

Configurando o Cisco VPN Client 3.x para Windows aos IO usando a autenticação estendida local

Índice

[Introdução](#)

[Antes de Começar](#)

[Convenções](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Habilitando a divisão de túnel](#)

[Verificar](#)

[Troubleshooting](#)

[Registros de Cliente](#)

[Informações Relacionadas](#)

Introdução

Este documento demonstra como configurar uma conexão entre um roteador que usa a autenticação estendida local e o Cisco VPN Client. Cisco IOS® Software Releases 12.2(15)T2 e versões posteriores suportam conexões do Cisco VPN Client 3.x. O VPN Client 3.x usa a política de grupo 2 Diffie Hellman (DH). O comando `isakmp policy # group 2` permite que os clientes 3.x se conectem.

Para obter informações sobre de configurar estes dispositivos usando o Cisco Secure VPN Client 1.1, veja [configurar o Cisco Secure VPN Client 1.1 para Windows aos IO usando a autenticação estendida local](#).

Refira o [túnel de IPsec entre o IOS Router e o Cisco VPN Client 4.x para Windows com exemplo de configuração da autenticação de usuário TACACS+](#) a fim aprender mais sobre a encenação onde a autenticação de usuário ocorre externamente com protocolo TACACS+.

Refira [configurar o IPsec entre um roteador do Cisco IOS e um Cisco VPN Client 4.x para Windows usando o RAIO para a autenticação de usuário](#) a fim aprender mais sobre a encenação onde a autenticação de usuário ocorre externamente com protocolo de raio.

Antes de Começar

Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Pré-requisitos

Antes de tentar utilizar esta configuração, verifique se os seguintes pré-requisitos são atendidos:

- um conjunto de endereço a ser atribuído para a Segurança IP (IPsec)
- um usuário local no IOS Router com o **Cisco** como o nome e o **Cisco** como a senha
- um grupo chamou **3000clients** com **cisco123** da senha

Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware abaixo.

- um 3640 Router que executa 12.2(15)T2
- Cisco VPN Client para Windows versão 3.5 (qualquer VPN Client 3.x deve funcionar)

A saída do comando show version no roteador é mostrada abaixo.

```
3640#show version
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-JK9O3S-M), Version 12.2(15)T2,
    RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 30-Apr-03 05:42 by nmasa
Image text-base: 0x60008950, data-base: 0x6202E000

ROM: System Bootstrap, Version 11.1(20)AA2,
    EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
```

```
3640 uptime is 21 hours, 29 minutes
System returned to ROM by reload
System image file is "flash:c3640-jk9o3s-mz.122-15.T2.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

cisco 3640 (R4700) processor (revision 0x00)

with 126976K/4096K bytes of memory.
Processor board ID 22789386
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2 Ethernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)
16384K bytes of processor board PCMCIA Slot0 flash (Read/Write)

Configuration register is 0x102

3640#

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.

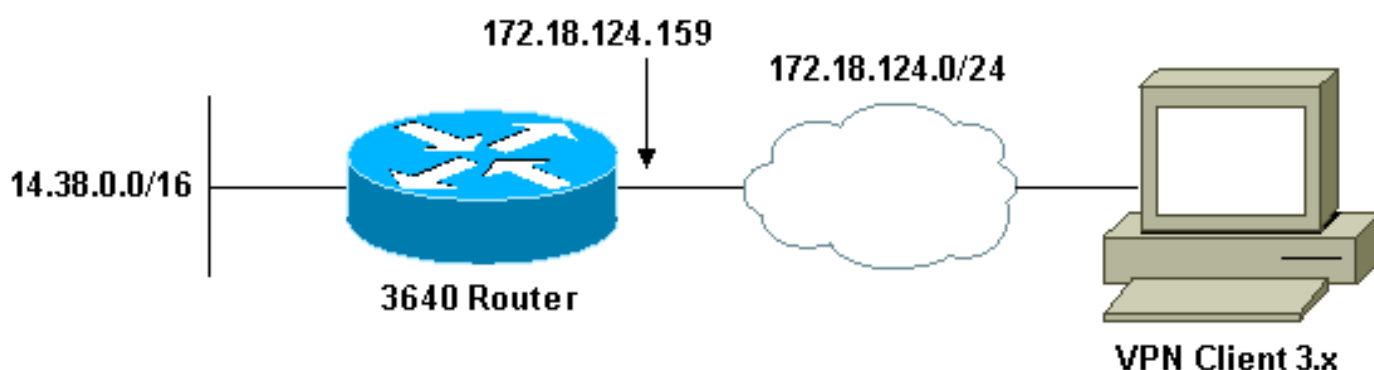
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Note: 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 instalação de rede mostrada no diagrama abaixo.



Configurações

Este documento utiliza as configurações mostradas abaixo.

- [Configurando o roteador 3640](#)
- [Configurando o VPN Client 3.x](#)

Configurando o roteador 3640

3640 Router

```
3640#show run
Building configuration...

Current configuration : 1884 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3640
!
!--- Enable Authentication, Authorizing and Accounting (AAA) !-- for user authentication and group authorization. aaa new-model
aaa new-model
!
!--- To enable X-Auth for user authentication, !-- enable the aaa authentication commands.
aaa authentication login userauthen local
!
!--- To enable group authorization, !-- enable the aaa authorization commands.
aaa authorization network groupauthor local
!
!--- For local authentication of the IPSec user, !-- create the user with password. username cisco password 0 cisco
username cisco password 0 cisco
!
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
!--- Create an Internet Security Association and !-- Key Management Protocol (ISAKMP) policy for Phase 1 negotiations. crypto isakmp policy 3
crypto isakmp policy 3
  encr 3des
  authentication pre-share
  group 2
!
!--- Create a group that will be used to specify the !-- Windows Internet Naming Service (WINS) and !-- Domain Naming Service (DNS) server addresses to the client, !-- along with the pre-shared key for authentication.
crypto isakmp client configuration group 3000client
  key cisco123
  dns 14.1.1.10
  wins 14.1.1.20
  domain cisco.com
  pool ippool
!
!--- Create the Phase 2 Policy for actual data encryption. crypto ipsec transform-set myset esp-3des esp-sha-hmac
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
!--- Create a dynamic map and !-- apply the transform set that was created above. crypto dynamic-map dynmap 10
crypto dynamic-map dynmap 10
```

```
set transform-set myset
!
!--- Create the actual crypto map, !--- and apply the
aaa lists that were created earlier. crypto map
clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor
crypto map clientmap client configuration address
respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
!
!--- Apply the crypto map on the outside interface.
interface Ethernet0/0 ip address 172.18.124.159
255.255.255.0
half-duplex
crypto map clientmap
!
interface Serial10/0
no ip address
shutdown
!
interface Ethernet0/1
ip address 14.38.100.201 255.255.0.0
no keepalive
half-duplex
!
interface Serial11/0
no ip address
shutdown
!
interface Serial11/1
no ip address
shutdown
!
interface Serial11/2
no ip address
shutdown
!
interface Serial11/3
no ip address
shutdown
!
interface Serial11/4
no ip address
shutdown
!
interface Serial11/5
no ip address
shutdown
!
interface Serial11/6
no ip address
shutdown
!
interface Serial11/7
no ip address
shutdown
!
```

```
!--- Create a pool of addresses to be assigned to the
VPN Clients. ip local pool ippool 14.1.1.100 14.1.1.200
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
ip http server
ip pim bidir-enable
!
!
!
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
!
!
end
3640#
```

[Configurando o VPN Client 3.x](#)

Esta seção mostra como configurar o cliente VPN 3.x.

1. Lance o cliente VPN, a seguir clique-o **novo** para criar uma nova



conexão.

2. Quando solicitado, atribua um nome para sua entrada. Você pode inserir também uma descrição se desejar. Clique em "Avançar" quando terminar.

New Connection Entry Wizard

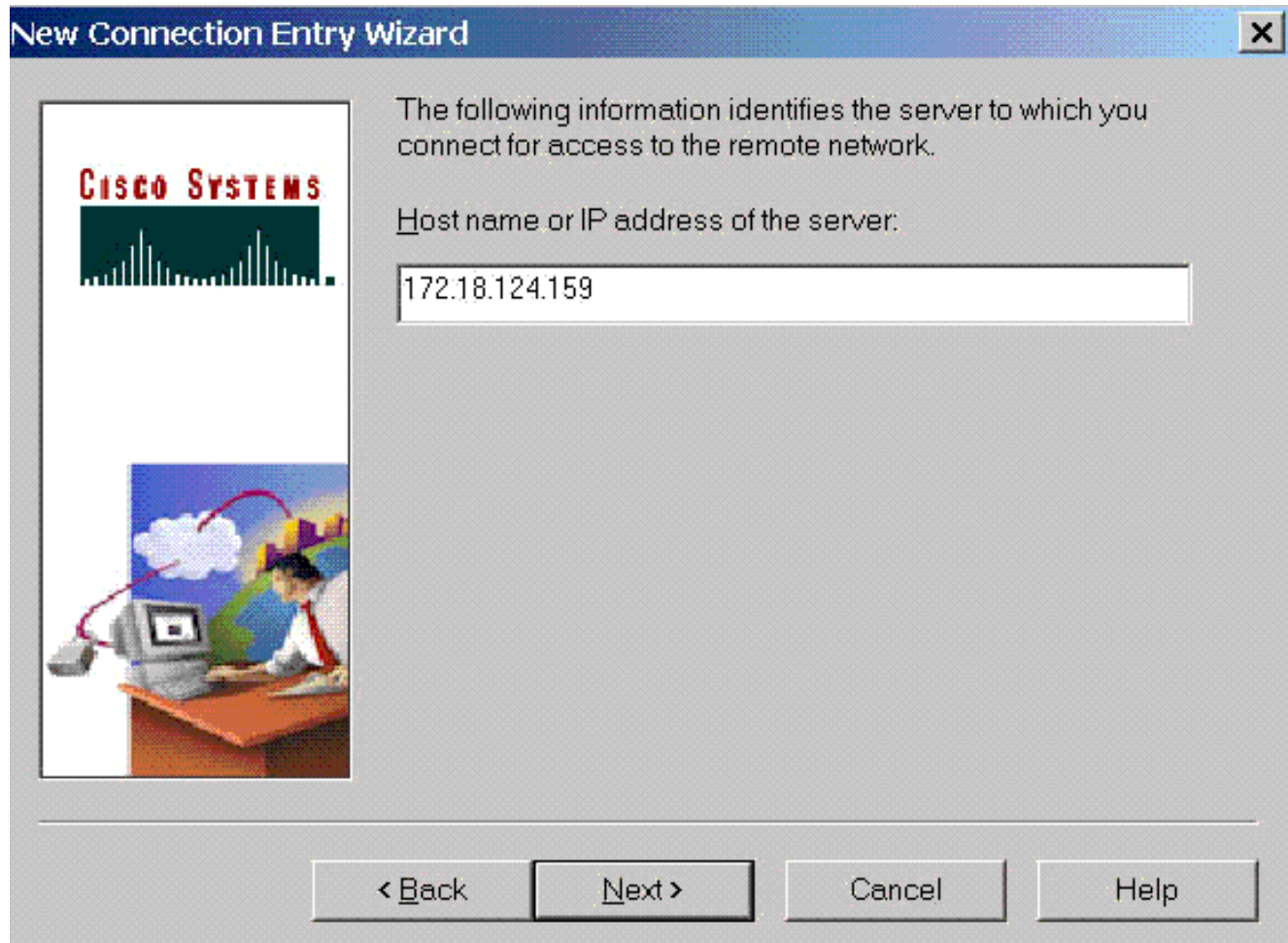


The VPN Client lets you create secure connections to remote networks. This wizard helps you create a connection entry for connecting to a specific remote network.

Name of the new connection entry:

Description of the new connection entry (optional):

3. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface pública do roteador. Clique em “Avançar” quando terminar.



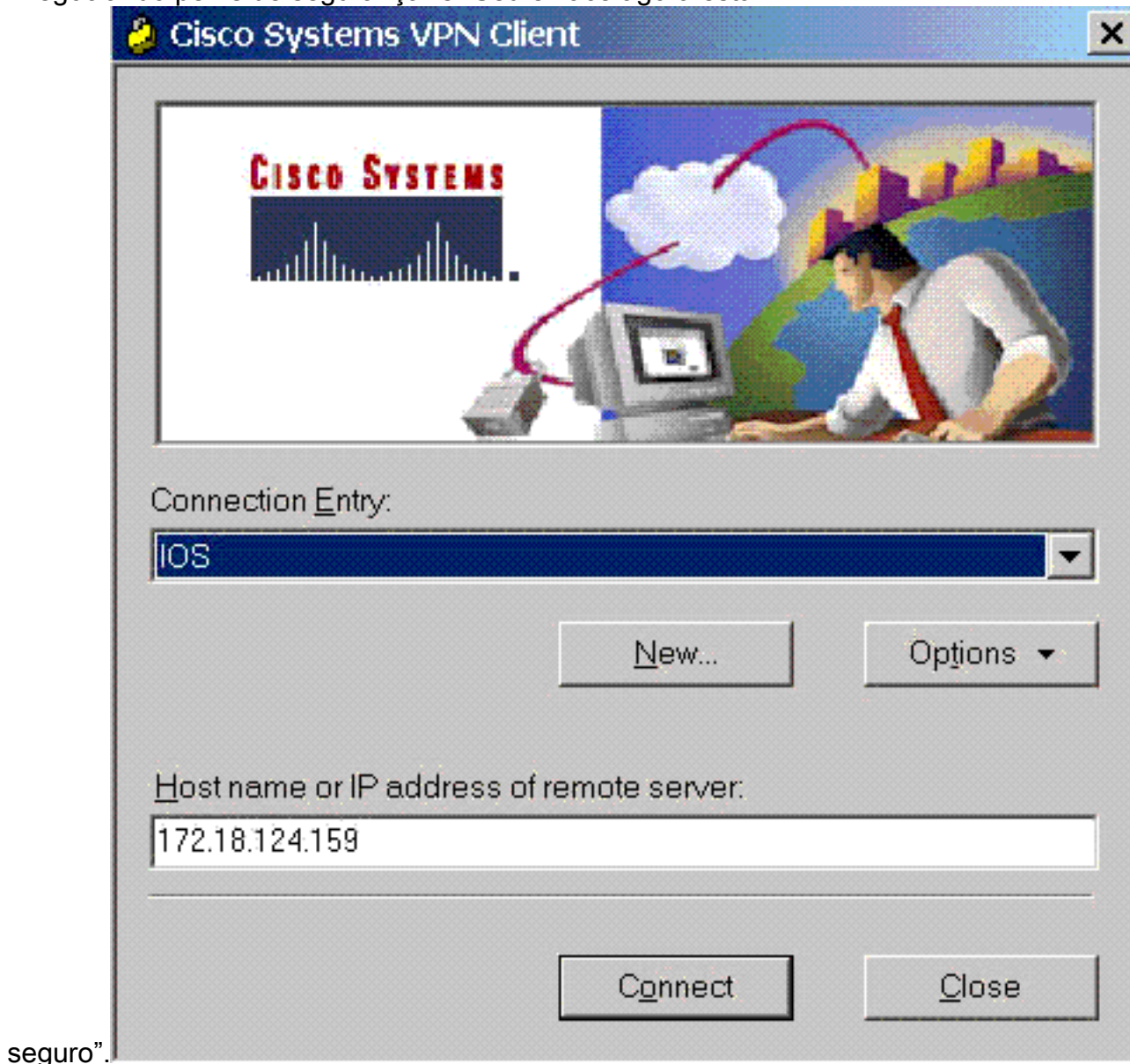
4. Em Group Access Information, digite o nome do grupo e a senha. O exemplo abaixo mostra um grupo com o nome "3000client" e senha "cisco123". Confirme a senha, a seguir clique-a **ao lado de** **continuar**.



5. Clique em Encerrar para salvar o perfil no registro.



6. Clique em Connect para se conectar ao roteador. A janela exibirá mensagens de “Negociando perfis de segurança” e “Seu enlace agora está



Habilitando a divisão de túnel

Para permitir o Split Tunneling para as conexões de VPN, certifique-se de que você tem uma lista de acessos configurada no roteador. No exemplo abaixo, o **comando access-list 108** é associado com o grupo para propósitos de split-tunneling, e o túnel é formado à rede 14.38.X.X /16. Fluxos de tráfego unencrypted aos dispositivos não na lista de acessos 108 (por exemplo, o Internet).

```
access-list 108 permit ip 14.38.0.0 0.0.255.255  
14.1.1.0 0.0.0.255
```

Aplice então a lista de acessos nas propriedades de grupo.

```
crypto isakmp client configuration group 3000client  
key cisco123  
dns 14.38.100.10
```

```
wins 14.38.100.20
domain cisco.com
pool ippool
acl 108
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

```
3640#show crypto isakmp sa
dst          src          state      conn-id     slot
172.18.124.159 172.18.124.96 QM_IDLE      3           0
```

```
3640#show crypto ipsec sa
interface: Ethernet0/0
Crypto map tag: clientmap, local addr. 172.18.124.96
```

```
protected vrf:
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port):
  (14.1.1.106/255.255.255.255/0/0)
current_peer: 172.18.124.159:500
PERMIT, flags={}
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest 6
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 172.18.124.96,
  remote crypto endpt.: 172.18.124.159
path mtu 1500, media mtu 1500
current outbound spi: D026E0BA
```

```
inbound esp sas:
spi: 0x84E901C8(2229862856)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2002, flow_id: 3, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4450694/3532)
IV size: 8 bytes
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0xD026E0BA(3492208826)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2003, flow_id: 4, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4450699/3532)
IV size: 8 bytes
```

```

replay detection support: Y

outbound ah sas:

outbound pcp sas:

protected vrf:
local ident (addr/mask/prot/port):
  (172.18.124.159/255.255.255.255/0/0)
remote ident (addr/mask/prot/port):
  (14.1.1.105/255.255.255.255/0/0)
current_peer: 172.18.124.159:500
PERMIT, flags={}
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest 6
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.18.124.159,
  remote crypto endpt.: 172.18.124.96
path mtu 1500, media mtu 1500
current outbound spi: E8E398F8

inbound esp sas:
spi: 0xDFE24DFC(3756150268)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4572253/3530)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xE8E398F8(3907229944)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4572253/3528)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

```

3640#**show crypto engine connections active**

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
3	Ethernet0/0	172.18.124.159	set	HMAC_MD5+3DES_56_C	0	0
2000	Ethernet0/0	172.18.124.159	set	HMAC_MD5+3DES_56_C	0	6
2001	Ethernet0/0	172.18.124.159	set	HMAC_MD5+3DES_56_C	6	0
2004	Ethernet0/0	172.18.124.159	set	HMAC_MD5+3DES_56_C	0	6
2005	Ethernet0/0	172.18.124.159	set	HMAC_MD5+3DES_56_C	6	0

[Troubleshooting](#)

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

configuração.

3640#**debug crypto ipsec**

Crypto IPSEC debugging is on

3640#**debug crypto isakmp**

Crypto ISAKMP debugging is on

3640#

ISAKMP (0:0): received packet from 172.18.124.96

dport 500 sport 500 Global (N) NEW SA

ISAKMP: Found a peer struct for 172.18.124.96, peer port 500

ISAKMP: Locking peer struct 0x63B2EAE4, IKE refcount 1 for
crypto_ikmp_config_initialize_sa

ISAKMP (0:0): (Re)Setting client xauth list and state

ISAKMP: local port 500, remote port 500

ISAKMP: insert sa successfully sa = 63972310

ISAKMP (0:1): processing SA payload. message ID = 0

ISAKMP (0:1): processing ID payload. message ID = 0

ISAKMP (0:1): peer matches *none* of the profiles

ISAKMP (0:1): processing vendor id payload

ISAKMP (0:1): vendor ID seems Unity/DPD but major 215 mismatch

ISAKMP (0:1): vendor ID is XAUTH

ISAKMP (0:1): processing vendor id payload

ISAKMP (0:1): vendor ID is DPD

ISAKMP (0:1): processing vendor id payload

ISAKMP (0:1): vendor ID seems Unity/DPD but major 123 mismatch

ISAKMP (0:1): vendor ID is NAT-T v2

ISAKMP (0:1): processing vendor id payload

ISAKMP (0:1): vendor ID seems Unity/DPD but major 194 mismatch

ISAKMP (0:1): processing vendor id payload

ISAKMP (0:1): vendor ID is Unity

ISAKMP (0:1) Authentication by xauth preshared

ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy

ISAKMP: encryption AES-CBC

ISAKMP: hash SHA

ISAKMP: default group 2

ISAKMP: auth XAUTHInitPreShared

ISAKMP: life type in seconds

ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B

ISAKMP: keylength of 256

ISAKMP (0:1): Encryption algorithm offered does not match policy!

ISAKMP (0:1): atts are not acceptable. Next payload is 3

ISAKMP (0:1): Checking ISAKMP transform 2 against priority 1 policy

ISAKMP: encryption AES-CBC

ISAKMP: hash MD5

ISAKMP: default group 2

ISAKMP: auth XAUTHInitPreShared

ISAKMP: life type in seconds

ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B

ISAKMP: keylength of 256

ISAKMP (0:1): Encryption algorithm offered does not match policy!

ISAKMP (0:1): atts are not acceptable. Next payload is 3

ISAKMP (0:1): Checking ISAKMP transform 3 against priority 1 policy

ISAKMP: encryption AES-CBC

ISAKMP: hash SHA

ISAKMP: default group 2

ISAKMP: auth pre-share

ISAKMP: life type in seconds

ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B

ISAKMP: keylength of 256

ISAKMP (0:1): Encryption algorithm offered does not match policy!

ISAKMP (0:1): atts are not acceptable. Next payload is 3

ISAKMP (0:1): Checking ISAKMP transform 4 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 256
ISAKMP (0:1): Encryh of 128
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 7 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 128
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 8 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 128
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 9 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 5 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 128
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 6 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 128
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 10 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared

ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 11 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 12 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 13 against priority 1 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable. Next payload is 3
ISAKMP (0:1): processing KE payload. message ID = 0
ISAKMP (0:1): processing NONCE payload. message ID = 0
ISAKMP (0:1): vendor ID is NAT-T v2
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
ISAKMP (0:1): Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT
ISAKMP: got callback 1
ISAKMP (0:1): SKEYID state generated
ISAKMP (0:1): constructed NAT-T vendor-02 ID
ISAKMP (0:1): SA is doing pre-shared key authentication
 plus XAUTH using id type ID_IPV4_ADDR
ISAKMP (1): ID payload
next-payload : 10
type : 1
addr : 172.18.124.159
protocol : 17
port : 0
length : 8
ISAKMP (1): Total payload length: 12
ISAKMP (0:1): constructed HIS NAT-D
ISAKMP (0:1): constructed MINE NAT-D
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
 peer_port 500 (R) AG_INIT_EXCH
ISAKMP (0:1): Input = IKE_MSG_FROM_AAA, PRESHARED_KEY_REPLY
ISAKMP (0:1): Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
 sport 500 Global (R) AG_INIT_EXCH
ISAKMP (0:1): processing HASH payload. message ID = 0
ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 63972310
ISAKMP (0:1): Process initial contact,
bring down existing phase 1 and 2 SA's with local 172.18.124.159
 remote 172.18.124.96 remote port 500
ISAKMP (0:1): returning IP addr to the address pool: 14.1.1.105
ISAKMP (0:1): returning address 14.1.1.105 to pool


```
ISAKMP:received payload type 17
ISAKMP (0:1): Detected NAT-D payload
ISAKMP (0:1): recalc my hash for NAT-D
ISAKMP (0:1): NAT match MINE hash
ISAKMP:received payload type 17
ISAKMP (0:1): Detected NAT-D payload
ISAKMP (0:1): recalc his hash for NAT-D
ISAKMP (0:1): NAT match HIS hash
ISAKMP (0:1): SA has been authenticated with 172.18.124.96
ISAKMP: set new node 1397605141 to CONF_XAUTH
ISAKMP (0:1): sending packet to 172.18.124.96
    my_port 500 peer_port 500 (R) QM_IDLE
ISAKMP (0:1): purging node 1397605141
ISAKMP: Sending phase 1 responder lifetime 86400
ISAKMP (0:1): peer matches *none* of the profiles
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
ISAKMP (0:1): Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE
IPSEC(key_engine): got a queue event...
ISAKMP (0:1): Need XAUTH
ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP (0:1): Old State = IKE_P1_COMPLETE
    New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT
ISAKMP: got callback 1
ISAKMP: set new node 1446280258 to CONF_XAUTH
ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
ISAKMP (0:1): initiating peer config to 172.18.124.96. ID = 1446280258
ISAKMP (0:1): sending packet to 172.18.124.96
    my_port 500 peer_port 500 (R) CONF_XAUTH
ISAKMP (0:1): Input = IKE_MSG_FROM_AAA, IKE_AAA_START_LOGIN
ISAKMP (0:1): Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT
    New State = IKE_XAUTH_REQ_SENT
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
    sport 500 Global (R) CONF_XAUTH
ISAKMP (0:1): processing transaction payload from 172.18.124.96.
    message ID = 1446280258
ISAKMP: Config payload REPLY
ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
ISAKMP (0:1): deleting node 1446280258 error FALSE
    reason "done with xauth request/reply exchange"
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_CFG_REPLY
ISAKMP (0:1): Old State = IKE_XAUTH_REQ_SENT
    New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
ISAKMP: got callback 1
ISAKMP: set new node 117774567 to CONF_XAUTH
ISAKMP (0:1): initiating peer config to 172.18.124.96.
    ID = 117774567
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
    peer_port 500 (R) CONF_XAUTH
ISAKMP (0:1): Input = IKE_MSG_FROM_AAA, IKE_AAA_CONT_LOGIN
ISAKMP (0:1): Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
    New State = IKE_XAUTH_SET_SENT
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
    sport 500 Global (R) CONF_XAUTH
ISAKMP (0:1): processing transaction payload from 172.18.124.96.
    message ID = 117774567
ISAKMP: Config payload ACK
ISAKMP (0:1): XAUTH ACK Processed
ISAKMP (0:1): deleting node 117774567 error FALSE
    reason "done with transaction"
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_CFG_ACK
ISAKMP (0:1): Old State = IKE_XAUTH_SET_SENT
    New State = IKE_P1_COMPLETE
```

```
ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP (0:1): Old State = IKE_P1_COMPLETE
  New State = IKE_P1_COMPLETE
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
  sport 500 Global (R) QM_IDLE
ISAKMP: set new node 188739171 to QM_IDLE
ISAKMP (0:1): processing transaction payload from 172.18.124.96.
  message ID = 188739171
ISAKMP: Config payload REQUEST
ISAKMP (0:1): checking request:
ISAKMP: IP4_ADDRESS
ISAKMP: IP4_NETMASK
ISAKMP: IP4_DNS
ISAKMP: IP4_NBNS
ISAKMP: ADDRESS_EXPIRY
ISAKMP: APPLICATION_VERSION
ISAKMP: UNKNOWN Unknown Attr: 0x7000
ISAKMP: UNKNOWN Unknown Attr: 0x7001
ISAKMP: DEFAULT_DOMAIN
ISAKMP: SPLIT_INCLUDE
ISAKMP: UNKNOWN Unknown Attr: 0x7003
ISAKMP: UNKNOWN Unknown Attr: 0x7007
ISAKMP: UNKNOWN Unknown Attr: 0x7008
ISAKMP: UNKNOWN Unknown Attr: 0x7009
ISAKMP: UNKNOWN Unknown Attr: 0x700A
ISAKMP: UNKNOWN Unknown Attr: 0x7005
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST
ISAKMP (0:1): Old State = IKE_P1_COMPLETE
  New State = IKE_CONFIG_AUTHOR_AAA_AWAIT
ISAKMP: got callback 1
ISAKMP (0:1): attributes sent in message:
Address: 0.2.0.0
ISAKMP (0:1): allocating address 14.1.1.106
ISAKMP: Sending private address: 14.1.1.106
ISAKMP: Sending IP4_DNS server address: 14.1.1.10
ISAKMP: Sending IP4_NBNS server address: 14.1.1.20
ISAKMP: Sending ADDRESS_EXPIRY seconds left to
  use the address: 86396
ISAKMP: Sending APPLICATION_VERSION string: Cisco
  Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-JK903S-M), Version 12.2(15)T2,
  RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 30-Apr-03 05:42 by nmasa
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7000)
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7001)
ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7003)
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7007)
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7008)
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7009)
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x700A)
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7005)
ISAKMP (0:1): responding to peer config from 172.18.124.96.
  ID = 188739171
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
  peer_port 500 (R) CONF_ADDR
ISAKMP (0:1): deleting node 188739171 error FALSE reason ""
ISAKMP (0:1): Input = IKE_MSG_FROM_AAA, IKE_AAA_GROUP_ATTR
ISAKMP (0:1): Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT
  New State = IKE_P1_COMPLETE
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
  sport 500 Global (R) QM_IDLE
```

ISAKMP: set new node -1836135476 to QM_IDLE
ISAKMP (0:1): processing HASH payload. message ID = -1836135476
ISAKMP (0:1): processing SA payload. message ID = -1836135476
ISAKMP (0:1): Checking IPsec proposal 1
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 1
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
not supported for identity:
{esp-aes 256 esp-md5-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 2
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 2
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),

```
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes 256 esp-sha-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 3
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 3
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes esp-md5-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 4
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 4
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
```

```
protocol= ESP, transform= esp-aes esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes esp-sha-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 5
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes 256 esp-md5-hmac }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 6
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes 256 esp-sha-hmac }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 7
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
```

```
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes esp-md5-hmac }
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 8
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes esp-sha-hmac }
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 9
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPSec proposal 9
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
```

```
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-3des esp-md5-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 10
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 10
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-3des esp-sha-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 11
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
ISAKMP (0:1): processing NONCE payload. message ID = -1836135476
ISAKMP (0:1): processing ID payload. message ID = -1836135476
ISAKMP (0:1): processing ID payload. message ID = -1836135476
ISAKMP (0:1): asking for 1 spis from ipsec
ISAKMP (0:1): Node -1836135476, Input = IKE_MSG_FROM_PEER,
    IKE_QM_EXCH
ISAKMP (0:1): Old State = IKE_QM_READY
    New State = IKE_QM_SPI_STARVE
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
```

```
sport 500 Global (R) QM_IDLE
ISAKMP: set new node -1171731793 to QM_IDLE
ISAKMP (0:1): processing HASH payload. message ID = -1171731793
ISAKMP (0:1): processing SA payload. message ID = -1171731793
ISAKMP (0:1): Checking IPsec proposal 1
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 1
ISAKMP (0:1): transform 1, IPsec LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
not supported for identity:
{esp-aes 256 esp-md5-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 2
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 2
ISAKMP (0:1): transform 1, IPsec LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
```



```
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes 256 esp-sha-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 3
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 3
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes esp-md5-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 4
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 4
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
```

```
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes esp-sha-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 5
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): processing ID payload. message ID = -1171731793
ISAKMP (0:1): processing ID payload. message ID = -1171731793
ISAKMP (0:1): asking for 1 spis from ipsec
ISAKMP (0:1): Node -1171731793, Input = IKE_MSG_FROM_PEER,
    IKE_QM_EXCH
ISAKMP (0:1): Old State = IKE_QM_READY
    New State = IKE_QM_SPI_STARVE
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 3756150268 for SA
from 172.18.124.159 to 172.18.124.96 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 2229862856 for SA
from 172.18.124.159 to 172.18.124.96 for prot 3
ISAKMP: received ke message (2/1)
ISAKMP: received ke message (2/1)
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
    peer_port 500 (R) QM_IDLE
ISAKMP (0:1): Node -1836135476, Input = IKE_MSG_FROM_IPSEC,
    IKE_SPI_REPLY
ISAKMP (0:1): Old State = IKE_QM_SPI_STARVE
    New State = IKE_QM_R_QM2
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
    sport 500 Global (R) QM_IDLE
ISAKMP: Locking peer struct 0x63B2EAE4,
    IPSEC refcount 1 for for stuff_ke
ISAKMP (0:1): Creating IPsec SAs
inbound SA from 172.18.124.96 to 172.18.124.159 (f/i) 0/ 0
(proxy 14.1.1.106 to 172.18.124.159)
has spi 0xDFE24DFC and conn_id 2000 and flags 2
lifetime of 2147483 seconds
has client flags 0x0
ISAKMP (0:1): Old State = IKE_QM_SPI_STARVE
    New State = IKE_QM_R_QM2
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
    sport 500 Global (R) QM_IDLE
ISAKMP: Locking peer struct 0x63B2EAE4,
    IPSEC refcount 2 for for stuff_ke
ISAKMP (0:1): Creating IPsec SAs
inbound SA from 172.18.124.96 to 172.18.124.159 (f/i) 0/ 0
(proxy 14.1.1.106 to 0.0.0.0)
```

```
has spi 0x84E901C8 and conn_id 2002 and flags 2
lifetime of 2147483 seconds
has client flags 0x0
outbound SA from 172.18.124.159 to 172.18.124.96 (f/i) 0/ 0
(proxy 0.0.0.0 to 14.1.1.106 )
has spi -802758470 and conn_id 2003 and flags A
IPSEC(add mtree): src 0.0.0.0, dest 14.1.1.106, dest_port 0
IPSEC(create_sa): sa created,
(sa) sa_dest= 172.18.124.159, sa_prot= 50,
sa_spi= 0x84E901C8(2229862856),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
IPSEC(create_sa): sa created,
(sa) sa_dest= 172.18.124.96, sa_prot= 50,
sa_spi= 0xD026E0BA(3492208826),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2003
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
sport 500 Global (R) QM_IDLE
ISAKMP: set new node 839140381 to QM_IDLE
ISAKMP (0:1): processing HASH payload. message ID = 839140381
ISAKMP (0:1): processing NOTIFY R_U_THERE protocol 1
spi 0, message ID = 839140381, sa = 63972310
ISAKMP (0:1): deleting node 839140381 error FALSE
reason "informational (in) state 1"
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_INFO_NOTIFY
ISAKMP (0:1): Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE
ISAKMP (0:1): DPD/R_U_THERE received from peer 172.18.124.96,
sequence 0xA5A4632A
ISAKMP: set new node 760238809 to QM_IDLE
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
peer_port 500 (R) QM_IDLE
ISAKMP (0:1): purging node 760238809
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER,
IKE_MSG_KEEP_ALIVE
ISAKMP (0:1): Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE
ISAKMP (0:1): purging node 188739171
ISAKMP (0:1): purging node -1836135476
ISAKMP (0:1): purging node -1171731793
3640#
```

Registros de Cliente

Para ver os logs, lance LogViewer no cliente VPN, e certifique-se de que o filtro está ajustado à elevação para todas as classes configuradas. O exemplo de saída do registro é mostrado abaixo.

```
3640#debug crypto ipsec
Crypto IPSEC debugging is on
3640#debug crypto isakmp
Crypto ISAKMP debugging is on
3640#

ISAKMP (0:0): received packet from 172.18.124.96
dport 500 sport 500 Global (N) NEW SA
ISAKMP: Found a peer struct for 172.18.124.96, peer port 500
ISAKMP: Locking peer struct 0x63B2EAE4, IKE refcount 1 for
crypto_ikmp_config_initialize_sa
ISAKMP (0:0): (Re)Setting client xauth list and state
ISAKMP: local port 500, remote port 500
ISAKMP: insert sa successfully sa = 63972310
ISAKMP (0:1): processing SA payload. message ID = 0
ISAKMP (0:1): processing ID payload. message ID = 0
```

ISAKMP (0:1): peer matches *none* of the profiles
ISAKMP (0:1): processing vendor id payload
ISAKMP (0:1): vendor ID seems Unity/DPD but major 215 mismatch
ISAKMP (0:1): vendor ID is XAUTH
ISAKMP (0:1): processing vendor id payload
ISAKMP (0:1): vendor ID is DPD
ISAKMP (0:1): processing vendor id payload
ISAKMP (0:1): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP (0:1): vendor ID is NAT-T v2
ISAKMP (0:1): processing vendor id payload
ISAKMP (0:1): vendor ID seems Unity/DPD but major 194 mismatch
ISAKMP (0:1): processing vendor id payload
ISAKMP (0:1): vendor ID is Unity
ISAKMP (0:1) Authentication by xauth preshared
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 256
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 2 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 256
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 256
ISAKMP (0:1): Encryh of 128
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 4 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 256
ISAKMP (0:1): Encryh of 128
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 7 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 128
ISAKMP (0:1): Encryption algorithm offered does not match policy!

ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 8 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 128
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 9 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 5 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 128
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 6 against priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 10 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 11 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 12 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B

ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 3
ISAKMP (0:1): Checking ISAKMP transform 13 against priority 1 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable. Next payload is 3
ISAKMP (0:1): processing KE payload. message ID = 0
ISAKMP (0:1): processing NONCE payload. message ID = 0
ISAKMP (0:1): vendor ID is NAT-T v2
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
ISAKMP (0:1): Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT
ISAKMP: got callback 1
ISAKMP (0:1): SKEYID state generated
ISAKMP (0:1): constructed NAT-T vendor-02 ID
ISAKMP (0:1): SA is doing pre-shared key authentication
 plus XAUTH using id type ID_IPV4_ADDR
ISAKMP (1): ID payload
next-payload : 10
type : 1
addr : 172.18.124.159
protocol : 17
port : 0
length : 8
ISAKMP (1): Total payload length: 12
ISAKMP (0:1): constructed HIS NAT-D
ISAKMP (0:1): constructed MINE NAT-D
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
 peer_port 500 (R) AG_INIT_EXCH
ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY
ISAKMP (0:1): Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
 sport 500 Global (R) AG_INIT_EXCH
ISAKMP (0:1): processing HASH payload. message ID = 0
ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 63972310
ISAKMP (0:1): Process initial contact,
bring down existing phase 1 and 2 SA's with local 172.18.124.159
 remote 172.18.124.96 remote port 500
ISAKMP (0:1): returning IP addr to the address pool: 14.1.1.105
ISAKMP (0:1): returning address 14.1.1.105 to pool
ISAKMP:received payload type 17
ISAKMP (0:1): Detected NAT-D payload
ISAKMP (0:1): recalc my hash for NAT-D
ISAKMP (0:1): NAT match MINE hash
ISAKMP:received payload type 17
ISAKMP (0:1): Detected NAT-D payload
ISAKMP (0:1): recalc his hash for NAT-D
ISAKMP (0:1): NAT match HIS hash
ISAKMP (0:1): SA has been authenticated with 172.18.124.96
ISAKMP: set new node 1397605141 to CONF_XAUTH
ISAKMP (0:1): sending packet to 172.18.124.96
 my_port 500 peer_port 500 (R) QM_IDLE
ISAKMP (0:1): purging node 1397605141
ISAKMP: Sending phase 1 responder lifetime 86400
ISAKMP (0:1): peer matches *none* of the profiles
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
ISAKMP (0:1): Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE
IPSEC(key_engine): got a queue event...
ISAKMP (0:1): Need XAUTH
ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE

ISAKMP (0:1): Old State = IKE_P1_COMPLETE
New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT
ISAKMP: got callback 1
ISAKMP: set new node 1446280258 to CONF_XAUTH
ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
ISAKMP (0:1): initiating peer config to 172.18.124.96. ID = 1446280258
ISAKMP (0:1): sending packet to 172.18.124.96
my_port 500 peer_port 500 (R) CONF_XAUTH
ISAKMP (0:1): Input = IKE_MSG_FROM_AAA, IKE_AAA_START_LOGIN
ISAKMP (0:1): Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT
New State = IKE_XAUTH_REQ_SENT
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
sport 500 Global (R) CONF_XAUTH
ISAKMP (0:1): processing transaction payload from 172.18.124.96.
message ID = 1446280258
ISAKMP: Config payload REPLY
ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
ISAKMP (0:1): deleting node 1446280258 error FALSE
reason "done with xauth request/reply exchange"
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_CFG_REPLY
ISAKMP (0:1): Old State = IKE_XAUTH_REQ_SENT
New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
ISAKMP: got callback 1
ISAKMP: set new node 117774567 to CONF_XAUTH
ISAKMP (0:1): initiating peer config to 172.18.124.96.
ID = 117774567
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
peer_port 500 (R) CONF_XAUTH
ISAKMP (0:1): Input = IKE_MSG_FROM_AAA, IKE_AAA_CONT_LOGIN
ISAKMP (0:1): Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
New State = IKE_XAUTH_SET_SENT
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
sport 500 Global (R) CONF_XAUTH
ISAKMP (0:1): processing transaction payload from 172.18.124.96.
message ID = 117774567
ISAKMP: Config payload ACK
ISAKMP (0:1): XAUTH ACK Processed
ISAKMP (0:1): deleting node 117774567 error FALSE
reason "done with transaction"
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_CFG_ACK
ISAKMP (0:1): Old State = IKE_XAUTH_SET_SENT
New State = IKE_P1_COMPLETE
ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP (0:1): Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
sport 500 Global (R) QM_IDLE
ISAKMP: set new node 188739171 to QM_IDLE
ISAKMP (0:1): processing transaction payload from 172.18.124.96.
message ID = 188739171
ISAKMP: Config payload REQUEST
ISAKMP (0:1): checking request:
ISAKMP: IP4_ADDRESS
ISAKMP: IP4_NETMASK
ISAKMP: IP4_DNS
ISAKMP: IP4_NBNS
ISAKMP: ADDRESS_EXPIRY
ISAKMP: APPLICATION_VERSION
ISAKMP: UNKNOWN Unknown Attr: 0x7000
ISAKMP: UNKNOWN Unknown Attr: 0x7001
ISAKMP: DEFAULT_DOMAIN
ISAKMP: SPLIT_INCLUDE

ISAKMP: UNKNOWN Unknown Attr: 0x7003
ISAKMP: UNKNOWN Unknown Attr: 0x7007
ISAKMP: UNKNOWN Unknown Attr: 0x7008
ISAKMP: UNKNOWN Unknown Attr: 0x7009
ISAKMP: UNKNOWN Unknown Attr: 0x700A
ISAKMP: UNKNOWN Unknown Attr: 0x7005
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST
ISAKMP (0:1): Old State = IKE_P1_COMPLETE
New State = IKE_CONFIG_AUTHOR_AAA_AWAIT
ISAKMP: got callback 1
ISAKMP (0:1): attributes sent in message:
Address: 0.2.0.0
ISAKMP (0:1): allocating address 14.1.1.106
ISAKMP: Sending private address: 14.1.1.106
ISAKMP: Sending IP4_DNS server address: 14.1.1.10
ISAKMP: Sending IP4_NBNS server address: 14.1.1.20
ISAKMP: Sending ADDRESS_EXPIRY seconds left to
use the address: 86396
ISAKMP: Sending APPLICATION_VERSION string: Cisco
Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-JK903S-M), Version 12.2(15)T2,
RELEASE SOFTWARE (fc2)
TAC Support: <http://www.cisco.com/tac>
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 30-Apr-03 05:42 by nmasa
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7000)
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7001)
ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7003)
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7007)
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7008)
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7009)
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x700A)
ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7005)
ISAKMP (0:1): responding to peer config from 172.18.124.96.
ID = 188739171
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
peer_port 500 (R) CONF_ADDR
ISAKMP (0:1): deleting node 188739171 error FALSE reason ""
ISAKMP (0:1): Input = IKE_MSG_FROM_AAA, IKE_AAA_GROUP_ATTR
ISAKMP (0:1): Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT
New State = IKE_P1_COMPLETE
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
sport 500 Global (R) QM_IDLE
ISAKMP: set new node -1836135476 to QM_IDLE
ISAKMP (0:1): processing HASH payload. message ID = -1836135476
ISAKMP (0:1): processing SA payload. message ID = -1836135476
ISAKMP (0:1): Checking IPsec proposal 1
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 1
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,


```
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes 256 esp-md5-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 2
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 2
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes 256 esp-sha-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 3
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 3
ISAKMP (0:1): transform 1, IPPCP LZS
```

```
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes esp-md5-hmac comp-lzs }
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 4
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPSec proposal 4
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes esp-sha-hmac comp-lzs }
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 5
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
```

```
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes 256 esp-md5-hmac }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 6
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes 256 esp-sha-hmac }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 7
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes esp-md5-hmac }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 8
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 128
```

ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
not supported for identity:
{esp-aes esp-sha-hmac }
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 9
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPSec proposal 9
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
not supported for identity:
{esp-3des esp-md5-hmac comp-lzs }
ISAKMP (0:1): IPSec policy invalidated proposal
ISAKMP (0:1): Checking IPSec proposal 10
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPSec proposal 10
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.

```
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-3des esp-sha-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 11
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 172.18.124.159/255.255.255.255/0/0 (type=1),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
ISAKMP (0:1): processing NONCE payload. message ID = -1836135476
ISAKMP (0:1): processing ID payload. message ID = -1836135476
ISAKMP (0:1): processing ID payload. message ID = -1836135476
ISAKMP (0:1): asking for 1 spis from ipsec
ISAKMP (0:1): Node -1836135476, Input = IKE_MSG_FROM_PEER,
    IKE_QM_EXCH
ISAKMP (0:1): Old State = IKE_QM_READY
    New State = IKE_QM_SPI_STARVE
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
    sport 500 Global (R) QM_IDLE
ISAKMP: set new node -1171731793 to QM_IDLE
ISAKMP (0:1): processing HASH payload. message ID = -1171731793
ISAKMP (0:1): processing SA payload. message ID = -1171731793
ISAKMP (0:1): Checking IPsec proposal 1
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 1
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
```

```
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes 256 esp-md5-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 2
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 2
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes 256 esp-sha-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 3
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 3
```

```
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes esp-md5-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 4
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: key length is 128
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
ISAKMP (0:1): Checking IPsec proposal 4
ISAKMP (0:1): transform 1, IPPCP LZS
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.18.124.159, remote= 172.18.124.96,
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 14.1.1.106/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
IPSEC(validate_transform_proposal): transform proposal
    not supported for identity:
{esp-aes esp-sha-hmac comp-lzs }
ISAKMP (0:1): IPsec policy invalidated proposal
ISAKMP (0:1): Checking IPsec proposal 5
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
```

ISAKMP: encaps is 1
ISAKMP: key length is 256
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:1): processing ID payload. message ID = -1171731793
ISAKMP (0:1): processing ID payload. message ID = -1171731793
ISAKMP (0:1): asking for 1 spis from ipsec
ISAKMP (0:1): Node -1171731793, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
ISAKMP (0:1): Old State = IKE_QM_READY
New State = IKE_QM_SPI_STARVE
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 3756150268 for SA
from 172.18.124.159 to 172.18.124.96 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 2229862856 for SA
from 172.18.124.159 to 172.18.124.96 for prot 3
ISAKMP: received ke message (2/1)
ISAKMP: received ke message (2/1)
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
peer_port 500 (R) QM_IDLE
ISAKMP (0:1): Node -1836135476, Input = IKE_MESG_FROM_IPSEC,
IKE_SPI_REPLY
ISAKMP (0:1): Old State = IKE_QM_SPI_STARVE
New State = IKE_QM_R_QM2
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
sport 500 Global (R) QM_IDLE
ISAKMP: Locking peer struct 0x63B2EAE4,
IPSEC refcount 1 for for stuff_ke
ISAKMP (0:1): Creating IPsec SAs
inbound SA from 172.18.124.96 to 172.18.124.159 (f/i) 0/ 0
(proxy 14.1.1.106 to 172.18.124.159)
has spi 0xDFE24DFC and conn_id 2000 and flags 2
lifetime of 2147483 seconds
has client flags 0x0
ISAKMP (0:1): Old State = IKE_QM_SPI_STARVE
New State = IKE_QM_R_QM2
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
sport 500 Global (R) QM_IDLE
ISAKMP: Locking peer struct 0x63B2EAE4,
IPSEC refcount 2 for for stuff_ke
ISAKMP (0:1): Creating IPsec SAs
inbound SA from 172.18.124.96 to 172.18.124.159 (f/i) 0/ 0
(proxy 14.1.1.106 to 0.0.0.0)
has spi 0x84E901C8 and conn_id 2002 and flags 2
lifetime of 2147483 seconds
has client flags 0x0
outbound SA from 172.18.124.159 to 172.18.124.96 (f/i) 0/ 0
(proxy 0.0.0.0 to 14.1.1.106)
has spi -802758470 and conn_id 2003 and flags A
IPSEC(add mtree): src 0.0.0.0, dest 14.1.1.106, dest_port 0
IPSEC(create_sa): sa created,
(sa) sa_dest= 172.18.124.159, sa_prot= 50,
sa_spi= 0x84E901C8(2229862856),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
IPSEC(create_sa): sa created,
(sa) sa_dest= 172.18.124.96, sa_prot= 50,
sa_spi= 0xD026E0BA(3492208826),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2003
ISAKMP (0:1): received packet from 172.18.124.96 dport 500
sport 500 Global (R) QM_IDLE
ISAKMP: set new node 839140381 to QM_IDLE
ISAKMP (0:1): processing HASH payload. message ID = 839140381
ISAKMP (0:1): processing NOTIFY R_U_THERE protocol 1


```
spi 0, message ID = 839140381, sa = 63972310
ISAKMP (0:1): deleting node 839140381 error FALSE
    reason "informational (in) state 1"
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_INFO_NOTIFY
ISAKMP (0:1): Old State = IKE_P1_COMPLETE
    New State = IKE_P1_COMPLETE
ISAKMP (0:1): DPD/R_U_THERE received from peer 172.18.124.96,
    sequence 0xA5A4632A
ISAKMP: set new node 760238809 to QM_IDLE
ISAKMP (0:1): sending packet to 172.18.124.96 my_port 500
    peer_port 500 (R) QM_IDLE
ISAKMP (0:1): purging node 760238809
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER,
    IKE_MSG_KEEP_ALIVE
ISAKMP (0:1): Old State = IKE_P1_COMPLETE
    New State = IKE_P1_COMPLETE
ISAKMP (0:1): purging node 188739171
ISAKMP (0:1): purging node -1836135476
ISAKMP (0:1): purging node -1171731793
3640#
```

[Informações Relacionadas](#)

- [Sustentação do produto dos concentradores do Cisco VPN 3000](#)
- [Sustentação do produto do Cisco VPN 3000 Client](#)
- [Suporte por tecnologia da Negociação IPSec/Protocolos IKE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)