Exemple de configuration de transmission tunnel partagée pour clients VPN sur le concentrateur VPN 3000

Contenu

Introduction Conditions préalables Conditions requises Components Used Diagramme du réseau Conventions Informations générales Configurer la transmission tunnel partagée sur le concentrateur VPN Vérification Se connecter avec le client VPN Afficher le journal du client VPN Dépannage Informations connexes

Introduction

Ce document fournit des instructions pas à pas sur la façon d'autoriser les clients VPN à accéder à Internet pendant qu'ils sont connectés par tunnel à un concentrateur de la gamme VPN 3000. Cette configuration offre aux clients VPN un accès sécurisé aux ressources de l'entreprise par l'intermédiaire d'IPsec tout en bénéficiant d'un accès non sécurisé à 'Internet.

Remarque : La transmission tunnel partagée peut présenter un risque de sécurité lorsqu'elle est configurée. Puisque les clients VPN ont un accès à Internet non sécurisé, ils peuvent être compromis par un attaquant. Cet attaquant pourrait alors accéder au réseau local de l'entreprise par l'intermédiaire du tunnel IPsec. Une compromission entre une transmission tunnel totale et une transmission tunnel partagée peut être de ne permettre aux clients VPN que l'accès au LAN. Référez-vous à Exemple de configuration de l'accès LAN local pour les clients VPN sur le concentrateur VPN 3000 pour plus d'informations.

Conditions préalables

Conditions requises

Ce document suppose qu'une configuration VPN d'accès à distance fonctionnelle existe déjà sur le concentrateur VPN. Reportez-vous à <u>Exemple de configuration d'IPsec avec un client VPN vers</u>

un concentrateur VPN 3000 si un n'est pas déjà configuré.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel de la gamme Cisco VPN 3000 Concentrator version 4.7.2.H
- Client VPN Cisco Version 4.0.5

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.

Diagramme du réseau

Le client VPN est situé sur un réseau SOHO standard et se connecte à travers l'Internet au bureau central.



Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

Informations générales

Dans un scénario de client VPN de base vers concentrateur VPN, tout le trafic du client VPN est chiffré et envoyé au concentrateur VPN, quelle que soit la destination. En fonction de votre configuration et du nombre d'utilisateurs pris en charge, une telle configuration peut devenir gourmande en bande passante. La transmission tunnel partagée peut résoudre ce problème en permettant aux utilisateurs d'envoyer uniquement le trafic destiné au réseau d'entreprise via le tunnel. Tout autre trafic, tel que la messagerie instantanée, la messagerie électronique ou la navigation occasionnelle, est envoyé sur Internet via le réseau local du client VPN.

Configurer la transmission tunnel partagée sur le concentrateur

<u>VPN</u>

Complétez ces étapes afin de configurer votre groupe de tunnels pour autoriser la transmission tunnel partagée pour les utilisateurs du groupe. Créez d'abord une liste de réseaux. Cette liste définit les réseaux de destination vers lesquels le client VPN envoie du trafic chiffré. Une fois la liste créée, ajoutez-la à la stratégie de fractionnement en canaux du groupe de tunnels client.

1. Choisissez Configuration > Policy Management > Traffic Management > Network Lists et cliquez sur



2. Cette liste définit les réseaux de destination vers lesquels le client VPN envoie du trafic chiffré. Entrez ces réseaux manuellement ou cliquez sur Generate Local List afin de créer une liste basée sur les entrées de routage sur l'interface privée du concentrateur VPN.Dans cet exemple, la liste a été créée automatiquement.

	VPN 3000			Main Help Support Logout
R 7 1	Concentrator Ser	ies Manager		Logged in: admin
		, i i i i i i i i i i i i i i i i i i i	Configurati	on Administration Monitoring
Configuration Interfaces Distant Output Cossent Cossent Cossent Cossent Cossent Cossent Network Lists Eules	Configuration Configure and entries on the I List Name	Policy Management Traffic Managem add a new Network List. Click on Gener Private interface.	ent Network Lists Add rate Local List to generate a netw Name of the Network List y must be unique.	ork list based on routing ou are adding. The name
	Control Network Lis	¢	 Enter the Networks a following format n.n. 10. 10. 0.000. 0.255.25 Note: Enter a wilder reverse of a subnet 1s in bit positions to ig match. For example, 10. 10. 1.mm addresse Each Network and W entered on a single im The Wildcard mask n 	nd Wildcard masks using the n.n/n.n.n.n (e.g. (5). avd mask, which is the mask. A wildcard mask has gnore, 0s in bit positions to 10.10.1.0/0.0.0.255 = all s. Fildcard mask pair must be e. has be omitted if the natural
Cisco Systems	Add	Cancel Generate Local List	windpard mask is to b	e used.

3. Une fois créé ou rempli, indiquez un nom pour la liste et cliquez sur

Ajouter.			
VPN 3	3000		Main Help Support Logout
K Z Conce	entrator Series Manager		Logged in: admin
Configuration Interfaces Polystem Polystem Polystem Access Hours	Configuration Policy Management Traffic Configure and add a new Network List. Click entries on the Private interface.	Configura Management Network Lists Add : on Generate Local List to generate a net	tion Administration Monitoring work list based on routing
Access Hours Hicks Hervork Lists Hervork Lists Hervork Lists Hervork Lists Hervork Lists Hervork Achieston Control Hervork Achieston Control Hervork Achieston Control Hervork Achieston Hervork Achieston	List Name Main Office	Name of the Network List must be unique. • Enter the Networks following format n.n 10, 10, 0,000, 0,255,2 • Note: Enter a wild	you are adding. The name and Wildcard masks using the .m.n/n.n.n.n (e.g. 55). <i>card</i> mask, which is the
	Network List	 Feverse of a subne ls in bit positions to match. For example, 10.10.1.mm address Each Network and V entered on a single in The Wildcard mask is to 	t mask. A widdard mask has ignore, 0s in bit positions to 10.10.1.0/0.0.0.255 = all ies. Wilddard mask pair must be ne. may be omitted if the natural be used.
Cisco Systems	Add N Cancel Generate Loc	al List	

 Une fois que vous avez créé la liste réseau, affectez-la à un groupe de tunnels. Choisissez Configuration > User Management > Groups, sélectionnez le groupe que vous souhaitez modifier, puis cliquez sur Modify Group.

VPN	3000			Main Help Sup	port Logout
Ka 🕂 💋 Conc	entrator Series Manager			Log	ged in: admir
			Configurati	on Administratio	n Monitoring
-Stantiguration Interfaces -D-System -O-User Management 	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	ted as a single en Delete Group or	Save F Ety. Modify Group. T	leeded 🗖
■Tunneling and Security	other group parameters, select a gr	oup and click the appropriate button.			
- El Administration - El Monitoring	Actions	Current Groups	Mo	dify	
		ipsecgroup (Internally Contigured)	Authenticati	on Servers	
			Authorizati	on Servers	
	Add Crown		Accountin	g Servers	
	Addicatoup		Address	s Pools	
	Modify Group		Client L	Jpdate	
	Delete Group		Bandwidth /	Assignment	
			WebVPN Serv	vers and URLs	
			WebVPN Po	rt Forwarding	
		,			
Cisco Systems					

5. Accédez à l'onglet Configuration du client du groupe que vous avez choisi de modifier.

	VPN 3	000			Main Help Support Logout
K 2	Concer	ntrator Seri	es Manager		Logged in: admin
					Configuration Administration Monitoring
Configuration Interfaces Description Description	×	Configuration Check the Inha enter a new vab	User Management Groups Modify ipsect arit? box to set a field that you want to defau ue to override base group values. eral IPSec Client Config Client FW H Client Configurat	group It to the bi W Client tion Par	ase group value. Uncheck the Inherit? box and PPTPAL2TP WebVPN NAC rameters
Monitoring			Cisco Client I	Paramete	rs
		Attribute	Value	Inherit?	Description
		Allow Password Storage on Client		ম	Check to allow the IPSec client to store the password locally.
		IPSec over UDP		E	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 System	s	IPSec Backup Servers	Use Client Configured List	ব	 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. Faites défiler jusqu'aux sections Politique de fractionnement en canaux et Liste de réseaux de fractionnement en canaux, puis cliquez sur **Réseaux de tunnels uniquement dans la liste**.
- 7. Sélectionnez la liste créée précédemment dans la liste déroulante. Dans ce cas, il s'agit du **bureau principal**. L'héritage ? sont automatiquement vidées dans les deux cas.

	VPN 3000 Main Help Support Logout Concentrator Series Manager Logged in: admir				
-OConfiguration					Configuration Administration Monitoring
Distin Distin Distin District Distrit Distrit District District District District	l x	Split Tunneling Policy	 C Tunnel everything Allow the networks in list to bypass the tunnel Conly 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
-279060000000		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 System		Apply	Cancel		 _

8. Cliquez sur Apply lorsque vous avez terminé.

Vérification

Se connecter avec le client VPN

Connectez votre client VPN au concentrateur VPN afin de vérifier votre configuration.

1. Choisissez votre entrée de connexion dans la liste et cliquez sur

VPN Client - Version 4.0.5 (Rel)			- 0 >
onnection Entries Status Certificates Log Opl	tions <u>H</u> elp		
Connect New Import Modifi		Cisco Si	YSTEM
Connection Entries Certificates Log			
Connection Entry	Host	Transport	
to_3000	172.22.1.106	IPSec/UDP	
to_3000	172.22.1.106	IPSec/UDP	
to_3000	172.22.1.106	IPSec/UDP	

2. Entrez dans vos informations d'identification.

👌 VPN Client - Versi	ion 4.0.5 (Rel)	_ 🗆 🗵
Connection Entries St	atus C <u>e</u> rtificates Log <u>O</u> ptions <u>H</u> elp	
8 4	🛋 🚂 🐜 🔀	CISCO SYSTEMS
Cancel Connect N	VPN Client User Authentication for "to_3000"	
Connection Entries	Enter Username and Password.	
Connection E	CISCO STSTEMS Username: ipsecuser	
to_3000	antilling Bassword:	- P
	OK Cancel	
1.00		
•		
Authenticating user		

 Choisissez Status > Statistics... afin d'afficher la fenêtre Tunnel Details (Détails du tunnel) dans laquelle vous pouvez inspecter les détails du tunnel et voir le flux du trafic.

👌 VPN Client Sl	tatistics			×
Tunnel Details	Route Details	Firewall		_
ہا Address Inforr	nation	Connection Information		
Client: 1 Server: 1	10.0.1.50 172.22.1.106	Entry: Time:	to_3000 0 day(s), 00:00.38	
Bytes		Crypto		
Received: 4 Sent: 2	420 2470	Encryption: Authentication:	168-bit 3-DES HMAC-MD5	
Packets		Transport		
Encrypted: 1	17	Transparent Tunneling:	Active on UDP port 4500	
Decrypted: 7 Discarded: 0	/]	Local LAN: Compression:	Disabled None	
Bypassed: 5	56			
			Reset	
			<u>C</u> lose	

4. Accédez à l'onglet Route Details afin de voir à quels réseaux le client VPN envoie du trafic chiffré. Dans cet exemple, le client VPN communique en toute sécurité avec 10.0.1.0/24 alors que tout autre trafic est envoyé non chiffré à Internet.

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

Afficher le journal du client VPN

Lorsque vous examinez le journal du client VPN, vous pouvez déterminer si le paramètre qui autorise la transmission tunnel partagée est défini. Accédez à l'onglet Log du client VPN afin d'afficher le journal. Cliquez sur **Paramètres du journal** afin d'ajuster ce qui est consigné. Dans cet exemple, IKE et IPsec sont définis sur **3- Élevé** tandis que tous les autres éléments de journal sont définis sur **1 - Faible**.



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.

Dépannage

Référez-vous à <u>Exemple de configuration d'IPsec avec client VPN vers concentrateur VPN 3000 -</u> <u>Dépannage</u> pour des informations générales sur le dépannage de cette configuration.

Informations connexes

- Exemple de configuration d'IPsec avec client VPN vers concentrateur VPN 3000
- <u>Concentrateurs VPN de la gamme Cisco 3000</u>
- <u>Client VPN Cisco</u>
- Support et documentation techniques Cisco Systems