Configurando chaves IKE pré-compartilhadas com um servidor RADIUS para o cliente VPN do Cisco Secure

Índice

Introdução

Este documento descreve como configurar o segredo compartilhado do Internet Key Exchange (IKE) usando o servidor RADIUS. A característica do segredo compartilhado de IKE que usa um server do Authentication, Authorization, and Accounting (AAA) permite a consulta chave do servidor AAA. As chaves pré-compartilhada não escalam bem quando você distribui um sistema de VPN em grande escala sem um Certification Authority (CA). Ao usar o IP dinâmico que endereça como tratamentos por imagens do protocolo de configuração dinâmica host (DHCP) ou do Point-to-Point Protocol (PPP), o endereço IP de Um ou Mais Servidores Cisco ICM NT em mudança pode fazer a consulta chave difícil ou impossível a menos que uma chave pré-compartilhada do convite for usada. No recurso de segredo compartilhado IKE que usa um servidor AAA, o segredo compartilhado é acessado durante o modo agressivo de negociação IKE por meio do servidor AAA. A ID da troca é utilizada como o nome de usuário para consultar AAA se nenhuma chave local puder ser encontrada no roteador Cisco IOS® ao qual o usuário está tentando se conectar. Isto foi introduzido no Cisco IOS Software Release 12.1.T. Você deve ter o modo assertivo habilitado no VPN Client para usar este recurso.

Pré-requisitos

Requisitos

Você deve ter o modo assertivo permitido no cliente VPN, e você deve ser Cisco IOS Software Release 12.1.T running ou mais tarde o roteador.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure ACS for Windows
- Cisco IOS Software Release 12.2.8T
- Cisco 1700 Router

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configurar

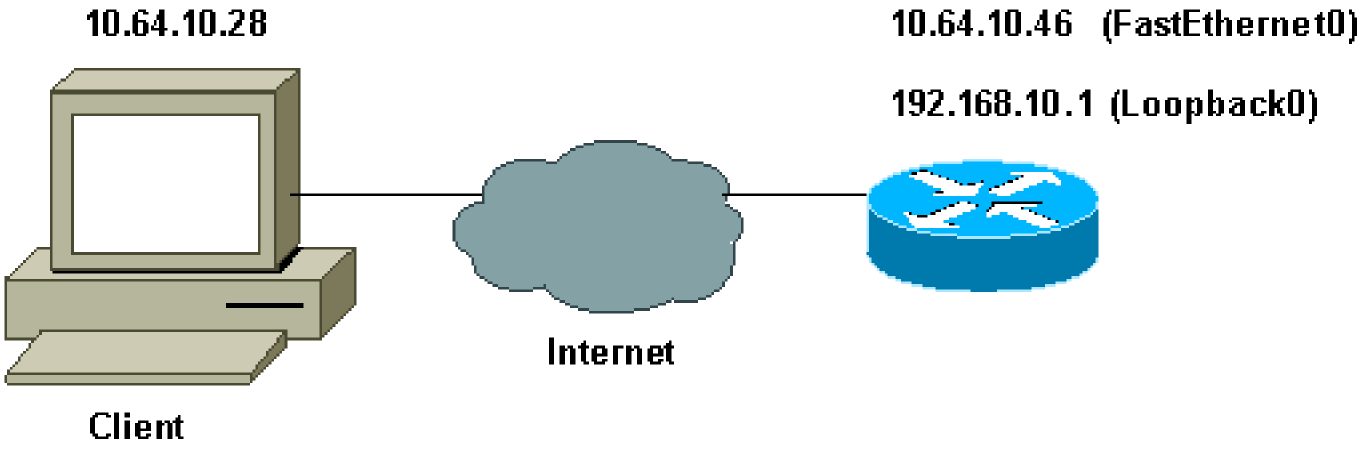
Este documento utiliza as configurações mostradas abaixo.

- Criando um perfil do Cisco Secure
- Configurando o Roteador
- Configurando o cliente

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes registrados).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Criando um perfil do Cisco Secure

Este perfil foi criado com UNIX, mas um perfil similar pode ser criado no Cisco Secure ACS for 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= {
6=5
64=9
65=1
!--- Pre-shared key. 9,1="ipsec:tunnel-password=secret12345"
9,1="ipsec:key-exchange=ike"
}
}

}
```

Esta saída mostra o script que é usada para adicionar um perfil de usuário no Cisco Secure ACS para UNIX.

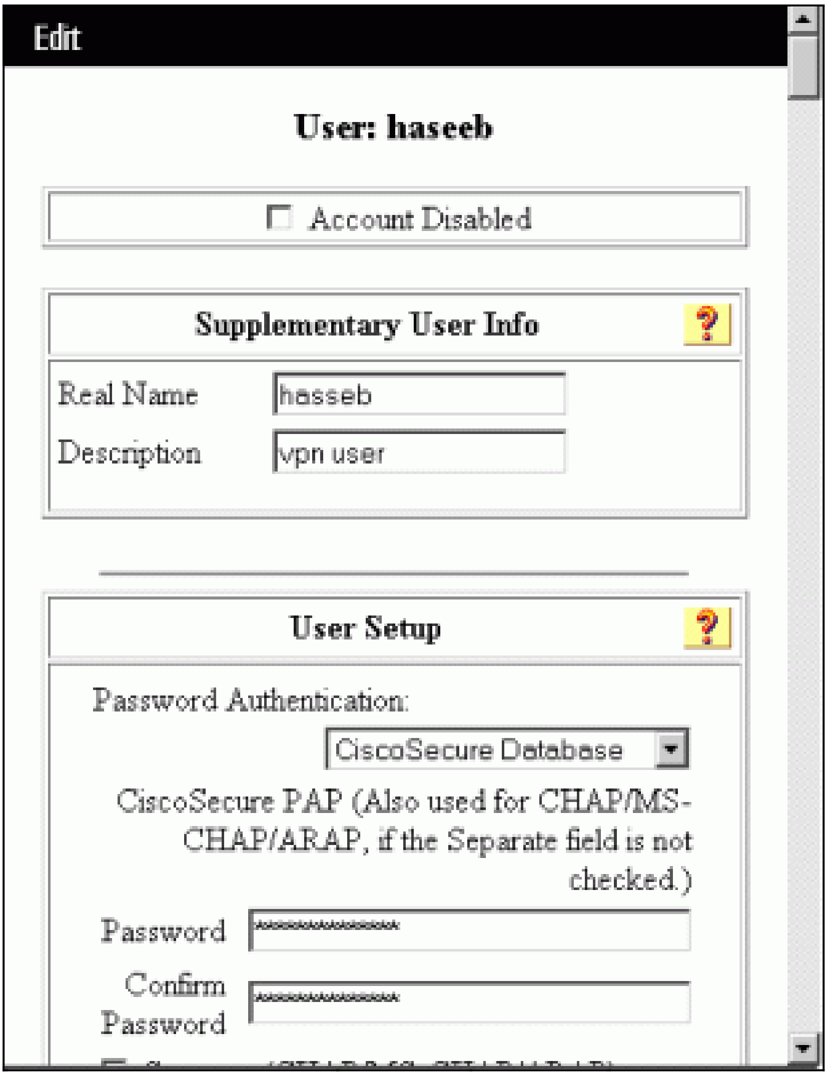
```
# ./ViewProfile -p 9900 -u haseeb
User Profile Information
!--- The user name is sent by the VPN Client; !--- look at the client configuration. user =
haseeb{

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"
}
}

}
```

Siga estas etapas para usar o GUI para configurar o perfil de usuário no Cisco Secure ACS for Windows 2.6.

1. Defina o nome do usuário, com "cisco" como a



User: haseeb

□ Account Disabled

Supplementary User Info

Real Name: hasseb

Description: vpn user

User Setup

Password Authentication: CiscoSecure Database

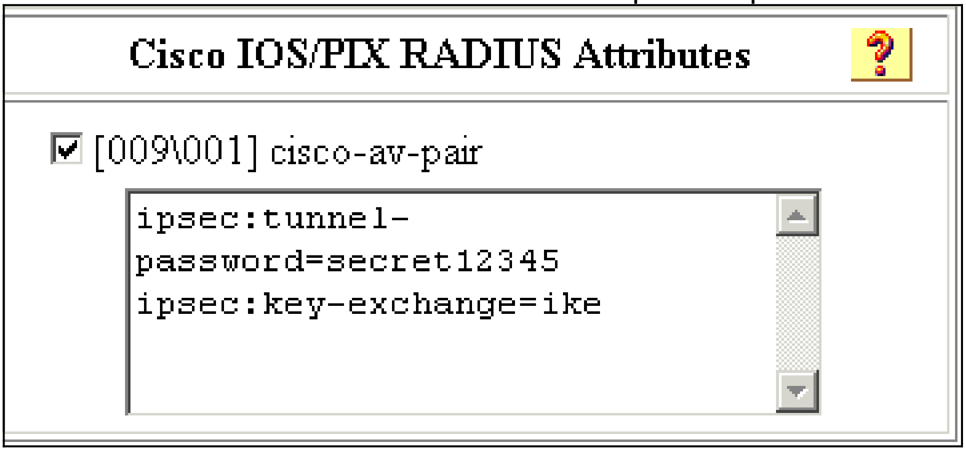
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

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

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

senha.

2. Defina o intercâmbio chave como IKE e a chave pré-compartilhada no Cisco av-



Cisco IOS/PIX RADIUS Attributes

☑ [009\001] cisco-av-pair

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

pair.

Configurando o Roteador

Cisco 1751 com IO 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
!
```

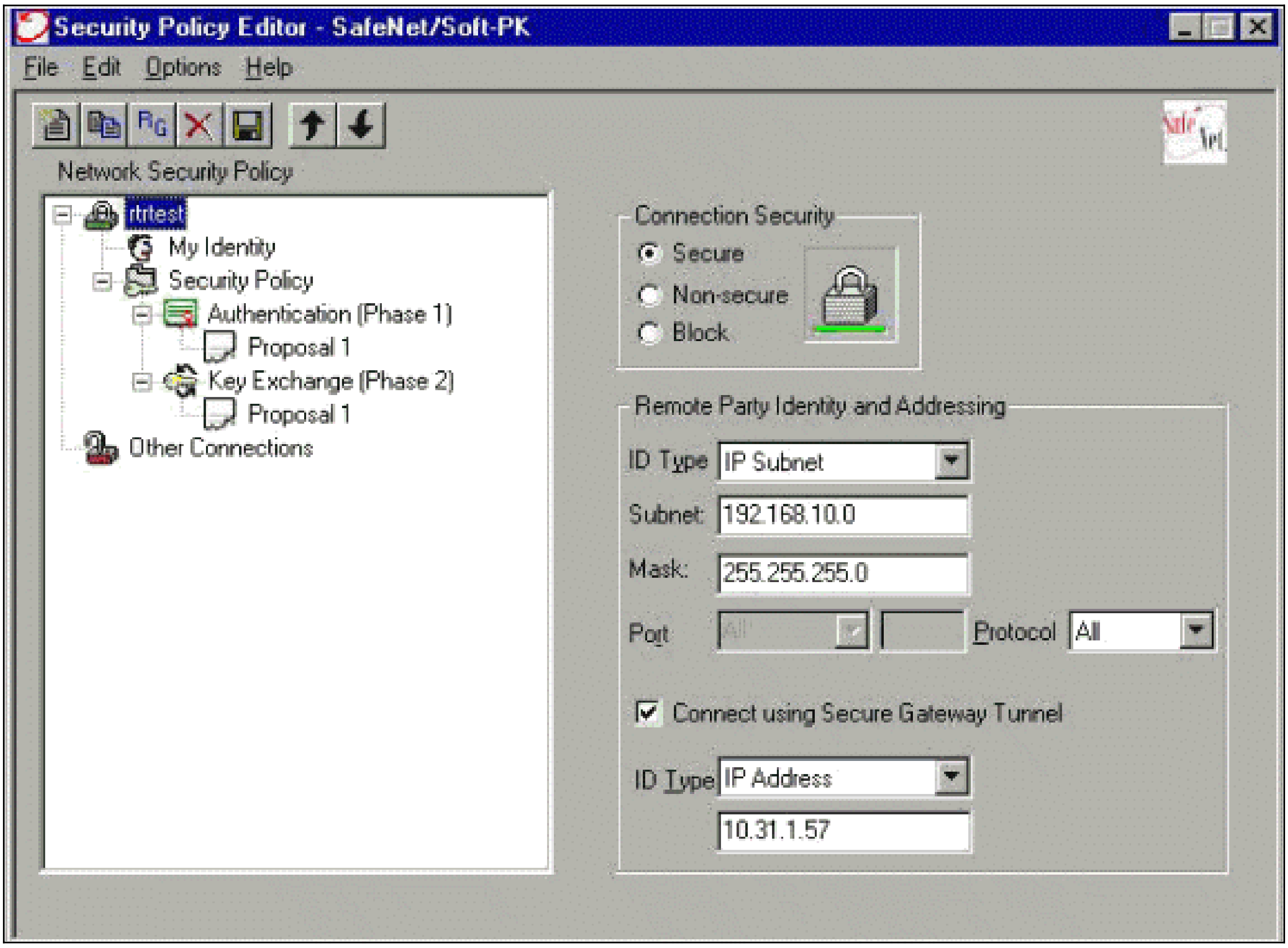
```
!
aaa authentication login default none
!--- Configure authorization. aaa authorization network
vpn_users group radius
aaa session-id common
!
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
no ip domain-lookup
!
!--- Define IKE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

Configurando o cliente

Siga estas etapas para configurar o cliente.

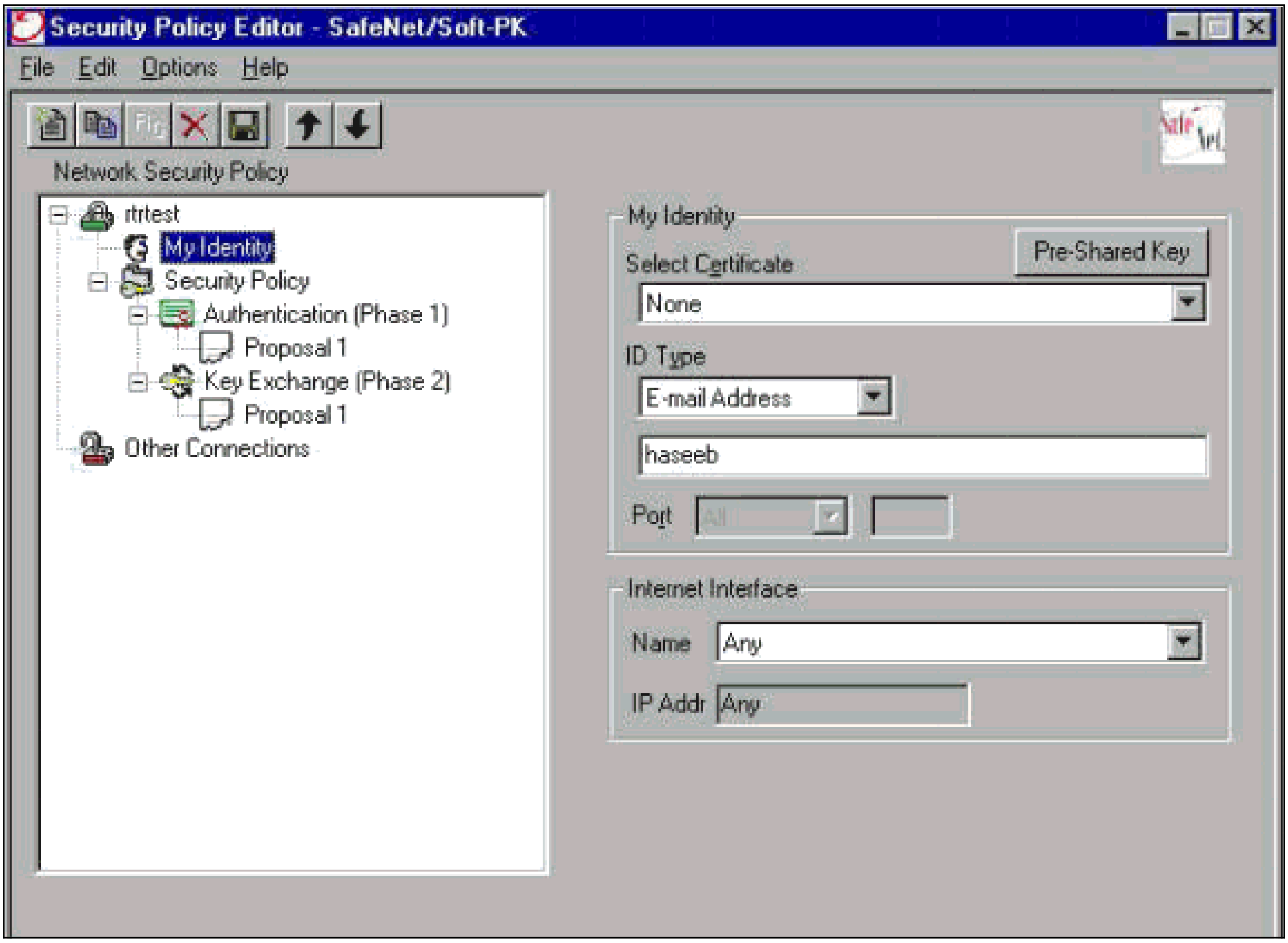
1. No editor da política de segurança, vá a **Network Security Policy > rtrtest**. Selecione o **tipo ID** como um endereço email e põe-no em um nome de usuário a ser configurado no servidor Radius. Se essa configuração for deixada como "Endereço IP", o nome do usuário enviado para o servidor RADIUS será o endereço IP do PC cliente.



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. Vá ao **política de segurança de rede > teste de rtr > minha identidade** e selecione o **modo assertivo**. A configuração não funcionará se esse modo não for selecionado.



My Identity

Select Certificate: None

ID Type: E-mail Address

haseeb

Port: All

Internet Interface

Name: Any

IP Addr: Any

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Esta saída mostra debug correto para esta configuração:

```
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
```

Informações Relacionadas

- Página de suporte RADIUS
- Cisco Secure ACS para página de suporte do Windows
- Cisco Secure ACS para página de suporte do UNIX

- Página de suporte do IPSec
- Solicitações de Comentários (RFCs)
- Suporte Técnico - Cisco Systems