Verbindung mit IPSec VPN Server auf RV130 und RV130W über Shrew Soft VPN Client

Ziel

IPSec VPN (Virtual Private Network) ermöglicht die sichere Bereitstellung von Remote-Ressourcen über einen verschlüsselten Tunnel im Internet.

Der RV130 und der RV130W arbeiten als IPSec VPN Server und unterstützen den Shrew Soft VPN Client.

Laden Sie die neueste Version der Client-Software herunter.

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

Anmerkung: Um den Shrew Soft VPN Client erfolgreich mit einem IPSec VPN Server einrichten und konfigurieren zu können, müssen Sie zuerst den IPSec VPN Server konfigurieren. Weitere Informationen hierzu finden Sie im Artikel <u>Konfiguration eines IPSec</u> <u>VPN Servers auf RV130 und RV130W.</u>

In diesem Dokument wird erläutert, wie Sie den Shrew Soft VPN-Client für die Verbindung mit einem IPSec VPN-Server der RV130 und RV130W verwenden.

Unterstützte Geräte

- · RV130W Wireless-N VPN Firewall
- · RV130 VPN-Firewall

Systemanforderungen

- · 32- oder 64-Bit-Systeme
- · Windows 2000, XP, Vista oder Windows 7/8

Topologie

Nachfolgend wird eine Topologie der obersten Ebene dargestellt, die die Geräte veranschaulicht, die an einer Konfiguration zwischen Client und Standort beteiligt sind.



Im Folgenden finden Sie ein detailliertes Flussdiagramm, das die Rolle von DNS-Servern in einer Netzwerkumgebung für kleine und mittlere Unternehmen veranschaulicht.



Software-Version

•1.0.1.3

Shrew Soft VPN-Client einrichten

IPSec-VPN-Einrichtung und -Benutzerkonfiguration

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie VPN > IPSec VPN Server > Setup. Die Seite *Setup* wird geöffnet.

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>Schritt 2:</u> Überprüfen der ordnungsgemäßen Konfiguration des IPSec VPN-Servers für den RV130 Wenn der IPSec VPN Server nicht konfiguriert oder falsch konfiguriert ist, lesen Sie <u>Konfiguration eines IPSec VPN Servers auf RV130 und RV130W</u>, und klicken Sie auf **Speichern**.

Satur	
Setup	
Configuration setti	ings have been saved successfully
	······································
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	

Anmerkung: Die obigen Einstellungen sind ein Beispiel für eine RV130/RV130W IPSec VPN Server-Konfiguration. Die Einstellungen basieren auf dem Dokument "*Configuration of an IPSec VPN Server on RV130 and RV130W*" und werden in den nachfolgenden Schritten beschrieben.

Schritt 3: Navigieren Sie zu VPN > IPSec VPN Server > User. Die Seite *Benutzer* wird angezeigt.

User		
User Account Table		
UserName	Password	
No data to display		
Add Row Edit Delete Import		
Save Cancel		

<u>Schritt 4:</u> Klicken Sie auf **Zeile hinzufügen**, um Benutzerkonten hinzuzufügen, die zur Authentifizierung der VPN-Clients verwendet werden (erweiterte Authentifizierung), und geben Sie den gewünschten Benutzernamen und das gewünschte Kennwort in die dafür vorgesehenen Felder ein.

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

Schritt 5: Klicken Sie auf Speichern, um die Einstellungen zu speichern.

Konfiguration des VPN-Clients

Schritt 1: Öffnen Sie SHREW VPN Access Manager, und klicken Sie auf **Hinzufügen**, um ein Profil hinzuzufügen.



Das Fenster VPN-Standortkonfiguration wird angezeigt.

VPN Site Configuration		
General Client Name Resolution Authenticatic		
Remote Host		
Host Name or IP Address Port		
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		

Schritt 2: Geben Sie im Abschnitt *Remote Host* auf der Registerkarte *General (Allgemein)* den öffentlichen Hostnamen oder die IP-Adresse des Netzwerks ein, mit dem Sie eine Verbindung herstellen möchten.

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

Anmerkung: Stellen Sie sicher, dass die Portnummer auf den Standardwert 500 festgelegt ist. Damit das VPN funktioniert, verwendet der Tunnel den UDP-Port 500, der so festgelegt werden sollte, dass ISAKMP-Datenverkehr an die Firewall weitergeleitet werden kann.

Schritt 3: Wählen Sie in der Dropdown-Liste "*Automatische Konfiguration*" die Option **Deaktiviert aus**.

VPN Site Configuration		
General Client Name Resolution 4	Authenticatic	
Remote Host		
Host Name or IP Address	Port	
1211102	500	
Auto Configuration ike config	pull	
- Local Host ike config	pull_	
Adapter Mode dhcp over ipsec		
Use a virtual adapter and assigned address 🔻		
MTU 📝 Obtain A	Automatically	
1380 Address .		
Netmask .		
Save	Cancel	

Die verfügbaren Optionen sind wie folgt definiert:

· Deaktiviert - Deaktiviert alle automatischen Client-Konfigurationen.

• IKE Config Pull - Ermöglicht das Einstellen von Anforderungen eines Computers durch den Client. Mit der Unterstützung der Pull-Methode durch den Computer gibt die Anforderung eine Liste von Einstellungen zurück, die vom Client unterstützt werden.

• IKE Config Push - Bietet einem Computer die Möglichkeit, dem Client während des Konfigurationsprozesses Einstellungen anzubieten. Mit der Unterstützung der Push-Methode durch den Computer gibt die Anforderung eine Liste von Einstellungen zurück, die vom Client unterstützt werden.

• DHCP Over IPSec - Ermöglicht dem Client, Einstellungen vom Computer über DHCP over IPSec anzufordern.

Schritt 4: Wählen Sie im Abschnitt "*Lokaler Host*" in der Dropdown-Liste "*Adaptermodus*" die Option **Vorhandenen Adapter und aktuelle Adresse verwenden**.

VPN Site Configuration		
General Client Name Resolution Authenticatic		
Remote Host		
Host Name or IP Address Port		
13F114fFP 500		
Auto Configuration disabled 🔹		
Local 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		

Die verfügbaren Optionen sind wie folgt definiert:

• Virtuellen Adapter und zugewiesene Adresse verwenden — Ermöglicht dem Client, einen virtuellen Adapter mit einer angegebenen Adresse als Quelle für seine IPsec-Kommunikation zu verwenden.

• Verwendung eines virtuellen Adapters und einer zufälligen Adresse — Ermöglicht dem Client, einen virtuellen Adapter mit einer zufälligen Adresse als Quelle für seine IPsec-Kommunikation zu verwenden.

• Vorhandenen Adapter und aktuelle Adresse verwenden — Ermöglicht dem Client, nur den vorhandenen physischen Adapter mit der aktuellen Adresse als Quelle für seine IPsec-Kommunikation zu verwenden.

Schritt 5: Klicken Sie auf die Registerkarte *Client*. Wählen Sie in der Dropdown-Liste *NAT Traversal* im Artikel <u>Configuration of an IPSec VPN Server on RV130 and RV130W</u> (Konfiguration eines IPSec VPN Servers auf RV130 und RV130W) die gleiche Einstellung aus, die Sie auf dem RV130W konfiguriert haben.

VPN Site Configuration		
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 Deter	ction	
Enable ISAKMP Failure Notifications		
Enable Client Login Banner		
Save Cancel		

Die verfügbaren NAT-Menüoptionen (Network Address Translation Traversal) sind wie folgt definiert:

· Disable (Deaktivieren) - Die NATT-Protokollerweiterungen werden nicht verwendet.

• Aktivieren - Die NATT-Protokollerweiterungen werden nur verwendet, wenn das VPN-Gateway Unterstützung während der Aushandlung anzeigt und NAT erkannt wird.

• Force-Draft - Die Draft-Version der NATT-Protokoll-Erweiterungen wird verwendet, unabhängig davon, ob das VPN-Gateway Unterstützung bei Verhandlungen anzeigt oder NAT erkannt wird.

 Force-RFC - Die RFC-Version des NATT-Protokolls wird unabhängig davon verwendet, ob das VPN-Gateway Unterstützung während der Aushandlung anzeigt oder ob NAT erkannt wird.

• Force-Cisco-UDP: Erzwingt die UDP-Kapselung für VPN-Clients ohne NAT.

Schritt 6. Klicken Sie auf die Registerkarte *Namensauflösung* und aktivieren Sie das Kontrollkästchen **DNS aktivieren**, wenn Sie DNS aktivieren möchten. Wenn für die Standortkonfiguration keine spezifischen DNS-Einstellungen erforderlich sind, deaktivieren Sie das Kontrollkästchen **DNS aktivieren**.

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

Schritt 7: (Optional) Wenn Ihr Remote-Gateway für die Unterstützung von Configuration Exchange konfiguriert ist, kann das Gateway die DNS-Einstellungen automatisch bereitstellen. Wenn nicht, stellen Sie sicher, dass das Kontrollkästchen **Automatisch beziehen** deaktiviert ist, und geben Sie manuell eine gültige DNS-Serveradresse ein.

VPN Site Configuration		
Client Name Resolution Auther	ntication Phase	
DNS WINS		
🛛 🖾 Enable DNS 🛛 🕢 Obta	ain Automatically	
Server Address #1		
Server Address #2		
Server Address #3		
Server Address #4		
I Obta DNS Suffix	ain Automatically	
Sav	/e Cancel	

Schritt 8. (Optional) Klicken Sie auf die Registerkarte *Namensauflösung*, aktivieren Sie das Kontrollkästchen **WINS aktivieren**, wenn Sie den Windows Internet Name Server (WINS) aktivieren möchten. Wenn Ihr Remote-Gateway für die Unterstützung von Configuration Exchange konfiguriert ist, kann das Gateway die WINS-Einstellungen automatisch bereitstellen. Wenn nicht, stellen Sie sicher, dass das Kontrollkästchen **Automatisch beziehen** deaktiviert ist, und geben Sie manuell eine gültige WINS-Serveradresse ein.

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

Anmerkung: Durch die Bereitstellung von WINS-Konfigurationsinformationen kann ein Client WINS-Namen mithilfe eines Servers auflösen, der sich im privaten Remote-Netzwerk befindet. Dies ist nützlich, wenn Sie versuchen, über einen Pfadnamen für die Uniform Naming Convention auf Remote-Windows-Netzwerkressourcen zuzugreifen. Der WINS-Server gehört normalerweise zu einem Windows-Domänencontroller oder einem Samba-Server.

Schritt 9: Klicken Sie auf die Registerkarte *Authentication (Authentifizierung*), und wählen Sie **Mutual PSK + XAuth** in der Dropdown-Liste *Authentication Method* (*Authentifizierungsmethode*) aus.

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

Die verfügbaren Optionen sind wie folgt definiert:

• Hybrid-RSA + XAuth — Die Client-Anmeldeinformationen werden nicht benötigt. Der Client authentifiziert das Gateway. Die Anmeldeinformationen werden in Form von PEModer PKCS12-Zertifikatsdateien oder Schlüsseldateitypen bereitgestellt.

 Hybrid GRP + XAuth — Die Client-Anmeldeinformationen werden nicht benötigt. Der Client authentifiziert das Gateway. Die Anmeldeinformationen werden in Form einer PEModer PKCS12-Zertifikatsdatei und einer Zeichenfolge mit gemeinsamem Schlüssel bereitgestellt.

 Gegenseitiges RSA + XAuth — Client und Gateway benötigen beide Anmeldeinformationen zur Authentifizierung. Die Anmeldeinformationen werden in Form von PEM- oder PKCS12-Zertifikatsdateien oder Schlüsseltypen bereitgestellt.

Gegenseitiges PSK + XAuth — Client und Gateway benötigen beide
Anmeldeinformationen, um sich zu authentifizieren. Die Anmeldeinformationen werden in
Form einer Zeichenfolge für den gemeinsamen geheimen Schlüssel bereitgestellt.

 Gegenseitiges RSA - Client und Gateway benötigen zur Authentifizierung Anmeldeinformationen. Die Anmeldeinformationen werden in Form von PEM- oder PKCS12-Zertifikatsdateien oder Schlüsseltypen bereitgestellt.

 Gegenseitiges PSK: Client und Gateway benötigen zur Authentifizierung Anmeldeinformationen. Die Anmeldeinformationen werden in Form einer Zeichenfolge für den gemeinsamen geheimen Schlüssel bereitgestellt. Schritt 10: Klicken Sie im Abschnitt "*Authentifizierung*" auf die Unterregisterkarte " *Anmeldedaten*" und geben Sie den gleichen vorinstallierten Schlüssel ein, den Sie auf der Seite "*IPsec VPN Server Setup*" im Feld "*Vorinstallierter Schlüssel*" konfiguriert haben.

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

Schritt 11: Klicken Sie auf die Registerkarte *Phase 1*. Konfigurieren Sie die folgenden Parameter so, dass sie die gleichen Einstellungen aufweisen, die Sie in <u>Schritt 2 des</u> Abschnitts "<u>IPSec VPN Server User Configuration</u>" für <u>den</u> RV130/RV130W konfiguriert haben.

VPN Site Configuration	×	
Name Resolution Authe	ntication 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	

Die Parameter in Shrew Soft müssen mit den RV130/RV130W-Konfigurationen in Phase 1 übereinstimmen:

- "Exchange Type" sollte mit "Exchange Mode" übereinstimmen.
- "DH Exchange" sollte mit "DH Group" übereinstimmen.
- "Cipher Algorithm" sollte mit "Encryption Algorithm" übereinstimmen.
- "Hash Algorithm" sollte mit "Authentication Algorithm" übereinstimmen.

Schritt 12: Wenn Ihr Gateway während der Phase-1-Verhandlungen eine mit Cisco kompatible Anbieter-ID anbietet, aktivieren Sie das Kontrollkästchen **Enable Check Point Compatible Vendor ID (Check Point-kompatible Anbieter-ID aktivieren)**. Wenn das Gateway dies nicht tut, oder wenn Sie sich nicht sicher sind, lassen Sie das Kontrollkästchen deaktiviert.

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	

Schritt 13. Klicken Sie auf die Registerkarte *Phase 2*. Konfigurieren Sie die folgenden Parameter so, dass sie die gleichen Einstellungen aufweisen, die Sie in <u>Schritt 2 des</u> Abschnitts "<u>IPSec VPN Server User Configuration</u>" für <u>den</u> RV130/RV130W konfiguriert haben.

VPN Site Configuration	X
Authentication Phase 1	Phase 2 Policy
Proposal Parameters	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

Die Parameter in Shrew Soft müssen mit den RV130/RV130W-Konfigurationen in Phase 2 übereinstimmen:

- "Transform Algorithm" sollte mit "Encryption Algorithm" übereinstimmen.
- "HMAC Algorithm" sollte mit "Authentication Algorithm" übereinstimmen.

• PFS Exchange" sollte mit "DH Group" übereinstimmen, wenn PFS Key Group auf dem RV130/RV130W aktiviert ist. Andernfalls wählen Sie **Disabled (Deaktiviert)**.

• "Key Life Time limit" sollte mit "IPSec SA Lifetime" übereinstimmen.

Schritt 14: Klicken Sie auf die Registerkarte *Policy* (*Richtlinie*), und wählen Sie in der Dropdown-Liste *Policy Generation Level* (*Richtlinienerstellungsebene*) die Option **require** aus. Mit der Option *Richtlinienerstellungsebene* wird die Ebene geändert, auf der IPsec-Richtlinien generiert werden. Die verschiedenen Ebenen in der Dropdown-Liste entsprechen dem IPSec SA-Verhandlungsverhalten, das von verschiedenen Anbieterimplementierungen implementiert wurde.

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

Die verfügbaren Optionen sind wie folgt definiert:

· Auto - Der Client bestimmt automatisch die entsprechende IPSec-Richtlinienebene.

 Erforderlich - Der Client handelt keine eindeutige Sicherheitszuordnung (Security Association, SA) für jede Richtlinie aus. Richtlinien werden unter Verwendung der lokalen öffentlichen Adresse als lokale Richtlinien-ID und der Remote-Netzwerkressourcen als Remote-Richtlinien-ID generiert. Bei dem Vorschlag für Phase 2 werden die Richtlinien-IDs während der Verhandlung verwendet.

• Eindeutig - Der Client handelt für jede Richtlinie eine eindeutige Sicherheitszuordnung aus.

• Freigegeben - Richtlinien werden auf der erforderlichen Ebene erstellt. Im Vorschlag für Phase 2 wird die lokale Richtlinien-ID als lokale ID und Any (0.0.0.0/0) als Remote-ID während der Verhandlung verwendet.

Schritt 15: Deaktivieren Sie das Kontrollkästchen **Topologie automatisch beziehen oder Tunnel All**. Mit dieser Option wird die Konfiguration von Sicherheitsrichtlinien für die Verbindung geändert. Wenn deaktiviert, muss eine manuelle Konfiguration durchgeführt werden. Wenn diese Option aktiviert ist, wird die automatische Konfiguration durchgeführt.

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

Schritt 16. Klicken Sie auf **Hinzufügen**, um die Remote-Netzwerkressource hinzuzufügen, mit der Sie eine Verbindung herstellen möchten. Zu den Remote-Netzwerkressourcen gehören der Remote-Zugriff auf Desktops, Abteilungsressourcen, Netzlaufwerke und gesicherte elektronische Post.

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 Lancel

Das Fenster Topologieeintrag wird angezeigt:

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 Address . . Netmask . . Ok Cancel
Add Modify Delete
Save Cancel

Schritt 17: Geben Sie im Feld *Adresse* die Subnetz-ID des RV130/RV130W ein. Die Adresse muss mit dem Feld *IP-Adresse* in <u>Schritt 2 des</u> Abschnitts "<u>*IPSec VPN Server Setup and*</u> <u>*User Configuration*</u>" dieses Dokuments übereinstimmen.

VPN Site Configuration	
Authentication Phase 1 Phase 2 Policy	
Add Modify Delete	
Save Cancel	

Schritt 18: Geben Sie in das Feld *Netzmaske* die Subnetzmaske für das lokale Netzwerk des RV130/RV130W ein. Die Netzmaske muss mit dem Feld *Subnetzmaske* in <u>Schritt 2 des</u> Abschnitts "<u>IPSec VPN Server User Configuration</u>" dieses Dokuments übereinstimmen.

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy
Type Include Address 192.168.1.0 Netmask 255.255.255.0 Ok Cancel
Add Modify Delete
Save Cancel

Schritt 19: Klicken Sie auf **OK**, um die Remote-Netzwerkressource hinzuzufügen.

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy
Add Modify Delete

Schritt 20: Klicken Sie auf **Speichern**, um die Konfigurationen für die Verbindung mit der VPN-Site zu speichern.

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
↔ 192.168.1.0 / 255.255.255.0
Add Modify Delete
Save Cancel

Schritt 21: Kehren Sie zum Fenster *VPN Access Manager zurück,* um den von Ihnen konfigurierten VPN-Standort auszuwählen, und klicken Sie auf die Schaltfläche **Verbinden**.

OPN Acces	ss Mar	nager			x
File Edit	√iew	Help			
	•	2			
Connect	Add	Modify	Delete		
8					
13.16.91.11					

Das Fenster VPN Connect (VPN-Verbindung) wird angezeigt.

S VPN Connect - LTT LILIUM
Connect Network
config loaded for site 38 4085
Credentials
Username
Password
Connect Exit

Schritt 22. Geben Sie im Abschnitt *Anmeldedaten* den Benutzernamen und das Kennwort des Kontos ein, das Sie in <u>Schritt 4 des</u> Abschnitts "<u>IPSec VPN Server-</u> <u>Benutzerkonfiguration</u>" dieses Dokuments eingerichtet haben.

S VPN Connect - Ditt I 4 TI H
Connect Network
config loaded for site ' 🖽 🛛 🖬 🖬 🖬 🖬
Credentials
Username TestUser
Password

Schritt 23: Klicken Sie auf Connect to VPN into the RV130/RV130W.

VPN Connect - DH114 TLH	J
Connect Network	
config loaded for site " 🖽 🖬 🖬 🖬 🖬 🖬	
Credentials	
Username TestUser	
Password •••••	
Connect Exit	

Der IPSec-VPN-Tunnel ist eingerichtet, und der VPN-Client kann auf die Ressource hinter dem RV130/RV130W-LAN zugreifen.

🕑 VPN C	onnect - 1311147174	x
Connect	Network	
esp prop client co local id remote i pre-shar bringing	posal configured onfigured configured d configured red key configured up tunnel	4 III >
- Creder	ntials	
Usern	ame TestUser	
Pass	word	
	Connect Cancel	



Video zu diesem Artikel anzeigen ...

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.