

Konfiguration des Gateway-to-Gateway-VPN auf den VPN-Routern RV016, RV042, RV042G und RV082

Ziel

Ein Virtual Private Network (VPN) wird verwendet, um eine sichere Verbindung zwischen zwei Endpunkten über ein öffentliches oder gemeinsam genutztes Internet über einen so genannten VPN-Tunnel herzustellen. Insbesondere ermöglicht eine Gateway-to-Gateway-VPN-Verbindung, dass zwei Router sicher miteinander verbunden sind und dass ein Client an einem Ende logisch so aussieht, als wären sie Teil des Netzwerks am anderen Ende. So können Daten und Ressourcen einfacher und sicherer über das Internet gemeinsam genutzt werden.

Die Konfiguration muss auf beiden Routern erfolgen, um ein Gateway-to-Gateway-VPN zu ermöglichen. Die Konfigurationen in den Abschnitten "*Lokale Gruppeneinrichtung*" und "*Remote-Gruppeneinrichtung*" sollten zwischen den beiden Routern rückgängig gemacht werden, sodass die lokale Gruppe des einen die Remote-Gruppe des anderen ist.

In diesem Dokument wird erläutert, wie Gateway-to-Gateway-VPN auf Routern der VPN-Serien RV016, RV042, RV042G und RV082 konfiguriert wird.

Unterstützte Geräte

RV016
RV042
RV042G
RV082

Software-Version

v4.2.2.08

Konfigurieren des Gateways zum Gateway-VPN

Schritt 1: Melden Sie sich beim Router-Konfigurationsprogramm an, und wählen Sie **VPN > Gateway to Gateway aus**. Die Seite *Gateway zu Gateway* wird geöffnet:

Gateway To Gateway

Add a New Tunnel

Tunnel No. : 2

Tunnel Name :

Interface : ▼

Enable :

Local Group Setup

Local Security Gateway Type : ▼

IP Address : 0.0.0.0

Local Security Group Type : ▼

IP Address :

Subnet Mask :

Remote Group Setup

Remote Security Gateway Type : ▼

▼ :

Remote Security Group Type : ▼

IP Address :

Subnet Mask :

Für die Konfiguration des Gateway-to-Gateway-VPNs müssen die folgenden Funktionen konfiguriert werden:

1. [Einen neuen Tunnel hinzufügen](#)
2. [Einrichtung der lokalen Gruppe](#)
3. [Remote-Gruppeneinrichtung](#)
4. [IPSec-Einrichtung](#)

Neuen Tunnel hinzufügen

Gateway To Gateway

Add a New Tunnel

Tunnel No. 2

Tunnel Name :

Interface :

Enable :

Tunnel No. (Tunnelnummer) ist ein schreibgeschütztes Feld, das den aktuellen Tunnel anzeigt, der erstellt werden soll.

Schritt 1: Geben Sie im Feld "Tunnel Name" einen Namen für den VPN-Tunnel ein. Er muss nicht mit dem Namen übereinstimmen, der am anderen Ende des Tunnels verwendet wird.

Schritt 2: Wählen Sie aus der Dropdown-Liste Interface (Schnittstelle) den WAN-Port aus, den Sie für den Tunnel verwenden möchten.

âf» WAN1: Der dedizierte WAN-Port der VPN-Router der Serie RV0XX.

âf» WAN2 - Der WAN2/DMZ-Port der VPN-Router der Serie RV0XX. Wird nur im Dropdown-Menü angezeigt, wenn es als WAN-Port und nicht als DMZ-Port konfiguriert wurde.

Schritt 3: (Optional) Um das VPN zu aktivieren, aktivieren Sie das Kontrollkästchen im Feld **Aktivieren**. Das VPN ist standardmäßig aktiviert.

Lokale Gruppeneinrichtung

Hinweis: Die Konfiguration für die lokale Gruppeneinrichtung auf einem Router sollte mit der Konfiguration für die Remote-Gruppeneinrichtung auf dem anderen Router identisch sein.

Gateway To Gateway

Add a New Tunnel

Tunnel No. 2

Tunnel Name :

Interface :

Enable :

Local Group Setup

Local Security Gateway Type :

IP Address : 0.0.0.0

Local Security Group Type :

IP Address :

Subnet Mask :

Schritt 1: Wählen Sie in der Dropdown-Liste "Local Security Gateway Type" (Lokaler Sicherheits-Gateway-Typ) die geeignete Methode zur Routeridentifizierung aus, um einen VPN-Tunnel einzurichten.

âf» Nur IP - Der lokale Router (dieser Router) wird von einer statischen IP-Adresse erkannt. Sie können diese Option nur auswählen, wenn der Router über eine statische WAN-IP verfügt. Die statische WAN-IP-Adresse wird automatisch im Feld "IP Address" (IP-Adresse) angezeigt.

âf» IP + Domain Name (FQDN) Authentication - Der Zugriff auf den Tunnel ist über eine statische IP-Adresse und eine registrierte Domain möglich. Wenn Sie diese Option wählen, geben Sie den Namen der registrierten Domäne in das Feld Domain Name (Domänenname) ein. Die statische WAN-IP-Adresse wird automatisch im Feld "IP Address" (IP-Adresse) angezeigt.

âf» IP + E-Mail-Adresse (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 im Feld "IP Address" (IP-Adresse) angezeigt.

âf» Dynamische IP + Domain Name (FQDN)-Authentifizierung - 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 Domain Name (Domänenname) ein.

âf» 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.

Schritt 2: Wählen Sie in der Dropdown-Liste "Lokale Sicherheitsgruppe" den lokalen LAN-Benutzer oder die Benutzergruppe aus, der bzw. die auf den VPN-Tunnel zugreifen kann. Der Standardwert ist "Subnet".

âf» IP - Nur ein LAN-Gerät kann auf den VPN-Tunnel zugreifen. Wenn Sie diese Option auswählen, geben Sie die IP-Adresse des LAN-Geräts in das Feld IP Address (IP-Adresse) ein.

âf» Subnetz - Alle LAN-Geräte in einem bestimmten Subnetz können auf den Tunnel zugreifen. Wenn Sie diese Option auswählen, geben Sie die IP-Adresse und die Subnetzmaske der LAN-Geräte im Feld IP Address (IP-Adresse) bzw. Subnet Mask (Subnetzmaske) ein. Die Standardmaske ist 255.255.255.0.

âf» 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" bzw. "End IP" ein.

Schritt 3: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Remote-Gruppen-Setup

Hinweis: Die Konfiguration für die Einrichtung der Remote-Gruppe auf einem Router sollte mit der Konfiguration für die Einrichtung der lokalen Gruppe auf dem anderen Router identisch sein.

Local Group Setup

Local Security Gateway Type :

Email Address : @

IP Address :

Local Security Group Type :

IP Address :

Remote Group Setup

Remote Security Gateway Type :

:

Remote Security Group Type :

IP Address :

Subnet Mask :

Schritt 1: Wählen Sie in der Dropdown-Liste "Remote Security Gateway Type" (Remote-Sicherheits-Gateway-Typ) die Methode zur Identifizierung des Remote-Routers aus, um den VPN-Tunnel einzurichten.

âf» Nur IP - Der Zugriff auf den Tunnel ist über eine statische WAN-IP möglich. Wenn Sie die IP-Adresse des Remote-Routers kennen, wählen Sie die IP-Adresse aus der Dropdown-Liste direkt unter dem Feld "Remote Security Gateway Type" (Typ des Remote-Sicherheits-Gateways) aus, und geben Sie die IP-Adresse ein. Wählen Sie IP by DNS Resolved (IP durch DNS aufgelöst), wenn Sie die IP-Adresse nicht kennen, aber den Domännennamen kennen, und geben Sie den Domännennamen des Routers in das Feld IP by DNS Resolved (IP durch DNS aufgelöst) ein.

âf» IP + Domain Name (FQDN) Authentication - Der Zugriff auf den Tunnel ist über eine statische IP-Adresse und eine registrierte Domäne für den Router möglich. Wenn Sie die IP-Adresse des Remote-Routers kennen, wählen Sie die IP-Adresse in der Dropdown-Liste direkt unter dem Feld "Remote Security Gateway Type" (Typ des Remote-Sicherheits-Gateways) aus, und geben Sie die Adresse ein. Wählen Sie IP by DNS Resolved (IP durch DNS aufgelöst), wenn Sie die IP-Adresse nicht kennen, aber den Domännennamen kennen, und geben Sie den Domännennamen des Routers in das Feld IP by DNS Resolved (IP durch DNS aufgelöst) ein. Geben Sie den Domännennamen des Routers im Feld Domain Name (Domänenname) ein, unabhängig davon, mit welcher Methode Sie ihn identifizieren möchten.

âf» IP + Email Addr.(USER FQDN) Authentifizierung - Der Zugriff auf den Tunnel ist über eine statische IP-Adresse und eine E-Mail-Adresse möglich. Wenn Sie die IP-Adresse des Remote-Routers kennen, wählen Sie die IP-Adresse in der Dropdown-Liste direkt unterhalb des Felds Remote Security Gateway Type (Remote-Sicherheits-Gateway-Typ) aus, und geben Sie die Adresse ein. Wählen Sie IP by DNS Resolved (IP durch DNS aufgelöst), wenn Sie die IP-Adresse nicht kennen, aber den Domännennamen kennen, und geben Sie den Domännennamen des Routers in das Feld IP by DNS Resolved (IP durch DNS aufgelöst) ein. Geben Sie die E-Mail-Adresse in das Feld E-Mail-Adresse ein.

âf» Dynamische IP + Domain Name (FQDN)-Authentifizierung - 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 Domain Name (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.

Schritt 2: Wählen Sie in der Dropdown-Liste "Remote Security Group Type" (Typ der Remote-Sicherheitsgruppe) den entsprechenden Remote-LAN-Benutzer oder die entsprechende Benutzergruppe aus, die auf den VPN-Tunnel zugreifen kann.

» IP - Nur ein spezielles LAN-Gerät kann auf den Tunnel zugreifen. Wenn Sie diese Option auswählen, geben Sie die IP-Adresse des LAN-Geräts in das Feld IP Address (IP-Adresse) ein.

» Subnetz - Alle LAN-Geräte in einem bestimmten Subnetz können auf den Tunnel zugreifen. Wenn Sie diese Option auswählen, geben Sie die IP-Adresse und die Subnetzmaske der LAN-Geräte im Feld IP Address (IP-Adresse) bzw. Subnet Mask (Subnetzmaske) ein.

» 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" bzw. "End IP" ein.

Hinweis: Die beiden Router am Tunnelende können sich nicht im gleichen Subnetz befinden.

Schritt 3: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

IPSec-Einrichtung

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Advanced +

Save Cancel

Internet Protocol Security (IPSec) ist ein Sicherheitsprotokoll auf der Internetschicht, das eine End-to-End-Sicherheit durch Authentifizierung und Verschlüsselung während einer Kommunikationssitzung bietet.

Hinweis: Beide VPN-Enden müssen die gleichen Verschlüsselungs-, Entschlüsselungs- und Authentifizierungsmethoden aufweisen, damit sie ordnungsgemäß funktionieren. Geben Sie für beide Router die gleichen IPSec-Setup-Einstellungen ein.

The screenshot shows the 'IPSec Setup' configuration page. The 'Keying Mode' dropdown menu is highlighted with a red box, showing 'IKE with Preshared key' selected. Other settings include Phase 1 and 2 encryption (DES), authentication (MD5), and SA Life Time (28800 and 3600 seconds). The 'Perfect Forward Secrecy' checkbox is checked. The 'Minimum Preshared Key Complexity' checkbox is also checked and labeled 'Enable'. The 'Preshared Key Strength Meter' is shown at the bottom with a red bar.

Schritt 1: Wählen Sie aus der Dropdown-Liste "Schlüsselmodus" den entsprechenden Modus für die Schlüsselverwaltung aus, um die Sicherheit zu gewährleisten. Der Standardmodus ist IKE mit vorinstalliertem Schlüssel.

âf» [Manuell](#) - Ein benutzerdefinierter Sicherheitsmodus, in dem Sie selbst einen neuen Sicherheitsschlüssel generieren und keine Verhandlung mit dem Schlüssel durchführen können. Die Lösung lässt sich am besten während der Fehlerbehebung und in einer kleinen statischen Umgebung einsetzen.

âf» [IKE mit Preshared Key](#) â€” Das Internet Key Exchange (IKE)-Protokoll dient zum automatischen Generieren und Austauschen eines Preshared Keys, um eine authentifizierte Kommunikation für den Tunnel herzustellen.

IPSec-Setup für manuellen Schlüsselmodus

IPSec Setup

Keying Mode :

Incoming SPI :

Outgoing SPI :

Encryption :

Authentication :

Encryption Key :

Authentication Key :

Schritt 1: Geben Sie den eindeutigen Hexadezimalwert für den eingehenden Sicherheitsparameterindex (Security Parameter Index, SPI) in das Feld Incoming SPI (Eingehender SPI) ein. SPI wird im Encapsulating Security Payload Protocol (ESP)-Header übertragen und bestimmt den Schutz für das eingehende Paket. Sie können einen Wert zwischen 100 und ffffff eingeben. Der eingehende SPI des lokalen Routers muss mit dem ausgehenden SPI des Remote-Routers übereinstimmen.

Schritt 2: Geben Sie den eindeutigen Hexadezimalwert für den ausgehenden Sicherheitsparameterindex (Security Parameter Index, SPI) in das Feld Ausgehender SPI ein. Sie können einen Wert zwischen 100 und ffffff eingeben. Der ausgehende SPI des Remote-Routers muss mit dem eingehenden SPI des lokalen Routers übereinstimmen.

Hinweis: Keine zwei Tunnel können denselben SPI haben.

IPSec Setup

Keying Mode :

Incoming SPI :

Outgoing SPI :

Encryption :

Authentication :

Encryption Key :

Authentication Key :

Schritt 3: Wählen Sie in der Dropdown-Liste Verschlüsselung die entsprechende Verschlüsselungsmethode für die Daten aus. Die empfohlene Verschlüsselung ist 3DES. Der VPN-Tunnel muss auf beiden Seiten die gleiche Verschlüsselungsmethode verwenden.

» DES - Data Encryption Standard (DES) verwendet eine Schlüssellänge von 56 Bit für die Datenverschlüsselung. DES ist veraltet und sollte nur verwendet werden, wenn nur ein Endpunkt DES unterstützt.

» 3DES - Triple Data Encryption Standard (3DES) ist eine einfache 168-Bit-

Verschlüsselungsmethode. 3DES verschlüsselt die Daten dreimal, wodurch mehr Sicherheit als DES geboten wird.

IPSec Setup

Keying Mode : Manual

Incoming SPI : 101

Outgoing SPI : 101

Encryption : 3DES

Authentication : MD5

Encryption Key : [] [] []

Authentication Key : []

Schritt 4: Wählen Sie in der Dropdown-Liste "Authentifizierung" die entsprechende Authentifizierungsmethode für die Daten aus. Die empfohlene Authentifizierung ist SHA1, da sie sicherer ist als MD5. Der VPN-Tunnel muss für beide Zwecke die gleiche Authentifizierungsmethode verwenden.

âf» MD5 â€” Message Digest Algorithm-5 (MD5) ist eine 128-Bit-Hash-Funktion, die die Daten durch die Prüfsummenberechnung vor böswilligen Angriffen schützt.

âf» SHA1 - Secure Hash Algorithm Version 1 (SHA1) ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5, aber mehr Zeit für die Berechnung benötigt.

IPSec Setup

Keying Mode : Manual

Incoming SPI : 101

Outgoing SPI : 101

Encryption : 3DES

Authentication : SHA1

Encryption Key : acb1230000000000 ab456fbc00000000 87600bca00000000

Authentication Key : acbd123400000000000000000000000000000000

Schritt 5: Geben Sie den Schlüssel zum Verschlüsseln und Entschlüsseln von Daten in das Feld Verschlüsselungsschlüssel ein. Wenn Sie DES als Verschlüsselungsmethode in Schritt 3 auswählen, geben Sie einen 16-stelligen Hexadezimalwert ein. Wenn Sie in Schritt 3 3DES als Verschlüsselungsmethode auswählen, geben Sie einen 40-stelligen Hexadezimalwert 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 SHA1 als Authentifizierungsmethode in Schritt 4 auswählen, geben Sie einen 40-stelligen Hexadezimalwert ein. Wenn Sie nicht genügend Ziffern hinzufügen, werden Nullen an das Ende angehängt, bis genügend Ziffern vorhanden sind. Der VPN-Tunnel muss für beide Enden denselben Pre-Shared Key verwenden.

Schritt 7. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

IKE mit Konfiguration des Modus für vorinstallierte Schlüssel

The screenshot shows the 'IPSec Setup' configuration interface. The 'Keying Mode' is set to 'IKE with Preshared key'. The 'Phase 1 DH Group' dropdown menu is open, displaying four options: 'Group 1 - 768 bit' (highlighted in blue), 'Group 1 - 768 bit', 'Group 2 - 1024 bit', and 'Group 5 - 1536 bit'. A red rectangle highlights the dropdown menu area. Other settings include 'Phase 1 Encryption' (MD5), 'Phase 1 Authentication' (MD5), 'Phase 1 SA Life Time' (28800 seconds), 'Perfect Forward Secrecy' (checked), 'Phase 2 DH Group' (Group 1 - 768 bit), 'Phase 2 Encryption' (DES), 'Phase 2 Authentication' (MD5), 'Phase 2 SA Life Time' (3600 seconds), 'Preshared Key' (empty field), 'Minimum Preshared Key Complexity' (checked, Enable), and 'Preshared Key Strength Meter' (a progress bar with four red segments).

Schritt 1: Wählen Sie in der Dropdown-Liste "Phase 1 DH Group" (DH-Gruppe für Phase 1) die gewünschte Phase 1 DH-Gruppe aus. Phase 1 wird verwendet, um die Simplex-Sicherheitszuordnung (Logical Security Association, SA) zwischen den beiden Tunnelenden herzustellen, die eine sichere Authentifizierungskommunikation unterstützt. Diffie-Hellman (DH) ist ein kryptographisches Schlüsselaustauschprotokoll, das verwendet wird, um die Stärke des Schlüssels während Phase 1 zu bestimmen, und es teilt sich auch den geheimen Schlüssel, um die Kommunikation zu authentifizieren.

âf» Gruppe 1 - 768 Bit - Der Schlüssel mit der niedrigsten Stärke und die unsicherste Authentifizierungsgruppe. Die IKE-Schlüssel werden jedoch am wenigsten berechnet. Diese Option wird bevorzugt, wenn die Netzwerkgeschwindigkeit niedrig ist.

âf» Gruppe 2 - 1024 Bit - Ein Schlüssel mit höherer Stärke und eine sicherere Authentifizierungsgruppe als Gruppe 1. Die Berechnung der IKE-Schlüssel nimmt jedoch mehr Zeit in Anspruch.

âf» Gruppe 5 - 1536 Bit - Der Schlüssel mit der höchsten Stärke und die sicherste Authentifizierungsgruppe. Die IKE-Schlüssel müssen schneller berechnet werden. Es ist bevorzugt, wenn die Geschwindigkeit des Netzwerks hoch ist.

IPSec Setup

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

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

Phase 1 Authentication :

Phase 1 SA Life Time :

Perfect Forward Secrecy :

Phase 2 DH Group :

Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time : seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Schritt 2: Wählen Sie in der Dropdown-Liste "Phase 1 Encryption" (Verschlüsselung der Phase 1) die entsprechende Phase 1-Verschlüsselung aus, um den Schlüssel zu verschlüsseln. AES-128, AES-192 oder AES-256 wird empfohlen. Der VPN-Tunnel muss für beide Enden die gleiche Verschlüsselungsmethode verwenden.

âf» DES - Data Encryption Standard (DES) verwendet eine Schlüssellänge von 56 Bit für die Datenverschlüsselung. DES ist veraltet und sollte nur verwendet werden, wenn nur ein Endpunkt DES unterstützt.

âf» 3DES - Triple Data Encryption Standard (3DES) ist eine einfache 168-Bit-Verschlüsselungsmethode. 3DES verschlüsselt die Daten dreimal, wodurch mehr Sicherheit als DES geboten wird.

âf» AES-128 â€” Advanced Encryption Standard (AES) ist eine 128-Bit-Verschlüsselungsmethode, die den Klartext durch 10-Zyklen-Wiederholungen in verschlüsselten Text umwandelt.

âf» AES-192 â€” Advanced Encryption Standard (AES) ist eine 192-Bit-Verschlüsselungsmethode, die den Klartext durch 12 Zyklen Wiederholungen in Text umwandelt. AES-192 ist sicherer als AES-128.

âf» AES-256 â€” Advanced Encryption Standard (AES) ist eine 256-Bit-Verschlüsselungsmethode, die den Klartext durch 14 Zyklen Wiederholungen in Text umwandelt. AES-256 ist die sicherste Verschlüsselungsmethode.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time :

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

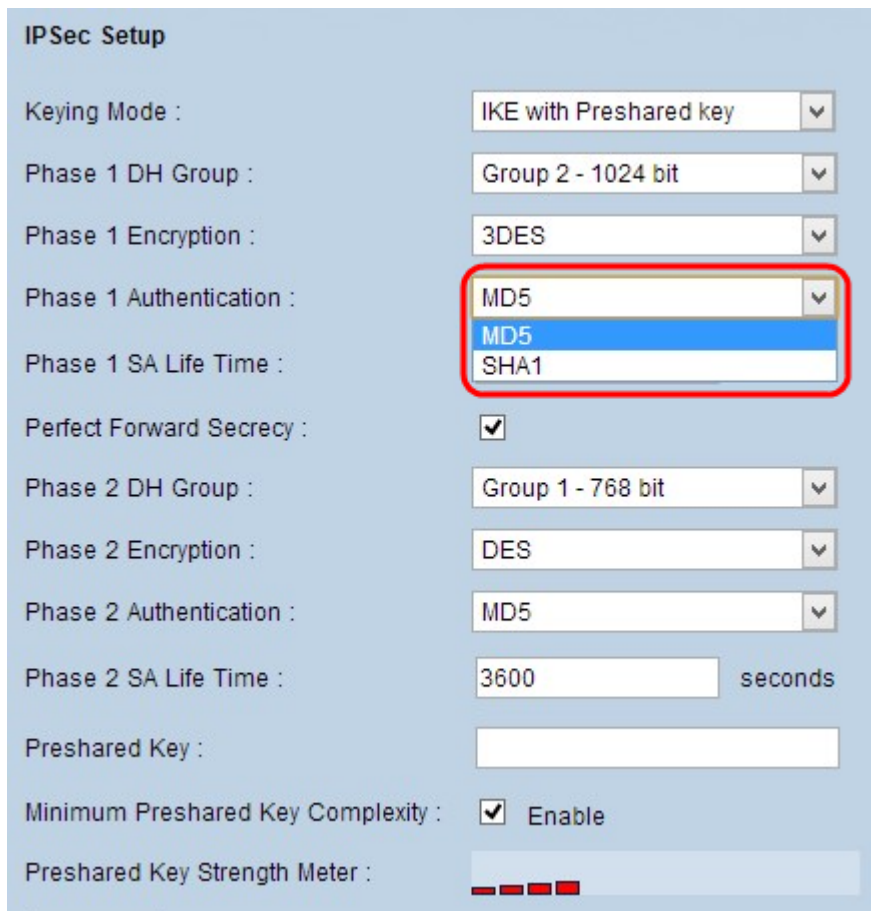
Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :



Schritt 3: Wählen Sie in der Dropdown-Liste "Authentifizierung Phase 1" die entsprechende Authentifizierungsmethode für Phase 1 aus. Der VPN-Tunnel muss für beide Enden die gleiche Authentifizierungsmethode verwenden. SHA1 wird empfohlen.

âf» MD5 â€” Message Digest Algorithm-5 (MD5) ist eine 128-Bit-Hash-Funktion, die die Daten durch die Prüfsummenberechnung vor böswilligen Angriffen schützt.

âf» SHA1 - Secure Hash Algorithm Version 1 (SHA1) ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5, aber mehr Zeit für die Berechnung benötigt.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 27800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

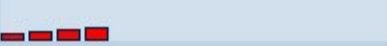
Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :



Schritt 4: Geben Sie im Feld "SA-Lebensdauer der Phase 1" die Zeit in Sekunden ein, während der die Schlüssel für Phase 1 gültig sind und der VPN-Tunnel aktiv bleibt.

Schritt 5: Aktivieren Sie das Kontrollkästchen **Perfect Forward Secrecy** (Perfektes Weiterleitungsgeheimnis), um die Schlüssel besser zu schützen. Mit dieser Option kann der Router einen neuen Schlüssel generieren, wenn ein Schlüssel kompromittiert wird. Die verschlüsselten Daten werden nur durch den kompromittierten Schlüssel kompromittiert. Dies ist eine empfohlene Aktion, da sie mehr Sicherheit bietet.

IPSec Setup

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time : seconds

Perfect Forward Secrecy :

Phase 2 DH Group :

Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time : seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Schritt 6: Wählen Sie in der Dropdown-Liste "Phase 2 DH Group" (DH-Gruppe für Phase 2) die entsprechende DH-Gruppe aus. Phase 2 nutzt die Sicherheitszuordnung und wird verwendet, um die Sicherheit des Datenpakets beim Durchlaufen der beiden Endpunkte zu bestimmen.

» Gruppe 1 - 768 Bit - Der Schlüssel mit der niedrigsten Stärke und die unsicherste Authentifizierungsgruppe. Die IKE-Schlüssel werden jedoch am wenigsten berechnet. Diese Option wird bevorzugt, wenn die Netzwerkgeschwindigkeit niedrig ist.

» Gruppe 2 - 1024 Bit - Ein Schlüssel mit höherer Stärke und eine sicherere Authentifizierungsgruppe als Gruppe 1. Die Berechnung der IKE-Schlüssel dauert jedoch länger.

» Gruppe 5 - 1536 Bit » Der Schlüssel mit der höchsten Stärke und die sicherste Authentifizierungsgruppe. Die IKE-Schlüssel müssen schneller berechnet werden. Es ist bevorzugt, wenn die Geschwindigkeit des Netzwerks hoch ist.

IPSec Setup

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time : seconds

Perfect Forward Secrecy :

Phase 2 DH Group :

Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Schritt 7. Wählen Sie in der Dropdown-Liste "Phase 2 Encryption" (Verschlüsselung der Phase 2) die geeignete Phase 2-Verschlüsselung aus, um den Schlüssel zu verschlüsseln. AES-128, AES-192 oder AES-256 wird empfohlen. Der VPN-Tunnel muss für beide Enden die gleiche Verschlüsselungsmethode verwenden.

âf» NULL â€" Es wird keine Verschlüsselung verwendet.

âf» DES - Data Encryption Standard (DES) verwendet eine Schlüssellänge von 56 Bit für die Datenverschlüsselung. DES ist veraltet und sollte nur verwendet werden, wenn nur ein Endpunkt DES unterstützt.

âf» 3DES - Triple Data Encryption Standard (3DES) ist eine einfache 168-Bit-Verschlüsselungsmethode. 3DES verschlüsselt die Daten dreimal, wodurch mehr Sicherheit als DES geboten wird.

âf» AES-128 â€" Advanced Encryption Standard (AES) ist eine 128-Bit-Verschlüsselungsmethode, die den Klartext durch 10-Zykluswiederholungen in verschlüsselten Text umwandelt.

âf» AES-192 â€" Advanced Encryption Standard (AES) ist eine 192-Bit-Verschlüsselungsmethode, die den Klartext durch 12 Zykluswiederholungen in verschlüsselten Text umwandelt. AES-192 ist sicherer als AES-128.

âf» AES-256 â€" Advanced Encryption Standard (AES) ist eine 256-Bit-Verschlüsselungsmethode, die den Klartext durch 14 Wiederholungen in Chiffre-Text umwandelt. AES-256 ist die sicherste Verschlüsselungsmethode.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 27800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 2 - 1024 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Schritt 8: Wählen Sie in der Dropdown-Liste "Authentifizierung in Phase 2" die entsprechende Authentifizierungsmethode aus. Der VPN-Tunnel muss für beide Zwecke die gleiche Authentifizierungsmethode verwenden. SHA1 wird empfohlen.

âf» MD5 â€” Message Digest Algorithm-5 (MD5) ist eine hexadezimale Hash-Funktion mit 128 Bit, die die Daten durch die Prüfsummenberechnung vor böswilligen Angriffen schützt.

âf» SHA1 - Secure Hash Algorithm Version 1 (SHA1) ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5, aber mehr Zeit für die Berechnung benötigt.

âf» Null â€” Es wird keine Authentifizierungsmethode verwendet.

IPSec Setup

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time : seconds

Perfect Forward Secrecy :

Phase 2 DH Group :


Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time : seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Schritt 9. Geben Sie im Feld "SA-Lebensdauer der Phase 2" die Zeit in Sekunden ein, während der die Schlüssel für Phase 2 gültig sind und der VPN-Tunnel aktiv bleibt.

Schritt 10. Geben Sie einen Schlüssel ein, der zuvor von den IKE-Peers zur Authentifizierung der Peers im Feld Vorinstallierter Schlüssel gemeinsam verwendet wird. Als vorinstallierter Schlüssel können bis zu 30 Hexadezimal- und Zeichencodes verwendet werden. Der VPN-Tunnel muss für beide Enden denselben Pre-Shared Key verwenden.

Hinweis: Es wird dringend empfohlen, den vorinstallierten Schlüssel für die IKE-Peers regelmäßig zu ändern, um den VPN-Schutz zu gewährleisten.

Schritt 11. (Optional) Wenn Sie den Kraftmesser für den vorinstallierten Schlüssel aktivieren möchten, aktivieren Sie das Kontrollkästchen **Minimale vorinstallierte Schlüsselkomplexität**. Er wird verwendet, um die Stärke des vorinstallierten Schlüssels durch Farbbalken zu bestimmen.

âf» Messgerät für die Stärke des vorinstallierten Schlüssels â€” Zeigt die Stärke des vorinstallierten Schlüssels durch farbige Balken an. Rot bedeutet schwache Festigkeit, Gelb bedeutet akzeptable Festigkeit und Grün bedeutet starke Festigkeit.

Schritt 12: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Hinweis: Wenn Sie die im Abschnitt *Advanced (Erweitert)* verfügbaren Optionen für Gateway to Gateway VPN konfigurieren möchten, lesen Sie den Artikel [Configure Advanced Settings for Gateway to Gateway VPN on RV016, RV042, RV042G, and RV082 VPN Routers \(Erweiterte Einstellungen für Gateway zu VPN auf RV0010 konfigurieren\)](#).

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.