

IPsec-profielen configureren (Auto Keying Mode) op de RV160 en RV260

Doel

Dit document zal aantonen hoe u een nieuw IPsec-profiel (Internet Protocol Security) kunt maken met behulp van de automatische modus voor het vastzetten van routers RV160 en RV260.

Inleiding

IPsec garandeert dat u beveiligde privé-communicatie via het internet hebt. Het geeft twee of meer hosts privacy, integriteit en authenticiteit voor het verzenden van gevoelige informatie via het internet. IPsec wordt algemeen gebruikt in Virtual Private Network (VPN) en wordt op de IP-laag geïmplementeerd en het gebruik ervan kan veel toepassingen ondersteunen die geen beveiliging bieden. Een VPN wordt gebruikt om een veilig communicatiemechanisme voor gevoelige gegevens en IP-informatie te bieden die door een onveilig netwerk zoals het internet wordt doorgegeven. Het biedt een flexibele oplossing voor gebruikers op afstand en de organisatie om gevoelige informatie van andere partijen op hetzelfde netwerk te beschermen.

Om de twee extremen van een VPN-tunnel te kunnen versleutelen en opzetten, moeten ze het allebei eens worden over de methoden voor encryptie, decryptie en authenticatie. IPsec-profiel is de centrale configuratie in IPsec die de algoritmen definieert zoals encryptie, verificatie en Diffie-Hellman (DH) groep voor Fase I- en II-onderhandeling in automatische modus evenals handmatige modus. Fase 1 stelt de vooraf gedeelde sleutels vast om een veilige geauthentiseerde communicatie te creëren. Fase 2 is waar het verkeer versleuteld wordt. U kunt de meeste IPsec-parameters configureren, zoals protocol, modus, algoritme, Perfect Forward Security (PFS), Security Association (SA) leven en beheerprotocol.

Merk op dat wanneer u Site-to-Site VPN configureren de externe router dezelfde profielinstellingen moet hebben als uw lokale router.

Aanvullende informatie over Cisco IPsec-technologie is te vinden in deze link: [Inleiding aan Cisco IPSec-technologie](#).

Als u IPsec-profiel en site-to-site VPN wilt configureren met de VPN-wizard, klikt u op de link: [VPN Setup-wizard configureren op RV160 en RV260](#).

U kunt Site-to-Site VPN configureren via het document: [Het configureren van site-to-site VPN op RV160 en RV260](#).

Toepasselijke apparaten

RV160

RV260

Softwareversie

·1.0.00.13

IPsec-profielen configureren

Stap 1. Meld u aan bij de webconfiguratie op uw router.



Router

cisco

●●●●●●●●

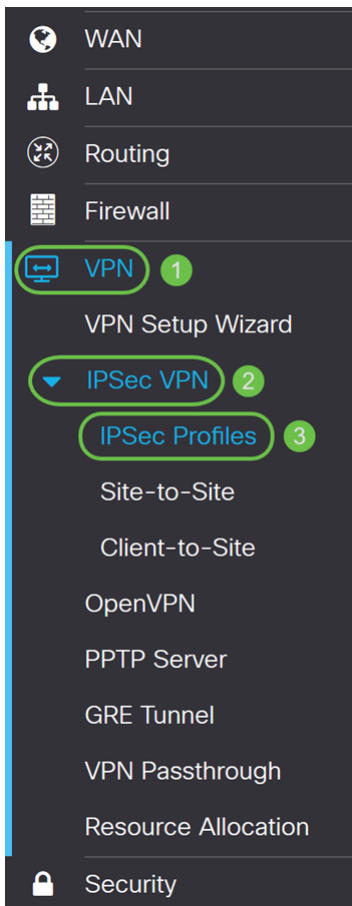
English ▼

Login

©2018 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Stap 2. Navigeer naar **VPN > IPsec VPN > IPsec VPN-profielen**.



Stap 3. In de tabel met *IPsec-profielen* klikt u op **Add** om een nieuw IPsec-profiel te maken. Er zijn ook opties om een profiel te bewerken, te verwijderen of af te sluiten.

IPsec Profiles				Apply	Cancel
<input type="checkbox"/> Name	Policy	IKE Version	In Use		
<input type="checkbox"/> Default	Auto	IKEv1	Yes		
<input type="checkbox"/> Amazon_Web_Services	Auto	IKEv1	No		
<input type="checkbox"/> Microsoft_Azure	Auto	IKEv1	No		

Stap 4. Voer een profielnaam in en selecteer de modus (Auto of Handmatig).

HomeOffice wordt ingevoerd als *profielnaam*.

Auto is geselecteerd voor *Toetsenmodus*.

Add/Edit a New IPsec Profile

Profile Name:

1

HomeOffice

Keying Mode:

2

Auto Manual

IKE Version:

IKEv1 IKEv2

Phase I Options

DH Group:

Group2 - 1024 bit

Encryption:

3DES

Authentication:

MD5

SA Lifetime:

28800

sec. (Range: 120 - 86400. Default: 28800)

Phase II Options

Stap 5. Kies *Internet Key Exchange versie 1 (IKEv1)* of *Internet Key Exchange versie 2 (IKEv2)* als uw IKE-versie. IKE is een hybride protocol ter uitvoering van de Oakley-uitwisseling en de Skeme-sleuteluitwisseling binnen het kader van Internet Security Association en Key Management Protocol (ISAKMP). Oakley en Skeme bepalen beiden hoe geauthentiseerd kookmateriaal moet worden afgeleid, maar Skeme omvat ook snelle basisverfrissing. IKE biedt verificatie van de IPsec-peers, onderhandelt over IPsec-toetsen en onderhandelt over IPsec-beveiligingsassociaties. IKEv2 is efficiënter omdat het minder pakket nodig heeft om de belangrijke uitwisseling te doen, ondersteunt meer authenticatieopties terwijl IKEv1 alleen gedeelde sleutel en op certificaat gebaseerde authenticatie doet. In dit voorbeeld is **IKEv1** geselecteerd als onze IKE-versie.

Opmerking: Als uw apparaat IKEv2 ondersteunt, wordt het aanbevolen IKEv2 te gebruiken. Als uw apparaten IKEv2 niet ondersteunen, gebruik dan IKEv1.

Add/Edit a New IPsec Profile

Profile Name:

Keying Mode: Auto Manual

IKE Version: IKEv1 IKEv2

Phase I Options

DH Group:

Encryption:

Authentication:

SA Lifetime: sec. (Range: 120 - 86400. Default: 28800)

Phase II Options

Stap 6. Fase I stelt de toetsen in die u wilt gebruiken om gegevens in fase II te versleutelen. Selecteer in *fase I* een groep Diffie-Hellman (DH). DH is een belangrijk uitwisselingsprotocol, met twee groepen van verschillende primaire sleutellengtes, **groep 2 - 1024 bit** en **groep 5 - 1536 bit**. We hebben **groep 2-1024-bit** geselecteerd voor deze demonstratie.

Opmerking: Voor snellere en lagere veiligheid, kies Groep 2. Voor langzamere snelheid en hogere veiligheid, kies Groep 5. Groep 2 wordt geselecteerd als standaard.

Phase I Options

DH Group:

Encryption:

Authentication:

SA Lifetime: sec. (Range: 120 - 86400. Default: 28800)

Phase II Options

Protocol Selection:

Encryption:

Authentication:

SA Lifetime: sec. (Range: 120 - 28800. Default: 3600)

Stap 7. Selecteer een coderingsoptie (**3DES**, **AES-128**, **AES-192** of **AES-256**) in de vervolgkeuzelijst. Deze methode bepaalt het algoritme dat wordt gebruikt om ESP/ISAKMP pakketten te versleutelen en te decrypteren. Triple Data Encryption Standard (3DES) gebruikt DES-encryptie drie keer, maar is nu een legacy-algoritme. Dit betekent dat het alleen gebruikt mag worden als er geen betere alternatieven zijn, aangezien het nog steeds een marginaal maar aanvaardbaar veiligheidsniveau biedt. Gebruikers mogen het alleen gebruiken als het vereist is voor achterwaartse compatibiliteit omdat het kwetsbaar is voor een of andere "blokbotsing"-aanvallen. Het gebruik van 3DES wordt niet aanbevolen, omdat het niet veilig wordt geacht. Advanced Encryption Standard (AES) is een cryptografisch algoritme dat ontworpen is om veiliger te zijn dan DES. AES gebruikt een grotere key size die ervoor zorgt dat de enige bekende benadering om een bericht te decrypteren voor een indringer is om elke mogelijke sleutel te proberen. Het wordt aanbevolen AES te gebruiken als uw apparaat dit kan ondersteunen. In dit voorbeeld hebben we **AES-128** geselecteerd als onze encryptie optie.

Opmerking: Hier zijn een paar extra hulpmiddelen die kunnen helpen: [Beveiliging voor VPN's configureren met IPsec](#) en [encryptie van de volgende generatie](#).

The image shows a configuration interface for IPsec. It is divided into two sections: Phase I Options and Phase II Options. Each section contains several settings, most of which are dropdown menus and one is a text input field. The 'Encryption' dropdown in Phase I is highlighted with a green border.

Section	Setting	Value	Additional Info
Phase I Options	DH Group	Group2 - 1024 bit	
	Encryption	AES-128	
	Authentication	MD5	
	SA Lifetime	28800	sec. (Range: 120 - 86400. Default: 28800)
Phase II Options	Protocol Selection	ESP	
	Encryption	3DES	
	Authentication	MD5	
	SA Lifetime	3600	sec. (Range: 120 - 28800. Default: 3600)

Stap 8. De verificatiemethode bepaalt hoe de ESP-headerpakketten worden gevalideerd. Dit is het hashing algoritme dat gebruikt wordt in de authenticatie om ze te valideren... dat kant A en kant B echt zijn wie ze zijn. De MD5 is een one-way hashing algoritme dat een 128-bits vertering produceert en sneller is dan SHA1. SHA1 is een one-way hashing algoritme dat een 160-bits digest produceert terwijl SHA2-256 een 256-bits vertering produceert. SHA2-256 wordt aanbevolen omdat het veiliger is. Zorg ervoor dat beide uiteinden van de VPN-tunnel dezelfde authenticatiemethode gebruiken. Selecteer een verificatie (**MD5**, **SHA1** of **SHA2-256**).

SHA2-256 is voor dit voorbeeld geselecteerd.

Phase I Options

DH Group:

Group2 - 1024 bit ▼

Encryption:

AES-128 ▼

Authentication:

SHA2-256 ▼

SA Lifetime:

28800

sec. (Range: 120 - 86400. Default: 28800)

Phase II Options

Protocol Selection:

ESP ▼

Encryption:

3DES ▼

Authentication:

MD5 ▼

Stap 9. De *SA Lifetime (SEC)* vertelt u de hoeveelheid tijd die een IKE SA in deze fase actief is. Als de SA na de respectieve levensduur afloopt, begint er een nieuwe onderhandeling voor een nieuwe. Het bereik loopt van 120 tot 86400 en de standaard is 28800.

We gebruiken de standaardwaarde van **28800** seconden als onze SA-levensduur voor fase I.

Opmerking: Aanbevolen wordt dat uw SA-levensduur in fase I langer is dan uw fase II SA-levensduur. Als je fase I korter maakt dan fase II, dan moet je regelmatig opnieuw onderhandelen over de tunnel dan vaak in tegenstelling tot de datunnel. Gegevenstunnel is wat meer veiligheid nodig heeft, zodat het beter is om de levensduur in fase II korter te hebben dan fase I.

Phase I Options

DH Group:

Group2 - 1024 bit ▼

Encryption:

AES-128 ▼

Authentication:

SHA2-256 ▼

SA Lifetime:

28800

sec. (Range: 120 - 86400. Default: 28800)

Phase II Options

Protocol Selection:

ESP ▼

Encryption:

3DES ▼

Authentication:

MD5 ▼

Stap 10. Fase II is waar u de gegevens versleutelt die heen en weer worden doorgegeven. In de optie *Fase 2* selecteert u een protocol uit de vervolgkeuzelijst. De opties zijn:

Security payload (ESP) insluiten - selecteer ESP voor gegevenscodering en voer de encryptie in.

Verificatieheader (AH) - Selecteer dit voor gegevensintegriteit in situaties waar gegevens niet geheim zijn, d.w.z. dat de gegevens niet versleuteld maar echt moeten worden. Het wordt alleen gebruikt om de bron en bestemming van het verkeer te valideren.

In dit voorbeeld zullen we **ESP** gebruiken als *protocolselectie*.

Phase II Options

Protocol Selection:	<input type="text" value="ESP"/>	
Encryption:	<input type="text" value="3DES"/>	
Authentication:	<input type="text" value="MD5"/>	
SA Lifetime:	<input type="text" value="3600"/>	sec. (Range: 120 - 28800. Default: 3600)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	<input type="text" value="Group2 - 1024 bit"/>	

Stap 1. Selecteer een coderingsoptie (**3DES**, **AES-128**, **AES-192** of **AES-256**) in de vervolgkeuzelijst. Deze methode bepaalt het algoritme dat wordt gebruikt om ESP/ISAKMP pakketten te versleutelen en te decrypteren.

In dit voorbeeld zullen we **AES-128** gebruiken als onze encryptie optie.

Opmerking: Hier zijn een paar extra hulpmiddelen die kunnen helpen: [Beveiliging voor VPN's configureren met IPsec](#) en [encryptie van de volgende generatie](#).

Phase II Options

Protocol Selection:	<input type="text" value="ESP"/>	
Encryption:	<input type="text" value="AES-128"/>	
Authentication:	<input type="text" value="MD5"/>	
SA Lifetime:	<input type="text" value="3600"/>	sec. (Range: 120 - 28800. Default: 3600)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	<input type="text" value="Group2 - 1024 bit"/>	

Stap 12. De verificatiemethode bepaalt hoe de ESP-headerpakketten (Encapsulation Security Payload Protocol) worden gevalideerd. Selecteer een verificatie (**MD5**, **SHA1** of

SHA2-256).

SHA2-256 is voor dit voorbeeld geselecteerd.

Phase II Options

Protocol Selection:	<input type="text" value="ESP"/>	
Encryption:	<input type="text" value="AES-128"/>	
Authentication:	<input type="text" value="SHA2-256"/>	
SA Lifetime:	<input type="text" value="3600"/>	sec. (Range: 120 - 28800. Default: 3600)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	<input type="text" value="Group2 - 1024 bit"/>	

Stap 13. Voer de hoeveelheid tijd in dat een VPN-tunnel (IPsec SA) in deze fase actief is. De standaardwaarde voor fase 2 is 3600 seconden. We zullen de standaardwaarde voor deze demonstratie gebruiken.

Phase II Options

Protocol Selection:	<input type="text" value="ESP"/>	
Encryption:	<input type="text" value="AES-128"/>	
Authentication:	<input type="text" value="SHA2-256"/>	
SA Lifetime:	<input type="text" value="3600"/>	sec. (Range: 120 - 28800. Default: 3600)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	<input type="text" value="Group2 - 1024 bit"/>	

Stap 14. Controleer of u het perfecte termijgeheim kunt activeren. Wanneer Perfect Forward Security (PFS) is ingeschakeld, genereert IKE Fase 2-onderhandeling nieuw belangrijk materiaal voor IPsec-verkeersencryptie en -verificatie. PFS wordt gebruikt om de beveiliging van communicatie via het internet te verbeteren door middel van openbare sleutelcryptografie. Dit wordt aanbevolen als uw apparaat het ondersteunt.

Phase II Options

Protocol Selection:	ESP	▼
Encryption:	AES-128	▼
Authentication:	SHA2-256	▼
SA Lifetime:	3600	sec. (Range: 120 - 28800. Default: 3600)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	Group2 - 1024 bit	▼

Stap 15. Selecteer een Diffie-Hellman (DH) groep. DH is een belangrijk uitwisselingsprotocol, met twee groepen van verschillende primaire sleutellengtes, **groep 2 - 1024 bit** en **groep 5 - 1536 bit**. We hebben **groep 2-1024-bit** geselecteerd voor deze demonstratie.

Opmerking: Voor snellere en lagere veiligheid, kies Groep 2. Voor langzamere snelheid en hogere veiligheid, kies Groep 5. Groep 2 wordt door standaard geselecteerd.

Phase II Options

Protocol Selection:	ESP	▼
Encryption:	AES-128	▼
Authentication:	SHA2-256	▼
SA Lifetime:	3600	sec. (Range: 120 - 28800. Default: 3600)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	Group2 - 1024 bit	▼

Stap 16. Klik op **Toepassen** om een nieuw IPsec-profiel toe te voegen.

Add/Edit a New IPsec Profile

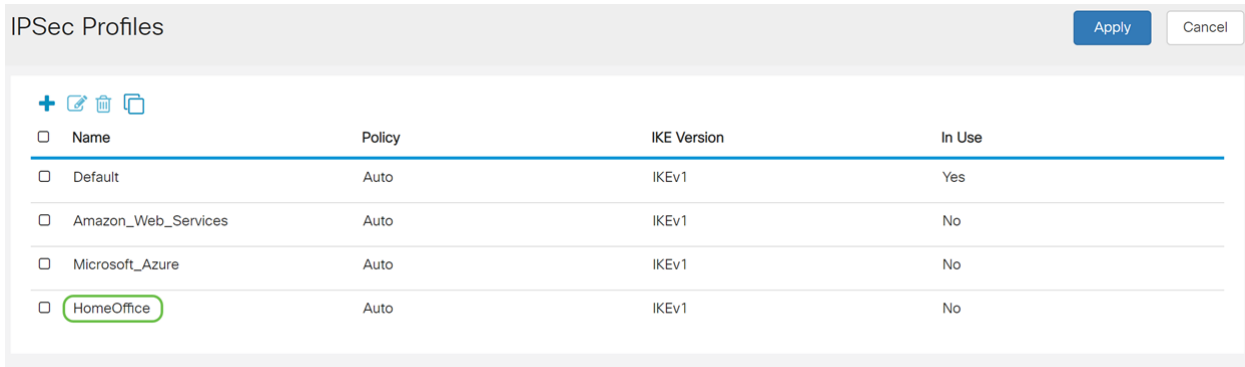
Apply

Cancel

Authentication:	SHA2-256	▼
SA Lifetime:	28800	sec. (Range: 120 - 86400. Default: 28800)
Phase II Options		
Protocol Selection:	ESP	▼
Encryption:	AES-128	▼
Authentication:	SHA2-256	▼
SA Lifetime:	3600	sec. (Range: 120 - 28800. Default: 3600)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	Group2 - 1024 bit	▼

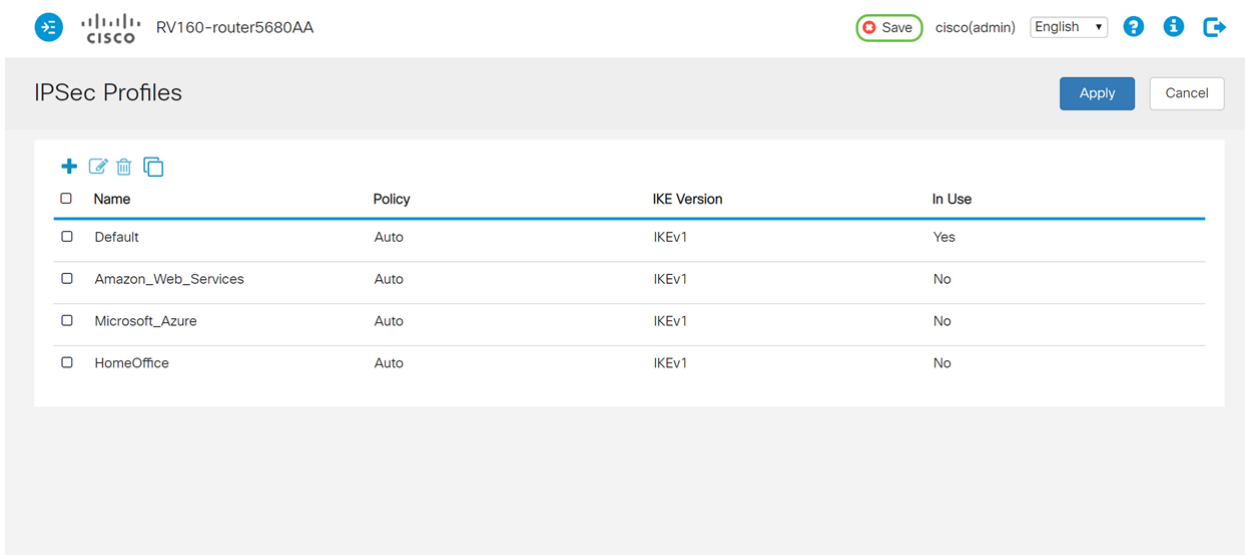
U hebt nu een nieuw IPsec-profiel gemaakt. Ga hieronder verder om te controleren of uw IPsec-profiel is toegevoegd. U kunt ook de stappen volgen om uw configuratie-bestand te kopiëren naar het opstartconfiguratiebestand, zodat alle configuratie tussen de herstart blijft behouden.

Stap 1. Nadat u op *Toepassen* hebt geklikt, moet uw nieuwe IPsec-profiel worden toegevoegd.



<input type="checkbox"/>	Name	Policy	IKE Version	In Use
<input type="checkbox"/>	Default	Auto	IKEv1	Yes
<input type="checkbox"/>	Amazon_Web_Services	Auto	IKEv1	No
<input type="checkbox"/>	Microsoft_Azure	Auto	IKEv1	No
<input type="checkbox"/>	HomeOffice	Auto	IKEv1	No

Stap 2. Klik boven op de pagina op de knop **Opslaan** om in het *Configuratiebeheer* te navigeren om de actieve configuratie in de opstartconfiguratie op te slaan. Dit is om de configuratie tussen de herstart te behouden.



RV160--router5680AA

Save cisco(admin) English ? i

<input type="checkbox"/>	Name	Policy	IKE Version	In Use
<input type="checkbox"/>	Default	Auto	IKEv1	Yes
<input type="checkbox"/>	Amazon_Web_Services	Auto	IKEv1	No
<input type="checkbox"/>	Microsoft_Azure	Auto	IKEv1	No
<input type="checkbox"/>	HomeOffice	Auto	IKEv1	No

Stap 3. *Controleer* in het *Configuratiebeheer* of de **bron de configuratie uitvoert** en de **bestemming de opstartconfiguratie is**. Druk vervolgens op **Toepassen** om de actieve configuratie op te slaan. Alle configuratie die de router momenteel gebruikt, bevindt zich in het configuratiebestand dat vluchtig is en niet tussen de herstart blijft behouden. Het kopiëren van het Configuration-bestand dat naar het opstartconfiguratiebestand wordt uitgevoerd, behoudt alle configuratie tussen de herstart.

Configuration Management

 **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: 

Destination: 