

Een site-to-site VPN-tunnel configureren tussen RV Series routers en ASA 5500 Series adaptieve security applicaties

Doel

Beveiliging is van essentieel belang om de intellectuele eigendom van een bedrijf te beschermen en tegelijkertijd de bedrijfscontinuïteit te waarborgen en de mogelijkheid te bieden om de werkplek van het bedrijf uit te breiden naar werknemers die altijd en overal toegang tot bedrijfsbronnen nodig hebben.

VPN-beveiligingsoplossingen worden steeds belangrijker voor kleine en middelgrote bedrijven. Een VPN is een privénetwerk dat is opgebouwd binnen een openbare netwerkinfrastructuur, zoals het wereldwijde internet. Een VPN breidt een privénetwerk uit tussen geografisch gescheiden kantoorlocaties. Het laat een server toe om gegevens over openbare netwerken te verzenden en te ontvangen aangezien zij een integraal deel van het privé netwerk met al functionaliteit waren. VPN's verhogen de beveiliging voor een gedistribueerde organisatie, waardoor het voor medewerkers gemakkelijker wordt om vanaf verschillende locaties te werken zonder het netwerk te verstoren. De redenen om VPN te gebruiken zijn de vereisten om een deel van de communicatie van een organisatie en de economie van de communicatie te "virtualiseren".

Er zijn verschillende VPN-topologieën: hub and spoke, point-to-point en Full mesh. Deze slimme tip dekt site-to-site (point-to-point) VPN, die een op internet gebaseerde infrastructuur biedt om netwerkresources uit te breiden naar externe kantoren, thuishandlers en zakelijke partnersites. Al het verkeer tussen sites wordt versleuteld met het IP Security (IPsec) protocol en netwerkfuncties zoals routing, Quality of Service (QoS) en multicast-ondersteuning zijn geïntegreerd.

De routers uit de Cisco RV-serie leveren robuuste en eenvoudig beheerde VPN-oplossingen aan prijsbewuste kleine bedrijven. Cisco ASA 5500 Series adaptieve security applicaties helpen organisaties om beveiliging in balans te brengen met productiviteit. Het combineert de meest geïmplementeerde stateful inspection firewall van de branche met uitgebreide next-generation netwerkbeveiligingsservices, waaronder: zichtbaarheid en granulaire controle van toepassingen en microtoepassingen, webbeveiliging, inbraakpreventiesystemen (IPS), zeer beveiligde externe toegang en andere.

Deze korte handleiding beschrijft een voorbeeld van het ontwerp voor het bouwen van een Site-to-Site IPsec VPN tussen routers uit de RV-serie en ASA 5500 Series adaptieve security applicaties en biedt configuratievoorbeelden.

Toepasselijke apparaten

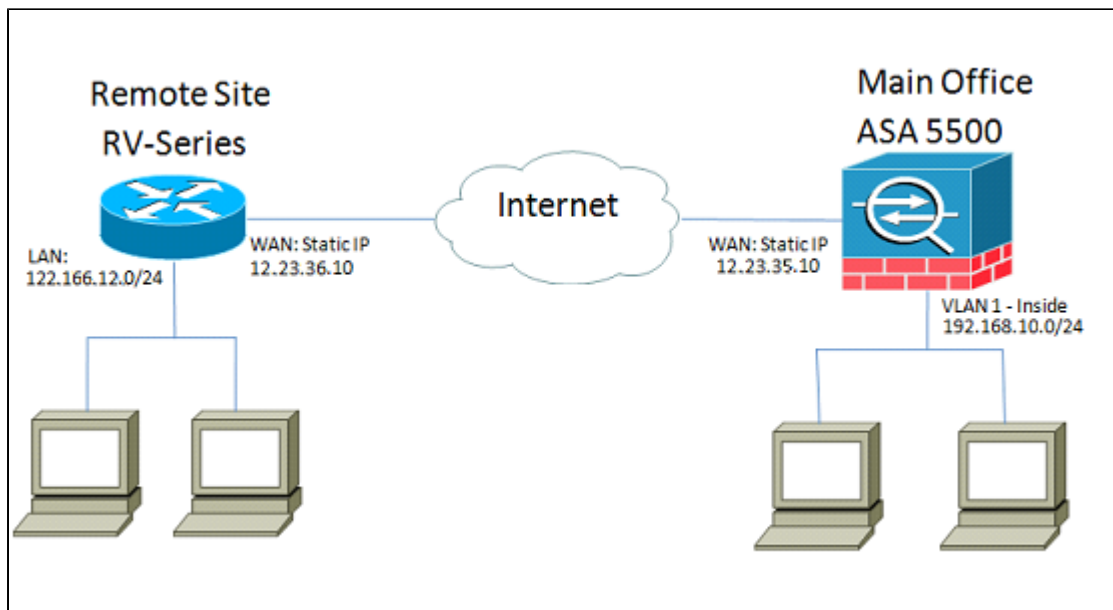
- Cisco RV0xx Series VPN-routers
- Adaptieve security applicaties van Cisco ASA 5500 Series

Softwareversie

- 4.2.2.08 [Cisco RV0xx Series VPN-routers]

Voorconfiguratie

Het volgende beeld toont een voorbeeldimplementatie van een Site-to-Site VPN-tunnel met behulp van een RV-Series router (Remote Site) en een ASA 5500 (Main Office).



Met deze configuratie kunnen een host in het netwerk van de externe site van 12.16.12.x en een host in VLAN 1 op het hoofdkantoor veilig met elkaar communiceren.

Belangrijkste kenmerken

Internet Key Exchange (IKE)

Internet Key Exchange (IKE) is het protocol waarmee een beveiligingsassociatie (SA) in de IPsec-protocolreeks wordt ingesteld. IKE bouwt voort op het Oakley protocol en Internet Security Association en Key Management Protocol (ISAKMP), en gebruikt een Diffie-Hellman sleuteluitwisseling om een gedeeld sessiegeheim op te zetten, waaruit cryptografische sleutels worden afgeleid. Een veilig beleid voor elke peer moet handmatig worden onderhouden.

Internet Protocol Security (IPSec)

IPsec gebruikt cryptografische beveiligingsservices om communicatie via IP-netwerken (Internet Protocol) te beschermen. IPsec ondersteunt peer-authenticatie op netwerkniveau, authenticatie van de herkomst van gegevens, gegevensintegriteit, vertrouwelijkheid van gegevens (encryptie) en bescherming tegen terugspelen. IPsec omvat veel componenttechnologieën en coderingsmethoden.

Toch kan de werking van IPsec worden opgesplitst in vijf hoofdstappen:

Stap 1. "Interessant verkeer" start het IPsec-proces - Traffic wordt als interessant beschouwd wanneer het IPsec-beveiligingsbeleid dat in de IPsec-peers is geconfigureerd, het IKE-proces start.

Stap 2. IKE fase 1 - IKE verifieert IPsec-peers en onderhandelt over IKE SA's™ tijdens deze fase, waarbij een beveiligd kanaal wordt opgezet voor onderhandelingen over IPsec SA's™ in fase 2.

Stap 3. IKE fase 2 - IKE onderhandelt over IPsec SA-parameters en stelt overeenkomende IPsec SA's™ in de peers.

Stap 4. Gegevensoverdracht - Gegevens worden tussen IPsec-peers overgedragen op basis van de IPsec-parameters en -toetsen die in de SA-database zijn opgeslagen.

Stap 5. IPsec-tunnelbeëindiging - IPsec SA's™ eindigen door verwijdering of door timing uit.

ISAKMP

Internet Security Association en Key Management Protocol (ISAKMP) worden gebruikt om te onderhandelen over de tunnel tussen de twee eindpunten. Het definieert de procedures voor authenticatie, communicatie en sleutelgeneratie en wordt door het IKE-protocol gebruikt om coderingssleutels uit te wisselen en de beveiligde verbinding tot stand te brengen.

Ontwerptips

VPN-topologie – Met een site-to-site VPN wordt een beveiligde IPsec-tunnel geconfigureerd tussen elke site en elke andere site. Een topologie van meerdere sites wordt meestal geïmplementeerd als een volledig netwerk van site-to-site VPN-tunnels (dat wil zeggen dat elke site tunnels heeft ingesteld voor elke andere site). Als er geen communicatie nodig is tussen externe kantoren, wordt een hub-spoke VPN-topologie gebruikt om het aantal VPN-tunnels te verminderen (dat wil zeggen dat elke site een VPN-tunnel maakt voor alleen het hoofdkantoor).

WAN IP-adressering en DNS – De VPN-tunnel moet worden opgezet tussen twee openbare IP-adressen. Als de WAN-routers statische IP-adressen van de Internet Service Provider (ISP) ontvangen, kan de VPN-tunnel direct worden geïmplementeerd met behulp van statische openbare IP-adressen. Nochtans, gebruiken de meeste kleine ondernemingen rendabele breedbanddiensten van Internet zoals DSL of kabelmodem, en ontvangen dynamische IP adressen van hun ISPs. In dergelijke gevallen kan DDNS worden gebruikt om het dynamische IP-adres toe te wijzen aan een volledig gekwalificeerde domeinnaam (FQDN).

LAN IP-adressering – Het IP-netwerkadres van elke locatie voor privénetwerken mag niet overlappen. Het standaard LAN IP-netwerkadres op elke externe locatie moet altijd worden gewijzigd.

VPN-verificatie – Het IKE-protocol wordt gebruikt om VPN-peers te verifiëren bij het instellen van een VPN-tunnel. Er bestaan verschillende IKE-verificatiemethoden en de vooraf gedeelde sleutel is de handigste methode. Cisco raadt het toepassen van een sterke vooraf gedeelde sleutel aan.

VPN-encryptie – Om de vertrouwelijkheid van gegevens die via VPN worden getransporteerd te garanderen, worden versleutelingsalgoritmen gebruikt om de payload van IP-pakketten te versleutelen. DES, 3DES, en AES zijn drie gemeenschappelijke encryptienormen. AES wordt als de veiligste beschouwd in vergelijking met DES en 3DES. Cisco raadt het toepassen van AES-128-bits of hogere codering ten zeerste aan (bijvoorbeeld AES-192 en AES-256). Hoe sterker het coderingsalgoritme echter is, des te meer verwerkingsbronnen het nodig heeft.

Configuratietips

Checklist voor de configuratie vooraf

Stap 1. Zorg ervoor dat de ASA en de RV router beide zijn aangesloten op de internetgateway (de ISP router of modem).

Stap 2. Zet de Cisco RV-router aan en sluit vervolgens interne pc's, servers en andere IP-apparaten aan op de LAN-switch of de switch-poorten op de RV-router.

Stap 3. Doe hetzelfde voor het netwerk achter de ASA. Stap 4. Zorg ervoor dat de LAN IP-netwerkadressen op elke locatie zijn geconfigureerd en niet hetzelfde zijn als subnetten. In dit voorbeeld, het belangrijkste bureau LAN gebruikt 192.168.10.0/24, and de verre plaats LAN gebruikt 122.166.12.0/24.

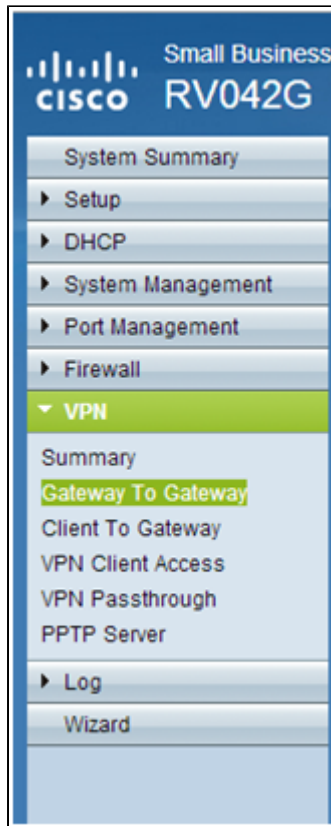
Stap 4. Zorg ervoor dat lokale pc's en servers met elkaar en met de router kunnen communiceren.

WAN-verbinding identificeren

U moet weten of uw ISP een dynamisch IP-adres doorgeeft of dat u een statisch IP-adres hebt ontvangen. Gewoonlijk zal ISP dynamische IP geven, maar u zult dit moeten bevestigen om de configuratie te voltooien.

De RV042G configureren op kantoor op afstand

Stap 1. Log in op de Web UI en ga naar de sectie **VPN > Gateway to Gateway**. Aangezien wij een LAN-to-LAN verbinding toevoegen, zullen de eindpunten de gateway van elk netwerk zijn.



Stap 2. De lokale en externe endpoints op de router configureren

a) Configureer de tunnelnaam om deze te identificeren uit andere tunnels die u mogelijk al geconfigureerd hebt.

The screenshot shows the 'Gateway To Gateway' configuration page in the Web UI. The title 'Gateway To Gateway' is at the top. Below it is the section 'Add a New Tunnel'. There are four configuration fields: 'Tunnel No.' with a value of '1', 'Tunnel Name' with a text input containing 'TestVPN', 'Interface' with a dropdown menu showing 'WAN1', and 'Enable' with a checked checkbox.

b) Local Group Setup configureert de lokale host(s) die in de VPN-tunnel toegestaan moeten worden. Zorg ervoor dat u het juiste Subnet en Masker voor het netwerk hebt dat u over de tunnel wilt worden toegestaan.

Local Group Setup	
Local Security Gateway Type :	IP Only
IP Address :	12.23.36.10
Local Security Group Type :	Subnet
IP Address :	122.166.12.0
Subnet Mask :	255.255.255.0

C) Remote Group Setup configureert het externe eindpunt en netwerkverkeer waar de router naar moet zoeken. Voer het statische IP van de externe gateway in om de verbinding in het veld IP-adres van de gateway tot stand te brengen. Voer vervolgens het toegestane subnetnummer in via VPN vanaf de externe site (het LAN van het hoofdkantoor).

Remote Group Setup	
Remote Security Gateway Type :	IP Only
IP Address :	12.23.35.10
Remote Security Group Type :	Subnet
IP Address :	192.168.10.0
Subnet Mask :	255.255.255.0

Stap 3. Configureer de tunnelinstellingen.

a) U zult een pre-gedeelde sleutel voor optimale resultaten willen vormen.

Fase 1 en Fase 2 zijn verschillende fasen van verificatie, fase 1 leidt tot de eerste tunnel en begint met onderhandeling, en fase 2 voltooit encryptie zeer belangrijke onderhandeling en beschermt de gegevenstransmissie zodra de tunnel wordt gevestigd.

b) De DH-groep komt overeen met de crypto isakmp-beleidsgroep voor de ASA, die u in de volgende sectie zult zien. Op de ASA is de standaardinstelling Group 2, en nieuwere versies van ASA-code vereisen ten minste DH Group 2. De inruil is dat het een hoger bit is en dus meer CPU-tijd vergt.

c) In fase 1 wordt het gebruikte coderingsalgoritme gedefinieerd. Het standaardmodel voor de RV-serie is DES, maar het standaardmodel voor de ASA is 3DES. Dit zijn echter oudere standaarden en zijn niet efficiënt in de huidige implementatie. AES-encryptie is sneller en veiliger, en Cisco raadt minimaal AES-128 (of eenvoudigweg AES) aan voor het beste resultaat.

d) Fase 1-verificatie verifieert de pakketintegriteit. De opties zijn SHA-1 en MD5, en één van beiden zou moeten werken aangezien zij gelijkaardige resultaten veroorzaken.

Fase 2-configuratie volgt dezelfde regels als fase 1. Bij het configureren van de IPSec-instellingen moet u er rekening mee houden dat de instellingen van de ASA moeten overeenkomen met die van de RV042G. Als er discrepanties zijn, kunnen de apparaten niet onderhandelen over de coderingssleutel en zal de verbinding mislukken.

Opmerking: Sla de instellingen op voordat u weggaat van deze pagina!

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : AES-128

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy : ☐

Phase 2 DH Group : Group 2 - 1024 bit

Phase 2 Encryption : AES-128

Phase 2 Authentication : SHA1

Phase 2 SA Life Time : 28800 seconds

Preshared Key : c12c0VPn3x4mPL3

De ASA 5500 configureren op het hoofdkantoor (CLI)

Opmerking: zorg ervoor dat u de opdracht "schrijf me" vaak gebruikt om te voorkomen dat configuraties verloren gaan. Ten eerste zijn hier de interfaces die we op de ASA hebben geconfigureerd. Uw instellingen kunnen afwijken. Controleer dus of de configuraties aangepast zijn.

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan10
 nameif outside
 security-level 0
 ip address 12.23.35.10 255.255.255.0
```

Stap 1. Encryptiebeheer configureren (ISAKMP)

De eerste stap is het opstellen van het ISAKMP-beleid, dat wordt gebruikt om te onderhandelen over de versleuteling van de tunnel. Deze configuratie moet op beide endpoints IDENTIEK zijn. Hier kunt u de coderingsinstellingen configureren zodat deze overeenkomen met fase 1 van de RV-configuratie.

```
ASA5505(config)# crypto isakmp policy 1
ASA5505(config-isakmp-policy)# authentication pre-share
ASA5505(config-isakmp-policy)# encryption aes
ASA5505(config-isakmp-policy)# hash sha
ASA5505(config-isakmp-policy)# group 2
ASA5505(config-isakmp-policy)# lifetime 28800
ASA5505(config-isakmp-policy)# exit
ASA5505(config)#
```

Stap 2. Verkeerselectie

Dit is hetzelfde als de Local and Remote Security Group op de RV042G. Op de ASA gebruiken we toegangslijsten om te definiëren wat het netwerk als "interessant verkeer" beschouwt om op de VPN toe te staan.

Configureer eerst de netwerkobjecten voor de externe site en de lokale site:

```
object network insidenet
  subnet 192.168.10.0 255.255.255.0
object network rsite
  subnet 122.166.12.0 255.255.255.0
```

Configureer vervolgens de toegangslijst om deze objecten te gebruiken:

```
access-list vpn extended permit ip object insidenet object rsite
```

U kunt ook de subnetten zelf gebruiken, maar in grotere implementaties is het gemakkelijker om objecten en objectgroepen te gebruiken.

Stap 3. IPsec-tunnelconfiguratie (fase 2-verificatie)

Hier zullen wij de "Reeks van de Transformatie" en de tunnelgroep vormen, die de authenticatie fase-2 zal opzetten. Als u fase-2 anders instelt dan fase-1, krijgt u een andere transformatie-set. Hier definieert esp-aes de codering en esp-sha-hmac definieert de hash.

Het tunnelgroepbevel vormt de verbindingsspecifieke tunnelinformatie, zoals de vooraf gedeelde sleutel. Gebruik het openbare IP van de externe peer als naam van de tunnelgroep.

```
ASA5505(config)# crypto ipsec transform-set asarv esp-aes esp-sha-hmac
ASA5505(config)# tunnel-group 12.23.36.10 type ipsec-l2l
ASA5505(config)# tunnel-group 12.23.36.10 ipsec-attributes
ASA5505(config-tunnel-ipsec)# pre-shared-key c12c0VPn3x4mPL3
ASA5505(config-tunnel-ipsec)# exit
ASA5505(config)#
```

Stap 4. Configuratie Crypto Map

Nu moeten we de configuratie van fase-1 en fase-2 toepassen op een 'crypto map' waarmee de ASA VPN kan opzetten en het juiste verkeer kan versturen. Zie dit als het samenbinden van de stukken van VPN.

```
ASA5505(config)# crypto map asarv 1 match address vpn
ASA5505(config)# crypto map asarv 1 set peer 12.23.36.10
ASA5505(config)# crypto map asarv 1 set transform-set asarv
ASA5505(config)# crypto map asarv interface outside
ASA5505(config)#
```

Stap 5. Controleer de VPN-status

Controleer tot slot de eindpunten om te controleren of de VPN-verbinding actief is. De verbinding zal niet omhoog op zijn eigen komen, zult u verkeer moeten overgaan zodat ASA het kan ontdekken en proberen om de verbinding te vestigen. Gebruik op de ASA het commando "show crypto isakamsa" om de status weer te geven.

```



ASA5505(config)# show crypto isakmp sa

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 12.23.36.10
  Type    : L2L                Role    : responder
  Rekey    : no                 State   : MM_ACTIVE
ASA5505(config)#

```

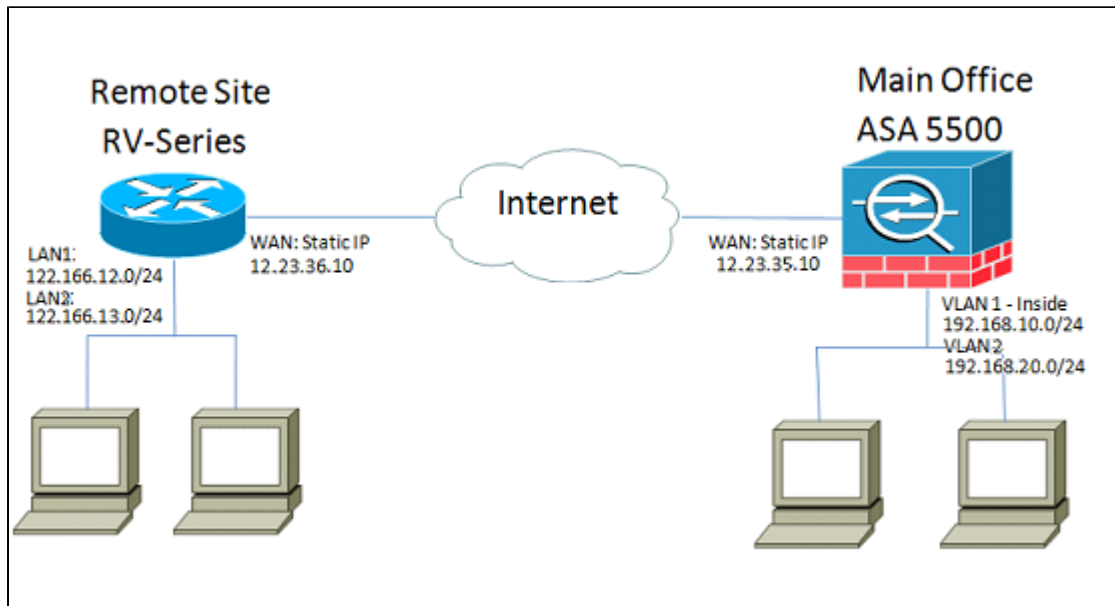
Ga op de RV42G naar de pagina **VPN > Samenvatting** en controleer de status.

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	TestVPN	Connected	AES/SHA1	122.166.12.0 255.255.255.0	192.168.10.0 255.255.255.0	12.23.35.10	Disconnect	 
Add								

Page 1 of 1

Alternatief scenario: meerdere subnetten op het netwerk

Geen paniek. Dit kan een overweldigend gecompliceerd proces lijken wanneer u het netwerk aan het opzetten bent, maar u hebt het harde deel hierboven al gedaan. Het configureren van VPN voor meerdere subnetten vereist enige extra configuratie, maar zeer weinig extra complexiteit (tenzij uw subnetschema uitgebreid is). Het voorbeeld dat wij voor deze sectie hebben gebruikt gebruikt 2 subnets bij elke plaats. De bijgewerkte netwerktopologie is zeer gelijkaardig:



De RV042G configureren

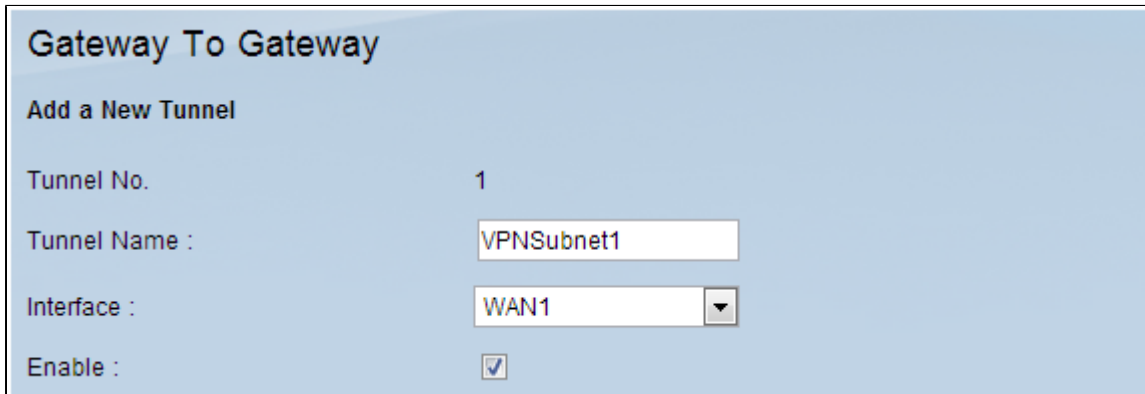
Net als voorheen zullen we de RV042G eerst configureren. RV042G kan niet meerdere subnetten via één tunnel configureren, dus we moeten een extra ingang toevoegen voor het nieuwe subnet. Deze sectie zal alleen betrekking hebben op de VPN-configuratie voor meerdere subnetten en niet op enige extra setup-configuratie voor deze subnetten.

Stap 1. De eerste tunnel configureren

We zullen voor elke tunnel dezelfde configuratie gebruiken als voor het enkele subnetvoorbeeld.

Zoals voorheen, vormt u dit door te gaan naar **VPN > Gateway naar Gateway** en een nieuwe tunnel toe te voegen, of als u een bestaande tunnel gebruikt ga naar de **VPN > Samenvatting** pagina en bewerk de bestaande.

a) Configureren van de tunnelnaam, maar verandering omdat we meer dan één verandering van de naam meer beschrijvend te hebben.



Gateway To Gateway

Add a New Tunnel

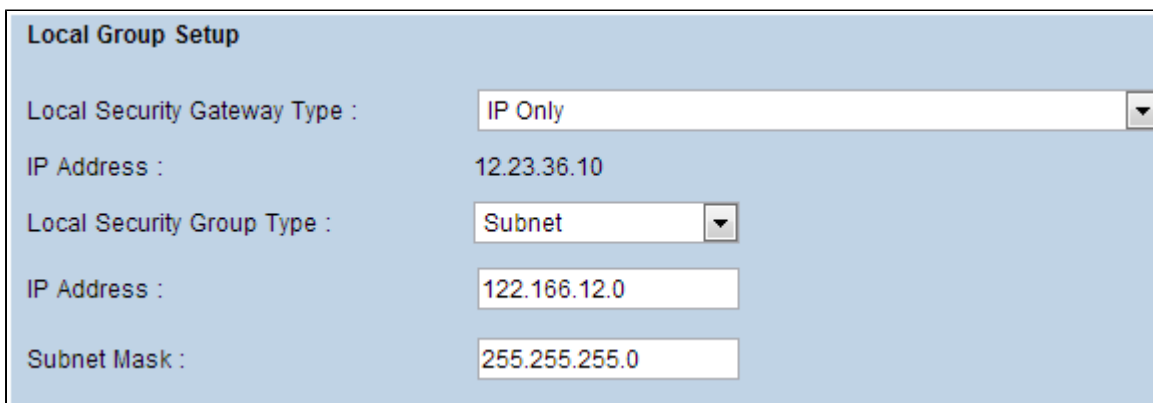
Tunnel No. : 1

Tunnel Name : VPNSubnet1

Interface : WAN1

Enable : ☒

b) Daarna zullen we de lokale groep configureren, hetzelfde als voorheen. Configureer dit voor slechts één van de subnetten die toegang nodig hebben. We zullen een tunnelingang hebben voor 122.166.12.x en een andere voor het 122.166.13.x-subnet.



Local Group Setup

Local Security Gateway Type : IP Only

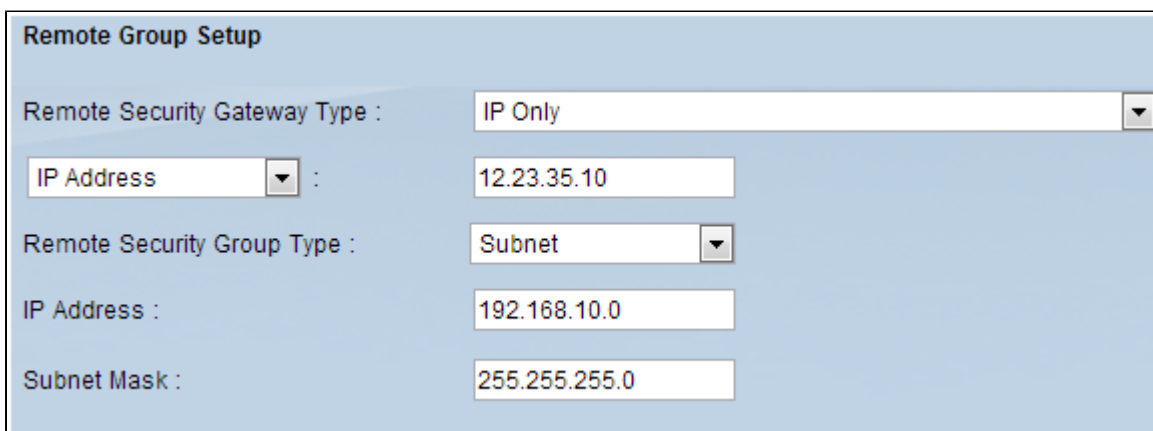
IP Address : 12.23.36.10

Local Security Group Type : Subnet

IP Address : 122.166.12.0

Subnet Mask : 255.255.255.0

c) Configureer nu de externe site, opnieuw met behulp van dezelfde procedure als hierboven.



Remote Group Setup

Remote Security Gateway Type : IP Only

IP Address : 12.23.35.10

Remote Security Group Type : Subnet

IP Address : 192.168.10.0

Subnet Mask : 255.255.255.0

d) Configureer tot slot de coderingsinstellingen. Onthoud deze instellingen omdat u wilt dat ze hetzelfde zijn op beide tunnels die we configureren.

IPSec Setup

Keying Mode :	IKE with Preshared key	▼
Phase 1 DH Group :	Group 2 - 1024 bit	▼
Phase 1 Encryption :	AES-128	▼
Phase 1 Authentication :	SHA1	▼
Phase 1 SA Life Time :	28800	seconds
Perfect Forward Secrecy :	<input type="checkbox"/>	
Phase 2 DH Group :	Group 2 - 1024 bit	▼
Phase 2 Encryption :	AES-128	▼
Phase 2 Authentication :	SHA1	▼
Phase 2 SA Life Time :	28800	seconds
Preshared Key :	c12c0VPn3x4mPL3	

Stap 2. De tweede tunnel configureren

Nu Subnet 1 voor de VPN-tunnel is geconfigureerd, moeten we naar **VPN > Gateway naar Gateway** gaan en een tweede tunnel toevoegen. Deze tweede ingang zal worden gevormd veel het zelfde als eerste, maar met de secundaire subnets van elke plaats.

a) Noem het iets dat onderscheidt zodat u weet welke verbinding het is.

Gateway To Gateway

Add a New Tunnel

Tunnel No.	2
Tunnel Name :	VPNsubnet2
Interface :	WAN1 ▼
Enable :	<input checked="" type="checkbox"/>

b) Gebruik het tweede subnetnummer als groep "Local Security".

Local Group Setup

Local Security Gateway Type :	IP Only ▼
IP Address :	12.23.36.10
Local Security Group Type :	Subnet ▼
IP Address :	122.166.13.0
Subnet Mask :	255.255.255.0

C) En gebruik het tweede externe subnetnummer als de groep "Beveiliging op afstand".

The screenshot shows the 'Remote Group Setup' configuration window. It contains the following fields and values:

Field	Value
Remote Security Gateway Type :	IP Only
IP Address :	12.23.35.10
Remote Security Group Type :	Subnet
IP Address :	192.168.20.0
Subnet Mask :	255.255.255.0

d) Configureer de codering voor fase 1 en 2 op dezelfde manier als voor de eerste tunnel.

The screenshot shows the 'IPSec Setup' configuration window. It contains the following fields and values:

Field	Value
Keying Mode :	IKE with Preshared key
Phase 1 DH Group :	Group 2 - 1024 bit
Phase 1 Encryption :	AES-128
Phase 1 Authentication :	SHA1
Phase 1 SA Life Time :	28800 seconds
Perfect Forward Secrecy :	<input type="checkbox"/>
Phase 2 DH Group :	Group 2 - 1024 bit
Phase 2 Encryption :	AES-128
Phase 2 Authentication :	SHA1
Phase 2 SA Life Time :	3600 seconds
Preshared Key :	c12c0VPn3x4mPL3

De ASA configureren

Nu zullen we de configuratie op de ASA aanpassen. Deze configuratie is ongelooflijk eenvoudig. U kunt dezelfde configuratie gebruiken als hierboven, aangezien alle dezelfde coderingsinstellingen worden gebruikt, met slechts een kleine wijziging. We moeten extra verkeer als "interessant" labelen voor de firewall om het via VPN te versturen. Aangezien we een toegangslijst gebruiken om interessant verkeer te identificeren, hoeven we alleen deze toegangslijst aan te passen.

Stap 1. Om te beginnen met, verwijder de oude toegangslijst, zodat we de objecten in de ASA kunnen wijzigen. Gebruik het "nee" formulier van de opdracht om configuraties in de CLI te verwijderen.

Stap 2. Nadat de ACL is verwijderd, willen we nieuwe objecten maken voor de betrokken nieuwe subnetten (ervan uitgaande dat u dit nog niet hebt gedaan bij het instellen van die subnetten). We willen ze ook wat beschrijvender maken.

Gebaseerd op onze VLAN-configuratie hieronder:

```

interface Vlan1
  nameif inside
  security-level 100
  ip address 192.168.10.1 255.255.255.0
!
interface Vlan2
  nameif engineering
  security-level 100
  ip address 192.168.20.1 255.255.255.0
!
interface Vlan10
  nameif outside
  security-level 0
  ip address 12.23.35.10 255.255.255.0
!

```

We hebben een objectgroep nodig voor het hoofdnetwerk (192.168.10.x) en het ingenieursnetwerk (192.168.20.x). Configureer de netwerkobjecten als volgt:

```

ASA5505(config)# show run object
object network ASAvlan1
  subnet 192.168.10.0 255.255.255.0
object network ASAvlan2
  subnet 192.168.20.0 255.255.255.0
object network RVvlan1
  subnet 122.166.12.0 255.255.255.0
object network RVvlan2
  subnet 122.166.13.0 255.255.255.0

```

Stap 3. Nu de relevante netwerkobjecten zijn geconfigureerd, kunnen we de toegangslijst configureren om het juiste verkeer te labelen. U wilt ervoor zorgen dat u een toegangslijst hebt voor beide netwerken achter de ASA naar beide externe subnetten. Het eindresultaat moet er zo uitzien.

```

ASA5505(config)# show run access-list
access-list vpn extended permit ip object ASAvlan1 object RVvlan1
access-list vpn extended permit ip object ASAvlan1 object RVvlan2
access-list vpn extended permit ip object ASAvlan2 object RVvlan1
access-list vpn extended permit ip object ASAvlan2 object RVvlan2

```

Stap 4. Omdat we de oude toegangslijst hebben verwijderd, moeten we deze opnieuw toepassen op de crypto-kaart met dezelfde opdracht als voorheen:

```

ASA5505(config)# crypto map asarv 1 match address vpn

```

Controleer de verbinding

En dat is het dan! Uw tunnel zou nu operationeel moeten zijn. Start de verbinding en controleer de status met de opdracht "show crypto isakamsa" op de ASA.

```





ASA5505(config)# show crypto isakmp sa

  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 12.23.36.10
   Type    : L2L                Role    : responder
   Rekey    : no                 State    : MM_ACTIVE
ASA5505(config)# █

```

In de RV-serie wordt de status weergegeven op de pagina VPN > Samenvatting.

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	VPNSubnet1	Connected	AES/SHA1	122.166.12.0 255.255.255.0	192.168.10.0 255.255.255.0	12.23.35.10	Disconnect	 
2	VPNsubnet2	Connected	AES/SHA1	122.166.13.0 255.255.255.0	192.168.20.0 255.255.255.0	12.23.35.10	Disconnect	 
<div> Add <div> Page 1 of 1 </div> </div>								

Bekijk een video met betrekking tot dit artikel...

[Klik hier om andere Tech Talks van Cisco te bekijken](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.