Split Tunneling für VPN-Clients im VPN 3000 Concentrator - Konfigurationsbeispiel

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Netzwerkdiagramm Konventionen Hintergrundinformationen Konfigurieren von Split Tunneling auf dem VPN Concentrator Überprüfen Herstellen einer Verbindung mit dem VPN-Client VPN-Clientprotokoll anzeigen Fehlerbehebung Zugehörige Informationen

Einführung

Dieses Dokument enthält schrittweise Anweisungen, wie VPN-Clients Zugriff auf das Internet gewähren, während sie in einen VPN-Konzentrator der Serie 300 getunnelt werden. Diese Konfiguration ermöglicht VPN-Clients den sicheren Zugriff auf Unternehmensressourcen über IPsec und bietet gleichzeitig einen ungesicherten Zugriff auf das Internet.

Hinweis: Split-Tunneling kann bei der Konfiguration ein Sicherheitsrisiko darstellen. Da VPN-Clients über ungesicherten Zugriff auf das Internet verfügen, können sie von einem Angreifer kompromittiert werden. Dieser Angreifer kann dann über den IPsec-Tunnel auf das Firmen-LAN zugreifen. Ein Kompromiss zwischen Full-Tunneling und Split-Tunneling kann darin bestehen, nur den lokalen LAN-Zugriff von VPN-Clients zuzulassen. Weitere Informationen finden Sie im Konfigurationsbeispiel für den VPN-Concentrator für VPN-Clients den lokalen LAN-Zugriff zulassen.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass auf dem VPN Concentrator bereits eine funktionierende VPN-Konfiguration für den Remote-Zugriff vorhanden ist. Weitere Informationen finden Sie im Konfigurationsbeispiel IPsec mit VPN Client to VPN 3000 Concentrator (IPsec mit VPN-Client für VPN 3000-Konzentrator), falls dieses noch nicht konfiguriert ist.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco VPN Concentrator der Serie 300 Softwareversion 4.7.2.H
- Cisco VPN Client Version 4.0.5

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

Der VPN-Client befindet sich in einem typischen SOHO-Netzwerk und ist über das Internet mit der Hauptniederlassung verbunden.



Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

In einem grundlegenden VPN-Client-zu-VPN-Concentrator-Szenario wird der gesamte Datenverkehr vom VPN-Client verschlüsselt und an den VPN-Concentrator gesendet, unabhängig vom Ziel. Basierend auf Ihrer Konfiguration und der Anzahl der unterstützten Benutzer kann eine solche Konfiguration eine hohe Bandbreite beanspruchen. Split-Tunneling kann zur Behebung dieses Problems beitragen, indem Benutzern ermöglicht wird, nur den für das Unternehmensnetzwerk bestimmten Datenverkehr über den Tunnel zu senden. Sämtlicher anderer Datenverkehr wie IM, E-Mail oder Surfen im Internet wird über das lokale LAN des VPN-Clients übertragen.

Konfigurieren von Split Tunneling auf dem VPN Concentrator

Führen Sie diese Schritte aus, um Ihre Tunnelgruppe so zu konfigurieren, dass Split-Tunneling für Benutzer in der Gruppe möglich ist. Erstellen Sie zunächst eine Netzwerkliste. Diese Liste definiert die Zielnetzwerke, an die der VPN-Client verschlüsselten Datenverkehr sendet. Nachdem die Liste erstellt wurde, fügen Sie sie der Split-Tunneling-Richtlinie der Client-Tunnelgruppe hinzu.

 Wählen Sie Configuration > Policy Management > Traffic Management > Network Lists (Konfiguration > Richtlinienverwaltung > Datenverkehrsmanagement > Netzwerklisten) aus, und klicken Sie auf Add



2. Diese Liste definiert die Zielnetzwerke, an die der VPN-Client verschlüsselten Datenverkehr sendet. Geben Sie diese Netzwerke entweder manuell ein, oder klicken Sie auf Lokale Liste generieren, um eine Liste auf der Grundlage von Routing-Einträgen auf der privaten Schnittstelle des VPN Concentrator zu erstellen. In diesem Beispiel wurde die Liste automatisch erstellt.

	PN 3000		Main Help Support Logout
N 7 2 C	oncentrator Series	s Manager	Logged in: admin
			Configuration Administration Monitoring
Configuration Interfaces System Constant Answement Constant Answement Constant Answement Constant Management	Configuration P Configure and ad entries on the Priv	Policy Management Traffic Management Network Id a new Network List. Click on Generate Local Li rate interface.	t Lists Add
	List Name	Maria i must be	or the Network List you are adding. The name : unique. Enter the Networks and Wildcard masks using the
BNAI BY Policies -Group Matchine -Group Matchine -Difference Administration -Difference Administration	Network List	Cancel Generate Local List	olloving tormat n.n.n.n.n.n.n. (e.g. 10.10.0.0/0.0.255.255). Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has is in bit positions to ignore, 0s in bit positions to natch. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nm addresses. Each Network and Wildcard mask pair must be intered on a single line. The Wildcard mask may be omitted if the natural Wildcard mask is to be used.
Cisco Systems		мg	

3. Geben Sie nach dem Erstellen oder Ausfüllen einen Namen für die Liste an, und klicken Sie auf

Hinzufügen.		
VPN 3	000	Main Help Support Logout
Nonce 🕂 🖉 Conce	ntrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
Configuration Interfaces Policy Management Policy Management Access Hours Retwork Lists Retwork Lists Retwork Lists Retwork Control Policy Management Retwork Activities Retwork Activ	Configuration Policy Management Traffic M Configure and add a new Network List. Click of entries on the Private interface. List Name Main Office List Name Main Office Io.o.1.0/0.0.0.255 Network List Io.O.1.0/0.0.0.255 Add Cancel Generate Local	 Anagement Network Lists Add In 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. 10.10.0/00.0255.255). 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, 10.10.1.0/00.0.255 = all 10.10.1.min addresses. Each Network and Wildcard mask pair must be entered on a single line. The Wildcard mask is to be used.
Cisco Systems		

4. Nachdem Sie die Netzwerkliste erstellt haben, weisen Sie sie einer Tunnelgruppe zu. Wählen Sie Konfiguration > Benutzerverwaltung > Gruppen aus, wählen Sie die Gruppe aus, die geändert werden soll, und klicken Sie auf Gruppe ändern.

VPN	3000			Main Help Su	pport Logout
Ka 🕂 💋 Conce	entrator Series Manager			Log	jged in: admin
			Configuratio	on Administratio	n Monitoring
	Configuration User Managemen	t Groups	ated as a single ent	Save	Needed 🚽
-Grouxe Users 	Click the Add Group button to ad other group parameters, select a gr	d a group, or select a group and click l oup and click the appropriate button.	Delete Group or)	my. Modify Group. T	lo modify
- Monitoring	Actions	Current Groups	Mod	dify	
		ipsecgroup (Internally Contigured)	Authenticati	on Servers	
			Authorizatio	on Servers	
	Add Group		Accounting	g Servers	
			Address	s Pools	
	Modify Group		Client U	lpdate	
	Delete Group		Bandwidth A	Assignment	
			WebVPN Serv	ers and URLs	
			WebVPN Por	rt Forwarding	
		,			
Cisco Systems					

5. Öffnen Sie die Registerkarte Client Config (Client-Konfiguration) der Gruppe, die Sie ändern möchten.

	VPN 3	000			Main Help Support Logout
R 7 /	Concer	ntrator Seri	es Manager		Logged in: admin
					Configuration Administration Monitoring
Configuration Interfaces Description Organized Statement Description Description Description Description	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. Blättern Sie nach unten zu den Abschnitten "Split Tunneling Policy" und "Split Tunneling Network List", und klicken Sie **in der Liste** auf **Only Tunnel Networks**.
- 7. Wählen Sie die zuvor erstellte Liste aus dem Dropdown-Menü aus. In diesem Fall ist es die **Hauptniederlassung**. Die Erben? in beiden Fällen werden die Kontrollkästchen automatisch geleert.

	VPN 3000 Concentra) itor Serie	es Manager		Main Help Support Logout Logged in: admin
- Configuration					Configuration Administration Monitoring
Distin Disclarity Discl	<u>Ix</u>	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
-279804000000		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		ঘ	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 tunnel.
Cisco System	i. I	Apply 12	Cancel		 _

8. Klicken Sie abschließend auf Übernehmen.

<u>Überprüfen</u>

Herstellen einer Verbindung mit dem VPN-Client

Verbinden Sie den VPN-Client mit dem VPN-Konzentrator, um Ihre Konfiguration zu überprüfen.

1. Wählen Sie den Eintrag für die Verbindung aus der Liste aus, und klicken Sie auf **Verbinden**.

👌 VPN Client - Version 4.0.5 (Rel)		_ [] ×
Connection Entries Status Certificates Log Opt	ions <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
4		
Not connected		

2. Geben Sie Ihre Anmeldeinformationen

👌 VPN Client - Version 4.0.5 (Rel)	_ 🗆 🗵
Connection Entries Status Certificates Log Options Help	
💊 🖛 🖉 🌭 🔽	CISCO SYSTEMS
Cancel Connect	×1
Connection Entries Exter Upername and Paceword	
Enter Osemanie and Fassivoid.	
Connection E CISCO SYSTEMS Username: ipsecuser	·
to_3000	P
OK Carcel	
al and a second s	
Authenticating user	

3. Wählen Sie Status > Statistics.. (Status > Statistik) aus. um das Fenster Tunneldetails anzuzeigen, in dem Sie die Einzelheiten des Tunnels überprüfen und den Verkehrsfluss sehen können

		1-licyvali	
Address Info	rmation	Connection Informa	tion
Client:	10.0.1.50	Entry:	to_3000
Server:	172.22.1.106	Time:	0 day(s), 00:00.38
Bytes		Crypto	
Received:	420	Encryption:	168-bit 3-DES
Sent:	2470	Authentication:	HMAC-MD5
Packets		Transport	
Encrypted:	17	Transparent Tunne	ling: Active on UDP port 4500
Decrypted:	7	Local LAN:	Disabled
Discarded:	0	Compression:	None
Bypassed:	56		
			Reset

4. Wechseln Sie zur Registerkarte Routendetails, um zu sehen, an welche Netzwerke der VPN-Client verschlüsselten Datenverkehr sendet. In diesem Beispiel kommuniziert der VPN-Client sicher mit 10.0.1.0/24, während der gesamte andere Datenverkehr unverschlüsselt in das Internet gesendet wird.

VPN Client	Statistics	all	
Local LAN Ro	utes	Secured Rout	es
Network	Subnet Mask	Network	Subnet Mask
		10.0.1.0	255.255.255.0
			Close

VPN-Clientprotokoll anzeigen

Wenn Sie das VPN-Clientprotokoll überprüfen, können Sie bestimmen, ob der Parameter für Split-Tunneling festgelegt ist. Öffnen Sie im VPN-Client die Registerkarte Log (Protokoll), um das Protokoll anzuzeigen. Klicken Sie auf **Protokolleinstellungen**, um die protokollierten Einstellungen anzupassen. In diesem Beispiel sind IKE und IPsec auf **3-High** festgelegt, während alle anderen Protokollelemente auf **1-Low** festgelegt sind.



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.

Fehlerbehebung

Weitere allgemeine Informationen zur Fehlerbehebung finden Sie unter Konfigurationsbeispiel für IPsec mit VPN-Client für VPN 3000 Concentrator - Fehlerbehebung.

Zugehörige Informationen

- Konfigurationsbeispiel: IPsec mit VPN-Client für VPN 3000-Concentrator
- <u>Cisco VPN Concentrators der Serie 3000</u>
- <u>Cisco VPN-Client</u>
- Technischer Support und Dokumentation Cisco Systems