使用RADIUS伺服器為Cisco安全VPN客戶端配置IKE預共用金鑰

目錄

簡介

本文說明如何使用RADIUS伺服器設定Internet金鑰交換(IKE)共用密碼。使用身份驗證、授權和記帳(AAA)伺服器的IKE共用金鑰功能允許從AAA伺服器查詢金鑰。部署沒有證書頒發機構(CA)的大規模VPN系統時，預共用金鑰無法很好地擴展。 使用動態IP定址(例如動態主機配置協定(DHCP)或點對點協定(PPP)撥號時，變化的IP地址可能會使金鑰查詢變得困難或無法進行，除非使用萬用字元預共用金鑰。在使用AAA伺服器的IKE共用金鑰功能中，在IKE協商的主動模式下，通過AAA伺服器訪問共用金鑰。如果在使用者嘗試連線的Cisco IOS®路由器上找不到本地金鑰，則使用交換機的ID作為使用者名稱來查詢AAA。這是在Cisco IOS軟體版本12.1.T中匯入。您必須在VPN客戶端上啟用主動模式才能使用此功能。

必要條件

需求

必須在VPN客戶端上啟用主動模式，並且必須在路由器上運行Cisco IOS軟體版本12.1.T或更高版本。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Secure ACS for Windows

- Cisco IOS軟體版本12.2.8T
- 思科1700路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

設定

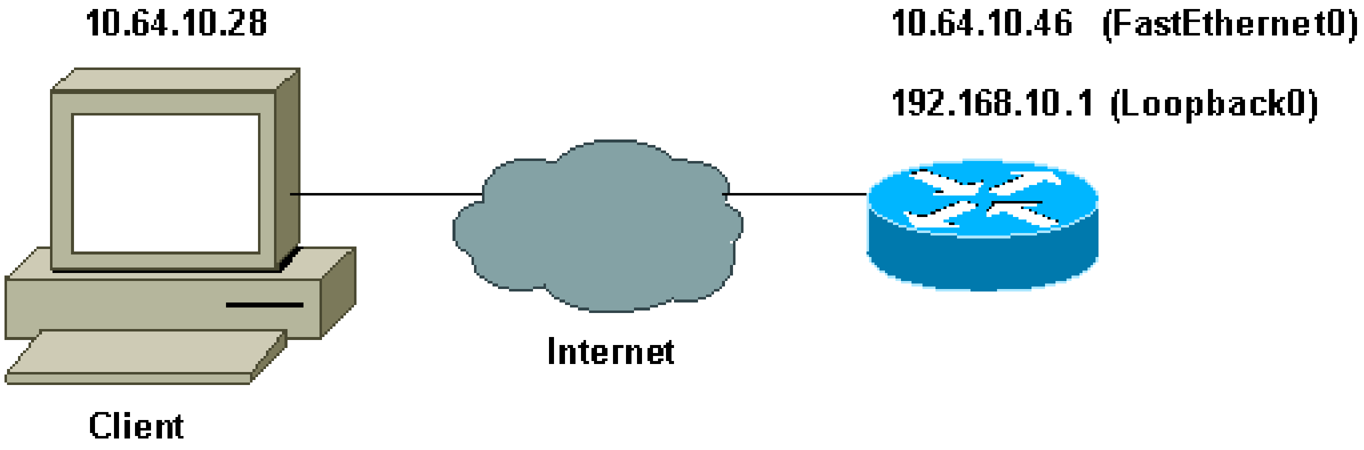
本文檔使用如下所示的配置。

- 建立思科安全設定檔
- 配置路由器
- 配置客戶端

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

網路圖表

本檔案會使用以下網路設定：



建立思科安全設定檔

此配置檔案是使用UNIX建立的，但可以在Cisco Secure ACS for Windows上建立類似的配置檔案。

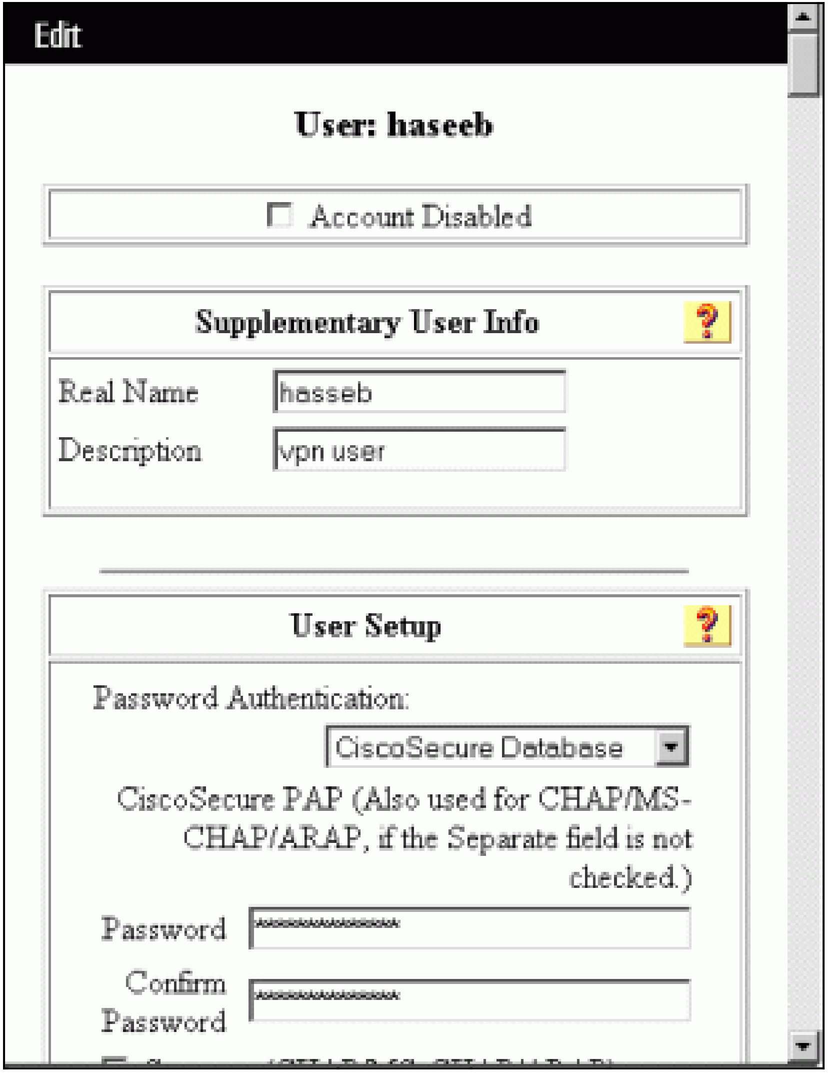
```
# ./ViewProfile -p 9900 -u haseeb
User Profile Information
!--- The user name is sent by the VPN Client; !--- look at the client configuration. user =
haseeb{

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

}
```

此輸出顯示用於在Cisco Secure ACS for UNIX中新增使用者配置檔案的指令碼。

```
#!/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
9,1="ipsec:tunnel-password=cisco" \n
9,1="ipsec:key-exchange=ike" \n } \n }'
```

按照以下步驟使用GUI在適用於Windows 2.6的Cisco Secure ACS上配置使用者配置檔案。

1. 定義使用者名稱，密碼為「cisco」。



Edit

User: haseeb

□ Account Disabled

Supplementary User Info

Real Name: hasseb

Description: vpn user

User Setup

Password Authentication:

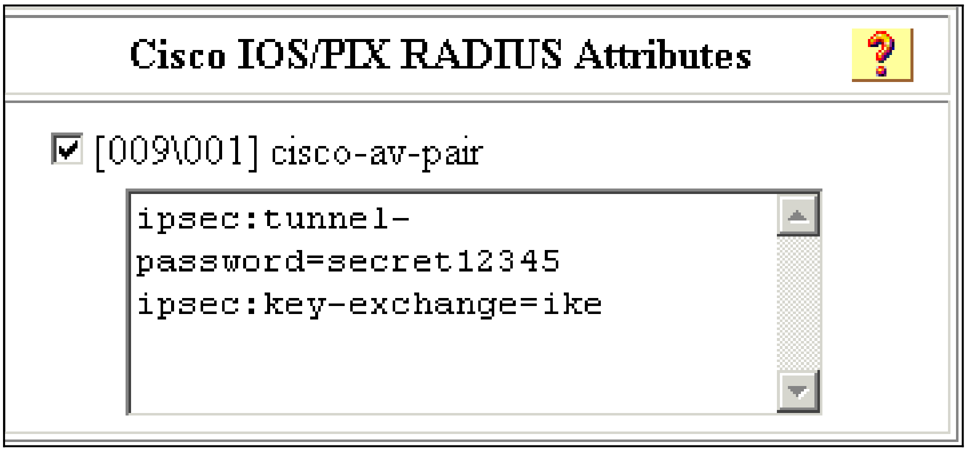
CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

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

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

2. 將金鑰交換定義為IKE和Cisco av對下的預共用金鑰。



Cisco IOS/PIX RADIUS Attributes

☑ [009\001] cisco-av-pair

```
ipsec:tunnel-
password=secret12345
ipsec:key-exchange=ike
```

配置路由器

採用IOS 12.2.8T的Cisco 1751

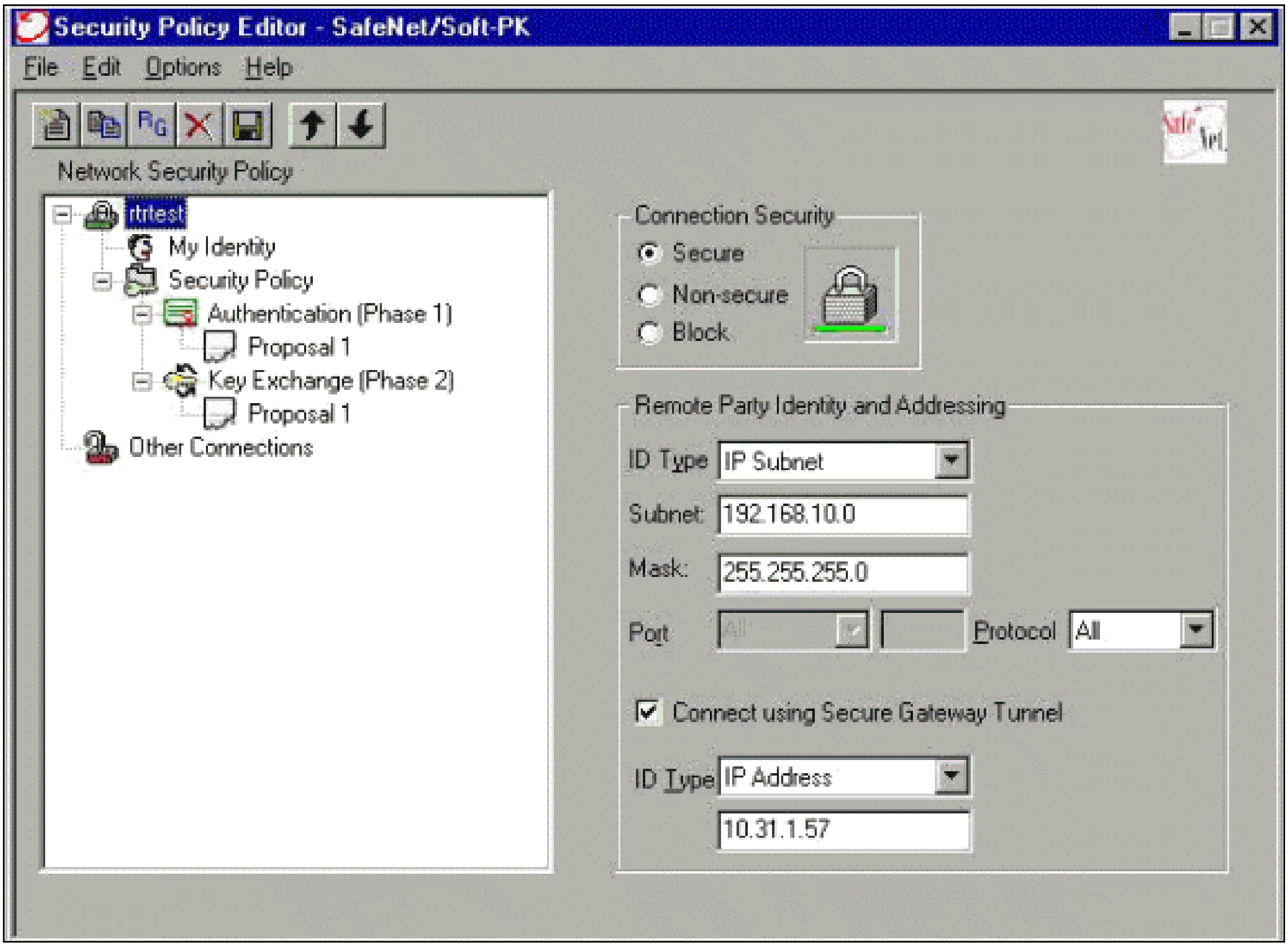
```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1751-vpn
!
!--- Enable AAA. aaa new-model
!
!
aaa authentication login default none
!--- Configure authorization. aaa authorization network
vpn_users group radius
aaa session-id common
!
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
```

配置客戶端

按照以下步驟配置客戶端。

1. 在安全策略編輯器中，轉至**Network Security Policy > rtrtest**。選擇**ID Type**作為電子郵件地址，並輸入要在RADIUS伺服器上配置的使用者名稱。如果此設定保留為「IP地址」，則傳送到RADIUS伺服器的使用者名稱將是客戶端PC的IP地址。



Security Policy Editor - SafeNet/Soft-PK

File Edit Options Help

Network Security Policy

- rtrtest
  - My Identity
  - Security Policy
    - Authentication (Phase 1)
      - Proposal 1
    - Key Exchange (Phase 2)
      - Proposal 1
- Other Connections

Connection Security

● Secure

○ Non-secure

○ Block

Remote Party Identity and Addressing

ID Type: IP Subnet

Subnet: 192.168.10.0

Mask: 255.255.255.0

Port: All

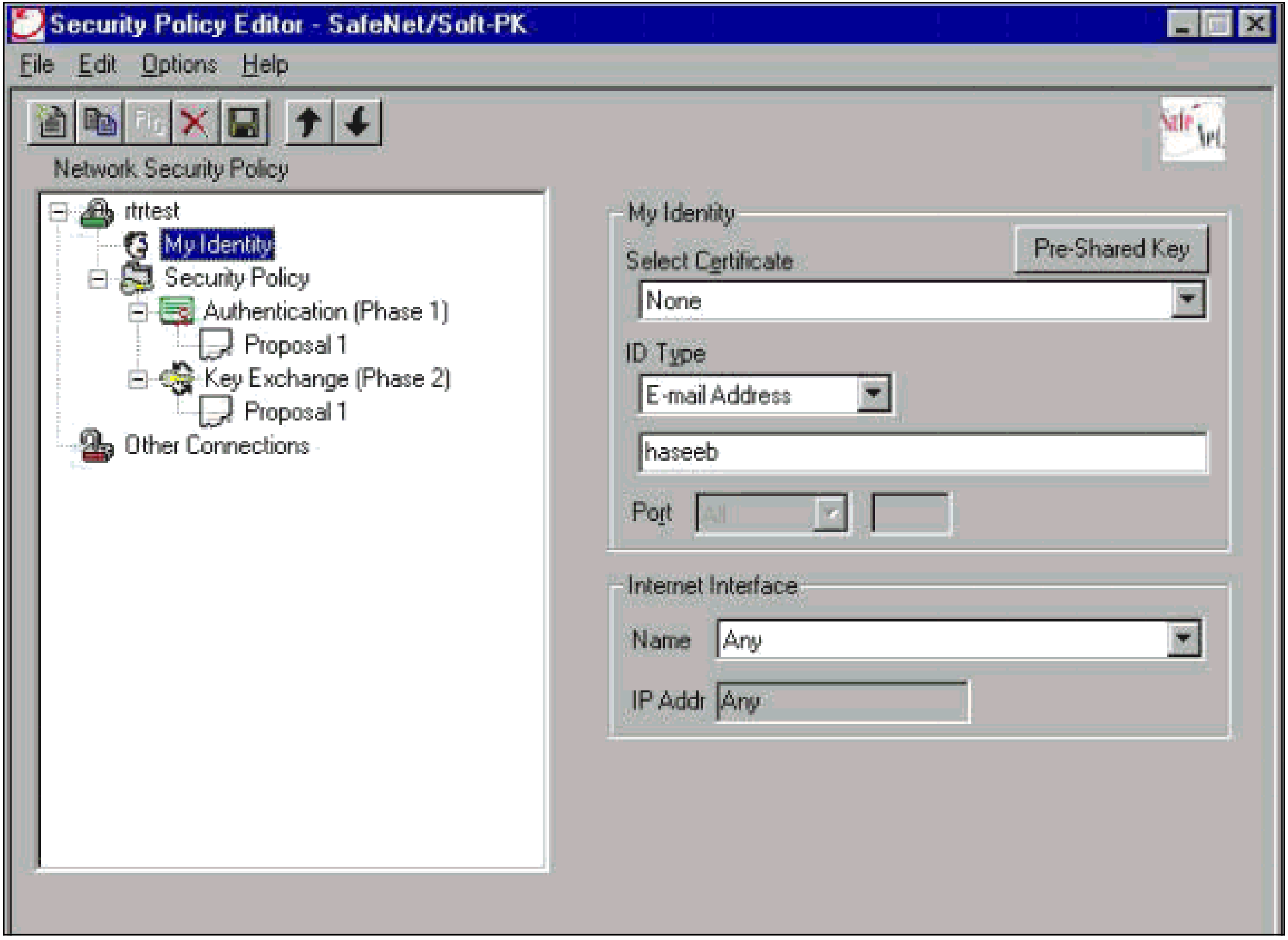
Protocol: All

☑ Connect using Secure Gateway Tunnel

ID Type: IP Address

10.31.1.57

2. 轉到**Network Security Policy > rtrtest > My Identity**，然後選擇**Aggressive Mode**。如果未選擇此模式，則安裝程式將不工作。



Security Policy Editor - SafeNet/Soft-PK

File Edit Options Help

Network Security Policy

- rtrtest
  - My Identity
  - Security Policy
    - Authentication (Phase 1)
      - Proposal 1
    - Key Exchange (Phase 2)
      - Proposal 1
- Other Connections

My Identity

Select Certificate: None

Pre-Shared Key

ID Type: E-mail Address

haseeb

Port: All

Internet Interface

Name: Any

IP Addr: Any

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

此輸出顯示了此配置的良好調試：

```
23:43:41: 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
     crypto_ikmp_config_initialize_sa, count 2
23:43:41: 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
!--- ISAKMP policy proposed by VPN Client !--- matched the configured ISAKMP policy. 23:43:41:
ISAKMP (0:3): atts are acceptable. Next payload is 0
23:43:41: 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
     using id type ID_IPV4_ADDR
23:43:41: ISAKMP (3): ID payload
  next-payload : 10
   type        : 1
    protocol    : 17
   port         : 500
  length       : 8

23:43:41: 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
Old State = IKE_READY New State = IKE_R_AM2
23:43:42: 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
Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE
23:43:43: 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.
     ID = -1082015193
23:43:43: 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
```

```
Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_MODE_SET_SENT
23:43:43: 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.
     message ID = -1082015193
23:43:43: 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
     reason "done with transaction"
23:43:43: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK
Old State = IKE_CONFIG_MODE_SET_SENT New State = IKE_P1_COMPLETE
23:43:43: ISAKMP (0:3): Delaying response to QM request.
23:43:43: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
23:43:44: 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
 !--- Proposed Phase 2 transform set !--- matched configured IPSec transform set. 23:43:44:
ISAKMP (0:3): atts are acceptable.
23:43:44: IPSEC(validate_proposal_request): proposal part #1,
(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
23:43:44: 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,
     Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
23:43:44: IPSEC(key_engine): got a queue event...
23:43:44: IPSEC(spi_response): getting spi 2940839732 for SA
from 10.64.10.46 to 10.64.10.28 for prot 3
23:43:44: ISAKMP: received ke message (2/1)
23:43:45: ISAKMP (0:3): sending packet to 10.64.10.28 (R) QM_IDLE
23:43:45: ISAKMP (0:3): Node -920829332,
     Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
23:43:45: 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
     (proxy 10.1.2.2 to 192.168.10.0)
23:43:45: 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
     (proxy 192.168.10.0 to 10.1.2.2 )
23:43:45: has spi 1531785085 and conn_id 201 and flags C
23:43:45: ISAKMP (0:3): deleting node 1961959105 error FALSE
     reason "saved qm no longer needed"
23:43:45: ISAKMP (0:3): deleting node -920829332 error FALSE
     reason "quick mode done (await()"
23:43:45: ISAKMP (0:3): Node -920829332,
     Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
23:43:45: IPSEC(key_engine): got a queue event...
23:43:45: IPSEC(initialize_sas): ,
(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
23:43:45: IPSEC(initialize_sas): ,
(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
23:43:45: IPSEC(create_sa): sa created, (sa) sa_dest= 10.64.10.28,
     sa_prot= 50, sa_spi= 0x5B4D2F7D(1531785085),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 201
23:43:45: ISAKMP: received ke message (4/1)
23:43:45: ISAKMP: Locking CONFIG struct 0x8180BEF4
     for crypto_ikmp_config_handle_kei_mess, count 3
23:43:50: ISAKMP (0:2): purging node 618568216
23:43:50: ISAKMP (0:2): purging node -497663485
23:44:00: ISAKMP (0:2): purging SA., sa=816B5724, delme=816B5724
23:44:00: ISAKMP: Unlocking CONFIG struct 0x8180BEF4 on
     return of attributes, count 2
```

相關資訊

- RADIUS 支援頁面
- Cisco Secure ACS for Windows支援頁
- Cisco Secure ACS for UNIX支援頁
- IPSec支援頁面
- 要求建議 (RFC)
- 技術支援 - Cisco Systems