Consejos de instalación de Cisco QuickVPN para sistemas operativos Windows

Para ver un vídeo que muestra sugerencias de instalación de Quick VPN, visite <u>http://youtu.be/hHu2z6A78N8</u>

Objetivo

Cisco QuickVPN es un software gratuito diseñado para el acceso remoto a una red. Es fácil de instalar en un PC y fácil de gestionar. QuickVPN es compatible con el sistema operativo Windows (tanto la edición de 32 bits como la de 64 bits). Para que QuickVPN funcione correctamente, se debe desactivar un conjunto de requisitos para garantizar la conectividad VPN con la red.

En este artículo se explican los requisitos y sugerencias para ejecutar correctamente QuickVPN, así como una explicación de cómo QuickVPN obtiene acceso a su red.

Dispositivos aplicables

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

Proceso QuickVPN

La siguiente es una explicación de cómo actúa QuickVPN en su computadora y por qué es importante cumplir con los requisitos antes de intentar ejecutar QuickVPN.

1. El cliente se conecta al router mediante SSL (Secure Socket Layer). La conexión utiliza el número de puerto 443 o 60443 (según la configuración de VPN del router) y busca un certificado. Para obtener más información, consulte la sección <u>*Requisitos del router*</u>.

Nota: Si utiliza un certificado, asegúrese de que está guardado en el equipo. De lo contrario, haga clic en **No** para no utilizar un certificado cuando aparezca el mensaje de advertencia del certificado.

2. El router autentica el nombre de usuario y la contraseña del cliente. Una vez autenticado el usuario, se establece el túnel IPSec.

Nota: Si no puede iniciar sesión en la VPN, recibirá un mensaje de error.

3. El cliente envía un paquete de solicitud de eco ICMP a la dirección IP interna del router. El router responde con un paquete de respuesta de eco ICMP. El propósito es establecer la conectividad entre ambos extremos. Esta es la razón por la que debe asegurarse (dependiendo de su sistema operativo) de establecer los requisitos adecuados para ICMP. Para obtener más información, consulte la sección *Requisitos del sistema operativo Windows Vista / Windows 7*.

Nota: si la conexión falla, aparecerá el mensaje de error El gateway remoto no responde.

Requisitos del router

A continuación se incluye una lista de los requisitos que debe cumplir su router para pequeñas empresas.

- · La administración remota debe estar habilitada para los puertos 443 y 60443.
- · Los usuarios deben crear y activar el túnel VPN.

 \cdot El nombre de usuario y la contraseña distinguen entre mayúsculas y minúsculas y deben coincidir en ambos extremos de la conexión.

· Solo se permite una conexión por cuenta de usuario.

 \cdot La subred de la red local debe ser diferente de la subred de la red remota.

 \cdot Si está utilizando un certificado, el archivo del certificado debe guardarse en su computadora en la carpeta Cliente QuickVPN.

Requisitos del sistema operativo Windows Vista / Windows 7

Paso 1. Si el ordenador tiene Windows Vista, debe tener instalada la compatibilidad con Service Pack 2 o Vista Service Pack 2 para Windows 7. Para comprobarlo, elija **Inicio > Propiedades del sistema informático**. Si su equipo tiene Windows 7, omita este paso.

Nota: Para Windows Vista, si no tiene el Service Pack instalado, elija Inicio > Todos los programas > Windows Update para actualizar el sistema.

System	✓ Search	٩
Tasks Image: Device Manager Remote settings System protection Advanced system settings	View basic information Windows edition Windows Vista™ Ultima Copyright © 2007 Micro Service Pack 2	on about your com
See also Windows Update Security Center Performance	System Rating: Processor: Memory (RAM): System type: Computer name, domain, a Computer name:	Pentium(R) Dual-Co 1.00 GB 32-bit Operating Sy and workgroup settings – WIN-WYIN8UCKRZI 🕶

Paso 2. El Firewall de Windows debe estar activado. Para comprobarlo, elija **Inicio > Panel de control > Sistema y seguridad > Firewall de Windows**.



Paso 3. Se debe crear una regla para permitir las transmisiones de paquetes ICMP (protocolo de mensajes de control de Internet). Para ello, elija **Inicio > Panel de control > Sistema y seguridad > Firewall de Windows > Configuración avanzada**. Se abre la ventana *Firewall de Windows con seguridad avanzada*:



Paso 4. Haga clic con el botón derecho en Inbound Rules y elija New Rule. Se abre la página

Asistente para nueva regla entrante:



Paso 5. Haga clic en Custom para crear una regla personalizada.

Prew Inbound Rule Wizar	d		
Protocol and Ports Specify the protocols and ports	to which this rule applies.		
Steps: Program	To which ports and pro	tocols does this rule apply?	
Protocol and Ports	Protocol type:	ICMPv4	
ScopeAction	Protocol number:	Any Custom HOPOPT	
ProfileName	Local port:	CICMPv4 TGMP TCP	Ρ
	Remote port:	IPv6 IPv6-Route IPv6-Frag GRE ICMPv6 IPv6 No.Net	
	Internet Control Messa (ICMP) settings:	IPV6-Notxa IPv6-Opts VRRP PGM L2TP	
	Learn more about proto	ocol and ports	
	<	Back Next > Can	cel

Paso 6. En la lista desplegable Protocol Type , elija ICMPv4.

Nota: Los demás campos pueden permanecer como configuración predeterminada.

Prew Inbound Rule Wizard	ł
Name Specify the name and descriptio	n of this rule.
Steps:	
Rule Type	
Program	
Protocol and Ports	
Scope	Name:
Action	
Profile	Description (optional):
Name	
	< Back Finish Cancel

Paso 7. En el campo Nombre, introduzca un nombre que describa esta regla.

Paso 8. Haga clic en Finish (Finalizar).

Paso 9. Debe tener el servicio IPSec en ejecución. Para marcar esto, haga clic en **Inicio** y en el campo Buscar programas y archivos, ingrese **msconfig**. Se abre la ventana *System Configuration*:

				Syster	n Configu	ration		
General	Boot	Services	Startup	Tools				
Start ON	up select ormal st .oad all d	tion artup levice driver	s and ser	vices				
	iagnostio .oad bas	c startup ic devices ar	nd service	s only				
۰s	elective	startup od system se	rvices					
	Loa	id startup ite	ems					
	Use	e original boo	ot configu	ration				
					ОК	Cancel	Apply	Help

Paso 10. Haga clic en la pestaña **Servicios** para asegurarse de que el Agente de políticas IPSec está habilitado. Si no está habilitada, active la casilla de verificación **Agente de directivas IPSec** para permitir el servicio 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 Windows Audio Video Ex	Microsoft Corporation	Stopped		
Remote Access Auto Connection	Microsoft Corporation	Stopped		1
Remote Access Connection 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 Scheduler	Microsoft Corporation	Runnina		4
Note that some secure Microsoft service:	s may not be disabled.	Frahla	-II Disable a	

Paso 11. Haga clic en Apply para guardar la configuración.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).