Konfigurieren eines Site-to-Site-VPN-Tunnels zwischen dem Cisco RV320 Gigabit Dual-WAN VPN-Router und dem Cisco Integrated Services Adapter der Serie 500

Ziel

Ein Virtual Private Network (VPN) ist eine Technologie, die häufig zum Verbinden von Remote-Netzwerken mit einem privaten Hauptnetzwerk verwendet wird. Dabei wird eine private Verbindung in Form eines verschlüsselten Kanals über öffentliche Leitungen simuliert. Ein Remote-Netzwerk kann eine Verbindung zu einem privaten Hauptnetzwerk herstellen, als ob es als Teil des privaten Hauptnetzwerks ohne Sicherheitsbedenken existiert, da der VPN-Datenverkehr in zwei Phasen verschlüsselt wird, sodass nur die VPN-Endpunkte wissen, wie er entschlüsselt werden kann.
Diese Kurzanleitung enthält ein Beispieldesign für den Aufbau eines Site-to-Site-IPsec-VPN-Tunnels zwischen einem Cisco Integrated Services Adapter der Serie 500 und einem Cisco Router der Serie RV.

Anwendbare Geräte

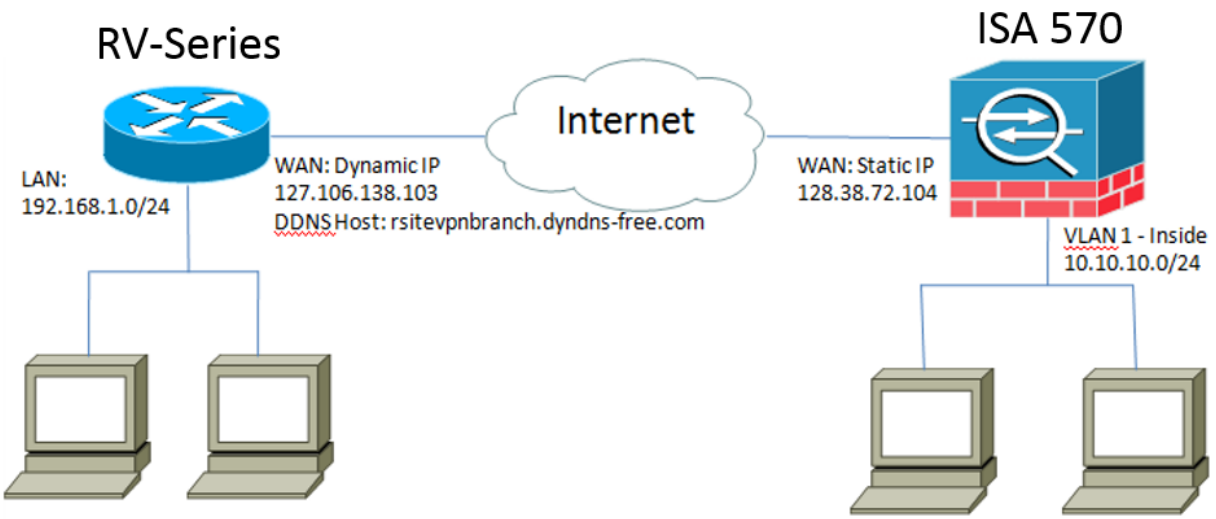
·Cisco Router der RV-Serie (RV320)
· Cisco Integrated Services Adapter der Serie 500 (ISA570)

Softwareversion

·4.2.2.08 [Cisco VPN-Router der RV0xx-Serie]

Vorkonfiguration

Netzwerkdiagramm
Im Folgenden sehen Sie eine Site-to-Site-VPN-Topologie.



Ein standortübergreifender IPsec-VPN-Tunnel wird zwischen dem Cisco Router der RV-Serie in der Außenstelle und dem Cisco ISA der Serie 500 in der Hauptniederlassung konfiguriert und eingerichtet.
Mit dieser Konfiguration können ein Host in LAN 192.168.1.0/24 in der Außenstelle und ein Host in LAN 10.10.10.0/24 in der Hauptniederlassung sicher über VPN miteinander kommunizieren.

Kernkonzepte

Internet Key Exchange (IKE)

Internet Key Exchange (IKE) ist das Protokoll zum Einrichten einer Sicherheitszuordnung (Security Association, SA) in der IPsec-Protokoll-Suite. IKE baut auf dem Oakley-Protokoll, der Internet Security Association und dem Key Management Protocol (ISAKMP) auf und richtet mithilfe eines Diffie-Hellman-Schlüsselaustauschs einen gemeinsamen Sitzungsgeheim ein, von dem kryptografische Schlüssel abgeleitet werden.

Internet Security Association und Key Management Protocol (ISAKMP)

Die Aushandlung des VPN-Tunnels zwischen zwei VPN-Endpunkten erfolgt über die Internet Security Association und das Key Management Protocol (ISAKMP). Sie definiert die Verfahren für Authentifizierung, Kommunikation und Schlüsselgenerierung und wird vom IKE-Protokoll zum Austausch von Verschlüsselungsschlüsseln und zum Herstellen einer sicheren Verbindung verwendet.

Internet Protocol Security (IPsec)

IP Security Protocol (IPsec) ist eine Protokoll-Suite zur Sicherung der IP-Kommunikation durch Authentifizierung und Verschlüsselung jedes IP-Pakets eines Datenstroms. IPsec enthält außerdem Protokolle zur Einrichtung der gegenseitigen Authentifizierung zwischen Agenten zu Beginn der Sitzung und zur Aushandlung der während der Sitzung zu verwendenden kryptografischen Schlüssel. IPsec kann verwendet werden, um Datenflüsse

zwischen zwei Hosts, Gateways oder Netzwerken zu schützen.

Tipps zum Design

VPN-Topologie - Eine Point-to-Point-VPN-Topologie bedeutet, dass zwischen dem Hauptstandort und dem Remote-Standort ein sicherer IPsec-Tunnel konfiguriert wird. Unternehmen benötigen häufig mehrere Remote-Standorte in einer Topologie mit mehreren Standorten und implementieren entweder eine Hub-and-Spoke-VPN-Topologie oder eine Full-Mesh-VPN-Topologie. Eine Hub-and-Spoke-VPN-Topologie bedeutet, dass Remote-Standorte keine Kommunikation mit anderen Remote-Standorten benötigen, und jeder Remote-Standort stellt nur einen sicheren IPsec-Tunnel mit der Hauptniederlassung her. Eine vollständig vermaschte VPN-Topologie bedeutet, dass Außenstellen mit anderen Remote-Standorten kommunizieren müssen. Jeder entfernte Standort richtet ein sicheres IPsec-Tunnel mit dem Hauptstandort und allen anderen Remote-Standorten ein.
VPN-Authentifizierung - Das IKE-Protokoll dient zum Authentifizieren von VPN-Peers beim Aufbau eines VPN-Tunnels. Es gibt verschiedene IKE-Authentifizierungsmethoden, und der vorinstallierte Schlüssel ist die praktischste Methode. Cisco empfiehlt die Verwendung eines starken vorinstallierten Schlüssels.
VPN Encryption - Um die Vertraulichkeit der über das VPN übertragenen Daten sicherzustellen, werden Verschlüsselungsalgorithmen zum Verschlüsseln der Nutzlast von IP-Paketen verwendet. DES, 3DES und AES sind drei gängige Verschlüsselungsstandards. Im Vergleich zu DES und 3DES gilt AES als die sicherste Variante. Cisco empfiehlt nachdrücklich die Anwendung einer AES-128-Bit- oder höheren Verschlüsselung (z. B. AES-192 und AES-256). Stärkere Verschlüsselungsalgorithmen erfordern jedoch mehr Verarbeitungsressourcen von einem Router.
Dynamic WAN IP Addressing and Dynamic Domain Name Service (DDNS) - Der VPN-Tunnel muss zwischen zwei öffentlichen IP-Adressen eingerichtet werden. Wenn die WAN-Router statische IP-Adressen vom Internet Service Provider (ISP) erhalten, kann der VPN-Tunnel direkt über statische öffentliche IP-Adressen implementiert werden. Die meisten kleinen Unternehmen nutzen jedoch kosteneffiziente Breitband-Internetdienste wie DSL oder Kabel und erhalten dynamische IP-Adressen von ihren ISPs. In solchen Fällen kann der Dynamic Domain Name Service (DDNS) verwendet werden, um die dynamische IP-Adresse einem vollqualifizierten Domänennamen (FQDN) zuzuordnen.
LAN-IP-Adressierung - Die private LAN-IP-Netzwerkadresse jedes Standorts darf sich nicht überschneiden. Die Standard-LAN-IP-Netzwerkadresse an jedem Remote-Standort sollte immer geändert werden.

Tipps zur Konfiguration

Checkliste vor der Konfiguration

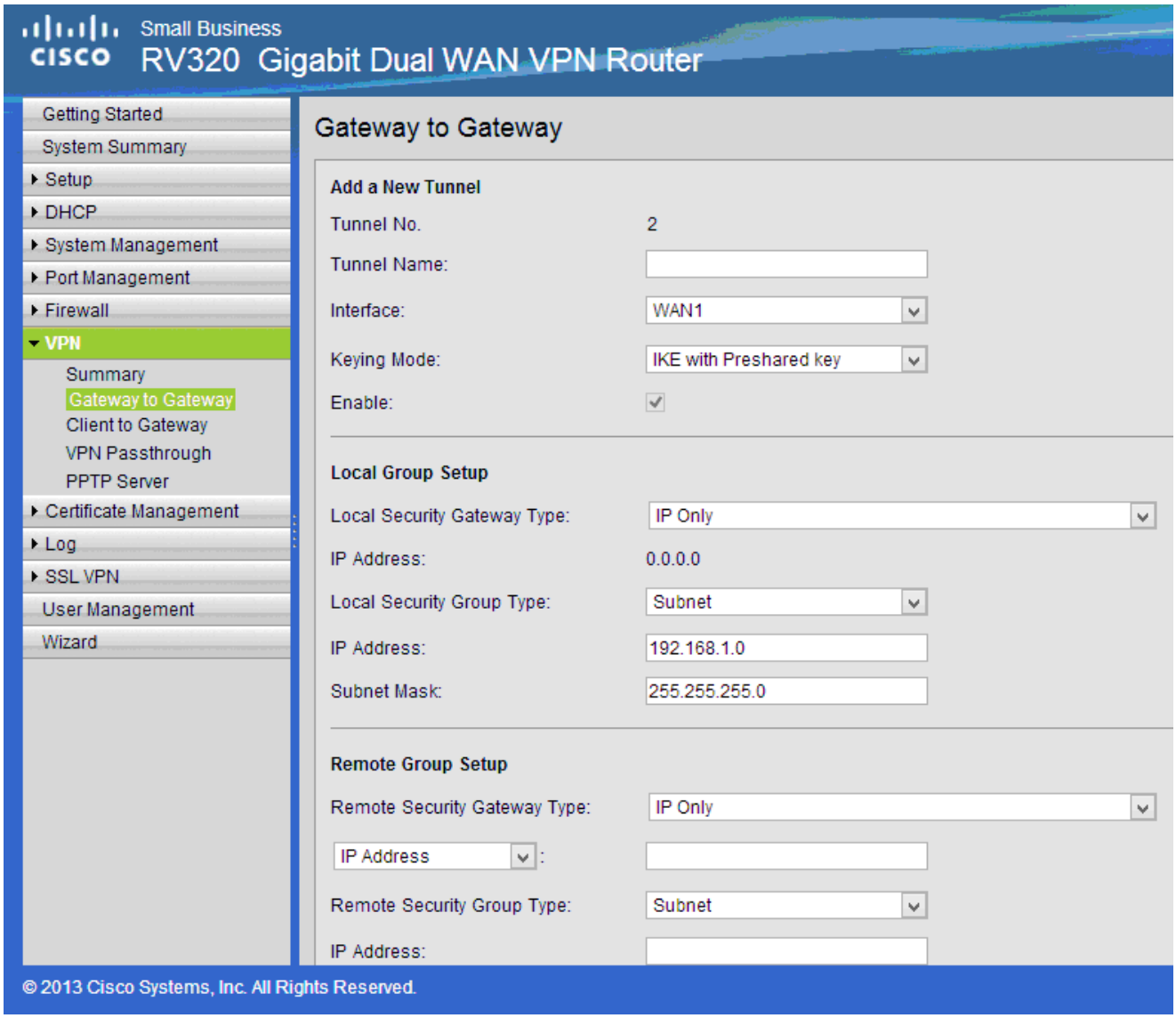
Schritt 1: Schließen Sie ein Ethernetkabel zwischen dem RV320 und dem DSL- oder Kabelmodem an, und verbinden Sie ein Ethernetkabel zwischen dem ISA570 und dem DSL- oder Kabelmodem.
Schritt 2: Schalten Sie den RV320 ein, und verbinden Sie dann interne PCs, Server und andere IP-Geräte mit den LAN-Ports des RV320.
Schritt 3: Schalten Sie die ISA570 ein, und verbinden Sie dann interne PCs, Server und andere IP-Geräte mit den LAN-Ports der ISA570.
Schritt 4: Konfigurieren Sie die Netzwerk-IP-Adressen an jedem Standort in verschiedenen Subnetzen. In diesem Beispiel wird für das LAN der Außenstelle 192.168.1.0 und für das LAN der Hauptniederlassung 10.10.10.0 verwendet.
Schritt 5: Stellen Sie sicher, dass lokale PCs eine Verbindung zu ihren jeweiligen Routern und mit anderen PCs im selben LAN herstellen können.

Identifizieren der WAN-Verbindung

Sie müssen wissen, ob Ihr ISP eine dynamische IP-Adresse oder eine statische IP-Adresse bereitstellt. Der ISP stellt in der Regel eine dynamische IP-Adresse bereit. Sie sollten dies jedoch bestätigen, bevor Sie die Konfiguration des Site-to-Site-VPN-Tunnels abschließen.

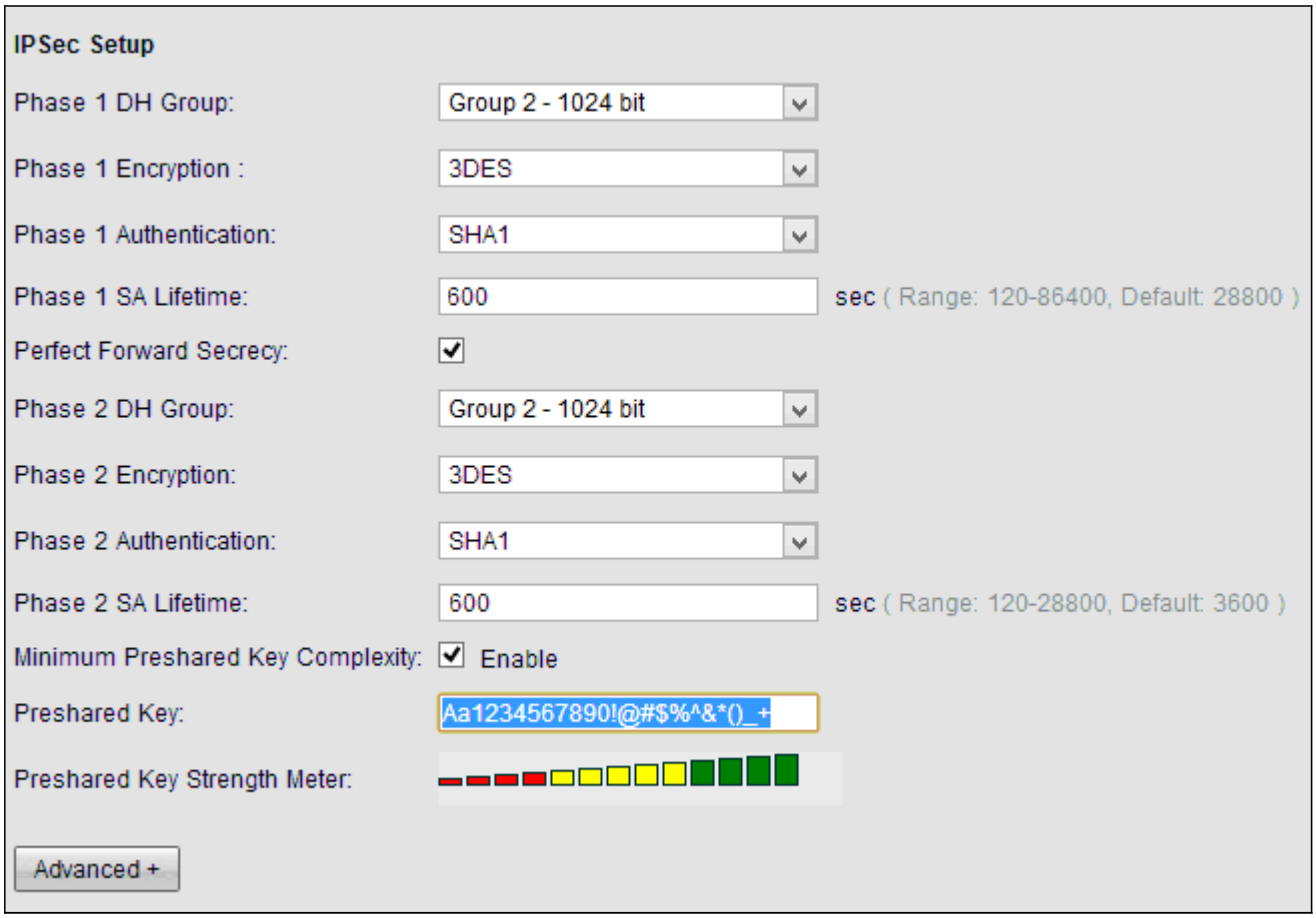
Konfigurieren des Site-to-Site-IPsec-VPN-Tunnels für RV320 in der Außenstelle

Schritt 1: Gehen Sie zu **VPN > Gateway-to-Gateway** (siehe Abbildung).
a) Geben Sie einen Tunnel-Namen ein, z. B. RemoteOffice.
b) Legen Sie für die Schnittstelle WAN1 fest.
c) Legen Sie für den Keying Mode IKE mit vorinstalliertem Schlüssel fest.
d) Geben Sie die lokale IP-Adresse und die Remote-IP-Adresse ein.
Die folgende Abbildung zeigt die Seite RV320 Gigabit Dual-WAN VPN-Router Gateway-to-Gateway:



Schritt 2: IPSec-Tunneleinstellungen einrichten (siehe Bild)
a) Legen Sie *Verschlüsselung* auf 3DES fest.
b) Legen Sie die *Authentifizierung* auf SHA1 fest.
c) Aktivieren Sie *Perfect Forward Secrecy (Perfektes Weiterleiten)*.

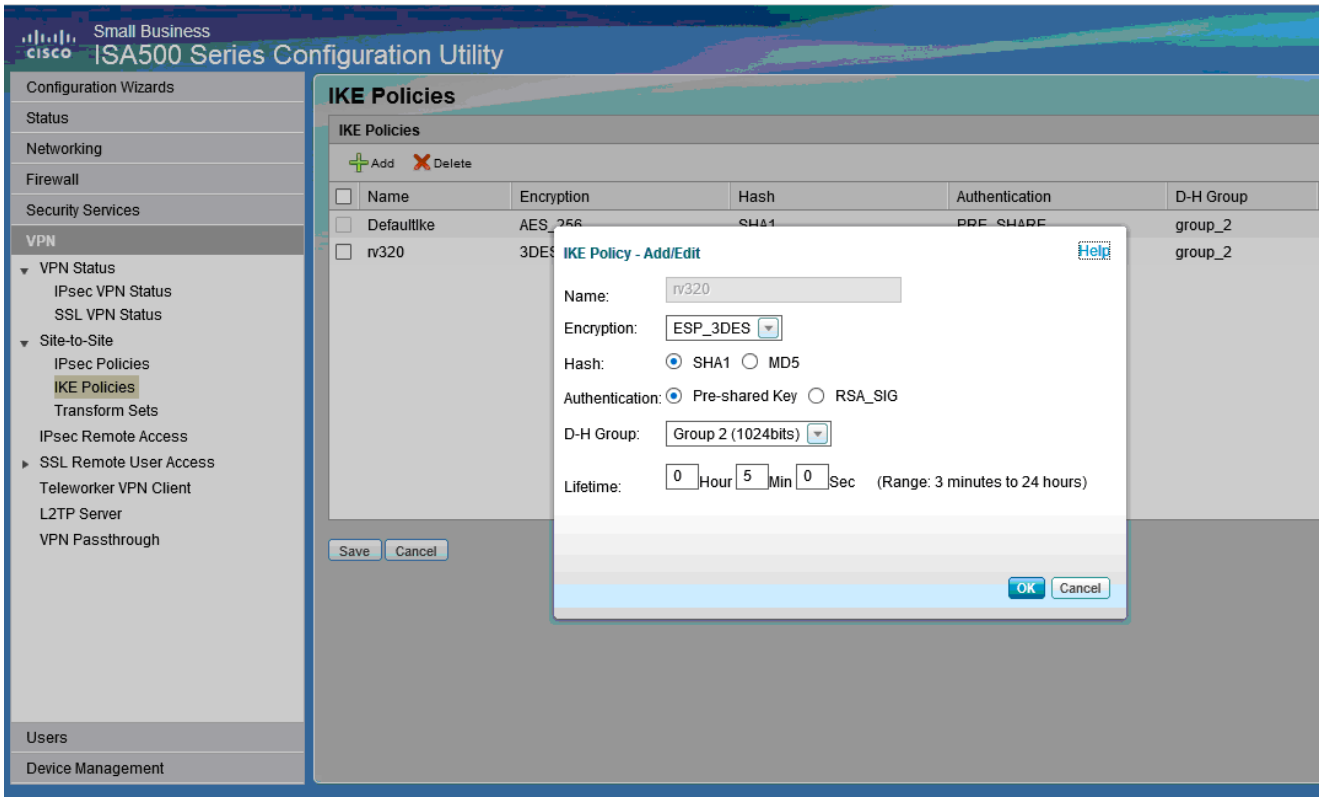
d) Richten Sie den *vorinstallierten Schlüssel ein* (muss auf beiden Routern identisch sein).
Im Folgenden sehen Sie IPSec-Setup (Phase 1 und 2):



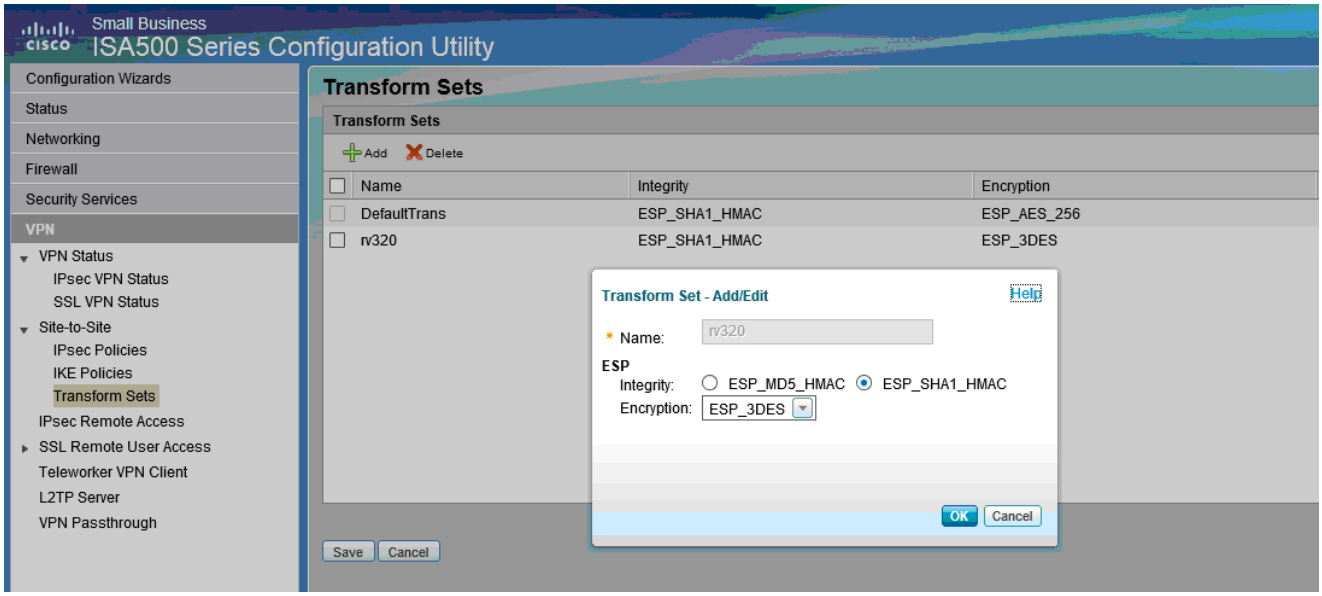
Hinweis: Beachten Sie, dass die IPsec-Tunneleinstellungen auf beiden Seiten des standortübergreifenden IPsec-VPN-Tunnels übereinstimmen müssen. Wenn zwischen den IPsec-Tunneleinstellungen des RV320 und der ISA570 Diskrepanzen bestehen, verhandeln beide Geräte den Verschlüsselungsschlüssel nicht und können keine Verbindung herstellen.
Schritt 3: Klicken Sie auf **Speichern**, um die Konfiguration abzuschließen.

Konfigurieren des Site-to-Site-IPsec-VPN-Tunnels für ISA570 in der Hauptniederlassung

Schritt 1: Gehen Sie zu **VPN > IKE-**Richtlinien (siehe Bild).
a) Legen Sie *Verschlüsselung* auf ESP_3DES fest.
b) Legen Sie *Hash* auf SHA1 fest.
c) Legen Sie *für die Authentifizierung* den vorinstallierten Schlüssel fest.
d) Legen Sie *D-H Group* auf Group 2 (1024 Bit) fest.
Das folgende Bild zeigt IKE-Richtlinien:



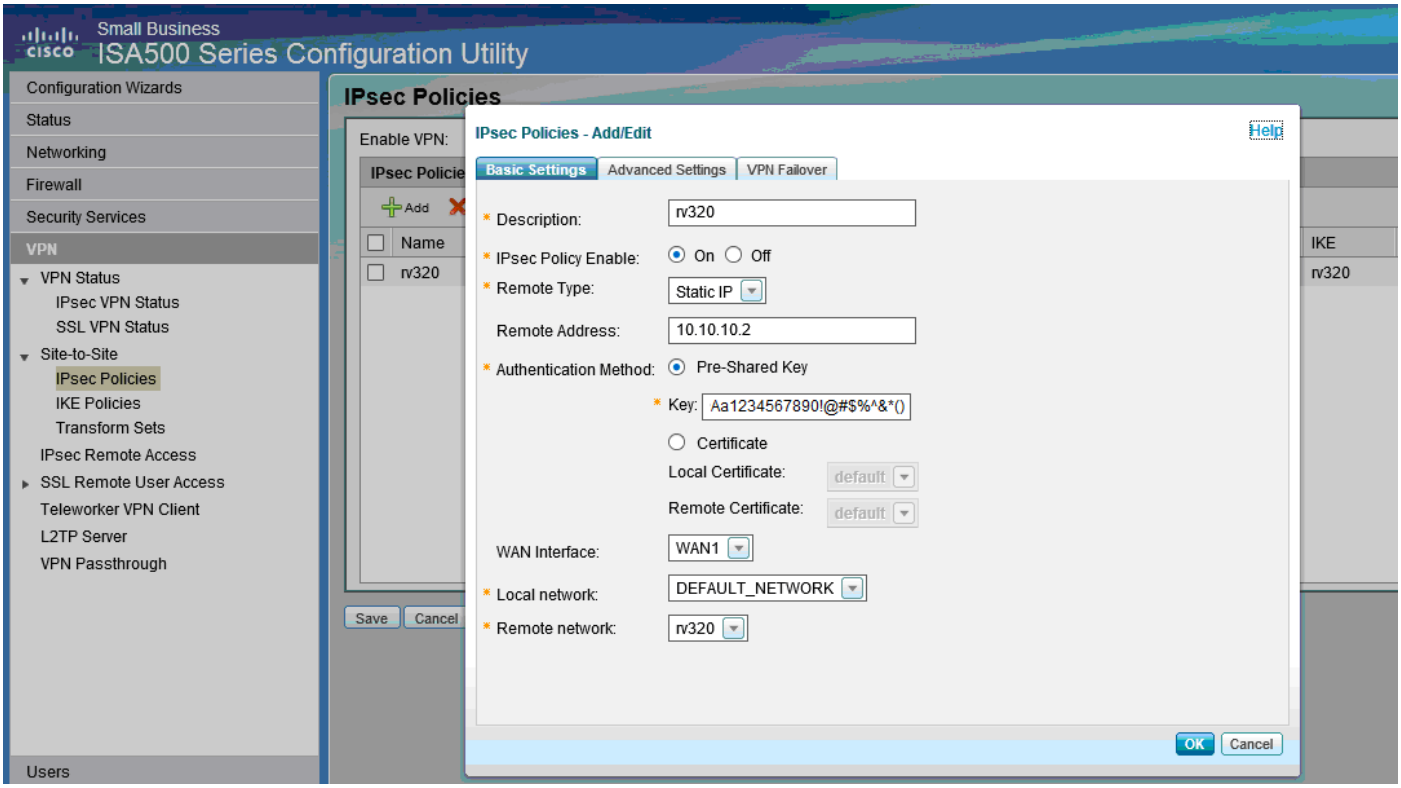
Schritt 2: Gehen Sie zu **VPN > IKE Transform Sets** (siehe Bild).
a) Legen Sie *Integrity* auf ESP_SHA1_HMAC fest.
b) Legen Sie *Verschlüsselung* auf ESP_DES fest.
Im Folgenden werden IKE-Transformationssätze dargestellt:



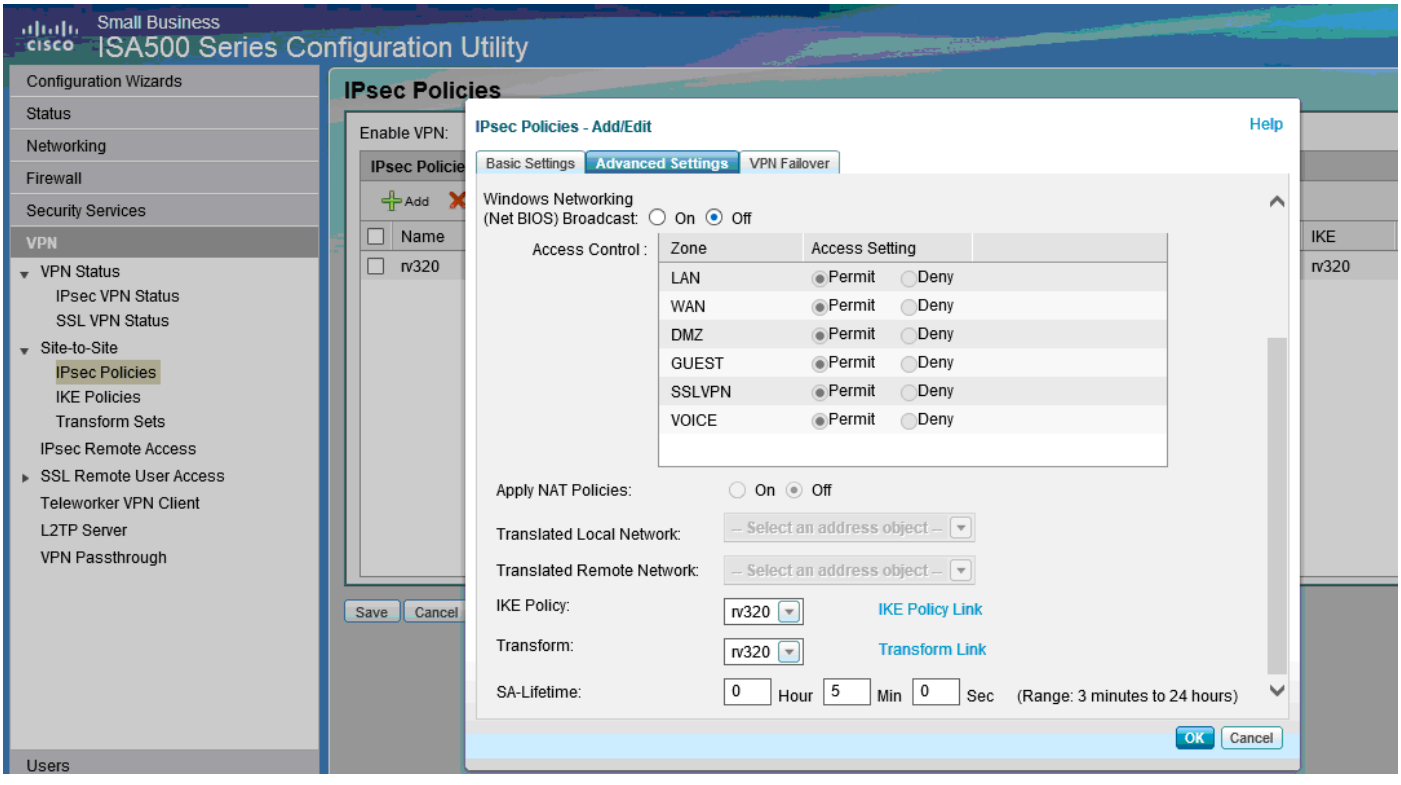
Schritt 3: Gehen Sie zu **VPN > IPsec Policies > Add > Basic Settings** (siehe Bild)

a) Geben Sie eine *Beschreibung* ein, z. B. RV320.
b) Legen Sie *IPsec Policy Enable* auf On fest.
c) Legen Sie *den Remote-Typ auf Static IP (Statische IP) fest*.
d) Geben Sie die *Remote-Adresse ein*.
e) Legen Sie die *Authentifizierungsmethode* auf Pre-Shared Key fest.
f) Legen Sie *die WAN-Schnittstelle* auf WAN1 fest.
B. Legen Sie *für das lokale Netzwerk* den Wert DEFAULT_NETWORK fest.

h) *Remote-Netzwerk* auf RV320 eingestellt.
Das folgende Bild zeigt die grundlegenden Einstellungen der IPsec-Richtlinien:



Schritt 4: Gehen Sie zu **VPN > IPsec Policies > Add > Advanced Settings** (siehe Bild).
a) Legen Sie *IKE-Richtlinien* und *IKE-Transform-Sets* jeweils auf die in den Schritten 1 und 2 erstellten fest.
b) Legen Sie *SA-Lifetime* auf 0 Stunde 5 Minuten 0 Sek. fest.
c) Klicken Sie auf **OK**.
Im Folgenden werden erweiterte Einstellungen für IPsec-Richtlinien dargestellt:



Schritt 5: Verbinden des Site-to-Site-IPsec-VPN-Tunnels (siehe Abbildung)
a) *VPN aktivieren* auf Ein
b) Klicken Sie auf die Schaltfläche **Verbinden**.
Die folgende Abbildung zeigt die Verbindungstaste: