Konfigurieren von IKEv2 auf dem Router der Serie RV34x

Ziel

In diesem Dokument wird erläutert, wie Sie das IPsec-Profil mit IKEv2 auf Routern der Serie RV34x konfigurieren.

Einführung

Die Firmware-Version 1.0.02.16 für Router der Serie RV34x unterstützt jetzt Internet Key Exchange Version 2 (IKEv2) für Site-to-Site-VPN und Client-to-Site-VPN. IKE ist ein Hybridprotokoll, das den Oakley-Schlüsselaustausch und den Skeme-Schlüsselaustausch innerhalb des ISAKMP-Frameworks (Internet Security Association and Key Management Protocol) implementiert. IKE stellt die Authentifizierung der IPsec-Peers bereit, handelt IPsec-Schlüssel aus und handelt IPsec-Sicherheitszuordnungen aus.

IKEv2 verwendet weiterhin den UDP-Port 500, aber einige Änderungen sind zu beachten. Dead Peer Detection (DPD) wird anders verwaltet und ist jetzt integriert. Die Aushandlung von Security Association (SA)-Inhalten ist auf 4 Nachrichten beschränkt. Dieses neue Update unterstützt auch die Extensible Authentication Protocol (EAP)-Authentifizierung, die nun einen AAA-Server und einen Denial of Service-Schutz nutzen kann.

In der folgenden Tabelle werden die Unterschiede zwischen IKEv1 und IKEv2 genauer veranschaulicht.

IKEv1	IKEv2
Aushandlung in zwei Phasen SA (Hauptmodus vs. aggressiver Modus)	SA Single Phase Negotiation (vereinfacht)
	Unterstützung für lokale/Remote-Zertifikate
	Verbesserte Kollisionsbehandlung
	Verbesserte Neueingabemechanik
	Integrierte NAT-Traversal
	EAP-Unterstützung für AAA-Server

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 in einem Virtual Private Network (VPN) verwendet und auf der IP-Ebene implementiert, was dazu beiträgt, viele unsichere Anwendungen mit Sicherheit auszustatten. 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. Sie bietet auch 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. Ein IPsec-Profil ist die zentrale Konfiguration in IPsec, die die Algorithmen wie Verschlüsselung, Authentifizierung und DH-Gruppe (Diffie-Hellman) für Phase-I- und II-Aushandlung im automatischen Modus sowie im manuellen Keying-Modus definiert. In Phase I werden die vorinstallierten Schlüssel zur Erstellung einer sicheren authentifizierten Kommunikation eingerichtet. In Phase II wird der Datenverkehr verschlüsselt. Sie können die meisten IPsec-Parameter konfigurieren, z. B. Protocol (Encapsulation Security Payload (ESP)), Authentication Header (AH), Mode (Tunnel, Transport), Algorithmen (Verschlüsselung, Integrität, Diffie-Hellman), Perfect Forward Secrecy (PFS), SA-Lebensdauer und Key Management Protocol (Internet Key Exchange (IKE) - IKEv1 und IKEv2).

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

Beachten Sie, dass der Remote-Router beim Konfigurieren von Site-to-Site-VPN dieselbe IPsec-Profilkonfiguration benötigt wie der lokale Router.

Nachfolgend finden Sie eine Tabelle der Konfiguration für den lokalen Router und den Remote-Router. In diesem Dokument wird der lokale Router mithilfe von Router A konfiguriert.

Felder	Lokaler Router (Router A)	Remote-Router (Router B)
Profilname	HomeOffice	Außenstelle
Keying Mode	Automatisch	Automatisch
IKE-Version	IKEv2	IKEv2
Phase I - Optionen	**Phase I - Optionen**	**Phase I - Optionen**
DH-Gruppe	Gruppe 2 - 1024 Bit	Gruppe 2 - 1024 Bit
Verschlüsselung	AES-192	AES-192
Authentifizierung	SHA2-256	SHA2-256
SA-Lebensdauer	28800	28800
Phase II-Optionen	**Phase II-Optionen**	**Phase II-Optionen**
Protokollauswahl	ESP	ESP
Verschlüsselung	AES-192	AES-192
Authentifizierung	SHA2-256	SHA2-256
SA-Lebensdauer	3600	3600
Perfekte Rufweiterleitung	Aktiviert	Aktiviert
DH-Gruppe	Gruppe 2 - 1024 Bit	Gruppe 2 - 1024 Bit

Klicken Sie auf den folgenden Link, um zu erfahren, wie Sie das Site-to-Site-VPN auf dem RV34x konfigurieren: Konfigurieren des Site-to-Site-VPN auf dem RV34x.

Anwendbare Geräte

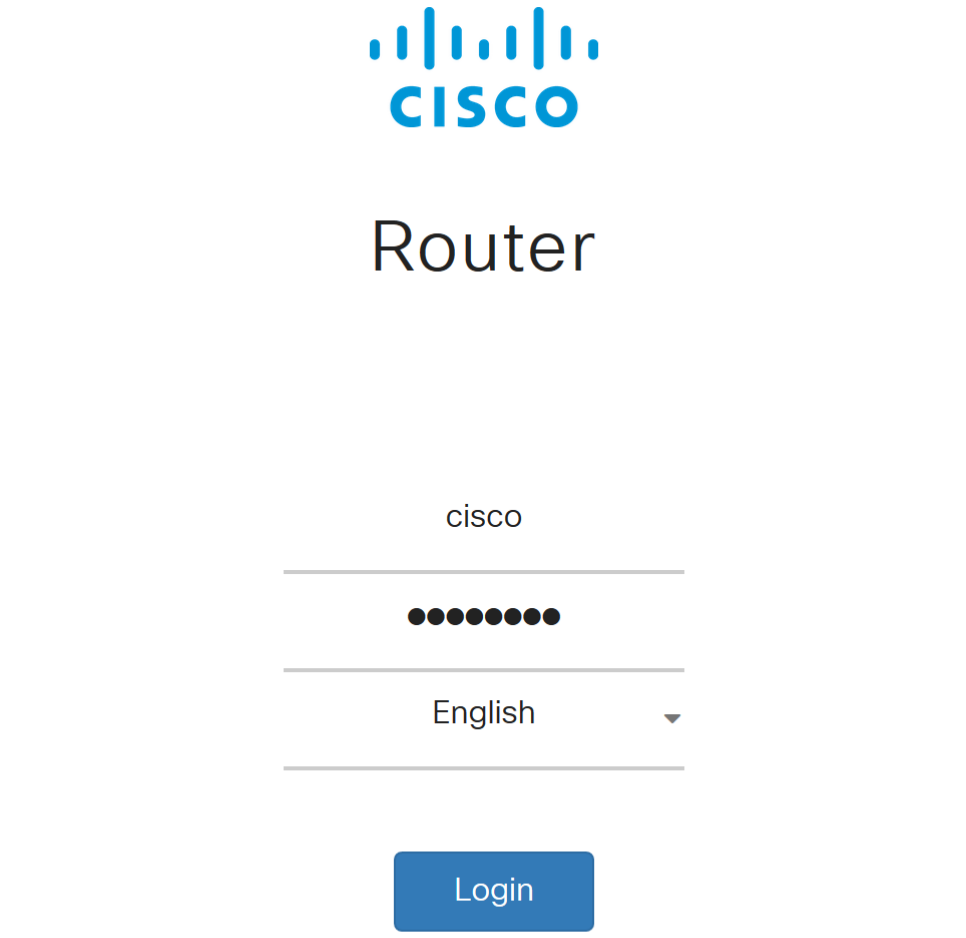
- RV34x

Softwareversion

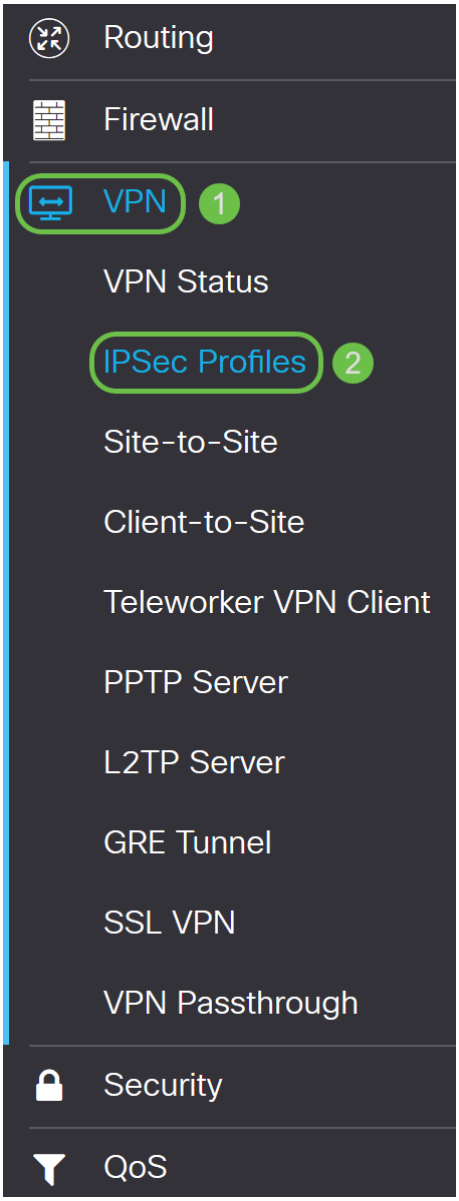
- 1.0.02.16

Konfigurieren des IPsec-Profils mit IKEv2

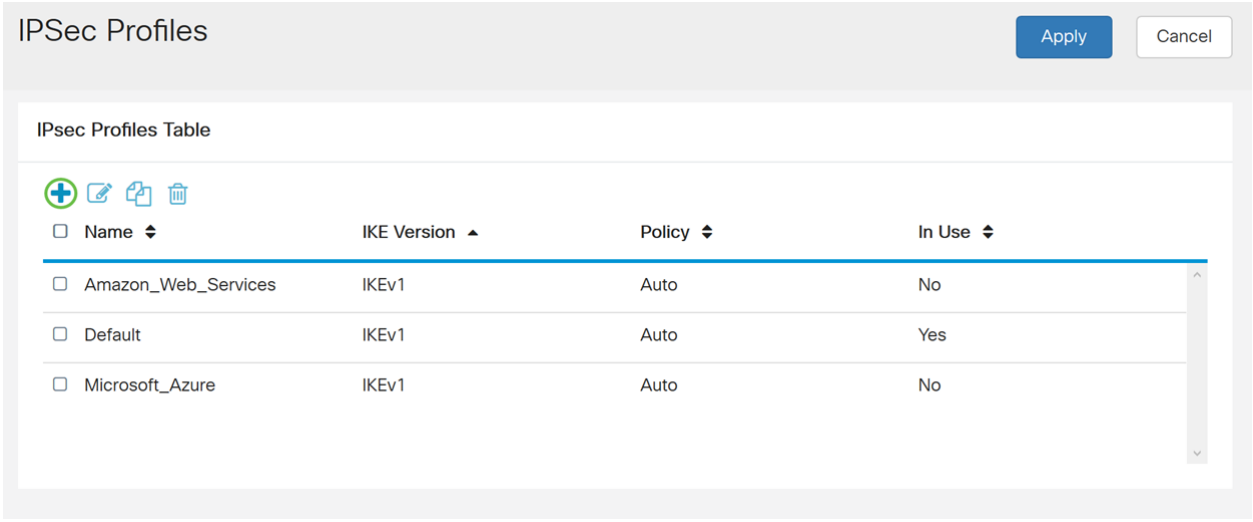
Schritt 1: Melden Sie sich auf der Webkonfigurationsseite Ihres lokalen Routers (Router A) an.



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



Schritt 3: Klicken Sie in der Tabelle *IPSec-Profile* auf **Hinzufügen,** um ein neues IPsec-Profil zu erstellen. Es gibt auch Optionen zum Bearbeiten, Löschen oder Klonen eines Profils. Durch das Klonen eines Profils können Sie schnell ein Profil duplizieren, das bereits in der *IPsec-Profiltabelle* vorhanden ist. Wenn Sie jemals mehrere Profile mit derselben Konfiguration erstellen müssen, können Sie durch das Klonen Zeit sparen.

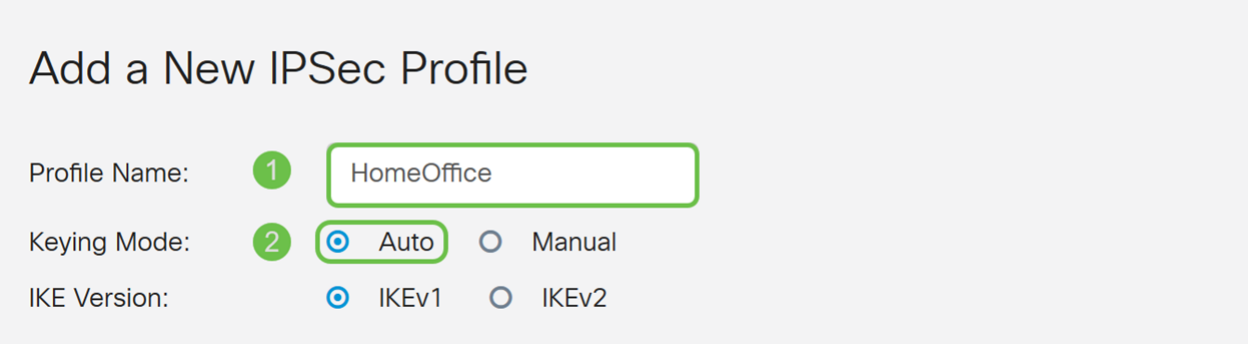


Schritt 4: Geben Sie einen Profilnamen ein, und wählen Sie den Keying-Modus (Automatisch oder

Manuell) aus. Der Profilname muss nicht mit dem anderen Router übereinstimmen, aber der Keying-Modus muss übereinstimmen.

HomeOffice wird als *Profilname* eingegeben.

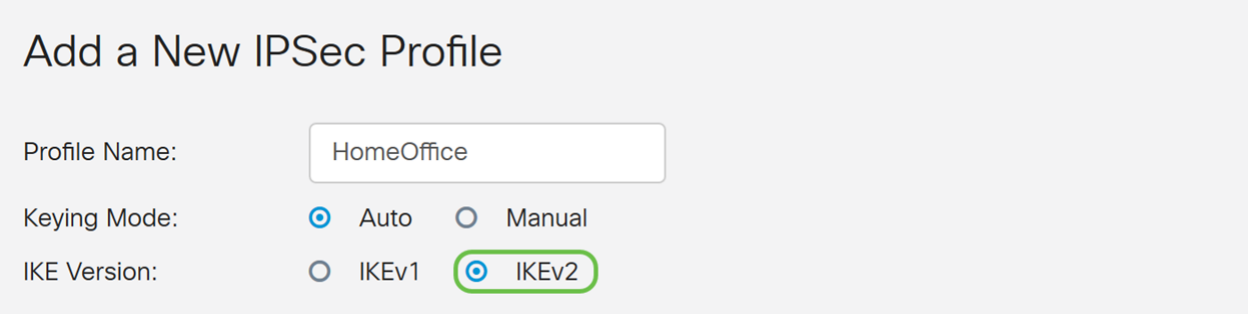
Auto (Automatisch) ist für den *Keying Mode* ausgewählt.



Schritt 5: Wählen Sie **IKEv1** oder **IKEv2** als *IKE-Version aus*. IKE ist ein Hybridprotokoll, das den Oakley-Schlüsselaustausch und den Skeme-Schlüsselaustausch innerhalb des ISAKMP-Frameworks implementiert. Oakley und Skeme legen beide fest, wie authentifiziertes Keying-Material abgeleitet werden soll. Skeme beinhaltet jedoch auch eine schnelle Schlüsselerfrischung. IKEv2 ist effizienter, da weniger Pakete für den Schlüsselaustausch erforderlich sind und mehr Authentifizierungsoptionen unterstützt werden, während IKEv1 nur über gemeinsam genutzten Schlüssel und zertifikatbasierte Authentifizierung verfügt.

In diesem Beispiel wurde **IKEv2** als unsere IKE-Version ausgewählt.

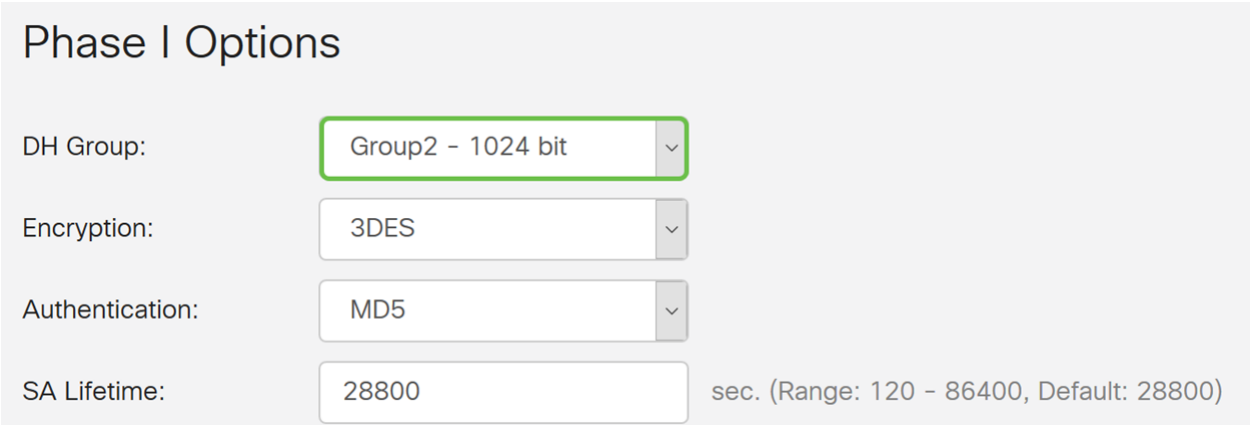
Hinweis: Wenn Ihre Geräte IKEv2 unterstützen, wird die Verwendung von IKEv2 empfohlen. Wenn Ihre Geräte IKEv2 nicht unterstützen, verwenden Sie IKEv1.



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 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.

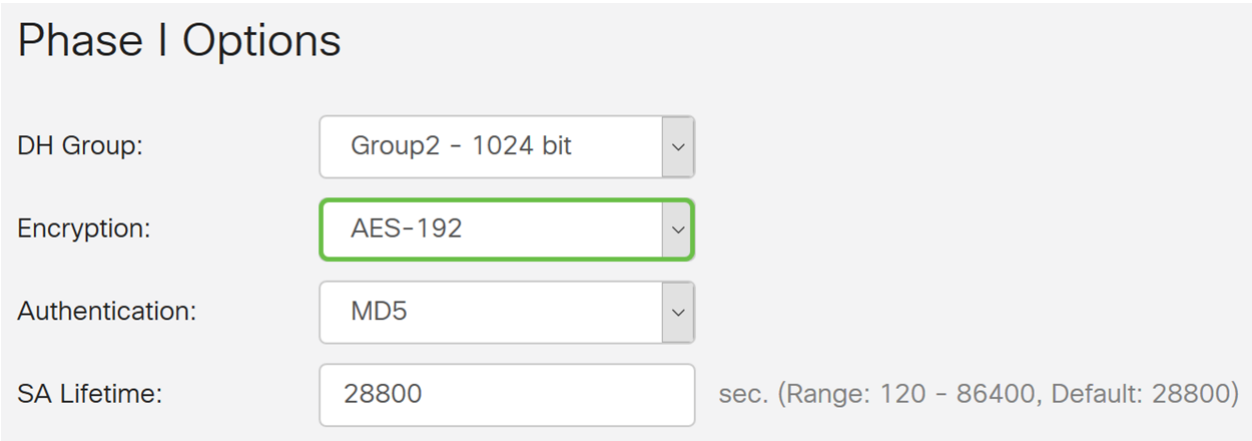
Hinweis: Wählen Sie Gruppe 2 aus, um die Geschwindigkeit zu erhöhen und die Sicherheit zu verringern. Wählen Sie Gruppe 5 aus, um die Geschwindigkeit zu verlangsamen und die Sicherheit zu erhöhen. Gruppe 2 ist standardmäßig ausgewählt.



Schritt 7: Wählen Sie eine Verschlüsselungsoption (**3DS**, **AES-128**, **AES-192** oder **AES-256**) aus der Dropdown-Liste aus. Diese Methode bestimmt den Algorithmus zur Verschlüsselung und Entschlüsselung von ESP-/ISAKMP-Paketen. Der Triple Data Encryption Standard (3DES) nutzt die DES-Verschlüsselung dreimal, ist aber jetzt ein Legacy-Algorithmus und sollte nur verwendet werden, wenn es keine anderen Alternativen gibt, da er immer noch eine marginale, aber akzeptable Sicherheitsstufe bietet. Benutzer sollten diese Daten nur dann verwenden, wenn sie für die Abwärtskompatibilität erforderlich sind, da sie für einige "Block-Kollision"-Angriffe anfällig sind. 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.

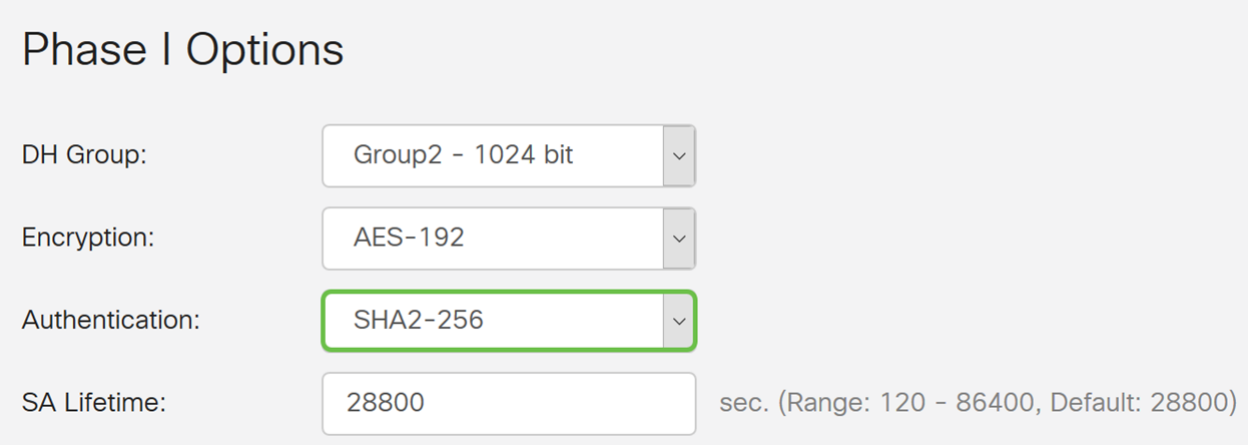
In diesem Beispiel haben wir **AES-192** als Verschlüsselungsoption ausgewählt.

Hinweis: Klicken Sie auf die Hyperlinks, um weitere Informationen zur Konfiguration der Sicherheit für VPNs mit IPsec oder Verschlüsselung der nächsten Generation zu erhalten.



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**).

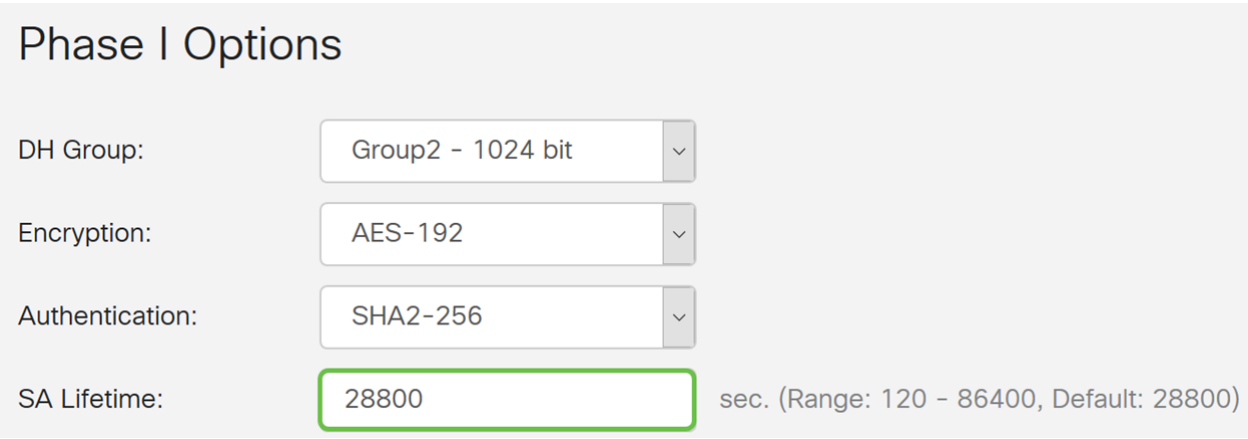
Für dieses Beispiel wurde **SHA2-256** ausgewählt.



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.

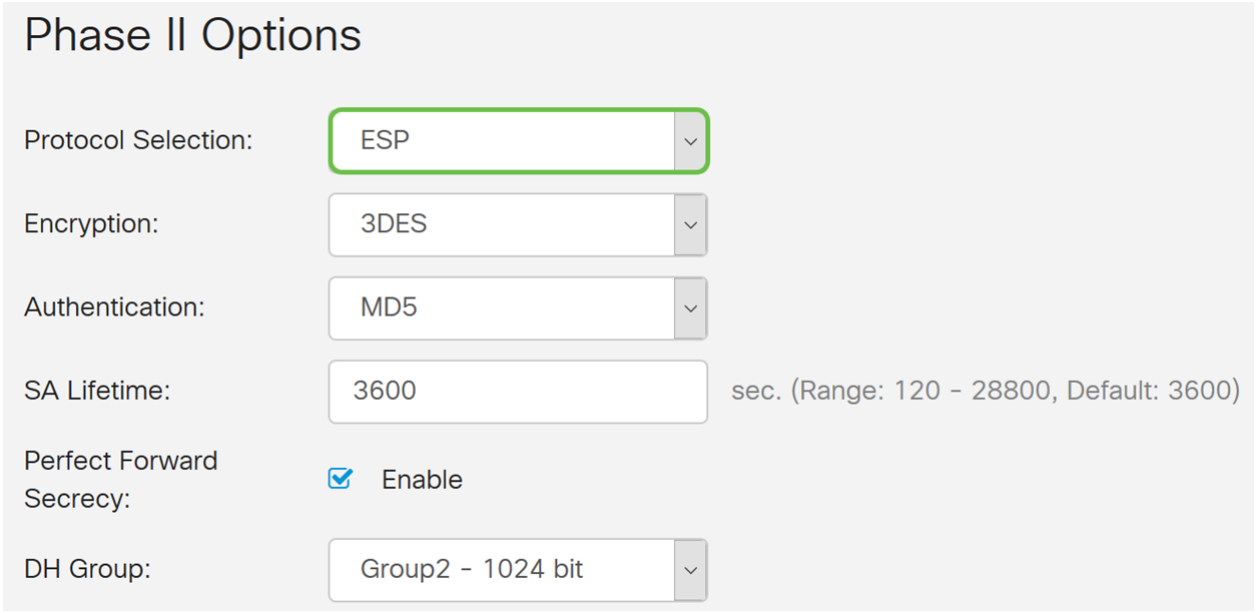


Schritt 10: In Phase II werden die Daten verschlüsselt, die an- und weitergeleitet werden. Wählen Sie in den *Phase-2-Optionen* ein Protokoll aus der Dropdown-Liste aus:

- 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.

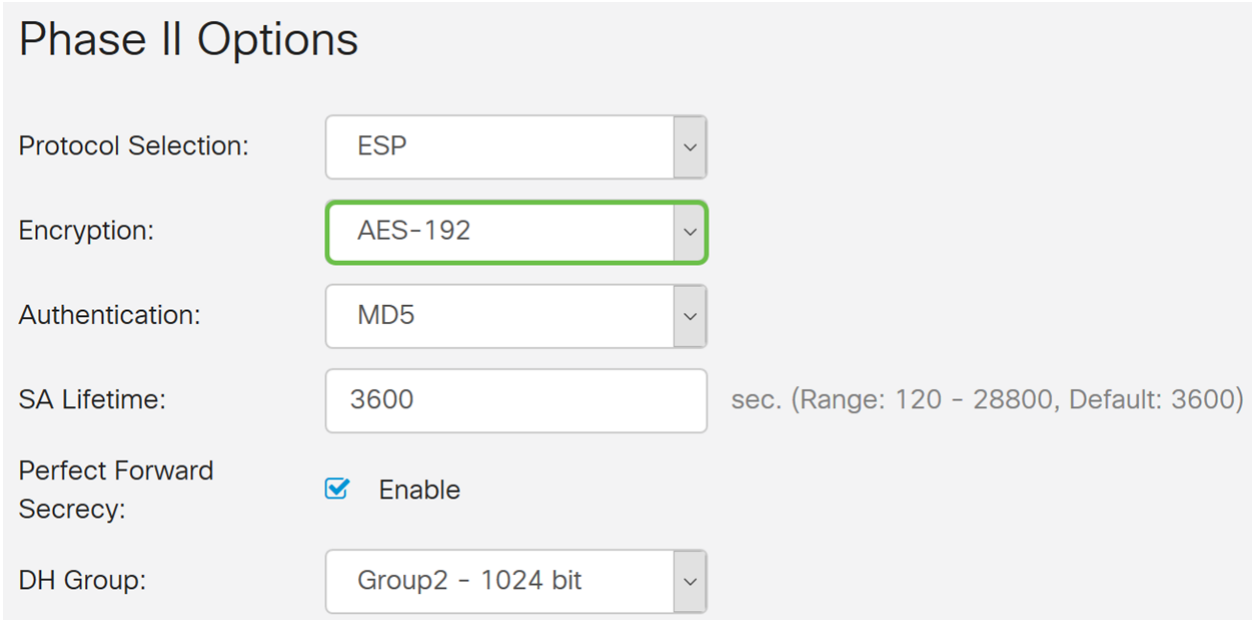
In diesem Beispiel wird **ESP** als *Protokollauswahl* verwendet.



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.

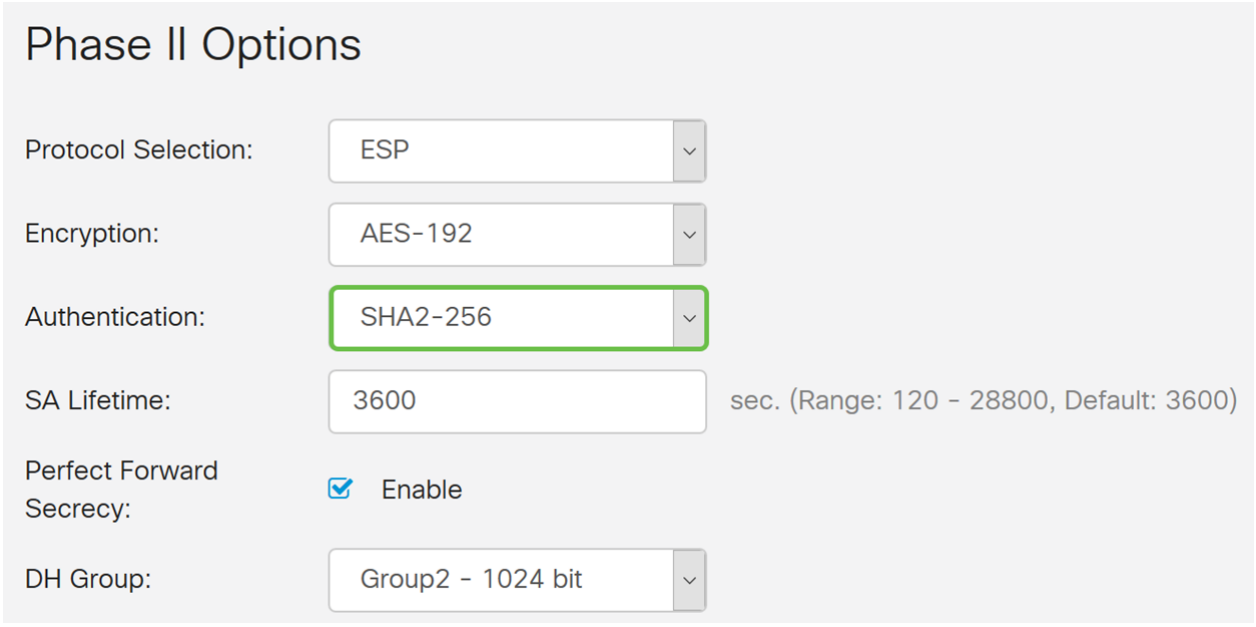
In diesem Beispiel verwenden wir **AES-192** als Verschlüsselungsoption.

Hinweis: Klicken Sie auf die Hyperlinks, um weitere Informationen zur Konfiguration der Sicherheit für VPNs mit IPsec oder Verschlüsselung der nächsten Generation zu erhalten.

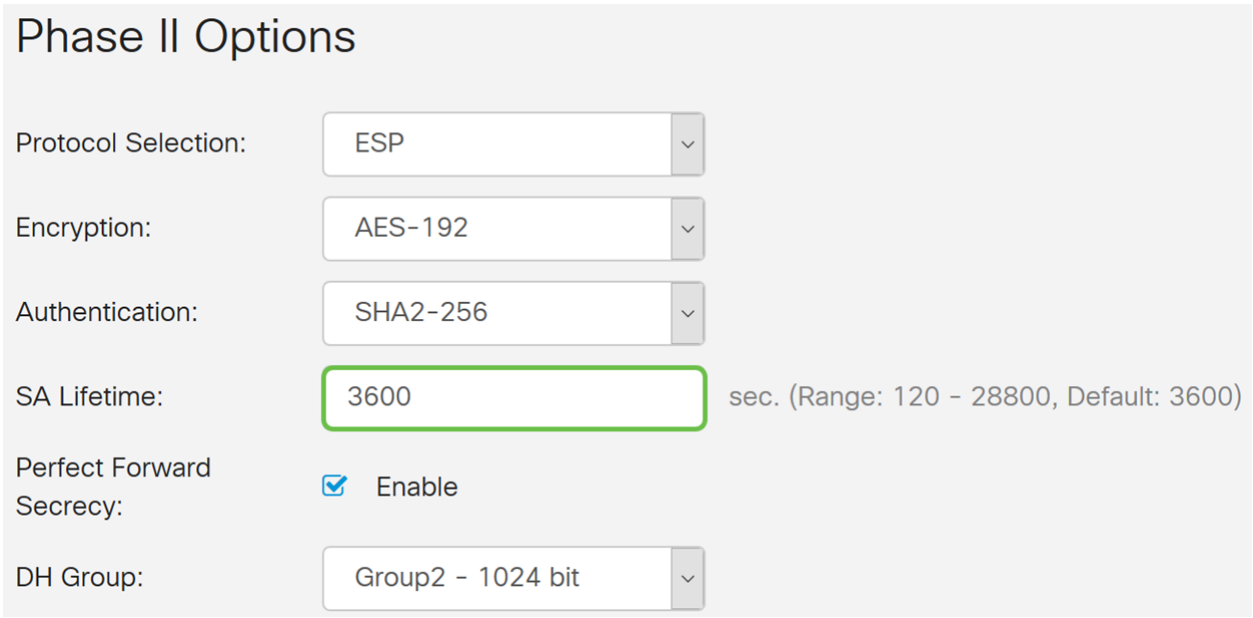


Schritt 12: Die Authentifizierungsmethode legt fest, wie die ESP-Headerpakete (Encapsulating Security Payload Protocol) validiert werden. Wählen Sie eine Authentifizierung aus (**MD5, SHA1** oder **SHA2-256**).

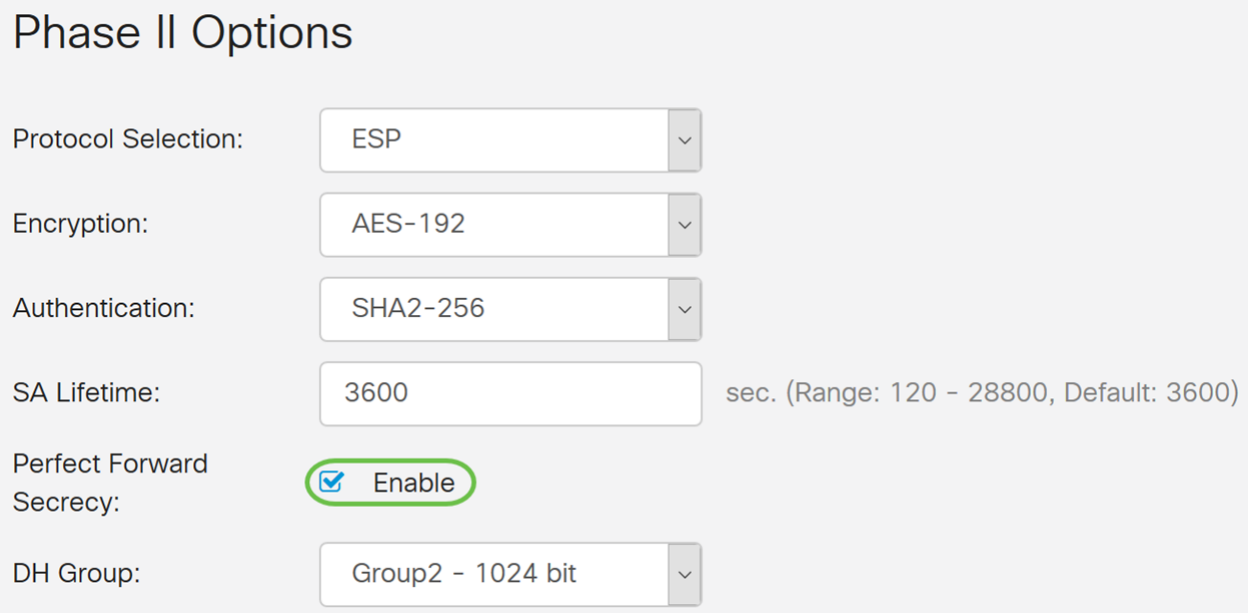
Für dieses Beispiel wurde **SHA2-256** ausgewählt.



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.

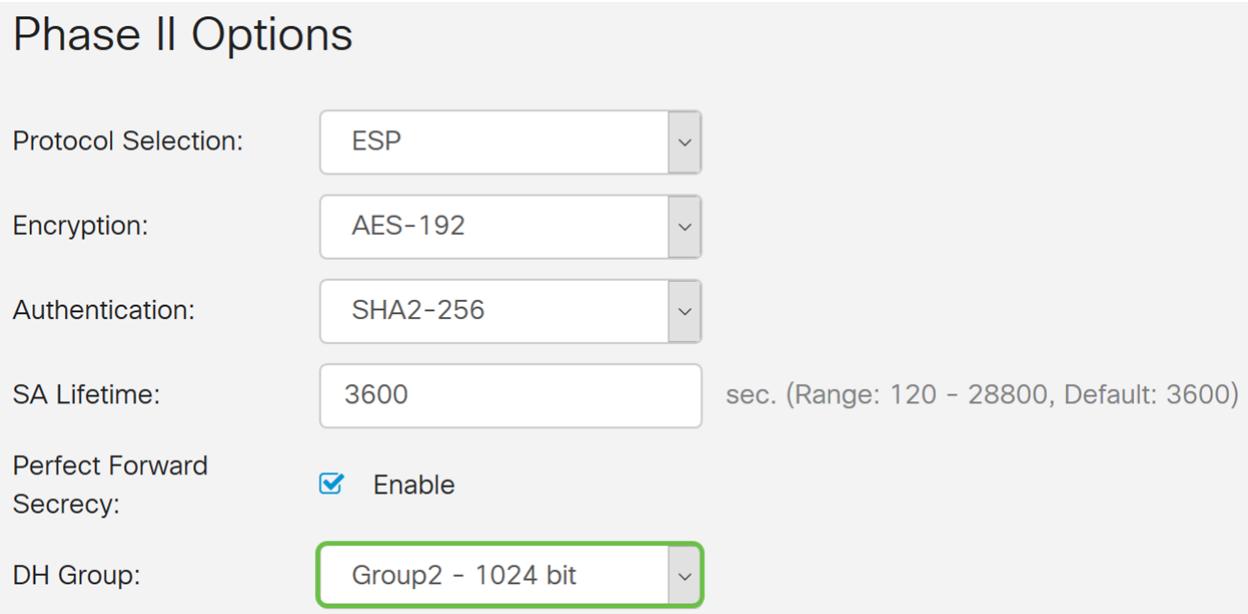


Schritt 14: Aktivieren Sie **Enable (Aktivieren)**, um das perfekte Vorwärtsgeheimnis zu aktivieren. Wenn Perfect Forward Secrecy (PFS) aktiviert ist, generiert die IKE Phase 2-Aushandlung neues Schlüsselmaterial für die Verschlüsselung und Authentifizierung des IPsec-Datenverkehrs. PFS wird verwendet,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

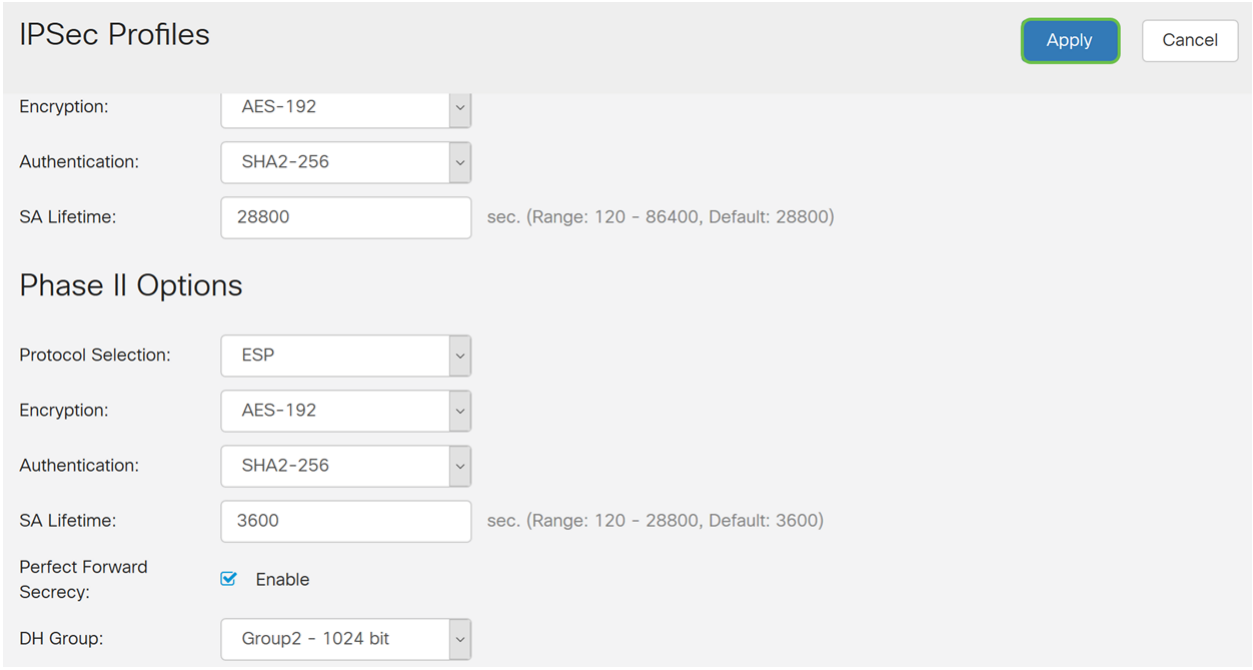


Schritt 15: Wählen Sie eine Diffie-Hellman (DH)-Gruppe aus. DH ist ein Schlüsselaustauschprotokoll mit zwei Gruppen unterschiedlicher Primkey-Längen, **Gruppe 2 - 1024 Bit** und **Gruppe 5 - 1536 Bit**. Für diese Demonstration wurde **Gruppe 2 - 1024 Bit** ausgewählt.

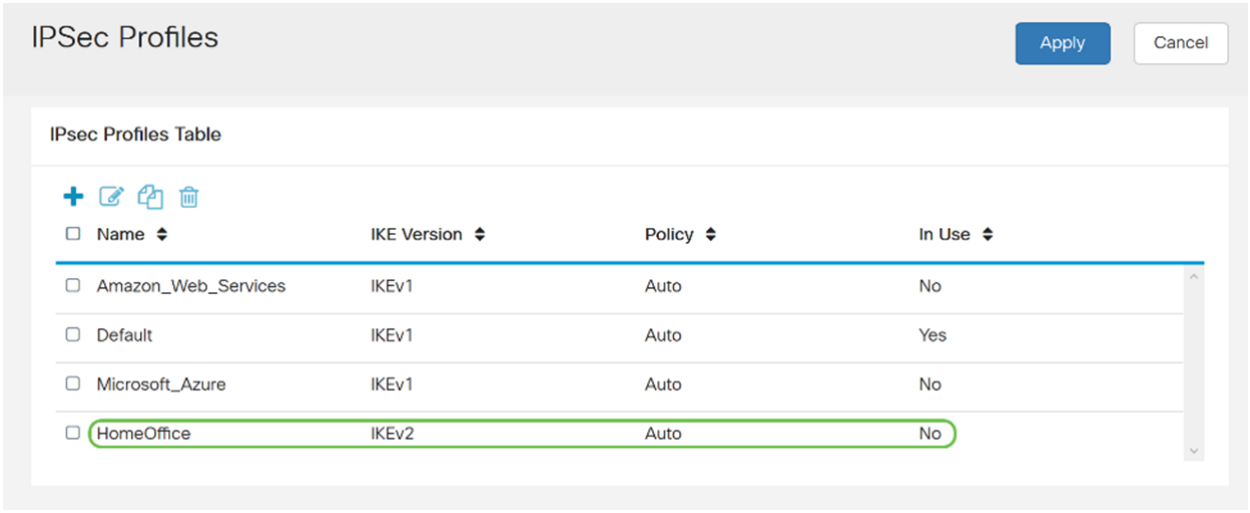
Hinweis: Wählen Sie Gruppe 2 aus, um die Geschwindigkeit zu erhöhen und die Sicherheit zu verringern. Wählen Sie Gruppe 5 aus, um die Geschwindigkeit zu verlangsamen und die Sicherheit zu erhöhen. Gruppe 2 ist standardmäßig ausgewählt.



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

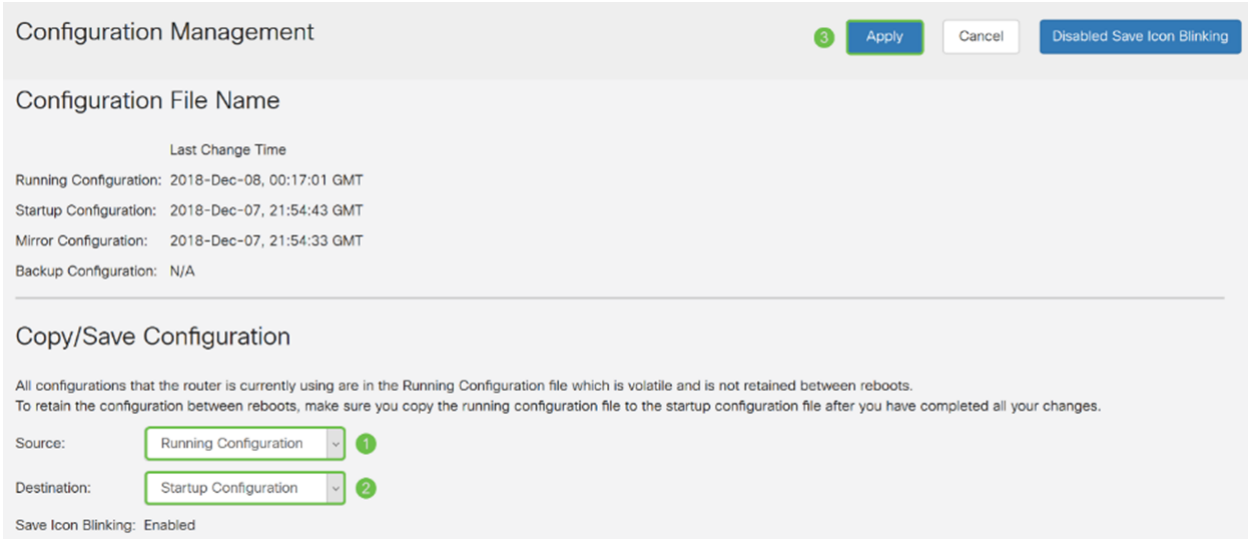


Schritt 17: Wenn Sie auf *Apply* klicken, sollte Ihr neues IPsec-Profil hinzugefügt werden.



Schritt 18: Klicken Sie oben auf der Seite auf das Symbol **Speichern**, um zur *Konfigurationsverwaltung* zu navigieren, um die aktuelle Konfiguration in der Startkonfiguration zu speichern. Dadurch wird die Konfiguration zwischen Neustarts beibehalten.

Schritt 19: 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 aktuellen Konfigurationsdatei in die Startkonfigurationsdatei wird die gesamte Konfiguration zwischen den Neustarts beibehalten.



Schritt 20: Befolgen Sie erneut alle Schritte, um Router B einzurichten.

Schlussfolgerung

Sie sollten jetzt erfolgreich ein neues IPsec-Profil mit IKEv2 als IKE-Version für beide Router erstellt haben. Sie können ein Site-to-Site-VPN konfigurieren.