VPN 3000集中器上用於VPN客戶端的分割隧道配 置示例

目錄

 簡介

 必要條件

 需求

 採用元件

 網路圖表

 慣例

 背景資訊

 在VPN集中器上配置拆分隧道

 驗證

 連線VPN客戶端

 檢視VPN客戶端日誌

 疑難排解

 相關資訊

<u>簡介</u>

本文檔提供了有關如何允許VPN客戶端在通過隧道連線到VPN 3000系列集中器時訪問Internet的逐步說明。此配置允許VPN客戶端通過IPsec安全地訪問公司資源,同時提供對Internet的不安全訪問。

注意:配置分割隧道可能會帶來安全風險。因為VPN客戶端擁有對Internet的不安全訪問,所以攻擊 者可能會入侵它們。然後,攻擊者可能能夠通過IPsec隧道訪問公司LAN。完全通道和分割通道之間 的危害可以只允許使用VPN客戶端本地LAN訪問。有關詳細資訊,請參閱<u>在VPN 3000集中器上允許</u> VPN客戶端本地LAN訪問的配置示例。

<u>必要條件</u>

<u>需求</u>

本文檔假定VPN集中器上已存在有效的遠端訪問VPN配置。如果尚未配置<u>IPsec with VPN Client to</u> VPN 3000集中器配置示例,請參閱。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

• Cisco VPN 3000 Concentrator系列軟體版本4.7.2.H

• Cisco VPN使用者端版本4.0.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

網路圖表

VPN客戶端位於典型的SOHO網路上,通過Internet連線到總部。



慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

<u>背景資訊</u>

在基本VPN客戶端到VPN集中器場景中,無論目的地是什麼,來自VPN客戶端的所有流量都會被加 密並傳送到VPN集中器。根據您的配置和支援的使用者數量,此類設定可能會佔用大量頻寬。分割 通道可以透過允許使用者透過通道僅傳送目的地為公司網路的流量來緩解此問題。所有其他流量 (例如IM、電子郵件或隨意瀏覽)均通過VPN客戶端的本地LAN傳送到網際網路。

在VPN集中器上配置拆分隧道

完成這些步驟,將通道組配置為允許組內使用者使用分割通道。首先建立網路清單。此清單定義 VPN客戶端向其傳送加密流量的目標網路。建立該清單後,將該清單新增到客戶端隧道組的拆分隧 道策略中。

1. 選擇Configuration > Policy Management > Traffic Management > Network Lists,然後點選 Add。



 2. 此清單定義VPN客戶端向其傳送加密流量的目標網路。手動輸入這些網路,或按一下Generate Local List以根據VPN集中器專用介面上的路由條目建立清單。在此示例中,清單是自動建立 的。

HJO					
	VPN 3	000	N		Main Help Support Logout
T 1/2	Concer	ntrator Serie	es Manager		Logged in: admin
				Config	uration Administration Monitoring
-Configuration Interfaces -DScalan	1	Configuration 1 Configure and ad entries on the Pri List Name	Policy Management . Traffic Man dd a new Network List. Click on C ivate interface.	agement Network Lists Add Generate Local List to generate a Name of the Network ; must be unique. • Enter the Netwo	network list based on routing List you are adding. The name rics and Wildcard masks using the
Clicical DNAT DNAT DY Policies Dy Polici Dy Polici Dy Policies Dy Policies Dy Policies	<u>a Combrol</u> L	Network List	4	 following format 10.10.0.00.0.2; Note: Enter a v reverse of a su 1s in bit position match. For exam 10.10.1.mm add Each Network a entered on a sing The Wildcard m Wildcard mask i 	n.n.n.v/n.n.n.n (e.g. i5.255). vildcard mask , which is the bnet mask . A wildcard mask has s to ignore, 0s in bit positions to ple, 10.10.1.0/0.0.0.255 = all resses. nd Wildcard mask pair must be de line ask may be omitted if the natural s to be used.
		Add	Cancel Generate Local Lis	- 12	
CISCO SYSTEMS					

3. 建立或填充清單後,為清單提供一個名稱,然後按一下Add。

VPN	1 3000	Main Help Support Logout
K Z Con	centrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
-Cronfiguration 	Configuration Policy Management Traffic Ma Configure and add a new Network List. Click on entries on the Private interface. List Name Main Office	Augement Network Lists Add Generate Local List to generate a network list based on routing Name of the Network List you are adding. The name must be unique. • Enter the Networks and Wildcard masks using the following format n.n.n.n.n.n. (e.g.
Order State S	Network List	 10.10.0/0.0.255.255). 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, 10.10.1.0/0.0.255 = all 10.10.1.0.1.nm addresses. Each Network and Wildcard mask pair must be entered on a single line. The Wildcard mask may be omitted if the natural Wildcard mask is to be used.
	Add Cancel Generate Local Li	st
Cisco Systems		

4. 建立網路清單後,將其分配給隧道組。選擇Configuration > User Management > Groups,選 擇要更改的組,然後按一下Modify Group。

VPN	N 3000			Main Help Support Logo	out
Cor	centrator Series Manager			Logged in: adm	nin
			Configurati	ion Administration Monitori	ng
-Stenfiguration -Staten -Discriment -Discriment -Discriment -Base Group -Croups -Users -Users -Discriment -Discr	Configuration User Managemen This section lets you configure grou Click the Add Group button to ad	t Groups ups. A group is a collection of users trea d a group, or select a group and click I	ated as a single en Delete Group or	Save Needed 🗖 nity. Modify Group. To modify	
	other group parameters, select a gr	roup and click the appropriate button			
Monitoring	Actions	Current Groups	Mo	dify	
		ipsecgroup (Internally Contigured)	Authenticet	ion Servers	
			Authorizati	on Servers	
	Add Group		Accountin	ig Servers	
	Medifu Crown		Addres	s Pools	
	Relate Group		Client l	Jpdate	
	Delete Group		Bandwidth	Assignment	
			WebVPN Serv	vers and URLs	
			WebVPN Po	nt Forwarding	
Cisco Systems					

5. 轉到已選擇修改的組的Client Config(客戶端配置)頁籤。

VPN Conce	3000 entrator Seri	es Manager		Main Help Support Logou Logged in: admi Configuration Administration Monitoring
Configuration Understand Configuration User Management Groups Modify ipsecgroup Check the Inherit? box to set a field that you want to default to the base group value. Uncheck the Inherit? box ar enter a new value to override base group values. Users Users Herein and Security Check the Inherit? Client Config Client FW HW Client PPTP/L2TP WelsVPN NAC Client Configuration Parameters				
- Monitoring		Cisco Client I	Paramete	ers
	Attribute	Value	Inherit?	Description
	Allow Password Storage on Client		я	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).
Cesco 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. 向下滾動到Split Tunneling Policy和Split Tunneling Network List部分,然後按一下清單**中的** Only tunnel networks。
- 7. 從下拉選單中選擇之前建立的清單。本例中為總部。繼承者?兩種情況下覈取方塊均自動清空

	PN 3000 oncentrator Seri	es Manager		Main Help Support Logout Logged in: admin
				Configuration Administration Monitoring
Configuration interfaces				
Base Croup Group Group	Split Tunneling Policy	 C Turnel 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 Tunneling. 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		N	Enter the default domain name given to users of this group.
	Split DNS Names		ম	Enter the set of domains, separated by commas without spaces, to be resolved through the Split Tuanel. The Default Domain Name must be explicitly included in Split DNS Names list if it is to be resolved through the tunnel.
CISCO SYSTEMS	Apply 1	Cancel		

8. 完成後按一下Apply。





將VPN客戶端連線到VPN集中器以驗證您的配置。

1. 促肩串甲迭倖理椓除日, 然 夜 按	一下Connect。
----------------------	------------

👌 VPN Client - Version 4.0.5 (Rel)		-0×
Connection Entries Status Certificates Log	Options Help	
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. 輸入您的憑據。

👌 YPN Client - Version 4.0.5 (Rel)	
Connection Entries Status Certificates Log Options Help	
Cancel Connect VPN Client User Authentication for "to_3000"	CISCO SYSTEMS
Connection Entries Enter Username and Password. Connection E Cisco Systems Latificant Username: [ipsecuser to_3000 Latificant Password: [xxxxxxx] OK Cancel	
Authenticating user	

3. 選擇**Status > Statistics...**以顯示「Tunnel Details」視窗,您可以在此視窗中檢查隧道的詳細資 訊並檢視流量流。

(👌 VPN Client 🕴 🤉	statistics					×
	Tunnel Details	Route Details	Fire	wall			
	Address Info Client:	mation 10.0.1.50	Co	nnection Infor	matior	to_3000	
	Server:	172.22.1.106		Time:		0 day(s), 00:00.38	
	Bytes Received: Sent:	420 2470	Cry	ypto Encryption: Authentication:		168-bit 3-DES HMAC-MD5	
	Packets Encrypted: Decrypted: Discarded: Bypassed:	17 7 0 56	Ти	a nsport Transparent Tur Local LAN: Compression:	nneling:	Active on UDP port 4500 Disabled None Reset	
						<u></u> lose	

4. 轉到Route Details頁籤以檢視VPN客戶端將加密流量傳送到哪些網路。在此示例中,VPN客戶 端與10.0.1.0/24安全通訊,而所有其他流量則以未加密的方式傳送到網際網路。

۵	VPN Client Stat	istics		×
ſ	Tunnel Details Ro	ute Details Firewall	1	
L	ocal LAN Routes	43	Secured Routes	
	Network	Subnet Mask	Network	Subnet Mask
			10.0.1.0	255.255.255.0
				<u>C</u> lose

<u>檢視VPN客戶端日誌</u>

當您檢查VPN客戶端日誌時,可以確定是否設定了允許分割隧道的引數。轉到VPN Client中的 Log頁籤以檢視日誌。按一下「Log Settings」以調整記錄的內容。在本示例中,IKE和IPsec設定為

3 — 高,而所有其他日誌元素設定為1 — 低。

👶 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.



請參閱IPsec with VPN Client to VPN 3000 Concentrator配置示例 — 故障排除,瞭解有關此配置故

相關資訊

- IPsec with VPN Client to VPN 3000 Concentrator配置示例
- <u>Cisco VPN 3000系列集中器</u>
- <u>Cisco VPN使用者端</u>
- 技術支援與文件 Cisco Systems