تكوين عميل Cisco VPN 3.x ل Windows إلى IOS باستخدام المصادقة الموسعة المحلية

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين اتصال بين موجه باستخدام المصادقة الموسعة المحلية وعميل Cisco VPN. برنامج IOS® الإصدارات 12.2(15)T2 من Cisco واتصالات الدعم الأكبر من عميل Cisco VPN 3.x. يستخدم عميل شبكة VPN 3.x سياسة Diffie Hellman (DH) المجموعة 2. يتيح الأمر **isakmp policy # group 2** لعملاء x.3 إمكانية الاتصال.

للحصول على معلومات حول تكوين هذه الأجهزة باستخدام عميل Cisco Secure VPN 1.1، راجع تكوين عميل VPN الآمن من Cisco 1.1 ل Windows to IOS باستخدام المصادقة الموسعة المحلية.

ارجع إلى نفق IPsec بين موجه IOS وزبون Cisco VPN 4.x ل Windows مع مثال تكوين مصادقة المستخدم TACACS+ لمعرفة المزيد حول السيناريو الذي تحدث فيه مصادقة المستخدم خارجيا مع بروتوكول TACACS+.

ارجع إلى تكوين IPSec بين موجه Cisco IOS وعميل Cisco VPN 4.x ل Windows الذي يستخدم RADIUS لمصادقة المستخدم لمعرفة المزيد حول السيناريو الذي تحدث فيه مصادقة المستخدم خارجيا مع بروتوكول RADIUS.

قبل البدء

الاصطلاحات

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

المتطلبات الأساسية

قبل محاولة هذا التكوين، يرجى التأكد من استيفاء المتطلبات الأساسية التالية:

- مجموعة من العناوين التي سيتم تعيينها لأمان IPSec) IP)
- مستخدم محلي على موجه IOS مع **Cisco** كاسم و **cisco** ككلمة المرور
- مجموعة تسمى **3000 عميل** بكلمة مرور **Cisco123**

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية أدناه.

- موجه طراز 3640 يشغل الإصدار 12.2(15)T2
- عميل Cisco VPN ل Windows الإصدار 3.5 (يجب أن يعمل أي عميل VPN الإصدار x.3)

يتم عرض الإخراج من الأمر **show version** على الموجه أدناه.

```
3640#show version
Cisco Internetwork Operating System Software
,IOS (tm) 3600 Software (C3640-JK9O3S-M), Version 12.2(15)T2
(RELEASE SOFTWARE (fc2
TAC Support: http://www.cisco.com/tac
.Copyright (c) 1986-2003 by cisco Systems, Inc
Compiled Wed 30-Apr-03 05:42 by nmasa
Image text-base: 0x60008950, data-base: 0x6202E000

,ROM: System Bootstrap, Version 11.1(20)AA2
(EARLY DEPLOYMENT RELEASE SOFTWARE (fc1

uptime is 21 hours, 29 minutes 3640
System returned to ROM by reload
"System image file is "flash:c3640-jk9o3s-mz.122-15.T2.bin


This product contains cryptographic features and is
subject to United States and local country laws governing
import, export, transfer and use. Delivery of Cisco cryptographic
,products does not imply third-party authority to import, export
distribute or use encryption. Importers, exporters, distributors
and users are responsible for compliance with U.S. and local
country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply
.with U.S. and local laws, return this product immediately

A summary of U.S. laws governing
:Cisco cryptographic products may be found at
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us
.by sending email to export@cisco.com

(cisco 3640 (R4700) processor (revision 0x00
.with 126976K/4096K bytes of memory
Processor board ID 22789386
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
.Bridging software
.X.25 software, Version 3.0.0
.(SuperLAT software (copyright 1990 by Meridian Technology Corp
.TN3270 Emulation software
(Ethernet/IEEE 802.3 interface(s 2
(Serial network interface(s 4
.DRAM configuration is 64 bits wide with parity disabled
.125K bytes of non-volatile configuration memory
(32768K bytes of processor board System flash (Read/Write
(16384K bytes of processor board PCMCIA Slot0 flash (Read/Write

Configuration register is 0x102

3640#
```

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

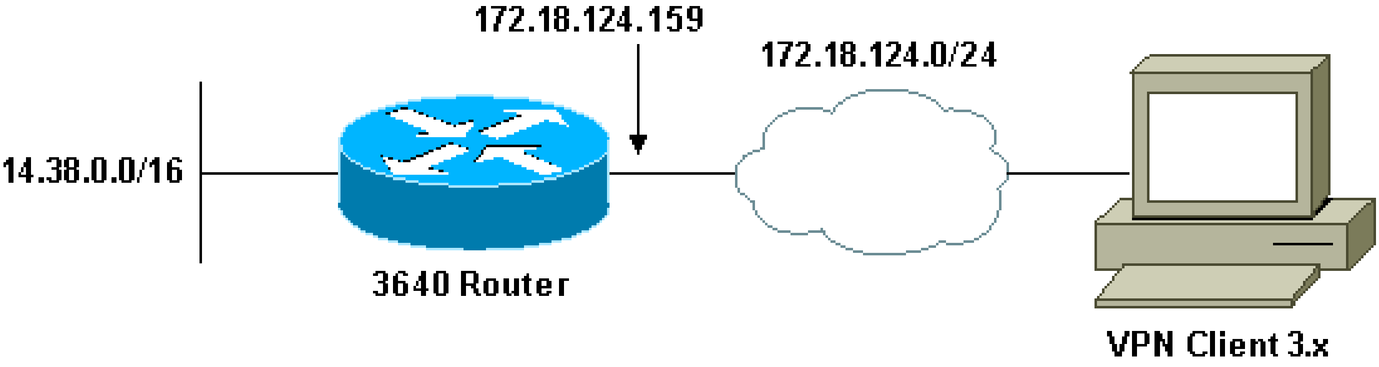
التكوين

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

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في الرسم التخطيطي أدناه.



التكوينات

يستخدم هذا المستند التكوينات الموضحة أدناه.

- تكوين الموجه 3640
- تكوين عميل VPN 3.x

تكوين الموجه 3640

الموجه 3640
3640#**show run** ...Building configuration Current configuration : 1884 bytes

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3640
!
Enable Authentication, Authorizing and Accounting ---!
(AAA) !--- for user authentication and group
authorization. aaa new-model
!
To enable X-Auth for user authentication, !--- ---!
.enable the aaa authentication commands

aaa authentication login userauthen local

To enable group authorization, !--- enable the aaa ---!
.authorization commands

aaa authorization network groupauthor local
!
For local authentication of the IPSec user, !--- ---!
create the user with password. username cisco password 0
cisco
!
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
Create an Internet Security Association and !--- ---!
Key Management Protocol (ISAKMP) policy for Phase 1
negotiations. crypto isakmp policy 3
encr 3des
authentication pre-share
group 2
!
Create a group that will be used to specify the !-- ---!
- Windows Internet Naming Service (WINS) and !--- Domain
Naming Service (DNS) server addresses to the client, !--
- along with the pre-shared key for authentication.
crypto isakmp client configuration group 3000client
key cisco123
dns 14.1.1.10
wins 14.1.1.20
domain cisco.com
pool ippool
!
Create the Phase 2 Policy for actual data ---!
encryption. crypto ipsec transform-set myset esp-3des
esp-sha-hmac
!
Create a dynamic map and !--- apply the transform ---!
set that was created above. crypto dynamic-map dynmap 10
set transform-set myset
!
Create the actual crypto map, !--- and apply the ---!
aaa lists that were created earlier. crypto map
clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor
```

```
crypto map clientmap client configuration address
respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
!
Apply the crypto map on the outside interface. ---!
interface Ethernet0/0 ip address 172.18.124.159
255.255.255.0
half-duplex
crypto map clientmap
!
interface Serial0/0
no ip address
shutdown
!
interface Ethernet0/1
ip address 14.38.100.201 255.255.0.0
no keepalive
half-duplex
!
interface Serial1/0
no ip address
shutdown
!
interface Serial1/1
no ip address
shutdown
!
interface Serial1/2
no ip address
shutdown
!
interface Serial1/3
no ip address
shutdown
!
interface Serial1/4
no ip address
shutdown
!
interface Serial1/5
no ip address
shutdown
!
interface Serial1/6
no ip address
shutdown
!
interface Serial1/7
no ip address
shutdown
!
Create a pool of addresses to be assigned to the ---!
VPN Clients. ip local pool ippool 14.1.1.100 14.1.1.200
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
ip http server
ip pim bidir-enable
!
```

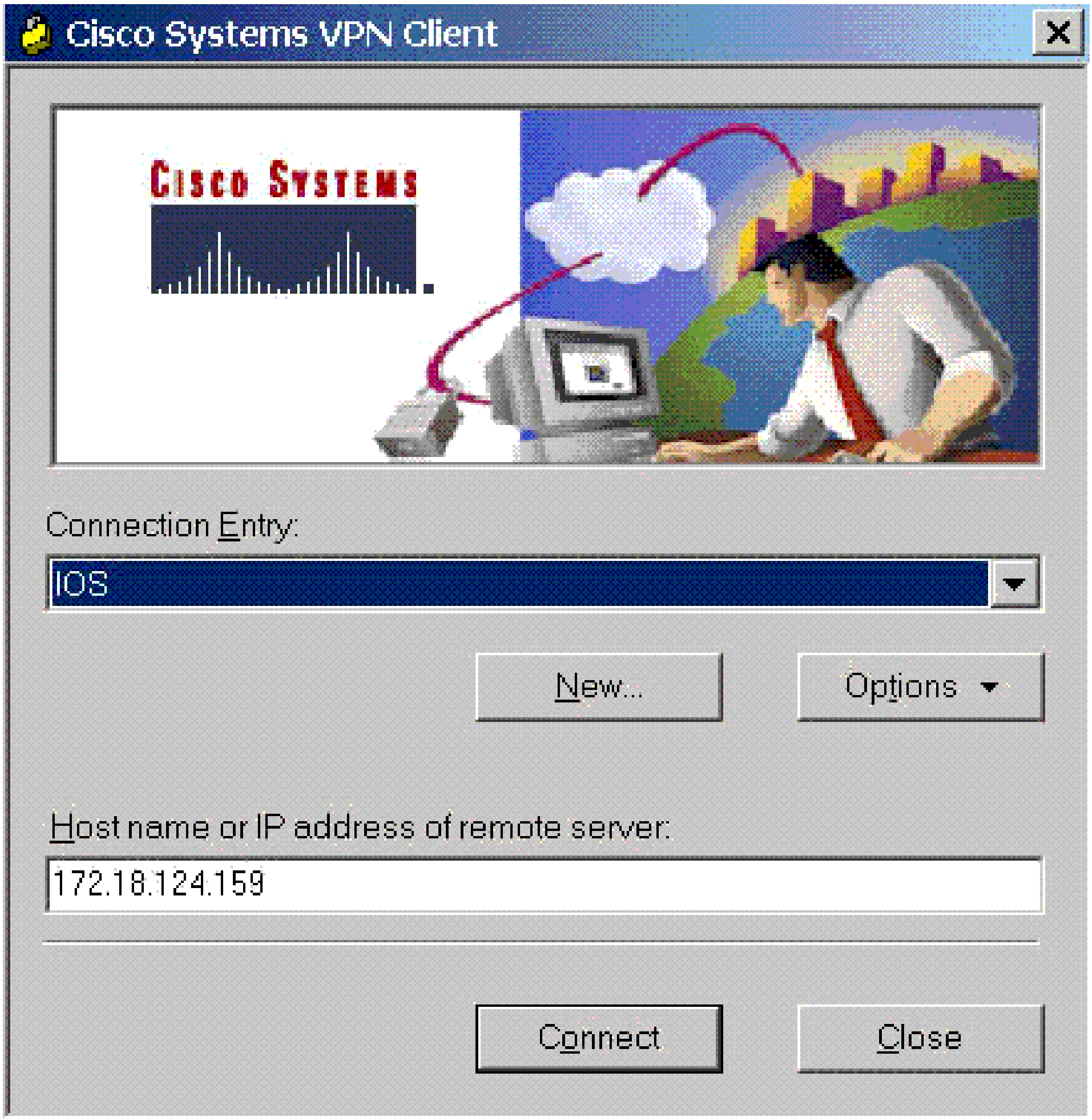
```
!
!
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
!
end

3640#
```

تكوين عميل VPN 3.x

يوضح هذا القسم كيفية تكوين عميل VPN 3.x.

1. أطلقت ال VPN زبون، بعد ذلك طقطقت **جديد** أن يخلق توصيل

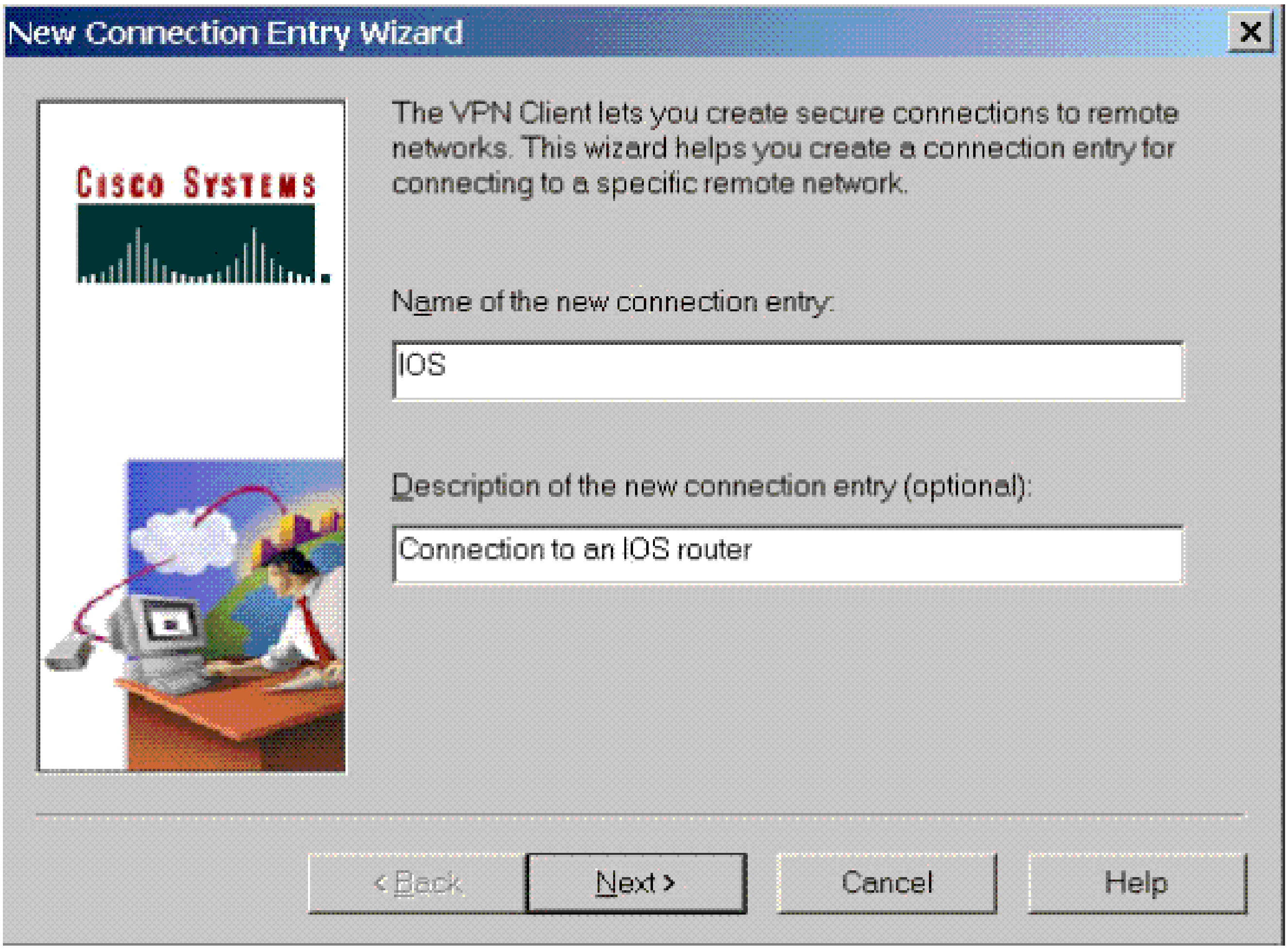


Connection Entry: IOS

Host name or IP address of remote server: 172.18.124.159

جديد.

2. عند مطالبتك، قم بتعيين اسم لإدخالك. يمكنك أيضا إدخال وصف إذا كنت تريد. انقر فوق **التالي** عند الانتهاء.



New Connection Entry Wizard

The VPN Client lets you create secure connections to remote networks. This wizard helps you create a connection entry for connecting to a specific remote network.

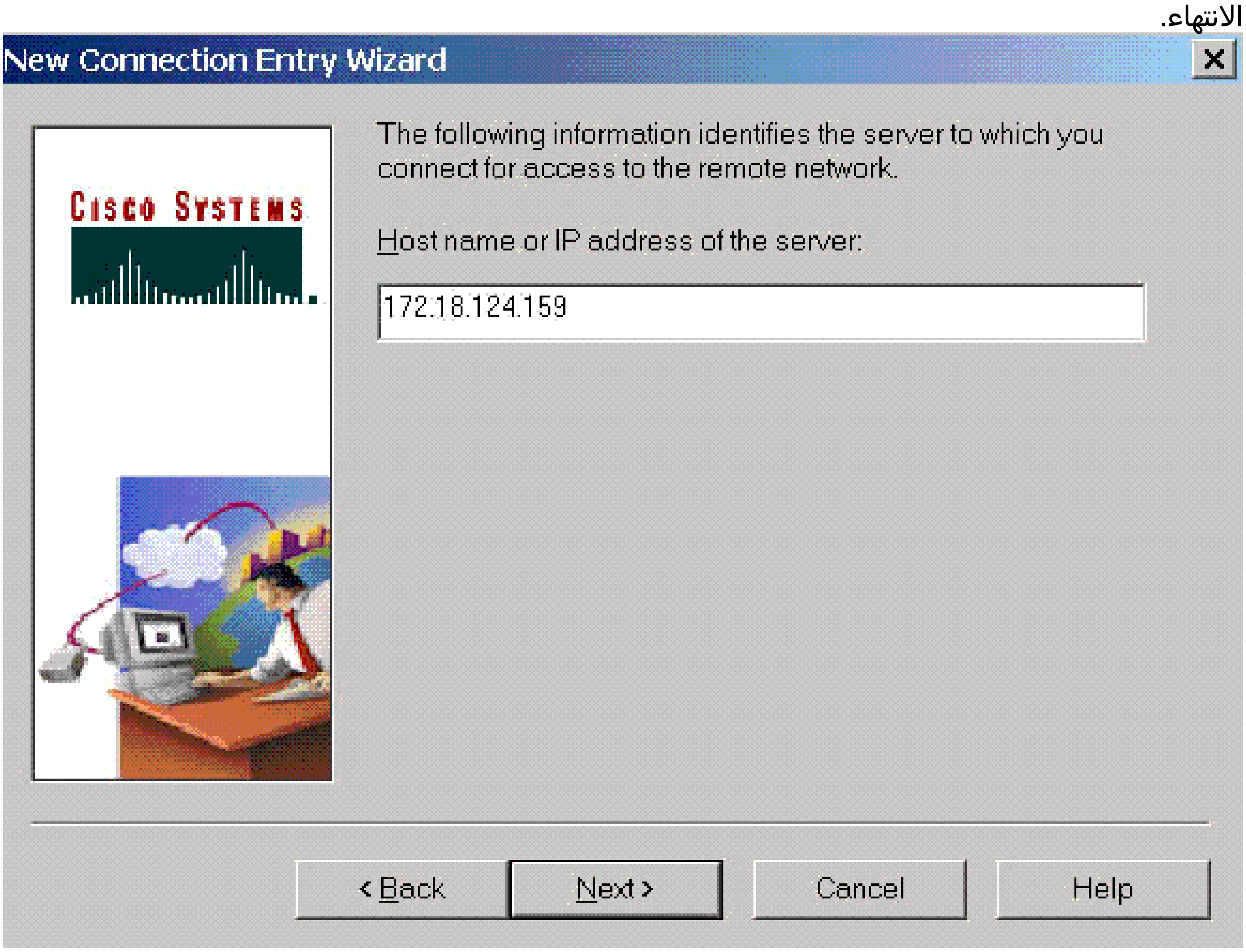
Name of the new connection entry:

IOS

Description of the new connection entry (optional):

Connection to an IOS router

3. أدخل عنوان IP الخاص بالواجهة العامة للموجه. انقر فوق **التالي** عند الانتهاء.



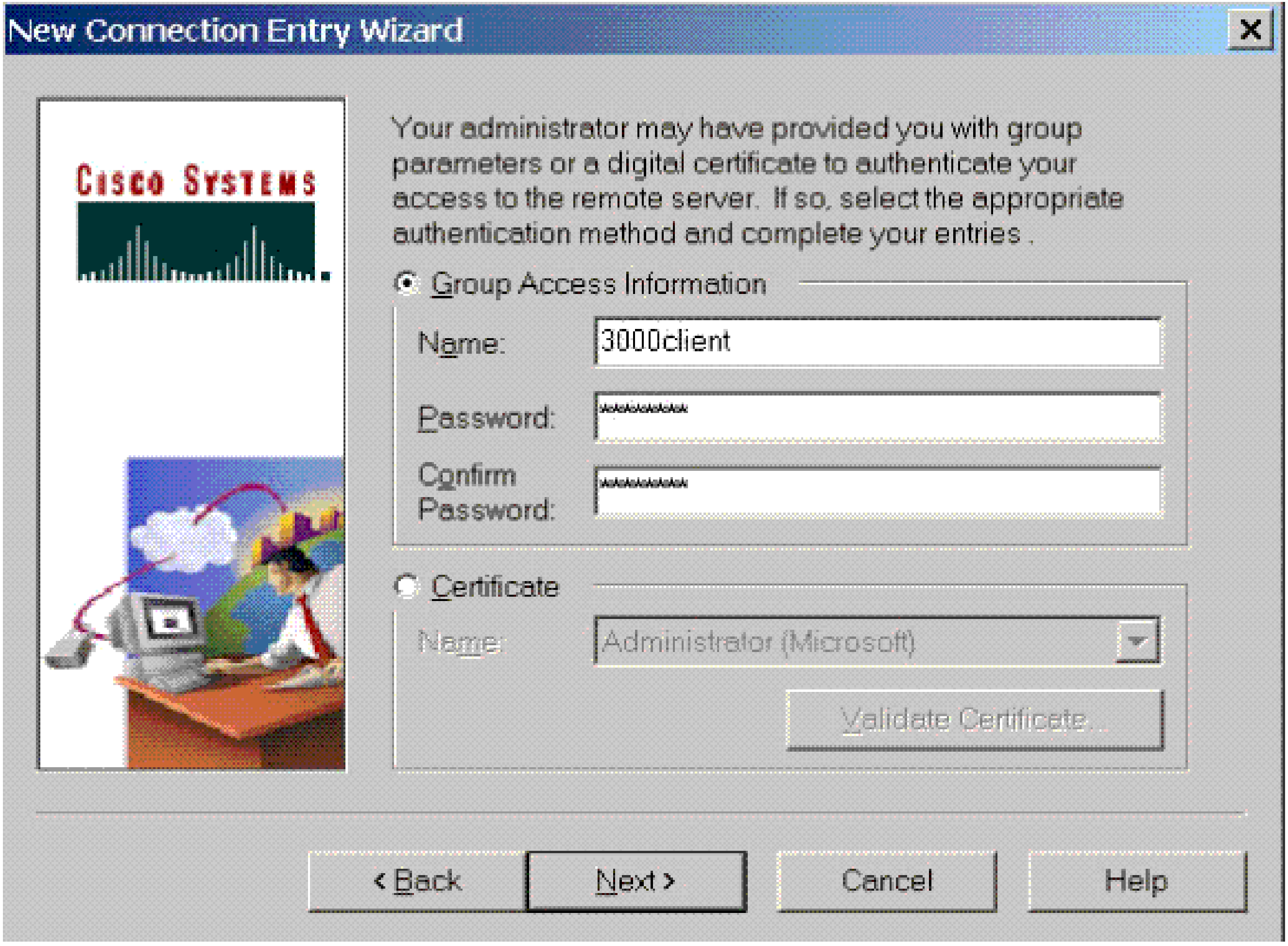
New Connection Entry Wizard

The following information identifies the server to which you connect for access to the remote network.

Host name or IP address of the server:

172.18.124.159

4. تحت **معلومات الوصول إلى المجموعة**، أدخل اسم المجموعة وكلمة المرور. يوضح المثال التالي مجموعة
بالاسم "3000 عميل" وكلمة المرور "Cisco123". قم بتأكيد كلمة المرور، ثم انقر فوق **التالي**
للمتابعة.



New Connection Entry Wizard

Your administrator may have provided you with group parameters or a digital certificate to authenticate your access to the remote server. If so, select the appropriate authentication method and complete your entries .

● Group Access Information

Name: 3000client

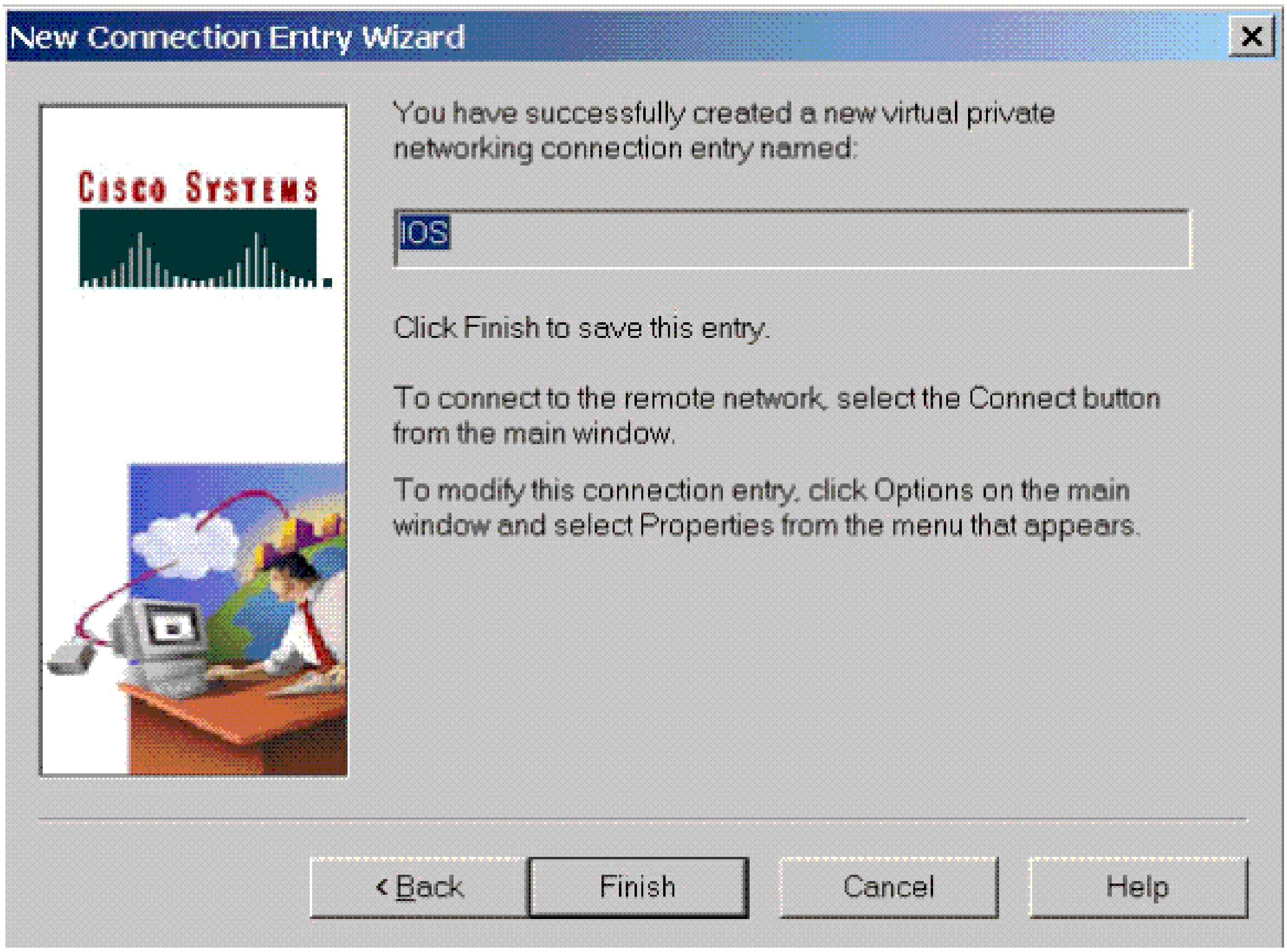
Password: **********

Confirm Password: **********

○ Certificate

Name: Administrator (Microsoft)

5. انقر على **إنهاء** لحفظ ملف التعريف في
السجل.



New Connection Entry Wizard

You have successfully created a new virtual private networking connection entry named:

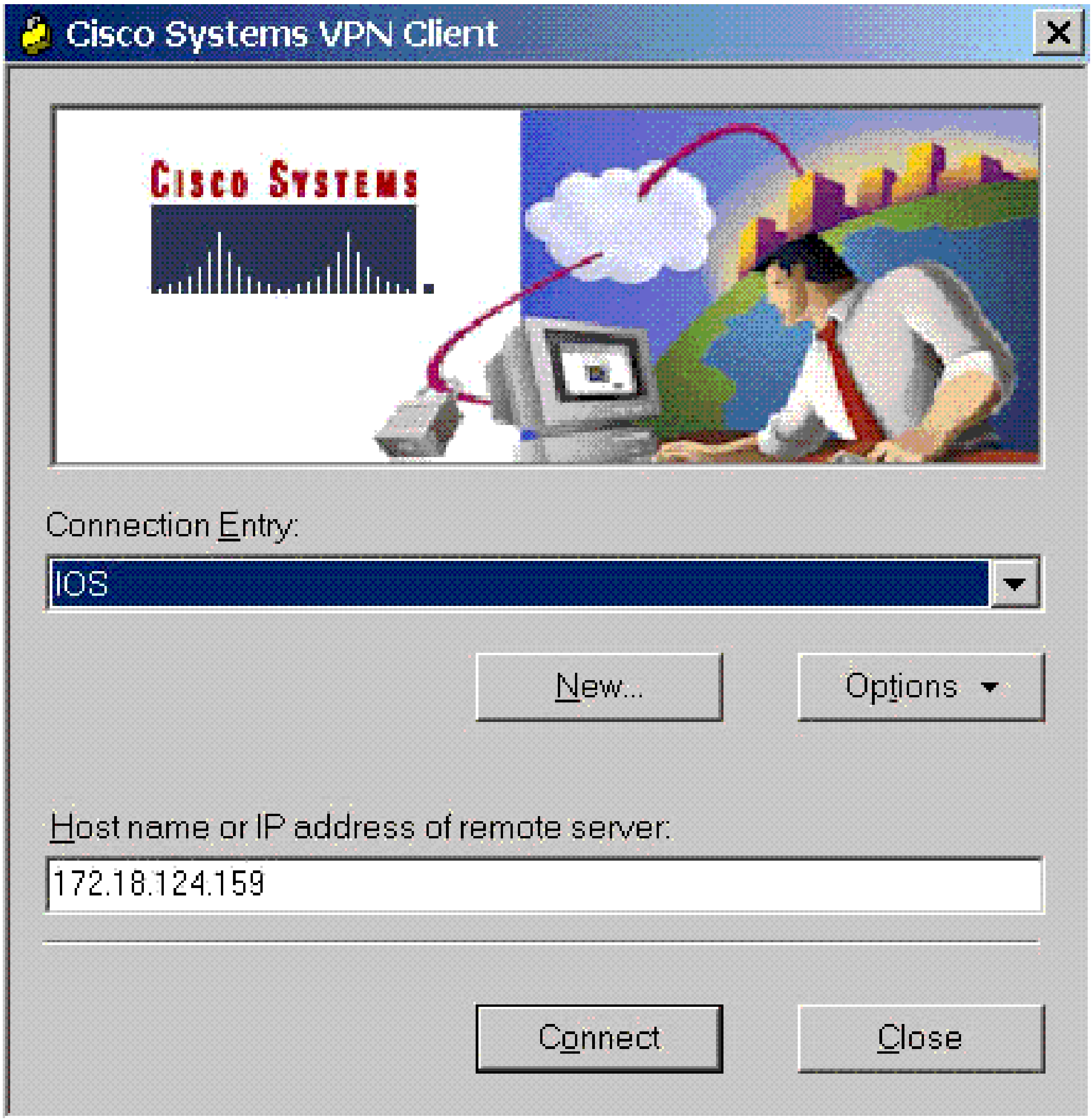
IOS

Click Finish to save this entry.

To connect to the remote network, select the Connect button from the main window.

To modify this connection entry, click Options on the main window and select Properties from the menu that appears.

6. انقر على **توصيل** للاتصال بالموجه. سيعرض الإطار رسائل تقرأ "التفاوض على ملفات تعريف الأمان" و"الارتباط الخاص بك آمن



Connection Entry: IOS

Host name or IP address of remote server: 172.18.124.159

الآن."

تمكين الاتصال النفقي للتقسيم

لتمكين الاتصال النفقي المنقسم لاتصالات VPN، تأكد من وجود قائمة وصول مكونة على الموجه. في المثال أدناه، يتم إقران الأمر **access-list 108** بالمجموعة لأغراض إنشاء قنوات اتصال عبر الاتصال النفقي، ويتم تكوين النفق لشبكة 16.14.38 /x.x. تتدفق حركة المرور غير مشفرة إلى الأجهزة غير الموجودة في قائمة الوصول 108 (على سبيل المثال، الإنترنت).

```
access-list 108 permit ip 14.38.0.0 0.0.255.255
   0.0.0.255 14.1.1.0
```

ثم قم بتطبيق قائمة الوصول على خصائص المجموعة.

```
crypto isakmp client configuration group 3000client
 key cisco123
 dns 14.38.100.10
 wins 14.38.100.20
 domain cisco.com
 pool ippool
```

```
                                                  acl 108
```

التحقق من الصحة

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

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

```
                               3640#show crypto isakmp sa
dst             src             state     conn-id    slot
QM_IDLE         3       0   172.18.124.96  172.18.124.159

                                3640#show crypto ipsec sa
                                   interface: Ethernet0/0
     Crypto map tag: clientmap, local addr. 172.18.124.96

                                           :protected vrf
 (local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
                      :(remote ident (addr/mask/prot/port
                      (14.1.1.106/255.255.255.255/0/0)   
                         current_peer: 172.18.124.159:500
                                         {}=PERMIT, flags
        pkts encaps: 6, #pkts encrypt: 6, #pkts digest 6#
        pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6#
               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.: 172.18.124.96
                  remote crypto endpt.: 172.18.124.159   
                            path mtu 1500, media mtu 1500
                           current outbound spi: D026E0BA

                                         :inbound esp sas
                              (spi: 0x84E901C8(2229862856
                       , transform: esp-3des esp-md5-hmac
                              { ,in use settings ={Tunnel
slot: 0, conn id: 2002, flow_id: 3, crypto map: clientmap
(sa timing: remaining key lifetime (k/sec): (4450694/3532
                                         IV size: 8 bytes
                              replay detection support: Y

                                          :inbound ah sas

                                         :inbound pcp sas

                                        :outbound esp sas
                              (spi: 0xD026E0BA(3492208826
                       , transform: esp-3des esp-md5-hmac
                              { ,in use settings ={Tunnel
slot: 0, conn id: 2003, flow_id: 4, crypto map: clientmap
(sa timing: remaining key lifetime (k/sec): (4450699/3532
                                         IV size: 8 bytes
                              replay detection support: Y

                                         :outbound ah sas
```

```
:outbound pcp sas

:protected vrf
:(local ident (addr/mask/prot/port
(172.18.124.159/255.255.255.255/0/0)
:(remote ident (addr/mask/prot/port
(14.1.1.105/255.255.255.255/0/0)
current_peer: 172.18.124.159:500
{}=PERMIT, flags
pkts encaps: 6, #pkts encrypt: 6, #pkts digest 6#
pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6#
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.: 172.18.124.159
remote crypto endpt.: 172.18.124.96
path mtu 1500, media mtu 1500
current outbound spi: E8E398F8

:inbound esp sas
(spi: 0xDFE24DFC(3756150268
, transform: esp-3des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 2000, flow_id: 1, crypto map: clientmap
(sa timing: remaining key lifetime (k/sec): (4572253/3530
IV size: 8 bytes
replay detection support: Y

:inbound ah sas

:inbound pcp sas

:outbound esp sas
(spi: 0xE8E398F8(3907229944
, transform: esp-3des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 2001, flow_id: 2, crypto map: clientmap
(sa timing: remaining key lifetime (k/sec): (4572253/3528
IV size: 8 bytes
replay detection support: Y

:outbound ah sas

:outbound pcp sas
```

```
3640#show crypto engine connections active

ID Interface     IP-Address      State  Algorithm          Encrypt Decrypt
Ethernet0/0  172.18.124.159  set    HMAC_MD5+3DES_56_C      0       0 3
Ethernet0/0  172.18.124.159  set    HMAC_MD5+3DES_56_C      0       6 2000
Ethernet0/0  172.18.124.159  set    HMAC_MD5+3DES_56_C      6       0 2001
Ethernet0/0  172.18.124.159  set    HMAC_MD5+3DES_56_C      0       6 2004
Ethernet0/0  172.18.124.159  set    HMAC_MD5+3DES_56_C      6       0 2005
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

```
3640#debug crypto ipsec
```

```
Crypto IPSEC debugging is on
3640#debug crypto isakmp
Crypto ISAKMP debugging is on
3640#

ISAKMP (0:0): received packet from 172.18.124.96
   dport 500 sport 500 Global (N) NEW SA
ISAKMP: Found a peer struct for 172.18.124.96, peer port 500
ISAKMP: Locking peer struct 0x63B2EAE4, IKE refcount 1 for
   crypto_ikmp_config_initialize_sa
ISAKMP (0:0): (Re)Setting client xauth list and state
ISAKMP: local port 500, remote port 500
ISAKMP: insert sa successfully sa = 63972310
ISAKMP (0:1): processing SA payload. message ID = 0
ISAKMP (0:1): processing ID payload. message ID = 0
ISAKMP (0:1): peer matches *none* of the profiles
ISAKMP (0:1): processing vendor id payload
ISAKMP (0:1): vendor ID seems Unity/DPD but major 215 mismatch
ISAKMP (0:1): vendor ID is XAUTH
ISAKMP (0:1): processing vendor id payload
ISAKMP (0:1): vendor ID is DPD
ISAKMP (0:1): processing vendor id payload
ISAKMP (0:1): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP (0:1): vendor ID is NAT-T v2
ISAKMP (0:1): processing vendor id payload
ISAKMP (0:1): vendor ID seems Unity/DPD but major 194 mismatch
ISAKMP (0:1): processing vendor id payload
ISAKMP (0:1): vendor ID is Unity
ISAKMP (0:1) Authentication by xauth preshared
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: encryption AES-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: keylength of 256
!ISAKMP (0:1): Encryption algorithm offered does not match policy
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 2 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 256
!ISAKMP (0:1): Encryption algorithm offered does not match policy
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 256
!ISAKMP (0:1): Encryption algorithm offered does not match policy
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 4 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
```

```
                                        ISAKMP: life type in seconds
                   ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
                                            ISAKMP: keylength of 256
                                         ISAKMP (0:1): Encryh of 128
   !ISAKMP (0:1): Encryption algorithm offered does not match policy
            ISAKMP (0:1): atts are not acceptable. Next payload is 3
 ISAKMP (0:1): Checking ISAKMP transform 7 against priority 1 policy
                                          ISAKMP: encryption AES-CBC
                                                    ISAKMP: hash SHA
                                             ISAKMP: default group 2
                                              ISAKMP: auth pre-share
                                        ISAKMP: life type in seconds
                   ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
            ISAKMP: keylength of 128ption algorithm offered does not
   !ISAKMP (0:1): Encryption algorithm offered does not match policy
            ISAKMP (0:1): atts are not acceptable. Next payload is 3
 ISAKMP (0:1): Checking ISAKMP transform 8 against priority 1 policy
                                          ISAKMP: encryption AES-CBC
                                                    ISAKMP: hash MD5
                                             ISAKMP: default group 2
                                              ISAKMP: auth pre-share
                                        ISAKMP: life type in seconds
                   ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
                                            ISAKMP: keylength of 128
   !ISAKMP (0:1): Encryption algorithm offered does not match policy
            ISAKMP (0:1): atts are not acceptable. Next payload is 3
 ISAKMP (0:1): Checking ISAKMP transform 9 against priority 1 policy
                                         ISAKMP: encryption 3DES-CBC
                                      !ISAKMP: hash SHA match policy
            ISAKMP (0:1): atts are not acceptable. Next payload is 3
 ISAKMP (0:1): Checking ISAKMP transform 5 against priority 1 policy
                                          ISAKMP: encryption AES-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: keylength of 128
   !ISAKMP (0:1): Encryption algorithm offered does not match policy
            ISAKMP (0:1): atts are not acceptable. Next payload is 3
 ISAKMP (0:1): Checking ISAKMP transform 6 against priority 1 policy
                                          ISAKMP: encryption AES-CBC
                                                    ISAKMP: hash MD5
                                             ISAKMP: default group 2
                                     ISAKMP: auth XAUTHInitPreShared
                                        ISAKMP: life type in seconds
                   ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
                                                    ISAKMP: keylengt
                                             ISAKMP: default group 2
                                     ISAKMP: auth XAUTHInitPreShared
                                        ISAKMP: life type in seconds
                   ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
   !ISAKMP (0:1): Encryption algorithm offered does not match policy
            ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 10 against priority 1 policy
                                         ISAKMP: encryption 3DES-CBC
                                                    ISAKMP: hash MD5
                                             ISAKMP: default group 2
                                     ISAKMP: auth XAUTHInitPreShared
                                        ISAKMP: life type in seconds
                   ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
   !ISAKMP (0:1): Encryption algorithm offered does not match policy
            ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 11 against priority 1 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 0x20 0xC4 0x9B
!ISAKMP (0:1): Encryption algorithm offered does not match policy
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 12 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
!ISAKMP (0:1): Encryption algorithm offered does not match policy
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 13 against priority 1 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable. Next payload is 3
ISAKMP (0:1): processing KE payload. message ID = 0
ISAKMP (0:1): processing NONCE payload. message ID = 0
ISAKMP (0:1): vendor ID is NAT-T v2
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
ISAKMP (0:1): Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT
ISAKMP: got callback 1
ISAKMP (0:1): SKEYID state generated
ISAKMP (0:1): constructed NAT-T vendor-02 ID
ISAKMP (0:1): SA is doing pre-shared key authentication
   plus XAUTH using id type ID_IPV4_ADDR
ISAKMP (1): ID payload
   next-payload : 10
   type : 1
   addr : 172.18.124.159
   protocol : 17
   port : 0
   length : 8
ISAKMP (1): Total payload length: 12
ISAKMP (0:1): constructed HIS NAT-D
ISAKMP (0:1): constructed MINE NAT-D
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
   peer_port 500 (R) AG_INIT_EXCH
ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY
ISAKMP (0:1): Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
   sport 500 Global (R) AG_INIT_EXCH
ISAKMP (0:1): processing HASH payload. message ID = 0
ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1
   spi 0, message ID = 0, sa = 63972310
,ISAKMP (0:1): Process initial contact
bring down existing phase 1 and 2 SA's with local 172.18.124.159
   remote 172.18.124.96 remote port 500
ISAKMP (0:1): returning IP addr to the address pool: 14.1.1.105
ISAKMP (0:1): returning address 14.1.1.105 to pool
ISAKMP:received payload type 17
ISAKMP (0:1): Detected NAT-D payload
ISAKMP (0:1): recalc my hash for NAT-D
ISAKMP (0:1): NAT match MINE hash
ISAKMP:received payload type 17
```

```
ISAKMP (0:1): Detected NAT-D payload
ISAKMP (0:1): recalc his hash for NAT-D
ISAKMP (0:1): NAT match HIS hash
ISAKMP (0:1): SA has been authenticated with 172.18.124.96
ISAKMP: set new node 1397605141 to CONF_XAUTH
ISAKMP (0:1): sending packet to 172.18.124.96
my_port 500 peer_port 500 (R) QM_IDLE
ISAKMP (0:1): purging node 1397605141
ISAKMP: Sending phase 1 responder lifetime 86400
ISAKMP (0:1): peer matches *none* of the profiles
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
ISAKMP (0:1): Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE
...IPSEC(key_engine): got a queue event
ISAKMP (0:1): Need XAUTH
ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP (0:1): Old State = IKE_P1_COMPLETE
New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT
ISAKMP: got callback 1
ISAKMP: set new node 1446280258 to CONF_XAUTH
ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
ISAKMP (0:1): initiating peer config to 172.18.124.96. ID = 1446280258
ISAKMP (0:1): sending packet to 172.18.124.96
my_port 500 peer_port 500 (R) CONF_XAUTH
ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, IKE_AAA_START_LOGIN
ISAKMP (0:1): Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT
New State = IKE_XAUTH_REQ_SENT
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
sport 500 Global (R) CONF_XAUTH
.ISAKMP (0:1): processing transaction payload from 172.18.124.96
message ID = 1446280258
ISAKMP: Config payload REPLY
ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
ISAKMP (0:1): deleting node 1446280258 error FALSE
"reason "done with xauth request/reply exchange
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY
ISAKMP (0:1): Old State = IKE_XAUTH_REQ_SENT
New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
ISAKMP: got callback 1
ISAKMP: set new node 117774567 to CONF_XAUTH
.ISAKMP (0:1): initiating peer config to 172.18.124.96
ID = 117774567
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
peer_port 500 (R) CONF_XAUTH
ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, IKE_AAA_CONT_LOGIN
ISAKMP (0:1): Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
New State = IKE_XAUTH_SET_SENT
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
sport 500 Global (R) CONF_XAUTH
.ISAKMP (0:1): processing transaction payload from 172.18.124.96
message ID = 117774567
ISAKMP: Config payload ACK
ISAKMP (0:1): XAUTH ACK Processed
ISAKMP (0:1): deleting node 117774567 error FALSE
"reason "done with transaction
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK
ISAKMP (0:1): Old State = IKE_XAUTH_SET_SENT
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
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
sport 500 Global (R) QM_IDLE
```

```
ISAKMP: set new node 188739171 to QM_IDLE
.ISAKMP (0:1): processing transaction payload from 172.18.124.96
message ID = 188739171
ISAKMP: Config payload REQUEST
:ISAKMP (0:1): checking request
ISAKMP: IP4_ADDRESS
ISAKMP: IP4_NETMASK
ISAKMP: IP4_DNS
ISAKMP: IP4_NBNS
ISAKMP: ADDRESS_EXPIRY
ISAKMP: APPLICATION_VERSION
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: 0x7008
ISAKMP: UNKNOWN Unknown Attr: 0x7009
ISAKMP: UNKNOWN Unknown Attr: 0x700A
ISAKMP: UNKNOWN Unknown Attr: 0x7005
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST
ISAKMP (0:1): Old State = IKE_P1_COMPLETE
New State = IKE_CONFIG_AUTHOR_AAA_AWAIT
ISAKMP: got callback 1
:ISAKMP (0:1): attributes sent in message
Address: 0.2.0.0
ISAKMP (0:1): allocating address 14.1.1.106
ISAKMP: Sending private address: 14.1.1.106
ISAKMP: Sending IP4_DNS server address: 14.1.1.10
ISAKMP: Sending IP4_NBNS server address: 14.1.1.20
ISAKMP: Sending ADDRESS_EXPIRY seconds left to
use the address: 86396
ISAKMP: Sending APPLICATION_VERSION string: Cisco
Internetwork Operating System Software
,IOS (tm) 3600 Software (C3640-JK9O3S-M), Version 12.2(15)T2
(RELEASE SOFTWARE (fc2
TAC Support: http://www.cisco.com/tac
.Copyright (c) 1986-2003 by cisco Systems, Inc
Compiled Wed 30-Apr-03 05:42 by nmasa
(ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7000
(ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7001
ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com
(ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7003
(ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7007
(ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7008
(ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7009
(ISAKMP (0/1): Unknown Attr: UNKNOWN (0x700A
(ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7005
.ISAKMP (0:1): responding to peer config from 172.18.124.96
ID = 188739171
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
peer_port 500 (R) CONF_ADDR
"" ISAKMP (0:1): deleting node 188739171 error FALSE reason
ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR
ISAKMP (0:1): Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT
New State = IKE_P1_COMPLETE
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
sport 500 Global (R) QM_IDLE
ISAKMP: set new node -1836135476 to QM_IDLE
ISAKMP (0:1): processing HASH payload. message ID = -1836135476
ISAKMP (0:1): processing SA payload. message ID = -1836135476
ISAKMP (0:1): Checking IPSec proposal 1
ISAKMP: transform 1, ESP_AES
```

```
:ISAKMP: attributes in transform
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
ISAKMP (0:1): Checking IPSec proposal 1
ISAKMP (0:1): transform 1, IPPCP LZS
:ISAKMP: attributes in transform
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-aes 256 esp-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
,IPSEC(validate_proposal_request): proposal part #2
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= PCP, transform= comp-lzs
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
IPSEC(validate_transform_proposal): transform proposal
:not supported for identity
{ esp-aes 256 esp-md5-hmac comp-lzs}
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 2
ISAKMP: transform 1, ESP_AES
:ISAKMP: attributes in transform
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
ISAKMP (0:1): Checking IPSec proposal 2
ISAKMP (0:1): transform 1, IPPCP LZS
:ISAKMP: attributes in transform
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-aes 256 esp-sha-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
,IPSEC(validate_proposal_request): proposal part #2
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= PCP, transform= comp-lzs
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
```

```
IPSEC(validate_transform_proposal): transform proposal
:not supported for identity
{ esp-aes 256 esp-sha-hmac comp-lzs}
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 3
ISAKMP: transform 1, ESP_AES
:ISAKMP: attributes in transform
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
ISAKMP (0:1): Checking IPSec proposal 3
ISAKMP (0:1): transform 1, IPPCP LZS
:ISAKMP: attributes in transform
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-aes esp-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
,IPSEC(validate_proposal_request): proposal part #2
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= PCP, transform= comp-lzs
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
IPSEC(validate_transform_proposal): transform proposal
:not supported for identity
{ esp-aes esp-md5-hmac comp-lzs}
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 4
ISAKMP: transform 1, ESP_AES
:ISAKMP: attributes in transform
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
ISAKMP (0:1): Checking IPSec proposal 4
ISAKMP (0:1): transform 1, IPPCP LZS
:ISAKMP: attributes in transform
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-aes esp-sha-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
,IPSEC(validate_proposal_request): proposal part #2
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
```

```
,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= PCP, transform= comp-lzs
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
IPSEC(validate_transform_proposal): transform proposal
:not supported for identity
{ esp-aes esp-sha-hmac comp-lzs}
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 5
ISAKMP: transform 1, ESP_AES
:ISAKMP: attributes in transform
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-aes 256 esp-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
IPSEC(validate_transform_proposal): transform proposal
:not supported for identity
{ esp-aes 256 esp-md5-hmac}
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 6
ISAKMP: transform 1, ESP_AES
:ISAKMP: attributes in transform
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-aes 256 esp-sha-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
IPSEC(validate_transform_proposal): transform proposal
:not supported for identity
{ esp-aes 256 esp-sha-hmac}
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 7
ISAKMP: transform 1, ESP_AES
:ISAKMP: attributes in transform
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-aes esp-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
IPSEC(validate_transform_proposal): transform proposal
:not supported for identity
{ esp-aes esp-md5-hmac}
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 8
ISAKMP: transform 1, ESP_AES
:ISAKMP: attributes in transform
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-aes esp-sha-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
IPSEC(validate_transform_proposal): transform proposal
:not supported for identity
{ esp-aes esp-sha-hmac}
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 9
ISAKMP: transform 1, ESP_3DES
:ISAKMP: attributes in transform
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
ISAKMP (0:1): Checking IPSec proposal 9
ISAKMP (0:1): transform 1, IPPCP LZS
:ISAKMP: attributes in transform
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-3des esp-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
,IPSEC(validate_proposal_request): proposal part #2
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= PCP, transform= comp-lzs
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
IPSEC(validate_transform_proposal): transform proposal
:not supported for identity
{ esp-3des esp-md5-hmac comp-lzs}
ISAKMP (0:1): IPSec policy invalidated proposal
```

```
                             ISAKMP (0:1): Checking IPSec proposal 10
                                        ISAKMP: transform 1, ESP_3DES
                                     :ISAKMP: attributes in transform
                                    ISAKMP: authenticator is HMAC-SHA
                                                  ISAKMP: encaps is 1
                                      ISAKMP: SA life type in seconds
                 ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
                                   .ISAKMP (0:1): atts are acceptable
                             ISAKMP (0:1): Checking IPSec proposal 10
                                 ISAKMP (0:1): transform 1, IPPCP LZS
                                     :ISAKMP: attributes in transform
                                                  ISAKMP: encaps is 1
                                      ISAKMP: SA life type in seconds
                 ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
                                   .ISAKMP (0:1): atts are acceptable
                  ,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
            ,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
               ,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
                    , protocol= ESP, transform= esp-3des esp-sha-hmac
                                                 ,lifedur= 0s and 0kb
                      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
                  ,IPSEC(validate_proposal_request): proposal part #2
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
            ,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
               ,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
                                 , protocol= PCP, transform= comp-lzs
                                                 ,lifedur= 0s and 0kb
                      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
        = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
               IPSEC(validate_transform_proposal): transform proposal
                                       :not supported for identity   
                                    { esp-3des esp-sha-hmac comp-lzs}
                      ISAKMP (0:1): IPSec policy invalidated proposal
                             ISAKMP (0:1): Checking IPSec proposal 11
                                        ISAKMP: transform 1, ESP_3DES
                                     :ISAKMP: attributes in transform
                                    ISAKMP: authenticator is HMAC-MD5
                                                  ISAKMP: encaps is 1
                                      ISAKMP: SA life type in seconds
                 ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
                                   .ISAKMP (0:1): atts are acceptable
                  ,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
            ,(local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1
               ,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
                    , protocol= ESP, transform= esp-3des esp-md5-hmac
                                                 ,lifedur= 0s and 0kb
                      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
        = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
     ISAKMP (0:1): processing NONCE payload. message ID = -1836135476
        ISAKMP (0:1): processing ID payload. message ID = -1836135476
        ISAKMP (0:1): processing ID payload. message ID = -1836135476
                           ISAKMP (0:1): asking for 1 spis from ipsec
          ,ISAKMP (0:1): Node -1836135476, Input = IKE_MESG_FROM_PEER
                                                       IKE_QM_EXCH   
                               ISAKMP (0:1): Old State = IKE_QM_READY
                                     New State = IKE_QM_SPI_STARVE   
           ISAKMP (0:1): received packet from 172.18.124.96 dport 500
                                      sport 500 Global (R) QM_IDLE   
                          ISAKMP: set new node -1171731793 to QM_IDLE
      ISAKMP (0:1): processing HASH payload. message ID = -1171731793
        ISAKMP (0:1): processing SA payload. message ID = -1171731793
                              ISAKMP (0:1): Checking IPSec proposal 1
```

```
ISAKMP: transform 1, ESP_AES
:ISAKMP: attributes in transform
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
ISAKMP (0:1): Checking IPSec proposal 1
ISAKMP (0:1): transform 1, IPPCP LZS
:ISAKMP: attributes in transform
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-aes 256 esp-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
,IPSEC(validate_proposal_request): proposal part #2
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= PCP, transform= comp-lzs
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
IPSEC(validate_transform_proposal): transform proposal
:not supported for identity
{ esp-aes 256 esp-md5-hmac comp-lzs}
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 2
ISAKMP: transform 1, ESP_AES
:ISAKMP: attributes in transform
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
ISAKMP (0:1): Checking IPSec proposal 2
ISAKMP (0:1): transform 1, IPPCP LZS
:ISAKMP: attributes in transform
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-aes 256 esp-sha-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
,IPSEC(validate_proposal_request): proposal part #2
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= PCP, transform= comp-lzs
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
```

```
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
IPSEC(validate_transform_proposal): transform proposal
:not supported for identity
{ esp-aes 256 esp-sha-hmac comp-lzs}
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 3
ISAKMP: transform 1, ESP_AES
:ISAKMP: attributes in transform
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
ISAKMP (0:1): Checking IPSec proposal 3
ISAKMP (0:1): transform 1, IPPCP LZS
:ISAKMP: attributes in transform
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-aes esp-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
,IPSEC(validate_proposal_request): proposal part #2
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= PCP, transform= comp-lzs
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
IPSEC(validate_transform_proposal): transform proposal
:not supported for identity
{ esp-aes esp-md5-hmac comp-lzs}
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 4
ISAKMP: transform 1, ESP_AES
:ISAKMP: attributes in transform
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
ISAKMP (0:1): Checking IPSec proposal 4
ISAKMP (0:1): transform 1, IPPCP LZS
:ISAKMP: attributes in transform
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
.ISAKMP (0:1): atts are acceptable
,IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-aes esp-sha-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
,IPSEC(validate_proposal_request): proposal part #2
```

```
,key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96)
,(local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
,(remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1
, protocol= PCP, transform= comp-lzs
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf
IPSEC(validate_transform_proposal): transform proposal
:not supported for identity
{ esp-aes esp-sha-hmac comp-lzs}
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 5
ISAKMP: transform 1, ESP_AES
:ISAKMP: attributes in transform
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): processing ID payload. message ID = -1171731793
ISAKMP (0:1): processing ID payload. message ID = -1171731793
ISAKMP (0:1): asking for 1 spis from ipsec
,ISAKMP (0:1): Node -1171731793, 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 3756150268 for SA
from 172.18.124.159 to 172.18.124.96 for prot 3
...IPSEC(key_engine): got a queue event
IPSEC(spi_response): getting spi 2229862856 for SA
from 172.18.124.159 to 172.18.124.96 for prot 3
(ISAKMP: received ke message (2/1
(ISAKMP: received ke message (2/1
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
peer_port 500 (R) QM_IDLE
,ISAKMP (0:1): Node -1836135476, 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 172.18.124.96 dport 500
sport 500 Global (R) QM_IDLE
,ISAKMP: Locking peer struct 0x63B2EAE4
IPSEC refcount 1 for for stuff_ke
ISAKMP (0:1): Creating IPSec SAs
inbound SA from 172.18.124.96 to 172.18.124.159 (f/i) 0/ 0
(proxy 14.1.1.106 to 172.18.124.159)
has spi 0xDFE24DFC and conn_id 2000 and flags 2
lifetime of 2147483 seconds
has client flags 0x0
ISAKMP (0:1): Old State = IKE_QM_SPI_STARVE
New State = IKE_QM_R_QM2
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
sport 500 Global (R) QM_IDLE
,ISAKMP: Locking peer struct 0x63B2EAE4
IPSEC refcount 2 for for stuff_ke
ISAKMP (0:1): Creating IPSec SAs
inbound SA from 172.18.124.96 to 172.18.124.159 (f/i) 0/ 0
(proxy 14.1.1.106 to 0.0.0.0)
has spi 0x84E901C8 and conn_id 2002 and flags 2
lifetime of 2147483 seconds
has client flags 0x0
outbound SA from 172.18.124.159 to 172.18.124.96 (f/i) 0/ 0
( proxy 0.0.0.0 to 14.1.1.106)
```

```
has spi -802758470 and conn_id 2003 and flags A
IPSEC(add mtree): src 0.0.0.0, dest 14.1.1.106, dest_port 0
,IPSEC(create_sa): sa created
,sa) sa_dest= 172.18.124.159, sa_prot= 50)
,(sa_spi= 0x84E901C8(2229862856
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
,IPSEC(create_sa): sa created
,sa) sa_dest= 172.18.124.96, sa_prot= 50)
,(sa_spi= 0xD026E0BA(3492208826
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2003
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
sport 500 Global (R) QM_IDLE
ISAKMP: set new node 839140381 to QM_IDLE
ISAKMP (0:1): processing HASH payload. message ID = 839140381
ISAKMP (0:1): processing NOTIFY R_U_THERE protocol 1
spi 0, message ID = 839140381, sa = 63972310
ISAKMP (0:1): deleting node 839140381 error FALSE
"reason "informational (in) state 1
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY
ISAKMP (0:1): Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE
,ISAKMP (0:1): DPD/R_U_THERE received from peer 172.18.124.96
sequence 0xA5A4632A
ISAKMP: set new node 760238809 to QM_IDLE
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
peer_port 500 (R) QM_IDLE
ISAKMP (0:1): purging node 760238809
,ISAKMP (0:1): Input = IKE_MESG_FROM_PEER
IKE_MESG_KEEP_ALIVE
ISAKMP (0:1): Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE
ISAKMP (0:1): purging node 188739171
ISAKMP (0:1): purging node -1836135476
ISAKMP (0:1): purging node -1171731793
3640#
```

سجلات العميل

لعرض السجلات، قم بتشغيل LogViewer على عميل VPN، وتأكد من تعيين عامل التصفية على "عالي" لجميع الفئات التي تم تكوينها. يتم عرض إخراج نموذج السجل أدناه.

```
Sev=Info/6       DIALER/0x63300002  02/26/02  10:24:17.492      1
.Initiating connection

Sev=Info/4       CM/0x63100002  02/26/02  10:24:17.492      2
Begin connection process

Sev=Info/4       CM/0x63100004  02/26/02  10:24:17.512      3
Establish secure connection using Ethernet

Sev=Info/4       CM/0x63100026  02/26/02  10:24:17.512      4
"Attempt connection with server "172.18.124.159

Sev=Info/6       IKE/0x6300003B  02/26/02  10:24:17.512      5
.Attempting to establish a connection with 172.18.124.159

Sev=Info/4       IKE/0x63000013  02/26/02  10:24:17.562      6
(SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID
to 172.18.124.159

Sev=Info/4       IPSEC/0x63700014  02/26/02  10:24:17.962      7
Deleted all keys
```

```
               Sev=Info/5       IKE/0x6300002F  02/26/02  10:24:18.223      8
                                Received ISAKMP packet: peer = 172.18.124.159

               Sev=Info/4       IKE/0x63000014  02/26/02  10:24:18.223      9
                     ,RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, VID, KE
                                                         $ID, NON, HASH) from

               Sev=Info/5       IKE/0x63000059  02/26/02  10:24:18.223     10
                         Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

               Sev=Info/5       IKE/0x63000001  02/26/02  10:24:18.223     11
                                         Peer is a Cisco-Unity compliant peer

               Sev=Info/5       IKE/0x63000059  02/26/02  10:24:18.223     12
                         Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

               Sev=Info/5       IKE/0x63000001  02/26/02  10:24:18.223     13
                                                            Peer supports DPD

               Sev=Info/5       IKE/0x63000059  02/26/02  10:24:18.223     14
                         Vendor ID payload = 4C72E0B594C3C20DFCB7F4419CCEB0BE

               Sev=Info/5       IKE/0x63000059  02/26/02  10:24:18.223     15
                                         Vendor ID payload = 09002689DFD6B712

               Sev=Info/4       IKE/0x63000013  02/26/02  10:24:18.263     16
             (SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT
                                                                 to 172.18.1$

               Sev=Info/5       IKE/0x6300002F  02/26/02  10:24:18.283     17
                                Received ISAKMP packet: peer = 172.18.124.159

               Sev=Info/4       IKE/0x63000014  02/26/02  10:24:18.283     18
           (RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME
                                                                   $.from 172

               Sev=Info/5       IKE/0x63000044  02/26/02  10:24:18.283     19
                         RESPONDER-LIFETIME notify has value of 86400 seconds

               Sev=Info/5       IKE/0x63000046  02/26/02  10:24:18.283     20
$This SA has already been alive for 1 seconds, setting expiry to 86399 second

               Sev=Info/5       IKE/0x6300002F  02/26/02  10:24:18.303     21
                                Received ISAKMP packet: peer = 172.18.124.159

               Sev=Info/4       IKE/0x63000014  02/26/02  10:24:18.303     22
             RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.18.124.159

                Sev=Info/4       CM/0x63100015  02/26/02  10:24:18.303     23
                                                     Launch xAuth application

                Sev=Info/4       CM/0x63100017  02/26/02  10:24:20.546     24
                                                   xAuth application returned

               Sev=Info/4       IKE/0x63000013  02/26/02  10:24:20.546     25
                 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.18.124.159

               Sev=Info/5       IKE/0x6300002F  02/26/02  10:24:20.566     26
                                Received ISAKMP packet: peer = 172.18.124.159

               Sev=Info/4       IKE/0x63000014  02/26/02  10:24:20.566     27
             RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.18.124.159
```

```
                Sev=Info/4       CM/0x6310000E  02/26/02  10:24:20.566     28
                          Established Phase 1 SA.  1 Phase 1 SA in the system

               Sev=Info/4       IKE/0x63000013  02/26/02  10:24:20.576     29
                 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.18.124.159

               Sev=Info/4       IKE/0x63000013  02/26/02  10:24:20.586     30
                 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.18.124.159

               Sev=Info/5       IKE/0x6300002F  02/26/02  10:24:20.636     31
                                Received ISAKMP packet: peer = 172.18.124.159

               Sev=Info/4       IKE/0x63000014  02/26/02  10:24:20.636     32
             RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.18.124.159

               Sev=Info/5       IKE/0x63000010  02/26/02  10:24:20.636     33
      MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 14.1.1.102

               Sev=Info/5       IKE/0x63000010  02/26/02  10:24:20.636     34
     MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): , value = 14.38.100.10

               Sev=Info/5       IKE/0x63000010  02/26/02  10:24:20.636     35
$ = MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS) : , value

               Sev=Info/5       IKE/0xA3000017  02/26/02  10:24:20.636     36
$) MODE_CFG_REPLY: The received (INTERNAL_ADDRESS_EXPIRY) attribute and value

               Sev=Info/5       IKE/0x6300000E  02/26/02  10:24:20.636     37
$ MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Internetwork
$IOS (tm) C2600 Software (C2600-JK9O3S-M), Version 12.2(8)T,  RELEASE SOFTWAR
                                        TAC Support: http://www.cisco.com/tac
                               .Copyright (c) 1986-2002 by cisco Systems, Inc
                                         Compiled Thu 14-Feb-02 16:50 by ccai

               Sev=Info/5       IKE/0x6300000E  02/26/02  10:24:20.636     38
     MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: , value = cisco.com

                Sev=Info/4       CM/0x63100019  02/26/02  10:24:20.646     39
                                                    Mode Config data received

               Sev=Info/5       IKE/0x63000055  02/26/02  10:24:20.676     40
Received a key request from Driver for IP address 172.18.124.159, GW IP = 17$

               Sev=Info/4       IKE/0x63000013  02/26/02  10:24:20.676     41
         SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 172.18.124.159

               Sev=Info/5       IKE/0x63000055  02/26/02  10:24:20.676     42
$.Received a key request from Driver for IP address 10.10.10.255, GW IP = 172

               Sev=Info/4       IKE/0x63000013  02/26/02  10:24:20.676     43
         SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 172.18.124.159

             Sev=Info/4       IPSEC/0x63700014  02/26/02  10:24:20.967     44
                                                             Deleted all keys

               Sev=Info/5       IKE/0x6300002F  02/26/02  10:24:20.987     45
                                Received ISAKMP packet: peer = 172.18.124.159

               Sev=Info/4       IKE/0x63000014  02/26/02  10:24:20.987     46
                             ,RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID
                                                 $ID, NOTIFY:STATUS_RESP_LIFE

               Sev=Info/5       IKE/0x63000044  02/26/02  10:24:20.987     47
                          RESPONDER-LIFETIME notify has value of 3600 seconds
               Sev=Info/5       IKE/0x63000045  02/26/02  10:24:20.987     48
                            RESPONDER-LIFETIME notify has value of 4608000 kb

               Sev=Info/4       IKE/0x63000013  02/26/02  10:24:20.987     49
                          SENDING >>> ISAKMP OAK QM *(HASH) to 172.18.124.159

               Sev=Info/5       IKE/0x63000058  02/26/02  10:24:20.987     50
$ Loading IPsec SA (Message ID = 0x49D93B33 OUTBOUND SPI = 0x4637A127 INBOUND

               Sev=Info/5       IKE/0x63000025  02/26/02  10:24:20.987     51
                                          Loaded OUTBOUND ESP SPI: 0x4637A127

               Sev=Info/5       IKE/0x63000026  02/26/02  10:24:20.987     52
                                           Loaded INBOUND ESP SPI: 0xCE633EA8

                Sev=Info/4       CM/0x6310001A  02/26/02  10:24:20.987     53
                                            One secure connection established

            Sev=Info/6       DIALER/0x63300003  02/26/02  10:24:21.017     54
                                                      .Connection established

            Sev=Info/6       DIALER/0x63300008  02/26/02  10:24:21.357     55
                         MAPI32 Information - Outlook not default mail client

               Sev=Info/5       IKE/0x6300002F  02/26/02  10:24:21.617     56
                                Received ISAKMP packet: peer = 172.18.124.159

               Sev=Info/4       IKE/0x63000014  02/26/02  10:24:21.617     57
                              ,RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID
                                                 $ID, NOTIFY:STATUS_RESP_LIFE

               Sev=Info/5       IKE/0x63000044  02/26/02  10:24:21.617     58
                          RESPONDER-LIFETIME notify has value of 3600 seconds

               Sev=Info/5       IKE/0x63000045  02/26/02  10:24:21.617     59
                            RESPONDER-LIFETIME notify has value of 4608000 kb

               Sev=Info/4       IKE/0x63000013  02/26/02  10:24:21.617     60
                          SENDING >>> ISAKMP OAK QM *(HASH) to 172.18.124.159

               Sev=Info/5       IKE/0x63000058  02/26/02  10:24:21.617     61
$ Loading IPsec SA (Message ID = 0x41AC9838 OUTBOUND SPI = 0x287931C6 INBOUND

               Sev=Info/5       IKE/0x63000025  02/26/02  10:24:21.617     62
                                          Loaded OUTBOUND ESP SPI: 0x287931C6

               Sev=Info/5       IKE/0x63000026  02/26/02  10:24:21.617     63
                                           Loaded INBOUND ESP SPI: 0x26EC8782

                Sev=Info/4       CM/0x63100022  02/26/02  10:24:21.617     64
                                           .Additional Phase 2 SA established

               Sev=Info/5       IKE/0x63000055  02/26/02  10:24:21.617     65
$.Received a key request from Driver for IP address 14.38.100.10, GW IP = 172

               Sev=Info/4       IKE/0x63000013  02/26/02  10:24:21.617     66
         SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 172.18.124.159

               Sev=Info/5       IKE/0x6300002F  02/26/02  10:24:21.948     67
                                Received ISAKMP packet: peer = 172.18.124.159

               Sev=Info/4       IKE/0x63000014  02/26/02  10:24:21.948     68
                              ,RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID
                                                 $ID, NOTIFY:STATUS_RESP_LIFE

               Sev=Info/5       IKE/0x63000044  02/26/02  10:24:21.948     69
                          RESPONDER-LIFETIME notify has value of 3600 seconds

               Sev=Info/5       IKE/0x63000045  02/26/02  10:24:21.948     70
                            RESPONDER-LIFETIME notify has value of 4608000 kb

               Sev=Info/4       IKE/0x63000013  02/26/02  10:24:21.948     71
                          SENDING >>> ISAKMP OAK QM *(HASH) to 172.18.124.159

               Sev=Info/5       IKE/0x63000058  02/26/02  10:24:21.948     72
$ Loading IPsec SA (Message ID = 0xCDC476F0 OUTBOUND SPI = 0xFDE4BA9C INBOUND

               Sev=Info/5       IKE/0x63000025  02/26/02  10:24:21.948     73
                                          Loaded OUTBOUND ESP SPI: 0xFDE4BA9C

               Sev=Info/5       IKE/0x63000026  02/26/02  10:24:21.948     74
                                           Loaded INBOUND ESP SPI: 0xDEA46284

                Sev=Info/4       CM/0x63100022  02/26/02  10:24:21.948     75
                                           .Additional Phase 2 SA established

             Sev=Info/4       IPSEC/0x63700010  02/26/02  10:24:22.248     76
                                                  Created a new key structure

             Sev=Info/4       IPSEC/0x6370000F  02/26/02  10:24:22.248     77
                                  Added key with SPI=0x27a13746 into key list

             Sev=Info/4       IPSEC/0x63700010  02/26/02  10:24:22.248     78
                                                  Created a new key structure

             Sev=Info/4       IPSEC/0x6370000F  02/26/02  10:24:22.248     79
                                  Added key with SPI=0xa83e63ce into key list

             Sev=Info/4       IPSEC/0x63700010  02/26/02  10:24:22.248     80
             Sev=Info/4       IPSEC/0x6370000F  02/26/02  10:24:22.248     81
                                  Added key with SPI=0xc6317928 into key list

             Sev=Info/4       IPSEC/0x63700010  02/26/02  10:24:22.248     82
                                                  Created a new key structure

             Sev=Info/4       IPSEC/0x6370000F  02/26/02  10:24:22.248     83
                                  Added key with SPI=0x8287ec26 into key list

             Sev=Info/4       IPSEC/0x63700010  02/26/02  10:24:22.248     84
                                                  Created a new key structure

             Sev=Info/4       IPSEC/0x6370000F  02/26/02  10:24:22.248     85
                                  Added key with SPI=0x9cbae4fd into key list

             Sev=Info/4       IPSEC/0x63700010  02/26/02  10:24:22.248     86
                                                  Created a new key structure

             Sev=Info/4       IPSEC/0x6370000F  02/26/02  10:24:22.248     87
                                  Added key with SPI=0x8462a4de into key list
```

معلومات ذات صلة

- دعم منتجات مركزات Cisco VPN 3000
- دعم منتج عميل Cisco VPN 3000
- مفاوضة IPSec/دعم تقنية بروتوكولات 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).