

Configurazione di DMVPN (Dynamic Multipoint VPN) con GRE su IPsec tra più router

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Nozioni di base](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Flag del tunnel DMVPN in modo intermittente](#)

[Comandi per la risoluzione dei problemi](#)

[Output di esempio del comando debug](#)

[Informazioni correlate](#)

[Introduzione](#)

La funzionalità DMVPN (Dynamic Multipoint VPN) consente agli utenti di scalare in modo migliore le VPN IPsec di grandi e piccole dimensioni combinando tunnel GRE (Generic Routing Encapsulation), crittografia IPsec e protocollo NHRP (Next Hop Resolution Protocol) per offrire agli utenti una configurazione semplice tramite profili crittografici, che sostituiscono la necessità di definire mappe crittografiche statiche e di rilevare dinamicamente gli endpoint del tunnel.

[Prerequisiti](#)

[Requisiti](#)

Nessun requisito specifico previsto per questo documento.

[Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle versioni software e hardware riportate di seguito.

- Cisco 2691 e 3725 router

- Software Cisco IOS® versione 12.3(3)

Nota: l'accesso automatico a più pacchetti IPsec è supportato solo nei software Cisco IOS versione 12.2.2(2)XK e 12.2(13)T e successive.

Di seguito è riportato l'output del comando **show version** sul router:

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
```

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Nozioni di base

La funzionalità funziona in base alle seguenti regole.

- Ogni spoke dispone di un tunnel IPsec permanente che lo collega all'hub e non agli altri spoke all'interno della rete. Ogni spoke viene registrato come client del server NHRP.
- Quando un spoke deve inviare un pacchetto a una subnet di destinazione (privata) su un altro spoke, esegue una query sul server NHRP per ottenere l'indirizzo reale (esterno) della destinazione (destinazione) spoke.
- Dopo che il spoke di origine ha appreso l'indirizzo peer del spoke di destinazione, può avviare un tunnel IPsec dinamico per il spoke di destinazione.
- Il tunnel spoke-to-spoke è costruito sull'interfaccia GRE (multipoint GRE).
- I collegamenti spoke vengono stabiliti su richiesta ogni volta che c'è traffico tra i spoke. Successivamente, i pacchetti possono ignorare l'hub e utilizzare il tunnel spoke.

Al set di regole vengono applicate le definizioni seguenti.

- NHRP - Protocollo client e server in cui l'hub è il server e gli spoke sono i client. L'hub gestisce un database NHRP degli indirizzi dell'interfaccia pubblica di ogni spoke. Ogni spoke registra il proprio indirizzo reale all'avvio e richiede al database NHRP gli indirizzi reali degli spoke di destinazione per costruire tunnel diretti.
- Interfaccia tunnel GRE: consente a una singola interfaccia GRE di supportare più tunnel IPsec e semplifica le dimensioni e la complessità della configurazione.

Nota: dopo un periodo di inattività preconfigurato sui tunnel spoke, il router interromperà i tunnel per risparmiare risorse (associazioni di sicurezza IPsec [SA]).

Nota: il profilo del traffico deve seguire la regola dell'80-20%: L'80% del traffico è costituito da traffico spoke-to-hub e il 20% è costituito da traffico spoke-to-spoke.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

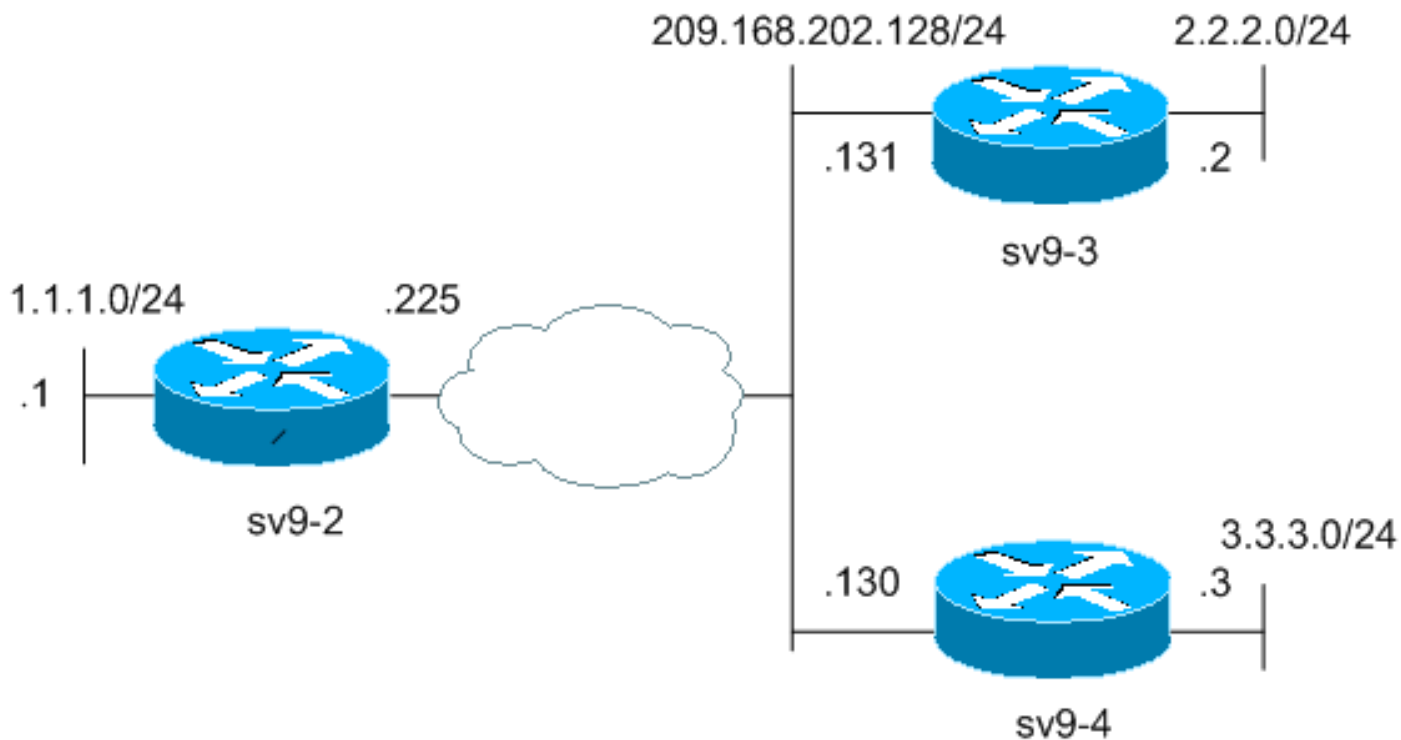
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca dei comandi](#) (solo utenti [registrati](#)).

Esempio di rete

Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.



Configurazioni

Questo documento utilizza le configurazioni mostrate di seguito.

- [Configurazione router hub \(sv9-2\)](#)
- [Configurazione spoke n. 1 \(sv9-3\)](#)
- [Configurazione spoke n. 2 \(sv9-4\)](#)

Configurazione router 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
```

Configurazione spoke n. 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
```

Configurazione spoke n. 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

```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

- **show crypto engine connection active**: visualizza il totale di crittografie e decrittografie per SA.
- **show crypto ipsec sa**: visualizza lo stato dei tunnel attivi.
- **show crypto isakmp sa**: visualizza lo stato dell'associazione di protezione ISAKMP.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Flag del tunnel DMVPN in modo intermittente

Problema

I flap del tunnel DMVPN vengono eseguiti in modo intermittente.

Soluzione

Quando i tunnel DMVPN scollegano, controllare le aree adiacenti tra i router perché problemi di formazione delle aree adiacenti tra i router possono causare il collegamento del tunnel DMVPN. Per risolvere questo problema, verificare che il vicinato tra i router sia sempre attivo.

Comandi per la risoluzione dei problemi

Nota: prima di usare i comandi di **debug**, consultare le [informazioni importanti sui comandi di debug](#).

- **debug crypto ipsec**: visualizza gli eventi IPsec.
- **debug crypto isakmp**: visualizza i messaggi sugli eventi IKE (Internet Key Exchange).
- **debug crypto engine**: visualizza le informazioni provenienti dal crypto engine.

Per ulteriori informazioni sulla risoluzione dei problemi relativi a IPsec, consultare il documento sulla [risoluzione dei problemi relativi alla protezione IP - descrizione e uso dei comandi di debug](#).

Output di esempio del comando debug

- [Debug NHRP](#)
- [Debug della negoziazione ISAKMP e IPsec](#)

Debug NHRP

L'output di debug seguente mostra la richiesta NHRP e la risposta alla risoluzione NHRP. I bug sono stati acquisiti dai raggi sv9-4 e sv9-3 e dall'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

```

[Debug della negoziazione ISAKMP e IPSec](#)

Nell'output di debug seguente viene illustrata la negoziazione ISAKMP e IPSec. I bug sono stati catturati dai raggi sv9-4 e 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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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_MSG_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_MSG_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_MSG_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_MSG_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_MSG_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_MSG_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_MESG_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#
```

[Informazioni correlate](#)

- [Negoziazione IPSec/protocolli IKE](#)
- [Supporto tecnico – Cisco Systems](#)