Einrichten eines L2TP-Tunnels zwischen einem Windows-Computer und einem Cisco Router

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Netzwerkdiagramm Konfigurationen Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie ein L2TP-Tunnel (Layer 2 Tunneling Protocol) zwischen einem Windows-Computer und einem Cisco-Router konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie wissen, dass Windows-Computer die IP-Adresse der physischen Schnittstelle auf dem Router pingen kann.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

Aggregator-Konfiguration:

Ein Beispiel für die Konfiguration auf dem Aggregator wird angezeigt:

```
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 12tp 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-Systemkonfigurationen und -einstellungen

Gehen Sie wie folgt vor:

Schritt 1: Öffnen Sie **Netzwerk- und Freigabecenter**, und klicken Sie auf **Neue Verbindung oder neues Netzwerk einrichten**, wie in diesem Bild gezeigt.

Control Panel Home View your basic network information and set up connections Change adapter settings Change adapter settings Change adapter settings Optimitient of the panel				×
Control Panel Home View your basic network information and set up connections Change adapter settings Change advanced sharing Change advanced sharing	💽 🗢 👯 « Network and Inte	net Network and Sharing Center	✓ Search Control Panel	9
Change adapter settings See full ma Change advanced sharing ADMIN DC	Control Panel Home	View your basic network informat	ition and set up connections	?
settings ADMIN-PC Network 3 Internet (This computer) View your active networks Connect or disconnet View your active networks Access type: Internet Network 5 Access type: Internet View your active networking settings Access type: Internet View your networking settings Set up a new connection or network Set up a new connection or network Set up a new connection or network Set up a new connection or network Set up a new connection or network Set up a new connection or network Connect to a network Connect or a connect to a wireless, wired, dial-up, or VPN connection; or set up a router or access point. View Connect to a network Connect or reconnect to a wireless, wired, dial-up, or VPN network connection. View Choose homegroup and sharing options Access files and printers located on other network computers, or change sharing settings. Troubleshoot problems Diagnose and repair network problems, or get troubleshooting information. Windows Firewall Viewall	Change adapter settings Change advanced sharing settings	ADMIN-PC Networks ADMIN-PC Networks Wiew your active networks Network 5 Work network Change your networking settings Set up a new connection or network Set up a wireless, broadband, dialy 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 of Troubleshoot problems Diagnose and repair network prob	See full ma See full ma Connect or disconner Access type: Internet Connections: Local Area Connection 5 Connections: Local Area Connection 5 Connection; or set up a router or access ss, wired, dial-up, or VPN network connection. Coptions on other network computers, or change sharing settings. blems, or get troubleshooting information.	sct

Schritt 2: Wählen Sie Connect to a Workplace (Mit Arbeitsplatz verbinden) aus, und klicken Sie auf Next (Weiter)

💮 🐏 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.	
	d Cancel

Schritt 3: Wählen Sie Meine Internetverbindung (VPN) verwenden aus.



Schritt 4: Geben Sie die IP-Adresse des Aggregators ein (in diesem Fall 192.168.1.1), geben Sie der Verbindung einen Namen (in diesem Fall den Namen als VPDN), und klicken Sie auf **Weiter**.

		- • •
🕝 🔚 Connect to a Workplace		
Type the Internet addr	ress to connect to	
Varia activada a desircitata ta		
Your network administrator	can give you this address.	
Internet address:	192.168.1.1	
Destination name:	VPDN	
-		
Use a <u>s</u> mart card		
Image: Allow other people to use this connection		
I his option allows anyone with access to this computer to use this connection.		
Don't connect now; just set it up so I can connect later		
	<u>N</u> e	kt Cancel

Schritt 5: Geben Sie den Benutzernamen und das Kennwort ein, und klicken Sie auf Verbinden.

📀 🗽 Connect to a Workplac	:e	
Type your user name	e and password	
<u>U</u> ser name:	cisco	
Password:	•••••]
	Show characters Remember this password	
<u>D</u> omain (optional):]
		Connect Cancel

Schritt 6: Benutzername und Kennwort überprüfen



Schritt 7: Es kann zum ersten Mal fehlschlagen, wie in diesem Bild gezeigt.

Connect to a Workplace	- • •
Connection failed with error 800	
N	
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.	*
<u> </u>	
Set up the connection anyway	
Diagnose the problem	
	Cancel

Schritt 8: Klicken Sie auf Verbindung sowieso einrichten und öffnen Sie die Registerkarte Netzwerke.



Schritt 9: Klicken Sie mit der rechten Maustaste auf die Verbindung (hier VPDN), und klicken Sie auf **Eigenschaften**. Überprüfen Sie die IP-Adresse des Aggregators (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		

Schritt 10: Navigieren Sie zu **Optionen>PPP-Einstellungen**, und überprüfen Sie die Einstellungen, wie in diesem Bild gezeigt.

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 Cancel		
PPP Settings		
OK Cancel		

Schritt 11: Navigieren Sie zu Security > Type of VPN >Layer 2 Tunneling Protocol mit IPsec, wie in diesem Bild gezeigt.

VPDN Properties		
General Options Security Networking Sharing		
Type of VPN:		
Automatic		
Automatic Point to Point Tunneling Protocol (PPTP) Layer 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)		
Automatically use my Windows logon name and password (and domain, if any)		
OK Cancel		

Schritt 12: Wählen Sie im Dropdown-Menü Datenverschlüsselung die Option Keine Verschlüsselung zulässig aus:

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)	
Properties Properties	
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	

Schritt 13: Deaktivieren Sie Microsoft CHAP Version 2 und klicken Sie auf OK.

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

Schritt 14: Öffnen Sie das Netzwerk (hier VPDN), und klicken Sie auf Verbinden.



Schritt 15: Geben Sie Benutzername und Kennwort ein, und klicken Sie auf Verbinden.

💐 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

Überprüfen

Schritt 1: Öffnen Sie erneut die Registerkarte **Netzwerke**, wählen Sie das Netzwerk aus (in diesem Beispiel mit dem Namen VPDN), und überprüfen Sie, ob der Status Verbunden ist.



Schritt 2: Öffnen Sie die Eingabeaufforderung, und führen Sie den Befehl ipconfig /all aus.

PPP adapter VPDN:	
Connection-specific DNS Suffix	ix . :
Description	: VPDN
Physical Address	:
DHCP Enabled	: No
Autoconfiguration Enabled	: Yes
IPv4 Address	: : 10.1.1.9(Preferred)
Subnet Mask	: 255.255.255.255
Default Gateway	: 0.0.0.0
DNS Servers	: 4.2.2.1
	4.2.2.2
NetBIOS over Tcpip	: Enabled

IPv4-Adresse und Domian Name Server (DNS) werden vom Aggregator nach Abschluss der Phase des PPP Internet Protocol Control Protocol (IPCP) zugewiesen.

Schritt 3: Führen Sie den Befehl **debug ppp negotiation** aus, und die anderen show-Befehle auf dem 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	caller ip				
Line	User	IP Address	Local Number	Remote Numb	er <->
Vi3.1	-	10.1.1.9	-	-	in
Aggregator#show ip interface brief exclude un					
Interface	IP-	Address	OK? Method Status		Protocol
GigabitEthernet	0/0/1 192	.168.1.1	YES manual up		up
Loopback100	172	.16.1.1	YES manual up		up
Schritt 4: Überprüfen Sie, ob der Windows-Computer das Remote-Netzwerk hinter dem					

Aggregator erreichen kann (in diesem Fall Loopback 100-Schnittstelle).

```
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
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- VPDN im Überblick
- <u>TTechnischer Support und Dokumentation Cisco Systems</u>