

Konfiguration eines einzelnen Client-zu-Gateway Virtual Private Network (VPN) auf den VPN-Routern der Serien RV320 und RV325

Ziel

In diesem Dokument wird erläutert, wie Sie ein einzelnes Client-to-Gateway Virtual Private Network (VPN) auf VPN-Routern der Serie RV32x konfigurieren.

Einführung

Ein VPN ist ein privates Netzwerk, das verwendet wird, um einen Remote-Benutzer virtuell über ein öffentliches Netzwerk zu verbinden. Ein VPN-Typ ist ein Client-to-Gateway-VPN. Ein Client-to-Gateway-VPN ist eine Verbindung zwischen einem Remote-Benutzer und dem Netzwerk. Der Client wird auf dem Gerät des Benutzers mit VPN-Clientsoftware konfiguriert. Sie ermöglicht Benutzern die sichere Remote-Verbindung mit einem Netzwerk.

Anwendbare Geräte

- RV320 Dual-WAN VPN-Router
- RV325 Dual-WAN-VPN-Router mit Gigabit

Softwareversion

- V1.1.0.09

VPN-Konfiguration für Einzelclient an Gateway

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **VPN > Client to Gateway** aus. Die Seite *Client to Gateway* wird geöffnet:

Client to Gateway

Add a New Tunnel

Tunnel Group VPN Easy VPN

Tunnel No.

1

Tunnel Name:

Interface:

WAN1

Keying Mode:

IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type:

IP Only

IP Address:

0.0.0.0

Local Security Group Type:

Subnet

IP Address:

192.168.1.0

Subnet Mask:

255.255.255.0

Remote Client Setup

Remote Security Gateway Type:

IP Only

IP Address

:

Schritt 2: Klicken Sie auf das Optionsfeld **Tunnel**, um einen Tunnel für das VPN zwischen Client und Gateway hinzuzufügen.

Client to Gateway

Add a New Tunnel

Tunnel

Group VPN

Easy VPN

Tunnel No. 1

Tunnel Name:

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type: IP Only

IP Address: 0.0.0.0

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address :

Neuen Tunnel hinzufügen

Client to Gateway

Add a New Tunnel

Tunnel Group VPN Easy VPN

Tunnel No. 1

Tunnel Name:

Interface: ▼

Keying Mode: ▼

Enable:

Local Group Setup

Local Security Gateway Type: ▼

IP Address: 0.0.0.0

Local Security Group Type: ▼

IP Address:

Subnet Mask:

Remote Client Setup

Remote Security Gateway Type: ▼

▼ :

Hinweis: Tunnel No (Tunnelnr): Stellt die Nummer des Tunnels dar. Diese Nummer wird automatisch generiert.

Schritt 1: Geben Sie den Namen des Tunnels in das Feld *Tunnelname* ein.

Schritt 2: Wählen Sie aus der Dropdown-Liste *Interface (Schnittstelle)* die Schnittstelle aus, über die der Remote-Client auf das VPN zugreift.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode:

Enable:

Local Group Setup

Local Security Gateway Type: IP Only

IP Address: 0.0.0.0

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Schritt 3: Wählen Sie in der Dropdown-Liste *Keying Mode* den entsprechenden Modus für die Schlüsselverwaltung aus, um die Sicherheit sicherzustellen. Der Standardmodus ist IKE mit vorinstalliertem Schlüssel.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type: IP Only

IP Address: 0.0.0.0

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Die Optionen sind wie folgt definiert:

- Manual (Manuell) - Benutzerdefinierter Sicherheitsmodus zum Erstellen eines neuen Sicherheitsschlüssels allein und ohne Verhandlung mit dem Schlüssel. Sie eignet sich am besten für die Fehlerbehebung oder in einer kleinen statischen Umgebung.
- IKE mit vorinstalliertem Schlüssel - Das IKE-Protokoll (Internet Key Exchange) wird verwendet, um automatisch einen vorinstallierten Schlüssel zu generieren und auszutauschen, um eine authentifizierte Kommunikation für den Tunnel herzustellen.
- IKE mit Zertifikat - Das IKE-Protokoll (Internet Key Exchange) mit Zertifikat ist eine sicherere Methode zum automatischen Generieren und Austausch von vorinstallierten Schlüsseln, um eine sicherere Kommunikation für den Tunnel zu ermöglichen.

Schritt 4: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um das VPN zwischen Client und Gateway zu aktivieren. Es ist standardmäßig aktiviert.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No.

Tunnel Name:

Interface:

Keying Mode:

Enable:

Local Group Setup

Local Security Gateway Type:

Domain Name:

Local Security Group Type:

IP Address:

Schritt 5: Wenn Sie die Einstellungen speichern möchten, scrollen Sie nach unten, und klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Lokale Gruppeneinrichtung

Lokale Gruppeneinrichtung mit manueller oder IKE mit vorinstalliertem Schlüssel

Hinweis: Führen Sie die folgenden Schritte aus, wenn Sie in der Dropdown-Liste *Keying Mode* in Schritt 3 des Abschnitts *Add a New Tunnel (Neuen Tunnel hinzufügen)* die Option Manual (Manuell) oder IKE mit vorinstalliertem Schlüssel ausgewählt haben.

Schritt 1: Wählen Sie in der Dropdown-Liste *Local Security Gateway (Lokales Sicherheitsgateway)* die entsprechende Router-Identifizierungsmethode aus, um einen VPN-Tunnel einzurichten.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No.: 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type: IP Only

IP Address: 192.168.1.1

Local Security Group Type: Subnet

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Die Optionen sind wie folgt definiert:

- IP Only (Nur IP): Der Zugriff auf den Tunnel ist nur über eine statische WAN-IP möglich. Sie können diese Option auswählen, wenn nur der Router über eine statische WAN-IP verfügt. Die statische WAN-IP-Adresse wird automatisch generiert.
- IP + Domain Name (FQDN)-Authentifizierung - Der Zugriff auf den Tunnel ist über eine statische IP-Adresse und eine registrierte Domäne möglich. Wenn Sie diese Option wählen, geben Sie den Namen der registrierten Domäne in das Feld *Domänenname ein*. Die statische WAN-IP-Adresse wird automatisch generiert.
- IP + E-Mail Addr. (USER FQDN) Authentifizierung - Der Zugriff auf den Tunnel ist über eine statische IP-Adresse und eine E-Mail-Adresse möglich. Wenn Sie diese Option wählen, geben Sie die E-Mail-Adresse in das Feld *E-Mail-Adresse ein*. Die statische WAN-IP-Adresse wird automatisch generiert.
- Dynamic IP + Domain Name (FQDN) Authentication - Der Zugriff auf den Tunnel ist über eine dynamische IP-Adresse und eine registrierte Domäne möglich. Wenn Sie diese Option wählen, geben Sie den Namen der registrierten Domäne in das Feld *Domänenname ein*.
- Dynamische IP- + E-Mail-Adresse (USER FQDN) Authentifizierung - Der Zugriff auf den Tunnel ist über eine dynamische IP-Adresse und eine E-Mail-Adresse möglich. Wenn Sie diese Option wählen, geben Sie die E-Mail-Adresse in das Feld *E-Mail-Adresse ein*.
- IP-Adresse - Stellt die IP-Adresse der WAN-Schnittstelle dar. Es ist ein schreibgeschütztes Feld.

Schritt 2: Wählen Sie aus der Dropdown-Liste *Local Security Group Type (Typ der lokalen Sicherheitsgruppe)* den entsprechenden lokalen LAN-Benutzer oder eine Benutzergruppe aus, die auf den VPN-Tunnel zugreifen kann. Der Standardwert ist "Subnet".

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type: Dynamic IP + Domain Name(FQDN) Authentication

Domain Name: domain_1

Local Security Group Type: Subnet

IP Address:

Subnet Mask: 255.255.255.0

- IP - Nur ein bestimmtes LAN-Gerät kann auf den Tunnel zugreifen. Wenn Sie diese Option wählen, geben Sie die IP-Adresse des LAN-Geräts in das Feld *IP-Adresse ein*. Die Standard-IP-Adresse lautet 192.168.1.0.
- Subnetz - Alle LAN-Geräte in einem bestimmten Subnetz können auf den Tunnel zugreifen. Wenn Sie diese Option wählen, geben Sie die IP-Adresse und die Subnetzmaske der LAN-Geräte in das Feld *IP-Adresse* und *Subnetzmaske ein*. Die Standardmaske ist 255.255.255.0.
- IP Range (IP-Bereich) - Eine Reihe von LAN-Geräten kann auf den Tunnel zugreifen. Wenn Sie diese Option wählen, geben Sie die Start- und End-IP-Adresse in die Felder *Start IP* und *End IP (Endadresse)* ein. Der Standardbereich liegt zwischen 192.168.1.0 und 192.168.1.254.

Schritt 3: Wenn Sie die Einstellungen speichern möchten, scrollen Sie nach unten, und klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Lokale Gruppen-Einrichtung mit IKE mit Zertifikat für Tunnel-VPN

Hinweis: Führen Sie die folgenden Schritte aus, wenn Sie IKE mit Zertifikat aus der Dropdown-Liste *Keying Mode* in Schritt 3 des Abschnitts *Add a New Tunnel (Neuen Tunnel hinzufügen)* ausgewählt haben.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name:

Interface:

Keying Mode:

Enable:

Local Group Setup

Local Security Gateway Type:

IP Address:

Local Certificate:

Local Security Group Type:

IP Address:

- Lokaler Sicherheits-Gateway-Typ - Der Zugriff auf den Tunnel ist über IP mit einem Zertifikat möglich.
- IP-Adresse - Stellt die IP-Adresse der WAN-Schnittstelle dar. Es ist ein schreibgeschütztes Feld.

Schritt 1: Wählen Sie das entsprechende lokale Zertifikat aus, um den Router in der Dropdown-Liste *Lokales Zertifikat* zu identifizieren. Klicken Sie auf **Self-Generator**, um das Zertifikat automatisch zu generieren, oder klicken Sie auf **Zertifikat importieren**, um ein neues Zertifikat zu importieren.

Hinweis: Weitere Informationen zum automatischen Generieren von Zertifikaten finden Sie unter *Generate Certificates on RV320 Routers (Zertifikate generieren auf RV320-Routern)*. Informationen zum Importieren von Zertifikaten finden Sie unter *Configure My Certificate on RV320 Routers*.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name:

Interface:

Keying Mode:

Enable:

Local Group Setup

Local Security Gateway Type:

IP Address: 0.0.0.0

Local Certificate:

Local Security Group Type:

IP Address:

- IP
- IP
- Subnet
- IP Range

Schritt 2: Wählen Sie aus der Dropdown-Liste *Local Security Group Type* (Typ der lokalen Sicherheitsgruppe) den entsprechenden Typ des lokalen LAN-Benutzers oder der Benutzergruppe aus, der auf den VPN-Tunnel zugreifen kann. Der Standardwert ist "Subnet".

- IP - Nur ein bestimmtes LAN-Gerät kann auf den Tunnel zugreifen. Wenn Sie diese Option wählen, geben Sie die IP-Adresse des LAN-Geräts im Feld IP Address (IP-Adresse) ein. Die Standard-IP-Adresse lautet 192.168.1.0.
- Subnetz - Alle LAN-Geräte in einem bestimmten Subnetz können auf den Tunnel zugreifen. Wenn Sie diese Option wählen, geben Sie die IP-Adresse und die Subnetzmaske der LAN-Geräte in das Feld IP Address (IP-Adresse) bzw. Subnet Mask (Subnetzmaske) ein. Die Standardmaske ist 255.255.255.0.
- IP Range (IP-Bereich) - Eine Reihe von LAN-Geräten kann auf den Tunnel zugreifen. Wenn Sie diese Option wählen, geben Sie die Start- bzw. End IP-Adresse in die Felder Start IP bzw. End IP (IP starten und beenden) ein. Der Standardbereich liegt zwischen 192.168.1.0 und 192.168.1.254.

Schritt 3: Wenn Sie die Einstellungen speichern möchten, scrollen Sie nach unten, und klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Remote-Client-Setup

Remote-Client-Setup mit manueller oder IKE mit vorinstalliertem Schlüssel

Hinweis: Führen Sie die folgenden Schritte aus, wenn Sie in der Dropdown-Liste *Keying*

Mode in Schritt 3 des Abschnitts *Add a New Tunnel (Neuen Tunnel hinzufügen)* die Option Manual (Manuell) oder IKE mit vorinstalliertem Schlüssel ausgewählt haben.

Client to Gateway

Add a New Tunnel

Tunnel Group VPN Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type: IP Only

IP Address: 0.0.0.0

Local Security Group Type: IP

IP Address: 192.168.2.1

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address :

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

Schritt 1: Wählen Sie aus der Dropdown-Liste *Remote Security Gateway* die entsprechende Client-Identifizierungsmethode zum Einrichten eines VPN-Tunnels aus. Der Standardwert ist "Nur IP".

- IP Only (Nur IP): Der Zugriff auf den Tunnel ist nur über die statische WAN-IP des Clients möglich. Sie können diese Option nur auswählen, wenn Sie die statische WAN-IP oder den Domännennamen des Clients kennen. Wählen Sie entweder die IP-Adresse aus der Dropdown-Liste aus, und geben Sie die statische IP des Clients in das angrenzende Feld ein, oder wählen Sie IP by DNS Resolved aus der Dropdown-Liste aus, und geben Sie den Domännennamen der IP-Adresse in das angrenzende Feld ein. Über den lokalen DNS-Server der IP-Adresse kann der Router die IP-Adresse automatisch abrufen.

Hinweis: Wenn Sie in Schritt 3 im Abschnitt *Add a New Tunnel Through Tunnel (Neuen Tunnel durch Tunnel hinzufügen)* oder im Abschnitt *Group VPN (Gruppen-VPN)* die Option Manual (Manuell) aus der Dropdown-Liste auswählen, ist dies die einzige verfügbare Option.

- IP + Domain Name (FQDN)-Authentifizierung - Der Zugriff auf den Tunnel ist über eine

statische IP-Adresse des Clients und eine registrierte Domäne möglich. Wenn Sie diese Option wählen, geben Sie den Namen der registrierten Domäne im Feld Domain Name (Domänenname) ein. Wählen Sie entweder die IP-Adresse aus der Dropdown-Liste aus, und geben Sie die statische IP des Clients in das angrenzende Feld ein, oder wählen Sie IP by DNS Resolved aus der Dropdown-Liste aus, und geben Sie den Domännennamen der IP-Adresse in das angrenzende Feld ein. Über den lokalen DNS-Server der IP-Adresse kann der Router die IP-Adresse automatisch abrufen.

- IP + E-Mail Addr. (USER FQDN) Authentifizierung - Der Zugriff auf den Tunnel ist über eine statische IP-Adresse des Clients und eine E-Mail-Adresse möglich. Wenn Sie diese Option wählen, geben Sie die E-Mail-Adresse in das Feld E-Mail-Adresse ein. Wählen Sie entweder die IP-Adresse aus der Dropdown-Liste aus, und geben Sie die statische IP des Clients in das angrenzende Feld ein, oder wählen Sie IP by DNS Resolved aus der Dropdown-Liste aus, und geben Sie den Domännennamen der IP-Adresse in das angrenzende Feld ein. Über den lokalen DNS-Server der IP-Adresse kann der Router die IP-Adresse automatisch abrufen.
- Dynamische IP + Domänenname (FQDN)-Authentifizierung - Der Zugriff auf den Tunnel ist über eine dynamische IP-Adresse des Clients und eine registrierte Domäne möglich. Wenn Sie diese Option wählen, geben Sie den Namen der registrierten Domäne im Feld Domain Name (Domänenname) ein.
- Dynamische IP- + E-Mail-Adressierung (USER FQDN) Authentifizierung - Der Zugriff auf den Tunnel ist über eine dynamische IP-Adresse des Clients und eine E-Mail-Adresse möglich. Wenn Sie diese Option wählen, geben Sie die E-Mail-Adresse in das Feld E-Mail-Adresse ein.

Schritt 2: Wenn Sie die Einstellungen speichern möchten, scrollen Sie nach unten, und klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Remote-Gruppeneinrichtung mit IKE mit Zertifikat

Hinweis: Führen Sie die folgenden Schritte aus, wenn Sie IKE mit Zertifikat aus der Dropdown-Liste *Keying Mode* in Schritt 3 des Abschnitts *Add a New Tunnel (Neuen Tunnel hinzufügen)* ausgewählt haben.

Local Group Setup

Local Security Gateway Type: IP + Certificate

IP Address: 0.0.0.0

Local Certificate: 01. Issuer : 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52

Self-Generator Import Certificate

Local Security Group Type: Subnet

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Security Gateway Type: IP + Certificate

IP Address : 192.168.3.2

Remote Certificate: 01. Issuer : 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52

Import Remote Certificate Authorize CSR

- Remote Security Gateway Type (Gateway-Typ für Remote-Sicherheit) - Die Client-Identifikation ist über IP mit einem Zertifikat zum Herstellen einer VPN-Verbindung möglich.

Schritt 1: Wählen Sie **IP-Adresse** oder **IP by DNS Resolved** aus der Dropdown-Liste aus.

- IP-Adresse - Der Zugriff auf den Tunnel ist nur über die statische WAN-IP des Clients möglich. Sie können diese Option nur auswählen, wenn Sie die statische WAN-IP des Clients kennen. Geben Sie die statische IP des Clients in das Feld *IP-Adresse ein*.
- IP By DNS Resolved (IP durch DNS aufgelöst): Dieser Befehl ist nützlich, wenn Sie die IP-Adresse des Clients nicht kennen, die Domäne dieser IP-Adresse jedoch kennen. Geben Sie den Domännennamen der IP-Adresse ein. Über den lokalen DNS-Server der IP-Adresse kann der Router die IP-Adresse automatisch abrufen.

Schritt 2: Wählen Sie das entsprechende Remote-Zertifikat aus der Dropdown-Liste *Remote Certificate* aus. Klicken Sie auf **Remote-Zertifikat importieren**, um ein neues Zertifikat zu importieren, oder auf **CSR autorisieren**, um ein Zertifikat mit einer digitalen Signierungsanfrage zu identifizieren.

Hinweis: Weitere Informationen zum Importieren eines neuen Zertifikats finden Sie unter *View/Add Trusted SSL Certificate auf RV320 Routern*. Weitere Informationen zu autorisierten CSR-Zertifikaten finden Sie unter *Certificate Signing Request (CSR) auf RV320 Routern*.

Schritt 3: Wenn Sie die Einstellungen speichern möchten, scrollen Sie nach unten, und klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

IPSec-Einrichtung

IPSec-Einrichtung mit manuellem Schlüssel

Hinweis: Führen Sie die folgenden Schritte aus, wenn Sie in der Dropdown-Liste *Keying Mode* in Schritt 3 des Abschnitts *Add a New Tunnel (Neuen Tunnel hinzufügen)* die Option *Manual (Manuell)* auswählen.

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address: 192.168.3.2

IPSec Setup

Incoming SPI: 1023ac (Range: 100-FFFFFFFF, Default: 100)

Outgoing SPI: 1023cb (Range: 100-FFFFFFFF, Default: 100)

Encryption: DES

Authentication: MD5

Encryption Key: (HEX Number, DES: 16bits, 3DES: 48bits)

Authentication Key: (HEX Number, MD5: 32bits, SHA1: 40bits)

Schritt 1: Geben Sie den eindeutigen Hexadezimalwert für den eingehenden Security Parameter Index (SPI) im Feld *Incoming SPI (Incoming SPI)* ein. Der SPI wird im ESP-Header (Encapsulating Security Payload Protocol) übertragen, der zusammen die Sicherheitszuordnung (Security Association, SA) für das eingehende Paket bestimmt. Der Bereich liegt zwischen 100 und 100, der Standardwert ist 100.

Schritt 2: Geben Sie den eindeutigen Hexadezimalwert für den ausgehenden Security Parameter Index (SPI) im Feld *Outgoing SPI (Ausgehender SPI)* ein. Der SPI wird im ESP-Header (Encapsulating Security Payload Protocol) übertragen, der zusammen die Sicherheitszuordnung (Security Association, SA) für das ausgehende Paket bestimmt. Der Bereich liegt zwischen 100 und 100, der Standardwert ist 100.

Hinweis: Der eingehende SPI des angeschlossenen Geräts und der ausgehende SPI am anderen Ende des Tunnels sollten übereinstimmen, um einen Tunnel einzurichten.

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address: 192.168.3.2

IPSec Setup

Incoming SPI: 1023ac (Range: 100-FFFFFFFF, Default: 100)

Outgoing SPI: 1023cb (Range: 100-FFFFFFFF, Default: 100)

Encryption: DES

Authentication: DES

Encryption Key: (HEX Number, DES: 16bits, 3DES: 48bits)

Authentication Key: (HEX Number, MD5: 32bits, SHA1: 40bits)

Save Cancel

Schritt 3: Wählen Sie die entsprechende Verschlüsselungsmethode aus der Dropdown-Liste *Encryption* aus. Die empfohlene Verschlüsselung ist 3DES. Der VPN-Tunnel muss für beide Enden dieselbe Verschlüsselungsmethode verwenden.

- DES - Data Encryption Standard (DES) ist eine nicht so sichere, ältere, abwärtskompatible Verschlüsselungsmethode mit 56 Bit.
- 3DES - Triple Data Encryption Standard (3DES) ist eine einfache 168-Bit-Verschlüsselungsmethode, mit der die Schlüsselgröße durch dreimal verschlüsselte Daten erhöht werden kann, was mehr Sicherheit bietet als DES.

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address: 192.168.3.2

IPSec Setup

Incoming SPI: 1023ac (Range: 100-FFFFFFFF, Default: 100)

Outgoing SPI: 1023cb (Range: 100-FFFFFFFF, Default: 100)

Encryption: DES

Authentication: MD5

Encryption Key: (HEX Number, DES: 16bits, 3DES: 48bits)

Authentication Key: (HEX Number, MD5: 32bits, SHA1: 40bits)

Save Cancel

Schritt 4: Wählen Sie die entsprechende Authentifizierungsmethode aus der Dropdown-Liste *Authentication (Authentifizierung)* aus. Die empfohlene Authentifizierung ist SHA1. Der

VPN-Tunnel muss für beide Enden dieselbe Authentifizierungsmethode verwenden.

- MD5 - Message Digest Algorithm-5 (MD5) stellt eine 32-stellige hexadezimale Hashfunktion dar, die die Daten durch die Berechnung der Prüfsumme vor böswilligen Angriffen schützt.
- SHA1 - Secure Hash Algorithm Version 1 (SHA1) ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5.

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address: 192.168.3.2

IPSec Setup

Incoming SPI: 1023ac (Range: 100-FFFFFFFF, Default: 100)

Outgoing SPI: 1023cb (Range: 100-FFFFFFFF, Default: 100)

Encryption: DES

Authentication: SHA1

Encryption Key: adbc234987bc (HEX Number, DES: 16bits, 3DES: 48bits)

Authentication Key: 233445bcfacfb (HEX Number, MD5: 32bits, SHA1: 40bits)

Save Cancel

Schritt 5: Geben Sie im Feld *Verschlüsselungsschlüssel* den Schlüssel zum Verschlüsseln und Entschlüsseln von Daten ein. Wenn Sie DES in Schritt 3 als Verschlüsselungsmethode ausgewählt haben, geben Sie einen 16-stelligen Hexadezimalwert ein. Wenn Sie in Schritt 3 3DES als Verschlüsselungsmethode auswählen, geben Sie einen Hexadezimalwert mit 40 Ziffern ein.

Schritt 6: Geben Sie im Feld *Authentifizierungsschlüssel* einen vorinstallierten Schlüssel zur Authentifizierung des Datenverkehrs ein. Wenn Sie in Schritt 4 MD5 als Authentifizierungsmethode auswählen, geben Sie einen 32-stelligen Hexadezimalwert ein. Wenn Sie in Schritt 4 SHA als Authentifizierungsmethode auswählen, geben Sie einen Hexadezimalwert mit 40 Ziffern ein. Der VPN-Tunnel muss für beide Enden denselben vorinstallierten Schlüssel verwenden.

Schritt 7: Wenn Sie die Einstellungen speichern möchten, scrollen Sie nach unten, und klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

IPSec-Einrichtung mit IKE mit vorinstalliertem Schlüssel oder IKE mit Zertifikat

Hinweis: Führen Sie die folgenden Schritte aus, wenn Sie IKE mit vorinstalliertem Schlüssel oder IKE mit Zertifikat in der Dropdown-Liste *Keying Mode* in Schritt 3 des Abschnitts *Add a New Tunnel (Neuen Tunnel hinzufügen)* auswählen.

Remote Client Setup

Remote Security Gateway Type:

IP Address:

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:


Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter: 

Schritt 1: Wählen Sie aus der Dropdown-Liste *Phase 1 DH Group* die entsprechende Phase 1 DH-Gruppe aus. Phase 1 dient zum Aufbau der Simplex, Logical Security Association (SA) zwischen den beiden Enden des Tunnels, um eine sichere authentische Kommunikation zu unterstützen. Diffie-Hellman (DH) ist ein kryptografisches Schlüsselaustauschprotokoll, das während der Phase-1-Verbindung verwendet wird, um geheime Schlüssel zur Authentifizierung der Kommunikation freizugeben.

- Gruppe 1 - 768 Bit - Stellt den niedrigsten Stärke-Schlüssel und die unsicherste Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert jedoch weniger Zeit. Es wird empfohlen, wenn die Netzwerkgeschwindigkeit niedrig ist.
- Gruppe 2 - 1024 Bit - Stellt einen leistungsfähigeren Schlüssel und eine sicherere Authentifizierungsgruppe dar. Die IKE-Schlüssel müssen jedoch erst nach einiger Zeit berechnet werden.
- Gruppe 5 - 1536 Bit - Stellt den höchsten Stärke-Schlüssel und die sicherste Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert mehr Zeit. Es wird empfohlen, wenn die Netzwerkgeschwindigkeit hoch ist.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption :

- DES
- DES
- 3DES
- AES-128
- AES-192
- AES-256

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Schritt 2: Wählen Sie aus der Dropdown-Liste *Phase 1 Encryption* die entsprechende Phase 1 Encryption aus, um den Schlüssel zu verschlüsseln. AES-256 wird empfohlen, da es sich um die sicherste Verschlüsselungsmethode handelt. Der VPN-Tunnel muss für beide Enden dieselbe Verschlüsselungsmethode verwenden.

- DES - Data Encryption Standard (DES) ist eine 56-Bit-Verschlüsselungsmethode, die nicht sehr sicher ist.
- 3DES - Triple Data Encryption Standard (3DES) ist eine einfache 168-Bit-Verschlüsselungsmethode, mit der die Schlüsselgröße durch dreimal verschlüsselte Daten erhöht werden kann, was mehr Sicherheit bietet als DES.
- AES-128 - Advanced Encryption Standard (AES) ist eine 128-Bit-Verschlüsselungsmethode, die den Klartext durch 10 Wiederholungszyklen in einen verschlüsselten Text umwandelt.
- AES-192 - Advanced Encryption Standard (AES) ist eine 192-Bit-Verschlüsselungsmethode, die den Klartext durch 12 Wiederholungszyklen in einen verschlüsselten Text umwandelt.
- AES-256 - Advanced Encryption Standard (AES) ist eine 256-Bit-Verschlüsselungsmethode, die den Klartext durch 14 Wiederholungszyklen in einen verschlüsselten Text umwandelt.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication: (MD5, MD5, SHA1)

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Schritt 3: Wählen Sie die entsprechende Authentifizierungsmethode aus der Dropdown-Liste *Phase 1 Authentication (Authentifizierung Phase 1)* aus. Der VPN-Tunnel muss für beide Enden dieselbe Authentifizierungsmethode verwenden.

- MD5 - Message Digest Algorithm-5 (MD5) stellt eine 32-stellige hexadezimale Hashfunktion dar, die die Daten durch die Berechnung der Prüfsumme vor böswilligen Angriffen schützt.
- SHA1 - Secure Hash Algorithm Version 1 (SHA1) ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:


Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter: 

Schritt 4: Geben Sie die Zeitdauer in Sekunden ein. In Phase 1 bleibt der VPN-Tunnel im Feld *SA Lifetime* (*SA-Lebensdauer der Phase 1*) aktiv. Die Standardzeit ist 28.800 Sekunden.

Schritt 5: Aktivieren Sie das Kontrollkästchen **Perfect Forward Secrecy (Perfekte Weiterleitungsgeheimnis)**, um die Schlüssel besser zu schützen. Mit dieser Option kann ein neuer Schlüssel generiert werden, wenn ein Schlüssel beschädigt ist. Die verschlüsselten Daten werden nur über den angegriffenen Schlüssel kompromittiert. So wird die Kommunikation sicherer und authentifizierter, da andere Schlüssel gesichert werden, wenn ein Schlüssel beschädigt ist. Dies ist eine empfohlene Maßnahme, da sie mehr Sicherheit bietet.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Schritt 6: Wählen Sie aus der Dropdown-Liste *Phase 2 DH Group* die entsprechende Phase 2 DH-Gruppe aus. Phase 1 dient zum Aufbau der Simplex, Logical Security Association (SA) zwischen den beiden Enden des Tunnels, um eine sichere authentifizierte Kommunikation zu unterstützen. Diffie-Hellman (DH) ist ein kryptografisches Schlüsselaustauschprotokoll, das während der Phase-1-Verbindung verwendet wird, um geheime Schlüssel zur Authentifizierung der Kommunikation freizugeben.

- Gruppe 1 - 768 Bit - Stellt den niedrigsten Stärke-Schlüssel und die unsicherste Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert jedoch weniger Zeit. Es wird empfohlen, wenn die Netzwerkgeschwindigkeit niedrig ist.
- Gruppe 2 - 1024 Bit - Stellt einen leistungsfähigeren Schlüssel und eine sicherere Authentifizierungsgruppe dar. Die IKE-Schlüssel müssen jedoch erst nach einiger Zeit berechnet werden.
- Gruppe 5 - 1536 Bit - Stellt den höchsten Stärke-Schlüssel und die sicherste Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert mehr Zeit. Es wird empfohlen, wenn die Netzwerkgeschwindigkeit hoch ist.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity:

Preshared Key:

Preshared Key Strength Meter: ■ ■ ■ ■

Schritt 7: Wählen Sie aus der Dropdown-Liste *Phase 2 Encryption* die entsprechende Phase 2-Verschlüsselung aus, um den Schlüssel zu verschlüsseln. AES-256 wird empfohlen, da es sich um die sicherste Verschlüsselungsmethode handelt. Der VPN-Tunnel muss für beide Enden dieselbe Verschlüsselungsmethode verwenden.

- DES - Data Encryption Standard (DES) ist eine 56-Bit-Verschlüsselungsmethode, die nicht sehr sicher ist.
- 3DES - Triple Data Encryption Standard (3DES) ist eine einfache 168-Bit-Verschlüsselungsmethode, mit der die Schlüsselgröße durch dreimal verschlüsselte Daten erhöht werden kann, was mehr Sicherheit bietet als DES.
- AES-128 - Advanced Encryption Standard (AES) ist eine 128-Bit-Verschlüsselungsmethode, die den Klartext durch 10-fache Wiederholungen in einen verschlüsselten Text umwandelt.
- AES-192 - Advanced Encryption Standard (AES) ist eine 192-Bit-Verschlüsselungsmethode, die den Klartext durch 12-fache Wiederholungen in einen verschlüsselten Text umwandelt.
- AES-256 - Advanced Encryption Standard (AES) ist eine 256-Bit-Verschlüsselungsmethode, die den Klartext durch 14-fache Wiederholungen in einen verschlüsselten Text umwandelt.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Schritt 8: Wählen Sie die entsprechende Authentifizierungsmethode aus der Dropdown-Liste *Phase-2-Authentifizierung* aus. Der VPN-Tunnel muss für beide Enden dieselbe Authentifizierungsmethode verwenden.

- MD5 - Message Digest Algorithm-5 (MD5) stellt eine 32-stellige hexadezimale Hashfunktion dar, die die Daten durch die Berechnung der Prüfsumme vor böswilligen Angriffen schützt.
- SHA1 - Secure Hash Algorithm Version 1 (SHA1) ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5.
- Null - Es wird keine Authentifizierungsmethode verwendet.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:


Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter: 

Schritt 9: Geben Sie die Zeitdauer in Sekunden ein. In Phase 2 bleibt der VPN-Tunnel im Feld "Phase 2 SA Lifetime" aktiv. Die Standardzeit ist 3600 Sekunden.

Schritt 10: Aktivieren Sie das Kontrollkästchen **Minimale Komplexität des vorinstallierten Schlüssels**, wenn Sie die Kraftanzeige für den vorinstallierten Schlüssel aktivieren möchten.

Schritt 11: Geben Sie einen Schlüssel ein, der zuvor von den IKE-Peers im Feld *Vorinstallierter Schlüssel* gemeinsam genutzt wird. Bis zu 30 alphanumerische Zeichen können als vorinstallierter Schlüssel verwendet werden. Der VPN-Tunnel muss für beide Enden denselben vorinstallierten Schlüssel verwenden.

Hinweis: Es wird dringend empfohlen, den vorinstallierten Schlüssel zwischen den IKE-Peers häufig zu ändern, damit das VPN sicher bleibt.

- Preshared Key Strength Meter - Zeigt die Stärke des vorinstallierten Schlüssels durch farbige Striche an. Rot bedeutet schwache Stärke, Gelb bedeutet akzeptable Stärke und Grün bedeutet starke Stärke. Wenn Sie das Kontrollkästchen **Minimale Komplexität des vorinstallierten Schlüssels** in Schritt 10 des Abschnitts "IPSec-Einrichtung" aktivieren, wird nur die Feststelltaste angezeigt.

Hinweis: Wenn Sie IKE mit vorinstalliertem Schlüssel aus der Dropdown-Liste *Keying Mode* in Schritt 3 für den Abschnitt *Add a New Tunnel (Neuen Tunnel hinzufügen)* auswählen, können Sie nur Schritt 10, Schritt 11 konfigurieren und die vorinstallierte Schlüsselstärke-Messanzeige anzeigen.

Schritt 12: Wenn Sie die Einstellungen speichern möchten, scrollen Sie nach unten, und klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Erweitertes Setup mit IKE mit vorinstalliertem Schlüssel oder IKE mit Zertifikat

Erweiterte Einstellungen sind nur für IKE mit vorinstalliertem Schlüssel und IKE mit Zertifizierungsschlüssel möglich. Die manuelle Tasteneinstellung hat keine erweiterten Einstellungen.

The screenshot shows the 'IPSec Setup' configuration window. It contains the following settings:

- Phase 1 DH Group: Group 1 - 768 bit
- Phase 1 Encryption: AES-128
- Phase 1 Authentication: SHA1
- Phase 1 SA Lifetime: 2870 sec (Range: 120-86400, Default: 28800)
- Perfect Forward Secrecy:
- Phase 2 DH Group: Group 2 - 1024 bit
- Phase 2 Encryption: AES-128
- Phase 2 Authentication: MD5
- Phase 2 SA Lifetime: 350 sec (Range: 120-28800, Default: 3600)
- Minimum Preshared Key Complexity: Enable
- Preshared Key: abcd1234ght
- Preshared Key Strength Meter: A progress bar with 5 segments, the first 4 are red and the last is yellow.

The 'Advanced +' button is highlighted with a red circle. At the bottom of the window are 'Save' and 'Cancel' buttons.

Schritt 1: Klicken Sie auf **Erweitert**, um die erweiterten Einstellungen für IKE mit vorinstalliertem Schlüssel abzurufen.

The image shows a configuration window titled "Advanced" with several options. A red rectangle highlights the following options: "Aggressive Mode" (unchecked), "Compress (Support IP Payload Compression Protocol(IPComp))" (unchecked), "Keep-Alive" (unchecked), "AH Hash Algorithm" (checked, set to SHA1), "NetBIOS Broadcast" (unchecked), and "NAT Traversal" (unchecked). Below these, "Dead Peer Detection Interval" is set to 15 seconds. "Extended Authentication" is checked, and "IPSec Host" is selected. There are input fields for "User Name" and "Password". "Edge Device" is set to "Default - Local Database" with an "Add/Edit" button. "Mode Configuration" is unchecked. At the bottom are "Save" and "Cancel" buttons.

Schritt 2: Aktivieren Sie das Kontrollkästchen **Aggressive Mode** (Aggressiver Modus), wenn die Netzwerkgeschwindigkeit niedrig ist. Die IDs der Endpunkte des Tunnels werden während der SA-Verbindung in Klartext getauscht, was weniger Zeit für den Austausch, aber weniger Sicherheit erfordert.

Schritt 3: Aktivieren Sie das Kontrollkästchen **Compress (Support IP Payload Compression Protocol (IPComp))**, wenn Sie die Größe des IP-Datagramms komprimieren möchten. IPComp ist ein IP-Komprimierungsprotokoll, das verwendet wird, um die Größe des IP-Datagramms zu komprimieren, wenn die Netzwerkgeschwindigkeit niedrig ist und der Benutzer die Daten schnell und ohne Verlust über das langsame Netzwerk übertragen möchte.

Schritt 4. Aktivieren Sie das Kontrollkästchen **Keep-Alive**, wenn die Verbindung des VPN-Tunnels immer aktiv bleiben soll. Es hilft, die Verbindungen sofort wieder herzustellen, wenn eine Verbindung inaktiv wird.

Schritt 5: Aktivieren Sie das Kontrollkästchen **AH Hash Algorithm**, wenn Sie den Authenticate Header (AH) authentifizieren möchten. AH ermöglicht die Authentifizierung von Daten, Datenintegrität durch Prüfsumme und Schutz wird auf den IP-Header erweitert. Der Tunnel sollte für beide Seiten denselben Algorithmus haben.

- MD5 - Message Digest Algorithm-5 (MD5) stellt eine 128-stellige Hexadezimalfunktion dar, die die Daten durch die Prüfsummenberechnung vor böswilligen Angriffen schützt.
- SHA1 - Secure Hash Algorithm Version 1 (SHA1) ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5.

Schritt 6: Aktivieren Sie **NetBIOS-Broadcast**, wenn Sie nicht routbaren Datenverkehr durch den VPN-Tunnel zulassen möchten. Die Standardeinstellung ist deaktiviert. NetBIOS wird verwendet, um Netzwerkressourcen wie Drucker, Computer usw. im Netzwerk über einige Softwareanwendungen und Windows-Features wie Network Neighborhood

(Netzwerkumgebung) zu erkennen.

Schritt 7: Aktivieren Sie das **NAT Traversal**-Kontrollkästchen, wenn Sie über eine öffentliche IP-Adresse aus Ihrem privaten LAN auf das Internet zugreifen möchten. NAT-Traversal wird verwendet, um die privaten IP-Adressen der internen Systeme als öffentliche IP-Adressen anzuzeigen, um die privaten IP-Adressen vor böswilligen Angriffen oder Entdeckungen zu schützen.

Schritt 8: Aktivieren Sie das **Dead Peer Detection Interval (Intervall zur Erkennung von Dead-Peers)**, um die Lebensbereitschaft des VPN-Tunnels durch Hello oder ACK regelmäßig zu überprüfen. Wenn Sie dieses Kontrollkästchen aktivieren, geben Sie die Dauer oder das Intervall der Hello-Nachrichten ein, die Sie senden möchten.

The screenshot shows a configuration window titled 'Advanced'. It contains several checkboxes and input fields. The 'Extended Authentication' section is highlighted with a red border. Within this section, the 'IPSec Host' radio button is selected. The 'User Name' field contains 'user_1' and the 'Password' field is masked with asterisks. Below this, the 'Edge Device' radio button is unselected, and a dropdown menu shows 'Default - Local Database' with an 'Add/Edit' button next to it. At the bottom of the window are 'Save' and 'Cancel' buttons.

Schritt 9: Aktivieren Sie **Extended Authentication**, um mehr Sicherheit und Authentifizierung für die VPN-Verbindung bereitzustellen. Klicken Sie auf das entsprechende Optionsfeld, um die Authentifizierung der VPN-Verbindung zu erweitern.

- IPSec-Host - erweiterte Authentifizierung über IPSec-Host. Wenn Sie diese Option wählen, geben Sie den Benutzernamen des IPSec-Hosts im Feld User Name (Benutzername) und ein Kennwort im Feld Password (Kennwort) ein.
- Edge Device (Edge-Gerät): Erweiterte Authentifizierung über das Edge-Gerät. Wenn Sie diese Option wählen, wählen Sie aus der Dropdown-Liste die Datenbank aus, die das Edge-Gerät enthält. Wenn Sie die Datenbank hinzufügen oder bearbeiten möchten, klicken Sie auf **Hinzufügen/Bearbeiten**.

Hinweis: Weitere Informationen zum Hinzufügen oder Bearbeiten der lokalen Datenbank finden Sie unter *Konfiguration der Benutzer- und Domänenverwaltung auf dem RV320 Router*.

Schritt 10: Aktivieren Sie **Mode Configuration** (Konfiguration des Modus), um die IP-Adresse

für den eingehenden Tunnelanforderer anzugeben.

Hinweis: Die Schritte 9 bis 11 sind für den IKE Preshared Keying Mode für Tunnel VPN verfügbar.

Schritt 11: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Schlussfolgerung

Nun haben Sie die Schritte zur Konfiguration eines VPN-VPN-Client-zu-Gateway auf VPN-Routern der Serie RV32x gelernt.

Sehen Sie sich ein Video zu diesem Artikel an..

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)