# Utilizzare Show Soft VPN Client per connettersi con IPSec VPN Server su RV130 e RV130W

### Obiettivo

La VPN IPSec (Virtual Private Network) consente di ottenere risorse remote in modo sicuro tramite la creazione di un tunnel crittografato su Internet.

RV130 e RV130W funzionano come server VPN IPSec e supportano il client Shrew Soft VPN.

Accertarsi di scaricare l'ultima versione del software client.

·Mostrare Soft (https://www.shrew.net/download/vpn)

**Nota:** Per configurare correttamente il client VPN Show Soft con un server VPN IPSec, è necessario innanzitutto configurare il server VPN IPSec. Per informazioni su come eseguire questa operazione, fare riferimento all'articolo <u>Configurazione di un server VPN IPSec su</u> <u>RV130 e RV130W.</u>

L'obiettivo di questo documento è mostrare come utilizzare il client Show Soft VPN per connettersi a un server VPN IPSec sui modelli RV130 e RV130W.

### Dispositivi interessati

·RV130W Wireless-N VPN Firewall

·RV130 VPN Firewall

#### Requisiti di sistema

·Sistemi a 32 o 64 bit

Windows 2000, XP, Vista o Windows 7/8

### Topologia

Di seguito è riportata una topologia di livello superiore che illustra i dispositivi coinvolti nella configurazione di un client Shrewsoft per il sito.



Di seguito è riportato un diagramma di flusso più dettagliato che illustra il ruolo dei server DNS in un ambiente di rete per piccole imprese.



## Versione del software

•1.0.1.3

### Configurazione client VPN avanzata

#### Configurazione e configurazione utente della VPN IPSec

Passaggio 1. Accedere all'utility di configurazione Web e scegliere VPN > Server VPN IPSec > Configurazione. Viene visualizzata la pagina *Setup* (Impostazione).

Setup		
Server Enable:		
NAT Traversal:	Disabled Edit	
Phase 1 Configuration		
Pre-Shared Key:	Testkey	]
Exchange Mode:	Main 👻	
Encryption Algorithm:	DES 👻	
Authentication Algorithm:	MD5 🗸	
DH Group:	Group1 (768 bit) 👻	
IKE SA Life Time:	3600	Seconds (Range: 30 - 86400, Default: 3600)
Phase 2 Configuration		
Local IP:	Subnet 👻	
IP Address:	192.168.1.0	(Hint: 1.2.3.4)
Subnet Mask:	255.255.255.0	(Hint: 255.255.255.0)
IPSec SA Lifetime:	28800	Seconds (Range: 30 - 86400, Default: 28800)
Encryption Algorithm:	DES 👻	
Authentication Algorithm:	MD5 👻	
PFS Key Group:	Enable	
DH Group:	Group 1(768 bit) 👻	
Save Cancel		

<u>Passaggio 2.</u> Verificare che il server VPN IPSec per RV130 sia configurato correttamente. Se il server VPN IPSec non è configurato o non è configurato correttamente, vedere <u>Configurazione di un server VPN IPSec sugli switch RV130 e RV130W</u> e fare clic su **Salva**.

Setup			
Connguration setti			
Server Enable:			
NAT Traversal:	Disabled Edit		
Phase 1 Configuration			
Pre-Shared Key:	Testkey		
Exchange Mode:	Main 👻		
Encryption Algorithm:	DES -		
Authentication Algorithm:	MD5 -		
DH Group:	Group1 (768 bit) -		
IKE SA Life Time:	3600 Seconds (Range: 30 - 86400, Default: 3600)		
Phase 2 Configuration			
Local IP:	Subnet -		
IP Address:	192.168.1.0 (Hint: 1.2.3.4)		
Subnet Mask:	255.255.255.0 (Hint: 255.255.255.0)		
IPSec SA Lifetime:	28800 Seconds (Range: 30 - 86400, Default: 28800)		
Encryption Algorithm:	DES -		
Authentication Algorithm:	MD5 -		
PFS Key Group:	🗹 Enable		
DH Group:	Group 1(768 bit) -		
Save Cancel			

**Nota:** Le impostazioni precedenti sono un esempio di configurazione di un server VPN IPSec RV130/RV130W. Le impostazioni sono basate sul documento <u>Configurazione di un server</u> <u>VPN IPSec su RV130 e RV130W</u> e verranno usate nei passaggi successivi.

Passaggio 3. Passare a VPN > IPSec VPN Server > Utente. Viene visualizzata la pagina *User*.

User		
liser årcount Table		
UserName	Password	
No data to display		
Aud Ruw Edit Delete Import		
Save Cancel		

<u>Passaggio 4.</u> Fare clic su **Aggiungi riga** per aggiungere gli account utente utilizzati per autenticare i client VPN (autenticazione estesa) e immettere il nome utente e la password desiderati negli appositi campi.

User			
You must save before you can edit or delete.			
User Account Table			
UserName	Password		
TestUser	•••••		
Add Row Edit Delete Import			
Save Cancel			

Passaggio 5. Fare clic su **Save** per salvare le impostazioni.

#### Configurazione client VPN

Passaggio 1. Aprire Show VPN Access Manager e fare clic su **Add** (Aggiungi) per aggiungere un profilo.



Viene visualizzata la finestra Configurazione sito VPN.

VPN Site Configuration		
General Client Name Resolution Authenticatic		
Remote Host		
Host Name or IP Address Port		
I 500		
Auto Configuration ike config pull 🔻		
Local Host		
Adapter Mode		
Use a virtual adapter and assigned address 🔷 💌		
MTU 👽 Obtain Automatically		
1380 Address		
Netmask		
Save Cancel		

Passaggio 2. Nella sezione *Host remoto* della scheda *Generale*, immettere il nome host pubblico o l'indirizzo IP della rete a cui si sta tentando di connettersi.

VPN Site Configuration
General Client Name Resolution Authenticatic
Remote Host Host Name or IR Address
ds - Udd 500
Auto Configuration ike config pull 🔻
Local Host
Adapter Mode
MTU Øbtain Automaticallu
1380 Address
Netmask
Save Cancel

**Nota:** Verificare che il numero di porta sia impostato sul valore predefinito 500. Affinché la VPN funzioni, il tunnel utilizza la porta UDP 500 che deve essere impostata in modo da consentire l'inoltro del traffico ISAKMP nel firewall.

Passaggio 3. Nell'elenco a discesa Configurazione automatica, scegliere disabilitato.

VPN Site Configuration		
General Client Name Resolution	Authenticatic	
Remote Host		
Host Name or IP Address	Port	
12114128	500	
Auto Configuration ike confi	g pull 🔻	
CLocal Host	g pull <sub>.</sub>	
ike config push Adapter Mode dhcp over ipsec		
Use a virtual adapter and assigne	d address 🔻	
MTU 📝 Obtair	n Automatically	
1380 Address .		
Netmask .		
Save	Cancel	

Le opzioni disponibili sono definite come segue:

·Disattivato: disattiva qualsiasi configurazione client automatica.

·IKE Config Pull: consente al client di impostare le richieste da un computer. Se il computer supporta il metodo Pull, la richiesta restituisce un elenco di impostazioni supportate dal client.

·IKE Config Push: fornisce a un computer l'opportunità di offrire impostazioni al client attraverso il processo di configurazione. Se il computer supporta il metodo Push, la richiesta restituisce un elenco di impostazioni supportate dal client.

·DHCP over IPSec: consente al client di richiedere le impostazioni al computer tramite DHCP su IPSec.

Passaggio 4. Nella sezione *Host locale*, scegliere **Utilizza un adattatore esistente e l'indirizzo corrente** nell'elenco a discesa *Modalità adattatore*.

VPN Site Configuration
General Client Name Resolution Authenticatic
Remote Host
Host Name or IP Address Port
13F114fFR 500
Auto Configuration disabled 🔹
CLocal Host
Adapter Mode
Use a virtual adapter and assigned address 🔹
Use a virtual adapter and assigned address Use a virtual adapter and random address
Use an existing adapter and current address
Netmask
Save Cancel

Le opzioni disponibili sono definite come segue:

·Utilizza una scheda virtuale e un indirizzo assegnato - Consente al client di utilizzare una scheda virtuale con un indirizzo specificato come origine per le comunicazioni IPsec.

·Utilizza una scheda virtuale e un indirizzo casuale: consente al client di utilizzare una scheda virtuale con un indirizzo casuale come origine delle comunicazioni IPsec.

·Utilizza una scheda esistente e l'indirizzo corrente: consente al client di utilizzare solo la scheda fisica esistente con l'indirizzo corrente come origine per le comunicazioni IPsec.

Passaggio 5. Fare clic sulla scheda *Client*. Nell'elenco a discesa *NAT Traversal*, selezionare la stessa impostazione configurata sull'RV130/RV130W per NAT Traversal nell'articolo *Configuration of an IPSec VPN Server on RV130 and RV130W*.

VPN Site Configuration	<b>X</b>	
General Client Name Reso	ution Authenticatic	
Firewall Options		
NAT Traversal	disable 🔻	
NAT Traversal Port	disable enable	
Keep-alive packet rate	force-draft force-rfc	
IKE Fragmentation	force-cisco-udp	
Maximum packet size	540 Bytes	
Other Options		
Enable Dead Peer Detection		
Enable ISAKMP Failure Notifications		
Enable Client Login Banner		
Save Cancel		

Le opzioni di menu disponibili per NAT (Network Address Translation) sono definite come segue:

·Disabilita: le estensioni del protocollo NAT non verranno utilizzate.

·Abilita: le estensioni del protocollo NAT verranno utilizzate solo se il gateway VPN indica il supporto durante le negoziazioni e se viene rilevato NAT.

·Force-Draft: la versione bozza delle estensioni del protocollo NAT verrà utilizzata indipendentemente dal fatto che il gateway VPN indichi o meno il supporto durante le negoziazioni o che venga rilevato NAT.

·Force-RFC: la versione RFC del protocollo NAT verrà utilizzata indipendentemente dal fatto che il gateway VPN indichi o meno il supporto durante le negoziazioni o che sia stato rilevato NAT.

·Force-Cisco-UDP: forza l'incapsulamento UDP per i client VPN senza NAT.

Passaggio 6. Fare clic sulla scheda *Risoluzione nomi* e selezionare la casella di controllo **Abilita DNS** se si desidera abilitare il DNS. Se per la configurazione del sito non sono necessarie impostazioni DNS specifiche, deselezionare la casella di controllo **Abilita DNS**.

VPN Site Configuration		
Client Name Resolution	Authentication Phase	
DNS Split DNS WI	NS	
Enable DNS	Obtain Automatically	
Server Address #1		
Server Address #2		
Server Address #3		
Server Address #4		
DNS Suffix	Obtain Automatically	
	Save Cancel	

Passaggio 7. (Facoltativo) Se il gateway remoto è configurato per supportare Configuration Exchange, il gateway è in grado di fornire automaticamente le impostazioni DNS. In caso contrario, verificare che la casella di controllo **Ottieni automaticamente** sia deselezionata e immettere manualmente un indirizzo server DNS valido.

VPN	Site Configuration	
Cli	ient Name Resolution	Authentication Phase
lГ	DNS WINS	
	🔽 Enable DNS	Obtain Automatically
	Server Address #1	
	Server Address #2	
	Server Address #3	
	Server Address #4	
	DNS Suffix	Obtain Automatically
	(	Save Cancel

Passaggio 8. (Facoltativo) Fare clic sulla scheda *Risoluzione nome*, selezionare la casella di controllo **Abilita WINS** se si desidera abilitare Windows Internet Name Server (WINS). Se il gateway remoto è configurato per supportare Configuration Exchange, il gateway è in grado di fornire automaticamente le impostazioni WINS. In caso contrario, verificare che la casella di controllo **Ottieni automaticamente** sia deselezionata e immettere manualmente un indirizzo di server WINS valido.

VPN Site Configuration	<b></b>
Client Name Resolution	Authentication Phase
DNS Split DNS WI	NS
Enable WINS	Obtain Automatically
Server Address #1	
Server Address #2	
(	Save Cancel

**Nota:** Fornendo informazioni sulla configurazione di WINS, un client sarà in grado di risolvere i nomi WINS utilizzando un server situato nella rete privata remota. Ciò è utile quando si tenta di accedere a risorse di rete di Windows remote utilizzando un nome percorso Uniform Naming Convention. Il server WINS appartiene in genere a un controller di dominio di Windows o a un server Samba.

Passaggio 9. Fare clic sulla scheda *Authentication* (Autenticazione) e selezionare **Mutual PSK + XAuth** nell'elenco a discesa *Authentication Method* (Metodo di autenticazione).

VPN Site Configuration	×
Client Name Resolution	Authentication Phase
Authentication Method	Mutual PSK + XAuth 🛛 🗸
Local Identity Remote	Hybrid RSA + XAuth Hybrid GRP + XAuth Mutual RSA + XAuth
Identification Type	Mutual PSK + XAuth
IP Address	Mutual RSA
Address String	ocal host address
	Save Cancel

Le opzioni disponibili sono definite come segue:

·Hybrid RSA + XAuth: credenziali client non necessarie. Il client autenticherà il gateway. Le credenziali saranno nel formato dei file di certificato PEM o PKCS12 o del tipo dei file di chiave.

·Hybrid GRP + XAuth: credenziali client non necessarie. Il client autenticherà il gateway. Le credenziali saranno sotto forma di file di certificato PEM o PKCS12 e di una stringa segreta condivisa.

·RSA + XAuth reciproci: client e gateway richiedono entrambi credenziali per l'autenticazione. Le credenziali saranno in formato PEM o PKCS12, file di certificato o tipo di chiave.

·PSK reciproco + XAuth: il client e il gateway richiedono entrambi credenziali per l'autenticazione. Le credenziali saranno in forma di stringa segreta condivisa.

·RSA reciproca: client e gateway richiedono entrambi credenziali per l'autenticazione. Le credenziali saranno in formato PEM o PKCS12, file di certificato o tipo di chiave.

·PSK reciproco: il client e il gateway richiedono entrambi credenziali per l'autenticazione. Le credenziali saranno in forma di stringa segreta condivisa.

Passaggio 10. Nella sezione *Autenticazione*, fare clic sulla scheda secondaria *Credenziali* e immettere la stessa chiave precondivisa configurata nella pagina *IPsec VPN Server Setup* del campo *Chiave precondivisa*.

VPN Site Configuration
Client Name Resolution Authentication Phase
Authentication Method Mutual PSK + XAuth
Local Identity Remote Identity Credentials
Server Certificate Autority File
Client Certificate File
Client Private Key File
Pre Shared Key
Save Cancel

Passaggio 11. Fare clic sulla scheda *Fase 1*. Configurare i seguenti parametri in modo che abbiano le stesse impostazioni configurate per RV130/RV130W nel <u>passaggio 2 della</u> sezione <u>IPSec VPN Server User Configuration</u> di questo documento.

VPN Site Configuration	×
Name Resolution Authen	tication Phase 1 Pha:
Proposal Parameters —	
Exchange Type	main 🔻
DH Exchange	group 1 🔹
Cipher Algorithm	des 🔻
Cipher Key Length	- Bits
Hash Algorithm	md5 🔹
Key Life Time limit	3600 Secs
Key Life Data limit	0 Kbytes
Enable Check Point Compatible Vendor ID	
ſ	

I parametri in Shrew Soft devono corrispondere alle configurazioni RV130/RV130W nella fase 1 come segue:

·"Exchange Type" deve corrispondere a "Exchange Mode".

"DH Exchange" deve corrispondere a "DH Group".

"Cipher Algorithm" deve corrispondere a "Encryption Algorithm".

·"Hash Algorithm" deve corrispondere a "Authentication Algorithm".

Passaggio 12. (Facoltativo) Se il gateway offre un ID fornitore compatibile con Cisco durante le negoziazioni della fase 1, selezionare la casella di controllo **Abilita ID fornitore compatibile con checkpoint**. Se il gateway non funziona o non si è certi, lasciare deselezionata la casella di controllo.

VPN Site Configuration	×
Name Resolution Authent	ication Phase 1 Pha:
Proposal Parameters	
Exchange Type	main 🔻
DH Exchange	group 1 🔹
Cipher Algorithm	des 💌
Cipher Key Length	Bits
Hash Algorithm	md5 💌
Key Life Time limit	3600 Secs
Key Life Data limit	0 Kbytes
Enable Check Point Compatible Vendor ID Save Cancel	

Passaggio 13. Fare clic sulla scheda *Fase 2*. Configurare i seguenti parametri in modo che abbiano le stesse impostazioni configurate per RV130/RV130W nel <u>passaggio 2 della</u> sezione <u>IPSec VPN Server User Configuration</u> di questo documento.

VPN Site Configuration	×
Authentication Phase 1	Phase 2 Policy
Proposal Parameters Transform Algorithm	(esp-des
Transform Key Length	- Bits
HMAC Algorithm	md5 🔹
PFS Exchange	group 1 🔻
Compress Algorithm	disabled 🔹
Key Life Time limit	28800 Secs
Key Life Data limit	0 Kbytes
[(	Save Cancel

I parametri in Shrew Soft devono corrispondere alle configurazioni RV130/RV130W nella fase 2 come segue:

"Transform Algorithm" deve corrispondere a "Encryption Algorithm".

"HMAC Algorithm" deve corrispondere a "Authentication Algorithm".

·PFS "Exchange" deve corrispondere a "DH Group" se PFS Key Group è abilitato su RV130/RV130W. In caso contrario, selezionare **Disattivato**.

"Key Life Time limit" deve corrispondere a "IPSec SA Lifetime".

Passaggio 14. Fare clic sulla scheda *Criterio* e selezionare **obbligatorio** nell'elenco a discesa *Livello di generazione criteri*. L'opzione *Policy Generation Level* (Livello di generazione criteri) consente di modificare il livello di generazione dei criteri IPSec. I diversi livelli forniti nell'elenco a discesa corrispondono ai comportamenti di negoziazione delle associazioni di protezione IPSec implementati da diverse implementazioni di fornitori.

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy   IPSEC Policy Configuration Policy Generation Level require   Maintain Persistent Security auto require   Obtain Topology Automatic unique shared   Remote Network Resource Add Modify Delete
Save Cancel

Le opzioni disponibili sono definite come segue:

·Automatico: il client determina automaticamente il livello di criteri IPSec appropriato.

•Richiedi: il client non negozierà un'associazione di sicurezza (SA) univoca per ogni criterio. I criteri vengono generati utilizzando l'indirizzo pubblico locale come ID dei criteri locali e le risorse di rete remota come ID dei criteri remoti. La proposta per la fase 2 utilizzerà gli ID dei criteri durante la negoziazione.

·Univoco: il client negozia un'associazione di protezione univoca per ogni criterio.

•Condiviso: le policy vengono generate al livello richiesto. La proposta per la fase 2 utilizzerà l'ID del criterio locale come ID locale e Any (0.0.0.0/0) come ID remoto durante la negoziazione.

Passaggio 15. Deselezionare la casella di controllo **Ottieni topologia automaticamente o Tunnel tutto**. Questa opzione modifica la modalità di configurazione dei criteri di sicurezza per la connessione. Quando è disattivato, è necessario eseguire la configurazione manuale. Se questa opzione è abilitata, viene eseguita la configurazione automatica.

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy
IPSEC Policy Configuration
Policy Generation Level require 🔻
Maintain Persistent Security Associations
Dobtain Topology Automatically or Tunnel All
Remote Network Resource
Add Modify Delete
Save Cancel
Save Cancel

Passaggio 16. Per aggiungere la risorsa di rete remota a cui si desidera connettersi, fare clic su **Add** (Aggiungi). Le risorse di rete remote includono l'accesso remoto ai desktop, le risorse di reparto, le unità di rete e la posta elettronica protetta.

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy
IPSEC Policy Configuration
Policy Generation Level require 🔻
Maintain Persistent Security Associations
Obtain Topology Automatically or Tunnel All
Remote Network Resource
Add Modify Delete
Save Cancel

Viene visualizzata la finestra Voce topologia:

VPN Site Configuration	
Authentication Phase 1 Phase 2 Policy   IPSEC Policy Configuration Policy Generation Level require   Policy Generation Level require Image: Configuration   Type Include X   Address X X   Netmask X X	
Add Modify Delete	
Save Cancel	

Passaggio 17. Nel campo *Address* (Indirizzo), immettere l'ID subnet della RV130/RV130W. L'indirizzo deve corrispondere al campo *IP Address* nel <u>passaggio 2 della</u> sezione <u>IPSec</u> <u>VPN Server Setup and User Configuration</u> di questo documento.

VPN Site Configuration	
Authentication Phase 1 Phase 2 Policy   IPSEC Policy Configuration Policy Generation Level require   Policy Generation Level require Image: Configuration   Topology Entry X X   Type Include X   Address 192.168.1.0 Netmask   Ok Cancel Image: Concel	
Add Modify Delete	
Save Cancel	

Passaggio 18. Nel campo *Netmask*, immettere la subnet mask della rete locale dell'RV130/RV130W. La netmask deve corrispondere al campo *Subnet Mask* nel <u>passaggio</u> <u>2 della</u> sezione <u>IPSec VPN Server User Configuration</u> in questo documento.

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy   IPSEC Policy Configuration Policy Generation Level require   Policy Generation Level require Topology Entry   Type Include Address 192.168.1.0   Netmask 255.255.255.0 Ok
Add Modify Delete

Passaggio 19. Fare clic su **OK** per completare l'aggiunta della risorsa di rete remota.

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy   IPSEC Policy Configuration   Policy Generation Level require   Topology Entry   Type   Address 192.168.1.0   Netmask 255.255.255.0
Add Modify Delete
Save Cancel

Passaggio 20. Fare clic su **Save** per salvare le configurazioni per la connessione al sito VPN.

VPN Site Configu	iration			×
Authentication	Phase 1	Phase 2	Policy	••
- IPSEC Policy	Configura	tion		
Policy Gene	ration Leve	el re	quire	•
📃 📃 Maintain	Persistent	Security A:	ssociation	ns
📄 Obtain T	opology Au	utomatically	or Tunn	el All
Remo	e Network	Resource		
<b>↔</b> 192.1	68.1.0 / 25	5.255.255.	0	
Add		4odify	Del	ete
		Caus		Cancel
		Save		Cancer

Passaggio 21. Tornare alla finestra *VPN Access Manager* per selezionare il sito VPN configurato e fare clic sul pulsante **Connect**.

🕑 VPN Acc	ess Ma	nager			
File Edit	View	Help			
	•	2	0		
Connect	Add	Modify	Delete		
8					
19116-003	н				

Viene visualizzata la finestra VPN Connect.

🐼 VPN Connect - 💵 💵 🖬 💶 📼 🗙
Connect Network
config loaded for site 38 3085
Credentials
Username
Password
Connect Exit

Passaggio 2. Nella sezione *Credenziali*, immettere il nome utente e la password dell'account configurato nel <u>passaggio 4 della</u> sezione <u>*Configurazione utente server VPN IPSec*</u> di questo documento.

VPN Connect - Dituite The Connect - Dituite The Connect
Connect Network
config loaded for site ' 🖽 🛛 🖬 🖬 🖬 🖬
Credentials
Username TestUser
Password
Connect Exit

Passaggio 23. Fare clic su Connect to VPN (Connetti a VPN) in RV130/RV130W.

VPN Connect - Dit I 4 11 H	J
Connect Network	
config loaded for site ' 🖽 🖬 🖬 🖬 🖬	
Credentials	
Username TestUser	
Password ••••••	
Connect Exit	

Il tunnel VPN IPSec viene stabilito e il client VPN può accedere alla risorsa sottostante la LAN RV130/RV130W.

S VPN Cor	nect - 1911 4 11 14 - 😐 🗷 🗙				
Connect N	etwork				
esp proposal configured client configured local id configured remote id configured pre-shared key configured bringing up tunnel					
- Credentia	als				
Usernan	ne TestUser				
Passwo	rd				
	Connect Cancel				



Qui è disponibile un video relativo a questo articolo...

Fare clic qui per visualizzare altre Tech Talks di Cisco

#### 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).