Konfigurieren von IPSec-Profilen (Auto Keying Mode) auf dem RV160 und dem RV260

Ziel

In diesem Dokument wird die Erstellung eines neuen IPsec-Profils mithilfe des automatischen Keying-Modus auf Routern der Serien RV160 und RV260 beschrieben.

Einführung

IPsec stellt sicher, dass Sie eine sichere private Kommunikation über das Internet haben. Sie bietet zwei oder mehr Hosts Datenschutz, Integrität und Authentizität für die Übertragung vertraulicher Informationen über das Internet. IPsec wird in der Regel im Virtual Private Network (VPN) verwendet und auf der IP-Ebene implementiert. Die Verwendung von IPsec kann viele Anwendungen unterstützen, denen es an Sicherheit mangelt. Ein VPN wird verwendet, um einen sicheren Kommunikationsmechanismus für vertrauliche Daten und IP-Informationen bereitzustellen, die über ein unsicheres Netzwerk wie das Internet übertragen werden. Es bietet eine flexible Lösung für Remote-Benutzer und das Unternehmen, um vertrauliche Informationen von anderen Parteien im gleichen Netzwerk zu schützen.

Damit die beiden Enden eines VPN-Tunnels erfolgreich verschlüsselt und eingerichtet werden können, müssen beide die Methoden der Verschlüsselung, Entschlüsselung und Authentifizierung vereinbaren. IPsec-Profil ist die zentrale Konfiguration in IPsec, die Algorithmen wie Verschlüsselung, Authentifizierung und DH-Gruppe (Diffie-Hellman) für Phase-I- und II-Aushandlung im Auto-Modus sowie im manuellen Keying-Modus definiert. In Phase 1 werden die vorinstallierten Schlüssel zur Erstellung einer sicheren, authentifizierten Kommunikation eingerichtet. In Phase 2 wird der Datenverkehr verschlüsselt. Sie können die meisten IPsec-Parameter konfigurieren, z. B. Protokolle, Modus, Algorithmen, Perfect Forward Secrecy (PFS), Security Association (SA)-Lebensdauer und das Schlüsselverwaltungsprotokoll.

Beachten Sie, dass der Remote-Router beim Konfigurieren von Site-to-Site-VPN dieselben Profileinstellungen wie der lokale Router verwenden muss.

Weitere Informationen zur Cisco IPsec-Technologie finden Sie unter: Einführung in die Cisco IPSec-Technologie.

Um das IPsec-Profil und das Site-to-Site-VPN mithilfe des VPN-Setup-Assistenten zu konfigurieren, klicken Sie auf den Link: Konfigurieren des VPN-Setup-Assistenten auf dem RV160 und dem RV260.

Informationen zum Konfigurieren von Site-to-Site-VPN finden Sie im Dokument: Konfigurieren von Site-to-Site-VPN auf dem RV160 und dem RV260.

Anwendbare Geräte

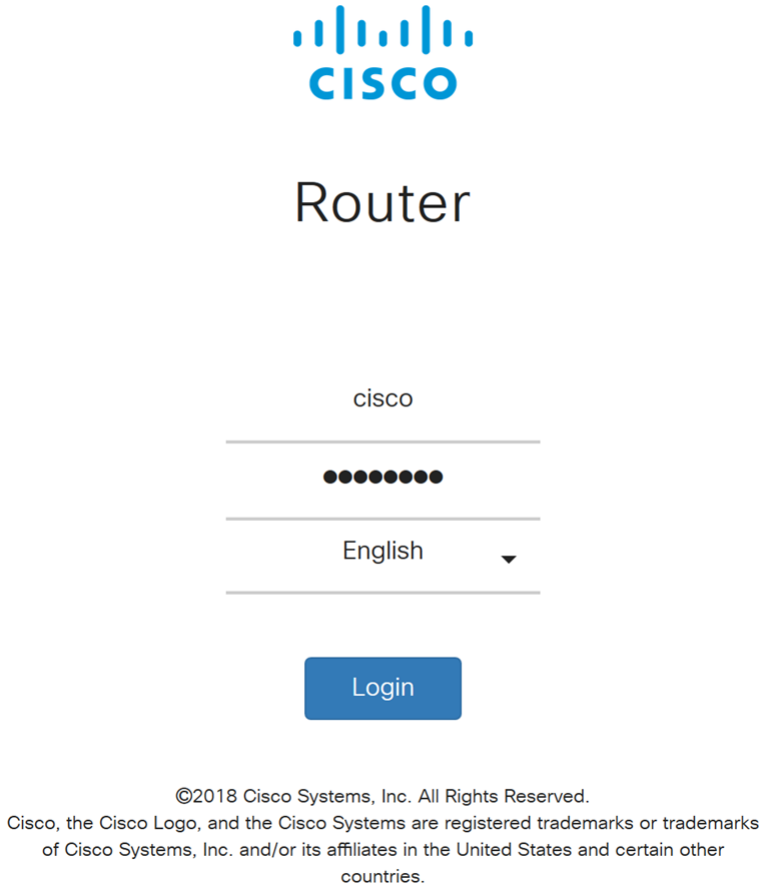
- RV160
- RV260

Softwareversion

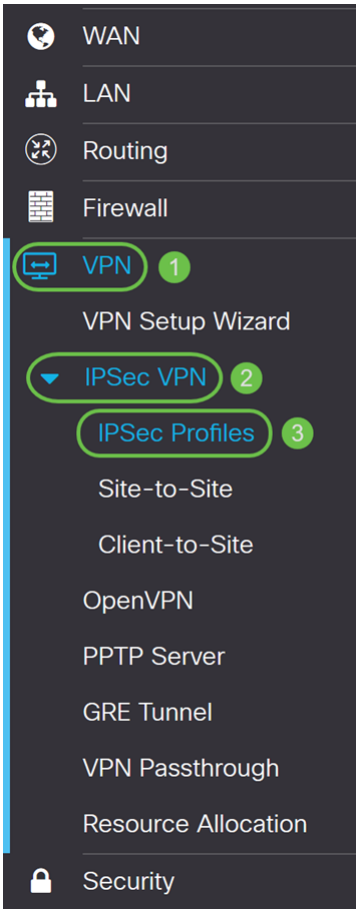
- 1.0.00.13

Konfigurieren von IPsec-Profilen

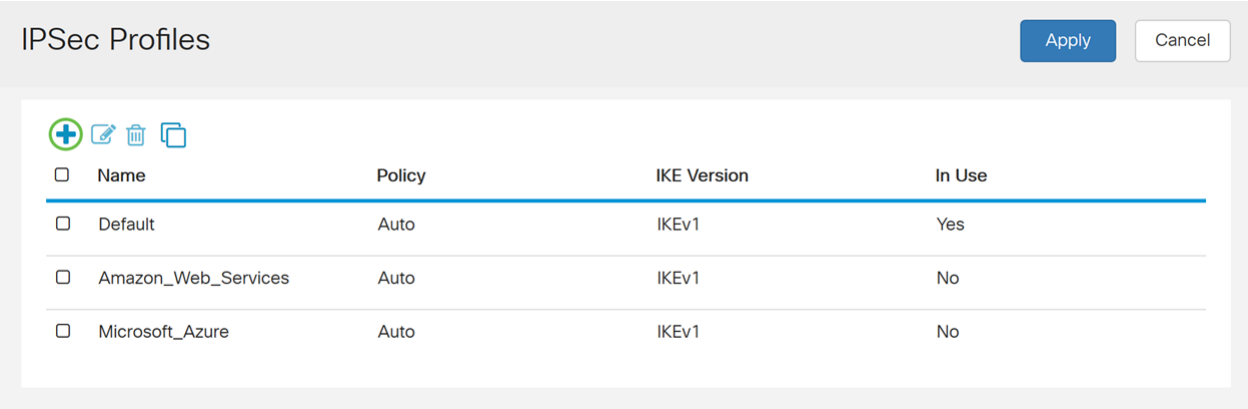
Schritt 1: Melden Sie sich auf der Webkonfigurationsseite Ihres Routers an.



Schritt 2: Navigieren Sie zu **VPN > IPSec VPN > IPSec Profiles**.



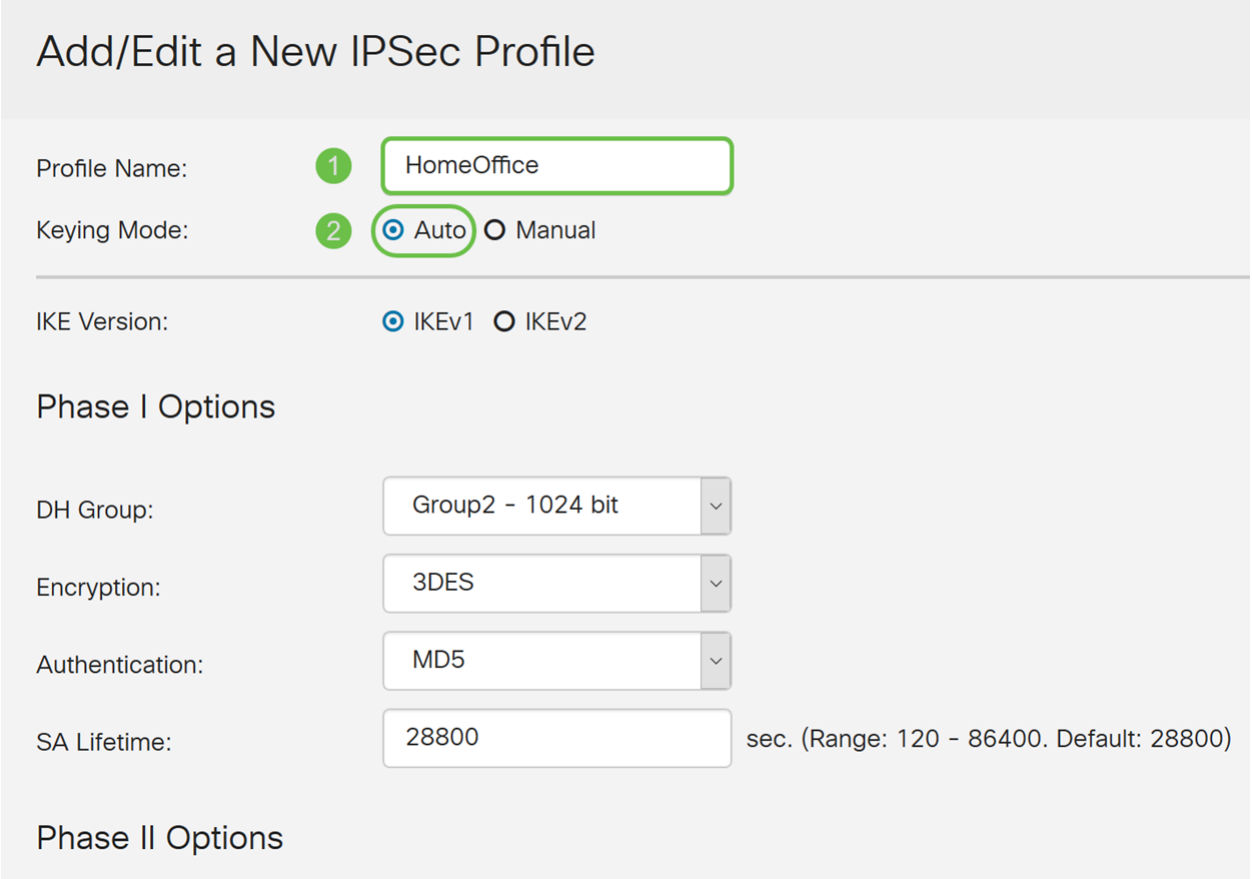
Schritt 3: Klicken Sie in der Tabelle *IPSec-Profile* auf **Hinzufügen,** um ein neues IPsec-Profil zu erstellen. Sie können auch ein Profil bearbeiten, löschen oder kopieren.



Schritt 4: Geben Sie einen Profilnamen ein, und wählen Sie den Keying-Modus (Automatisch oder Manuell) aus.

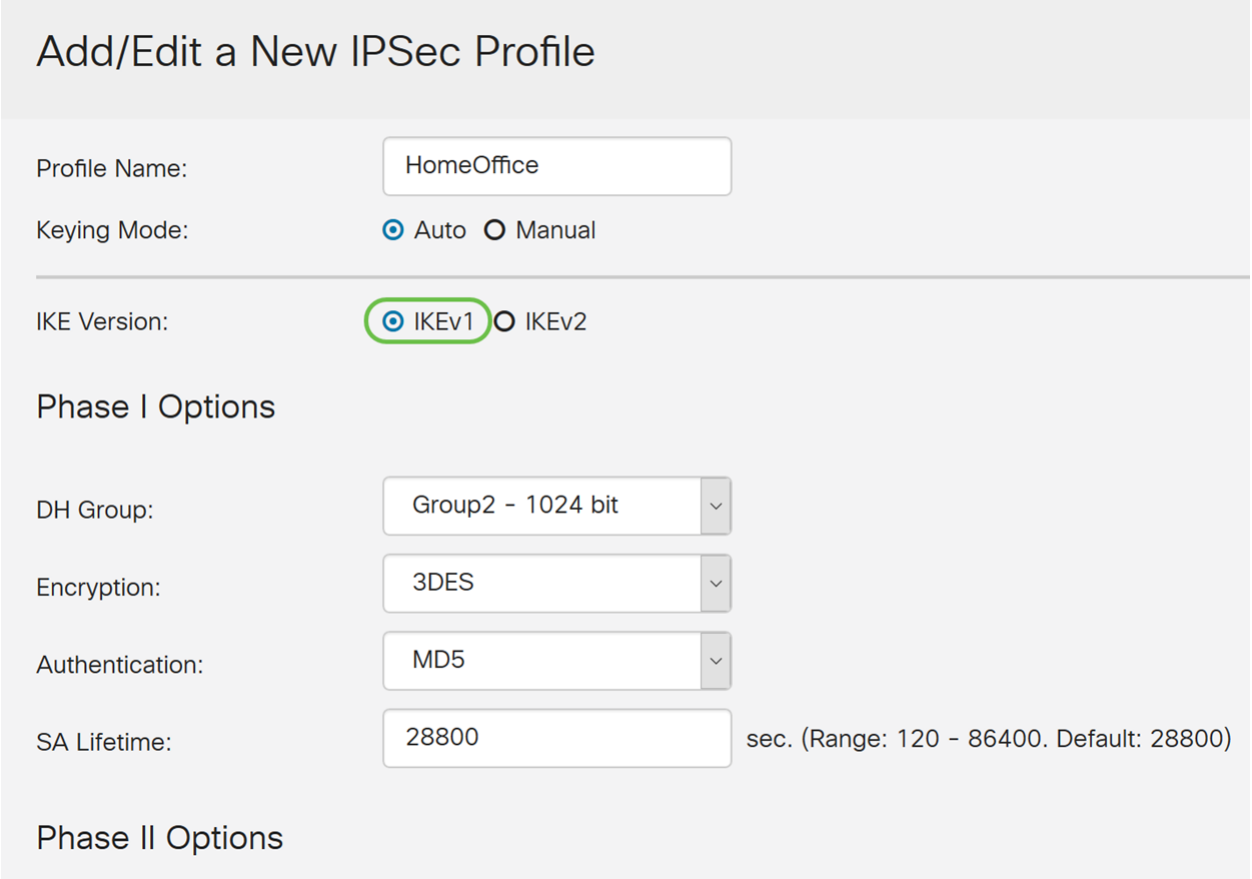
HomeOffice wird als *Profilname* eingegeben.

Auto (Automatisch) ist für den *Keying Mode* ausgewählt.



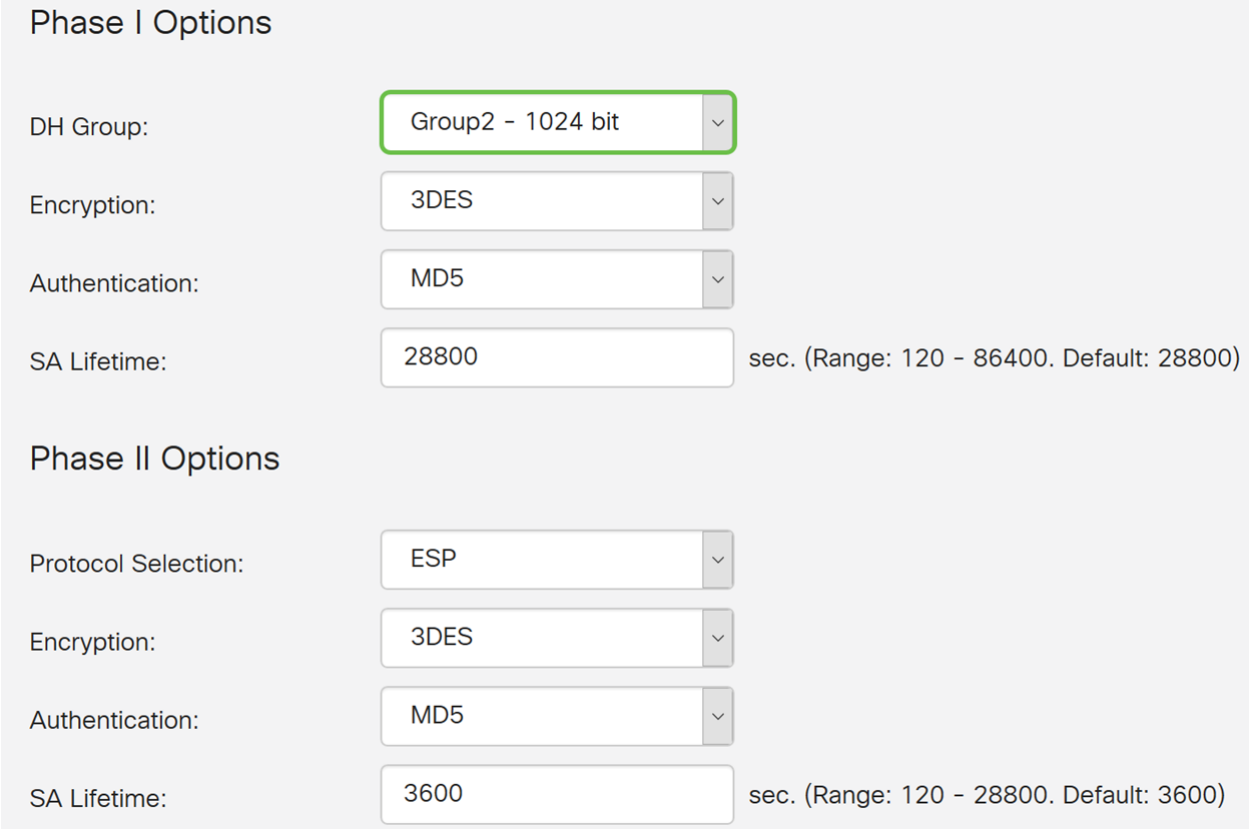
Schritt 5: Wählen Sie *Internet Key Exchange Version 1* (*IKEv1)* oder *Internet Key Exchange Version 2 (IKEv2)* als IKE-Version aus. IKE ist ein Hybridprotokoll, das den Oakley-Schlüsselaustausch und den Skeme-Schlüsselaustausch innerhalb des ISAKMP-Frameworks (Internet Security Association and Key Management Protocol) implementiert. Oakley und Skeme legen beide fest, wie authentifiziertes Keying-Material abgeleitet werden kann. Skeme beinhaltet jedoch auch eine schnelle Schlüsselerfrischung. IKE stellt die Authentifizierung der IPsec-Peers bereit, handelt IPsec-Schlüssel aus und handelt IPsec-Sicherheitszuordnungen aus. IKEv2 ist effizienter, da weniger Pakete für den Schlüsselaustausch erforderlich sind, mehr Authentifizierungsoptionen unterstützt werden, während IKEv1 nur über gemeinsam genutzten Schlüssel und zertifikatbasierte Authentifizierung verfügt. In diesem Beispiel wurde **IKEv1** als unsere IKE-Version ausgewählt.

Hinweis: Wenn Ihr Gerät IKEv2 unterstützt, wird die Verwendung von IKEv2 empfohlen. Wenn Ihre Geräte IKEv2 nicht unterstützen, verwenden Sie IKEv1.



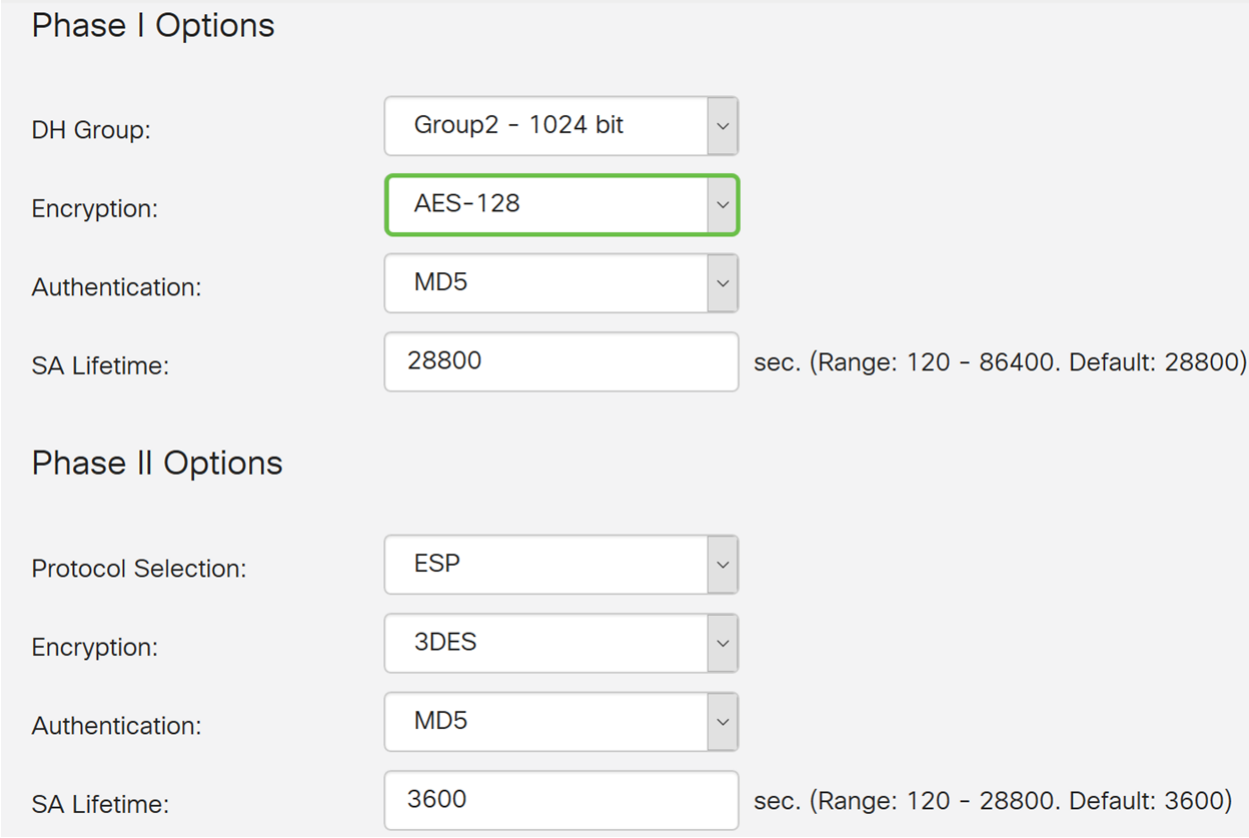
Schritt 6: In Phase I werden die Schlüssel eingerichtet, mit denen Sie Daten in Phase II verschlüsseln können. Wählen Sie im Abschnitt *Phase I* eine Diffie-Hellman-Gruppe (DH) aus. DH ist ein Schlüsselaustauschprotokoll mit zwei Gruppen unterschiedlicher Primkey-Längen, **Gruppe 2 - 1024 Bit** und **Gruppe 5 - 1536 Bit**. Für diese Demonstration wurde **Gruppe 2 - 1024 Bit** ausgewählt.

Hinweis: Wählen Sie Gruppe 2 aus, um die Geschwindigkeit zu erhöhen und die Sicherheit zu verringern. Wählen Sie Gruppe 5 aus, um die Geschwindigkeit zu verlangsamen und die Sicherheit zu erhöhen. Gruppe 2 ist standardmäßig ausgewählt.



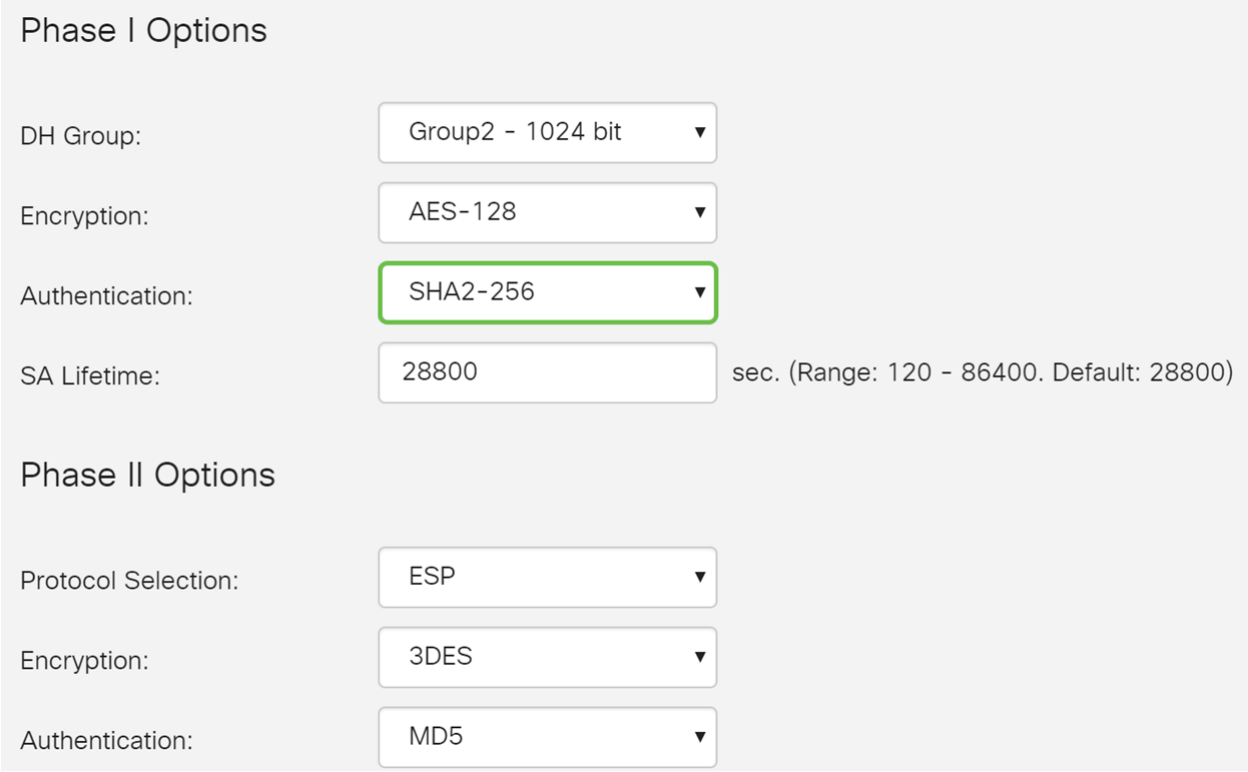
Schritt 7: Wählen Sie eine Verschlüsselungsoption (**3DES**, **AES-128**, **AES-192** oder **AES-256**) aus der Dropdown-Liste aus. Diese Methode bestimmt den Algorithmus, der zum Verschlüsseln und Entschlüsseln von ESP-/ISAKMP-Paketen verwendet wird. Der Triple Data Encryption Standard (3DES) verwendet dreimal die DES-Verschlüsselung, ist aber jetzt ein Legacy-Algorithmus. Dies bedeutet, dass sie nur verwendet werden sollte, wenn es keine besseren Alternativen gibt, da sie immer noch ein marginales, aber akzeptables Sicherheitsniveau bietet. Benutzer sollten diese Daten nur dann verwenden, wenn sie für die Abwärtskompatibilität erforderlich sind, da sie für einige "Block-Kollision"-Angriffe anfällig sind. 3DES wird nicht empfohlen, da es nicht als sicher gilt. Advanced Encryption Standard (AES) ist ein Verschlüsselungsalgorithmus, der sicherer ist als DES. AES verwendet eine größere Schlüsselgröße, die sicherstellt, dass der einzige bekannte Ansatz zur Entschlüsselung einer Nachricht darin besteht, dass ein Eindringling jeden möglichen Schlüssel ausprobiert. Es wird empfohlen, AES zu verwenden, wenn Ihr Gerät es unterstützen kann. In diesem Beispiel haben wir **AES-128** als Verschlüsselungsoption ausgewählt.

Hinweis: Hier einige weitere Ressourcen, die Ihnen helfen können: Konfigurieren der Sicherheit für VPNs mit IPsec und Verschlüsselung der nächsten Generation.



Schritt 8: Die Authentifizierungsmethode legt fest, wie die ESP-Headerpakete validiert werden. Dies ist der Hashing-Algorithmus, der in der Authentifizierung verwendet wird, um zu überprüfen, ob Seite A und Seite B wirklich die sind, die sie angeblich sind. MD5 ist ein unidirektionaler Hash-Algorithmus, der einen 128-Bit-Digest erzeugt und schneller als SHA1 ist. SHA1 ist ein unidirektionaler Hashing-Algorithmus, der ein 160-Bit-Digest erzeugt, während SHA2-256 ein 256-Bit-Digest erzeugt. SHA2-256 wird empfohlen, da es sicherer ist. Stellen Sie sicher, dass beide Enden des VPN-Tunnels dieselbe Authentifizierungsmethode verwenden. Wählen Sie eine Authentifizierung aus (**MD5, SHA1** oder **SHA2-256**).

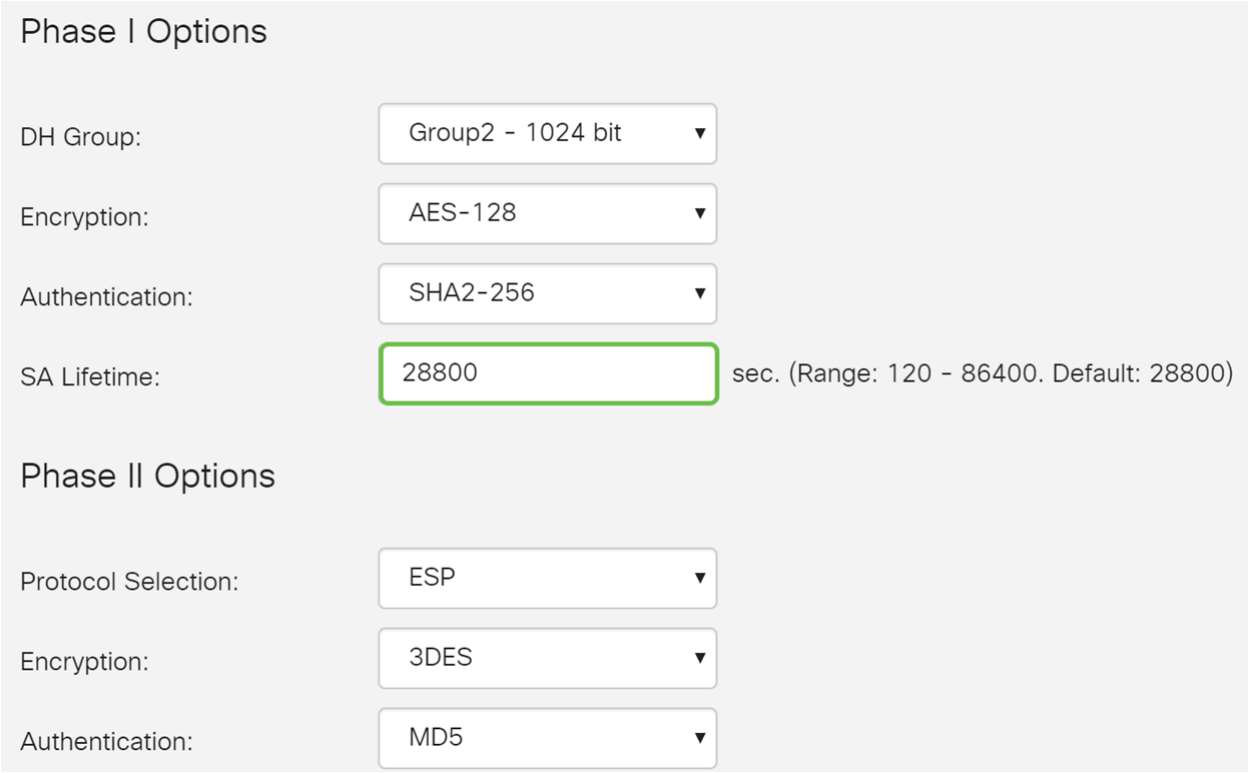
Für dieses Beispiel wurde **SHA2-256** ausgewählt.



Schritt 9: Die *SA Lifetime (Sec)* gibt Ihnen an, wie lange eine IKE SA in dieser Phase aktiv ist. Wenn die SA nach der entsprechenden Lebensdauer abläuft, beginnt eine neue Aushandlung für eine neue. Der Bereich liegt zwischen 120 und 86400, der Standardwert ist 28800.

Wir verwenden den Standardwert von **28800** Sekunden als unsere SA Lifetime für Phase I.

Hinweis: Es wird empfohlen, dass die SA-Lebensdauer in Phase I länger als die Lebensdauer der Phase II SA ist. Wenn Sie Phase I kürzer als Phase II gestalten, müssen Sie den Tunnel häufiger hin und her verhandeln als den Datentunnel. Ein Datentunnel benötigt mehr Sicherheit. Daher sollte die Lebensdauer in Phase II kürzer sein als in Phase I.

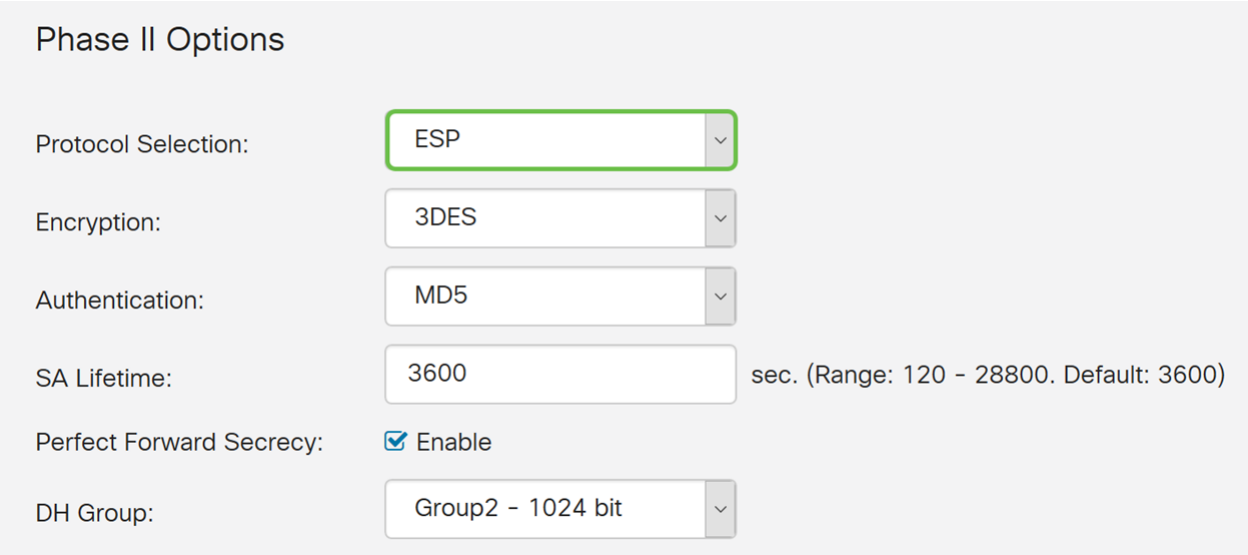


Schritt 10: In Phase II werden die Daten verschlüsselt, die an- und weitergeleitet werden. In den *Phase-2-Optionen* wählen Sie ein Protokoll aus der Dropdown-Liste aus:

- Encapsulating Security Payload (ESP) - Wählen Sie ESP für die Datenverschlüsselung aus, und geben Sie die Verschlüsselung ein.

- Authentication Header (AH) - Wählen Sie diese Option für Datenintegrität in Situationen aus, in denen Daten nicht geheim sind, d. h. nicht verschlüsselt sind, sondern authentifiziert werden müssen. Sie wird nur zur Validierung von Quelle und Ziel des Datenverkehrs verwendet.

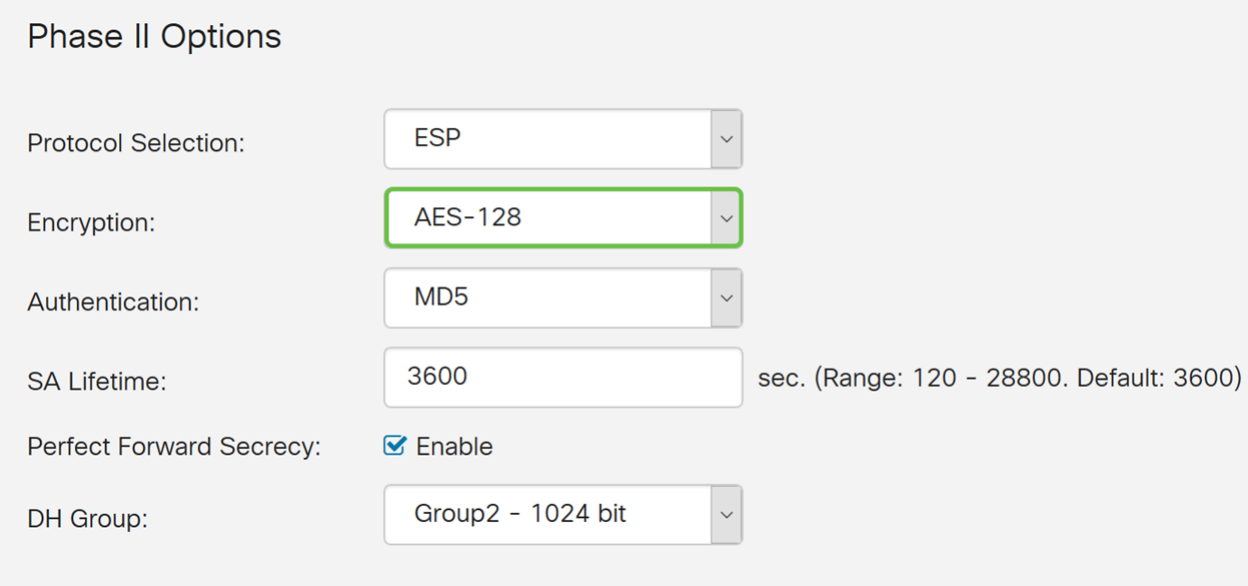
In diesem Beispiel wird **ESP** als *Protokollauswahl* verwendet.



Schritt 11: Wählen Sie eine Verschlüsselungsoption (**3DES**, **AES-128**, **AES-192** oder **AES-256**) aus der Dropdown-Liste aus. Diese Methode bestimmt den Algorithmus, der zum Verschlüsseln und Entschlüsseln von ESP-/ISAKMP-Paketen verwendet wird.

In diesem Beispiel verwenden wir **AES-128** als Verschlüsselungsoption.

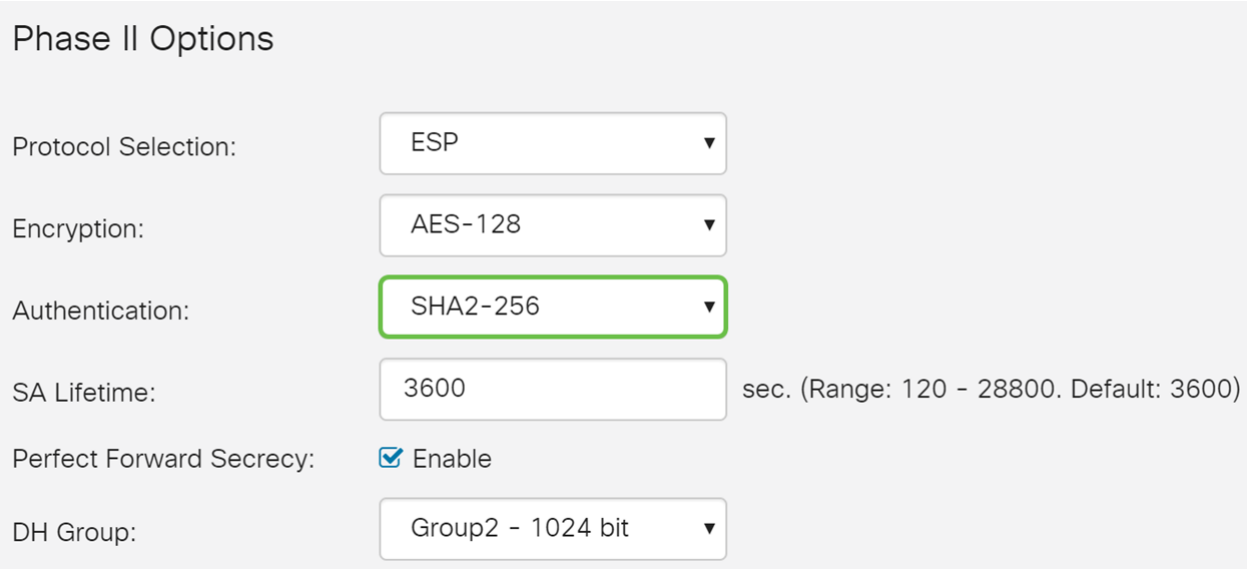
Hinweis: Hier einige weitere Ressourcen, die Ihnen helfen können: [Konfigurieren der Sicherheit für VPNs mit IPsec] und [Verschlüsselung der nächsten Generation].



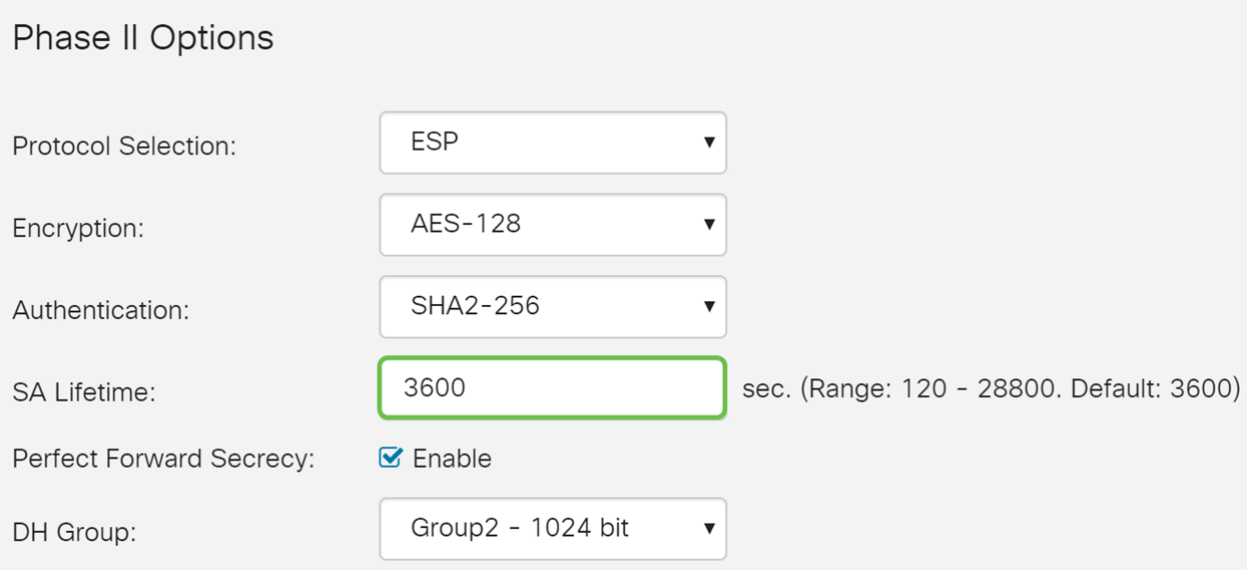
Schritt 12: Die Authentifizierungsmethode legt fest, wie die ESP-Headerpakete

(Encapsulating Security Payload Protocol) validiert werden. Wählen Sie eine Authentifizierung aus (**MD5, SHA1** oder **SHA2-256**).

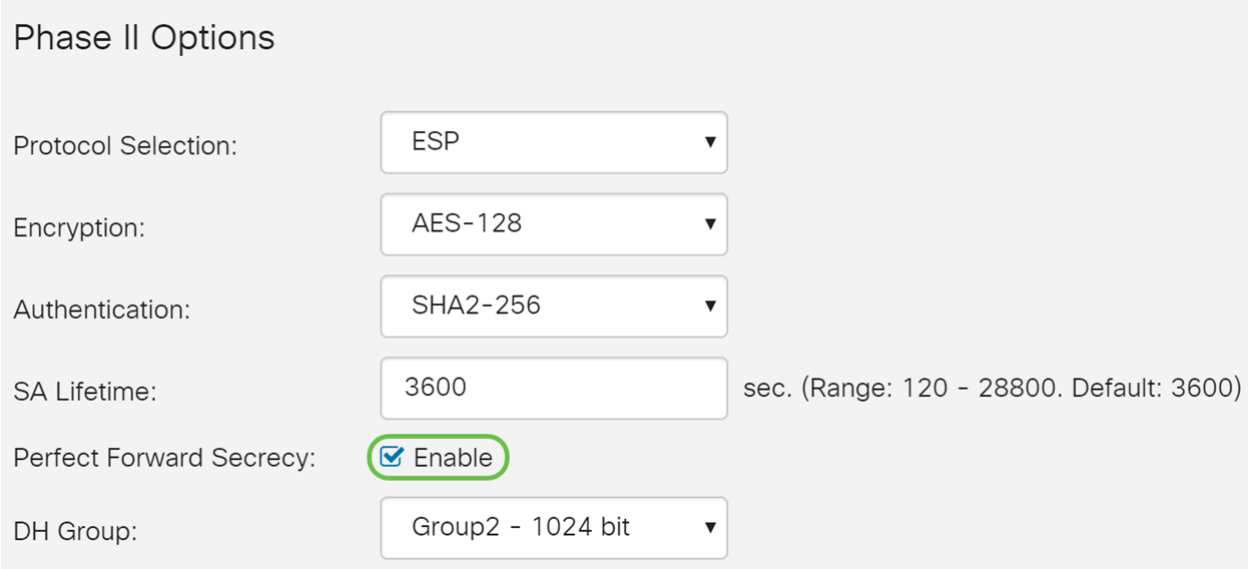
Für dieses Beispiel wurde **SHA2-256** ausgewählt.



Schritt 13: Geben Sie die Zeitdauer ein, die ein VPN-Tunnel (IPsec SA) in dieser Phase aktiv ist. Der Standardwert für Phase 2 ist 3600 Sekunden. Für diese Demonstration wird der Standardwert verwendet.

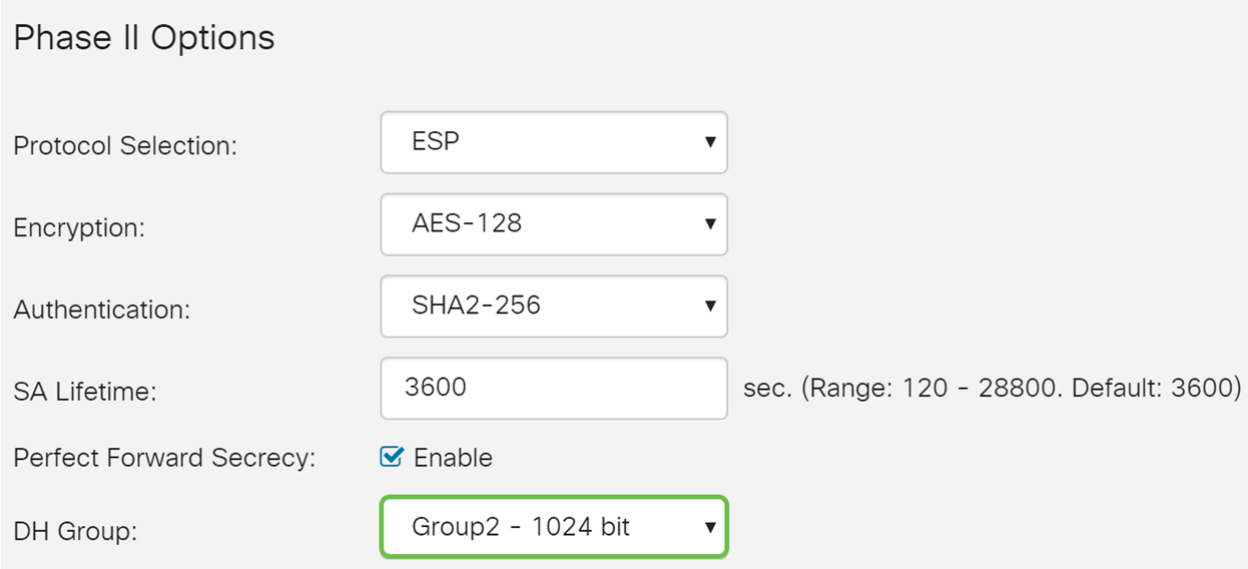


Schritt 14: Aktivieren Sie **Enable (Aktivieren)**, um das perfekte Vorwärtsgeheimnis zu aktivieren. Wenn Perfect Forward Secrecy (PFS) aktiviert ist, generiert die IKE Phase 2-Aushandlung neues Schlüsselmaterial für die Verschlüsselung und Authentifizierung des IPsec-Datenverkehrs. PFS wird verwendet, um die Sicherheit der über das Internet übertragenen Kommunikation mithilfe von Public-Key-Verschlüsselung zu verbessern. Dies wird empfohlen, wenn Ihr Gerät es unterstützt.



Schritt 15: Wählen Sie eine Diffie-Hellman (DH)-Gruppe aus. DH ist ein Schlüsselaustauschprotokoll mit zwei Gruppen unterschiedlicher Primkey-Längen, **Gruppe 2 - 1024 Bit** und **Gruppe 5 - 1536 Bit**. Für diese Demonstration wurde **Gruppe 2 - 1024 Bit** ausgewählt.

Hinweis: Wählen Sie Gruppe 2 aus, um die Geschwindigkeit zu erhöhen und die Sicherheit zu verringern. Wählen Sie Gruppe 5 aus, um die Geschwindigkeit zu verlangsamen und die Sicherheit zu erhöhen. Gruppe 2 ist standardmäßig ausgewählt.

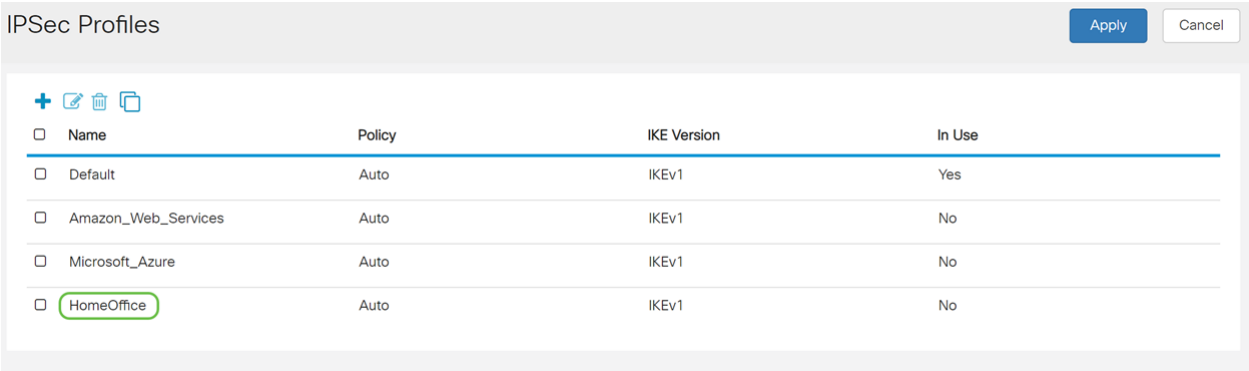


Schritt 16: Klicken Sie auf **Apply**, um ein neues IPsec-Profil hinzuzufügen.

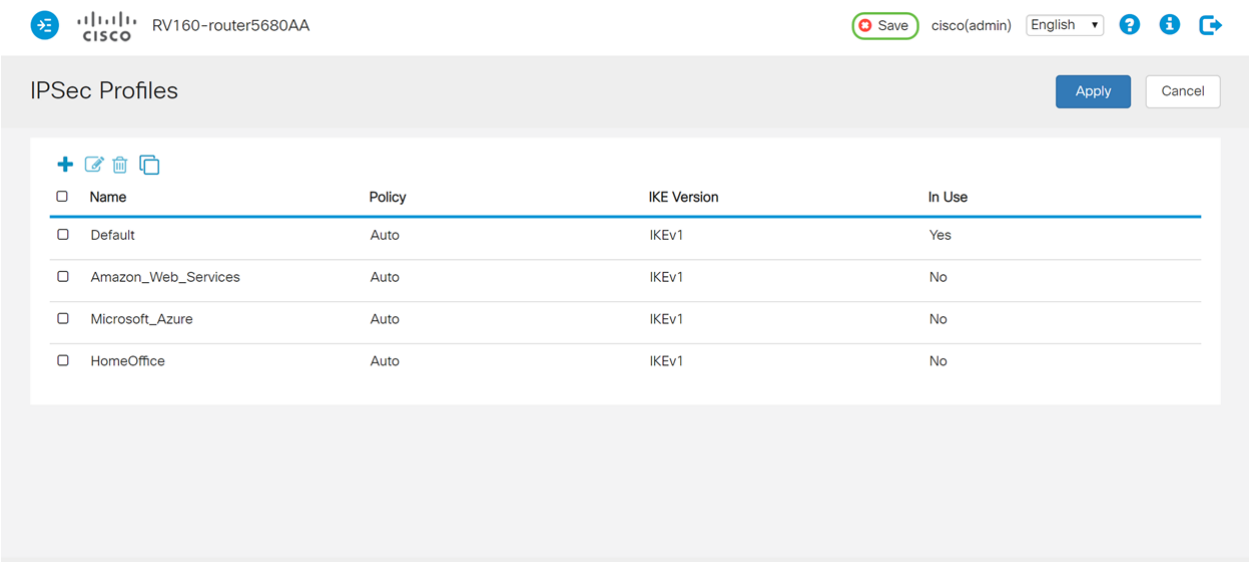
Schlussfolgerung

Sie sollten jetzt erfolgreich ein neues IPsec-Profil erstellt haben. Bitte fahren Sie unten fort, um zu überprüfen, ob Ihr IPsec-Profil hinzugefügt wurde. Sie können auch die Schritte ausführen, um die aktuelle Konfigurationsdatei in die Startkonfigurationsdatei zu kopieren, damit die gesamte Konfiguration zwischen Neustarts beibehalten wird.

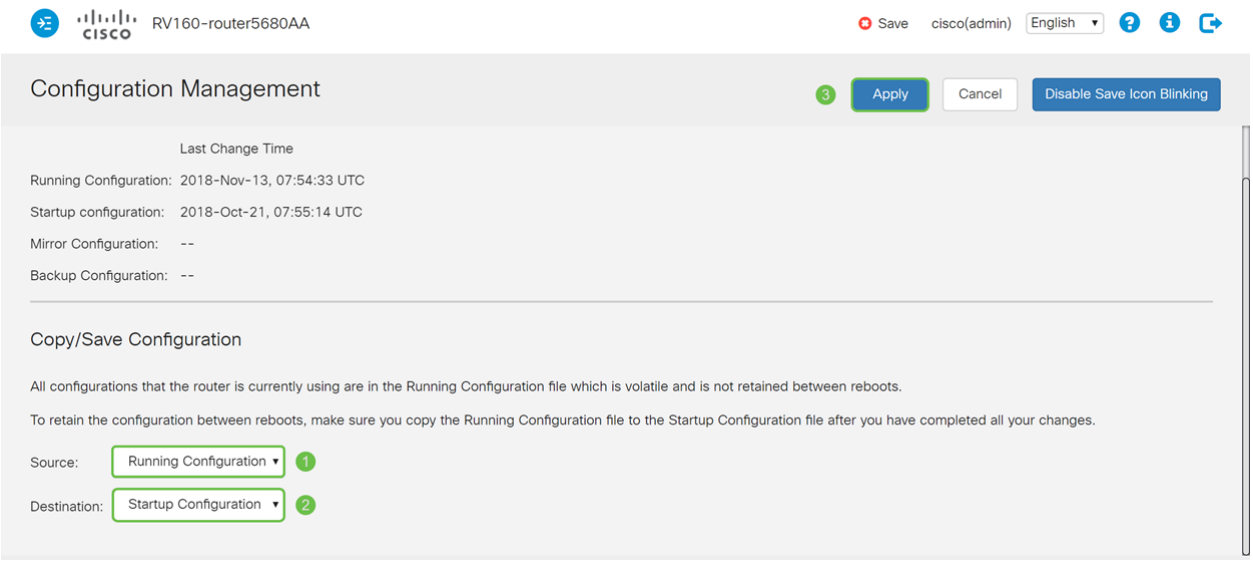
Schritt 1: Wenn Sie auf *Apply* klicken, sollte Ihr neues IPsec-Profil hinzugefügt werden.



Schritt 2: Klicken Sie oben auf der Seite auf die Schaltfläche **Speichern**, um zur *Konfigurationsverwaltung* zu navigieren, um die aktuelle Konfiguration in der Startkonfiguration zu speichern. Dadurch wird die Konfiguration zwischen Neustarts beibehalten.



Schritt 3: Vergewissern Sie sich im *Konfigurationsmanagement*, dass die *Quelle* die **Konfiguration ausführt** und das *Ziel* die **Startkonfiguration** ist. Drücken Sie anschließend **Apply**, um die aktuelle Konfiguration in der Startkonfiguration zu speichern. Alle Konfigurationen, die der Router derzeit verwendet, befinden sich in der Running Configuration-Datei, die flüchtig ist und zwischen Neustarts nicht beibehalten wird. Beim Kopieren der Running Configuration-Datei in die Startkonfigurationsdatei wird die gesamte Konfiguration zwischen Neustarts beibehalten.


RV160-router5680AA
Save
cisco(admin)
English
Configuration Management
3
Apply
Cancel
Disable Save Icon Blinking
Last Change Time
Running Configuration: 2018-Nov-13, 07:54:33 UTC
Startup configuration: 2018-Oct-21, 07:55:14 UTC
Mirror Configuration: --
Backup Configuration: --
Copy/Save Configuration
All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.
To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.
Source:
Running Configuration
1
Destination:
Startup Configuration
2