Contenido

Introducción

Este documento ilustra la configuración del IPSec entre la característica de la función Easy VPN Remote de PIX del cliente de hardware y del Easy VPN Server disponible en versiones posteriores del software de Cisco IOS®. La característica Easy VPN Remote para PIX se presentó en PIX versión 6.2 y también se considera cliente de hardware/cliente EzVPN. Cuando el Easy VPN Remote se conecta a un dispositivo de cabecera, existe un mínimo de cinco asociaciones de seguridad (SA), que incluyen una asociación de Intercambio de claves de Internet (IKE) y cuatro de IPSec. Cuando Easy VPN Remote se conecta a la cabecera, negocia siempre dos SA de IPSec con la dirección IP de la interfaz exterior del PIX a cualquier dirección que haya detrás del servidor VPN. Esto se puede utilizar con fines de administración para conectarse a la interfaz exterior del PIX desde la red que hay detrás del router de Cisco IOS (mediante Secure Shell [SSH], Secure HTTP for PIX Device Manager [PDM] o Telnet). El SA se crea de forma predeterminada sin ninguna configuración, y los otros dos SA se crean para el tráfico de datos entre las redes que hay detrás del PIX y el router de Cisco IOS.

Refiera a PIX-a-PIX 6.x: Ejemplo de configuración fácil VPN (NEM) para más información sobre un escenario similar donde el PIX 506 6.x actúa como el Easy VPN Server.

Refiera al PIX/ASA 7.x VPN fácil con un ASA 5500 como el servidor y el PIX 506E como el ejemplo de configuración del cliente (NEM) para más información sobre un escenario similar donde el PIX/ASA 7.x actúa como el Easy VPN Server.

Refiera al PIX/ASA 7.x VPN fácil con un ASA 5500 como el servidor y Cisco 871 como el ejemplo de la configuración VNP remota sencilla para más información sobre un escenario similar donde el Cisco 871 Router actúa como el Easy VPN Remote.

Refiera al hardware cliente VPN en un dispositivo de seguridad de las 501/506 Series PIX con el ejemplo de configuración concentrador VPN 3000 para más información sobre un escenario

similar donde el Cisco VPN 3000 Concentrator actúa como el Easy VPN Server.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Firewall PIX que funciona con la versión de software 6.3(5)**Nota:** La característica fácil del cliente VPN en el PIX fue introducida en la versión 6.2.
- Router IOS de las Cisco 7200 Series que funciona con la versión de software 12.4(4)T1**Nota:** La característica del Easy VPN Server fue introducida en la versión 12.2(8)T).

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.

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:

Configuraciones

En este documento, se utilizan estas configuraciones:

- Router del Cisco IOS
- PIX

Router del Cisco IOS

```
ezvpn_server#show running-configBuilding
configuration...Current configuration : 1894
bytes!version 12.4service timestamps debug datetime
msecservice timestamps log datetime msecno service
password-encryption!hostname ezvpn_server!boot-start-
markerboot system disk1:c7200-adventerprisek9-mz.124-
4.T1.binboot-end-marker!!!--- Enable the authentication,
authorization, and accounting (AAA) !--- access control
model.aaa new-model!!!--- Enable X-Auth for user
authentication.aaa authentication login userauthen
local!--- Enable group authorization.aaa authorization
network groupauthor local!aaa session-id common!resource
policy!ip subnet-zeroip cef!!!!!!!!!!!!!!!!!!!!!--- For
local authentication of the IPSec user, !--- create the
user with password.username remoteuser1 password 0
remotepassusername cisco password 0 cisco!!!!--- Create
an Internet Security Association and Key Management
Protocol !--- (ISAKMP) policy for Phase 1 negotiations
for the hardware client.crypto isakmp policy 10 hash md5
authentication pre-share group 2!!--- Create a group
that will be used to specify the !--- Windows Internet
Name Service (WINS) and Domain Name System (DNS) !---
servers' addresses to the hardware client for
authentication.crypto isakmp client configuration group
hwclient key test123 dns 172.22.1.101 wins 172.22.1.102
domain cisco.com pool ippool!!!--- Create the Phase 2
Policy for actual data encryption.crypto ipsec
transform-set myset esp-des esp-md5-hmac!!--- Create a
dynamic map and apply the transform set that was created
above.crypto dynamic-map dynmap 10 set transform-set
myset!!!--- Create the actual crypto map, and apply !---
the aaa lists that were created earlier.crypto map
clientmap client authentication list userauthencrypto
map clientmap isakmp authorization list
groupauthorcrypto map clientmap client configuration
address respondcrypto map clientmap 10 ipsec-isakmp
dynamic dynmap!!!!!interface FastEthernet0/0 ip address
10.10.10.2 255.255.255.0 duplex half!--- Apply the
crypto map on the outside interface. crypto map
clientmap!interface ATM2/0 no ip address shutdown no atm
ilmi-keepalive!interface FastEthernet4/0 no ip address
shutdown duplex half!interface Ethernet5/0 ip address
172.22.1.1 255.255.255.0 duplex half!interface
Ethernet5/1 no ip address shutdown duplex half!interface
Ethernet5/2 no ip address shutdown duplex half!interface
Ethernet5/3 no ip address shutdown duplex half!!---
Create a pool of addresses to be assigned to the VPN
Clients.ip local pool ippool 172.22.1.50 172.22.1.70ip
classlessno ip http serverno ip http secure-
server!!!logging alarm informational!!!!control-
plane!!!!!!gatekeeper shutdown!!line con 0 stopbits
1line aux 0 stopbits 1line vty 0 4!!endezvpn_server#
```

PIX

```
pix506#show running-config: Saved:PIX Version 6.3(5)!---
```

```
Specify speed and duplex settings.interface ethernet0
autointerface ethernet1 autonameif ethernet0 outside
security0nameif ethernet1 inside security100enable
password WwXYvtKrnjXqGbu1 encryptedpasswd
2KFQnbNIdI.2KYOU encryptedhostname pix506domain-name
cisco.comfixup protocol dns maximum-length 512fixup
protocol ftp 21fixup protocol h323 h225 1720fixup
protocol h323 ras 1718-1719fixup protocol http 80fixup
protocol rsh 514fixup protocol rtsp 554fixup protocol
sip 5060fixup protocol sip udp 5060fixup protocol skinny
2000fixup protocol smtp 25fixup protocol sqlnet
1521fixup protocol tftp 69namespager lines 24mtu outside
1500mtu inside 1500!--- Define IP addresses for the
PIX's inside and outside interfaces.ip address outside
10.10.10.1 255.255.255.0ip address inside 172.16.1.1
255.255.255.0ip audit info action alarmip audit attack
action alarmpdm history enablearp timeout 14400!---
Define the outside router as the default gateway. !---
Typically this is the IP address of your ISP's
router.route outside 0.0.0.0 0.0.0.0 10.10.10.2 1timeout
xlate 3:00:00timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 rpc 0:10:00 h225 1:00:00timeout h323 0:05:00
mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00timeout sip-
disconnect 0:02:00 sip-invite 0:03:00timeout uauth
0:05:00 absoluteaaa-server TACACS+ protocol tacacs+aaa-
server TACACS+ max-failed-attempts 3aaa-server TACACS+
deadtime 10aaa-server RADIUS protocol radiusaaa-server
RADIUS max-failed-attempts 3aaa-server RADIUS deadtime
10aaa-server LOCAL protocol localno snmp-server
locationno snmp-server contactsnmp-server community
publicno snmp-server enable trapsfloodguard enabletelnet
timeout 5ssh timeout 5console timeout 0!--- Define the
VPN peer IP address.vpnclient server 10.10.10.2!---
Specify whether Client/PAT (Port Address Translation)
mode !--- is to be used or whether Network Extension
Mode (NEM) is to be used.vpnclient mode network-
extension-mode!--- Define Easy VPN Remote parameters. !-
-- This is the pre-shared key used in IKE
negotiation.vpnclient vpngroup hwclient password
********!--- This is the extended authentication
username and password.vpnclient username cisco password
********!---This enables vpnclient on the PIX.vpnclient
enableterminal width
80Cryptochecksum:fdbd365f0b4cdc6707a50efeeeb8ed44: end
```

Verificación

Comandos show de PIX y salida de ejemplo

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.

- ¿**comando vpnclient enable**? Habilita una conexión del Easy VPN Remote. En NEM el túnel está activo aun cuando no existe tráfico interesante para ser intercambiado con el servidor de cabecera Easy VPN.`pix506(config)#`**`vpnclient enable`**
- ¿**muestre la política isakmp crypto**? Visualiza los parámetros para cada política

IKE.pix506(config)#**show crypto isakmp policy** Default protection suite encryption algorithm: DES - Data Encryption Standard (56 bit keys). hash algorithm: Secure Hash Standard authentication method: Rivest-Shamir-Adleman Signature Diffie-Hellman group: #1 (768 bit) lifetime: 86400 seconds, no volume limitEste ejemplo muestra la salida del **comando show crypto isakmp policy** después de que habiliten al hardware cliente.pix506(config)#**show crypto isakmp policy** Protection suite of priority 65001 encryption algorithm: DES - Data Encryption Standard (56 bit keys). hash algorithm: Message Digest 5 authentication method: Pre-Shared Key with XAUTH Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limitProtection suite of priority 65002 encryption algorithm: DES - Data Encryption Standard (56 bit keys). hash algorithm: Message Digest 5 authentication method: Pre-Shared Key Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit

- ¿**el IPSec crypto de la demostración transforma**? Visualiza el IPSec actual transforma.pix506(config)#**show crypto ipsec transform**Este ejemplo muestra la salida del **comando show crypto ipsec transform** después de que habiliten al hardware cliente. Antes de que utilicen al **comando vpnclient enable**, había solamente un conjunto de protección predeterminada para el ISAKMP. Luego de ejecutar el comando, Easy VPN Remote crea automáticamente cuatro propuestas además del conjunto de protección predeterminada. Además, no hay IPSec transforma el conjunto antes de que utilicen al **comando enable**. El conjunto de transformaciones se crea de manera dinámica luego de la ejecución del comando.pix506(config)#**show crypto ipsec transform-set**Transform set _vpnc_tset_9: { esp-des esp-md5-hmac } will negotiate = { Tunnel, }, Transform set _vpnc_tset_10: { esp-null esp-md5-hmac } will negotiate = { Tunnel, }, Transform set _vpnc_tset_11: { esp-null esp-sha-hmac } will negotiate = { Tunnel, },
- ¿**muestre isakmp crypto sa**? Visualiza todo el IKE actual SA en un par.pix506(config)#**show crypto isakmp sa**Total : 1Embryonic : 0 dst src state pending created 10.10.10.2 10.10.10.1 QM_IDLE 0 2
- ¿**show vpnclient**? Información de la configuración del dispositivo del cliente VPN o del Easy VPN Remote de las visualizaciones.pix506(config)#**show vpnclient**LOCAL CONFIGURATIONvpnclient server 10.10.10.2vpnclient mode network-extension-modevpnclient vpngroup hwclient password ********vpnclient username cisco password ********vpnclient enableDOWNLOADED DYNAMIC POLICYCurrent Server : 10.10.10.2Primary DNS : 172.22.1.101Primary WINS : 172.22.1.102Default Domain : cisco.comPFS Enabled : NoSecure Unit Authentication Enabled : NoUser Authentication Enabled : NoBackup Servers : Deleted by order of the headend
- ¿**muestre IPSec crypto sa**? SA de IPSec de las visualizaciones construido entre los pares.pix506(config)#**show crypto ipsec sa** interface: outside Crypto map tag: _vpnc_cm, local addr. 10.10.10.1 local ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 10.10.10.2:500 PERMIT, flags={origin_is_acl,} #pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3 #pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0*!--- As shown here, ping packets were successfully exchanged !--- between the Easy VPN Remote (PIX) and the Easy VPN Server (IOS).*local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: 533f74a9 inbound esp sas: spi: 0xad0984cc(2903082188) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 4, crypto map: _vpnc_cm sa timing: remaining key lifetime (k/sec): (4607999/3001) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x533f74a9(1396667561) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 3, crypto map: _vpnc_cm sa timing: remaining key lifetime (k/sec): (4607999/3001) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 10.10.10.2:500 PERMIT, flags={origin_is_acl,} #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*!--- As shown here, ping packets were successfully exchanged !--- between hosts behind the Easy VPN Remote (PIX) and the Easy !--- VPN Server (IOS).* local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: 2eca448b inbound esp sas: spi: 0xc82c0695(3358328469) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2, crypto map: _vpnc_cm sa timing: remaining key lifetime (k/sec): (4607999/2997) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x2eca448b(785007755) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 1, crypto map: _vpnc_cm sa timing: remaining key lifetime (k/sec): (4607999/2988) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:

- ¿**muestre la lista de acceso**? Visualiza el contenido de las Listas de acceso.pix506(config)#**show crypto ipsec sa** interface: outside Crypto map tag: _vpnc_cm, local addr. 10.10.10.1 local ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 10.10.10.2:500 PERMIT, flags={origin_is_acl,} #pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3 #pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0*!--- As shown here, ping packets were successfully exchanged !--- between the Easy VPN Remote (PIX) and the Easy VPN Server (IOS).*local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: 533f74a9 inbound esp sas: spi: 0xad0984cc(2903082188) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 4, crypto map: _vpnc_cm sa timing: remaining key lifetime (k/sec): (4607999/3001) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x533f74a9(1396667561) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 3, crypto map: _vpnc_cm sa timing: remaining key lifetime (k/sec): (4607999/3001) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 10.10.10.2:500 PERMIT, flags={origin_is_acl,} #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*!--- As shown here, ping packets were successfully exchanged !--- between hosts behind the Easy VPN Remote (PIX) and the Easy !--- VPN Server (IOS).* local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: 2eca448b inbound esp sas: spi: 0xc82c0695(3358328469) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2, crypto map: _vpnc_cm sa timing: remaining key lifetime (k/sec): (4607999/2997) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x2eca448b(785007755) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 1, crypto map: _vpnc_cm sa timing: remaining key lifetime (k/sec): (4607999/2988) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:

Comandos show del IOS y ejemplo de resultado

- ¿**muestre isakmp crypto sa**? Visualiza todo el IKE actual SA en un par.ezvpn_server#**show crypto isakmp sa** IPv4 Crypto ISAKMP SAdst src state conn-id slot status10.10.10.2 10.10.10.1 QM_IDLE 1026 0 ACTIVE
- ¿**muestre IPSec crypto sa**? SA de IPSec de las visualizaciones construido entre los pares.ezvpn_server#**show crypto ipsec sa***!--- As shown above, ping packets were successfully exchanged !--- between the Easy VPN Remote (PIX) and the Easy VPN Server (IOS) !--- as well as hosts behind them.*interface: FastEthernet0/0 Crypto map tag: clientmap, local addr 10.10.10.2 protected vrf: (none) local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0) current_peer 10.10.10.1 port 500 PERMIT, flags={} #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3 #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1 path mtu 1500, ip mtu 1500 current outbound spi: 0xAD0984CC(2903082188) inbound esp sas: spi: 0x533F74A9(1396667561) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } conn id: 21, flow_id: SW:21, crypto map: clientmap sa timing: remaining key

```
lifetime (k/sec): (4470133/2836) IV size: 8 bytes replay detection support: Y Status: ACTIVE
inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xAD0984CC(2903082188) transform:
esp-des esp-md5-hmac , in use settings ={Tunnel, } conn id: 22, flow_id: SW:22, crypto map:
clientmap sa timing: remaining key lifetime (k/sec): (4470133/2834) IV size: 8 bytes replay
detection support: Y Status: ACTIVE outbound ah sas: outbound pcp sas: protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0) current_peer 10.10.10.1 port 500 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 not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors
0 local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1 path mtu 1500, ip mtu
1500 current outbound spi: 0xC82C0695(3358328469) inbound esp sas: spi:
0x2ECA448B(785007755) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } conn id:
23, flow_id: SW:23, crypto map: clientmap sa timing: remaining key lifetime (k/sec):
(4589382/2832) IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas:
inbound pcp sas: outbound esp sas: spi: 0xC82C0695(3358328469) transform: esp-des esp-md5-
hmac , in use settings ={Tunnel, } conn id: 24, flow_id: SW:24, crypto map: clientmap sa
timing: remaining key lifetime (k/sec): (4589382/2830) IV size: 8 bytes replay detection
support: Y Status: ACTIVE outbound ah sas: outbound pcp sas:
```

Troubleshooting

Use esta sección para resolver problemas de configuración.

Si ha configurado el Remoto VPN Easy (PIX) y el Servidor VPN Easy (IOS) como se describe en este documento y todavía tiene problemas, recopile el resultado de la depuración del PIX y del IOS y el resultado del comando show para que el Centro de asistencia técnica de Cisco (TAC) lo analice. Consulte también Solución de problemas de PIX para pasar el tráfico de datos en un túnel IPSec establecido o Solución de problemas de seguridad IP – Información y uso de los comandos de depuración. Habilitar depuración de IPSec en el PIX.

Comandos de depuración PIX y salida de ejemplo

Comandos de depuración PIX

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

- ¿**IPSec del debug crypto**? Visualiza los IPSec Negotiations de la fase 2.
- ¿**isakmp del debug crypto**? Visualiza negociaciones ISAKMP de la fase 1.

Salida de muestra PIX

```
ezvpn_server#show crypto ipsec sa!--- As shown above, ping packets were successfully exchanged
!--- between the Easy VPN Remote (PIX) and the Easy VPN Server (IOS) !--- as well as hosts
behind them.interface: FastEthernet0/0 Crypto map tag: clientmap, local addr 10.10.10.2
protected vrf: (none) local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident
(addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0) current_peer 10.10.10.1 port 500 PERMIT,
flags={} #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3 #pkts decaps: 3, #pkts decrypt: 3,
#pkts verify: 3 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr.
failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0
local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1 path mtu 1500, ip mtu 1500
current outbound spi: 0xAD0984CC(2903082188) inbound esp sas: spi: 0x533F74A9(1396667561)
transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } conn id: 21, flow_id: SW:21,
crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4470133/2836) IV size: 8 bytes
replay detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas:
```

```
spi: 0xAD0984CC(2903082188) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } conn
id: 22, flow_id: SW:22, crypto map: clientmap sa timing: remaining key lifetime (k/sec):
(4470133/2834) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound ah sas:
outbound pcp sas: protected vrf: (none) local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0) current_peer 10.10.10.1 port
500 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 not decompressed: 0, #pkts decompress failed: 0 #send errors 0,
#recv errors 0 local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1 path mtu 1500,
ip mtu 1500 current outbound spi: 0xC82C0695(3358328469) inbound esp sas: spi:
0x2ECA448B(785007755) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } conn id: 23,
flow_id: SW:23, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4589382/2832)
IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas:
outbound esp sas: spi: 0xC82C0695(3358328469) transform: esp-des esp-md5-hmac , in use settings
={Tunnel, } conn id: 24, flow_id: SW:24, crypto map: clientmap sa timing: remaining key lifetime
(k/sec): (4589382/2830) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound ah
sas: outbound pcp sas:
```

Comandos de depuración del IOS y ejemplo de resultado

Comandos de depuración IOS

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

- ¿**IPSec del debug crypto**? Eventos detallados del IPSec de las visualizaciones.
- ¿**isakmp del debug crypto**? Muestra mensajes sobre los eventos IKE.
- ¿**motor del debug crypto**? Visualiza el tráfico se cifra que.

Salida de muestra del IOS

```
!--- As soon as the vpnclient enable command is issued on the PIX, !--- the IOS device receives
an IKE negotiation request.*Jan 20 16:48:22.267: ISAKMP (0:0): received packet from 10.10.10.1
dport 500 sport 500 Global (N) NEW SA*Jan 20 16:48:22.271: ISAKMP: Created a peer struct for
10.10.10.1, peer port 500*Jan 20 16:48:22.271: ISAKMP: New peer created peer = 0x6758C6D0
peer_handle = 0x80000026*Jan 20 16:48:22.271: ISAKMP: Locking peer struct 0x6758C6D0, refcount 1
for crypto_isakmp_process_block*Jan 20 16:48:22.271: ISAKMP:(0):Setting client config settings
6679B340*Jan 20 16:48:22.271: ISAKMP:(0):(Re)Setting client xauth list  and state*Jan 20
16:48:22.271: ISAKMP/xauth: initializing AAA request*Jan 20 16:48:22.271: ISAKMP: local port
500, remote port 500*Jan 20 16:48:22.271: insert sa successfully sa = 658E0874*Jan 20
16:48:22.271: ISAKMP:(0): processing SA payload. message ID = 0*Jan 20 16:48:22.271: ISAKMP:(0):
processing ID payload. message ID = 0*Jan 20 16:48:22.271: ISAKMP (0:0): ID payload next-payload
: 13type         : 11 group id     : hwclient protocol     : 17 port         : 0 length       :
16*Jan 20 16:48:22.271: ISAKMP:(0):: peer matches *none* of the profiles*Jan 20 16:48:22.271:
ISAKMP:(0): processing vendor id payload*Jan 20 16:48:22.271: ISAKMP:(0): vendor ID seems
Unity/DPD but major 215 mismatch*Jan 20 16:48:22.271: ISAKMP:(0): vendor ID is XAUTH*Jan 20
16:48:22.271: ISAKMP:(0): processing vendor id payload*Jan 20 16:48:22.271: ISAKMP:(0): vendor
ID is DPD*Jan 20 16:48:22.271: ISAKMP:(0): processing vendor id payload*Jan 20 16:48:22.271:
ISAKMP:(0): claimed IOS but failed authentication*Jan 20 16:48:22.271: ISAKMP:(0): processing
vendor id payload*Jan 20 16:48:22.271: ISAKMP:(0): vendor ID is Unity*Jan 20 16:48:22.271:
ISAKMP:(0): Authentication by xauth preshared*Jan 20 16:48:22.271: ISAKMP:(0):Checking ISAKMP
transform 1 against priority 10 policy*Jan 20 16:48:22.271: ISAKMP:      encryption AES-CBC*Jan
20 16:48:22.271: ISAKMP:      keylength of 256*Jan 20 16:48:22.271: ISAKMP:      hash SHA*Jan 20
16:48:22.271: ISAKMP:      default group 2*Jan 20 16:48:22.271: ISAKMP:      auth
XAUTHInitPreShared*Jan 20 16:48:22.271: ISAKMP:      life type in seconds*Jan 20 16:48:22.271:
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80 *Jan 20 16:48:22.271:
ISAKMP:(0):Encryption algorithm offered does not match policy!*Jan 20 16:48:22.271:
ISAKMP:(0):atts are not acceptable. Next payload is 3*Jan 20 16:48:22.271: ISAKMP:(0):Checking
ISAKMP transform 2 against priority 10 policy*Jan 20 16:48:22.271: ISAKMP:      encryption AES-
CBC*Jan 20 16:48:22.275: ISAKMP:      keylength of 256*Jan 20 16:48:22.275: ISAKMP:      hash
```

MD5*Jan 20 16:48:22.275: ISAKMP: default group 2*Jan 20 16:48:22.275: ISAKMP: auth XAUTHInitPreShared*Jan 20 16:48:22.275: ISAKMP: life type in seconds*Jan 20 16:48:22.275: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 *Jan 20 16:48:22.275: ISAKMP:(0):Encryption algorithm offered does not match policy!*Jan 20 16:48:22.275: ISAKMP:(0):atts are not acceptable. Next payload is 3*Jan 20 16:48:22.275: ISAKMP:(0):Checking ISAKMP transform 3 against priority 10 policy*Jan 20 16:48:22.275: ISAKMP: encryption AES-CBC*Jan 20 16:48:22.275: ISAKMP: keylength of 192*Jan 20 16:48:22.275: ISAKMP: hash SHA*Jan 20 16:48:22.275: ISAKMP: default group 2*Jan 20 16:48:22.275: ISAKMP: auth XAUTHInitPreShared*Jan 20 16:48:22.275: ISAKMP: life type in seconds*Jan 20 16:48:22.275: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 *Jan 20 16:48:22.275: ISAKMP:(0):Encryption algorithm offered does not match policy!*Jan 20 16:48:22.275: ISAKMP:(0):atts are not acceptable. Next payload is 3*Jan 20 16:48:22.275: ISAKMP:(0):Checking ISAKMP transform 4 against priority 10 policy*Jan 20 16:48:22.275: ISAKMP: encryption AES-CBC*Jan 20 16:48:22.275: ISAKMP: keylength of 192*Jan 20 16:48:22.275: ISAKMP: hash MD5*Jan 20 16:48:22.275: ISAKMP: default group 2*Jan 20 16:48:22.275: ISAKMP: auth XAUTHInitPreShared*Jan 20 16:48:22.275: ISAKMP: life type in seconds*Jan 20 16:48:22.275: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 *Jan 20 16:48:22.275: ISAKMP:(0):Encryption algorithm offered does not match policy!*Jan 20 16:48:22.275: ISAKMP:(0):atts are not acceptable. Next payload is 3*Jan 20 16:48:22.275: ISAKMP:(0):Checking ISAKMP transform 5 against priority 10 policy*Jan 20 16:48:22.275: ISAKMP: encryption AES-CBC*Jan 20 16:48:22.275: ISAKMP: keylength of 128*Jan 20 16:48:22.275: ISAKMP: hash SHA*Jan 20 16:48:22.275: ISAKMP: default group 2*Jan 20 16:48:2f 0x0 0x1 0x51 0x80 *Jan 20 16:48:22.275: ISAKMP:(0):Encryption algorithm offered does not match policy!*Jan 20 16:48:22.275: ISAKMP:(0):atts are not acceptable. Next payload is 3*Jan 20 16:48:22.275: ISAKMP:(0):Checking ISAKMP transform 6 against priority 10 policy*Jan 20 16:48:22.275: ISAKMP: encryption AES-CBC*Jan 20 16:48:22.275: ISAKMP: keylength of 128*Jan 20 16:48:22.275: ISAKMP: hash MD52.275: ISAKMP: auth XAUTHInitPreShared*Jan 20 16:48:22.275: ISAKMP: life type in seconds*Jan 20 16:48:22.275: ISAKMP: life duration (VPI) o*Jan 20 16:48:22.275: ISAKMP: default group 2*Jan 20 16:48:22.275: ISAKMP: auth XAUTHInitPreShared*Jan 20 16:48:22.275: ISAKMP: life type in seconds*Jan 20 16:48:22.275: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 *Jan 20 16:48:22.275: ISAKMP:(0):Encryption algorithm offered does not match policy!*Jan 20 16:48:22.275: ISAKMP:(0):atts are not acceptable. Next payload is 3*Jan 20 16:48:22.275: ISAKMP:(0):Checking ISAKMP transform 7 against priority 10 policy*Jan 20 16:48:22.275: ISAKMP: encryption 3DES-CBC*Jan 20 16:48:22.275: ISAKMP: hash SHA*Jan 20 16:48:22.275: ISAKMP: default group 2*Jan 20 16:48:22.275: ISAKMP: auth XAUTHInitPreShared*Jan 20 16:48:22.279: ISAKMP: life type in seconds*Jan 20 16:48:22.279: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 *Jan 20 16:48:22.279: ISAKMP:(0):Encryption algorithm offered does not match policy!*Jan 20 16:48:22.279: ISAKMP:(0):atts are not acceptable. Next payload is 3*Jan 20 16:48:22.279: ISAKMP:(0):Checking ISAKMP transform 8 against priority 10 policy*Jan 20 16:48:22.279: ISAKMP: encryption 3DES-CBC*Jan 20 16:48:22.279: ISAKMP: hash MD5*Jan 20 16:48:22.279: ISAKMP: default group 2*Jan 20 16:48:22.279: ISAKMP: auth XAUTHInitPreShared*Jan 20 16:48:22.279: ISAKMP: life type in seconds*Jan 20 16:48:22.279: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 *Jan 20 16:48:22.279: ISAKMP:(0):Encryption algorithm offered does not match policy!*Jan 20 16:48:22.279: ISAKMP:(0):atts are not acceptable. Next payload is 3*Jan 20 16:48:22.279: ISAKMP:(0):Checking ISAKMP transform 9 against priority 10 policy*Jan 20 16:48:22.279: ISAKMP: encryption DES-CBC*Jan 20 16:48:22.279: ISAKMP: hash MD5*Jan 20 16:48:22.279: ISAKMP: default group 2*Jan 20 16:48:22.279: ISAKMP: auth XAUTHInitPreShared*Jan 20 16:48:22.279: ISAKMP: life type in seconds*Jan 20 16:48:22.279: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 *Jan 20 16:48:22.279: ISAKMP:(0):atts are acceptable. Next payload is 3*!--- Both the IOS device and the PIX accept the policy for ISAKMP.*Jan 20 16:48:22.279: ISAKMP:(0): processing KE payload. message ID = 0*Jan 20 16:48:22.279: crypto_engine: Create DH shared secret *Jan 20 16:48:22.279: crypto_engine: Modular Exponentiation *Jan 20 16:48:22.319: ISAKMP:(0): processing NONCE payload. message ID = 0*Jan 20 16:48:22.319: ISAKMP:(0): vendor ID is NAT-T v3*Jan 20 16:48:22.319: ISAKMP:(0): vendor ID is NAT-T v2*Jan 20 16:48:22.319: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH*Jan 20 16:48:22.319: ISAKMP:(0):Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT *Jan 20 16:48:22.319: crypto_engine: Create IKE SA *Jan 20 16:48:22.319: crypto engine: deleting DH phase 2 SW:38 *Jan 20 16:48:22.319: crypto_engine: Delete DH shared secret *Jan 20 16:48:22.319: ISAKMP:(1030): constructed NAT-T vendor-03 ID*Jan 20 16:48:22.319: ISAKMP:(1030):SA is doing pre-shared key authentication plus XAUTH using id type ID_IPV4_ADDR*Jan 20 16:48:22.323: ISAKMP (0:1030): ID payload next-payload : 10type : 1 address : 10.10.10.2 protocol : 17 port : 0 length : 12*Jan 20 16:48:22.323: ISAKMP:(1030):Total payload length: 12*Jan 20 16:48:22.323: crypto_engine: Generate IKE hash *Jan 20 16:48:22.323: ISAKMP:(1030): sending packet to

10.10.10.1 my_port 500 peer_port 500 (R) AG_INIT_EXCH*Jan 20 16:48:22.323: ISAKMP:(1030):Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY*Jan 20 16:48:22.323: ISAKMP:(1030):Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2 *Jan 20 16:48:22.479: ISAKMP (0:1030): received packet from 10.10.10.1 dport 500 sport 500 Global (R) AG_INIT_EXCH*Jan 20 16:48:22.479: crypto_engine: Decrypt IKE packet *Jan 20 16:48:22.479: ISAKMP:received payload type 20*Jan 20 16:48:22.479: ISAKMP:received payload type 20*Jan 20 16:48:22.479: ISAKMP:(1030): processing HASH payload. message ID = 0*Jan 20 16:48:22.479: crypto_engine: Generate IKE hash *Jan 20 16:48:22.483: ISAKMP:(1030): processing NOTIFY INITIAL_CONTACT protocol 1spi 0, message ID = 0, sa = 658E0874*Jan 20 16:48:22.483: ISAKMP:(1030):SA authentication status:authenticated*Jan 20 16:48:22.483: ISAKMP:(1030):SA has been authenticated with 10.10.10.1*Jan 20 16:48:22.483: ISAKMP:(1030):SA authentication status:authenticated*Jan 20 16:48:22.483: ISAKMP:(1030): Process initial contact,bring down existing phase 1 and 2 SA's with local 10.10.10.2 remote 10.10.10.1 remote port 500*Jan 20 16:48:22.483: ISAKMP:(1030):returning IP addr to the address pool*Jan 20 16:48:22.483: ISAKMP: Trying to insert a peer 10.10.10.2/10.10.10.1/500/, and inserted successfully 6758C6D0.*Jan 20 16:48:22.483: IPSEC(key_engine): got a queue event with 1 KMI message(s)*Jan 20 16:48:22.483: ISAKMP: set new node -1980405900 to CONF_XAUTH *Jan 20 16:48:22.483: crypto_engine: Generate IKE hash *Jan 20 16:48:22.483: ISAKMP:(1030):Sending NOTIFY RESPONDER_LIFETIME protocol 1spi 1727476520, message ID = -1980405900*Jan 20 16:48:22.483: crypto_engine: Encrypt IKE packet *Jan 20 16:48:22.483: ISAKMP:(1030): sending packet to 10.10.10.1 my_port 500 peer_port 500 (R) QM_IDLE *Jan 20 16:48:22.483: ISAKMP:(1030):purging node -1980405900*Jan 20 16:48:22.483: ISAKMP: Sending phase 1 responder lifetime 86400*Jan 20 16:48:22.483: ISAKMP:(1030):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH*Jan 20 16:48:22.483: ISAKMP:(1030):Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE *Jan 20 16:48:22.483: ISAKMP:(1030):Need XAUTH*!--- The IOS device now processes the Extended Authentication phase !--- after Phase 1 is successful.*Jan 20 16:48:22.483: ISAKMP: set new node -791275911 to CONF_XAUTH *Jan 20 16:48:22.487: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2*Jan 20 16:48:22.487: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2*Jan 20 16:48:22.487: crypto_engine: Generate IKE hash *Jan 20 16:48:22.487: ISAKMP:(1030): initiating peer config to 10.10.10.1. ID = -791275911*Jan 20 16:48:22.487: crypto_engine: Encrypt IKE packet *Jan 20 16:48:22.487: ISAKMP:(1030): sending packet to 10.10.10.1 my_port 500 peer_port 500 (R) CONF_XAUTH *Jan 20 16:48:22.487: ISAKMP:(1030):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE*Jan 20 16:48:22.487: ISAKMP:(1030):Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_REQ_SENT *Jan 20 16:48:22.519: ISAKMP (0:1030): received packet from 10.10.10.1 dport 500 sport 500 Global (R) CONF_XAUTH *Jan 20 16:48:22.519: crypto_engine: Decrypt IKE packet *Jan 20 16:48:22.519: ISAKMP:(1030):processing transaction payload from 10.10.10.1. message ID = -791275911*Jan 20 16:48:22.519: crypto_engine: Generate IKE hash *Jan 20 16:48:22.519: ISAKMP: Config payload REPLY*Jan 20 16:48:22.519: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2*Jan 20 16:48:22.519: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2*Jan 20 16:48:22.519: ISAKMP:(1030):deleting node -791275911 error FALSE reason "Done with xauth request/reply exchange"*Jan 20 16:48:22.519: ISAKMP:(1030):Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY*Jan 20 16:48:22.519: ISAKMP:(1030):Old State = IKE_XAUTH_REQ_SENT New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT *Jan 20 16:48:22.519: ISAKMP: set new node 44674085 to CONF_XAUTH *Jan 20 16:48:22.519: crypto_engine: Generate IKE hash *Jan 20 16:48:22.519: ISAKMP:(1030): initiating peer config to 10.10.10.1. ID = 44674085*Jan 20 16:48:22.519: crypto_engine: Encrypt IKE packet *Jan 20 16:48:22.519: ISAKMP:(1030): sending packet to 10.10.10.1 my_port 500 peer_port 500 (R) CONF_XAUTH *Jan 20 16:48:22.519: ISAKMP:(1030):Input = IKE_MESG_FROM_AAA, IKE_AAA_CONT_LOGIN*Jan 20 16:48:22.519: ISAKMP:(1030):Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT New State = IKE_XAUTH_SET_SENT *Jan 20 16:48:22.571: ISAKMP (0:1030): received packet from 10.10.10.1 dport 500 sport 500 Global (R) CONF_XAUTH *Jan 20 16:48:22.571: crypto_engine: Decrypt IKE packet *Jan 20 16:48:22.571: ISAKMP:(1030):processing transaction payload from 10.10.10.1. message ID = 44674085*Jan 20 16:48:22.571: crypto_engine: Generate IKE hash *Jan 20 16:48:22.571: ISAKMP: Config payload ACK*Jan 20 16:48:22.571: ISAKMP:(1030): XAUTH ACK Processed*Jan 20 16:48:22.571: ISAKMP:(1030):deleting node 44674085 error FALSE reason "Transaction mode done"*Jan 20 16:48:22.571: ISAKMP:(1030):Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK*Jan 20 16:48:22.571: ISAKMP:(1030):Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE *Jan 20 16:48:22.571: ISAKMP:(1030):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE*Jan 20 16:48:22.571: ISAKMP:(1030):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE *!--- Extended authentication is complete, !--- and mode configuration is now processed.*Jan 20 16:48:22.619: ISAKMP (0:1030): received packet from 10.10.10.1 dport 500 sport 500 Global (R) QM_IDLE *Jan 20 16:48:22.619: ISAKMP: set new node -2005047200 to QM_IDLE *Jan 20 16:48:22.619: crypto_engine: Decrypt IKE packet *Jan 20 16:48:22.623: ISAKMP:(1030):processing transaction payload from 10.10.10.1. message ID = -2005047200*Jan 20 16:48:22.623: crypto_engine: Generate IKE hash*Jan 20 16:48:22.623: ISAKMP: Config payload REQUEST*Jan 20 16:48:22.623: ISAKMP:(1030):checking

request:*Jan 20 16:48:22.623: ISAKMP: DEFAULT_DOMAIN*Jan 20 16:48:22.623: ISAKMP: IP4_NBNS*Jan 20 16:48:22.623: ISAKMP: IP4_DNS*Jan 20 16:48:22.623: ISAKMP: SPLIT_INCLUDE*Jan 20 16:48:22.623: ISAKMP: SPLIT_DNS*Jan 20 16:48:22.623: ISAKMP: PFS*Jan 20 16:48:22.623: ISAKMP: CONFIG_MODE_UNKNOWN Unknown Attr: 0x7800*Jan 20 16:48:22.623: ISAKMP: CONFIG_MODE_UNKNOWN Unknown Attr: 0x7801*Jan 20 16:48:22.623: ISAKMP: CONFIG_MODE_UNKNOWN Unknown Attr: 0x7802*Jan 20 16:48:22.623: ISAKMP: CONFIG_MODE_UNKNOWN Unknown Attr: 0x7803*Jan 20 16:48:22.623: ISAKMP: CONFIG_MODE_UNKNOWN Unknown Attr: 0x7804*Jan 20 16:48:22.623: ISAKMP: CONFIG_MODE_UNKNOWN Unknown Attr: 0x7805*Jan 20 16:48:22.623: ISAKMP: CONFIG_MODE_UNKNOWN Unknown Attr: 0x7806*Jan 20 16:48:22.623: ISAKMP: BACKUP_SERVER*Jan 20 16:48:22.623: ISAKMP: APPLICATION_VERSION*Jan 20 16:48:22.623: ISAKMP/author: Author request for group hw client successfully sent to AAA*Jan 20 16:48:22.623: ISAKMP:(1030):Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST*Jan 20 16:48:22.623: ISAKMP:(1030):Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT *Jan 20 16:48:22.623: ISAKMP:(1030):attributes sent in message:*Jan 20 16:48:22.623: ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com*Jan 20 16:48:22.623: ISAKMP: Sending IP4_NBNS server address: 172.22.1.102*Jan 20 16:48:22.623: ISAKMP: Sending IP4_DNS server address: 172.22.1.101*Jan 20 16:48:22.623: ISAKMP (0/1030): Unknown Attr: CONFIG_MODE_UNKNOWN (0x7800)*Jan 20 16:48:22.623: ISAKMP (0/1030): Unknown Attr: CONFIG_MODE_UNKNOWN (0x7801)*Jan 20 16:48:22.623: ISAKMP (0/1030): Unknown Attr: CONFIG_MODE_UNKNOWN (0x7802)*Jan 20 16:48:22.623: ISAKMP (0/1030): Unknown Attr: CONFIG_MODE_UNKNOWN (0x7803)*Jan 20 16:48:22.623: ISAKMP (0/1030): Unknown Attr: CONFIG_MODE_UNKNOWN (0x7804)*Jan 20 16:48:22.623: ISAKMP (0/1030): Unknown Attr: CONFIG_MODE_UNKNOWN (0x7805)*Jan 20 16:48:22.627: ISAKMP (0/1030): Unknown Attr: CONFIG_MODE_UNKNOWN (0x7806)*Jan 20 16:48:22.627: ISAKMP: Sending APPLICATION_VERSION string: Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 12.4(4)T1, RELEASE SOFTWARE (fc4)Technical Support: http://www.cisco.com/techsupportCopyright (c) 1986-2005 by Cisco Systems, Inc.Compiled Wed 21-Dec-05 22:58 by ccai*Jan 20 16:48:22.627: crypto_engine: Generate IKE hash *Jan 20 16:48:22.627: ISAKMP:(1030): responding to peer config from 10.10.10.1. ID = -2005047200*Jan 20 16:48:22.627: crypto_engine: Encrypt IKE packet *Jan 20 16:48:22.627: ISAKMP:(1030): sending packet to 10.10.10.1 my_port 500 peer_port 500 (R) CONF_ADDR *Jan 20 16:48:22.627: ISAKMP:(1030):deleting node -2005047200 error FALSE reason "No Error"*Jan 20 16:48:22.627: ISAKMP:(1030):Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR*Jan 20 16:48:22.627: ISAKMP:(1030):Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE *Jan 20 16:48:22.627: ISAKMP:(1030):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE*Jan 20 16:48:22.627: ISAKMP:(1030):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE *Jan 20 16:48:27.695: ISAKMP (0:1030): received packet from 10.10.10.1 dport 500 sport 500 Global (R) QM_IDLE *Jan 20 16:48:27.695: ISAKMP: set new node 1887305923 to QM_IDLE *Jan 20 16:48:27.695: crypto_engine: Decrypt IKE packet *Jan 20 16:48:27.699: crypto_engine: Generate IKE hash *Jan 20 16:48:27.699: ISAKMP:(1030): processing HASH payload. message ID = 1887305923*Jan 20 16:48:27.699: ISAKMP:(1030): processing SA payload. message ID = 1887305923*Jan 20 16:48:27.699: ISAKMP:(1030):Checking IPSec proposal 1*Jan 20 16:48:27.699: ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.699: ISAKMP: attributes in transform:*Jan 20 16:48:27.699: ISAKMP: encaps is 1 (Tunnel)*Jan 20 16:48:27.699: ISAKMP: SA life type in seconds*Jan 20 16:48:27.699: ISAKMP: SA life duration (basic) of 28800*Jan 20 16:48:27.699: ISAKMP: SA life type in kilobytes*Jan 20 16:48:27.699: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.699: ISAKMP: authenticator is HMAC-SHA*Jan 20 16:48:27.699: ISAKMP: key length is 256*Jan 20 16:48:27.699: CryptoEngine0: validate proposal*Jan 20 16:48:27.699: ISAKMP:(1030):atts are acceptable.*Jan 20 16:48:27.699: IPSEC(validate_proposal_request): proposal part #1*Jan 20 16:48:27.699: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 256 esp-sha-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0*Jan 20 16:48:27.699: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes 256 esp-sha-hmac }*Jan 20 16:48:27.699: ISAKMP:(1030): IPSec policy invalidated proposal*Jan 20 16:48:27.699: ISAKMP:(1030):Checking IPSec proposal 2*Jan 20 16:48:27.699: ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.699: ISAKMP: attributes in transform:*Jan 20 16:48:27.699: ISAKMP: encaps is 1 (Tunnel)*Jan 20 16:48:27.699: ISAKMP: SA life type in seconds*Jan 20 16:48:27.699: ISAKMP: SA life duration (basic) of 28800*Jan 20 16:48:27.699: ISAKMP: SA life type in kilobytes*Jan 20 16:48:27.699: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.699: ISAKMP: authenticator is HMAC-MD5*Jan 20 16:48:27.699: ISAKMP: key length is 256*Jan 20 16:48:27.699: CryptoEngine0: validate proposal*Jan 20 16:48:27.699: ISAKMP:(1030):atts are acceptable.*!--- Proceed for processing Phase 2.*Jan 20 16:48:27.699: IPSEC(validate_proposal_request): proposal part #1*Jan 20 16:48:27.699: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 256 esp-md5-hmac

(Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0*Jan 20 16:48:27.699: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes 256 esp-md5-hmac }*Jan 20 16:48:27.699: ISAKMP:(1030): IPSec policy invalidated proposal*Jan 20 16:48:27.703: ISAKMP:(1030):Checking IPSec proposal 3*Jan 20 16:48:27.703: ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.703: ISAKMP: attributes in transform:*Jan 20 16:48:27.703: ISAKMP: encaps is 1 (Tunnel)*Jan 20 16:48:27.703: ISAKMP: SA life type in seconds*Jan 20 16:48:27.703: ISAKMP: SA life duration (basic) of 28800*Jan 20 16:48:27.703: ISAKMP: SA life type in kilobytes*Jan 20 16:48:27.703: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.703: ISAKMP: authenticator is HMAC-SHA*Jan 20 16:48:27.703: ISAKMP: key length is 192*Jan 20 16:48:27.703: CryptoEngine0: validate proposal*Jan 20 16:48:27.703: ISAKMP:(1030):atts are acceptable.*Jan 20 16:48:27.703: IPSEC(validate_proposal_request): proposal part #1*Jan 20 16:48:27.703: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 192 esp-sha-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 192, flags= 0x0*Jan 20 16:48:27.703: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes 192 esp-sha-hmac }*Jan 20 16:48:27.703: ISAKMP:(1030): IPSec policy invalidated proposal*Jan 20 16:48:27.703: ISAKMP:(1030):Checking IPSec proposal 4*Jan 20 16:48:27.703: ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.703: ISAKMP: attributes in transform:*Jan 20 16:48:27.703: ISAKMP: encaps is 1 (Tunnel)*Jan 20 16:48:27.703: ISAKMP: SA life type in seconds*Jan 20 16:48:27.703: ISAKMP: SA life duration (basic) of 28800*Jan 20 16:48:27.703: ISAKMP: SA life type in kilobytes*Jan 20 16:48:27.703: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.703: ISAKMP: authenticator is HMAC-MD5*Jan 20 16:48:27.703: ISAKMP: key length is 192*Jan 20 16:48:27.703: CryptoEngine0: validate proposal*Jan 20 16:48:27.703: ISAKMP:(1030):atts are acceptable.*Jan 20 16:48:27.703: IPSEC(validate_proposal_request): proposal part #1*Jan 20 16:48:27.703: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 192 esp-md5-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 192, flags= 0x0*Jan 20 16:48:27.703: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes 192 esp-md5-hmac }*Jan 20 16:48:27.703: ISAKMP:(1030): IPSec policy invalidated proposal*Jan 20 16:48:27.703: ISAKMP:(1030):Checking IPSec proposal 5*Jan 20 16:48:27.703: ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.703: ISAKMP: attributes in transform:*Jan 20 16:48:27.703: ISAKMP: encaps is 1 (Tunnel)*Jan 20 16:48:27.703: ISAKMP: SA life type in seconds*Jan 20 16:48:27.703: ISAKMP: SA life duration (basic) of 28800*Jan 20 16:48:27.703: ISAKMP: SA life type in kilobytes*Jan 20 16:48:27.707: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.707: ISAKMP: authenticator is HMAC-SHA*Jan 20 16:48:27.707: ISAKMP: key length is 128*Jan 20 16:48:27.707: CryptoEngine0: validate proposal*Jan 20 16:48:27.707: ISAKMP:(1030):atts are acceptable.*Jan 20 16:48:27.707: IPSEC(validate_proposal_request): proposal part #1*Jan 20 16:48:27.707: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-sha-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0*Jan 20 16:48:27.707: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes esp-sha-hmac }*Jan 20 16:48:27.707: ISAKMP:(1030): IPSec policy invalidated proposal*Jan 20 16:48:27.707: ISAKMP:(1030):Checking IPSec proposal 6*Jan 20 16:48:27.707: ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.707: ISAKMP: attributes in transform:*Jan 20 16:48:27.707: ISAKMP: encaps is 1 (Tunnel)*Jan 20 16:48:27.707: ISAKMP: SA life type in seconds*Jan 20 16:48:27.707: ISAKMP: SA life duration (basic) of 28800*Jan 20 16:48:27.707: ISAKMP: SA life type in kilobytes*Jan 20 16:48:27.707: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.707: ISAKMP: authenticator is HMAC-MD5*Jan 20 16:48:27.707: ISAKMP: key length is 128*Jan 20 16:48:27.707: CryptoEngine0: validate proposal*Jan 20 16:48:27.707: ISAKMP:(1030):atts are acceptable.*Jan 20 16:48:27.707: IPSEC(validate_proposal_request): proposal part #1*Jan 20 16:48:27.707: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-md5-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0*Jan 20 16:48:27.707: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes esp-md5-hmac }*Jan 20 16:48:27.707: ISAKMP:(1030): IPSec policy invalidated proposal*Jan 20 16:48:27.707: ISAKMP:(1030):Checking IPSec proposal 7*Jan 20 16:48:27.707:

ISAKMP: transform 1, ESP_3DES*Jan 20 16:48:27.707: ISAKMP: attributes in transform:*Jan 20 16:48:27.707: ISAKMP: encaps is 1 (Tunnel)*Jan 20 16:48:27.707: ISAKMP: SA life type in seconds*Jan 20 16:48:27.707: ISAKMP: SA life duration (basic) of 28800*Jan 20 16:48:27.707: ISAKMP: SA life type in kilobytes*Jan 20 16:48:27.707: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.707: ISAKMP: authenticator is HMAC-SHA*Jan 20 16:48:27.711: CryptoEngine0: validate proposal*Jan 20 16:48:27.711: ISAKMP:(1030):atts are acceptable.*Jan 20 16:48:27.711: IPSEC(validate_proposal_request): proposal part #1*Jan 20 16:48:27.711: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0*Jan 20 16:48:27.711: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-3des esp-sha-hmac }*Jan 20 16:48:27.711: ISAKMP:(1030): IPSec policy invalidated proposal*Jan 20 16:48:27.711: ISAKMP:(1030):Checking IPSec proposal 8*Jan 20 16:48:27.711: ISAKMP: transform 1, ESP_3DES*Jan 20 16:48:27.711: ISAKMP: attributes in transform:*Jan 20 16:48:27.711: ISAKMP: encaps is 1 (Tunnel)*Jan 20 16:48:27.711: ISAKMP: SA life type in seconds*Jan 20 16:48:27.711: ISAKMP: SA life duration (basic) of 28800*Jan 20 16:48:27.711: ISAKMP: SA life type in kilobytes*Jan 20 16:48:27.711: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.711: ISAKMP: authenticator is HMAC-MD5*Jan 20 16:48:27.711: CryptoEngine0: validate proposal*Jan 20 16:48:27.711: ISAKMP:(1030):atts are acceptable.*Jan 20 16:48:27.711: IPSEC(validate_proposal_request): proposal part #1*Jan 20 16:48:27.711: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-3des esp-md5-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0*Jan 20 16:48:27.715: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-3des esp-md5-hmac }*Jan 20 16:48:27.715: ISAKMP:(1030): IPSec policy invalidated proposal*Jan 20 16:48:27.715: ISAKMP:(1030):Checking IPSec proposal 9*Jan 20 16:48:27.715: ISAKMP: transform 1, ESP_DES*Jan 20 16:48:27.715: ISAKMP: attributes in transform:*Jan 20 16:48:27.715: ISAKMP: encaps is 1 (Tunnel)*Jan 20 16:48:27.715: ISAKMP: SA life type in seconds*Jan 20 16:48:27.715: ISAKMP: SA life duration (basic) of 28800*Jan 20 16:48:27.715: ISAKMP: SA life type in kilobytes*Jan 20 16:48:27.715: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.715: ISAKMP: authenticator is HMAC-MD5*Jan 20 16:48:27.715: CryptoEngine0: validate proposal*Jan 20 16:48:27.715: ISAKMP:(1030):atts are acceptable.*Jan 20 16:48:27.715: IPSEC(validate_proposal_request): proposal part #1*Jan 20 16:48:27.715: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0*Jan 20 16:48:27.715: ISAKMP:(1030): processing NONCE payload. message ID = 1887305923*Jan 20 16:48:27.715: ISAKMP:(1030): processing ID payload. message ID = 1887305923*Jan 20 16:48:27.715: ISAKMP:(1030): processing ID payload. message ID = 1887305923*Jan 20 16:48:27.715: ISAKMP:(1030): asking for 1 spis from ipsec*Jan 20 16:48:27.715: ISAKMP:(1030):Node 1887305923, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH*Jan 20 16:48:27.715: ISAKMP:(1030):Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE*Jan 20 16:48:27.719: IPSEC(key_engine): got a queue event with 1 KMI message(s)*Jan 20 16:48:27.719: IPSEC(spi_response): getting spi 185206738 for SA from 10.10.10.2 to 10.10.10.1 for prot 3*Jan 20 16:48:27.719: crypto_engine: Generate IKE hash *Jan 20 16:48:27.719: crypto_engine: Generate IKE QM keys *Jan 20 16:48:27.719: crypto_engine: Create IPSec SA (by keys) *Jan 20 16:48:27.719: crypto_engine: Generate IKE QM keys *Jan 20 16:48:27.719: crypto_engine: Create IPSec SA (by keys) *Jan 20 16:48:27.719: ISAKMP:(1030): Creating IPSec SAs*Jan 20 16:48:27.719: inbound SA from 10.10.10.1 to 10.10.10.2 (f/i) 0/ 0 (proxy 10.10.10.1 to 0.0.0.0)*Jan 20 16:48:27.719: has spi 0xB0A07D2 and conn_id 0*Jan 20 16:48:27.719: lifetime of 28800 seconds*Jan 20 16:48:27.719: lifetime of 4608000 kilobytes*Jan 20 16:48:27.719: outbound SA from 10.10.10.2 to 10.10.10.1 (f/i) 0/0 (proxy 0.0.0.0 to 10.10.10.1)*Jan 20 16:48:27.719: has spi 0xB22446D and conn_id 0*Jan 20 16:48:27.719: lifetime of 28800 seconds*Jan 20 16:48:27.719: lifetime of 4608000 kilobytes*Jan 20 16:48:27.719: crypto_engine: Encrypt IKE packet *Jan 20 16:48:27.719: ISAKMP:(1030): sending packet to 10.10.10.1 my_port 500 peer_port 500 (R) QM_IDLE *Jan 20 16:48:27.719: ISAKMP:(1030):Node 1887305923, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY*Jan 20 16:48:27.719: ISAKMP:(1030):Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2*Jan 20 16:48:27.719: IPSEC(key_engine): got a queue event with 1 KMI message(s)*Jan 20 16:48:27.723: IPSec: Flow_switching Allocated flow for sibling 80000014 *Jan 20 16:48:27.723: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 10.10.10.1, dest_port 0*Jan 20 16:48:27.723: IPSEC(create_sa): sa created, (sa) sa_dest= 10.10.10.2, sa_proto= 50, sa_spi=

```
0xB0A07D2(185206738), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 37*Jan 20 16:48:27.723:
IPSEC(create_sa): sa created, (sa) sa_dest= 10.10.10.1, sa_proto= 50, sa_spi=
0xB22446D(186795117), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 38!--- The two IPSec SAs
shown above are for management purposes.*Jan 20 16:48:27.771: ISAKMP (0:1030): received packet
from 10.10.10.1 dport 500 sport 500 Global (R) QM_IDLE *Jan 20 16:48:27.771: crypto_engine:
Decrypt IKE packet *Jan 20 16:48:27.771: crypto_engine: Generate IKE hash *Jan 20 16:48:27.771:
ISAKMP:(1030):deleting node 1887305923 error FALSE reason "QM done (await)"*Jan 20 16:48:27.771:
ISAKMP:(1030):Node 1887305923, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH*Jan 20 16:48:27.771:
ISAKMP:(1030):Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE*Jan 20 16:48:27.771:
IPSEC(key_engine): got a queue event with 1 KMI message(s)*Jan 20 16:48:27.771:
IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP*Jan 20 16:48:27.771:
IPSEC(key_engine_enable_outbound): enable SA with spi 186795117/50 *Jan 20 16:48:27.771:
IPSEC(update_current_outbound_sa): updated peer 10.10.10.1 current outbound sa to SPI
B22446D*Jan 20 16:48:27.771: ISAKMP (0:1030): received packet from 10.10.10.1 dport 500 sport
500 Global (R) QM_IDLE *Jan 20 16:48:27.771: ISAKMP: set new node -1259355083 to QM_IDLE *Jan 20
16:48:27.771: crypto_engine: Decrypt IKE packet *Jan 20 16:48:27.775: crypto_engine: Generate
IKE hash *Jan 20 16:48:27.775: ISAKMP:(1030): processing HASH payload. message ID = -
1259355083*Jan 20 16:48:27.775: ISAKMP:(1030): processing SA payload. message ID = -
1259355083*Jan 20 16:48:27.775: ISAKMP:(1030):Checking IPSec proposal 1*Jan 20 16:48:27.775:
ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.775: ISAKMP: attributes in transform:*Jan 20
16:48:27.775: ISAKMP: encaps is 1 (Tunnel)*Jan 20 16:48:27.775: ISAKMP: SA life type in
seconds*Jan 20 16:48:27.775: ISAKMP: SA life duration (basic) of 28800*Jan 20 16:48:27.775:
ISAKMP: SA life type in kilobytes*Jan 20 16:48:27.775: ISAKMP: SA life duration (VPI) of 0x0
0x46 0x50 0x0 *Jan 20 16:48:27.775: ISAKMP: authenticator is HMAC-SHA*Jan 20 16:48:27.775:
ISAKMP: key length is 256*Jan 20 16:48:27.775: CryptoEngine0: validate proposal*Jan 20
16:48:27.775: ISAKMP:(1030):atts are acceptable.*Jan 20 16:48:27.775:
IPSEC(validate_proposal_request): proposal part #1*Jan 20 16:48:27.775:
IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2,
remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy=
172.16.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-aes 256 esp-sha-hmac
(Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0*Jan 20
16:48:27.775: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for
identity: {esp-aes 256 esp-sha-hmac }*Jan 20 16:48:27.775: ISAKMP:(1030): IPSec policy
invalidated proposal*Jan 20 16:48:27.775: ISAKMP:(1030):Checking IPSec proposal 2*Jan 20
16:48:27.775: ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.775: ISAKMP: attributes in
transform:*Jan 20 16:48:27.775: ISAKMP: encaps is 1 (Tunnel)*Jan 20 16:48:27.775: ISAKMP: SA
life type in seconds*Jan 20 16:48:27.775: ISAKMP: SA life duration (basic) of 28800*Jan 20
16:48:27.775: ISAKMP: SA life type in kilobytes*Jan 20 16:48:27.775: ISAKMP: SA life duration
(VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.775: ISAKMP: authenticator is HMAC-MD5*Jan 20
16:48:27.775: ISAKMP: key length is 256*Jan 20 16:48:27.775: CryptoEngine0: validate
proposal*Jan 20 16:48:27.775: ISAKMP:(1030):atts are acceptable.*Jan 20 16:48:27.775:
IPSEC(validate_proposal_request): proposal part #1*Jan 20 16:48:27.799: IPSEC(create_sa): sa
created, (sa) sa_dest= 10.10.10.2, sa_proto= 50, sa_spi= 0x990A0C2C(2567572524), sa_trans= esp-
des esp-md5-hmac , sa_conn_id= 39*Jan 20 16:48:27.799: IPSEC(create_sa): sa created, (sa)
sa_dest= 10.10.10.1, sa_proto= 50, sa_spi= 0x9FBC4C0D(2679917581), sa_trans= esp-des esp-md5-
hmac , sa_conn_id= 40!--- The two IPSec SAs shown above are for actual data traffic.
```

Información Relacionada

- IPSec Negotiation/IKE Protocols
- Dispositivos de seguridad de la serie PIX 500
- Referencias de Comando PIX
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems