VPN-Konfiguration (Gateway to Gateway Virtual Private Network) auf den VPN-Routern der Serien RV320 und RV325

Ziel

VPNs werden zur Herstellung sehr sicherer Verbindungen über zwei Endpunkte über das öffentliche oder gemeinsam genutzte Internet über einen so genannten VPN-Tunnel verwendet. Insbesondere eine Gateway-to-Gateway-VPN-Verbindung ermöglicht es zwei Routern, sich sicher miteinander zu verbinden, und einem Client an einem Ende wird logisch der Eindruck vermittelt, dass er Teil desselben Remote-Netzwerks am anderen Ende ist. So können Daten und Ressourcen einfacher und sicherer über das Internet gemeinsam genutzt werden. Die Konfiguration muss auf beiden Seiten der Verbindung erfolgen, damit eine erfolgreiche Gateway-to-Gateway-VPN-Verbindung hergestellt werden kann. Dieser Artikel enthält eine Anleitung zur Konfiguration einer Gateway-to-Gateway-VPN-Verbindung auf der RV32x VPN-Router-Serie.

Anwendbare Geräte

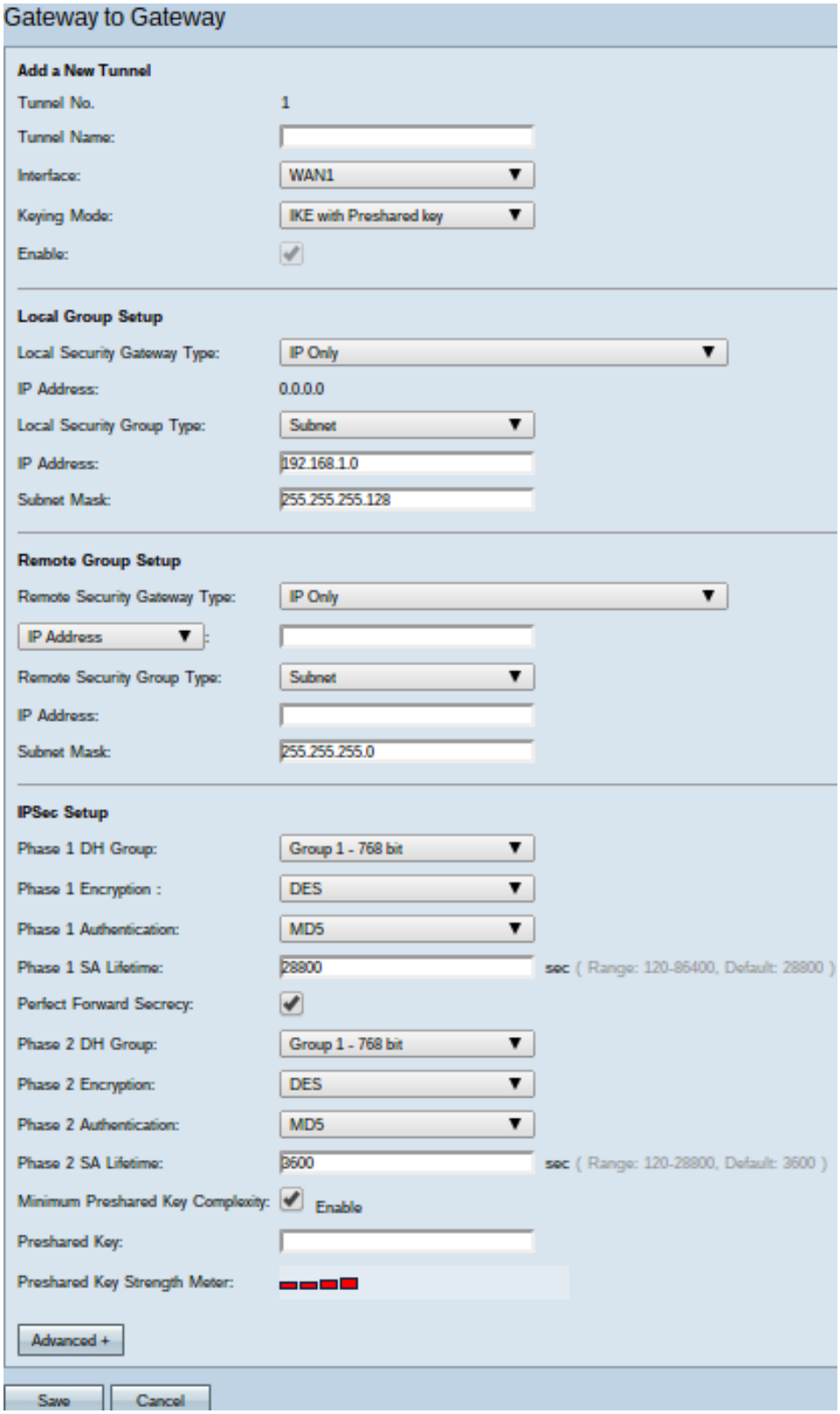
·RV320 Dual-WAN VPN-Router
· RV325 Gigabit Dual-WAN VPN-Router

Softwareversion

·v1.1.0.09

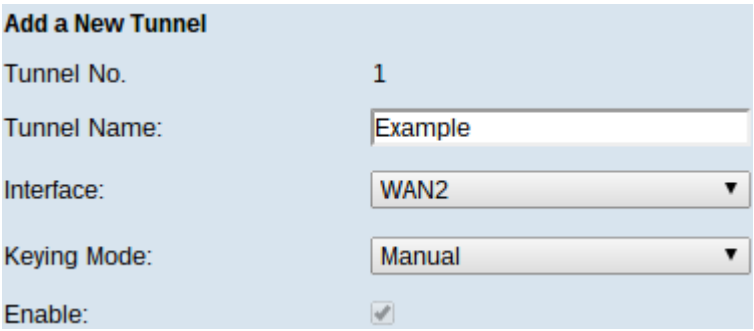
Gateway zu Gateway

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



Damit die VPN-Verbindung ordnungsgemäß funktioniert, müssen die IPSec-Werte (Internet Protocol Security) auf beiden Seiten der Verbindung identisch sein. Beide Seiten der Verbindung müssen zu unterschiedlichen LANs (Local Area Networks) gehören. Mindestens einer der Router muss durch eine statische IP-Adresse oder einen dynamischen DNS-Hostnamen identifiziert werden können.

Neuen Tunnel hinzufügen



·Tunnel No. — Zeigt den aktuellen Tunnel an, der erstellt werden soll. Der Router unterstützt 100 Tunnel.

Schritt 1: Geben Sie im Feld "Tunnel Name" einen Namen für den VPN-Tunnel ein. Sie 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 (Wide Area Network) aus, der für den Tunnel verwendet werden soll.

·WAN1 - Der dedizierte WAN-Port des Routers.

·WAN2 - Der WAN2/DMZ-Port des Routers. Wird nur im Dropdown-Menü angezeigt, wenn es als WAN und nicht als DMZ-Port (Demilitarize Zone) konfiguriert wurde.

·USB1 - Der USB1-Port des Routers. Funktioniert nur, wenn ein 3G/4G/LTE-USB-Dongle an den Port angeschlossen ist.

·USB2 - Der USB2-Port des Routers. Funktioniert nur, wenn ein 3G/4G/LTE-USB-Dongle an den Port angeschlossen ist.

Schritt 3: Wählen Sie aus der Dropdown-Liste Keying Mode (Keying Mode) die zu verwendende Tunnelsicherheit aus.

·Manual (Manuell): Mit dieser Option können Sie den Schlüssel manuell konfigurieren, anstatt den Schlüssel mit der anderen Seite der VPN-Verbindung zu verhandeln.

·IKE mit vorinstalliertem Schlüssel - Wählen Sie diese Option aus, um das Internet Key Exchange Protocol (IKE) zu aktivieren, das eine Sicherheitszuordnung im VPN-Tunnel einrichtet. IKE verwendet einen vorinstallierten Schlüssel zur Authentifizierung eines Remote-Peers.

·IKE mit Zertifikat - Wählen Sie diese Option aus, um das IKE-Protokoll (Internet Key Exchange) mit Zertifikat zu aktivieren, das eine sicherere Möglichkeit bietet, vorinstallierte Schlüssel automatisch zu generieren und auszutauschen, um eine authentifiziertere und sicherere Kommunikation für den Tunnel zu ermöglichen.

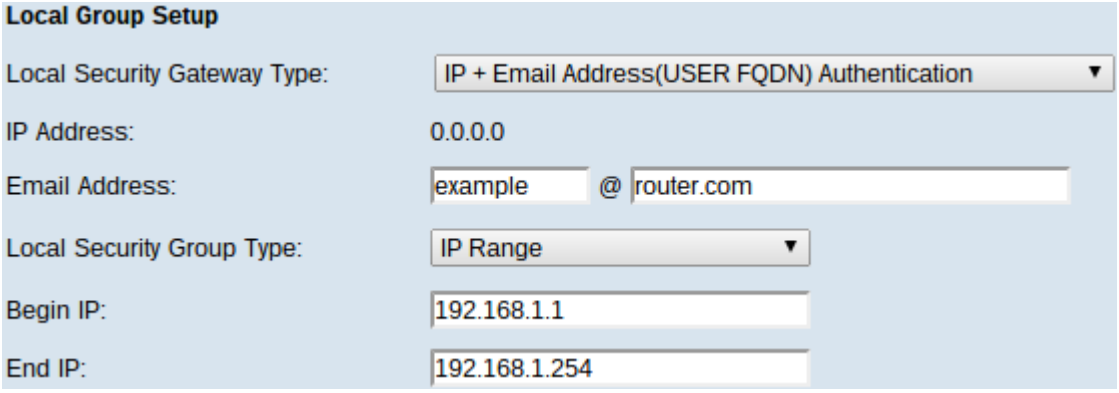
Schritt 4: Aktivieren Sie das Kontrollkästchen Enable (Aktivieren), um den VPN-Tunnel zu aktivieren. Standardmäßig ist sie aktiviert.

Lokale Gruppeneinrichtung

Diese Einstellungen sollten den Einstellungen für die "Remote Group Setup" (Remote-Gruppeneinrichtung) für den Router am anderen Ende des VPN-Tunnels entsprechen.

Hinweis: Wenn Manual (Manuell) oder IKE mit dem vorinstallierten Schlüssel aus der

Dropdown-Liste Keying Mode (Keying Mode) aus Schritt 3 von Add a New Tunnel (Neuen Tunnel hinzufügen) ausgewählt wurde, beginnen Sie von Schritt 1 aus und überspringen Sie die Schritte 2 bis 4. Wenn IKE mit Zertifikat ausgewählt wurde, überspringen Sie Schritt 1.



Schritt 1: Wählen Sie in der Dropdown-Liste Local Security Gateway Type (Typ des lokalen Sicherheitsgateways) die Methode aus, um den Router zum Herstellen des VPN-Tunnels zu identifizieren.

·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 ist ein automatisch generiertes Feld.

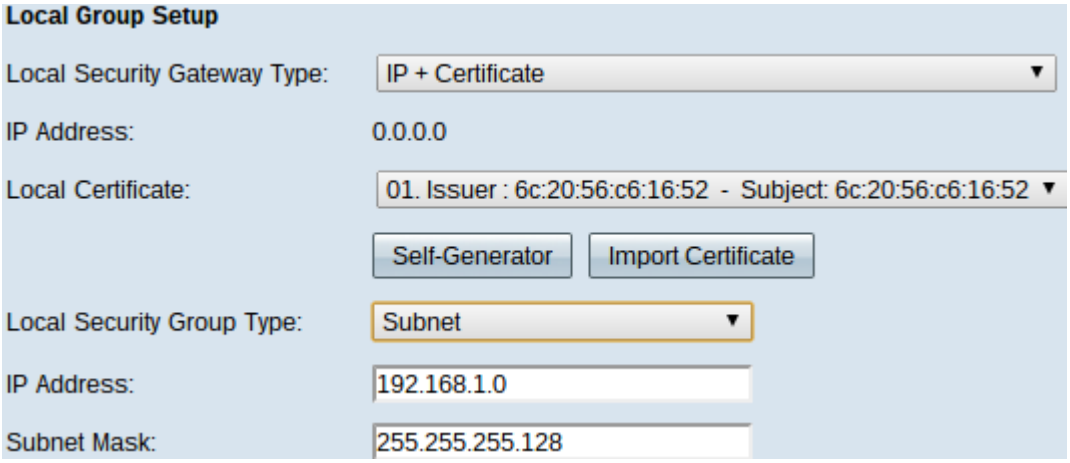
·IP + Domain Name (FQDN)-Authentifizierung - Der Zugriff auf den Tunnel ist über eine statische IP-Adresse und eine registrierte Domäne möglich. Wenn Sie diese Option wählen, geben Sie den Namen der registrierten Domäne im Feld Domain Name (Domänenname) ein. Die statische WAN-IP-Adresse ist ein automatisch generiertes Feld.

·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 ist ein automatisch generiertes Feld.

·Dynamische IP + Domänenname (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 im 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.

Hinweis: Die folgenden Änderungen im Bereich "Local Group Setup" (Lokale Gruppe einrichten) werden bei der Arbeit mit IKE mit Zertifikat geändert.



Die Dropdown-Liste Local Security Gateway Type (Typ des lokalen Sicherheitsgateways) kann nicht bearbeitet werden, und es wird IP + Certificate angezeigt. Dies ist die LAN-Ressource, die den Tunnel verwenden kann.
Im Feld "IP Address" (IP-Adresse) wird die WAN-IP-Adresse des Geräts angezeigt. Es kann nicht vom Benutzer bearbeitet werden.

Schritt 2: Wählen Sie in der Dropdown-Liste "Lokales Zertifikat" ein Zertifikat aus. Zertifikate bieten eine höhere Authentifizierungssicherheit für die VPN-Verbindungen.

Schritt 3: (Optional) Klicken Sie auf die Schaltfläche **Self-Generator**, um das Fenster *Certificate Generator* zum Konfigurieren und Generieren von Zertifikaten anzuzeigen.

Schritt 4: (Optional) Klicken Sie auf die Schaltfläche **Zertifikat importieren**, um das Fenster *Mein Zertifikat* zum Anzeigen und Konfigurieren von Zertifikaten anzuzeigen.

Schritt 5: Wählen Sie in der Dropdown-Liste Local Security Group Type (Typ der lokalen Sicherheitsgruppe) eine der folgenden Optionen aus:

·IP Address (IP-Adresse): Mit dieser Option können Sie ein Gerät angeben, das diesen VPN-Tunnel verwenden kann. Sie müssen nur die IP-Adresse des Geräts in das IP-Adressfeld eingeben.

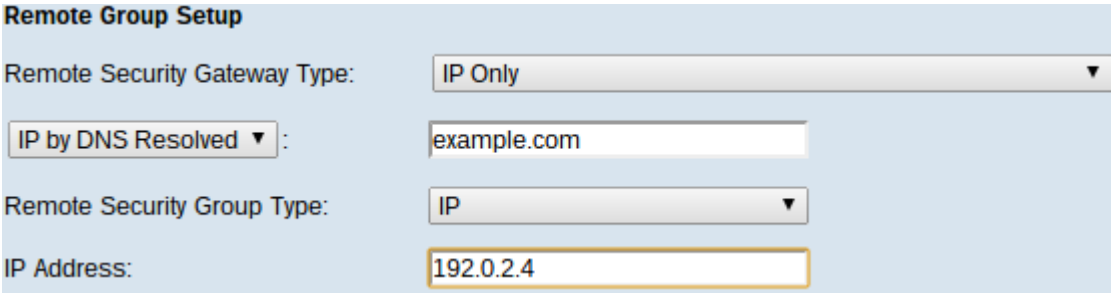
·Subnetz - Wählen Sie diese Option, damit alle Geräte, die demselben Subnetz angehören, den VPN-Tunnel verwenden können. Sie müssen die Netzwerk-IP-Adresse im Feld IP Address (IP-Adresse) und die entsprechende Subnetzmaske im Feld Subnet Mask (Subnetzmaske) eingeben.

·IP Range (IP-Bereich): Wählen Sie diese Option, um eine Reihe von Geräten anzugeben, die den VPN-Tunnel verwenden können. Sie müssen die erste IP-Adresse und die letzte IP-Adresse des Gerätespektrums in das Feld "Start IP" und das Feld "End IP" eingeben.

Remote-Gruppeneinrichtung

Diese Einstellungen sollten den Einstellungen für die "Local Group Setup" (Einrichtung der lokalen Gruppe) für den Router am anderen Ende des VPN-Tunnels entsprechen.

Hinweis: Wenn Manual (Manuell) oder IKE mit dem vorinstallierten Schlüssel aus der Dropdown-Liste Keying Mode (Keying Mode) aus Schritt 3 von Add a New Tunnel (Neuen Tunnel hinzufügen) ausgewählt wurde, beginnen Sie von Schritt 1 aus und überspringen Sie die Schritte 2 bis 5. Wenn IKE mit Zertifikat ausgewählt wurde, überspringen Sie Schritt 1.



Schritt 1: Wählen Sie in der Dropdown-Liste "Remote Security Gateway Type" (Typ des Remote-Sicherheitsgateways) die Methode aus, um den anderen Router zu identifizieren, der den VPN-Tunnel einrichten soll.

·Nur IP - Der Zugriff auf den Tunnel ist nur über eine statische WAN-IP 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-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 Domänennamen kennen, und geben Sie den Domänennamen des Routers in das Feld IP by DNS Resolved (IP durch DNS aufgelöst) ein.

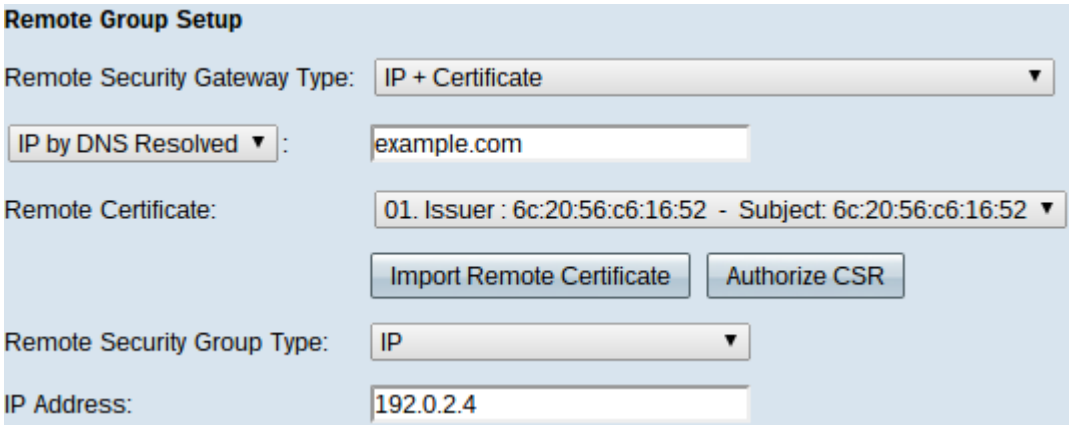
·IP + Domain Name (FQDN)-Authentifizierung - Der Zugriff auf den Tunnel ist über eine statische IP-Adresse und eine registrierte Domäne des Routers möglich. Wenn Sie die IP-Adresse des Remote-Routers kennen, wählen Sie die IP-Adresse in der Dropdown-Liste direkt unterhalb des Felds Remote Security Gateway Type (Remote-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 Domänennamen kennen, und geben Sie den Domänennamen des Routers in das Feld IP by DNS Resolved (IP durch DNS aufgelöst) ein. Wenn Sie diese Option wählen, geben Sie den Namen der registrierten Domäne im Feld Domain Name (Domänenname) ein.

·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 die IP-Adresse des Remote-Routers kennen, wählen Sie die IP-Adresse in der Dropdown-Liste direkt unter "Remote Security Gateway Type" (Remote-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 Domänennamen kennen, und geben Sie den Domänennamen 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.

·Dynamische IP + Domänenname (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 im 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.
Hinweis: Wenn beide Router dynamische IP-Adressen haben, wählen Sie NICHT Dynamic IP + Email Address für beide Gateways aus.

Hinweis: Die folgenden Änderungen im Bereich "Remote Group Setup" (Remote-Gruppeneinrichtung) ändern sich, wenn Sie mit IKE mit Zertifikat arbeiten.



Die Dropdown-Liste "Remote Security Gateway Type" (Typ des Remote-Sicherheitsgateways) kann nicht mehr bearbeitet werden, und es wird IP + Zertifikat angezeigt. Dies ist die LAN-Ressource, die den Tunnel verwenden kann.

Schritt 2: 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-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 Domänennamen kennen, und geben Sie den Domänennamen des Remote-Routers in die IP by DNS Resolved (IP durch DNS aufgelöst)-Feld ein.

Schritt 3: Wählen Sie ein Zertifikat aus der Dropdown-Liste Remote Certificate aus. Zertifikate bieten eine höhere Authentifizierungssicherheit für die VPN-Verbindungen.

Schritt 4: (Optional) Klicken Sie auf die Schaltfläche **Remote Certificate importieren**, um ein neues Zertifikat zu importieren.

Schritt 5: (Optional) Klicken Sie auf die Schaltfläche **CSR autorisieren**, um das Zertifikat mit einer digitalen Signierungsanfrage zu identifizieren.

Schritt 6: Wählen Sie in der Dropdown-Liste Local Security Group Type (Typ der lokalen Sicherheitsgruppe) eine der folgenden Optionen aus:

·IP Address (IP-Adresse): Mit dieser Option können Sie ein Gerät angeben, das diesen VPN-Tunnel verwenden kann. Sie müssen nur die IP-Adresse des Geräts in das IP-Adressfeld eingeben.

·Subnetz - Wählen Sie diese Option, damit alle Geräte, die demselben Subnetz angehören, den VPN-Tunnel verwenden können. Sie müssen die Netzwerk-IP-Adresse im Feld IP Address (IP-Adresse) und die entsprechende Subnetzmaske im Feld Subnet Mask (Subnetzmaske) eingeben.

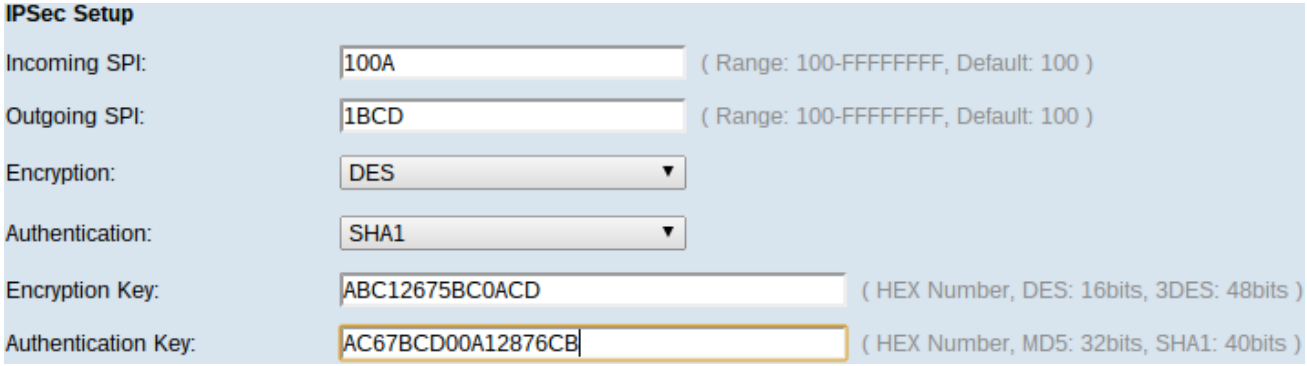
·IP Range (IP-Bereich): Wählen Sie diese Option, um eine Reihe von Geräten anzugeben, die den VPN-Tunnel verwenden können. Sie müssen die erste IP-Adresse und die letzte IP-Adresse des Gerätespektrums eingeben. Im Feld "Start IP" und "End IP".

IPSec-Einrichtung

Damit die Verschlüsselung zwischen den beiden Enden des VPN-Tunnels richtig eingerichtet werden kann, müssen beide die exakten gleichen Einstellungen haben. IPSec erstellt in diesem Fall eine sichere Authentifizierung zwischen den beiden Geräten. Dies geschieht in zwei Phasen.

IPSec-Einrichtung für den manuellen Keying-Modus

Nur verfügbar, wenn Manual (Manuell) aus der Dropdown-Liste Keying Mode (Keying Mode) aus Schritt 3 von Add a New Tunnel (Neuen Tunnel hinzufügen) ausgewählt wurde. Dies ist ein benutzerdefinierter Sicherheitsmodus, mit dem Sie einen neuen Sicherheitsschlüssel selbst generieren und nicht mit dem Schlüssel verhandeln können. Sie eignet sich am besten zur Fehlerbehebung und für kleine statische Umgebungen.



Schritt 1: Geben Sie im Feld Eingehender SPI den eindeutigen Hexadezimalwert für eingehenden Security Parameter Index (SPI) ein. SPI wird in einem ESP-Header (Encapsulating Security Payload) übertragen, der zusammen den Schutz für das eingehende Paket bestimmt. Sie können zwischen 100 und FFFFFF eingeben.

Schritt 2: Geben Sie den eindeutigen Hexadezimalwert für SPI in das Feld Ausgehender SPI ein. SPI wird im ESP-Header übertragen, der zusammen den Schutz für das ausgehende Paket bestimmt. Sie können zwischen 100 und FFFFFF eingeben.

Hinweis: Der eingehende und der ausgehende SPI müssen an beiden Enden übereinstimmen, um einen Tunnel einzurichten.

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

·DES - DES (Data Encryption Standard) ist eine 56-Bit-Verschlüsselungsmethode, die abwärtskompatibel ist und nicht so sicher ist, wie sie leicht zu durchbrechen ist.

·3DES - 3DES (Triple Data Encryption Standard) ist eine einfache 168-Bit-Verschlüsselungsmethode zur dreifachen Erhöhung der Schlüssellänge durch Verschlüsselung der Daten, die mehr Sicherheit bietet als DES.

Schritt 4: Wählen Sie in der Dropdown-Liste Authentifizierung die entsprechende Authentifizierungsmethode aus. Die empfohlene Authentifizierung ist SHA1. Der VPN-Tunnel muss für beide Enden dieselbe Authentifizierungsmethode verwenden.

·MD5 - MD5 (Message Digest Algorithm-5) stellt eine 32-stellige hexadezimale Hashfunktion dar, die die Daten durch die Prüfsummenberechnung vor böswilligen Angriffen schützt.

·SHA1 — SHA1 (Secure Hash Algorithm Version 1) ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5.

Schritt 5: Geben Sie im Feld Verschlüsselungsschlüssel den Schlüssel zum Verschlüsseln und Entschlüsseln von Daten ein. Wenn Sie DES in Schritt 3 als Verschlüsselungsmethode

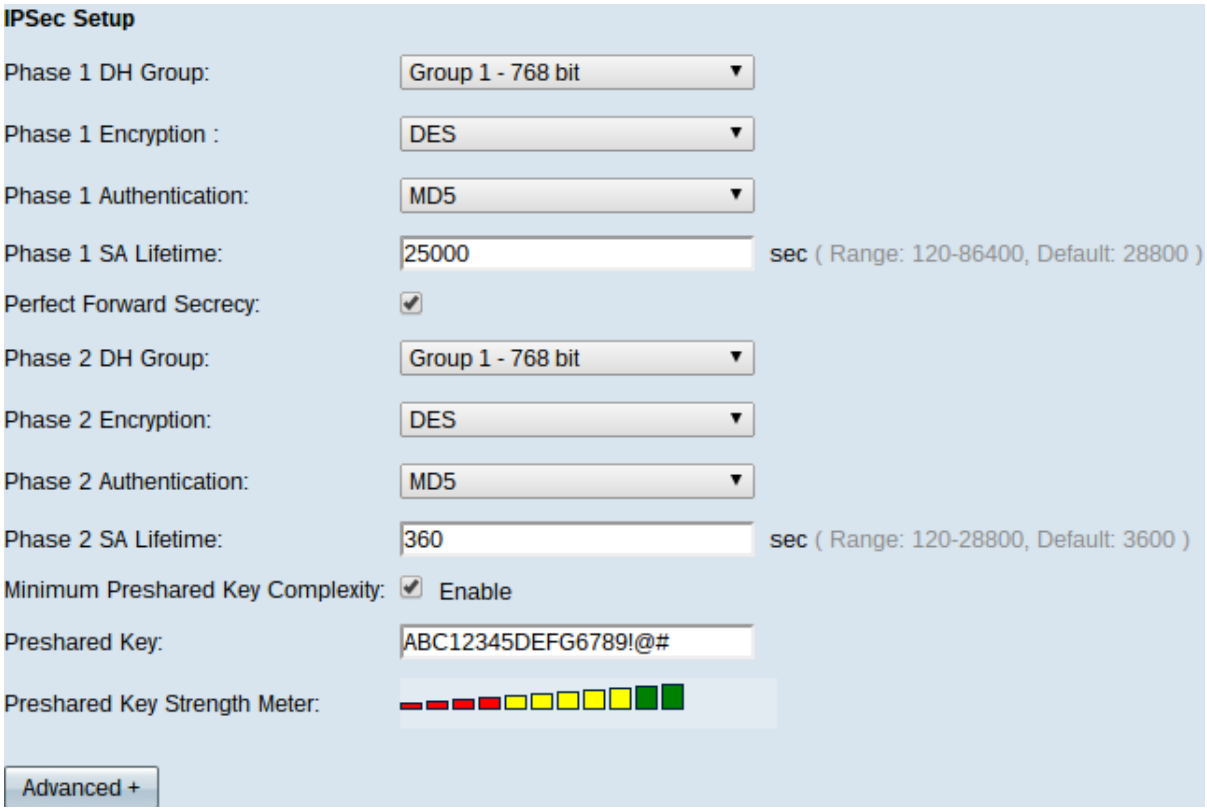
auswählen, geben Sie einen 16-stelligen Hexadezimalwert ein. Wenn Sie in Schritt 3 3DES als Verschlüsselungsmethode auswählen, geben Sie einen 40-stelligen Hexadezimalwert ein.

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

IPSec-Einrichtung für IKE mit vorinstalliertem Schlüssel

Nur verfügbar, wenn IKE mit vorinstalliertem Schlüssel aus der Dropdown-Liste Keying Mode (Keying Mode) aus Schritt 3 von Add a New Tunnel (Neuen Tunnel hinzufügen) ausgewählt wurde.



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

·Gruppe 1 - 768 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.

·Gruppe 2 - 1024 Bit - Stellt einen leistungsfähigeren Schlüssel und eine sicherere Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert etwas Zeit.

·Gruppe 5 - 1536 Bit - Stellt den niedrigsten Stärke-Schlüssel und die unsicherste Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert weniger Zeit. Es wird empfohlen, wenn die Netzwerkgeschwindigkeit niedrig ist.

Schritt 2: Wählen Sie aus der Dropdown-Liste Verschlüsselung für Phase 1 die entsprechende Verschlüsselung für Phase 1 aus. AES-128, AES-192 oder AES-256 werden empfohlen. Der VPN-Tunnel muss für beide Enden dieselbe Verschlüsselungsmethode verwenden.

·DES - Der Data Encryption Standard (DES) ist eine 56-Bit-Verschlüsselungsmethode, die in der heutigen Welt keine besonders sichere Verschlüsselungsmethode 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 - Eine 192-Bit-Verschlüsselungsmethode, die den Klartext durch 12 Wiederholungen in einen verschlüsselten Text umwandelt.

·AES-256 — ist eine 256-Bit-Verschlüsselungsmethode, die den Klartext durch 14 Zykluswiederholungen in einen verschlüsselten Text umwandelt.

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

·MD5 - Message Digest Algorithm-5 (MD5) stellt eine 32-stellige Hexadezimalfunktion dar, die die Daten durch die Prüfsummenberechnung vor böswilligen Angriffen schützt.

·SHA1 - Eine 160-Bit-Hash-Funktion, die sicherer als MD5 ist.

Schritt 4: Geben Sie die Zeitdauer (in Sekunden) ein, die der VPN-Tunnel im Feld "Phase 1 SA Life Time" (SA-Lebensdauer) aktiv bleibt.

Schritt 5: Aktivieren Sie das Kontrollkästchen Perfect Forward Secrecy (Perfekte Weiterleitungsgeheimnis), um den 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.

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

·Gruppe 1 - 768 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.

·Gruppe 2 - 1024 Bit - Stellt einen leistungsfähigeren Schlüssel und eine sicherere Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert etwas Zeit.

·Gruppe 5 - 1536 Bit - Stellt den niedrigsten Stärke-Schlüssel und die unsicherste Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert weniger Zeit. Es wird empfohlen, wenn die Netzwerkgeschwindigkeit niedrig ist.

Hinweis: Da kein neuer Schlüssel generiert wird, müssen Sie die DH-Gruppe für Phase 2 nicht konfigurieren, wenn Sie in Schritt 5 die Option Perfect Forward Secrecy (Vorwärtsgeheimnis perfekt) deaktivieren.

Schritt 7: Wählen Sie aus der Dropdown-Liste "Verschlüsselung für Phase 2" die entsprechende Verschlüsselung für Phase 2 aus. AES-128, AES-192 oder AES-256 werden empfohlen. Der VPN-Tunnel muss für beide Enden dieselbe Verschlüsselungsmethode verwenden.

·DES - DES ist eine 56-Bit-Verschlüsselungsmethode, die in der heutigen Welt nicht sehr sicher ist.

·3DES - 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 - AES ist eine 128-Bit-Verschlüsselungsmethode, die den Klartext durch 10-fache Wiederholungen in einen verschlüsselten Text umwandelt.

·AES-192 - Eine 192-Bit-Verschlüsselungsmethode, die den Klartext durch 12 Wiederholungen in einen verschlüsselten Text umwandelt.

·AES-256 — ist eine 256-Bit-Verschlüsselungsmethode, die den Klartext durch 14 Zykluswiederholungen in einen verschlüsselten Text umwandelt.

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

·MD5 - MD5 steht für eine hexadezimale Hashfunktion mit 32 Stellen, 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.

·Null - Es wird keine Authentifizierungsmethode verwendet.

Schritt 9: Geben Sie die Zeitdauer (in Sekunden) ein, die der VPN-Tunnel im Feld "Phase 2 SA Life Time" (SA-Lebensdauer in Phase 2) aktiv bleibt.

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. Als vorinstallierter Schlüssel können bis zu 30 Hexadezimalzeichen und Zeichen verwendet werden. Der VPN-Tunnel muss für beide Enden denselben vorinstallierten Schlüssel verwenden.

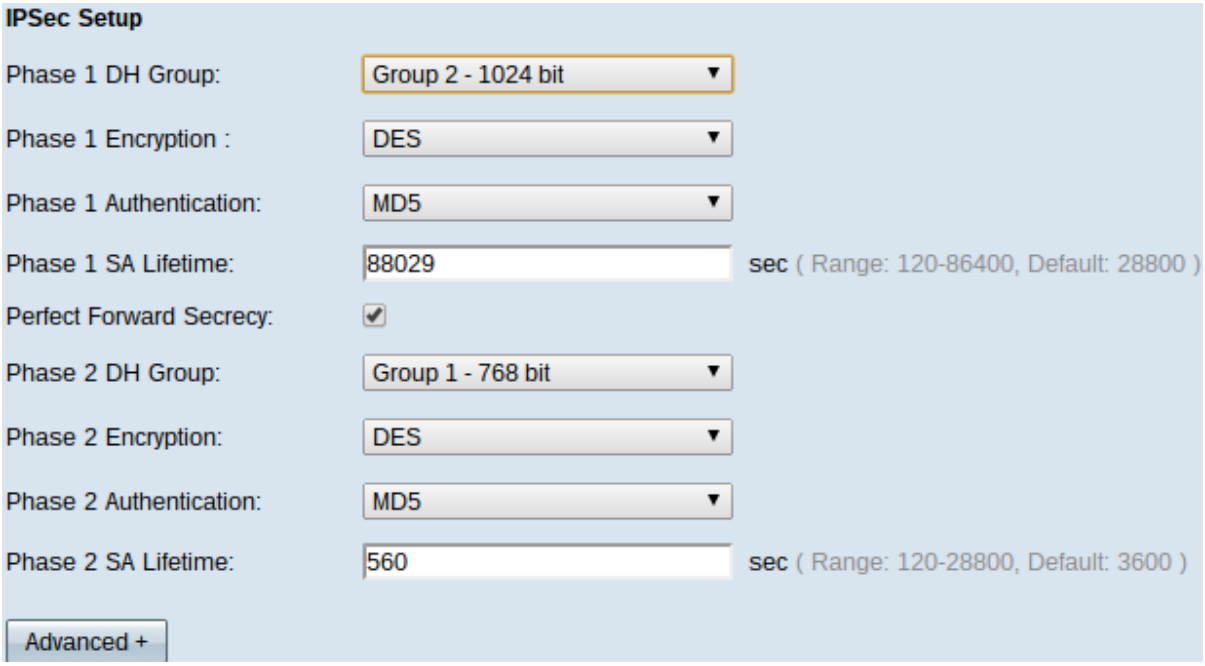
Hinweis: Es wird dringend empfohlen, den vorinstallierten Schlüssel zwischen den IKE-Peers häufig zu ändern, um die Sicherheit des VPN zu gewährleisten.

Das Preshared Key Strength Meter zeigt die Stärke des vorinstallierten Schlüssels durch Farbbalken an. Rot bedeutet schwache Stärke, Gelb bedeutet akzeptable Stärke und Grün bedeutet starke Stärke.

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

IPSec-Einrichtung für IKE mit Zertifikat

Nur verfügbar, wenn IKE mit Zertifikat aus der Dropdown-Liste Keying Mode (Keying Mode) aus Schritt 3 von Add a New Tunnel (Neuen Tunnel hinzufügen) ausgewählt wurde.



Schritt 1: Wählen Sie aus der Dropdown-Liste Phase 1 DH Group (DH-Gruppe Phase 1) die passende DH-Gruppe aus. Phase 1 dient zur Einrichtung der Simplex, logischen SA (Security Association) zwischen den beiden Enden des Tunnels, um eine sichere authentifizierte Kommunikation zu unterstützen. DH ist ein kryptografisches Schlüsselaustauschprotokoll, das während der Phase-1-Verbindung verwendet wird, um geheime Schlüssel für die Authentifizierung der Kommunikation freizugeben.

·Gruppe 1 - 768 Bit - Stellt den höchsten Stärke-Schlüssel und die sicherste Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert jedoch mehr Zeit. Es wird empfohlen, wenn die Netzwerkgeschwindigkeit hoch 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 niedrigsten Stärke-Schlüssel und die unsicherste Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert weniger Zeit. Es wird empfohlen, wenn die Netzwerkgeschwindigkeit niedrig ist.

Schritt 2: Wählen Sie aus der Dropdown-Liste Verschlüsselung für Phase 1 die entsprechende Verschlüsselung für Phase 1 aus. AES-128, AES-192 oder AES-256 werden empfohlen. Der VPN-Tunnel muss für beide Enden dieselbe Verschlüsselungsmethode

verwenden.

·DES - DES ist eine 56-Bit-Verschlüsselungsmethode, die in der heutigen Welt nicht sehr sicher ist.

·3DES - 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 - AES ist eine 128-Bit-Verschlüsselungsmethode, die den Klartext durch 10-fache Wiederholungen in einen verschlüsselten Text umwandelt.

·AES-192 - Eine 192-Bit-Verschlüsselungsmethode, die den Klartext durch 12 Wiederholungen in einen verschlüsselten Text umwandelt.

·AES-256 — ist eine 256-Bit-Verschlüsselungsmethode, die den Klartext durch 14 Zykluswiederholungen in einen verschlüsselten Text umwandelt.

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

·MD5 - MD5 steht für eine hexadezimale Hashfunktion mit 32 Stellen, die die Daten durch die Prüfsummenberechnung vor böswilligen Angriffen schützt.

·SHA1 - Eine 160-Bit-Hash-Funktion, die sicherer als MD5 ist.

Schritt 4: Geben Sie die Zeitdauer (in Sekunden) ein, die der VPN-Tunnel im Feld "Phase 1 SA Life Time" (SA-Lebensdauer) aktiv bleibt.

Schritt 5: Aktivieren Sie das Kontrollkästchen Perfect Forward Secrecy (Perfekte Weiterleitungsgeheimnis), um den 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 anderer Schlüssel beschädigt wird. Dies ist eine empfohlene Maßnahme, da sie mehr Sicherheit bietet.

Schritt 6: Wählen Sie in der Dropdown-Liste "Phase 2 DH Group" (Phase 2-DH-Gruppe) die passende Phase 2-DH-Gruppe aus. Phase 1 dient zur Einrichtung der Simplex-logischen SA zwischen den beiden Enden des Tunnels, um eine sichere authentifizierte Kommunikation zu unterstützen. DH ist ein kryptografisches Schlüsselaustauschprotokoll, das während der Phase-1-Verbindung verwendet wird, um geheime Schlüssel für die Authentifizierung der Kommunikation freizugeben.

·Gruppe 1 - 768 Bit - Stellt den höchsten Stärke-Schlüssel und die sicherste Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert jedoch mehr Zeit. Es wird empfohlen, wenn die Netzwerkgeschwindigkeit hoch 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 niedrigsten Stärke-Schlüssel und die unsicherste Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert weniger Zeit. Es

wird empfohlen, wenn die Netzwerkgeschwindigkeit niedrig ist.

Hinweis: Da kein neuer Schlüssel generiert wird, müssen Sie die DH-Gruppe für Phase 2 nicht konfigurieren, wenn Sie in Schritt 5 die Option Perfect Forward Secrecy (Vorwärtsgeheimnis perfekt) deaktiviert haben.

Schritt 7: Wählen Sie aus der Dropdown-Liste "Verschlüsselung für Phase 2" die entsprechende Verschlüsselung für Phase 2 aus. AES-128, AES-192 oder AES-256 werden empfohlen. Der VPN-Tunnel muss für beide Enden dieselbe Verschlüsselungsmethode verwenden.

·DES - DES ist eine 56-Bit-Verschlüsselungsmethode, die in der heutigen Welt nicht sehr sicher ist.

·3DES - 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 - AES ist eine 128-Bit-Verschlüsselungsmethode, die den Klartext durch 10-fache Wiederholungen in einen verschlüsselten Text umwandelt.

·AES-192 - Eine 192-Bit-Verschlüsselungsmethode, die den Klartext durch 12 Wiederholungen in einen verschlüsselten Text umwandelt.

·AES-256 — ist eine 256-Bit-Verschlüsselungsmethode, die den Klartext durch 14 Zykluswiederholungen in einen verschlüsselten Text umwandelt.

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

·MD5 - MD5 steht für eine hexadezimale Hashfunktion mit 32 Stellen, die die Daten durch die Prüfsummenberechnung vor böswilligen Angriffen schützt.

·SHA1 — SHA1 ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5.

·Null - Es wird keine Authentifizierungsmethode verwendet.

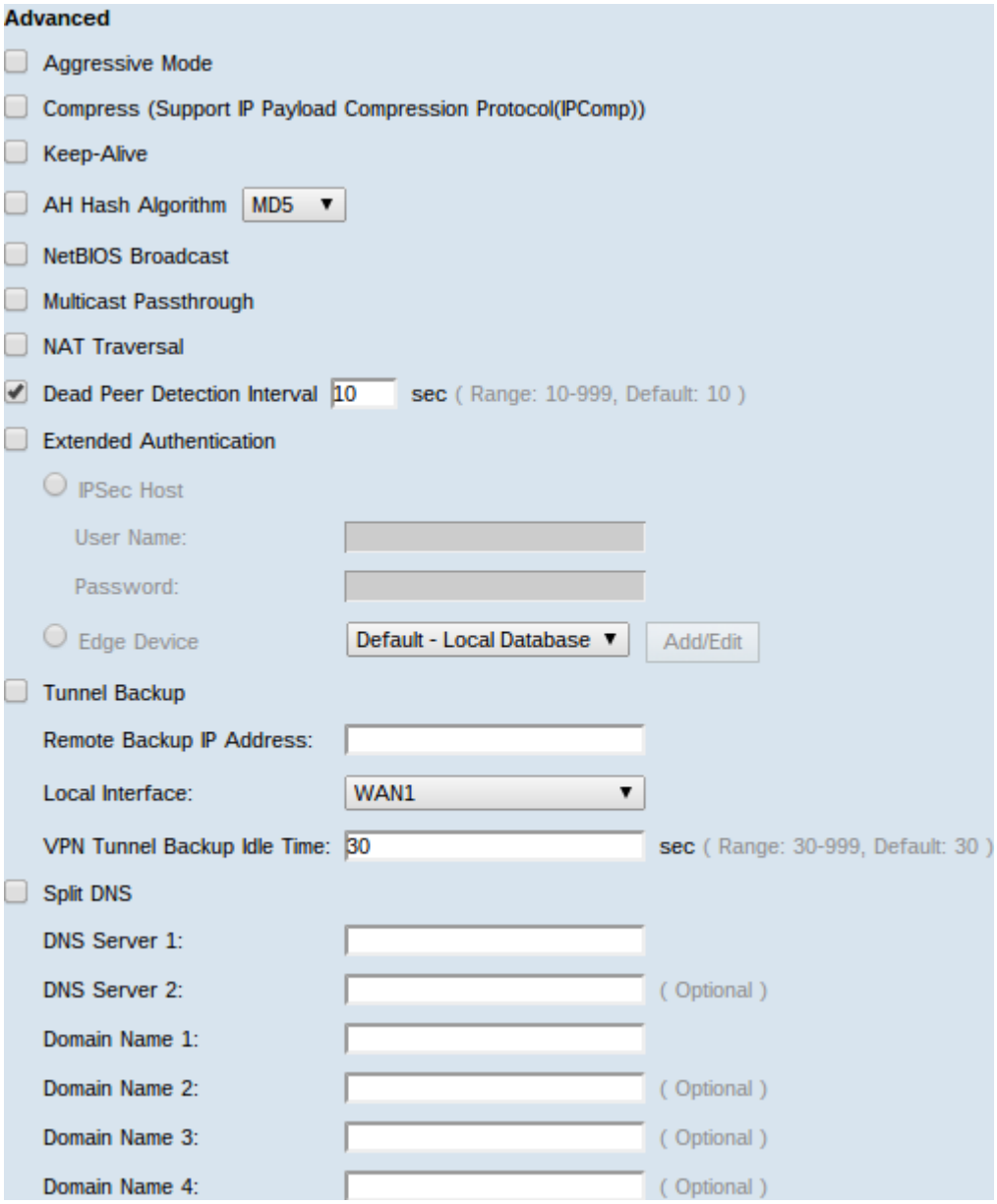
Schritt 9: Geben Sie die Zeitdauer (in Sekunden) ein, die der VPN-Tunnel im Feld "Phase 2 SA Life Time" (SA-Lebensdauer in Phase 2) aktiv bleibt.

Schritt 10: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

(Optional) IPSec Advance Setup für IKE mit Zertifikat und IKE mit vorinstalliertem Schlüssel

Die erweiterten Optionen sind verfügbar, wenn IKE mit Zertifikat oder IKE mit Drucktaste aus der Dropdown-Liste Keying Mode (Keying Mode) aus Schritt 3 von Add a New Tunnel (Neuen Tunnel hinzufügen) ausgewählt wurde. Die gleichen Einstellungen sind für beide Arten von Keying-Modi verfügbar.

Schritt 1: Klicken Sie auf die **Schaltfläche Erweitert+**, um die erweiterten IPSec-Optionen anzuzeigen.



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 Verbindung aufrecht halten, 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 - MD5 steht für eine hexadezimale Hashfunktion mit 128 Stellen, die die Daten durch die Prüfsummenberechnung vor böswilligen Angriffen schützt.

·SHA1 — 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: Wenn sich Ihr VPN-Router hinter einem NAT-Gateway befindet, aktivieren Sie das Kontrollkästchen, um NAT-Traversal zu aktivieren. Network Address Translation (NAT) ermöglicht Benutzern mit privaten LAN-Adressen den Zugriff auf Internetressourcen, indem eine öffentlich routbare IP-Adresse als Quelladresse verwendet wird. Beim eingehenden Datenverkehr kann das NAT-Gateway jedoch nicht automatisch die öffentliche IP-Adresse in ein bestimmtes Ziel im privaten LAN übersetzen. Dieses Problem verhindert erfolgreiche IPSec-Austauschvorgänge. NAT Traversal richtet diese eingehende Übersetzung ein. Die gleiche Einstellung muss an beiden Enden des Tunnels verwendet werden.

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

Schritt 9: Aktivieren Sie die Option Extended Authentication (Erweiterte Authentifizierung), um einen IPSec-Hostbenutzernamen und ein Kennwort für die Authentifizierung von VPN-Clients zu verwenden oder die in User Management (Benutzerverwaltung) gefundene Datenbank zu verwenden. Diese Funktion muss auf beiden Geräten aktiviert sein, damit sie funktioniert. Klicken Sie auf das Optionsfeld **IPSec Host**, um den IPSec-Host und den Benutzernamen zu verwenden, und geben Sie den Benutzernamen und das Kennwort in das Feld Benutzername und das Feld Kennwort ein. Oder klicken Sie auf das Optionsfeld **Edge Device** (**Edge-Gerät**), um eine Datenbank zu verwenden. Wählen Sie die gewünschte Datenbank aus der Dropdown-Liste Edge Device (Edge-Gerät) aus.

Schritt 10: Aktivieren Sie das Kontrollkästchen Tunnel Backup (Tunnel-Sicherung), um Tunnel-Backup zu aktivieren. Diese Funktion ist verfügbar, wenn das Intervall zur Erkennung von Dead-Peers überprüft wurde. Diese Funktion ermöglicht dem Gerät die Wiederherstellung des VPN-Tunnels über eine alternative WAN-Schnittstelle oder IP-Adresse.

·Remote-Backup-IP-Adresse - Eine alternative IP-Adresse für den Remote-Peer. Geben Sie ihn oder die WAN-IP ein, die in diesem Feld bereits für das Remote-Gateway festgelegt wurde.

·Local Interface (Lokale Schnittstelle) - Die WAN-Schnittstelle, die zum Wiederherstellen der Verbindung verwendet wird. Wählen Sie die gewünschte Schnittstelle aus der Dropdown-Liste aus.

·Backup-Leerlaufzeit für VPN-Tunnel — Die Zeit, die gewählt wurde, um den Backup-Tunnel zu verwenden, wenn der primäre Tunnel nicht verbunden ist. Geben Sie es in Sekunden ein.

Schritt 11: Aktivieren Sie das Kontrollkästchen Split DNS (DNS aufteilen), um Split DNS zu aktivieren. Diese Funktion ermöglicht das Senden von DNS-Anfragen an einen definierten

DNS-Server, der auf angegebenen Domänennamen basiert. Geben Sie die DNS-Servernamen in die Felder DNS Server 1 und DNS Server 2 ein, und geben Sie die Domänennamen in die Felder Domain Name # (Domänenname #) ein.

Schritt 12: Klicken Sie auf **Speichern**, um die Konfiguration des Geräts abzuschließen.