Configurez les tunnels site à site IPsec IKEv1 avec l'ASDM ou l'interface de ligne de commande sur l'ASAv

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Configurer
  - Diagramme du réseau
  - Configuration via l'assistant ASDM VPN
  - Configuration via l'interface CLI
    - Configurer le site B
    - Stratégie de groupe
- Vérifier
  - ASDM
  - CLI
    - Phase 1
    - Phase 2
- Dépannage

Introduction

Ce document décrit comment configurer un tunnel site à site IKEv1 IPsec entre deux pare-feu virtuels sécurisés Cisco (ASAv) exécutant v9.18.3.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connectivité IP de bout en bout doit être établie
- Ces protocoles doivent être autorisés :
  1. Protocole UDP (User Datagram Protocol) 500 et 4500 pour le plan de contrôle IPsec
  2. Encapsulating Security Payload (ESP) IP Protocol 50 pour le plan de données IPsec

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles et

matérielles suivantes :

- Cisco Secure Firewall ASA Virtual qui exécute le logiciel version 9.18.3

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Cette section décrit comment configurer le tunnel VPN site à site via l'assistant VPN ASDM (Adaptive Security Device Manager) ou via l'interface de ligne de commande.

Diagramme du réseau

Cette topologie est utilisée pour les exemples de ce document :

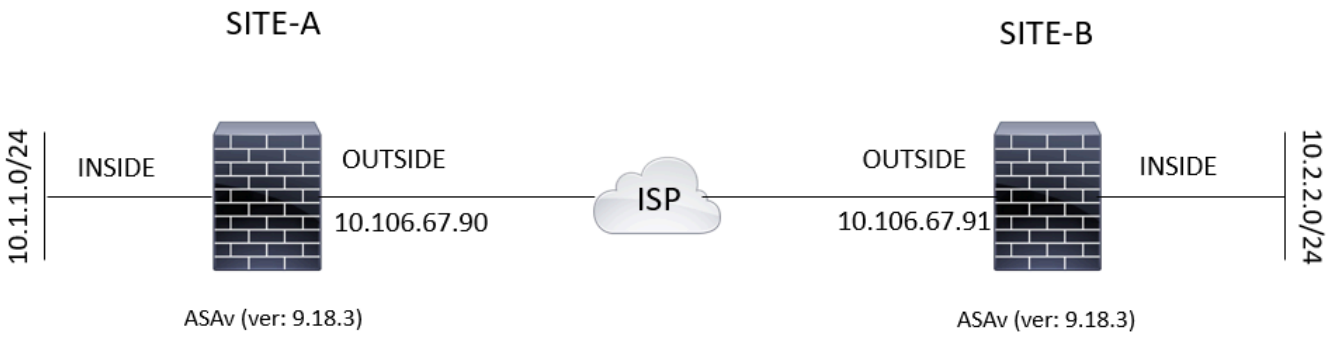
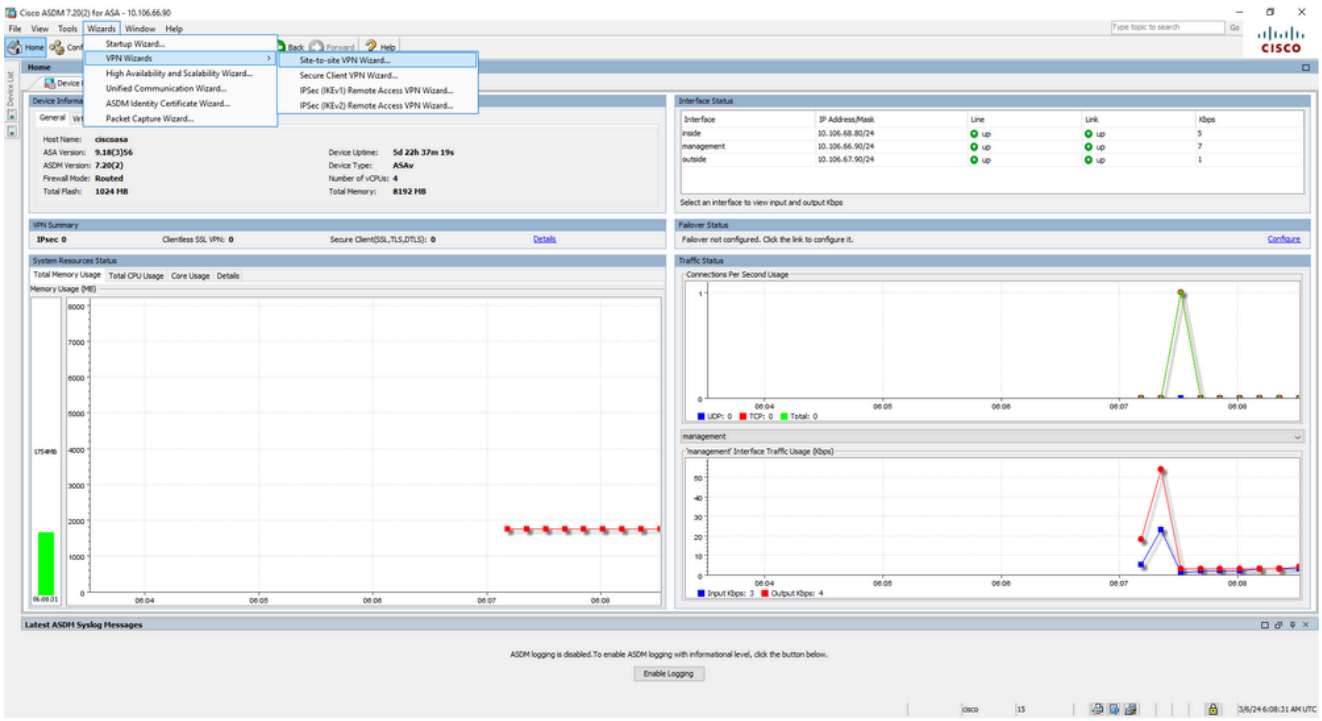


Schéma de topologie

Configuration via l'assistant ASDM VPN

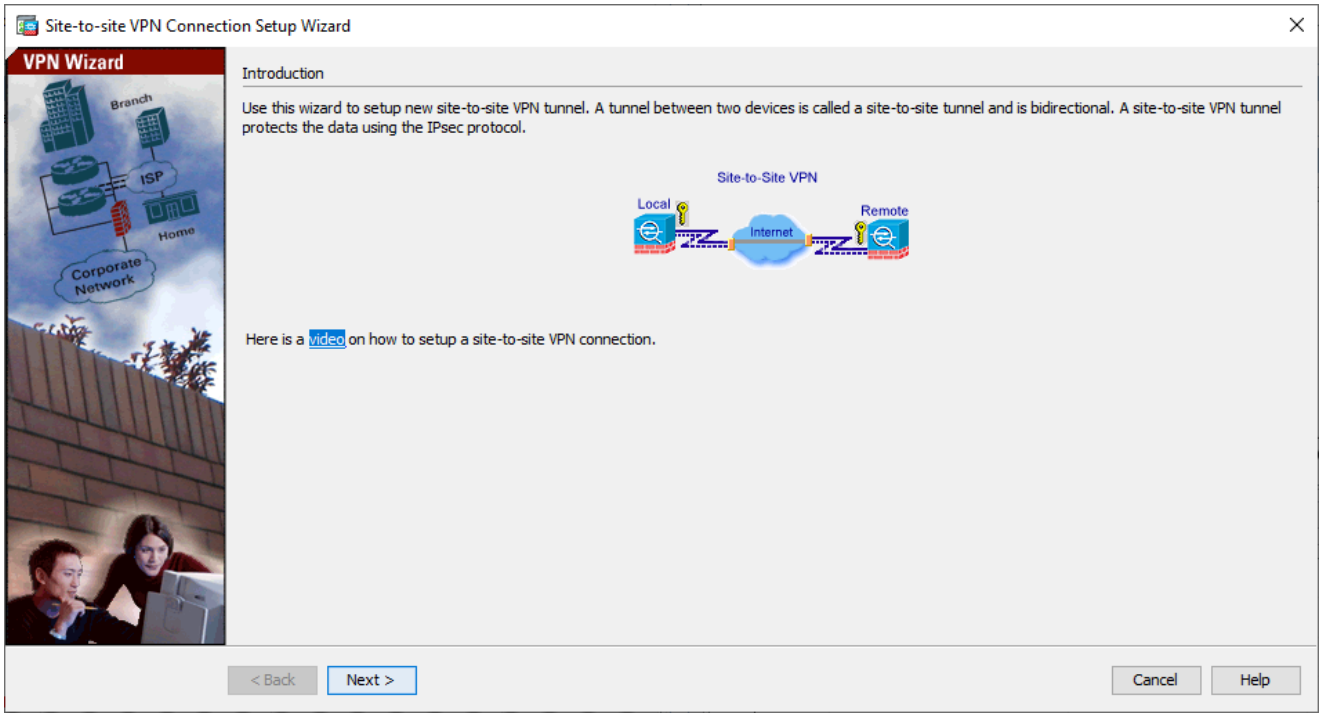
Complétez ces étapes afin de configurer le tunnel VPN site à site via l'assistant ASDM :

1. Ouvrez l'ASDM et accédez à Wizards > VPN Wizards > Site-to-site VPN Wizard.



Navigation de l'assistant VPN

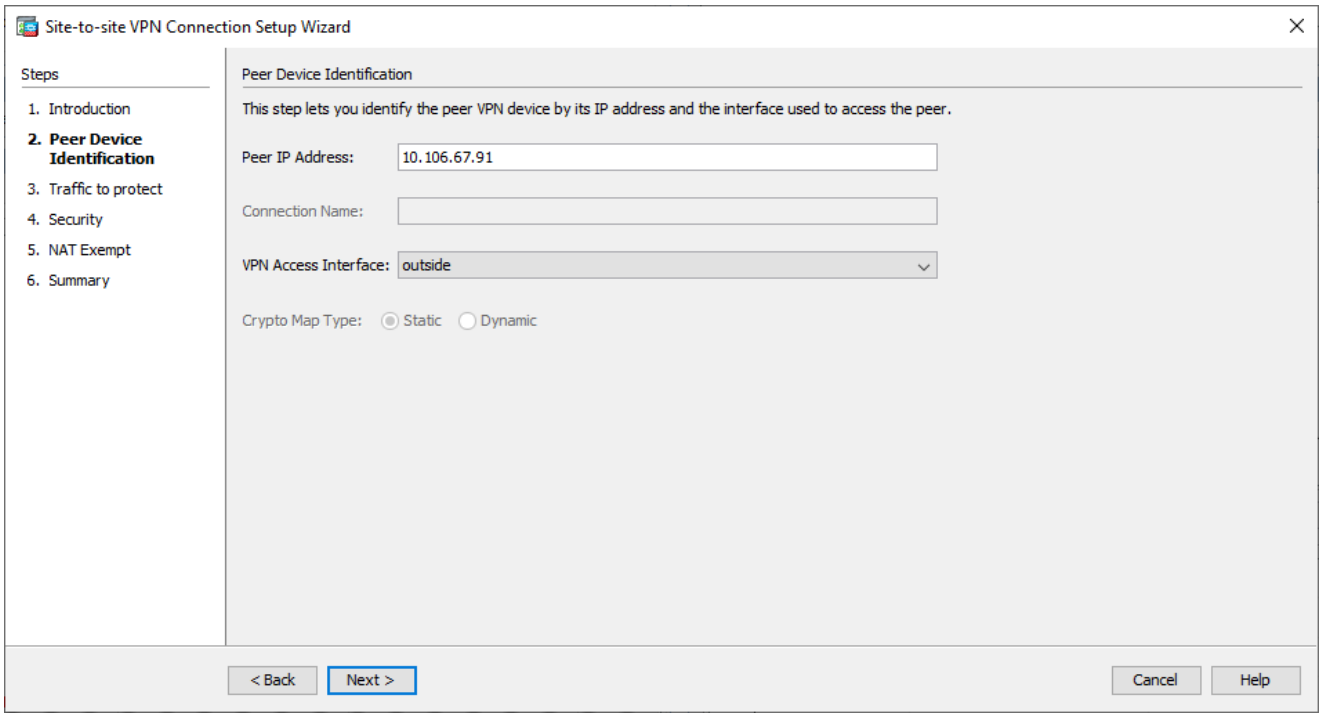
- Cliquez sur Next une fois que vous avez atteint la page d'accueil de l'Assistant.



Fenêtre 1 de l'assistant VPN

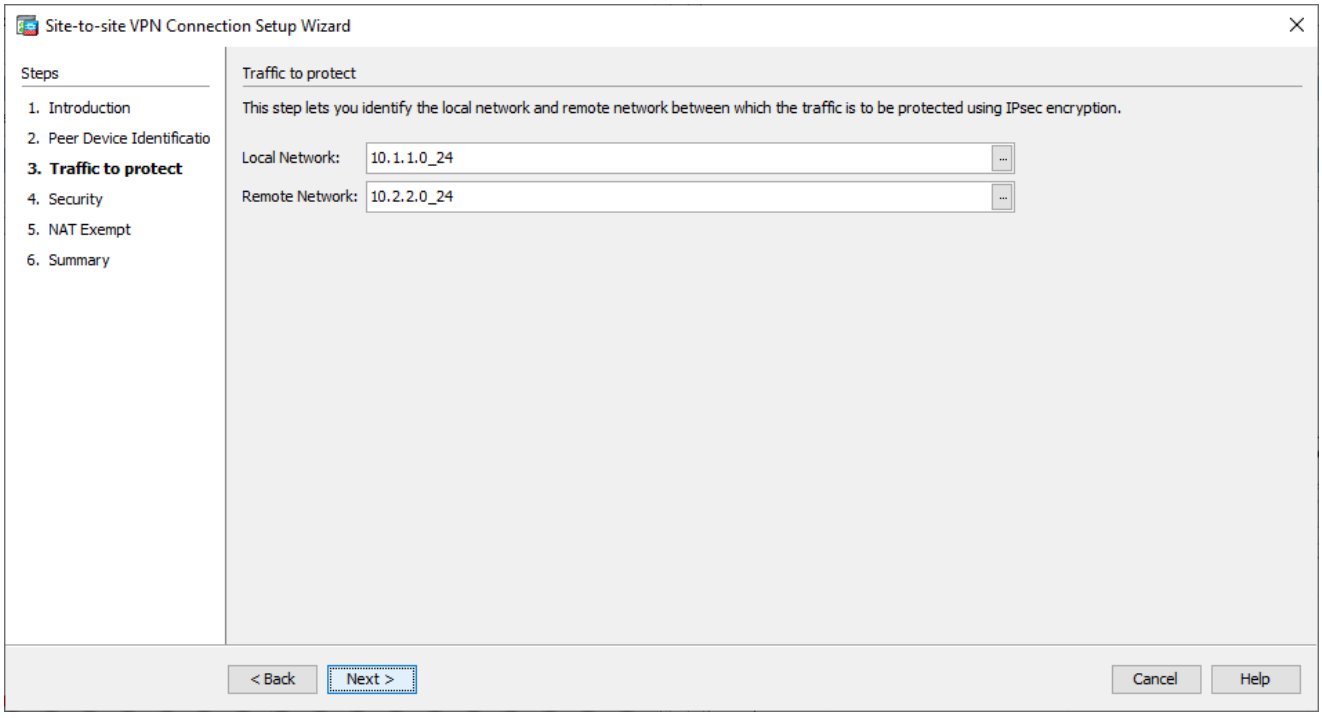
Remarque : les versions ASDM les plus récentes fournissent un lien vers une vidéo expliquant cette configuration.

- Configurez l'adresse IP homologue. Dans cet exemple, l'adresse IP de l'homologue est définie sur **10.106.67.91** sur le site B. Si vous configurez l'adresse IP de l'homologue sur le site A, elle doit être changée en **10.106.67.90**. L'interface par laquelle l'extrémité distante peut être atteinte est également spécifiée. Cliquez uneNext fois terminé.



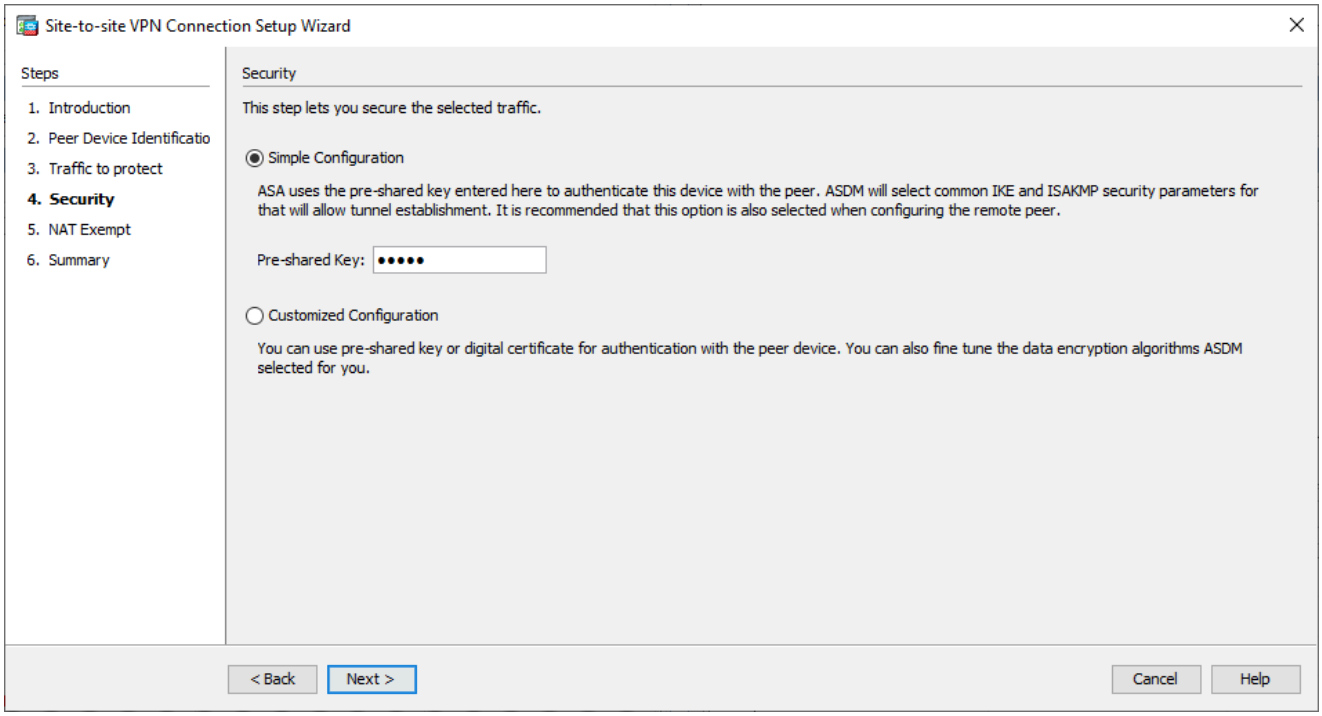
Fenêtre 2 de l'assistant VPN

- Configurez les réseaux locaux et distants (source et destination du trafic). Cette image montre la configuration du site B (l'inverse s'applique au site A).



Fenêtre 3 de l'assistant VPN

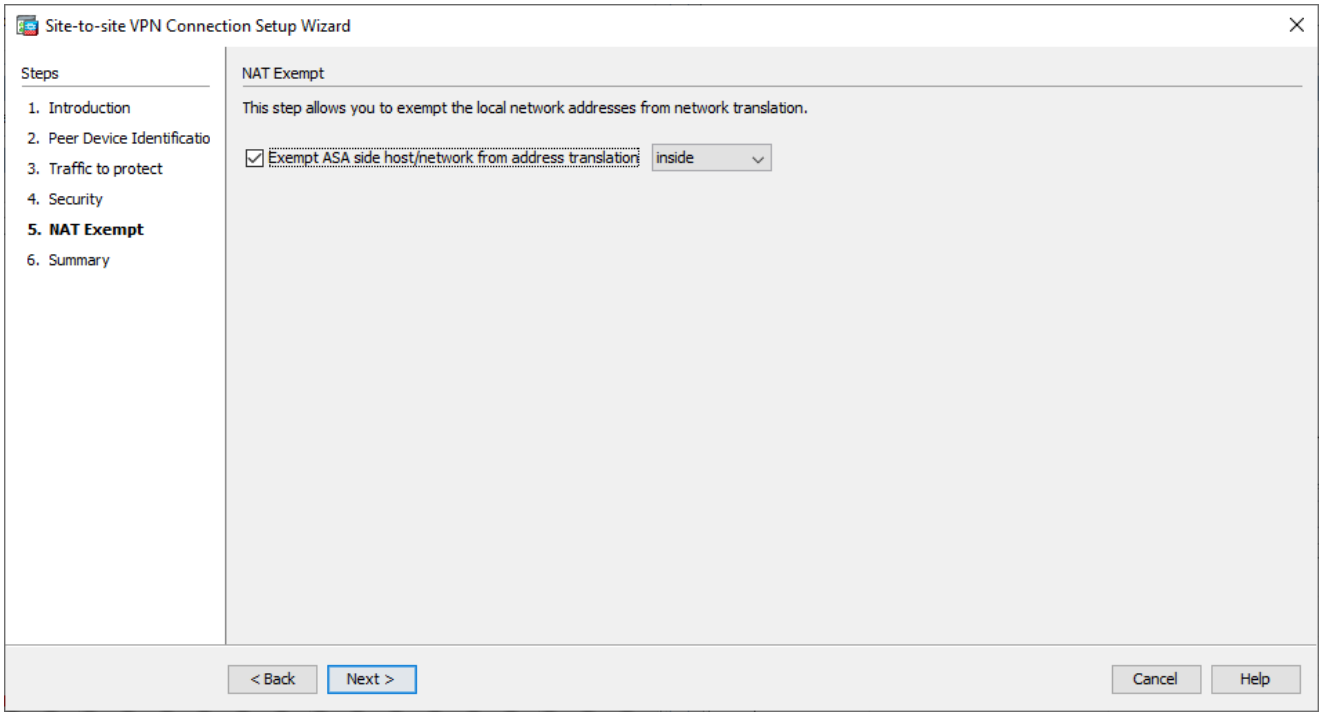
- Sur la page Security, configurez la clé pré-partagée (elle doit correspondre aux deux extrémités). Cliquez uneNext fois terminé.



Fenêtre 4 de l'assistant VPN

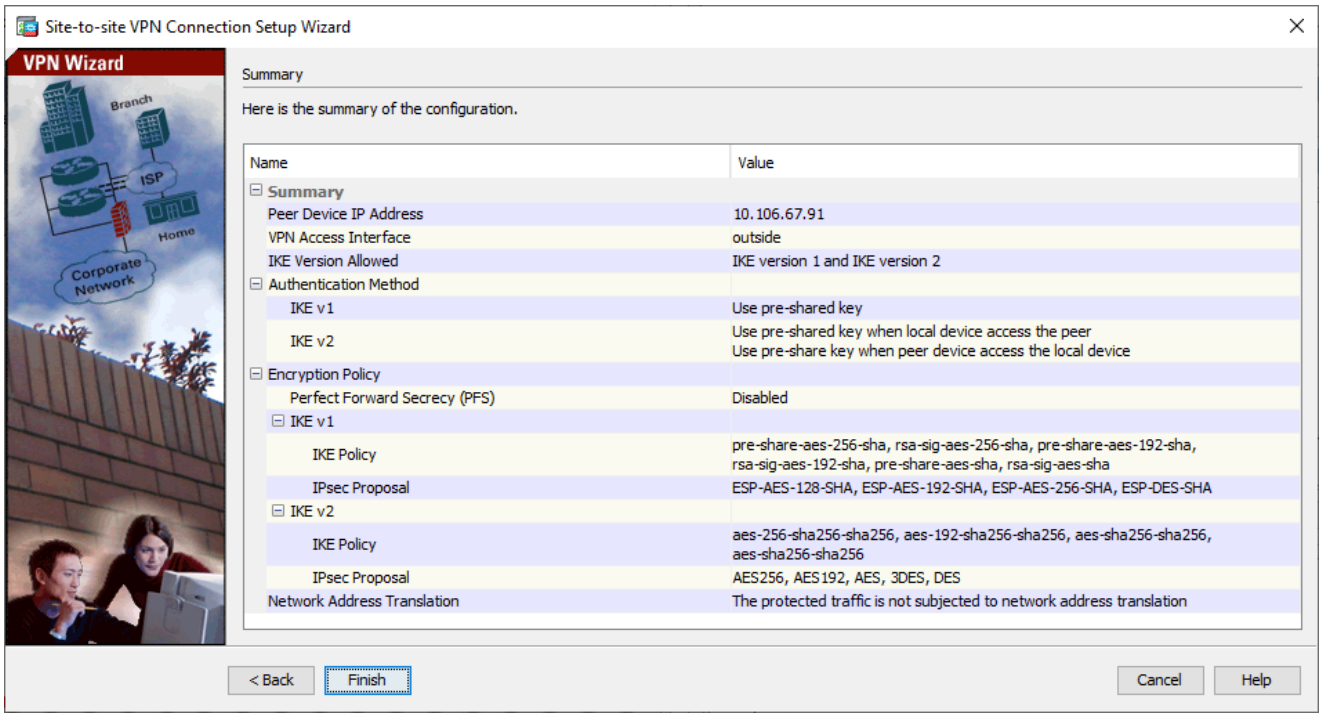
- Configurez l'interface source pour le trafic sur l'ASA. L'ASDM crée automatiquement la règle de traduction d'adresses de réseau (NAT) en fonction de la version de l'ASA et l'applique avec le reste de la configuration à l'étape finale.

Remarque : dans l'exemple utilisé dans ce document, « inside » est la source du trafic.



Fenêtre 5 de l'assistant VPN

- L'assistant fournit maintenant un résumé de la configuration qui est envoyée à l'ASA. Vérifiez les paramètres de configuration, puis cliquez sur Finish.



Fenêtre 6 de l'assistant VPN

Configuration via l'interface CLI

Cette section décrit comment configurer le tunnel site à site IKEv1 IPsec via l'interface de ligne de commande.

Configurer le site B

Conseil : pour obtenir un exemple de configuration IKEv2 avec l'ASA, consultez le document Cisco Site-to-Site IKEv2 Tunnel between ASA and Router Configuration Exemples.

Phase 1 (IKEv1)

Complétez ces étapes pour la configuration de la phase 1 :

- Entrez cette commande dans l'interface de ligne de commande afin d'activer IKEv1 sur l'interface externe :

```
crypto ikev1 enable outside
```

- Créez une stratégie IKEv1 qui définit les algorithmes/méthodes à utiliser pour le hachage, l'authentification, le groupe Diffie-Hellman, la durée de vie et le cryptage :

```
crypto ikev1 policy 1
! The 1 in the above command refers to the Policy suite priority (1 highest, 65535 lowest)
  authentication pre-share
  encryption aes-256
  hash sha
  group 14
  lifetime 86400
```

- Créez un groupe de tunnels sous les attributs IPsec et configurez l'adresse IP de l'homologue et la clé pré-partagée du tunnel :

```
tunnel-group 10.106.67.90 type ipsec-l2l
tunnel-group 10.106.67.90 ipsec-attributes
 ikev1 pre-shared-key cisco
 ! Note the IKEv1 keyword at the beginning of the pre-shared-key command.
```

Phase 2 (IPsec)

Complétez ces étapes pour la configuration de la phase 2 :

- Créez une liste d'accès qui définit le trafic à chiffrer et à tunnelliser. Dans cet exemple, le trafic d'intérêt est le trafic du tunnel qui est originaire du sous-réseau **10.2.2.0** vers **10.1.1.0**. Elle peut contenir plusieurs entrées si plusieurs sous-réseaux sont impliqués entre les sites.

```
object network 10.2.2.0_24
 subnet 10.2.2.0 255.255.255.0
object network 10.1.1.0_24
 subnet 10.1.1.0 255.255.255.0

access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

- Configurez le Transform Set (TS), qui doit impliquer le mot clé IKEv1. Un TS identique doit également être créé sur l'extrémité distante.

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

- Configurez la crypto-carte, qui contient les composants suivants :

- Adresse IP de l'homologue
- La liste d'accès définie qui contient le trafic d'intérêt
- Le TS
- Paramètre PFS (Perfect Forward Secrecy) facultatif, qui crée une nouvelle paire de clés Diffie-Hellman utilisées afin de protéger les données (les deux côtés doivent être compatibles PFS avant que la phase 2 ne s'affiche)

- Appliquez la crypto-carte sur l'interface externe :

```
crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 10.106.67.90
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside
```

Exemption NAT

Assurez-vous que le trafic VPN n'est soumis à aucune autre règle NAT. Il s'agit de la règle NAT utilisée :

nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static 10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup



Remarque : lorsque plusieurs sous-réseaux sont utilisés, vous devez créer des groupes d'objets avec tous les sous-réseaux source et de destination et les utiliser dans la règle NAT.

object-group network 10.x.x.x_SOURCE
 network-object 10.4.4.0 255.255.255.0
 network-object 10.2.2.0 255.255.255.0

object network 10.x.x.x_DESTINATION

```
 network-object 10.3.3.0 255.255.255.0
 network-object 10.1.1.0 255.255.255.0

nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE destination static 10.x.x.x_DESTINATION 10.x.x.x_DESTINATION no-proxy-
```

Exemple complet de configuration

Voici la configuration complète du site B :

```
crypto ikev1 enable outside

crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 14
 lifetime 86400

tunnel-group 10.106.67.90 type ipsec-l2l
tunnel-group 10.106.67.90 ipsec-attributes
 ikev1 pre-shared-key cisco
 !Note the IKEv1 keyword at the beginning of the pre-shared-key command.

object network 10.2.2.0_24
 subnet 10.2.2.0 255.255.255.0
object network 10.1.1.0_24
 subnet 10.1.1.0 255.255.255.0

access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24

crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac

crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 10.106.67.90
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside

nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static 10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

Stratégie de groupe

Les stratégies de groupe sont utilisées afin de définir des paramètres spécifiques qui s'appliquent au tunnel. Ces politiques sont utilisées conjointement avec le groupe de tunnels.

La stratégie de groupe peut être définie comme interne, ce qui signifie que les attributs sont extraits de celui qui est défini sur l'ASA, ou elle peut être définie comme externe, où les attributs sont interrogés à partir d'un serveur externe. Il s'agit de la commande utilisée pour définir la stratégie de groupe :

```
group-policy SITE_A internal
```

Remarque : vous pouvez définir plusieurs attributs dans la stratégie de groupe. Pour obtenir la liste de tous les attributs possibles, reportez-vous à la section Configuration des stratégies de groupe.

Attributs facultatifs de stratégie de groupe

L'attributvpn-tunnel-protocol détermine le type de tunnel auquel ces paramètres doivent être appliqués. Dans cet exemple, IPsec est utilisé :

```
vpn-tunnel-protocol ?
 group-policy mode commands/options:
 IPSec IP Security Protocol l2tp-ipsec L2TP using IPSec for security
 svc SSL VPN Client
 webvpn WebVPN

vpn-tunnel-protocol ikev1 - Version 8.4 and later
```

Vous avez la possibilité de configurer le tunnel de sorte qu'il reste inactif (aucun trafic) et ne tombe pas en panne. Pour configurer cette option, la valeur de l'attribut doit utiliservpn-idle-timeout minutes, ou vous pouvez définir la valeur sur none, ce qui signifie que le tunnel ne s'arrête jamais.

Voici un exemple :

```
group-policy SITE_A attributes
  vpn-idle-timeout ?

group-policy mode commands/options:
 <1-35791394> Number of minutes
 alert-interval Specify timeout alert interval in minutes
 none Site-to-Site (IKEv1, IKEv2) and IKEv1 remote-access: Disable
 timeout and allow an unlimited idle period; AnyConnect (SSL,
 IPSec/IKEv2): Use value of default-idle-timeout
```

La commandedefault-group-policy sous les attributs généraux du groupe de tunnels définit la stratégie de groupe qui est utilisée afin de pousser certains paramètres de stratégie pour le tunnel qui est établi. Les paramètres par défaut des options que vous n'avez pas définies dans la stratégie de groupe proviennent d'une stratégie de groupe globale par défaut :

```
tunnel-group 10.106.67.91 general-attributes
 default-group-policy SITE_A
```

Vérifier

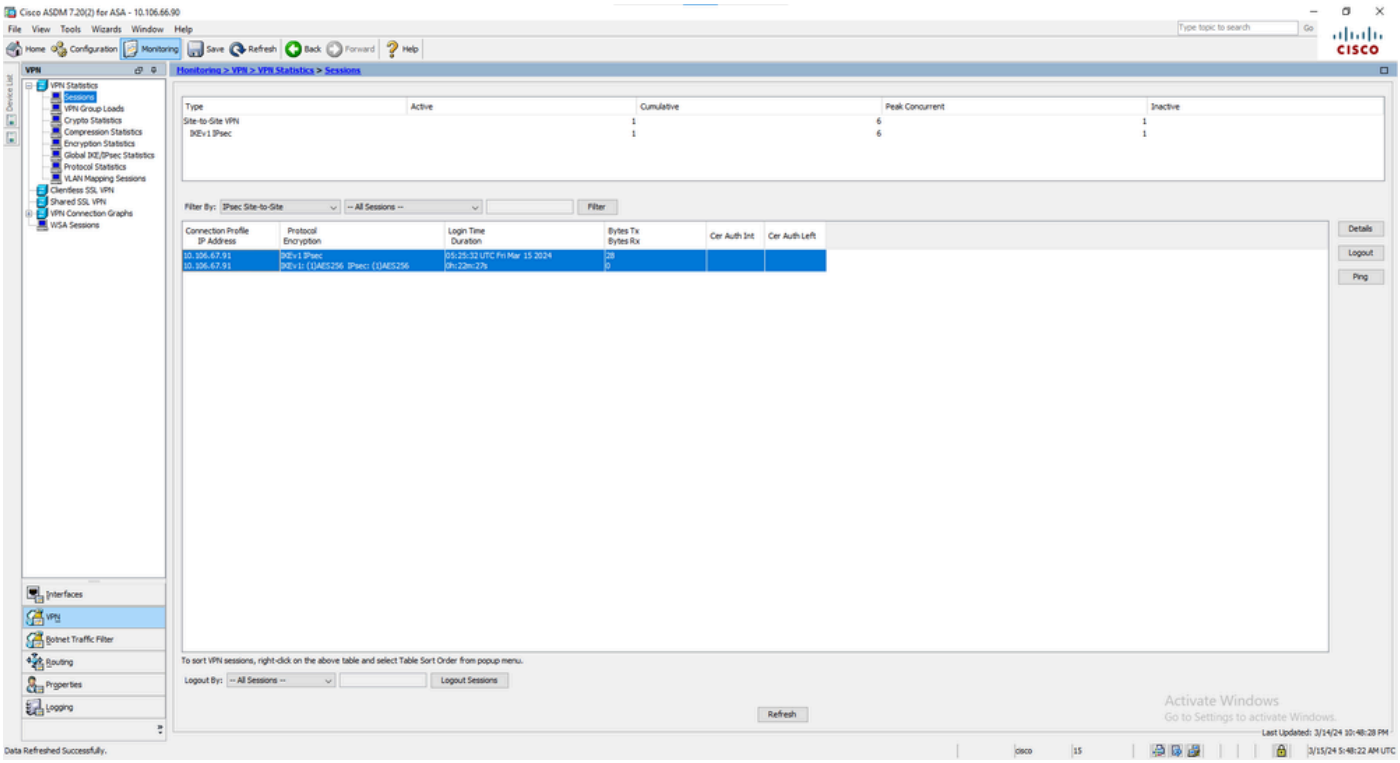
Utilisez les informations fournies dans cette section afin de vérifier que votre configuration fonctionne correctement.

ASDM

Pour afficher l'état du tunnel à partir de l'ASDM, accédez à Monitoring > VPN. Ces informations sont fournies :

- Adresse IP de l'homologue
- Protocole utilisé afin de construire le tunnel.
- Algorithme de chiffrement utilisé.
- L'heure à laquelle le tunnel est arrivé et le temps de disponibilité
- Nombre de paquets reçus et transférés.

 **Conseil** : cliquez Refresh pour afficher les dernières valeurs, car les données ne sont pas mises à jour en temps réel.



Fenêtre de surveillance VPN

CLI

Cette section décrit comment vérifier votre configuration via l'interface de ligne de commande.

Phase 1

Entrez cette commande dans l'interface de ligne de commande afin de vérifier la configuration de la phase 1 côté site B :

<#root>

show crypto ikev1 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:

10.106.67.91

 Type : L2L Role :

initiator

Rekey : no State :

MM_ACTIVE

Phase 2

La commandeshow crypto ipsec sa affiche les associations de sécurité IPsec qui sont créées entre les homologues. Le tunnel chiffré est construit entre les adresses IP 10.106.67.90 et 10.106.67.91 pour le trafic qui circule entre les réseaux 10.1.1.0 et 10.2.2.0. Vous pouvez voir les deux associations de sécurité ESP conçues pour le trafic entrant et sortant. L'en-tête d'authentification (AH) n'est pas utilisé car il n'existe aucune SA AH.

Entrez cette commande dans l'interface de ligne de commande afin de vérifier la configuration de phase 2 côté site A :

<#root>

interface: outside
Crypto map tag:

outside_map

, seq num: 20, local addr: 10.106.67.90

access-list 100 extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0

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

remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)

current_peer: 10.106.67.91

#pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20

#pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 20, #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.: 10.106.67.90/0, remote crypto endpt.: 10.106.67.91/0

```
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: F8951DA2

current inbound spi : 662C7ABE

inbound esp sas:
spi: 0x662C7ABE (1714191038)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression

in use settings ={L2L, Tunnel, PFS Group 14, IKEv1, }
slot: 0, conn_id: 1, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (3914998/28074)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x001FFFFF
outbound esp sas:
spi: 0xF8951DA2 (4170522018)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression

in use settings ={L2L, Tunnel, PFS Group 14, IKEv1, }
slot: 0, conn_id: 1, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (3914998/28073)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

Entrez cette commande dans l'interface de ligne de commande afin de vérifier la configuration de phase 2 côté site B :

<#root>

interface: outside
Crypto map tag:

outside_map

, seq num: 20, local addr: 10.106.67.91

access-list 100 extended permit ip 10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0

local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)

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

current_peer: 10.106.67.90

#pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20

#pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 20, #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.: 10.106.67.91/0, remote crypto endpt.: 10.106.67.90/0

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: 662C7ABE

current inbound spi : F8951DA2

inbound esp sas:
spi: 0xF8951DA2 (4170522018)
SA State: active

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

in use settings ={L2L, Tunnel, PFS Group 14, IKEv1, }
slot: 0, conn_id: 1, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373998/27737)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x001FFFFF
outbound esp sas:
spi: 0x662C7ABE (1714191038)
SA State: active

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

in use settings ={L2L, Tunnel, PFS Group 14, IKEv1, }
slot: 0, conn_id: 1, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373998/27737)

```
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

Dépannage

Utilisez les informations fournies dans cette section afin de résoudre les problèmes de configuration.

Entrez ces commandes debug afin de déterminer l'emplacement de la défaillance du tunnel :

- debug crypto ikev1 127 (Phase 1)
- debug crypto ipsec 127 (Phase 2)

Voici un exemple complet des résultats du débogage :

<#root>

IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1, saddr=10.1.1.10, sport=23043, daddr=10.2.2.10, dport=23043
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Mar 15 05:41:39 [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=23043, daddr=10.2.2.10, dport=23043

IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.

```
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE Initiator: New Phase 1, Intf inside, IKE Peer 10.106.67.9
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing ISAKMP SA payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing NAT-Traversal VID ver 02 payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing NAT-Traversal VID ver 03 payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing NAT-Traversal VID ver RFC payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing Fragmentation VID + extended capabilities
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA
Mar 15 05:41:39 [IKEv1]IKE Receiver: Packet received on 10.106.67.90:500 from 10.106.67.91:500
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + SA
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing SA payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Oakley proposal is acceptable
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Received NAT-Traversal RFC VID
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Received Fragmentation VID
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, IKE Peer included IKE fragmentation capability flags: M
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing ke payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing nonce payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing Cisco Unity VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing xauth V6 VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Send IOS VID
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Constructing ASA spoofing IOS Vendor ID payload (versio
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing VID payload
```

```
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing NAT-Discovery payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, computing NAT Discovery hash
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing NAT-Discovery payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, computing NAT Discovery hash
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE
Mar 15 05:41:39 [IKEv1]IKE Receiver: Packet received on 10.106.67.90:500 from 10.106.67.91:500
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + K
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing ke payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing ISA_KE payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing nonce payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Received Cisco Unity client VID
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Received xauth V6 VID
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Processing VPN3000/ASA spoofing IOS Vendor ID payload (
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Received Altiga/Cisco VPN3000/Cisco ASA GW VID
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing NAT-Discovery payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, computing NAT Discovery hash
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing NAT-Discovery payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, computing NAT Discovery hash
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, Connection landed on tunnel_group 10.106.67.91
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Generating keys for Initiator...
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing ID payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing hash payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Computing hash for ISAKMP
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Constructing IOS keep alive payload: proposal=32767/327
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing dpd vid payload
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID
Mar 15 05:41:39 [IKEv1]Group = 10.106.67.91, IP = 10.106.67.91, Automatic NAT Detection Status: Remote
Mar 15 05:41:39 [IKEv1]IKE Receiver: Packet received on 10.106.67.90:500 from 10.106.67.91:500
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + I
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing ID payload
Mar 15 05:41:39 [IKEv1 DECODE]Group = 10.106.67.91, IP = 10.106.67.91, ID_IPV4_ADDR ID received 10.106.
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing hash payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Computing hash for ISAKMP
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Processing IOS keep alive payload: proposal=32767/32767
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Received DPD VID
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, Connection landed on tunnel_group 10.106.67.91
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Oakley begin quick mode
Mar 15 05:41:39 [IKEv1 DECODE]Group = 10.106.67.91, IP = 10.106.67.91, IKE Initiator starting QM: msg i
```

Mar 15 05:41:39 [IKEv1]Group = 10.106.67.91, IP = 10.106.67.91, PHASE 1 COMPLETED

```
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, Keep-alive type for this connection: DPD
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Starting P1 rekey timer: 73440 se
Mar 15 05:41:39 [IKEv1]Group = 10.106.67.91, IP = 10.106.67.91, Add to IKEv1 Tunnel Table succeeded for
Mar 15 05:41:39 [IKEv1]Group = 10.106.67.91, IP = 10.106.67.91, Add to IKEv1 MIB Table succeeded for SA
IPSEC INFO: Setting an IPSec timer of type SA Purge Timer for 30 seconds with a jitter value of 0
IPSEC INFO: IPSec SA PURGE timer started SPI 0x0001B739
IPSEC: New embryonic SA created @ 0x00007f05294f4620,
 SCB : 0x294CFE60,
 Direction : inbound
 SPI : 0x50EF49AD
 Session ID : 0x00002000
 VPIF num : 0x00000002
 Tunnel type : l2l
 Protocol : esp
 Lifetime : 240 seconds
```

```
 SA handle : 0x0001B739
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, IKE got SPI from key engine: SPI =
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, oakley constructing quick mode
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing blank hash payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing IPSec SA payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing IPSec nonce payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing pfs ke payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing proxy ID
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Transmitting Proxy Id:
 Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
 Remote subnet: 10.2.2.0 Mask 255.255.255.0 Protocol 0 Port 0
Mar 15 05:41:39 [IKEv1 DECODE]Group = 10.106.67.91, IP = 10.106.67.91, IKE Initiator sending Initial Co
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing qm hash payload
Mar 15 05:41:39 [IKEv1 DECODE]Group = 10.106.67.91, IP = 10.106.67.91, IKE Initiator sending 1st QM pkt
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE SENDING Message (msgid=ad712fa9) with payloads : HD
Mar 15 05:41:39 [IKEv1]IKE Receiver: Packet received on 10.106.67.90:500 from 10.106.67.91:500
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE RECEIVED Message (msgid=ad712fa9) with payloads : H
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing hash payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing SA payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing nonce payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing ke payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing ISA_KE for PFS in phas
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing ID payload
Mar 15 05:41:39 [IKEv1 DECODE]Group = 10.106.67.91, IP = 10.106.67.91, ID_IPV4_ADDR_SUBNET ID received-
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing ID payload
Mar 15 05:41:39 [IKEv1 DECODE]Group = 10.106.67.91, IP = 10.106.67.91, ID_IPV4_ADDR_SUBNET ID received-
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, loading all IPSEC SAs
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Generating Quick Mode Key!
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Generating Quick Mode Key!
Mar 15 05:41:39 [IKEv1]Group = 10.106.67.91, IP = 10.106.67.91, Security negotiation complete for LAN-t
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, oakley constructing final quick m
Mar 15 05:41:39 [IKEv1 DECODE]Group = 10.106.67.91, IP = 10.106.67.91, IKE Initiator sending 3rd QM pkt
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE SENDING Message (msgid=ad712fa9) with payloads : HD
IPSEC INFO: Setting an IPSec timer of type SA Purge Timer for 30 seconds with a jitter value of 0
IPSEC INFO: IPSec SA PURGE timer started SPI 0x00024311
IPSEC: New embryonic SA created @ 0x00007f05294fd920,
 SCB : 0x294CCDB0,
 Direction : outbound
 SPI : 0xEA689811
 Session ID : 0x00002000
 VPIF num : 0x00000002
 Tunnel type : l2l
 Protocol : esp
 Lifetime : 240 seconds
 SA handle : 0x00024311
```

Rule Lookup for local 10.1.1.0 to remote 10.2.2.0

Peer matched map outside_map sequence 20

PROXY MATCH on crypto map outside_map seq 20

```
IPSEC DEBUG: Using NP outbound permit rule for SPI 0xEA689811
IPSEC: Completed host OBSA update, SPI 0xEA689811
IPSEC: Creating outbound VPN context, SPI 0xEA689811
 Flags : 0x00000005
 SA : 0x00007f05294fd920
 SPI : 0xEA689811
 MTU : 1500 bytes
```

```
 VCID : 0x00000000
 Peer : 0x00000000
 SCB : 0x02CEE703
 Channel: 0x00007f0533c4f700
IPSEC: Completed outbound VPN context, SPI 0xEA689811
VPN handle: 0x000000000000763c
IPSEC: New outbound encrypt rule, SPI 0xEA689811
 Src addr: 10.1.1.0
 Src mask: 255.255.255.0
 Dst addr: 10.2.2.0
 Dst mask: 255.255.255.0
 Src ports
 Upper: 0
 Lower: 0
 Op : ignore
 Dst ports
 Upper: 0
 Lower: 0
 Op : ignore
 Protocol: 0
 Use protocol: false
 SPI: 0x00000000
 Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0xEA689811
Rule ID: 0x00007f05294f8a60
IPSEC: New outbound permit rule, SPI 0xEA689811
 Src addr: 10.106.67.90
 Src mask: 255.255.255.255
 Dst addr: 10.106.67.91
 Dst mask: 255.255.255.255
 Src ports
 Upper: 0
 Lower: 0
 Op : ignore
 Dst ports
 Upper: 0
 Lower: 0
 Op : ignore
 Protocol: 50
 Use protocol: true
 SPI: 0xEA689811
 Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0xEA689811
Rule ID: 0x00007f05294f9110
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, IKE got a KEY_ADD msg for SA: SPI
IPSEC: New embryonic SA created @ 0x00007f05294f4620,
 SCB : 0x294CFE60,
 Direction : inbound
 SPI : 0x50EF49AD
 Session ID : 0x00002000
 VPIF num : 0x00000002
 Tunnel type: l2l
 Protocol : esp
 Lifetime : 240 seconds
 SA handle : 0x0001B739
Rule Lookup for local 10.1.1.0 to remote 10.2.2.0
Peer matched map outside_map sequence 20
PROXY MATCH on crypto map outside_map seq 20
IPSEC DEBUG: Using NP inbound permit rule for SPI 0x50EF49AD
IPSEC: Completed host IBSA update, SPI 0x50EF49AD
IPSEC: Creating inbound VPN context, SPI 0x50EF49AD
 Flags: 0x00000006
```

```
 SA : 0x00007f05294f4620
 SPI : 0x50EF49AD
 MTU : 0 bytes
 VCID : 0x00000000
 Peer : 0x0000763C
 SCB : 0x02CE8BB3
 Channel: 0x00007f0533c4f700
IPSEC: Completed inbound VPN context, SPI 0x50EF49AD
VPN handle: 0x00000000000086bc
IPSEC: Updating outbound VPN context 0x0000763C, SPI 0xEA689811
 Flags: 0x00000005
 SA : 0x00007f05294fd920
 SPI : 0xEA689811
 MTU : 1500 bytes
 VCID : 0x00000000
 Peer : 0x000086BC
 SCB : 0x02CEE703
 Channel: 0x00007f0533c4f700
IPSEC: Completed outbound VPN context, SPI 0xEA689811
VPN handle: 0x000000000000763c
IPSEC: Completed outbound inner rule, SPI 0xEA689811
Rule ID: 0x00007f05294f8a60
IPSEC: Completed outbound outer SPD rule, SPI 0xEA689811
Rule ID: 0x00007f05294f9110
IPSEC: New inbound tunnel flow rule, SPI 0x50EF49AD
 Src addr: 10.2.2.0
 Src mask: 255.255.255.0
 Dst addr: 10.1.1.0
 Dst mask: 255.255.255.0
 Src ports
 Upper: 0
 Lower: 0
 Op : ignore
 Dst ports
 Upper: 0
 Lower: 0
 Op : ignore
 Protocol: 0
 Use protocol: false
 SPI: 0x00000000
 Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x50EF49AD
Rule ID: 0x00007f05294f8180
IPSEC: New inbound decrypt rule, SPI 0x50EF49AD
 Src addr: 10.106.67.91
 Src mask: 255.255.255.255
 Dst addr: 10.106.67.90
 Dst mask: 255.255.255.255
 Src ports
 Upper: 0
 Lower: 0
 Op : ignore
 Dst ports
 Upper: 0
 Lower: 0
 Op : ignore
 Protocol: 50
 Use protocol: true
 SPI: 0x50EF49AD
 Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x50EF49AD
Rule ID: 0x00007f05294f7ad0
```

```
IPSEC: New inbound permit rule, SPI 0x50EF49AD
 Src addr: 10.106.67.91
 Src mask: 255.255.255.255
 Dst addr: 10.106.67.90
 Dst mask: 255.255.255.255
 Src ports
 Upper: 0
 Lower: 0
 Op : ignore
 Dst ports
 Upper: 0
 Lower: 0
 Op : ignore
 Protocol: 50
 Use protocol: true
 SPI: 0x50EF49AD
 Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x50EF49AD
Rule ID: 0x00007f05294f4510
IPSEC INFO: Destroying an IPSec timer of type SA Purge Timer
IPSEC INFO: Destroying an IPSec timer of type SA Purge Timer
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Pitcher: received KEY_UPDATE, spi
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Starting P2 rekey timer: 24480 se
```

Mar 15 05:41:39 [IKEv1]Group = 10.106.67.91, IP = 10.106.67.91, PHASE 2 COMPLETED (msgid=ad712fa9)

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.