IPSec ASA y debugs IKE (modo agresivo IKEv1) que resuelven problemas la nota técnica

Contenido

Introducción

Este documento describe los debugs en el dispositivo de seguridad adaptante de Cisco (ASA) cuando utilizan al modo agresivo y la clave previamente compartida (PSK). También se trata la traducción de ciertas líneas de debug en la configuración. Cisco le recomienda tiene un conocimiento básico del IPSec y del Internet Key Exchange (IKE).

Este documento no discute el pasar del tráfico después de que se haya establecido el túnel.

Cuestión central

Los debugs IKE y del IPSec son a veces secretos, pero usted puede utilizarlos para entender los problemas con el establecimiento del túnel del IPSec VPN.

Situación

¿Utilizan al modo agresivo típicamente en caso de VPN fácil (EzVPN) con el software (Cliente Cisco VPN) y los hardwares cliente (dispositivo de seguridad o Cisco IOS adaptante de Cisco ASA 5505? Routeres con software), pero solamente cuando se utiliza una clave previamente compartida. El modo de los a diferencia de las principales, modo agresivo consiste en tres mensajes.

Los debugs son de un ASA que funcione con la versión de software 8.3.2 y actúe como servidor EzVPN. El cliente EzVPN es un software cliente.

comandos debug usados

Éstos son los comandos debug usados en este documento:

```
debug crypto isakmp 127
debug crypto ipsec 127
```

Configuración ASA

La configuración ASA en este ejemplo se significa para ser estrictamente básica; no se utiliza a ningunos servidores externos.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.48.67.14 255.255.254.0

crypto ipsec transform-set TRA esp-aes esp-sha-hmac

crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000

crypto dynamic-map DYN 10 set transform-set TRA
crypto dynamic-map DYN 10 set reverse-route

crypto map MAP 65000 ipsec-isakmp dynamic DYN
crypto map MAP interface outside
crypto isakmp enable outside

crypto isakmp policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
lifetime 86400

username cisco password  cisco
username cisco attributes
vpn-framed-ip-address 192.168.1.100 255.255.255.0

tunnel-group EZ type remote-access
tunnel-group EZ general-attributes
 default-group-policy EZ
tunnel-group EZ ipsec-attributes
 pre-shared-key *****

group-policy EZ internal
group-policy EZ attributes
 password-storage enable
 dns-server value 192.168.1.99
 vpn-tunnel-protocol ikev1
 split-tunnel-policy tunnelall
 split-tunnel-network-list value split
 default-domain value jyoungta-labdomain.cisco.com
```

Depuración

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

Descripción del mensaje del servidor	Depuraciones		Descripción de mensaje del cliente
	49711:28:30.28908/24/12Sev=Info/6IKE/0x6300003B El intentar establecer una conexión con 64.102.156.88. 49811:28:30.29708/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_INITIALEvent: EV_INITIATOR 49911:28:30.29708/24/12Sev=Info/4IKE/0x63000001 Comenzar la negociación de la fase 1 IKE 50011:28:30.29708/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_GEN_DHKEY 50111:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_BLD_MSG 50211:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_START_RETRY_TMR 50311:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_SND_MSG		Comienzo del modo agresivo. Construcción AM1. Este proceso incluye: - ISAKMP HDR - El dispositivo de seguridad (SA) que contiene todo transforma las cargas útiles y las ofertas soportadas por el cliente - Payload del intercambio de claves - Iniciador ID de la fase 1 - Nonce
	50411:28:30.30408/24/12Sev=Info/4IKE/0x63000013 ENVIANDO ISAKMP OAK AG (SA, KE, NON, ID del >>>, VID(Xauth), VID(dpd), VID(Frag), VID (NAT-T), VID(Unity)) a 64.102.156.88		Envíe AM1.
	========== agresivo del mensaje 1 del <========== (AM1)		
Reciba AM1 del cliente.	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECIBIÓ el mensaje (msgid=0) con las cargas útiles: HDR + SA (1) + KE	50611:28:30.33308/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_WAIT_MSG2Event: EV_NO_EVENT	Espera para la respuesta del servidor.

	(4) + NONCE (10) + ID (5) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NINGUNOS (0) longitudes totales: 849		

Proceso AM1. Compare recibió las ofertas y las transforma con ésos configurados ya para las coincidencias. Configuración pertinente:
El ISAKMP se habilita en la interfaz, y por lo menos una directiva se define que hace juego lo que envió el cliente:
`crypto isakmp enable outside`
`crypto isakmp policy 10`
`authentication pre-share`
`encryption aes`
`hash sha`
`group 2`
`lifetime 86400`
Grupo de túnel que corresponde con el presente del nombre de la identidad:
`tunnel-group EZ type remote-access`
`tunnel-group EZ general-attributes`
`default-group-policy EZ`
`tunnel-group EZ ipsec-attributes`
`pre-shared-key cisco`
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, procesando el payload SA
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, procesando el payload KE
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, procesando el payload ISA_KE
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, procesando el payload del nonce
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, payload identificador de proceso
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, procesando el payload VID
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, Xauth recibido V6 VID
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, procesando el payload VID
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, DPD recibido VID
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, procesando el payload VID
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, fragmentación recibida VID
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, indicadores incluidos de la capacidad de la fragmentación del par IKE IKE: Modo principal: Modo de TrueAggressive: Falso
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, procesando el payload VID
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, ver recibido 02 VID del NAT-Traversal
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, procesando el payload VID
	24 de agosto DEBUG [IKEv1] IP= de 11:31:03 64.102.156.87, cliente recibido VID del Cisco Unity
	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, conexión aterrizada en el IPSec del tunnel_group
	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, procesando el payload	

	IKE SA 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto error de 11:31:03 [IKEv1]Phase 1: Tipos unidos mal del atributo para la descripción del grupo de la clase: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, oferta IKE SA # 1, transforman de # la entrada global 5 acceptableMatches IKE # 1	

Construcción AM2. Este proceso incluye: - directivas elegidas - Diffie-Hellman (DH) - Respondedor ID - auth - Payload de la detección del Network Address Translation (NAT)	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo el payload ISAKMP SA 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo el payload KE 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo el payload del nonce 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, generando las claves para el respondedor… 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo el payload ID 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo el payload del hash 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, hash computacional para el ISAKMP 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo el payload del Cisco Unity VID 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo el payload del Xauth V6 VID 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo el payload del vid del dpd 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo el payload del ver 02 del NAT-Traversal VID 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo el payload de la NAT-detección 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, hash computacional de la detección NAT 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo el payload de la NAT-detección 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, hash computacional de la detección NAT 24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo la fragmentación VID + ampliaron el payload de las capacidades 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo el payload VID 24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de	

	11:31:03], IP= 64.102.156.87, envían Altiga/Cisco VPN3000/Cisco ASA GW VID	
Envíe AM2.	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE QUE ENVÍA el mensaje (msgid=0) con las cargas útiles: HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NAT-D (130) + NAT-D (130) + VENDEDOR (13) + VENDEDOR (13) + NINGUNOS (0) longitudes totales: 444	
	==========> agresivo del mensaje 2 del ========== (AM2)	
	50711:28:30.40208/24/12Sev=Info/5IKE/0x6300002F Paquete ISAKMP recibido: par = 64.102.156.8 50811:28:30.40308/24/12Sev=Info/4IKE/0x63000014 RECIBIENDO ISAKMP OAK AG (SA del <<<, KE, NON, ID, HASH, VID(Unity), VID(Xauth), VID(dpd), VID (NAT-T), NAT-D, NAT-D, VID(Frag), VID (?)) a partir del 64.102.156.88 51011:28:30.41208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_RCVD_MSG	Reciba AM2.
	51111:28:30.41208/24/12Sev=Info/5IKE/0x63000001 El par es un par obediente del Cisco Unity 51211:28:30.41208/24/12Sev=Info/5IKE/0x63000001 El par soporta el XAUTH 51311:28:30.41208/24/12Sev=Info/5IKE/0x63000001 El par soporta el DPD 51411:28:30.41208/24/12Sev=Info/5IKE/0x63000001 El par soporta el NAT-T 51511:28:30.41208/24/12Sev=Info/5IKE/0x63000001 El par soporta las cargas útiles de la fragmentación IKE 51611:28:30.41208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_GEN_SKEYID 51711:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_AUTHENTICATE_PEER 51811:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_ADJUST_PORT 51911:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5	Proceso 2.

	R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_CRYPTO_ACTIVE	
	52011:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Event: EV_BLD_MSG] 52111:28:30.42208/24/12Sev=Debug/8IKE/0x63000001 El Vendor ID Contruction IOS comenzó 52211:28:30.42208/24/12Sev=Info/6IKE/0x63000001 Vendor ID Contruction IOS acertado	Construcción AM3. Este proceso incluye el auth del cliente. En este momento todos los datos relevantes para el cifrado se han intercambiado ya.
	52311:28:30.42308/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Event: EV_SND_MSG 52411:28:30.42308/24/12Sev=Info/4IKE/0x63000013 ENVIANDO ISAKMP OAK AG DEL >>> * (EL HASH, NOTIFICA: STATUS_INITIAL_CONTACT, NAT-D, NAT-D, VID (?), VID(Unity)) a 64.102.156.88	Envíe AM3.
	========== agresivo del mensaje 3 del <========== (AM3)	
Reciba AM3 del cliente.	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECIBIÓ el mensaje (msgid=0) con las cargas útiles: HDR + el HASH (8) + NOTIFICAN (11) + NAT-D (130) + NAT-D (130) + el VENDEDOR (13) + el VENDEDOR (13) + NINGUNOS (0) longitudes totales: 168	
El proceso 3. confirma el uso del traversal NAT (NAT-T). Los ambos lados están listos ahora para comenzar la encripción del tráfico.	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, procesando el payload del hash 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, hash computacional para el ISAKMP 24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, procesando notifican el payload 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, procesando el payload de la NAT-detección 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, hash computacional de la detección NAT 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, procesando el payload de la NAT-detección 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, hash computacional de la detección NAT 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, procesando el payload VID	

	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, procesando el payload del Vendor ID IOS/PIX (versión: 1.0.0, capacidades: 00000408) 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, procesando el payload VID 24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, recibieron al cliente VID del Cisco Unity 24 de agosto 11:31:03 [IKEv1]Group = IPSec, IP= 64.102.156.87, detección automática NAT Estado: El endISbehind remoto un deviceThisend NAT no está detrás de un dispositivo NAT	
Fase iniciado 1.5 (XAUTH), y credenciales de usuario de la petición.	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo el payload en blanco del hash 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:03], IP= 64.102.156.87, construyendo el payload del hash del qm 24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE QUE ENVÍA el mensaje (msgid=fb709d4d) con las cargas útiles: HDR + HASH (8) + ATTR (14) + NINGUNOS (0) longitudes totales: 72	
	Xauth del ========== - ==========> de la petición de las credenciales	
	53511:28:30.43008/24/12Sev=Info/4IKE/0x63000014 RECIBIENDO EL transporte del ISAKMP OAK del <<< * (HASH, ATTR) a partir del 64.102.156.88 53611:28:30.43108/24/12Sev=Decode/11IKE/0x63000001 Encabezado ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Respondedor COOKIE:1B301D2DE710EDA0 Payload siguiente: Hash Ver (Hex):10 Tipo del intercambio: Transacción Indicadores: (Cifrado) MessageID(Hex):FB709D4D Length:76 Hash del payload Payload siguiente: Atributos Reservado: 00 Magnitud de carga útil: 24 Datos (en el hex.): C779D5CBC5C75E3576C478A15A7CAB8A83A232D0 Atributos del payload Payload siguiente: Ninguno Reservado: 00 Magnitud de carga útil: 20 Tipo: ISAKMP_CFG_REQUEST Reservado: 00	Reciba el pedido de autenticación. Las demostraciones desencriptadas del payload vacian los campos del nombre de usuario y contraseña.

	Identificador: 0000 Tipo del XAUTH: Genérico Nombre de usuario del XAUTH: (vacío) Contraseña del usuario del XAUTH: (vacío) 53711:28:30.43108/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_INITIALEvent: EV_RCVD_MSG	
	53811:28:30.43108/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQEvent: EV_INIT_XAUTH 53911:28:30.43108/24/12 Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQEvent: EV_START_RETRY_TMR 54011:28:30.43208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_NO_EVENT 541 11:28:36.41508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_RCVD_USER_INPUT	Fase iniciado 1.5 (XAUTH). Temporizador iniciado de la recomprobación como aguarda la entrada de usuario. Cuando el temporizador de la recomprobación se ejecuta hacia fuera, la conexión se desconecta automáticamente.
	54211:28:36.41508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_SND_MSG 54311:28:36.41508/24/12Sev=Info/4IKE/0x63000013 ENVIANDO EL transporte del ISAKMP OAK del >>> * (HASH, ATTR) a 64.102.156.88 54411:28:36.41508/24/12Sev=Decode/11IKE/0x63000001 Encabezado ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Respondedor COOKIE:1B301D2DE710EDA0 Payload siguiente: Hash Ver (Hex):10 Tipo del intercambio: Transacción Indicadores: (Cifrado) MessageID(Hex):FB709D4D Length:85 Hash del payload Payload siguiente: Atributos Reservado: 00 Magnitud de carga útil: 24 Datos (en el hex.): 1A3645155BE9A81CB80FCDB5F7F24E03FF8239F5 Atributos del payload Payload siguiente: Ninguno Reservado: 00 Magnitud de carga útil: 33	Una vez que se recibe la entrada de usuario, envíe los credenciales de usuario al servidor. Las demostraciones desencriptadas del payload llenaron (pero ocultado) los campos del nombre de usuario y contraseña. Envíe la petición de la configuración de modo (diversos atributos).

	Tipo: ISAKMP_CFG_REPLY Reservado: 00 Identificador: 0000 Tipo del XAUTH: Genérico Nombre de usuario del XAUTH: (datos no visualizados) Contraseña del usuario del XAUTH: (datos no visualizados)	
	Xauth del <========== - ========== de los credenciales de usuario	
Reciba los credenciales de usuario.	24 de agosto 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECIBIÓ el mensaje (msgid=fb709d4d) con las cargas útiles: HDR + HASH (8) + ATTR (14) + NINGUNOS (0) longitud total: 85 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], IP= 64.102.156.87, process_attr(): ¡Ingrese!	
Procese los credenciales de usuario. Verifique las credenciales, y genere el payload de la configuración de modo. Configuración pertinente: `username cisco password cisco`	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], IP= 64.102.156.87, procesando los atributos de la contestación MODE_CFG. 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], nombre de usuario = user1, IP= 64.102.156.87, IKEGetUserAttributes: DN primarios = 192.168.1.99 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], nombre de usuario = user1, IP= 64.102.156.87, IKEGetUserAttributes: DN secundarios = borrado 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], nombre de usuario = user1, IP= 64.102.156.87, IKEGetUserAttributes: TRIUNFOS primarios = borrado 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], nombre de usuario = user1, IP= 64.102.156.87, IKEGetUserAttributes: TRIUNFOS secundarios = borrado 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], nombre de usuario = user1, IP= 64.102.156.87, IKEGetUserAttributes: la lista del Túnel dividido = partió 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], nombre de usuario = user1, IP= 64.102.156.87, IKEGetUserAttributes: Default Domain = jyoungta-labdomain.cisco.com 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], nombre de usuario = user1, IP= 64.102.156.87, IKEGetUserAttributes: La compresión IP = inhabilitó 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], nombre de usuario = user1, IP= 64.102.156.87, IKEGetUserAttributes: La directiva del Túnel dividido = inhabilitó 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], nombre de usuario = user1, IP=	

	64.102.156.87, IKEGetUserAttributes: La configuración de representación del navegador = ninguno-se modifica 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], nombre de usuario = user1, IP= 64.102.156.87, IKEGetUserAttributes: Local = neutralización de puente del proxy del navegador 24 de agosto 11:31:09 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, usuario (user1) autenticado.	
Envíe el resultado del xuath.	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], nombre de usuario = user1, IP= 64.102.156.87, construyendo el payload en blanco del hash 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], nombre de usuario = user1, IP= 64.102.156.87, construyendo el payload del hash del qm 24 de agosto 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE QUE ENVÍA el mensaje (msgid=5b6910ff) con las cargas útiles: HDR + HASH (8) + ATTR (14) + NINGUNOS (0) longitudes totales: 64	
	Xauth del ========== - ==========> del resultado de la autorización	
	54511:28:36.41608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_XAUTHREQ_DONE 54611:28:36.41608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_NO_EVENT 54711:28:36.42408/24/12Sev=Info/5IKE/0x6300002F Paquete ISAKMP recibido: par = 64.102.156.88 54811:28:36.42408/24/12Sev=Info/4IKE/0x63000014 RECIBIENDO EL transporte del ISAKMP OAK del <<< * (HASH, ATTR) a partir del 64.102.156.88 54911:28:36.42508/24/12Sev=Decode/11IKE/0x63000001 Encabezado ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Respondedor COOKIE:1B301D2DE710EDA0 Payload siguiente: Hash Ver (Hex):10 Tipo del intercambio: Transacción Indicadores: (Cifrado) MessageID(Hex):5B6910FF Length:76 Hash del payload Payload siguiente: Atributos Reservado: 00	Reciba los resultados del auth, y los resultados del proceso.

	Magnitud de carga útil: 24 Datos (en el hex.): 7DCF47827164198731639BFB7595F694C9DDFE85 Atributos del payload Payload siguiente: Ninguno Reservado: 00 Magnitud de carga útil: 12 Tipo: ISAKMP_CFG_SET Reservado: 00 Identificador: 0000 Estatus del XAUTH: Pass 55011:28:36.42508/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=5B6910FFCurState: TM_INITIALEvent: EV_RCVD_MSG 55111:28:36.42508/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETEvent: EV_INIT_XAUTH 55211:28:36.42508/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETEvent: EV_CHK_AUTH_RESULT	
	55311:28:36.42508/24/12Sev=Info/4IKE/0x63000013 ENVIANDO EL transporte del ISAKMP OAK del >>> * (HASH, ATTR) a 64.102.156.88	Resultado ACK.
	Xauth del <========== - ========== del acuse de recibo	
Reciba y procese el ACK; ninguna respuesta del servidor.	24 de agosto 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECIBIÓ el mensaje (msgid=5b6910ff) con las cargas útiles: HDR + HASH (8) + ATTR (14) + NINGUNOS (0) longitudes totales: 60 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], nombre de usuario = user1, IP= 64.102.156.87, process_attr(): ¡Ingrese! 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:09], nombre de usuario = user1, IP= 64.102.156.87, procesando los atributos del cfg ACK	
	55511:28:36.42608/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEEvent: EV_XAUTH_DONE_SUC 55611:28:36.42608/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEEvent: EV_NO_EVENT 55711:28:36.42608/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_TERM_REQUEST 55811:28:36.42608/24/12Sev=Debug/7IKE/0x6300007	Genere la petición de la configuración de modo. Las demostraciones desencriptadas del payload pidieron los parámetros del servidor.

	6 NAV Trace->TM:MsgID=FB709D4DCurState: TM_FREEEvent: EV_REMOVE 55911:28:36.42608/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=FB709D4DCurState: TM_FREEEvent: EV_NO_EVENT 56011:28:36.42608/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_XAUTH_PROGEvent: EV_XAUTH_DONE_SUC 56111:28:38.40608/24/12Sev=Debug/8IKE/0x6300004 C Comenzar el temporizador DPD para IKE SA (I_Cookie=D56197780D7BE3E5) Sa->state R_Cookie=1B301D2DE710EDA0 = 1, sa- >dpd.worry_freq(mSec) = 5000 56211:28:38.40608/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_MODECFG 56311:28:38.40608/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_NO_EVENT 56411:28:38.40608/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=84B4B653CurState: TM_INITIALEvent: EV_INIT_MODECFG 56511:28:38.40808/24/12Sev=Info/5IKE/0x6300005E Cliente que envía una petición del Firewall al concentrador 56611:28:38.40908/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_START_RETRY_TMR	
	56711:28:38.40908/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_SND_MSG 56811:28:38.40908/24/12Sev=Info/4IKE/0x63000013 ENVIANDO EL transporte del ISAKMP OAK del >>> * (HASH, ATTR) a 64.102.156.88 56911:28:38.62708/24/12Sev=Decode/11IKE/0x63000 001 Encabezado ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Respondedor COOKIE:1B301D2DE710EDA0 Payload siguiente: Hash	Envíe la petición de la configuración de modo.

	Ver (Hex):10 Tipo del intercambio: Transacción Indicadores: (Cifrado) MessageID(Hex):84B4B653 Length:183 Hash del payload Payload siguiente: Atributos Reservado: 00 Magnitud de carga útil: 24 Datos (en el hex.): 81BFBF6721A744A815D69A315EF4AAA571D6B687 Atributos del payload Payload siguiente: Ninguno Reservado: 00 Magnitud de carga útil: 131 Tipo: ISAKMP_CFG_REQUEST Reservado: 00 Identificador: 0000 Direccionamiento del IPv4: (vacío) Netmask del IPv4: (vacío) IPv4 DNS: (vacío) IPv4 NBNS (TRIUNFOS): (vacío) Vencimiento del direccionamiento: (vacío) Extensión de Cisco: Banner: (vacío) Extensión de Cisco: Salve al PWD: (vacío) Extensión de Cisco: Domain Name predeterminado: (vacío) Extensión de Cisco: La fractura incluye: (vacío) Extensión de Cisco: Nombre del DNS dividido: (vacío) Extensión de Cisco: Haga el PFS: (vacío) Desconocido: (vacío) Extensión de Cisco: Servidores de backup: (vacío) Extensión de Cisco: Desconexión del retiro de la placa inteligente: (vacío) Versión de aplicación: Cliente VPN 5.0.07.0290:WinNT de Cisco Systems Extensión de Cisco: Tipo del Firewall: (vacío) Extensión de Cisco: Nombre de host de los dn dinámico: ATBASU-LABBOX		
	========== de la petición de la configuración de modo del <==========		
Reciba la petición de la configuración de modo.	24 de agosto 11:31:11 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECIBIÓ el mensaje (msgid=84b4b653) con las	57011:28:38.62808/24/12Sev= Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_NO_EVENT	Espera para la respuesta del servidor.

	cargas útiles: HDR + HASH (8) + ATTR (14) + NINGUNOS (0) longitudes totales: 183 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, process_attr(): ¡Ingrese!		
Petición de proceso de la configuración de modo. Muchos de estos valores se configuran generalmente en la grupo-directiva. Sin embargo, puesto que el servidor en este ejemplo tiene mismo una configuración básica, usted no los ve aquí.	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, procesando los atributos de la petición del cfg 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Pedido recibido el direccionamiento del IPV4! 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Pedido recibido la máscara de red del IPV4! 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Pedido recibido el DNS Server Address! 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Pedido recibido la dirección del servidor de los TRIUNFOS! 24 de agosto 11:31:11 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, atributo sin apoyo recibido del modo de transacción: 5 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Pedido recibido el banner! 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Pedido recibido la configuración picovatio de la salvaguardia! 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Pedido recibido el Domain Name predeterminado!	

	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Petición recibida la lista del túnel dividido! 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Pedido recibido el DNS dividido! 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Pedido recibido la configuración PFS! 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Pedido recibido la configuración de representación del buscador del cliente! 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Petición recibida la lista del peer de reserva IP-SEC! 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Pedido recibido la configuración de la desconexión del retiro del Smartcard del cliente! 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Pedido recibido la versión de aplicación! 24 de agosto 11:31:11 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, tipo de cliente: Versión de aplicación de WinNTClient: 5.0.07.0290 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: ¡Petición recibida para FWTYPE! 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, MODE_CFG: El pedido recibido el nombre de host del DHCP para el DDNS es: ¡ATBASU-LABBOX!	
Construya la respuesta de la configuración de modo con todos los valores se configuren que. Configuración pertinente: Observe en este caso, el usuario se asigna siempre el	24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, obtuvieron el addr IP (192.168.1.100) antes de iniciar el cfg del modo (el Xauth habilitado) 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, enviando a la máscara de subred (255.255.255.0) al cliente remoto 24 de agosto 11:31:11 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, asignó el IP Address privado 192.168.1.100 al usuario remoto	

mismo IP.
`username cisco attributes`
`vpn-framed-ip-address 192.168.1.100 255.255.255.0`
`group-policy EZ internal`
`group-policy EZ attributes`
`password-storage enabledns-server value 192.168.1.129`
`vpn-tunnel-protocol ikev1`
`split-tunnel-policy tunnelall`
`split-tunnel-network-list value split`
`default-domain value jyoungta-labdomain.cisco.com`
	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, construyendo el payload en blanco del hash
	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, construct_cfg_set: Default Domain = jyoungta-labdomain.cisco.com
	¡24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, envían los atributos del proxy del buscador del cliente!
	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, proxy del navegador fijado Ninguno-para modificarse. Los datos del proxy del navegador no serán incluidos en la contestación del MODE-cfg
	¡24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, envían el permiso de la desconexión del retiro del Smartcard de Cisco!!
	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:11], nombre de usuario = user1, IP= 64.102.156.87, construyendo el payload del hash del qm	

Envíe la respuesta de la configuración de modo.	24 de agosto 11:31:11 [IKEv1]IP = 64.102.156.87, IKE_DECODE QUE ENVÍA el mensaje (msgid=84b4b653) con las cargas útiles: HDR + HASH (8) + ATTR (14) + NINGUNOS (0) longitudes totales: 215	
	==========> de la respuesta de la configuración de modo del ==========	
	57111:28:38.63808/24/12Sev=Info/5IKE/0x6300002F Paquete ISAKMP recibido: par = 64.102.156.88 57211:28:38.63808/24/12Sev=Info/4IKE/0x63000014 RECIBIENDO EL transporte del ISAKMP OAK del <<< * (HASH, ATTR) a partir del 64.102.156.88 57311:28:38.63908/24/12Sev=Decode/11IKE/0x63000001 Encabezado ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Respondedor COOKIE:1B301D2DE710EDA0 Payload siguiente: Hash Ver (Hex):10 Tipo del intercambio: Transacción Indicadores: (Cifrado) MessageID(Hex):84B4B653 Length:220 Hash del payload Payload siguiente: Atributos Reservado: 00 Magnitud de carga útil: 24 Datos (en el hex.):	Reciba los Valores de parámetro de la configuración de modo del servidor.

	6DE2E70ACF6B1858846BC62E590C00A66745D14D Atributos del payload Payload siguiente: Ninguno Reservado: 00 Magnitud de carga útil: 163 Tipo: ISAKMP_CFG_REPLY Reservado: 00 Identificador: 0000 Direccionamiento del IPv4: 192.168.1.100 Netmask del IPv4: 255.255.255.0 IPv4 DNS: 192.168.1.99 Extensión de Cisco: Salve al PWD: No Extensión de Cisco: Domain Name predeterminado: jyoungta-labdomain.cisco.com Extensión de Cisco: Haga el PFS: No Versión de aplicación: Versión 8.4(4)1 de Cisco Systems, Inc ASA5505 construida por los constructores el Thu 14-Jun-12 11:20 Extensión de Cisco: Desconexión del retiro de la placa inteligente: Sí		
La fase 1 completa en el servidor. Proceso iniciado del quick mode (QM).	24 de agosto 11:31:13 [IKEv1 DECODIFICA] IP= 64.102.156.87, respondedor IKE que comienza el QM: msg identificación = 0e83792e 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, Quick Mode del retardo que procesa, CERT/transporte Exch/RM DSID en curso 24 de agosto 11:31:13 [IKEv1]Group = IPSec, nombre de usuario =	57411:28:38.63908/24/12Sev= Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_RCVD_MSG 57511:28:38.63908/24/12Sev= Info/5IKE/0x63000010 MODE_CFG_REPLY: Atributo = INTERNAL_IPV4_ADDRESS: , valor = 192.168.1.100 57611:28:38.63908/24/12Sev=Info/5IKE/0x63000010 MODE_CFG_REPLY: Atributo = INTERNAL_IPV4_NETMASK: , valor = 255.255.255.0 57711:28:38.63908/24/12Sev= Info/5IKE/0x63000010 MODE_CFG_REPLY: Atributo = INTERNAL_IPV4_DNS(1): , valor = 192.168.1.99 57811:28:38.63908/24/12Sev=Info/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = MODECFG_UNITY_SAVEPWD: , valor = 0x00000000 57911:28:38.63908/24/12Sev=Info/5IKE/0x6300000E MODE_CFG_REPLY: Atributo = MODECFG_UNITY_DEFDOMAIN: , valor = jyoungta-labdomain.cisco.com 58011:28:38.63908/24/12Sev=	Parámetros de proceso, y configuración sí mismo por consiguiente.

	user1, IP= 64.102.156.87, ARP gratuito enviado para 192.168.1.100 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, Quick Mode del curriculum vitae que procesa, CERT/transporte Exch/RM DSID completado 24 de agosto 11:31:13 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, FASE 1 COMPLETADA	Info/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = MODECFG_UNITY_PFS: , valor = 0x00000000 58111:28:38.63908/24/12Sev=Info/5IKE/0x6300000E MODE_CFG_REPLY: Atributo = APPLICATION_VERSION, valor = versión 8.4(4)1 de Cisco Systems, Inc ASA5505 construida por constructores el Thu 14-Jun-12 11:20 58211:28:38.63908/24/12Sev= Info/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = MODECFG_UNITY_SMARTCARD_REMOVAL_DISCONNECT: , valor = 0x00000001 58311:28:38.63908/24/12Sev= Info/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = recibido y con el NAT-T número del puerto, valor = 0x00001194 58411:28:39.36708/24/12Sev= Debug/9IKE/0x63000093 El valor para el parámetro. ini EnableDNSRedirection es 1 58511:28:39.36708/24/12Sev= Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_MODECFG_DONEEvent: EV_MODECFG_DONE_SUC	
Construya y envíe el DPD para el cliente.	24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, tipo señal de mantenimiento para esta conexión: DPD 24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, comenzando el P1 reintroducen el temporizador: 82080 segundos. 24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, enviando notifican el mensaje 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, construyendo el payload en blanco del hash 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, construyendo el payload del hash del qm 24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE QUE ENVÍA el mensaje (msgid=be8f7821) con las cargas útiles: HDR + el		

	HASH (8) + NOTIFICAN (11) + NINGUNOS (0) longitudes totales: 92	
	==========> del Dead Peer Detection del ========== (DPD)	
	58811:28:39.79508/24/12Sev=Debug/7IKE/0x63000015 intf_data: lcl=0x0501A8C0, mask=0x00FFFFFF, bcast=0xFF01A8C0, bcast_vra=0xFF07070A 58911:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_P2 59011:28:39.79508/24/12Sev=Info/4IKE/0x63000056 Recibió una petición dominante del driver: IP local = 192.168.1.100, GW IP= 64.102.156.88, IP remoto = 0.0.0.0 59111:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_ACTIVEEvent: EV_NO_EVENT 59211:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_INITIALEvent: EV_INITIATOR 59311:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG1Event: EV_CHK_PFS 59411:28:39.79608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG1Event: EV_BLD_MSG 59511:28:39.79608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG1Event: EV_START_RETRY_TMR	QM iniciado, construcción QM1 de la fase 2. Este proceso incluye: - Hash - SA con todas las ofertas de la fase 2 soportadas por el cliente, el tipo de túnel y el cifrado - Nonce - ID de cliente - ID de proxy
	59611:28:39.79608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG1Event: EV_SND_MSG 59711:28:39.79608/24/12Sev=Info/4IKE/0x63000013 ENVIANDO EL ISAKMP OAK QM del >>> * (HASH, SA, NON, ID, ID) a 64.102.156.88	Envíe QM1.
	========== del mensaje 1 del Quick Mode del <========== (QM1)	
Reciba QM1.	24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECIBIÓ el mensaje (msgid=e83792e) con las cargas útiles: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NINGUNOS (0) longitudes totales: 1026	

Proceso QM1. Configuración pertinente: `crypto dynamic-map DYN 10 set transform-set TRA`	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, procesando el payload del hash 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, procesando el payload SA 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, procesando el payload del nonce 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, payload identificador de proceso 24 de agosto 11:31:13 [IKEv1 DECODIFICA] el grupo = el IPSec, nombre de usuario = user1, IP= 64.102.156.87, ID_IPV4_ADDR ID recibido 192.168.1.100 24 de agosto 11:31:13 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, recibió los datos del host remotos del proxy en el payload ID: Dirija 192.168.1.100, el protocolo 0, el puerto 0 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, payload identificador de proceso 24 de agosto 11:31:13 [IKEv1 DECODIFICA] el grupo = el IPSec, nombre de usuario = user1, IP= 64.102.156.87, ID_IPV4_ADDR_SUBNET ID received--0.0.0.0--0.0.0.0 24 de agosto 11:31:13 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, recibió los datos de la subred del proxy del IP local en el payload ID: Dirija 0.0.0.0, máscara 0.0.0.0, el protocolo 0, el puerto 0 24 de agosto 11:31:13 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, sa viejo QM IsRekeyed no encontrado por el addr 24 de agosto 11:31:13 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, control de la correspondencia de criptografía estática, marcando la correspondencia = el hacia fuera-mapa, = 10 seq… 24 de agosto 11:31:13 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, control de la correspondencia de criptografía estática desviado: ¡Entrada de correspondencia de criptografía incompleta! 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, seleccionando solamente los modos del andUDP-Encapsular-transporte del UDP-Encapsular-túnel definidos por el NAT-Traversal 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, seleccionando solamente los modos del andUDP-Encapsular-transporte del UDP-	

	Encapsular-túnel definidos por el NAT-Traversal 24 de agosto 11:31:13 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, peer remoto IKE configurado para la correspondencia de criptografía: hacia fuera-dyn-mapa 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, procesando el payload IPSec SA	

Construcción QM2.
Configuración pertinente:
`tunnel-group EZ`
`type` **`remote-access`** *`! (tunnel type ra = tunnel type remote-access)`*
`crypto ipsec transform-set TRA` **`esp-aes esp-sha-hmac`**
`crypto ipsec security-association` **`lifetime seconds 28800`**
`crypto ipsec security-association lifetime kilobytes 4608000`
`crypto dynamic-map DYN 10 set transform-set TRA`
`crypto map MAP 65000 ipsec-isakmp dynamic DYN`
`crypto map MAP interface outside`
	24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, oferta IPSec SA # 12, transforman # 1 entrada global IPSec SA de los acceptableMatches # 10
	24 de agosto 11:31:13 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, IKE: ¡petición de SPI!
	IPSEC: Nuevo @ 0xcfdffc90 creado SA embrionario, SCB: 0xCFDFFB58, dirección: entrante
	SPI: 0x9E18ACB2
	ID de sesión: 0x00138000
	VPIF numérico: 0x00000004
	Tipo de túnel: ra
	Protocolo: especialmente
	Vida útil: 240 segundos
	24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, IKE consiguieron SPI del motor dominante: SPI = 0x9e18acb2
	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, oakley que construye el Quick Mode
	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, construyendo el payload en blanco del hash
	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, construyendo el payload IPSec SA
	24 de agosto 11:31:13 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, el IPSec del iniciador el reemplazar que reintroduce la duración a partir del 2147483 a 86400 segundos
	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, construyendo el payload del nonce del IPSec
	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, construyendo el ID de proxy
	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, ID de proxy que transmite:
	Host remoto: 192.168.1.100Protocol 0Port 0	

	Protocolo local 0Port 0 subnet:0.0.0.0mask 0.0.0.0 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, enviando la notificación del CURSO DE LA VIDA del RESPONDEDOR al iniciador 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, construyendo el payload del hash del qm	
Envíe QM2.	24 de agosto 11:31:13 [IKEv1 DECODIFICA] el grupo = el IPSec, nombre de usuario = user1, IP= 64.102.156.87, respondedor IKE que envía el 2do pkt QM: msg identificación = 0e83792e 24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE QUE ENVÍA el mensaje (msgid=e83792e) con las cargas útiles: HDR + HASH (8) + SA (1) + NONCE (10) + el ID (5) + ID (5) + NOTIFICA (11) + NINGUNOS (0) longitudes totales: 184	
	==========> del mensaje 2 del Quick Mode del ========== (QM2)	
	60811:28:39.96208/24/12Sev=Info/4IKE/0x63000014 RECIBIENDO EL ISAKMP OAK QM DEL <<< * (HASH, SA, NON, ID, ID, NOTIFIQUE: STATUS_RESP_LIFETIME) a partir del 64.102.156.88	Reciba QM2.
	60911:28:39.96408/24/12Sev=Decode/11IKE/0x63000001 Encabezado ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Respondedor COOKIE:1B301D2DE710EDA0 Payload siguiente: Hash Ver (Hex):10 Tipo del intercambio: Quick Mode Indicadores: (Cifrado) MessageID(Hex):E83792E Length:188 Hash del payload Payload siguiente: Asociación de seguridad Reservado: 00 Magnitud de carga útil: 24 Datos (en el hex.): CABF38A62C9B88D1691E81F3857D6189534B2EC0 Asociación de seguridad del payload Payload siguiente: Nonce Reservado: 00 Magnitud de carga útil: 52 DOI: IPSec Situación: (SIT_IDENTITY_ONLY) Oferta del payload Payload siguiente: Ninguno Reservado: 00	Proceso QM2. Ofertas elegidas demostraciones desencriptadas del payload.

	Magnitud de carga útil: 40 Oferta #: 1 ID del protocolo: PROTO_IPSEC_ESP Tamaño de SPI: 4 # de transforma: 1 SPI: 9E18ACB2 El payload transforma Payload siguiente: Ninguno Reservado: 00 Magnitud de carga útil: 28 Transforme #: 1 Transformar-identificación: ESP_3DES Reserved2: 0000 Tipo de la vida: Segundos Duración de la vida (hex.): 0020C49B Modo de encapsulación: Túnel UDP Algoritmo de autenticación: SHA1 Nonce del payload Payload siguiente: Identificación Reservado: 00 Magnitud de carga útil: 24 Datos (en el hex.): 3A079B75DA512473706F235EA3FCA61F1D15D4CD Identificación del payload Payload siguiente: Identificación Reservado: 00 Magnitud de carga útil: 12 Tipo ID: Dirección IPv4 ID del protocolo (UDP/TCP, etc…): 0 Puerto: 0 ID Data: 192.168.1.100 Identificación del payload Payload siguiente: Notificación Reservado: 00 Magnitud de carga útil: 16 Tipo ID: Subred del IPv4 ID del protocolo (UDP/TCP, etc…): 0 Puerto: 0 ID Data: 0.0.0.0/0.0.0.0 Notificación del payload Payload siguiente: Ninguno Reservado: 00 Magnitud de carga útil: 28 DOI: IPSec ID del protocolo: PROTO_IPSEC_ESP Tamaño de Spi: 4 Notifique el tipo: STATUS_RESP_LIFETIME SPI: 9E18ACB2 Data: Tipo de la vida: Segundos Duración de la vida (hex.): 00015180	
	61011:28:39.96508/24/12Sev=Debug/7IKE/0x6300007	Proceso QM2.

	6 NAV Trace->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Event: EV_RCVD_MSG 61111:28:39.96508/24/12Sev=Info/5IKE/0x63000045 RESPONDER-LIFETIME notifican tienen valor de 86400 segundos 61211:28:39.96508/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Event: EV_CHK_PFS 61311:28:39.96508/24/12Sev=Debug/7IKE/0x6300007 6	
	NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG3Event: EV_BLD_MSG 61411:28:39.96508/24/12Sev=Debug/7IKE/0x6300007 6 Encabezado ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Respondedor COOKIE:1B301D2DE710EDA0 Payload siguiente: Hash Ver (Hex):10 Tipo del intercambio: Quick Mode Indicadores: (Cifrado) MessageID(Hex):E83792E Length:52 Hash del payload Payload siguiente: Ninguno Reservado: 00 Magnitud de carga útil: 24 Datos (en el hex.): CDDC20D91EB4B568C826D6A5770A5CF020141236	Construcción QM3. Payload desencriptado para QM3 mostrado aquí. Este hash de proceso de los ncludes.
	61511:28:39.96508/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG3Event: EV_SND_MSG 61611:28:39.96508/24/12Sev=Info/4IKE/0x63000013 ENVIANDO EL ISAKMP OAK QM del >>> * (HASH) a 64.102.156.88	Envíe QM3. El cliente está listo ahora para cifrar y para desencriptar.
	========== del mensaje 3 del Quick Mode del <========== (QM3)	
Reciba QM3.	24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECIBIÓ el mensaje (msgid=e83792e) con las cargas útiles: HDR + HASH (8) + NINGUNOS (0) longitudes totales: 52	
Proceso QM3. Cree los índices entrantes y salientes del parámetro de seguridad (SPI). Agregue la Static ruta para el host. Configuración	24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, procesando el payload del hash 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, cargando todo el SA de IPSec ¡24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP=	

pertinente:
`crypto ipsec transform-set TRA esp-aes esp-sha-hmac`
`crypto ipsec security-association lifetime seconds 28800`
`crypto ipsec security-association lifetime kilobytes 4608000`
`crypto dynamic-map DYN 10 set transform-set TRA`
`crypto dynamic-map DYN 10` **`set reverse-route`**
	64.102.156.87, generando la clave del Quick Mode!
	24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, NP cifran la regla miran para arriba para el desconocido que corresponde con del hacia fuera-dyn-mapa 10 ACL de la correspondencia de criptografía: vuelto
	cs_id=cc107410; rule=00000000
	¡24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, generando la clave del Quick Mode!
	IPSEC: Nuevo @ 0xccc9ed60 creado SA embrionario, SCB: 0xCF7F59E0,
	Dirección: saliente
	SPI: 0xC055290A
	ID de sesión: 0x00138000
	VPIF numérico: 0x00000004
	Tipo de túnel: ra
	Protocolo: especialmente
	Vida útil: 240 segundos
	IPSEC: Actualización completada del host OBSA, SPI 0xC055290A
	IPSEC: Crear el contexto saliente VPN, SPI 0xC055290A
	Indicadores: 0x00000025
	SA: 0xccc9ed60
	SPI: 0xC055290A
	MTU: 1500 bytes
	VCID: 0x00000000
	Entidad par: 0x00000000
	SCB: 0xA5922B6B
	Canal: 0xc82afb60
	IPSEC: Contexto saliente completado VPN, SPI 0xC055290A
	Manija VPN: 0x0015909c
	IPSEC: Nuevo saliente cifra la regla, SPI 0xC055290A
	Addr del src: 0.0.0.0
	Máscara del src: 0.0.0.0
	Addr del dst: 192.168.1.100
	Máscara del dst: 255.255.255.255
	Puertos del src
	Parte superior: 0
	Baje: 0
	De Op. Sys.: ignore
	Puertos del dst
	Parte superior: 0
	Baje: 0
	De Op. Sys.: ignore
	Protocolo: 0
	Protocolo del uso: falso
	SPI: 0x00000000
	Uso SPI: falso
	IPSEC: Saliente completado cifra la regla, SPI	

	0xC055290A Regla ID: 0xcb47a710 IPSEC: Nueva regla saliente del permiso, SPI 0xC055290A Addr del src: 64.102.156.88 Máscara del src: 255.255.255.255 Addr del dst: 64.102.156.87 Máscara del dst: 255.255.255.255 Puertos del src Parte superior: 4500 Baje: 4500 De Op. Sys.: igual Puertos del dst Parte superior: 58506 Baje: 58506 De Op. Sys.: igual Protocolo: 17 Protocolo del uso: verdad SPI: 0x00000000 Uso SPI: falso IPSEC: Regla saliente completada del permiso, SPI 0xC055290A Regla ID: 0xcdf3cfa0 24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, NP cifran la regla miran para arriba para el desconocido que corresponde con del hacia fuera-dyn-mapa 10 ACL de la correspondencia de criptografía: vuelto cs_id=cc107410; rule=00000000 24 de agosto 11:31:13 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, negociación de seguridad completa para el usuario (user1)Responder, SPI entrante = 0x9e18acb2, saliente SPI = 0xc055290a 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, IKE consiguió un msg KEY_ADD para el SA: SPI = 0xc055290a IPSEC: Actualización completada del host IBSA, SPI 0x9E18ACB2 IPSEC: Crear el contexto entrante VPN, SPI 0x9E18ACB2 Indicadores: 0x00000026 SA: 0xcfdffc90 SPI: 0x9E18ACB2 MTU: bytes 0 VCID: 0x00000000 Entidad par: 0x0015909C SCB: 0xA5672481 Canal: 0xc82afb60 IPSEC: Contexto entrante completado VPN, SPI	

	0x9E18ACB2 Manija VPN: 0x0016219c IPSEC: Puesta al día del contexto saliente 0x0015909C VPN, SPI 0xC055290A Indicadores: 0x00000025 SA: 0xccc9ed60 SPI: 0xC055290A MTU: 1500 bytes VCID: 0x00000000 Entidad par: 0x0016219C SCB: 0xA5922B6B Canal: 0xc82afb60 IPSEC: Contexto saliente completado VPN, SPI 0xC055290A Manija VPN: 0x0015909c IPSEC: Regla interna saliente completada, SPI 0xC055290A Regla ID: 0xcb47a710 IPSEC: Regla externa saliente completada SPD, SPI 0xC055290A Regla ID: 0xcdf3cfa0 IPSEC: Nueva regla entrante del flujo del túnel, SPI 0x9E18ACB2 Addr del src: 192.168.1.100 Máscara del src: 255.255.255.255 Addr del dst: 0.0.0.0 Máscara del dst: 0.0.0.0 Puertos del src Parte superior: 0 Baje: 0 De Op. Sys.: ignore Puertos del dst Parte superior: 0 Baje: 0 De Op. Sys.: ignore Protocolo: 0 Protocolo del uso: falso SPI: 0x00000000 Uso SPI: falso IPSEC: Regla entrante completada del flujo del túnel, SPI 0x9E18ACB2 Regla ID: 0xcdf15270 IPSEC: Nueva regla entrante del decrypt, SPI 0x9E18ACB2 Addr del src: 64.102.156.87 Máscara del src: 255.255.255.255 Addr del dst: 64.102.156.88 Máscara del dst: 255.255.255.255 Puertos del src Parte superior: 58506 Baje: 58506 De Op. Sys.: igual Puertos del dst	

	Parte superior: 4500 Baje: 4500 De Op. Sys.: igual Protocolo: 17 Protocolo del uso: verdad SPI: 0x00000000 Uso SPI: falso IPSEC: Regla entrante completada del decrypt, SPI 0x9E18ACB2 Regla ID: 0xce03c2f8 IPSEC: Nueva regla entrante del permiso, SPI 0x9E18ACB2 Addr del src: 64.102.156.87 Máscara del src: 255.255.255.255 Addr del dst: 64.102.156.88 Máscara del dst: 255.255.255.255 Puertos del src Parte superior: 58506 Baje: 58506 De Op. Sys.: igual Puertos del dst Parte superior: 4500 Baje: 4500 De Op. Sys.: igual Protocolo: 17 Protocolo del uso: verdad SPI: 0x00000000 Uso SPI: falso IPSEC: Regla entrante completada del permiso, SPI 0x9E18ACB2 Regla ID: 0xcf6f58c0 24 de agosto grupo = IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, jarra: KEY_UPDATE recibido, spi 0x9e18acb2 24 de agosto el grupo = el IPSec del DEBUG [IKEv1 de 11:31:13], nombre de usuario = user1, IP= 64.102.156.87, comenzando el P2 reintroducen el temporizador: 82080 segundos. 24 de agosto 11:31:13 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, agregando la Static ruta para la dirección cliente: 192.168.1.100	
Fase 2 completa. Los ambos lados son que cifran y que desencriptan ahora.	24 de agosto 11:31:13 [IKEv1]Group = IPSec, nombre de usuario = user1, IP= 64.102.156.87, la FASE 2 COMPLETÓ (msgid=0e83792e)	
Para los hardwares cliente, se recibe un más mensaje donde el cliente envía la información sobre sí mismo. Si usted mira cuidadosamente,	24 de agosto 11:31:13 [IKEv1]: El IP= 10.48.66.23, IKE_DECODE RECIBIÓ el mensaje (msgid=91facca9) con las cargas útiles: HDR + el HASH (8) + NOTIFICAN (11) + NINGUNOS (0) longitudes totales: 184 24 de agosto DEBUG [IKEv1 de 11:31:13]: Grupo = EZ, nombre de usuario = Cisco, IP= 10.48.66.23,	

usted debe encontrar el nombre de host del cliente EzVPN, el software que se funciona con en el cliente, y ubicación y nombre del software	procesando el payload del hash 24 de agosto DEBUG [IKEv1 de 11:31:13]: El grupo = el EZ, nombre de usuario = Cisco, IP= 10.48.66.23, procesando notifican el payload 24 de agosto 11:31:13 [IKEv1 DECODIFICA]: DESCRIPTOR OBSOLETO - ÍNDICE 1 24 de agosto 11:31:13 [IKEv1 DECODIFICA]: 0000: 00000000 7534000B 62736E73 2D383731 ….u4. .bsns-871 0010: 2D332E75 32000943 6973636F 20383731 **-3.u2. Cisco 871** 0020: 7535000B 46484B30 39343431 32513675 u5..FHK094412Q6u 0030: 36000932 32383538 39353638 75390009 6..228589568u9. 0040: 31343532 31363331 32753300 2B666C61 145216312u3.+fla 0050: 73683A63 3837302D 61647669 70736572 **sh:c870-advipser** 0060: 76696365 736B392D 6D7A2E31 32342D32 **vicesk9-mz.124-2** 0070: 302E5435 2E62696E **0.T5.bin** 24 de agosto DEBUG [IKEv1 de 11:31:13]: Grupo = EZ, nombre de usuario = Cisco, IP= 10.48.66.23, procesando el hash del PSK 24 de agosto 11:31:13 [IKEv1]: Grupo = EZ, nombre de usuario = Cisco, IP= 192.168.1.100, tamaño contrario del hash del PSK 24 de agosto DEBUG [IKEv1 de 11:31:13]: ¡Grupo = EZ, nombre de usuario = Cisco, IP= 10.48.66.23, verificación del hash del PSK fallada!	

Verificación del túnel

ISAKMP

La salida del comando **sh del det AIA sa del grito** es:

```
 Active SA: 1
 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.48.66.23
 Type : user Role : responder
 Rekey : no State : AM_ACTIVE
 Encrypt : aes Hash : SHA
 Auth : preshared Lifetime: 86400
 Lifetime Remaining: 86387
 AM_ACTIVE - aggressive mode is active.
```

IPSec

Puesto que el Internet Control Message Protocol (ICMP) se utiliza para accionar el túnel, sólo un IPSec SA está para arriba. El protocolo 1 es ICMP. Observe que los valores de SPI diferencian de los negociados en los debugs. Éste es, de hecho, el mismo túnel después de la fase 2 reintroduce.

Haga salir del comando **crypto sh IPSec sa** es:

```
interface: outside
 Crypto map tag: DYN, seq num: 10, local addr: 10.48.67.14

 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
 remote ident (addr/mask/prot/port): (192.168.1.100/255.255.255.255/0/0)
 current_peer: 10.48.66.23, username: cisco
 dynamic allocated peer ip: 192.168.1.100

 #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: 5, #pkts comp failed: 0, #pkts decomp failed: 0
 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
 #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.48.67.14/0, remote crypto endpt.: 10.48.66.23/0
 path mtu 1500, ipsec overhead 74, media mtu 1500
 current outbound spi: C4B9A77C
 current inbound spi : EA2B6B15

 inbound esp sas:
 spi: 0xEA2B6B15 (3928714005)
 transform: esp-aes esp-sha-hmac no compression
 in use settings ={RA, Tunnel, }
 slot: 0, conn_id: 425984, crypto-map: DYN
 sa timing: remaining key lifetime (sec): 28714
 IV size: 16 bytes
 replay detection support: Y
 Anti replay bitmap:
 0x00000000 0x0000003F
 outbound esp sas:
 spi: 0xC4B9A77C (3300501372)
 transform: esp-aes esp-sha-hmac no compression
 in use settings ={RA, Tunnel, }
 slot: 0, conn_id: 425984, crypto-map: DYN
 sa timing: remaining key lifetime (sec): 28714
 IV size: 16 bytes
 replay detection support: Y
 Anti replay bitmap:
 0x00000000 0x00000001
```

Información Relacionada

- Artículo de Wikipedia sobre el IPSec
- Troubleshooting de IPSec: Entendiendo y con los comandos debug
- Soporte Técnico y Documentación - Cisco Systems