Stel L2TP-tunnelheid in tussen een Windowsmachine en een Cisco-router

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Netwerkdiagram Configuraties Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u een Layer 2 Tunneling Protocol (L2TP)-tunnels tussen een Windows-machine en een Cisco-router kunt configureren.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben dat de Windows-machine het fysieke IP-adres van de interface op de router kan ping.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Configuratie aggregator:

Een voorbeeld van de configuratie van de Aggregator is:

```
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
      ip local pool test 10.1.1.2 10.1.1.100
end
```

Windows Machine-configuraties en -instellingen

Voer de volgende stappen uit:

Stap 1. Open **Network and Sharing Center** en klik op **Stel een nieuwe verbinding of een nieuw netwerk** in zoals in deze afbeelding.

💽 🗢 👯 « Network and Inte	rnet Network and Sharing Center	- - - f - j	Search Control Panel	٩					
Control Panel Home	View your basic network inform	ation and set	up connections	0					
Change adapter settings Change advanced sharing settings	ADMIN-PC N (This computer) View your active networks Network 5 Work network	letwork 5	Internet Con cess type: Internet nnections: I Local Area	See full map inect or disconnect Connection 5					
	Change your networking settings Set up a new connection or network Set up a wireless, broadband, dia p, ad hoc, or VPN connection; or set up a router point.								
	Connect to a network Connect or reconnect to a wirele	ess, wired, dial-up	o, or VPN network connect	ion.					
	Choose homegroup and sharing Access files and printers located	g options on other networl	k computers, or change sh	aring settings.					
See also HomeGroup Internet Options Windows Firewall	Troubleshoot problems Diagnose and repair network pro	oblems, or get tro	ubleshooting information.						

Stap 2. Selecteer Connect met een werkplaats en klik op Volgende

₽	
🌀 🐏 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.	
<u>N</u> ext	Cancel

Stap 3. Selecteer Gebruik mijn internetverbinding (VPN)



Stap 4. Voer het IP-adres van de aggregator in (in dit geval 192.168.1.1), geef een naam aan de verbinding (in dit geval met de naam VPDN) en klik op **Volgende**.

		- • ×									
🚱 🜆 Connect to a Workplace											
Type the Internet addr	Type the Internet address to connect to										
Your network administrator	can give you this address.										
Internet address:	192.168.1.1										
D <u>e</u> stination name:	VPDN										
Use a smart card											
😗 🔲 Allow other people to	o use this connection										
This option allows ar	yone with access to this computer to use this connection.										
Don't connect now; j	ust set it up so I can connect later										
	Ne	t Cancel									

Stap 5. Voer de gebruikersnaam en het wachtwoord in en klik op Connect

Connect to a Workplace		
Type your user name	and password	
<u>U</u> ser name:	cisco	
Password:	•••••]
	Show characters	
	<u>Remember this password</u>	
Domain (optional):]
		Connect Cancel

Stap 6. Controleer de gebruikersnaam en het wachtwoord



Stap 7. Mogelijk faalt dit voor het eerst zoals in deze afbeelding.

Connect to a Workplace	
Connection failed with error 800	
	
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	
	Canad
	Cancer

Stap 8. Klik **op** sowieso **op Setup** en open het tabblad **Networks**.



Stap 9. Klik met de rechtermuisknop op de verbinding (hier VPDN) en klik op **Eigenschappen**. Controleer het IP-adres van de Aggregator (hier 192.168.1.1)

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									

Stap 10. Navigeer naar **Opties>PPP-instellingen** en controleer de instellingen, zoals in deze afbeelding.

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									

Stap 1. Navigeer naar Security > Type VPN > Layer 2 Tunneling Protocol met IPsec, zoals in deze afbeelding weergegeven.

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)									
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>Automatically use my Windows logon name and password (and domain, if any)</u>									
OK Cancel									

Stap 12. Selecteer Geen encryptie toegestaan optie onder het menu Datacenencryptie:

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)
No encryption allowed (server will disconnect if it requires encryption
Optional encryption (connect even if no encryption) Require encryption (disconnect if server declines) Maximum strength encryption (disconnect if server declines)
P <u>r</u> operties
Allow these protocols
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

Stap 13. Controleer Microsoft CHAP versie 2 en klik op OK.

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										

Stap 14. Open een netwerk (hier VPDN) en klik op Connect.



Stap 15. Voer een gebruikersnaam en wachtwoord in en klik op Connect

💱 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

Verifiëren

Stap 1. Open opnieuw **het** tabblad **Networks**, selecteer het netwerk (met de naam VPDN in dit voorbeeld) en controleer of de status is aangesloten.



Stap 2. Open commando prompt en voer ipfig /all opdracht uit.

PPP adapter VPDN:																	
	Conn	ect	ion	-s]	peo	cił	fi	C	Dł	٩S	Sı	ιff	fi>	ĸ	-	=	
	Desc	rip	tio	n	-	-		-	-	-	-	-	-	-	-		VPDN
	Phys	ica	1 A	ddı	re:	SS.		-	-	-	-	-	-	-	-		
	DHĒF	'En	abl	ed	_			-	-	-	-	-	-	-	-		No
	Auto	con	fig	ura	at:	ior	ì	Еп	ıaJ	510	ed	-	_	_			Yes
	IPv4	l Ad	dre	SS	_	_		-	-	-	_	_	_	_			10.1.1.9(Preferred)
	Subn	et	Mas	\mathbf{k}	_			_	_	_	_	_	_	_			255.255.255.255
	Defa	ult	Ga	te	wai	υ		_	_	_	_	_	_	_	_		0.0.0.0
	DNS	Ser	ver	s		_		-	-	-						-	4.2.2.1
	2110			-							-						4 2 2 2
	NetE	3I OS	OV	er	Τı	cp:	iŗ).	-	-	-	-	-	-	-	=	Enabled

IPv4-adres en Domian Name Server (DNS) worden door de Aggregator toegewezen na voltooiing van de IPCP-fase (PPP Internet Protocol Control Protocol).

Stap 3. Start debug ppp onderhandeling en de andere showopdrachten op Aggregator:

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 Line Vi3.1	caller ip User -	IP Addres 10.1.1.9	ss Local Number -	Remote Number -	<-> in
Aggregator#show ip interface brief exclude un					
Interface	IP	-Address	OK? Method Status	I	Protocol
GigabitEthernet	0/0/1 19 2	2.168.1.1	YES manual up	up	
Loopback100	17:	2.16.1.1	YES manual up	ι	qu

Stap 4. Controleer of de Windows-machine het externe netwerk achter Aggregator kan bereiken (in dit geval Loopback 100-interface)

```
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
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Inzicht VPDN
- OTechnische ondersteuning en documentatie Cisco-systemen