Tunelización dividida para los clientes de VPN en el ejemplo de configuración del Concentrador VPN 3000

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Diagrama de la red Convenciones Antecedentes Configuración de la Tunelización Dividida en el Concentrador VPN Verificación Conéctese con el cliente VPN Ver el registro del cliente VPN Ver el registro del cliente VPN Troubleshoot Información Relacionada

Introducción

Este documento proporciona instrucciones paso a paso sobre cómo permitir que los clientes VPN accedan a Internet mientras son tunelizados en un Concentrador VPN 3000 Series. Esta configuración concede a los clientes VPN acceso seguro a los recursos corporativos a través de IPsec, mientras que concede acceso no seguro a Internet.

Nota: La tunelización dividida puede suponer un riesgo de seguridad cuando se configura. Como los clientes VPN tienen acceso no seguro a Internet, un atacante puede ponerles en peligro. Ese atacante podría entonces poder acceder a la LAN corporativa a través del túnel IPsec. Un riesgo entre la tunelización completa y la tunelización dividida puede ser permitir solamente el acceso LAN local de los clientes VPN. Refiérase a Ejemplo de Configuración de Permitir Acceso LAN Local para Clientes VPN en el Concentrador VPN 3000 para obtener más información.

Prerequisites

Requirements

Este documento asume que ya existe una configuración de VPN de acceso remoto en funcionamiento en el concentrador VPN. Consulte <u>Ejemplo de Configuración de IPsec con VPN</u> <u>Client a VPN 3000 Concentrator</u> si uno no está configurado todavía.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software Cisco VPN 3000 Concentrator Series versión 4.7.2.H
- Versión 4.0.5 de Cisco VPN Client

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagrama de la red

VPN Client se encuentra en una red SOHO típica y se conecta a través de Internet a la oficina principal.



Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

En un escenario básico de VPN Client a VPN Concentrator, todo el tráfico del VPN Client se cifra y se envía al VPN Concentrator sin importar el destino. En función de su configuración y del número de usuarios admitidos, dicha configuración puede requerir un gran ancho de banda. La tunelización dividida puede ayudar a aliviar este problema al permitir que los usuarios envíen sólo el tráfico destinado a la red corporativa a través del túnel. El resto del tráfico como IM, correo electrónico o navegación casual se envía a Internet a través de la LAN local del VPN Client.

Configuración de la Tunelización Dividida en el Concentrador VPN

Complete estos pasos para configurar su grupo de túnel para permitir la tunelización dividida para los usuarios del grupo. En primer lugar, cree una lista de red. Esta lista define las redes de destino a las que el cliente VPN envía tráfico cifrado. Una vez creada la lista, agregue la lista a la política de tunelización dividida del grupo de túnel del cliente.

1. Elija Configuration > Policy Management > Traffic Management > Network Lists y haga clic en

Add.				
VPN 3	000			Main Help Support Logout
Ka 🕂 💋 Concer	ntrator Series Manager			Logged in: admin
			Configurat	ion Administration Monitoring
interfaces	Configuration Policy Managem	ent Traffic Management Networ	k Lists	
- III-System				Save Needed 📊
PHUser Management Policy Management <u>Access Hours</u>	This section lets you add, modify,	copy, and delete Network Lists.		
Harins Management Network Lists Rules	Click Add to create a Network Li	st, or select a Network List and clic	k Modify, Copy, or	Delete
SA8		Network List	Actions	
- ENAT		VPN Client Local LAN (Default)		
			Add	
Network Admission Control			Modify	
			Сору	
- The Monitoring			Delete	
		l		
Cisco Systems				

 Esta lista define las redes de destino a las que el cliente VPN envía tráfico cifrado. Ingrese estas redes manualmente o haga clic en Generar lista local para crear una lista basada en las entradas de ruteo en la interfaz privada del concentrador VPN.En este ejemplo, la lista se creó

automáticamente.

	VPN 3	000				Main Help Support Logout
K 2	Conce	ntrator Serie	es Manager			Logged in: admin
					Configurat	ion Administration Monitoring
Configuration Interfaces Dystem Overlapped Anosement Costs Hours Costs Hours Network Lats Network Lats	mi.	Configuration Configure and s entries on the P List Name	Policy Management (dd a new Network List rivate interface.	Traffic Management t. Click on Generate	Network Lists Add Local List to generate a netw Name of the Network List ;	vork list based on routing you are adding. The name
Huss SAs Chara Char	<u>n Control</u> X	Network List	4	× F	 must be unique. Enter the Networks a following format n.n. 10, 10, 0, 00, 0, 255, 22 Note: Enter a wilds reverse of a subnet 1s in bit positions to i match. For example, 10, 10, 1, mm address: Each Network and V entered on a single in The Wildcard mask is to 1 	and Wildcard masks using the n.n/n.n.n (e.g. 55). covel mask, which is the transk. A wildcard mask has gnore, 0s in bit positions to $10.10.1.0/0.0.0.255 = all$ es. Wildcard mask pair must be ne. may be omitted if the natural be used.
		Add	Cancel Genera	ate Local List		
Cisco Systems						

3. Una vez creada o rellenada, proporcione un nombre para la lista y haga clic en

Agregar.			
VPI	N 3000		Main Help Support Logout
💦 🕂 💋 Сог	ncentrator Series Manager		Logged in: admin
		Configuratio	on Administration Monitoring
Configuration Interfaces DSystem DSystem Delicer Management Delicer Management Access Hours OFIcatific Management Network Lists DRate SAs DEstate DEstate	Configuration Policy Management Traffic Management Network List Configure and add a new Network List. Click on Generate Local List t entries on the Private interface. List Name Main Office Name of the must be under the content of the must be under the content of the	ists Add to generate a netwo he Network List yo hique. er the Networks ar owing format n.n.n	ork list based on routing ou are adding. The name of Wildcard masks using the .n/n.n.n. (e.g.
Oversies Oversies	Network List	te: Enter a wilder erse of a subnet 1 n bit positions to ig ich. For example, 1 10.1.mn addresses th Network and Wi ered on a single line Wildcard mask m dcard mask is to b	So x^{α} mask, which is the mask. A wildcard mask has nore, 0s in bit positions to 0.10, 1, 0/0, 0, 0, 255 = all silicard mask pair must be a y be omitted if the natural sused.
Cisco Systems	ų		

4. Una vez creada la lista de red, asígnala a un grupo de túnel. Elija **Configuration > User Management > Groups**, seleccione el grupo que desea cambiar y haga clic en **Modify Group**.

VPN	3000			Main Help Su	pport Logout
Ka A Z Conce	entrator Series Manager			Lo	gged in: admir
			Configurati	ion Administratio	in Monitoring
-SConfiguration Inforfaces -Statem -	Configuration User Managemen This section lets you configure grou Click the Add Groun button to ad	t Groups ups. A group is a collection of users trea d a group, or select a group and click I	ited as a single en	Save tity. Modify Group '	Needed 🚽
-D-Administration	other group parameters, select a gr	oup and click the appropriate button			
- Monitoring	Actions	Current Groups	Mo	dify	
		ipsecgroup (Internally Contigured)	Authenticet Authorizeti	ion Servers on Servers	
	Add Group		Accountin	g Servers	
	Modify Group		Addres	s Pools	
	Delate Group		Client L	Jpdate	
	Delete Group		Bandwidth /	Assignment	
			WebVPN Serv	vers and URLs	
			WebVPN Po	rt Forwarding	
Casco Systems		,			

5. Vaya a la ficha Configuración de cliente del grupo que ha elegido modificar.

	VPN 3	000			Main Help Support Logout
R 7 /	Concer	ntrator Seri	es Manager		Logged in: admin
					Configuration Administration Monitoring
Configuration Interfaces Description Organization Organization Organization Organization Organization Organization Organization Organization	X	Configuration Check the Inha enter a new vab	User Management Groups Modify ipsect arit? box to set a field that you want to defaul ue to override base group values. eral IPSec Client Config Client FW HW Client Configurat	proup t to the ba V Client ion Par	ase group value. Uncheck the Inherit? box and PPTP/L2TP WebVPN NAC rameters
- Administration - The Administration			Cisco Client I	Paramete	rs
		Attribute	Value	Inherit?	Description
		Allow Password Storage on Client		ঘ	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	N	Enter the UDP port to be used for IPSec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
Cisco System	s	IPSec Backup Servers	Use Client Configured List	त	 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. Desplácese hasta las secciones Dividir la Política de Tunelización y Dividir la Lista de Red de Tunelización y haga clic en **Sólo redes de túnel en la lista**.
- 7. Elija la lista creada anteriormente en la lista desplegable. En este caso, es la **Oficina Principal**. ¿La Herencia? las casillas de verificación se vacían automáticamente en ambos casos.

	VPN 300 Concentr	VPN 3000 Main Help Support Logo Concentrator Series Manager Loggød in: adm						
Configuration Interfaces					Configuration Administration Monitoring			
	X	Split Tunneling Policy	 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 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 Chent. 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		N	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 tuanel.			
CISCO SYSTEM	. [Apply	Cancel					

8. Haga clic en Aplicar cuando haya terminado.

Verificación

Conéctese con el cliente VPN

Conecte su VPN Client al VPN Concentrator para verificar su configuración.

1. Elija la entrada de conexión de la lista y haga clic en

VPN Client - Version 4.0.5 (Rel)			
onnection Entries Status Certificates Log G	ptions <u>H</u> elp		
Connect New Import Mo	dify Delete	Cisco St	STEMS
Connection Entries Certificates Log			
Connection Entry	Host	Transport	*
to_3000	172.22.1.106	IPSec/UDP	
<			-

2. Introduzca sus

credenciales.

🥝 VPN Client - Versi	on 4.0.5 (Rel)	-0×
Connection Entries St	atus Certificates Log Options Help	
8 4	a 🕼 🐚 🕍	CISCO SYSTEMS
Cancel Connect N	VPN Client User Authentication for "to_3000"	
Connection Entries	Enter Username and Password.	
Connection E	CISCO SYSTEMS Username: ipsecuser	
to_3000	authliturantillitura Bassword: ********	- P
	OK Cancel	
		_
		-1
4		<u> </u>
Authenticating user		

3. Elija Estado > Estadísticas... para mostrar la ventana Detalles del túnel donde puede inspeccionar los detalles del túnel y ver el tráfico que fluve.

2 VPN Client Statistics	
Tunnel Details Route Det	ils Firewall
Address Information Client: 10.0.1.50 Server: 172.22.1.10	Connection Information Entry: to_3000 6 Time: 0 day(s), 00:00.38
Bytes Received: 420 Sent: 2470	Crypto Encryption: 168-bit 3-DES Authentication: HMAC-MD5
Packets Encrypted: 17 Decrypted: 7 Discarded: 0 Bypassed: 56	Transport Transparent Tunneling: Active on UDP port 4500 Local LAN: Disabled Compression: None Reset
	<u>lose</u>

4. Vaya a la ficha Route Details para ver a qué redes envía el cliente VPN tráfico cifrado. En este ejemplo, VPN Client se comunica de forma segura con 10.0.1.0/24 mientras que el resto del tráfico se envía sin cifrar a Internet.

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

Ver el registro del cliente VPN

Cuando examina el registro de VPN Client, puede determinar si el parámetro que permite la tunelización dividida está configurado o no. Vaya a la ficha Log (Registro) en VPN Client para ver el registro. Haga clic en Log Settings para ajustar lo que está registrado. En este ejemplo, IKE e IPsec se establecen en 3- Alto mientras que todos los demás elementos de registro se establecen en 1 - Bajo.



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.

Troubleshoot

Refiérase a <u>Ejemplo de Configuración de IPsec con VPN Client to VPN 3000 Concentrator</u> - <u>Troubleshooting</u> para obtener información general sobre la solución de problemas de esta configuración.

Información Relacionada

- Ejemplo de Configuración de IPsec con VPN Client to VPN 3000 Concentrator
- <u>Cisco VPN 3000 Series Concentrators</u>
- <u>Cliente de Cisco VPN</u>
- Soporte Técnico y Documentación Cisco Systems