

Debugs ASA IKEv2 para el troubleshooting del VPN de acceso remoto

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Cuestión central](#)

[Situación](#)

[Comandos de Debug](#)

[Configuración ASA](#)

[Archivo XML](#)

[Registros y descripciones del debug](#)

[Verificación del túnel](#)

[AnyConnect](#)

[ISAKMP](#)

[IPSec](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo entender los debugs en el dispositivo de seguridad adaptante de Cisco (ASA) cuando el intercambio de claves de Internet versión 2 (IKEv2) se utiliza con un Cliente de movilidad Cisco AnyConnect Secure. Este documento también proporciona la información sobre cómo traducir ciertas líneas del debug en una configuración ASA.

Este documento no describe cómo pasar el tráfico después de que un túnel VPN se haya establecido al ASA, ni incluye los conceptos básicos de IPSec o de IKE.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento del intercambio de paquetes para IKEv2. Para más información, refiera al [intercambio de paquetes IKEv2 y al debugging del nivel del protocolo](#).

Componentes Utilizados

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

- Intercambio de claves de Internet versión 2 (IKEv2)
- Versión 8.4 o posterior adaptante del dispositivo de seguridad de Cisco (ASA)

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

Cuestión central

El Centro de Asistencia Técnica de Cisco (TAC) utiliza a menudo los comandos debug IKE y del IPsec para entender donde hay un problema con el establecimiento del túnel del IPsec VPN, pero los comandos pueden ser secretos.

Situación

Comandos de Debug

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
debug aggregate-auth xml 5
```

Configuración ASA

Esta configuración ASA es estrictamente básica, sin el uso de los servidores externos.

```
interface Ethernet0/1
  nameif outside
  security-level 0
  ip address 10.0.0.1 255.255.255.0

ip local pool webvpn1 10.2.2.1-10.2.2.10

crypto ipsec ikev2 ipsec-proposal 3des
  protocol esp encryption aes-256 aes 3des des
  protocol esp integrity sha-1
crypto dynamic-map dynmap 1000 set ikev2 ipsec-proposal 3des
crypto map crymap 10000 ipsec-isakmp dynamic dynmap
crypto map crymap interface outside

crypto ca trustpoint Anu-ikev2
  enrollment self
  crl configure
```

```

crypto ikev2 policy 10
  encryption aes-192
  integrity sha
  group 2
  prf sha
  lifetime seconds 86400

crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint Anu-ikev2
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1
ssl trust-point Anu-ikev2 outside

webvpn
  enable outside
  anyconnect image disk0:/anyconnect-win-3.0.1047-k9.pkg 1
  anyconnect profiles Anyconnect-ikev2 disk0:/anyconnect-ikev2.xml
  anyconnect enable
  tunnel-group-list enable

group-policy ASA-IKEV2 internal
group-policy ASA-IKEV2 attributes
  wins-server none
  dns-server none
  vpn-tunnel-protocol ikev2
  default-domain none
  webvpn
  anyconnect modules value dart
  anyconnect profiles value Anyconnect-ikev2 type user

username Anu password lAuoFgF7KmB3D0WI encrypted privilege 15

tunnel-group ASA-IKEV2 type remote-access
tunnel-group ASA-IKEV2 general-attributes
  address-pool webvpn1
  default-group-policy ASA-IKEV2
tunnel-group ASA-IKEV2 webvpn-attributes
  group-alias ASA-IKEV2 enable

```

Archivo XML

```

<ServerList>
  <HostEntry>
    <HostName>Anu-IKEV2</HostName>
    <HostAddress>10.0.0.1</HostAddress>
    <UserGroup>ASA-IKEV2</UserGroup>
    <PrimaryProtocol>IPsec</PrimaryProtocol>
  </HostEntry>
</ServerList>

```

Note: El nombre del grupo de usuarios en el perfil del cliente XML debe ser lo mismo que el nombre del grupo de túnel en el ASA. Si no, entrada de host inválida del mensaje de error “Entre de nuevo por favor” se ve en el cliente de AnyConnect.

Haga el debug de los registros y las descripciones

Note: Los registros de los diagnósticos y de la herramienta de informe (DARDO) son generalmente registros muy habladores, así que ciertos del DARDO se han omitido en este

ejemplo debido a la insignificancia.

Descripción del mensaje del servidor

Depuraciones

Fecha: 04/23/2013
Hora: 16:24:55
Tipo: Información
Fuente: acvpnu

Descripción: Función: ClientIcBase:: conecte
Archivo: . \ ClientIcBase.cpp
Línea: 964
Una conexión VPN a Anu-IKEV2 ha sido pedida por el usuario.

Fecha: 04/23/2013
Hora: 16:24:55
Tipo: Información
Fuente: acvpnu

Descripción: Información del Tipo de mensaje enviada al usuario:
Entrar en contacto Anu-IKEV2.

Fecha: 04/23/2013
Hora: 16:24:55
Tipo: Información
Fuente: acvpnu

Descripción: Función: ApiCert:: getCertList
Archivo: . \ ApiCert.cpp
Línea: 259
Número de Certificados encontrados: 0

Fecha: 04/23/2013
Hora: 16:25:00
Tipo: Información
Fuente: acvpnu

Descripción: **Iniciación de la conexión VPN al gateway seguro**
https://10.0.0.1/ASA-IKEV2

Fecha: 04/23/2013
Hora: 16:25:00
Tipo: Información
Fuente: acvpnagent

Descripción: Túnel iniciado por el GUI del cliente.

Fecha: 04/23/2013
Hora: 16:25:02
Tipo: Información
Fuente: acvpnagent

Descripción: Función: CIPsecProtocol:: connectTransport

Archivo: . \ IPsecProtocol.cpp

Línea: 1629

Socket abierto IKE a partir de la 192.168.1.1:25170 a 10.0.0.1:500

-----Comienzo del intercambio IKE_SA_INIT-----

El ASA recibe el mensaje IKE_SA_INIT del cliente.

El primer par de mensajes es el intercambio IKE_SA_INIT. Estos mensajes negocian los algoritmos criptográficos, nonces del intercambio, y hacen un intercambio del Diffie-Hellman (DH).

El mensaje IKE_SA_INIT recibido del cliente contiene estos campos:

1. **Encabezado ISAKMP** - SPI/version/flags.
2. **SAi1** - Algoritmo criptográfico que el iniciador IKE soporta.
3. **KEi** - Valor de clave pública DH del iniciador.
4. **N** - Nonce del iniciador.

IKEv2-PLAT-4: [IKE_SA_INIT] [192.168.1.1]:25170->[10.0.0.1]:500
InitSPI=0x58aff71141ba436b RespSPI=0x0000000000000000 MID=0000
del PKT RECV

IKEv2-PROTO-3: Rx [L m_id 10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0

IKEv2-PROTO-3: **HDR[i:58AFF71141BA436B** - r: 0000000000000000]

IKEv2-PROTO-4: **Ispi IKEV2 HDR: 58AFF71141BA436B - rspi: 0000000000000000**

IKEv2-PROTO-4: Payload siguiente: SA, **versión: 2.0**

IKEv2-PROTO-4: Tipo del intercambio: IKE_SA_INIT, **indicadores: INICIA**

IKEv2-PROTO-4: ID del mensaje: 0x0, longitud: 528

Payload siguiente **SA**: KE, reservado: 0x0, longitud: 168

IKEv2-PROTO-4: la oferta más reciente: 0x0, reservado: 0x0, longitud: 1

Oferta: 1, ID del protocolo: IKE, tamaño de SPI: 0, #trans: 18

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 12
tipo: 1, reservado: 0x0, identificación: AES-CBC

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 12
tipo: 1, reservado: 0x0, identificación: AES-CBC

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 12
tipo: 1, reservado: 0x0, identificación: AES-CBC

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 1, reservado: 0x0, identificación: 3DES

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 1, reservado: 0x0, identificación: DES

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 2, reservado: 0x0, identificación: SHA512

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 2, reservado: 0x0, identificación: SHA384

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 2, reservado: 0x0, identificación: SHA256

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 2, reservado: 0x0, identificación: SHA1

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 2, reservado: 0x0, identificación: MD5

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: SHA512

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: SHA384

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: SHA256

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: SHA96

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: MD596

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 4, reservado: 0x0, identificación: DH_GROUP_1536_MODP/Group

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 4, reservado: 0x0, identificación: DH_GROUP_1024_MODP/Group
IKEv2-PROTO-4: el último transforma: 0x0, reservado: 0x0: longitud: 8
tipo: 4, reservado: 0x0, identificación: DH_GROUP_768_MODP/Group

Payload siguiente **KE**: N, reservada: 0x0, longitud: 104
Grupo DH: 1, reservado: 0x0

ed 4a 54 b1 13 7c b8 89 de los Cb 2e d1 28 FE eb 5e 29
f7 62 13 6b df 95 88 28 vago b5 97 52 e4 ef 1d 28
Ca 06 d1 36 b6 67 DD 4e d8 c7 80 de 20 32 9a c2
36 34 ed 5f c5 b3 3e 1d 83 1a c7 fb 9d b8 c5 f5
vago 4f b6 b2 e2 2.o de los vago 43 4f a0 b6 90 9a 11 3f 7d
0a 21 c3 4d d3 0a d2 1e 33 43 e0 del cc 4b 38 d3 5e
Payload siguiente **N**: VID, reservado: 0x0, longitud: 24

20 12 8f 22 7b 16 23 52 e4 29 4d 98 c7 fd a8 77
ce 7c 0b b4

IKEv2-PROTO-5: Analice el payload específico del vendedor: Payload
siguiente CISCO-DELETE-REASON VID: VID, reservado: 0x0, longitud: 2

El ASA verifica y procesa
Mensaje IKE_INIT. El ASA:

1. Elige la habitación crypto de éstos ofrecidos por el iniciador.
2. Computa su propia clave secreta DH.
3. Computa un valor SKEYID de para cuál todas las claves se pueden derivar este IKE_SA. Las encabezados de todos los mensajes subsiguientes son cifrado y autenticado. claves usadas para el cifrado y se deriva la protección de la integridad de SKEYID y se conocen como:

SK_e - Cifrado.**SK_a** - Autenticación.**SK_d** - Derivado y utilizado para la derivación de más futuro material de codificación

Paquete descifrado: Datos: 528 bytes
IKEv2-PLAT-3: Cargas útiles de proceso de la aduana VID
IKEv2-PLAT-3: Cisco Copyright VID recibido del par
IKEv2-PLAT-3: AnyConnect EAP VID recibido del par
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento OC
EV_RECV_INIT
IKEv2-PROTO-3: (6): Detección del control NAT
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento OC
EV_CHK_REDIRECT
IKEv2-PROTO-5: (6): Reoriente el control no es necesario, saltándolo
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento OC
EV_CHK_CAC
IKEv2-PLAT-5: **Nueva petición ikev2 sa admitida**
IKEv2-PLAT-5: Incrementar la cuenta de negociación entrante sa por una
IKEv2-PLAT-5: MANIJA INVÁLIDA PSH
IKEv2-PLAT-5: MANIJA INVÁLIDA PSH
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento OC
EV_CHK_COOKIE
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento OC
EV_CHK4_COOKIE_NOTIFY
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento R_I
EV_VERIFY_MSG
IKEv2-PROTO-3: (6): **Verifique el mensaje del init SA**
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento R_I
EV_INSERT_SA
IKEv2-PROTO-3: (6): Inserte el SA

para
CHILD_SAs.Un SK_e y
un SK_a separados son
computado para cada
dirección.

Configuración pertinente:

```
crypto ikev2 policy 10
  encryption aes-192 integrity
  sha group 2 prf sha lifetime
  seconds 86400
crypto ikev2 enable outside
```

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento R_...
EV_GET_IKE_POLICY
IKEv2-PROTO-3: (6): **Conseguir las directivas configuradas**
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento R_...
EV_PROC_MSG
IKEv2-PROTO-2: (6): Proceso del mensaje inicial
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento R_...
EV_DETECT_NAT
IKEv2-PROTO-3: (6): La detección de proceso NAT notifica
IKEv2-PROTO-5: (6): El proceso nacional detecta el src para notificar
IKEv2-PROTO-5: (6): Dirección remota no correspondida con
IKEv2-PROTO-5: (6): El proceso nacional detecta el dst para notificar
IKEv2-PROTO-5: (6): Dirección local correspondida con
IKEv2-PROTO-5: (6): El host es NAT localizado afuera
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento R_...
EV_CHK_CONFIG_MODE
IKEv2-PROTO-3: (6): Datos válidos recibidos del modo de configuración
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento R_...
EV_SET_RECD_CONFIG_MODE
IKEv2-PROTO-3: (6): Fije los datos recibidos del modo de configuración
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento
R_BLD_INIT: EV_SET_POLICY
IKEv2-PROTO-3: (6): **Determinación de las directivas configuradas**
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento
R_BLD_INIT: EV_CHK_AUTH4PKI
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento
R_BLD_INIT: EV_PKI_SESH_OPEN
IKEv2-PROTO-3: (6): Apertura de una sesión PKI
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento
R_BLD_INIT: EV_GEN_DH_KEY
IKEv2-PROTO-3: (6): **Clave pública computacional DH**
IKEv2-PROTO-3: (6):
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento
R_BLD_INIT: EV_NO_EVENT
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento
R_BLD_INIT: EV_OK_RECD_DH_PUBKEY_RESP
IKEv2-PROTO-5: (6): Acción: Action_Null
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento
R_BLD_INIT: EV_GEN_DH_SECRET
IKEv2-PROTO-3: (6): **Clave secreta computacional DH**
IKEv2-PROTO-3: (6):

El ASA construye el mensaje de respuesta para el intercambio IKE_SA_INIT.

Este paquete contiene:

1. **Encabezado ISAKMP** - SPI/version/flags.
2. **SAr1** - Algoritmo criptográfico que el respondedor IKE elige.
3. **KEr** - Valor de clave pública DH del respondedor.
4. **N** - Nonce del respondedor.

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_NO_EVENT

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_OK_REC'D_DH_SECRET_RESP

IKEv2-PROTO-5: (6): Acción: Action_Null

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_GEN_SKEYID

IKEv2-PROTO-3: (6): **Genere el skeyid**

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_GET_CONFIG_MODE

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: **EV_BLD_MSG**

IKEv2-PROTO-2: (6): **Envío del mensaje inicial**

IKEv2-PROTO-3: Propuesta IKE: 1, tamaño de SPI: 0 (negociación inicial). Numérico. transforma: 4

AES-CBC SHA1 SHA96 DH_GROUP_768_MODP/Group 1

IKEv2-PROTO-5: Payload específico del vendedor de la construcción: DE

REASONIKEv2-PROTO-5: Payload específico del vendedor de la construcción

(CUSTOM)IKEv2-PROTO-5: Payload específico del vendedor de la construcción: (CUSTOM)IKEv2-PROTO-5: La construcción notifica el pay

NAT_DETECTION_SOURCE_IPIKEv2-PROTO-5: La construcción notifica

payload: NAT_DETECTION_DESTINATION_IPIKEv2-PLAT-2: No podido

los emisores de confianza desmenuza o ningunos disponibles

IKEv2-PROTO-5: Payload específico del vendedor de la construcción:

FRAGMENTATIONIKEv2-PROTO-3: Tx [L m_id 10.0.0.1:500/R

192.168.1.1:25170/VRF i0:f0]: 0x0

IKEv2-PROTO-3: **HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]**

IKEv2-PROTO-4: **Ispi IKEV2 HDR: 58AFF71141BA436B - rspi: FC696330E6B94D7F**

FC696330E6B94D7F

IKEv2-PROTO-4: Payload siguiente: SA, versión: 2.0

IKEv2-PROTO-4: Tipo del intercambio: IKE_SA_INIT, **indicadores:**

RESPONDEDOR MSG-RESPONSE

IKEv2-PROTO-4: ID del mensaje: 0x0, longitud: 386

Payload siguiente **SA**: KE, reservado: 0x0, longitud: 48

IKEv2-PROTO-4: la oferta más reciente: 0x0, reservado: 0x0, longitud: 4

Oferta: 1, ID del protocolo: IKE, tamaño de SPI: 0, #trans: 4

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 12

tipo: 1, reservado: 0x0, identificación: AES-CBC

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8

tipo: 2, reservado: 0x0, identificación: SHA1

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8

tipo: 3, reservado: 0x0, identificación: SHA96

IKEv2-PROTO-4: el último transforma: 0x0, reservado: 0x0: longitud: 8

tipo: 4, reservado: 0x0, identificación: DH_GROUP_768_MODP/Group 1

Payload siguiente **KE**: N, reservada: 0x0, longitud: 104

Grupo DH: 1, reservado: 0x0

c9 30 f9 32 d4 7c d1 a7 5b 71 72 09 6e 7e 91 0c
ce b4 a4 3c F2 8b 74 4e 20 del e1 59 a1 FF 65 b4 0b
37 88 cc c4 a4 b6 fa 4a 63 03 93 89 bd 6a del e1 7e
64 9a 38 24 cc ef e2 a8 40 f5 a3 d6 f7 1a df 33
C.C. 9c 34 del a1 8e fa 45 79 1a 7c 29 05 87 8a CA 02
98 Cb 41 2e 7d fc c7 76 FE 51 d6 83 1d 03 b0 d7
Payload siguiente N: VID, reservado: 0x0, longitud: 24

EC 97 b8 67 eb f1 97 del fc c2 28 7f 8c 7d b3 1e 51
d5 e7 c2 f5

Payload siguiente VID: VID, reservado: 0x0, longitud: 23

El ASA envía el mensaje de respuesta para el intercambio IKE_SA_INIT. El intercambio IKE_SA_INIT es completo ahora. El ASA comienza el temporizador para el proceso de autenticación.

IKEv2-PLAT-4: [IKE_SA_INIT] ENVIADO *****

[10.0.0.1]:500->[192.168.1.1]:25170

Fecha: 04/23/2013

InitSPI=0x58aff71141ba436b

Hora: 16:25:02

RespSPI=0xfc696330e6b94d7f

Tipo: Información

MID=00000000 del PKT

Fuente: acvpngent

IKEv2-PROTO-5: (6): Trace-> SA SM:

I_SPI=58AFF71141BA436B

Descripción: Función:

R_SPI=FC696330E6B94D7F (r) MsgID =

CIPsecProtocol:: initiateTur

00000000 CurState: Evento INIT_DONE:

Archivo: . \ IPsecProtocol.cp

EV_DONE

Línea: 345

IKEv2-PROTO-3: (6): Se habilita la fragmentación

El túnel IPsec está iniciand

IKEv2-PROTO-3: (6): Se habilita Cisco

DeleteReason Notify

IKEv2-PROTO-3: (6): Intercambio completo del init SA

IKEv2-PROTO-5: (6): Trace-> SA SM:

I_SPI=58AFF71141BA436B

R_SPI=FC696330E6B94D7F (r) MsgID =

00000000 CurState: Evento INIT_DONE:

EV_CHK4_ROLE

IKEv2-PROTO-5: (6): Trace-> SA SM:

I_SPI=58AFF71141BA436B

R_SPI=FC696330E6B94D7F (r) MsgID =

00000000 CurState: Evento INIT_DONE:

EV_START_TMR

IKEv2-PROTO-3: (6): Comenzando el temporizador para esperar mensaje auth (sec 30)

IKEv2-PROTO-5: (6): Trace-> SA SM:

I_SPI=58AFF71141BA436B

R_SPI=FC696330E6B94D7F (r) MsgID =

00000000 CurState: Evento R_WAIT_AUTH:

EV_NO_EVENT

-----IKE_SA_INIT completan-----

-----IKE_AUTH comienza-----

Fecha: 04/23/2013

Hora: 16:25:00

Tipo: Información

Fuente: acvpngent

Descripción: Asegure los parámetros de gateway:
Dirección IP: 10.0.0.1
Puerto: 443
URL: el "10.0.0.1"
Método del auth: IKE - EAP-AnyConnect
Identidad IKE:

Fecha: 04/23/2013
Hora: 16:25:00
Tipo: Información
Fuente: acvpnagent

Descripción: **Iniciación de la conexión del Cliente de movilidad Cisco AnyConnect Secure, versión 3.0.1047**

Fecha: 04/23/2013
Hora: 16:25:02
Tipo: Información
Fuente: acvpnagent

Descripción: Función: ikev2_log
Archivo: .\ikev2_anyconnect_osal.cpp
Línea: 2730

Petición recibida de establecer un túnel IPsec; selector = intervalo de direcciones del tráfico local: 0.0.0.0-255.255.255.255 Protocolo: 0 rangos de puertos: 65535; selector remoto = intervalo de direcciones del tráfico: 0.0.0.0-255.255.255.255 Protocolo: 0 rangos de puertos: 0-65535

Fecha: 04/23/2013
Hora: 16:25:02
Tipo: Información
Fuente: acvpnagent

Descripción: Función: CIPsecProtocol:: connectTransport
Archivo: . \ IPsecProtocol.cpp
Línea: 1629

Socket abierto IKE a partir de la 192.168.1.1:25171 a 10.0.0.1:4500

La autenticación se hace con el EAP. Solamente un solo método de autenticación EAP se permite dentro de una conversación EAP. El ASA recibe el mensaje IKE_AUTH del cliente. Cuando el cliente incluye un payload IDI pero no un payload AUTH, esto indica el cliente ha declarado una identidad pero la tiene no probado le. En los debugs, el AUTH

IKEv2-PLAT-4: **[IKE_AUTH]** [192.168.1.1]:25171->[10.0.0.1] DEL PKT RE 4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000001

IKEv2-PROTO-3: **Rx** [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f

IKEv2-PROTO-3: **HDR[i:58AFF71141BA436B** - r: FC696330E6B94D7F]

IKEv2-PROTO-4: **Ispi IKEV2 HDR: 58AFF71141BA436B - rspi: FC696330E6B94D7F**

IKEv2-PROTO-4: Payload siguiente: ENCR, **versión: 2.0**

IKEv2-PROTO-4: Tipo del intercambio: IKE_AUTH, **indicadores: INICIADO**

IKEv2-PROTO-4: ID del mensaje: 0x1, longitud: 540

IKEv2-PROTO-5: (6): La petición tiene mess_id 1; 1 previsto a 1

Paquete descifrado REAL: Datos: 465 bytes

el payload no está presente en el IKE_AUTH paquete enviado por el cliente. El cliente envía el payload AUTH sólo después del

El intercambio EAP es acertado. Si el ASA está dispuesto a utilizar un extensible método de autenticación, coloca un EAP el payload en el mensaje 4 y difiere el envío SAr2, TSi, y TSr hasta el iniciador la autenticación es completa en a intercambio subsiguiente IKE_AUTH.

El paquete del iniciador IKE_AUTH contiene:

1. **Encabezado ISAKMP** - SPI/version/flags.
2. **IDI** - El nombre de grupo de túnel eso los deseos del cliente a conectar con puede ser entregado por la IDI payload del tipo ID_KEY_ID adentro el mensaje inicial del Intercambio IKE_AUTH. Esto ocurre cuando es el profile* del cliente preconfigurado con un nombre del grupo o, después de un acertado anterior la autenticación, el cliente tiene ocultó el nombre del grupo en su archivo de las preferencias. El ASA tentativas de hacer juego a un grupo de túnel nombre con el contenido

IKEv2-PROTO-5: Analice el payload específico del vendedor: (ADUANA) payload siguiente VID: IDI, reservada: 0x0, longitud: 20

58 af f6 11 52 8d b0 2c b8 DA 30 46 sean 91 56 fa
Payload siguiente **IDI**: CERTREQ, reservado: 0x0, longitud: 28
Tipo identificación: Nombre del grupo, reservado: 0x0 0x0

2a 24 41 6e 79 43 6f 6e 6e 65 63 74 43 6c 69 65
6e 74 24 2a
Payload siguiente **CERTREQ**: CFG, reservado: 0x0, longitud: 25
CERT que codifica el certificado X.509 - firma
Data&colon de CertReq; 20 bytes

Payload siguiente **CFG**: SA, reservado: 0x0, longitud: 196
tipo del cfg: **CFG_REQUEST**, reservado: 0x0, reservado: 0x0

tipo del attrib: direccionamiento interno IP4, longitud: 0

tipo del attrib: netmask interno IP4, longitud: 0

tipo del attrib: IP4 interno DNS, longitud: 0

tipo del attrib: IP4 interno NBNS, longitud: 0

tipo del attrib: vencimiento de la dirección interna, longitud: 0

tipo del attrib: versión de aplicación, longitud: 27

41 6e 79 43 6f 6e 6e 65 63 74 20 57 69 6e 64 6f
77 73 20 33 2e 30 2e 31 30 34 37
tipo del attrib: direccionamiento interno IP6, longitud: 0

tipo del attrib: subred interna IP4, longitud: 0

tipo del attrib: Desconocido - 28682, longitud: 15

77 69 6e 78 70 36 34 74 65 6d 70 6c 61 74 65
tipo del attrib: Desconocido - 28704, longitud: 0

tipo del attrib: Desconocido - 28705, longitud: 0

tipo del attrib: Desconocido - 28706, longitud: 0

tipo del attrib: Desconocido - 28707, longitud: 0

tipo del attrib: Desconocido - 28708, longitud: 0

tipo del attrib: Desconocido - 28709, longitud: 0

tipo del attrib: Desconocido - 28710, longitud: 0

tipo del attrib: Desconocido - 28672, longitud: 0

tipo del attrib: Desconocido - 28684, longitud: 0

del IKE	tipo del attrib: Desconocido - 28711, longitud: 2
Payload IDI. Después	
del primer	05 7e
el IPsec VPN acertado	tipo del attrib: Desconocido - 28674, longitud: 0
es	
establecido, los cachés	tipo del attrib: Desconocido - 28712, longitud: 0
del cliente	
nombre del grupo (grupo	tipo del attrib: Desconocido - 28675, longitud: 0
alias) al cual	
el usuario autenticado.	tipo del attrib: Desconocido - 28679, longitud: 0
Este grupo	
el nombre se entrega en	tipo del attrib: Desconocido - 28683, longitud: 0
la IDI	tipo del attrib: Desconocido - 28717, longitud: 0
payload de la conexión	
siguiente	tipo del attrib: Desconocido - 28718, longitud: 0
tentativa para indicar	
grupo probable deseado	tipo del attrib: Desconocido - 28719, longitud: 0
por	
usuario. Cuando es la	tipo del attrib: Desconocido - 28720, longitud: 0
autenticación EAP	
especificado o implicado	tipo del attrib: Desconocido - 28721, longitud: 0
por el cliente	
el perfil y el perfil no	tipo del attrib: Desconocido - 28722, longitud: 0
hace	
contenga el	tipo del attrib: Desconocido - 28723, longitud: 0
<IKEIdentity>	tipo del attrib: Desconocido - 28724, longitud: 0
el elemento, el cliente	
envía	tipo del attrib: Desconocido - 28725, longitud: 0
Payload IDI del tipo	
ID_GROUP	tipo del attrib: Desconocido - 28726, longitud: 0
con la cadena fija	
\$AnyConnectClient\$.	tipo del attrib: Desconocido - 28727, longitud: 0
3. CERTREQ - El cliente es	tipo del attrib: Desconocido - 28729, longitud: 0
petición del ASA para a	
certificado preferido.	Payload siguiente SA : TSi, reservado: 0x0, longitud: 124
Certificado	IKEv2-PROTO-4: la oferta más reciente: 0x0, reservado: 0x0, longitud: 12
las cargas útiles de la	Oferta: 1, ID del protocolo: ESP, tamaño de SPI: 4, #trans: 12
petición pueden ser	IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 12
incluidas	tipo: 1, reservado: 0x0, identificación: AES-CBC
en un intercambio	IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 12
cuando el remitente	tipo: 1, reservado: 0x0, identificación: AES-CBC
necesita conseguir el	IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 12
certificado de	tipo: 1, reservado: 0x0, identificación: AES-CBC
receptor. El pedido de	IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
certificado	tipo: 1, reservado: 0x0, identificación: 3DES
el payload se procesa	IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
por	tipo: 1, reservado: 0x0, identificación: DES
	IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
	tipo: 1, reservado: 0x0, identificación: NULO

examen de la "codificación CERT" campo para determinar si el procesador tiene ningunos Certificados de este tipo. Si es así El campo de las "autoridades de certificación" es examinado para determinar si el procesador tiene cualquier Certificados eso se puede validar hasta uno de la certificación especificada autoridades. Esto puede ser un encadenamiento de Certificados.

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
 tipo: 3, reservado: 0x0, identificación: SHA512
 IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
 tipo: 3, reservado: 0x0, identificación: SHA384
 IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
 tipo: 3, reservado: 0x0, identificación: SHA256
 IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
 tipo: 3, reservado: 0x0, identificación: SHA96
 IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8
 tipo: 3, reservado: 0x0, identificación: MD596
 IKEv2-PROTO-4: el último transforma: 0x0, reservado: 0x0: longitud: 8
 tipo: 5, reservado: 0x0, identificación:

Payload siguiente de **TSi**: TSr, reservado: 0x0, longitud: 24
 Numérico de los TS: 1, 0x0 reservado, 0x0 reservado
 Tipo TS: TS_IPV4_ADDR_RANGE, identificación proto: 0, longitud: 16
 puerto del comienzo: 0, puerto del extremo: 65535
 addr del comienzo: 0.0.0.0, addr del final: 255.255.255.255
 Payload siguiente de **TSr**: NOTIFIQUE, reservó: 0x0, longitud: 24
 Numérico de los TS: 1, 0x0 reservado, 0x0 reservado
 Tipo TS: TS_IPV4_ADDR_RANGE, identificación proto: 0, longitud: 16
 puerto del comienzo: 0, puerto del extremo: 65535
 addr del comienzo: 0.0.0.0, addr del final: 255.255.255.255

4. **CFG** - CFG_REQUEST/CFG_REPLY permite un IKE punto final para pedir la información de su par. Si un atributo en Configuración CFG_REQUEST el payload no es cero-longitud, él es tomado como sugerencia para eso atributo. El CFG_REPLY el payload de la configuración puede volver ese valor o un nuevo. Puede también agregue los nuevos atributos y no incluya alguno pidió unos. Los solicitantes ignoran vuelto

atributos que no lo hacen reconocen. En estos debugs, el cliente está pidiendo el túnel configuración en CFG_REQUEST. El ASA las contestaciones a esto y envían el túnel atributos de la configuración sólo después de el intercambio EAP es acertado.

5. **SAi2** - SAi2 inicia el SA, cuál es similar a la fase 2 transforme el intercambio del conjunto en IKEv1.
6. **TSi** y **TSr** - El iniciador y selectores del tráfico del respondedor contenga, respectivamente, la fuente y dirección destino del iniciador y respondedor para remita y reciba cifrado tráfico. El intervalo de direcciones especifica que todo el tráfico a y desde ese rango es tunneled. Si la oferta es aceptable por respondedor, envía el TS idéntico las cargas útiles apoyan.

Los atributos que el cliente debe entregar para la autenticación del grupo se salva en Archivo de perfil de AnyConnect.

Configuración del perfil

***Relevant:**

```
<ServerList>
<HostEntry>
  <HostName>Anu-IKEV2
</HostName>
  <HostAddress>10.0.0.1
</HostAddress>
  <UserGroup>ASA-IKEV2
</UserGroup>
<PrimaryProtocol>IPsec
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

El ASA genera una respuesta al mensaje IKE_AUTH y se prepara para autenticarse al cliente.

Paquete descifrado: Data: 540 bytes

```
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_WAIT_AUTH: EV_RECV_AUTH
IKEv2-PROTO-3: (6): Parando el temporizador para esperar mensaje aut
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_WAIT_AUTH: EV_CHK_NAT_T
IKEv2-PROTO-3: (6): Detección del control NAT
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_WAIT_AUTH: EV_CHG_NAT_T_PORT
IKEv2-PROTO-2: (6): Flotador detectado NAT al puerto 25171 del init, pu
4500 del resp
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_WAIT_AUTH: EV_PROC_ID
IKEv2-PROTO-2: (6): Parámetros válidos recibidos en el identificador de
proceso
IKEv2-PLAT-3: (6) método del auth del par fijado a: 0
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_WAIT_AUTH:
EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SE
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_WAIT_AUTH: EV_GET_POLICY_BY_PEERID
IKEv2-PROTO-3: (6): Conseguir las directivas configuradas
IKEv2-PLAT-3: Nueva conexión cliente de AnyConnect detectada basada
payload ID
IKEv2-PLAT-3: my_auth_method = 1
IKEv2-PLAT-3: (6) método del auth del par fijado a: 256
IKEv2-PLAT-3: supported_peers_auth_method = 16
IKEv2-PLAT-3: (6) tp_name fijado a: Anu-ikev2
IKEv2-PLAT-3: punta de la confianza fijada a: Anu-ikev2
IKEv2-PLAT-3: P1 ID= 0
IKEv2-PLAT-3: Traducir IKE_ID_AUTO a = 9
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_WAIT_AUTH: EV_SET_POLICY
IKEv2-PROTO-3: (6): Determinación de las directivas configuradas
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
```

R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_WAIT_AUTH: EV_VERIFY_POLICY_BY_PEERID
IKEv2-PROTO-3: (6): Verifique la directiva del par
IKEv2-PROTO-3: (6): **Certificado que corresponde con encontrado**
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_WAIT_AUTH: EV_CHK_CONFIG_MODE
IKEv2-PROTO-3: (6): Datos válidos recibidos del modo de configuración
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_WAIT_AUTH: EV_SET_RECDD_CONFIG_MODE
IKEv2-PLAT-3: (6) el nombre de host del DHCP para el DDNS se fija a:
winxp64template
IKEv2-PROTO-3: (6): Fije los datos recibidos del modo de configuración
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_WAIT_AUTH: EV_CHK_AUTH4EAP
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_WAIT_AUTH: EV_CHK_EAP
IKEv2-PROTO-3: (6): **Comprobación para el intercambio EAP**
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_BLD_AUTH: EV_GEN_AUTH
IKEv2-PROTO-3: (6): **Genere mis datos de autenticación**
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_BLD_AUTH: EV_CHK4_SIGN
IKEv2-PROTO-3: (6): Consiga mi método de autenticación
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_BLD_AUTH: EV_SIGN
IKEv2-PROTO-3: (6): **Datos del auth de la muestra**
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_BLD_AUTH: EV_OK_AUTH_GEN
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_BLD_EAP_AUTH_REQ: EV_AUTHEN_REQ
IKEv2-PROTO-2: (6): **Pedir el authenticator para enviar la petición EAP**
Valor creado del config-auth del nombre de elemento
Vpn agregado del valor del cliente del nombre del atributo al config-auth del
elemento
Valor agregado del tipo del nombre del atributo hola al config-auth del ele
Valor creado 9.0(2)8 de la versión del nombre de elemento
Valor agregado 9.0(2)8 de la versión del nombre de elemento al config-auth
elemento
Nombre agregado del atributo que valora al sg a la versión del elemento
Mensaje generado XML abajo
¿<? xml el version="1.0" encoding="UTF-8"?>
type= " del " vpn del client=" del <config-auth hola " >
<version who="sg">9.0(2)8</version>
</config-auth>

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_BLD_EAP_AUTH_REQ: EV_RECV_EAP_AUTH
IKEv2-PROTO-5: (6): Acción: Action_Null
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_BLD_EAP_AUTH_REQ: EV_CHK_REDIRECT
IKEv2-PROTO-3: (6): Reoriente el control con la plataforma para el balanceo de carga
IKEv2-PLAT-3: Reoriente el control en la plataforma
IKEv2-PLAT-3: ikev2_osal_redirect: Sesión validada por 10.0.0.1
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000001 CurState: Evento
R_BLD_EAP_AUTH_REQ: EV_SEND_EAP_AUTH_REQ
IKEv2-PROTO-2: (6): **Envío de la petición EAP**
IKEv2-PROTO-5: Payload específico del vendedor de la construcción: CISCO
GRANITEIKEv2-PROTO-3: (6): Estructura
Payload siguiente **IDR**: CERT, reservado: 0x0, longitud: 36
Tipo identificación: ASN1 DN DER, reservado: 0x0 0x0
30 1a 31 18 30 16 06 09 2a 86 48 86 f7 0d 01 09
02 16 09 41 53 41 2.0s 49 4b 45 56 32
Payload siguiente **CERT**: CERT, reservado: 0x0, longitud: 436
CERT que codifica el certificado X.509 - firma
Data&colon CERT; 431 bytes
Payload siguiente CERT: AUTH, reservado: 0x0, longitud: 436
CERT que codifica el certificado X.509 - firma
Data&colon CERT; 431 bytes
Payload siguiente **AUTH**: EAP, reservado: 0x0, longitud: 136
Método RSA del auth, reservado: 0x0, 0x0 reservado
Data&colon del auth; bytes 128
Payload siguiente **EAP**: NINGUNOS, reservado: 0x0, longitud: 154
Código de petición: **identificación**: 1, **longitud**: 150
Tipo: Desconocido - 254
Datos EAP: 145 bytes
IKEv2-PROTO-3: Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f
IKEv2-PROTO-3: **HDR[i:58AFF71141BA436B** - r: FC696330E6B94D7F]
IKEv2-PROTO-4: **Ispi IKEV2 HDR: 58AFF71141BA436B** - **rspi:**
FC696330E6B94D7F
IKEv2-PROTO-4: Payload siguiente: ENCR, versión: 2.0
IKEv2-PROTO-4: Tipo del intercambio: IKE_AUTH, **indicadores:**
RESPONDEDOR MSG-RESPONSE
IKEv2-PROTO-4: ID del mensaje: 0x1, longitud: 1292
Payload siguiente ENCR: VID, reservado: 0x0, longitud: 1264
Data&colon cifrado; 1260 bytes

El ASA envía el payload AUTH para pedir los credenciales de usuario del cliente. El ASA envía el método AUTH como el "RSA," así que él envía su propio certificado al cliente, así que el cliente puede autenticar el servidor ASA. Puesto que el ASA está dispuesto a utilizar un método de autenticación ampliable, coloca un payload EAP en el mensaje 4 y difiere el envío de SA_r2, de TS_i, y de TS_r hasta que la autenticación del iniciador sea completa en un intercambio subsiguiente IKE_AUTH. Así, esas tres cargas útiles no están presentes en los debugs. Los paquetes EAP contienen:

1. **Código: petición** - Este código es enviado por el authenticator al par.
2. **identificación: 1** - Las ayudas identificación hacen juego las respuestas EAP con las peticiones. Aquí el valor es 1, que indica que es el primer paquete en el intercambio EAP. Esta petición EAP tiene el

“config-auth” tipo de “hola;” se envía del ASA al cliente para iniciar el intercambio EAP.

3. **Longitud: 150** - La longitud de los paquetes EAP incluye el código, la identificación, la longitud, y los datos EAP.

4. **Datos EAP.**

La fragmentación puede resultar si los Certificados son grandes o si las Cadenas de certificados son incluidas. Las cargas útiles del iniciador y del respondedor KE pueden también incluir las claves grandes, que pueden también contribuir a la fragmentación.

```
IKEv2-PROTO-5: (6): Hacer fragmentos del paquete, fragmento MTU: 54
número de fragmentos: 3, fragmento ID: 1
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT
```

Fecha: 04/23/2013
Hora: 16:25:02
Tipo: Información
Fuente: acvpnagent

Descripción: Función: ikev2_verify_X509_SIG_certs
Archivo: .\ikev2_anyconnect_osal.cpp
Línea: 2077

Petición de la aceptación del certificado del usuario

Fecha: 04/23/2013
Hora: 16:25:02
Tipo: Error
Fuente: acvpnui

Descripción: Función: CCapiCertificate:: verifyChainPolicy
Archivo: . \ Certificados \ CapiCertificate.cpp
Línea: 2032

Función invocada: CertVerifyCertificateChainPolicy
Código de retorno: -2146762487 (0x800B0109)

Descripción: Una Cadena de certificados procesada, pero terminada en un certificado raíz que no es confiado en por el proveedor de la confianza.

Fecha: 04/23/2013
Hora: 16:25:04
Tipo: Información
Fuente: acvpnagent

Descripción: Función: CEAPMgr:: dataRequestCB
Archivo: . \ EAPMgr.cpp

Línea: 400

Tipo propuesto EAP: EAP-ANYCONNECT

El cliente responde a la petición EAP con una respuesta.

Los paquetes EAP contienen:

1. **Código: respuesta** - Este código es enviado por el par al authenticator en respuesta a la petición EAP.

2. **identificación: 1** - Las ayudas identificación hacen juego las respuestas EAP con las peticiones. Aquí el valor es 1, que indica que esto es una respuesta a la petición enviada previamente por el ASA (authenticator). Esta respuesta EAP tiene el tipo del "config-auth" de "init"; el cliente está inicializando el intercambio EAP y está esperando el ASA para generar el pedido de autenticación.

3. **Longitud: 252** - La longitud de los paquetes EAP incluye el código, la identificación, la longitud, y los datos EAP.

4. **Datos EAP.**

El ASA descripta esta respuesta, y el cliente dice que ha recibido el payload AUTH en el paquete anterior (con el certificado) y lo ha recibido el primer paquete de pedidos EAP del ASA. Esto es lo que contiene el paquete de respuesta EAP del "init".

Ésta es la segunda petición enviada por el ASA al cliente.

Los paquetes EAP contienen:

1. **Código: petición** - Este código es enviado por el

IKEv2-PLAT-4: [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4500
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000

PKT RECV

IKEv2-PROTO-3: Rx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f

IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]

IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi:
FC696330E6B94D7F

IKEv2-PROTO-4: Payload siguiente: ENCR, versión: 2.0

IKEv2-PROTO-4: Tipo del intercambio: IKE_AUTH, indicadores: INICIADO

IKEv2-PROTO-4: ID del mensaje: 0x2, longitud: 332

IKEv2-PROTO-5: (6): La petición tiene mess_id 2; 2 previstos a 2

Paquete descifrado REAL: Datos: bytes 256

Payload siguiente **EAP**: NINGUNOS, reservado: 0x0, longitud: 256

Código: respuesta: identificación: 1, longitud: 252

Tipo: Desconocido - 254

Bytes **EAP data:247**

Paquete descifrado: Data: 332 bytes

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B

R_SPI=FC696330E6B94D7F (r) MsgID = 00000002 CurState: Evento

R_WAIT_EAP_RESP: EV_RECV_AUTH

IKEv2-PROTO-3: (6): Parando el temporizador para esperar mensaje aut

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B

R_SPI=FC696330E6B94D7F (r) MsgID = 00000002 CurState: Evento

R_WAIT_EAP_RESP: EV_RECV_EAP_RESP

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B

R_SPI=FC696330E6B94D7F (r) MsgID = 00000002 CurState: Evento

R_PROC_EAP_RESP: EV_PROC_MSG

IKEv2-PROTO-2: (6): **Proceso de la respuesta EAP**

Mensaje recibido XML abajo del cliente

¿<? xml el version="1.0" encoding="UTF-8"?>

type= " init " del " vpn " del client= del <config-auth >

<device-id>win</device-id>

<version who="vpn">3.0.1047</version>

<group-select>ASA-IKEV2</group-select>

<group-access>ASA-IKEV2</group-access>

</config-auth>

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B

R_SPI=FC696330E6B94D7F (r) MsgID = 00000002 CurState: Evento

R_PROC_EAP_RESP: **EV_RECV_EAP_AUTH**

IKEv2-PROTO-5: (6): Acción: Action_Null

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B

R_SPI=FC696330E6B94D7F (r) MsgID = 00000002 CurState: Evento

R_BLD_EAP_REQ: **EV_RECV_EAP_REQ**

IKEv2-PROTO-2: (6): Envío de la petición EAP

Mensaje generado XML abajo

¿<? xml el version="1.0" encoding="UTF-8"?>

Fecha: 04/23/2013

Hora: 16:25:04

Tipo: Información

Fuente: acvpnu

<p>authenticator al par.</p> <p>2. Identificación: 2 - Las ayudas identificación hacen juego las respuestas EAP con las peticiones. Aquí el valor es 2, que indica que es el segundo paquete en el intercambio. Esta petición tiene el tipo del "config-auth" de "pedido de autenticación"; el ASA está pidiendo que el cliente envíe las credenciales de la autenticación de usuario.</p> <p>3. Longitud: 457 - La longitud de los paquetes EAP incluye el código, la identificación, la longitud, y los datos EAP.</p> <p>4. Datos EAP. Payload ENCR: Se descripta este payload, y su contenido se analiza como cargas útiles adicionales.</p>	<pre> type= " pedido de autenticación " del " vpn" del client= del <config-auth > <version who="sg">9.0(2)8</version> is-for= " sg " del <opaque > <tunnel-group>ASA-IKEV2</tunnel-group> <config-hash>1367268141499</config-hash> </opaque> <csport>443</csport> id= <authentic " tubería " > <form> nombre de usuario del label= " del " nombre de usuario del name=" del " texto" del type= del <input: "></input> contraseña del label= " de la " contraseña del name=" de la " contraseña" del type= del <input: "></input> </form> </authentic> </config-auth> IKEv2-PROTO-3: (6): Paquete constructivo para el cifrado; el contenido es: Payload siguiente EAP: NINGUNOS, reservado: 0x0, longitud: 461 Código petición: identificación: 2, longitud: 457 Tipo: Desconocido - 254 Datos EAP: 452 bytes IKEv2-PROTO-3: Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0]: 0x2 IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F] IKEv2-PROTO-4: lspi IKEV2 HDR: 58AFF71141BA436B - rspi: FC696330E6B94D7F IKEv2-PROTO-4: Payload siguiente: ENCR, versión: 2.0 IKEv2-PROTO-4: Tipo del intercambio: IKE_AUTH, indicadores: RESPONDEDOR MSG-RESPONSE IKEv2-PROTO-4: ID del mensaje: 0x2, longitud: 524 Payload siguiente ENCR: EAP, reservado: 0x0, longitud: 496 Data&colon cifrado; 492 bytes IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000002 del PKT IKEv2-PROTO-5: (6): Trace-> SA SM: </pre>	<p>Descripción: Función: SDIMgr:: ProcessPromptDa Archivo: . \ SDIMgr.cpp Línea: 281 El tipo de autenticación no *****</p> <p>Fecha: 04/23/2013 Hora: 16:25:07 Tipo: Información Fuente: acvpnu</p> <p>Descripción: Función: ConnectMgr:: userRespons Archivo: . \ ConnectMgr.cpp Línea: 985 Proceso de la respuesta de usuario. *****</p>
--	--	---

I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID =
00000002 CurState: Evento
R_BLD_EAP_REQ: EV_START_TMR
IKEv2-PROTO-3: (6): **Comenzando el
temporizador para esperar al usuario
mensaje auth** (sec 120)
IKEv2-PROTO-5: (6): Trace-> SA SM:
I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID =
00000002 CurState: Evento
R_WAIT_EAP_RESP: EV_NO_EVENT

El cliente envía otro mensaje del iniciador IKE_AUTH con el payload EAP.

Los paquetes EAP contienen:

1. **Código: respuesta** - Este código es enviado por el par al authenticator en respuesta a la petición EAP.

2. **identificación: 2** - Las ayudas identificación hacen juego las respuestas EAP con las peticiones. Aquí el valor es 2, que indica que esto es una respuesta a la petición enviada previamente por el ASA (authenticator).

3. **Longitud: 420** - La longitud de los paquetes EAP incluye el código, la identificación, la longitud, y los datos EAP.

4. **Datos EAP.**

El ASA procesa esta respuesta. El cliente había pedido que el usuario ingresa las credenciales. Esta respuesta EAP tiene el tipo del "config-auth" de "auténtico-contestación." Este paquete contiene las credenciales ingresadas por el usuario.

IKEv2-PLAT-4: [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4500
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT RECV
IKEv2-PROTO-3: Rx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi:
FC696330E6B94D7F
IKEv2-PROTO-4: Payload siguiente: ENCR, versión: 2.0
IKEv2-PROTO-4: **Tipo del intercambio: IKE_AUTH, indicadores: INICIADO**
IKEv2-PROTO-4: ID del mensaje: 0x3, longitud: 492
IKEv2-PROTO-5: (6): La petición tiene mess_id 3; 3 previstos a 3

Paquete descifrado REAL: Datos: 424 bytes
Payload siguiente **EAP: NINGUNOS**, reservado: 0x0, longitud: 424
Código: respuesta: identificación: 2, longitud: 420
Tipo: Desconocido - 254
Datos EAP: 415 bytes

Paquete descifrado: Datos: 492 bytes
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000003 CurState: Evento
R_WAIT_EAP_RESP: EV_RECV_AUTH
IKEv2-PROTO-3: (6): Parando el temporizador para esperar mensaje aut
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000003 CurState: Evento
R_WAIT_EAP_RESP: EV_RECV_EAP_RESP
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000003 CurState: Evento
R_PROC_EAP_RESP: EV_PROC_MSG
IKEv2-PROTO-2: (6): **Proceso de la respuesta EAP**
Mensaje recibido XML abajo del cliente
¿<? xml el version="1.0" encoding="UTF-8"?>

```

type= " auténtico-contestación " del " vpn" del client= del <config-auth >
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
<session-token></session-token>
<session-id></session-id>
is-for= " sg " del <opaque >
<tunnel-group>ASA-IKEV2</tunnel-group>
<config-hash>1367268141499</config-hash></opaque>
<authentic>
<password>cisco123</password>
<username>Anu</username></authentic>
</config-auth>

```

```

IKEv2-PLAT-1: EAP: Autenticación de usuario iniciada
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000003 CurState: Evento
R_PROC_EAP_RESP: EV_NO_EVENT

```

```

IKEv2-PLAT-5: EAP: En el servicio repetido AAA
Publicación extraída CERT del servidor:
DACE1C274785F28BA11D64453096BAE294A3172E

```

```

IKEv2-PLAT-5: EAP: éxito en el servicio repetido AAA
IKEv2-PROTO-3: Respuesta recibida del authenticator
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000003 CurState: Evento
R_PROC_EAP_RESP: EV_RECV_EAP_AUTH

```

```

IKEv2-PROTO-5: (6): Acción: Action_Null
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000003 CurState: Evento
R_BLD_EAP_REQ: EV_RECV_EAP_REQ

```

```

IKEv2-PROTO-2: (6): Envío de la petición EAP

```

Mensaje generado XML abajo

```

¿<? xml el version="1.0" encoding="UTF-8"?>
el type= " del " vpn del client=" del <config-auth completa " >
<version who="sg">9.0(2)8</version>
<session-id>32768</session-id>
<session-token>18wA0TtGmDxPKPQCJywC7fB7EWLCEgz-
ZtjYpAyXx2yJH0H3G3H8t5xpBOx3lxag</session-token>
id= <authentic " éxito " >
<message el id="0" el param1="" param2=""></message>
</authentic>

```

```

IKEv2-PROTO-3: (6): Paquete constructivo para el cifrado; el contenido e
Payload siguiente EAP: NINGUNOS, reservado: 0x0, longitud: 4239

```

Código: petición: identificación: 3, longitud: 4235

Tipo: Desconocido - 254

Datos EAP: 4230 bytes

```

IKEv2-PROTO-3: Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f

```

```

IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]

```

```

IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi:
FC696330E6B94D7F

```

```

IKEv2-PROTO-4: Payload siguiente: ENCR, versión: 2.0

```

```

IKEv2-PROTO-4: Tipo del intercambio: IKE_AUTH, indicadores:

```

RESPONDEDOR MSG-RESPONSE

El ASA construye una tercera petición EAP en el intercambio.

Los paquetes EAP contienen:

1. **Código: petición** - Este código es enviado por el authenticator al par.
2. **identificación: 3** - Las ayudas identificación hacen juego las respuestas EAP con las peticiones. Aquí el valor es 3, que indica que es el tercer paquete en el intercambio. Este paquete tiene el tipo del "config-auth" de "completar"; el ASA ha recibido una contestación, y el intercambio EAP es completo.
3. **Longitud: 4235** - La longitud de los paquetes EAP incluye el código, la identificación, la longitud,

y los datos EAP.

4. Datos EAP.

Payload **ENCR**:

Se desencripta este payload, y su contenido se analiza como cargas útiles adicionales.

IKEv2-PROTO-4: ID del mensaje: 0x3, longitud: 4300

Payload siguiente **ENCR**: EAP, reservado: 0x0, longitud: 4272

Bytes cifrados data:4268

IKEv2-PROTO-5: (6): Hacer fragmentos del paquete, fragmento MTU: 54
número de fragmentos: 9, fragmento ID: 2

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000003 CurState: Evento
R_BLD_EAP_REQ: EV_START_TMR

IKEv2-PROTO-3: (6): Comenzando el temporizador para esperar al usuario
mensaje auth (sec 120)

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000003 CurState: Evento
R_WAIT_EAP_RESP: EV_NO_EVENT

Fecha: 04/23/2013

Hora: 16:25:07

Tipo: Información

Fuente: acvpnagent

Descripción: **Perfil actual: Anyconnect-ikev2.xml**

Ajustes de la configuración recibidos de la sesión de VPN:

Mantenga instalado: habilitado

Configuración de representación: no se modifique

Servidor proxy: ninguno

Proxy PAC URL: ninguno

Excepciones del proxy: ninguno

Lockdown del proxy: habilitado
La fractura excluye: se inhabilita la preferencia del acceso del LAN local
La fractura incluye: inhabilitado
DNS Dividido: inhabilitado
Comodín del LAN local: se inhabilita la preferencia del acceso del LAN local
Reglas de firewall: ninguno
Dirección cliente: 10.2.2.1
Máscara del cliente: 255.0.0.0
Direccionamiento del IPv6 del cliente: desconocido
Máscara del IPv6 del cliente: desconocido
MTU: 1406
Señal de mantenimiento IKE: 20 segundos
IKE DPD: 30 segundos
Tiempo de espera de la sesión: segundos 0
Descanso de la desconexión: 1800 segundos
Tiempo de inactividad: 1800 segundos
Servidor: desconocido
Host MUS: desconocido
Mensaje del usuario DAP: ninguno
Estado de la cuarentena: inhabilitado
Siempre en el VPN: no discapacitado
Tiempo de validez: segundos 0
Default Domain: desconocido
Home Page: desconocido
Desconexión del retiro de la placa inteligente: habilitado
Respuesta de la licencia: desconocido

El cliente envía el paquete del iniciador con el payload EAP.

Los paquetes EAP contienen:

1. **Código: respuesta** - Este código es enviado por el par al authenticator en respuesta a la petición EAP.

2. **Identificación: 3** - Las ayudas identificación hacen juego las respuestas EAP con las peticiones. Aquí el valor es 3, que indica que esto es una respuesta a la petición enviada previamente por el ASA (authenticator). El ASA ahora recibe el paquete de respuesta del cliente, que tiene el tipo del "config-auth" de "ack"; esta respuesta reconoce el mensaje "completo"

IKEv2-PLAT-4: [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4500
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000

PKT RECV

IKEv2-PROTO-3: Rx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f

IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]

IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi:
FC696330E6B94D7F

IKEv2-PROTO-4: Payload siguiente: ENCR, versión: 2.0

IKEv2-PROTO-4: **Tipo del intercambio: IKE_AUTH, indicadores: INICIADO**

IKEv2-PROTO-4: ID del mensaje: 0x4, longitud: 252

IKEv2-PROTO-5: (6): La petición tiene mess_id 4; 4 previstos a 4

Paquete descifrado REAL: Datos: 177 bytes

Payload siguiente **EAP: NINGUNOS**, reservado: 0x0, longitud: 177

Código: respuesta: identificación: 3, longitud: 173

Tipo: Desconocido - 254

Datos EAP: 168 bytes

EAP enviado
previamente por el ASA.

3. **Longitud: 173** - La longitud de los paquetes EAP incluye el código, la identificación, la longitud, y los datos EAP.

4. **Datos EAP.**

El ASA procesa este paquete. El intercambio EAP es acertado. El ASA se prepara para enviar al grupo de túnel configuración en el próximo paquete, que fue pedido previamente por el cliente adentro el payload IDI. El ASA recibe paquete de respuesta del cliente, que tiene el tipo del "config-auth" de "ack". Esto la respuesta reconoce el EAP "complete" el mensaje que fue enviado por ASA previamente.

Configuración pertinente:

```
<ServerList>  
<HostEntry>  
  <HostName>Anu-IKEV2  
</HostName>  
  <HostAddress>10.0.0.1  
</HostAddress>  
  <UserGroup>ASA-IKEV2  
</UserGroup>  
<PrimaryProtocol>IPsec  
</PrimaryProtocol>  
</HostEntry>  
</ServerList>
```

El intercambio EAP es acertado ahora.

Los paquetes EAP contienen:

1. **Código: éxito** - Este código es enviado por el authenticator al par tras completar un EAP método de autenticación. Esto indica que el par tiene autenticado con éxito al

Bytes desencriptados packet:Data:252

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000004 CurState: Evento
R_WAIT_EAP_RESP: EV_RECV_AUTH

IKEv2-PROTO-3: (6): Parando el temporizador para esperar mensaje aut

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000004 CurState: Evento
R_WAIT_EAP_RESP: EV_RECV_EAP_RESP

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000004 CurState: Evento
R_PROC_EAP_RESP: EV_PROC_MSG

IKEv2-PROTO-2: (6): **Proceso de la respuesta EAP**

Mensaje recibido XML abajo del cliente

¿<? xml el version="1.0" encoding="UTF-8"?>

type= " ack " del " vpn" del client= del <config-auth >

<device-id>win</device-id>

<version who="vpn">3.0.1047</version>

</config-auth>

IKEv2-PLAT-3: (6) aggrAuthHdl fijado a 0x2000

IKEv2-PLAT-3: (6) **tg_name fijado a: ASA-IKEV2**

IKEv2-PLAT-3: (6) **tipo del grp del tunn fijado a: RA**

IKEv2-PLAT-1: **EAP: Autenticación acertada**

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000004 CurState: Evento
R_PROC_EAP_RESP: EV_RECV_EAP_SUCCESS

IKEv2-PROTO-2: (6): Envío del mensaje de estado EAP

IKEv2-PROTO-3: (6): Paquete constructivo para el cifrado; el contenido e
Payload siguiente **EAP: NINGUNOS**, reservado: 0x0, longitud: 8

Código: éxito: identificación: 3, longitud: 4

IKEv2-PROTO-3: Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f

IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]

IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi:
FC696330E6B94D7F

IKEv2-PROTO-4: Payload siguiente: ENCR, versión: 2.0

**IKEv2-PROTO-4: Tipo del intercambio: IKE_AUTH, indicadores:
RESPONDEDOR MSG-RESPONSE**

IKEv2-PROTO-4: ID del mensaje: 0x4, longitud: 76

Payload siguiente ENCR: EAP, reservado: 0x0, longitud: 48

Bytes cifrados data:44

IKEv2-PLAT-4: **[IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251**

InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000

authenticator.

2. **identificación: 3** - Las ayudas identificación hacen juego Respuestas EAP con las peticiones. Aquí el valor es 3, que indica que esto es una respuesta a la petición enviada previamente por ASA (authenticator). El tercer conjunto de los paquetes en el intercambio era acertado, y el intercambio EAP es acertado.

3. **Longitud: 4** - Longitud del EAP el paquete incluye el código, identificación, longitud, y datos EAP.

4. Datos EAP.

Puesto que el intercambio EAP es acertado, el cliente envía el paquete del iniciador IKE_AUTH con el payload AUTH. El payload AUTH se genera de la clave secreta compartida.

Cuando se especifica la autenticación EAP o implicado por el perfil del cliente y el perfil no contiene el elemento del <IKEIdentity>, el cliente envía un payload IDI del tipo ID_GROUP con

PKT

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000004 CurState: Evento R_PROC_EAP_RESP: EV_START_TMR

IKEv2-PROTO-3: (6): Comenzando el temporizador para esperar mensaje (sec 30)

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000004 CurState: Evento R_WAIT_EAP_AUTH_VERIFY: EV_NO_EVENT

IKEv2-PLAT-4: [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000 PKT RECV

IKEv2-PROTO-3: Rx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f

IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]

IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi: FC696330E6B94D7F

IKEv2-PROTO-4: Payload siguiente: ENCR, versión: 2.0

IKEv2-PROTO-4: Tipo del intercambio: IKE_AUTH, **indicadores: INICIADO**

IKEv2-PROTO-4: ID del mensaje: 0x5, longitud: 92

IKEv2-PROTO-5: (6): La petición tiene mess_id 5; 5 previstos a 5

Bytes desencriptados REALES packet:Data:28

Payload siguiente **AUTH**: NINGUNOS, reservado: 0x0, longitud: 28

PSK del método del auth, reservado: 0x0, 0x0 reservado

Datos del auth: 20 bytes

Paquete descifrado: Datos: 92 bytes

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento R_WAIT_EAP_AUTH_VERIFY: EV_RECV_AUTH

IKEv2-PROTO-3: (6): Parando el temporizador para esperar mensaje aut

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento R_VERIFY_AUTH: EV_GET_EAP_KEY

IKEv2-PROTO-2: (6): Envíe el AUTH, para verificar al par después de que

la cadena fija

\$AnyConnectClient\$.

El ASA procesa este mensaje.

Configuración pertinente:

```
<ServerList>
<HostEntry>
  <HostName>Anu-IKEV2
</HostName>
  <HostAddress>10.0.0.1
</HostAddress>
  <UserGroup>ASA-IKEV2
</UserGroup>
<PrimaryProtocol>IPsec
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

intercambio EAP

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
R_VERIFY_AUTH: EV_VERIFY_AUTH

IKEv2-PROTO-3: (6): **Verifique los datos de autenticación**

IKEv2-PROTO-3: (6): **Utilice la clave del preshared para la identificación**
***\$AnyConnectClient\$*, clave len 20**

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
R_VERIFY_AUTH: EV_GET_CONFIG_MODE

IKEv2-PLAT-3: Contestación del modo de configuración hecha cola

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
R_VERIFY_AUTH: EV_NO_EVENT

IKEv2-PLAT-3: PSH: client-os-version= de los client-os=Windows del
client=AnyConnect client-version=3.0.1047

IKEv2-PLAT-3: Contestación del modo de configuración completada

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
R_VERIFY_AUTH: EV_OK_GET_CONFIG

IKEv2-PROTO-3: (6): Tenga datos del modo de configuración a enviar

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
R_VERIFY_AUTH: EV_CHK4_IC

IKEv2-PROTO-3: (6): Proceso del contacto inicial

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
R_VERIFY_AUTH: EV_CHK_REDIRECT

IKEv2-PROTO-5: (6): Reoriente el control se hace ya para esta sesión,
saltándola

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
R_VERIFY_AUTH: EV_PROC_SA_TS

IKEv2-PROTO-2: (6): **Proceso mensaje auth**

IKEv2-PLAT-1: **Correspondencia de criptografía: Dynmap 1000 seq del m**
Selector ajustado usando IP asignada

IKEv2-PLAT-3: **Correspondencia de criptografía: coincidencia en el dynm**
1000 seq del mapa dinámico

IKEv2-PLAT-3: PFS inhabilitado para la conexión RA

IKEv2-PROTO-3: (6):

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
R_VERIFY_AUTH: EV_NO_EVENT

IKEv2-PLAT-2: Servicio repetido recibido PFKEY SPI para SPI 0x30B848
error FALSO

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
R_VERIFY_AUTH: EV_OK_REC'D_IPSEC_RESP

IKEv2-PROTO-2: (6): **Proceso mensaje auth**

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
R_BLD_AUTH: EV_MY_AUTH_METHOD

IKEv2-PROTO-3: (6): **Consiga mi método de autenticación**

El ASA construye el mensaje
de respuesta IKE_AUTH con
las cargas útiles SA, de TSi, y
de TSr.

El paquete del respondedor IKE_AUTH contiene:

1. **Encabezado ISAKMP** - SPI/version/flags.
2. **Payload AUTH** - Con el método de autenticación elegido.
3. **CFG** - CFG_REQUEST/CFG_REPLY permite que un punto final IKE pida la información de su par. Si un atributo en el payload de la configuración CFG_REQUEST no es cero-longitud, se toma como sugerencia para ese atributo. El payload de la configuración CFG_REPLY puede volver ese valor o un nuevo. Puede también agregar los nuevos atributos y no incluir alguno pidió unos. Los solicitantes ignoran los atributos vueltos que no reconocen. El ASA contesta al cliente con los atributos de la configuración del túnel en el paquete CFG_REPLY.
4. **SAr2** - SAr2 inicia el SA, que es similar a la fase 2 transforma el intercambio del conjunto en IKEv1.
5. **TSi y TSr** - Los selectores del tráfico del iniciador y del respondedor contienen, respectivamente, las direcciones de origen y de destino del iniciador y al respondedor para remitir y recibir el tráfico encriptado. El intervalo

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento R_BLD_AUTH: EV_GET_PRESHR_KEY
IKEv2-PROTO-3: (6): **Consiga la clave del preshared del par para *\$AnyConnectClient\$***
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento R_BLD_AUTH: EV_GEN_AUTH
IKEv2-PROTO-3: (6): **Genere mis datos de autenticación**
IKEv2-PROTO-3: (6): **Utilice la clave del preshared para la identificación hostname=ASA-IKEV2, clave len 20**
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento R_BLD_AUTH: EV_CHK4_SIGN
IKEv2-PROTO-3: (6): **Consiga mi método de autenticación**
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento R_BLD_AUTH: EV_OK_AUTH_GEN
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento R_BLD_EAP_AUTH_VERIFY: EV_GEN_AUTH
IKEv2-PROTO-3: (6): **Genere mis datos de autenticación**
IKEv2-PROTO-3: (6): **Utilice la clave del preshared para la identificación hostname=ASA-IKEV2, clave len 20**
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento R_BLD_EAP_AUTH_VERIFY: EV_SEND_AUTH
IKEv2-PROTO-2: (6): **Envíe el AUTH, para verificar al par después de que intercambio EAP**
IKEv2-PROTO-3: **Oferta ESP: 1, tamaño de SPI: 4 (IPSec Negotiation), Numérico. transforma: 3 AES-CBC SHA96**
IKEv2-PROTO-5: La construcción notifica el payload:
ESP_TFC_NO_SUPPORTIKEv2-PROTO-5: La construcción notifica el payload:
NON_FIRST_FRAGSIKEv2-PROTO-3: (6): Paquete constructivo para el contenido es:
Payload siguiente **AUTH**: CFG, reservado: 0x0, longitud: 28 **PSK del método del auth**, reservado: 0x0, 0x0 reservado Data&colon del auth; 20 bytes
Payload siguiente **CFG**: SA, reservado: 0x0, longitud: 4196 tipo del cfg: **CFG_REPLY**, reservado: 0x0, reservado: 0x0
tipo del attrib: direccionamiento interno IP4, longitud: 4
01 01 01 01
tipo del attrib: netmask interno IP4, longitud: 4
00 00 00 00
tipo del attrib: vencimiento de la dirección interna, longitud: 4
00 00 00 00
tipo del attrib: versión de aplicación, longitud: 16

de direcciones especifica	41 53 41 20 31 30 30 2e 37 28 36 29 31 31 36 00
que todo el tráfico a y	tipo del attrib: Desconocido - 28704, longitud: 4
desde ese rango es	00 00 00 00
tunneled. Si la oferta es	tipo del attrib: Desconocido - 28705, longitud: 4
aceptable por el	00 00 07 08
respondedor, devuelve	tipo del attrib: Desconocido - 28706, longitud: 4
las cargas útiles	00 00 07 08
idénticas TS.	tipo del attrib: Desconocido - 28707, longitud: 1
Payload ENCR :	01
Se descripta este payload,	tipo del attrib: Desconocido - 28709, longitud: 4
y su contenido se analiza	00 00 00 1e
como cargas útiles	tipo del attrib: Desconocido - 28710, longitud: 4
adicionales.	00 00 00 14
	tipo del attrib: Desconocido - 28684, longitud: 1
	01
	tipo del attrib: Desconocido - 28711, longitud: 2
	05 7e
	tipo del attrib: Desconocido - 28679, longitud: 1
	00
	tipo del attrib: Desconocido - 28683, longitud: 4
	80 0b 00 01
	tipo del attrib: Desconocido - 28725, longitud: 1
	00
	tipo del attrib: Desconocido - 28726, longitud: 1
	00
	tipo del attrib: Desconocido - 28727, longitud: 4056
	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31
	2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54
	46 2.os 38 22 3f 3e 3c 63 6f 6e 66 69 67 2.os 61 75
	74 68 20 63 6c 69 65 6e 74 3d 22 76 70 6e 22 20
	74 79 70 65 3d 22 63 6f 6d 70 6c 65 74 65 22 3e
	3c 76 65 72 73 69 6f 6e 20 77 68 6f 3d 22 73 67
	22 3e 31 30 30 2e 37 28 36 29 31 31 36 3c 2f 76
	65 72 73 69 6f 6e 3e 3c 73 65 73 73 69 6f 6e 2.o
	69 64 3e 38 31 39 32 3c 2f 73 65 73 73 69 6f 6e
	<snip>
	72 6f 66 69 6c 65 2.o 6d 61 6e 69 66 65 73 74 3e
	3c 2f 63 6f 6e 66 69 67 3e 3c 2f 63 6f 6e 66 69
	67 2.os 61 75 74 68 3e 00
	tipo del attrib: Desconocido - 28729, longitud: 1

00

Payload siguiente **SA**: TSi, reservado: 0x0, longitud: 44

IKEv2-PROTO-4: la oferta más reciente: 0x0, reservado: 0x0, longitud: 4

Oferta: 1, ID del protocolo: ESP, tamaño de SPI: 4, #trans: 3

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 12

tipo: 1, reservado: 0x0, identificación: AES-CBC

IKEv2-PROTO-4: el último transforma: 0x3, reservado: 0x0: longitud: 8

tipo: 3, reservado: 0x0, identificación: SHA96

IKEv2-PROTO-4: el último transforma: 0x0, reservado: 0x0: longitud: 8

tipo: 5, reservado: 0x0, identificación:

Payload siguiente de **TSi**: TSr, reservado: 0x0, longitud: 24

Numérico de los TS: 1, 0x0 reservado, 0x0 reservado

Tipo TS: TS_IPV4_ADDR_RANGE, identificación proto: 0, longitud: 16

puerto del comienzo: 0, puerto del extremo: 65535

addr del comienzo: 10.2.2.1, addr del final: 10.2.2.1

Payload siguiente de **TSr**: NOTIFIQUE, reservó: 0x0, longitud: 24

Numérico de los TS: 1, 0x0 reservado, 0x0 reservado

Tipo TS: TS_IPV4_ADDR_RANGE, identificación proto: 0, longitud: 16

puerto del comienzo: 0, puerto del extremo: 65535

addr del comienzo: 0.0.0.0, addr del final: 255.255.255.255

IKEv2-PROTO-3: Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f

IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]

IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi:

FC696330E6B94D7F

IKEv2-PROTO-4: Payload siguiente: ENCR, versión: 2.0

IKEv2-PROTO-4: **Tipo del intercambio: IKE_AUTH, indicadores:**

RESPONDEDOR MSG-RESPONSE

IKEv2-PROTO-4: ID del mensaje: 0x5, longitud: 4396

Payload siguiente **ENCR**: AUTH, reservado: 0x0, longitud: 4368

Data&colon cifrado; 4364 bytes

El ASA envía este mensaje de respuesta IKE_AUTH, que se hace fragmentos en nueve paquetes. El intercambio IKE_AUTH es completo.

IKEv2-PROTO-5: (6): Hacer fragmentos del paquete, fragmento MTU: 54

número de fragmentos: 9, fragmento ID: 3

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251

InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000

PKT

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251

InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000

PKT

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251

InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000

PKT

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251

InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000

PKT

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251

InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000

PKT

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251

InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000

PKT

IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251

InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PKT
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
AUTH_DONE: EV_OK
IKEv2-PROTO-5: (6): Acción: Action_Null
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
AUTH_DONE: EV_PKI_SESH_CLOSE

Fecha: 04/23/2013
Hora: 16:25:07
Tipo: Información
Fuente: acvpnagent

Descripción: Función: ikev2_log
Archivo: .\ikev2_anyconnect_osal.cpp
Línea: 2730
Conexión IPsec se ha establecido.

Fecha: 04/23/2013
Hora: 16:25:07
Tipo: Información
Fuente: acvpnagent

Descripción: Sesión IPsec registro:
Cifrado: AES-CBC
PRF: SHA1
HMAC: SHA96
Método local del auth: PSK
Método remoto del auth: PSK
Identificación de la secuencia: 0
Tamaño de clave: 192
Grupo DH: 1
Reintroduzca el tiempo: 4294967 segundos
Dirección local: 192.168.1.1
Dirección remota: 10.0.0.1
Puerto local: 4500
Puerto remoto: 4500
ID de sesión: 1

Fecha: 04/23/2013
Hora: 16:25:07
Tipo: Información
Fuente: acvpnui

Descripción: **El perfil configurado en el gateway seguro es: Anyconnect-**

ikev2.xml

Fecha: 04/23/2013
Hora: 16:25:07
Tipo: Información
Fuente: acvpnui

Descripción: Información del Tipo de mensaje enviada al usuario:
Estableciendo a la sesión de VPN...

-----Extremos del intercambio IKE_AUTHENTIC-----

Fecha: 04/23/2013
Hora: 16:25:07
Tipo: Información
Fuente: acvpndownloader

Descripción: Función: ProfileMgr:: loadProfiles
Archivo: . \ Api \ ProfileMgr.cpp
Línea: 148

Perfiles cargados:

Usuarios de C:\Documents and Settings\All \ datos de aplicación \ Cisco \
movilidad segura Client\Profile\anyconnect-ikev2.xml de Cisco AnyConne

Fecha: 04/23/2013
Hora: 16:25:07
Tipo: Información
Fuente: acvpndownloader

Descripción: Configuraciones de preferencias actuales:

ServiceDisable: falso
CertificateStoreOverride: falso
CertificateStore: Todos
ShowPreConnectMessage: falso
AutoConnectOnStart: falso
MinimizeOnConnect: verdad
LocalLanAccess: falso
AutoReconnect: verdad
AutoReconnectBehavior: DisconnectOnSuspend
UseStartBeforeLogon: falso
AutoUpdate: verdad
RSASeclIDIntegration: Automático
WindowsLogonEnforcement: SingleLocalLogon
WindowsVPNEstablishment: LocalUsersOnly
ProxySettings: Nativo
AllowLocalProxyConnections: verdad
PPPEXclusion: Inhabilitar
PPPEXclusionServerIP:
AutomaticVPNPolicy: falso
TrustedNetworkPolicy: Desconecte
UntrustedNetworkPolicy: Conecte

TrustedDNSDomains:
TrustedDNSServers:
AlwaysOn: falso
ConnectFailurePolicy: Cerrado
AllowCaptivePortalRemediation: falso
CaptivePortalRemediationTimeout: 5
ApplyLastVPNLocalResourceRules: falso
AllowVPNDisconnect: verdad
EnableScripting: falso
TerminateScriptOnNextEvent: falso
EnablePostSBLOnConnectScript: verdad
AutomaticCertSelection: verdad
RetainVpnOnLogoff: falso
UserEnforcement: SameUserOnly
EnableAutomaticServerSelection: falso
AutoServerSelectionImprovement: 20
AutoServerSelectionSuspendTime: 4
AuthenticationTimeout: 12
SafeWordSoftTokenIntegration: falso
AllowIPsecOverSSL: falso
ClearSmartcardPin: verdad

Fecha: 04/23/2013
Hora: 16:25:07
Tipo: Información
Fuente: acvpnu

Descripción: Información del Tipo de mensaje enviada al usuario:
Estableciendo el VPN - Sistema de examen...

Fecha: 04/23/2013
Hora: 16:25:07
Tipo: Información
Fuente: acvpnu

Descripción: Información del Tipo de mensaje enviada al usuario:
Estableciendo el VPN - Adaptador VPN que activa...

Fecha: 04/23/2013
Hora: 16:25:07
Tipo: Información
Fuente: acvpnagent

Descripción: Función: CVirtualAdapter:: DoRegistryRepair
Archivo: . \ WindowsVirtualAdapter.cpp
Línea: 1869
Tecla de control encontrada VA:
SYSTEM\CurrentControlSet\ENUM\ROOT\NET\0000\Control

Fecha: 04/23/2013
Hora: 16:25:07
Tipo: Información
Fuente: acvpnagent

Descripción: **Se ha detectado una nueva interfaz de la red.**

Fecha: 04/23/2013

Hora: 16:25:07

Tipo: Información

Fuente: acvpnagent

Descripción: Función: CRouteMgr:: logInterfaces

Archivo: . \ RouteMgr.cpp

Línea: 2076

Función invocada: logInterfaces

Código de retorno: 0 (0x00000000)

Descripción: **Lista de interfaz de la dirección IP:**

10.2.2.1

192.168.1.1

Fecha: 04/23/2013

Hora: 16:25:08

Tipo: Información

Fuente: acvpnagent

Descripción: Configuración del host:

Dirección pública: 192.168.1.1

Máscara pública: 255.255.255.0

Dirección privada: 10.2.2.1

Máscara privada: 255.0.0.0

Direccionamiento privado del IPv6: N/A

Máscara privada del IPv6: N/A

Peeres remotos: 10.0.0.1 (puerto TCP 443, puerto 500 UDP), 10.0.0.1 (puerto TCP 4500 UDP)

Redes privadas: ninguno

Redes públicas: ninguno

Modo de túnel: sí

La conexión se ingresa en la base de datos de la asociación de seguridad (SA), y SE REGISTRA el estatus. El ASA también realiza algunos controles como el stats común del indicador luminoso LED amarillo de la placa muestra gravedad menor del acceso (CAC), la presencia del duplicado SA, y los valores de conjuntos como el Dead Peer Detection (DPD) y así sucesivamente.

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento AUTH_DONE: **EV_INSERT_IKE**

IKEv2-PROTO-2: (6): **SA creado; inserción del SA en la base de datos**

IKEv2-PLAT-3:

ESTADO DE LA CONEXIÓN: ENCIMA... del par: 192.168.1.1:25171, pha

\$AnyConnectClient\$

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento AUTH_DONE: **EV_REGISTER_SESSION**

IKEv2-PLAT-3: (6) **nombre de usuario fijado a: Anu**

IKEv2-PLAT-3:

ESTADO DE LA CONEXIÓN: ... Par REGISTRADO: 192.168.1.1:25171, phase1_id: *\$AnyConnectClient\$*

IKEv2-PROTO-3: (6): DPD de inicialización, configurado por 10 segundos

IKEv2-PLAT-3: (6) mib_index fijado a: 4501

IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento

AUTH_DONE: EV_GEN_LOAD_IPSEC
IKEv2-PROTO-3: (6): Material de la carga clave IPsec
IKEv2-PLAT-3: Correspondencia de criptografía: coincidencia en el dymn
1000 seq del mapa dinámico
IKEv2-PLAT-3: (6) el tiempo máximo DPD será: 30
IKEv2-PLAT-3: (6) el tiempo máximo DPD será: 30
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
AUTH_DONE: EV_START_ACCT
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
AUTH_DONE: EV_CHECK_DUPE
IKEv2-PROTO-3: (6): **El marcar para saber si hay duplicado SA**
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento
AUTH_DONE: EV_CHK4_ROLE
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento LIS
EV_R_UPDATE_CAC_STATS
IKEv2-PLAT-5: Nueva petición ikev2 sa activada
IKEv2-PLAT-5: Cuenta del decremento para la negociación entrante
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento LIS
EV_R_OK
IKEv2-PROTO-3: (6): Comenzar el temporizador para borrar el contexto c
negociación
IKEv2-PROTO-5: (6): Trace-> SA SM: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) MsgID = 00000005 CurState: Evento LIS
EV_NO_EVENT
IKEv2-PLAT-2: PFKEY recibidos agregan el SA para SPI 0x77EE5348, e
FALSO
IKEv2-PLAT-2: Actualización recibida SA PFKEY para SPI 0x30B848A4,
FALSO

Fecha: 04/23/2013
Hora: 16:25:08
Tipo: Información
Fuente: acvpnagent

Descripción: **La conexión VPN se ha establecido y puede ahora pasar los**

Fecha: 04/23/2013
Hora: 16:25:08
Tipo: Información
Fuente: acvpnui

Descripción: Información del Tipo de mensaje enviada al usuario:
Estableciendo el VPN - Configurando el sistema...

Fecha: 04/23/2013
Hora: 16:25:08
Tipo: Información
Fuente: acvpnui

Descripción: Información del Tipo de mensaje enviada al usuario:
Estableciendo el VPN...

Fecha: 04/23/2013

Hora: 16:25:37

Tipo: Información

Fuente: acvpnagent

Archivo: . \ IPsecProtocol.cpp

Línea: 945

Se establece el túnel IPsec

Verificación del túnel

AnyConnect

La salida de muestra del comando del **anyconnect** del detalle de VPN-sessiondb de la demostración es:

Session Type: AnyConnect Detailed

```
Username      : Anu                               Index       : 2
Assigned IP   : 10.2.2.1                         Public IP    : 192.168.1.1
Protocol      : IKEv2 IPsecOverNatT AnyConnect-Parent
License       : AnyConnect Premium
Encryption    : AES192 AES256                   Hashing      : none SHA1 SHA1
Bytes Tx      : 0                               Bytes Rx     : 11192
Pkts Tx       : 0                               Pkts Rx     : 171
Pkts Tx Drop  : 0                               Pkts Rx Drop : 0
Group Policy  : ASA-IKEV2                       Tunnel Group : ASA-IKEV2
Login Time    : 22:06:24 UTC Mon Apr 22 2013
Duration      : 0h:02m:26s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A                             VLAN         : none
```

IKEv2 Tunnels: 1

IPsecOverNatT Tunnels: 1

AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:

```
Tunnel ID     : 2.1
Public IP     : 192.168.1.1
Encryption    : none                               Auth Mode    : userPassword
Idle Time Out : 30 Minutes                         Idle TO Left : 27 Minutes
Client Type   : AnyConnect
Client Ver    : 3.0.1047
```

IKEv2:

```
Tunnel ID     : 2.2
UDP Src Port  : 25171                               UDP Dst Port : 4500
Rem Auth Mode : userPassword
```

```

Loc Auth Mode: rsaCertificate
Encryption   : AES192                Hashing      : SHA1
Rekey Int (T): 86400 Seconds         Rekey Left(T): 86254 Seconds
PRF          : SHA1                  D/H Group   : 1
Filter Name  :
Client OS    : Windows
IPsecOverNatT:
Tunnel ID    : 2.3
Local Addr   : 0.0.0.0/0.0.0.0/0/0
Remote Addr  : 10.2.2.1/255.255.255.255/0/0
Encryption   : AES256                Hashing      : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds         Rekey Left(T): 28654 Seconds
Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4607990 K-Bytes
Idle Time Out: 30 Minutes           Idle TO Left : 29 Minutes
Bytes Tx     : 0                     Bytes Rx     : 11192
Pkts Tx     : 0                     Pkts Rx     : 171
NAC:
Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
SQ Int (T)   : 0 Seconds             EoU Age(T)   : 146 Seconds
Hold Left (T): 0 Seconds             Posture Token:
Redirect URL :

```

ISAKMP

La salida de muestra del comando `crypto ikev2 sa de la demostración` es:

Session Type: AnyConnect Detailed

```

Username      : Anu                    Index        : 2
Assigned IP   : 10.2.2.1                Public IP    : 192.168.1.1
Protocol      : IKEv2 IPsecOverNatT AnyConnect-Parent
License       : AnyConnect Premium
Encryption    : AES192 AES256           Hashing      : none SHA1 SHA1
Bytes Tx      : 0                       Bytes Rx     : 11192
Pkts Tx       : 0                       Pkts Rx     : 171
Pkts Tx Drop  : 0                       Pkts Rx Drop : 0
Group Policy  : ASA-IKEV2               Tunnel Group : ASA-IKEV2
Login Time    : 22:06:24 UTC Mon Apr 22 2013
Duration      : 0h:02m:26s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A                     VLAN         : none

```

```

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

```

AnyConnect-Parent:

```

Tunnel ID     : 2.1
Public IP     : 192.168.1.1
Encryption    : none                    Auth Mode    : userPassword
Idle Time Out: 30 Minutes               Idle TO Left : 27 Minutes
Client Type   : AnyConnect
Client Ver    : 3.0.1047

```

IKEv2:

```

Tunnel ID     : 2.2
UDP Src Port  : 25171                    UDP Dst Port : 4500
Rem Auth Mode: userPassword
Loc Auth Mode: rsaCertificate
Encryption    : AES192                    Hashing      : SHA1

```

```

Rekey Int (T): 86400 Seconds           Rekey Left(T): 86254 Seconds
PRF           : SHA1                   D/H Group    : 1
Filter Name   :
Client OS     : Windows
IPsecOverNatT:
Tunnel ID     : 2.3
Local Addr    : 0.0.0.0/0.0.0.0/0/0
Remote Addr   : 10.2.2.1/255.255.255.255/0/0
Encryption    : AES256                 Hashing       : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds           Rekey Left(T): 28654 Seconds
Rekey Int (D): 4608000 K-Bytes         Rekey Left(D): 4607990 K-Bytes
Idle Time Out: 30 Minutes              Idle TO Left  : 29 Minutes
Bytes Tx      : 0                      Bytes Rx      : 11192
Pkts Tx       : 0                      Pkts Rx      : 171
NAC:
Reval Int (T): 0 Seconds               Reval Left(T): 0 Seconds
SQ Int (T)   : 0 Seconds               EoU Age(T)   : 146 Seconds
Hold Left (T): 0 Seconds               Posture Token:
Redirect URL  :

```

La salida de muestra del comando detail crypto ikev2 sa de la demostración es:

```
ASA-IKEV2# show crypto ikev2 sa detail
```

```
IKEv2 SAs:
```

```
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```

Tunnel-id           Local                Remote              Status              Role
55182129           10.0.0.1/4500        192.168.1.1/25171  READY              RESPONDER
  Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
  Life/Active Time: 86400/98 sec
  Session-id: 2
  Status Description: Negotiation done
  Local spi: FC696330E6B94D7F          Remote spi: 58AFF71141BA436B
  Local id: hostname=ASA-IKEV2
  Remote id: *$AnyConnectClient$*
  Local req mess id: 0                  Remote req mess id: 9
  Local next mess id: 0                Remote next mess id: 9
  Local req queued: 0                  Remote req queued: 9          Local window:
1                               Remote window: 1
  DPD configured for 10 seconds, retry 2
  NAT-T is detected outside
  Assigned host addr: 10.2.2.1
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
          remote selector 10.2.2.1/0 - 10.2.2.1/65535
          ESP spi in/out: 0x30b848a4/0x77ee5348
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

```

IPSec

La salida de muestra del comando show crypto ipsec sa es:

```
ASA-IKEV2# show crypto ipsec sa detail
```

```
IKEv2 SAs:
```

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote	Status	Role
55182129	10.0.0.1/4500	192.168.1.1/25171	READY	RESPONDER

Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
Life/Active Time: 86400/98 sec
Session-id: 2
Status Description: Negotiation done
Local spi: FC696330E6B94D7F Remote spi: 58AFF71141BA436B
Local id: hostname=ASA-IKEV2
Remote id: *\$AnyConnectClient\$*
Local req mess id: 0 Remote req mess id: 9
Local next mess id: 0 Remote next mess id: 9
Local req queued: 0 Remote req queued: 9 Local window:
1 Remote window: 1
DPD configured for 10 seconds, retry 2
NAT-T is detected outside
Assigned host addr: 10.2.2.1
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 10.2.2.1/0 - 10.2.2.1/65535
ESP spi in/out: 0x30b848a4/0x77ee5348
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

Información Relacionada

- [RFC 4306, protocolo del intercambio de claves de Internet \(IKEv2\)](#)
- [RFC 3748, Protocolo de Autenticación Extensible \(EAP\)](#)
- [RFC 5996, Internet Key Exchange Protocol versión 2 \(IKEv2\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)