تكوين نظير شبكة LAN إلى شبكة LAN إلى شبكة VPN عالمع وIPsec لموجه ديناميكية الديناميكية

المحتويات

المقدمة

يوضح هذا التكوين تكوين شبكة LAN إلى شبكة LAN بين موجهين في بيئة محكية. يتصل عملاء Cisco VPN أيضا بالموجه ويستخدمون المصادقة الموسعة (Xauth).

يحصل الموجه الذي يتحدث في هذا السيناريو على عنوان IP الخاص به بشكل ديناميكي عبر DHCP. يشيع إستخدام بروتوكول التكوين الديناميكي للمضيف (DHCP) في الحالات التي يكون فيها المحادثة متصلة بالإنترنت عبر DSL أو مودم كبل. وذلك لأن مزود خدمة الإنترنت (ISP) غالبا ما يوفر عناوين IP بشكل ديناميكي باستخدام DHCP على هذه الاتصالات منخفضة التكلفة.

بدون تكوين إضافي، لا يمكن إستخدام مفتاح بطاقة برية مشترك مسبقا على موجه الموزع في هذه الحالة. وذلك نظرا لأن Xauth لاتصالات عميل شبكة VPN تقوم بقطع اتصال شبكة LAN إلى شبكة LAN. مهما، عندما يعجز أنت Xauth، هو يقلل القدرة أن يصدق VPN زبون.

يجعل إدخال ملفات تعريف ISAKMP في الإصدار T(15)12.2 من برنامج Cisco IOS® هذا التكوين ممكنا حيث يمكنك المطابقة على خصائص أخرى للاتصال (مجموعة عميل VPN، عنوان IP للنظير، اسم المجال المؤهل بالكامل [FQDN]، وما إلى ذلك) بدلا من عنوان IP للنظير فقط. ملفات تعريف ISAKMP هي موضوع هذا التكوين.

ملاحظة: يمكنك أيضا إستخدام الكلمة الأساسية **no-xauth** مع الأمر **crypto isakmp key** **لتجاوز Xauth نظائر شبكة LAN إلى شبكة LAN.** ارجع إلى القدرة على تعطيل مصادقة (Xauth) نظائر IPsec الثابتة وتكوين IPsec بين موجهين وعميل Cisco VPN 4.x للحصول على مزيد من المعلومات.

يمكن نسخ تكوين الموجه الذي يتحدث عنه في هذا المستند نسخا متماثلا على جميع الموجهات الأخرى التي تتصل

بنفس الصرة. يكمن الاختلاف الوحيد بين الفروع في قائمة الوصول التي تشير إلى حركة المرور التي سيتم تشفيرها.

ارجع إلى عميل EzVPN والخادم على مثال تكوين الموجه نفسه لمعرفة المزيد حول السيناريو الذي يمكنك فيه تكوين موجه كعميل EzVPN والخادم على الواجهة نفسها.

ارجع إلى أنفاق شبكة LAN-to-LAN على مركز VPN 3000 باستخدام جدار حماية PIX مكون من أجل DHCP لتكوين سلسلة مركز Cisco VPN 3000 لإنشاء أنفاق IPsec بشكل ديناميكي باستخدام جدران حماية Cisco PIX البعيدة التي تستخدم DHCP للحصول على عناوين IP على واجهات IP الخاصة بها.

ارجع إلى نفق IPsec LAN-to-LAN على مركز VPN 3000 باستخدام موجه Cisco IOS تم تكوينه لمثال تكوين DHCP لتكوين سلسلة مركز VPN 3000 من أجل إنشاء أنفاق IPsec بشكل ديناميكي باستخدام أجهزة VPN البعيدة التي تتلقى عناوين IP الديناميكية على الواجهات العامة الخاصة بها.

ارجع إلى IPsec بين موجه IOS ثابت وموجه PIX/ASA 7.x ديناميكي مع مثال تكوين NAT لتمكين جهاز أمان PIX/ASA من قبول إتصالات IPsec الديناميكية من موجه IOS®.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تم تقديم ملفات تعريف IPsec في البرنامج Cisco IOS Software، الإصدار 12.2T(15). بسبب معرف تصحيح الأخطاء من Cisco CSCea77140 (العملاء المسجلون فقط) تحتاج إلى تشغيل برنامج Cisco IOS الإصدار 12.3(3) أو إصدار أحدث، أو برنامج Cisco IOS الإصدار 12.3T(2) أو إصدار أحدث من أجل أن يعمل هذا التكوين بنجاح. تم إختبار هذه التكوينات باستخدام إصدارات البرامج التالية:

- برنامج IOS الإصدار 12.3(6a) من Cisco على موجه الموزع
- برنامج IOS الإصدار 12.2(23a) من Cisco على الموجه المتصل (يمكن أن يكون هذا أي إصدار تشفير)
- Cisco VPN Client، الإصدار 4.0(4) على Windows 2000

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة 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.

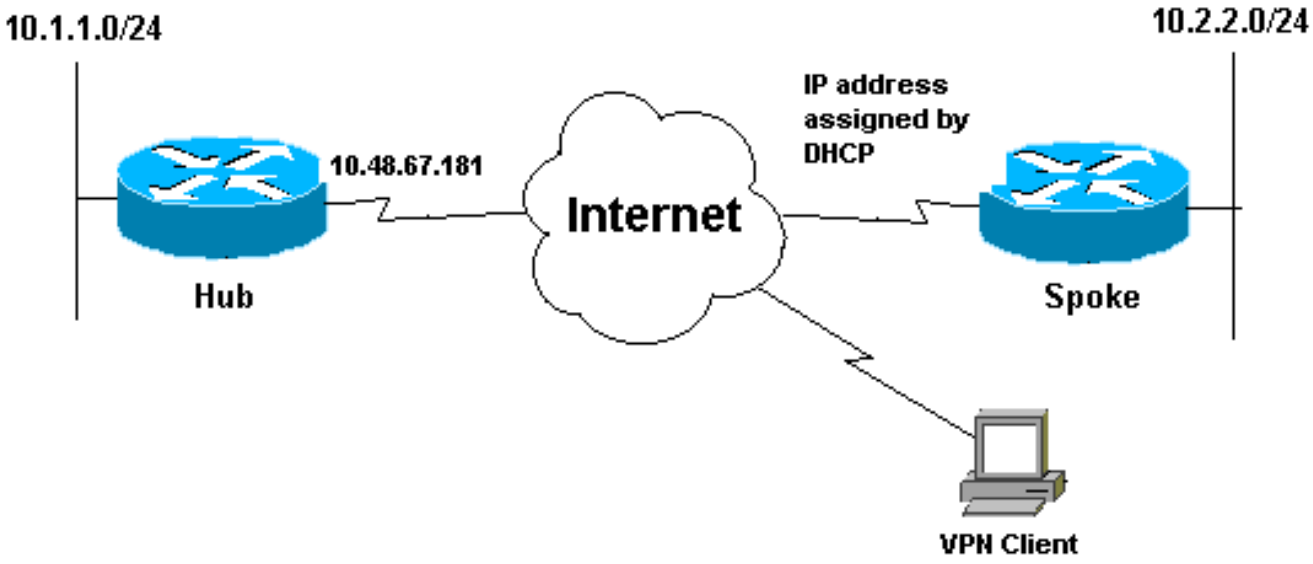
التكوين

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

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي.



التكوينات

يستخدم هذا المستند إعداد الشبكة التالي:

- تكوين الموزع
- التكوين الذي تم التحدث به

تكوين الموزع

```
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
```

التكوين الذي تم التحدث به

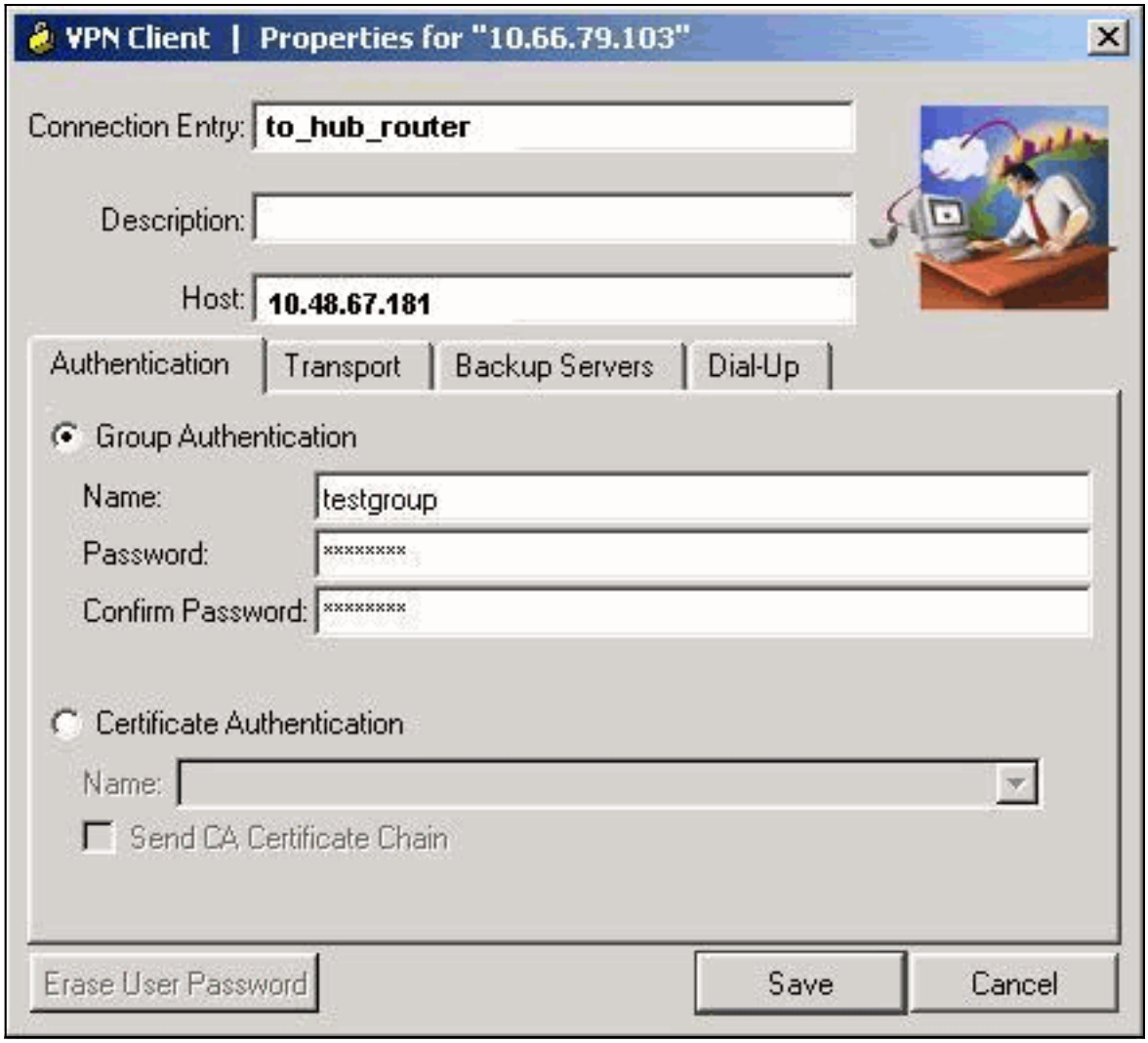
```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spoke
!
no logging on
!
ip subnet-zero
no ip domain lookup
!
ip cef
!
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco123 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
```

عميل شبكة VPN

قم بإنشاء إدخال اتصال جديد يشير إلى عنوان IP الخاص بموجه الموزع. اسم المجموعة في هذا المثال هو "testgroup" وكلمة المرور هي "cisco321". ويمكن ملاحظة ذلك في تكوين موجه الموزع.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

يمكن أن تؤكد أوامر تصحيح الأخطاء التي يتم تشغيلها على موجه الموزع تطابق المعلمات الصحيحة لاتصالات عميل VPN و TALK.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

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

- **show ip interface**— يعرض تعيين عنوان IP إلى الموجه الموجه الذي يتحدث.
- **show crypto isakmp sa detail**— يعرض شبكات IKE SAs، التي تم إعدادها بين أجهزة بدء IPsec. على سبيل المثال، الموجه الذي يتم التحدث به وعميل شبكة VPN، وموجه الموزع.
- **show crypto ipSec sa**— يعرض شبكات IPsec SAs، التي تم إعدادها بين أجهزة بدء IPsec. على سبيل المثال، الموجه الذي يتم التحدث به وعميل شبكة VPN، وموجه الموزع.
- **debug crypto isakmp**—يعرض رسائل حول أحداث IKE (Internet Key Exchange).
- **debug crypto ipSec**—يعرض أحداث IPsec.
- **debug crypto engine**—يعرض أحداث محرك التشفير.

هذا هو المخرج من الأمر **show ip interface f0/0**.

```
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
```

هذا هو مخرج الأمر **show crypto isakmp sa detail**.

```
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

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

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

هذا هو مخرج الأمر **show crypto ipSec sa**.

```
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
```

تم تجميع إخراج تصحيح الأخطاء هذا على موجه الموزع، عندما يقوم الموجه الموجه الموجه الذي تم التحدث به بتهيئة IKE و IPsec SAs.

```
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
                                        R) MM_SA_SETUP) 500
            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**
for prot 3 10.100.2.102
(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
```

تم تجميع إخراج تصحيح الأخطاء هذا على موجه الموزع، عندما يقوم عميل VPN بتهيئة IKE و IPsec SAs.

```
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
remote port 500 10.51.82.100
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
R) CONF_XAUTH) 500
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
```

التحقق من الأرقام التسلسلية لمخطط التشفير

إذا تم تكوين النظراء الثابته والحركي على خريطة التشفير نفسها، فإن ترتيب إدخالات خريطة التشفير مهم للغاية. **يجب أن يكون** الرقم التسلسلي لإدخال خريطة التشفير الديناميكية أعلى من جميع إدخالات خريطة التشفير الثابتة الأخرى. إذا كانت المدخلات الثابتة مرقمة أعلى من المدخل الديناميكي، فإن الاتصالات مع تلك الأقران تفشل.

هنا مثال على خريطة تشفير مرقمة بشكل صحيح تحتوي على مدخل ثابت ومدخل ديناميكي. لاحظ أن الإدخال الديناميكي يحتوي على أعلى رقم تسلسلي وأنه قد تم ترك الغرفة لإضافة إدخالات ثابتة إضافية:

```
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
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- تكوين ملف تعريف IPsec
- برنامج IOS الإصدار T(15)12.2 من Cisco الميزات الجديدة
- مفاوضة IPsec/صفحة دعم بروتوكول IKE
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).