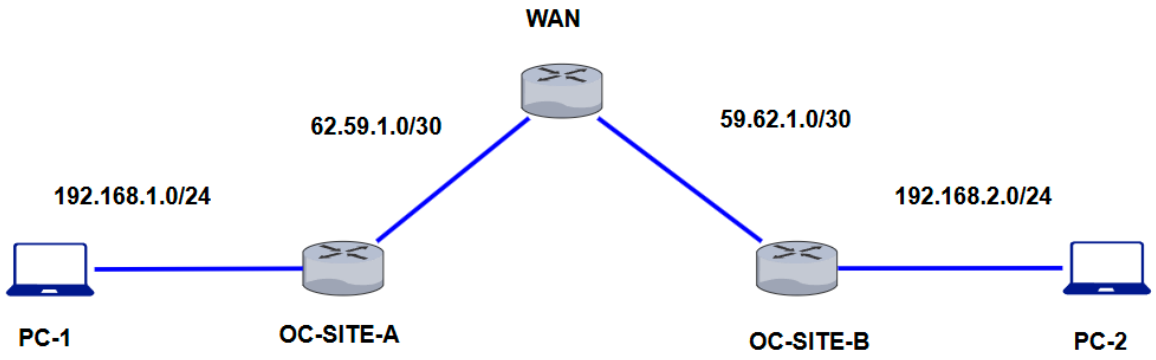
TP - VPN Site to site

Nous allons mettre en place cette architecture sur Packet Tracer avec des routeurs 1941 et des PC.
N'oubliez pas de renommer les routeurs et les PC pour que sur les screens on puisse voir où vous tapez les commandes !



Packet Tracer est un excellent outil de simulation qui permet de configurer IPSEC en IKEv1. Ceci dit, Packet Tracer ne permet pas de configurer IPSEC en IKEv2. Même si IKEv1 est remplacé par IKEv2, plus rapide, plus sécurisé, le principe de base reste le même.

Configurez la topologie de base

Commencez par la configuration de base des routeurs, en premier le routeur OC-SITE-A :

```
en
conf t
interface gig 0/0
ip address 192.168.1.254 255.255.255.0
ip nat inside
no shut
exit
interface gig 0/1
ip address 62.59.1.1 255.255.255.252
ip nat outside
no shut
exit
ip route 0.0.0.0 0.0.0.0 62.59.1.2
ip access-list extended NAT
deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 192.168.1.0 0.0.0.255 any
```

```
ip nat inside source list NAT interface gig 0/1 overload
```

Dans cette configuration de base on trouve : une route par défaut qui passe par le routeur WAN, le NAT avec identification de l'interface interne (INSIDE) et WAN (OUTSIDE), une ACL qui permet de définir ce qui doit être traduit par le NAT et ce qui ne doit pas être traduit car envoyé dans le VPN, notez que cette ACL n'est utilisée que pour le NAT, pas pour autoriser des paquets à entrer ou sortir des interfaces du routeur. Enfin on trouve la commande de NAT Overload qui va permettre de traduire toutes les IP du LAN 192.168.1.0/24 sur l'IP publique de l'interface GigabitEthernet 0/1.

1. Quelle est la différence entre une interface configurée en `ip nat inside` et une interface configurée en `ip nat outside` ?

2. Pourquoi utilise-t-on une adresse IP différente pour chaque réseau local ?

3. Expliquez le fonctionnement du NAT Overload. Pourquoi est-il utilisé dans cette architecture ?

Continuez avec le routeur OC-SITE-B, dont la configuration est similaire au routeur OC-SITE-A :

```
en
conf t
interface gig 0/0
ip address 192.168.2.254 255.255.255.0
ip nat inside
no shut
exit
interface gig 0/1
ip address 59.62.1.1 255.255.255.252
ip nat outside
no shut
exit
ip route 0.0.0.0 0.0.0.0 59.62.1.2
ip access-list extended NAT
deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
permit ip 192.168.2.0 0.0.0.255 any
ip nat inside source list NAT interface gig 0/1 overload
```

Configurez le routeur WAN. Sa configuration est très simple car il suffit de configurer les adresses IP sur ses interfaces :

```
en
conf t
int gig 0/0
```

```
ip address 62.59.1.2 255.255.255.252
no shutdown
exit
int gig 0/1
ip address 59.62.1.2 255.255.255.252
no shutdown
exit
```

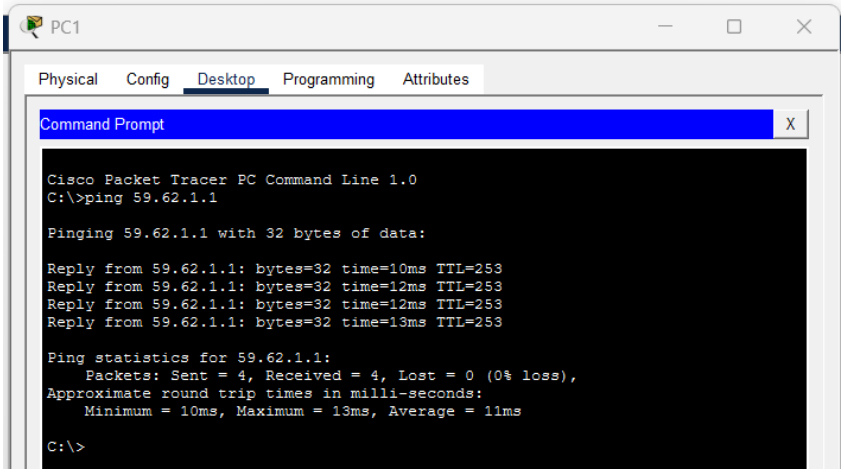
Du côté des PC, configurez PC1 avec l'IP 192.168.1.1, le masque 255.255.255.0, la passerelle 192.168.1.254 et PC2 avec l'IP 192.168.2.1, le masque 255.255.255.0, la passerelle 192.168.2.254.

4. Pourquoi les adresses IP des interfaces WAN des routeurs OC-SITE-A et OC-SITE-B appartiennent-elles à des réseaux différents ?

5. Quel est le rôle du routeur WAN dans cette architecture ?

6. Pourquoi PC1 doit-il utiliser 192.168.1.254 comme passerelle par défaut ?

Pour valider votre configuration de base, envoyez des pings depuis PC1 et PC2 vers une IP publique, vous obtenez ce résultat :




```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 62.59.1.1:6       192.168.1.1:6      59.62.1.1:6        59.62.1.1:6
icmp 62.59.1.1:7       192.168.1.1:7      59.62.1.1:7        59.62.1.1:7
icmp 62.59.1.1:8       192.168.1.1:8      59.62.1.1:8        59.62.1.1:8
icmp 62.59.1.1:9       192.168.1.1:9      59.62.1.1:9        59.62.1.1:9

Router#
```

Préparez les routeurs OC-SITE-A et OC-SITE-B pour la mise en place du VPN

Sur ces deux routeurs, entrez la commande qui va permettre d'utiliser les fonctionnalités de sécurité (IPSEC compris). Une fois cette commande entrée et validée, vous devrez enregistrer votre configuration et redémarrer les routeurs pour appliquer :

```
Router(config)#license boot module c1900 technology-package securityk9
```

Il se peut qu'il soit nécessaire de taper deux fois cette commande avant qu'elle ne fonctionne, c'est un comportement normal, nous sommes dans un simulateur, pas dans un vrai IOS.

À la demande d'acceptation, tapez yes : `ACCEPT? [yes/no] : yes`

Enregistrez votre configuration :

```
exit
copy running-config startup-config
reload
```

La configuration est exactement la même sur le OC-SITE-B :

```
license boot module c1900 technology-package securityk9
ACCEPT? [yes/no] : yes
exit
copy running-config startup-config
reload
```

7. Pourquoi doit-on activer le package de sécurité sur les routeurs Cisco 1941 ?

8. Pourquoi faut-il redémarrer les routeurs après cette activation ?

9. Le réseau peut-il continuer à fonctionner sans l'activation de ce package ? Justifiez votre réponse.

Configurez le VPN IPSEC

Vous allez configurer la phase 1 du VPN IPSEC, qui permet d'établir un canal sécurisé pour négocier le tunnel.

```
crypto isakmp policy 1
authentication pre-share
encryption aes 256
hash sha
group 5
lifetime 21600
```

Permettez-moi de vous expliquer la fonction des commandes mentionnées ci-dessus.

- `crypto isakmp policy 1` : permet de créer une politique ISAKMP qui utilise IKE pour négocier.
- `authentication pre-share` : met en place une authentification par clé prépartagée.
- `encryption aes 256` : définit l'algorithme de chiffrement utilisé pour sécuriser les échanges.
- `group 5` : définit le groupe Diffie-Hellman 5, sur 1536 bits (valeur max dans Packet tracer, on utilise de préférence le groupe 15 en 3072 bits sur un vrai routeur / firewall).
- `hash sha` : définit l'algorithme de Hachage, pour assurer l'intégrité des données (comme pour Diffie-Hellman, on ne peut pas dans Packet Tracer définir une valeur de Hash, on recommande d'utiliser SHA512 sur un vrai équipement)
- `lifetime 21600` : définit la durée de vie de l'association de sécurité ISAKMP, à la fin de ce délai, une nouvelle SA doit être établie. Notez qu'en cas de perte du correspondant, il est possible sur un vrai équipement, d'activer DPD (Dead Peer Detection). Ce mécanisme, optionnel en IKEv1 et intégré nativement en IKEv2 permet de détecter rapidement la perte du correspondant et de déclencher une renégociation ou une suppression de la SA avant expiration du délai.

10. Quel est le rôle de IKE dans un VPN IPsec ?

11. Pourquoi les paramètres de la politique ISAKMP doivent-ils être compatibles sur les deux routeurs ?

Voici une petite comparaison entre IKEv1 et IKEv2 : DPD en IKEv1 utilise des messages R-U-THERE et R-U-THERE-ACK, envoyés périodiquement si aucun trafic n'est détecté dans le tunnel. IKEv2 utilise un message vide envoyé pour tester la réactivité du correspondant, si le correspondant répond, la SA est active, sinon elle est considérée comme invalide. L'avantage de DPD avec IKEv2 : réduction du temps de détection de panne, maintien de la sécurité en supprimant les SA obsolètes et possibilité de renégociation rapide.

12. Pourquoi le mécanisme DPD est-il intéressant dans une infrastructure VPN reliant plusieurs sites distants ?

La configuration est exactement la même (**et doit être exactement la même**) sur OC-SITE-B :

```
crypto isakmp policy 1
authentication pre-share
encryption aes 256
hash sha
group 5
lifetime 21600
```

La suite de la phase 1 consiste à définir la clé pré partagée avec le correspondant :

```
crypto isakmp key OpenClassR00m$IP5ecL@b address 59.62.1.1
crypto isakmp key OpenClassR00m$IP5ecL@b address 62.59.1.1
```

Comme vous pouvez le constater, on indique la même clé sur les deux routeurs. En situation réelle, on pourrait préférer l'usage de certificats pour l'authentification. L'avantage serait de se baser sur des paires de clés asymétriques, plus difficiles à compromettre, facilement révocables (CRL), très adapté aux environnement multi sites, et disposant d'une authentification forte (vérification de la signature et de la validité du certificat). Nous ne pourrons pas l'utiliser ici en simulation.

Avant de configurer la phase 2, vous allez configurer sur OC-SITE-A et OC-SITE-B une ACL qui va permettre de définir le flux qui doit passer dans le tunnel :

SiteA
```
ip access-list extended VPN
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

SiteB
```
ip access-list extended VPN
permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Une fois les ACL VPN créées, vous allez configurer la phase 2. Commencez par créer le TRANSFORM-SET, qui va permettre de faire appel au protocole ESP, chargé de chiffrer et d'assurer l'intégrité des données qui passent dans le tunnel IPSEC :

SiteA
```
crypto ipsec transform-set OCSET esp-aes 256 esp-sha-hmac
```

SiteB
```
crypto ipsec transform-set OCSET esp-aes 256 esp-sha-hmac
```

Dans la commande ci-dessus, la même sur OC-SITE-A et OC-SITE-B, vous créez un TRANSFORM-SET nommé OCSET qui utilise ESP avec AES 256 pour le chiffrement et SHA pour l'intégrité.

Enfin, vous allez créer une CRYPTO MAP, qui est un objet qui comprend :

- Le TRANSFORM-SET
- L'ACL pour identifier le flux qui doit passer dans le VPN
- la durée de l'association de sécurité de phase 2
- l'adresse du correspondant

Avant de créer cette CRYPTO MAP, je vous propose de faire un point sur la SA :

- En phase 1, une Security Association (SA) est établie avec une durée de vie de 21600 secondes (6 heures). À son expiration, une nouvelle paire de clés Diffie-Hellman (DH) est générée, ce qui permet de réduire le risque de compromission des clés à long terme.
- En phase 2, les clés utilisées pour chiffrer et authentifier les données sont dérivées de la clé établie en phase 1. On ne refait pas un échange Diffie-Hellman complet à chaque expiration de SA de phase 2, sauf si l'option PFS (Perfect Forward Secrecy) est activée. Dans ce cas, une nouvelle clé est générée, ce qui renforce la sécurité : même si une clé est compromise, les autres sessions restent protégées. La durée de vie d'une SA de phase 2 est généralement configurée à 3600 secondes (1 heure).

Chaque correspondant IPsec génère une clé privée et une clé publique. Les correspondants échangent leurs clés publiques, puis chacun calcule localement une clé partagée à partir de sa propre clé privée et de la clé publique reçue. Cela leur permet de disposer de la même clé partagée, sans jamais l'avoir transmise sur le réseau. Ce mécanisme, connu sous le nom de Diffie-Hellman, constitue l'élément central du protocole IPsec.

Ne confondez pas la clé pré-partagée (PSK) utilisée pour l'authentification entre les correspondants (qui peut être remplacée par des certificats) avec la clé partagée Diffie-Hellman, également appelée "secret partagé". Ce sont deux mécanismes totalement différents.

Voici la configuration de la CRYPTO MAP sur OC-SITE-A et OC-SITE-B :

SiteA

```
crypto map OCMAP 10 ipsec-isakmp
set transform-set OCSET
set security-association lifetime seconds 3600
set peer 59.62.1.1
match address VPN
exit
```

SiteB

```
crypto map OCMAP 10 ipsec-isakmp
set transform-set OCSET
set security-association lifetime seconds 3600
set peer 62.59.1.1
match address VPN
exit
```

Derrière le nom donné à la CRYPTO MAP , OCMAP dans le cas présent, vous trouverez le numéro 10. Il s'agit d'un numéro de séquence, car vous ne pouvez appliquer qu'une seule CRYPTO MAP par interface, donc pour chaque VPN différent, si vous en avez plusieurs (et ce sera le cas à la suite de ce cours), vous devrez utiliser un numéro de séquence différent pour chaque VPN.

Les autres commandes sont assez explicites : vous définissez la durée de SA de phase 2 à 3600 secondes, vous appelez le TRANSFORM-SET OCSET , vous définissez l'IP du correspondant distant et vous appelez l'ACL qui permet d'identifier le flux qui peut passer dans le tunnel.

Il suffit maintenant d'appliquer cette CRYPTO MAP sur l'interfac ou se trouve votre IP publique :

SiteA
```
int gig 0/1
crypto map OCMAP
```

SiteB
```
int gig 0/1
crypto map OCMAP
```

Un message de log confirme l'activation de la CRYPTO MAP

*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

Vous voici arrivé à l'instant de vérité : faites un ping continu entre chaque PC :

```
Cisco Packet Tracer PC command Line 1.0
C:\&gt;ping -t 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time&lt;1ms TTL=126

Cisco Packet Tracer PC command Line 1.0
C:\&gt;ping -t 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time&lt;1ms TTL=126
```

Ça fonctionne ! Le VPN est établi, vous pouvez utiliser les commandes suivantes pour vérifier son fonctionnement :

SiteA
```
show crypto isakmp sa
IPv4 Crypto ISAKMP SA
```

```
dst src state conn-id slot status
59.62.1.1 62.59.1.1 QM_IDLE 1076 0 ACTIVE

SiteB
show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id slot status
62.59.1.1 59.62.1.1 QM_IDLE 1070 0 ACTIVE
```

La commande ci-dessus confirme que la phase 1 est établie (ACTIVE). QM_IDLE indique que la négociation de phase 1 est terminée.

```
OC-SITE-A#show crypto ipsec sa
interface: GigabitEthernet0/1
Crypto map tag: OCMAP, local addr 62.59.1.1
protected vrf: none
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer 59.62.1.1 port 500

PERMIT, flags={origin_is_acl,}
#pkts encaps: 688, #pkts encrypt: 688, #pkts digest: 0
#pkts decaps: 688, #pkts decrypt: 688, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

La commande ci-dessus confirme que la phase 2 est bien établie, les paquets sont bien chiffrés et déchiffrés, notez que la valeur `#pkts digest: 0` et `#pkts verify: 0` est anormal, c'est un bug connu dans Packet Tracer, un vrai IOS indiquerait ici les paquets dont l'intégrité à été vérifiée.

Félicitations, vous avez configuré votre premier VPN IPSEC en lignes de commandes !

Configurez un second VPN IPSEC

Vous allez maintenant ajouter un troisième site, le site OC-SITE-C, la topologie ressemble maintenant à ceci :

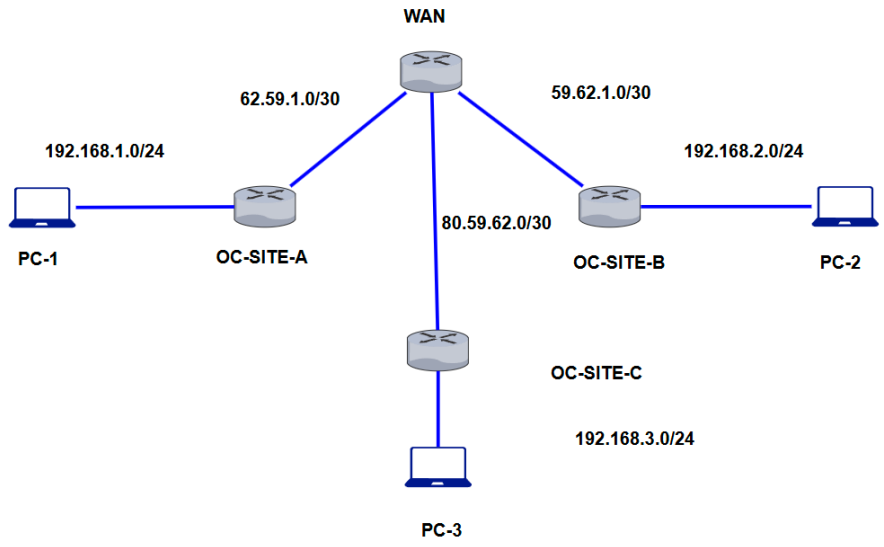
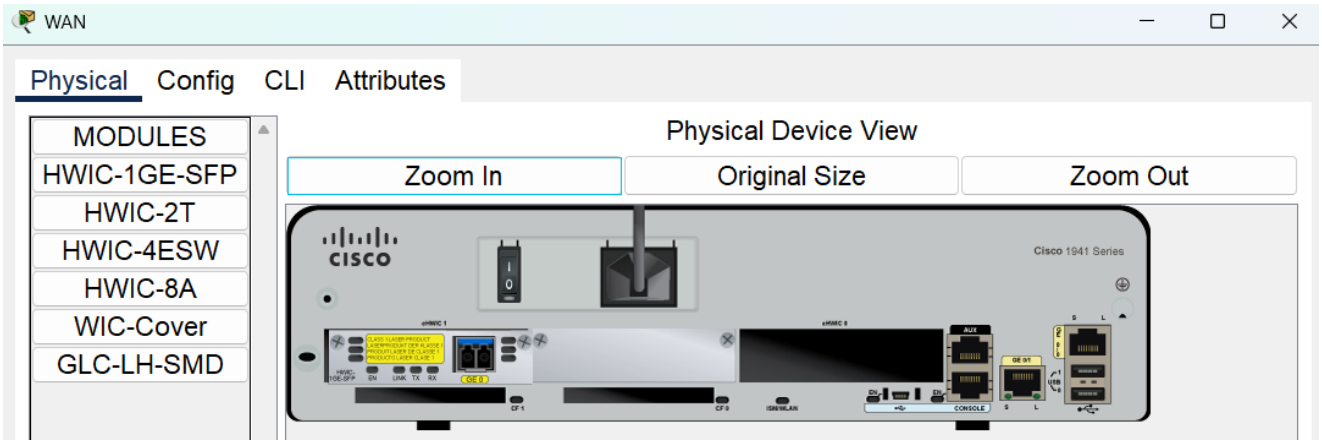


Schéma réseau avec trois sites OC-SITE-A, B et C connectés via un WAN. Chaque site relie un PC local avec des sous-réseaux privés distincts.

13. Quel est l'intérêt de relier trois sites grâce à des VPN site à site ?

14. Combien de tunnels VPN sont nécessaires dans cette architecture ?

Le routeur 1941 dispose de deux interfaces Ethernet RJ45, pour établir une connexion entre WAN et OC-SITE-C, ajoutez sur ces deux routeurs une carte HWIC-1GE-SFP dans laquelle vous ajouterez un module GLC-LH-SMD :



Interface d'un routeur Cisco 1941 dans Packet Tracer, affichant les modules physiques, ports réseau, alimentation, console et options d'extension à gauche. Ajoutez la carte HWIC-1GE-SFP, puis un module GLC-LH-SMD. Vous pourrez ensuite relier les deux routeurs en fibre optique.

Voici la configuration de base que vous allez mettre en place usr OC-SITE-C :

```
en
conf t
int gig 0/1/0
ip address 80.59.62.1 255.255.255.252
no shut
ip nat outside
exit
int gig 0/0
ip address 192.168.3.254 255.255.255.0
ip nat inside
no shut
exit
ip route 0.0.0.0 0.0.0.0 80.59.62.2
ip access-list extended NAT
deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 192.168.3.0 0.0.0.255 any
ip nat inside source list NAT interface gig 0/1/0 overload
```

Remarquez que dans l'ACL NAT, on interdit le flux du LAN 192.168.3.0/24 vers 192.168.1.0/24 et 192.168.2.0/24, ce qui est normal car ces flux doivent passer dans les VPN.

Vous allez devoir également actualiser l'ACL de NAT sur OC-SITE-A et OC-SITE-B :

SiteA
```
ip access-list extended NAT
15 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

SiteB
```
ip access-list extended NAT
15 deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
```

Vous avez sans doute remarqué un "15" avant l'ajout de l'état d'ACL. Ce 15 correspond au numéro de séquence, de base ce numéro de séquence va de 10 en 10, c'est à dire qu'à chaque fois que vous ajoutez une ligne dans votre ACL, elle a un numéro de séquence incrémenté de 10 en 10 : 10 20 30 40 etc…

Si on souhaite ajouter une séquence d'interdiction avant la séquence qui autorise tout le reste à être traduit, il faut choisir un numéro de séquence inférieur au numéro de séquence qui autorise tout le reste du flux à être traduit, ce qui donne le résultat suivant quand vous affichez l'ACL :

SiteA
```
show access-lists NAT
  Extended IP access list NAT
deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
permit ip 192.168.1.0 0.0.0.255 any
```

SiteB

```
show access-lists NAT
  Extended IP access list NAT
deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
permit ip 192.168.2.0 0.0.0.255 any
```

Comme vous pouvez le constater ci-dessus, la nouvelle séquence d'interdiction est correctement positionnée dans l'ACL.

Il faut ensuite créer les ACL dédiées à ce deuxième VPN :

SiteC
```
ip access-list extended C-TO-A
permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
exit

ip access-list extended C-TO-B
permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
exit

ip access-list extended A-TO-C
permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
ip access-list extended B-TO-C
permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
```

Activez le module SECURITY sur OC-SITE-C :

```
license boot module c1900 technology-package securityk9
```

Ensuite, configurez la première partie de la phase 1 sur OC-SITE-C, de la même façon que sur OC-SITE-A et OC-SITE-B :

SiteC
```
crypto isakmp policy 1
authentication pre-share
encryption aes 256
hash sha
group 5
lifetime 21600
```

L'étape suivante consiste à créer une clé partagée entre OC-SITE-C et OC-SITE-A et une clé partagée entre OC-SITE-C et OC-SITE-B. Vous allez également configurer la clé OC-SITE-C OC-SITE-A sur OC-SITE-A et la clé OC-SITE-C OC-SITE-B sur OC-SITE-B :

SiteC
```
crypto isakmp key OpenClassR00m$IP5ecL@bCtoA address 62.59.1.1
crypto isakmp key OpenClassR00m$IP5ecL@bCtoB address 59.62.1.1
```

SiteA
```
crypto isakmp key OpenClassR00m$IP5ecL@bCtoA address 80.59.62.1
```

SiteB
```
crypto isakmp key OpenClassR00m$IP5ecL@bCtoB address 80.59.62.1
```

Vous devez ensuite configurer le TRANSFORM-SET sur OC-SITE-C :

```
crypto ipsec transform-set OCSET esp-aes 256 esp-sha-hmac
```

Une fois cette étape réalisée, vous allez devoir créer une séquence de CRYPTO MAP sur OC-SITE-A et OC-SITE-B pour établir le VPN avec OC-SITE-C :

SiteA
```
crypto map OCMAP 20 ipsec-isakmp
set peer 80.59.62.1
set transform-set OCSET
match address A-TO-C
set security-association lifetime seconds 3600
```

SiteB
```
crypto map OCMAP 30 ipsec-isakmp
set transform-set OCSET
match address B-TO-C
set peer 80.59.62.1
set security-association lifetime seconds 3600
```

Configurez ensuite les deux numéros de séquence de CRYPTO MAP sur OC-SITE-C :

SiteC
```
crypto map OCMAP 20 ipsec-isakmp
set peer 62.59.1.1
set transform-set OCSET
match address C-TO-A
set security-association lifetime seconds 3600
exit
crypto map OCMAP 30 ipsec-isakmp
set peer 59.62.1.1
set transform-set OCSET
match address C-TO-B
set security-association lifetime seconds 3600
exit
```

Il suffit pour terminer d’appliquer la CRYPTO MAP sur l’interface gig 0/1/0 d’OC-SITE-C :

```
int gig 0/1/0
```

```
crypto map OCMAP
```

PC3 dispose de l'adresse IP 192.168.3.1, envoyez un ping vers PC1 et un ping vers PC2 depuis PC3, vous devriez obtenir ce résultat :

```
PC3> ping 192.168.1.1
 Pinging 192.168.1.1 with 32 bytes of data:
  Reply from 192.168.1.1: bytes=32 time&lt;1ms TTL=126
  Reply from 192.168.1.1: bytes=32 time=1ms TTL=126
  Reply from 192.168.1.1: bytes=32 time&lt;1ms TTL=126
  Reply from 192.168.1.1: bytes=32 time&lt;1ms TTL=126
 Ping statistics for 192.168.1.1:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC3> ping 192.168.3.1
 Pinging 192.168.3.1 with 32 bytes of data:
 Reply from 192.168.3.1: bytes=32 time=3ms TTL=128
  Reply from 192.168.3.1: bytes=32 time=4ms TTL=128
  Reply from 192.168.3.1: bytes=32 time=9ms TTL=128
  Reply from 192.168.3.1: bytes=32 time=1ms TTL=128
 Ping statistics for 192.168.3.1:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 9ms, Average = 4ms
```

Les deux VPN fonctionnent !

Vous pouvez également vérifier le fonctionnement de la phase 1 vers OC-SITE-A ainsi que la phase 1 vers OC-SITE-B :

SiteB

```
show crypto isakmp sa
  IPv4 Crypto ISAKMP SA
  dst        src         state    conn-id  slot  status
  62.59.1.1  80.59.62.1  QM_IDLE  1044     0     ACTIVE
  59.62.1.1  80.59.62.1  QM_IDLE  1049     0     ACTIVE
```

Vérifiez la phase 2 avec la commande `show crypto ipsec sa` :

Tunnel OC-SITE-C - OC-SITE-A :

```
#pkts encaps: 561, #pkts encrypt: 561
#pkts decaps: 561, #pkts decrypt
```

Tunnel OC-SITE-C - OC-SITE-B :

```
#pkts encaps: 449, #pkts encrypt: 449
#pkts decaps: 449, #pkts decrypt: 449
```

Vous venez de configurer un VPN IPSEC complet dans Cisco Packet Tracer — de la topologie réseau à l'établissement du tunnel sécurisé entre plusieurs sites. Vous avez appris à manipuler les

commandes essentielles, à comprendre les phases IKE, à sécuriser les flux, et à tester vos configurations avec rigueur.

15. Comment vérifier que les deux tunnels VPN sont opérationnels ?

16. Pourquoi est-il important de tester les communications entre les différents réseaux et pas uniquement entre deux routeurs ?

Ressources

Mettez en place un VPN IPSEC dans Cisco Packet Tracer - OpenClassrooms

CNED