为Cisco Secure VPN Client配置使用RADIUS服务器的IKE预先共享密钥

目录

简介
先决条件
要求
使用的组件
规则
配置
网络图
创建 Cisco Secure 配置文件
配置路由器
配置客户端
验证
故障排除
相关信息

简介

本文档介绍如何使用 RADIUS 服务器来配置 Internet Key Exchange (IKE) 共享密钥。通过使用身份验证、授权和记帐 (AAA) 服务器的 IKE 共享密钥功能，可以从 AAA 服务器进行密钥查找。在不通过证书颁发机构 (CA) 部署大型 VPN 系统时，预共享密钥无法很好地扩展。使用动态 IP 编址（如动态主机配置协议 (DHCP) 或点对点协议 (PPP) 拨号）时，不断更改的 IP 地址可能会导致很难或无法进行密钥查找，除非使用通配符预共享密钥。在使用 AAA 服务器的 IKE 共享密钥功能中，在 IKE 协商的主动模式期间，将通过 AAA 服务器来访问共享密钥。如果在用户正尝试连接的 Cisco IOS® 路由器上找不到本地密钥，则将交换 ID 用作用户名来查询 AAA。此功能是在 Cisco IOS 软件版本 12.1.T 中引入的。必须在 VPN 客户端上启用主动模式才能使用此功能。

先决条件

要求

必须在 VPN 客户端上启用主动模式，并且必须在路由器上运行 Cisco IOS 软件版本 12.1.T 或更高版本。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Secure ACS for Windows

- Cisco IOS 软件版本 12.2.8T
- Cisco 1700 路由器

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

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

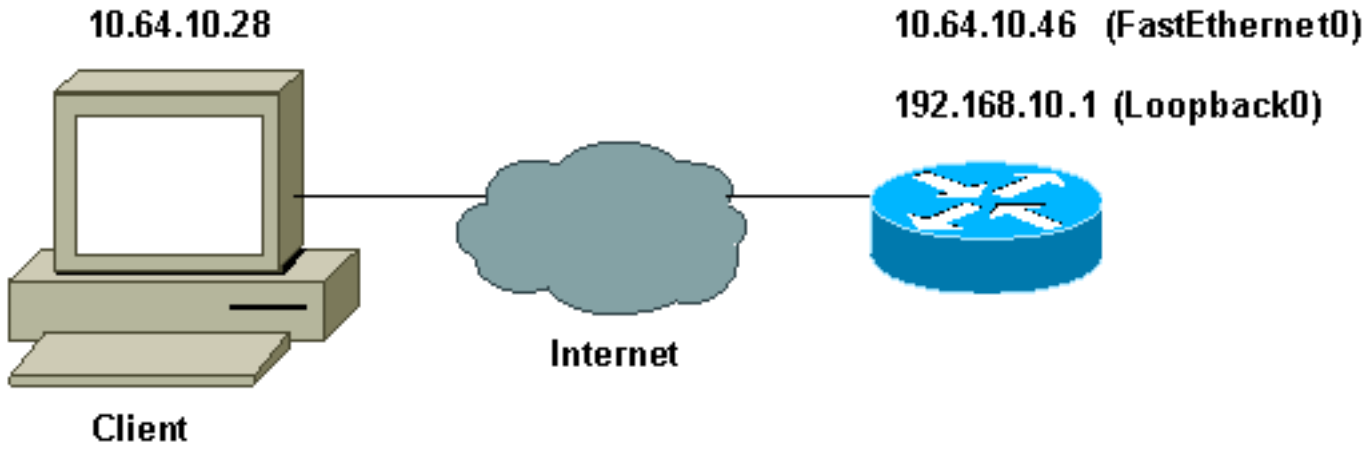
本文档使用如下所示的配置。

- 创建 Cisco Secure 配置文件
- 配置路由器
- 配置客户端

注意： 要查找本文档所用命令的其他信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用以下网络设置：



创建 Cisco Secure 配置文件

此配置文件是使用 UNIX 创建的，但也可在 Cisco Secure ACS for Windows 上创建类似配置文件。

```
# ./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
```

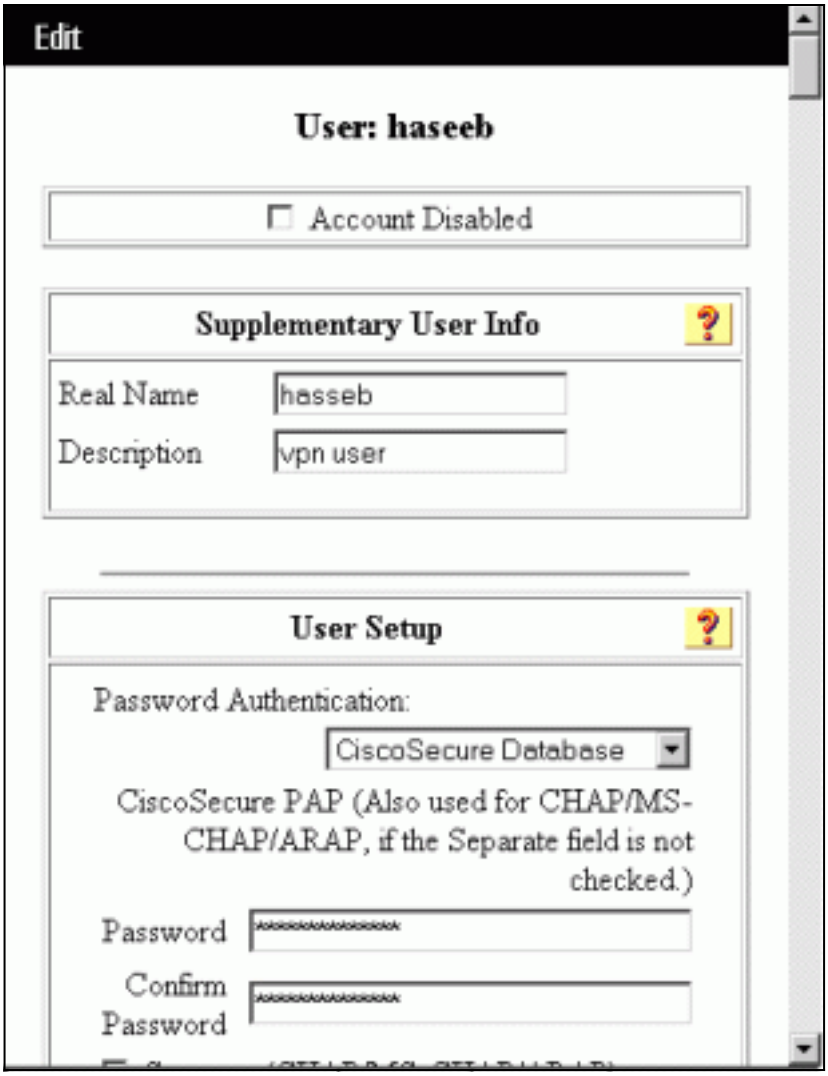
```
!--- Pre-shared key. 9,1="ipsec:tunnel-password=secret12345"
9,1="ipsec:key-exchange=ike"
}
}

}
```

下面的输出显示了用于在 Cisco Secure ACS for UNIX 中添加用户配置文件的脚本。

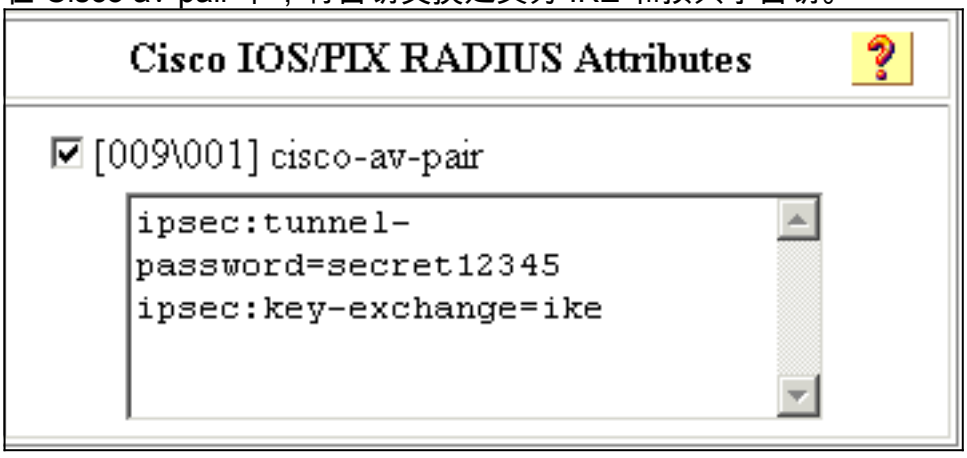
```
# ./ViewProfile -p 9900 -u haseeb
User Profile Information
!--- The user name is sent by the VPN Client; !--- look at the client configuration. user =
haseeb{

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"
}
}

}
```

按照以下步骤操作以使用 GUI 在 Cisco Secure ACS for Windows 2.6 中配置用户配置文件。

1. 定义用户名，并将“cisco”用作口令。



2. 在 Cisco av-pair 下，将密钥交换定义为 IKE 和预共享密钥。



配置路由器

带有 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
!
```

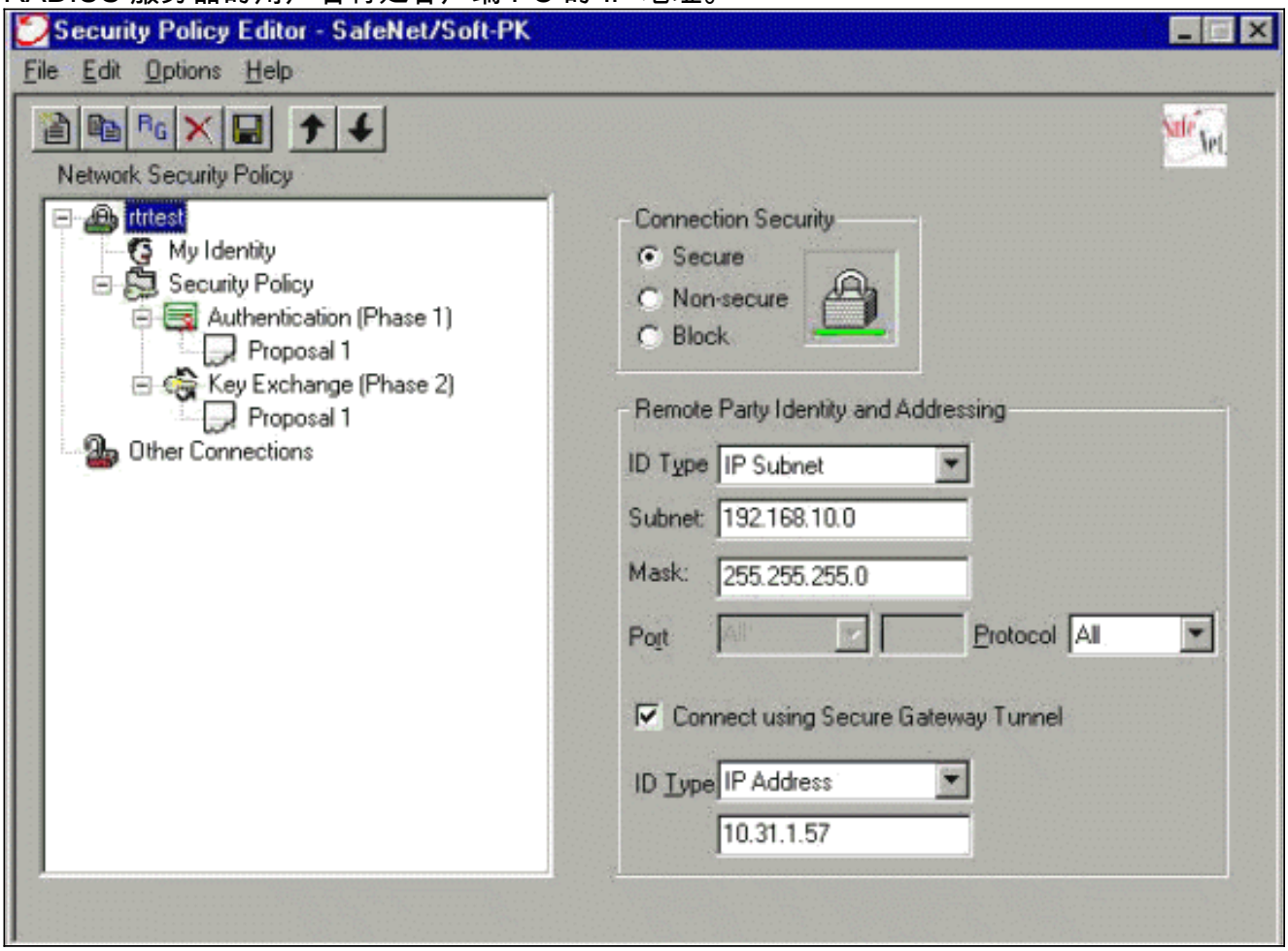
```
!
aaa authentication login default none
!--- Configure authorization. aaa authorization network
vpn_users group radius
aaa session-id common
!
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
no ip domain-lookup
!
!--- Define IKE 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
```

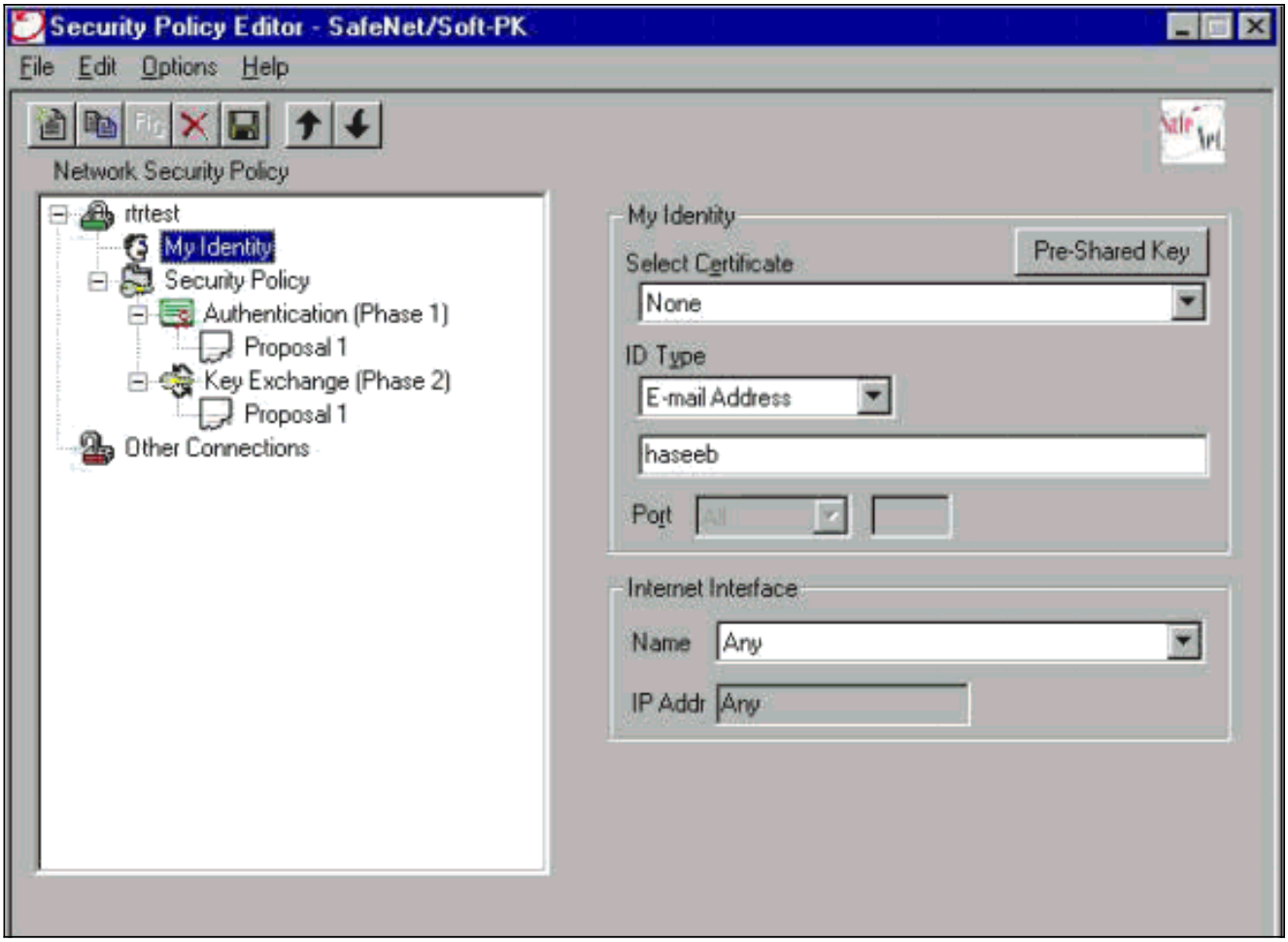
配置客户端

按照以下步骤操作以配置客户端。

1. 在安全策略编辑器中，转至 **Network Security Policy > rtrtest**。选择 **ID Type** 作为电子邮件地址并放入要在 RADIUS 服务器上配置的用户名。如果将此设置保留为“IP 地址”，则发送到 RADIUS 服务器的用户名将是客户端 PC 的 IP 地址。



2. 转至 **Network Security Policy > rtrtest > My Identity**，然后选择 **Aggressive Mode**。如果未选择此模式，则该设置将不起作用。



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。

下面的输出显示了此配置的成功调试：

```
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
```

相关信息

- RADIUS 支持页
- Cisco Secure ACS for Windows 支持页
- Cisco Secure ACS for UNIX 支持页
- IPSec 支持页面

- 请求注解 (RFC)
- 技术支持 - Cisco Systems