Nota técnica de solución de problemas de depuración de IPsec e IKE de ASA (modo agresivo IKEv1)

Contenido

Introducción

Este documento describe las depuraciones en Cisco Adaptive Security Appliance (ASA) cuando se utilizan el modo agresivo y la clave previamente compartida (PSK). También se trata la traducción de ciertas líneas de debug en la configuración. Cisco recomienda que tenga conocimientos básicos sobre IPsec e Intercambio de claves de Internet (IKE).

Este documento no explica el paso del tráfico después de que se haya establecido el túnel.

Problema principal

Las depuraciones IKE e IPsec son a veces crípticas, pero puede usarlas para comprender los problemas con el establecimiento del túnel VPN IPSec.

Situación

El modo agresivo se utiliza normalmente en el caso de Easy VPN (EzVPN) con software (Cisco VPN Client) y clientes de hardware (Cisco ASA 5505 Adaptive Security Appliance o Cisco IOS? Routers de software), pero sólo cuando se utiliza una clave previamente compartida. A diferencia del modo principal, el modo agresivo consta de tres mensajes.

Las depuraciones provienen de un ASA que ejecuta la versión de software 8.3.2 y actúa como

servidor EzVPN. El cliente EzVPN es un cliente de software.

Comandos debug utilizados

Estos son los comandos debug utilizados en este documento:

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

Configuración ASA

La configuración de ASA en este ejemplo está diseñada para ser estrictamente básica; no se utilizan 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 del mensaje del cliente
	49711:28:30.28908/24/12Sev=Información/6IKE/0x6300003B Intentando 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=000000000000000CurState: AM_INITIALEvent: EV_INITIATOR 49911:28:30.29708/24/12Sev=Información/4IKE/0x63000001 Inicio de la negociación de la fase 1 de IKE 50011:28:30.29708/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=000000000000000CurState: AM_SND_MSG1Evento: EV_GEN_DHKEY 50111:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=000000000000000CurState: AM_SND_MSG1Evento: EV_BLD_MSG 50211:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=000000000000000CurState: AM_SND_MSG1Evento: EV_START_RETRY_TMR 50311:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=000000000000000CurState: AM_SND_MSG1Evento: EV_SND_MSG		Se inicia el modo agresivo. Construir AM1. Este proceso incluye: - HDR ISAKMP - Dispositivo de seguridad (SA) que contiene todas las cargas útiles de transformación y las propuestas admitidas por el cliente - Carga útil de intercambio de claves - ID de iniciador de la fase 1 - Nonce
	50411:28:30.30408/24/12Sev=Información/4IKE/0x63000013 ENVÍO >> ISAKMP OAK AG (SA, KE, NON, ID, VID(Xauth), VID(dpd), VID(Frag), VID(Nat-T), VID(Unity)) a 64.102.156.88		Enviar AM1.
	<========== Mensaje agresivo 1 (AM1) ==========		
Recibir AM1 del cliente.	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87,	50611:28:30.33308/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5	Espere la respuesta del servidor.

	mensaje RECIBIDO IKE_DECODE (msgid=0) con cargas útiles: HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + NONE (0) longitud total: 849	R_Cookie=000000000000000CurState: AM_WAIT_MSG2Evento: EV_NO_EVENT	

Proceso AM1. Compare las propuestas recibidas y las transformaciones con las ya configuradas para las coincidencias. Configuración relevante: ISAKMP está habilitado en la interfaz y se define al menos una política que coincide con lo que el cliente envió:
 	
`crypto isakmp enable outside`
`crypto isakmp policy 10`
`authentication pre-share`
`encryption aes`
`hash sha`
`group 2`
`lifetime 86400`
Grupo de túnel que coincide con el nombre de identidad presente:
 	
`tunnel-group EZ type remote-access`
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, procesamiento de carga útil SA
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, procesamiento de carga útil de ke
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, procesamiento de la carga útil ISA_KE
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, procesamiento de carga útil única
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, carga útil de ID de procesamiento
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, procesamiento de la carga útil VID
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, VID de xauth V6 recibido
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, procesamiento de la carga útil VID
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, DPD VID recibido
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, procesamiento de la carga útil VID
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, VID de fragmentación recibida
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, IKE Peer incluía indicadores de capacidad de fragmentación IKE: Modo principal:Modo TrueAggressive:Falso
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, procesamiento de la carga útil VID
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, VID de NAT-Traversal recibida 02
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, procesamiento de la carga útil VID	

`tunnel-group EZ general-attributes`
`default-group-policy EZ`
`tunnel-group EZ ipsec-attributes`
`pre-shared-key cisco`
	24 de agosto 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, VID de cliente de Cisco Unity recibido
	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, la conexión aterrizó en el ipsec tunnel_group
	24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, procesamiento de la carga útil SA IKE
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5
	24 de agosto 11:31:03 [IKEv1]Fase 1 falla:Tipos de	

	atributo no coincidentes para la descripción del grupo de clase:Rcv'd: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, propuesta IKE SA nº 1, transformación # 5 aceptableCoincide con la entrada IKE global nº 1	
Construir AM2. Este proceso incluye: - políticas seleccionadas - Diffie-Hellman (DH) - ID del respondedor -autenticación - Carga útil de detección de traducción de direcciones de red (NAT)	24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construyendo la carga útil SA ISAKMP 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construyendo carga útil ke 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construyendo carga útil nonce 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, Generando claves para Respondedor.. 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construyendo carga útil de ID 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construyendo carga útil de troceo 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, hash informático para ISAKMP 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construyendo la carga útil VID de Cisco Unity 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construyendo la carga útil VID de xauth V6 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construyendo carga útil de vid dpd 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construyendo la carga útil de VID NAT-Traversal sobre 02 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construyendo la carga útil NAT-Discovery 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, hash de descubrimiento de NAT informático 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construyendo la carga útil NAT-Discovery 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, hash de descubrimiento de NAT informático 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construcción de VID de fragmentación + carga útil de capacidades extendidas 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construyendo carga útil VID 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, Enviar Altiga/Cisco VPN3000/Cisco ASA GW VID	

Enviar AM2.	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, mensaje de envío IKE_DECODE (msgid=0) con cargas útiles: HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + NAT-D (130) + PROVEEDOR (13) + PROVEEDOR 13) + NINGUNA (0) longitud total: 444	
	========== Mensaje agresivo 2 (AM2) ==========>	
	50711:28:30.40208/24/12Sev=Información/5IKE/0x6300002F Paquete ISAKMP recibido: peer = 64.102.156.8 50811:28:30.40308/24/12Sev=Información/4IKE/0x63000014 RECEPCIÓN DE << ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID(Unity), VID(Xauth), VID(dpd), VID(Nat-T), NAT-D, NAT-D, VID(Frag), VID(?)) desde 64.102.156.8 8 51011:28:30.41208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Evento: EV_RCVD_MSG	Recibir AM2.
	5111:28:30.41208/24/12Sev=Información/5IKE/0x63000001 Peer es un par compatible con Cisco-Unity 51211:28:30.41208/24/12Sev=Información/5IKE/0x63000001 El par admite XAUTH 51311:28:30.41208/24/12Sev=Información/5IKE/0x63000001 El par admite DPD 51411:28:30.41208/24/12Sev=Información/5IKE/0x63000001 Peer compatible con NAT-T 51511:28:30.41208/24/12Sev=Información/5IKE/0x63000001 El par admite cargas útiles de fragmentación IKE 51611:28:30.41208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Evento: EV_GEN_SKEYID 51711:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Evento: EV_AUTHENTICATE_PEER 51811:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Evento: EV_ADJUST_PORT	Proceso AM 2.

	51911:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Evento: EV_CRYPTO_ACTIVE	
	52011:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Evento: EV_BLD_MSG] 52111:28:30.42208/24/12Sev=Debug/8IKE/0x63000001 Se inició la construcción de ID de proveedor de IOS 52211:28:30.42208/24/12Sev=Información/6IKE/0x63000001 Contrusión de ID de proveedor de IOS exitosa	Construir AM3. Este proceso incluye Client Auth. En este momento, ya se han intercambiado todos los datos relevantes para el cifrado.
	52311:28:30.42308/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Evento: EV_SND_MSG 52411:28:30.42308/24/12Sev=Información/4IKE/0x63000013 ENVIAR >>> ISAKMP OAK AG *(HASH, NOTIFICAR:STATUS_INITIAL_CONTACT, NAT-D, NAT-D, VID(?), VID(Unity)) a 64.102.156.88	Enviar AM3.
	<========== Mensaje agresivo 3 (AM3) ==========	
Recibir AM3 del cliente.	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, mensaje RECIBIDO IKE_DECODE (msgid=0) con cargas útiles: HDR + HASH (8) + NOTIFICACIÓN (11) + NAT-D (130) + NAT-D (130) + PROVEEDOR (13) + PROVEEDOR (13) + NONE (0) longitud total : 168	
Proceso AM 3. Confirme el uso de NAT traversal (NAT-T). Ambos lados están listos para iniciar el cifrado del tráfico.	24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, carga útil de troceo de procesamiento 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, hash informático para ISAKMP 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, carga útil de notificación de procesamiento 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, procesamiento de la carga útil NAT-Discovery 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, hash de descubrimiento de NAT informático 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, procesamiento de la carga útil NAT-Discovery 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, hash de descubrimiento de NAT informático	

	24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, procesamiento de la carga útil VID 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, Procesamiento de la carga útil de ID de proveedor IOS/PIX (versión: 1.0.0, capacidades: 00000408) 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, procesamiento de la carga útil VID 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, VID de cliente de Cisco Unity recibido 24 de agosto 11:31:03 [IKEv1]Grupo = IPSec, IP = 64.102.156.87, Detección automática de NAT Estado: extremo remotoISdetrás de un dispositivo NATesteextremo NO está detrás de un dispositivo NAT	
Inicie la fase 1.5 (XAUTH) y solicite las credenciales del usuario.	24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construyendo carga útil de hash en blanco 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, construyendo carga útil de hash de qm 24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, mensaje de envío IKE_DECODE (msgid=fb709d4d) con cargas útiles: HDR + HASH (8) + ATTR (14) + NONE (0) longitud total : 72	
	========== XAuth - Solicitud de credenciales ==========>	
	53511:28:30.43008/24/12Sev=Información/4IKE/0x63000014 RECEPCIÓN DE << ISAKMP OAK TRANS *(HASH, ATTR) desde 64.102.156.88 53611:28:30.43108/24/12Sev=Decode/11IKE/0x63000001 Encabezado ISAKMP COOKIE del iniciador:D56197780D7BE3E5 COOKIE del contestador:1B301D2DE710EDA0 Siguiente carga útil:Hash Ver (hexadecimal):10 Tipo de intercambio:Transacción Indicadores:(Encriptación) MessageID (hexadecimal):FB709D4D Longitud:76 Hash de carga útil Siguiente carga útil: Atributos Reservado: 00 Longitud de carga útil: 24 Datos (En Hex): C779D5CBC5C75E3576C478A15A7CAB8A83A232D0 Atributos de carga útil Siguiente carga útil: Ninguno Reservado: 00 Longitud de carga útil: 20 Tipo: ISAKMP_CFG_REQUEST	Recibir solicitud de autenticación. La carga útil descifrada muestra los campos de nombre de usuario y contraseña vacíos.

	Reservado: 00 Identifier: 0000 Tipo XAUTH: GENÉRICO Nombre de usuario XAUTH: (empty) Contraseña de usuario XAUTH: (empty) 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	Iniciar la fase 1.5 (XAUTH). Inicie el temporizador de reintento mientras espera la entrada del usuario. Cuando se agota el temporizador de reintento, 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=Información/4IKE/0x63000013 ENVÍO >> ISAKMP OAK TRANS *(HASH, ATTR) a 64.102.156.88 54411:28:36.41508/24/12Sev=Decode/11IKE/0x63000001 Encabezado ISAKMP COOKIE del iniciador:D56197780D7BE3E5 COOKIE del contestador:1B301D2DE710EDA0 Siguiente carga útil:Hash Ver (hexadecimal):10 Tipo de intercambio:Transacción Indicadores:(Encriptación) MessageID (hexadecimal):FB709D4D Longitud:85 Hash de carga útil Siguiente carga útil: Atributos Reservado: 00 Longitud de carga útil: 24 Datos (En Hex): 1A3645155BE9A81CB80FCDB5F7F24E03FF8239F5 Atributos de carga útil Siguiente carga útil: Ninguno	Una vez recibida la entrada del usuario, envíe las credenciales del usuario al servidor. La carga útil descifrada muestra los campos de nombre de usuario y contraseña rellenados (pero ocultos). Send mode config request (varios atributos).

	Reservado: 00 Longitud de carga útil: 33 Tipo: ISAKMP_CFG_REPLY Reservado: 00 Identifier: 0000 Tipo XAUTH: GENÉRICO Nombre de usuario XAUTH: (datos no mostrados) Contraseña de usuario XAUTH: (datos no mostrados)	
	<========== Xauth - Credenciales de usuario ==========	
Recibir credenciales de usuario.	24 de agosto 11:31:09 [IKEv1]IP = 64.102.156.87, mensaje RECIBIDO IKE_DECODE (msgid=fb709d4d) con cargas útiles: HDR + HASH (8) + ATTR (14) + NINGUNO (0) longitud total: 85 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, process_tari(): Escriba!	

Procesar credenciales de usuario. Verifique las credenciales y genere la carga útil de configuración de modo.
Configuración relevante:
 	
`username cisco`
`password cisco`
	24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, IP = 64.102.156.87, Procesamiento de atributos de respuesta MODE_CFG.
	24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, IKEGetUserAttributes: DNS principal = 192.168.1.99
	24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, IKEGetUserAttributes: DNS secundario = borrado
	24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, IKEGetUserAttributes: WINS principal = borrado
	24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, IKEGetUserAttributes: WINS secundario = borrado
	24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, IKEGetUserAttributes: lista de túnel dividido = división
	24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, IKEGetUserAttributes: dominio predeterminado = jyoungta-labdomain.cisco.com
	24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, IKEGetUserAttributes: Compresión IP = inhabilitada
	24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, IKEGetUserAttributes: Política de túnel dividido = Desactivada
	24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, IKEGetUserAttributes: Configuración del proxy del navegador = no modificar
	24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, IKEGetUserAttributes: Proxy del navegador Omitir local	

	= inhabilitar 24 de agosto 11:31:09 [IKEv1]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Usuario (usuario1) autenticado.	
Enviar resultado xuath.	24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, construyendo carga útil de hash en blanco 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, construcción de carga útil de hash de qm 24 de agosto 11:31:09 [IKEv1]IP = 64.102.156.87, mensaje de envío IKE_DECODE (msgid=5b6910ff) con cargas útiles: HDR + HASH (8) + ATTR (14) + NONE (0) longitud total : 64	
	========== XAuth - 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=Información/5IKE/0x6300002F Paquete ISAKMP recibido: peer = 64.102.156.88 54811:28:36.42408/24/12Sev=Información/4IKE/0x63000014 RECEPCIÓN DE << ISAKMP OAK TRANS *(HASH, ATTR) desde 64.102.156.88 54911:28:36.42508/24/12Sev=Decode/11IKE/0x63000001 Encabezado ISAKMP COOKIE del iniciador:D56197780D7BE3E5 COOKIE del contestador:1B301D2DE710EDA0 Siguiente carga útil:Hash Ver (hexadecimal):10 Tipo de intercambio:Transacción Indicadores:(Encriptación) MessageID (hexadecimal):5B6910FF Longitud:76 Hash de carga útil Siguiente carga útil: Atributos Reservado: 00 Longitud de carga útil: 24 Datos (En Hex): 7DCF47827164198731639BFB7595F694C9DFE85 Atributos de carga útil Siguiente carga útil: Ninguno Reservado: 00 Longitud de carga útil: 12	Reciba resultados de autenticación y procese resultados.

	Tipo: ISAKMP_CFG_SET Reservado: 00 Identifier: 0000 Estado 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=Información/4IKE/0x630 00013 ENVÍO >> ISAKMP OAK TRANS *(HASH, ATTR) a 64.102.156.88	Resultados de ACK.
	<========== ==	
Recibir y procesar ACK; no hay respuesta del servidor.	24 de agosto 11:31:09 [IKEv1]IP = 64.102.156.87, mensaje RECIBIDO IKE_DECODE (msgid=5b6910ff) con cargas útiles: HDR + HASH (8) + ATTR (14) + NONE (0) longitud total : 60 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, process_tari(): Escriba! 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Procesamiento de atributos ACK de cfg	
	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 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:	Genere la solicitud mode-config. La carga útil descifrada muestra los parámetros solicitados desde el servidor.

	TM_FREEEvent: EV_NO_EVENT 56011:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_XAUTH_PROGEvent: EV_XAUTH_DONE_SUC 56111:28:38.40608/24/12Sev=Depurar/8IKE/0x630000 4C Inicio del temporizador DPD para IKE SA (I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0) sa->estado = 1, sa->dpd.care_freq(mSec) = 5000 56211:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_MODECFG 56311:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_NO_EVENT 56411:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_INITIALEvent: EV_INIT_MODECFG 56511:28:38.40808/24/12Sev=Información/5IKE/0x630 0005E Cliente que envía una solicitud de firewall al concentrador 56611:28:38.40908/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_START_RETRY_TMR	
	56711:28:38.40908/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_SND_MSG 56811:28:38.40908/24/12Sev=Información/4IKE/0x630 00013 ENVÍO >> ISAKMP OAK TRANS *(HASH, ATTR) a 64.102.156.88 56911:28:38.62708/24/12Sev=Decode/11IKE/0x63000 001 Encabezado ISAKMP COOKIE del iniciador:D56197780D7BE3E5 COOKIE del contestador:1B301D2DE710EDA0 Siguiente carga útil:Hash Ver (hexadecimal):10 Tipo de intercambio:Transacción Indicadores:(Encriptación) MessageID (hexadecimal):84B4B653	Enviar solicitud mode-config.

	Longitud:183 Hash de carga útil Siguiente carga útil: Atributos Reservado: 00 Longitud de carga útil: 24 Datos (En Hex): 81BFBF6721A744A815D69A315EF4AAA571D6B687 Atributos de carga útil Siguiente carga útil: Ninguno Reservado: 00 Longitud de carga útil: 131 Tipo: ISAKMP_CFG_REQUEST Reservado: 00 Identifier: 0000 Dirección IPv4: (empty) Máscara de red IPv4: (empty) DNS IPv4: (empty) NBNS IPv4 (WINS): (empty) Vencimiento de la dirección: (empty) Extensión de Cisco: Banner: (empty) Extensión de Cisco: Guardar PWD: (empty) Extensión de Cisco: Nombre de dominio predeterminado: (empty) Extensión de Cisco: Dividir incluir: (empty) Extensión de Cisco: Nombre DNS dividido: (empty) Extensión de Cisco: Hacer PFS: (empty) Desconocido: (empty) Extensión de Cisco: Servidores de respaldo: (empty) Extensión de Cisco: Desconexión de extracción de tarjeta inteligente: (empty) Versión de la aplicación: Cisco Systems VPN Client 5.0.07.0290:WinNT Extensión de Cisco: Tipo de firewall: (empty) Extensión de Cisco: Nombre de host DNS dinámico: ATBASU-LABBOX		
	<================ Solicitud de configuración de modo ==================		
Recibir solicitud de configuración de modo.	24 de agosto 11:31:11 [IKEv1]IP = 64.102.156.87, mensaje RECIBIDO IKE_DECODE (msgid=84b4b653) con cargas útiles: HDR + HASH (8) + ATTR (14) + NONE	57011:28:38.62808/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_NO_EVENT	Espere la respuesta del servidor.

	(0) longitud total : 183 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, process_tari(): Escriba!		
Process mode-config request. Muchos de estos valores se suelen configurar en la política de grupo. Sin embargo, dado que el servidor en este ejemplo tiene una configuración muy básica, no los ve aquí.	24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Procesamiento de atributos de solicitud de cfg 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Solicitud de dirección IPV4 recibida 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Solicitud recibida para máscara de red IPV4. 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Solicitud de dirección de servidor DNS recibida 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Solicitud recibida para la dirección del servidor WINS. 24 de agosto 11:31:11 [IKEv1]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, atributo de modo de transacción no admitido recibido: 5 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Solicitud de banner recibida 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Solicitud recibida para guardar la configuración de PW. 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Solicitud de nombre de dominio predeterminado recibida 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Solicitud recibida para la lista de túnel dividido. 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Se ha recibido la solicitud de DNS dividido.	

	24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Solicitud de configuración de PFS recibida 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Solicitud recibida para configuración de proxy del navegador de clientes. 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Solicitud de copia de seguridad de la lista de peers ip-sec recibida 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Solicitud recibida para la configuración de desconexión de la eliminación de Smartcard del cliente. 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Solicitud de versión de aplicación recibida 24 de agosto 11:31:11 [IKEv1]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Tipo de cliente: Versión de aplicación WinNTClient: 5.0.07.0290 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: Solicitud de FWTYPE recibida 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, MODE_CFG: La solicitud recibida para el nombre de host DHCP para DDNS es: ¡ATBASU-LABBOX!	

Construir la respuesta mode-config con todos los valores configurados.
Configuración relevante:
Tenga en cuenta que en este caso, siempre se asigna al usuario la misma 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 enableddns-server`
	24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, nombre de usuario = usuario1, IP = 64.102.156.87, dirección IP obtenida (192.168.1.100) antes de iniciar Mode Cfg habilitado (XAuth))
	24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Envío de máscara de subred (255.255.255.0) al cliente remoto
	24 de agosto 11:31:11 [IKEv1]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, dirección IP privada asignada 192.168.1.100 al usuario remoto
	24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, construyendo carga útil de hash en blanco
	24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, build_cfg_set: dominio predeterminado = jyoungta-labdomain.cisco.com
	24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Enviar atributos proxy del explorador de cliente!	

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 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Proxy del explorador establecido en No-Modify. Los datos del proxy del navegador NO se incluirán en la respuesta mode-cfg 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, Enviar desconexión de la eliminación de tarjetas inteligentes de Cisco activado!! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, construyendo carga útil de hash de qm	
Send mode-config response.	24 de agosto 11:31:11 [IKEv1]IP = 64.102.156.87, mensaje de envío IKE_DECODE (msgid=84b4b653) con cargas útiles: HDR + HASH (8) + ATTR (14) + NONE (0) longitud total : 215	
	==========>	
	57111:28:38.63808/24/12Sev=Información/5IKE/0x6300002F Paquete ISAKMP recibido: peer = 64.102.156.88 57211:28:38.63808/24/12Sev=Información/4IKE/0x63000014 RECEPCIÓN DE << ISAKMP OAK TRANS *(HASH, ATTR) desde 64.102.156.88 57311:28:38.63908/24/12Sev=Decode/11IKE/0x63000001 Encabezado ISAKMP COOKIE del iniciador:D56197780D7BE3E5 COOKIE del contestador:1B301D2DE710EDA0 Siguiente carga útil:Hash Ver (hexadecimal):10 Tipo de intercambio:Transacción Indicadores:(Encriptación) MessageID (hexadecimal):84B4B653 Longitud:220 Hash de carga útil Siguiente carga útil: Atributos Reservado: 00 Longitud de carga útil: 24 Datos (En Hex): 6DE2E70ACF6B1858846BC62E590C00A66745D14D Atributos de carga útil Siguiente carga útil: Ninguno Reservado: 00 Longitud de carga útil: 163 Tipo: ISAKMP_CFG_REPLY Reservado: 00 Identifier: 0000 Dirección IPv4: 192.168.1.100 Máscara de red IPv4: 255.255.255.0 DNS IPv4: 192.168.1.99 Extensión de Cisco: Guardar PWD: No Extensión de Cisco: Nombre de dominio	Recibir valores de parámetro mode-config del servidor.

	predeterminado: jyoungta-labdomain.cisco.com Extensión de Cisco: Hacer PFS: No Versión de la aplicación: Cisco Systems, Inc ASA5505 Versión 8.4(4)1 construida por los constructores el 14 de junio de 2012 11:20 Extensión de Cisco: Desconexión de extracción de tarjeta inteligente: Yes		
La fase 1 se completa en el servidor. Iniciar el proceso de modo rápido (QM).	24 de agosto 11:31:13 [IKEv1 DECODE]IP = 64.102.156.87, IKE Responder comienza QM: msg id = 0e83792e 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Retraso en el procesamiento del modo rápido, Cert/Trans Exch/RM DSID en curso 24 de agosto 11:31:13 [IKEv1]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, ARP Gratuito enviado para 192.168.1.100 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP =	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= Información/5IKE/0x63000010 MODE_CFG_REPLY: Atributo = INTERNAL_IPV4_ADDRESS:, valor = 192.168.1.100 57611:28:38.63908/24/12Sev=Información/5IKE/0x63000010 MODE_CFG_REPLY: Atributo = INTERNAL_IPV4_NETMASK:, valor = 255.255.255.0 57711:28:38.63908/24/12Sev= Información/5IKE/0x63000010 MODE_CFG_REPLY: Atributo = INTERNAL_IPV4_DNS(1): , valor = 192.168.1.99 57811:28:38.63908/24/12Sev=Información/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = MODECFG_UNITY_SAVEPWD: , valor = 0x0000000 57911:28:38.63908/24/12Sev=Información/5IKE/0x6300000E MODE_CFG_REPLY: Atributo = MODECFG_UNITY_DEFDOMAIN: , valor = jyoungta-labdomain.cisco.com 58011:28:38.63908/24/12Sev= Información/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = MODECFG_UNITY_PFS: , valor = 0x0000000 58111:28:38.63908/24/12Sev=Información/5IKE/0x6300000E MODE_CFG_REPLY: Atributo = APPLICATION_VERSION, valor = Cisco Systems, Inc ASA5505 Versión 8.4(4)1 generada por constructores en Thu 14-Jun-12 11:20 58211:28:38.63908/24/12Sev=	Procese los parámetros y configúrese en consecuencia.

	64.102.156.87, Reanudar el procesamiento en modo rápido, Cert/Trans Exch/RM DSID completado 24 de agosto 11:31:13 [IKEv1]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, FASE 1 COMPLETADA	Información/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = MODECFG_UNITY_SMARTCARD_REMOVAL_DISCONNECT: , valor = 0x00000001 58311:28:38.63908/24/12Sev= Información/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = Recibido y usando NAT-T número de puerto , valor = 0x00001194 58411:28:39.36708/24/12Sev= Debug/9IKE/0x63000093 El valor del 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	
Construir y enviar DPD para el cliente.	24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, Tipo de señal de mantenimiento para esta conexión: DPD 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Inicio del temporizador de nueva clave P1: 82080 segundos. 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, envío del mensaje de notificación 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, construyendo carga útil de hash en blanco 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, construyendo carga útil de hash de qm 24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, mensaje de envío IKE_DECODE (msgid=be8f7821) con cargas útiles: HDR + HASH (8) + NOTIFICACIÓN (11) + NONE (0) longitud total : 92		
	========== Detección de par muerto (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=Información/4IKE/0x63000056 Recibió una solicitud clave del controlador: IP local =	Iniciar QM, fase 2. Construir QM1. Este proceso incluye: - Hash - SA con todas las propuestas de la Fase 2 soportadas por el cliente, tipo de túnel y cifrado - Nonce

	192.168.1.100, IP GW = 64.102.156.88, IP remota = 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: Evento QM_BLD_MSG1: EV_CHK_PFS 59411:28:39.79608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: Evento QM_BLD_MSG1: EV_BLD_MSG 59511:28:39.79608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG1Evento: EV_START_RETRY_TMR	- ID del cliente - ID de proxy
	59611:28:39.79608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG1Evento: EV_SND_MSG 59711:28:39.79608/24/12Sev=Información/4IKE/0x63000013 ENVIAR >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) a 64.102.156.88	Enviar QM1.
	<========== Mensaje de modo rápido 1 (QM1) ==========	
Recibir QM1.	24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, mensaje RECIBIDO IKE_DECODE (msgid=e83792e) con cargas útiles: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) longitud total : 1026	
Proceso QM1. Configuración relevante: `crypto dynamic-map DYN 10 set transform-set TRA`	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, carga útil de troceo de procesamiento 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, procesamiento de carga útil SA 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, carga útil de procesamiento 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, carga útil de ID de procesamiento 24 de agosto 11:31:13 [IKEv1 DECODE]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, ID_IPV4_ADDR ID recibido 192.168.1.100	

	24 de agosto 11:31:13 [IKEv1]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Datos del host proxy remoto recibido en carga de ID:Dirección 192.168.1.100, Protocolo 0, Puerto 0 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, carga útil de ID de procesamiento 24 de agosto 11:31:13 [IKEv1 DECODE]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, ID_IPV4_ADDR_SUBNET ID recibido—0.0.0—0.0.0 24 de agosto 11:31:13 [IKEv1]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Datos de subred de proxy IP local recibidos en carga de ID:Dirección 0.0.0.0, Máscara 0.0.0, Protocolo 0, Puerto 0 24 de agosto 11:31:13 [IKEv1]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, QM se reescribe antigua si no se encuentra por addr 24 de agosto 11:31:13 [IKEv1]Grupo = ipsec, nombre de usuario = usuario1, IP = 64.102.156.87, verificación de mapa criptográfico estático, verificación de mapa = mapa externo, seq = 10... 24 de agosto 11:31:13 [IKEv1]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Verificación de mapa criptográfico estática superada: Entrada de mapa criptográfico incompleta. 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Selección sólo de los modos UDP-Encapsulated-Tunnel y UDP-Encapsulated-Transport definidos por NAT-Traversal 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Selección sólo de los modos UDP-Encapsulated-Tunnel y UDP-Encapsulated-Transport definidos por NAT-Traversal 24 de agosto 11:31:13 [IKEv1]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Peer remoto IKE configurado para mapa criptográfico: out-dyn-map 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, procesamiento de carga útil SA IPSec	

Construir QM2. Configuración relevante:
 	
`tunnel-group EZ`
`type` **`remote-access`** *`!`*
`(tunnel type ra = tunnel`
`type remote-access)`
`crypto ipsec`
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nombre de usuario = usuario1, IP = 64.102.156.87, propuesta SA IPSec nº 12, transformación # 1 aceptableCoincide con la entrada SA IPSec global nº 10
	24 de agosto 11:31:13 [IKEv1]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, IKE: ¡Pidiendo SPI!
	: Nueva SA embrionaria creada a @ 0xcfdffc90,	

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	SCB: 0xCFDFFB58, dirección: entrantes SPI: 0x9E18ACB2 ID de Sesión: 0x00138000 Número VPIF: 0x0000004 Tipo de túnel: ra Protocolo: esp Vida útil: 240 segundos 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, IKE obtuvo SPI del motor de claves: SPI = 0x9e18acb2 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, modo rápido de construcción de carro 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, construyendo carga útil de hash en blanco 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, construyendo carga útil SA IPSec 24 de agosto 11:31:13 [IKEv1]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, invalidación de la duración de la nueva codificación IPSec del iniciador de 2147483 a 86400 segundos 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, construyendo carga útil de IPSec nonce 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, que crea ID de proxy 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Transmisión de ID de proxy: Host remoto: 192.168.1.100Protocolo 0Puerto 0 Subred local:0.0.0.0mask 0.0.0 Protocolo 0Puerto 0 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Envío de la notificación DE DURACIÓN DEL RESPONSABLE al iniciador 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, construyendo carga útil de hash de qm	
Enviar QM2.	24 de agosto 11:31:13 [IKEv1 DECODE]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, IKE Responder envía 2a paquete QM: msg id = 0e83792e 24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, mensaje de envío IKE_DECODE (msgid=e83792e) con cargas útiles: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFICACIÓN (11) + NONE (0) longitud total: 184	
	========== Mensaje de modo rápido 2 (QM2) ==========>	
	60811:28:39.96208/24/12Sev=Información/4IKE/0x630	Recibir QM2.

	00014 RECIBIENDO <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFICACIÓN:STATUS_RESP_LIFETIME) desde 64.102.156.88	
	60911:28:39.96408/24/12Sev=Decode/11IKE/0x63000001 Encabezado ISAKMP COOKIE del iniciador:D56197780D7BE3E5 COOKIE del contestador:1B301D2DE710EDA0 Siguiente carga útil:Hash Ver (hexadecimal):10 Tipo de intercambio:Modo rápido Indicadores:(Encriptación) MessageID (hexadecimal):E83792E Longitud:188 Hash de carga útil Siguiente carga útil: Asociación de seguridad Reservado: 00 Longitud de carga útil: 24 Datos (En Hex): CABF38A62C9B88D1691E81F3857D6189534B2EC0 Asociación de seguridad de carga útil Siguiente carga útil: Nonce Reservado: 00 Longitud de carga útil: 52 DOI: IPsec Situación: (SIT_IDENTITY_ONLY) Propuesta de carga útil Siguiente carga útil: Ninguno Reservado: 00 Longitud de carga útil: 40 N.º de propuesta: 1 ID de protocolo: PROTO_IPSEC_ESP Tamaño de SPI: 4 Nº de transformaciones: 1 SPI: 9E18ACB2 Transformación de carga útil Siguiente carga útil: Ninguno Reservado: 00 Longitud de carga útil: 28 N.º de transformación: 1 ID de transformación: ESP_3DES Reservado2: 0000 Tipo de vida: Segundos Duración de la vida (hexadecimal): 0020C49B Modo de encapsulación: Túnel UDP Algoritmo de autenticación: SHA1 Payload Nonce Siguiente carga útil: Identificación Reservado: 00	Procesar QM2. La carga útil descifrada muestra las propuestas elegidas.

	Longitud de carga útil: 24 Datos (En Hex): 3A079B75DA512473706F235EA3FCA61F1D15D4CD Identificación de carga útil Siguiente carga útil: Identificación Reservado: 00 Longitud de carga útil: 12 Tipo de ID: Dirección IPv4 ID de protocolo (UDP/TCP, etc..): 0 Puerto: 0 ID Data: 192.168.1.100 Identificación de carga útil Siguiente carga útil: Notificación Reservado: 00 Longitud de carga útil: 16 Tipo de ID: Subred IPv4 ID de protocolo (UDP/TCP, etc..): 0 Puerto: 0 ID Data: 0.0.0.0/0.0.0.0 Notificación de carga útil Siguiente carga útil: Ninguno Reservado: 00 Longitud de carga útil: 28 DOI: IPsec ID de protocolo: PROTO_IPSEC_ESP Tamaño De Spi: 4 Tipo de notificación: STATUS_RESP_LIFETIME SPI: 9E18ACB2 Data: Tipo de vida: Segundos Duración de la vida (hexadecimal): 00015180	
	61011:28:39.96508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Evento: EV_RCVD_MSG 61111:28:39.96508/24/12Sev=Información/5IKE/0x63000045 El valor de notificación RESPONDER-LIFETIME es 86400 segundos 61211:28:39.96508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Evento: EV_CHK_PFS 61311:28:39.96508/24/12Sev=Debug/7IKE/0x63000076	Procesar QM2.
	NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG3Evento: EV_BLD_MSG 61411:28:39.96508/24/12Sev=Debug/7IKE/0x63000076 Encabezado ISAKMP COOKIE del iniciador:D56197780D7BE3E5 COOKIE del contestador:1B301D2DE710EDA0 Siguiente carga útil:Hash	Construir QM3. Carga útil descifrada para QM3 mostrada aquí. Este proceso incluye el hash.

	Ver (hexadecimal):10 Tipo de intercambio:Modo rápido Indicadores:(Encriptación) MessageID (hexadecimal):E83792E Longitud:52 Hash de carga útil Siguiente carga útil: Ninguno Reservado: 00 Longitud de carga útil: 24 Datos (En Hex): CDDC20D91EB4B568C826D6A5770A5CF020141236	
	61511:28:39.96508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG3Evento: EV_SND_MSG 61611:28:39.96508/24/12Sev=Información/4IKE/0x63000013 ENVIAR >>> ISAKMP OAK QM *(HASH) a 64.102.156.88	Enviar QM3. El cliente ya está listo para cifrar y descifrar.
	<========== Mensaje de modo rápido 3 (QM3) ==========	
Recibir QM3.	24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, mensaje RECIBIDO IKE_DECODE (msgid=e83792e) con cargas útiles: HDR + HASH (8) + NONE (0) longitud total : 52	

Procesar QM3. Cree los índices de parámetros de seguridad (SPI) entrantes y salientes. Agregue una ruta estática para el host. Configuración relevante:
 	
`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`**
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, carga útil de troceo de procesamiento
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, cargando todas las SA IPSEC
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, Generación de clave de modo rápido!
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, regla de cifrado NP buscar crypto map out-dyn-map 10 que coincida con ACL Desconocido: devuelto cs_id=cc107410; rule=00000000
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, Generación de clave de modo rápido!
	: Nueva SA embrionaria creada @ 0xccc9ed60, SCB: 0xCF7F59E0,
	Dirección: saliente
	SPI: 0xC055290A
	ID de Sesión: 0x00138000
	Número VPIF: 0x0000004
	Tipo de túnel: ra
	Protocolo: esp
	Vida útil: 240 segundos
	: Actualización de OBSA de host finalizada, SPI	

	0xC055290A : Creación del contexto de VPN saliente, SPI 0xC055290A Indicadores: 0x0000025 SA: 0xccc9ed60 SPI: 0xC055290A MTU: 1500 bytes VCID: 0x00000000 Entidad par: 0x00000000 SCB: 0xA5922B6B Canal: 0xc82afb60 : Contexto de VPN saliente completado, SPI 0xC055290A Identificador de VPN: 0x0015909c : Nueva regla de cifrado saliente, SPI 0xC055290A Dirección Src: 0.0.0.0 Máscara Src: 0.0.0.0 Dirección Dst: 192.168.1.100 Máscara Dst: 255.255.255.255 Puertos Src Superior: 0 Menor: 0 Op: ignore Puertos Dst Superior: 0 Menor: 0 Op: ignore Protocolo: 0 Usar protocolo: falso SPI: 0x00000000 Utilice SPI: falso : Regla de cifrado saliente completada, SPI 0xC055290A ID de regla: 0xcb47a710 : Nueva regla de permiso de salida, SPI 0xC055290A Dirección Src: 64.102.156.88 Máscara Src: 255.255.255.255 Dirección Dst: 64.102.156.87 Máscara Dst: 255.255.255.255 Puertos Src Superior: 4500 Menor: 4500 Op: igual Puertos Dst Superior: 58506 Menor: 58506 Op: igual Protocolo: 17 Usar protocolo: verdadero SPI: 0x00000000 Utilice SPI: falso : Regla de permiso saliente completada, SPI 0xC055290A	

	ID de regla: 0xcdf3cfa0 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, regla de cifrado NP buscar crypto map out-dyn-map 10 que coincida con ACL Desconocido: devuelto cs_id=cc107410; rule=00000000 24 de agosto 11:31:13 [IKEv1]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Negociación de seguridad completa para el usuario (usuario1)Respondedor, SPI entrante = 0x9e18acb2, Saliente SPI = 0xc055290a 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, nombre de usuario = usuario1, IP = 64.102.156.87, IKE obtuvo un mensaje KEY_ADD para SA: SPI = 0xc055290a : Actualización de IBSA de host finalizada, SPI 0x9E18ACB2 : Creación del contexto de VPN entrante, SPI 0x9E18ACB2 Indicadores: 0x0000026 SA: 0xcfdffc90 SPI: 0x9E18ACB2 MTU: 0 bytes VCID: 0x00000000 Entidad par: 0x0015909C SCB: 0xA5672481 Canal: 0xc82afb60 : Contexto de VPN entrante completado, SPI 0x9E18ACB2 Identificador de VPN: 0x0016219c : Actualización del contexto de VPN saliente 0x0015909C, SPI 0xC055290A Indicadores: 0x0000025 SA: 0xccc9ed60 SPI: 0xC055290A MTU: 1500 bytes VCID: 0x00000000 Entidad par: 0x0016219C SCB: 0xA5922B6B Canal: 0xc82afb60 : Contexto de VPN saliente completado, SPI 0xC055290A Identificador de VPN: 0x0015909c : Regla interna saliente completada, SPI 0xC055290A ID de regla: 0xcb47a710 : Regla SPD externa saliente completada, SPI 0xC055290A ID de regla: 0xcdf3cfa0 : Nueva regla de flujo de túnel entrante, SPI 0x9E18ACB2 Dirección Src: 192.168.1.100 Máscara Src: 255.255.255.255	

	Dirección Dst: 0.0.0.0 Máscara Dst: 0.0.0.0 Puertos Src Superior: 0 Menor: 0 Op: ignore Puertos Dst Superior: 0 Menor: 0 Op: ignore Protocolo: 0 Usar protocolo: falso SPI: 0x00000000 Utilice SPI: falso : Regla de flujo de túnel entrante completada, SPI 0x9E18ACB2 ID de regla: 0xcdf15270 : Nueva regla de descifrado entrante, SPI 0x9E18ACB2 Dirección Src: 64.102.156.87 Máscara Src: 255.255.255.255 Dirección Dst: 64.102.156.88 Máscara Dst: 255.255.255.255 Puertos Src Superior: 58506 Menor: 58506 Op: igual Puertos Dst Superior: 4500 Menor: 4500 Op: igual Protocolo: 17 Usar protocolo: verdadero SPI: 0x00000000 Utilice SPI: falso : Regla de descifrado entrante completada, SPI 0x9E18ACB2 ID de regla: 0xce03c2f8 : Nueva regla de permiso entrante, SPI 0x9E18ACB2 Dirección Src: 64.102.156.87 Máscara Src: 255.255.255.255 Dirección Dst: 64.102.156.88 Máscara Dst: 255.255.255.255 Puertos Src Superior: 58506 Menor: 58506 Op: igual Puertos Dst Superior: 4500 Menor: 4500 Op: igual Protocolo: 17 Usar protocolo: verdadero	

	SPI: 0x00000000 Utilice SPI: falso : Regla de permiso entrante completada, SPI 0x9E18ACB2 ID de regla: 0xcf6f58c0 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Pitcher: received KEY_UPDATE, spi 0x9e18acb2 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Temporizador de reinicio P2: 82080 segundos. 24 de agosto 11:31:13 [IKEv1]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, Agregar ruta estática para dirección de cliente: 192.168.1.100	
Fase 2 completa. Ambos lados están cifrando y descifrando ahora.	24 de agosto 11:31:13 [IKEv1]Grupo = IPSec, Nombre de usuario = usuario1, IP = 64.102.156.87, FASE 2 COMPLETADA (msgid=0e83792e)	
Para los clientes de hardware, se recibe un mensaje más donde el cliente envía información sobre sí mismo. Si observa con cuidado, debe encontrar el nombre de host del cliente EzVPN, el software que se ejecuta en el cliente, y la ubicación y el nombre del software	24 de agosto 11:31:13 [IKEv1]: IP = 10.48.66.23, mensaje IKE_DECODE RECIBIDO (msgid=91facca9) con cargas útiles: HDR + HASH (8) + NOTIFICACIÓN (11) + NONE (0) longitud total : 184 24 de agosto 11:31:13 [DEPURACIÓN IKEv1]: Grupo = EZ, Nombre de usuario = cisco, IP = 10.48.66.23, carga útil de hash de procesamiento 24 de agosto 11:31:13 [DEPURACIÓN IKEv1]: Grupo = EZ, Nombre de usuario = Cisco, IP = 10.48.66.23, carga útil de notificación de procesamiento 24 de agosto 11:31:13 [IKEv1 DECODE]: DESCRIPTOR OBSOLETO - ÍNDICE 1 24 de agosto 11:31:13 [IKEv1 DECODE]: 0000: 0000000 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-consepser** 0060: 76696365 736B392D 6D7A2E31 32342D32 **vicesk9-mz.124-2** 0070: 302E5435 2E62696E **0.T5.bin** 24 de agosto 11:31:13 [DEPURACIÓN IKEv1]: Grupo = EZ, Nombre de usuario = Cisco, IP = 10.48.66.23, Procesamiento de Hash PSK 24 de agosto 11:31:13 [IKEv1]: Grupo = EZ, Nombre de usuario = cisco, IP = 192.168.1.100, tamaño hash	

	PSK incoherente 24 de agosto 11:31:13 [DEPURACIÓN IKEv1]: Grupo = EZ, Nombre de usuario = Cisco, IP = 10.48.66.23, Error de verificación de hash PSK.	

Verificación del túnel

ISAKMP

El resultado del comando **sh cry isa sa det** 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

Dado que el protocolo de mensajes de control de Internet (ICMP) se utiliza para activar el túnel, solo una SA IPsec está activa. El protocolo 1 es ICMP. Tenga en cuenta que los valores SPI difieren de los negociados en las depuraciones. Este es, de hecho, el mismo túnel después de la nueva clave de la Fase 2.

El resultado del comando **sh crypto 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 IPSec
- Resolución de problemas de IPsec: Introducción y uso de los comandos debug
- Soporte Técnico y Documentación - Cisco Systems