# Exemplo de Configuração da Separação de Túneis para Clientes VPN no VPN 3000 Concentrator

### Contents

Introduction Prerequisites Requirements Componentes Utilizados Diagrama de Rede Conventions Informações de Apoio Configurar o tunelamento dividido no VPN Concentrator Verificar Conexão com o Cliente VPN Exibir o log do cliente VPN Troubleshoot Informações Relacionadas

# **Introduction**

Este documento fornece instruções passo a passo sobre como permitir que os Clientes VPN acessem a Internet enquanto são enviados pelo túnel para um VPN 3000 Series Concentrator. Esta configuração fornece aos Clientes VPN acesso seguro aos recursos corporativos através do IPsec, ao passo que gera acesso não protegido à Internet.

**Observação:** o tunelamento dividido pode potencialmente representar um risco à segurança quando configurado. Como os VPN Clients têm acesso desprotegido à Internet, eles podem ser comprometidos por um invasor. Esse invasor poderá então acessar a LAN corporativa através do túnel IPsec. Um comprometimento entre o tunelamento completo e o tunelamento dividido pode ser permitir apenas o acesso de VPN Clients à LAN local. Consulte <u>Exemplo de Configuração de</u> <u>Permitir Acesso LAN Local para Clientes VPN no VPN 3000 Concentrator</u> para obter mais informações.

### **Prerequisites**

### **Requirements**

Este documento pressupõe que já existe uma configuração de VPN de acesso remoto em funcionamento no VPN Concentrator. Consulte o <u>Exemplo de Configuração de IPsec com VPN</u>

Client para VPN 3000 Concentrator se um ainda não estiver configurado.

### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco VPN 3000 Concentrator Series versão 4.7.2.H
- Cisco VPN Client versão 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.

#### Diagrama de Rede

O VPN Client está localizado em uma rede SOHO típica e se conecta através da Internet ao escritório principal.



### **Conventions**

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.</u>

# Informações de Apoio

Em um cenário de VPN Client to VPN Concentrator básico, todo o tráfego do VPN Client é criptografado e enviado ao VPN Concentrator independentemente do destino. Com base na sua configuração e no número de usuários suportados, essa configuração pode se tornar uma largura de banda intensa. O tunelamento dividido pode funcionar para aliviar esse problema, permitindo que os usuários enviem apenas o tráfego destinado à rede corporativa através do túnel. Todo o tráfego restante, como IM, e-mail ou navegação casual, é enviado para a Internet através da LAN local do VPN Client.

## Configurar o tunelamento dividido no VPN Concentrator

Conclua estes passos para configurar seu grupo de túneis para permitir o tunelamento dividido para usuários no grupo. Primeiro, crie uma lista de rede. Essa lista define as redes de destino para as quais o VPN Client envia tráfego criptografado. Quando a lista for criada, adicione a lista à política de tunelamento dividido do grupo de túneis do cliente.

1. Escolha Configuration > Policy Management > Traffic Management > Network Lists e clique em

 Essa lista define as redes de destino para as quais o VPN Client envia tráfego criptografado. Insira essas redes manualmente ou clique em Gerar lista local para criar uma lista com base em entradas de roteamento na interface privada do VPN Concentrator.Neste exemplo, a lista foi criada

automaticamente.

	VPN 300 Concentra	0 ator Serie	s Manager			Main   Help   Support   Logout
	ooneener		5 III MARKEN		Configuratio	on   Administration   Monitoring
Configuration     Interfaces     Dystem     Outer Management     Ou	Control No	infiguration ( onfigure and ac tries on the Pri List Name [ etwork List	Policy Management   Traffic Ma dd a new Network List. Click on ivate interface.	Generate Lo	<ul> <li>tetwork Lists   Add</li> <li>ocal List to generate a network List to generate a network list yet must be unique.</li> <li>Enter the Networks ar following format n.n.n 10, 10, 0,000, 0, 255, 253</li> <li>Note: Enter a wilder reverse of a subnet 1 ls in bit positions to ig match. For example, 1 10, 10, 1, nn addresses To a black of the day of</li></ul>	ork list based on routing ou are adding. The name ad Wildcard masks using the <b>un/n.n.n.</b> (e.g. 5). <b>ord mask, which is the</b> <b>mask.</b> A wildcard mask has nore, 0s in bit positions to 0.10.1.0/0.0.0.255 = all s.
Cisco Systems	ŀ	Add	Cancel Generate Local L		<ul> <li>Each Network and W entered on a single line</li> <li>The Wildcard mask m Wildcard mask is to be</li> </ul>	ldcard mask pair must be ay be omitted if the natural a used.

3. Depois de criada ou preenchida, forneça um nome para a lista e clique em **Adicionar**.

/ taroronan						
	VPN 3	000				Main   Help   Support   Logout
N ホ 🎽	Concer	ntrator Series	Manager			Logged in: admin
					Configurat	on   Administration   Monitoring
Configuration     Interfaces     System     Orliger Management     Orliger Management     Access Hours		Configuration   Po Configure and add entries on the Priva	licy Management - Traffic M a new Network List. Click o te interface.	lanagement   Netwo n Generate Local )	nk Lists   Add List to generate a netw	rork list based on routing
Network Lists Rules SAs Others		List Name Ma	in Office	Name must 1	e of the Network List 3 be unique. Enter the Networks a	ou are adding. The name nd Wildcard masks using the
Otal     Otal	<u>Control</u>	Network List	.0.1.0/0.0.0.255	× • •	following format n.n. 10.10.0.0/0.0.255.22 Note: Enter a wilde reverse of a subnet 1s in bit positions to i match. For example, 10.10.1.mm addresse Each Network and V entered on a single lim The Wildcard mask is to b	n.n.n.n.n (e.g. 55). www.mask, which is the mask. A wildcard mask has gnore, 0s in bit positions to 10.10.10.00.0.0.255 = all s. Fildcard mask pair must be e. hay be omitted if the natural is used.
Cisco Systems		×				

 Depois de criar a lista de rede, atribua-a a um grupo de túneis. Escolha Configuration > User Management > Groups, selecione o grupo que deseja alterar e clique em Modify Group.

VPN 3	3000			Main   Help   Su	ipport   Logout
Ka 🕂 💋 Conce	ntrator Series Manager			Log	gged in: admin
			Configurat	ion   Administratio	an   Monitoring
-Excention Interfaces 	Configuration   User Managemen This section lets you configure grou	t   Groups .ps. A group is a collection of users trea	ited as a single er	Save	Needed 🚽
Device Management     Device Management     Device Management     Device Management     Device Management	Click the Add Group button to ad other group parameters, select a gr	d a group, or select a group and click I oup and click the appropriate button	)elete Group or	Modify Group. 7	fo modify
-t±HMonitoring	Actions	Current Groups	Mo	dify	
	Add Group	lipsecaroup (Internally Contigured)	Authenticat Authorizati Accountin	ion Servers on Servers ig Servers	
	Belete Group		Client I Bandwidth	Jpdate Assignment	
Cisco Systems			WebVPN Pr	in Forwarding	
ամիտամիտո					

5. Vá até a guia Client Config do grupo que você escolheu modificar.

	VPN 3	000			Main   Help   Support   Logout	
T 12	Concer	itrator Seri	es Manager		Logged in: admin	
					Configuration   Administration   Monitoring	
Configuration     Interfaces     Development     Development     Development     Development     Development     Development     Development     Development     Development	anfiguration Interfaces Description 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 and enter a new value to override base group values. Users Henty General IPSec Client Config Client FW HW Client PPTP/L2TP WebVPN NAC					
- Administration	T		Client Configurat	ion Par	ameters	
- Monitoring			Cisco Client I	Paramete	ers	
		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	N	Enter the UDP port to be used for IPSec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).	
Cisco Systems		IPSec Backup Servers	Use Client Configured List	ব	<ul> <li>Select a method to use or disable backup servers.</li> <li>Enter up to 10 IPSec backup server addresses/names starting from high priority to low.</li> <li>Enter each IPSec backup server address/name on a single line.</li> </ul>	

- 6. Role para baixo até as seções Split Tunneling Policy e Split Tunneling Network List e clique em **Only tunnel networks na lista**.
- 7. Escolha a lista criada anteriormente na lista suspensa. Neste caso, é o **escritório central**. O Herdar? as caixas de seleção são automaticamente esvaziadas em ambos os casos.

	VPN 3000 Main   Help   Support   Lo Concentrator Series Manager Logged in: a Configuration   Administration   Monitor					
Configuration Interfaces					Configuration   Administration   Monitoring	
	X	Split Tunneling Policy	<ul> <li>Tunnel everything</li> <li>Allow the networks in list to bypass the tunnel</li> <li>Only tunnel networks in the list</li> </ul>		Select the method and network list to be used for Split Tunneling. <b>Tunnel Everything:</b> Send all traffic through the tunnel. <b>Allow the networks in the list to bypass the</b> <b>tunnel:</b> 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. <b>Tunnel networks in the list:</b> Send traffic to addresses in this list through the tunnel. Send all other traffic to the client's LAN.	
	Defau Domai Nam	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 <b>Default Domain</b> <b>Name</b> must be explicitly included in <b>Split</b> <b>DNS Names</b> list if it is to be resolved through the tuanel.	
CISCO SYSTEM	. [	Apply	Cancel			

8. Clique em Apply quando terminar.

# **Verificar**

### Conexão com o Cliente VPN

Conecte seu VPN Client ao VPN Concentrator para verificar sua configuração.

1. Selecione sua entrada de conexão da lista e clique em

VPN Client - Version 4.0.5 (Rel)			
onnection Entries Status Certificates Log	Options Help		
Connect New Import N	Aodify Delete	Cisco Sve	STEN Ullu
Connection Entries Certificates Log			
Connection Entry	Host	Transport	
1 2022	170.001.100	IDC #IDD	
to_3000	172.22.1.10b	IFSEC/UDF	
to_3UUU	172.22.1.10b	IFSECUDES	

#### 2. Digite suas

#### credenciais.

🥝 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 1	e 🕼 🐜 🕍	CISCO SYSTEMS
Cancel Connect N	VPN Client   User Authentication for "to_3000"	
Connection Entries	Enter Username and Password.	
Connection E	CISCO SYSTEMS Username: ipsecuser	<u> </u>
to_3000	autility autility - Password: [XXXXXX	P
	OK Canc	
		-1
•		
Authenticating user		

 Escolha Status > Estatísticas... para exibir a janela Detalhes do túnel onde você pode inspecionar os detalhes do túnel e ver o tráfego fluindo.

Ø VPN Client   Statistics		×
Tunnel Details Route Details	Firewall	
Address Information Client: 10.0.1.50 Server: 172.22.1.106	Connection Informal Entry: Time:	tion to_3000 0 dav(s), 00:00.38
<b>Bytes</b> Received: 420 Sent: 2470	<b>Crypto</b> Encryption: Authentication:	168-bit 3-DES HMAC-MD5
Packets Encrypted: 17 Decrypted: 7 Discarded: 0 Bypassed: 56	<b>Transport</b> Transparent Tunnel Local LAN: Compression:	ing: Active on UDP port 4500 Disabled None Reset
		<u>C</u> lose

4. Vá até a guia Route Details (Detalhes da rota) para ver para quais redes o VPN Client envia tráfego criptografado. Neste exemplo, o VPN Client se comunica com segurança com 10.0.1.0/24 enquanto todo o tráfego restante é enviado sem criptografia para a Internet.

ć	VPN Client   Stat	istics			×
	Tunnel Details Ro	ute Details Firewall	1		
	Local LAN Routes	13	Secured Routes		
	Network	Subnet Mask	Network	Subnet Mask	
			10.0.1.0	255.255.255.0	
					- 1
					- 1
					_
				<u>lose</u>	

#### Exibir o log do cliente VPN

Ao examinar o log do VPN Client, você pode determinar se o parâmetro que permite o tunelamento dividido está definido ou não. Acesse a guia Log no VPN Client para visualizar o log. Clique em **Configurações de log** para ajustar o que está registrado. Neste exemplo, IKE e IPsec são definidos como **3- High** enquanto todos os outros elementos de log são definidos como **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/0x6300000D 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**

Consulte <u>Exemplo de Configuração de IPsec com VPN Client para VPN 3000 Concentrator -</u> <u>Troubleshooting</u> para obter informações gerais sobre Troubleshooting desta configuração.

### Informações Relacionadas

- Exemplo de configuração de IPsec com VPN Client para VPN 3000 Concentrator
- <u>Cisco VPN 3000 Series Concentrators</u>
- <u>Cisco VPN Client</u>
- Suporte Técnico e Documentação Cisco Systems