VPN 3000 コンセントレータでの VPN クライア ントのスプリット トンネリング設定例

内容

 概要

 前提条件

 要件

 使用するコンポーネント

 ネットワーク図

 表記法

 背景説明

 VPN コンセントレータでのスプリット トンネリングの設定

 確認

 VPN Client で接続する

 VPN Client ログの表示

 トラブルシュート

 関連情報

<u>概要</u>

このドキュメントでは、VPN Client が VPN 3000 シリーズ コンセントレータにトンネリングされ ている間に、それにインターネットへのアクセスを許可する方法の段階的な手順について説明し ます。この設定により、VPN Client は IPSec を使用した企業リソースへのセキュアなアクセスと 、セキュリティ保護されていないインターネット アクセスの両方を実現できます。

注:スプリットトンネリングを設定すると、セキュリティ上のリスクが生じる可能性があります 。VPN クライアントに許可されるため、攻撃者がクライアントに侵入する可能性があります。 IPsec トンネル経由で企業 LAN にアクセスできるようになる可能性があります。フル トンネリン グとスプリット トンネリングの折衷案として、VPN Client にローカル LAN アクセスだけを許可 することができます。詳細については、『<u>VPN 3000 コンセントレータで VPN Client のローカル</u> LAN アクセスを許可する設定例』を参照してください。

前提条件

<u>要件</u>

このドキュメントでは、VPN コンセントレータでリモート アクセス VPN 設定がすでに存在して いることを前提としています。まだ設定していない場合は、『<u>VPN 3000 コンセントレータに接</u> 続する VPN Client での IPsec 設定例』を参照してください。

<u>使用するコンポーネント</u>

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco VPN 3000 コンセントレータ シリーズ ソフトウェア バージョン 4.7.2.H
- Cisco VPN Client バージョン 4.0.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

<u>ネットワーク図</u>

VPN Client は一般的な SOHO ネットワーク上にあり、インターネット経由で本社に接続しています。



<u>表記法</u>

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

<u>背景説明</u>

VPN Client と VPN コンセントレータの基本的な接続シナリオでは、宛先に関係なく、VPN Client からのすべてのトラフィックは暗号化されて VPN コンセントレータに送信されます。企業 の構成とサポートしているユーザ数によっては、このような設定は帯域幅を多く消費します。ス プリット トンネリングでは、トンネル接続で、企業ネットワーク向けトラフィックの送信だけが ユーザに許可されるため、この問題の軽減に役立ちます。IM、電子メール、または通常の Web 閲覧など、その他すべてのトラフィックは、VPN Client のローカル LAN 経由でインターネット に送出されます。

VPN コンセントレータでのスプリット トンネリングの設定

次の手順を実施して、グループのユーザにスプリット トンネリングを許可するトンネル グループ を設定します。最初にネットワーク リストを作成します。このリストは、VPN Client が暗号化ト ラフィックを送信する宛先ネットワークを定義します。リストが作成されたら、このリストをク

ライアント トンネル グループのスプリット トンネリング ポリシーに追加します。

1. [Configuration] > [Policy Management] > [Traffic Management] > [Network Lists] を選択し、 [Add] をクリックします。

VPN 3 Conce	3000 ntrator Series Manager			Main Help Support Logout
			Configuratio	n Administration Monitoring
Configuration Interfaces DSystem CRUser Management CRUser Management CRUses Hours	Configuration Policy Management This section lets you add, modify, copy	Traffic Management Netword	t Lists	Save Needed 🕞
Network Lists	Click Add to create a Network List, or	r select a Network List and clic	k Modify , Copy, or l	Delete.
Bules SAs SAs Bites Barris Bites Bite	VF	Network List N ClientLocal LAN (Default)	Actions Add Modify Copy Delete	
Cisco Systems				

2. このリストは、VPN Client が暗号化トラフィックを送信する宛先ネットワークを定義します 。これらのネットワークを手動で入力するか、[Generate Local List] をクリックして、VPN コンセントレータのプライベート インターフェイスのルーティング エントリに基づいてリ ストを作成します、次の例では、リストが自動的に作成されています

<u>へ下を1F成しまり。</u>	人の例では、ワストル日動の	りにTFRCイレくいより。
VPN 3	000	Main Help Support Logout
Conce	ntrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
-Configuration 	Configuration Policy Management Traffic & Configure and add a new Network List. Click of entries on the Private interface.	anagement Network Lists Add n Generate Local List to generate a network list based on routing Name of the Network List you are adding. The name must be unique
SAs SAs Chars Others Ot	Network List Add Cancel Generate Local	 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). 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, 10.10.1.0/0.0.255 = all 10.10.0.0.000 = all 10.10.0.0.000 = all 10.10.0.0.000 = all 10.10.0.000 = all 10.10.000 = all 10.1000 = all 10.1000 = a
Cisco Systems		

3. 作成され、データが取り込まれたリストに名前を指定し、[Add] をクリックします。

VPN	3000	Main Help Support Logout
Ka 🕂 💋 Con	centrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
Configuration Interfaces OSystem OSys	Configuration Policy Management Traffic Ma Configure and add a new Network List. Click on entries on the Private interface. List Name Main Office	Generate Local List to generate a network list based on routing Name of the Network List you are adding. The name must be unique.
	Network List	 Enter the Networks and Wildcard masks using the following format 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 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1.nm 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 N Cancel Generate Local L	ist
Cisco Systems		

4. 作成したネットワーク リストをトンネル グループに割り当てます。[Configuration] > [User Management] > [Groups] を選択し、変更するグループを選択して、[Modify Group] をクリックレます

ノしみ 90					
	VPN 3 Conce	0000 ntrator Series Manager		Mai	n Help Support Logout Logged in: admin
		, in the second s		Configuration #	Administration Monitoring
Configuration Interfaces Discribution Order Discribution Order Orde	¥	Configuration User Management This section lets you configure grout Click the Add Group button to ad- other group parameters, select a gr	t Groups ps. A group is a collection of users tres d a group, or select a group and click I oup and click the appropriate button.	uted as a single entity Delete Group or Mod	Save Needed 🚽 ify Group. To modify
-3)Administration -3)Monitoring	-	Actions	Current Groups	Modify	
			ipsecgroup (Internally Contigured)	Authentication Se	anvers
				Authorization Se	rvers
		Add Crown		Accounting Ser	vers
		Madiatop		Address Poo	ls
		Moony Group		Client Updat	e
		Delete Group		Bandwidth Assig	nment
				WebVPN Servers a	nd URLs
				WebVPN Port For	warding
Cisco System					

5. 変更するように選択したグループの [Client Config] タブに移動します。

VPN Cone	3000 entrator Seri	es Manager		Main Help Support Logour Logged in: admin Configuration Administration Monitoring			
Configuration Interfaces DSrsten OUser Management Desc Croup Orouse Users Desclay Management DTurneling and Security OAdministration	Configuration 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. Identity General IPSec Client Config Client FW HW Client PPTP/L2TP WebVPN NAC Client Configuration Parameters						
- Monitoring	Attribute	Value	Inherit?	Description			
	Allow Password Storage on Client		R	Check to allow the IPSec client to store the password locally.			
	IPSec over UDP		M	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 Systems	IPSec Backup Servers	Use Client Configured List	R	 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. [Split Tunneling Policy] および [Split Tunneling Network List] セクションにスクロールし、 [Only tunnel networks in the list] をクリックします。
- 7. 前に作成したリストをドロップダウンから選択します。この場合は [Main Office] です。いず れの場合も、[Inherit?]チェックボックスは自動的にオフになります。

Main Help Support Logou							
Concer	ntrator Seri	es Manager		Logged in: admin			
				Configuration Administration Monitoring			
- Configuration							
Base Croup Base Croup Groups Users Users Deblocy Management Drunneling and Security Administration	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 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 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		য	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 SYSTEMS	Apply	Cancel					

8. 設定が終了したら、[Apply] をクリックします。

<u>確認</u>

<u>VPN Client で接続する</u>

VPN Client を VPN コンセントレータに接続して、設定を確認します。

1. リストから接続エントリを選択して [Connect] をクリックします。

실 VPN Client - Version 4.0.5 (Rel)		_ 🗆 ×
Connection Entries Status Certificates Log Opti	ons <u>H</u> elp	
Connect New Import Modify		CISCO SYSTEMS
Connection Entries Certificates Log		
Connection Entry	Host	Transport 🔶
to_3000	172.22.1.106	IPSec/UDP
▲		
Not connected.		1

2. 認証情報を入力してください。

🤌 YPN Client - Versi	on 4.0.5 (Rel)						- 🗆 ×
Connection Entries St	atus C <u>e</u> rtificates <u>L</u> o	og Options	Help				
Cancel Connect	🔄 🕌 🎉 VPN Client L	ser Auther	tication for	"to_3000"		Cisco S	YSTEMS
Connection Entries Connection E to_3000	Enter Username an CISCO SYSTEMS	d Password. Username: , Password:	ipsecuser	<u> </u>	Cancel	P	
Authenticating user					•		۲ ۲

3. [Status] > [Statistics...] の順に選択して、[Tunnel Details] ウィンドウを表示します。ここで トンネルの詳細を調べ、トラフィックの流れを確認できます。

1	👌 VPN Client 🕴 S	statistics				×
	Tunnel Details	Route Details	Fire	wall		
	Address Info	1				
	Client: Server	10.0.1.50		Entry: Time:	to_3000 0.dag(s)_00:00.38	
	Bytes	112.22.1.100	Сп	inno.		
	Received: Sent:	420 2470		Encryption: Authentication:	168-bit 3-DES HMAC-MD5	
	Packets		Tra	ansport		
	Encrypted: Decrypted: Discarded: Bypassed:	17 7 0 56		Transparent Tunneling: Local LAN: Compression:	Active on UDP port 4500 Disabled None	
					Reset	
					<u>C</u> lose	

4. [Route Details] タブに移動して、VPN Client が暗号化トラフィックを送信するネットワーク を確認します。この例では、VPN Client は 10.0.1.0/24 と安全に通信しますが、その他のす べてのトラフィックは暗号化されていない状態でインターネットに送信されます。

VPN Client Sta	tistics		×
Tunnel Details	oute Details Firewall	1	
Local LAN Route	, k	Secured Routes	
Network	Subnet Mask	Network	Subnet Mask
		10.0.1.0	255.255.255.0
			<u>C</u> lose

<u>VPN Client ログの表示</u>

VPN Client ログを調査すると、スプリット トンネリングを許可するパラメータが設定されている

かどうかを確認できます。ログを表示するには、VPN Client の [Log] タブに移動します。[Log Settings] をクリックして、記録される内容を調整します。この例では、IKE および IPsec は **3-High** に設定されており、他のすべてのログ要素は **1 - Low** に設定されています。



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.



この設定のトラブルシューティングに関する一般的な情報については、<u>『VPN 3000 コンセント</u> レータに接続する VPN Client での IPsec 設定例』の「トラブルシューティング」</u>を参照してくだ さい。

<u>関連情報</u>

- VPN 3000 コンセントレータに接続する VPN Client での IPsec 設定例
- <u>Cisco VPN 3000 シリーズ コンセントレータ</u>
- <u>Cisco VPN Client</u>
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>