Esempio di configurazione del tunneling ripartito per i client VPN su VPN 3000 Concentrator

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Esempio di rete Convenzioni Premesse Configurazione del tunneling ripartito sul concentratore VPN Verifica Connessione con il client VPN Visualizza registro client VPN Risoluzione dei problemi Informazioni correlate

Introduzione

Questo documento offre istruzioni dettagliate su come consentire ai client VPN di accedere a Internet mentre sono tunneling in un concentratore VPN serie 3000. Questa configurazione consente ai client VPN di accedere in modo sicuro alle risorse aziendali tramite IPsec e di accedere a Internet in modo non protetto.

Nota: la configurazione del tunneling ripartito può rappresentare un potenziale rischio per la sicurezza. Poiché i client VPN hanno accesso non protetto a Internet, possono essere compromessi da un utente non autorizzato. L'utente non autorizzato potrebbe quindi accedere alla LAN aziendale tramite il tunnel IPsec. Un compromesso tra il tunneling completo e il tunneling suddiviso può essere quello di consentire solo l'accesso LAN locale ai client VPN. per ulteriori informazioni, fare riferimento a <u>Consenti accesso LAN locale per i client VPN sull'esempio di configurazione di VPN 3000 Concentrator</u>.

Prerequisiti

Requisiti

In questo documento si presume che nel concentratore VPN esista già una configurazione VPN ad accesso remoto funzionante. Fare riferimento all'<u>esempio di configurazione di IPsec con client</u> <u>VPN su VPN 3000 Concentrator</u> se non ne è già stato configurato uno.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco VPN serie 3000 Concentrator versione 4.7.2.H
- Cisco VPN Client versione 4.0.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Il client VPN si trova su una tipica rete SOHO e si connette tramite Internet all'ufficio principale.



Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.</u>

Premesse

In uno scenario di base da client VPN a concentratore VPN, tutto il traffico proveniente dal client VPN viene crittografato e inviato al concentratore VPN, a prescindere dalla destinazione. In base alla configurazione e al numero di utenti supportati, tale configurazione può richiedere un utilizzo intensivo della larghezza di banda. Il tunneling ripartito può risolvere questo problema consentendo agli utenti di inviare solo il traffico destinato alla rete aziendale attraverso il tunnel. Tutto il resto del traffico, ad esempio messaggistica istantanea, e-mail o navigazione casuale, viene inviato a Internet tramite la LAN locale del client VPN.

Configurazione del tunneling ripartito sul concentratore VPN

Completare questa procedura per configurare il gruppo di tunnel in modo da consentire il tunneling

suddiviso per gli utenti del gruppo. Creare innanzitutto un elenco delle reti. Questo elenco definisce le reti di destinazione a cui il client VPN invia il traffico crittografato. Una volta creato l'elenco, aggiungerlo ai criteri di tunneling suddiviso del gruppo di tunnel client.

1. Scegliere Configurazione > Gestione delle policy > Gestione del traffico > Elenchi di rete e fare clic su

Aggiungi.			
VPN 3	000	Main Help Support Lo	gout
Conce	ntrator Series Manager	Logged in: a	dmin
	, i i i i i i i i i i i i i i i i i i i	Configuration Administration Monito	iring
	Configuration Policy Management Traffic Management This section lets you add, modify, copy, and delete Network Click Add to create a Network List, or select a Network Lis Network Lis VPN Client Local LAN (nt Network Lists sk Lists: List and click Modify, Copy, or Delete. st Actions (Defoul) Add Modify Delete	

2. Questo elenco definisce le reti di destinazione a cui il client VPN invia il traffico crittografato. Immettere manualmente queste reti o fare clic su Genera elenco locale per creare un elenco basato sulle voci di routing sull'interfaccia privata di VPN Concentrator.Nell'esempio riportato sotto, l'elenco è stato creato automaticamente.

	VPN 3	000			Main Help Support Logout
R 7 2	Conce	ntrator Serie	es Manager		Logged in: admin
				Configurat	ion Administration Monitoring
Configuration Interfaces Description Descript	ni. n <u>Combrol</u> X	Configuration Policy Management Traffic Management Network Configure and add a new Network List. Click on Generate Local I entries on the Private interface. List Name Name must 1 • Network List		 Network Lists Add Local List to generate a network List y must be unique. Enter the Network List y following format n.n. 10, 10, 0, 00, 0, 255, 25 Note: Enter a wilde reverse of a subnet 1s in bit positions to i match. For example, 10, 10, 1, mm addresses 	rork list based on routing rou are adding. The name and Wildcard masks using the n.n/n.n.n (e.g. 55). www mask, which is the mask. A wildcard mask has gnore, 0s in bit positions to 10.10.1.000.0.0.255 = all s.
Cisco Systems		Add	Cancel Generate Local List	 Each Network and V entered on a single in The Wildcard mask n Wildcard mask is to b 	Aldcard mask pair must be e. nay be omitted if the natural se used.

3. Una volta creato o compilato, fornire un nome per l'elenco e fare clic su

በጠ	~	inai
nu	uit	II IUI.
-3	3	

VPN	3000	Main Help Support Logout
New Karl Conc	entrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
Configuration Interfaces Configuration Interfaces Configuration Interfaces Configuration Interfacement Configuration Interfacem	Configuration Policy Management Traffic Management 1 Configure and add a new Network List. Click on Generate L entries on the Private interface. List Name Main Office 10.0.1.0/0.0.0.255	Network Lists Add ocal 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.n (e.g. 10.10.0.0/0.0.255.255).
Count Matching	Network List	 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.tim 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 Generate Local List	
Cisco Systems		

 Dopo aver creato l'elenco delle reti, assegnarlo a un gruppo di tunnel. Scegliere Configurazione > Gestione utente > Gruppi, selezionare il gruppo che si desidera modificare e fare clic su Modifica gruppo.

VPN	3000			Main Help Sup	oport Logout
Nonc Transformed T	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. Andare alla scheda Configurazione client del gruppo che si è scelto di modificare.

1	VPN 3	000			Main Help Support Logout
K /	Concer	ntrator Seri	es Manager		Logged in: admin
					Configuration Administration Monitoring
Configuration Interfaces Discrimination Organization Organization Organization Organization Organization Organization Organization Organization	м	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 Hy Client Configurat	group It to the bi W Client tion Par	ase group value. Uncheck the Inherit? box and PPTP/L2TP WebVPN NAC rameters
HHAdministration			Cisco Client I	Paramete	ers
_		Attribute	Value	Inherit?	Description
		Allow Password Storage on Client		R	Check to allow the IPSec client to store the password locally.
		IPSec over UDP		R	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 I.	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. Scorrere l'elenco fino alle sezioni Criteri di tunneling suddivisi e Elenco reti tunneling suddivise e fare clic su **Solo reti tunnel nell'elenco**.
- 7. Selezionare l'elenco creato in precedenza dall'elenco a discesa. In questo caso si tratta dell'**ufficio principale**. L'eredità? le caselle di controllo vengono svuotate automaticamente in entrambi i

casi.

VPN 3	000 ntrator Seri	es Manager		Main Help Support Logout
Conte		es munger		Configuration Administration Monitoring
Configuration Interfaces Disclars Discla	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 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
	Split Tunneling Network List	Main Office		traffic to addresses in this list to the chent's 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		N	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.
CISCO SYSTEMS	Apply	Cancel		·

8. Al termine, fare clic su **Apply** (Applica).

Verifica

Connessione con il client VPN

Connettere il client VPN a VPN Concentrator per verificare la configurazione.

1. Scegliere la voce di connessione dall'elenco e fare clic su

VPN Client - Vers	sion 4.0.5 (Rel)			-10
onnection Entries	Status Certificates	Log Options Help		
Connect Ne	w Import	Modify Delete	Cisco S	YSTEM
Connection Entries	Certificates Log	9		
Connection 8	Entry 🗸	Host	Transport	
to 3000		172 22 1 106	 IPSec/UDP	

2. Immettere le

credenziali.

👌 VPN Client - Versi	on 4.0.5 (Rel)	_ 🗆 🗵
Connection Entries St	atus Certificates Log Options Help	
8 🛉	a 🚝 🐚 🖌	CISCO SYSTEMS
Cancel Connect N	VPN Client User Authentication for "to_3000"	
Connection Entries	Enter Username and Password.	
Connection E to_3000	CISCO SYSTEMS Username: ipsecuser	
7	additionant lines. Password:	
	OK Can	
-		لعي ا
	(man)	
Authenticating user		11.

 Scegliere Stato > Statistiche... per visualizzare la finestra Dettagli tunnel, in cui è possibile esaminare i dettagli del tunnel e verificare il flusso del traffico.

VPN Client Statistics	
Tunnel Details Route Detail	Firewall
Address Information Client: 10.0.1.50 Server: 172.22.1.106	Connection InformationEntry:to_3000Time: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	Transparent Tunneling: Active on UDP port 4500 Local LAN: Disabled Compression: None Reset
	<u>C</u> lose

4. Andare alla scheda Dettagli route per vedere a quali reti il client VPN invia il traffico crittografato. Nell'esempio, il client VPN comunica in modo sicuro con 10.0.1.0/24, mentre tutto il resto del traffico viene inviato a Internet in modalità non crittografata.

8	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
				<u>C</u> lose

Visualizza registro client VPN

Quando si esamina il registro del client VPN, è possibile determinare se è impostato o meno il parametro che consente il tunneling suddiviso. Andare alla scheda Log nel client VPN per visualizzare il log. Fare clic su **Log Settings** (Impostazioni registro) per regolare gli elementi registrati. Nell'esempio, IKE e IPsec sono impostati su **3- High** mentre tutti gli altri elementi del log sono impostati su **1 - Low**.



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.

Risoluzione dei problemi

Per informazioni generali sulla risoluzione dei problemi relativi a questa configurazione, fare riferimento a <u>Esempio di configurazione di IPsec con VPN Client su VPN 3000 Concentrator</u>.

Informazioni correlate

- Esempio di configurazione di IPsec con VPN Client su VPN 3000 Concentrator
- <u>Cisco VPN serie 3000 concentrator</u>
- <u>Cisco VPN Client</u>
- Documentazione e supporto tecnico Cisco Systems