

Configurar el Dynamic Multipoint VPN (DMVPN) usando el GRE sobre IPSec entre los routers múltiples

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Teoría Precedente](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[El Túnel DMVPN se Desestabiliza de Forma Intermitente](#)

[Comandos para resolución de problemas](#)

[Ejemplo de resultado del comando debug](#)

[Información Relacionada](#)

[Introducción](#)

La función Dynamic Multipoint VPN (DMVPN) le permite a los usuarios adaptarse mejor a IPSec VPNs grandes y pequeñas al combinar túneles de generic routing encapsulation (GRE), encriptación IPSec, y Next Hop Resolution Protocol (NHRP) para ofrecer a los usuarios una configuración a través de los perfiles de crypto, que invalidan el requisito para definir los mapas estáticos crypto, y la detección dinámica de los extremos del túnel.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

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

- Routers Cisco 2691 y 3725
- Cisco IOS® Software Release 12.3(3)

Nota: La transferencia de IPSec múltiple se soporta solamente en Cisco IOS Software Releases 12.2.(2)XK, 12.2.(13)T y posteriores.

El resultado del comando **show version** en el router se muestra a continuación:

```
sv9-4#show version Cisco Internetwork Operating System Software IOS (tm) 2600 Software (C2691-
IK9S-M), Version 12.3(3), RELEASE SOFTWARE (fc2) Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Tue 19-Aug-03 05:52 by dchih Image text-base: 0x60008954, data-base: 0x61D08000 ROM:
System Bootstrap, Version 12.2(8r)T2, RELEASE SOFTWARE (fc1) sv9-4 uptime is 1 hour, 39 minutes
System returned to ROM by reload System image file is "flash:c2691-ik9s-mz.123-3.bin" This
product contains cryptographic features and is subject to United States and local country laws
governing import, export, transfer and use. Delivery of Cisco cryptographic products does not
imply third-party authority to import, export, distribute or use encryption. Importers,
exporters, distributors and users are responsible for compliance with U.S. and local country
laws. By using this product you agree to comply with applicable laws and regulations. If you are
unable to comply with U.S. and local laws, return this product immediately. A summary of U.S.
laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html If you require further assistance please
contact us by sending email to export@cisco.com. cisco 2691 (R7000) processor (revision 0.1)
with 98304K/32768K bytes of memory. Processor board ID JMX0710L5CE R7000 CPU at 160Mhz,
Implementation 39, Rev 3.3, 256KB L2 Cache Bridging software. X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp). 2 FastEthernet/IEEE 802.3
interface(s) 2 Serial(sync/async) network interface(s) 1 ATM network interface(s) 1 Virtual
Private Network (VPN) Module(s) DRAM configuration is 64 bits wide with parity disabled. 55K
bytes of non-volatile configuration memory. 125184K bytes of ATA System CompactFlash
(Read/Write) Configuration register is 0x2102
```

La información que se presenta en este documento se originó a partir de dispositivos dentro de 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 un comando antes de ejecutarlo.

Teoría Precedente

La característica funciona según las reglas siguientes.

- Cada radio tiene un túnel IPsec permanente al hub, no a otras radios dentro de la red. Cada radio se registra como cliente del servidor NHRP.
- Cuando una radio necesita enviar un paquete a una subred (privada) de destino en otra radio, consulta al servidor NHRP para obtener la dirección (externa) real de la radio de destino.
- Después de que la radio aprende la dirección de par de la radio de destino, puede iniciar un túnel IPsec dinámico a la radio de destino.
- El túnel de radio a radio se construye sobre la interfaz de múltiples puntos GRE (mGRE).
- Los links de radio a radio se establecen según la demanda cada vez que hay tráfico entre radios. Luego, los paquetes pueden eludir el eje de conexión y utilizar el túnel radio a radio.

Las siguientes definiciones se aplican al conjunto de reglas.

- NHRP — Un protocolo del cliente y servidor donde está el concentrador el servidor y el spokes es los clientes. El hub mantiene una base de datos NHRP de las direcciones de interfaz pública de cada radio. Cada radio registra su dirección real cuando inicia las bases de datos NHRP y las consulta para obtener las direcciones reales de las radios de destino con el fin de construir túneles directos.

- Interfaz de Túnel mGRE: permite una única interfaz GRE para soportar múltiples túneles IPsec y simplifica el tamaño y la complejidad de la configuración.

Nota: Después de una cantidad preconfigurada de inactividad en los túneles de radio a radio, el router cerrará esos túneles para guardar los recursos (asociaciones de seguridad [SA] IPsec).

Nota: El perfil del tráfico debe seguir la regla del 80-20 por ciento: el 80 por ciento del tráfico consiste en el tráfico de radio a hub, y el 20 por ciento del tráfico consiste en el tráfico de radio a radio.

Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes [registrados](#)).

Diagrama de la red

Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.

Configuraciones

Este documento usa las configuraciones detalladas a continuación.

- [Configuración de Router del Hub \(sv9-2\)](#)
- [Configuración de Radio #1 \(sv9-3\)](#)
- [Configuración de Radio #2 \(sv9-4\)](#)

Configuración de Router del Hub (sv9-2)

```
sv9-2#show run Building configuration... Current
configuration : 1827 bytes ! version 12.3 service config
service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname sv9-2 ! boot-start-marker boot-
end-marker ! enable password cisco ! no aaa new-model ip
subnet-zero ! ! no ip domain lookup ! ip ssh break-
string ! !--- Create an Internet Security Association
and Key Management !--- Protocol (ISAKMP) policy for
Phase 1 negotiations. ! crypto isakmp policy 10 hash md5
authentication pre-share !--- Add dynamic pre-shared
keys for all the remote VPN !--- routers. crypto isakmp
key cisco123 address 0.0.0.0 0.0.0.0 ! !--- Create the
Phase 2 policy for actual data encryption. crypto ipsec
transform-set strong esp-3des esp-md5-hmac ! !--- Create
an IPsec profile to be applied dynamically to the !---
GRE over IPsec tunnels. crypto ipsec profile cisco set
```

```

security-association lifetime seconds 120 set transform-
set strong ! ! ! ! ! ! ! ! ! ! no voice hpi capture
buffer no voice hpi capture destination ! ! ! ! ! ! ! ! -
-- Create a GRE tunnel template which will be applied to
!--- all the dynamically created GRE tunnels. interface
Tunnel0 ip address 192.168.1.1 255.255.255.0 no ip
redirects ip mtu 1440 ip nhrp authentication cisco123 ip
nhrp map multicast dynamic ip nhrp network-id 1 no ip
split-horizon eigrp 90 no ip next-hop-self eigrp 90
tunnel source FastEthernet0/0 tunnel mode gre multipoint
tunnel key 0 tunnel protection ipsec profile cisco ! ! --
- This is the outbound interface. interface
FastEthernet0/0 ip address 209.168.202.225 255.255.255.0
duplex auto speed auto ! ! --- This is the inbound
interface. interface FastEthernet0/1 ip address 1.1.1.1
255.255.255.0 duplex auto speed auto ! interface BRI1/0
no ip address shutdown ! interface BRI1/1 no ip address
shutdown ! interface BRI1/2 no ip address shutdown !
interface BRI1/3 no ip address shutdown ! ! --- Enable a
routing protocol to send and receive ! --- dynamic
updates about the private networks. router eigrp 90
network 1.1.1.0 0.0.0.255 network 192.168.1.0 no auto-
summary ! ip http server no ip http secure-server ip
classless ip route 0.0.0.0 0.0.0.0 209.168.202.226 ! ! !
! ! ! ! ! ! ! ! line con 0 exec-timeout 0 0 transport
preferred all transport output all escape-character 27
line aux 0 transport preferred all transport output all
line vty 0 4 password cisco login transport preferred
all transport input all transport output all ! ! end

```

Configuración de Radio #1 (sv9-3)

```

sv9-3#show run Building configuration... Current
configuration : 1993 bytes ! version 12.3 service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname sv9-3 ! boot-
start-marker boot system flash:c3725-ik9s-mz.123-3.bin
boot-end-marker ! ! no aaa new-model ip subnet-zero ! !
no ip domain lookup ! ip ssh break-string ! ! ! ---
Create an ISAKMP policy for Phase 1 negotiations. crypto
isakmp policy 10 hash md5 authentication pre-share ! ---
Add dynamic pre-shared keys for all the remote VPN ! ---
routers and the hub router. crypto isakmp key cisco123
address 0.0.0.0 0.0.0.0 ! ! ! --- Create the Phase 2
policy for actual data encryption. crypto ipsec
transform-set strong esp-3des esp-md5-hmac ! ! --- Create
an IPSec profile to be applied dynamically to ! --- the
GRE over IPSec tunnels. crypto ipsec profile cisco set
security-association lifetime seconds 120 set transform-
set strong ! ! ! ! ! ! ! ! ! ! no voice hpi capture
buffer no voice hpi capture destination ! ! fax
interface-type fax-mail ! ! ! ! ! ! ! ! --- Create a GRE
tunnel template to be applied to ! --- all the
dynamically created GRE tunnels. interface Tunnel0 ip
address 192.168.1.2 255.255.255.0 no ip redirects ip mtu
1440 ip nhrp authentication cisco123 ip nhrp map
multicast dynamic ip nhrp map 192.168.1.1
209.168.202.225 ip nhrp map multicast 209.168.202.225 ip
nhrp network-id 1 ip nhrp nhs 192.168.1.1 tunnel source
FastEthernet0/0 tunnel mode gre multipoint tunnel key 0
tunnel protection ipsec profile cisco ! ! --- This is the
outbound interface. interface FastEthernet0/0 ip address
209.168.202.131 255.255.255.0 duplex auto speed auto !
!--- This is the inbound interface. interface
FastEthernet0/1 ip address 2.2.2.2 255.255.255.0 duplex

```

```

auto speed auto ! interface BRI1/0 no ip address
shutdown ! interface BRI1/1 no ip address shutdown !
interface BRI1/2 no ip address shutdown ! interface
BRI1/3 no ip address shutdown ! !--- Enable a routing
protocol to send and receive !--- dynamic updates about
the private networks. router eigrp 90 network 2.2.2.0
0.0.0.255 network 192.168.1.0 no auto-summary ! ip http
server no ip http secure-server ip classless ip route
0.0.0.0 0.0.0.0 209.168.202.225 ip route 3.3.3.0
255.255.255.0 Tunnel0 ! ! ! ! ! ! ! ! dial-peer cor
custom ! ! ! ! ! line con 0 exec-timeout 0 0 transport
preferred all transport output all escape-character 27
line aux 0 transport preferred all transport output all
line vty 0 4 login transport preferred all transport
input all transport output all ! ! end

```

Configuración de Radio #2 (sv9-4)

```

sv9-4#show run Building configuration... Current
configuration : 1994 bytes ! version 12.3 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
sv9-4 ! boot-start-marker boot system flash:c2691-ik9s-
mz.123-3.bin boot-end-marker ! ! no aaa new-model ip
subnet-zero ! ! no ip domain lookup ! ip ssh break-
string ! ! ! !--- Create an ISAKMP policy for Phase 1
negotiations. crypto isakmp policy 10 hash md5
authentication pre-share !--- Add dynamic pre-shared
keys for all the remote VPN !--- routers and the hub
router. crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0 ! ! !--- Create the Phase 2 policy for actual
data encryption. crypto ipsec transform-set strong esp-
3des esp-md5-hmac ! !--- Create an IPSec profile to be
applied dynamically to !--- the GRE over IPSec tunnels.
crypto ipsec profile cisco set security-association
lifetime seconds 120 set transform-set strong ! ! ! ! !
! ! ! ! ! ! no voice hpi capture buffer no voice hpi
capture destination ! ! ! ! ! ! ! !--- Create a GRE
tunnel template to be applied to !--- all the
dynamically created GRE tunnels. interface Tunnel0 ip
address 192.168.1.3 255.255.255.0 no ip redirects ip mtu
1440 ip nhrp authentication cisco123 ip nhrp map
multicast dynamic ip nhrp map 192.168.1.1
209.168.202.225 ip nhrp map multicast 209.168.202.225 ip
nhrp network-id 1 ip nhrp nhs 192.168.1.1 tunnel source
FastEthernet0/0 tunnel mode gre multipoint tunnel key 0
tunnel protection ipsec profile cisco ! !--- This is the
outbound interface. interface FastEthernet0/0 ip address
209.168.202.130 255.255.255.0 duplex auto speed auto !
interface Serial0/0 no ip address shutdown clockrate
2000000 no fair-queue ! !--- This is the inbound
interface. interface FastEthernet0/1 ip address 3.3.3.3
255.255.255.0 duplex auto speed auto ! interface
Serial0/1 no ip address shutdown clockrate 2000000 !
interface ATM1/0 no ip address shutdown no atm ilmi-
keepalive ! !--- Enable a routing protocol to send and
receive !--- dynamic updates about the private networks.
router eigrp 90 network 3.3.3.0 0.0.0.255 network
192.168.1.0 no auto-summary ! ip http server no ip http
secure-server ip classless ip route 2.2.2.0
255.255.255.0 Tunnel0 ip route 0.0.0.0 0.0.0.0
209.168.202.225 ! ! ! ! ! ! ! ! dial-peer cor custom ! !
! ! ! line con 0 exec-timeout 0 0 transport preferred
all transport output all escape-character 27 line aux 0
transport preferred all transport output all line vty 0

```

```
4 password cisco login transport preferred all transport
input all transport output all ! ! end
```

Verificación

En esta sección encontrará información que puede utilizar para corroborar que su configuración esté funcionando correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes [registrados](#)) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show crypto engine connection active:** muestra las encriptaciones y los descifrados totales por SA.
- **show crypto ipsec sa:** muestra las estadísticas en los túneles activos.
- **show crypto isakmp sa:** muestra el estado para ISAKMP SA.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

El Túnel DMVPN se Desestabiliza de Forma Intermitente

Problema

El túnel DMVPN se desestabiliza de forma intermitente.

Solución

Cuando los túneles DMVPN se desestabilizan, verifique la vecindad entre los routers ya que los problemas con la formación de vecindad entre los routers pueden desestabilizar el túnel DMVPN. Para resolver este problema, asegúrese de que la vecindad entre los routers esté siempre activa.

Comandos para resolución de problemas

Nota: Antes de ejecutar un comando debug, consulte [Información Importante sobre Comandos Debug](#).

- **debug crypto ipsec** — Muestra eventos de IPSec.
- **debug crypto isakmp** — Muestra mensajes acerca de eventos de intercambio de claves por Internet (IKE).
- **debug crypto engine** — Muestra información del motor de criptografía.

[Puede encontrar información adicional sobre la resolución de problemas de IPSec en Resolución de problemas de seguridad IP – Introducción y uso de los comandos de depuración.](#)

Ejemplo de resultado del comando debug

- [Debugs NHRP](#)

- [Debugs ISAKMP y la Negociación IPsec](#)

[Debugs NHRP](#)

El siguiente resultado debug muestra la solicitud de NHRP y la respuesta de resolución NHRP. Los debugs fueron capturados de las radios sv9-4 y sv9-3 y el hub sv9-2.

```
sv9-4#show debug NHRP: NHRP protocol debugging is on sv9-4#ping 2.2.2.2 Type escape sequence to
abort. Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds: !!!!! Success rate is
100 percent (5/5), round-trip min/avg/max = 4/4/4 ms sv9-4# *Mar 1 02:06:01.667: NHRP: Sending
packet to NHS 192.168.1.1 on Tunnel0 *Mar 1 02:06:01.671: NHRP: Sending packet to NHS
192.168.1.1 on Tunnel0 *Mar 1 02:06:01.675: NHRP: Sending packet to NHS 192.168.1.1 on Tunnel0
*Mar 1 02:06:01.679: NHRP: Encapsulation succeeded. Tunnel IP addr 209.168.202.225 *Mar 1
02:06:01.679: NHRP: Send Resolution Request via Tunnel0, packet size: 84 *Mar 1 02:06:01.679:
src: 192.168.1.3, dst: 192.168.1.1 *Mar 1 02:06:01.679: NHRP: 84 bytes out Tunnel0 *Mar 1
02:06:01.679: NHRP: Sending packet to NHS 192.168.1.1 on Tunnel0 *Mar 1 02:06:01.683: NHRP:
Sending packet to NHS 192.168.1.1 on Tunnel0 *Mar 1 02:06:03.507: NHRP: Encapsulation succeeded.
Tunnel IP addr 209.168.202.225 *Mar 1 02:06:03.507: NHRP: Send Resolution Request via Tunnel0,
packet size: 84 *Mar 1 02:06:03.507: src: 192.168.1.3, dst: 192.168.1.1 *Mar 1 02:06:03.507:
NHRP: 84 bytes out Tunnel0 *Mar 1 02:06:03.511: NHRP: Receive Resolution Reply via Tunnel0,
packet size: 132 *Mar 1 02:06:03.511: NHRP: netid_in = 0, to_us = 1 *Mar 1 02:06:03.511: NHRP:
No need to delay processing of resolution event nbma src:209.168.202.130 nbma
dst:209.168.202.131 sv9-3# 05:31:12: NHRP: Sending packet to NHS 192.168.1.1 on Tunnel0
05:31:12: NHRP: Sending packet to NHS 192.168.1.1 on Tunnel0 05:31:12: NHRP: Sending packet to
NHS 192.168.1.1 on Tunnel0 05:31:12: NHRP: Encapsulation succeeded. Tunnel IP addr
209.168.202.225 05:31:12: NHRP: Send Resolution Request via Tunnel0, packet size: 84 05:31:12:
src: 192.168.1.2, dst: 192.168.1.1 05:31:12: NHRP: 84 bytes out Tunnel0 05:31:12: NHRP: Sending
packet to NHS 192.168.1.1 on Tunnel0 05:31:12: NHRP: Receive Resolution Request via Tunnel0,
packet size: 104 05:31:12: NHRP: netid_in = 1, to_us = 0 05:31:12: NHRP: Delaying resolution
request nbma src:209.168.202.131 nbma dst:209.168.202.130 reason:IPSEC-IFC: need to wait for
IPsec SAs. 05:31:12: NHRP: Receive Resolution Reply via Tunnel0, packet size: 112 05:31:12:
NHRP: netid_in = 0, to_us = 1 05:31:12: NHRP: Resolution request is already being processed
(delayed). 05:31:12: NHRP: Resolution Request not queued. Already being processed (delayed).
05:31:12: NHRP: Sending packet to NHS 192.168.1.1 on Tunnel0 05:31:13: NHRP: Process delayed
resolution request src:192.168.1.3 dst:2.2.2.2 05:31:13: NHRP: No need to delay processing of
resolution event nbma src:209.168.202.131 nbma dst:209.168.202.130 sv9-2# *Mar 1 06:03:40.174:
NHRP: Forwarding packet within same fabric Tunnel0 -> Tunnel0 *Mar 1 06:03:40.174: NHRP:
Forwarding packet within same fabric Tunnel0 -> Tunnel0 *Mar 1 06:03:40.178: NHRP: Forwarding
packet within same fabric Tunnel0 -> Tunnel0 *Mar 1 06:03:40.182: NHRP: Receive Resolution
Request via Tunnel0, packet size: 84 *Mar 1 06:03:40.182: NHRP: netid_in = 1, to_us = 0 *Mar 1
06:03:40.182: NHRP: No need to delay processing of resolution event nbma src:209.168.202.225
nbma dst:209.168.202.130 *Mar 1 06:03:40.182: NHRP: nhrp_rtlookup yielded Tunnel0 *Mar 1
06:03:40.182: NHRP: netid_out 1, netid_in 1 *Mar 1 06:03:40.182: NHRP: nhrp_cache_lookup_comp
returned 0x0 *Mar 1 06:03:40.182: NHRP: calling nhrp_forward *Mar 1 06:03:40.182: NHRP:
Encapsulation succeeded. Tunnel IP addr 209.168.202.131 *Mar 1 06:03:40.182: NHRP: Forwarding
Resolution Request via Tunnel0, packet size: 104 *Mar 1 06:03:40.182: src: 192.168.1.1, dst:
2.2.2.2 *Mar 1 06:03:40.182: NHRP: 104 bytes out Tunnel0 *Mar 1 06:03:40.182: NHRP: Forwarding
packet within same fabric Tunnel0 -> Tunnel0 *Mar 1 06:03:40.182: NHRP: Receive Resolution
Request via Tunnel0, packet size: 84 *Mar 1 06:03:40.182: NHRP: netid_in = 1, to_us = 0 *Mar 1
06:03:40.182: NHRP: No need to delay processing of resolution event nbma src:209.168.202.225
nbma dst:209.168.202.131 *Mar 1 06:03:40.182: NHRP: nhrp_rtlookup yielded Tunnel0 *Mar 1
06:03:40.182: NHRP: netid_out 1, netid_in 1 *Mar 1 06:03:40.182: NHRP: nhrp_cache_lookup_comp
returned 0x63DE9498 *Mar 1 06:03:40.182: NHRP: Encapsulation succeeded. Tunnel IP addr
209.168.202.131 *Mar 1 06:03:40.182: NHRP: Send Resolution Reply via Tunnel0, packet size: 112
*Mar 1 06:03:40.186: src: 192.168.1.1, dst: 192.168.1.2 *Mar 1 06:03:40.186: NHRP: 112 bytes out
Tunnel0 *Mar 1 06:03:40.186: NHRP: Forwarding packet within same fabric Tunnel0 -> Tunnel0 *Mar
1 06:03:42.010: NHRP: Receive Resolution Request via Tunnel0, packet size: 84 *Mar 1
06:03:42.010: NHRP: netid_in = 1, to_us = 0 *Mar 1 06:03:42.010: NHRP: No need to delay
processing of resolution event nbma src:209.168.202.225 nbma dst:209.168.202.130
```

[Debugs ISAKMP y la Negociación IPsec](#)

El siguiente resultado de debug muestra el ISAKMP y la negociación IPsec. Los debugs fueron capturados de las radios sv9-4 y sv9-3.

```
sv9-4#ping 2.2.2.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 2.2.2.2,
timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
sv9-4# *Mar 1 02:25:37.107: ISAKMP (0:0): received packet from 209.168.202.131 dport 500 sport
500 Global (N) NEW SA *Mar 1 02:25:37.107: ISAKMP: local port 500, remote port 500 *Mar 1
02:25:37.107: ISAKMP: insert sa successfully sa = 63B38288 *Mar 1 02:25:37.107: ISAKMP (0:12):
Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH *Mar 1 02:25:37.107: ISAKMP (0:12): Old State =
IKE_READY New State = IKE_R_MM1 *Mar 1 02:25:37.107: ISAKMP (0:12): processing SA payload.
message ID = 0 *Mar 1 02:25:37.107: ISAKMP (0:12): processing vendor id payload *Mar 1
02:25:37.107: ISAKMP (0:12): vendor ID seems Unity/DPD but major 157 mismatch *Mar 1
02:25:37.107: ISAKMP (0:12): vendor ID is NAT-T v3 *Mar 1 02:25:37.107: ISAKMP (0:12):
processing vendor id payload *Mar 1 02:25:37.107: ISAKMP (0:12): vendor ID seems Unity/DPD but
major 123 mismatch *Mar 1 02:25:37.107: ISAKMP (0:12): vendor ID is NAT-T v2 *Mar 1
02:25:37.107: ISAKMP: Looking for a matching key for 209.168.202.131 in default : success *Mar 1
02:25:37.107: ISAKMP (0:12): found peer pre-shared key matching 209.168.202.131 *Mar 1
02:25:37.107: ISAKMP (0:12) local preshared key found *Mar 1 02:25:37.107: ISAKMP : Scanning
profiles for xauth ... *Mar 1 02:25:37.107: ISAKMP (0:12): Checking ISAKMP transform 1 against
priority 10 policy *Mar 1 02:25:37.107: ISAKMP: encryption DES-CBC *Mar 1 02:25:37.107: ISAKMP:
hash MD5 *Mar 1 02:25:37.107: ISAKMP: default group 1 *Mar 1 02:25:37.107: ISAKMP: auth pre-
share *Mar 1 02:25:37.107: ISAKMP: life type in seconds *Mar 1 02:25:37.107: ISAKMP: life
duration (VPI) of 0x0 0x1 0x51 0x80 *Mar 1 02:25:37.107: ISAKMP (0:12): atts are acceptable.
Next payload is 0 *Mar 1 02:25:37.115: ISAKMP (0:12): processing vendor id payload *Mar 1
02:25:37.115: ISAKMP (0:12): vendor ID seems Unity/DPD but major 157 mismatch *Mar 1
02:25:37.115: ISAKMP (0:12): vendor ID is NAT-T v3 *Mar 1 02:25:37.115: ISAKMP (0:12):
processing vendor id payload *Mar 1 02:25:37.115: ISAKMP (0:12): vendor ID seems Unity/DPD but
major 123 mismatch *Mar 1 02:25:37.115: ISAKMP (0:12): vendor ID is NAT-T v2 *Mar 1
02:25:37.115: ISAKMP (0:12): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE *Mar 1
02:25:37.115: ISAKMP (0:12): Old State = IKE_R_MM1 New State = IKE_R_MM1 *Mar 1 02:25:37.115:
ISAKMP (0:12): constructed NAT-T vendor-03 ID *Mar 1 02:25:37.115: ISAKMP (0:12): sending packet
to 209.168.202.131 my_port 500 peer_port 500 (R) MM_SA_SETUP *Mar 1 02:25:37.115: ISAKMP (0:12):
Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE *Mar 1 02:25:37.115: ISAKMP (0:12): Old State =
IKE_R_MM1 New State = IKE_R_MM2 *Mar 1 02:25:37.123: ISAKMP (0:12): received packet from
209.168.202.131 dport 500 sport 500 Global (R) MM_SA_SETUP *Mar 1 02:25:37.123: ISAKMP (0:12):
Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH *Mar 1 02:25:37.123: ISAKMP (0:12): Old State =
IKE_R_MM2 New State = IKE_R_MM3 *Mar 1 02:25:37.123: ISAKMP (0:12): processing KE payload.
message ID = 0 *Mar 1 02:25:37.131: ISAKMP (0:12): processing NONCE payload. message ID = 0 *Mar
1 02:25:37.131: ISAKMP: Looking for a matching key for 209.168.202.131 in default : success *Mar
1 02:25:37.131: ISAKMP (0:12): found peer pre-shared key matching 209.168.202.131 *Mar 1
02:25:37.131: ISAKMP: Looking for a matching key for 209.168.202.131 in default : success *Mar 1
02:25:37.131: ISAKMP (0:12): found peer pre-shared key matching 209.168.202.131 *Mar 1
02:25:37.135: ISAKMP (0:12): SKEYID state generated *Mar 1 02:25:37.135: ISAKMP (0:12):
processing vendor id payload *Mar 1 02:25:37.135: ISAKMP (0:12): vendor ID is Unity *Mar 1
02:25:37.135: ISAKMP (0:12): processing vendor id payload *Mar 1 02:25:37.135: ISAKMP (0:12):
vendor ID is DPD *Mar 1 02:25:37.135: ISAKMP (0:12): processing vendor id payload *Mar 1
02:25:37.135: ISAKMP (0:12): speaking to another IOS box! *Mar 1 02:25:37.135: ISAKMP:received
payload type 17 *Mar 1 02:25:37.135: ISAKMP:received payload type 17 *Mar 1 02:25:37.135: ISAKMP
(0:12): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE *Mar 1 02:25:37.135: ISAKMP (0:12): Old
State = IKE_R_MM3 New State = IKE_R_MM3 *Mar 1 02:25:37.135: ISAKMP (0:12): sending packet to
209.168.202.131 my_port 500 peer_port 500 (R) MM_KEY_EXCH *Mar 1 02:25:37.135: ISAKMP (0:12):
Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE *Mar 1 02:25:37.135: ISAKMP (0:12): Old State =
IKE_R_MM3 New State = IKE_R_MM4 *Mar 1 02:25:37.147: ISAKMP (0:12): received packet from
209.168.202.131 dport 500 sport 500 Global (R) MM_KEY_EXCH *Mar 1 02:25:37.151: ISAKMP (0:12):
Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH *Mar 1 02:25:37.151: ISAKMP (0:12): Old State =
IKE_R_MM4 New State = IKE_R_MM5 *Mar 1 02:25:37.151: ISAKMP (0:12): processing ID payload.
message ID = 0 *Mar 1 02:25:37.151: ISAKMP (0:12): peer matches *none* of the profiles *Mar 1
02:25:37.151: ISAKMP (0:12): processing HASH payload. message ID = 0 *Mar 1 02:25:37.151: ISAKMP
(0:12): processing NOTIFY_INITIAL_CONTACT protocol 1 spi 0, message ID = 0, sa = 63B38288 *Mar 1
02:25:37.151: ISAKMP (0:12): Process initial contact, bring down existing phase 1 and 2 SA's
with local 209.168.202.130 remote 209.168.202.131 remote port 500 *Mar 1 02:25:37.151: ISAKMP
(0:12): SA has been authenticated with 209.168.202.131 *Mar 1 02:25:37.151: ISAKMP (0:12): peer
matches *none* of the profiles *Mar 1 02:25:37.151: ISAKMP (0:12): Input = IKE_MSG_INTERNAL,
```


IKE_PROCESS_MAIN_MODE *Mar 1 02:25:37.151: ISAKMP (0:12): Old State = IKE_R_MM5 New State = IKE_R_MM5 *Mar 1 02:25:37.151: IPSEC(key_engine): got a queue event... *Mar 1 02:25:37.151: ISAKMP (0:12): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR *Mar 1 02:25:37.151: ISAKMP (12): ID payload next-payload : 8 type : 1 addr : 209.168.202.130 protocol : 17 port : 500 length : 8 *Mar 1 02:25:37.151: ISAKMP (12): Total payload length: 12 *Mar 1 02:25:37.155: ISAKMP (0:12): sending packet to 209.168.202.131 my_port 500 peer_port 500 (R) MM_KEY_EXCH *Mar 1 02:25:37.155: ISAKMP (0:12): Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE *Mar 1 02:25:37.155: ISAKMP (0:12): Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE *Mar 1 02:25:37.155: ISAKMP (0:12): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE *Mar 1 02:25:37.155: ISAKMP (0:12): Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE *Mar 1 02:25:37.159: ISAKMP (0:12): received packet from 209.168.202.131 dport 500 sport 500 Global (R) QM_IDLE *Mar 1 02:25:37.159: ISAKMP: set new node -1682446278 to QM_IDLE *Mar 1 02:25:37.159: ISAKMP (0:12): processing HASH payload. message ID = -1682446278 *Mar 1 02:25:37.159: ISAKMP (0:12): processing SA payload. message ID = -1682446278 *Mar 1 02:25:37.159: ISAKMP (0:12): Checking IPsec proposal 1 *Mar 1 02:25:37.159: ISAKMP: transform 1, ESP_3DES *Mar 1 02:25:37.159: ISAKMP: attributes in transform: *Mar 1 02:25:37.159: ISAKMP: encaps is 1 *Mar 1 02:25:37.159: ISAKMP: SA life type in seconds *Mar 1 02:25:37.159: ISAKMP: SA life duration (basic) of 120 *Mar 1 02:25:37.159: ISAKMP: SA life type in kilobytes *Mar 1 02:25:37.159: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Mar 1 02:25:37.159: ISAKMP: authenticator is HMAC-MD5 *Mar 1 02:25:37.159: ISAKMP (0:12): atts are acceptable. *Mar 1 02:25:37.163: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 209.168.202.130, remote= 209.168.202.131, local_proxy= 209.168.202.130/255.255.255.255/47/0 (type=1), remote_proxy= 209.168.202.131/255.255.255.255/47/0 (type=1), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2 *Mar 1 02:25:37.163: IPSEC(kei_proxy): head = Tunnel0-head-0, map->ivrf = , kei->ivrf = *Mar 1 02:25:37.163: IPSEC(kei_proxy): head = Tunnel0-head-0, map->ivrf = , kei->ivrf = *Mar 1 02:25:37.163: ISAKMP (0:12): processing NONCE payload. message ID = -1682446278 *Mar 1 02:25:37.163: ISAKMP (0:12): processing ID payload. message ID = -1682446278 *Mar 1 02:25:37.163: ISAKMP (0:12): processing ID payload. message ID = -1682446278 *Mar 1 02:25:37.163: ISAKMP (0:12): asking for 1 spis from ipsec *Mar 1 02:25:37.163: ISAKMP (0:12): Node -1682446278, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH *Mar 1 02:25:37.163: ISAKMP (0:12): Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE *Mar 1 02:25:37.163: IPSEC(key_engine): got a queue event... *Mar 1 02:25:37.163: IPSEC(spi_response): getting spi 3935077313 for SA from 209.168.202.130 to 209.168.202.131 for prot 3 *Mar 1 02:25:37.163: ISAKMP: received ke message (2/1) *Mar 1 02:25:37.415: ISAKMP (0:12): sending packet to 209.168.202.131 my_port 500 peer_port 500 (R) QM_IDLE *Mar 1 02:25:37.415: ISAKMP (0:12): Node -1682446278, Input = IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY *Mar 1 02:25:37.415: ISAKMP (0:12): Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2 *Mar 1 02:25:37.427: ISAKMP (0:12): received packet from 209.168.202.131 dport 500 sport 500 Global (R) QM_IDLE *Mar 1 02:25:37.439: ISAKMP (0:12): Creating IPsec SAs *Mar 1 02:25:37.439: inbound SA from 209.168.202.131 to 209.168.202.130 (f/i) 0/ 0 (proxy 209.168.202.131 to 209.168.202.130) *Mar 1 02:25:37.439: has spi 0xEA8C83C1 and conn_id 5361 and flags 2 *Mar 1 02:25:37.439: lifetime of 120 seconds *Mar 1 02:25:37.439: lifetime of 4608000 kilobytes *Mar 1 02:25:37.439: has client flags 0x0 *Mar 1 02:25:37.439: outbound SA from 209.168.202.130 to 209.168.202.131 (f/i) 0/ 0 (proxy 209.168.202.130 to 209.168.202.131) *Mar 1 02:25:37.439: has spi 1849847934 and conn_id 5362 and flags A *Mar 1 02:25:37.439: lifetime of 120 seconds *Mar 1 02:25:37.439: lifetime of 4608000 kilobytes *Mar 1 02:25:37.439: has client flags 0x0 *Mar 1 02:25:37.439: ISAKMP (0:12): deleting node -1682446278 error FALSE reason "quick mode done (await)" *Mar 1 02:25:37.439: ISAKMP (0:12): Node -1682446278, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH *Mar 1 02:25:37.439: ISAKMP (0:12): Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE *Mar 1 02:25:37.439: IPSEC(key_engine): got a queue event... *Mar 1 02:25:37.439: IPSEC(initialize_sas): , (key eng. msg.) INBOUND local= 209.168.202.130, remote= 209.168.202.131, local_proxy= 209.168.202.130/0.0.0.0/47/0 (type=1), remote_proxy= 209.168.202.131/0.0.0.0/47/0 (type=1), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 120s and 4608000kb, spi= 0xEA8C83C1(3935077313), conn_id= 5361, keysize= 0, flags= 0x2 *Mar 1 02:25:37.439: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 209.168.202.130, remote= 209.168.202.131, local_proxy= 209.168.202.130/0.0.0.0/47/0 (type=1), remote_proxy= 209.168.202.131/0.0.0.0/47/0 (type=1), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 120s and 4608000kb, spi= 0x6E42707E(1849847934), conn_id= 5362, keysize= 0, flags= 0xA *Mar 1 02:25:37.439: IPSEC(kei_proxy): head = Tunnel0-head-0, map->ivrf = , kei->ivrf = *Mar 1 02:25:37.439: IPSEC(kei_proxy): head = Tunnel0-head-0, map->ivrf = , kei->ivrf = *Mar 1 02:25:37.439: IPSEC(add mtree): src 209.168.202.130, dest 209.168.202.131, dest_port 0 *Mar 1 02:25:37.439: IPSEC(create_sa): sa created, (sa) sa_dest= 209.168.202.130, sa_prot= 50, sa_spi= 0xEA8C83C1(3935077313), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 5361 *Mar 1 02:25:37.439: IPSEC(create_sa): sa created, (sa) sa_dest= 209.168.202.131, sa_prot= 50, sa_spi=

0x6E42707E(1849847934), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 5362 sv9-4# *Mar 1
02:25:55.183: ISAKMP (0:10): purging node 180238748 *Mar 1 02:25:55.323: ISAKMP (0:10): purging
node -1355110639 sv9-4# sv9-3# 05:50:48: ISAKMP: received ke message (1/1) 05:50:48: ISAKMP
(0:0): SA request profile is (NULL) 05:50:48: ISAKMP: local port 500, remote port 500 05:50:48:
ISAKMP: set new node 0 to QM_IDLE 05:50:48: ISAKMP: insert sa successfully sa = 62DB93D0
05:50:48: ISAKMP (0:26): Can not start Aggressive mode, trying Main mode. 05:50:48: ISAKMP:
Looking for a matching key for 209.168.202.130 in default : success 05:50:48: ISAKMP (0:26):
found peer pre-shared key matching 209.168.202.130 05:50:48: ISAKMP (0:26): constructed NAT-T
vendor-03 ID 05:50:48: ISAKMP (0:26): constructed NAT-T vendor-02 ID 05:50:48: ISAKMP (0:26):
Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM 05:50:48: ISAKMP (0:26): Old State = IKE_READY New
State = IKE_I_MM1 05:50:48: ISAKMP (0:26): beginning Main Mode exchange 05:50:48: ISAKMP (0:26):
sending packet to 209.168.202.130 my_port 500 peer_port 500 (I) MM_NO_STATE 05:50:48: ISAKMP
(0:26): received packet from 209.168.202.130 dport 500 sport 500 Global (I) MM_NO_STATE
05:50:48: ISAKMP (0:26): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH 05:50:48: ISAKMP (0:26): Old
State = IKE_I_MM1 New State = IKE_I_MM2 05:50:48: ISAKMP (0:26): processing SA payload. message
ID = 0 05:50:48: ISAKMP (0:26): processing vendor id payload 05:50:48: ISAKMP (0:26): vendor ID
seems Unity/DPD but major 157 mismatch 05:50:48: ISAKMP (0:26): vendor ID is NAT-T v3 05:50:48:
ISAKMP: Looking for a matching key for 209.168.202.130 in default : success 05:50:48: ISAKMP
(0:26): found peer pre-shared key matching 209.168.202.130 05:50:48: ISAKMP (0:26) local
preshared key found 05:50:48: ISAKMP : Scanning profiles for xauth ... 05:50:48: ISAKMP (0:26):
Checking ISAKMP transform 1 against priority 10 policy 05:50:48: ISAKMP: encryption DES-CBC
05:50:48: ISAKMP: hash MD5 05:50:48: ISAKMP: default group 1 05:50:48: ISAKMP: auth pre-share
05:50:48: ISAKMP: life type in seconds 05:50:48: ISAKMP: life duration (VPI) of 0x0 0x1 0x51
0x80 **05:50:48: ISAKMP (0:26): atts are acceptable. Next payload is 0** 05:50:48: ISAKMP (0:26):
processing vendor id payload 05:50:48: ISAKMP (0:26): vendor ID seems Unity/DPD but major 157
mismatch 05:50:48: ISAKMP (0:26): vendor ID is NAT-T v3 05:50:48: ISAKMP (0:26): Input =
IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE 05:50:48: ISAKMP (0:26): Old State = IKE_I_MM2 New
State = IKE_I_MM2 05:50:48: ISAKMP (0:26): sending packet to 209.168.202.130 my_port 500
peer_port 500 (I) MM_SA_SETUP 05:50:48: ISAKMP (0:26): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE 05:50:48: ISAKMP (0:26): Old State = IKE_I_MM2 New State = IKE_I_MM3
05:50:48: ISAKMP (0:26): received packet from 209.168.202.130 dport 500 sport 500 Global (I)
MM_SA_SETUP 05:50:48: ISAKMP (0:26): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH 05:50:48: ISAKMP
(0:26): Old State = IKE_I_MM3 New State = IKE_I_MM4 05:50:48: ISAKMP (0:26): processing KE
payload. message ID = 0 05:50:48: ISAKMP (0:26): processing NONCE payload. message ID = 0
**05:50:48: ISAKMP: Looking for a matching key for 209.168.202.130 in default : success 05:50:48:
ISAKMP (0:26): found peer pre-shared key matching 209.168.202.130 05:50:48: ISAKMP: Looking for
a matching key for 209.168.202.130 in default : success 05:50:48: ISAKMP (0:26): found peer pre-
shared key matching 209.168.202.130** 05:50:48: ISAKMP (0:26): SKEYID state generated 05:50:48:
ISAKMP (0:26): processing vendor id payload 05:50:48: ISAKMP (0:26): vendor ID is Unity
05:50:48: ISAKMP (0:26): processing vendor id payload 05:50:48: ISAKMP (0:26): vendor ID is DPD
05:50:48: ISAKMP (0:26): processing vendor id payload 05:50:48: ISAKMP (0:26): speaking to
another IOS box! 05:50:48: ISAKMP:received payload type 17 05:50:48: ISAKMP:received payload
type 17 05:50:48: ISAKMP (0:26): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE 05:50:48:
ISAKMP (0:26): Old State = IKE_I_MM4 New State = IKE_I_MM4 05:50:48: ISAKMP (0:26): Send initial
contact 05:50:48: ISAKMP (0:26): SA is doing pre-shared key authentication using id type
ID_IPV4_ADDR 05:50:48: ISAKMP (26): ID payload next-payload : 8 type : 1 addr : 209.168.202.131
protocol : 17 port : 500 length : 8 05:50:48: ISAKMP (26): Total payload length: 12 05:50:48:
ISAKMP (0:26): sending packet to 209.168.202.130 my_port 500 peer_port 500 (I) MM_KEY_EXCH
05:50:48: ISAKMP (0:26): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE 05:50:48: ISAKMP
(0:26): Old State = IKE_I_MM4 New State = IKE_I_MM5 05:50:48: ISAKMP (0:26): received packet
from 209.168.202.130 dport 500 sport 500 Global (I) MM_KEY_EXCH 05:50:48: ISAKMP (0:26): Input =
IKE_MESG_FROM_PEER, IKE_MM_EXCH 05:50:48: ISAKMP (0:26): Old State = IKE_I_MM5 New State =
IKE_I_MM6 05:50:48: ISAKMP (0:26): processing ID payload. message ID = 0 05:50:48: ISAKMP
(0:26): processing HASH payload. message ID = 0 05:50:48: ISAKMP (0:26): SA has been
authenticated with 209.168.202.130 05:50:48: ISAKMP (0:26): peer matches *none* of the profiles
05:50:48: ISAKMP (0:26): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE 05:50:48: ISAKMP
(0:26): Old State = IKE_I_MM6 New State = IKE_I_MM6 05:50:48: ISAKMP (0:26): Input =
IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE 05:50:48: ISAKMP (0:26): Old State = IKE_I_MM6 New State
= IKE_P1_COMPLETE 05:50:48: ISAKMP (0:26): beginning Quick Mode exchange, M-ID of -1682446278
05:50:48: ISAKMP (0:26): sending packet to 209.168.202.130 my_port 500 peer_port 500 (I) QM_IDLE
05:50:48: ISAKMP (0:26): Node -1682446278, Input = IKE_MESG_INTERNAL, IKE_INIT_QM 05:50:48:
ISAKMP (0:26): Old State = IKE_QM_READY New State = IKE_QM_I_QM1 05:50:48: ISAKMP (0:26): Input
= IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE 05:50:48: ISAKMP (0:26): Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE 05:50:48: ISAKMP (0:26): received packet from 209.168.202.130 dport

500 sport 500 Global (I) QM_IDLE 05:50:48: ISAKMP (0:26): processing HASH payload. message ID = -1682446278 05:50:48: ISAKMP (0:26): processing SA payload. message ID = -1682446278 05:50:48: ISAKMP (0:26): Checking IPsec proposal 1 05:50:48: ISAKMP: transform 1, ESP_3DES 05:50:48: ISAKMP: attributes in transform: 05:50:48: ISAKMP: encaps is 1 05:50:48: ISAKMP: SA life type in seconds 05:50:48: ISAKMP: SA life duration (basic) of 120 05:50:48: ISAKMP: SA life type in kilobytes 05:50:48: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 05:50:48: ISAKMP: authenticator is HMAC-MD5 05:50:48: ISAKMP (0:26): atts are acceptable. 05:50:48: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 209.168.202.131, remote= 209.168.202.130, local_proxy= 209.168.202.131/255.255.255.255/47/0 (type=1), remote_proxy= 209.168.202.130/255.255.255.255/47/0 (type=1), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2 05:50:48: IPSEC(kei_proxy): head = Tunnel0-head-0, map->ivrf = , kei->ivrf = 05:50:48: IPSEC(kei_proxy): head = Tunnel0-head-0, map->ivrf = , kei->ivrf = 05:50:48: ISAKMP (0:26): processing NONCE payload. message ID = -1682446278 05:50:48: ISAKMP (0:26): processing ID payload. message ID = -1682446278 05:50:48: ISAKMP (0:26): processing ID payload. message ID = -1682446278 05:50:48: ISAKMP (0:26): Creating IPsec SAs 05:50:48: inbound SA from 209.168.202.130 to 209.168.202.131 (f/i) 0/ 0 (proxy 209.168.202.130 to 209.168.202.131) 05:50:48: has spi 0x6E42707E and conn_id 5547 and flags 2 05:50:48: lifetime of 120 seconds 05:50:48: lifetime of 4608000 kilobytes 05:50:48: has client flags 0x0 05:50:48: outbound SA from 209.168.202.131 to 209.168.202.130 (f/i) 0/ 0 (proxy 209.168.202.131 to 209.168.202.130) 05:50:48: has spi - 359889983 and conn_id 5548 and flags A 05:50:48: lifetime of 120 seconds 05:50:48: lifetime of 4608000 kilobytes 05:50:48: has client flags 0x0 05:50:48: IPSEC(key_engine): got a queue event... 05:50:48: IPSEC(initialize_sas): , (key eng. msg.) INBOUND local= 209.168.202.131, remote= 209.168.202.130, local_proxy= 209.168.202.131/0.0.0.0/47/0 (type=1), remote_proxy= 209.168.202.130/0.0.0.0/47/0 (type=1), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 120s and 4608000kb, spi= 0x6E42707E(1849847934), conn_id= 5547, keysize= 0, flags= 0x2 05:50:48: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 209.168.202.131, remote= 209.168.202.130, local_proxy= 209.168.202.131/0.0.0.0/47/0 (type=1), remote_proxy= 209.168.202.130/0.0.0.0/47/0 (type=1), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 120s and 4608000kb, spi= 0xEA8C83C1(3935077313), conn_id= 5548, keysize= 0, flags= 0xA 05:50:48: IPSEC(kei_proxy): head = Tunnel0-head-0, map->ivrf = , kei->ivrf = 05:50:48: IPSEC(kei_proxy): head = Tunnel0-head-0, map->ivrf = , kei->ivrf = 05:50:48: IPSEC(add mtree): src 209.168.202.131, dest 209.168.202.130, dest_port 0 **05:50:48: IPSEC(create_sa): sa created,** (sa) sa_dest= 209.168.202.131, sa_prot= 50, sa_spi= 0x6E42707E(1849847934), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 5547 05:50:48: IPSEC(create_sa): sa created, (sa) sa_dest= 209.168.202.130, sa_prot= 50, sa_spi= 0xEA8C83C1(3935077313), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 5548 05:50:48: ISAKMP (0:26): sending packet to 209.168.202.130 my_port 500 peer_port 500 (I) QM_IDLE 05:50:48: ISAKMP (0:26): deleting node -1682446278 error FALSE reason "" 05:50:48: ISAKMP (0:26): Node -1682446278, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH 05:50:48: ISAKMP (0:26): Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE 05:50:49: ISAKMP (0:21): purging node 334570133 sv9-3#

[Información Relacionada](#)

- [IPSec Negotiation/IKE Protocols](#)
- [Soporte Técnico - Cisco Systems](#)