Ejemplo de configuración Dinámico-a-estático ASA-a-ASA IKEv1/IPsec

Contenido

Introducción

Este documento describe cómo permitir al dispositivo de seguridad adaptante (ASA) para validar las conexiones dinámicas del VPN de sitio a sitio del IPSec de cualquier par dinámico (ASA en este caso). Mientras que el diagrama de la red en este documento muestra, se establece el túnel IPsec cuando el túnel se inicia del extremo Telecontrol-ASA solamente. El Central-ASA no puede iniciar un túnel VPN debido a la configuración IPSec dinámica. La dirección IP del Telecontrol-ASA es desconocida.

Configuración Central-ASA para validar dinámicamente las conexiones de una dirección IP del comodín (0.0.0.0/0) y de una clave comodín previamente compartida. El Telecontrol-ASA entonces se configura para cifrar el tráfico del local a las subredes Central-ASA según lo especificado por la lista de acceso crypto. Los ambos lados realizan la exención del Network Address Translation (NAT) para desviar el NAT para el tráfico IPSec.

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en la versión de software de firewall de Cisco ASA (5510 y 5520) 9.x y posterior.

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

> **Note**: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

Configuración de ASDM

Central-ASA (peer estático)

En un ASA con un IP Address estático, configure el VPN de una manera tal que valide las conexiones dinámicas de un par desconocido mientras que todavía autentica al par que usa una clave previamente compartida IKEv1:

1. Elija la **configuración > el VPN de sitio a sitio > avanzó > las correspondencias de criptografía.** La ventana visualiza la lista de entradas de correspondencia de criptografía que sean ya en el lugar (si hay ninguno). Puesto que el ASA no conoce cuáles es el IP Address de Peer, para que el ASA valide el **mapa dinámico de la** configuración de la conexión con el transforme el conjunto que corresponde con (oferta del IPSec). Haga clic en Add (Agregar).
2. En la ventana de la regla del IPSec del crear, de la directiva del túnel (correspondencia de criptografía) - la lengueta básica, elige **afuera de la** lista desplegable de la interfaz y **dinámico de la** lista desplegable del tipo de la directiva. En el campo de prioridad, asigne la prioridad para esta entrada en caso de que haya entradas múltiples bajo el mapa dinámico. Después, tecleo **selecto** al lado del campo de la oferta del IPSec del v1 IKE para seleccionar la oferta del IPSec.
3. Cuando el cuadro de diálogo selecto de las ofertas del IPSec (transforme los conjuntos) se abre, elija entre las ofertas actuales del IPSec o el tecleo **agrega** para crear un nuevo y

utilizar lo mismo. Haga Click en OK cuando le hacen.

4. De la directiva del túnel (correspondencia de criptografía) - la ficha Avanzadas, marca la casilla de verificación del **permiso NAT-T** (requerida si cualquier par está detrás de un dispositivo NAT) y la casilla de verificación del **Reverse Route Injection del permiso**. Cuando el túnel VPN sube para el par dinámico, el ASA instala una ruta dinámico para la red VPN remota negociada que las puntas al VPN interconectan.Opcionalmente, de la lengueta de la selección del tráfico usted puede también definir el tráfico interesante VPN para el par dinámico y hacer clic la **AUTORIZACIÓN**. Según lo mencionado anterior, puesto que el ASA no tiene ninguna información sobre el IP Address de Peer dinámico remoto, el pedido de conexión el desconocido aterriza bajo DefaultL2LGroup que exista en el ASA por abandono. Para que la autenticación tenga éxito la clave previamente compartida (cisco123 en este ejemplo) configurada en el peer remoto necesita hacer juego con un DefaultL2LGroup inferior.
5. Elija la **configuración > el VPN de sitio a sitio > avanzó > los grupos de túnel**, **DefaultL2LGroup** selecto, tecleo **editan** y configuran la clave previamente compartida deseada. Haga Click en OK cuando le hacen.**Note**: Esto crea una clave previamente compartida del comodín en el peer estático (Central-ASA). Cualquier dispositivo/par que conozca esta clave previamente compartida y sus ofertas que corresponden con puede establecer con éxito un túnel VPN y acceder los recursos sobre el VPN. Asegúrese que esta clave PRE-skared no esté compartida con las entidades desconocidas y que no sea fácil de conjeturar.
6. Elija las **directivas de la configuración** > del **VPN de sitio a sitio** > del **grupo** y seleccione la grupo-directiva de su opción (grupo-directiva predeterminada en este caso). El tecleo **edita** y edita la directiva del grupo en el cuadro de diálogo del Internal group policy (política grupal interna) del editar. Haga Click en OK cuando le hacen.
7. Elija la **configuración** > el **Firewall** > las **reglas NAT** y de la ventana nacional de la regla del agregar, configuran una regla no nacional (NAT-EXEMPT) para el tráfico VPN. Haga Click en OK cuando le hacen.

Telecontrol-ASA (par dinámico)

1. Elija los **Asisitente > los Asistentes VPN > al Asisitente del VPN de sitio a sitio** una vez que la aplicación ASDM conecta con el ASA.
2. Haga clic en Next (Siguiente).
3. Elija **afuera de la** lista desplegable de la interfaz de acceso VPN para especificar el IP Address externo del peer remoto. Seleccione la interfaz (**WAN)** donde está aplicada la correspondencia de criptografía. Haga clic en Next (Siguiente).
4. Especifique los host/las redes que se deben permitir pasar a través del túnel VPN. En este paso, usted necesita proporcionar las redes locales y las redes remotas para el VPN hacen un túnel. Haga clic los botones al lado de los campos de la red local y de la red remota y elija el direccionamiento según el requisito. Haga clic **después** cuando le hacen.
5. Ingrese la información de autenticación para utilizar, que es clave previamente compartida en este ejemplo. La clave previamente compartida usada en este ejemplo es cisco123. El nombre de grupo de túnel es la dirección IP del peer remoto por abandono si usted configura el LAN a LAN (L2L) VPN.**O**Usted puede personalizar la configuración para incluir el IKE y la directiva del IPSec de su opción. Necesita ser por lo menos una directiva que corresponde con entre los pares:De los métodos de autentificación tabule, ingrese la clave previamente

compartida de la versión 1 IKE en el campo de clave previamente compartida. En este ejemplo, es **cisco123**.Haga clic la lengueta de los **algoritmos de encripción**.
6. El tecleo **maneja** al lado del campo de la política IKE, el tecleo **agrega** y configura una política IKE de encargo **(**phase-1**)**. Haga Click en OK cuando le hacen.
7. Haga clic **selecto** al lado el campo de la oferta del IPSec y seleccione la oferta deseada del IPSec. Haga clic **después** cuando le hacen.Opcionalmente, usted puede ir a la lengueta de la perfecta reserva hacia adelante y marcar la casilla de verificación del **Confidencialidad directa perfecta (PFS) del permiso**. Tecleo **después** cuando le hacen.
8. Marque el **host/la red exentos del lado ASA de la** casilla de verificación de la **traducción de la dirección** para prevenir el tráfico de túnel desde el principio de la traducción de dirección de red. Elija el **local o el interior de la** lista desplegable para fijar la interfaz donde está accesible la red local. Haga clic en Next (Siguiente).
9. El ASDM visualiza un resumen del VPN apenas configurado. Verifique y clic en Finalizar.

Configuración de CLI

Configuración central ASA (peer estático)

1. Configure una regla NO-NAT/NAT-EXEMPT para el tráfico VPN como este ejemplo muestra:
```
object network 10.1.1.0-remote_network
subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-inside_network
 subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.2.0-inside_network 10.1.2.0-inside_network
destination static 10.1.1.0-remote_network 10.1.1.0-remote_network
no-proxy-arp route-lookup
```
2. Configure la clave del preshared bajo DefaultL2LGroup para autenticar cualquier telecontrol Dynamic-L2L-peer:
```
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key cisco123
```
3. Defina la directiva phase-2/ISAKMP:
```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```
4. Defina el phase-2 transforman el conjunto/la directiva del IPSec:
```
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
```
5. Configure el mapa dinámico con estos parámetros: Transforme el conjunto requeridoReverse Route Injection (RRI) del permiso, que permite que el dispositivo de seguridad aprenda la información de ruteo para los clientes conectados (opcionales)
```
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set tset
crypto dynamic-map outside_dyn_map 1 set reverse-route
```
6. Ate el mapa dinámico a la correspondencia de criptografía, aplique la correspondencia de criptografía y habilite ISAKMP/IKEv1 en la interfaz exterior:
```
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

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

Telecontrol-ASA (par dinámico)

1. Configure una regla de la exención de NAT para el tráfico VPN:
```
object network 10.1.1.0-inside_network
subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-remote_network
subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.1.0-inside_network 10.1.1.0-inside_network
destination static 10.1.2.0-remote_network 10.1.2.0-remote_network
no-proxy-arp route-lookup
```
2. Configure a un grupo de túnel para una clave estática del par y del preshared VPN.
```
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
ikev1 pre-shared-key cisco123
```
3. Defina la directiva PHASE-1/ISAKMP:
```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```
4. Defina un phase-2 transforman el conjunto/la directiva del IPSec:
```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```
5. Configure una lista de acceso que defina el tráfico interesante/la red VPN:
```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```
6. Configure la correspondencia de criptografía estática con estos parámetros: Lista de acceso Crypto/VPNDirección IP remota del peer IPSecTransforme el conjunto requerido
```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```
7. Aplique la correspondencia de criptografía y habilite ISAKMP/IKEv1 en la interfaz exterior:
```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```

Verificación

Utilice esta sección para confirmar que la configuración trabaja correctamente.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

- show crypto isakmp sa: muestra las asociaciones de seguridad IKE (SAs) actuales en una par.
- **muestre IPSec crypto sa** - Visualiza todo el SA de IPSec actual.

Esta sección muestra el outout de la verificación del ejemplo para los dos ASA.

ASA central

```
Central-ASA#show crypto isakmp sa

  IKEv1 SAs:

     Active SA: 1
```

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

  1   IKE Peer: 172.16.1.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

    Central-ASA# show crypto ipsec sa
interface: outside
    Crypto map tag: outside_dyn_map, seq num: 1, local addr: 172.16.2.1

        local ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      current_peer: 172.16.1.1

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

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

      inbound esp sas:
      spi: 0x38DA6E51 (953839185)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (kB/sec): (3914999/28588)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x30D071C0 (818966976)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (kB/sec): (3914999/28588)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

TELECONTROL-ASA

```
Remote-ASA#show crypto isakmp sa

  IKEv1 SAs:

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

```
Total IKE SA: 1

  1   IKE Peer: 172.16.2.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

  Remote-ASA#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

        access-list outside_cryptomap extended permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      current_peer: 172.16.2.1

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

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

      inbound esp sas:
      spi: 0x30D071C0 (818966976)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 8192, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4373999/28676)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x38DA6E51 (953839185)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 8192, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4373999/28676)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del

comando show.

Note: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Utilice estos comandos como se muestra a continuación:

```
Remote-ASA#show crypto isakmp sa

  IKEv1 SAs:

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

  1   IKE Peer: 172.16.2.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

  Remote-ASA#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

        access-list outside_cryptomap extended permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      current_peer: 172.16.2.1

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

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

      inbound esp sas:
      spi: 0x30D071C0 (818966976)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 8192, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4373999/28676)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x38DA6E51 (953839185)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 8192, crypto-map: outside_map
```

```
sa timing: remaining key lifetime (kB/sec): (4373999/28676)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
 0x00000000 0x00000001
```

Caution: **El comando clear crypto isakmp sa** es intruso pues borra todos los túneles activos VPN.

En el Software Release 8.0(3) y Posterior del PIX/ASA, IKE individual SA se puede borrar usando el *>command del IP Address del <peer del* **clear crypto isakmp sa**. En las versiones de software anterior de 8.0(3), utiliza el comando del *<tunnel-group-name> del* **grupo de túnel del cierre de sesión de VPN-sessiondb** para borrar el IKE y el SA de IPSec para un solo túnel.

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

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

Debugs usados:

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

Telecontrol-ASA (iniciador)

Ingrese este comando del paquete-**trazalíneas** para iniciar el túnel:

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

IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple:
Prot=1, saddr=10.1.1.10, sport=0, daddr=10.1.2.10, dport=0
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE Initiator: New Phase 1, Intf
inside, IKE Peer 172.16.2.1 local Proxy Address 10.1.1.0, remote Proxy Address
10.1.2.0, Crypto map (outside_map)
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 132
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
```

```
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
<skipped>...
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Automatic NAT Detection Status: Remote end is NOT behind a NAT device
This end is NOT behind a NAT device
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)
+ VENDOR (13) + NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR ID received 172.16.2.1
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,
Oakley begin quick mode
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1, PHASE 1 COMPLETED


Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1, IKE Initiator
starting QM: msg id = c45c7b30
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, Transmitting Proxy Id:
 Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
 Remote subnet: 10.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE
(10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) +
ID (5) + ID (5) + NONE (0) total length : 172
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.2.0--255.255.255.0
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Security negotiation complete for LAN-to-LAN Group (172.16.2.1)
Initiator, Inbound SPI = 0x30d071c0, Outbound SPI = 0x38da6e51
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 76
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
```

Central-ASA (respondedor)

Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length
:
132
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 20 12:42:35 **[IKEv1]IP = 172.16.1.1, Connection landed on tunnel_group
DefaultL2LGroup**
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Generating keys for Responder...
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) +
VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) +
NONE (0) total length : 304
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8)
+ IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1 DECODE]Group = DefaultL2LGroup, IP = 172.16.1.1,
ID_IPV4_ADDR ID received172.16.1.1
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +
VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1]**Group = DefaultL2LGroup, IP = 172.16.1.1, PHASE 1 COMPLETED**
:
.
Jan 20 12:42:35 [IKEv1 DECODE]IP = 172.16.1.1, **IKE Responder starting QM**:
msg id = c45c7b30
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE
RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) +
NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, **Received remote
IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,
Protocol 0, Port 0**:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup,
IP = 172.16.1.1, **Received local
IP Proxy Subnet data in ID Payload: Address 10.1.2.0, Mask 255.255.255.0,
Protocol 0, Port 0**Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup,
IP = 172.16.1.1, processing notify payload
Jan 20 12:42:35 [IKEv1] Group = DefaultL2LGroup, IP = 172.16.1.1, QM
IsRekeyed old sa not found by addr
Jan 20 12:42:35 **[IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Static Crypto Map
check, map outside_dyn_map, seq = 1 is a successful match**
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, IKE
Remote Peer configured for crypto map: outside_dyn_map
:
.
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
**Transmitting Proxy Id: Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0
Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0**:

```
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=c45c7b30)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE
(0) total length : 172 Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED
Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 52:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Security
negotiation complete for LAN-to-LAN Group (DefaultL2LGroup) Responder,
Inbound SPI = 0x38da6e51, Outbound SPI = 0x30d071c0:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Adding static
route for L2L peer coming in on a dynamic map. address: 10.1.1.0, mask: 255.255.255.0
```

Información Relacionada

- Referencias de comandos de la serie de Cisco ASA
- Página de Soporte de IPSec Negotiation/IKE Protocols
- Solicitudes de Comentarios (RFC)
- Soporte técnico y documentación - Sistema de Cisco