Windows マシンと Cisco ルータの間で L2TP ト ンネルを設定する

内容

<u>概要 前提条件</u> <u>要件</u> 使用するコンポーネント <u>設定</u> <u>ネットワーク図</u> <u>設定</u> 確認 トラブルシュート <u>関連情報</u>

概要

このドキュメントでは、Windows マシンと Cisco ルータ間で Layer 2 Tunneling Protocol (L2TP)トンネルを設定する方法について説明します。

前提条件

要件

Windows マシンがルータ上の物理インターフェイスの IP アドレスに ping を実行できることに関する知識があることを推奨します。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるもの ではありません。

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。

設定

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

アグリゲータ構成

アグリゲータ上の構成の例は次のとおりです。

interface GigabitEthernet0/0/1 ip address 192.168.1.1 255.255.255.0 negotiation auto interface Loopback100 end ip address 172.16.1.1 255.255.255.255 end vpdn enable vpdn-group 1 ! Default L2TP VPDN group accept-dialin protocol 12tp virtual-template 1 no l2tp tunnel authentication interface Virtual-Template1 ip unnumbered Loopback100 peer default ip address pool test ppp authentication chap callout ppp ipcp dns 4.2.2.1 4.2.2.2 end ip local pool test 10.1.1.2 10.1.1.100 Windows のマシン構成と設定

次のステップを実行します。

手順 1 : [Network and Sharing Center] を開き、次の画像のように [Set up a new connection or network] をクリックします。

💽 🗢 👯 « Network and Inte	rnet • Network and Sharing Center	- - i i j	Search Control Panel	٩
Control Panel Home	View your basic network informat	ion and set	t up connections	0
Control Panel Home Change adapter settings Change advanced sharing settings	View your basic network information ADMIN-PC Network (This computer) View your active networks Network 5 Work network Change your networking settings Set up a new connection or network Set up a wireless, broadband, dial point. Connect to a network Connect to a network Connect or reconnect to a wireless Choose homegroup and sharing of Access files and printers located or	ion and set vork 5 Ac Co k)p, ad hoc, or , wired, dial-u ptions o other networ	t up connections Internet Con ccess type: Internet connections: Local Area VPN connection; or set up p, or VPN network connect rk computers, or change sh	See full map anect or disconnect Connection 5 a router or access tion.
See also HomeGroup Internet Options Windows Firewall	Troubleshoot problems Diagnose and repair network probl	ems, or get tro	oubleshooting information	

手順 2:[Connect to a Workplace] を選択し、[Next] をクリックします。

C3	- • •
💮 🔄 Set Up a Connection or Network	
Choose a connection option	
Connect to the Internet Set up a wireless, broadband, or dial-up connection to the Internet.	
Set up a new network Configure a new router or access point.	
Connect to a workplace Set up a dial-up or VPN connection to your workplace.	
Set up a dial-up connection Connect to the Internet using a dial-up connection.	
Ne	t Cancel

手順 3:[Use my Internet Connection (VPN)] を選択します。



手順 4:アグリゲータの IP アドレス(この例では 192.168.1.1)を入力し、接続に名前(この例 では、VPDN という名前)を付け、[Next] をクリックします。

		- • •
🚱 🔚 Connect to a Workplace		
Type the Internet addr	ess to connect to	
Your network administrator		
Internet address:	192.168.1.1]
Destination name:	VPDN]
Use a <u>s</u> mart card		
😵 🥅 <u>A</u> llow other people to This option allows an	o use this connection yone with access to this computer to use this connection.	
Don't connect now; j	ust set it up so I can connect later	
	<u>N</u> e	ext Cancel

手順 5:ユーザ名とパスワードを入力し、[Connect] をクリックします。

	- Connect to a Workplace		
\mathbf{V}	Connect to a workplace		
	Type your user name a	and password	
	<u>U</u> ser name:	cisco	
	Password:	•••••	
		Show characters	
		<u>Remember this password</u>	
	Domain (optional):		
			Connect Cancel

手順6:ユーザ名とパスワードを確認します。



ステップ7:この図に示すように、最初に失敗する可能性があります。

🚱 🌆 Connect to a Workplace	
Connection failed with error 800	
I	
The remote connection was not made because the attempted VPN tunnels failed. The VPN server might be unreachable. If this connection is attempting to use an L2TP/IPsec tunnel, the security parameters required for IPsec negotiation might not be configured properly.	*
→ Iry again	
Set up the connection anyway	
Diagnose the problem	
	Cancel

手順 8:[Set up the connection anyway] をクリックし、[Networks] タブを開きます。



手順 9:接続(この例では VPDN)を右クリックし、[Properties] をクリックします。アグリゲー タの IP アドレス(この例では 192.168.1.1)を確認します

VPDN Properties								
General Options Security Networking Sharing								
Host name or IP address of destination (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):								
192.168.1.1								
First connect								
Windows can first connect to a public network, such as the Internet, before trying to establish this virtual connection.								
Dial another connection first:								
See our online <u>privacy statement</u> for data collection and use information.								
OK Cancel								

手順 10 : [Options] > [PPP Settings] に移動し、次の図のように設定を確認します。

VPDN Properties							
General Options Security Networking Sharing							
Dialing options Display progress while connecting Prompt for name and password, certificate, etc. Include Windows logon domain							
PPP Settings							
Enable LCP extensions Enable software compression Negotiate multi-link for single-link connections OK							
PPP Settings							
OK Cancel							

手順 11:次の図のように、[Security] > [Type of VPN] > [Layer 2 Tunneling Protocol with IPsec] に移動します。

VPDN Properties
General Options Security Networking Sharing
Type of VPN:
Automatic
Automatic Point to Point Tunneling Protocol (PPTP) Laver 2 Tunneling Protocol with IPsec (L2TP/IPSec) Secure Socket Tunneling Protocol (SSTP)
Authentication
Use Extensible Authentication Protocol (EAP)
· · · · · · · · · · · · · · · · · · ·
Properties
Allow these protocols EAP-MSCHAPv2 will be used for IKEv2 VPN type. Select any of these protocols for other VPN types.
Unencrypted password (PAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP Version 2 (MS-CHAP v2)
<u>A</u> utomatically use my Windows logon name and password (and domain, if any)
OK Cancel

ステップ12:[Data encryption]ドロップダウン**メニューで[No encryption allowed]**オプションを選択 します。

VPDN Properties
General Options Security Networking Sharing
Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)
Advanced settings
Require encryption (disconnect if server declines)
Optional encryption (connect even if no encryption) Require encryption (disconnect if server declines) Maximum strength encryption (disconnect if server declines)
Allow these protocols
Unencrypted password (PAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP Version 2 (MS-CHAP v2)
Automatically use my Windows logon name and password (and domain, if any)
OK Cancel

ステップ13:[Microsoft CHAP Version 2]をオフにし、[OK]をクリックします。

VPDN Properties
General Options Security Networking Sharing
Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)
Advanced settings
No encryption allowed (server will disconnect if it requires encry
Authentication
Use Extensible Authentication Protocol (EAP)
Properties
Allow these protocols
Unencrypted password (PAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP Version 2 (MS-CHAP v2)
Automatically use my Windows logon name and
password (and domain, if any)
OK Cancel

ステップ14:ネットワーク(ここではVPDN)を開き、[接続]をクリック**します。**



ステップ15:ユーザ名とパスワードを入力し、[Connect]をクリックします

See Connect VPDN
User name: cisco
Password:
Do <u>m</u> ain:
Save this user name and password for the following users:
⊘ Me o <u>n</u> ly
O Anyone who uses this computer
Connect Cancel Properties Help

確認

手順 1:[Network] タブを再度開き、ネットワーク(この例では VPDN という名前)を選択し、 ステータスが [Connected] になっていることを確認します。



手順2:コマンドプロンプトを開き、ipconfig /all コマンドを実行します。

PPP	adaj	pter	• VPD	N:											
	Conne	ecti	ion-s	pec	ifi	ic	D١	S	Sι	ιff	i)	¢	-	:	
	Desci	ript	ion		-	-	-	-	-	-	-	-	-		VPDN
	Phys:	ica]	l Add	lres	s.	-	-	-	-	-	-	-	-		
	DHČP	Ena	bled	l 	_	-	-	-	_	-	-				No
	Autod	conf	igur	ati	lon	Ег	at	16	ed	-	-				Yes
	IPv4	Add	lress		_	-	-	-	_	-	-	-	-	=	10.1.1.9(Preferred)
	Subne	et M	lask		_	_	-	-	_	_	-	_	-	-	255.255.255.255
	Defau	ult	Gate	way		_	_	_	_	_	_	-			0.0.0.0
	DNS S	Serv	ers		_	_	_	-	_	_	_	-			4.2.2.1
															4.2.2.2
	Net B)	IOS	over	·To	pip).	-	-	-	-	-	-	-	=	Enabled

PPP インターネット プロトコル制御プロトコル(IPCP)フェーズが完了すると、アグリゲータ によって IPv4 アドレスおよびドメインネーム サーバ(DNS)が割り当てられます。

手順3: debug ppp negotiation およびその他の show コマンドをアグリゲータで実行します。

Aggregator# *Apr 12 06:17:38.148: PPP: Alloc Context [38726D0C] *Apr 12 06:17:38.148: ppp11 PPP: Phase is ESTABLISHING *Apr 12 06:17:38.148: ppp11 PPP: Using vpn set call direction *Apr 12 06:17:38.148: ppp11 PPP: Treating connection as a callin

*Apr 12 06:17:38.148: ppp11 PPP: Session handle[A600000B] Session id[11] *Apr 12 06:17:38.148: ppp11 LCP: Event[OPEN] State[Initial to Starting] *Apr 12 06:17:38.148: ppp11 PPP: No remote authentication for call-in *Apr 12 06:17:38.148: ppp11 PPP LCP: Enter passive mode, state[Stopped] *Apr 12 06:17:38.607: ppp11 LCP: I CONFREQ [Stopped] id 0 len 21

 *Apr 12 06:17:38.607: ppp11 LCP:
 MRU 1400 (0x01040578)

 *Apr 12 06:17:38.607: ppp11 LCP:
 MagicNumber 0x795C7CD1 (0x0506795C7CD1)

 *Apr 12 06:17:38.607: ppp11 LCP:
 PFC (0x0702)

 *Apr 12 06:17:38.607: ppp11 LCP:
 ACFC (0x0802)

 *Apr 12 06:17:38.607: ppp11 LCP:
 Callback 6 (0x0D0306)

 *Apr 12 06:17:38.608: ppp11 LCP: O CONFREQ [Stopped] id 1 len 10 *Apr 12 06:17:38.608: ppp11 LCP: MagicNumber 0xF7C3D2B9 (0x0506F7C3D2B9) *Apr 12 06:17:38.608: ppp11 LCP: O CONFREJ [Stopped] id 0 len 7 *Apr 12 06:17:38.608: ppp11 LCP: Callback 6 (0x0D0306) *Apr 12 06:17:38.608: ppp11 LCP: Event[Receive ConfReq-] State[Stopped to REQsent] *Apr 12 06:17:38.615: ppp11 LCP: I CONFACK [REQsent] id 1 len 10 *Apr 12 06:17:38.615: ppp11 LCP: MagicNumber 0xF7C3D2B9 (0x0506F7C3D2B9) *Apr 12 06:17:38.615: ppp11 LCP: Event[Receive ConfAck] State[REQsent to ACKrcvd] *Apr 12 06:17:38.615: ppp11 LCP: I CONFREQ [ACKrcvd] id 1 len 18 *Apr 12 06:17:38.615: ppp11 LCP: MRU 1400 (0x01040578) *Apr 12 06:17:38.615: ppp11 LCP: MagicNumber 0x795C7CD1 (0x0506795C7CD1) *Apr 12 06:17:38.616: ppp11 LCP: PFC (0x0702) *Apr 12 06:17:38.616: ppp11 LCP: ACFC (0x0802) *Apr 12 06:17:38.616: ppp11 LCP: O CONFNAK [ACKrcvd] id 1 len 8 *Apr 12 06:17:38.616: ppp11 LCP: MRU 1500 (0x010405DC) *Apr 12 06:17:38.616: ppp11 LCP: Event[Receive ConfReq-] State[ACKrcvd to ACKrcvd] *Apr 12 06:17:38.617: ppp11 LCP: I CONFREQ [ACKrcvd] id 2 len 18 *Apr 12 06:17:38.617: ppp11 LCP: MRU 1400 (0x01040578) *Apr 12 06:17:38.617: ppp11 LCP: MagicNumber 0x795C7CD1 (0x0506795C7CD1) *Apr 12 06:17:38.617: ppp11 LCP: PFC (0x0702) *Apr 12 06:17:38.617: ppp11 LCP: ACFC (0x0802) *Apr 12 06:17:38.617: ppp11 LCP: O CONFNAK [ACKrcvd] id 2 len 8 *Apr 12 06:17:38.617: ppp11 LCP: MRU 1500 (0x010405DC) *Apr 12 06:17:38.617: ppp11 LCP: Event[Receive ConfReq-] State[ACKrcvd to ACKrcvd] *Apr 12 06:17:38.618: ppp11 LCP: I CONFREQ [ACKrcvd] id 3 len 18 *Apr 12 06:17:38.618: ppp11 LCP: MRU 1500 (0x010405DC) *Apr 12 06:17:38.618: ppp11 LCP: MagicNumber 0x795C7CD1 (0x0506795C7CD1) *Apr 12 06:17:38.618: ppp11 LCP: PFC (0x0702) *Apr 12 06:17:38.618: ppp11 LCP: ACFC (0x0802) *Apr 12 06:17:38.618: ppp11 LCP: O CONFACK [ACKrcvd] id 3 len 18 *Apr 12 06:17:38.618: ppp11 LCP: MRU 1500 (0x010405DC) *Apr 12 06:17:38.618: ppp11 LCP: MagicNumber 0x795C7CD1 (0x0506795C7CD1) *Apr 12 06:17:38.618: ppp11 LCP: PFC (0x0702) *Apr 12 06:17:38.619: ppp11 LCP: ACFC (0x0802) *Apr 12 06:17:38.619: ppp11 LCP: Event[Receive ConfReq+] State[ACKrcvd to Open] *Apr 12 06:17:38.621: ppp11 LCP: I IDENTIFY [Open] id 4 len 18 magic 0x795C7CD1MSRASV5.20 *Apr 12 06:17:38.621: ppp11 LCP: I IDENTIFY [Open] id 5 len 24 magic 0x795C7CD1MSRAS-0-ADMIN-PC *Apr 12 06:17:38.621: ppp11 LCP: I IDENTIFY [Open] id 6 len 24 magic 0x795C7CD1Z8Of(U3G.cIwR<#! *Apr 12 06:17:38.626: ppp11 PPP: Queue IPV6CP code[1] id[7] *Apr 12 06:17:38.626: ppp11 PPP: Queue IPCP code[1] id[8] *Apr 12 06:17:38.640: ppp11 PPP: Phase is FORWARDING, Attempting Forward *Apr 12 06:17:38.640: ppp11 LCP: State is Open *Apr 12 06:17:38.657: Vi3.1 PPP: Phase is ESTABLISHING, Finish LCP *Apr 12 06:17:38.657: Vi3.1 PPP: Phase is UP *Apr 12 06:17:38.657: Vi3.1 IPCP: Protocol configured, start CP. state[Initial] *Apr 12 06:17:38.657: Vi3.1 IPCP: Event[OPEN] State[Initial to Starting] *Apr 12 06:17:38.657: Vi3.1 IPCP: O CONFREQ [Starting] id 1 len 10 *Apr 12 06:17:38.657: Vi3.1 IPCP: Address 172.16.1.1 (0x0306AC100101) *Apr 12 06:17:38.657: Vi3.1 IPCP: Event[UP] State[Starting to REQsent] *Apr 12 06:17:38.657: Vi3.1 PPP: Process pending ncp packets *Apr 12 06:17:38.657: Vi3.1 IPCP: Redirect packet to Vi3.1 *Apr 12 06:17:38.657: Vi3.1 IPCP: I CONFREQ [REQsent] id 8 len 34 *Apr 12 06:17:38.657: Vi3.1 IPCP: Address 0.0.0.0 (0x03060000000) *Apr 12 06:17:38.657: Vi3.1 IPCP: PrimaryDNS 0.0.0.0 (0x81060000000)

*Apr 12 06:17:38.657: Vi3.1 IPCP: PrimaryWINS 0.0.0.0 (0x82060000000) *Apr 12 06:17:38.657: Vi3.1 IPCP: SecondaryDNS 0.0.0.0 (0x83060000000) *Apr 12 06:17:38.657: Vi3.1 IPCP: SecondaryWINS 0.0.0.0 (0x84060000000) *Apr 12 06:17:38.657: Vi3.1 IPCP AUTHOR: Done. Her address 0.0.0.0, we want 0.0.0.0 *Apr 12 06:17:38.657: Vi3.1 IPCP: Pool returned 10.1.1.9 *Apr 12 06:17:38.657: Vi3.1 IPCP: O CONFREJ [REQsent] id 8 len 16 *Apr 12 06:17:38.658: Vi3.1 IPCP: PrimaryWINS 0.0.0.0 (0x82060000000) *Apr 12 06:17:38.658: Vi3.1 IPCP: SecondaryWINS 0.0.0.0 (0x84060000000) *Apr 12 06:17:38.658: Vi3.1 IPCP: Event[Receive ConfReq-] State[REQsent to REQsent] *Apr 12 06:17:38.658: Vi3.1 IPV6CP: Redirect packet to Vi3.1 *Apr 12 06:17:38.658: Vi3.1 IPV6CP: I CONFREQ [UNKNOWN] id 7 len 14 *Apr 12 06:17:38.658: Vi3.1 IPV6CP: Interface-Id F0AA:D7A4:5750:D93E (0x010AF0AAD7A45750D93E) *Apr 12 06:17:38.658: Vi3.1 LCP: O PROTREJ [Open] id 2 len 20 protocol IPV6CP (0x0107000E010AF0AAD7A45750D93E) *Apr 12 06:17:38.672: Vi3.1 IPCP: I CONFACK [REQsent] id 1 len 10 *Apr 12 06:17:38.672: Vi3.1 IPCP: Address 172.16.1.1 (0x0306AC100101) *Apr 12 06:17:38.672: Vi3.1 IPCP: Event[Receive ConfAck] State[REQsent to ACKrcvd] *Apr 12 06:17:38.672: Vi3.1 IPCP: I CONFREQ [ACKrcvd] id 9 len 22 *Apr 12 06:17:38.672: Vi3.1 IPCP: Address 0.0.0.0 (0x03060000000) *Apr 12 06:17:38.672: Vi3.1 IPCP: PrimaryDNS 0.0.0.0 (0x81060000000) *Apr 12 06:17:38.672: Vi3.1 IPCP: SecondaryDNS 0.0.0.0 (0x83060000000) *Apr 12 06:17:38.672: Vi3.1 IPCP: O CONFNAK [ACKrcvd] id 9 len 22 *Apr 12 06:17:38.672: Vi3.1 IPCP: Address 10.1.1.9 (0x03060A010109) *Apr 12 06:17:38.672: Vi3.1 IPCP: PrimaryDNS 4.2.2.1 (0x810604020201) *Apr 12 06:17:38.672: Vi3.1 IPCP: SecondaryDNS 4.2.2.2 (0x830604020202) *Apr 12 06:17:38.672: Vi3.1 IPCP: Event[Receive ConfReq-] State[ACKrcvd to ACKrcvd] *Apr 12 06:17:38.747: Vi3.1 IPCP: I CONFREQ [ACKrcvd] id 10 len 22 *Apr 12 06:17:38.747: Vi3.1 IPCP: Address 10.1.1.9 (0x03060A010109) *Apr 12 06:17:38.747: Vi3.1 IPCP: PrimaryDNS 4.2.2.1 (0x810604020201) *Apr 12 06:17:38.747: Vi3.1 IPCP: SecondaryDNS 4.2.2.2 (0x830604020202) *Apr 12 06:17:38.747: Vi3.1 IPCP: O CONFACK [ACKrcvd] id 10 len 22 *Apr 12 06:17:38.748: Vi3.1 IPCP: Address 10.1.1.9 (0x03060A010109) *Apr 12 06:17:38.748: Vi3.1 IPCP: PrimaryDNS 4.2.2.1 (0x810604020201) *Apr 12 06:17:38.748: Vi3.1 IPCP: SecondaryDNS 4.2.2.2 (0x830604020202) *Apr 12 06:17:38.748: Vi3.1 IPCP: Event[Receive ConfReq+] State[ACKrcvd to Open] *Apr 12 06:17:38.768: Vi3.1 IPCP: State is Open *Apr 12 06:17:38.769: Vi3.1 Added to neighbor route AVL tree: topoid 0, address 10.1.1.9 *Apr 12 06:17:38.769: Vi3.1 IPCP: Install route to 10.1.1.9

Aggregator#show caller ip Line User IP Address Local Number Remote Number <-> Vi3.1 - 10.1.1.9 - - in Aggregator#show ip interface brief | exclude un Interface IP-Address OK? Method Status Protocol GigabitEthernet0/0/1 192.168.1.1 YES manual up up Loopback100 172.16.1.1 YES manual up up 手順 4 : Windows マシンがアグリゲータの背後にあるリモート ネットワーク(この例ではループ

```
バック 100 インターフェイス)に到達できるかどうかを確認します。
```

C:\Users\admin>ping 172.16.1.1 Pinging 172.16.1.1 with 32 bytes of data: Reply from 172.16.1.1: bytes=32 time=1ms TTL=255 Reply from 172.16.1.1: bytes=32 time<1ms TTL=255 Reply from 172.16.1.1: bytes=32 time<1ms TTL=255 Reply from 172.16.1.1: bytes=32 time<1ms TTL=255 Ping statistics for 172.16.1.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- <u>VPDN について</u>
- Tテクニカルサポートとドキュメント Cisco Systems