为 VPN 客户端配置 TACACS+ 与 RADIUS 扩展认证

目录

简介

本文档显示 TACACS+ 和 RADIUS Internet 工程任务组 (IETF) 扩展身份验证 (Xauth) 的配置示例。Xauth 允许您在 Internet Key Exchange (IKE) 协议内，使用 TACACS+ 或 RADIUS 作为用户身份验证方法，在虚拟私有网络 (VPN) 上部署 IP Security (IPSec)。此功能允许对已在 PC 上安装 CiscoSecure VPN 客户端 1.1 的用户进行身份验证，具体方法是：先提示用户输入用户名和口令，然后使用身份验证、授权和记帐 (AAA) 服务器、TACACS+ 或 RADIUS 数据库中存储的信息对其进行验证。身份验证发生在 IKE 第 1 阶段与 IKE 第 2 阶段之间。如果用户成功地进行了身份验证，则会建立第 2 阶段安全连接 (SA)，然后即可安全地将数据发送至受保护的网络。

Xauth 仅包括*身份验证*，不包括*授权*（用户可以在建立连接之后离开）。未实现*记帐*（用户已离开）。

在实现 Xauth 之前，配置必须在没有 Xauth 的情况下工作。我们的示例展示的是除 Xauth 之外的模式配置 (Mode Config) 和网络地址转换 (NAT)，但是会假定在添加 Xauth 命令之前已存在 IPSec 连接。

请确保在尝试 TACACS+ 或 RADIUS Xauth 之前，本地 Xauth（路由器的用户名/口令) 有效。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- VPN 客户端版本 1.1（或更高版本）
- Cisco IOS版本12.1.2.2.T， 12.1.2.2.P (或以上)
- RADIUS 身份验证使用运行 c3640-jo3s56i-mz.121-2.3.T 的 Cisco 3640 进行测试

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

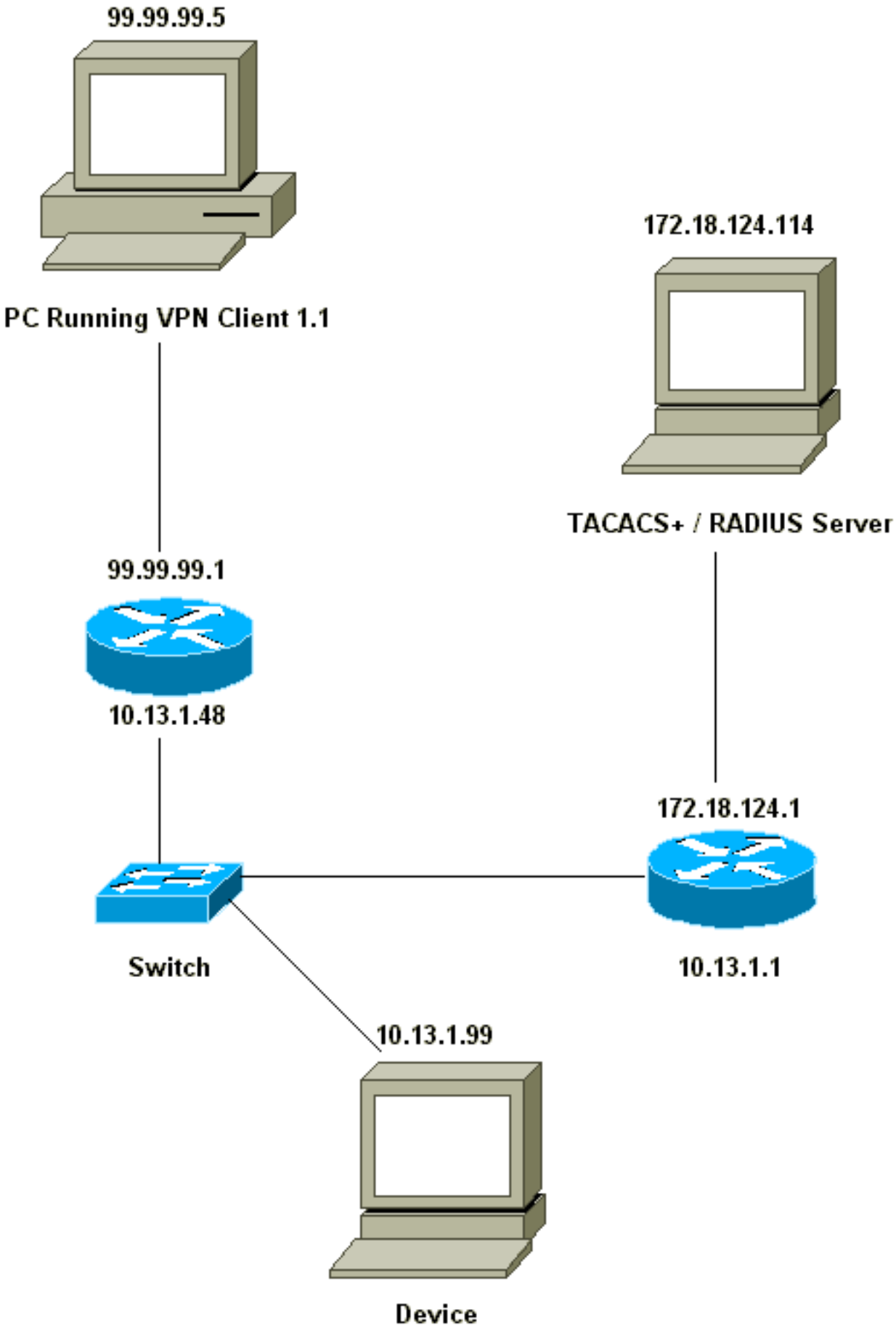
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



VPN Client 1.1 安装

```
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
```

在路由器上启用 Xauth 之后，当用户尝试连接至路由器中的设备时（此处我们执行 ping -t #.#.#.#），会出现灰色的画面：

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

配置

服务器配置

Xauth 身份验证既可以由 TACACS+ 也可以由 RADIUS 完成。我们要确保允许 Xauth 用户执行 Xauth，但是不允许他们远程登录到路由器。因此，我们添加了 **aaa authorization exec** 命令。我们为 RADIUS 用户设置了“reply-attribute Service-Type=Outbound=5”（而不是管理或登录）。在 CiscoSecure UNIX 中为“Outbound”；在 CiscoSecure NT 中为“Dialout Framed”。如果是 TACACS+ 用户，则不会为其提供 shell/exec 权限。

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
```

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug aaa authentication** - 显示 AAA/TACACS+ 身份验证的信息。
- **debug crypto isakmp** — 显示关于 IKE 事件的消息。
- **debug crypto ipsec** — 显示 IPSec 事件。
- **debug crypto key-exchange** - 显示数字签字标准 (DSS) 公钥交换消息。
- **debug radius** - 显示与 RADIUS 相关的信息。
- **debug tacacs** - 显示与 TACACS 相关的信息。
- **clear crypto isakmp** - 指定要清除的连接。
- **clear crypto sa** - 删除 IPsec 安全连接。

调试输出示例

注意： TACACS+ 调试非常类似。请使用 **debug tacacs+** 命令，而非 **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
```

相关信息

- Cisco VPN 客户端支持页
- IPsec 协商/IKE 协议支持页
- 终端访问控制器访问控制系统 (TACACS+) 支持页
- Remote Authentication Dial-In User Service (RADIUS) 支持页
- 请求注释
- 技术支持和文档 - Cisco Systems