

Exemple de configuration d'ASA VPN avec les scénarios superposants

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Traduction sur les deux points finaux VPN](#)

[ASA 1](#)

[Créez les objets nécessaires pour les sous-réseaux en service](#)

[Configurez la déclaration NAT](#)

[Configurez le crypto ACL avec les sous-réseaux traduits](#)

[Crypto configuration appropriée](#)

[ASA 2](#)

[Créez les objets nécessaires pour les sous-réseaux en service](#)

[Configurez la déclaration NAT](#)

[Configurez le crypto ACL avec les sous-réseaux traduits](#)

[Crypto configuration appropriée](#)

[Vérifiez](#)

[ASA 1](#)

[ASA 2](#)

[Topologie de hub and spoke avec les rais superposants](#)

[ASA1](#)

[Créez les objets nécessaires pour les sous-réseaux en service](#)

[Créez les déclarations manuelles pour se traduire :](#)

[Configurez le crypto ACL avec les sous-réseaux traduits](#)

[Crypto configuration appropriée](#)

[ASA2 \(SPOKE1\)](#)

[Configurez le crypto ACL allant au sous-réseau traduit \(10.20.20.0 /24\)](#)

[Crypto configuration appropriée](#)

[R1 \(SPOKE2\)](#)

[Configurez le crypto ACL allant au sous-réseau traduit \(10.30.30.0 /24\)](#)

[Crypto configuration appropriée](#)

[Vérifiez](#)

[ASA 1](#)

[ASA2 \(SPOKE1\)](#)

[R1 \(SPOKE2\)](#)

[Dépannez](#)

[Suppression des associations de sécurité](#)

[Configuration NAT d'examen](#)

[Dépannage des commandes](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes utilisées pour traduire le trafic VPN que les voyages au-dessus d'un entre réseaux locaux (L2L) IPsec percent un tunnel entre deux appliances de sécurité adaptable (ASA) dans les scénarios et également la translation d'adresses d'adresse du port superposants (PAT) le trafic sur Internet.

Conditions préalables

Conditions requises

Veillez-vous pour avoir configuré l'appliance de sécurité adaptable Cisco avec des adresses IP sur les interfaces, et ayez la Connectivité de base avant que vous poursuiviez cet exemple de configuration.

[Composants utilisés](#)

Les informations dans ce document sont basées sur cette version de logiciel :

- Version de logiciel 8.3 d'appliance de sécurité adaptable Cisco et plus tard.

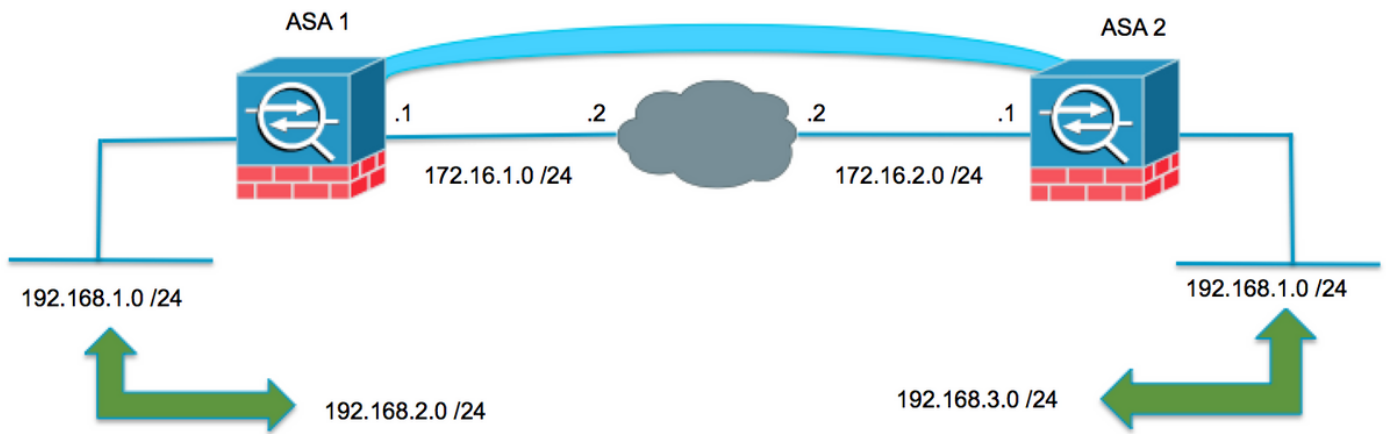
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

[Informations générales](#)

Chaque périphérique a un réseau privé et protégé derrière lui. Dans les scénarios superposants, la transmission à travers le VPN ne se produit jamais parce que les paquets ne partent jamais du sous-réseau local puisque le trafic est envoyé à une adresse IP du même sous-réseau. Ceci peut être accompli avec le Traduction d'adresses de réseau (NAT) comme expliqué dans les sections suivantes.

Traduction sur les deux points finaux VPN

Quand les réseaux protégés par VPN superposent et la configuration peut être modifiée sur les deux points finaux ; NAT peut être utilisé pour traduire le réseau local à un différent sous-réseau en allant au distant a traduit le sous-réseau.



ASA 1

Créez les objets nécessaires pour les sous-réseaux en service

```
object network LOCAL
  subnet 192.168.1.0 255.255.255.0
object network XLATED-LOCAL
  subnet 192.168.2.0 255.255.255.0
object network XLATED-REMOTE
  subnet 192.168.3.0 255.255.255.0
```

Configurez la déclaration NAT

Créez une déclaration manuelle pour traduire le réseau local à un différent sous-réseau seulement en allant au sous-réseau distant (également traduit)

```
nat (inside,outside) source static LOCAL XLATED-LOCAL destination static XLATED-REMOTE XLATED-REMOTE
```

Configurez le crypto ACL avec les sous-réseaux traduits

```
access-list VPN-TRAFFIC extended permit ip object XLATED-LOCAL object XLATED-REMOTE Rele
```

Crypto configuration appropriée

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.2.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

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

ASA 2

Créez les objets nécessaires pour les sous-réseaux en service

```
object network LOCAL
  subnet 192.168.1.0 255.255.255.0
object network XLATED-LOCAL
  subnet 192.168.3.0 255.255.255.0
object network XLATED-REMOTE
  subnet 192.168.2.0 255.255.255.0
```

Configurez la déclaration NAT

Créez une déclaration manuelle pour traduire le réseau local à un différent sous-réseau seulement en allant au sous-réseau distant (également traduit)

```
nat (inside,outside) source static LOCAL XLATED-LOCAL destination static XLATED-REMOTE XLATED-REMOTE
```

Configurez le crypto ACL avec les sous-réseaux traduits

```
access-list VPN-TRAFFIC extended permit ip object XLATED-LOCAL object XLATED-REMOTE Rele
```

Crypto configuration appropriée

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.1.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

ASA 1

```
ASA1(config)# sh cry isa 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
```

```
There are no IKEv2 SAsASA1(config)# show crypto ipsec sa
```

```

interface: outside
  Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.1.1

  access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 192.168.3.0
  255.255.255.0
  local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer: 172.16.2.1

  #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
  #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 9, #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: F90C149A
  current inbound spi : 6CE656C7

inbound esp sas:
  spi: 0x6CE656C7 (1827034823)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, IKEv1, }
  slot: 0, conn_id: 16384, crypto-map: MYMAP
  sa timing: remaining key lifetime (kB/sec): (3914999/28768)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x000003FF

outbound esp sas:
  spi: 0xF90C149A (4178318490)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, IKEv1, }
  slot: 0, conn_id: 16384, crypto-map: MYMAP
  sa timing: remaining key lifetime (kB/sec): (3914999/28768)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001

```

ASA 2

```
ASA2(config)# show crypto isa 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

```

```

There are no IKEv2 SAs
ASA2(config)# show crypto ipsec sa
interface: outside

```

Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.2.1

```
access-list VPN-TRAFFIC extended permit ip 192.168.3.0 255.255.255.0 192.168.2.0
255.255.255.0
```

```
local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer: 172.16.1.1
```

```
#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #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: 6CE656C7
current inbound spi : F90C149A
```

inbound esp sas:

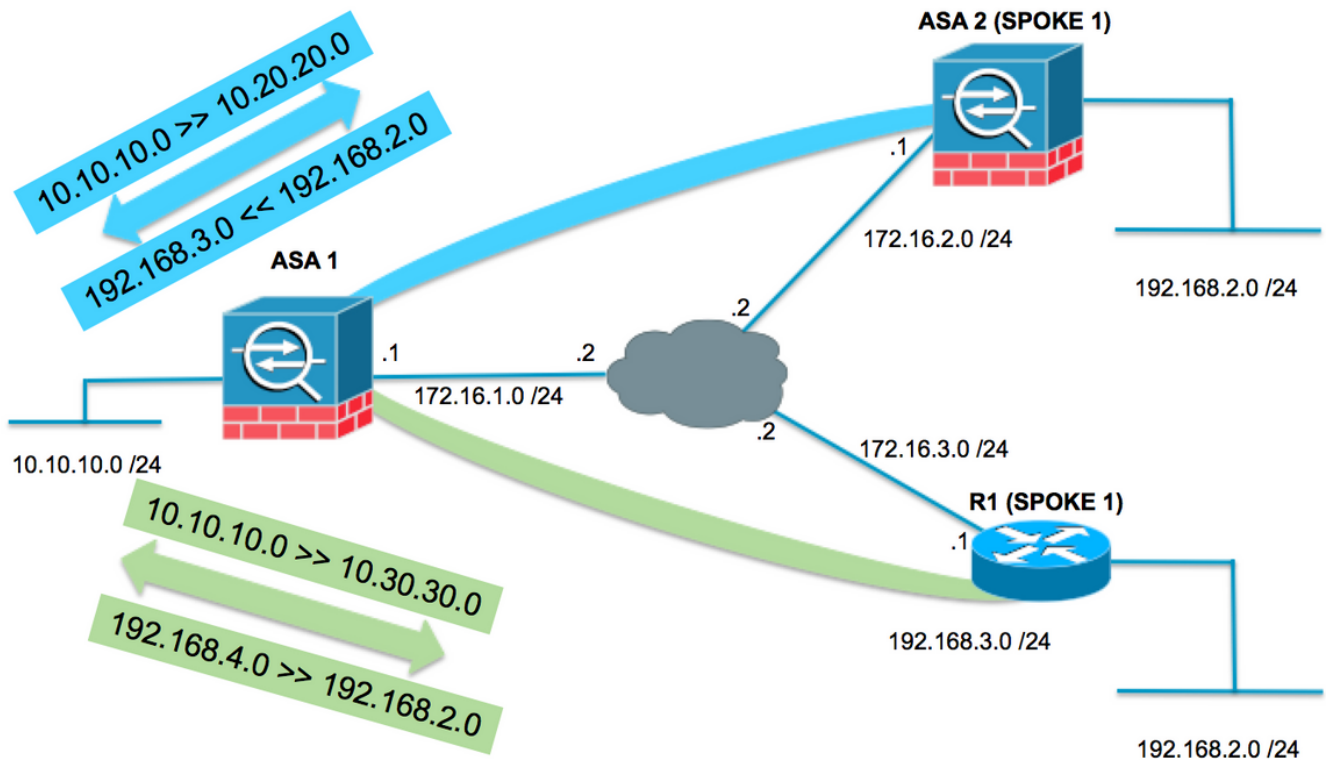
```
spi: 0xF90C149A (4178318490)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28684)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000003FF
```

outbound esp sas:

```
spi: 0x6CE656C7 (1827034823)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28683)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

Topologie de hub and spoke avec les rais superposants

Dans la topologie folloing, les deux rais ont le même sous-réseau qui doit être protégé au-dessus du tunnel d'IPsec vers le hub. Pour faciliter la Gestion sur les rais la configuration NAT au contournement le problème superposant est exécutée sur le hub seulement.



ASA1

Créez les objets nécessaires pour les sous-réseaux en service

```
object network LOCAL
  subnet 10.10.10.0 255.255.255.0
object network SPOKES-NETWORK
  subnet 192.168.2.0 255.255.255.0
object network LOCAL-XLATE-TO-SPOKE1
  subnet 10.20.20.0 255.255.255.0
object network LOCAL-XLATE-TO-SPOKE2
  subnet 10.30.30.0 255.255.255.0
object network REMOTE-XLATE-SPOKE1
  subnet 192.168.3.0 255.255.255.0
object network REMOTE-XLATE-SPOKE2
  subnet 192.168.4.0 255.255.255.0
```

Créez les déclarations manuelles pour se traduire :

- Le réseau local 10.10.10.0 /24 à 10.20.20.0 /24 en allant au SPOKE1 (192.168.2.0 /24).
- SPOKE1 le réseau 192.168.2.0 /24 à 192.168.3.0 /24 en étant livré à 10.20.20.0 /24.
- Le réseau local 10.10.10.0 /24 à 10.30.30.0 /24 en allant au SPOKE3 (192.168.2.0 /24).
- SPOKE2 le réseau 192.168.2.0 /24 à 192.168.4.0 /24 en étant livré à 10.30.30.0 /24.

```
nat (inside,outside) source static LOCAL LOCAL-XLATE-SPOKE1 destination static REMOTE-XLATE-SPOKE1 SPOKES-NETWORK
nat (inside,outside) source static LOCAL LOCAL-XLATE-SPOKE2 destination static REMOTE-XLATE-SPOKE2 SPOKES-NETWORK
```

Configurez le crypto ACL avec les sous-réseaux traduits

```
access-list VPN-to-SPOKE1 extended permit ip object LOCAL-XLATE-SPOKE1 object SPOKES-NETWORKS
```

```
access-list VPN-to-SPOKE2 extended permit ip object LOCAL-XLATE-SPOKE2 object SPOKES-NETWORKS
```

Crypto configuration appropriée

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-to-SPOKE1
crypto map MYMAP 10 set peer 172.16.2.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP 20 match address VPN-to-SPOKE2
crypto map MYMAP 20 set peer 172.16.3.1
crypto map MYMAP 20 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
tunnel-group 172.16.3.1 type ipsec-l2l
tunnel-group 172.16.3.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

ASA2 (SPOKE1)

Configurez le crypto ACL allant au sous-réseau traduit (10.20.20.0 /24)

```
access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 10.20.20.0 255.255.255.0
```

Crypto configuration appropriée

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400

crypto ipsec ikev1 transform-set esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.1.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

R1 (SPOKE2)

Configurez le crypto ACL allant au sous-réseau traduit (10.30.30.0 /24)

```
ip access-list extended VPN-TRAFFIC
  permit ip 192.168.2.0 0.0.0.255 10.30.30.0 0.0.0.255
```


Crypto configuration appropriée

```
crypto isakmp policy 1
  encr aes 256
  authentication pre-share
  group 2

crypto isakmp key secure_PSK address 172.16.1.1

crypto ipsec transform-set AES256-SHA esp-aes 256 esp-sha-hmac
mode tunnel

crypto map MYMAP 10 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set AES256-SHA
  match address VPN-TRAFFIC

interface GigabitEthernet0/1
  ip address 172.16.3.1 255.255.255.0
  duplex auto
  speed auto
  media-type rj45
  crypto map MYMAP
```

Vérifiez

ASA 1

```
ASA1(config)# show crypto isakmp sa
```

```
IKEv1 SAs:
```

```
  Active SA: 2
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2
```

```
1  IKE Peer: 172.16.3.1
   Type    : L2L           Role    : responder
   Rekey   : no           State   : MM_ACTIVE
2  IKE Peer: 172.16.2.1
   Type    : L2L           Role    : responder
   Rekey   : no           State   : MM_ACTIVE
```

```
There are no IKEv2 SAsASA1(config)# show crypto ipsec sa
```

```
interface: outside
```

```
  Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.1.1
```

```
    access-list VPN-to-SPOKE1 extended permit ip 10.20.20.0 255.255.255.0 192.168.2.0
255.255.255.0
```

```
    local ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
```

```
    remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
```

```
    current_peer: 172.16.2.1
```

```
    #pkts encaps: 10, #pkts encrypt: 9, #pkts digest: 10
```

```
    #pkts decaps: 10, #pkts decrypt: 9, #pkts verify: 10
```

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

```
    #pkts not compressed: 9, #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: 79384296
current inbound spi : 2189BF7A

inbound esp sas:

spi: 0x2189BF7A (562675578)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/28618)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x000003FF

outbound esp sas:

spi: 0x79384296 (2033730198)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/28618)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

Crypto map tag: MYMAP, seq num: 20, local addr: 172.16.1.1

access-list VPN-to-SPOKE2 extended permit ip 10.30.30.0 255.255.255.0 192.168.2.0
255.255.255.0

local ident (addr/mask/prot/port): (10.30.30.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer: 172.16.3.1

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#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.: 172.16.3.1/0
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: 65FDF4F5
current inbound spi : 05B7155D

inbound esp sas:

spi: 0x05B7155D (95884637)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/2883)
IV size: 16 bytes
replay detection support: Y

```
Anti replay bitmap:
0x00000000 0x0000001F
outbound esp sas:
spi: 0x65FDF4F5 (1711142133)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/2883)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

ASA2 (SPOKE1)

```
ASA2(config)# 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      : initiator
Rekey     : no           State     : MM_ACTIVE
```

```
There are no IKEv2 SAs
ASA2(config)# show crypto ipsec sa
interface: outside
```

```
Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.2.1
```

```
access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 10.20.20.0
255.255.255.0
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
current_peer: 172.16.1.1
```

```
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #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: 2189BF7A
current inbound spi : 79384296
```

```
inbound esp sas:
```

```
spi: 0x79384296 (2033730198)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28494)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
```

```
0x00000000 0x000003FF
outbound esp sas:
spi: 0x2189BF7A (562675578)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28494)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

R1 (SPOKE2)

```
R3lshow crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
```

dst	src	state	conn-id	status
172.16.1.1	172.16.3.1	QM_IDLE	1001	ACTIVE

```
IPv6 Crypto ISAKMP SARl#show crypto ipsec sa
```

```
interface: GigabitEthernet0/1
```

```
Crypto map tag: MYMAP, local addr 172.16.3.1
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.30.30.0/255.255.255.0/0/0)
```

```
current_peer 172.16.1.1 port 500
```

```
PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
```

```
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
```

```
#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
```

```
local crypto endpt.: 172.16.3.1, remote crypto endpt.: 172.16.1.1
```

```
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
```

```
current outbound spi: 0x5B7155D(95884637)
```

```
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
```

```
spi: 0x65FDF4F5(1711142133)
```

```
transform: esp-256-aes esp-sha-hmac ,
```

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

```
conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map: MYMAP
```

```
sa timing: remaining key lifetime (k/sec): (4188495/2652)
```

```
IV size: 16 bytes
```

```
replay detection support: Y
```

```
Status: ACTIVE(ACTIVE)
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
```

```
spi: 0x5B7155D(95884637)
```

```
transform: esp-256-aes esp-sha-hmac ,
```

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

```
conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map: MYMAP
```

```
sa timing: remaining key lifetime (k/sec): (4188495/2652)
```

```
IV size: 16 bytes
```

```
replay detection support: Y
```

```
Status: ACTIVE(ACTIVE)
```

outbound ah sas:

outbound pcp sas:

Dépannez

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

[Suppression des associations de sécurité](#)

Quand vous dépannez, soyez sûr d'effacer SAS existante après que vous apportiez une modification. En mode privilégiée du PIX, utilisez les commandes suivantes :

- **clear crypto ipsec sa** - Supprime l'IPsec actif SAS.
- **clear crypto isakmp SA** - Supprime l'IKE actif SAS.

Configuration NAT d'examen

- **affichez le détail nat** - Affiche la configuration NAT avec les objets/groupes d'objets développés

Dépannage des commandes

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

[L'analyseur de Cisco CLI](#) (clients [enregistrés](#) seulement) prend en charge certaines **commandes show**. Employez l'analyseur de Cisco CLI afin de visualiser une analyse de sortie de commande show.

Remarque: Consultez [Informations importantes sur les commandes debug](#) et [Dépannage de la sécurité IP - Présentation et utilisation des commandes debug](#) avant d'utiliser les commandes **debug**.

- **debug crypto ipsec** - Affiche les négociations IPSEcs du Phase 2.
- **debug crypto isakmp** - Affiche les négociations ISAKMP du Phase 1.

[Informations connexes](#)

- [Guide de configuration NAT](#)
- [Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance](#)
- [Négociation IPsec/Protocoles IKE](#)
- [Support et documentation techniques - Cisco Systems](#)