配置IPsec路由器動態LAN到LAN對等路由器和VPN客戶端

目錄

簡介

此配置顯示了中心輻射環境中的兩台路由器之間的LAN到LAN配置。Cisco VPN使用者端也會連線到集線器並使用擴展驗證(Xauth)。

在此方案中，分支路由器通過DHCP動態獲取其IP地址。在分支通過DSL或電纜數據機連線到網際網路的情況下，動態主機配置協定(DHCP)的使用很常見。這是因為ISP通常在這些低成本連線上使用DHCP動態調配IP地址。

如果沒有進一步的配置，則無法在集線器路由器上使用萬用字元預共用金鑰。這是因為VPN使用者端連線的Xauth確實會中斷LAN到LAN連線。但是停用Xauth時，會降低驗證VPN使用者端的功能。

在Cisco IOS®軟體版本12.2(15)T中匯入ISAKMP設定檔使此設定成為可能，因為您可以對連線的其他屬性（VPN使用者端群組、對等IP位址、完全限定網域[FQDN]等）進行比對，而不只是對等IP位址。ISAKMP配置檔案是此配置的主題。

注意：您還可以將**no-xauth關鍵字與crypto isakmp key 命令結合使用，以繞過LAN到LAN對等路由器的Xauth。**如需詳細資訊，請參閱能夠對靜態IPsec對等停用Xauth和設定兩台路由器和Cisco VPN使用者端4.x之間的IPsec。

本文檔中的分支路由器配置可在連線到同一中心的所有其他分支路由器上複製。分支之間的唯一區別是引用要加密的流量的訪問清單。

請參閱同一路由器上的EzVPN客戶端和伺服器配置示例，以瞭解有關可以在同一介面上將路由器配置為EzVPN客戶端和伺服器的方案的詳細資訊。

請參閱VPN 3000集中器上的LAN到LAN隧道（配置了DHCP的PIX防火牆），以配置Cisco VPN 3000集中器系列，從而動態建立IPsec隧道（使用遠端的Cisco PIX防火牆使用DHCP獲取其公共介面上的IP地址）。

請參閱VPN 3000集中器上的IPsec LAN到LAN隧道和配置用於DHCP的Cisco IOS路由器配置示例，配置VPN 3000集中器系列，以便使用在其公共介面上接收動態IP地址的遠端VPN裝置動態建立IPsec隧道。

請參閱靜態IOS路由器與帶NAT的動態PIX/ASA 7.x之間的IPsec配置示例，以啟用PIX/ASA安全裝置以接受來自IOS®路由器的動態IPsec連線。

必要條件

需求

本文件沒有特定需求。

採用元件

IPsec設定檔是在Cisco IOS軟體版本12.2(15)T中匯入。由於Cisco錯誤ID CSCea77140(僅註冊客戶)，您需要執行Cisco IOS軟體版本12.3(3)或更新版本或Cisco IOS軟體版本12.3(2)T或更新版本，才能使此組態成功運作。已使用以下軟體版本測試這些組態：

- 中心路由器上的Cisco IOS軟體版本12.3(6a)
- 分支路由器上的Cisco IOS軟體版本12.2(23a)（可以是任何加密版本）
- Windows 2000上的Cisco VPN客戶端版本4.0(4)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

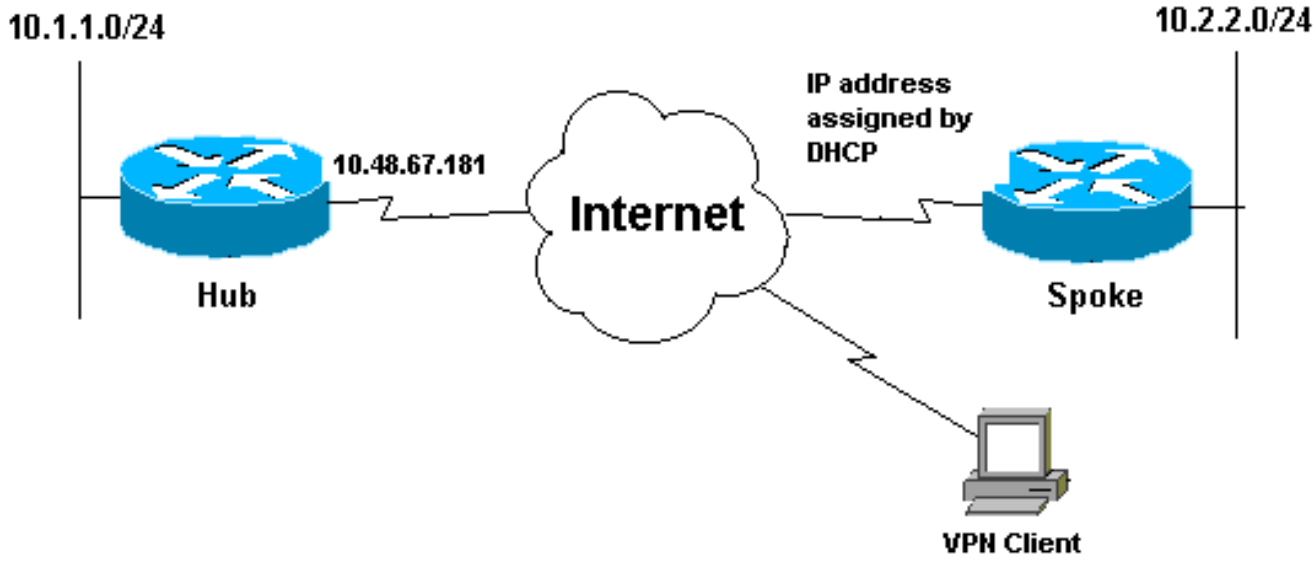
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用下圖中所示的網路設定。



組態

本檔案會使用以下網路設定：

- 集線器配置
- 分支配置

集線器配置

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Hub
!
no logging on
!
username gfullage password 7 0201024E070A0E2649
aaa new-model
!
!
aaa authentication login clientauth local
aaa authorization network groupauthor local
aaa session-id common
ip subnet-zero
!
!
no ip domain lookup
!
!  !--- Keyring that defines wildcard pre-shared key.
crypto keyring spokes
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!  !--- VPN Client configuration for group "testgroup"
!--- (this name is configured in the VPN Client). crypto
```

```
isakmp client configuration group testgroup
 key cisco321
 dns 1.1.1.1 2.2.2.2
 wins 3.3.3.3 4.4.4.4
 domain cisco.com
 pool ippool
!
!--- Profile for LAN-to-LAN connection, that references
!--- the wildcard pre-shared key and a wildcard !---
identity (this is what is broken in !--- Cisco bug ID
CSCea77140) and no Xauth. crypto isakmp profile L2L
   description LAN-to-LAN for spoke router(s) connection
   keyring spokes
   match identity address 0.0.0.0  !--- Profile for VPN
Client connections, that matches !--- the "testgroup"
group and defines the Xauth properties. crypto isakmp
profile VPNclient
   description VPN clients profile
   match identity group testgroup
   client authentication list clientauth
   isakmp authorization list groupauthor
   client configuration address respond
!
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
!--- Two instances of the dynamic crypto map !---
reference the two previous IPsec profiles. crypto
dynamic-map dynmap 5
 set transform-set myset
 set isakmp-profile VPNclient
crypto dynamic-map dynmap 10
 set transform-set myset
 set isakmp-profile L2L
!
!
!--- Crypto-map only references the two !--- instances
of the previous dynamic crypto map. crypto map mymap 10
ipsec-isakmp dynamic dynmap
!
!
!
interface FastEthernet0/0
 description Outside interface
 ip address 10.48.67.181 255.255.255.224
 no ip mroute-cache
 duplex auto
 speed auto
 crypto map mymap
!
interface FastEthernet0/1
 description Inside interface
 ip address 10.1.1.1 255.255.254.0

 duplex auto
 speed auto
 no keepalive
!
ip local pool ippool 10.5.5.1 10.5.5.254
no ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 10.48.66.181
```

```
!
!
call rsvp-sync
!
!
dial-peer cor custom
!
!
line con 0
 exec-timeout 0 0
 escape-character 27
line aux 0
line vty 0 4
 password 7 121A0C041104
!
!
end
```

分支配置

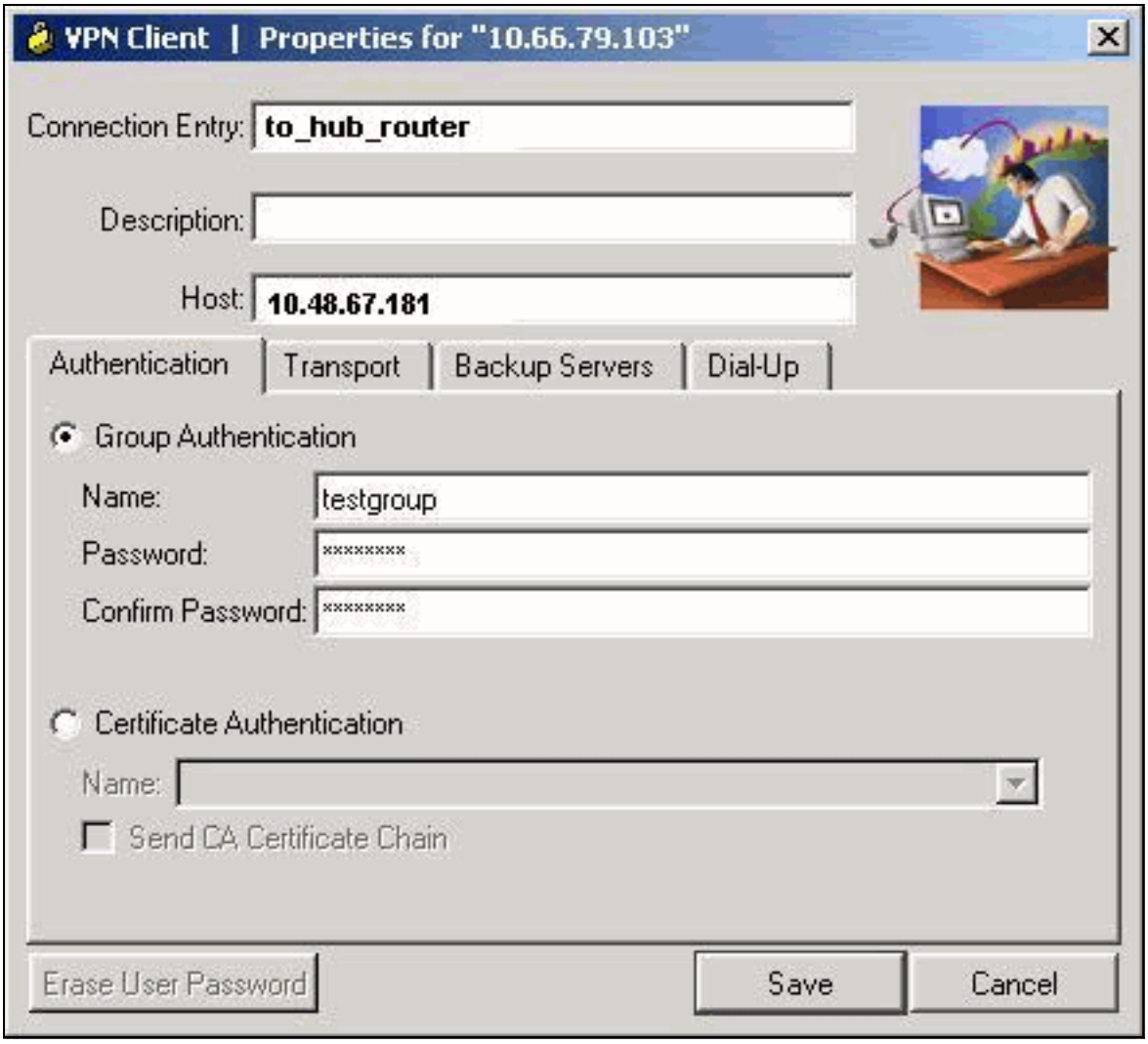
```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spoke
!
no logging on
!
ip subnet-zero
no ip domain lookup
!
ip cef
!
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 10.48.67.181
!
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
!--- Standard crypto map on the spoke router !--- that
references the known hub IP address. crypto map mymap 10
ipsec-isakmp
 set peer 10.48.67.181
 set transform-set myset
 match address 100
!
!
controller ISA 5/1
!
!
interface FastEthernet0/0
 description Outside interface

 ip address dhcp
 duplex auto
 speed auto
 crypto map mymap
!
```

```
interface FastEthernet0/1
 description Inside interface
 ip address 10.2.2.2 255.255.255.0
 duplex auto
 speed auto
 no keepalive
!
interface ATM1/0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.100.2.3
no ip http server
no ip http secure-server
!
!
!--- Standard access-list that references traffic to be
!--- encrypted. This is the only thing that needs !---
to be changed between different spoke routers. access-
list 100 permit ip 10.2.0.0 0.0.255.255 10.1.0.0
0.0.255.255
!
!
call rsvp-sync
!
!
mgcp profile default
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password cisco
 login
!
!
end
```

VPN使用者端

建立一個引用中心路由器IP地址的新連線條目。本示例中的組名稱為「testgroup」，密碼為「cisco321」。 這在集線器路由器配置中可以看到。



驗證

使用本節內容，確認您的組態是否正常運作。

在中心路由器上運行的Debug命令可確認分支和VPN客戶端連線的引數是否匹配。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **show ip interface** — 顯示分配給分支路由器的IP地址。
- **show crypto isakmp sa detail** — 顯示已在IPsec啟動器之間設定的IKE SA。例如，分支路由器和VPN客戶端，以及中心路由器。
- **show crypto ipsec sa** — 顯示已在IPsec啟動器之間設定的IPsec SA。例如，分支路由器和VPN客戶端，以及中心路由器。
- **debug crypto isakmp** — 顯示有關Internet金鑰交換(IKE)事件的消息。
- **debug crypto ipsec** — 顯示IPsec事件。
- **debug crypto engine** — 顯示加密引擎事件。

以下是**show ip interface f0/0**命令的輸出。

```
spoke#show ip interface f0/0
```

```
FastEthernet0/1 is up, line protocol is up
Internet address is 10.100.2.102/24
Broadcast address is 255.255.255.255
Address determined by DHCP
```

以下是**show crypto isakmp sa detail**命令的輸出。

```
hub#show crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection

       K - Keepalives, N - NAT-traversal

       X - IKE Extended Authentication

       psk - Preshared key, rsig - RSA signature

       renc - RSA encryption



C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.

1     10.48.67.181    10.100.2.102             3des sha  psk  2   04:15:43

2     10.48.67.181    10.51.82.100             3des sha          2   05:31:58 CX
```

以下是**show crypto ipsec sa**命令的輸出。

```
hub#show crypto ipsec sa

interface: FastEthernet0/0
Crypto map tag: mymap, local addr. 10.48.67.181

protected vrf:
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.5.5.1/255.255.255.255/0/0)
current_peer: 10.51.82.100:500
PERMIT, flags={}
#pkts encaps: 8, #pkts encrypt: 8, #pkts digest 8
#pkts decaps: 189, #pkts decrypt: 189, #pkts verify 189
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.48.67.181, remote crypto endpt.: 10.51.82.100
path mtu 1500, ip mtu 1500
current outbound spi: B0C0F4AC

inbound esp sas:
spi: 0x7A1AB8F3(2048571635)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2004, flow_id: 5, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4602415/3169)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:
```

```
inbound pcp sas:

outbound esp sas:
spi: 0xB0C0F4AC(2965435564)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2005, flow_id: 6, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4602445/3169)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

protected vrf:
local ident (addr/mask/prot/port): (10.1.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (10.2.0.0/255.255.0.0/0/0)
current_peer: 10.100.2.102:500
PERMIT, flags={}
#pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
#pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.48.67.181, remote crypto endpt.: 10.100.2.102
path mtu 1500, ip mtu 1500
current outbound spi: 5FBE5408

inbound esp sas:
spi: 0x9CD7288C(2631346316)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2002, flow_id: 3, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4569060/2071)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x5FBE5408(1606308872)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2003, flow_id: 4, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4569060/2070)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

當分支路由器啟動IKE和IPsec SA時，已在中心路由器上收集了此調試輸出。

```
ISAKMP (0:0): received packet from 10.100.2.102 dport 500 sport 500
              Global (N) NEW SA
ISAKMP: local port 500, remote port 500
ISAKMP: insert sa successfully sa = 63D5BE0C
```

```
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP (0:1): Old State = IKE_READY New State = IKE_R_MM1

ISAKMP (0:1): processing SA payload. message ID = 0
ISAKMP: Looking for a matching key for 10.100.2.102 in default
ISAKMP: Looking for a matching key for 10.100.2.102 in spokes : success
ISAKMP (0:1): found peer pre-shared key matching 10.100.2.102
ISAKMP (0:1) local preshared key found
ISAKMP : Scanning profiles for xauth ... L2L VPNclient
ISAKMP (0:1) Authentication by xauth preshared
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0:1): atts are acceptable. Next payload is 0
CryptoEngine0: generate alg parameter
CRYPTO_ENGINE: Dh phase 1 status: 0
CRYPTO_ENGINE: Dh phase 1 status: 0
ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP (0:1): Old State = IKE_R_MM1 New State = IKE_R_MM1

ISAKMP (0:1): sending packet to 10.100.2.102 my_port 500 peer_port
              500 (R) MM_SA_SETUP
ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP (0:1): Old State = IKE_R_MM1 New State = IKE_R_MM2

ISAKMP (0:1): received packet from 10.100.2.102 dport 500 sport 500
              Global (R) MM_SA_SETUP
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP (0:1): Old State = IKE_R_MM2 New State = IKE_R_MM3

ISAKMP (0:1): processing KE payload. message ID = 0
CryptoEngine0: generate alg parameter
ISAKMP (0:1): processing NONCE payload. message ID = 0
ISAKMP: Looking for a matching key for 10.100.2.102 in default
ISAKMP: Looking for a matching key for 10.100.2.102 in spokes : success
ISAKMP (0:1): found peer pre-shared key matching 10.100.2.102
CryptoEngine0: create ISAKMP SKEYID for conn id 1
ISAKMP (0:1): SKEYID state generated
ISAKMP (0:1): processing vendor id payload
ISAKMP (0:1): speaking to another IOS box!
ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP (0:1): Old State = IKE_R_MM3 New State = IKE_R_MM3

ISAKMP (0:1): sending packet to 10.100.2.102 my_port 500 peer_port 500
              (R) MM_KEY_EXCH
ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP (0:1): Old State = IKE_R_MM3 New State = IKE_R_MM4

ISAKMP (0:1): received packet from 10.100.2.102 dport 500 sport 500
              Global (R) MM_KEY_EXCH
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP (0:1): Old State = IKE_R_MM4 New State = IKE_R_MM5

ISAKMP (0:1): processing ID payload. message ID = 0
ISAKMP (0:1): ID payload
next-payload : 8
type : 1
address : 10.100.2.102
protocol : 17
port : 500
```

length : 12
ISAKMP (0:1): peer matches L2L profile
ISAKMP: Looking for a matching key for 10.100.2.102 in default
ISAKMP: Looking for a matching key for 10.100.2.102 in spokes : success
ISAKMP (0:1): Found ADDRESS key in keyring spokes
ISAKMP (0:1): processing HASH payload. message ID = 0
CryptoEngine0: generate hmac context for conn id 1
ISAKMP (0:1): SA authentication status: authenticated
ISAKMP (0:1): SA has been authenticated with 10.100.2.102
ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP (0:1): Old State = IKE_R_MM5 New State = IKE_R_MM5

ISAKMP (0:1): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP (0:1): ID payload
next-payload : 8
type : 1
address : 10.48.67.181
protocol : 17
port : 500
length : 12
ISAKMP (1): Total payload length: 12
CryptoEngine0: generate hmac context for conn id 1
CryptoEngine0: clear dh number for conn id 1
ISAKMP (0:1): sending packet to 10.100.2.102 my_port 500 peer_port 500
(R) MM_KEY_EXCH
ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP (0:1): Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE

ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP (0:1): Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

!--- IKE phase 1 is complete. ISAKMP (0:1): received packet from 10.100.2.102 dport 500 sport 500 Global (R) QM_IDLE ISAKMP: set new node 904613356 to QM_IDLE CryptoEngine0: generate hmac context for conn id 1 ISAKMP (0:1): processing HASH payload. message ID = 904613356 ISAKMP (0:1): processing SA payload. message ID = 904613356 ISAKMP (0:1): Checking IPSec proposal 1 ISAKMP: transform 1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: encaps is 1 (Tunnel) ISAKMP: SA life type in seconds ISAKMP: SA life duration (basic) of 3600 ISAKMP: SA life type in kilobytes ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: authenticator is HMAC-SHA CryptoEngine0: validate proposal **ISAKMP (0:1): atts are acceptable.**
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 10.48.67.181, remote= 10.100.2.102,
local_proxy= 10.1.0.0/255.255.0.0/0/0 (type=4),
remote_proxy= 10.2.0.0/255.255.0.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
CryptoEngine0: validate proposal request
IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
ISAKMP (0:1): processing NONCE payload. message ID = 904613356
ISAKMP (0:1): processing ID payload. message ID = 904613356
ISAKMP (0:1): processing ID payload. message ID = 904613356
ISAKMP (0:1): asking for 1 spis from ipsec
ISAKMP (0:1): Node 904613356, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP (0:1): Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): **getting spi 4172528328 for SA from 10.48.67.181 to**
10.100.2.102 for prot 3
ISAKMP: received ke message (2/1)
CryptoEngine0: generate hmac context for conn id 1
ISAKMP (0:1): sending packet to 10.100.2.102 my_port 500 peer_port 500 (R) QM_IDLE
ISAKMP (0:1): Node 904613356, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
ISAKMP (0:1): Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
ISAKMP (0:1): received packet from 10.100.2.102 dport 500 sport 500 Global

```
              (R) QM_IDLE
CryptoEngine0: generate hmac context for conn id 1
CryptoEngine0: ipsec allocate flow
CryptoEngine0: ipsec allocate flow
ISAKMP (0:1): Creating IPSec SAs
inbound SA from 10.100.2.102 to 10.48.67.181 (f/i) 0/ 0
(proxy 10.2.0.0 to 10.1.0.0)
has spi 0xF8B3BAC8 and conn_id 2000 and flags 2
lifetime of 3600 seconds
lifetime of 4608000 kilobytes
has client flags 0x0
outbound SA from 10.48.67.181 to 10.100.2.102 (f/i) 0/ 0
(proxy 10.1.0.0 to 10.2.0.0 )
has spi 1757151497 and conn_id 2001 and flags A
lifetime of 3600 seconds
lifetime of 4608000 kilobytes
has client flags 0x0
ISAKMP (0:1): deleting node 904613356 error FALSE reason "quick mode done (await)"
ISAKMP (0:1): Node 904613356, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP (0:1): Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.48.67.181, remote= 10.100.2.102,
local_proxy= 10.1.0.0/255.255.0.0/0/0 (type=4),
remote_proxy= 10.2.0.0/255.255.0.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),
lifedur= 3600s and 4608000kb,
spi= 0xF8B3BAC8(4172528328), conn_id= 2000, keysize= 0, flags= 0x2
IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 10.48.67.181, remote= 10.100.2.102,
local_proxy= 10.1.0.0/255.255.0.0/0/0 (type=4),
remote_proxy= 10.2.0.0/255.255.0.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),
lifedur= 3600s and 4608000kb,
spi= 0x68BC0109(1757151497), conn_id= 2001, keysize= 0, flags= 0xA
IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
IPSEC(add mtree): src 10.1.0.0, dest 10.2.0.0, dest_port 0

IPSEC(create_sa): sa created,
(sa) sa_dest= 10.48.67.181, sa_prot= 50,
sa_spi= 0xF8B3BAC8(4172528328),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2000
IPSEC(create_sa): sa created,
(sa) sa_dest= 10.100.2.102, sa_prot= 50,
sa_spi= 0x68BC0109(1757151497),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2001
```

當VPN客戶端啟動IKE和IPsec SA時，已在中心路由器上收集此調試輸出。

```
ISAKMP (0:0): received packet from 10.51.82.100 dport 500 sport 500 Global
              (N) NEW SA
ISAKMP: local port 500, remote port 500
ISAKMP: insert sa successfully sa = 63D3D804
ISAKMP (0:2): processing SA payload. message ID = 0
ISAKMP (0:2): processing ID payload. message ID = 0
ISAKMP (0:2): ID payload
next-payload : 13
type : 11
group id : testgroup
protocol : 17
port : 500
length : 17
```

ISAKMP (0:2): peer matches VPNclient profile
ISAKMP: Looking for a matching key for 10.51.82.100 in default
ISAKMP: Looking for a matching key for 10.51.82.100 in spokes : success
ISAKMP: Created a peer struct for 10.51.82.100, peer port 500
ISAKMP: Locking peer struct 0x644AFC7C, IKE refcount 1 for
crypto_ikmp_config_initialize_sa
ISAKMP (0:2): Setting client config settings 644AFCF8
ISAKMP (0:2): (Re)Setting client xauth list and state
ISAKMP (0:2): processing vendor id payload
ISAKMP (0:2): vendor ID seems Unity/DPD but major 215 mismatch
ISAKMP (0:2): vendor ID is Xauth
ISAKMP (0:2): processing vendor id payload
ISAKMP (0:2): vendor ID is DPD
ISAKMP (0:2): processing vendor id payload
ISAKMP (0:2): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP (0:2): vendor ID is NAT-T v2
ISAKMP (0:2): processing vendor id payload
ISAKMP (0:2): vendor ID seems Unity/DPD but major 194 mismatch
ISAKMP (0:2): processing vendor id payload
ISAKMP (0:2): vendor ID is Unity
ISAKMP (0:2) Authentication by xauth preshared

!--- Check of ISAKMP transforms against the configured ISAKMP policy. ISAKMP (0:2): Checking
ISAKMP transform 9 against priority 10 policy ISAKMP: encryption 3DES-CBC ISAKMP: hash SHA
ISAKMP: default group 2 ISAKMP: auth XAUTHInitPreShared ISAKMP: life type in seconds ISAKMP:
life duration (VPI) of 0x0 0x20 0xC4 0x9B ISAKMP (0:2): **atts are acceptable.** Next payload is 3
CryptoEngine0: generate alg parameter
CRYPTO_ENGINE: Dh phase 1 status: 0
CRYPTO_ENGINE: Dh phase 1 status: 0
ISAKMP (0:2): processing KE payload. message ID = 0
CryptoEngine0: generate alg parameter
ISAKMP (0:2): processing NONCE payload. message ID = 0
ISAKMP (0:2): vendor ID is NAT-T v2
ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
ISAKMP (0:2): Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT

ISAKMP: got callback 1
CryptoEngine0: create ISAKMP SKEYID for conn id 2
ISAKMP (0:2): SKEYID state generated
ISAKMP (0:2): constructed NAT-T vendor-02 ID
ISAKMP (0:2): SA is doing pre-shared key authentication plus XAUTH
using id type ID_IPV4_ADDR
ISAKMP (0:2): ID payload
next-payload : 10
type : 1
address : 10.48.67.181
protocol : 17
port : 0
length : 12
ISAKMP (2): Total payload length: 12
CryptoEngine0: generate hmac context for conn id 2
ISAKMP (0:2): sending packet to 10.51.82.100 my_port 500 peer_port 500
(R) AG_INIT_EXCH
ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY
ISAKMP (0:2): Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2

ISAKMP (0:2): received packet from 10.51.82.100 dport 500 sport 500 Global
(R) AG_INIT_EXCH
ISAKMP (0:2): processing HASH payload. message ID = 0
CryptoEngine0: generate hmac context for conn id 2
ISAKMP (0:2): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 63D3D804
ISAKMP (0:2): SA authentication status: authenticated
ISAKMP (0:2): Process initial contact,

```
bring down existing phase 1 and 2 SA's with local 10.48.67.181 remote
        10.51.82.100 remote port 500
ISAKMP (0:2): returning IP addr to the address pool
IPSEC(key_engine): got a queue event...
ISAKMP:received payload type 17
ISAKMP:received payload type 17
ISAKMP (0:2): SA authentication status: authenticated
ISAKMP (0:2): SA has been authenticated with 10.51.82.100
CryptoEngine0: clear dh number for conn id 1
ISAKMP: Trying to insert a peer 10.48.67.181/10.51.82.100/500/,
        and inserted successfully.
ISAKMP: set new node 1257790711 to CONF_XAUTH
CryptoEngine0: generate hmac context for conn id 2
ISAKMP (0:2): sending packet to 10.51.82.100 my_port 500 peer_port 500 (R) QM_IDLE
ISAKMP (0:2): purging node 1257790711
ISAKMP: Sending phase 1 responder lifetime 86400

ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
ISAKMP (0:2): Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE

ISAKMP (0:2): Need XAUTH
ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP (0:2): Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT

ISAKMP: got callback 1
ISAKMP: set new node 955647754 to CONF_XAUTH

!--- Extended authentication begins. ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
CryptoEngine0: generate hmac context for conn id 2
ISAKMP (0:2): initiating peer config to 10.51.82.100. ID = 955647754
ISAKMP (0:2): sending packet to 10.51.82.100 my_port 500 peer_port 500
             (R) CONF_XAUTH
ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, IKE_AAA_START_LOGIN
ISAKMP (0:2): Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT New State =
              IKE_XAUTH_REQ_SENT

ISAKMP (0:2): received packet from 10.51.82.100 dport 500 sport 500 Global
             (R) CONF_XAUTH
ISAKMP (0:2): processing transaction payload from 10.51.82.100. message
              ID = 955647754
CryptoEngine0: generate hmac context for conn id 2
ISAKMP: Config payload REPLY

!--- Username/password received from the VPN Client. ISAKMP/xauth: reply attribute
XAUTH_USER_NAME_V2
ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
ISAKMP (0:2): deleting node 955647754 error FALSE reason "done with
              xauth request/reply exchange"
ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY
ISAKMP (0:2): Old State = IKE_XAUTH_REQ_SENT New State =
             IKE_XAUTH_AAA_CONT_LOGIN_AWAIT

ISAKMP: got callback 1
ISAKMP: set new node -1118110738 to CONF_XAUTH
CryptoEngine0: generate hmac context for conn id 2
ISAKMP (0:2): initiating peer config to 10.51.82.100. ID = -1118110738
ISAKMP (0:2): sending packet to 10.51.82.100 my_port 500 peer_port
              500 (R) CONF_XAUTH
ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, IKE_AAA_CONT_LOGIN
ISAKMP (0:2): Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT New State =
              IKE_XAUTH_SET_SENT

ISAKMP (0:2): received packet from 10.51.82.100 dport 500 sport 500 Global
```

```
            (R) CONF_XAUTH
ISAKMP (0:2): processing transaction payload from 10.51.82.100. message
              ID = -1118110738
CryptoEngine0: generate hmac context for conn id 2

 !--- Success ISAKMP: Config payload ACK ISAKMP (0:2): XAUTH ACK Processed
ISAKMP (0:2): deleting node -1118110738 error FALSE reason "done with transaction"
ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK
ISAKMP (0:2): Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE

ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP (0:2): Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

ISAKMP (0:2): received packet from 10.51.82.100 dport 500 sport 500
              Global (R) QM_IDLE
ISAKMP: set new node -798495444 to QM_IDLE
ISAKMP (0:2): processing transaction payload from 10.51.82.100. message
              ID = -798495444
CryptoEngine0: generate hmac context for conn id 2
ISAKMP: Config payload REQUEST
ISAKMP (0:2): checking request:
ISAKMP: IP4_ADDRESS
ISAKMP: IP4_NETMASK
ISAKMP: IP4_DNS
ISAKMP: IP4_NBNS
ISAKMP: ADDRESS_EXPIRY
ISAKMP: UNKNOWN Unknown Attr: 0x7000
ISAKMP: UNKNOWN Unknown Attr: 0x7001
ISAKMP: DEFAULT_DOMAIN
ISAKMP: SPLIT_INCLUDE
ISAKMP: UNKNOWN Unknown Attr: 0x7003
ISAKMP: UNKNOWN Unknown Attr: 0x7007
ISAKMP: UNKNOWN Unknown Attr: 0x7009
ISAKMP: APPLICATION_VERSION
ISAKMP: UNKNOWN Unknown Attr: 0x7008
ISAKMP: UNKNOWN Unknown Attr: 0x700A
ISAKMP: UNKNOWN Unknown Attr: 0x7005
ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST
ISAKMP (0:2): Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

ISAKMP: got callback 1
ISAKMP (0:2): attributes sent in message:
Address: 0.2.0.0
ISAKMP (0:2): allocating address 10.5.5.1
ISAKMP: Sending private address: 10.5.5.1
ISAKMP: Sending IP4_DNS server address: 1.1.1.1
ISAKMP: Sending IP4_DNS server address: 2.2.2.2
ISAKMP: Sending IP4_NBNS server address: 3.3.3.3
ISAKMP: Sending IP4_NBNS server address: 4.4.4.4
ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address: 86386
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x7000)
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x7001)
ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x7003)
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x7007)
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x7009)
ISAKMP: Sending APPLICATION_VERSION string: Cisco Internetwork Operating
       System Software
IOS (tm) 7200 Software (C7200-IK9S-M), Version 12.3(6a), RELEASE SOFTWARE (fc4)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 02-Apr-04 15:52 by kellythw
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x7008)
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x700A)
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x7005)
```

```
CryptoEngine0: generate hmac context for conn id 2
ISAKMP (0:2): responding to peer config from 10.51.82.100. ID = -798495444
ISAKMP (0:2): sending packet to 10.51.82.100 my_port 500 peer_port 500 (R) CONF_ADDR
ISAKMP (0:2): deleting node -798495444 error FALSE reason ""
ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR
ISAKMP (0:2): Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE

ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP (0:2): Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
```

!--- IKE phase 1 and Config Mode complete. !--- Check of IPsec proposals against configured transform set(s). ISAKMP (0:2): Checking IPSec proposal 12 ISAKMP: transform 1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-SHA ISAKMP: encaps is 1 (Tunnel) ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B CryptoEngine0: validate proposal ISAKMP (0:2): atts are acceptable. IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.48.67.181, remote= 10.51.82.100, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.5.5.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2 CryptoEngine0: validate proposal request IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf = IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf = ISAKMP (0:2): processing NONCE payload. message ID = 381726614 ISAKMP (0:2): processing ID payload. message ID = 381726614 ISAKMP (0:2): processing ID payload. message ID = 381726614 ISAKMP (0:2): asking for 1 spis from ipsec ISAKMP (0:2): Node 381726614, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH ISAKMP (0:2): Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE IPSEC(key_engine): got a queue event... IPSEC(spi_response): getting spi 2048571635 for SA from 10.48.67.181 to 10.51.82.100 for prot 3 ISAKMP: received ke message (2/1) CryptoEngine0: generate hmac context for conn id 2 ISAKMP (0:2): sending packet to 10.51.82.100 my_port 500 peer_port 500 (R) QM_IDLE ISAKMP (0:2): Node 381726614, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY ISAKMP (0:2): Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2 ISAKMP (0:2): received packet from 10.51.82.100 dport 500 sport 500 Global (R) QM_IDLE CryptoEngine0: generate hmac context for conn id 2 CryptoEngine0: ipsec allocate flow CryptoEngine0: ipsec allocate flow ISAKMP: Locking peer struct 0x644AFC7C, IPSEC refcount 1 for for stuff_ke ISAKMP (0:2): Creating IPSec SAs inbound SA from 10.51.82.100 to 10.48.67.181 (f/i) 0/ 0 (proxy 10.5.5.1 to 0.0.0.0) has spi 0x7A1AB8F3 and conn_id 2004 and flags 2 lifetime of 2147483 seconds has client flags 0x0 outbound SA from 10.48.67.181 to 10.51.82.100 (f/i) 0/ 0 (proxy 0.0.0.0 to 10.5.5.1) has spi -1329531732 and conn_id 2005 and flags A lifetime of 2147483 seconds has client flags 0x0 ISAKMP (0:2): deleting node 381726614 error FALSE reason "quick mode done (await)" ISAKMP (0:2): Node 381726614, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH ISAKMP (0:2): Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE IPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) **INBOUND** local= 10.48.67.181, remote= 10.51.82.100,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 10.5.5.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),
lifedur= 2147483s and 0kb,
spi= 0x7A1AB8F3(2048571635), conn_id= 2004, keysize= 0, flags= 0x2
IPSEC(initialize_sas): ,
(key eng. msg.) **OUTBOUND** local= 10.48.67.181, remote= 10.51.82.100,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 10.5.5.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),
lifedur= 2147483s and 0kb,
spi= 0xB0C0F4AC(2965435564), conn_id= 2005, keysize= 0, flags= 0xA
IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
IPSEC(add mtree): src 0.0.0.0, dest 10.5.5.1, dest_port 0

IPSEC(create_sa): **sa created,**
(sa) sa_dest= 10.48.67.181, sa_prot= 50,
sa_spi= 0x7A1AB8F3(2048571635),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2004
IPSEC(create_sa): **sa created,**
(sa) sa_dest= 10.51.82.100, sa_prot= 50,
sa_spi= 0xB0C0F4AC(2965435564),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2005
```
```

驗證加密對映序列號

如果靜態對等體和動態對等體配置在同一加密對映上，則加密對映條目的順序非常重要。動態加密對映條目的序列號必**須高於**所有其他靜態加密對映條目。如果靜態條目的編號高於動態條目的編號，則與這些對等體的連線將失敗。

以下是包含靜態專案與動態專案的正確編號密碼編譯對應範例。請注意，動態條目的序列號最高，並且預留空間以新增其他靜態條目：

```
crypto dynamic-map dynmap 20
set transform-set myset
crypto map mymap 10 ipsec-isakmp
match address 100
set peer 172.16.77.10
set transform-set myset
crypto map mymap 60000 ipsec-isakmp dynamic dynmap
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- IPsec設定檔組態
- Cisco IOS軟體版本12.2(15)T新功能
- IPsec協商/IKE通訊協定支援頁面
- 技術支援與文件 - Cisco Systems