

عم ل هس VPN م داخو DMVPN م داخ ني وكت ت اف ي صوت ISAKMP

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [التكوينات](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يصف هذا وثيقة كيف أن يشكل DMVPN (Dynamic Multipoint VPN) و Easy VPN مع Xauth على ال نفسه مسحاج تخديد. يستخدم هذا الإعداد الإعداد لمعالجة جهات DMVPN بشكل ديناميكي. توفر توصيفات بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP) إمكانية فصل طرق المصادقة الخاصة بخادمت DMVPN التي يتم معالجتها بشكل ديناميكي أو عملاء شبكات VPN السهلة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- موجهات Cisco 2691 و Cisco 3725 التي تشغل برنامج Cisco IOS® Software، الإصدار 12.3(3) و 12.3(3)a
- تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

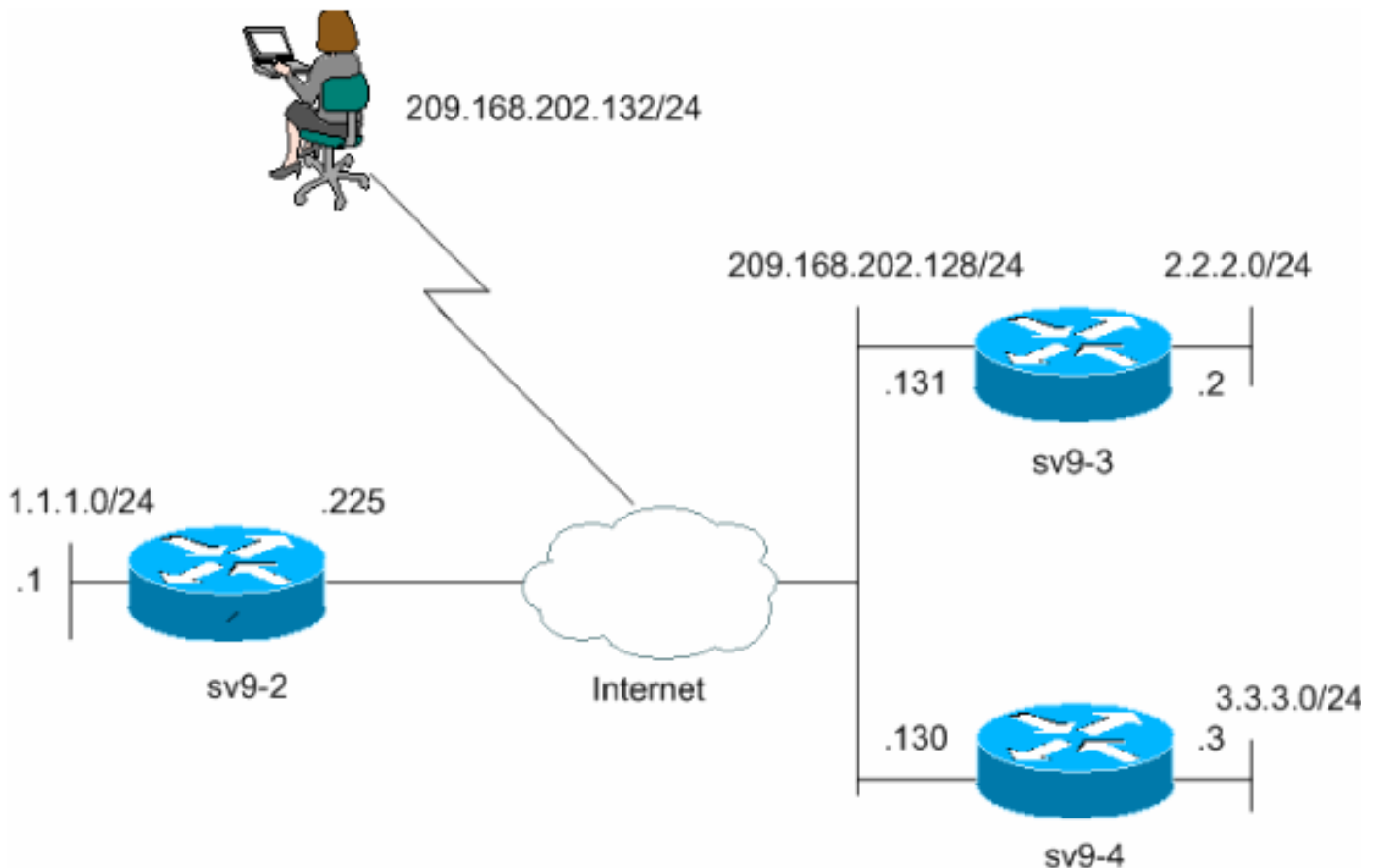
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم [أداة بحث الأوامر](#) (للعلماء [المسجلين](#) فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي.



التكوينات

يستخدم هذا المستند هذه التكوينات.

- [تكوين موزع SV9-2](#)
- [تكوين التحدث عبر SV9-3](#)
- [التكوين الذي تم التحدث به عبر بروتوكول SV9-4](#)

تكوين موزع SV9-2

```
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 dmvpnsokes
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

```

تكوين التحدث عبر SV9-3

```

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 ---!

```



```

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

```

التكوين الذي تم التحدث به عبر بروتوكول SV9-4

```

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

```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك استخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

تؤكد أوامر تصحيح الأخطاء التي يتم تشغيلها على موجه الموزع مطابقة المعلمات الصحيحة لاتصالات عميل VPN و TALK. قم بتشغيل أوامر تصحيح الأخطاء هذه.

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر **show**.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل استخدام أوامر **debug**.

- **debug crypto isakmp**—يعرض الرسائل المتعلقة بأحداث IKE.
- **debug crypto ipSec**—يعرض معلومات حول أحداث IPsec.

```

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_MSG_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*
mismatch 157
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_MSG_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_MSG_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*
sport 500 Global (R) MM_SA_SETUP 500
Mar 13 04:38:21.203: ISAKMP (0:689): Input = IKE_MSG_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_MSG_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_MSG_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_MSG_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
      remote 209.168.202.225
      remote port 500 209.168.202.130
      ...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_MSG_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_MSG_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_MSG_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*
dport 500 sport 500 Global (R) QM_IDLE 209.168.202.130

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_MSG_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*
dport 500 sport 500 Global (R) QM_IDLE 209.168.202.130

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*
my_port 500 peer_port 500 (R) QM_IDLE 209.168.202.130
= 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*
    f/i) 0/ 0) 209.168.202.225
(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*
f/i) 0/ 0 (proxy 209.168.202.225) 209.168.202.130
    (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 mtrees): src 209.168.202.225, dest*
    dest_port 0 ,209.168.202.130

,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*
dport 500 sport 500 Global (R) QM_IDLE 209.168.202.130

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_MSG_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*
```

Tunnel0) is up: new adjacency) 192.168.1.3

استكشاف الأخطاء وإصلاحها

راجع استكشاف أخطاء أمان IP وإصلاحها - فهم أوامر debug واستخدامها للحصول على معلومات إضافية حول استكشاف الأخطاء وإصلاحها.

معلومات ذات صلة

- نظرة عامة على برنامج DMVPN و Cisco IOS
- مفاوضة IPsec/بروتوكولات IKE
- الدعم التقني والمستندات - Cisco Systems

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلأل يزيلچنلإ دن تسمل