ISAKMPプロファイルを使用したDMVPNおよびEasy VPNサーバの設定

内容

概要

このドキュメントでは、Xauth を使用して、Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）と Easy VPN を同じルータ上に設定する方法について説明します。この設定により、DMVPN スポークにダイナミック アドレスを指定できるようになります。Internet Security Association and Key Management Protocol（ISAKMP）プロファイルは、ダイナミックにアドレス指定された DMVPN スポークまたは Easy VPN Client の認証方式を区別する機能を提供します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS ソフトウェア リリース 12.3(3) および 12.3(3)a を実行している Cisco 2691 および 3725 ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

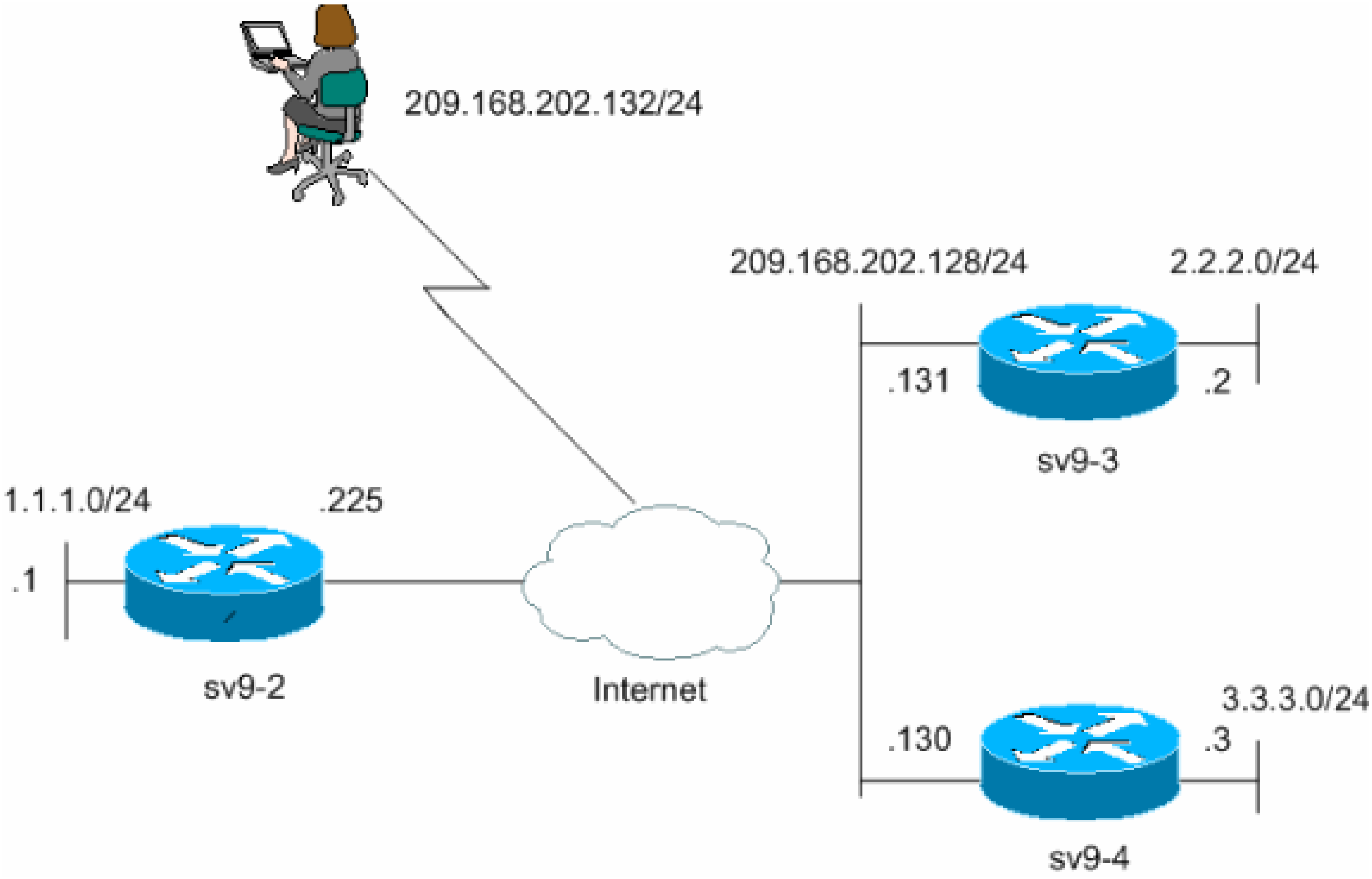
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注： このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク設定を使用します。



設定

このドキュメントでは次の設定を使用します。

- sv9-2 ハブ設定
- sv9-3 スポーク設定
- sv9-4 スポーク設定

sv9-2 ハブ設定

```
sv9-2#show run
Building configuration...

Current configuration : 2876 bytes
!
version 12.3
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
!
username cisco password 0 cisco
aaa new-model
!
!
!--- Xauth is configured for local authentication. aaa
authentication login userauthen local
aaa authorization network hw-client-groupname local
aaa session-id common
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!

!--- Keyring that defines the wildcard pre-shared key.
crypto keyring dmvpnspokes
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!



!--- Create an ISAKMP policy for Phase 1 negotiations.
!--- This policy is for DMVPN spokes. crypto isakmp
policy 10
hash md5
authentication pre-share
!

!--- Create an ISAKMP policy for Phase 1 negotiations.
!--- This policy is for Easy VPN Clients. crypto isakmp
policy 20
hash md5
authentication pre-share
group 2

!

!--- VPN Client configuration for group "hw-client-
groupname" !--- (this name is configured in the VPN
Client). crypto isakmp client configuration group hw-
client-groupname
```

```
key hw-client-password
dns 1.1.11.10 1.1.11.11
wins 1.1.11.12 1.1.11.13
domain cisco.com
pool dynpool


!--- Profile for VPN Client connections, matches the !--
- "hw-client-group" group and defines the XAuth
properties. crypto isakmp profile VPNclient
match identity group hw-client-groupname
client authentication list userauthen
isakmp authorization list hw-client-groupname
client configuration address respond


!--- Profile for LAN-to-LAN connection, 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 DMVPN
keyring dmvpnspokes
match identity address 0.0.0.0
!
!

!--- Create the Phase 2 policy for actual data
encryption. crypto ipsec transform-set strong esp-3des
esp-md5-hmac
mode transport
!

!--- Create an IPsec profile to be applied dynamically
to the !--- generic routing encapsulation (GRE) over
IPsec tunnels. crypto ipsec profile cisco
set security-association lifetime seconds 120
set transform-set strong
set isakmp-profile DMVPN
!
!

!--- This dynamic crypto map references the ISAKMP !---
Profile VPN Client above. !--- Reverse route injection
is used to provide the !--- DMVPN networks access to any
Easy VPN Client networks. crypto dynamic-map dynmap 10
set isakmp-profile VPNclient
reverse-route
set transform-set strong
!
!

!--- Crypto map only references the dynamic crypto map
above. crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
!
!
!
!
!
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
```

```
!
!
!
!
!
!

!--- Create a GRE tunnel template which is 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
ip nhrp holdtime 300
no ip split-horizon eigrp 90
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco
!
interface FastEthernet0/0
ip address 209.168.202.225 255.255.255.0
duplex auto
speed auto
crypto map dynmap
!
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
redistribute static
network 1.1.1.0 0.0.0.255
network 192.168.1.0
no auto-summary
!
ip local pool dynpool 1.1.11.60 1.1.11.80
ip http server
no ip http secure-server
ip classless
!
```

```
!
!
!
!
!
!
!
!
!
!
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
transport preferred all
transport input all
transport output all
!
!
end
```

sv9-3 スポーク設定

```

sv9-3#show run
Building configuration...

Current configuration : 2052 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sv9-3
!
boot-start-marker
boot system flash:c3725-ik9o3s-mz.123-3.bin
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!
!--- Create an ISAKMP policy for Phase 1 negotiations.
crypto isakmp policy 10
hash md5
authentication pre-share
```

```
!--- Add dynamic pre-shared keys for all 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
mode transport
!
!--- 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 is 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 holdtime 300
ip nhrp nhs 192.168.1.1
no ip split-horizon eigrp 90
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco
!
interface FastEthernet0/0
ip address 209.168.202.130 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 3.3.3.3 255.255.255.0
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 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 0.0.0.0 0.0.0.0 209.168.202.225
ip route 2.2.2.0 255.255.255.0 Tunnel0
!
!
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
```

sv9-4 スポーク設定

```
sv9-4#show run
Building configuration...

Current configuration : 1992 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-jk9o3s-mz.123-3a.bin
boot-end-marker
!
enable password cisco
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
```

```
!
!
!
!--- Create an ISAKMP policy for Phase 1 negotiations.
crypto isakmp policy 10
hash md5
authentication pre-share
!--- Add dynamic pre-shared keys for all 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
mode transport
!
!--- Create an IPsec profile apply 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 is 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 holdtime 300
ip nhrp nhs 192.168.1.1
no ip split-horizon eigrp 90
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco
!
interface FastEthernet0/0
ip address 209.168.202.131 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 2.2.2.2 255.255.255.0
duplex auto
speed auto
!
!--- 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
!
!
dial-peer cor custom
!
!
line con 0
exec-timeout 0 0
transport output lat pad v120 lapb-ta mop telnet rlogin
udptn ssh
escape-character 27
line aux 0
transport output lat pad v120 lapb-ta mop telnet rlogin
udptn ssh
line vty 0 4
login
transport input lat pad v120 lapb-ta mop telnet rlogin
udptn ssh
transport output lat pad v120 lapb-ta mop telnet rlogin
udptn ssh
!
!
end
```

確認

この項では、設定が正常に動作しているかどうかを確認する際に役立つ情報を紹介しています。

ハブ ルータ上で debug コマンドを実行すると、スポークと VPN Client の接続に正しいパラメータが対応しているかどうかが確認されます。次の **debug コマンドを実行します。**

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **debug crypto isakmp**：IKE イベントに関するメッセージを表示します。
- **debug crypto ipsec** - IPsec イベントに関する情報を表示します。

```
sv9-2#
*Mar 13 04:38:21.187: ISAKMP (0:0): received packet from 209.168.202.130
                      dport 500 sport 500 Global (N) NEW SA
*Mar 13 04:38:21.187: ISAKMP: local port 500, remote port 500
*Mar 13 04:38:21.187: ISAKMP: insert sa successfully sa = 63F585CC
*Mar 13 04:38:21.187: ISAKMP (0:689): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Mar 13 04:38:21.187: ISAKMP (0:689): Old State = IKE_READY New State = IKE_R_MM1

*Mar 13 04:38:21.187: ISAKMP (0:689): processing SA payload. message ID = 0
*Mar 13 04:38:21.187: ISAKMP (0:689): processing vendor id payload
*Mar 13 04:38:21.187: ISAKMP (0:689): vendor ID seems Unity/DPD but
                       major 157 mismatch
*Mar 13 04:38:21.187: ISAKMP (0:689): vendor ID is NAT-T v3
*Mar 13 04:38:21.187: ISAKMP (0:689): processing vendor id payload
*Mar 13 04:38:21.191: ISAKMP (0:689): vendor ID seems Unity/DPD but
                       major 123 mismatch
*Mar 13 04:38:21.191: ISAKMP (0:689): vendor ID is NAT-T v2
```

```
*Mar 13 04:38:21.191: ISAKMP: Looking for a matching key for 209.168.202.130
                      in default
*Mar 13 04:38:21.191: ISAKMP: Looking for a matching key for 209.168.202.130
                      in dmvpnspokes : success
*Mar 13 04:38:21.191: ISAKMP (0:689): found peer pre-shared key matching
                      209.168.202.130
*Mar 13 04:38:21.191: ISAKMP (0:689) local preshared key found
*Mar 13 04:38:21.191: ISAKMP : Scanning profiles for xauth ... VPNclient
*Mar 13 04:38:21.191: ISAKMP (0:689) Authentication by xauth preshared
*Mar 13 04:38:21.191: ISAKMP (0:689): Checking ISAKMP transform 1 against
                       priority 10 policy
*Mar 13 04:38:21.191: ISAKMP: encryption DES-CBC
*Mar 13 04:38:21.191: ISAKMP: hash MD5
*Mar 13 04:38:21.191: ISAKMP: default group 1
*Mar 13 04:38:21.191: ISAKMP: auth pre-share
*Mar 13 04:38:21.191: ISAKMP: life type in seconds
*Mar 13 04:38:21.191: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
*Mar 13 04:38:21.191: ISAKMP (0:689): atts are acceptable. Next payload is 0
*Mar 13 04:38:21.195: ISAKMP (0:689): processing vendor id payload
*Mar 13 04:38:21.195: ISAKMP (0:689): vendor ID seems Unity/DPD but major
                       157 mismatch
*Mar 13 04:38:21.195: ISAKMP (0:689): vendor ID is NAT-T v3
*Mar 13 04:38:21.195: ISAKMP (0:689): processing vendor id payload
*Mar 13 04:38:21.195: ISAKMP (0:689): vendor ID seems Unity/DPD but
                       major 123 mismatch
*Mar 13 04:38:21.195: ISAKMP (0:689): vendor ID is NAT-T v2
*Mar 13 04:38:21.195: ISAKMP (0:689): Input = IKE_MESG_INTERNAL,
                      IKE_PROCESS_MAIN_MODE
*Mar 13 04:38:21.195: ISAKMP (0:689): Old State = IKE_R_MM1 New State = IKE_R_MM1

*Mar 13 04:38:21.195: ISAKMP (0:689): constructed NAT-T vendor-03 ID
*Mar 13 04:38:21.195: ISAKMP (0:689): sending packet to 209.168.202.130
                      my_port 500 peer_port 500 (R) MM_SA_SETUP
*Mar 13 04:38:21.195: ISAKMP (0:689): Input = IKE_MESG_INTERNAL,
                      IKE_PROCESS_COMPLETE
*Mar 13 04:38:21.195: ISAKMP (0:689): Old State = IKE_R_MM1 New State = IKE_R_MM2

*Mar 13 04:38:21.203: ISAKMP (0:689): received packet from 209.168.202.130 dport
                      500 sport 500 Global (R) MM_SA_SETUP
*Mar 13 04:38:21.203: ISAKMP (0:689): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Mar 13 04:38:21.203: ISAKMP (0:689): Old State = IKE_R_MM2 New State = IKE_R_MM3

*Mar 13 04:38:21.203: ISAKMP (0:689): processing KE payload. message ID = 0
*Mar 13 04:38:21.211: ISAKMP (0:689): processing NONCE payload. message ID = 0
*Mar 13 04:38:21.211: ISAKMP: Looking for a matching key for 209.168.202.130
                      in default
*Mar 13 04:38:21.211: ISAKMP: Looking for a matching key for 209.168.202.130
                      in dmvpnspokes : success
*Mar 13 04:38:21.211: ISAKMP (0:689): found peer pre-shared key matching
                      209.168.202.130
*Mar 13 04:38:21.211: ISAKMP: Looking for a matching key for 209.168.202.130
                      in default
*Mar 13 04:38:21.211: ISAKMP: Looking for a matching key for 209.168.202.130
                      in dmvpnspokes : success
*Mar 13 04:38:21.211: ISAKMP (0:689): found peer pre-shared key matching
                      209.168.202.130
*Mar 13 04:38:21.215: ISAKMP (0:689): SKEYID state generated
*Mar 13 04:38:21.215: ISAKMP (0:689): processing vendor id payload
*Mar 13 04:38:21.215: ISAKMP (0:689): vendor ID is Unity
*Mar 13 04:38:21.215: ISAKMP (0:689): processing vendor id payload
*Mar 13 04:38:21.215: ISAKMP (0:689): vendor ID is DPD
*Mar 13 04:38:21.215: ISAKMP (0:689): processing vendor id payload
*Mar 13 04:38:21.215: ISAKMP (0:689): speaking to another IOS box!
*Mar 13 04:38:21.215: ISAKMP:received payload type 17
```

```
*Mar 13 04:38:21.215: ISAKMP:received payload type 17
*Mar 13 04:38:21.215: ISAKMP (0:689): Input = IKE_MESG_INTERNAL,
                      IKE_PROCESS_MAIN_MODE
*Mar 13 04:38:21.215: ISAKMP (0:689): Old State = IKE_R_MM3 New State = IKE_R_MM3

*Mar 13 04:38:21.215: ISAKMP (0:689): sending packet to 209.168.202.130
                      my_port 500 peer_port 500 (R) MM_KEY_EXCH
*Mar 13 04:38:21.215: ISAKMP (0:689): Input = IKE_MESG_INTERNAL,
                      IKE_PROCESS_COMPLETE
*Mar 13 04:38:21.215: ISAKMP (0:689): Old State = IKE_R_MM3 New State = IKE_R_MM4

*Mar 13 04:38:21.227: ISAKMP (0:689): received packet from 209.168.202.130
                      dport 500 sport 500 Global (R) MM_KEY_EXCH
*Mar 13 04:38:21.227: ISAKMP (0:689): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Mar 13 04:38:21.227: ISAKMP (0:689): Old State = IKE_R_MM4 New State = IKE_R_MM5

*Mar 13 04:38:21.227: ISAKMP (0:689): processing ID payload. message ID = 0
*Mar 13 04:38:21.227: ISAKMP (0:689): peer matches DMVPN profile
*Mar 13 04:38:21.227: ISAKMP: Looking for a matching key for 209.168.202.130
                      in default
*Mar 13 04:38:21.227: ISAKMP: Looking for a matching key for 209.168.202.130
                      in dmvpnspokes : success
*Mar 13 04:38:21.227: ISAKMP (0:689): Found ADDRESS key in keyring dmvpnspokes
*Mar 13 04:38:21.227: ISAKMP (0:689): processing HASH payload. message ID = 0
*Mar 13 04:38:21.227: ISAKMP (0:689): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 63F585CC
*Mar 13 04:38:21.227: ISAKMP (0:689): Process initial contact,
                      bring down existing phase 1 and 2 SA's with local
                      209.168.202.225 remote
                      209.168.202.130 remote port 500
*Mar 13 04:38:21.227: IPSEC(key_engine): got a queue event...
*Mar 13 04:38:21.231: ISAKMP (0:689): SA has been authenticated
                      with 209.168.202.130
*Mar 13 04:38:21.231: ISAKMP (0:689): Input = IKE_MESG_INTERNAL,
                      IKE_PROCESS_MAIN_MODE
*Mar 13 04:38:21.231: ISAKMP (0:689): Old State = IKE_R_MM5 New State = IKE_R_MM5

*Mar 13 04:38:21.231: ISAKMP (0:689): SA is doing pre-shared key
                      authentication using id type ID_IPV4_ADDR
*Mar 13 04:38:21.231: ISAKMP (689): ID payload
next-payload : 8
type : 1
addr : 209.168.202.225
protocol : 17
port : 500
length : 8
*Mar 13 04:38:21.231: ISAKMP (689): Total payload length: 12
*Mar 13 04:38:21.231: ISAKMP (0:689): sending packet to 209.168.202.130
                      my_port 500 peer_port 500 (R) MM_KEY_EXCH
*Mar 13 04:38:21.231: ISAKMP (0:689): Input = IKE_MESG_INTERNAL,
                      IKE_PROCESS_COMPLETE
*Mar 13 04:38:21.231: ISAKMP (0:689): Old State = IKE_R_MM5 New State =
                      IKE_P1_COMPLETE

*Mar 13 04:38:21.231: ISAKMP (0:689): Input = IKE_MESG_INTERNAL,
                      IKE_PHASE1_COMPLETE
*Mar 13 04:38:21.231: ISAKMP (0:689): Old State = IKE_P1_COMPLETE
                      New State = IKE_P1_COMPLETE

*Mar 13 04:38:21.235: ISAKMP (0:689): received packet from
                      209.168.202.130 dport 500 sport 500 Global (R) QM_IDLE

*Mar 13 04:38:21.235: ISAKMP: set new node -1213418274 to QM_IDLE
*Mar 13 04:38:21.235: ISAKMP (0:689): processing HASH payload. message ID = -1213418274
```

```
*Mar 13 04:38:21.235: ISAKMP (0:689): processing SA payload. message ID = -1213418274
*Mar 13 04:38:21.235: ISAKMP (0:689): Checking IPSec proposal 1
*Mar 13 04:38:21.235: ISAKMP: transform 1, ESP_3DES
*Mar 13 04:38:21.235: ISAKMP: attributes in transform:
*Mar 13 04:38:21.235: ISAKMP: encaps is 2
*Mar 13 04:38:21.235: ISAKMP: SA life type in seconds
*Mar 13 04:38:21.235: ISAKMP: SA life duration (basic) of 120
*Mar 13 04:38:21.235: ISAKMP: SA life type in kilobytes
*Mar 13 04:38:21.235: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Mar 13 04:38:21.235: ISAKMP: authenticator is HMAC-MD5
*Mar 13 04:38:21.235: ISAKMP (0:689): atts are acceptable.
*Mar 13 04:38:21.235: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 209.168.202.225, remote= 209.168.202.130,
local_proxy= 209.168.202.225/255.255.255.255/47/0 (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= 0x4
*Mar 13 04:38:21.239: IPSEC(kei_proxy): head = Tunnel0-head-0,
                      map->ivrf = , kei->ivrf =
*Mar 13 04:38:21.239: IPSEC(kei_proxy): head = Tunnel0-head-0,
                      map->ivrf = , kei->ivrf =
*Mar 13 04:38:21.239: ISAKMP (0:689): processing NONCE payload.
                      message ID = -1213418274
*Mar 13 04:38:21.239: ISAKMP (0:689): processing ID payload.
                      message ID = -1213418274
*Mar 13 04:38:21.239: ISAKMP (0:689): processing ID payload.
                      message ID = -1213418274
*Mar 13 04:38:21.239: ISAKMP (0:689): asking for 1 spis from ipsec
*Mar 13 04:38:21.239: ISAKMP (0:689): Node -1213418274, Input =
                      IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Mar 13 04:38:21.239: ISAKMP (0:689): Old State = IKE_QM_READY
                      New State = IKE_QM_SPI_STARVE
*Mar 13 04:38:21.239: IPSEC(key_engine): got a queue event...
*Mar 13 04:38:21.239: IPSEC(spi_response): getting spi 3759277150 for SA
from 209.168.202.225 to 209.168.202.130 for prot 3
*Mar 13 04:38:21.239: ISAKMP (0:689): received packet from
                      209.168.202.130 dport 500 sport 500 Global (R) QM_IDLE

*Mar 13 04:38:21.239: ISAKMP: set new node -1392382616 to QM_IDLE
*Mar 13 04:38:21.239: ISAKMP (0:689): processing HASH payload.
                      message ID = -1392382616
*Mar 13 04:38:21.239: ISAKMP (0:689): processing SA payload.
                      message ID = -1392382616
*Mar 13 04:38:21.239: ISAKMP (0:689): Checking IPSec proposal 1
*Mar 13 04:38:21.239: ISAKMP: transform 1, ESP_3DES
*Mar 13 04:38:21.239: ISAKMP: attributes in transform:
*Mar 13 04:38:21.239: ISAKMP: encaps is 2
*Mar 13 04:38:21.239: ISAKMP: SA life type in seconds
*Mar 13 04:38:21.239: ISAKMP: SA life duration (basic) of 120
*Mar 13 04:38:21.239: ISAKMP: SA life type in kilobytes
*Mar 13 04:38:21.239: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Mar 13 04:38:21.239: ISAKMP: authenticator is HMAC-MD5
*Mar 13 04:38:21.239: ISAKMP (0:689): atts are acceptable.
*Mar 13 04:38:21.243: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 209.168.202.225, remote= 209.168.202.130,
local_proxy= 209.168.202.225/255.255.255.255/47/0 (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= 0x4
*Mar 13 04:38:21.243: IPSEC(kei_proxy): head = Tunnel0-head-0,
                      map->ivrf = , kei->ivrf =
*Mar 13 04:38:21.243: IPSEC(kei_proxy): head = Tunnel0-head-0,
                       map->ivrf = , kei->ivrf =
*Mar 13 04:38:21.243: ISAKMP (0:689): processing NONCE payload.
                      message ID = -1392382616
*Mar 13 04:38:21.243: ISAKMP (0:689): processing ID payload.
                       message ID = -1392382616
*Mar 13 04:38:21.243: ISAKMP (0:689): processing ID payload.
                      message ID = -1392382616
*Mar 13 04:38:21.243: ISAKMP (0:689): asking for 1 spis from ipsec
*Mar 13 04:38:21.243: ISAKMP (0:689): Node -1392382616, Input =
                      IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Mar 13 04:38:21.243: ISAKMP (0:689): Old State = IKE_QM_READY
                      New State = IKE_QM_SPI_STARVE
*Mar 13 04:38:21.243: ISAKMP: received ke message (2/1)
*Mar 13 04:38:21.243: IPSEC(key_engine): got a queue event...
*Mar 13 04:38:21.243: IPSEC(spi_response): getting spi 1258185233 for SA
from 209.168.202.225 to 209.168.202.130 for prot 3
*Mar 13 04:38:21.243: ISAKMP: received ke message (2/1)
*Mar 13 04:38:21.491: ISAKMP (0:689): sending packet to
                      209.168.202.130 my_port 500 peer_port 500 (R) QM_IDLE
*Mar 13 04:38:21.491: ISAKMP (0:689): Node -1213418274, Input =
                      IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
*Mar 13 04:38:21.491: ISAKMP (0:689): Old State = IKE_QM_SPI_STARVE
                      New State = IKE_QM_R_QM2
*Mar 13 04:38:21.495: ISAKMP (0:689): sending packet to 209.168.202.130
                       my_port 500 peer_port 500 (R) QM_IDLE
*Mar 13 04:38:21.495: ISAKMP (0:689): Node -1392382616, Input =
                      IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
*Mar 13 04:38:21.495: ISAKMP (0:689): Old State = IKE_QM_SPI_STARVE
                       New State = IKE_QM_R_QM2
*Mar 13 04:38:21.503: ISAKMP (0:689): received packet from 209.168.202.130
                      dport 500 sport 500 Global (R) QM_IDLE

*Mar 13 04:38:21.511: ISAKMP (0:689): Creating IPSec SAs
*Mar 13 04:38:21.511: inbound SA from 209.168.202.130 to
                       209.168.202.225 (f/i) 0/ 0
                      (proxy 209.168.202.130 to 209.168.202.225)
*Mar 13 04:38:21.511: has spi 0xE012045E and conn_id 13777 and flags 4
*Mar 13 04:38:21.511: lifetime of 120 seconds
*Mar 13 04:38:21.511: lifetime of 4608000 kilobytes
*Mar 13 04:38:21.511: has client flags 0x0
*Mar 13 04:38:21.511: outbound SA from 209.168.202.225 to
                      209.168.202.130 (f/i) 0/ 0 (proxy 209.168.202.225
                      to 209.168.202.130)
*Mar 13 04:38:21.511: has spi 1398157896 and conn_id 13778 and flags C
*Mar 13 04:38:21.511: lifetime of 120 seconds
*Mar 13 04:38:21.511: lifetime of 4608000 kilobytes
*Mar 13 04:38:21.511: has client flags 0x0
*Mar 13 04:38:21.511: ISAKMP (0:689): deleting node -1213418274 error
                      FALSE reason "quick mode done (await)"
*Mar 13 04:38:21.511: ISAKMP (0:689): Node -1213418274, Input =
                      IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Mar 13 04:38:21.511: ISAKMP (0:689): Old State = IKE_QM_R_QM2
                       New State = IKE_QM_PHASE2_COMPLETE
*Mar 13 04:38:21.511: IPSEC(key_engine): got a queue event...
*Mar 13 04:38:21.511: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 209.168.202.225, remote= 209.168.202.130,
local_proxy= 209.168.202.225/0.0.0.0/47/0 (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= 0xE012045E(3759277150), conn_id= 13777, keysize= 0, flags= 0x4
*Mar 13 04:38:21.511: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 209.168.202.225, remote= 209.168.202.130,
local_proxy= 209.168.202.225/0.0.0.0/47/0 (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= 0x53563248(1398157896), conn_id= 13778, keysize= 0, flags= 0xC
*Mar 13 04:38:21.511: IPSEC(kei_proxy): head = Tunnel0-head-0,
                      map->ivrf = , kei->ivrf =
*Mar 13 04:38:21.511: IPSEC(kei_proxy): head = Tunnel0-head-0,
                       map->ivrf = , kei->ivrf =
*Mar 13 04:38:21.511: IPSEC(add mtree): src 209.168.202.225, dest
                      209.168.202.130, dest_port 0

*Mar 13 04:38:21.511: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.168.202.225, sa_prot= 50,
sa_spi= 0xE012045E(3759277150),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 13777
*Mar 13 04:38:21.511: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.168.202.130, sa_prot= 50,
sa_spi= 0x53563248(1398157896),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 13778
*Mar 13 04:38:21.511: ISAKMP (0:689): received packet from
                      209.168.202.130 dport 500 sport 500 Global (R) QM_IDLE

*Mar 13 04:38:21.519: ISAKMP (0:689): Creating IPSec SAs
*Mar 13 04:38:21.519: inbound SA from 209.168.202.130 to 209.168.202.225 (f/i) 0/ 0
(proxy 209.168.202.130 to 209.168.202.225)
*Mar 13 04:38:21.519: has spi 0x4AFE6211 and conn_id 13779 and flags 4
*Mar 13 04:38:21.519: lifetime of 120 seconds
*Mar 13 04:38:21.519: lifetime of 4608000 kilobytes
*Mar 13 04:38:21.519: has client flags 0x0
*Mar 13 04:38:21.519: outbound SA from 209.168.202.225 to 209.168.202.130
                      (f/i) 0/ 0 (proxy 209.168.202.225 to 209.168.202.130)
*Mar 13 04:38:21.523: has spi -1567576395 and conn_id 13780 and flags C
*Mar 13 04:38:21.523: lifetime of 120 seconds
*Mar 13 04:38:21.523: lifetime of 4608000 kilobytes
*Mar 13 04:38:21.523: has client flags 0x0
*Mar 13 04:38:21.523: ISAKMP (0:689): deleting node -1392382616 error
                      FALSE reason "quick mode done (await)"
*Mar 13 04:38:21.523: ISAKMP (0:689): Node -1392382616, Input = IKE_MESG_FROM_PEER,
                      IKE_QM_EXCH
*Mar 13 04:38:21.523: ISAKMP (0:689): Old State = IKE_QM_R_QM2 New State =
                      IKE_QM_PHASE2_COMPLETE
*Mar 13 04:38:21.523: IPSEC(key_engine): got a queue event...
*Mar 13 04:38:21.523: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 209.168.202.225, remote= 209.168.202.130,
local_proxy= 209.168.202.225/0.0.0.0/47/0 (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= 0x4AFE6211(1258185233), conn_id= 13779, keysize= 0, flags= 0x4
*Mar 13 04:38:21.523: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 209.168.202.225, remote= 209.168.202.130,
local_proxy= 209.168.202.225/0.0.0.0/47/0 (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= 0xA290AEB5(2727390901), conn_id= 13780, keysize= 0, flags= 0xC
*Mar 13 04:38:21.523: IPSEC(kei_proxy): head = Tunnel0-head-0,
                       map->ivrf = , kei->ivrf =
*Mar 13 04:38:21.523: IPSEC(kei_proxy): head = Tunnel0-head-0,
                      map->ivrf = , kei->ivrf =
*Mar 13 04:38:21.523: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.168.202.225, sa_prot= 50,
sa_spi= 0x4AFE6211(1258185233),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 13779
```

```
*Mar 13 04:38:21.523: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.168.202.130, sa_prot= 50,
sa_spi= 0xA290AEB5(2727390901),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 13780
*Mar 13 04:38:21.571: ISAKMP (0:687): purging node -114623302
*Mar 13 04:38:24.339: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 90: Neighbor
                       192.168.1.3 (Tunnel0) is up: new adjacency
```

トラブルシュート

その他のトラブルシューティング情報については、『IP Security のトラブルシューティング - debug コマンドの理解と使用』を参照してください。

関連情報

- **DMVPN と Cisco IOS ソフトウェアの概要**
- **IPSec ネゴシエーション/IKE プロトコル**
- **テクニカル サポートとドキュメント – Cisco Systems**