

# Exemple de configuration d'ASA à ASA dynamique à statique IKEv1/IPsec

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration ASDM](#)

[Central-ASA \(homologue statique\)](#)

[Remote-ASA \(homologue dynamique\)](#)

[Configuration CLI](#)

[Configuration ASA centrale \(homologue statique\)](#)

[Remote-ASA \(homologue dynamique\)](#)

[Vérification](#)

[ASA central](#)

[Remote-ASA](#)

[Dépannage](#)

[Remote-ASA \(initiateur\)](#)

[Central-ASA \(répondeur\)](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment permettre à l'appliance de sécurité adaptative (ASA) d'accepter des connexions VPN site à site IPsec dynamiques de n'importe quel homologue dynamique (ASA dans ce cas). Comme le montre le diagramme de réseau de ce document, le tunnel IPsec est établi lorsque le tunnel est initié à partir de la fin Remote-ASA uniquement. Le Central-ASA ne peut pas initier de tunnel VPN en raison de la configuration dynamique IPsec. L'adresse IP de Remote-ASA est inconnue.

Configurez Central-ASA afin d'accepter dynamiquement les connexions à partir d'une adresse IP générique (0.0.0.0/0) et d'une clé pré-partagée générique. Remote-ASA est ensuite configuré pour chiffrer le trafic des sous-réseaux locaux vers Central-ASA comme spécifié par la liste d'accès de chiffrement. Les deux côtés procèdent à l'exemption NAT (Network Address Translation) afin de contourner NAT pour le trafic IPsec.

## Conditions préalables

## Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

## Components Used

Les informations de ce document sont basées sur le logiciel pare-feu Cisco ASA (5510 et 5520) version 9.x et ultérieure.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configuration

**Note:** Utilisez l'[Outil de recherche de commande \(clients inscrits seulement\) pour obtenir plus d'informations sur les commandes utilisées dans cette section.](#)

## Diagramme du réseau

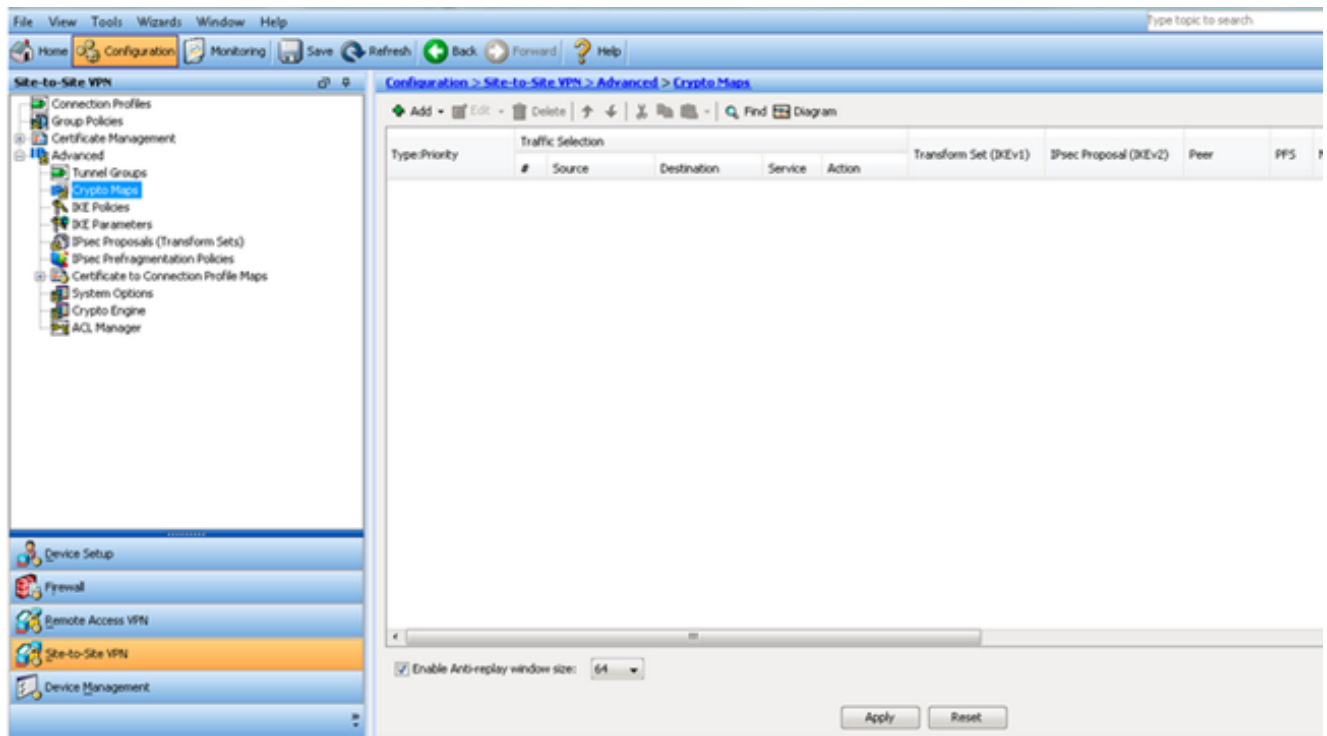


## Configuration ASDM

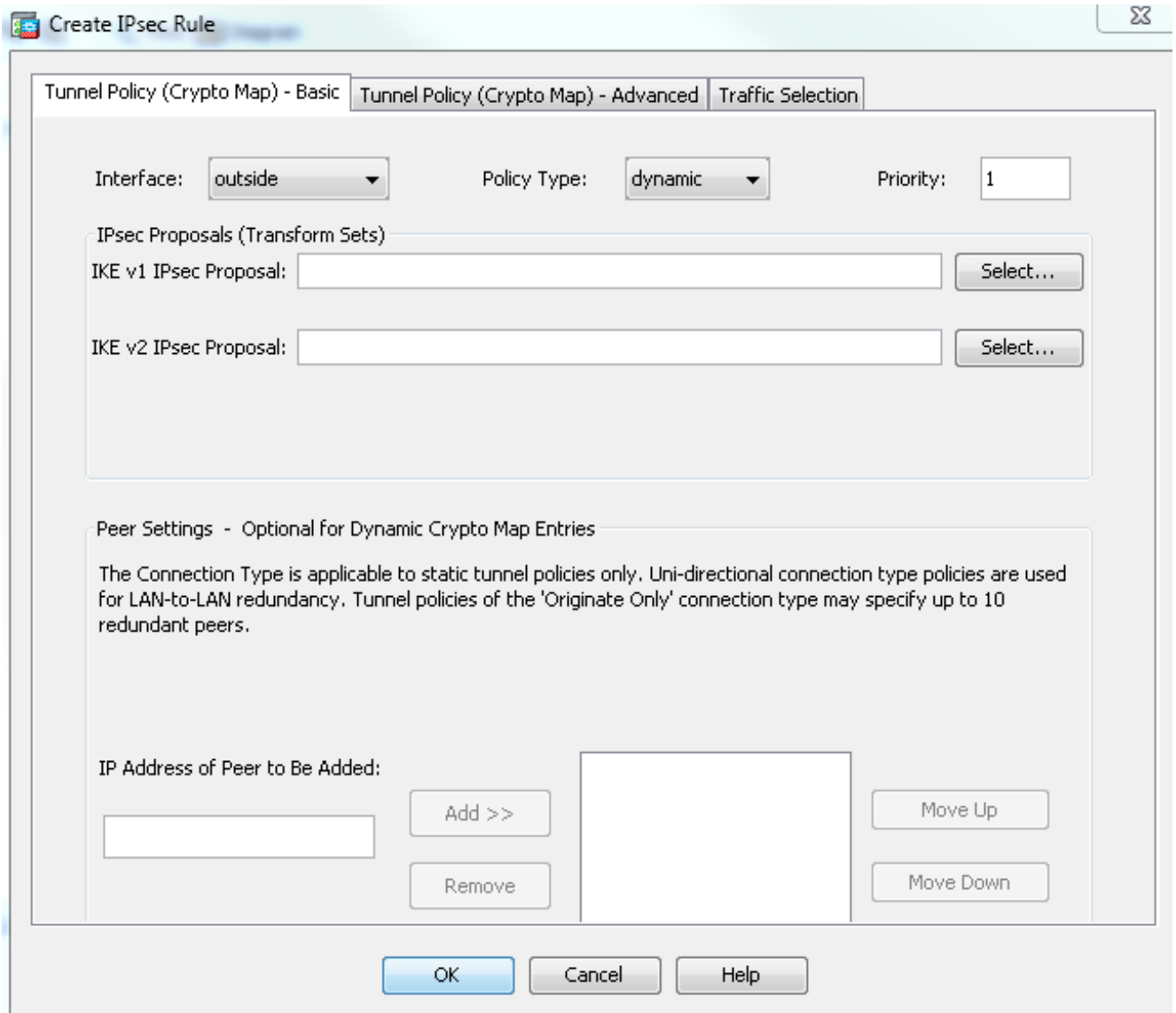
### Central-ASA (homologue statique)

Sur un ASA avec une adresse IP statique, configurez le VPN de telle manière qu'il accepte les connexions dynamiques d'un homologue inconnu alors qu'il authentifie toujours l'homologue à l'aide d'une clé pré-partagée IKEv1 :

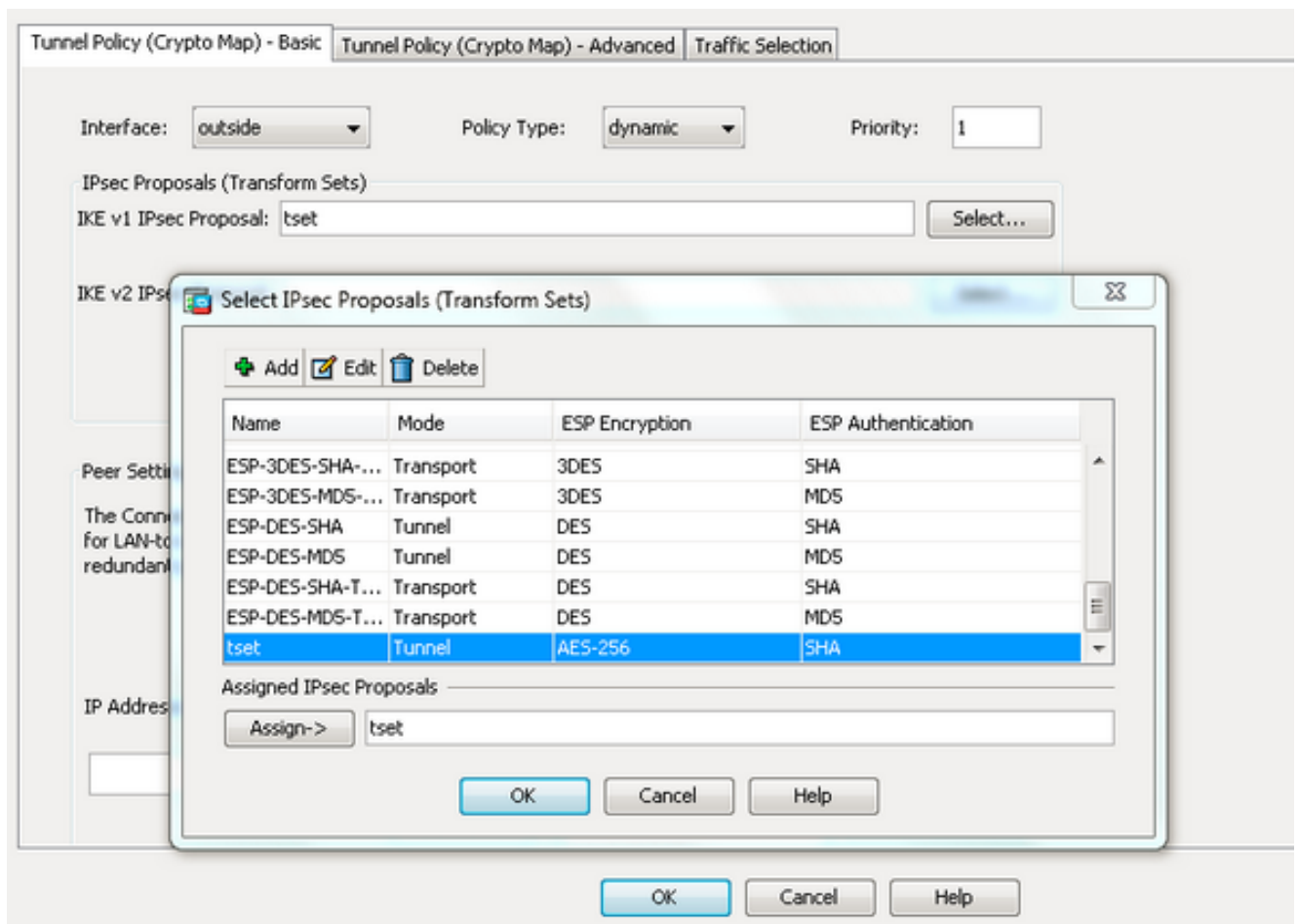
1. Choisissez **Configuration > Site-to-Site VPN > Advanced > Crypto Maps**. La fenêtre affiche la liste des entrées de crypto-carte déjà en place (s'il y en a). Comme ASA ne sait pas quelle est l'adresse IP homologue, pour que ASA accepte la connexion, configurer **Dynamic-map** avec jeu de transformation correspondant (proposition IPsec). Cliquez sur **Add**.



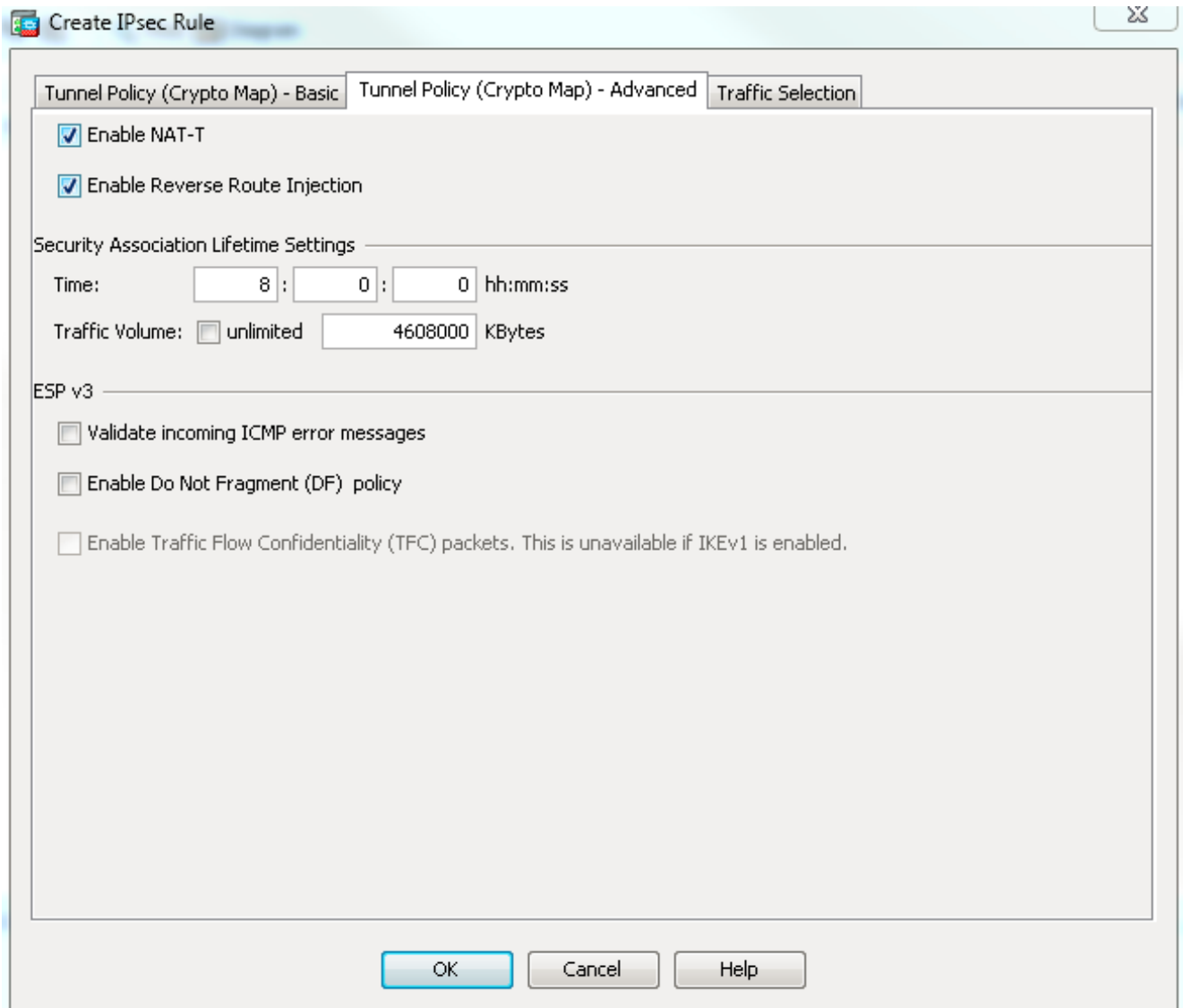
2. Dans la fenêtre Créer une règle IPsec, dans l'onglet Stratégie de tunnel (Crypto Map) - Basic, choisissez **en dehors** de la liste déroulante Interface et **dynamique** dans la liste déroulante Type de stratégie. Dans le champ Priorité, affectez la priorité de cette entrée en cas de plusieurs entrées sous Dynamic-Map. Ensuite, cliquez sur **Sélectionner** en regard du champ Proposition IPsec IKE v1 afin de sélectionner la proposition IPsec.



3. Lorsque la boîte de dialogue Sélectionner les propositions IPsec (Jeux de transformations) s'ouvre, choisissez parmi les propositions IPsec actuelles ou cliquez sur **Ajouter** afin de créer une nouvelle proposition et d'utiliser la même. Cliquez sur **OK** lorsque vous avez terminé.



4. Dans l'onglet Tunnel Policy (Crypto Map)-Advanced, cochez la case **Enable NAT-T** (obligatoire si l'un des homologues est derrière un périphérique NAT) et la case **Enable Reverse Route Injection (Activer l'injection de route inverse)**. Lorsque le tunnel VPN apparaît pour l'homologue dynamique, ASA installe une route dynamique pour le réseau VPN distant négocié qui pointe vers l'interface VPN.



Éventuellement, dans l'onglet Traffic Selection, vous pouvez également définir le trafic VPN intéressant pour l'homologue dynamique et cliquer sur **OK**.

Tunnel Policy (Crypto Map) - Basic | Tunnel Policy (Crypto Map) - Advanced | **Traffic Selection**

Action:  Protect  Do not Protect

Source Criteria

Source: any4

Destination Criteria

Destination: any4

Service: ip

Description:

**More Options**

Enable Rule

Source Service: (TCP or UDP service only) ⓘ

Time Range:

OK

Cancel

Help

**Configuration > Site-to-Site VPN > Advanced > Crypto Maps**

+ Add | Edit | Delete | ↑ ↓ | Copy | Paste | Find | Diagram

Type:Priority	Traffic Selection					Transform Set (IKEv1)
	#	Source	Destination	Service	Action	
[-] interface: outside						
dynamic: 65535.1	1	any4	any4	IP ip	Protect	tset

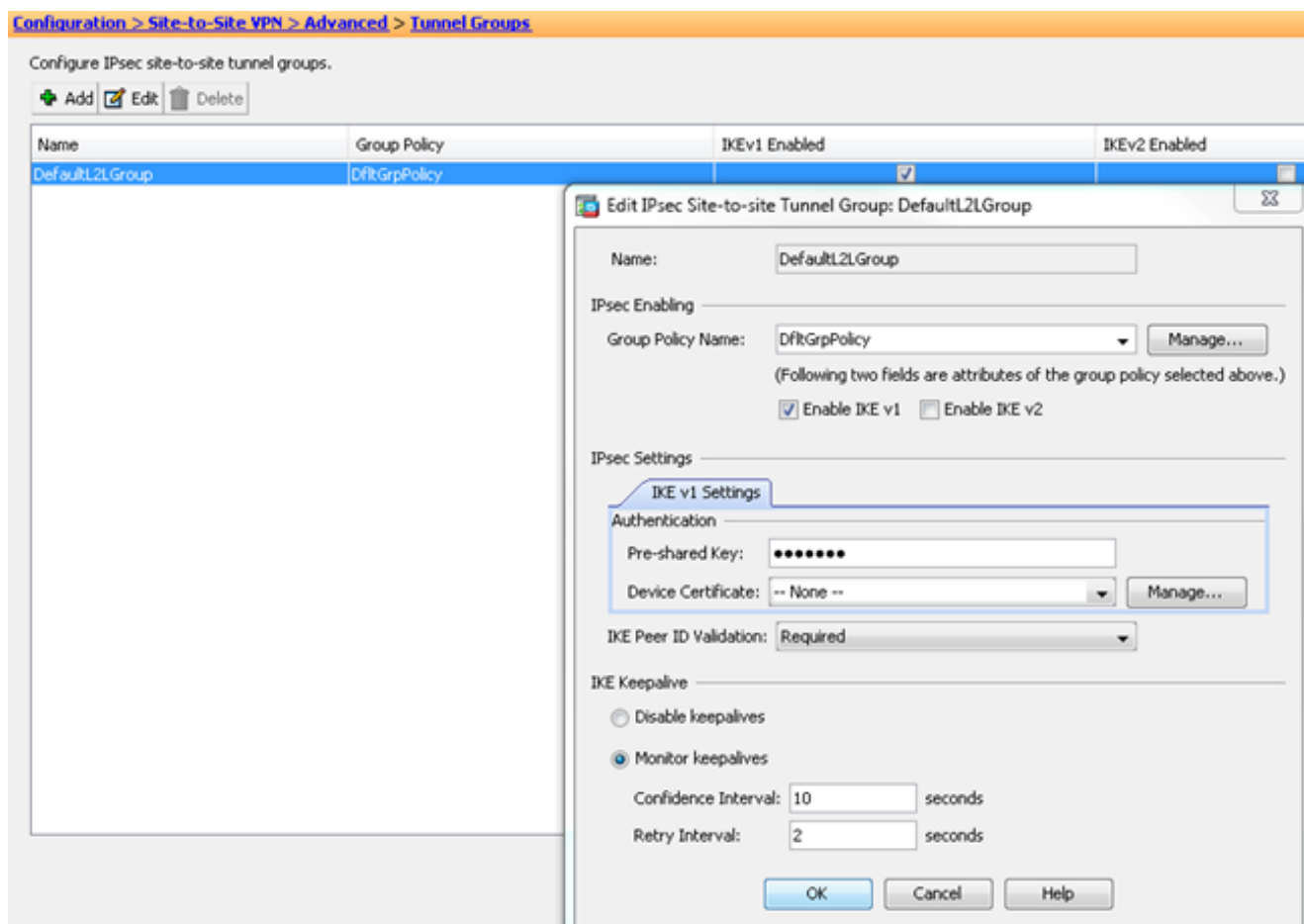
Enable Anti-replay window size: 64

Apply Reset

Comme indiqué précédemment, comme ASA ne dispose d'aucune information sur l'adresse IP d'homologue dynamique distante, la demande de connexion inconnue se trouve sous DefaultL2LGroup qui existe par défaut sur ASA. Pour que l'authentification réussisse, la clé pré-partagée (cisco123 dans cet exemple) configurée sur l'homologue distant doit correspondre à une clé sous DefaultL2LGroup.

5. Choisissez **Configuration > Site-to-Site VPN > Advanced > Tunnel Groups**, sélectionnez **DefaultL2LGroup**, cliquez sur **Edit** et configurez la clé pré-partagée souhaitée. Cliquez sur **OK** lorsque vous avez terminé.





**Note:** Ceci crée une clé pré-partagée générique sur l'homologue statique (Central-ASA). Tout périphérique/homologue qui connaît cette clé pré-partagée et ses propositions correspondantes peut établir un tunnel VPN et accéder aux ressources via VPN. Assurez-vous que cette clé pré-parée n'est pas partagée avec des entités inconnues et n'est pas facile à deviner.

6. Choisissez **Configuration > VPN site à site > Stratégies de groupe** et sélectionnez la stratégie de groupe de votre choix (dans ce cas, la stratégie de groupe par défaut). Cliquez sur **Modifier** et modifiez la stratégie de groupe dans la boîte de dialogue Modifier la stratégie de groupe interne. Cliquez sur **OK** lorsque vous avez **terminé**.

**Configuration > Site-to-Site VPN > Group Policies**

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. Policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an [LDAP attribute map](#).

Add Edit Delete Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
DfltGrpPolicy (System Default)	Internal	ikev1;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultWEBVPNGroup;

**Edit Internal Group Policy: DfltGrpPolicy**

Name:

Tunneling Protocols:  Clientless SSL VPN  SSL VPN Client  IPsec IKEv1  IPsec IKEv2  L2TP/IPsec

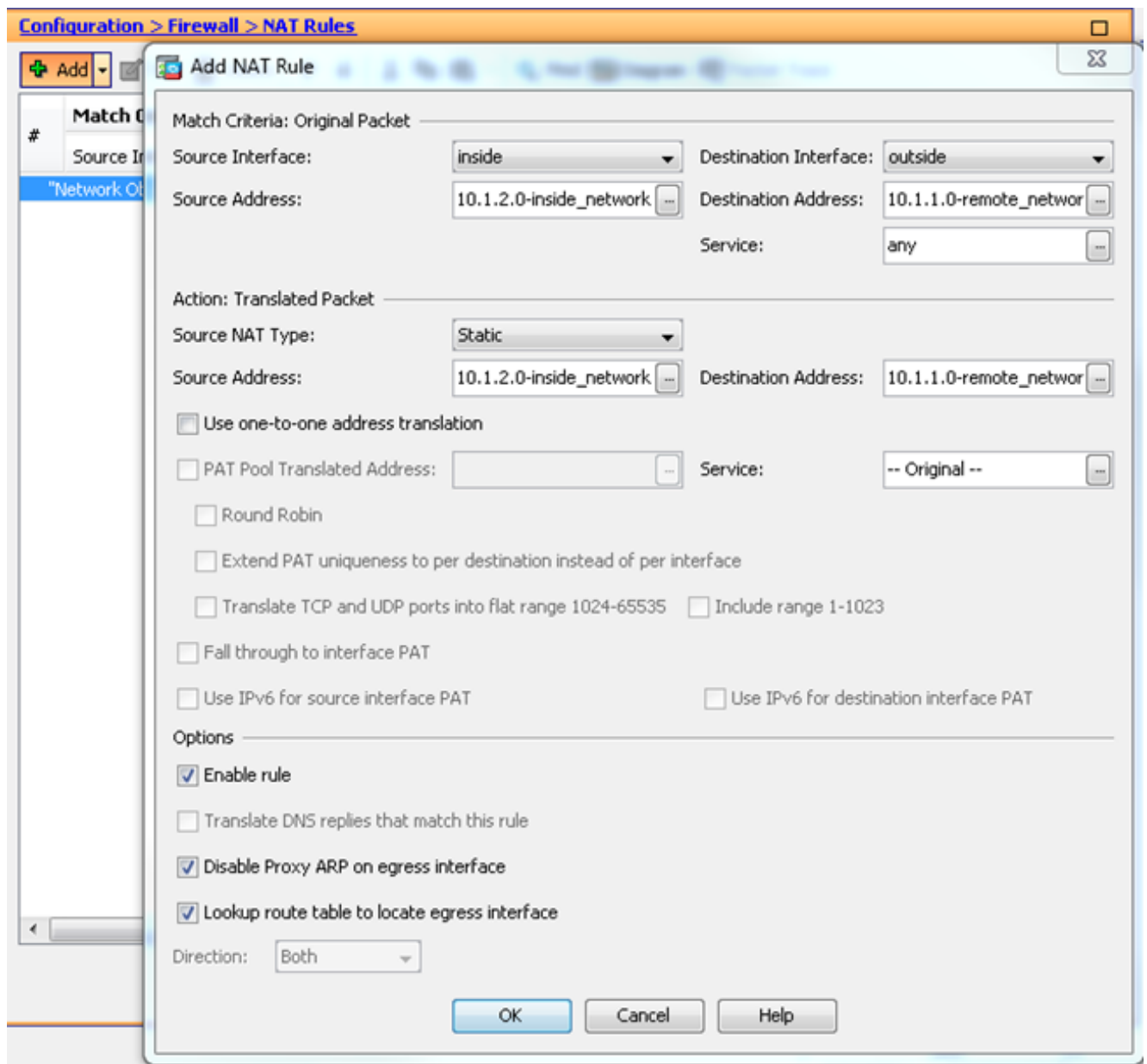
Filter:

Idle Timeout:  Unlimited  minutes

Maximum Connect Time:  Unlimited  minutes

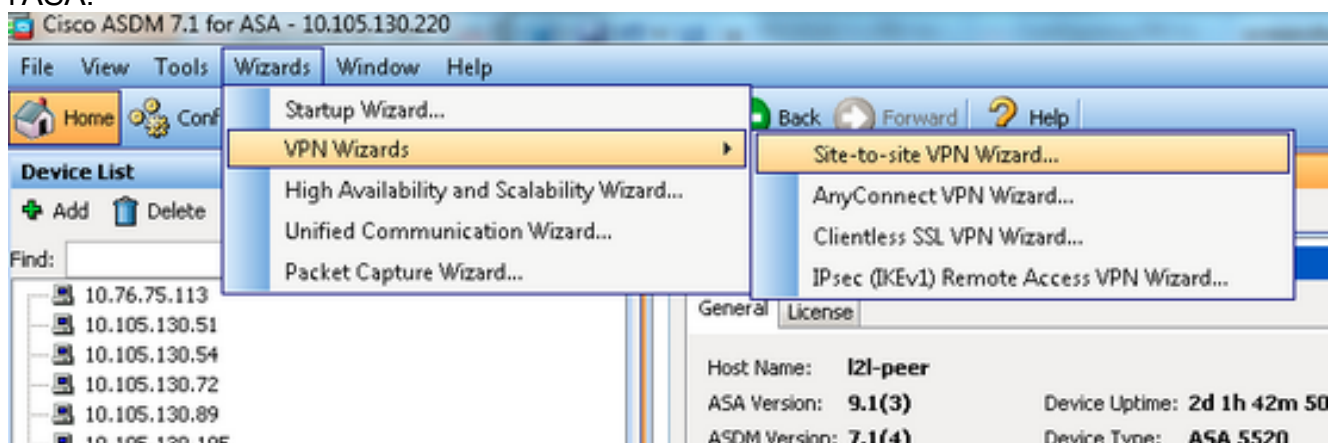
Find:     Match Case

7. Choisissez **Configuration > Firewall > NAT Rules** et dans la fenêtre Add Nat Rule, configurez une règle no nat (NAT-EXEMPT) pour le trafic VPN. Cliquez sur **OK** lorsque vous avez terminé.



## Remote-ASA (homologue dynamique)


1. Choisissez **Wizards > VPN Wizards > Site-to-site VPN Wizard** une fois que l'application ASDM se connecte à l'ASA.



2. Cliquez sur **Next (Suivant)**.


Site-to-site VPN Connection Setup Wizard

### VPN Wizard



**Introduction**

Use this wizard to setup new site-to-site VPN tunnel. A tunnel between two devices is called a site-to-site tunnel and is bidirectional protects the data using the IPsec protocol.



Here is a [video](#) on how to setup a site-to-site VPN connection.

< Back   Next >

3. Choisissez **outside** dans la liste déroulante VPN Access Interface afin de spécifier l'adresse IP externe de l'homologue distant. Sélectionnez l'interface (**WAN**) où la carte de chiffrement est appliquée. Cliquez sur **Next** (Suivant).

Site-to-site VPN Connection Setup Wizard

### Peer Device Identification

This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.

Peer IP Address:

VPN Access Interface:

< Back   Next >

4. Spécifiez les hôtes/réseaux qui doivent être autorisés à traverser le tunnel VPN. Au cours de cette étape, vous devez fournir les réseaux locaux et distants pour le tunnel VPN. Cliquez sur les boutons en regard des champs Local Network (Réseau local) et Remote Network (Réseau distant) et sélectionnez l'adresse selon les besoins. Cliquez sur **Suivant** lorsque

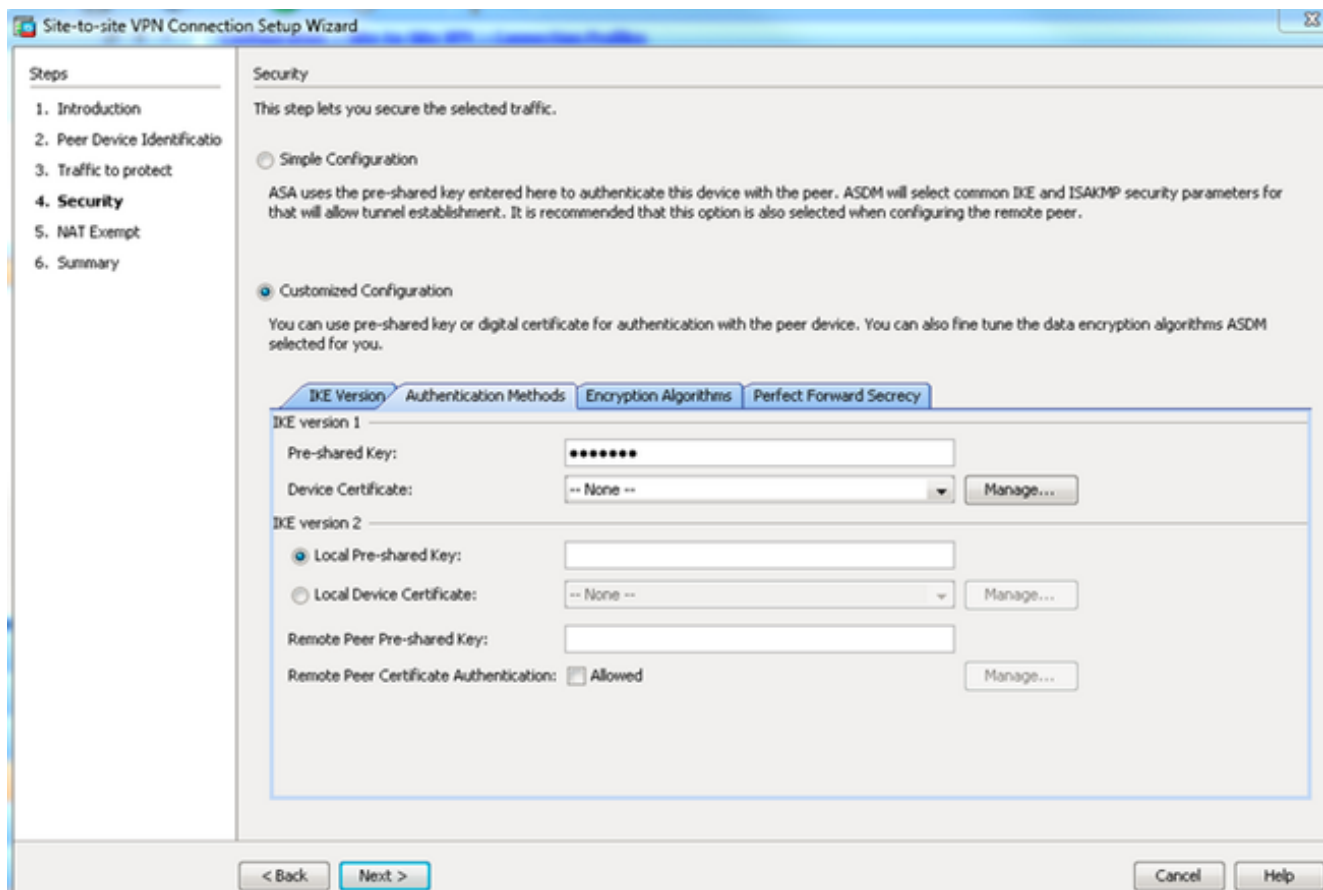
vous avez  
terminé.

The screenshot shows the 'Site-to-site VPN Connection Setup Wizard' window. On the left, a 'Steps' sidebar lists: 1. Introduction, 2. Peer Device Identification, 3. Traffic to protect (highlighted), 4. Security, 5. NAT Exempt, and 6. Summary. The main area is titled 'Traffic to protect' and contains the text: 'This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.' Below this, there are two radio buttons for 'IP Address Type': 'IPv4' (selected) and 'IPv6'. There are two text input fields: 'Local Network:' with the value '10.1.1.0/24' and 'Remote Network:' with the value '10.1.2.0/24'. At the bottom, there are '< Back' and 'Next >' buttons.

5. Entrez les informations d'authentification à utiliser, qui sont des clés pré-partagées dans cet exemple. La clé pré-partagée utilisée dans cet exemple est cisco123. Le nom du groupe de tunnels est l'adresse IP d'homologue distant par défaut si vous configurez le VPN LAN à LAN (L2L).

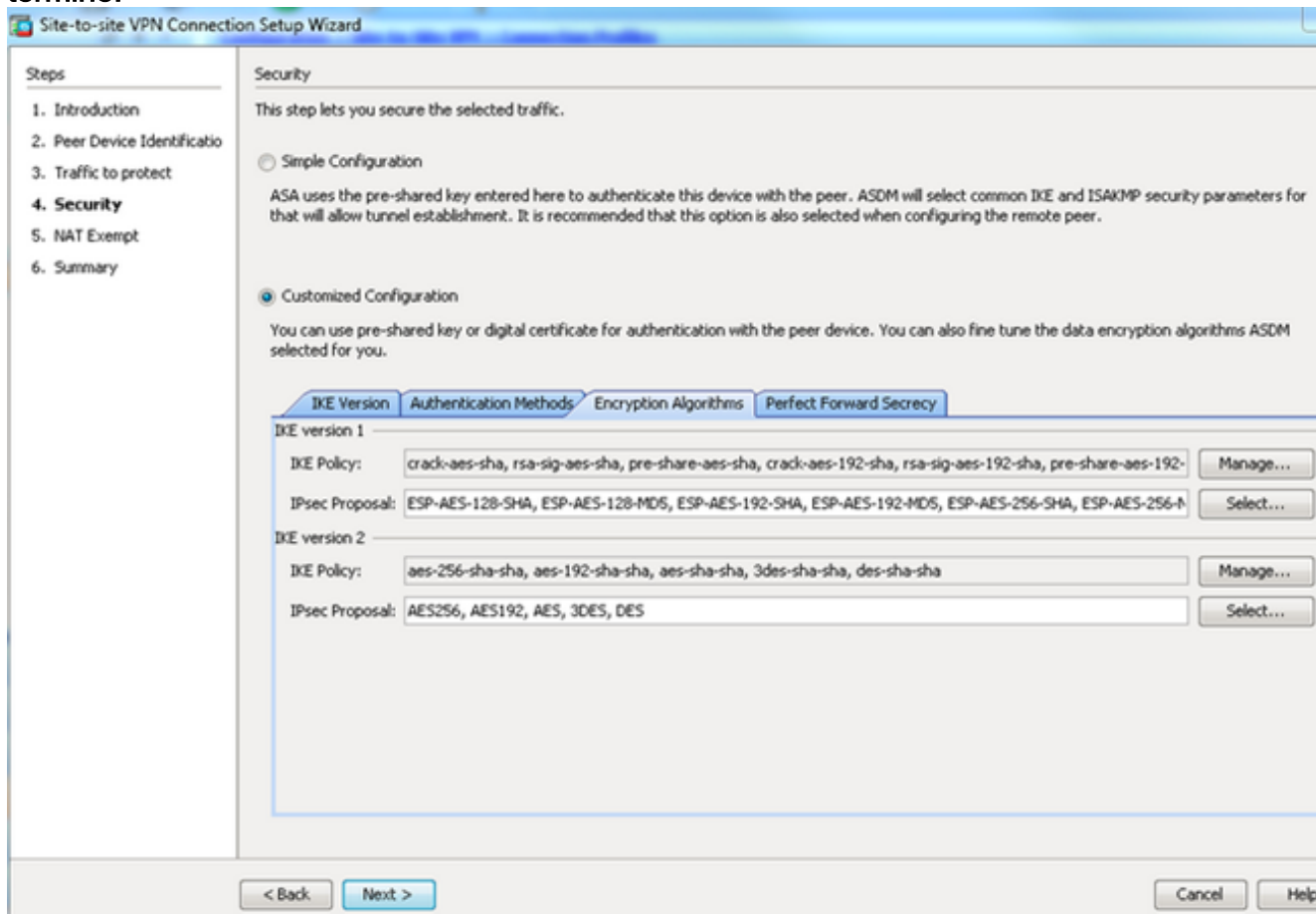
The screenshot shows the 'Site-to-site VPN Connection Setup Wizard' window at Step 4: Security. The 'Steps' sidebar on the left highlights '4. Security'. The main area is titled 'Security' and contains the text: 'This step lets you secure the selected traffic.' There are two radio buttons: 'Simple Configuration' (selected) and 'Customized Configuration'. Below 'Simple Configuration', there is a text input field for 'Pre-shared Key:' containing seven dots. Below 'Customized Configuration', there is explanatory text: 'You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.' At the bottom, there are '< Back', 'Next >', 'Cancel', and 'Help' buttons.

OU Vous pouvez personnaliser la configuration pour inclure la stratégie IKE et IPsec de votre choix. Il doit y avoir au moins une stratégie correspondante entre les homologues : Dans l'onglet Authentication Methods, saisissez la clé pré-partagée IKE version 1 dans le champ Pre-shared Key. Dans cet exemple, il s'agit de cisco123.



Cliquez sur l'onglet **Encryption Algorithms**.

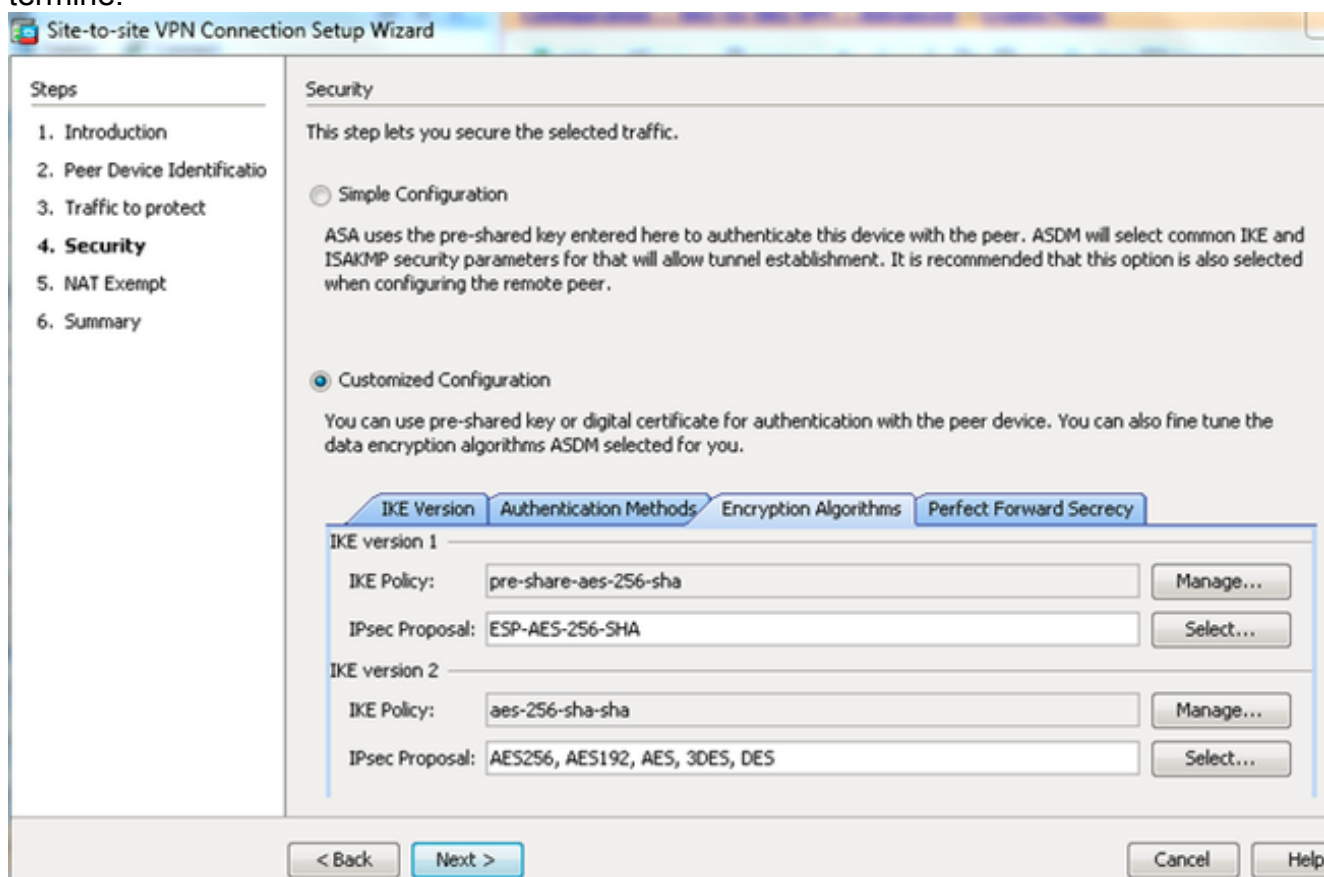
6. Cliquez sur **Manage** en regard du champ IKE Policy, cliquez sur **Add** et configurez une stratégie IKE personnalisée (phase-1). Cliquez sur **OK** lorsque vous avez terminé.



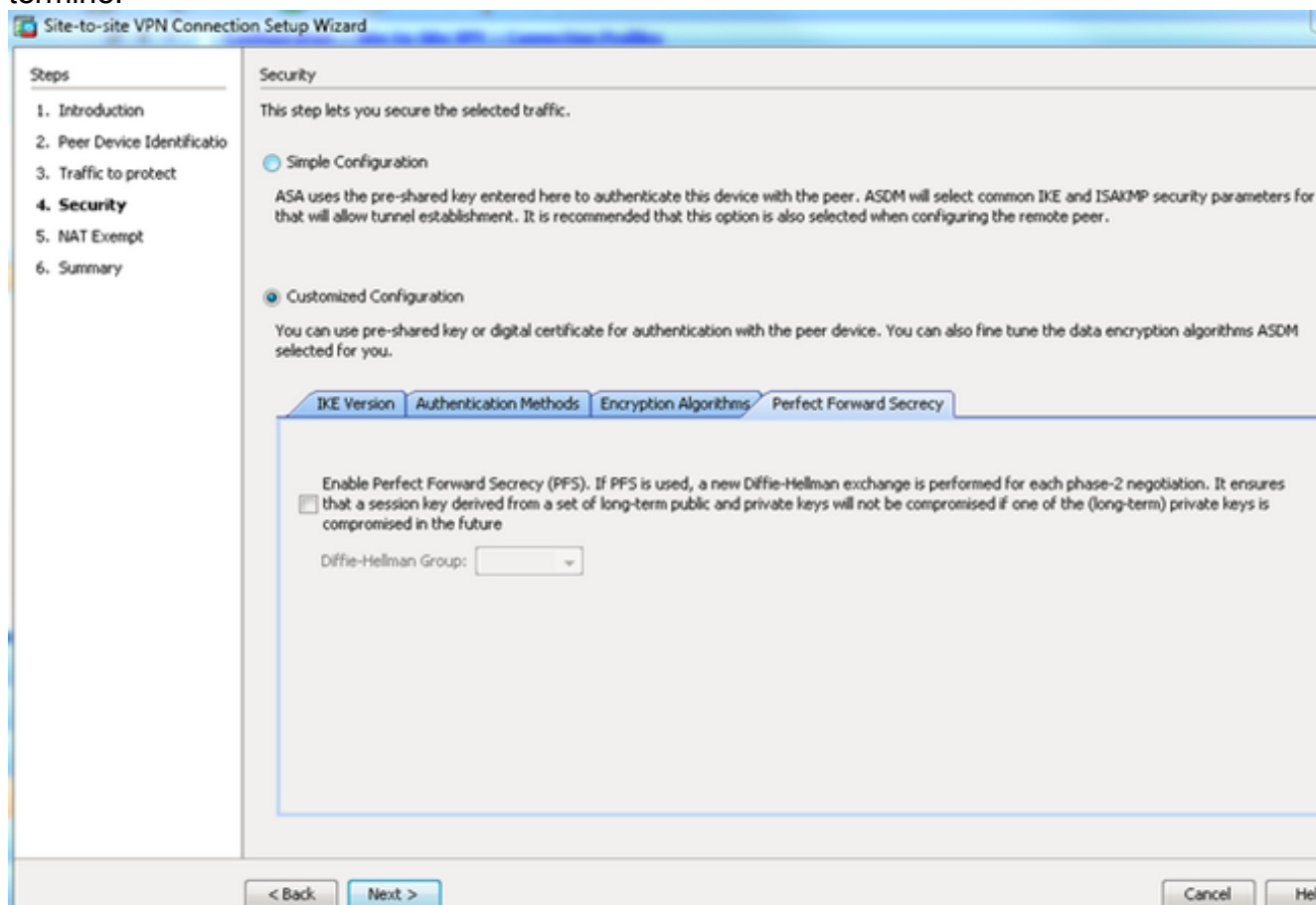
7. Cliquez sur **Sélectionner** en regard du champ Proposition IPsec et sélectionnez la



proposition IPsec souhaitée. Cliquez sur **Suivant** lorsque vous avez terminé.



Vous pouvez également accéder à l'onglet Perfect Forward Secrecy et cocher la case **Enable Perfect Forward Secrecy (PFS)**. Cliquez sur **Suivant** lorsque vous avez terminé.



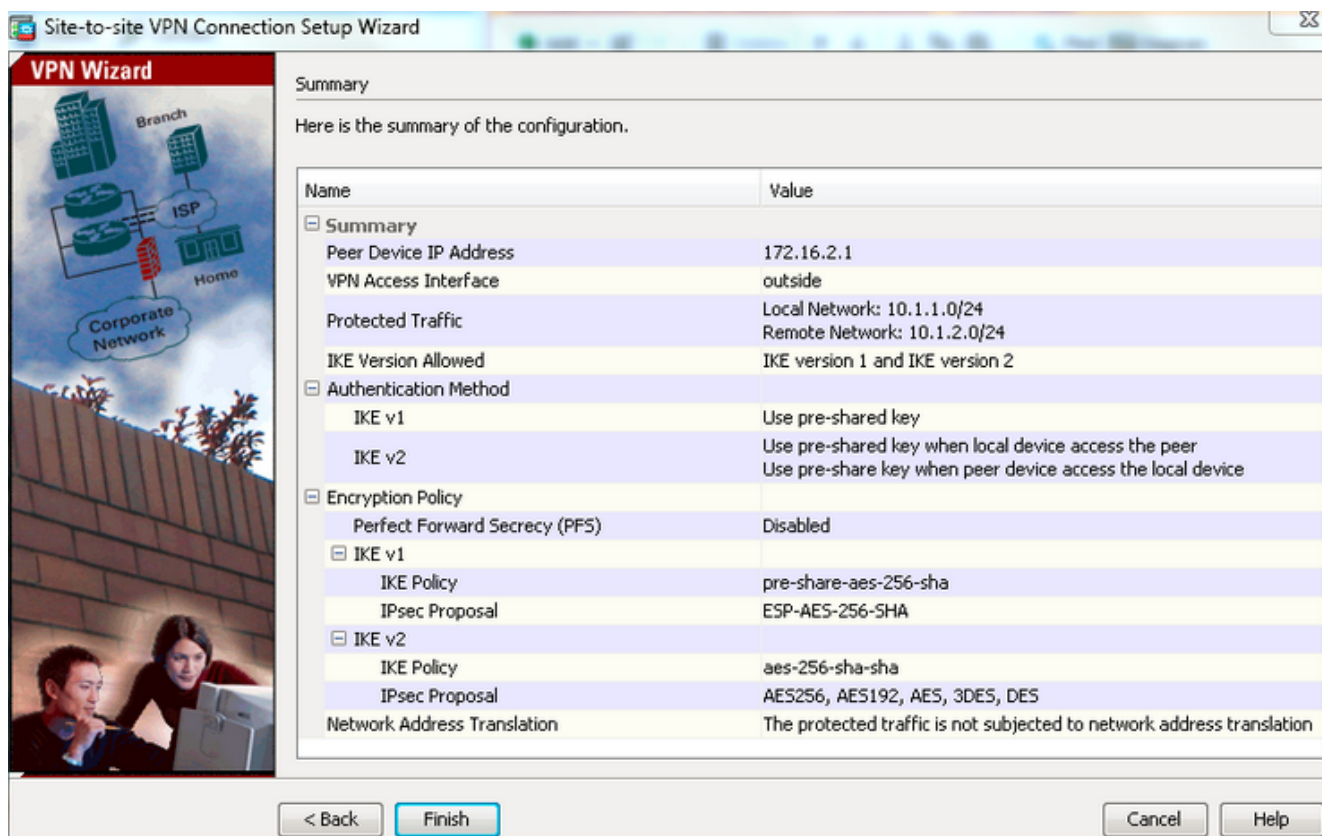
8. Cochez la case **Exempter l'hôte/le réseau côté ASA de la traduction d'adresses** afin

d'empêcher le trafic du tunnel du début de la traduction d'adresses réseau. Choisissez **local** ou **inside** dans la liste déroulante afin de définir l'interface à laquelle le réseau local est accessible. Cliquez sur **Next** (Suivant).

The screenshot shows the 'Site-to-site VPN Connection Setup Wizard' window. On the left, a 'Steps' pane lists the following steps: 1. Introduction, 2. Peer Device Identificatio, 3. Traffic to protect, 4. Security, 5. NAT Exempt (highlighted), and 6. Summary. The main area is titled 'NAT Exempt' and contains the text: 'This step allows you to exempt the local network addresses from network translation.' Below this text is a checked checkbox labeled 'Exempt ASA side host/network from address translation' and a dropdown menu currently set to 'inside'. At the bottom of the window, there are two buttons: '< Back' and 'Next >'. The 'Next >' button is highlighted with a blue border.

9. ASDM affiche un résumé du VPN qui vient d'être configuré. Vérifiez et cliquez sur **Terminer**.





## Configuration CLI

### Configuration ASA centrale (homologue statique)

1. Configurez une règle NO-NAT/NAT-EXEMPT pour le trafic VPN comme le montre cet exemple :

```
object network 10.1.1.0-remote_network
subnet 10.1.1.0 255.255.255.0
```

```
object network 10.1.2.0-inside_network
subnet 10.1.2.0 255.255.255.0
```

```
nat (inside,outside) source static 10.1.2.0-inside_network 10.1.2.0-inside_network
destination static 10.1.1.0-remote_network 10.1.1.0-remote_network
no-proxy-arp route-lookup
```

2. Configurez la clé pré-partagée sous DefaultL2LGroup afin d'authentifier tout homologue Dynamic-L2L distant :

```
tunnel-group DefaultL2LGroup ipsec-attributes
ikev1 pre-shared-key cisco123
```

3. Définissez la stratégie Phase-2/ISAKMP :

```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```

4. Définissez le jeu de transformation de phase 2/la stratégie IPsec :

```
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
```

5. Configurez la carte dynamique avec les paramètres suivants : Ensemble de transformation requis Activer l'injection de route inverse (RRI), qui permet au dispositif de sécurité d'apprendre les informations de routage pour les clients connectés (facultatif)

```
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set tset
crypto dynamic-map outside_dyn_map 1 set reverse-route
```

6. Liez la carte dynamique à la carte de chiffrement, appliquez la carte de chiffrement et activez ISAKMP/IKEv1 sur l'interface externe :

```
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

crypto map outside_map interface outside
crypto ikev1 enable outside
```

## Remote-ASA (homologue dynamique)

1. Configurez une règle d'exemption NAT pour le trafic VPN :

```
object network 10.1.1.0-inside_network
subnet 10.1.1.0 255.255.255.0
```

```
object network 10.1.2.0-remote_network
subnet 10.1.2.0 255.255.255.0
```

```
nat (inside,outside) source static 10.1.1.0-inside_network 10.1.1.0-inside_network
destination static 10.1.2.0-remote_network 10.1.2.0-remote_network
no-proxy-arp route-lookup
```

2. Configurez un groupe de tunnels pour un homologue VPN statique et une clé pré-partagée.

```
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
ikev1 pre-shared-key cisco123
```

3. Définissez la stratégie PHASE-1/ISAKMP :

```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```

4. Définissez un jeu de transformation de phase 2/une stratégie IPsec :

```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```

5. Configurez une liste d'accès qui définit le trafic/réseau VPN intéressant :

```
access-list outside_cryptomap extended permit ip object
10.1.1.0-inside_network object 10.1.2.0-remote_network
```

6. Configurez la carte de chiffrement statique avec les paramètres suivants : Liste d'accès Crypto/VPN Adresse IP homologue IPsec distante Ensemble de transformation requis

```
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set peer 172.16.2.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-256-SHA
```

7. Appliquez la carte de chiffrement et activez ISAKMP/IKEv1 sur l'interface externe :

```
crypto map outside_map interface outside
crypto ikev1 enable outside
```

## Vérification

Utilisez cette section pour confirmer que la configuration fonctionne correctement.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

- **show crypto isakmp sa** - Affiche toutes les associations de sécurité IKE (SA) actuelles sur un homologue.

- **show crypto ipsec sa** - Affiche toutes les SA IPsec actuelles.

Cette section présente un exemple de sortie de vérification pour les deux ASA.

## ASA central

```
Central-ASA#show crypto isakmp sa
```

```
IKEv1 SAs:
```

```
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: 172.16.1.1
```

```
Type      : L2L           Role       : responder
```

```
Rekey     : no           State      : MM_ACTIVE
```

```
Central-ASA# show crypto ipsec sa
```

```
interface: outside
```

```
Crypto map tag: outside_dyn_map, seq num: 1, local addr: 172.16.2.1
```

```
local ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
```

```
current_peer: 172.16.1.1
```

```
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
```

```
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
```

```
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
```

```
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

```
#TFC rcvd: 0, #TFC sent: 0
```

```
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
```

```
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
```

```
path mtu 1500, ipsec overhead 74(44), media mtu 1500
```

```
PMTU time remaining (sec): 0, DF policy: copy-df
```

```
ICMP error validation: disabled, TFC packets: disabled
```

```
current outbound spi: 30D071C0
```

```
current inbound spi : 38DA6E51
```

```
inbound esp sas:
```

```
spi: 0x38DA6E51 (953839185)
```

```
transform: esp-aes-256 esp-sha-hmac no compression
```

```
in use settings ={L2L, Tunnel, IKEv1, }
```

```
slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
```

```
sa timing: remaining key lifetime (kB/sec): (3914999/28588)
```

```
IV size: 16 bytes
```

```
replay detection support: Y
```

```
Anti replay bitmap:
```

```
0x00000000 0x0000001F
```

```
outbound esp sas:
```

```
spi: 0x30D071C0 (818966976)
```

```
transform: esp-aes-256 esp-sha-hmac no compression
```

```
in use settings ={L2L, Tunnel, IKEv1, }
```

```
slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
```

```
sa timing: remaining key lifetime (kB/sec): (3914999/28588)
```

```
IV size: 16 bytes
```

```
replay detection support: Y
```

Anti replay bitmap:  
0x00000000 0x00000001

## Remote-ASA

Remote-ASA#**show crypto isakmp sa**

IKEv1 SAs:

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: **172.16.2.1**  
Type : L2L Role : **initiator**  
Rekey : no State : **MM\_ACTIVE**

Remote-ASA#**show crypto ipsec sa**

interface: outside

Crypto map tag: **outside\_map**, seq num: 1, local addr: 172.16.1.1

access-list outside\_cryptomap extended permit ip 10.1.1.0  
255.255.255.0 10.1.2.0 255.255.255.0  
**local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)**  
**remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)**  
current\_peer: 172.16.2.1

**#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4**  
**#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4**  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0  
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0  
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0  
#TFC rcvd: 0, #TFC sent: 0  
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0  
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0  
path mtu 1500, ipsec overhead 74(44), media mtu 1500  
PMTU time remaining (sec): 0, DF policy: copy-df  
ICMP error validation: disabled, TFC packets: disabled  
current outbound spi: 38DA6E51  
current inbound spi : 30D071C0

**inbound esp sas:**

**spi: 0x30D071C0 (818966976)**  
transform: esp-aes-256 esp-sha-hmac no compression  
in use settings ={L2L, Tunnel, IKEv1, }  
slot: 0, conn\_id: 8192, crypto-map: outside\_map  
sa timing: remaining key lifetime (kB/sec): (4373999/28676)  
IV size: 16 bytes  
replay detection support: Y  
Anti replay bitmap:  
0x00000000 0x0000001F

**outbound esp sas:**

**spi: 0x38DA6E51 (953839185)**  
transform: esp-aes-256 esp-sha-hmac no compression  
in use settings ={L2L, Tunnel, IKEv1, }  
slot: 0, conn\_id: 8192, crypto-map: outside\_map  
sa timing: remaining key lifetime (kB/sec): (4373999/28676)  
IV size: 16 bytes

```
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

**Note:** Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Servez-vous de ces commandes comme montré :

```
clear crypto ikev1 sa <peer IP address>
Clears the Phase 1 SA for a specific peer.
```

**Attention :** La commande **clear crypto isakmp sa** est intrusive car elle efface tous les tunnels VPN actifs.

Dans le logiciel PIX/ASA version 8.0(3) et ultérieure, une SA IKE individuelle peut être effacée à l'aide de la commande **clear crypto isakmp sa <peer ip address>**. Dans les versions logicielles antérieures à la version 8.0(3), utilisez la commande [vpn-sessiondb logoff tunnel-group <tunnel-group-name>](#) afin d'effacer les SA IKE et IPsec pour un seul tunnel.

```
Remote-ASA#vpn-sessiondb logoff tunnel-group 172.16.2.1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1
```

```
clear crypto ipsec sa peer <peer IP address>
!!! Clears the required Phase 2 SA for specific peer.
debug crypto condition peer < Peer address>
!!! Set IPsec/ISAKMP debug filters.
debug crypto isakmp sa <debug level>
!!! Provides debug details of ISAKMP SA negotiation.
debug crypto ipsec sa <debug level>
!!! Provides debug details of IPsec SA negotiations
undebug all
!!! To stop the debugs
```

Débogues utilisés :

```
debug cry condition peer <remote peer public IP>
debug cry ikev1 127
debug cry ipsec 127
```

## Remote-ASA (initiateur)

Entrez cette commande **packet-tracer** afin d'initier le tunnel :

Remote-ASA#packet-tracer input inside icmp 10.1.1.10 8 0 10.1.2.10 detailed

```
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple:
Prot=1, saddr=10.1.1.10, sport=0, daddr=10.1.2.10, dport=0
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE Initiator: New Phase 1, Intf
inside, IKE Peer 172.16.2.1 local Proxy Address 10.1.1.0, remote Proxy Address
10.1.2.0, Crypto map (outside_map)
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 132
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
<skipped>...
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Automatic NAT Detection Status: Remote end is NOT behind a NAT device
This end is NOT behind a NAT device
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)
+ VENDOR (13) + NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR ID received 172.16.2.1
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,
Oakley begin quick mode
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1, PHASE 1 COMPLETED

Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1, IKE Initiator
starting QM: msg id = c45c7b30
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, Transmitting Proxy Id:
Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
Remote subnet: 10.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE
(10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
```

```
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) +
ID (5) + ID (5) + NONE (0) total length : 172
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.2.0--255.255.255.0
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Security negotiation complete for LAN-to-LAN Group (172.16.2.1)
Initiator, Inbound SPI = 0x30d071c0, Outbound SPI = 0x38da6e51
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 76
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
```

## Central-ASA (répondeur)

```
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length
:
132
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, Connection landed on tunnel_group
DefaultL2LGroup
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Generating keys for Responder...
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) +
VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) +
NONE (0) total length : 304
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8)
+ IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1 DECODE]Group = DefaultL2LGroup, IP = 172.16.1.1,
ID_IPV4_ADDR ID received172.16.1.1
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +
VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, PHASE 1 COMPLETED
:
```

```

.
Jan 20 12:42:35 [IKEv1 DECODE]IP = 172.16.1.1, IKE Responder starting QM:
msg id = c45c7b30
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE
RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) +
NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Received remote
IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,
Protocol 0, Port 0:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup,
IP = 172.16.1.1, Received local
IP Proxy Subnet data in ID Payload: Address 10.1.2.0, Mask 255.255.255.0,
Protocol 0, Port 0Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup,
IP = 172.16.1.1, processing notify payload
Jan 20 12:42:35 [IKEv1] Group = DefaultL2LGroup, IP = 172.16.1.1, QM
IsRekeyed old sa not found by addr
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Static Crypto Map
check, map outside_dyn_map, seq = 1 is a successful match
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, IKE
Remote Peer configured for crypto map: outside_dyn_map
:
.
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Transmitting Proxy Id: Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0
Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=c45c7b30)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE
(0) total length : 172 Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED
Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 52:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Security
negotiation complete for LAN-to-LAN Group (DefaultL2LGroup) Responder,
Inbound SPI = 0x38da6e51, Outbound SPI = 0x30d071c0:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Adding static
route for L2L peer coming in on a dynamic map. address: 10.1.1.0, mask: 255.255.255.0

```

## Informations connexes

- [Références des commandes de la gamme Cisco ASA](#)
- [Page de support de la négociation IPSec/des protocoles IKE](#)
- [Demandes de commentaires \(RFC\)](#)
- [Assistance technique et documentation - Cisco System](#)