

Richten Sie auf den VPN-Routern RV016, RV042, RV042G und RV082 einen Remote Access Tunnel (Client-to-Gateway) für VPN-Clients ein.

Ziel

In diesem Artikel wird erläutert, wie der Virtual Private Network (VPN)-Tunnel für den Remote-Zugriff von Client zu Gateway auf den VPN-Routern RV016, RV042, RV042G und RV082 mithilfe von VPN-Client-Software von Drittanbietern wie The Green Bow oder VPN Tracker konfiguriert wird.

Einleitung

Ein VPN ist ein privates Netzwerk, das verwendet wird, um Geräte des Remote-Benutzers virtuell über das öffentliche Netzwerk zu verbinden, um die Sicherheit zu gewährleisten. Remote Access Tunnel VPN ist der Prozess, mit dem ein VPN zwischen einem Client-Computer und einem Netzwerk konfiguriert wird. Der Client wird über die VPN-Client-Software auf dem Desktop oder Laptop der Benutzer konfiguriert. Es bietet Benutzern die Möglichkeit, eine sichere Remote-Verbindung mit dem Netzwerk herzustellen. Eine Client-to-Gateway-VPN-Verbindung ist für Mitarbeiter an Remote-Standorten nützlich, um eine sichere Remote-Verbindung mit dem Büronetzwerk herzustellen.

Unterstützte Geräte

- RV016
- RV042
- RV042G
- RV082

Software-Version

- Version 4.2.2.08

Konfigurieren eines VPN-Tunnels

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

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. 1

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 Client Setup

Remote Security Gateway Type : ▼

▼ :

IPSec Setup

Neuen Tunnel hinzufügen

Schritt 1: Klicken Sie auf das entsprechende Optionsfeld für den Tunnel, den Sie hinzufügen möchten.

- Tunnel - Stellt einen Tunnel für einen einzelnen Remote-Benutzer dar.
- Gruppen-VPN - Stellt einen Tunnel für eine entfernte Benutzergruppe dar.

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. : 1

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 Client Setup

Remote Security Gateway Type :

:

IPSec Setup

Die Tunnelnummer ist ein automatisch generiertes Feld, in dem die Nummer des Tunnels angezeigt wird.

Client To Gateway

Add a New Tunnel

Tunnel
 Group VPN

Tunnel No. : 1
 Tunnel Name : tunnel_1
 Interface : WAN1
 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 :

IPSec Setup

Schritt 2: Geben Sie im Feld Tunnelname einen Namen für den Tunnel ein.

Schritt 3: Wählen Sie aus der Dropdown-Liste Interface (Schnittstelle) die passende WAN-Schnittstelle für den VPN-Tunnel aus.

Schritt 4: (Optional) Um das VPN zu aktivieren, aktivieren Sie das Kontrollkästchen im Feld Aktivieren. Standardmäßig ist diese Option immer aktiviert.

Lokale Gruppeneinrichtung

Schritt 1: Wählen Sie in der Dropdown-Liste *Local Security Gateway (Lokales Sicherheits-Gateway)* die geeignete Methode zur Routeridentifizierung aus, um einen VPN-Tunnel einzurichten. Überspringen Sie diesen Schritt, wenn Sie in Schritt 1 des Abschnitts "Neuen Tunnel hinzufügen" Group VPN ausgewählt haben.

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. : 1

Tunnel Name : tunnel_1

Interface : WAN1

Enable :

Local Group Setup

Local Security Gateway Type : IP Only

IP Address : []

Local Security Group Type : []

IP Address : []

Subnet Mask : 255.255.255.0

Remote Client Setup

Remote Security Gateway Type : IP Only

IP Address : []

IPSec Setup

Keying Mode : IKE with Preshared key

- Nur IP - Der Zugriff auf den Tunnel ist über eine statische WAN-IP-Adresse möglich. Sie können diese Option nur auswählen, wenn der Router über eine statische WAN-IP verfügt. Die statische WAN-IP-Adresse wird automatisch angezeigt.
- IP + Domain Name (FQDN) Authentication - Der Zugriff auf den Tunnel ist über eine statische IP-Adresse und eine registrierte FQDN-Domäne (Fully Qualified Domain Name) möglich. Die statische WAN-IP-Adresse wird automatisch generiert.
- IP + E-Mail-Adresse (USER FQDN) Authentifizierung - Der Zugriff auf den Tunnel ist über eine statische IP-Adresse und eine E-Mail-Adresse möglich. Die statische WAN-IP-Adresse wird automatisch generiert.
- Dynamische IP + Domain Name (FQDN)-Authentifizierung - Der Zugriff auf den Tunnel ist über eine dynamische IP-Adresse und eine registrierte Domäne möglich.
- 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.

Schritt 2: Geben Sie den Namen der registrierten vollqualifizierten Domäne in das Feld Domain Name (Domänenname) ein, wenn Sie in Schritt 1 die Option *IP + Domain Name (FQDN) Authentication (IP- + Domänenname)* oder *Dynamic IP + Domain Name (FQDN) Authentication (dynamische IP + Domänenname)* wählen.

Schritt 3: Geben Sie die E-Mail-Adresse in das Feld "E-Mail-Adresse" ein, wenn Sie in Schritt 1 die Option *IP + E-Mail-Adresse (USER FQDN) Authentifizierung* oder *Dynamische IP + E-Mail-Adresse (USER FQDN) Authentifizierung* wählen.

Schritt 4: Wählen Sie in der Dropdown-Liste "Lokale Sicherheitsgruppe" den entsprechenden lokalen LAN-

Benutzer oder die entsprechende Benutzergruppe aus, die 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 auswählen, geben Sie die IP-Adresse des LAN-Geräts in das 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 auswählen, geben Sie die IP-Adresse und die Subnetzmaske der LAN-Geräte in die entsprechenden Felder IP Address (IP-Adresse) und Subnet Mask (Subnetzmaske) ein. Die Standardmaske ist 255.255.255.0.
- 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. Der Standardbereich liegt zwischen 192.168.1.0 und 192.168.1.254.

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. : 1

Tunnel Name : tunnel_1

Interface : WAN1

Enable :

Local Group Setup

Local Security Gateway Type : IP Only

IP Address : 0.0.0.0

Local Security Group Type : Subnet (dropdown menu open, options: Subnet, IP, Subnet, IP Range)

IP Address :

Subnet Mask : 255.255.255.0

Remote Client Setup

Remote Security Gateway Type : IP Only

IP Address :

IPSec Setup

Keying Mode : IKE with Preshared key

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

Remote-Client-Einrichtung

Schritt 1: Wenn Sie Tunnel auswählen, wählen Sie in der Dropdown-Liste *Remote Security Gateway Type* (*Remote-Sicherheits-Gateway-Typ*) die geeignete Methode zur Client-Identifizierung aus, um einen VPN-Tunnel einzurichten. Der Standardwert ist "Nur IP". Überspringen Sie diesen Schritt, wenn Sie im Abschnitt *Add A New Tunnel* (*Neuen Tunnel hinzufügen*) in Schritt 1 die Option *Group VPN* ausgewählt haben.

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. : 1

Tunnel Name :

Interface :

Enable :

Local Group Setup

Local Security Gateway Type :

IP Address :

Local Security Group Type :

IP Address :

Subnet Mask :

Remote Client Setup

Remote Security Gateway Type :

:

IPSec Setup

Keying Mode :

- Nur IP - Der Zugriff auf den Tunnel ist nur über die statische WAN-IP des Clients möglich. Sie müssen die statische WAN-IP des Clients kennen, um diese Option verwenden zu können.
- IP + Domain Name (FQDN) Authentication - Der Zugriff auf den Tunnel ist über eine statische IP-Adresse des Clients und eine registrierte Domäne möglich.
- IP + E-Mail-Adresse (USER FQDN) Authentifizierung - Der Zugriff auf den Tunnel ist über eine statische IP-Adresse des Clients und eine E-Mail-Adresse möglich.
- Dynamische IP + Domain Name (FQDN)-Authentifizierung - Der Zugriff auf den Tunnel ist über eine dynamische IP-Adresse des Clients und eine registrierte Domäne möglich.
- Dynamische IP + E-Mail-Adresse (USER FQDN) Authentifizierung - Der Zugriff auf den Tunnel ist über eine dynamische IP-Adresse des Clients und eine E-Mail-Adresse möglich.

Schritt 2: Geben Sie die IP-Adresse des Remote-Clients in das Feld *IP-Adresse* ein, wenn Sie in Schritt 1 die *Authentifizierungsmethode* Nur IP + Domänenname (FQDN) oder IP + E-Mail-Adresse (Benutzer-FQDN) ausgewählt haben.

Schritt 3: Wählen Sie die entsprechende Option aus der Dropdown-Liste aus, um die bekannte IP-Adresse einzugeben, oder lösen Sie die IP-Adresse vom DNS-Server auf, wenn Sie in Schritt 1 die *Authentifizierung* Nur IP oder IP + Domänenname (FQDN) oder IP + E-Mail-Adresse (USER FQDN) wählen.

- IP-Adresse - Stellt die statische IP-Adresse des Remote-Clients dar. Geben Sie die statische IP-Adresse in das Feld ein.
- IP by DNS Resolved (IP durch DNS aufgelöst): Stellt den Domännennamen der IP-Adresse dar, die die IP-Adresse automatisch über den lokalen DNS-Server abrufen, wenn Sie die statische IP-Adresse des Remote-Clients nicht kennen. Geben Sie den Domännennamen der IP-Adresse in das Feld ein.

Schritt 4: Geben Sie den Domännennamen der IP-Adresse in das Feld Domänenname ein, wenn Sie in Schritt 1 die Optionen *IP + Domänenname (FQDN)-Authentifizierung* oder *Dynamische IP + Domänenname (FQDN)-Authentifizierung* auswählen.

Schritt 5: Geben Sie die E-Mail-Adresse in das Feld E-Mail-Adresse ein, wenn Sie in Schritt 1 die Option *IP + E-Mail-Adresse (USER FQDN) Authentifizierung* oder *Dynamische IP + E-Mail-Adresse (USER FQDN) Authentifizierung* wählen.

Schritt 6: Wenn Sie Group (Gruppe) auswählen, wählen Sie in der Dropdown-Liste *Remote Client (Remote-Client)* den entsprechenden Remote-Client-Typ aus. Überspringen Sie diesen Schritt, wenn Tunnel VPN in Schritt 1 des Abschnitts *Add A New Tunnel* ausgewählt wurde.

- Domain Name (FQDN) - Der Zugriff auf den Tunnel ist über eine registrierte Domäne möglich. Wenn Sie diese Option wählen, geben Sie den Namen der registrierten Domäne in das Feld Domain Name (Domänenname) ein.
- E-Mail-Adresse (USER FQDN) - Der Zugriff auf den Tunnel ist über eine E-Mail-Adresse des Clients möglich. Wenn Sie diese Option wählen, geben Sie die E-Mail-Adresse in das Feld E-Mail-Adresse ein.
- Microsoft XP/2000 VPN Client - Der Zugriff auf den Tunnel ist über Microsoft XP oder Microsoft 2000 Windows-Software möglich. Remote-Benutzer mit Microsoft VPN-Client-Software können über die Software auf den Tunnel zugreifen.

Client To Gateway

Add a New Group VPN

Tunnel Group VPN

Group No. 1

Tunnel Name : Tunnel_2

Interface : WAN2

Enable :

Local Group Setup

Local Security Group Type : Subnet

IP Address : 192.168.1.0

Subnet Mask : 255.255.255.0

Remote Client Setup

Remote Client : Microsoft XP/2000 VPN Client

Domain Name(FQDN)

Email Address(USER FQDN)

Microsoft XP/2000 VPN Client

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

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

IPSec-Einrichtung

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: Damit IPSec funktioniert, müssen beide Enden des VPNs die gleichen Verschlüsselungs-, Entschlüsselungs- und Authentifizierungsmethoden haben. Der Schlüssel Perfect Forward Secrecy muss auf beiden Seiten des Tunnels gleich sein.

Schritt 1: Wählen Sie den entsprechenden Modus für die Schlüsselverwaltung aus, um die Sicherheit aus der Dropdown-Liste "*Keying Mode*" (Schlüsselmodus) sicherzustellen. Der Standardmodus ist *IKE mit vorinstalliertem Schlüssel*.

- **Manual (Manuell)** - Ein benutzerdefinierter Sicherheitsmodus zum Generieren eines neuen Sicherheitsschlüssels durch Sie selbst und ohne Verhandlung mit dem Schlüssel. Es ist am besten bei der Fehlerbehebung und in kleinen statischen Umgebungen zu verwenden. Wenn Sie in Schritt 1 im Abschnitt "Add A New Tunnel" die Option Group VPN (Gruppen-VPN) auswählen, ist diese Option deaktiviert.
- **IKE mit vorinstalliertem Schlüssel** - Das IKE-Protokoll (Internet Key Exchange) dient zum automatischen Generieren und Austauschen eines vorinstallierten Schlüssels, um eine authentifizierte Kommunikation für den Tunnel herzustellen.

Subnet Mask : 255.255.255.0

Remote Client Setup

Remote Security Gateway Type : IP Only

IP Address : 192.168.1.2

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group :

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 +

Manuelle Konfiguration des Schlüsselmodus

Schritt 1: Geben Sie den eindeutigen Hexadezimalwert für den eingehenden Sicherheitsparameterindex (Security Parameter Index, SPI) in das Feld *Eingehender SPI ein*. SPI wird im Encapsulating Security Payload Protocol (ESP)-Header transportiert, der zusammen den Schutz für das eingehende Paket bestimmt. Sie können zwischen 100 und fffff wählen. 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*. SPI wird im Encapsulating Security Payload Protocol (ESP)-Header transportiert, der zusammen den Schutz für das ausgehende Paket bestimmt. Sie können zwischen 100 und fffff wählen. Der ausgehende SPI des Remote-Routers muss mit dem eingehenden SPI des lokalen Routers übereinstimmen.

The screenshot shows a configuration interface with two main sections: "Remote Client Setup" and "IPSec Setup".

Remote Client Setup

- Remote Security Gateway Type : IP Only
- IP Address : 192.168.1.2

IPSec Setup

- Keying Mode : Manual
- Incoming SPI : 100A
- Outgoing SPI : 1BCD
- Encryption : DES
- Authentication : MD5
- Encryption Key : [empty field]
- Authentication Key : [empty field]

The "Incoming SPI" and "Outgoing SPI" fields are highlighted with a red rectangular box.

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 für beide Zwecke 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 :

Incoming SPI :

Outgoing SPI :

Encryption :

Authentication :

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.

- MD5 - Message Digest Algorithm-5 (MD5) stellt eine 32-stellige Hexadezimal-Hash-Funktion 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, aber mehr Zeit für die Berechnung benötigt.

IPSec Setup

Keying Mode :

Incoming SPI :

Outgoing SPI :

Encryption :

Authentication :

Encryption Key :

Authentication Key :

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 einen vorinstallierten Schlüssel ein, um den Datenverkehr im Feld *Authentifizierungsschlüssel* zu authentifizieren. Wenn Sie in Schritt 4 MD5 als Authentifizierungsmethode auswählen, geben Sie einen 32-stelligen Hexadezimalwert ein. Wenn Sie SHA als Authentifizierungsmethode in Schritt 4 auswählen, geben Sie einen 40-stelligen Hexadezimalwert ein. Der VPN-Tunnel muss für beide Enden denselben Pre-Shared Key verwenden.

IPSec Setup

Keying Mode :

Incoming SPI :

Outgoing SPI :

Encryption :

Authentication :

Encryption Key :

Authentication Key :

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

IKE mit Konfiguration des Modus für vorinstallierte Schlüssel

Schritt 1: Wählen Sie aus der Dropdown-Liste "*Phase 1 DH Group*" (*Phase 1 DH-Gruppe*) die entsprechende 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.

- Gruppe 1 - 768 Bit - Der Schlüssel mit der niedrigsten Stärke und die unsicherste Authentifizierungsgruppe. Die IKE-Schlüssel lassen sich jedoch in kürzerer Zeit berechnen. Diese Option wird bevorzugt, wenn die Netzwerkgeschwindigkeit niedrig ist.
- Gruppe 2 - 1024 Bit - Der leistungsstärkere Schlüssel und die sicherere Authentifizierungsgruppe. Die IKE-Schlüssel können jedoch erst nach einiger Zeit berechnet werden.
- Gruppe 5 - 1536 Bit - Stellt den Schlüssel mit der höchsten Stärke und die sicherste Authentifizierungsgruppe dar. Die IKE-Schlüssel müssen schneller berechnet werden. Es ist bevorzugt, wenn die Geschwindigkeit des Netzwerks hoch ist.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : Group 1 - 768 bit

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 +

Schritt 2: Wählen Sie in der Dropdown-Liste "Phase 1 Encryption" (*Verschlüsselung der Phase 1*) die geeignete Phase 1-Verschlüsselung aus, um den Schlüssel zu verschlüsseln. 3DES wird empfohlen, da es die sicherste Verschlüsselungsmethode ist. Der VPN-Tunnel muss für beide Enden 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.
- AES-128 - Advanced Encryption Standard (AES) ist eine 128-Bit-Verschlüsselungsmethode, die den Klartext durch 10 Zyklen Wiederholungen in Text umwandelt.
- AES-192 - 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.
- AES-256 - 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 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication : DES

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 : 

Advanced +

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

- MD5 - Message Digest Algorithm-5 (MD5) stellt eine 32-stellige Hexadezimal-Hash-Funktion 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, aber mehr Zeit für die Berechnung benötigt.

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 : 3600 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 +

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. Dadurch wird die Kommunikation sicherer und authentifizierter, da auch andere Schlüssel gesichert werden, wenn ein Schlüssel kompromittiert wird. 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 :

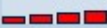
Phase 2 Encryption :

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*" (*Phase 2 DH-Gruppe*) die entsprechende Phase 2 DH-Gruppe aus. Phase 2 nutzt die Sicherheitszuordnung und wird verwendet, um die Sicherheit des Datenpakets während des Durchlaufs der Datenpakete durch die beiden Endpunkte zu bestimmen.

- Gruppe 1 - 768 Bit - Stellt den Schlüssel mit der niedrigsten Stärke und die unsicherste Authentifizierungsgruppe dar. Die IKE-Schlüssel lassen sich jedoch in kürzerer Zeit berechnen. Es ist bevorzugt, wenn die Geschwindigkeit des Netzwerks niedrig ist.
- Gruppe 2 - 1024 Bit - Stellt einen Schlüssel mit höherer Stärke und eine sicherere Authentifizierungsgruppe dar. Die IKE-Schlüssel können jedoch erst nach einiger Zeit berechnet werden.
- Gruppe 5 - 1536 Bit - Stellt den Schlüssel mit der höchsten Stärke und die sicherste Authentifizierungsgruppe dar. Die IKE-Schlüssel müssen schneller berechnet werden. Es ist bevorzugt, wenn die Geschwindigkeit des Netzwerks hoch ist.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : MD5

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Advanced +

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-256 wird empfohlen, da es die sicherste Verschlüsselungsmethode ist. Der VPN-Tunnel muss für beide Enden 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.
- AES-128 - Advanced Encryption Standard (AES) ist eine 128-Bit-Verschlüsselungsmethode, die den Klartext durch 10 Zyklen Wiederholungen in Text umwandelt.
- AES-192 - 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.
- AES-256 - 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 : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit


Phase 2 Encryption : DES

Phase 2 Authentication : **DES**

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Advanced +

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

- MD5 - Message Digest Algorithm-5 (MD5) stellt eine 32-stellige Hexadezimal-Hash-Funktion 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, aber mehr Zeit für die Berechnung benötigt.
- Null - Es wird keine Authentifizierungsmethode verwendet.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 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 :

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Advanced +

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 *Preshared Key (Vorinstallierter Schlüssel)* 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. Aktivieren Sie das Kontrollkästchen **Minimale vorinstallierte Schlüsselkomplexität**, wenn Sie den Stärkemesser für den vorinstallierten Schlüssel aktivieren möchten. Er wird verwendet, um die Stärke des vorinstallierten Schlüssels durch Farbbalken zu bestimmen

Hinweis: Das Messgerät für die Stärke des vorinstallierten Schlüssels zeigt die Stärke des vorinstallierten Schlüssels durch farbige Balken an. Rot bedeutet schwache Festigkeit, Gelb bedeutet akzeptable Festigkeit und Grün bedeutet starke Festigkeit.

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

Erweitertes IKE mit Konfiguration des Modus für vorinstallierte Schlüssel

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

Advanced

Aggressive Mode

Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive

AH Hash Algorithm

NetBIOS Broadcast

NAT Traversal

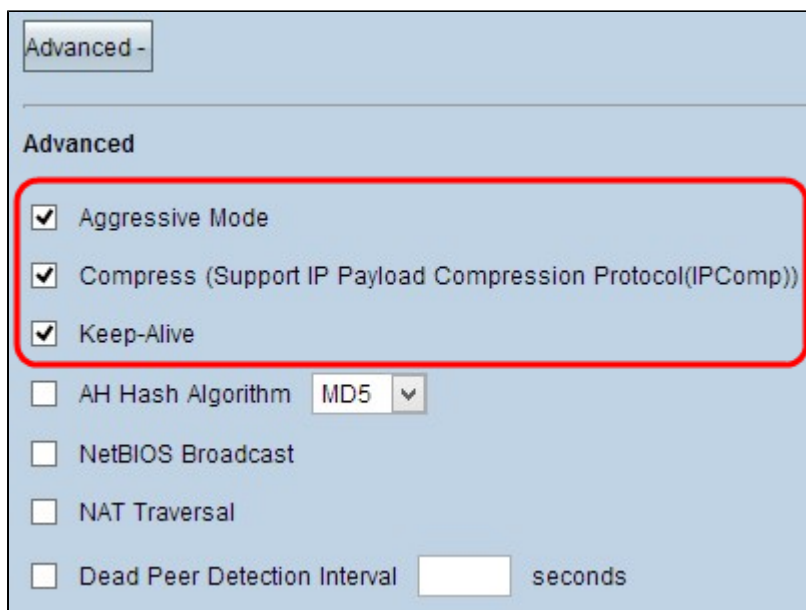
Dead Peer Detection Interval seconds

Schritt 2: Aktivieren Sie das Kontrollkästchen **Aggressive Mode** (Aggressiver Modus), wenn Ihre Netzwerkgeschwindigkeit niedrig ist. Dadurch werden die IDs der Endpunkte des Tunnels während der SA-Verbindung (Phase 1) im Klartext ausgetauscht, was weniger Zeit für den Austausch benötigt, aber weniger Sicherheit bietet.

Hinweis: Der aggressive Modus ist für die Gruppen-Client-Gateway-VPN-Verbindung nicht verfügbar.

Schritt 3: Aktivieren Sie das Kontrollkästchen **Compress (Support IP Payload Compression Protocol (IPComp))**, wenn Sie die Größe der IP-Datagramme komprimieren möchten. IPComp ist ein IP-Komprimierungsprotokoll, mit dem die Größe von IP-Datagrammen komprimiert wird. Die IP-Komprimierung ist nützlich, wenn die Netzwerkgeschwindigkeit niedrig ist und der Benutzer die Daten schnell und ohne Verluste über das langsame Netzwerk übertragen möchte, jedoch keine Sicherheit bietet.

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



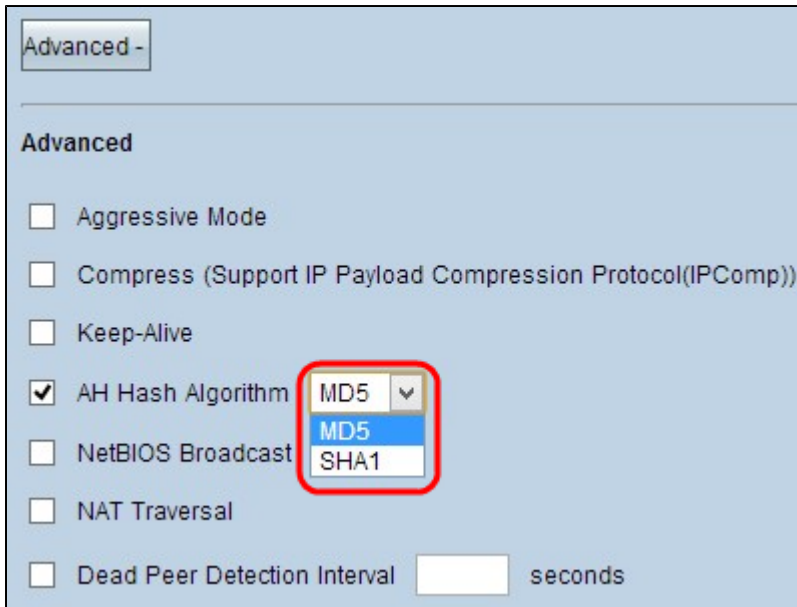
Advanced -

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol (IPComp))
- Keep-Alive
- AH Hash Algorithm MD5
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval 0 seconds

Schritt 5: Aktivieren Sie das Kontrollkästchen **AH Hash Algorithm**, wenn Sie Authenticate Header (AH) aktivieren möchten. AH bietet Authentifizierung für Ursprungsdaten, Datenintegrität durch Prüfsumme und Schutz im IP-Header. Der Tunnel sollte für beide Seiten den gleichen Algorithmus haben.

- MD5 - Message Digest Algorithm-5 (MD5) stellt eine 128-stellige Hexadezimal-Hashfunktion 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, aber mehr Zeit für die Berechnung benötigt.

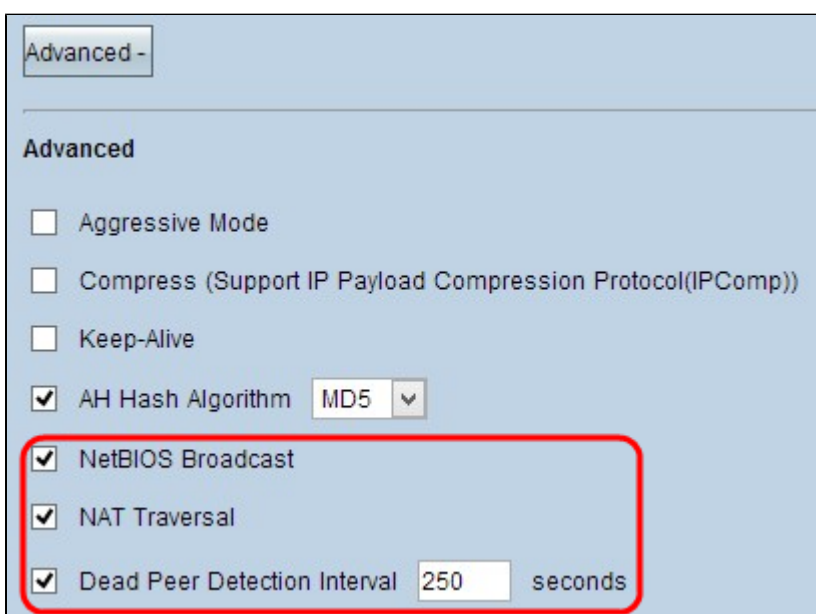


Schritt 6: Aktivieren Sie **NetBIOS Broadcast**, wenn Sie nicht routbaren Datenverkehr durch den VPN-Tunnel zulassen möchten. Standardmäßig ist diese Option deaktiviert. NetBIOS wird verwendet, um Netzwerkressourcen wie Drucker, Computer usw. im Netzwerk über einige Softwareanwendungen und Windows-Funktionen wie Netzwerkumgebung zu erkennen.

Schritt 7. Aktivieren Sie das Kontrollkästchen **NAT Traversal**, wenn Sie über eine öffentliche IP-Adresse von Ihrem privaten LAN aus auf das Internet zugreifen möchten. Wenn sich Ihr VPN-Router hinter einem NAT-Gateway befindet, aktivieren Sie dieses Kontrollkästchen, um NAT-Traversal zu aktivieren. Beide Enden des Tunnels müssen die gleichen Einstellungen aufweisen.

Schritt 8: Überprüfen Sie das **Intervall für die Erkennung von abgestorbenen Peers**, um die Lebhaftigkeit des VPN-Tunnels durch hello oder ACK in regelmäßigen Abständen zu überprüfen. Wenn Sie dieses Kontrollkästchen aktivieren, geben Sie die gewünschte Dauer oder das gewünschte Intervall für die Begrüßungsmeldungen ein.

Hinweis: Sie können das Intervall für die Dead Peer-Erkennung nur für die VPN-Verbindung zwischen einem Client und Gateway konfigurieren, nicht für die VPN-Verbindung zwischen Gruppen-Client und Gateway.



Schritt 9. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Nun weißt du, wie man einen VPN-Tunnel für den Remote-Zugriff auf den VPN-Routern RV016, RV042, RV042G und RV082 von Client zu Gateway konfiguriert.

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.