Contenido

Introducción

Este documento demuestra cómo configurar una conexión entre un router y Cisco VPN Client 4.x mediante RADIUS (Remote Authentication Dial-in User Service) para la autenticación de usuarios. Los Software Release 12.2(8)T y Posterior de Cisco IOS® soportan las conexiones del Cliente Cisco VPN 4.x. Los clientes VPN 3.x y 4.x utilizan la política Diffie Hellman (DH) group 2. El comando isakmp policy # group 2 permite conectarse a los clientes VPN.

Este documento muestra la autenticación en el servidor de RADIUS, y la autorización (tal como asignación del Windows Internet Naming Service (TRIUNFOS) y del Domain Naming Service (el DNS)) localmente por el router. Si usted está interesado en hacer la autenticación y autorización a través del servidor de RADIUS, refiera a configurar el IPSec entre un router y un Cliente Cisco VPN 4.x del Cisco IOS para Windows usando el RADIUS.

Nota: El considerar del IPSec VPN está disponible ahora. Refiera al IPSec VPN que explica más información y configuraciones de muestra.

Refiera al túnel IPsec entre el router IOS y el Cliente Cisco VPN 4.x para Windows con el ejemplo de configuración de la autenticación de usuario TACACS+ para más información sobre el escenario donde la autenticación de usuario ocurre externamente con el protocolo TACACS+.

Refiera a configurar al Cliente Cisco VPN 3.x para Windows al IOS usando la autenticación ampliada local para más información sobre el escenario donde la autenticación de usuario ocurre localmente en el router del Cisco IOS.

Refiera al PIX/ASA 7.x y al Cliente Cisco VPN 4.x para Windows con el ejemplo de configuración de la autenticación de RADIUS de Microsoft Windows 2003 IAS para la información sobre cómo configurar la conexión VPN de acceso remoto entre un Cliente Cisco VPN (4.x para Windows) y el dispositivo de seguridad 7.x de la serie PIX 500 usando un servidor de RADIUS del Internet Authentication Service de Microsoft Windows 2003 (IAS).

Refiera al IPSec - PIX al Wild-card del cliente VPN, al Pre-shared, a la configuración de modo con la autenticación ampliada para la información sobre cómo conectar a un cliente VPN con un firewall PIX usando los comodines, a la configuración de modo, al **comando sysopt connection permit-ipsec**, y al Autenticación ampliada (Xauth).

Refiera al IPSec entre un concentrador VPN 3000 y un cliente VPN 4.x para Windows usando el RADIUS para el ejemplo de configuración de la autenticación de usuario y de las estadísticas para la información sobre cómo establecer un túnel IPsec entre un Cisco VPN 3000 Concentrator y un Cliente Cisco VPN 4.x para Windows usando el RADIUS para la autenticación de usuario y las estadísticas.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Una agrupación de direcciones que se asignará para el IPSec
- Un grupo llamado el "3000clients" con una contraseña del "cisco123"
- Autenticación de usuario en un servidor de RADIUS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Un 2621XM Router que funciona con el Cisco IOS Software Release 12.2(15)T2
- CiscoSecure ACS para la versión 4.2 del Windows 2000 (cualquier servidor de RADIUS debe trabajar)
- Cliente Cisco VPN para la versión de Windows 4.8 (cualquier cliente VPN 4.x y posterior debe trabajar)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Esto se hace salir del **comando show version** en el router:

```
vpn2621#show versionCisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-
IK9S-M), Version 12.2(15)T2,  RELEASE SOFTWARE (fc2)TAC Support:
http://www.cisco.com/tacCopyright (c) 1986-2003 by cisco Systems, Inc.Compiled Thu 01-May-03
10:39 by nmasaImage text-base: 0x80008098, data-base: 0x81BBB0BCROM: System Bootstrap, Version
12.2(7r) [cmong 7r], RELEASE SOFTWARE (fc1)vpn2621 uptime is 1 hour, 34 minutesSystem returned
to ROM by reloadSystem image file is "flash:c2600-ik9s-mz.122-15.T2.bin"This product contains
cryptographic features and is subject to UnitedStates and local country laws governing import,
```

```
export, transfer anduse. Delivery of Cisco cryptographic products does not implythird-party
authority to import, export, distribute or use encryption.Importers, exporters, distributors and
users are responsible forcompliance with U.S. and local country laws. By using this product
youagree to comply with applicable laws and regulations. If you are unableto 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/wwl/export/crypto/tool/stqrg.htmlIf
you require further assistance please contact us by sending email toexport@cisco.com.cisco
2621XM (MPC860P) processor (revision 0x100) with 125952K/5120K bytes of memory.Processor board
ID JAD064503FK (64188517)M860 processor: part number 5, mask 2Bridging software.X.25 software,
Version 3.0.0.2 FastEthernet/IEEE 802.3 interface(s)2 Serial(sync/async) network interface(s)1
terminal line(s)1 Virtual Private Network (VPN) Module(s)1 cisco content engine(s)32K bytes of
non-volatile configuration memory.32768K bytes of processor board System flash
(Read/Write)Configuration register is 0x2102
```

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

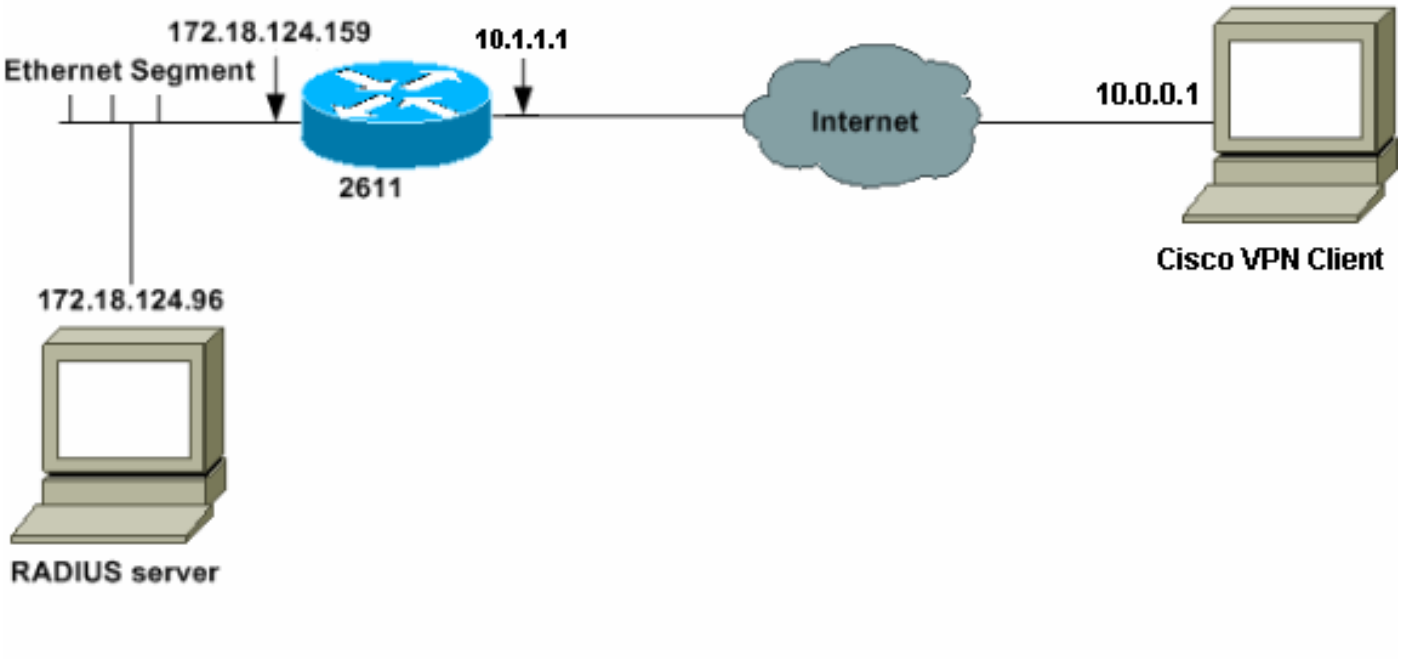
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configure al 2621XM Router

2621XM Router
!--- Enable authentication, authorization and accounting

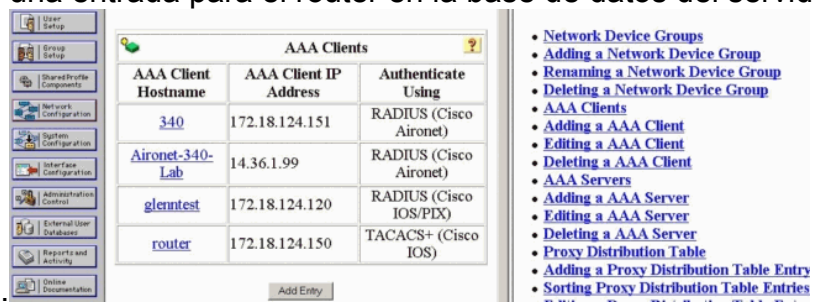
```
(AAA) !--- for user authentication and group
authorization.aaa new-model!!--- In order to enable
extended authentication (Xauth) for user authentication,
!--- enable the aaa authentication commands. !--- "Group
radius local" specifies RADIUS user authentication !---
to be used by default and to use local database if
RADIUS server is not reachable.aaa authentication login
userauthen group radius local!--- In order to enable
group authorization, !--- enable the aaa authorization
commands.aaa authorization network groupauthor local!---
Create an Internet Security Association and !--- Key
Management Protocol (ISAKMP) policy for Phase 1
negotiations.crypto isakmp policy 3encr
3desauthentication pre-sharegroup 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 3000clientkey cisco123dns
10.1.1.10wins 10.1.1.20domain cisco.compool ippool!!---
Create the Phase 2 policy for actual data
encryption.crypto ipsec transform-set myset esp-3des
esp-sha-hmac!!--- Create a dynamic map and !--- apply
the transform set that was created.crypto dynamic-map
dynmap 10set transform-set myset!!--- Create the actual
crypto map, !--- and apply the AAA lists that were
created earlier.crypto map clientmap client
authentication list userauthencrypto map clientmap
isakmp authorization list groupauthorcrypto map
clientmap client configuration address respondcrypto map
clientmap 10 ipsec-isakmp dynamic dynmap!--- Apply the
crypto map on the outside interface.interface
Ethernet0/0 ip address 10.1.1.1 255.255.255.0 half-
duplex crypto map clientmapinterface Ethernet0/1 ip
address 172.18.124.159 255.255.255.0 half-duplex!!---
Create a pool of addresses to be assigned to the VPN
Clients.ip local pool ippool  10.16.20.1 10.16.20.200ip
classlessip route 0.0.0.0 0.0.0.0 10.1.1.2ip http
serverip pim bidir-enable!!!!--- Specify the IP address
of the RADIUS server, !--- along with the RADIUS shared
secret key.radius-server host 172.18.124.96 auth-port
1645 acct-port 1646 key cisco123radius-server retransmit
3
```

Configuración del servidor de RADIUS

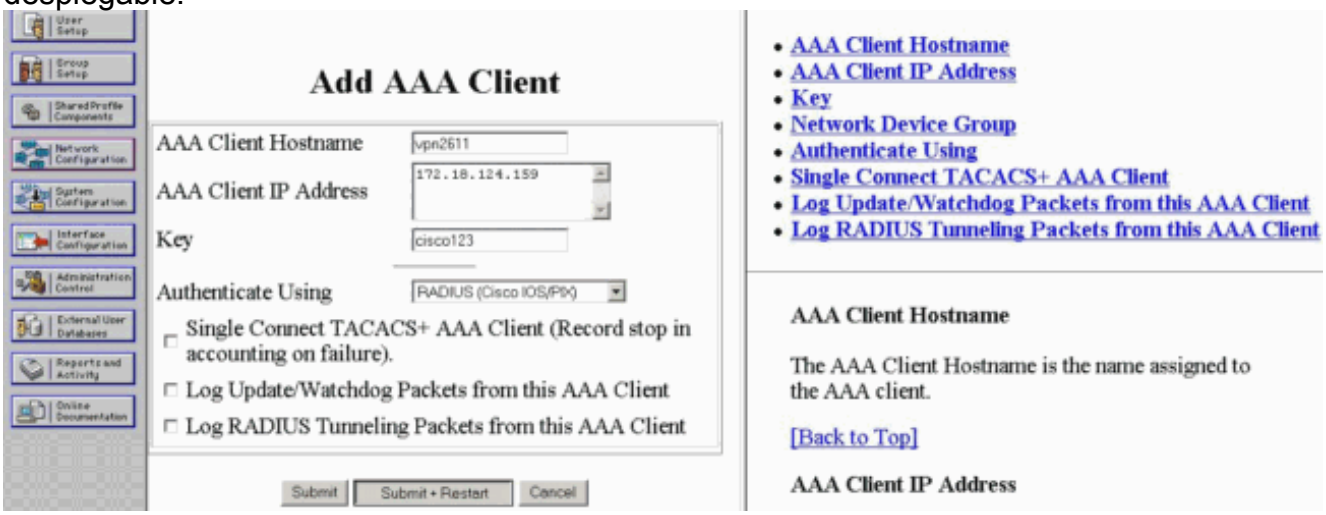
Configure al servidor de RADIUS para la autenticación de usuario

Complete estos pasos para configurar al servidor de RADIUS:

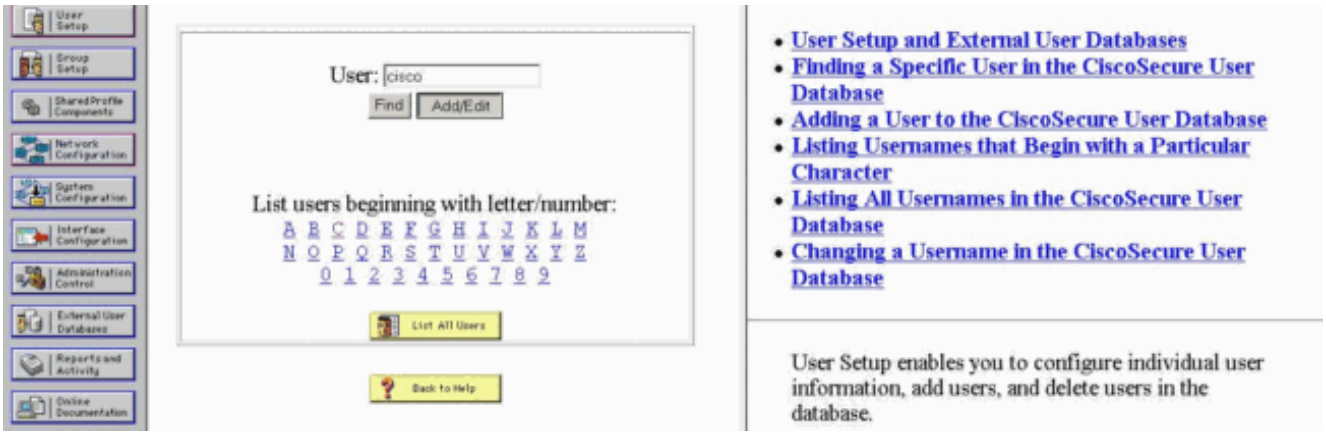
1. Agregue una entrada para el router en la base de datos del servidor RADIUS.



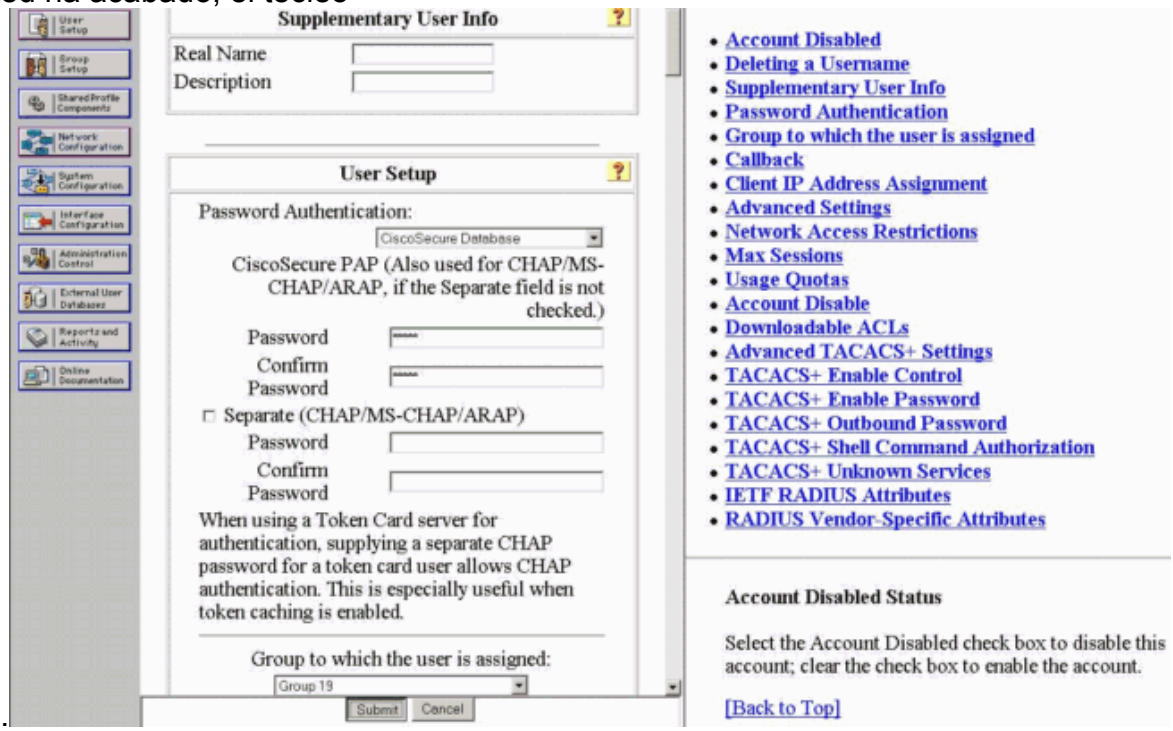
2. Especifique la dirección IP del router el "172.18.124.159", junto con la clave secreta compartida el "cisco123". Elija el **RADIUS** en la autenticidad usando la casilla desplegable.



3. Agregue el nombre de usuario para el usuario de VPN en la base de datos de CiscoSecure. En el ejemplo, el nombre de usuario es Cisco.



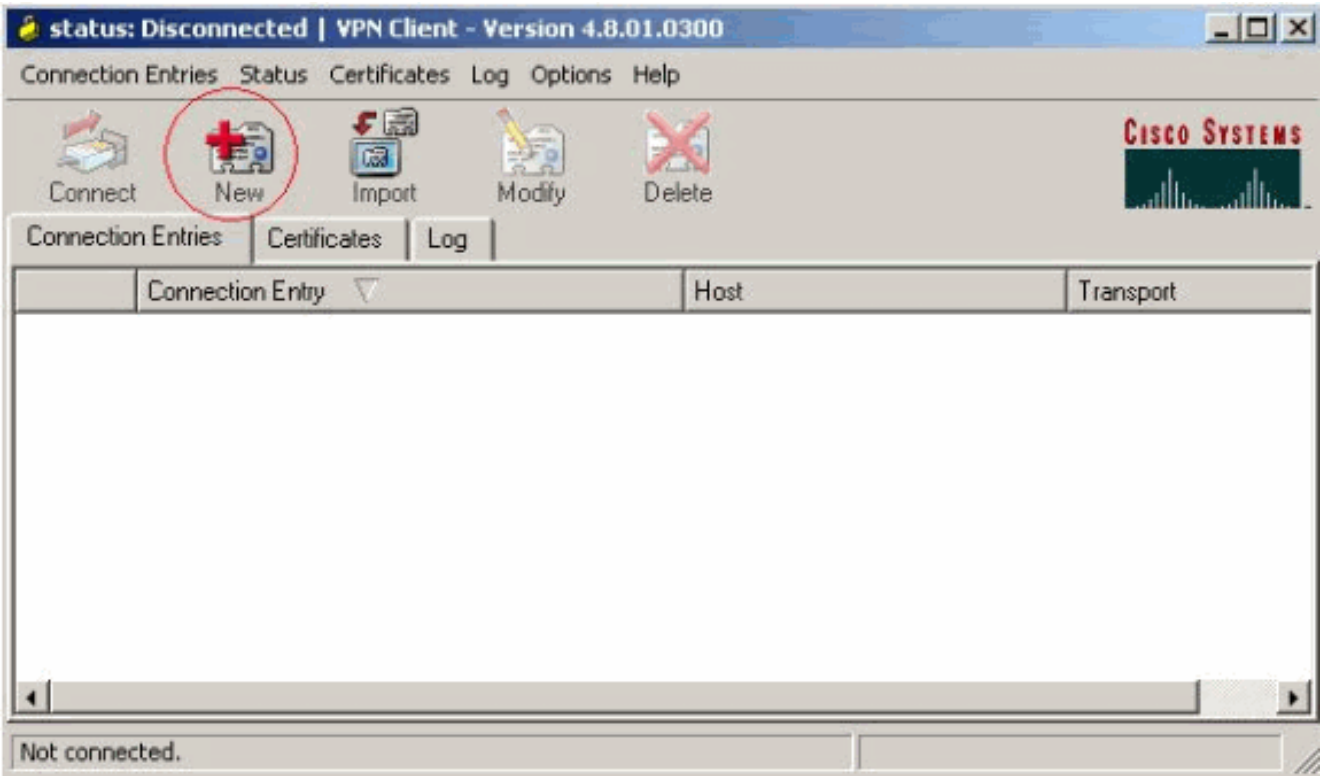
4. En la próxima ventana, especifique la contraseña para el usuario Cisco. En este ejemplo, la contraseña es también Cisco. Usted puede asociar la cuenta de usuario a un grupo. Una vez que usted ha acabado, el tecleo somete.



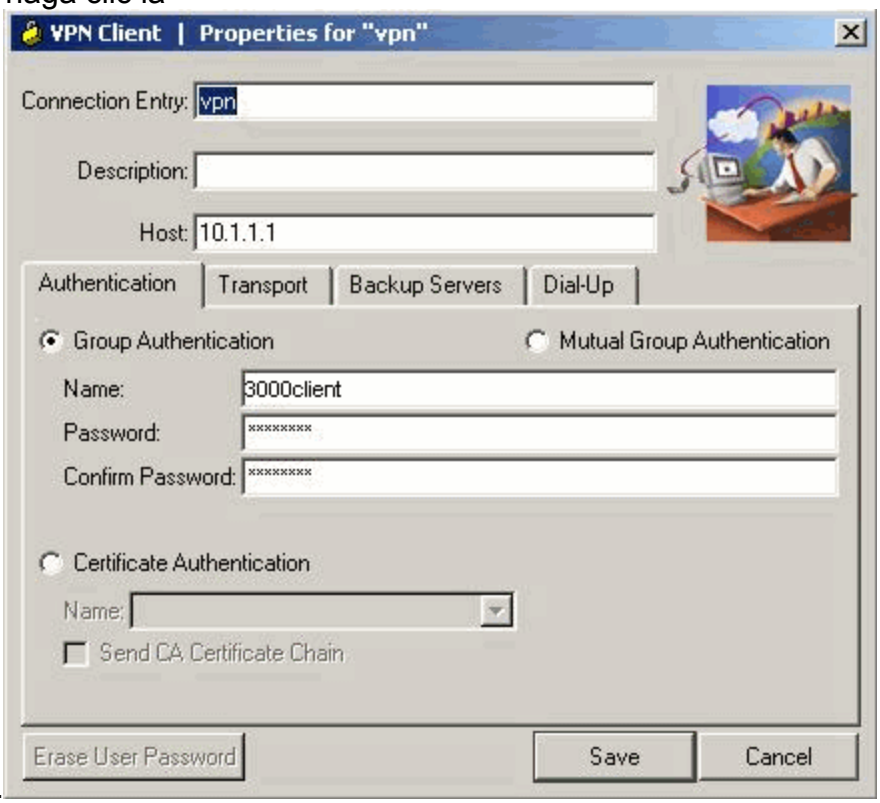
Configuración del cliente VPN 4.8

Complete estos pasos para configurar al cliente VPN 4.8:

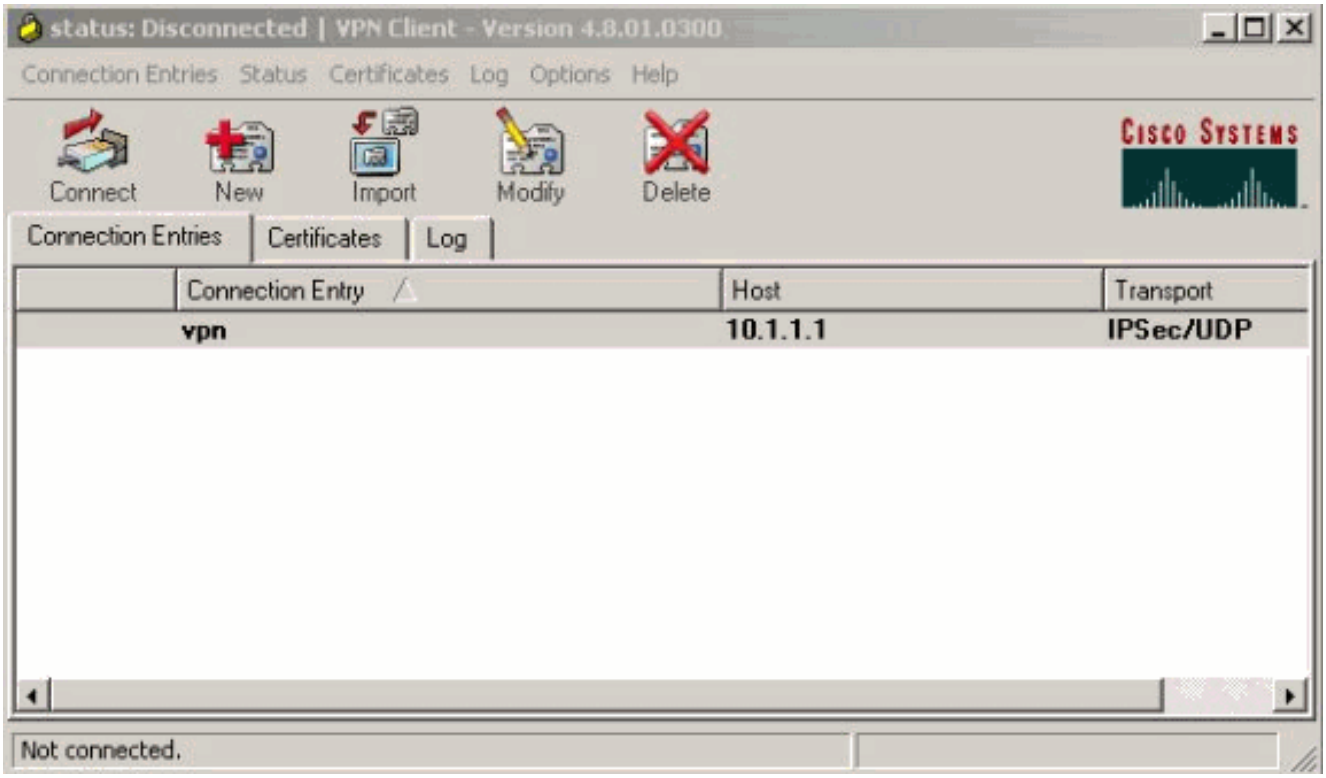
1. Elija el **Start (Inicio) > Programs (Programas) > Cisco Systems VPN Client (VPN Client de Cisco Systems) > al cliente VPN**.
2. Tecleo **nuevo** iniciar la nueva ventana de entrada de la conexión VPN del crear.



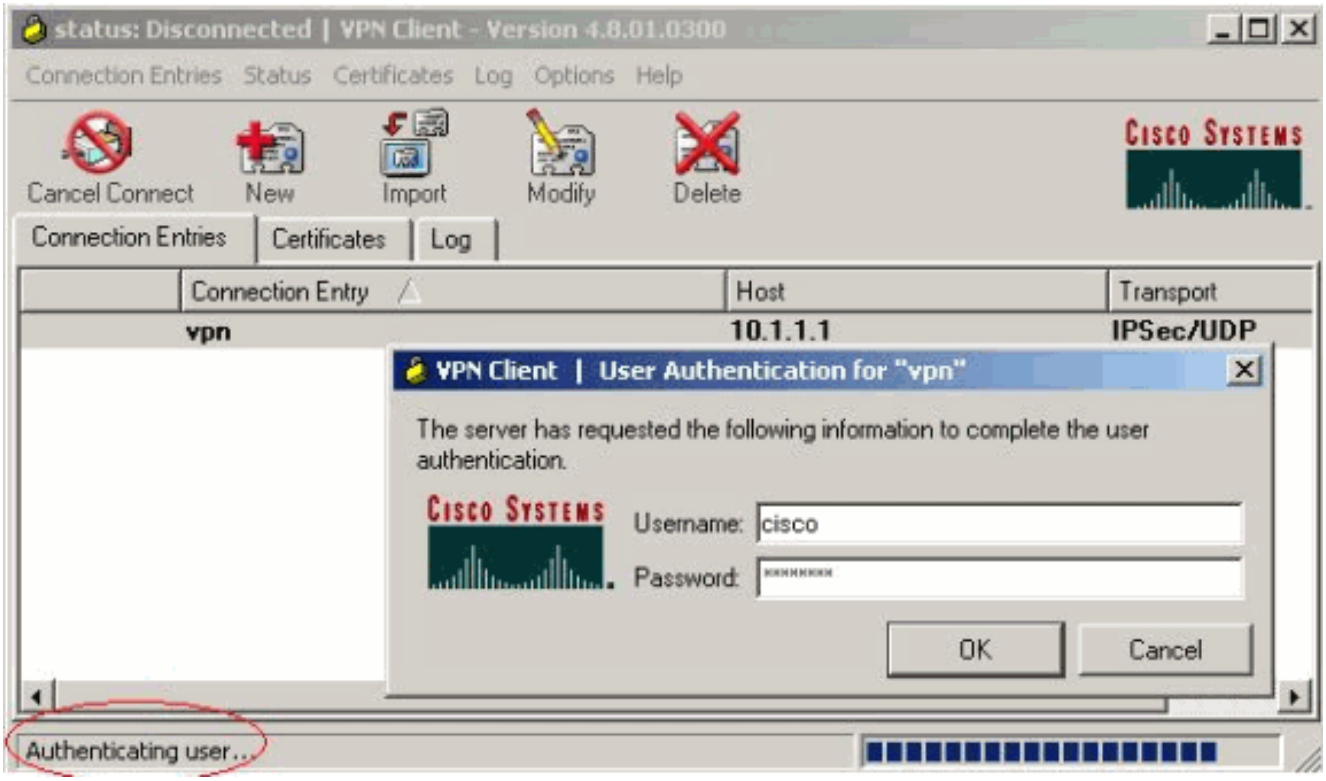
3. Ingrese el nombre del Entrada de conexión junto con una descripción. Ingrese el IP Address externo del router en el rectángulo del host. Después ingrese el nombre del grupo VPN y la contraseña y haga clic la **salvaguardia**.

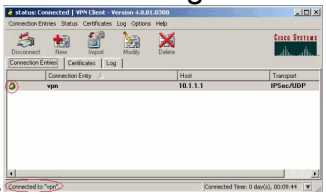


4. Haga clic en la conexión que usted quisiera utilizar y el tecleo **conecta de la** ventana principal del cliente
   VPN.



5. Cuando se le pregunte, ingrese la información del nombre de usuario y contraseña para el Xauth y haga clic la **AUTORIZACIÓN** para conectar con la red
   remota.



   El cliente VPN consigue conectado con el router en el sitio
   central. 

Habilitación de la tunelización dividida

Para habilitar el Túnel dividido para las conexiones VPN, aseegurese que usted tiene un Access Control List (ACL) configurado en el router. En este ejemplo, asocian al **comando access-list 108 al** grupo para los fines de tunelización dividida, y el túnel se forma a la red 14.38.X.X /16. Flujos de tráfico unencrypted a los dispositivos no en ACL 108 (por ejemplo, Internet).

```
access-list 108 permit ip 172.18.124.0 0.0.255.255 10.16.20.0 0.0.0.255
```

Aplicar ACL en las propiedades del grupo.

```
crypto isakmp client configuration group 3000client key cisco123 dns 10.1.1.10 wins 10.1.1.20
domain cisco.com pool ippool acl 108
```

Configure la característica del retraso del servidor de RADIUS

Cuando el servidor de RADIUS primario hace inasequible, el router Conmutación por falla al servidor de RADIUS de reserva activo siguiente. El router continuará utilizando al servidor RADIUS secundario para siempre, incluso si el servidor primario está disponible. El servidor primario es generalmente rendimiento alto y el servidor preferido. Si el servidor secundario no está disponible, la base de datos local se puede utilizar para la autenticación usando la conexión con el sistema de autenticación aaa userauthen el comando local del RADIUS de grupo.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Esto se hace salir de los **comandos show** relevantes:

```
vpn2621#show crypto isakmp sadst             src             state          conn-id
slot10.1.1.1  10.0.0.1   QM_IDLE          3       0vpn2621#show crypto ipsec sa interface:
Ethernet0/0    Crypto map tag: clientmap, local addr. 10.1.1.1   local  ident
(addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0)   remote ident (addr/mask/prot/port):
(10.16.20.2/255.255.255.255/0/0)   current_peer: 10.0.0.1     PERMIT, flags={}    #pkts encaps:
5, #pkts encrypt: 5, #pkts digest 5    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
#pkts compressed: 0, #pkts decompressed: 0    #pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0    #send errors 0, #recv errors 0     local crypto endpt.: 10.1.1.1,
remote crypto endpt.: 10.0.0.1     path mtu 1500, media mtu 1500     current outbound spi:
77AFCCFA     inbound esp sas:      spi: 0xC7AC22AB(3349947051)        transform: esp-3des esp-
sha-hmac ,        in use settings ={Tunnel, }        slot: 0, conn id: 2000, flow_id: 1, crypto
map: clientmap        sa timing: remaining key lifetime (k/sec): (4608000/3444)        IV size:
8 bytes        replay detection support: Y     inbound ah sas:     inbound pcp sas:     outbound
esp sas:      spi: 0x77AFCCFA(2008009978)        transform: esp-3des esp-sha-hmac ,        in
use settings ={Tunnel, }        slot: 0, conn id: 2001, flow_id: 2, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4608000/3444)        IV size: 8 bytes        replay
detection support: Y     outbound ah sas:     outbound pcp sas:   local  ident
(addr/mask/prot/port): (172.18.124.0/255.255.255.0/0/0)   remote ident (addr/mask/prot/port):
(10.16.20.2/255.255.255.255/0/0)   current_peer: 10.0.0.1     PERMIT, flags={}#pkts encaps: 4,
#pkts encrypt: 4, #pkts digest 4    #pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6    #pkts
compressed: 0, #pkts decompressed: 0    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0    #send errors 0, #recv errors 0     local crypto endpt.: 10.1.1.1, remote
crypto endpt.: 10.0.0.1     path mtu 1500, media mtu 1500     current outbound spi: 2EE5BF09
inbound esp sas:      spi: 0x3565451F(895829279)        transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }        slot: 0, conn id: 2002, flow_id: 3, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607999/3469)        IV size: 8 bytes        replay
```

```
detection support: Y     inbound ah sas:                inbound pcp sas:     outbound esp sas:
spi: 0x2EE5BF09(786808585)        transform: esp-3des esp-sha-hmac ,        in use settings
={Tunnel, }        slot: 0, conn id: 2003, flow_id: 4, crypto map: clientmap        sa timing:
remaining key lifetime (k/sec): (4607999/3469)        IV size: 8 bytes        replay detection
support: Y     outbound ah sas:     outbound pcp sas:vpn2621#show crypto engine connections
active    ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt   3
Ethernet0/0     10.1.1.1  set    HMAC_SHA+3DES_56_C        0        02000 Ethernet0/0
10.1.1.1  set    HMAC_SHA+3DES_56_C        0        52001 Ethernet0/0     10.1.1.1  set
HMAC_SHA+3DES_56_C        5        02002 Ethernet0/0     10.1.1.1  set    HMAC_SHA+3DES_56_C
0        62003 Ethernet0/0     10.1.1.1  set    HMAC_SHA+3DES_56_C        4        0vpn2621#show
crypto engine accelerator statisticVirtual Private Network (VPN) Module in aim slot :
0Statistics for Hardware VPN Module since the last clear of counters 5570 seconds ago
14 packets in                        14 packets out             0 packet overruns
0 output packets dropped             0 packets decompressed              0 packets compressed
0 compressed bytes in                0 uncompressed bytes in            0 decompressed bytes
out             0 compressed bytes out             0 packets bypass compression         0
packets abort compression             0 packets fail decompression         0 packets fail
compression             7 packets decrypted                  7 packets encrypted           532
bytes decrypted                  532 bytes encrypted           784 bytes before decrypt
19200 bytes after encrypt             0 paks/sec in                        0 paks/sec out
0 Kbits/sec decrypted                0 Kbits/sec encrypted        Last 5 minutes:            14
packets in                          14 packets out            7 packets decrypted
7 packets encrypted          532 bytes decrypted                  420 bytes encrypted
784 bytes before decrypt             672 bytes after encrypt            0 paks/sec in
0 paks/sec out            0 Kbits/sec decrypted                0 Kbits/sec encrypted
rx_no_endp:          0  rx_hi_discards:       0    fw_failure:              0    invalid_sa:
0  invalid_flow:         0    cgx_errors              0    fw_qs_filled:        0
fw_resource_lock:     0    lotx_full_err:          0    null_ip_error:       0  pad_size_error:
0    out_bound_dh_acc:       0    esp_auth_fail:       0  ah_auth_failure:      0
crypto_pad_error:       0    ah_prot_absent:      0  ah_seq_failure:       0    ah_spi_failure:
0    esp_prot_absent:     0  esp_seq_fail:         0    esp_spi_failure:        0
obound_sa_acc:       0  invalid_sa:           0    out_bound_sa_flow:      0    invalid_dh:
0  bad_keygroup:         0    out_of_memory:          0    no_sh_secret:        0  no_skeys:
0    invalid_cmd:            0    dsp_coproc_err:      0  comp_unsupported:     0
pak_too_big:            0    null packets:        0    pak_mp_length_spec_fault:      0 cmd
queue errors:      0    tx_lo_queue_size_max      0 cmd_unimplemented:      0    Interrupts:
439  Immed:      0  HiPri ints:      14    LoPri ints:    425  POST Errs:      0 Alerts:      0
Unk Cmds:        0  UnexpCmds:      0    cgx_cmd_pending:0   packet_loop_max:
0packet_loop_limit: 0vpn2621#sh crypto engine configuration         crypto engine name:  Virtual
Private Network (VPN) Module        crypto engine type:  hardware              Product Name:
AIM-VPN/BP             Configuration:  0x000109010F00F00784000000                          :
0x995FB1441BA279D5BD46CF6C                          :  0xECE77614C30835CB0A000300
:  0x00000000000000000000000000          CryptIC Version:  001.000              CGX Version:
001.009             CGX Reserved:  0x000F                PCDB info:  0x07F0 0x0084 0x0000
Serial Number:  0x5F9944B1A21BD57946BD                       :  0x6CCFE7EC14768C3CB35
DSP firmware version:  000.010     DSP Bootstrap Version:  000.003        DSP Bootstrap Info:
0x0000              Compression:  Yes                    DES:  Yes                     3
DES:  Yes                  AES CBC:  No                  AES CNTR:  No     Maximum buffer
length:  4096          Maximum DH index:  0210          Maximum SA index:  0420        Maximum
Flow index:  0840      Maximum RSA key size:  0000     crypto engine in slot:  0
platform:  VPN hardware accelerator   Crypto Adjacency Counts:               Lock Count:  0
Unlock Count:  0        crypto lib version:  16.0.0         ipsec lib version:  2.0.0
```

Troubleshooting

Use esta sección para resolver problemas de configuración.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- ¿**IPSec del debug crypto**? Información del debug de las visualizaciones sobre las conexiones del IPSec.
- ¿**isakmp del debug crypto**? La información del debug de las visualizaciones sobre las conexiones del IPSec, y muestra el primer conjunto de los atributos que se niega debido a las incompatibilidades en los ambos extremos.
- ¿**motor del debug crypto**? Visualiza la información del motor de criptografía.
- ¿**autenticación aaa del debug**? Visualiza la información sobre el Terminal Access Controller Access Control System AAA/más la autenticación (TACACS+).
- ¿**debug aaa authorization raduis**? Visualiza la información sobre la autorización AAA/TACACS+.
- ¿**radio del debug**? Información de las visualizaciones sobre la comunicación del troubleshooting entre el servidor de RADIUS y el router.

'Resultado de debug'

En esta sección encontrará información de depuración del router que también puede utilizar para solucionar los problemas de su configuración.

Registros de router

```
vpn2621#show debugGeneral OS:  AAA Authentication debugging is on  AAA Authorization debugging
is onRadius protocol debugging is onRadius packet protocol debugging is onCryptographic
Subsystem:  Crypto ISAKMP debugging is on  Crypto Engine debugging is on  Crypto IPSEC debugging
is onvpn2621#*ISAKMP (0:0): received packet from 10.0.0.1 dport 500 sport 500 Global (N) NEW
SA*ISAKMP: Created a peer struct for 10.0.0.1, peer port 500*ISAKMP: Locking peer struct
0x83166B20, IKE refcount 1 for          crypto_ikmp_config_initialize_sa*ISAKMP (0:0): Setting
client config settings 82F0F82C*ISAKMP (0:0): (Re)Setting client xauth list  and state*ISAKMP:
local port 500, remote port 500*ISAKMP: insert sa successfully sa = 83165694*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 3 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!/en/US/docs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html-
snip/en/US/docs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html/en/US/d
ocs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html/en/US/docs/net_mgmt
/wan_service_administrator/1.1/administrator/guide/getstart.html!--- ISAKMP values are
acceptable and then the router continues with the !--- ISAKMP negotiation process.*ISAKMP (0:1):
Checking ISAKMP transform 9 against priority 3 policy*ISAKMP:      encryption 3DES-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 (0:1): atts are
acceptable. Next payload is 3*CryptoEngine0: generate alg parameter*CryptoEngine0:
CRYPTO_ISA_DH_CREATE(hw)(ipsec)*CRYPTO_ENGINE: Dh phase 1 status: 0*ISAKMP (0:1): processing KE
payload. message ID = 0*CryptoEngine0: generate alg parameter*CryptoEngine0:
CRYPTO_ISA_DH_SHARE_SECRET(hw)(ipsec)*ISAKMP (0:1): processing NONCE payload. message ID =
0*ISAKMP (0:1): vendor ID is NAT-T v2*AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-
```

1*AAA/MEMORY: create_user (0x830E12E8) user='3000client' ruser='NULL' ds0=0 port='ISAKMP-ID-AUTH' rem_addr='10.0.0.1' authen_type=NONE service=LOGIN priv=0 initial_task_id='0', vrf= (id=0)*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-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): Port='ISAKMP-ID-AUTH' list='groupauthor' service=NET*AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(54534875) user='3000client'*ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): send AV service=ike*ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): send AV protocol=ipsec*ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): found list "groupauthor"*ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): Method=LOCAL*AAA/AUTHOR (54534875): Post authorization status = PASS_ADD*ISAKMP: got callback 1*AAA/AUTHOR/IKE: Processing AV service=ike*AAA/AUTHOR/IKE: Processing AV protocol=ipsec*AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123*AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com*AAA/AUTHOR/IKE: Processing AV addr-pool*ippool*AAA/AUTHOR/IKE: Processing AV key-exchange=ike*AAA/AUTHOR/IKE: Processing AV group-lock*0*AAA/AUTHOR/IKE: Processing AV timeout*0*AAA/AUTHOR/IKE: Processing AV idletime*0*AAA/AUTHOR/IKE: Processing AV inacl*108*AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0*AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0*CryptoEngine0: create ISAKMP SKEYID for conn id 1*CryptoEngine0: CRYPTO_ISA_SA_CREATE(hw)(ipsec)*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   : 10.1.1.1   protocol   : 17   port : 0   length   : 8*ISAKMP (1): Toine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*ISAKMP (0:1): processing HASH payload. message ID = 0*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)tal payload length: 12*CryptoEngine0: generate hmac conte*ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1   spi 0, message ID = 0, sa = 83165694*ISAKMP (0:1): Process initial contact,bring down existing phase 1 and 2 SA's with local 10.1.1.1 remote 10.0.0.1 remote port 500*ISAKMP (0:1): returning IP addr to the address 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 17xt for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*ISAKMP (0:1): constructed HIS NAT-D*ISAKMP (0:1): constructed MINE NAT-D*ISAKMP (0:1): sending packet to 10.0.0.1 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 *AAA/MEMORY: free_user (0x830E12E8) user='3000client' ruser='NULL' port='ISAKMP-ID-AUTH' rem_addr='10.0.0.1' authen_type=NONE service=LOGIN priv=0 vrf= (id=0)*ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) AG_INIT_EXCH*CryptoEng*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 10.0.0.1*CryptoEngine0: clear dh number for conn id 1*ISAKMP: Trying to insert a peer 10.0.0.1/500/, and inserted successfully.*ISAKMP (0:1): IKE_DPD is enabled, initializing timers*ISAKMP: set new node 2011892843 to CONF_XAUTH *CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*IPSEC(key_engine): got a queue event...*CryptoEngine0: CRYPTO_ISA_DH_DELETE(hw)(ipsec)*CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)*ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) QM_IDLE   *ISAKMP (0:1): purging node 2011892843*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 *ISAKMP (0:1): Need XAUTH*AAA: parse name=ISAKMP idb type=-1 tty=-1*AAA/MEMORY: create_user (0x830DE43C) user='NULL' ruser='NULL' ds0=0 port='ISAKMP' rem_addr='10.0.0.1' authen_type=ASCII service=LOGIN priv=0 initial_task_id='0', vrf= (id=0)*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 *AAA/AUTHEN/START (992119247): port='ISAKMP' list='userauthen' action=LOGIN service=LOGIN*AAA/AUTHEN/START (992119247): found list userauthen*AAA/AUTHEN/START (992119247): Method=radius (radius)*AAA/AUTHEN(992119247): Status=GETUSER*ISAKMP: got callback 1*ISAKMP: set new node -883516238 to CONF_XAUTH *ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2*ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*ISAKMP (0:1): initiating peer config to 10.0.0.1. ID = -883516238*CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)*ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) CONF_XAUTH   *ISAKMP (0:1): Input = IKE_MESG_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): retransmitting phase 2 CONF_XAUTH   -883516238 ...*ISAKMP (0:1): incrementing error counter on sa: retransmit phase 2*ISAKMP (0:1): incrementing error counter on sa: retransmit phase 2*ISAKMP (0:1): retransmitting phase 2 -883516238 CONF_XAUTH *ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) CONF_XAUTH   *ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) CONF_XAUTH   *CryptoEngine0:

CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*ISAKMP (0:1): processing transaction payload from 10.0.0.1. message ID = -883516238*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*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 -883516238 error FALSE reason "done with xauth request/reply exchange"*ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY*ISAKMP (0:1): Old State = IKE_XAUTH_REQ_SENT New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT *AAA/AUTHEN/CONT (992119247): continue_login (user='(undef)')*AAA/AUTHEN(992119247): Status=GETUSER*AAA/AUTHEN(992119247): Method=radius (radius)*AAA/AUTHEN(992119247): Status=GETPASS*AAA/AUTHEN/CONT (992119247): continue_login (user='cisco')*AAA/AUTHEN(992119247): Status=GETPASS*AAA/AUTHEN(992119247): Method=radius (radius)*RADIUS: Pick NAS IP for u=0x830DE43C tableid=0 cfg_addr=0.0.0.0 best_addr=10.1.1.1*RADIUS: ustruct sharecount=2*Radius: radius_port_info() success=0 radius_nas_port=1*RADIUS(00000000): **Send Access-Request to 172.18.124.96:1645 id 21645/4, len 72***RADIUS: authenticator F2 7F ED 86 2B D9 80 1F - 74 D7 8F 90 3B EF F0 D5*RADIUS: NAS-IP-Address [4] 6 10.1.1.1 *RADIUS: NAS-Port-Type [61] 6 Async [0]*RADIUS: User-Name [1] 9 "cisco"*RADIUS: Calling-Station-Id [31] 13 "10.0.0.1"*RADIUS: User-Password [2] 18 **RADIUS: Retransmit to (172.18.124.96:1645,1646) for id 21645/4*RADIUS: **Received from id 21645/4 172.18.124.96:1645, Access-Accept, len 62***RADIUS: authenticator 97 DF CB C8 74 AC 92 D6 - 3B D8 D9 DC 9E 85 94 35*RADIUS: Framed-IP-Address [8] 6 172.17.8.123 *RADIUS: Class [25] 36 *RADIUS: 43 49 53 43 4F 41 43 53 3A 30 30 30 30 31 38 32 [CISCOACS:0000182]*RADIUS: 62 2F 61 63 31 32 37 63 39 66 2F 74 6E 65 75 62 [b/ac127c9f/cisco]*RADIUS: 65 72 *RADIUS: saved authorization data for user 830DE43C at 830DB5FC*AAA/AUTHEN(992119247): Status=PASS*ISAKMP: got callback 1*ISAKMP: set new node -1874799558 to CONF_XAUTH *CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*ISAKMP (0:1): initiating peer config to 10.0.0.1. ID = -1874799558*CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)*ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) CONF_XAUTH *ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, IKE_AAA_CONT_LOGIN*ISAKMP (0:1): Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT New State = IKE_XAUTH_SET_SENT *AAA/MEMORY: free_user (0x830DE43C) user='cisco' ruser='NULL' port='ISAKMP' rem_addr='10.0.0.1' authen_type=ASCII service=LOGIN priv=0 vrf= (id=0)*ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) CONF_XAUTH *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*ISAKMP (0:1): processing transaction payload from 10.0.0.1. message ID = -1874799558*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*ISAKMP: Config payload ACK*ISAKMP (0:1): XAUTH ACK Processed*ISAKMP (0:1): deleting node -1874799558 error FALSE reason "done with transaction"*ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK*ISAKMP (0:1): Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE *ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE*ISAKMP (0:1): Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE *ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE *ISAKMP: set new node -1474156599 to QM_IDLE *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*ISAKMP (0:1): processing transaction payload from 10.0.0.1. message ID = -1474156599*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*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*AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-1*AAA/MEMORY: create_user (0x831663A0) user='3000client' ruser='NULL' ds0=0 port='ISAKMP-GROUP-AUTH' rem_addr='10.0.0.1' authen_type=NONE service=LOGIN priv=0 initial_task_id='0', vrf= (id=0)*ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST*ISAKMP (0:1): Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT *ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): Port='ISAKMP-GROUP-AUTH' list='groupauthor' service=NET*AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(3136771130) user='3000client'*ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): send AV service=ike*ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): send AV protocol=ipsec*ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): found list "groupauthor"*ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): Method=LOCAL*AAA/AUTHOR (3136771130): Post authorization status = PASS_ADD*ISAKMP: got callback 1* AAA/AUTHOR/IKE: Processing AV service=ike* AAA/AUTHOR/IKE: Processing AV protocol=ipsec* AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123* AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com*AAA/AUTHOR/IKE: Processing AV addr-pool*ippool*AAA/AUTHOR/IKE: Processing AV key-exchange=ike*AAA/AUTHOR/IKE:

Processing AV group-lock*0*AAA/AUTHOR/IKE: Processing AV timeout*0*AAA/AUTHOR/IKE: Processing AV idletime*0*AAA/AUTHOR/IKE: Processing AV inacl*108*AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0*AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0*ISAKMP (0:1): attributes sent in message:* Address: 0.2.0.0*ISAKMP (0:1): allocating address 10.16.20.1*ISAKMP: Sending private address: 10.16.20.1*ISAKMP: Sending IP4_DNS server address: 10.1.1.10*ISAKMP: Sending IP4_NBNS server address: 10.1.1.20*ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address: 86388*ISAKMP: Sending APPLICATION_VERSION string: Cisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-IK9S-M), Version 12.2(15)T2, RELEASE SOFTWARE (fc2)TAC Support: http://www.cisco.com/tacCopyright (c) 1986-2003 by cisco Systems, Inc.Compiled Thu 01-May-03 10:39 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: Sending split include name 108 network 172.18.124.0 mask 255.255.255.0 protocol 0, src port 0, dst port 0*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)*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*ISAKMP (0:1): responding to peer config from 10.0.0.1. ID = -1474156599*CryptoEngi*ISAKMP (0:1): deleting node -1474156599 error FALSE reason ""ne0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)*ISAKMP (0:1): sending packet to 10.0.0.1 my_por231*ISAKMP (0:1): processing SA payload. message ID = 2058744231*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 256t 500 peer_port 500 (R) CONF_ADDR *ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR*ISAKMP (0:1): Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE *AAA/MEMORY: free_user (0x831663A0) user='3000client' ruser='NULL' port='ISAKMP-GROUP-AUTH' rem_addr='10.0.0.1' authen_type=NONE service=LOGIN priv=0 vrf= (id=0)*ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE *ISAKMP: set new node 2058744231 to QM_IDLE *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*ISAKMP (0:1): processing HASH payload. message ID = 2058744*ISAKMP: SA life type in seconds*ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags=

0x2*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*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*IPSEC(spi_response): getting spi 3233689542 for SA from 10.1.1.1 to 10.0.0.1 for prot 3*ISAKMP: received ke message (2/1)*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)*ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) QM_IDLE *ISAKMP (0:1): Node 2058744231, 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 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*CryptoEngine0: ipsec allocate flow*CryptoEngine0: ipsec allocate flow*CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)*CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)*ISAKMP: Locking peer struct 0x83166B20, IPSEC refcount 1 for for stuff_ke*!--- A matching IPSec policy has been negotiated and authenticated. !--- Next, the SA's are set up.***ISAKMP (0:1): Creating IPSec SAs*** **inbound SA from 10.0.0.1 to 10.1.1.1 (f/i) 0/ 0 (proxy 10.16.20.1 to 10.1.1.1)*** **has spi 0xC0BE2FC6 and conn_id 420 and flags 2*** **lifetime of 2147483 seconds*** **has client flags 0x0*** **outbound SA from 10.1.1.1 to 10.0.0.1 (f/i) 0/ 0 (proxy 10.1.1.1** to 10.16.20.1)*ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE *ISAKMP: set new node 1101355775 to QM_IDLE *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*ISAKMP (0:1): processing HASH payload. message ID = 1101355775*ISAKMP (0:1): processing SA payload. message ID = 1101355775*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 *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1, local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1, local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *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 *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),   protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb,   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *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 *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),   protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb,   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *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 *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),   remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),   remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),   protocol= PCP, transform= comp-lzs ,   lifedur= 0s and 0kb,   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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*CryptoEngine0: validate proposal request*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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*CryptoEngine0: validate proposal request*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2*CryptoEngine0: validate proposal request*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(spi_response): getting spi 3438126624 for SA from 10.1.1.1 to 10.0.0.1 for prot 3*ISAKMP: received ke message (2/1)*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)*ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) QM_IDLE *ISAKMP (0:1): Node 1101355775, 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 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*CryptoEngine0: ipsec allocate flow*CryptoEngine0: ipsec allocate flow*CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)*CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)*ISAKMP: Locking peer struct 0x83166B20, IPSEC refcount 2 for for stuff_ke***ISAKMP (0:1): Creating IPSec SAs* inbound SA from 10.0.0.1 to 10.1.1.1 (f/i) 0/ 0 (proxy 10.16.20.1 to 172.18.124.0)* has spi 0xCCEDA620 and conn_id 422 and flags 2* lifetime of 2147483 seconds* has client flags 0x0* outbound SA from 10.1.1.1 to 10.0.0.1 (f/i) 0/ 0 (proxy 172.18.124.0** to 10.16.20.1)

Registros del cliente

Inicie el LogViewer en el cliente VPN para ver los registros. Aseegurese que el filtro está fijado al alto para todas las clases configuradas. Esto es una salida del registro de la muestra:

vpn2621#**show debug**General OS: AAA Authentication debugging is on AAA Authorization debugging is onRadius protocol debugging is onRadius packet protocol debugging is onCryptographic Subsystem: Crypto ISAKMP debugging is on Crypto Engine debugging is on Crypto IPSEC debugging is onvpn2621#*ISAKMP (0:0): **received packet from 10.0.0.1 dport 500 sport 500 Global (N) NEW SA***ISAKMP: Created a peer struct for 10.0.0.1, peer port 500*ISAKMP: Locking peer struct 0x83166B20, IKE refcount 1 for crypto_ikmp_config_initialize_sa*ISAKMP (0:0): Setting client config settings 82F0F82C*ISAKMP (0:0): (Re)Setting client xauth list and state*ISAKMP: local port 500, remote port 500*ISAKMP: insert sa successfully sa = 83165694*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 3 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!/en/US/docs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html-snip/en/US/docs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html/en/US/docs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html/en/US/docs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html*!--- ISAKMP values are acceptable and then the router continues with the !--- ISAKMP negotiation process.***ISAKMP (0:1): Checking ISAKMP transform 9 against priority 3 policy*ISAKMP: encryption 3DES-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 (0:1): atts are acceptable. Next payload is 3***CryptoEngine0: generate alg parameter*CryptoEngine0: CRYPTO_ISA_DH_CREATE(hw)(ipsec)*CRYPTO_ENGINE: Dh phase 1 status: 0*ISAKMP (0:1): processing KE payload. message ID = 0*CryptoEngine0: generate alg parameter*CryptoEngine0: CRYPTO_ISA_DH_SHARE_SECRET(hw)(ipsec)*ISAKMP (0:1): processing NONCE payload. message ID = 0*ISAKMP (0:1): vendor ID is NAT-T v2*AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1*AAA/MEMORY: create_user (0x830E12E8) user='3000client' ruser='NULL' ds0=0 port='ISAKMP-ID-AUTH' rem_addr='10.0.0.1' authen_type=NONE service=LOGIN priv=0 initial_task_id='0', vrf= (id=0)*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-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): Port='ISAKMP-ID-AUTH' list='groupauthor' service=NET*AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(54534875) user='3000client'*ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): send AV service=ike*ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): send AV protocol=ipsec*ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): found list "groupauthor"*ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): Method=LOCAL*AAA/AUTHOR (54534875): Post authorization status = PASS_ADD*ISAKMP: got callback 1*AAA/AUTHOR/IKE: Processing AV service=ike*AAA/AUTHOR/IKE: Processing AV protocol=ipsec*AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123*AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com*AAA/AUTHOR/IKE: Processing AV addr-pool*ippool*AAA/AUTHOR/IKE: Processing AV key-exchange=ike*AAA/AUTHOR/IKE: Processing AV group-lock*0*AAA/AUTHOR/IKE: Processing AV timeout*0*AAA/AUTHOR/IKE: Processing AV idletime*0*AAA/AUTHOR/IKE: Processing AV inacl*108*AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0*AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0*CryptoEngine0: create ISAKMP SKEYID for conn id 1*CryptoEngine0: CRYPTO_ISA_SA_CREATE(hw)(ipsec)*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 : 10.1.1.1 protocol : 17 port : 0 length : 8*ISAKMP (1): Toine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*ISAKMP (0:1): processing HASH payload. message ID = 0*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)tal payload length: 12*CryptoEngine0: generate hmac conte*ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1 spi 0, message ID = 0, sa = 83165694*ISAKMP (0:1): Process initial contact,bring down existing phase 1 and 2 SA's with local 10.1.1.1 remote 10.0.0.1 remote port 500*ISAKMP (0:1): returning IP addr to the address 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 17xt for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*ISAKMP (0:1): constructed HIS NAT-D*ISAKMP (0:1): constructed MINE NAT-D*ISAKMP (0:1): sending packet to 10.0.0.1 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 *AAA/MEMORY: free_user (0x830E12E8) user='3000client' ruser='NULL' port='ISAKMP-ID-AUTH' rem_addr='10.0.0.1' authen_type=NONE service=LOGIN priv=0 vrf= (id=0)*ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) AG_INIT_EXCH*CryptoEng*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 10.0.0.1*CryptoEngine0: clear dh number for conn id 1*ISAKMP: Trying to insert a peer 10.0.0.1/500/, and inserted successfully.*ISAKMP (0:1): IKE_DPD is enabled, initializing timers*ISAKMP: set new node 2011892843 to CONF_XAUTH *CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*IPSEC(key_engine): got a queue event...*CryptoEngine0: CRYPTO_ISA_DH_DELETE(hw)(ipsec)*CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)*ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) QM_IDLE *ISAKMP (0:1): purging

node 2011892843*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 *ISAKMP (0:1): Need XAUTH*AAA: parse name=ISAKMP idb type=-1 tty=-1*AAA/MEMORY: create_user (0x830DE43C) user='NULL' ruser='NULL' ds0=0 port='ISAKMP' rem_addr='10.0.0.1' authen_type=ASCII service=LOGIN priv=0 initial_task_id='0', vrf= (id=0)*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 *AAA/AUTHEN/START (992119247): port='ISAKMP' list='userauthen' action=LOGIN service=LOGIN*AAA/AUTHEN/START (992119247): found list userauthen*AAA/AUTHEN/START (992119247): Method=radius (radius)*AAA/AUTHEN(992119247): Status=GETUSER*ISAKMP: got callback 1*ISAKMP: set new node -883516238 to CONF_XAUTH *ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2*ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*ISAKMP (0:1): initiating peer config to 10.0.0.1. ID = -883516238*CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)*ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) CONF_XAUTH   *ISAKMP (0:1): Input = IKE_MESG_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): retransmitting phase 2 CONF_XAUTH   -883516238 ...*ISAKMP (0:1): incrementing error counter on sa: retransmit phase 2*ISAKMP (0:1): incrementing error counter on sa: retransmit phase 2*ISAKMP (0:1): retransmitting phase 2 -883516238 CONF_XAUTH *ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) CONF_XAUTH   *ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) CONF_XAUTH   *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*ISAKMP (0:1): processing transaction payload from 10.0.0.1. message ID = -883516238*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*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 -883516238 error FALSE reason   "done with xauth request/reply exchange"*ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY*ISAKMP (0:1): Old State = IKE_XAUTH_REQ_SENT New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT *AAA/AUTHEN/CONT (992119247): continue_login (user='(undef)')*AAA/AUTHEN(992119247): Status=GETUSER*AAA/AUTHEN(992119247): Method=radius (radius)*AAA/AUTHEN(992119247): Status=GETPASS*AAA/AUTHEN/CONT (992119247): continue_login (user='cisco')*AAA/AUTHEN(992119247): Status=GETPASS*AAA/AUTHEN(992119247): Method=radius (radius)*RADIUS: Pick NAS IP for u=0x830DE43C tableid=0 cfg_addr=0.0.0.0 best_addr=10.1.1.1*RADIUS: ustruct sharecount=2*Radius: radius_port_info() success=0 radius_nas_port=1*RADIUS(00000000): **Send Access-Request to 172.18.124.96:1645 id 21645/4, len 72***RADIUS: authenticator F2 7F ED 86 2B D9 80 1F - 74 D7 8F 90 3B EF F0 D5*RADIUS: NAS-IP-Address   [4]   6   10.1.1.1   *RADIUS: NAS-Port-Type   [61] 6   Async [0]*RADIUS: User-Name   [1]   9   "cisco"*RADIUS: Calling-Station-Id [31] 13 "10.0.0.1"*RADIUS: User-Password   [2]   18 **RADIUS: Retransmit to (172.18.124.96:1645,1646) for id 21645/4*RADIUS: **Received from id 21645/4 172.18.124.96:1645, Access-Accept, len 62***RADIUS: authenticator 97 DF CB C8 74 AC 92 D6 - 3B D8 D9 DC 9E 85 94 35*RADIUS: Framed-IP-Address   [8]   6   172.17.8.123   *RADIUS: Class [25] 36 *RADIUS: 43 49 53 43 4F 41 43 53 3A 30 30 30 30 31 38 32 [CISCOACS:0000182]*RADIUS: 62 2F 61 63 31 32 37 63 39 66 2F 74 6E 65 75 62 [b/ac127c9f/cisco]*RADIUS: 65 72 *RADIUS: saved authorization data for user 830DE43C at 830DB5FC*AAA/AUTHEN(992119247): Status=PASS*ISAKMP: got callback 1*ISAKMP: set new node -1874799558 to CONF_XAUTH *CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*ISAKMP (0:1): initiating peer config to 10.0.0.1. ID = -1874799558*CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)*ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) CONF_XAUTH   *ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, IKE_AAA_CONT_LOGIN*ISAKMP (0:1): Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT New State = IKE_XAUTH_SET_SENT *AAA/MEMORY: free_user (0x830DE43C) user='cisco' ruser='NULL' port='ISAKMP' rem_addr='10.0.0.1' authen_type=ASCII service=LOGIN priv=0 vrf= (id=0)*ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) CONF_XAUTH   *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*ISAKMP (0:1): processing transaction payload from 10.0.0.1. message ID = -1874799558*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*ISAKMP: Config payload ACK*ISAKMP (0:1):   XAUTH ACK Processed*ISAKMP (0:1): deleting node -1874799558 error FALSE reason "done with transaction"*ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK*ISAKMP (0:1): Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE *ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE*ISAKMP (0:1): Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE *ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE *ISAKMP: set new node -1474156599 to QM_IDLE   *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*ISAKMP (0:1): processing transaction payload from 10.0.0.1. message ID = -1474156599*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0:

CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*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*AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-1*AAA/MEMORY: create_user (0x831663A0) user='3000client' ruser='NULL' ds0=0 port='ISAKMP-GROUP-AUTH' rem_addr='10.0.0.1' authen_type=NONE service=LOGIN priv=0 initial_task_id='0', vrf= (id=0)*ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST*ISAKMP (0:1): Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT *ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): Port='ISAKMP-GROUP-AUTH' list='groupauthor' service=NET*AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(3136771130) user='3000client'*ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): send AV service=ike*ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): send AV protocol=ipsec*ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): found list "groupauthor"*ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): Method=LOCAL*AAA/AUTHOR (3136771130): Post authorization status = PASS_ADD*ISAKMP: got callback 1* AAA/AUTHOR/IKE: Processing AV service=ike* AAA/AUTHOR/IKE: Processing AV protocol=ipsec* AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123* AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com*AAA/AUTHOR/IKE: Processing AV addr-pool*ippool*AAA/AUTHOR/IKE: Processing AV key-exchange=ike*AAA/AUTHOR/IKE: Processing AV group-lock*0*AAA/AUTHOR/IKE: Processing AV timeout*0*AAA/AUTHOR/IKE: Processing AV idletime*0*AAA/AUTHOR/IKE: Processing AV inacl*108*AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0*AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0*ISAKMP (0:1): attributes sent in message:*   Address: 0.2.0.0*ISAKMP (0:1): allocating address 10.16.20.1*ISAKMP: Sending private address: 10.16.20.1*ISAKMP: Sending IP4_DNS server address: 10.1.1.10*ISAKMP: Sending IP4_NBNS server address: 10.1.1.20*ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address: 86388*ISAKMP: Sending APPLICATION_VERSION string: Cisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-IK9S-M), Version 12.2(15)T2, RELEASE SOFTWARE (fc2)TAC Support: http://www.cisco.com/tacCopyright (c) 1986-2003 by cisco Systems, Inc.Compiled Thu 01-May-03 10:39 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: Sending split include name 108 network 172.18.124.0 mask 255.255.255.0 protocol 0, src port 0, dst port 0*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)*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*ISAKMP (0:1): responding to peer config from 10.0.0.1. ID = -1474156599*CryptoEngi*ISAKMP (0:1): deleting node -1474156599 error FALSE reason ""ne0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)*ISAKMP (0:1): sending packet to 10.0.0.1 my_por231*ISAKMP (0:1): processing SA payload. message ID = 2058744231*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 256t 500 peer_port 500 (R) CONF_ADDR   *ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR*ISAKMP (0:1): Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE *AAA/MEMORY: free_user (0x831663A0) user='3000client' ruser='NULL' port='ISAKMP-GROUP-AUTH' rem_addr='10.0.0.1' authen_type=NONE service=LOGIN priv=0 vrf= (id=0)*ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE   *ISAKMP: set new node 2058744231 to QM_IDLE *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*ISAKMP (0:1): processing HASH payload. message ID = 2058744*ISAKMP: SA life type in seconds*ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),   protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb,   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),   protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb,   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),   protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb,   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1),   remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1),   remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),   protocol= PCP, transform= comp-lzs ,   lifedur= 0s and 0kb,   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2*CryptoEngine0: validate proposal request*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 *CryptoEngine0: validate proposal*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*IPSEC(spi_response): getting spi 3233689542 for SA from 10.1.1.1 to 10.0.0.1 for prot 3*ISAKMP: received ke message (2/1)*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)*ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) QM_IDLE *ISAKMP (0:1): Node 2058744231, 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 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*CryptoEngine0: ipsec allocate flow*CryptoEngine0: ipsec allocate flow*CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)*CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)*ISAKMP: Locking peer struct 0x83166B20, IPSEC refcount 1 for for stuff_ke*!--- A matching IPSec policy has been negotiated and authenticated. !--- Next, the SA's are set up.***ISAKMP (0:1): Creating IPSec SAs*** **inbound SA from 10.0.0.1 to 10.1.1.1 (f/i) 0/ 0 (proxy 10.16.20.1 to 10.1.1.1)*** **has spi 0xC0BE2FC6 and conn_id 420 and flags 2*** **lifetime of 2147483 seconds*** **has client flags 0x0*** **outbound SA from 10.1.1.1 to 10.0.0.1 (f/i) 0/ 0 (proxy 10.1.1.1** to 10.16.20.1)*ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE *ISAKMP: set new node 1101355775 to QM_IDLE *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*ISAKMP (0:1): processing HASH payload. message ID = 1101355775*ISAKMP (0:1): processing SA payload. message ID = 1101355775*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 *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),   protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb,   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *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 *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),   protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb,   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *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 *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),   protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb,   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *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 *CryptoEngine0: validate proposal*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= 10.1.1.1, remote= 10.0.0.1,   local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),   remote_proxy= 10.16.20.1/255.255.255.255/0/0

(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= 10.1.1.1, remote= 10.0.0.1, local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2*CryptoEngine0: validate proposal request*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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*CryptoEngine0: validate proposal request*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (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*CryptoEngine0: validate proposal request*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2*CryptoEngine0: validate proposal request*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *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 *CryptoEngine0: validate proposal*ISAKMP (0:1): atts are acceptable.*IPSEC(spi_response): getting spi 3438126624 for SA from 10.1.1.1 to 10.0.0.1 for prot 3*ISAKMP: received ke message (2/1)*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)*ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) QM_IDLE *ISAKMP (0:1): Node 1101355775, 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 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)*CryptoEngine0: generate hmac context for conn id 1*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)*CryptoEngine0: ipsec allocate flow*CryptoEngine0: ipsec allocate flow*CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)*CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)*ISAKMP: Locking peer struct 0x83166B20, IPSEC refcount 2 for for stuff_ke***ISAKMP (0:1): Creating IPSec SAs* inbound SA from 10.0.0.1 to 10.1.1.1 (f/i) 0/ 0 (proxy 10.16.20.1 to 172.18.124.0)* has spi 0xCCEDA620 and conn_id 422 and flags 2* lifetime of 2147483 seconds* has client flags 0x0* outbound SA**

```
from 10.1.1.1  to 10.0.0.1     (f/i)  0/ 0         (proxy 172.18.124.0          to 10.16.20.1
)
```

Información Relacionada

- Página de soporte de la tecnología de RADIUS
- Página de Soporte de IPSec Negotiation/IKE Protocols
- Página de soporte para cliente Cisco VPN
- Request For Comments (RFC)
- Soporte Técnico y Documentación - Cisco Systems