VPN 3000 集中器上针对 VPN Client 使用分割隧 道的配置示例

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 网络图 <u>规则</u> <u>背景信息</u> <u>在 VPN 集中器上配置分割隧道</u> <u>验证</u> <u>连接 VPN 客户端</u> <u>查看 VPN 客户端日志</u> <u>故障排除</u> <u>相关信息</u>

<u>简介</u>

本文档提供有关如何允许 VPN 客户端在通过隧道技术进入 VPN 3000 系列集中器时访问互联网的 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:配置分割隧道时,可能会带来安全风险。由于 VPN 客户端不安全地访问 Internet,因此可能 会受到攻击者的安全威胁。然后,该攻击者可以通过 IPSec 隧道访问公司 LAN。可以在完全隧道和 分割隧道之间进行折衷,以允许 VPN 客户端仅访问本地 LAN。有关更多信息,请参阅<u>允许 VPN 客</u> 户端在 VPN 3000 集中器上进行本地 LAN 访问的配置示例。

<u>先决条件</u>

<u>要求</u>

本文档假定 VPN 集中器上已存在有效的远程访问 VPN 配置。如果尚未配置 IPsec,请参阅 <u>VPN</u> <u>客户端与 VPN 3000 集中器之间的 IPsec 配置示例。</u>

<u>使用的组件</u>

本文档中的信息基于以下软件和硬件版本:

- Cisco VPN 3000 集中器系列软件版本 4.7.2.H
- Cisco VPN 客户端 4.0.5 版

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。

<u>网络图</u>

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



<u>规则</u>

有关文档约定的更多信息,请参考 Cisco 技术提示约定。

<u>背景信息</u>

在 VPN 客户端至 VPN 集中器的基本场景中,VPN 客户端的所有流量将加密并发送至 VPN 集中器 ,不论目标为何。根据您的配置和支持的用户数量,此设置可变为带宽密集型设置。分割隧道可通 过允许用户在隧道上只发送去往企业网络的流量来缓解此问题。所有其他流量(例如 IM、邮件或随 意浏览)将通过 VPN 客户端的本地 LAN 发送至互联网。

在 VPN 集中器上配置分割隧道

完成以下步骤来配置隧道组,以便允许为组中的用户配置分割隧道。首先创建一个网络列表。此列 表定义了 VPN 客户端要向其发送加密流量的目标网络。创建列表后,将列表添加到客户端隧道组 的分割隧道策略。

1. 选择 Configuration > Policy Management > Traffic Management > Network Lists 并点击 Add。



2. 此列表定义了 VPN 客户端要向其发送加密流量的目标网络。手动输入这些网络,或点击 Generate Local List 以根据 VPN 集中器的专用接口的路由条目创建一个列表。在本例中,列 表是自动创建。

VPN 3	3000	Main Help Support Logout
Nonce	ntrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
Configuration Interfaces Description Description Description Description Constant Description Descripti Description Description Description Description	Configuration Policy Management Traffic Management Ne Configure and add a new Network List. Click on Generate Loo entries on the Private interface.	twork Lists Add ral List to generate a network list based on routing ame of the Network List you are adding. The name
Bules SAs SAs SAs BNAT BNAT BNAT BNAMACHINA BNAMACHINA C BNAMACHIN	Network List	 ust be unique. Enter the Networks and Wildcard masks using the following format n.n.n.n'n.n.n.n (e.g. 10.10.0/00.0.255.255). Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1 mm addresses. Each Network and Wildcard mask pair must be
Cisco Systems	Add Cancel Generate Local List	entered on a single line. • The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

3. 创建或填充列表后,为列表提供一个名称并点击 Add。

VPN 3	000 ateator Series Manager	Main Help	Support Logout
Concer	itrator series Manager	Configuration Administ	Logged in: admin
Configuration Interfaces PSystem Policy Nanogement Access Hours Pland Management Access Hours Pland Management Network Lists Pland Policies Policies	Configuration Policy Management Traffic Management Traffic Management Traffic Management Traffic Management Configuration Configuratio Configuration Configuratio Configuration	 gement Network Lists Add enerate Local List to generate a network list based Name of the Network List you are adding must be unique. Enter the Networks and Wildcard r following format n.n.n./n.n.n.n (e 10.10.0.00.0.255.255). Note: Enter a wildcard mask, wi reverse of a subnet mask. A wild 1s in bit positions to ignore, 0s in bit match. For example, 10.10.1.000.01.00.10.10.00.01.00.01.00.10.1	on routing The name nasks using the g hich is the deard mask has t positions to 0.255 = all pair must be d if the natural
Cisco Systems			

4. 创建网络列表后,将其分配到隧道组。选择 Configuration > User Management > Groups,然 后选择您希望更改的组,然后再单击 Modify Group。

VPN 3	3000		Main Help	Support Logout
Conce	ntrator Series Manager			Logged in: admin
			Configuration Administr	ation Monitoring
-Configuration interfaces 	Configuration User Managemen	t Groups	Si	we Needed 🗖
Base Group 	This section lets you configure grou Click the Add Group button to ad-	ps. A group is a collection of users tree d a group, or select a group and click I	ated as a single entity. Delete Group or Modify Grou	n. To modify
	other group parameters, select a gr	oup and click the appropriate button.		•
- <u> - Administration</u> - <u> - Monitoring</u>				
	Actions	Current Groups	Modify	
		ipsecaroup (Internally Contigured)	Authentication Servers	
			Authorization Servers	
	Add Onnun		Accounting Servers	
	Add Group		Address Pools	
	Modify Group		Client Update	1
	Delete Group		Bandwidth Assignment	
			WebVPN Servers and URLs	
			WebVPN Port Forwarding	
		,		
Cisco Systems				

5. 移至已选择要修改的组的 Client Config 选项卡。

VPN 3 Concer	000 ntrator Seri	es Manager		Main Help Support Logout Logged in: admin Configuration Administration Monitoring
Configuration Configuration User Management Groups Modify ipsecgroup Distin Distin Distin Check the Inherit? box to set a field that you want to default to the base group value. Uncheck the Inherit? box and enter a new value to override base group values. Distin Check the Inherit? box to set a field that you want to default to the base group value. Uncheck the Inherit? box and enter a new value to override base group values. Users Users Disting and Security General [IPSec Client Config Client FW [HW Client [PPTP/L2TP] WebVPN] NAC Ordering and Security Check the Inherit [Provide Config Client FW [HW Client [PPTP/L2TP] WebVPN] NAC				
	Attribute	Value	Inherit?	Description
	Allow Password Storage on Client		R	Check to allow the IPSec client to store the password locally.
	IPSec over UDP		ы	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
	IPSec over UDP Port	10000	ы	Enter the UDP port to be used for IPSec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
Cisco Systems	IPSec Backup Servers	Use Client Configured List	R	 Select a method to use or disable backup servers. Enter up to 10 IPSec backup server addresses/names starting from high priority to low. Enter each IPSec backup server address/name on a single line.

- 6. 向下滚动至 Split Tunneling Policy 和 Split Tunneling Network List 部分并点击**列表中的 Only** tunnel networks。
- 7. 从下拉列表中选择此前创建的列表。在本例中,选择的列表为 Main Office。"Inherit?"复选框 在这两种情况下均自动清空。

VPN 3	VPN 3000 Main Help Support Logout								
Ka 🕂 💋 Concer	Concentrator Series Manager Loggod in: admin								
Configuration Administration Monitoring									
-E-Configuration									
Base Croup Base Croup Groups Users Users Description Base Croup Groups Users Description Base Croup Groups Group	Split Tunneling Policy	 C Tunnel everything Allow the networks in list to bypass the tunnel Only tunnel networks in the list 		Select the method and network list to be used for Split Tuaneling. Tunnel Everything: Send all traffic through the tunnel. Allow the networks in the list to bypass the tunnel: The VPN Client may choose to send traffic to addresses in this list to the chent's					
	Split Tunneling Network List	Main Office		LAN. Send all other traffic through the tunnel. NOTE. This setting only applies to the Cisco VPN Client. Tunnel networks in the list: Send traffic to addresses in this list through the tunnel. Send all other traffic to the client's LAN.					
	Default Domain Name		M	Enter the default domain name given to users of this group.					
	Split DNS Names		য	Enter the set of domains, separated by commas without spaces, to be resolved through the Split Tunnel. The Default Domain Name must be explicitly included in Split DNS Names list if it is to be resolved through the tunnel.					
Cesco Systems	Apply	Cancel							

8. 完成后,请单击 Apply。

<u>验证</u>

<u>连接 VPN 客户端</u>

1. 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	; <u>H</u> elp	
Connect New Import Modify	Delete	CISCO SYSTEMS
Connection Entries Certificates Log		
Connection Entry	Host	Transport 🔺
to_3000	172.22.1.106	IPSec/UDP
Not connected.		

2. 输入您的凭证。

🤌 YPN Client - Versi	n 4.0.5 (Rel)		_ 🗆 🗵
Connection Entries St	itus Certificates Log Options <u>H</u> elp		
Cancel Connect	🖹 🛛 💒 🔪 🍋	tion for "to_3000"	CISCO SYSTEMS
Connection Entries	Enter Username and Password. CISCO SYSTEMS Username: jps. Password: see	ecuser	
Authenticating user			¥

3. 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。

(👌 VPN Client 🕴 🤉	statistics				×
	Tunnel Details	Route Details	Fire	wall		
	Address Info	mation	Co	nnection Information	1	
	Client:	10.0.1.50		Entry:	to_3000	
	Server:	172.22.1.106		Lime:	U day(s), UU:UU.38	
	Bytes		Cry	ypto		
	Received:	420		Encryption:	168-bit 3-DES	
	Sent:	2470		Authentication:	HMAC-MD5	
	Packets		Tra	ansport		
	Encrypted:	17		Transparent Tunneling	Active on UDP port 4500	
	Decrypted:	7		Local LAN:	Disabled	
	Discarded:	0		Compression:	None	
	Bypassed:	56				
					Heset	
					Close	
					<u></u> 1036	

4. 移至 Route Details 选项卡以查看 VPN 客户端要向其发送加密流量的网络。在本例中, VPN 客户端与 10.0.1.0/24 安全地通信,而其他流量以未加密的方式发送至互联网。

👶 ¥PN Client St	atistics		×
Tunnel Details	Route Details Firewall	1	
Local LAN Route	s 🖓	Secured Routes	
Network	Subnet Mask	Network	Subnet Mask
		10.0.1.0	255.255.255.0
			Close

查看 VPN 客户端日志

当您检查 VPN 客户端日志时,您可以确定是否设置允许分割隧道的参数。移至 VPN 客户端中的 Log 选项卡以查看日志。点击 Log Settings 以调整记录的内容。在本示例中,IKE 和 IPsec 设置为

3 - High,而所有其他日志元素均设置为 1 - Low。

👶 VPN Client - Version 4.0.5 (Rel)	_ 🗆 🗵
Connection Entries Status Certificates Log Options Help	
Disable Clear Log Settings Log Window	CISCO SYSTEMS
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.	11.

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 14:21:43.106 07/21/06 Sev=Info/6IKE/0x6300003B Attempting to establish a connection with 172.22.1.106.

!--- Output is supressed. 28 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005D Client sending a firewall request to concentrator 29 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy). 30 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion Prevention Security Agent, Capability= (Are you There?). 31 14:21:55.171 07/21/06 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.106 32 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.106 33 14:21:56.114 07/21/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.22.1.106 34 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50 35 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 36 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x6300000 MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000 !--- Split tunneling is configured. 37 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value = 0x00000001 38 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x6300000F SPLIT_NET #1 subnet = 10.0.1.0 mask = 255.255.255.0 protocol = 0 src port = 0 dest port=0 39 14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 40 14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc./VPN 3000 Concentrator Version 4.7.2.H built by vmurphy on Jun 29 2006 20:21:56 41 14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = Received and using NAT-T port number , value = 0x00001194 !--- Output is supressed.



有关对此配置进行故障排除的一般信息,请参阅使用 VPN 客户端的 IPsec 到 VPN 3000 集中器的

相关信息

- <u>使用 VPN 客户端的 IPsec 到 VPN 3000 集中器的配置示例</u>
- <u>Cisco VPN 3000 系列集中器</u>
- <u>Cisco VPN 客户端</u>
- <u>技术支持和文档 Cisco Systems</u>