

# Túneles del sitio a localizar del IPsec de la configuración IKEv1 con el ASDM o el CLI en el ASA

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configure vía el Asistente VPN del ASDM](#)

[Configuración vía el CLI](#)

[Sitio B de la configuración para las Versiones de ASA 8.4 y posterior](#)

[Sitio A de la configuración para las Versiones de ASA 8.2 y anterior](#)

[Directiva del grupo](#)

[Verificación](#)

[ASDM](#)

[CLI](#)

[Fase 1](#)

[Fase 2](#)

[Troubleshooting](#)

[Versiones de ASA 8.4 y posterior](#)

[Versiones de ASA 8.3 y anterior](#)

## Introducción

Este documento describe cómo configurar un túnel del sitio a localizar del IPsec de la versión 1 del intercambio de claves de Internet (IKEv1) entre un dispositivo de seguridad adaptante de las Cisco 5515-X Series (ASA) esa versión de software 9.2.x de los funcionamientos y las Cisco 5510 Series ASA que funcione con la versión de software 8.2.x.

## Prerequisites

### Requisitos

Cisco recomienda que estos requisitos estén cumplidos antes de que usted intente la configuración que se describe en este documento:

- La conectividad del IP de punta a punta debe ser establecida.
- Estos protocolos deben ser permitidos:

User Datagram Protocol (UDP) 500 y 4500 para el avión del control del IPSec

Encapsulating Security Payload (ESP) protocolo IP 50 para el avión de los datos del IPSec

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 5510 Series ASA que funcionan con la versión de software 8.2

- Cisco 5515-X ASA que funciona con la versión de software 9.2

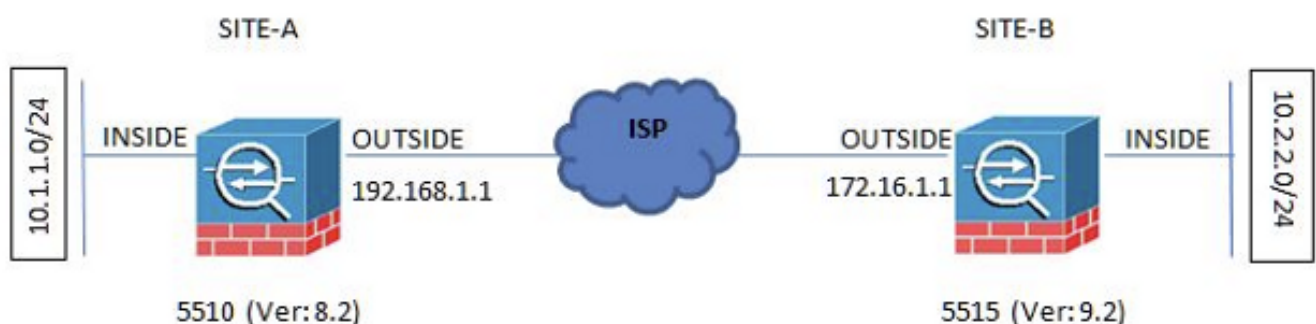
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Configurar

Esta sección describe cómo configurar el túnel del VPN de sitio a sitio vía el Asistente VPN adaptante del Administrador de dispositivos de seguridad (ASDM) o vía el CLI.

### Diagrama de la red

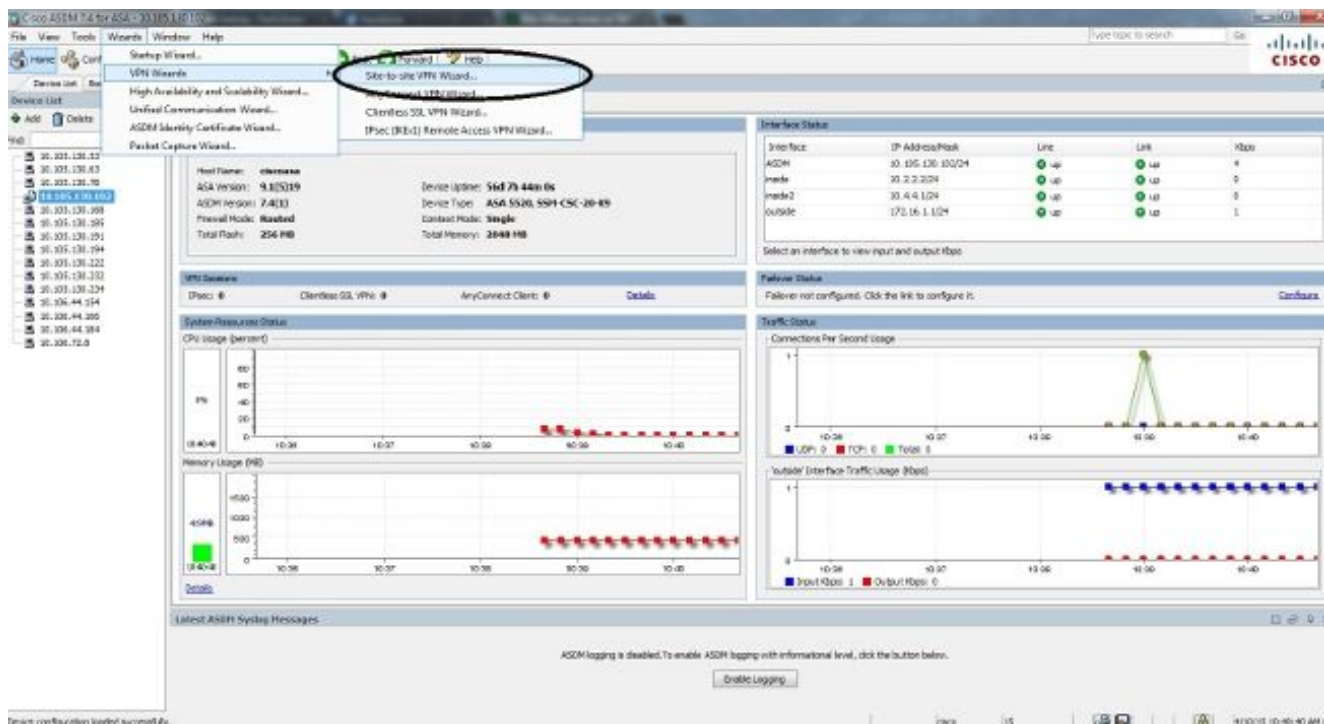
Ésta es la topología que se utiliza para los ejemplos en este documento:



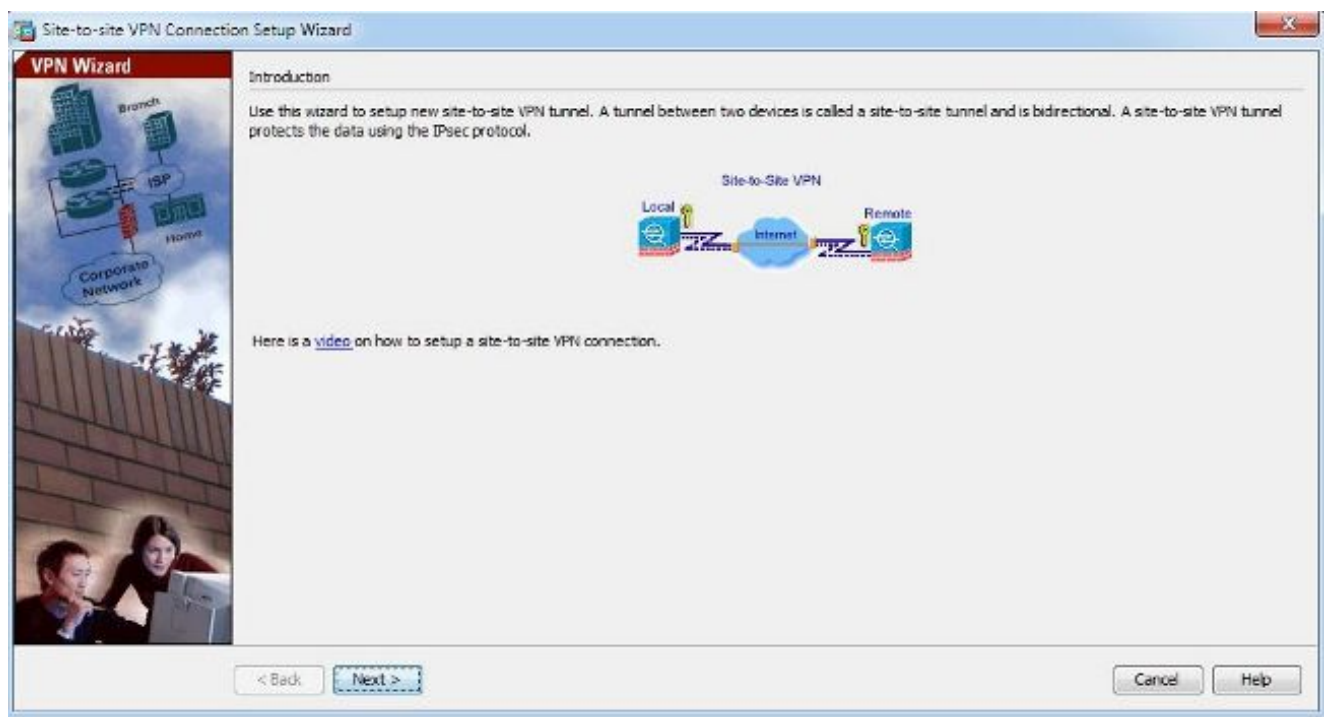
### Configure vía el Asistente VPN del ASDM

Complete estos pasos para configurar el túnel del VPN de sitio a sitio vía el Asistente del ASDM:

1. Abra el ASDM y navegue a los **Asistente > a los Asistentes VPN > al Asistente del VPN de sitio a sitio**:

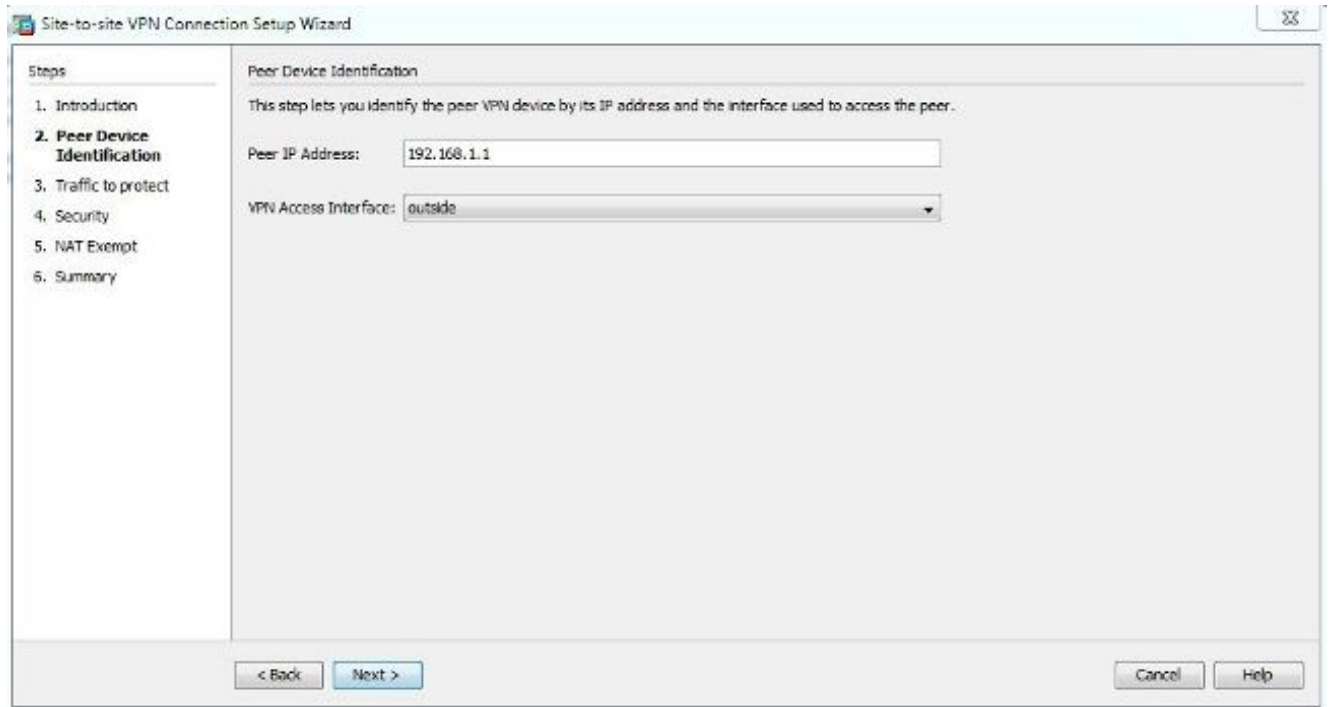


2. Haga clic **después** una vez que usted alcanza el Home Page del Asistente:

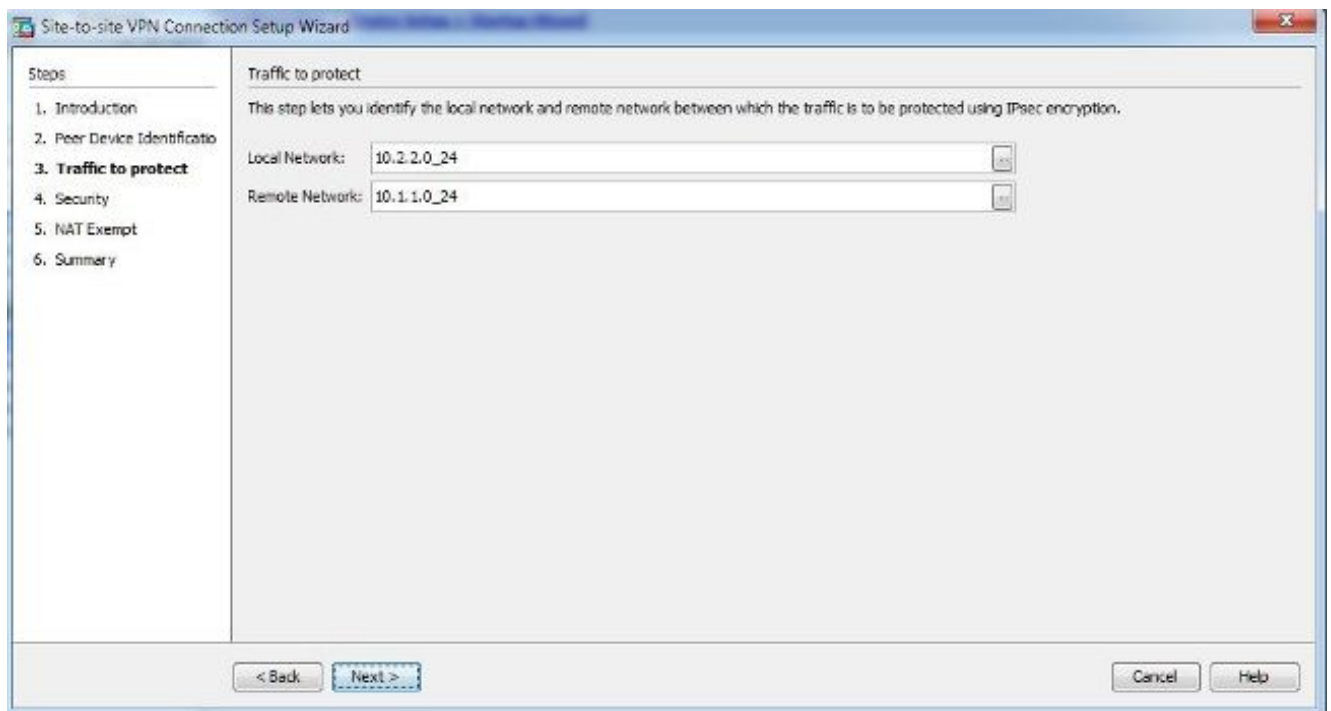


**Note:** Las versiones más recientes del ASDM proporcionan un link a un vídeo que explique esta configuración.

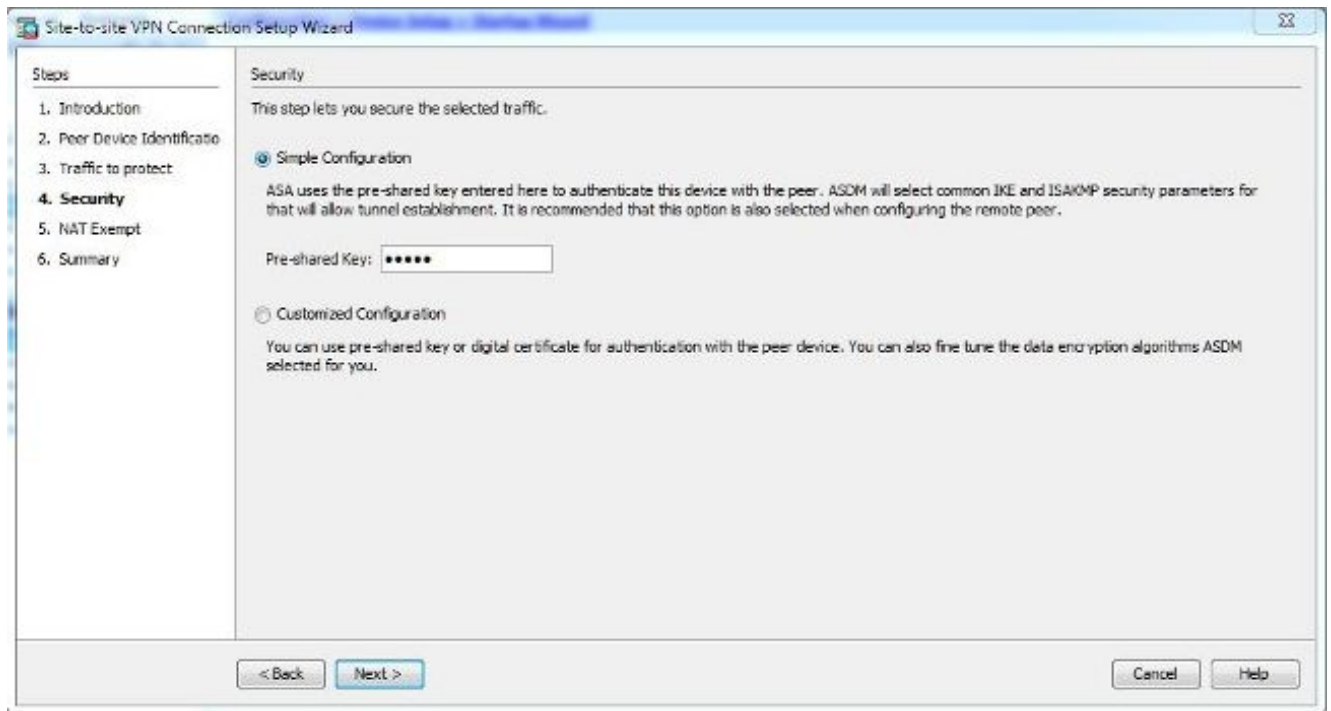
3. Configure el IP Address de Peer. En este ejemplo, el IP Address de Peer se fija a 192.168.1.1 en el sitio B. Si usted configura el IP Address de Peer en el sitio A, debe ser cambiado a 172.16.1.1. La interfaz a través de la cual el extremo remoto puede ser alcanzado también se especifica. Tecleo **después** una vez completo.



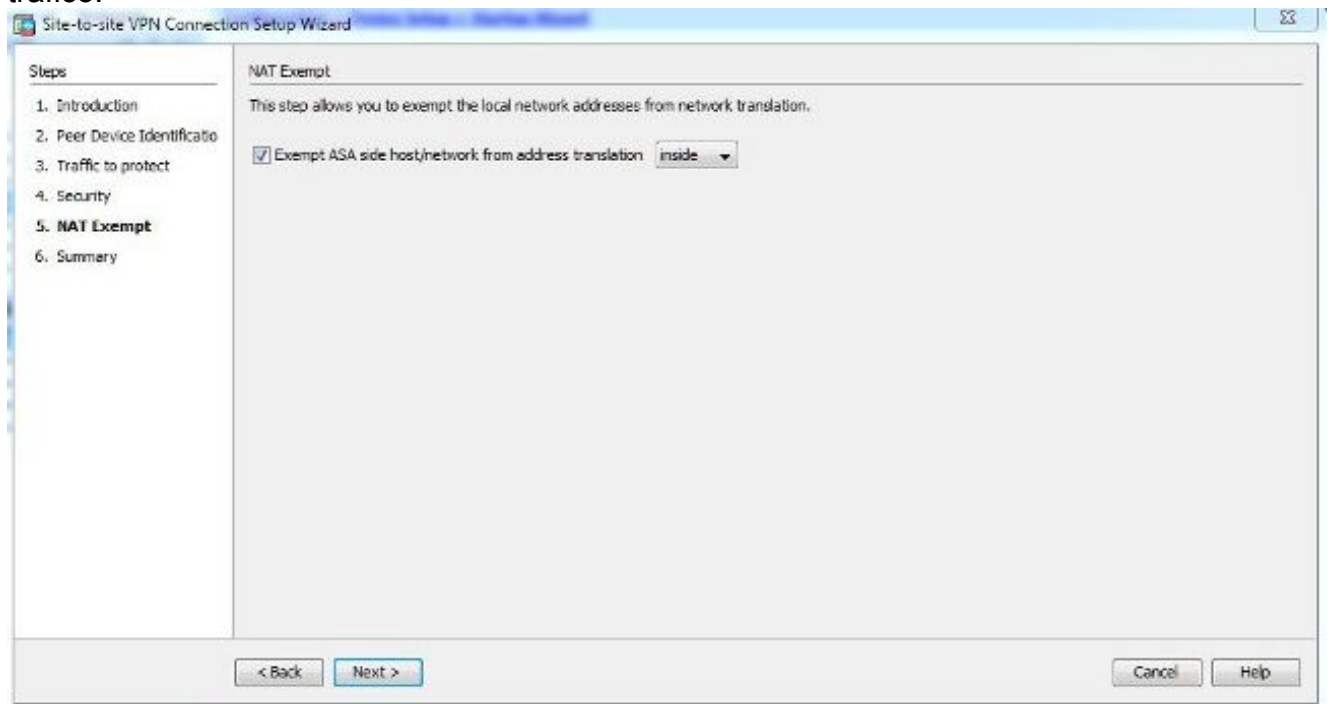
4. Configure las redes locales y remotas (fuente del tráfico y destino). Esta imagen muestra la configuración para el sitio B (el revés solicita el sitio A):



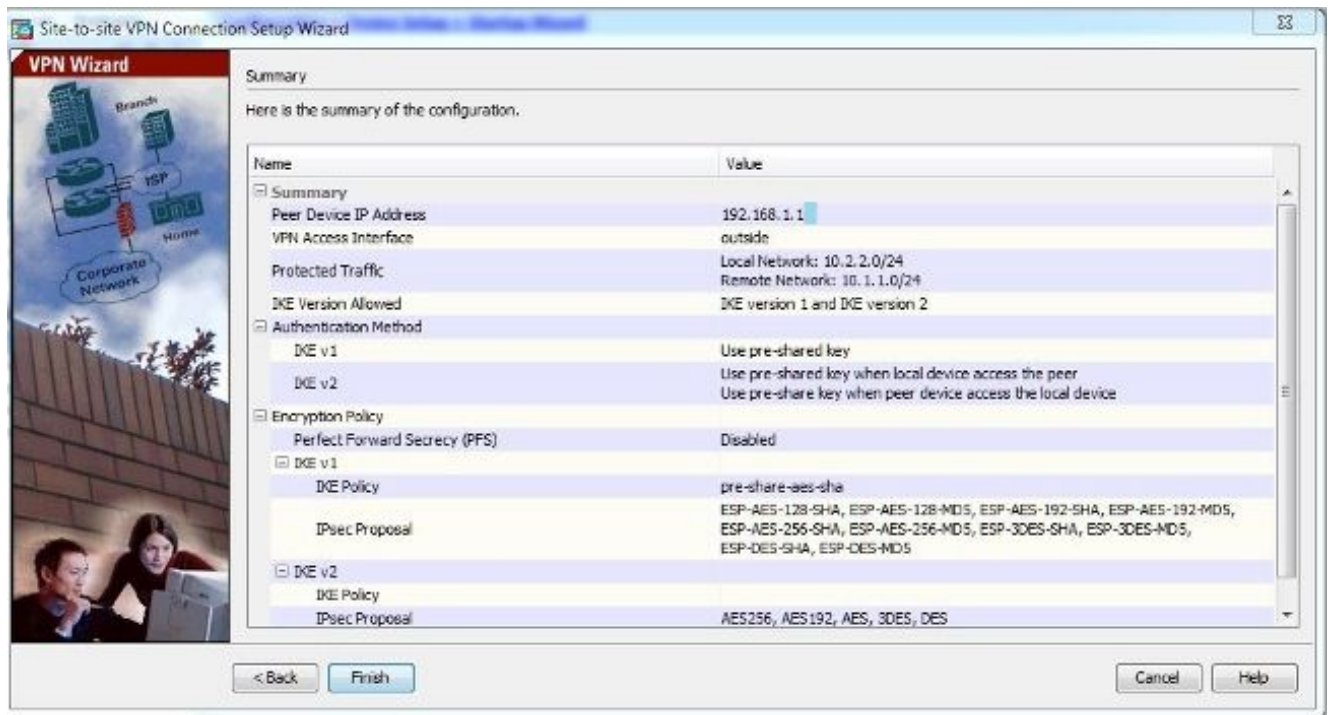
5. En la página Seguridad, configure la clave previamente compartida (debe hacer juego en ambos extremos). Haga clic **después** una vez completo.



6. Configure la interfaz de origen para el tráfico en el ASA. El ASDM crea automáticamente la regla del Network Address Translation (NAT) basada en la Versión de ASA y la avanza con el resto de la configuración en el último paso. **Note:** Por el ejemplo que se utiliza en este documento, *dentro de* es la fuente del tráfico.



7. El Asisistente ahora proporciona un resumen de la configuración que será avanzada al ASA. Revise y verifique los ajustes de la configuración, y entonces el clic en Finalizar.



## Configuración vía el CLI

Esta sección describe cómo configurar el túnel del sitio a localizar del IPsec IKEv1 vía el CLI.

### Sitio B de la configuración para las Versiones de ASA 8.4 y posterior

En las Versiones de ASA 8.4 y posterior, el soporte para IKEv1 y el intercambio de claves de Internet versión 2 (IKEv2) fue introducido.

**Tip:** ¿Para más información sobre las diferencias entre las dos versiones, refiera a [porqué emigre a IKEv2?](#) sección de la *migración rápida de IKEv1 a la configuración del túnel IKEv2 L2L* en el documento de Cisco del código ASA 8.4.

**Tip:** Para un ejemplo de configuración IKEv2 con el ASA, refiera al [túnel del sitio a localizar IKEv2 entre el ASA y el](#) documento de Cisco de los [ejemplos de la configuración del router](#).

### Fase 1 (IKEv1)

Complete estos pasos para la configuración de la fase 1:

1. Ingrese este comando en el CLI para habilitar IKEv1 en la interfaz exterior:

```
crypto ikev1 enable outside
```

2. Cree una directiva IKEv1 que defina los algoritmos/los métodos que se utilizarán para desmenuzar, la autenticación, el grupo Diffie-Hellman, el curso de la vida, y el cifrado:

```
crypto ikev1 enable outside
```

3. Cree a un grupo de túnel bajo atributos del IPsec y configure el IP Address de Peer y la

clave previamente compartida del túnel:

```
crypto ikev1 enable outside
```

## ***Fase 2 (IPSec)***

Complete estos pasos para la configuración de la fase 2:

1. Cree una lista de acceso que defina el tráfico para ser cifrada y tunneled. En este ejemplo, el tráfico del interés es el tráfico del túnel que es originado de la subred de 10.2.2.0 a 10.1.1.0. Puede contener las entradas múltiples si hay subredes múltiples implicadas entre los sitios.

En las versiones 8.4 y posterior, los objetos o los grupos de objetos pueden ser creados que sirven como envases para las redes, las subredes, los IP Addresses del host, o los varios objetos. Cree dos objetos que tengan el local y las subredes remotas y utilícelas para la lista de control de acceso (ACL) crypto y las sentencias NAT.

```
crypto ikev1 enable outside
```

2. Configure el conjunto de la transformación (TS), que debe implicar la palabra clave **IKEv1**. Un TS idéntico se debe crear en el extremo remoto también.

```
crypto ikev1 enable outside
```

3. Configure la correspondencia de criptografía, que contiene estos componentes:

El IP Address de Peer

La lista de acceso definida que contiene el tráfico del interés

El TS

Un Confidencialidad directa perfecta (PFS) opcional que fija, que crea un nuevo par de claves Diffie-Hellman que se utilicen para proteger los datos (ambos lados se debe PFS-habilitar antes de la fase 2 sube)

4. Aplique la correspondencia de criptografía en la interfaz exterior:

```
crypto ikev1 enable outside
```

## ***Exención de NAT***

Asegúrese de que el tráfico VPN no esté sujeto a ninguna otra regla NAT. Ésta es la regla NAT se utiliza que:

```
crypto ikev1 enable outside
```

**Note:** Cuando se utilizan las subredes múltiples, usted debe crear a los grupos de objetos con toda la fuente y subredes de destino y utilizarlas en la regla NAT.

```
crypto ikev1 enable outside
```

### ***Ejemplo de Configuración Completo***

Aquí está la configuración completa para el sitio B:

```
crypto ikev1 enable outside
```

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

```
tunnel-group 192.168.1.1 type ipsec-l2l
tunnel-group 192.168.1.1 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 192.168.1.1
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
```

### **Sitio A de la configuración para las Versiones de ASA 8.2 y anterior**

Esta sección describe cómo configurar el sitio A para las Versiones de ASA 8.2 y anterior.

#### ***Fase 1 (ISAKMP)***

Complete estos pasos para la configuración de la fase 1:

1. Ingrese este comando en el CLI para habilitar el Internet Security Association and Key Management Protocol (ISAKMP) en la interfaz exterior:

```
crypto isakmp enable outside
```

**Note:** Porque las versiones múltiples del IKE (IKEv1 e IKEv2) no se soportan más de largo,



el ISAKMP se utiliza para referir a la fase 1.

2. Cree una política isakmp que defina los algoritmos/los métodos que se utilizarán para construir la fase 1. **Note:** En este ejemplo de configuración, la palabra clave *IKEv1 de la versión 9.x* se substituye por el *ISAKMP*.  
`crypto isakmp enable outside`
3. Cree a un grupo de túnel para el IP Address de Peer (IP Address externo de 5515) con la clave previamente compartida:

```
crypto isakmp enable outside
```

## **Fase 2 (IPSec)**

Complete estos pasos para la configuración de la fase 2:

1. Similar a la configuración en la versión 9.x, usted debe crear una lista de acceso ampliada para definir el tráfico del interés.

```
crypto isakmp enable outside
```

2. Defina un TS que contenga todo el cifrado y algoritmos de troceo disponibles (ofrecidos los problemas tenga un signo de interrogación). Asegúrese de que sea idéntico al que fue configurada en el otro lado.

```
crypto isakmp enable outside
```

3. Configure una correspondencia de criptografía, que contiene estos componentes:

El IP Address de Peer

La lista de acceso definida que contiene el tráfico del interés

El TS

Los PF opcionales que fijan, que crea un nuevo par de claves Diffie-Hellman que se utilicen para proteger los datos (ambos lados deben PFS-ser habilitados de modo que suba la fase 2)

4. Aplique la correspondencia de criptografía en la interfaz exterior:

```
crypto isakmp enable outside
```

## **Exención de NAT**

Cree una lista de acceso que defina el tráfico que se eximirá de los controles NAT. En esta versión, aparece similar a la lista de acceso que usted definió para el tráfico del interés:

```
crypto isakmp enable outside
```

Cuando se utilizan las subredes múltiples, agregue otra línea a la misma lista de acceso:

```
crypto isakmp enable outside
```

La lista de acceso se utiliza con el NAT, como se muestra aquí:

```
crypto isakmp enable outside
```

**Note:** *El interior* aquí refiere al nombre de la interfaz interior en la cual el ASA recibe el tráfico que hace juego la lista de acceso.

### ***Ejemplo de Configuración Completo***

Aquí está la configuración completa para el sitio A:

```
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption aes
hash sha group 2
lifetime 86400

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
pre-shared-key cisco

access-list 100 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0
crypto ipsec transform-set myset esp-aes esp-sha-hmac

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

access-list nonat line 1 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0

nat (inside) 0 access-list nonat
```

### **Directiva del grupo**

Las directivas del grupo se utilizan para definir las configuraciones específicas que se aplican al túnel. Estas directivas se utilizan conjuntamente con el grupo de túnel.

La directiva del grupo se puede definir como cualquiera interno, así que significa que los atributos están tirados del que se defina en el ASA, o puede ser definida como externo, donde los atributos se preguntan de un servidor externo. Éste es el comando que se utiliza para definir la directiva del grupo:

```
group-policy SITE_A internal
```

**Note:** Usted puede definir los atributos múltiples en la directiva del grupo. Para una lista de todos los atributos posibles, refiera a la sección de las [directivas del grupo que configura de los procedimientos de configuración VPN seleccionados del ASDM para las 5500 Series de Cisco ASA, versión 5.2.](#)

## ***Agrupe los atributos opcionales de la directiva***

El atributo del VPN-túnel-**protocolo** determina el tipo de túnel a quien estas configuraciones deben ser aplicadas. En este ejemplo, se utiliza el *IPSec*:

```
group-policy SITE_A internal
```

Usted tiene la opción para configurar el túnel de modo que permanezca la marcha lenta (ningún tráfico) y no vaya abajo. Para configurar esta opción, el valor de atributo del VPN-ocioso-**descanso** debe utilizar los minutos, o usted puede fijar el valor a **ningunos**, así que significa que nunca va el túnel abajo.

Aquí tiene un ejemplo:

```
group-policy SITE_A internal
```

El comando de la valor por defecto-grupo-**directiva** bajo atributos generales del grupo de túnel define la directiva del grupo que se utiliza para avanzar ciertas configuraciones de la directiva para el túnel se establece que. Las configuraciones predeterminadas para las opciones que usted no definió en la directiva del grupo se toman de una directiva del grupo predeterminado global:

```
group-policy SITE_A internal
```

## **Verificación**

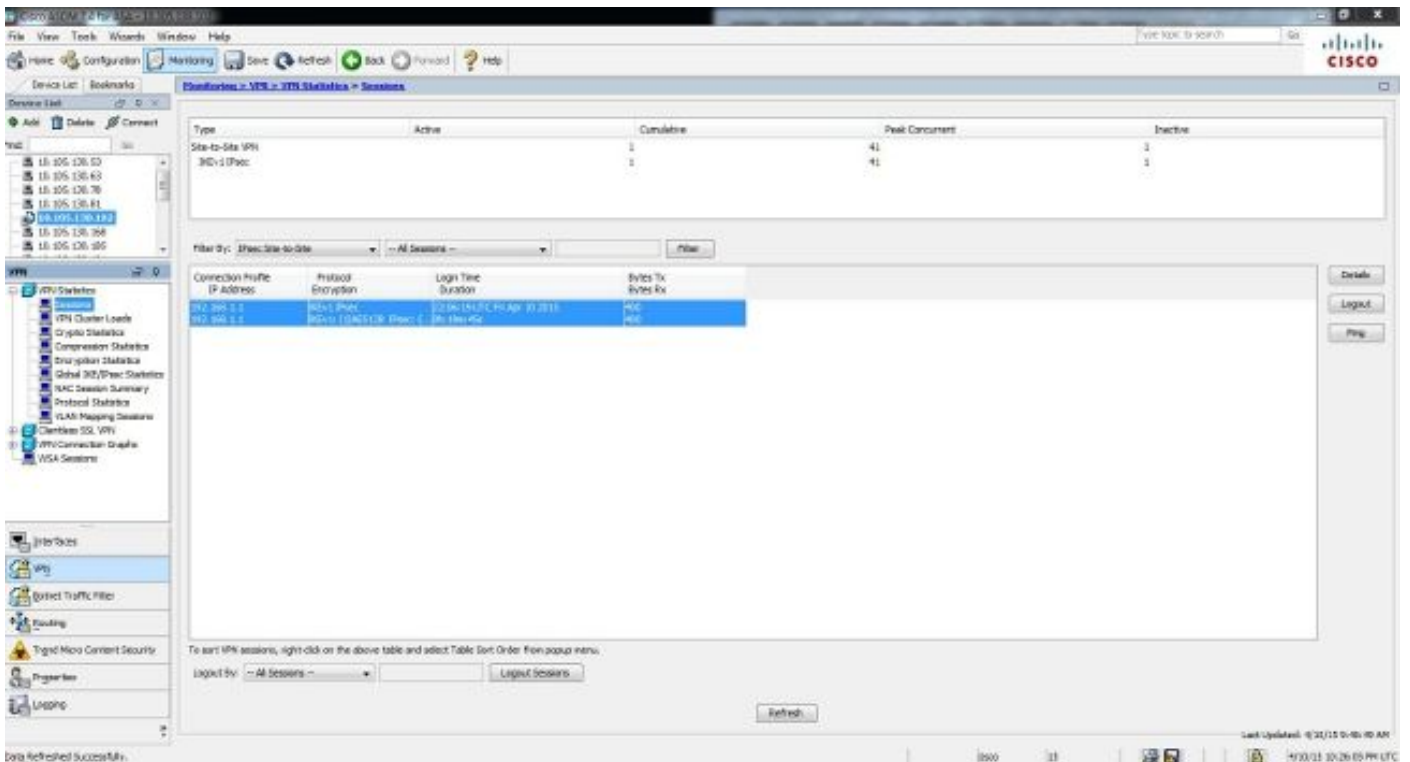
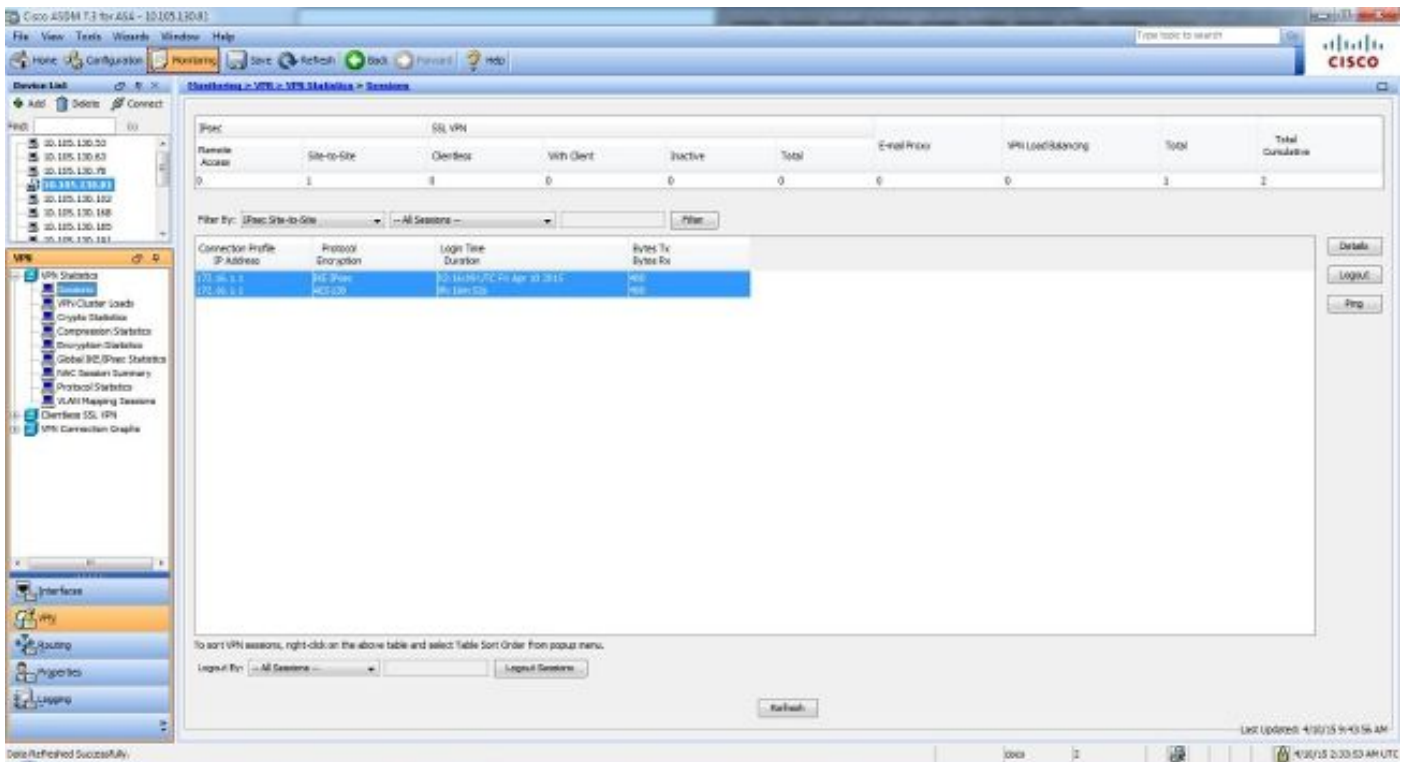
Utilice la información que se proporciona en esta sección para verificar que su configuración trabaja correctamente.

## **ASDM**

Para ver el estado del túnel del ASDM, navegue a **monitorear > VPN**. Se proporciona esta información:

- El IP Address de Peer
- El protocolo que se utiliza para construir el túnel
- El algoritmo de encriptación se utiliza que
- El tiempo en el cual el túnel subió y el para arriba-tiempo
- El número de paquetes se reciben y se transfieren que

**Tip:** El tecleo **restaura** para ver los últimos valores, pues los datos no se ponen al día en el tiempo real.



## CLI

Esta sección describe cómo verificar su configuración vía el CLI.

### Fase 1

Ingrese este comando en el CLI para verificar la configuración de la fase 1 en los 5515) lados del sitio B (:

```
show crypto ikev1 sa
```

```
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: 192.168.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```

Ingrese este comando en el CLI para verificar la configuración de la fase 1 en los 5510) lados del sitio A (:

```
show crypto isakmp sa
```

```
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
```

## Fase 2

El comando **show crypto ipsec sa** muestra el SA de IPsec que se construye entre los pares. El túnel encriptado se construye entre los IP Addresses 192.168.1.1 y 172.16.1.1 para el tráfico que fluye entre las redes 10.1.1.0 y 10.2.2.0. Usted puede ver los dos ESP SA construido para el tráfico entrante y saliente. El Encabezado de autenticación no se utiliza porque no hay AH SA.

Ingrese este comando en el CLI para verificar la configuración de la fase 2 en los 5515) lados del sitio B (:

```
interface: FastEthernet0
Crypto map tag: outside_map, local addr. 172.16.1.1
  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: 192.168.1.1
PERMIT, flags={origin_is_acl,}
#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: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0, #send errors 0, #recv errors 0
  local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound esp sas:
spi: 0x136A010F(325714191)
  transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: outside_map
  sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
inbound pcp sas:
outbound esp sas:
spi: 0x3D3(979)
  transform: esp-aes esp-sha-hmac ,
```

```
in use settings = {Tunnel, }
slot: 0, conn id: 3443, flow_id: 1444, crypto map: outside_map
    sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas
```

Ingrese este comando en el CLI para verificar la configuración de la fase 2 en los 5510) lados del sitio A (:

```
interface: FastEthernet0
Crypto map tag: outside_map, local addr. 192.168.1.1
    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: 172.16.1.1
PERMIT, flags={origin_is_acl,}
    #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: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0, #send errors 0, #recv errors 0
    local crypto endpt.: 192.168.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound esp sas:
spi: 0x136A010F(325714191)
    transform: esp-aes esp-sha-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: outside_map
    sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
inbound pcp sas:
outbound esp sas:
spi: 0x3D3(979)
    transform: esp-aes esp-sha-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 3443, flow_id: 1444, crypto map: outside_map
    sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas
```

## Troubleshooting

Utilice la información que se proporciona en esta sección para resolver problemas los problemas de configuración.

### Versiones de ASA 8.4 y posterior

Ingrese estos comandos debug para determinar la ubicación del incidente del túnel:

- debug crypto ikev1 127 (fase 1)

## • IPsec del debug crypto 127 (fase 2)

Aquí está una salida de los debugs completa del ejemplo:

```
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [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=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE Initiator: New Phase 1, Intf NP
Identity Ifc, IKE Peer 192.168.1.1 local Proxy Address 10.2.2.0, remote Proxy
Address 10.1.1.0, Crypto map (outside_map) Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing ISAKMP SA payload Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing NAT-Traversal VID ver 02 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver 03 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver RFC payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Fragmentation VID +
extended capabilities payload
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 172
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total
length : 132
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing SA payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Oakley proposal is acceptable
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received NAT-Traversal ver 02 VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Fragmentation VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, IKE Peer included IKE
fragmentation capability flags: Main Mode: True Aggressive Mode: True
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing ke payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Cisco Unity
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing xauth V6
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send IOS VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send Altiga/Cisco VPN3000/Cisco
ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
```

(13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ke payload  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ISA\_KE payload  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing nonce payload  
Feb 13 23:48:56 [IKEv1 DEBUG]?IP = 192.168.1.1, processing VID payload  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Cisco Unity client VID  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received xauth V6 VID  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing VPN3000/ASA spoofing  
IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Altiga/Cisco  
VPN3000/Cisco ASA GW VID  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload  
!  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash  
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, **Connection landed on tunnel\_group**  
**192.168.1.1**  
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, Generating  
keys for Initiator...  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing  
ID payload  
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, constructing  
hash payload  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing  
hash for ISAKMP  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing IOS keep alive  
payload: proposal=32767/32767 sec.  
!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/10 ms  
ciscoasa# Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,  
constructing dpd vid payload  
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE\_DECODE SENDING Message (msgid=0)  
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +  
NONE (0) total length : 96  
**Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Automatic NAT**  
**Detection Status: Remote end is NOT behind a NAT device This end is NOT behind**  
**a NAT device**  
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500  
from 192.168.1.1:500  
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE\_DECODE RECEIVED Message (msgid=0)  
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +  
NONE (0) total length : 96  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing  
ID payload  
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,  
ID\_IPV4\_ADDR ID received 192.168.1.1  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,  
processing hash payload  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing  
hash for ISAKMP  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing IOS keep alive payload:  
proposal=32767/32767 sec.  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing  
VID payload  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Received  
DPD VID  
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Connection landed on tunnel\_group  
192.168.1.1  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Oakley  
begin quick mode



Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator starting QM: msg id = 4c073b21

**Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 1 COMPLETED**

Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Keep-alive type for this connection: DPD

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting P1 rekey timer: 73440 seconds.

IPSEC: New embryonic SA created @ 0x75298588,  
SCB: 0x75C34F18,  
Direction: inbound  
SPI : 0x03FC9DB7  
Session ID: 0x00004000  
VPIF num : 0x00000002  
Tunnel type: 121  
Protocol : esp  
Lifetime : 240 seconds

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, IKE got SPI from key engine: SPI = 0x03fc9db7

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, oakley constructing quick mode

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing blank hash payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing IPsec SA payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing IPsec nonce payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing proxy ID

**Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Transmitting Proxy Id:**

**Local subnet: 10.2.2.0 mask 255.255.255.0 Protocol 0 Port 0**

**Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0**

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator sending Initial Contact

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing qm hash payload

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator sending 1st QM pkt: msg id = 4c073b21

Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE\_DECODE SENDING Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200

Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500 from 192.168.1.1:500

Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE\_DECODE RECEIVED Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing hash payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing SA payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing nonce payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing ID payload

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, ID\_IPV4\_ADDR\_SUBNET ID received--10.2.2.0--255.255.255.0

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing ID payload

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, ID\_IPV4\_ADDR\_SUBNET ID received--10.1.1.0--255.255.255.0

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, loading all IPSEC SAs

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Generating Quick Mode Key!

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

NP encrypt rule look up for crypto map outside\_map 20 matching ACL  
100: returned cs\_id=6ef246d0; encrypt\_rule=752972d0;  
tunnelFlow\_rule=75ac8020  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,  
Generating Quick Mode Key!  
IPSEC: New embryonic SA created @ 0x6f0e03f0,  
SCB: 0x75B6DD00,  
Direction: outbound  
SPI : 0x1BA0C55C  
Session ID: 0x00004000  
VPIF num : 0x00000002  
Tunnel type: 121  
Protocol : esp  
Lifetime : 240 seconds  
IPSEC: Completed host OBSA update, SPI 0x1BA0C55C  
IPSEC: Creating outbound VPN context, SPI 0x1BA0C55C  
Flags: 0x00000005  
SA : 0x6f0e03f0  
SPI : 0x1BA0C55C  
MTU : 1500 bytes  
VCID : 0x00000000  
Peer : 0x00000000  
SCB : 0x0B47D387  
Channel: 0x6ef0a5c0  
IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C  
VPN handle: 0x0000f614  
IPSEC: New outbound encrypt rule, SPI 0x1BA0C55C  
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 outbound encrypt rule, SPI 0x1BA0C55C  
Rule ID: 0x74e1c558  
IPSEC: New outbound permit rule, SPI 0x1BA0C55C  
Src addr: 172.16.1.1  
Src mask: 255.255.255.255  
Dst addr: 192.168.1.1  
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: 0x1BA0C55C  
Use SPI: true  
IPSEC: Completed outbound permit rule, SPI 0x1BA0C55C  
Rule ID: 0x6f0dec80

**Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, NP encrypt rule look up for crypto map outside\_map 20 matching ACL 100: returned cs\_id=6ef246d0; encrypt\_rule=752972d0; tunnelFlow\_rule=75ac8020**

Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Security negotiation complete for LAN-to-LAN Group (192.168.1.1) Initiator, Inbound SPI = 0x03fc9db7, Outbound SPI = 0x1ba0c55c

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, oakley constructing final quick mode

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator sending 3rd QM pkt: msg id = 4c073b21

Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE\_DECODE SENDING Message (msgid=4c073b21) with payloads : HDR + HASH (8) + NONE (0) total length : 76

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, IKE got a KEY\_ADD msg for SA: SPI = 0x1ba0c55c

IPSEC: New embryonic SA created @ 0x75298588,  
SCB: 0x75C34F18,

Direction: inbound

SPI : 0x03FC9DB7

Session ID: 0x00004000

VPIF num : 0x00000002

Tunnel type: 121

Protocol : esp

Lifetime : 240 seconds

IPSEC: Completed host IBSA update, SPI 0x03FC9DB7

IPSEC: Creating inbound VPN context, SPI 0x03FC9DB7

Flags: 0x00000006

SA : 0x75298588

SPI : 0x03FC9DB7

MTU : 0 bytes

VCID : 0x00000000

Peer : 0x0000F614

SCB : 0x0B4707C7

Channel: 0x6ef0a5c0

IPSEC: Completed inbound VPN context, SPI 0x03FC9DB7

VPN handle: 0x00011f6c

IPSEC: Updating outbound VPN context 0x0000F614, SPI 0x1BA0C55C

Flags: 0x00000005

SA : 0x6f0e03f0

SPI : 0x1BA0C55C

MTU : 1500 bytes

VCID : 0x00000000

Peer : 0x00011F6C

SCB : 0x0B47D387

Channel: 0x6ef0a5c0

IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C

VPN handle: 0x0000f614

IPSEC: Completed outbound inner rule, SPI 0x1BA0C55C

Rule ID: 0x74e1c558

IPSEC: Completed outbound outer SPD rule, SPI 0x1BA0C55C

Rule ID: 0x6f0dec80

IPSEC: New inbound tunnel flow rule, SPI 0x03FC9DB7

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 inbound tunnel flow rule, SPI 0x03FC9DB7
Rule ID: 0x74e1b4a0
IPSEC: New inbound decrypt rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
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: 0x03FC9DB7
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x03FC9DB7
Rule ID: 0x6f0de830
IPSEC: New inbound permit rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
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: 0x03FC9DB7
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x03FC9DB7
Rule ID: 0x6f0de8d8
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Pitcher:
received KEY_UPDATE, spi 0x3fc9db7
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting
P2 rekey timer: 24480 seconds.
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 2
COMPLETED (msgid=4c073b21)

```

## Versiones de ASA 8.3 y anterior

Ingrese estos comandos debug para determinar la ubicación del incidente del túnel:

- **isakmp del debug crypto 127 (fase 1)**
- **IPSec del debug crypto 127 (fase 2)**

Aquí está una salida de los debugs completa del ejemplo:

Feb 13 04:19:53 [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

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing SA payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Oakley proposal is acceptable

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal ver 02 VID

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal ver 03 VID

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal RFC VID

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Fragmentation VID

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, IKE Peer included IKE fragmentation capability flags: Main Mode: True Aggressive Mode: True

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing IKE SA payload

**Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, IKE SA Proposal # 1, Transform # 1 acceptable Matches global IKE entry # 1**

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing ISAKMP SA payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Traversal VID ver 02 payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing Fragmentation VID + extended capabilities payload

Feb 13 04:19:53 [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

Feb 13 04:19:53 [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) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing ke payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing ISA\_KE payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing nonce payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Cisco Unity client VID

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received xauth V6 VID

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing VPN3000/ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Altiga/Cisco VPN3000/Cisco ASA GW VID

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing NAT-Discovery payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing NAT-Discovery payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing ke payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing nonce payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing Cisco Unity VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing xauth V6 VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Send IOS VID

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Send Altiga/Cisco VPN3000/Cisco ASA GW VID

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash

**Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel\_group 172.16.1.1**

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating keys for Responder...

Feb 13 04:19:53 [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 (130) + NAT-D (130) + NONE (0) total length : 304

Feb 13 04:19:53 [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

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing ID payload

Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID\_IPV4\_ADDR ID received 172.16.1.1

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing hash payload

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Computing hash for ISAKMP

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing IOS keep alive payload: proposal=32767/32767 sec.

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Received DPD VID

**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device**

**Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel\_group 172.16.1.1**

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing ID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing hash payload

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Computing hash for ISAKMP

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing IOS keep alive payload: proposal=32767/32767 sec.

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing dpd vid payload

Feb 13 04:19:53 [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

**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 1 COMPLETED**

Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Keep-alive type for this connection: DPD

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P1 rekey timer: 82080 seconds.

Feb 13 04:19:53 [IKEv1 DECODE]: IP = 172.16.1.1, IKE Responder starting QM: msg id = 4c073b21

Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE\_DECODE RECEIVED Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing hash payload

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing SA payload

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing nonce payload

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing ID payload

Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID\_IPV4\_ADDR\_SUBNET ID received--10.2.2.0--255.255.255.0

Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received remote IP Proxy Subnet data in ID Payload: Address 10.2.2.0, Mask 255.255.255.0, Protocol 0, Port 0

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing ID payload

Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID\_IPV4\_ADDR\_SUBNET ID received--10.1.1.0--255.255.255.0

Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received local IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,

Protocol 0, Port 0  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing notify payload  
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, QM IsRekeyed old sa not found by addr  
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map check, checking map = outside\_map, seq = 20...  
**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map check, map outside\_map, seq = 20 is a successful match**  
**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Remote Peer configured for crypto map: outside\_map**  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing IPsec SA payload  
**Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IPsec SA Proposal # 1, Transform # 1 acceptable Matches global IPsec SA entry # 20**  
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE: requesting SPI!  
IPSEC: New embryonic SA created @ 0xAB5C63A8,  
SCB: 0xABD54E98,  
Direction: inbound  
SPI : 0x1BA0C55C  
Session ID: 0x00004000  
VPIF num : 0x00000001  
Tunnel type: 121  
Protocol : esp  
Lifetime : 240 seconds  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got SPI from key engine: SPI = 0x1ba0c55c  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, oakley constructing quick mode  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing blank hash payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing IPsec SA payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing IPsec nonce payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing proxy ID  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Transmitting Proxy Id:  
Remote subnet: 10.2.2.0 Mask 255.255.255.0 Protocol 0 Port 0  
Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing qm hash payload  
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Responder sending 2nd QM pkt: msg id = 4c073b21  
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE\_DECODE SENDING Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172  
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE\_DECODE RECEIVED Message (msgid=4c073b21) with payloads : HDR + HASH (8) + NONE (0) total length : 52  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing hash payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, loading all IPSEC SAs  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating Quick Mode Key!  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt rule look up for crypto map outside\_map 20 matching ACL 100: returned cs\_id=ab9302f0; rule=ab9309b0  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating Quick Mode Key!  
IPSEC: New embryonic SA created @ 0xAB570B58,  
SCB: 0xABD55378,  
Direction: outbound

SPI : 0x03FC9DB7  
Session ID: 0x00004000  
VPIF num : 0x00000001  
Tunnel type: 121  
Protocol : esp  
Lifetime : 240 seconds  
IPSEC: Completed host OBSA update, SPI 0x03FC9DB7  
IPSEC: Creating outbound VPN context, SPI 0x03FC9DB7  
Flags: 0x00000005  
SA : 0xAB570B58  
SPI : 0x03FC9DB7  
MTU : 1500 bytes  
VCID : 0x00000000  
Peer : 0x00000000  
SCB : 0x01512E71  
Channel: 0xA7A98400  
IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7  
VPN handle: 0x0000F99C  
IPSEC: New outbound encrypt rule, SPI 0x03FC9DB7  
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 0x03FC9DB7  
Rule ID: 0xABD557B0  
IPSEC: New outbound permit rule, SPI 0x03FC9DB7  
Src addr: 192.168.1.1  
Src mask: 255.255.255.255  
Dst addr: 172.16.1.1  
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: 0x03FC9DB7  
Use SPI: true  
IPSEC: Completed outbound permit rule, SPI 0x03FC9DB7  
Rule ID: 0xABD55848  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt rule  
look up for crypto map outside\_map 20 matching ACL 100: returned cs\_id=ab9302f0;  
rule=ab9309b0  
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Security negotiation  
complete for LAN-to-LAN Group (172.16.1.1) Responder, Inbound SPI = 0x1ba0c55c,  
Outbound SPI = 0x03fc9db7  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got a  
KEY\_ADD msg for SA: SPI = 0x03fc9db7



IPSEC: Completed host IBSA update, SPI 0x1BA0C55C  
IPSEC: Creating inbound VPN context, SPI 0x1BA0C55C  
Flags: 0x00000006  
SA : 0xAB5C63A8  
SPI : 0x1BA0C55C  
MTU : 0 bytes  
VCID : 0x00000000  
Peer : 0x0000F99C  
SCB : 0x0150B419  
Channel: 0xA7A98400  
IPSEC: Completed inbound VPN context, SPI 0x1BA0C55C  
VPN handle: 0x0001169C  
IPSEC: Updating outbound VPN context 0x0000F99C, SPI 0x03FC9DB7  
Flags: 0x00000005  
SA : 0xAB570B58  
SPI : 0x03FC9DB7  
MTU : 1500 bytes  
VCID : 0x00000000  
Peer : 0x0001169C  
SCB : 0x01512E71  
Channel: 0xA7A98400  
IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7  
VPN handle: 0x0000F99C  
IPSEC: Completed outbound inner rule, SPI 0x03FC9DB7  
Rule ID: 0xABD557B0  
IPSEC: Completed outbound outer SPD rule, SPI 0x03FC9DB7  
Rule ID: 0xABD55848  
IPSEC: New inbound tunnel flow rule, SPI 0x1BA0C55C  
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 0x1BA0C55C  
Rule ID: 0xAB8D98A8  
IPSEC: New inbound decrypt rule, SPI 0x1BA0C55C  
Src addr: 172.16.1.1  
Src mask: 255.255.255.255  
Dst addr: 192.168.1.1  
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: 0x1BA0C55C  
Use SPI: true  
IPSEC: Completed inbound decrypt rule, SPI 0x1BA0C55C

Rule ID: 0xABD55CB0  
IPSEC: New inbound permit rule, SPI 0x1BA0C55C  
Src addr: 172.16.1.1  
Src mask: 255.255.255.255  
Dst addr: 192.168.1.1  
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: 0x1BA0C55C  
Use SPI: true  
IPSEC: Completed inbound permit rule, SPI 0x1BA0C55C  
Rule ID: 0xABD55D48  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Pitcher: received  
KEY\_UPDATE, spi 0x1ba0c55c  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P2 rekey  
timer: 27360 seconds.  
**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 2 COMPLETED  
(msgid=4c073b21)**