使用VPN客戶端配置TACACS+和RADIUS擴展身份驗證

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[設定](#)
[網路圖表](#)
[VPN客戶端1.1設定](#)
[組態](#)
[驗證](#)
[疑難排解](#)
[疑難排解指令](#)
[調試輸出示例](#)
[相關資訊](#)

簡介

本檔案顯示TACACS+和RADIUS Internet工程工作小組(IETF)延伸驗證(Xauth)的組態範例。Xauth允許您使用TACACS+或RADIUS作為網際網路金鑰交換(IKE)通訊協定中的使用者驗證方式，在虛擬私人網路(VPN)上部署IP安全(IPSec)。此功能通過提示使用者輸入使用者名稱和密碼，為其PC上安裝了CiscoSecure VPN Client 1.1的使用者提供身份驗證，然後使用身份驗證、授權和記帳(AAA)伺服器、TACACS+或RADIUS資料庫中儲存的資訊驗證使用者。身份驗證發生在IKE第1階段和IKE第2階段之間。如果使用者成功進行身份驗證，則建立第2階段安全關聯(SA)，之後資料可以安全地傳送到受保護的網路。

Xauth僅包括*驗證*，而不包括*授權*（使用者可以在連線建立後前往該位置）。 *會*計（使用者到達的位置）未實現。

實施Xauth之前，組態必須不使用Xauth才能運作。我們的範例除了Xauth之外，還示範了模式組態（模式設定）和網路位址轉譯(NAT)，但假設在新增Xauth指令之前存在IPSec連線。

在嘗試TACACS+或RADIUS Xauth之前，請確保本地Xauth（路由器上的使用者名稱/密碼）工作正常。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- VPN客戶端版本1.1（或更高版本）
- Cisco IOS®版本12.1.2.2.T、12.1.2.2.P（或更高版本）
- 已在運行c3640-jo3s56i-mz.121-2.3.T的Cisco 3640上測試RADIUS身份驗證

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

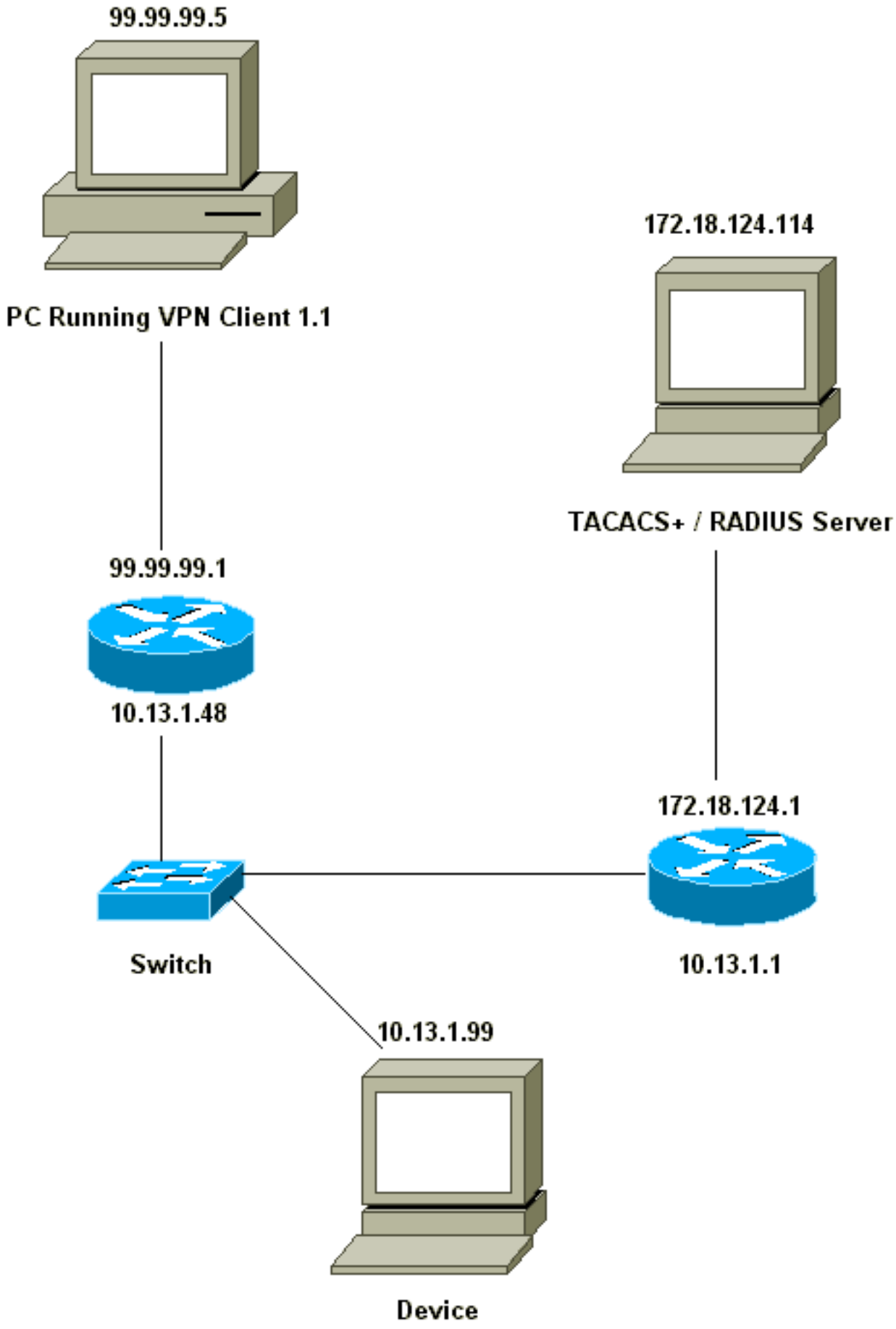
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：


99.99.99.5
PC Running VPN Client 1.1
172.18.124.114
TACACS+ / RADIUS Server
99.99.99.1
10.13.1.48
172.18.124.1
Switch
10.13.1.1
10.13.1.99
Device

[VPN客戶端1.1設定]

```
Network Security policy:
 1- Myconn
         My Identity = ip address
                 Connection security: Secure
                 Remote Party Identity and addressing
                         ID Type: IP subnet
                         10.13.1.0 (range of inside network)
                         Port all Protocol all

                 Connect using secure tunnel
                         ID Type: IP address
                         99.99.99.1
                         Pre-shared key = cisco1234

         Authentication (Phase 1)
         Proposal 1
                 Authentication method: pre-shared key
                 Encryp Alg: DES
                 Hash Alg: MD5
                 SA life: Unspecified
                 Key Group: DH 1

         Key exchange (Phase 2)
         Proposal 1
                 Encapsulation ESP
                 Encrypt Alg: DES
                 Hash Alg: MD5
                 Encap: tunnel
                 SA life: Unspecified
                 no AH

 2- Other Connections
             Connection security: Non-secure
             Local Network Interface
                 Name: Any
                 IP Addr: Any
                 Port: All
```

在路由器上啟用Xauth後，當使用者嘗試連線到路由器內部的裝置時（此處我們執行了ping -t #.#.#.#），系統會顯示灰色畫面：

```
User Authentication for 3660
Username:
Password:
```

組態

伺服器配置

Xauth驗證可以由TACACS+或RADIUS完成。我們想要確保允許Xauth使用者執行Xauth，但是不允許telnet到路由器，因此我們新增了**aaa authorization exec**命令。我們為RADIUS使用者指定了「reply-attribute Service-Type=Outbound=5」（而不是「管理」或「登入」）。 在CiscoSecure UNIX中，這是「出站」；在CiscoSecure NT中，這是「Dialout Framed」。 如果這些使用者是TACACS+使用者，我們將不會授予他們shell/exec許可權。

TACACS+或RADIUS Xauth的路由器配置
Current configuration: ! version 12.1

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname carter
!
!--- Enable AAA and define authentication and
authorization parameters aaa new-model
aaa authentication login default group radius|tacacs+
none
aaa authentication login xauth_list group radius|tacacs+
aaa authorization exec default group radius|tacacs+ none
enable secret 5 $1$VY18$uO2CRnqUzugV0NYtd14Gg0
enable password ww
!
username john password 0 doe
!
ip subnet-zero
ip audit notify log
ip audit po max-events 100
cns event-service server
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key cisco1234 address 0.0.0.0 0.0.0.0
crypto isakmp client configuration address-pool local
ourpool
!
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac
!
crypto dynamic-map dyna 10
set transform-set mypolicy
!
crypto map test client authentication list xauth_list
crypto map test client configuration address initiate
crypto map test client configuration address respond
crypto map test 5 ipsec-isakmp dynamic dyna
!
interface Ethernet0/0
ip address 10.13.1.48 255.255.255.0
ip nat inside
no ip route-cache
no ip mroute-cache
no mop enabled
!
interface TokenRing0/0
no ip address
shutdown
ring-speed 16
!
interface Ethernet2/0
ip address 99.99.99.1 255.255.255.0
ip nat outside
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map test
!
interface TokenRing2/0
no ip address
shutdown
ring-speed 16
!
```

```
ip local pool ourpool 10.2.1.1 10.2.1.254
ip nat pool outsidepool 99.99.99.50 99.99.99.60 netmask
255.255.255.0
ip nat inside source route-map nonat pool outsidepool
ip classless
ip route 0.0.0.0 0.0.0.0 10.13.1.1
no ip http server
!
access-list 101 deny ip 10.13.1.0 0.0.0.255 10.2.1.0
0.0.0.255
access-list 101 permit ip 10.13.1.0 0.0.0.255 any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
route-map nonat permit 10
match ip address 101
!
!--- Define TACACS server host and key parameters
tacacs-server host 172.18.124.114
tacacs-server key cisco
radius-server host 172.18.124.114 auth-port 1645 acct-
port 1646
radius-server retransmit 3
radius-server key cisco
!
line con 0
transport input none
line aux 0
line vty 0 4
password WW
!
end
```

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。

疑難排解指令

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **debug aaa authentication** — 顯示有關AAA/TACACS+身份驗證的資訊。
- **debug crypto isakmp** — 顯示有關IKE事件的消息。
- **debug crypto ipsec** — 顯示IPSec事件。
- **debug crypto key-exchange** — 顯示數位簽章標準(DSS)公鑰交換消息。
- **debug radius** — 顯示與RADIUS關聯的資訊。
- **debug tacacs** — 顯示與TACACS關聯的資訊。
- **clear crypto isakmp** — 指定要清除的連線。
- **clear crypto sa** — 刪除IPSec安全關聯。

調試輸出示例

注意：TACACS+調試將非常相似。使用**debug tacacs+**命令而不是**debug radius**命令。

```
Carter#show debug
General OS:
  AAA Authentication debugging is on
Radius protocol debugging is on
Cryptographic Subsystem:
  Crypto ISAKMP debugging is on
  Crypto Engine debugging is on
  Crypto IPSEC debugging is on
Carter#term mon
03:12:54: ISAKMP (0:0): received packet from 99.99.99.5 (N) NEW SA
03:12:54: ISAKMP: local port 500, remote port 500
03:12:54: ISAKMP (0:1): Setting client config settings 6269C36C
03:12:54: ISAKMP (0:1): (Re)Setting client xauth list xauth_list
   and state
03:12:54: ISAKMP: Created a peer node for 99.99.99.5
03:12:54: ISAKMP: Locking struct 6269C36C from
   crypto_ikmp_config_initialize_sa
03:12:54: ISAKMP (0:1): processing SA payload. message ID = 0
03:12:54: ISAKMP (0:1): found peer pre-shared key matching 99.99.99.5
03:12:54: ISAKMP (0:1): Checking ISAKMP transform 1 against
   priority 10 policy
03:12:54: ISAKMP:      encryption DES-CBC
03:12:54: ISAKMP:      hash MD5
03:12:54: ISAKMP:      default group 1
03:12:54: ISAKMP:      auth pre-share
03:12:54: ISAKMP (0:1): atts are acceptable. Next payload is 0
03:12:54: CryptoEngine0: generate alg parameter
03:12:54: CRYPTO_ENGINE: Dh phase 1 status: 0
03:12:54: CRYPTO_ENGINE: DH phase 1 status: 0
03:12:54: ISAKMP (0:1): SA is doing pre-shared key authentication using
   id type ID_IPV4_ADDR
03:12:54: ISAKMP (0:1): sending packet to 99.99.99.5 (R) MM_SA_SETUP
03:12:54: ISAKMP (0:1): received packet from 99.99.99.5 (R) MM_SA_SETUP
03:12:54: ISAKMP (0:1): processing KE payload. Message ID = 0
03:12:54: CryptoEngine0: generate alg parameter
03:12:54: ISAKMP (0:1): processing NONCE payload. Message ID = 0
03:12:54: ISAKMP (0:1): found peer pre-shared key matching 99.99.99.5
03:12:54: CryptoEngine0: create ISAKMP SKEYID for conn id 1
03:12:54: ISAKMP (0:1): SKEYID state generated
03:12:54: ISAKMP (0:1): processing vendor id payload
03:12:54: ISAKMP (0:1): processing vendor id payload
03:12:54: ISAKMP (0:1): sending packet to 99.99.99.5 (R) MM_KEY_EXCH
03:12:55: ISAKMP (0:1): received packet from 99.99.99.5 (R) MM_KEY_EXCH
03:12:55: ISAKMP (0:1): processing ID payload. Message ID = 0
03:12:55: ISAKMP (0:1): processing HASH payload. Message ID = 0
03:12:55: CryptoEngine0: generate hmac context for conn id 1
03:12:55: ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1
        spi 0, message ID = 0
03:12:55: ISAKMP (0:1): SA has been authenticated with 99.99.99.5
03:12:55: ISAKMP (1): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
03:12:55: ISAKMP (1): Total payload length: 12
03:12:55: CryptoEngine0: generate hmac context for conn id 1
```

```
03:12:55: CryptoEngine0: clear DH number for conn id 1
03:12:55: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH
03:12:55: ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_XAUTH
03:12:55: ISAKMP (0:1): (Re)Setting client xauth list
   xauth_list and state
03:12:55: ISAKMP (0:1): Need XAUTH
03:12:55: AAA: parse name=ISAKMP idb type=-1 tty=-1
03:12:55: AAA/MEMORY: create_user (0x6269AD80) user='' ruser=''
   port='ISAKMP' rem_addr='99.99.99.5' authen_type=ASCII
   service=LOGIN priv=0
03:12:55: AAA/AUTHEN/START (2289801324): port='ISAKMP'
   list='xauth_list' action=LOGIN service=LOGIN
03:12:55: AAA/AUTHEN/START (2289801324): found list xauth_list
03:12:55: AAA/AUTHEN/START (2289801324): Method=radius (radius)
03:12:55: AAA/AUTHEN (2289801324): status = GETUSER
03:12:55: ISAKMP: got callback 1
03:12:55: ISAKMP/xauth: request attribute XAUTH_TYPE
03:12:55: ISAKMP/xauth: request attribute XAUTH_MESSAGE
03:12:55: ISAKMP/xauth: request attribute XAUTH_USER_NAME
03:12:55: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
03:12:55: CryptoEngine0: generate hmac context for conn id 1
03:12:55: ISAKMP (0:1): initiating peer config to 99.99.99.5.
   ID = -280774539
03:12:55: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH
03:13:00: ISAKMP (0:1): retransmitting phase 2 CONF_XAUTH
    -280774539 ...
03:13:00: ISAKMP (0:1): incrementing error counter on sa:
   retransmit phase 2
03:13:00: ISAKMP (0:1): incrementing error counter on sa:
   retransmit phase 2
03:13:00: ISAKMP (0:1): retransmitting phase 2 -280774539 CONF_XAUTH
03:13:00: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH
03:13:02: ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_XAUTH
03:13:02: ISAKMP (0:1): processing transaction payload from
   99.99.99.5. Message ID = -280774539
03:13:02: CryptoEngine0: generate hmac context for conn id 1
03:13:02: ISAKMP: Config payload REPLY
03:13:02: ISAKMP/xauth: reply attribute XAUTH_TYPE
03:13:02: ISAKMP/xauth: reply attribute XAUTH_USER_NAME
03:13:02: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD
03:13:02: AAA/AUTHEN/CONT (2289801324): continue_login (user='(undef)')
03:13:02: AAA/AUTHEN (2289801324): status = GETUSER
03:13:02: AAA/AUTHEN (2289801324): Method=radius (radius)
03:13:02: AAA/AUTHEN (2289801324): status = GETPASS
03:13:02: AAA/AUTHEN/CONT (2289801324): continue_login (user='zeke')
03:13:02: AAA/AUTHEN (2289801324): status = GETPASS
03:13:02: AAA/AUTHEN (2289801324): Method=radius (radius)
03:13:02: RADIUS: ustruct sharecount=2
03:13:02: RADIUS: Initial Transmit ISAKMP id 29 172.18.124.114:1645,
   Access-Request, len 68
03:13:02:         Attribute 4 6 0A0D0130
03:13:02:         Attribute 61 6 00000000
03:13:02:         Attribute 1 6 7A656B65
03:13:02:         Attribute 31 12 39392E39
03:13:02:         Attribute 2 18 D687A79D
03:13:02: RADIUS: Received from id 29 172.18.124.114:1645,
   Access-Accept, Len 26
03:13:02:         Attribute 6 6 00000005
03:13:02: RADIUS: saved authorization data for user 6269AD80
   at 62634D0C
03:13:02: AAA/AUTHEN (2289801324): status = PASS
03:13:02: ISAKMP: got callback 1
03:13:02: CryptoEngine0: generate hmac context for conn id 1
03:13:02: ISAKMP (0:1): initiating peer config to 99.99.99.5.
```

```
   ID = -280774539
03:13:02: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH
03:13:03: ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_XAUTH
03:13:03: ISAKMP (0:1): processing transaction payload from 99.99.99.5.
   Message ID = -280774539
03:13:03: CryptoEngine0: generate hmac context for conn id 1
03:13:03: ISAKMP: Config payload ACK
03:13:03: ISAKMP (0:1): deleting node -280774539 error FALSE
   reason "done with transaction"
03:13:03: ISAKMP (0:1): allocating address 10.2.1.2
03:13:03: CryptoEngine0: generate hmac context for conn id 1
03:13:03: ISAKMP (0:1): initiating peer config to 99.99.99.5.
   ID = 2130856112
03:13:03: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_ADDR
03:13:03: ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_ADDR
03:13:03: ISAKMP (0:1): processing transaction payload
   from 99.99.99.5. Message ID = 2130856112
03:13:03: CryptoEngine0: generate hmac context for conn id 1
03:13:03: ISAKMP: Config payload ACK
03:13:03: ISAKMP (0:1): peer accepted the address!
03:13:03: ISAKMP (0:1): adding static route for 10.2.1.2
03:13:03: ISAKMP (0:1): installing route 10.2.1.2 255.255.255.255
   99.99.99.5
03:13:03: ISAKMP (0:1): deleting node 2130856112 error FALSE
   reason "done with transaction"
03:13:03: ISAKMP (0:1): Delaying response to QM request.
03:13:04: ISAKMP (0:1): received packet from 99.99.99.5 (R) QM_IDLE
03:13:04: ISAKMP (0:1): (Re)Setting client xauth list xauth_list
   and state
03:13:04: CryptoEngine0: generate hmac context for conn id 1
03:13:04: ISAKMP (0:1): processing HASH payload. Message ID = -1651205463
03:13:04: ISAKMP (0:1): processing SA payload. Message ID = -1651205463
03:13:04: ISAKMP (0:1): Checking IPSec proposal 1
03:13:04: ISAKMP: transform 1, ESP_DES
03:13:04: ISAKMP:   attributes in transform:
03:13:04: ISAKMP:      authenticator is HMAC-MD5
03:13:04: ISAKMP:      encaps is 1
03:13:04: validate proposal 0
03:13:04: ISAKMP (0:1): atts are acceptable.
03:13:04: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 99.99.99.1, src= 99.99.99.5,
    dest_proxy= 10.13.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.1.2/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= ESP-Des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
03:13:04: validate proposal request 0
03:13:04: ISAKMP (0:1): processing NONCE payload.
   Message ID = -1651205463
03:13:04: ISAKMP (0:1): processing ID payload.
   Message ID = -1651205463
03:13:04: ISAKMP (1): ID_IPV4_ADDR src 10.2.1.2 prot 0 port 0
03:13:04: ISAKMP (0:1): processing ID payload.
   Message ID = -1651205463
03:13:04: ISAKMP (1): ID_IPV4_ADDR_SUBNET dst 10.13.1.0/255.255.255.0
   port 0 port 0
03:13:04: ISAKMP (0:1): asking for 1 spis from ipsec
03:13:04: IPSEC(key_engine): got a queue event...
03:13:04: IPSEC(spi_response): getting spi 570798685 for SA
        from 99.99.99.5      to 99.99.99.1      for prot 3
03:13:04: ISAKMP: received ke message (2/1)
03:13:04: CryptoEngine0: generate hmac context for conn id 1
03:13:04: ISAKMP (0:1): sending packet to 99.99.99.5 (R) QM_IDLE
03:13:04: ISAKMP (0:1): received packet from 99.99.99.5 (R) QM_IDLE
```

```
03:13:04: CryptoEngine0: generate hmac context for conn id 1
03:13:04: ipsec allocate flow 0
03:13:04: ipsec allocate flow 0
03:13:04: ISAKMP (0:1): Creating IPSec SAs
03:13:04:         inbound SA from 99.99.99.5 to 99.99.99.1
        (proxy 10.2.1.2 to 10.13.1.0)
03:13:04:         has spi 0x2205B25D and conn_id 2000 and flags 4
03:13:04:         outbound SA from 99.99.99.1 to 99.99.99.5
   (proxy 10.13.1.0 to 10.2.1.2)
03:13:04:         has spi -1338747879 and conn_id 2001 and flags 4
03:13:04: ISAKMP (0:1): deleting node -195511155 error FALSE
   reason "saved qm no longer needed"
03:13:04: ISAKMP (0:1): deleting node -1651205463 error FALSE
   reason "quick mode done (await()"
03:13:04: IPSEC(key_engine): got a queue event...
03:13:04: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 99.99.99.1, src= 99.99.99.5,
    dest_proxy= 10.13.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.1.2/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x2205B25D(570798685), conn_id= 2000,
    keysize= 0, flags= 0x4
03:13:04: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 99.99.99.1, dest= 99.99.99.5,
    src_proxy= 10.13.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.2.1.2/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xB0345419(2956219417), conn_id= 2001,
    keysize= 0, flags= 0x4
03:13:04: IPSEC(create_sa): sa created,
  (sa) sa_dest= 99.99.99.1, sa_prot= 50,
    sa_spi= 0x2205B25D(570798685),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
03:13:04: IPSEC(create_sa): sa created,
  (sa) sa_dest= 99.99.99.5, sa_prot= 50,
    sa_spi= 0xB0345419(2956219417),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
03:13:04: ISAKMP: received ke message (4/1)
03:13:04: ISAKMP: Locking struct 6269C36C for IPSEC
03:13:05: IPSEC(decapsulate): error in decapsulation
   crypto_ipsec_sa_exists
```

相關資訊

- Cisco VPN使用者端支援頁面
- IPSec協商/IKE通訊協定支援頁面
- 終端存取控制器存取控制系統(TACACS+)支援頁面
- 遠端驗證撥入使用者服務(RADIUS)支援頁面
- 要求建議
- 技術支援與文件 - Cisco Systems