

Configurer un tunnel VPN de site à site entre les routeurs de la gamme RV et les appareils de sécurité adaptables ASA 5500

Objectif

La sécurité est essentielle pour protéger la propriété intellectuelle d'une entreprise tout en assurant la continuité de ses activités et en lui offrant l'occasion d'étendre son environnement de travail aux employés qui ont besoin d'un accès aux ressources de l'entreprise à tout moment et en tout lieu.

Les solutions de sécurité de VPN deviennent de plus en plus importantes pour les PME. Un VPN est un réseau privé construit au sein d'une infrastructure de réseau public, comme l'Internet mondial. Il étend un réseau privé entre des bureaux géographiquement séparés. Il permet à un ordinateur hôte d'envoyer et de recevoir des données sur des réseaux publics, car il fait partie intégrante du réseau privé avec toutes ses fonctionnalités. Les VPN améliorent la sécurité d'une entreprise décentralisée, ce qui permet au personnel de travailler facilement à partir de différents sites sans compromettre le réseau. Les raisons d'utiliser un VPN sont les exigences de « virtualisation » d'une partie des communications d'une entreprise et l'économie des communications.

Il existe différentes topologies VPN : Hub and Spoke, Point-to-point et Full Mesh. Ce conseil judicieux porte sur le VPN de site à site (point à point), qui fournit une infrastructure Internet permettant d'étendre les ressources réseau aux bureaux distants, aux bureaux à domicile et aux sites des partenaires commerciaux. Tout le trafic entre les sites est chiffré à l'aide du protocole de sécurité IP (IPsec), et des fonctionnalités réseau comme le routage, la qualité de service (QoS) et la prise en charge de la multidiffusion sont intégrées.

Les routeurs Cisco de la gamme RV offrent des solutions de VPN robustes et faciles à gérer aux petites entreprises économes. Les appareils de sécurité adaptables Cisco de la gamme ASA 5500 aident les entreprises à concilier sécurité et productivité. Il associe le pare-feu d'inspection dynamique le plus déployé du secteur à des services de sécurité réseau de nouvelle génération complets, notamment : visibilité et contrôle granulaire des applications et des micro-applications, sécurité Web, systèmes de prévention des intrusions (IPS), accès à distance hautement sécurisé, etc.

Ce petit guide montre un exemple de conception pour la création d'un VPN IPsec de site à site entre les routeurs de la gamme RV et les appareils de sécurité adaptables de la gamme ASA 5500, et en fournit des exemples de configuration.

Périphériques pertinents

Routeurs VPN de la gamme RV0xx de Cisco

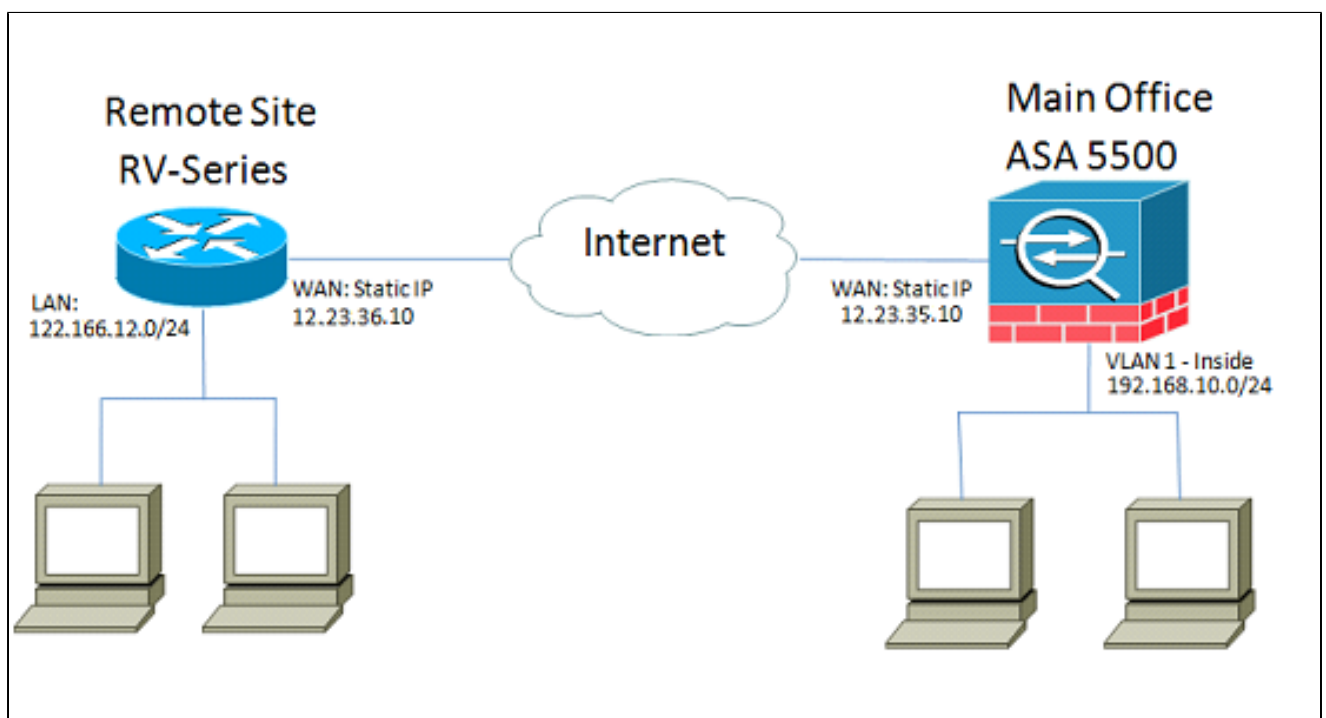
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500

Version du logiciel

- 4.2.2.08 [Routeurs VPN de la gamme RV0xx de Cisco]

Pré-configuration

L'image suivante présente un exemple de mise en œuvre d'un tunnel VPN de site à site à l'aide d'un routeur de la gamme RV (site distant) et d'un ASA 5500 (bureau principal).



Avec cette configuration, un hôte du réseau du site distant de 122.166.12.x et un hôte du VLAN 1 du bureau principal peuvent communiquer entre eux en toute sécurité.

Fonctionnalités principales

Protocole IKE (Internet Key Exchange)

Internet Key Exchange (IKE) est le protocole utilisé pour configurer une association de sécurité (SA) dans la suite de protocoles IPsec. Le protocole IKE s'appuie sur le protocole d'Oakley et sur le protocole ISAKMP (Internet Security Association and Key Management) et met à profit un échange de clés Diffie-Hellman pour configurer un secret de session partagé à partir duquel les clés cryptographiques sont dérivées. Une politique de sécurité pour chaque homologue doit être gérée manuellement.

Sécurité du protocole Internet (IPSec)

IPSec utilise des services de sécurité cryptographiques pour protéger les communications sur les réseaux IP (Internet Protocol). IPSec prend en charge l'authentification par les homologues au niveau du réseau, l'authentification de l'origine des données, l'intégrité des données, la confidentialité des données (chiffrement) et la protection contre la relecture. IPSec fait appel à de nombreuses technologies de composants et méthodes de chiffrement. Pourtant, le fonctionnement d'IPSec peut être décomposé en cinq étapes principales :
Étape 1. Le « trafic d'intérêt » lance le processus IPSec : le trafic est jugé d'intérêt lorsque la politique de sécurité IPSec configurée dans les homologues IPSec démarre le processus IKE.

Étape 2. IKE phase 1 : IKE authentifie les homologues IPSec et négocie les associations de sécurité IKE au cours de cette phase, en configurant un canal sécurisé pour la négociation des associations de sécurité IPSec au cours de la phase 2.

Étape 3. IKE phase 2 : IKE négocie les paramètres des associations de sécurité IPSec et configure les associations de sécurité IPSec correspondantes dans les homologues.

Étape 4. Transfert de données : les données sont transférées entre des homologues IPSec en fonction des paramètres et des clés IPSec stockés dans la base de données SA.

Étape 5. Fin du tunnel IPSec : les associations de sécurité IPSec se terminent par suppression ou par dépassement du délai d'attente.

ISAKMP

Le protocole ISAKMP (Internet Security Association and Key Management Protocol) est utilisé pour négocier le tunnel entre les deux terminaux. Il définit les procédures d'authentification, de communication et de génération de clés, et est utilisé par le protocole IKE pour échanger des clés de chiffrement et établir la connexion sécurisée.

Conseils de conception

Topologie de VPN : avec un VPN de site à site, un tunnel IPsec sécurisé est configuré entre chaque site et tous les autres. Une topologie multisite est généralement mise en œuvre sous la forme d'un maillage intégral de tunnels de VPN de site à site (c'est-à-dire que chaque site a établi des tunnels vers tous les autres sites). Si aucune communication n'est nécessaire entre les bureaux distants, on utilise une topologie de VPN en étoile pour réduire le nombre

de tunnels VPN (c'est-à-dire que chaque site établit un tunnel de VPN uniquement vers le bureau principal).

Adressage IP de réseau étendu (WAN) et système de nom de domaine dynamique : le tunnel de VPN doit être établi entre deux adresses IP publiques. Si les routeurs de réseau étendu se voient attribuer des adresses IP statiques du fournisseur d'accès Internet, le tunnel de VPN peut être mis en œuvre directement à l'aide d'adresses IP publiques statiques. Cependant, la plupart des petites entreprises utilisent des services Internet à large bande économiques tels que le modem DSL ou le câble, et reçoivent des adresses IP dynamiques de leur fournisseur d'accès Internet. Dans de tels cas, il est possible d'utiliser le DDNS pour mapper l'adresse IP dynamique à un nom de domaine complet (FQDN).

Adressage IP de réseau local : l'adresse IP du réseau local privé de chaque site ne doit pas se chevaucher. L'adresse IP du réseau local par défaut sur chaque site distant doit toujours être modifiée.

Authentification de VPN : le protocole IKE est utilisé pour authentifier les homologues de VPN lors de l'établissement d'un tunnel de VPN. Parmi les différentes méthodes d'authentification IKE, la clé prépartagée est la plus pratique. Cisco recommande l'utilisation d'une clé prépartagée renforcée.

Chiffrement de VPN : pour assurer la confidentialité des données transportées sur le VPN, des algorithmes de chiffrement sont utilisés pour chiffrer la charge utile des paquets IP. DES, 3DES et AES représentent trois normes de chiffrement courantes. AES est considéré comme la plus sécurisée par rapport à DES et 3DES. Cisco recommande fortement d'utiliser le chiffrement AES-128 bits ou supérieur (par exemple, AES-192 et AES-256). Cependant, plus l'algorithme de chiffrement est renforcé, plus il nécessite de ressources de traitement.

Conseils de configuration

Liste de vérification préalable à la configuration

Étape 1. Assurez-vous que l'ASA et le routeur RV sont tous les deux connectés à la passerelle Internet (routeur ou modem FAI).

Étape 2. Mettez le routeur Cisco RV sous tension, puis connectez les ordinateurs internes, les serveurs et les autres périphériques IP au commutateur LAN ou aux ports du commutateur sur le routeur RV.

Étape 3. Faites de même pour le réseau derrière l'ASA. Étape 4. Assurez-vous que les adresses réseau IP LAN sont configurées sur chaque site et qu'elles ne sont pas des sous-réseaux différents. Dans cet exemple, le réseau local du bureau principal utilise 192.168.10.0/24 et le réseau local du site distant 122.166.12.0/24.

Étape 4. Assurez-vous que les ordinateurs et les serveurs locaux peuvent communiquer entre eux et avec le routeur.

Identification de la connexion au réseau étendu

Vous devrez savoir si votre fournisseur de service Internet vous donne une adresse IP dynamique ou si vous avez reçu une adresse IP statique. Habituellement, le fournisseur de

service Internet fournira une adresse IP dynamique, mais vous devrez la confirmer pour terminer la configuration.

Configurer le routeur RV042G au bureau distant

Étape 1. Connectez-vous à l'interface utilisateur Web et accédez à la section VPN > Gateway to Gateway. Puisque nous ajoutons une connexion de réseau local à réseau local, les terminaux seront la passerelle de chaque réseau.



Small Business

RV042G

System Summary

▶ Setup

▶ DHCP

▶ System Management

▶ Port Management

▶ Firewall

▼ VPN

Summary

Gateway To Gateway

Client To Gateway

Étape 2. configuration des points d'extrémité locaux et distants sur le routeur

a) Configurez le nom du tunnel pour l'identifier à partir de tout autre tunnel que vous avez peut-être préalablement configuré.

Gateway To Gateway

Add a New Tunnel

Tunnel No.	1
Tunnel Name :	<input type="text" value="TestVPN"/>
Interface :	<input type="text" value="WAN1"/> ▼
Enable :	<input checked="" type="checkbox"/>

b) La configuration de groupe local configure le ou les hôtes locaux à autoriser sur le tunnel de VPN. Assurez-vous de disposer du sous-réseau et du masque approprié pour le réseau que vous souhaitez autoriser sur le tunnel.

Local Group Setup

Local Security Gateway Type :	<input type="text" value="IP Only"/> ▼
IP Address :	<input type="text" value="12.23.36.10"/>
Local Security Group Type :	<input type="text" value="Subnet"/> ▼
IP Address :	<input type="text" value="122.166.12.0"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>

c) La configuration de groupe distant configure le terminal distant et le trafic réseau que le routeur doit rechercher. Saisissez l'adresse IP statique de la passerelle distante dans le champ d'adresse IP pour établir la connexion de la passerelle. Saisissez ensuite le sous-réseau autorisé sur le VPN à partir du site distant (le réseau local du bureau principal).

Remote Group Setup

Remote Security Gateway Type :	<input type="text" value="IP Only"/> ▼
<input type="text" value="IP Address"/> ▼ :	<input type="text" value="12.23.35.10"/>
Remote Security Group Type :	<input type="text" value="Subnet"/> ▼
IP Address :	<input type="text" value="192.168.10.0"/>

Étape 3. Configurez les paramètres du tunnel.

a) Vous voudrez configurer une clé prépartagée pour obtenir des résultats optimaux.

Les phases 1 et 2 constituent des phases différentes d'authentification. La phase 1 crée le tunnel initial et entame la négociation, tandis que la phase 2 finalise la négociation de la clé de chiffrement et protège la transmission des données une fois le tunnel établi.

b) Le groupe DH correspondra au groupe de politiques de chiffrement isakmp sur l'ASA, qui sera traité dans la section suivante. Sur l'ASA, la valeur par défaut est le groupe 2, et les versions plus récentes du code ASA nécessitent au moins le groupe DH 2. Le compromis est qu'il s'agit d'un bit plus élevé, ce qui nécessite plus de temps processeur.

c) Le chiffrement de phase 1 définit l'algorithme de chiffrement utilisé. La valeur par défaut sur la gamme RV est DES, mais la valeur par défaut sur l'ASA sera 3DES. Cependant, ces normes anciennes et ne sont pas efficaces pour la mise en œuvre actuelle. Le chiffrement AES est plus rapide et plus sécurisé, et Cisco recommande au moins un chiffrement AES-128 (ou simplement AES) pour de meilleurs résultats.

d) L'authentification de phase 1 vérifie l'intégrité des paquets. Les options sont SHA-1 et MD5, et l'une ou l'autre devrait fonctionner, car elles produisent des résultats similaires.

La configuration de la phase 2 suit les mêmes règles que la phase 1. Lors de la configuration des paramètres IPsec, gardez à l'esprit que les paramètres de l'ASA devront CORRESPONDRE à ceux du RV042G. En cas de divergence, les périphériques ne pourront pas négocier la clé de cryptage et la connexion échouera.

Remarque : veuillez à enregistrer les paramètres avant de quitter cette page !

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

Configurer l'ASA 5500 au bureau principal (CLI)

Remarque : veillez à utiliser souvent la commande « write mem » pour éviter de perdre des configurations. Tout d'abord, voici les interfaces que nous avons configurées sur l'ASA. Les vôtres peuvent être différentes, alors assurez-vous de modifier les configurations en conséquence.

```
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
```

Étape 1. Configuration de la gestion du chiffrement (ISAKMP)

La première étape consistera à configurer la politique ISAKMP, qui est utilisée pour négocier le chiffrement du tunnel. Cette configuration doit être IDENTIQUE sur les deux terminaux. C'est ici que vous configurerez les paramètres de chiffrement pour qu'ils correspondent à ceux de la phase 1 de la configuration du routeur RV.

```
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)# █
```

Étape 2. Sélection du trafic

Il s'agit du même trafic que celui du groupe de sécurité local et distant sur le RV042G. Sur l'ASA, nous utilisons des listes d'accès pour définir ce que le réseau juge un « trafic d'intérêt » à autoriser sur le VPN.

Tout d'abord, configurez les objets réseau pour le site distant et le site local :

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

Configurez ensuite la liste d'accès pour utiliser ces objets :

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

Vous pouvez également utiliser les sous-réseaux eux-mêmes, mais il est plus facile d'utiliser des objets et des groupes d'objets pour des grandes mises en œuvre.

Étape 3. Configuration du tunnel IPSec (authentification de phase 2)

Ici, nous allons configurer le « Transform Set » et le groupe de tunnels, qui va configurer l'authentification de Phase-2. Si vous configurez Phase-2 pour qu'elle soit différente de Phase-1, vous aurez un jeu de transformation différent. Ici, esp-aes définit le chiffrement et esp-sha-hmac définit le hachage.

La commande « tunnel-group » configure les informations de tunnel spécifiques à la connexion, comme une clé prépartagée. Utilisez l'adresse IP publique de l'homologue distant comme nom de groupe de tunnels.

```
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)#
```

Étape 4. Configuration de la carte de chiffrement

Nous devons maintenant appliquer les configurations de Phase 1 et de Phase 2 à une « crypto-carte » qui permettra à l'ASA d'établir le VPN et d'envoyer le trafic correct.

Considérez cela comme un lien entre les parties du 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)#
```

Étape 5. Vérification de l'état VPN

Enfin, vérifiez les terminaux pour vous assurer que la connexion VPN est active et fonctionnelle. La connexion ne s'établira pas d'elle-même, vous devrez faire passer du trafic pour que l'ASA puisse le détecter et tenter d'établir la connexion. Sur l'ASA, utilisez la

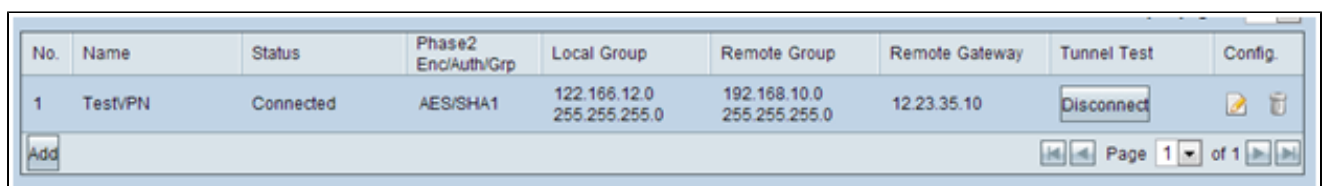
commande « show crypto isakmpsa » pour en afficher l'état.



```
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)# █
```

Sur le RV42G, accédez à la page VPN > Summary (résumé), puis vérifiez l'état.

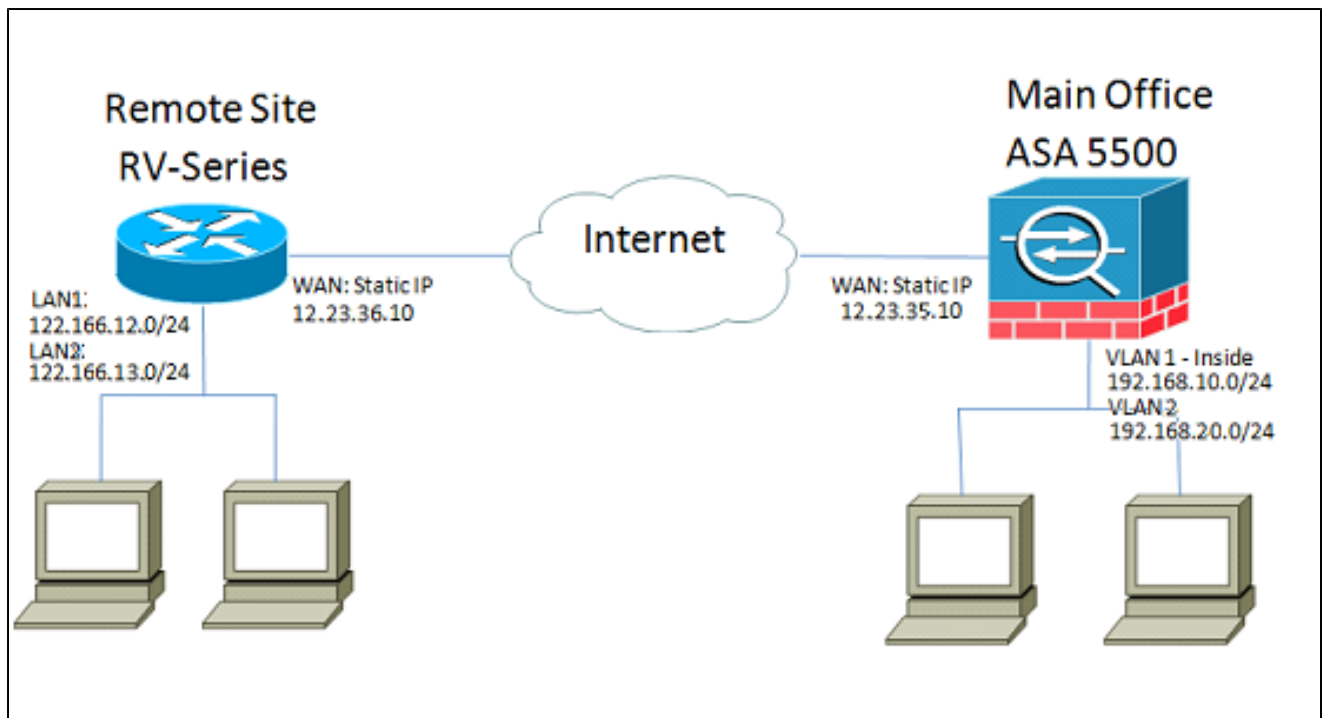


No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	TestVPN	Connected	AES/SHA1	122.166.12.0 255.255.255.0	192.168.10.0 255.255.255.0	12.23.35.10	Disconnect	 

Page 1 of 1

Autre scénario : plusieurs sous-réseaux sur le réseau

Pas de panique. Ce processus peut sembler extrêmement compliqué lorsque vous configurez le réseau, mais vous avez déjà fait la partie la plus difficile. La configuration d'un VPN pour plusieurs sous-réseaux nécessite une configuration supplémentaire, mais très peu de complexité supplémentaire (sauf si votre schéma de sous-réseau est grand). L'exemple que nous avons utilisé pour cette section met à profit deux sous-réseaux sur chaque site. La topologie du réseau mis à jour est très similaire :



Configuration du RV042G

Comme précédemment, nous allons d'abord configurer le RV042G. Le RV042G ne peut pas configurer plusieurs sous-réseaux sur un seul tunnel. Nous devons donc ajouter une entrée supplémentaire pour le nouveau sous-réseau. Cette section couvrira uniquement la configuration du VPN pour plusieurs sous-réseaux, et non leur configuration d'installation supplémentaire.

Étape 1. Configuration du premier tunnel

Nous utiliserons la même configuration pour chaque tunnel que pour l'exemple à sous-réseau unique. Comme auparavant, vous pouvez effectuer cette configuration en accédant à VPN > Gateway to Gateway (VPN > passerelle à passerelle) et en ajoutant un nouveau tunnel. Si vous utilisez un tunnel existant, rendez-vous à la page VPN > Summary (VPN > résumé) et modifiez celui qui est déjà configuré.

a) Configurez le nom du tunnel, mais modifiez-le, car plusieurs noms devront être modifiés pour être plus descriptifs.

Gateway To Gateway

Add a New Tunnel

Tunnel No.

Tunnel Name :

Interface :

Enable :

b) Ensuite, nous allons configurer le groupe local, comme précédemment. Configurez-le uniquement pour UN des sous-réseaux nécessitant un accès. Une entrée de tunnel sera donc en place pour 122.166.12.x et une autre pour le sous-réseau 122.166.13.x.

Local Group Setup	
Local Security Gateway Type :	<input type="text" value="IP Only"/>
IP Address :	<input type="text" value="12.23.36.10"/>
Local Security Group Type :	<input type="text" value="Subnet"/>
IP Address :	<input type="text" value="122.166.12.0"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>

c) Configurez maintenant le site distant en utilisant la même procédure que ci-dessus.

Remote Group Setup	
Remote Security Gateway Type :	<input type="text" value="IP Only"/>
<input type="text" value="IP Address"/> :	<input type="text" value="12.23.35.10"/>
Remote Security Group Type :	<input type="text" value="Subnet"/>
IP Address :	<input type="text" value="192.168.10.0"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>

d) Enfin, configurez les paramètres de chiffrement. N'oubliez pas ces paramètres, car ils doivent être les mêmes sur les deux tunnels que nous configurons.

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	

Étape 2. Configuration du deuxième tunnel

Maintenant que le sous-réseau 1 est configuré pour le tunnel de VPN, nous devons accéder à VPN > Gateway to Gateway (VPN > passerelle à passerelle) et ajouter un deuxième tunnel. Cette deuxième entrée sera configurée de la même manière que la première, mais avec les sous-réseaux secondaires de chaque site.

a) Assurez-vous de lui donner un nom distinctif afin de savoir de quelle connexion il s'agit.

Gateway To Gateway

Add a New Tunnel

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

b) Utilisez le deuxième sous-réseau comme groupe de « sécurité locale ».

Local Group Setup	
Local Security Gateway Type :	<input type="text" value="IP Only"/>
IP Address :	<input type="text" value="12.23.36.10"/>
Local Security Group Type :	<input type="text" value="Subnet"/>
IP Address :	<input type="text" value="122.166.13.0"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>

c) Et utilisez le deuxième sous-réseau distant comme groupe de « sécurité à distance ».

Remote Group Setup	
Remote Security Gateway Type :	<input type="text" value="IP Only"/>
<input type="text" value="IP Address"/> :	<input type="text" value="12.23.35.10"/>
Remote Security Group Type :	<input type="text" value="Subnet"/>
IP Address :	<input type="text" value="192.168.20.0"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>

d) Configurez le chiffrement pour les phases 1 et 2 de la même manière que pour le premier tunnel.

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 :	3600 seconds
Preshared Key :	c12c0VPn3x4mPL3

Configurer l'ASA

Nous allons maintenant modifier la configuration de l'ASA. Cette configuration est incroyablement simple. Vous pouvez utiliser la même configuration que celle ci-dessus, car elle utilise tous les mêmes paramètres de chiffrement, avec seulement une modification mineure. Nous devons marquer le trafic supplémentaire comme « intéressant » pour que le pare-feu l'envoie sur le VPN. Puisque nous utilisons une liste d'accès afin d'identifier le trafic intéressant, tout ce que nous devons faire est de modifier cette liste d'accès.

Étape 1. Pour commencer, supprimez l'ancienne liste de contrôle d'accès afin de pouvoir modifier les objets de l'ASA. Utilisez la forme « no » de la commande pour supprimer des configurations dans l'interface de ligne de commande.

Étape 2. Une fois la liste de contrôle d'accès supprimée, nous voulons créer de nouveaux objets pour les nouveaux sous-réseaux concernés (en supposant que vous ne l'avez pas déjà fait lors de la configuration de ces sous-réseaux). Nous voulons également les rendre plus descriptifs.

Selon notre configuration de VLAN ci-dessous :

```
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
!
```

Nous avons besoin d'un groupe d'objets pour le réseau interne principal (192.168.10.x) et le réseau d'ingénierie (192.168.20.x). Configurez les objets de réseau comme suit :

```
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
```

Étape 3. Maintenant que les objets réseau appropriés ont été configurés, nous pouvons

configurer la liste de contrôle d'accès pour marquer le trafic approprié. Vous voudrez vous assurer d'avoir une entrée de liste d'accès pour les deux réseaux derrière l'ASA vers les deux sous-réseaux distants. Le résultat final devrait ressembler à ceci.

```
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
```

Étape 4. Maintenant, comme nous avons supprimé l'ancienne liste de contrôle d'accès, nous devons la réappliquer à la crypto-carte à l'aide de la même commande que précédemment :

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

Vérifier la connexion





Et voilà! Votre tunnel devrait désormais être opérationnel. Établissez la connexion et vérifiez son état à l'aide de la commande « show crypto isakmpsa » sur l'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)#
```

Sur le routeur de la série RV, l'état sera affiché dans la page « VPN > Summary » (VPN > résumé).

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	 

Add Page 1 of 1



Visionner une vidéo connexe à cet article...

[Cliquez ici pour consulter les autres discussions techniques \(Tech Talks\) de Cisco](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.