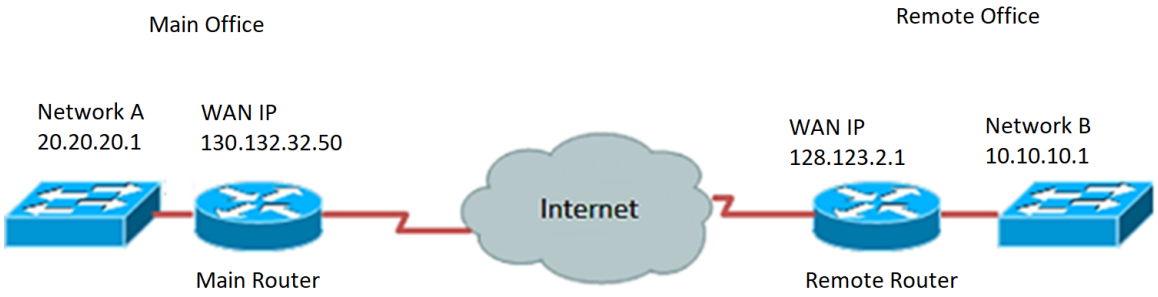
Konfigurieren der VPN-Verbindung (Virtual Private Network) mithilfe des Setup-Assistenten auf dem Router der Serie RV34x

Ziel

Über eine VPN-Verbindung (Virtual Private Network) können Benutzer auf ein privates Netzwerk (z. B. das Internet) zugreifen, Daten an ein privates Netzwerk senden und von diesem empfangen. Dabei werden jedoch sichere Verbindungen zu einer zugrunde liegenden Netzwerkinfrastruktur zum Schutz des privaten Netzwerks und seiner Ressourcen sichergestellt.

Ein VPN-Tunnel richtet ein privates Netzwerk ein, das Daten sicher mit Verschlüsselung und Authentifizierung senden kann. Die meisten Firmenbüros verwenden eine VPN-Verbindung, da es sowohl nützlich als auch notwendig ist, den Mitarbeitern den Zugriff auf ihr privates Netzwerk zu ermöglichen, selbst wenn sie sich außerhalb des Büros befinden.

Mit dem VPN kann ein Remote-Host so agieren, als ob er sich im selben lokalen Netzwerk befinde. Der Router unterstützt 50 Tunnel. Der VPN-Setup-Assistent ermöglicht die Konfiguration einer sicheren Verbindung für den standortübergreifenden IPSec-Tunnel. Diese Funktion vereinfacht die Konfiguration und verhindert komplexe Einstellungen und optionale Parameter. So kann jeder den IPSec-Tunnel schnell und effizient einrichten.



Vorteile einer VPN-Verbindung:

1. Die Verwendung einer VPN-Verbindung trägt zum Schutz vertraulicher Netzwerkdaten und -ressourcen bei.
2. Ermöglicht Remote-Mitarbeitern oder Mitarbeitern im Unternehmen einen einfachen Zugriff auf die Hauptniederlassung, ohne dass sie physisch anwesend sein müssen. Gleichzeitig wird die Sicherheit des privaten Netzwerks und seiner Ressourcen gewahrt.
3. Die Kommunikation über eine VPN-Verbindung bietet ein höheres Maß an Sicherheit als andere Remote-Kommunikationsmethoden. Modernste Technologie macht dies heute möglich und schützt damit das private Netzwerk vor unbefugtem Zugriff.
4. Die geografischen Standorte der Benutzer sind geschützt und nicht öffentlichen oder gemeinsam genutzten Netzwerken wie dem Internet ausgesetzt.
5. Das Hinzufügen neuer Benutzer oder Benutzergruppen zum Netzwerk ist denkbar einfach, da VPNs sehr anpassbar sind. Es ist möglich, das Netzwerk zu erweitern, ohne dass zusätzliche neue Komponenten oder komplizierte Konfigurationen erforderlich sind.

Risiken bei der Verwendung einer VPN-Verbindung:

1. Sicherheitsrisiko durch Fehlkonfiguration. Da das Design und die Implementierung eines VPNs kompliziert sein kann, ist es notwendig, die Konfiguration der Verbindung einem hoch qualifizierten und erfahrenen Experten zu übertragen, um sicherzustellen, dass die Sicherheit des privaten Netzwerks nicht beeinträchtigt wird.
2. Zuverlässigkeit. Da eine VPN-Verbindung eine Internetverbindung erfordert, ist es wichtig, einen Anbieter zu wählen, der bewährt und getestet ist, um einen ausgezeichneten Internetservice bereitzustellen und minimale bis keine Ausfallzeiten zu garantieren.
3. Skalierbarkeit. Wenn eine neue Infrastruktur hinzugefügt oder neue Konfigurationen festgelegt werden müssen, können technische Probleme aufgrund der Inkompatibilität auftreten, insbesondere wenn es sich um andere Produkte oder Anbieter als die handelt, die Sie bereits verwenden.
4. Sicherheitsprobleme bei Mobilgeräten. Manchmal können bei der Verwendung von Mobilgeräten bei der Initiierung der VPN-Verbindung Sicherheitsprobleme insbesondere bei der Nutzung einer Wireless-Verbindung auftreten. Einige nicht verifizierte Anbieter fungieren als "kostenlose VPN-Anbieter" und können sogar Malware auf Ihrem Computer installieren. Aus diesem Grund können weitere Sicherheitsmaßnahmen hinzugefügt werden, um solche Probleme bei der Verwendung von Mobilgeräten zu vermeiden.
5. Langsame Verbindungsgeschwindigkeiten. Wenn Sie einen VPN-Client verwenden, der einen kostenlosen VPN-Service bereitstellt, ist zu erwarten, dass sich Ihre Verbindungsgeschwindigkeit verlangsamt, da diese Anbieter die Verbindungsgeschwindigkeiten nicht priorisieren.

In diesem Dokument wird erläutert, wie Sie mithilfe des Installationsassistenten die VPN-Verbindung auf dem Router der Serie RV34x konfigurieren.

Anwendbare Geräte

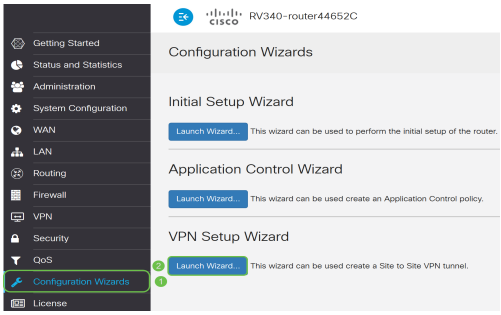
- Serie RV34x

Softwareversion

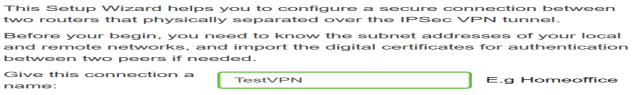
- 1,0/01,16

Konfigurieren der VPN-Verbindung mithilfe des Setup-Assistenten

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Routers an, und wählen Sie **Configuration Wizard (Konfigurationsassistent)** aus. Klicken Sie anschließend im Abschnitt *VPN-Einrichtungsassistent* auf **Launch Wizard (Startassistent starten)**.



Schritt 2: Geben Sie in das Feld einen Namen ein, um diese Verbindung zu identifizieren.



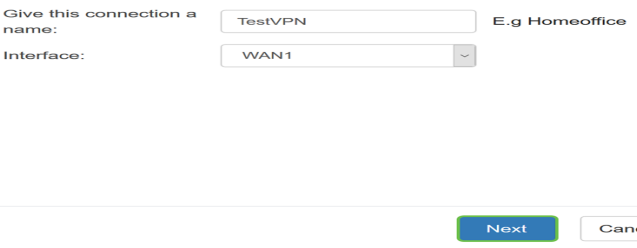
Hinweis: In diesem Beispiel wird TestVPN verwendet.

Schritt 3: Klicken Sie im Bereich Interface (Schnittstelle) auf das Dropdown-Menü, und wählen Sie die Schnittstelle aus, die Sie für diese Verbindung aktivieren möchten. Folgende Optionen stehen zur Verfügung:

- WAN1
- WAN2
- USB1
- USB2

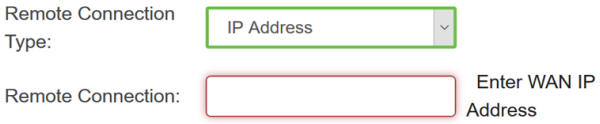
Hinweis: In diesem Beispiel wird WAN1 verwendet.

Schritt 4: Klicken Sie auf **Weiter**.



Schritt 5: Wählen Sie den Typ der Remote-Verbindung aus, indem Sie auf den Dropdown-Pfeil klicken. Folgende Optionen stehen zur Verfügung:

- IP Address (IP-Adresse): Wählen Sie diese Option aus, wenn Sie die IP-Adresse des Remote-Routers am anderen Ende des VPN-Tunnels verwenden möchten.
- FQDN - (Fully Qualified Domain Name) Wählen Sie diese Option aus, wenn Sie den Domänennamen des Remote-Routers am anderen Ende des VPN-Tunnels verwenden möchten.



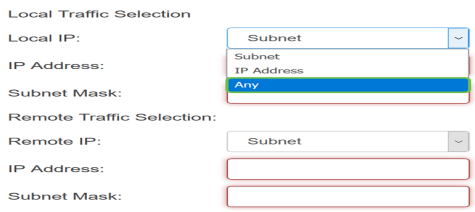
Hinweis: In diesem Beispiel wird die IP-Adresse ausgewählt.

Schritt 6: Geben Sie die WAN-IP-Adresse der Remote-Verbindung in das entsprechende Feld ein, und klicken Sie dann auf **Weiter**.

Hinweis: In diesem Beispiel wird 128.123.2.1 verwendet.

Schritt 7: Klicken Sie im Bereich "Lokale Datenverkehrsauswahl" auf das Dropdown-Menü, um die lokale IP auszuwählen. Folgende Optionen stehen zur Verfügung:

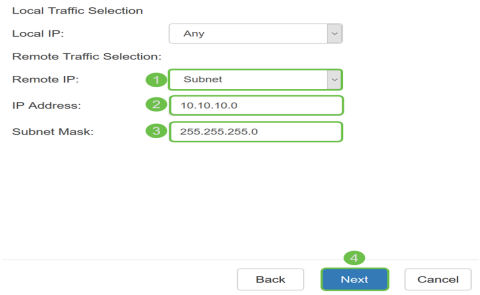
- Subnet (Subnetz): Wählen Sie diese Option aus, wenn Sie die IP-Adresse und die Subnetzmaske des lokalen Netzwerks eingeben möchten.
- IP Address (IP-Adresse): Wählen Sie diese Option aus, wenn Sie nur die IP-Adresse des lokalen Netzwerks eingeben möchten.
- Beliebig - Wählen Sie diese Option, wenn Sie eine der beiden Optionen möchten.



Hinweis: In diesem Beispiel wird Any (Beliebig) ausgewählt.

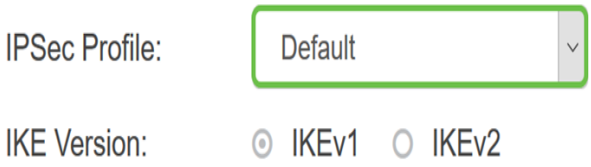
Schritt 8: Klicken Sie im Bereich Remote Traffic Selection (Remote-Datenverkehrsauswahl) auf den Dropdown-Pfeil, um die Remote-IP auszuwählen. Geben Sie die Remote-IP-Adresse und die Subnetzmaske in das dafür vorgesehene Feld ein, und klicken Sie dann auf **Weiter**. Folgende Optionen stehen zur Verfügung:

- Subnetz - Wählen Sie diese Option aus, wenn Sie die IP-Adresse und die Subnetzmaske des Remote-Netzwerks eingeben möchten.
- IP Address (IP-Adresse): Wählen Sie diese Option aus, wenn Sie nur die IP-Adresse des Remote-Netzwerks eingeben möchten.



Hinweis: In diesem Beispiel wird Subnet ausgewählt. 10.10.10.0 wurde als IP-Adresse eingegeben, und 255.255.255.0 wurde als Subnetzmaske eingegeben.

Schritt 9: Klicken Sie auf den Dropdown-Pfeil im Bereich IPSec Profile (IPSec-Profil), um das zu verwendende Profil auszuwählen.



Hinweis: In diesem Beispiel wird Default ausgewählt.

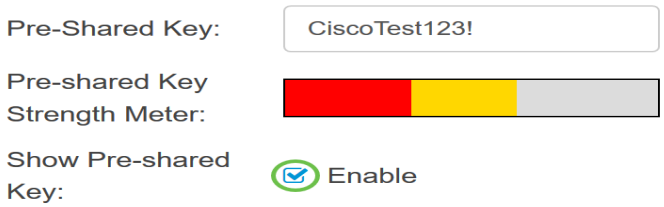
Schritt 10: Geben Sie im Bereich für Phase-1-Optionen den vorinstallierten Schlüssel für diese Verbindung in das dafür vorgesehene Feld ein. Hierbei handelt es sich um den vorinstallierten Schlüssel zur Authentifizierung des Remote-Internet Key Exchange (IKE)-Peers. An beiden Enden des VPN-Tunnels muss derselbe vorinstallierte Schlüssel verwendet werden. Für diesen Schlüssel können bis zu 30 Zeichen oder Hexadezimalwerte verwendet werden.

Hinweis: Es wird dringend empfohlen, den Pre-Shared Key regelmäßig zu ändern, um die Sicherheit Ihrer VPN-Verbindung zu gewährleisten.

Hinweis: Die Stärke des vorinstallierten Schlüssels gibt die Stärke des von Ihnen eingegebenen Schlüssels an, basierend auf:

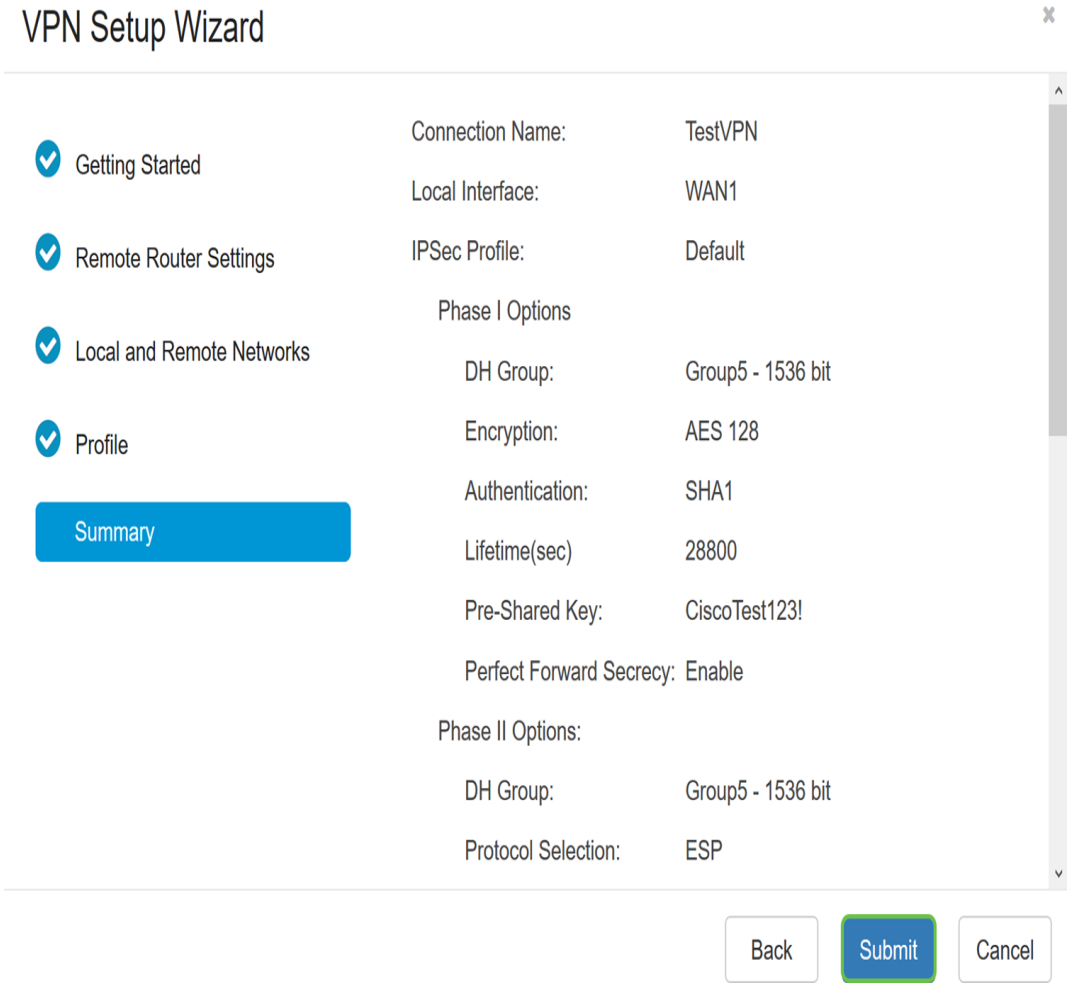
- Rot - Das Kennwort ist schwach.
- Gelb - Das Passwort ist ziemlich stark.
- Grün - Das Kennwort ist stark.

Schritt 11: (Optional) Sie können auch das Kontrollkästchen **Aktivieren** im Dialogfeld Nur Text anzeigen aktivieren aktivieren, wenn Sie das Kennwort im Klartext anzeigen möchten.



Schritt 12: Klicken Sie auf **Weiter**.  .

Schritt 13: Dann werden alle Konfigurationsdetails der VPN-Verbindung angezeigt. Klicken Sie auf **Senden**.



Sie sollten jetzt mithilfe des Installationsassistenten die VPN-Verbindung auf dem Router der Serie RV34x erfolgreich konfiguriert haben. Um ein Site-to-Site-VPN erfolgreich zu verbinden, müssen Sie den Einrichtungsassistenten auf dem Remote-Router konfigurieren.