Configuration d'un VPN ASA avec des scénarios de chevauchement

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Traduction sur les deux terminaux VPN
  - ASA 1
    - Créez les objets nécessaires pour les sous-réseaux utilisés
    - Configuration de l'instruction NAT
    - Configurer la liste de contrôle d'accès cryptographique avec les sous-réseaux traduits
    - Configuration de chiffrement appropriée
  - ASA 2
    - Créez les objets nécessaires pour les sous-réseaux utilisés
    - Configuration de l'instruction NAT
    - Configurer la liste de contrôle d'accès cryptographique avec les sous-réseaux traduits
    - Configuration de chiffrement appropriée
  - Vérifier
    - ASA 1
    - ASA 2
- Topologie Hub and Spoke avec chevauchement des rayons
  - ASA1
    - Créez les objets nécessaires pour les sous-réseaux utilisés
    - Créez des instructions manuelles à traduire :
    - Configurer la liste de contrôle d'accès cryptographique avec les sous-réseaux traduits
    - Configuration de chiffrement appropriée
  - ASA2 (SPOKE1)
    - Configurez la liste de contrôle d'accès cryptée vers le sous-réseau traduit (10.20.20.0 /24)
    - Configuration de chiffrement appropriée
  - R1(SPOKE2)
    - Configurez la liste de contrôle d'accès cryptée vers le sous-réseau traduit (10.30.30.0 /24)
    - Configuration de chiffrement appropriée
  - Vérifier
    - ASA 1
    - ASA2 (SPOKE1)
    - R1 (SPOKE2)
- Dépannage
  - Suppression des associations de sécurité
  - Examiner la configuration NAT
  - Dépannage des commandes
- Informations connexes

Introduction

Ce document décrit les étapes utilisées pour traduire le trafic VPN qui circule sur un tunnel IPsec LAN à LAN (L2L) entre deux dispositifs de sécurité adaptatifs (ASA) dans des scénarios de chevauchement et également la traduction d'adresses de port (PAT) pour le trafic Internet.

Conditions préalables

Exigences

Assurez-vous d'avoir configuré l'appliance de sécurité adaptative Cisco avec des adresses IP sur les interfaces et d'avoir une connectivité de base avant de poursuivre cet exemple de configuration.

Composants utilisés

L’information contenue dans le présent document est fondée sur cette version logicielle:

- Logiciel Cisco Adaptive Security Appliance versions 8.3 et ultérieures.

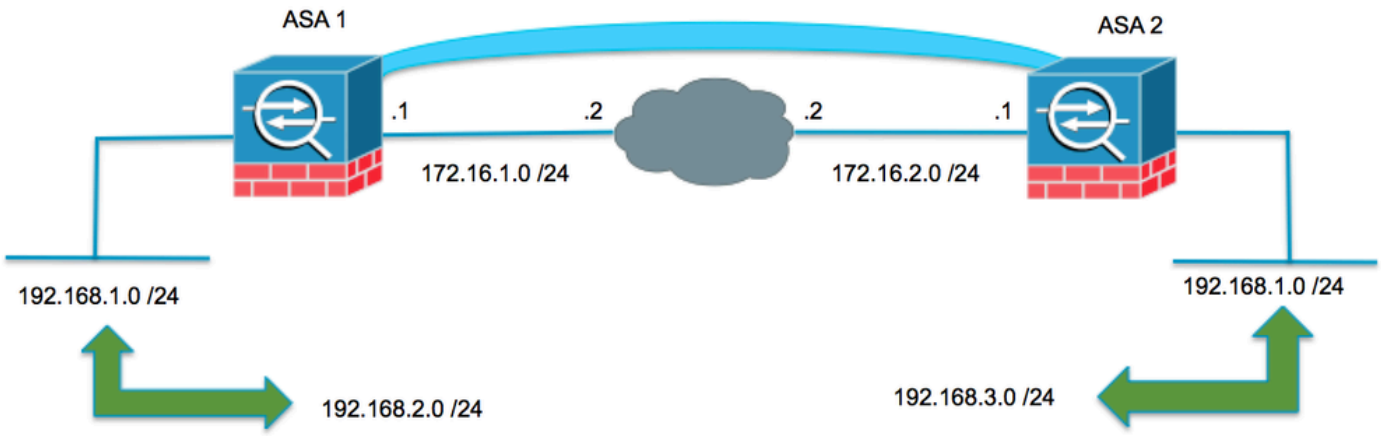
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Chaque périphérique dispose d'un réseau privé protégé derrière lui. Dans les scénarios de chevauchement, la communication à travers le VPN n'a jamais lieu parce que les paquets ne quittent jamais le sous-réseau local puisque le trafic est envoyé à une adresse IP du même sous-réseau. Ceci peut être effectué avec la traduction d'adresses de réseau (NAT) comme expliqué dans les sections suivantes.

Traduction sur les deux terminaux VPN

Lorsque les réseaux protégés par VPN se chevauchent et que la configuration peut être modifiée sur les deux terminaux ; La fonction NAT peut être utilisée pour traduire le réseau local en un sous-réseau différent lorsque vous accédez au sous-réseau traduit distant.



ASA 1

Créez les objets nécessaires pour les sous-réseaux utilisés

```
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
```

Configuration de l'instruction NAT

Créez une instruction manuelle pour traduire le réseau local en un sous-réseau différent uniquement lorsque vous accédez au sous-réseau distant (également traduit)

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

Configurer la liste de contrôle d’accès cryptographique avec les sous-réseaux traduits

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

Configuration de chiffrement 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 utilisés

```
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
```

Configuration de l'instruction NAT

Créez une instruction manuelle pour traduire le réseau local en un sous-réseau différent uniquement lorsque vous accédez au sous-réseau distant (également traduit)

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

Configurer la liste de contrôle d’accès cryptographique avec les sous-réseaux traduits

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

Configuration de chiffrement 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
```

Vérifier

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 SAs
```

```
ASA1(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

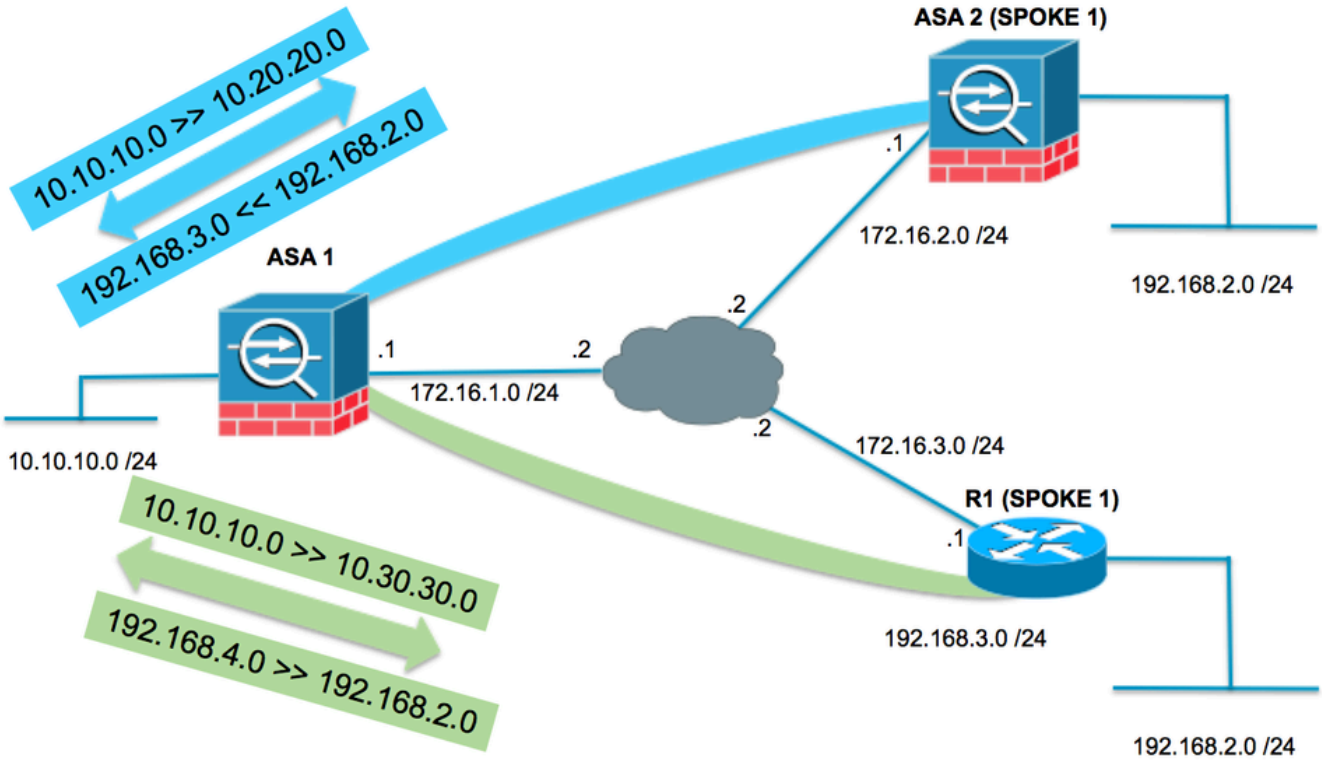

  #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
  #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs 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 0x000003FF
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 Hub and Spoke avec chevauchement des rayons

Dans la topologie suivante, les deux rayons ont le même sous-réseau qui doit être protégé sur le tunnel IPsec vers le concentrateur. Pour faciliter la gestion sur les rayons, la configuration NAT pour contourner le problème de chevauchement est effectuée sur le concentrateur uniquement.



ASA1

Créez les objets nécessaires pour les sous-réseaux utilisés

```
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 des instructions manuelles à traduire :

- Le réseau local 10.10.10.0 /24 à 10.20.20.0 /24 lorsque vous accédez à SPOKE1 (192.168.2.0 /24).
- Le réseau SPOKE1 192.168.2.0 /24 à 192.168.3.0 /24 lorsqu'il arrive à 10.20.20.0 /24.
- Le réseau local 10.10.10.0 /24 à 10.30.30.0 /24 lorsque vous accédez à SPOKE3 (192.168.2.0 /24).

- Le réseau SPOKE2 192.168.2.0 /24 à 192.168.4.0 /24 lorsqu'il arrive à 10.30.30.0 /24.

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

Configurer la liste de contrôle d’accès cryptographique 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
```

Configuration de chiffrement 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 la liste de contrôle d’accès cryptée vers le 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
```

Configuration de chiffrement 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 la liste de contrôle d’accès cryptée vers le 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
```

Configuration de chiffrement 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
```

Vérifier

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 SAs
```

```
ASA1(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)

```
R31show 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 SA
```

```
R1#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 pcp 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:
```

Dépannage

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

Suppression des associations de sécurité

Lorsque vous effectuez un dépannage, veillez à effacer les associations de sécurité existantes après avoir effectué une modification. En mode privilégiée du PIX, utilisez les commandes suivantes :

- clear crypto ipsec sa - Supprime les SA IPsec actives.
- clear crypto isakmp sa - Supprime les SA IKE actives.

Examiner la configuration NAT

- show nat detail - Affiche la configuration NAT avec le ou les objets / groupe(s) d'objets développés

Dépannage des commandes

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

Certaines commandes d'affichage (« show ») sont offertes par l'outil « Cisco CLI Analyzer » réservé aux clients inscrits. Utilisez cet outil pour obtenir une analyse des rapports produits par ces commandes.

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 IPsec de la Phase 2.
- debug crypto isakmp - Affiche les négociations ISAKMP de la Phase 1.

Informations connexes

- Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance
- Négociation IPSec/Protocoles IKE
- Assistance et documentation techniques - Cisco Systems

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.