تكوين مفاتيح IKE المشتركة مسبقا لعميل Cisco Secure VPN باستخدام خادم RADIUS

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين سر مشترك لـ IKE (Internet Key Exchange) باستخدام خادم RADIUS. تتيح ميزة سر IKE المشترك التي تستخدم خادم المصادقة والتفويض والمحاسبة (AAA) إمكانية البحث عن المفتاح من خادم AAA. لا يمكن توسعة المفاتيح المشتركة مسبقا بشكل جيد عند نشر نظام شبكات VPN واسع النطاق بدون مرجع مصدق (CA). عند إستخدام عنونة IP الديناميكية مثل إتصالات بروتوكول التكوين الديناميكي للمضيف (DHCP) أو بروتوكول الاتصال من نقطة إلى نقطة (PPP)، يمكن أن يجعل عنوان IP المتغير البحث عن المفتاح صعبا أو مستحيلا ما لم يتم إستخدام مفتاح مشترك مسبقا لحرف البدل. في ميزة "سر IKE المشترك" التي تستخدم خادم AAA، يتم الوصول إلى السر المشترك أثناء الوضع القوي لمفاوضات IKE من خلال خادم AAA. يتم إستخدام معرف Exchange كاسم مستخدم للاستعلام عن المصادقة والتفويض والمحاسبة (AAA) إذا لم يتم العثور على مفتاح محلي على موجه Cisco IOS® الذي يحاول المستخدم الاتصال به. تم تقديم هذا في البرنامج Cisco IOS Software، الإصدار T.12.1. أنت ينبغي يتلقى أسلوب واسع يمكن على ال VPN زبون أن يستعمل هذا سمة.

المتطلبات الأساسية

المتطلبات

أنت ينبغي يتلقى أسلوب عدواني يمكن على ال VPN زبون، وأنت ينبغي كنت يركض cisco ios برمجية إطلاق T.12.1 أو فيما بعد على المسحاج تخديد.

المكونات المستخدمة

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

- مصدر المحتوى الإضافي الآمن من Cisco لأنظمة التشغيل Windows
- برنامج IOS الإصدار 12.2.8T من Cisco
- موجّه Cisco 1700

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.

الاصطلاحات

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

التكوين

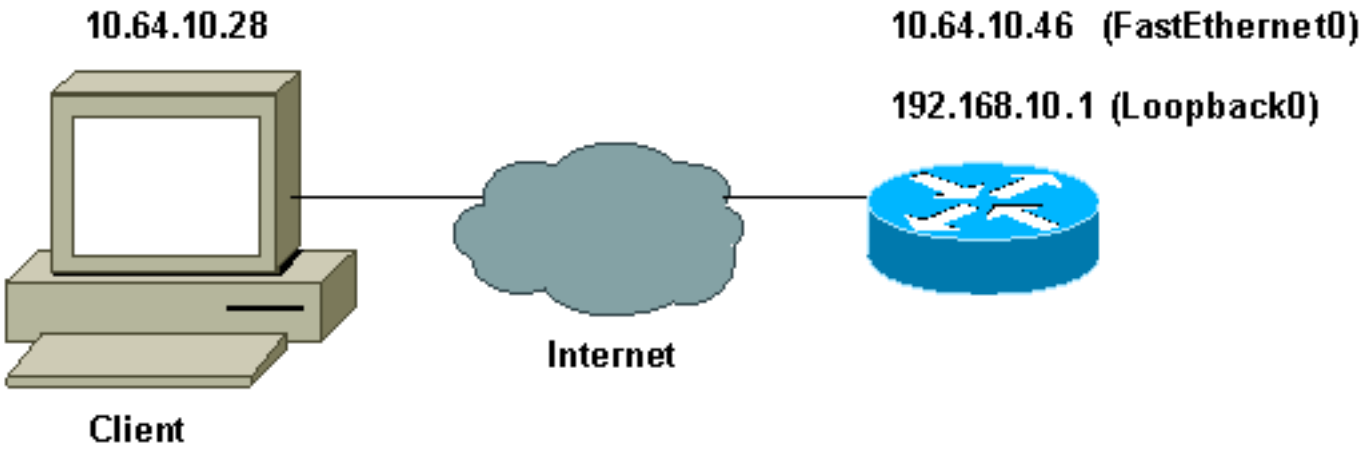
يستخدم هذا المستند التكوينات الموضحة أدناه.

- إنشاء ملف تعريف Cisco آمن
- تكوين الموجه
- تكوين العميل

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 التالي:



إنشاء ملف تعريف Cisco آمن

تم إنشاء ملف التعريف هذا باستخدام UNIX، ولكن يمكن إنشاء ملف تعريف مماثل على ACS الآمن من Cisco لأنظمة التشغيل Windows.

```
ViewProfile -p 9900 -u haseeb/. #
                User Profile Information
The user name is sent by the VPN Client; !--- look at the client configuration. user = ---!
}haseeb
```

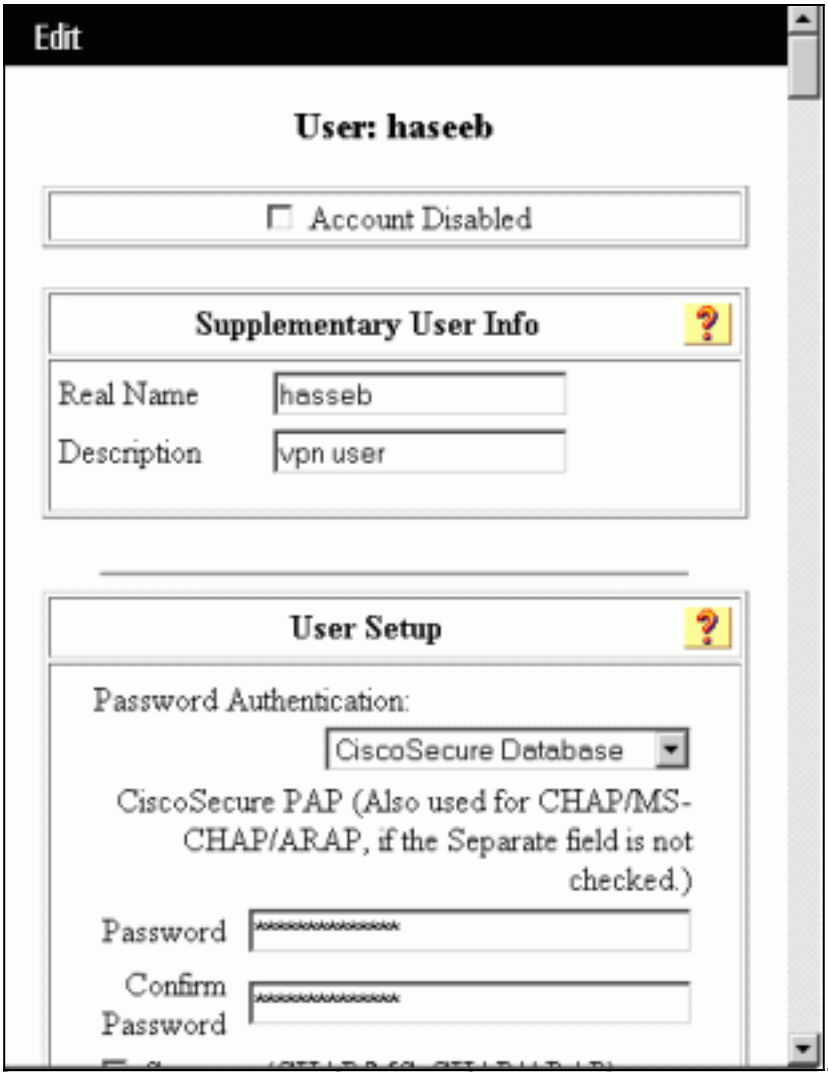
```
} radius=Cisco12.05
} =check_items
This should always be "cisco." 2=cisco ---!
{
} =reply_attributes
5=6
9=64
1=65
"Pre-shared key. 9,1="ipsec:tunnel-password=secret12345 ---!
"ipsec:key-exchange=ike"=9,1
{
{

{
```

يعرض هذا الإخراج النص البرمجي الذي يتم إستخدامه لإضافة ملف تعريف مستخدم في ACS الآمن من Cisco ل UNIX.

```
bin/sh/!#
DeleteProfile -p 9900 -u haseeb/.
AddProfile -p 9900 -u  haseeb -a 'radius=Cisco12.05/.
n check_items = { \n 2="cisco" \n } \n\ }
reply_attributes = { \n 6=5 \n 64=9 \n 65=1 \n
ipsec:tunnel-password=cisco" \n"=9,1
'{ ipsec:key-exchange=ike" \n } \n"=9,1
```

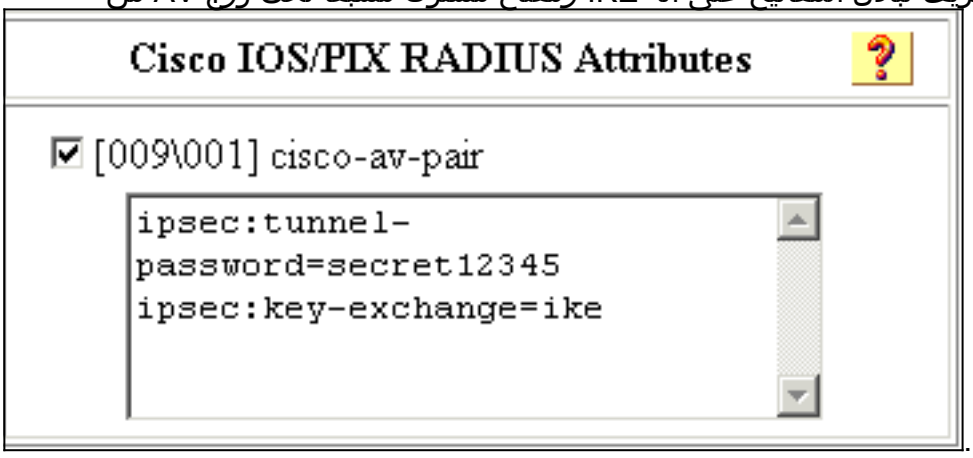
اتبع هذه الخطوات لاستخدام واجهة المستخدم الرسومية (GUI) لتكوين ملف تعريف المستخدم على مصدر المحتوى الإضافي الآمن من Cisco لنظام التشغيل Windows 2.6.

1. عينت المستعمل إسم، مع "cisco"



كالكلمة.

2. قم بتعريف تبادل المفاتيح على أنه IKE ومفتاح مشترك مسبقا تحت زوج AV من



Cisco.

تكوين الموجه

Cisco 1751 مع IOS 12.2.8T
version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname 1751-vpn ! *Enable AAA.* **aaa new-model** ---!

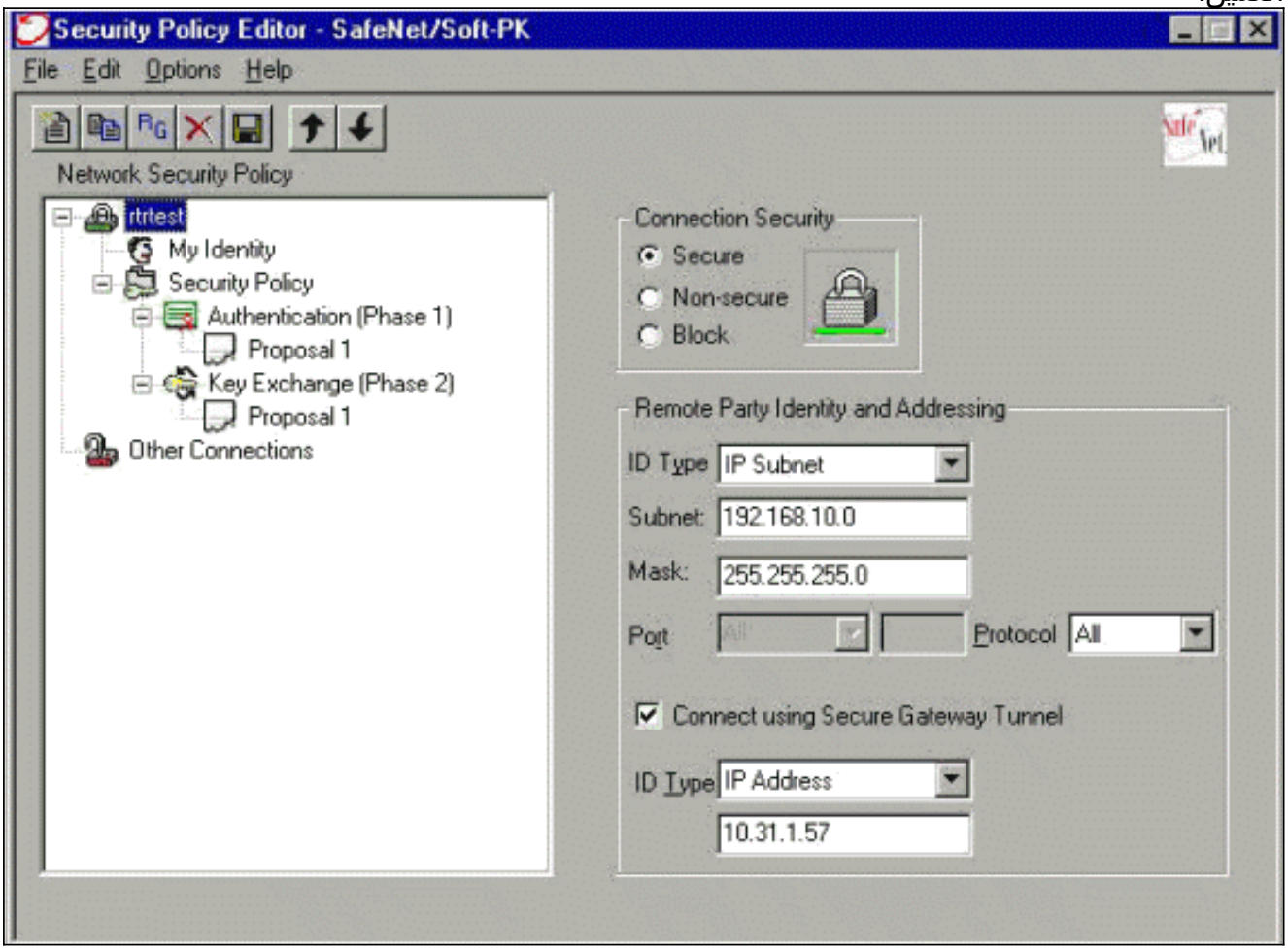
```
!
!
aaa authentication login default none
Configure authorization. aaa authorization network ---!
vpn_users group radius
aaa session-id common
!
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
no ip domain-lookup
!
Define IKE policy for phase 1 negotiations of the ---!
VPN Clients. crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp client configuration address-pool local
mypool
!
Define IPSec policies - Phase 2 Policy for actual ---!
data encryption. crypto ipsec transform-set myset esp-
des esp-md5-hmac
!
Create dynamic crypto map. crypto dynamic-map ---!
dynmap 10
set transform-set myset
!
Configure IKE shared secret using AAA server on ---!
this router. crypto map intmap isakmp authorization list
vpn_users
IKE Mode Configuration - the router will attempt !- ---!
-- to set IP addresses for each peer. crypto map intmap
client configuration address initiate
IKE Mode Configuration - the router will accept !-- ---!
- requests for IP addresses from any requesting peer.
crypto map intmap client configuration address respond
crypto map intmap 10 ipsec-isakmp dynamic dynmap
!
interface Loopback0
ip address 192.168.10.1 255.255.255.0
!
interface Loopback1
no ip address
!
interface Ethernet0/0
no ip address
half-duplex
!
interface FastEthernet0/0
ip address 10.64.10.46 255.255.255.224
speed auto
Assign crypto map to interface. crypto map intmap ---!
!
Configure a local pool of IP addresses to be used ---!
when a !--- remote peer connects to a point-to-point
interface. ip local pool mypool 10.1.2.1 10.1.2.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.64.10.33
no ip http server
ip pim bidir-enable
```

```
!
Specify the security server protocol and defines ---!
    security !--- server host IP address and UDP port
number. radius-server host 10.64.10.7 auth-port 1645
                                acct-port 1646 key cisco123
                                 radius-server retransmit 3
                                                         !
                                                 line con 0
                                            exec-timeout 0 0
                                                   line aux 0
                                                line vty 0 4
                                                         !
                                                       end
```

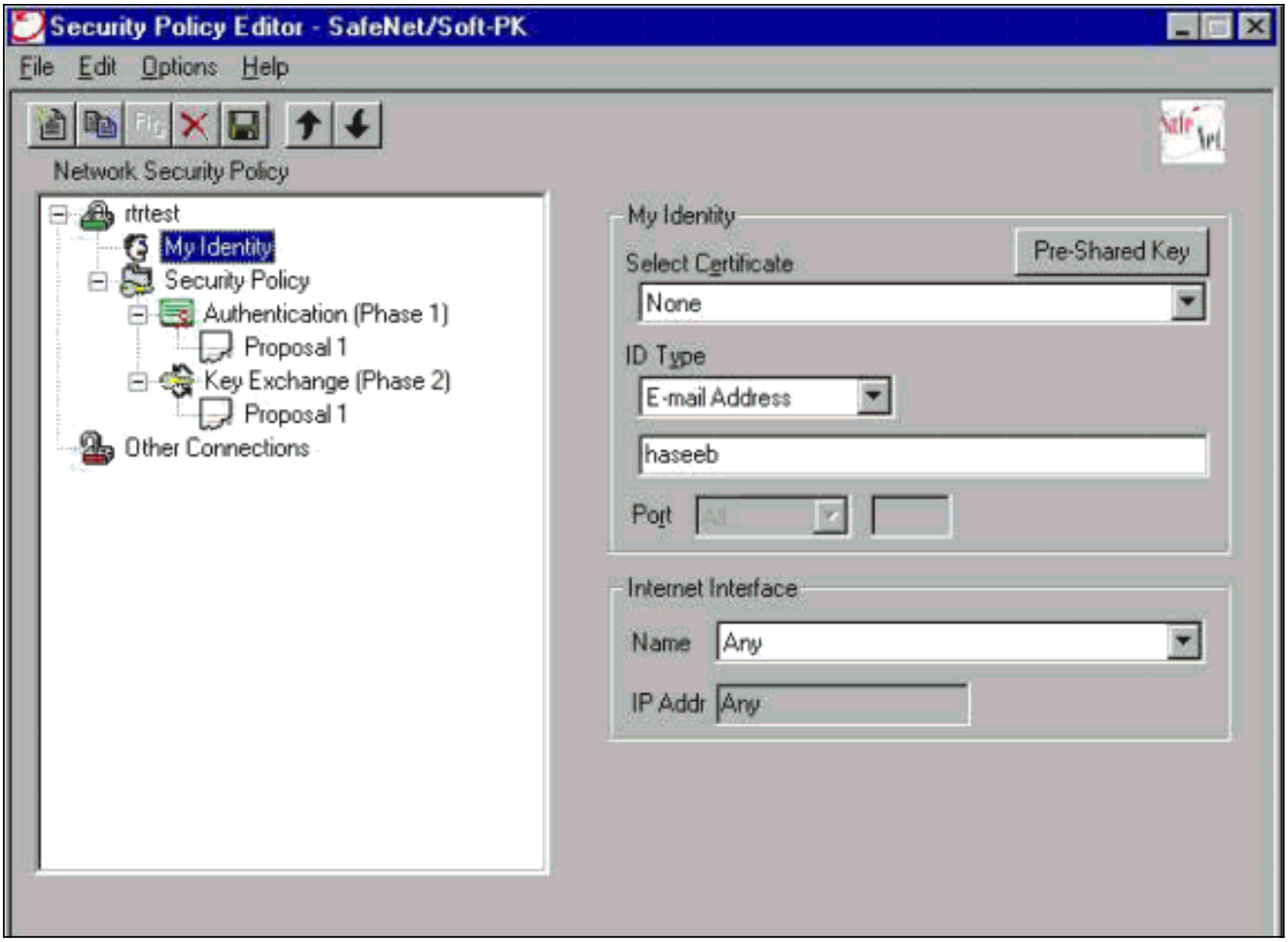
تكوين العميل

اتبع هذه الخطوات لتكوين العميل.

1. في "محرر نهج الأمان"، انتقل إلى **نهج أمان الشبكة > تغيير**. حدد **نوع المعرف** كعنوان بريد إلكتروني ووضعت اسم مستخدم ليتم تكوينه على خادم RADIUS. في حالة ترك هذا الإعداد ك "عنوان IP"، يكون اسم المستخدم المرسل إلى خادم RADIUS هو عنوان IP الخاص بالكمبيوتر العميل.



2. انتقل إلى **نهج أمان الشبكة > RTRTEST > هويتي** وحدد **الوضع المتميز**. لن يعمل الإعداد إذا لم يتم تحديد هذا الوضع.



التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

يعرض هذا الإخراج تصحيح أخطاء جيد لهذا التكوين:

```
ISAKMP (0:0): received packet from 10.64.10.28 (N) NEW SA :23:43:41
ISAKMP: local port 500, remote port 500 :23:43:41
ISAKMP: Locking CONFIG struct 0x8180BEF4 from :23:43:41
crypto_ikmp_config_initialize_sa, count 2
ISAKMP (0:3): processing SA payload. message ID = 0 :23:43:41
ISAKMP (0:3): processing ID payload. message ID = 0 :23:43:41
ISAKMP (0:3): processing vendor id payload :23:43:41
ISAKMP (0:3): vendor ID seems Unity/DPD but bad major :23:43:41
ISAKMP (0:3): vendor ID is XAUTH :23:43:41
ISAKMP (0:3): Checking ISAKMP transform 1 against priority 10 policy :23:43:41
ISAKMP: encryption DES-CBC :23:43:41
ISAKMP: hash MD5 :23:43:41
ISAKMP: default group 1 :23:43:41
ISAKMP: auth pre-share :23:43:41
ISAKMP policy proposed by VPN Client !--- matched the configured ISAKMP policy. 23:43:41: ---!
ISAKMP (0:3): atts are acceptable. Next payload is 0
ISAKMP (0:3): processing KE payload. message ID = 0 :23:43:41
```

```
ISAKMP (0:3): processing NONCE payload. message ID = 0 :23:43:41
ISAKMP (0:3): SKEYID state generated :23:43:41
ISAKMP (0:3): processing vendor id payload :23:43:41
ISAKMP (0:3): vendor ID seems Unity/DPD but bad major :23:43:41
ISAKMP (0:3): vendor ID is XAUTH :23:43:41
ISAKMP (0:3): SA is doing pre-shared key authentication :23:43:41
using id type ID_IPV4_ADDR
ISAKMP (3): ID payload :23:43:41
next-payload : 10
type : 1
protocol : 17
port : 500
length : 8

ISAKMP (3): Total payload length: 12 :23:43:41
ISAKMP (0:3): sending packet to 10.64.10.28 (R) AG_INIT_EXCH :23:43:41
ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH :23:43:41
Old State = IKE_READY New State = IKE_R_AM2
ISAKMP (0:3): received packet from 10.64.10.28 (R) AG_INIT_EXCH :23:43:42
ISAKMP (0:3): processing HASH payload. message ID = 0 :23:43:42
ISAKMP (0:3): SA has been authenticated with 10.64.10.28 :23:43:42
ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH :23:43:42
Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE
ISAKMP (0:3): received packet from 10.64.10.28 (R) QM_IDLE :23:43:43
ISAKMP (0:3): Need config/address :23:43:43
ISAKMP (0:3): Need config/address :23:43:43
ISAKMP: Sending private address: 10.1.2.2 :23:43:43
.ISAKMP (0:3): initiating peer config to 10.64.10.28 :23:43:43
ID = -1082015193
ISAKMP (0:3): sending packet to 10.64.10.28 (R) CONF_ADDR :23:43:43
ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE :23:43:43
Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_MODE_SET_SENT
ISAKMP (0:3): received packet from 10.64.10.28 (R) CONF_ADDR :23:43:43
.ISAKMP (0:3): processing transaction payload from 10.64.10.28 :23:43:43
message ID = -1082015193
ISAKMP: Config payload ACK :23:43:43
!ISAKMP (0:3): peer accepted the address :23:43:43
ISAKMP (0:3): deleting node -1082015193 error FALSE :23:43:43
"reason "done with transaction
ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK :23:43:43
Old State = IKE_CONFIG_MODE_SET_SENT New State = IKE_P1_COMPLETE
.ISAKMP (0:3): Delaying response to QM request :23:43:43
ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE :23:43:43
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
ISAKMP (0:3): received packet from 10.64.10.28 (R) QM_IDLE :23:43:44
ISAKMP (0:3): processing HASH payload. message ID = -920829332 :23:43:44
ISAKMP (0:3): processing SA payload. message ID = -920829332 :23:43:44
ISAKMP (0:3): Checking IPSec proposal 1 :23:43:44
ISAKMP: transform 1, ESP_DES :23:43:44
:ISAKMP: attributes in transform :23:43:44
ISAKMP: authenticator is HMAC-MD5 :23:43:44
ISAKMP: encaps is 1 :23:43:44
Proposed Phase 2 transform set !--- matched configured IPSec transform set. 23:43:44: ---!
.ISAKMP (0:3): atts are acceptable
,IPSEC(validate_proposal_request): proposal part #1 :23:43:44
,key eng. msg.) INBOUND local= 10.64.10.46, remote= 10.64.10.28)
,(local_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 10.1.2.2/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
ISAKMP (0:3): processing NONCE payload. message ID = -920829332 :23:43:44
ISAKMP (0:3): processing ID payload. message ID = -920829332 :23:43:44
ISAKMP (0:3): processing ID payload. message ID = -920829332 :23:43:44
```

```
                                    ISAKMP (0:3): asking for 1 spis from ipsec :23:43:44
                                                ,ISAKMP (0:3): Node -920829332 :23:43:44
                                            Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
                                    Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
                                        ...IPSEC(key_engine): got a queue event :23:43:44
                                IPSEC(spi_response): getting spi 2940839732 for SA :23:43:44
                                                from 10.64.10.46 to 10.64.10.28 for prot 3
                                            (ISAKMP: received ke message (2/1 :23:43:44
                            ISAKMP (0:3): sending packet to 10.64.10.28 (R) QM_IDLE :23:43:45
                                                ,ISAKMP (0:3): Node -920829332 :23:43:45
                                        Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
                                    Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
                        ISAKMP (0:3): received packet from 10.64.10.28 (R) QM_IDLE :23:43:45
                                            ISAKMP (0:3): Creating IPSec SAs :23:43:45
                                    inbound SA from 10.64.10.28 to 10.64.10.46 :23:43:45
                                                (proxy 10.1.2.2 to 192.168.10.0)
                                has spi 0xAF49A734 and conn_id 200 and flags 4 :23:43:45
                                    outbound SA from 10.64.10.46 to 10.64.10.28 :23:43:45
                                                ( proxy 192.168.10.0 to 10.1.2.2)
                                has spi 1531785085 and conn_id 201 and flags C :23:43:45
                                ISAKMP (0:3): deleting node 1961959105 error FALSE :23:43:45
                                            "reason "saved qm no longer needed
                                ISAKMP (0:3): deleting node -920829332 error FALSE :23:43:45
                                            "()reason "quick mode done (await
                                                ,ISAKMP (0:3): Node -920829332 :23:43:45
                                            Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
                                Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
                                        ...IPSEC(key_engine): got a queue event :23:43:45
                                                , :(IPSEC(initialize_sas :23:43:45
                        ,key eng. msg.) INBOUND local= 10.64.10.46, remote= 10.64.10.28)
                                    ,(local_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4
                                        ,(remote_proxy= 10.1.2.2/0.0.0.0/0/0 (type=1
                                    , protocol= ESP, transform= esp-des esp-md5-hmac
                                                ,lifedur= 0s and 0kb
                        spi= 0xAF49A734(2940839732), conn_id= 200, keysize= 0, flags= 0x4
                                                , :(IPSEC(initialize_sas :23:43:45
                        ,key eng. msg.) OUTBOUND local= 10.64.10.46, remote= 10.64.10.28)
                                    ,(local_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4
                                        ,(remote_proxy= 10.1.2.2/0.0.0.0/0/0 (type=1
                                    , protocol= ESP, transform= esp-des esp-md5-hmac
                                                ,lifedur= 0s and 0kb
                        spi= 0x5B4D2F7D(1531785085), conn_id= 201, keysize= 0, flags= 0xC
,IPSec SAs created. 23:43:45: IPSEC(create_sa): sa created, (sa) sa_dest= 10.64.10.46 ---!
                                    ,(sa_prot= 50,  sa_spi= 0xAF49A734(2940839732
                                        sa_trans= esp-des esp-md5-hmac , sa_conn_id= 200
                    ,IPSEC(create_sa): sa created, (sa) sa_dest= 10.64.10.28 :23:43:45
                                    ,(sa_prot= 50, sa_spi= 0x5B4D2F7D(1531785085
                                        sa_trans= esp-des esp-md5-hmac , sa_conn_id= 201
                                            (ISAKMP: received ke message (4/1 :23:43:45
                                    ISAKMP: Locking CONFIG struct 0x8180BEF4 :23:43:45
                                for crypto_ikmp_config_handle_kei_mess, count 3
                                        ISAKMP (0:2): purging node 618568216 :23:43:50
                                    ISAKMP (0:2): purging node -497663485 :23:43:50
                        ISAKMP (0:2): purging SA., sa=816B5724, delme=816B5724 :23:44:00
                                ISAKMP: Unlocking CONFIG struct 0x8180BEF4 on :23:44:00
                                            return of attributes, count 2
```

معلومات ذات صلة

- صفحة دعم RADIUS
- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم Windows
- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم UNIX

- صفحة دعم IPSec
- طلبات التعليقات (RFCs)
- الدعم الفني - 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).