Configurazione del tunnel L2TP tra un computer Windows e un router Cisco

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Esempio di rete Configurazioni Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene descritto come configurare un tunnel Layer 2 Tunneling Protocol (L2TP) tra un computer Windows e un router Cisco.

Prerequisiti

Requisiti

Cisco consiglia di essere a conoscenza del fatto che il computer Windows può eseguire il ping dell'indirizzo IP dell'interfaccia fisica sul router.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Configurazione aggregatore:

Di seguito è riportato un esempio della configurazione di Aggregator:

```
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
```

Configurazioni e impostazioni del computer Windows

Attenersi alla seguente procedura:

Passaggio 1. Aprire **Centro connessioni di rete e condivisione** e fare clic su **Configura una nuova connessione o rete** come mostrato nell'immagine.

💽 🗢 👯 « Network and Inte	rnet Network and Sharing Center	- 	Search Control Panel	٩
Control Panel Home	View your basic network informat	ion and set	up connections	0
Change adapter settings Change advanced sharing settings	ADMIN-PC Net (This computer) View your active networks Network 5 Work network	work 5	Local Area	See full map nnect or disconnect Connection 5
	Change your networking settings			
	Connect to a network Connect or reconnect to a wireless Choose homegroup and sharing o	 Connect to a network Connect or reconnect to a wireless, wired, dial-up, or VPN network connection. Choose homegroup and sharing options 		
See also HomeGroup Internet Options Windows Firewall	Access files and printers located o Troubleshoot problems Diagnose and repair network prob	Access files and printers located on other network computers, or change sharing settings. Troubleshoot problems Diagnose and repair network problems, or get troubleshooting information.		

Passaggio 2. Selezionare Connetti a una rete aziendale e fare clic su Avanti

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.	
<u>N</u> e	xt Cancel

Passaggio 3. Selezionare Usa connessione Internet (VPN)



Passaggio 4. Immettere l'indirizzo IP dell'aggregatore (in questo caso 192.168.1.1), assegnare un nome alla connessione (in questo caso assegnando il nome come VPDN) e fare clic su **Avanti**.

G 🔚 Connect to a Workplace		
Type the Internet add	ress 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 <u>s</u> mart card		
Image: Allow other people to use this connection This 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

Passaggio 5. Immettere il nome utente e la password e fare clic su Connetti

🚱 🗽 Connect to a Wo	orkplace	
Type your user	name and password	
<u>U</u> ser name:	cisco]
<u>P</u> assword:	•••••	
	Show characters Remember this password	
<u>D</u> omain (optional):		
		Connect Cancel

Passaggio 6. Verificare nome utente e password



Passaggio 7. Potrebbe verificarsi un errore per la prima volta, come mostrato nell'immagine.

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> <u> </u> <u> </u>	
Set up the connection anyway	
Diagnose the problem	
	Cancel

Passaggio 8. Fare clic su Configura comunque la connessione e aprire la scheda Reti.



Passaggio 9. Fare clic con il pulsante destro del mouse sulla connessione (qui VPDN) e fare clic su **Proprietà**. Verificare l'indirizzo IP dell'aggregatore (qui 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			

Passaggio 10. Passare a **Options>PPP Settings** (Opzioni>**Impostazioni PPP)** e verificare le impostazioni, come mostrato nell'immagine.

VPDN Properties		
General Options Security Networking Sharing Dialing options Image: Connecting Image: Connecting <t< td=""></t<>		
PPP Settings		
Enable LCP extensions Enable software compression Negotiate multi-link for single-link connections OK Cancel		
PPP Settings		
OK Cancel		

Passaggio 11. Passare a Security >Type of VPN > Layer 2 Tunneling Protocol with IPsec, come mostrato nell'immagine.

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

Passaggio 12. Selezionare l'opzione **Nessuna crittografia consentita** nel menu a discesa Crittografia dati:

🔋 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			

Passaggio 13. Deselezionare Microsoft CHAP versione 2 e fare clic su 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		
OK Cancel		

Passaggio 14. Aprire la rete (qui VPDN) e fare clic su Connect (Connetti).



Passaggio 15. Inserire il nome utente e la password e fare clic su Connect (Connetti)

💐 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		

Verifica

Passaggio 1. Aprire nuovamente la scheda **Reti**, selezionare la rete (in questo esempio la VPDN) e verificare che lo stato sia Connesso.



Passaggio 2. Aprire il prompt dei comandi ed eseguire il comando ipconfig /all.

PPP adapter VPDN:	
Connection-specific DNS Suffix	
Description	. : VPDN
Physical Address	
DHĈP 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

L'indirizzo IPv4 e il DNS (Domain Name Server) vengono assegnati dall'aggregatore dopo il completamento della fase IPCP (Internet Protocol Control Protocol).

Passaggio 3. Eseguire il comando debug ppp negotiation e gli altri comandi show su 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 Number	<->
Vi3.1	-	10.1.1.9	_	-	in
Aggregator#show ip interface brief exclude un					
Interface	IP-	Address	OK? Method Status	P	rotocol
GigabitEthernet0/0/1 192		.168.1.1 Y	YES manual up	up	
Loopback100	172	.16.1.1	YES manual up	u	p

Passaggio 4. Verificare se il computer Windows può raggiungere la rete remota dietro Aggregator (in questo caso interfaccia Loopback 100)

```
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
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Informazioni sulla VPDN
- <u>TDocumentazione e supporto tecnico Cisco Systems</u>