: Inherit Default Domain: Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Address pools		-	
Default Domain: Inherit Spit Tunnel DNS Names (space definited): Inherit Spit Tunnel Policy: Inherit Tunnel All Networks Tunnel All Networks Spit Tunnel Network List: Inherit Address pools Exclude Network List Below Address pools Address pools	Banner:	I≁ Inherit	Edit Banner
Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Inherit Tunnel All Networks Tunnel Network List: Inherit Address pools Adds> Adds Adds Adds Adds Adds Ad	Defer it Domaio	Juberit	
Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Inherit Tunnel All Networks Tunnel All Network List: Inherit Address pools Inherit Address pools Address pools Address pools Address pools (see a construction of the second of	Dorous Dorrow.	It in the fit	1
Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List: Inherit Address pools Address	Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Spit Tunnel Policy: Inherit Tunnel All Networks Tunnel Network List Below Address Address Address Address Address Address Tunnel All Networks Address Address Address Address <			
Split Tunnel Network List: Image: Image	Split Tunnel Policy:	🗌 Inherit	Tunnel All Networks
Split Tunnel Network List: Address pools Address pools Address pools Available Pools Addi>>			Tunnel All Networks
Address pools Address pools Inherit Avaïable Pools Add>> Add>> KRemove	Split Tunnel Network List:	🔽 Inherit	Tunnel Network List Below
Address pools Inherit Avaïable Pools Assigned Pools (up to 6 entries) Add>>			
Available Pools Assigned Pools (up to 6 entries) Add>>	Address pools		
Avarable Pools Addex Assigned Pools (up to 6 entries)	Inherit		
Add>> < <remove< td=""><td>Avarable Pools</td><td></td><td>Assigned Pools (up to 6 entries)</td></remove<>	Avarable Pools		Assigned Pools (up to 6 entries)
<#Remove		Add>>	1
			1
		**nemove	1
	1		,

取消选中 Split Tunnel Network List 所对应的 Inherit 框,然后单击 Manage 启动 ACL Manager。

ame: hilvalleyvpn		
eral IPSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN
heck an inherit checkbox to let the corresponding a	atting take its val	is from the default aroun policy
Incorder mineral checkbox to let the corresponding a	i	a non-the default group policy.
eneral Client Parameters Cisco Client Parameters	Microsoft Client	Parameters
Banner:	🔽 Inherit	Edit Benner
	E	
Default Domain:	I¥ Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Soit Tunnel Policy	Inherit	Tunnel Network List Below
Split Tunnel Network List:	Inherit	None Manage
- Address pools		10
l Inherit		
Available Pools		Assigned Pools (up to 6 entries)
	Add⊳⊳	1
	< <remove< td=""><td>i</td></remove<>	i
		, I

在 ACL Manager 中,选择 Add > Add ACL... 以创建新的访问列表。

ALL Manager						L L	X
Standard AG.	Extended AGL						
🗣 Add 🕞 🔤	Lou 🎚 o-se	+ +	发胎圈子				
Add A	a dress		Action	Description			
• A81.03	35						
The losert of	stor.						

为 ACL 提供一个名称,然后单击 OK。

ACL Manager			×
Standard ACL Extended ACL Add • Effect Dot to + + No Address	Adon Description		
	AGL Name: Spit_Turnel_List	Hotp	
- Rule Row Disgram	5- Inside and and	taide -5	×
	OK. Cancel	Hep	

创建ACL后,依次选择Add > Add ACE。.以便添加访问控制条目(ACE)。



定义与 ASA 后的 LAN 对应的 ACE。在本示例中,该网络为 10.0.1.0/24。

a.

选择 Permit。

b.

选择 IP 地址 10.0.1.0

c.

选择网络掩码 255.255.255.0。

d.

(可选) 提供相应说明。

单击>**确定**。

📫 ACL Manager					
Stended ACL Extended A	a				
🗣 Add 🕞 📑 D.C. 📋 D	Neite 🕈 6 🐰 🗞 🐘 -				
No Add	1019 Action	Description			
Spit_Turnel_List					
	Read ALL			×	
	Action				
	waan w Point				
	HortMetwork				
	P Address: F00.1.0				
	Netwask: ps6.255.255.0			-	
	Descriptions				
	The corporate network behind the AS	A			
		[]			
		Carco	Holp		
					_
Rule Flow Diagram	a_ inte	Star outside	La		×
		- U			

单击 OK 以退出 ACL Manager。

•

e.



确保在 Split Tunnel Network List 中选择刚刚创建的 ACL。

eral PCan Clert Continuation Clart Evenuel	Marchurer Clevel	NRC MARCEN
eral indec control of the control of	Pardware Cient	[Not] New York
heck an Inherit checkbox to let the corresponding a	setting take its valu	e from the default group policy.
eneral Client Parameters Cisco Client Parameters	Microsoft Client	Parametera
Barner.	🖂 inhert	Edit Enviren
Default Domain:	Interit	
Split Tunnel DNS Names (space delimited):	🖓 inhert	
Split Tunnel Policy:	interit	Tunnel Network List Below
Split Tunnel Network List:	[] Inhert	Spit_Turnel_L Manage
-Address pools		Splt_Turnel_List
Variable Prote		Assimut Ends (usto Electrics)
		1
-	Addee	
-	collemone	J

单击 OK 以返回组策略配置。

٠

it Internal Group Policy: hillvalleyvpn			X
Name: hitvaleyvpn			
General PSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN	
Check an Inherit checkbox to let the corresponding a	setting take its val.	e from the default group policy.	
General Client Parameters Cisco Client Parameters	Microsoft Client	Parametera	
Barner:	🖂 inhert	Edt Borner	
Default Domain:	I⊽ inherit		
Split Tunnel DNS Names (space delimited):	17 Inhert		
Split Tunnel Policy:	□ interit	Tunnel Network List Below	
Split Tunnel Network List:	inhert	Spit_Tunnet_L * Manage	
Address pools			

单击 Apply,然后单击 Send(如果需要),以将命令发送到 ASA。



使用ASDM 6.x配置ASA 8.x

完成以下步骤以便将隧道组配置为允许该组中的用户使用分割隧道。

依次选择 Configuration > Remote Access VPN > Network (Client) Access > Group Policies ,并选择您希望在其中启用本地 LAN 访问的组策略。然后单击 Edit。

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 internal externally on a RADIUS/LDAP server. The group policy information is referenced by VPN bunnel groups and user accounts.

🗣 Add 🔹 📝 Edk 📋 Delete			
Name	Туре	Tunneling Protocol	A
DfltGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N/A
Defaultgroup	Interna	Inherited	N/A
hivaleyvpn	Internal	svc, IPSec	N/A

1	Edit Internal Group Policy:	: hivalleyvpn	
	General Servers B-Advanced Golt Turneling - If Browser Procy B-SSL VPN Client B-IPsec Client	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and require tunneling. The security appliance makes split tunneling decisions on the basis of a network ACL that consists of list of addresses on the private network. DNS Names: 🖓 Inherit 📃	t those that do no k list, which is an
	Clent Firewal	Network List: 🔽 Inheriti	Manage
	Herdware Clent	Intercept DHCP Configuration Message from Micosoft Clients	
		prior to XP, DHCP Intercept provides the domain name and subnet mask. Intercept: ∇ Inherit $C \cong C$ is:	
		Subnet Mark (Optional): 0.0.0.0	<u>*</u>
	ž D		

取消选中 Split Tunnel Policy 所对应的 Inherit 框,然后选择 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 _v 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

取消选中 Split Tunnel Network List 所对应的 Inherit 框,然后单击 Manage 启动 ACL Manager。

🖬 Edit Internal Group Policy	i hiralleyvpn
General Servers E-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: 🖓 Initerit Driver: 🔽 Drivert Duranel National List Balance
⊡-IPsec Client Client Access Rule - Client Rrewall	Network List:
Hardware Client	Intercept DHCP Configuration Message from Micosoft Clients
	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.
	Intercept: 🔽 Inherit C Yes C No
	Subret Hark (Optional): 0.0.0.0

在 ACL Manager 中,选择 Add > Add ACL... 以创建新的访问列表。

ACL	Manager				
Stand	dard ACL Extended	ACL			
* A	vdd 🔸 🛒 EdR 🍵	Delete 🕈	4 % B		
-	Add ACL	-	Action	Description	
+	Add ACE				
*	Insert				
Ŧ	Insert After				

为此 ACL 提供一个名称,然后单击 OK。

•

 Address	Action	Description	
🔂 Add	ACL	x x x x x x	1
ACL N	ame: Split_Tunnel_List		
	OK Caricel	Help	

创建 ACL 之后,依次选择 Add > Add ACE... 以添加访问控制条目 (ACE)。



定义与 ASA 后的 LAN 对应的 ACE。在本示例中,该网络为 10.0.1.0/24。

a.

单击 Permit 单选按钮。

b.

选择掩码为 10.0.1.0/24 的网络地址。

c.

(可选) 提供相应说明。

d.

Click OK.

🔞 AEL Manager				
Standard ACL Extended AC	u)			
🗢 Add 🔹 🛒 Edt 📋 D	eloto 🛧 4 🐰 🕪 I	B		
No Addre	ss Action	Description		
Split_Tunnel_List			<u> </u>	
	Gradd ACE			×
	Annual Characteristics			
	Action: I+ Permit C Den	4		
	Address: [10:0:1:0]24			
	Description:			
	The Corporate network behind	the ASA		
		or creat f	Halo	

单击 OK 以退出 ACL Manager。

٠

ACL Manager	
Characterization () and () and ()	
Standard ACL Extended ACL	
🗣 Add 🔹 💽 Edit 🚺 Delete 🕈 🐇	92 11
No Address Action	Description
E Split_Turnel_List	
1 10.0.1.0/24 / Permit	The Corporate network behind the ASA
<u></u>	
	Cox Cancel Halp

确保在 Split Tunnel Network List 中选择刚刚创建的 ACL。

F	Edit Internal Group Policy:	hivalleyvpn
	General Servers Advanced -IE Browser Prozy (II-SS, VPN Client -IPsec Client	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do no 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: Image: Imag
	Clent Access Rule Clent Ficewal Hardware Clent	Network List: Dinherit Spik_Tunnel_List Manage Intercept DHCP Config Spik_Tunnel_List (\$
		Intercept:

单击 OK 以返回组策略配置。

•

Split bunneling network lists require tunneling. The sec ACL that consists of list of	s distinguish networks that require traffic to go through the burry appliance makes split tunneling decisions on the basis of addresses on the private network.	nnel and those that do no a network list, which is an
DNS Names: 🖾 Inherit		
Policy: 🗂 Inherit	Tunnel Network List Below	Ŧ
Network List: 🕅 Inherit	Splk_Tunnel_List	* Manage
Intercept DHCP Confi DHCP Intercept lets Micr prior to 3P, DHCP Interc	puration Message from Micosoft Clients osoft XP clients use split tunneling with the security appliance apt provides the domain name and subnet mask.	Por Windows clients
Intercept: 🔽 Inherit	с»» сл.	
	Split tunneling receivers list require tunneling. The sec ACL that consists of list of DNS Names: IF Inherit Policy: IF Inherit Network List: IF Inherit Intercept DHCP Confil DHCP Intercept lets Nice prior to 3P, DHCP Interce Intercept: IF Inherit	Split tunneling retrieors lets distinguish networks that require transing decisions on the basis of ACL that consists of list of addresses on the private network. DNS Names: Image:

单击 Apply,然后单击 Send(如果需要),以将命令发送到 ASA。

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

Manage YPN group policies. A YPN 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.

🗣 Add	Ŧ	Z	Edit	Û	Delete
-------	---	---	------	---	--------

Name	Туре	Tunneling Protocol	
OfbGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N/A -
Defaultgroup	Internal	Inherited	N/A -
hivaleyvpn	Internal	svc,IPSec	N/A -
	(- P	coly Reset	

通过 CLI 配置 ASA 7.x 及更高版本

您可以在 ASA CLI 中完成以下步骤(而不是使用 ASDM),以便允许在 ASA 上使用分割隧道:



注意:ASA 7.x和8.x的CLI分割隧道配置相同。

进入配置模式。

•

<#root>

ciscoasa>

enable

Password: ******* ciscoasa#

configure terminal

ciscoasa(config)#

创建定义 ASA 后台网络的访问列表。

<#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

进入您希望对其进行修改的策略的组策略配置模式。

<#root>

٠

ciscoasa(config)#

group-policy hillvalleyvpn attributes

ciscoasa(config-group-policy)#

指定分割隧道策略。在本示例中,此策略为 tunnelspecified。

<#root>

•

ciscoasa(config-group-policy)#

split-tunnel-policy tunnelspecified

指定分割隧道访问列表。在本示例中,此列表为 Split_Tunnel_List。

<#root>

٠

ciscoasa(config-group-policy)#

split-tunnel-network-list value Split_Tunnel_List

<#root>

ciscoasa(config)#

tunnel-group hillvalleyvpn general-attributes

将组策略与隧道组关联

<#root>

٠

ciscoasa(config-tunnel-ipsec)#

default-group-policy hillvalleyvpn

退出上述两种配置模式。

<#root>

٠

ciscoasa(config-group-policy)#

exit

ciscoasa(config)#

exit

ciscoasa#

将配置保存到非易失性 RAM (NVRAM),并在系统提示指定源文件名时按 Enter。

<#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#

通过 CLI 配置 PIX 6.x

请完成以下步骤:

•

创建定义 PIX 后台网络的访问列表。

<#root>

PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0

• 创建一个 VPN 组 vpn3000,并向其指定分割隧道 ACL,如下所示:

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split_Tunnel_List



注意:有关PIX 6.x的远程访问VPN配置的详细信息,请参阅<u>使用Microsoft Windows 2000和2003 IAS RADIUS身份验证配</u> 置适用于Windows的Cisco Secure PIX Firewall 6.x和Cisco VPN客户端3.5。

验证

完成以下部分中的步骤以验证您的配置。

<u>连接 VPN 客户端</u>

查看 VPN 客户端日志

通过 Ping 测试本地 LAN 访问

连接 VPN 客户端

•

•

•

将 VPN 客户端连接到 VPN 集中器,以便验证配置。

从列表中选择连接条目,并单击 Connect。

👌 VPN Client - Version 4.0.5 (Rel)		
Connection Entries Status Certificates Log	Options Help	
Connect New Import	Aodity Delete	Cisco Systems
Connection Entries Certificates Log		
Connection Entry	Host	Transport _
hilvaleyvpn	172.22.1.160	IPSec/UDP
1		

输入您的凭证。



选择 Status > Statistics... 以便显示 Tunnel Details 窗口,您可以在此窗口中检查隧道特定信息并查看数据流。

unnel Detaits	Houte Details	Firewal.	
Address Infor	mation	Connection Information	ř.
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

转至 Route Details 选项卡,以便查看 VPN 客户端已安全连接到 ASA 的路由。

在本示例中,VPN 客户端可以安全地访问 10.0.1.0/24,而所有其他流量将被加密并通过隧道发送。

6	VPN Client Sta	tistics			x
	Tunnel Details	oute Details Frewa			
	Local LAN Routes	, ki	Secured Routes		
	Network	Subnet Mask	Network	Subnet Mask	
			10.0.1.0	255.255.255.0	

查看 VPN 客户端日志

当检查 VPN 客户端日志时,您可以确定是否已设置指定分割隧道的参数。要查看日志,请在 VPN 客户端中转至 Log 选项卡。然后 单击 Log Settings 以调整所记录的内容。在本示例中,IKE 设置为 3 - High,而所有其他日志元素设置为 1 - Low。

VPN Client - Version 4.0.5 (Rel)	
Connection Entries Status Certificates Log Options Help	
Disable Clear Log Settings Log Window	CISCO STATEMS
Connection Entries Certificates Log	
Cisco Systems VPN Client Version 4.0.5 [Ref/C Copyright (C) 1999-2003 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 25 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x630000D 26 MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x630000D 27 MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 28 14:20:14.208 07/27/06 Sev=Info/5 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 = 0x000000130 14:20:14.238 07/27/06 Sev=Info/5 IKE/0x6300000F SPLIT_NET #1 subnet = 10.0.1.0mask = 255.255.255.0protocol = 0src port = 0dest port=0 !--- Output is supressed.

通过 Ping 测试本地 LAN 访问

测试 VPN 客户端在通过隧道连接到 ASA 时是否配置了分割隧道的另一种方法是:在 Windows 命令行中使用 ping 命令。VPN 客户端 的本地 LAN 为 192.168.0.0/24,并且网络中存在另一台 IP 地址为 192.168.0.3 的主机。

<#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 Reply from 192.168.0.3: bytes=32 time<1ms TTL=255 Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
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>

故障排除

分割隧道ACL中的条目数量限制

ACL中用于分割隧道的条目数量存在限制。建议使用的ACE条目不要超过50-60个,以便获得令人满意的功能。建议您实施子网划分功能以涵盖一系列IP地址。

相关信息

- 使用 ASDM 将 PIX/ASA 7.x 配置为远程 VPN 服务器的配置示例
- <u>Cisco ASA 5500 系列自适应安全设备</u>
- 思科技术支持和下载

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)。