Suggerimenti per l'installazione di Cisco QuickVPN per i sistemi operativi Windows

Per un video che mostra i suggerimenti per l'installazione su Quick VPN, visitare il sito <u>http://youtu.be/hHu2z6A78N8</u>

Obiettivo

Cisco QuickVPN è un software gratuito progettato per l'accesso remoto a una rete. È facile da installare su un PC e da gestire. QuickVPN è compatibile con il sistema operativo Windows (versioni a 32 bit e a 64 bit). Affinché QuickVPN funzioni correttamente, è necessario verificare una serie di requisiti per garantire la connettività VPN con la rete.

Questo articolo spiega i requisiti e i suggerimenti per la corretta esecuzione di QuickVPN, nonché una spiegazione di come QuickVPN ottiene l'accesso alla rete.

Dispositivi interessati

RV215W RV110W · RV180 / RV180W RV120W RV220W · RV016 RV042/RV042G RV082 · RVS4000 · SA520/SA520W SA540 WRV200 WRV210 WRV210 WRVS4400N · Windows XP, Windows Vista, Windows 7

Processo QuickVPN

Di seguito è riportata una spiegazione del funzionamento di QuickVPN nel computer e dei

motivi per cui è importante soddisfare i requisiti prima di eseguire QuickVPN.

1. Il client si connette al router utilizzando SSL (Secure Sockets Layer). La connessione utilizza il numero di porta 443 o 60443 (a seconda della configurazione VPN sul router) e cerca un certificato. Per ulteriori informazioni, fare riferimento alla sezione <u>Requisiti del</u> <u>router</u>.

Nota: se si utilizza un certificato, verificare che sia stato salvato nel computer. In caso contrario, fare clic su No per non utilizzare un certificato quando viene visualizzato il messaggio di avviso del certificato.

2. Il nome utente e la password del client vengono autenticati dal router. Una volta autenticato l'utente, viene stabilito il tunnel IPSec.

Nota: se non è possibile accedere alla VPN, verrà visualizzato un messaggio di errore.

3. Il client invia un pacchetto di richiesta echo ICMP all'indirizzo IP interno del router. Il router risponde con un pacchetto di risposta echo ICMP. Lo scopo è quello di stabilire una connettività tra entrambe le estremità. Per questo motivo, è necessario accertarsi (a seconda del sistema operativo in uso) di impostare i requisiti appropriati per ICMP. Per ulteriori informazioni, fare riferimento alla sezione Requisiti del sistema operativo Windows Vista/Windows 7.

Nota: se la connessione non riesce, viene visualizzato un messaggio di errore Gateway remoto che non risponde.

Requisiti del router

Di seguito è riportato un elenco di requisiti che il router per piccole imprese deve soddisfare.

- · La gestione remota deve essere abilitata per le porte 443 e 60443.
- · Gli utenti devono creare e abilitare il tunnel VPN.

· Il nome utente e la password fanno distinzione tra maiuscole e minuscole e devono corrispondere in entrambe le estremità della connessione.

· È consentita una sola connessione per account utente.

· La subnet della rete locale deve essere diversa dalla subnet della rete remota.

 \cdot Se si utilizza un certificato, il file del certificato deve essere salvato nel computer nella cartella QuickVPN Client.

Requisiti del sistema operativo Windows Vista / Windows 7

Passaggio 1. Se nel computer è installato Windows Vista, è necessario disporre della compatibilità con Service Pack 2 o Vista Service Pack 2 per Windows 7. Per verificare questa condizione, scegliere Start > Proprietà del computer. Se nel computer è installato Windows 7, ignorare questo passaggio.

Nota: se in Windows Vista non è installato il Service Pack, scegliere Start > Tutti i programmi > Windows Update per aggiornare il sistema.



Passaggio 2. Windows Firewall deve essere attivato. Per verificare questa condizione, scegliere Start > Pannello di controllo > Sistema e sicurezza > Windows Firewall.



Passaggio 3. È necessario creare una regola per consentire le trasmissioni di pacchetti ICMP (Internet Control Message Protocol). A tale scopo, scegliere Start > Pannello di controllo > Sistema e sicurezza > Windows Firewall > Impostazioni avanzate. Verrà visualizzata la finestra Windows Firewall con protezione avanzata:

Windows Firewall wit	th Advanced Security		
File Action View	Help		
Windows Firewall w Inbound Rules Outbound Rules Connection 1 Monitoring	ith Advance New Rule Filter by Profile Filter by State Filter by Group View Refresh Export List Help	 Rules TCP-In) JDP-In) Desktop Soft Desktop Soft	Actions Inbound Rules Inbound Rules New Rule Filter by Profile Filter by State Filter by Group View Refresh Export List
<	► Solution	our Service	

Passaggio 4. Fare clic con il pulsante destro del mouse su Regole in entrata e scegliere Nuova regola. Verrà visualizzata la pagina Creazione guidata nuova regola connessioni in entrata:

Prev Inbound Rule Wizard	
Rule Type Select the type of firewall rule to o	create.
Rule Type Select the type of firewall rule to of Steps: Rule Type Program Protocol and Ports Scope Action Profile Name	create. What type of rule would you like to create? Program Rule that controls connections for a program. Pot Rule that controls connections for a TCP or UDP pot. Predefined: Connect to a Network Projector Rule that controls connections for a Windows experience. Custom rule. Leam more about rule types
	< Back Next > Cancel

Passaggio 5. Fare clic su Personalizzato per creare una regola personalizzata.

Mew Inbound Rule Wizard	
Protocol and Ports Specify the protocols and ports t	which this rule applies.
Steps: Rule Type Program	To which ports and protocols does this rule apply?
Protocol and Ports	Protocol type: ICMPv4
ScopeAction	Protocol number: Any Custom HOPOPT
ProfileName	Local port: IGMP TCP UDP IPv6
	Remote port: IPv6-Route IPv6-Frag GRE ICMPv6 IPv6-NoNxt IPv6-Opts
	Internet Control Message (ICMP) settings: VRRP PGM L2TP
	Learn more about protocol and ports
	< Back Next > Cancel

Passaggio 6. Nell'elenco a discesa Protocol Type (Tipo di protocollo), selezionare ICMPv4.

Nota: gli altri campi possono rimanere nella configurazione predefinita.

Prew Inbound Rule Wizard	
Name Specify the name and description	of this rule.
Steps: Program Protocol and Ports Scope Action Profile Name	Name: ICMP Echo Request
	< Back Finish Cancel

Passaggio 7. Nel campo Nome immettere un nome che descriva questa regola.

Passaggio 8. Fare clic su Finish (Fine).

Passaggio 9. Il servizio IPSec deve essere in esecuzione. Per verificare questa condizione, fare clic su Start e nel campo Cerca programmi e file, immettere msconfig. Viene visualizzata la finestra Configurazione di sistema:

ľ				Syste	em Configu	uration	
General	Boot	Services	Startup	Tools			
Start	up select lormal st load all d Diagnostic load bas selective	tion artup device drive c startup ic devices a startup d system se d startup it	rs and service nd service ervices ems	vices s only			
	Use	e original bo	ot configu	ration			

Passaggio 10. Fare clic sulla scheda Servizi per verificare che l'Agente criteri IPSec sia abilitato. Se non è attivato, selezionare la casella di controllo Agente criteri IPSec per consentire il servizio IPSec.

Service			Manufacturer	Status	Date Disabled	^
▼ PNRP Machine Name Publication			Microsoft Corporation	Stopped		
Peer Name Resolution Protocol			Microsoft Corporation	Runnina		
IPsec Policy Agent			Microsoft Corporation	Running)	
✓ Power			Microsoft Corporation	Running		
✓ Printer Extensions and Notificati			Microsoft Corporation Stopped			
✓ Quality W	indows Audio	Video Ex	Microsoft Corporation	Stopped		
✓ Remote A	ccess Auto C	connection	Microsoft Corporation	Stopped		
Remote A	ccess Conne	ction Man	Microsoft Corporation	Stopped		
 RPC Endpoint Mapper 		Microsoft Corporation	Running			
Remote Procedure Call (RPC) Lo		Microsoft Corporation	Stopped			
 Security Accounts Manager 			Microsoft Corporation	Running		
✓ Task Sche	duler		Microsoft Corporation	Runnina		~
Note that some secure Microsoft services may not be disabled.			Enable	all Disable	all	

Passaggio 11. Fare clic su Apply (Applica) per salvare le impostazioni.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).