

IPSec FAQ: ¿Por qué es el Avaya teléfonos no más capaces de conectar vía el IPSec VPN después de la actualización de código en el ASA?

Contenido

[Introducción](#)

[¿Por qué es el Avaya teléfonos no más capaces de conectar vía el IPSEC VPN después de la actualización de código en el dispositivo de seguridad adaptante de Cisco \(ASA\)?](#)

Introducción

Este documento describe un problema encontrado cuando el Avaya se despliega en un sistema en el cual los teléfonos utilicen al cliente incorporado de la seguridad de protocolos en Internet (IPSec).

¿Por qué es el Avaya teléfonos no más capaces de conectar vía el IPSEC VPN después de la actualización de código en el dispositivo de seguridad adaptante de Cisco (ASA)?

Para entender este problema, usted necesita entender cómo el traversal de la traducción de dirección de red (NAT-T) y los trabajos de la detección NAT (NAT-D). El proceso NAT-D se comprende de estos pasos:

1. Detecta uno o más dispositivos NAT entre los host del IPSec.
2. Identifica si el par soporta el NAT-T.
3. Negocia el uso de la encapsulación del User Datagram Protocol (UDP) de los paquetes IPsec a través de los dispositivos NAT en el Internet Key Exchange (IKE).

NAT-D envía desmenuza de los IP Addresses y de los puertos de ambos pares IKE de cada extremo al otro. Si los ambos extremos calculan éstos desmenuzan y produzca los mismos resultados, ellos saben que no hay NAT en medio. Desmenuza se envían como serie de cargas útiles NAT-D. Cada payload contiene un hash. En el caso del múltiplo desmenuza, las cargas útiles múltiples NAT-D se envían. Normalmente, hay solamente dos cargas útiles NAT-D. Las cargas útiles NAT-D se incluyen en el tercero y los cuartos paquetes del modo principal, y en los segundos y terceros paquetes del modo agresivo. Puesto que este ejemplo utiliza un túnel de acceso remoto, es el modo agresivo.

Uno de los detalles incluidos en las cargas útiles NAT-D es el Vendor ID (VID). El intercambio de

los VID entre las ayudas de los pares determina la capacidad NAT-T del host remoto, según lo descrito en la [Solicitud de comentarios \(RFC\) 3947](#):

The format of the NAT-D packet is:

```

1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8
+-----+-----+-----+-----+-----+-----+-----+-----+
| Next Payload | RESERVED | Payload length |
+-----+-----+-----+-----+-----+-----+-----+-----+
~ HASH of the address and port
+-----+-----+-----+-----+-----+-----+-----+-----+
  
```

The payload type for the NAT discovery payload is 20.

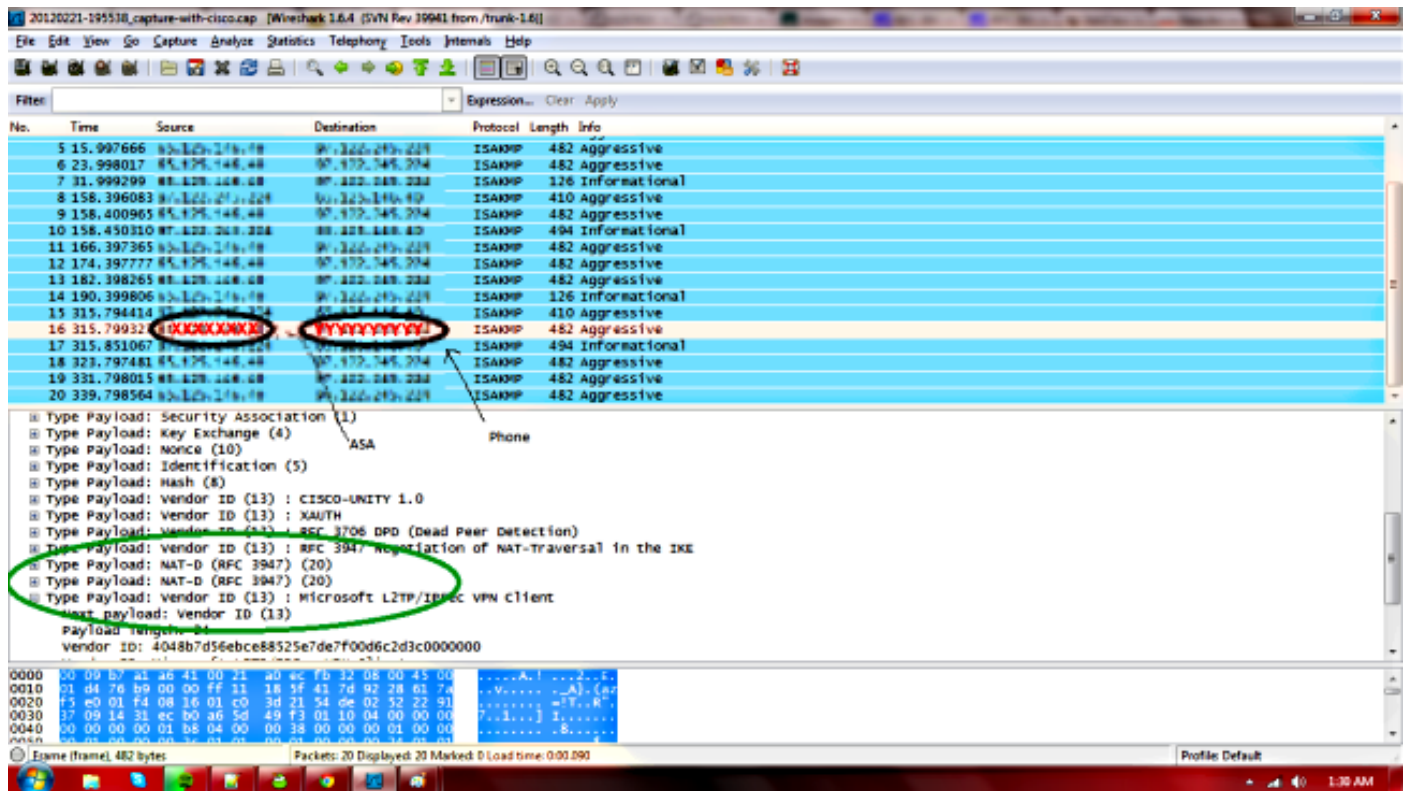
La corriente validó el tipo de carga útil del payload NAT-D es 20. Si usted mira los debugs en el ASA, usted ve:

```

[IKEv1]IP = 192.168.96.120, IKE_DECODE RECEIVED Message (msgid=0) with payloads:
HDR + KE (4) + NONCE (10) + UNKNOWN (15), *** ERROR *** + UNKNOWN (15),
*** ERROR *** + NONE (0) total length : 232
  
```

Aquí están las fotos de las capturas de paquetes:

ASA a llamar por teléfono:



Teléfono al ASA:

20120221-195518_capture-with-cisco.cap [Wireshark 1.6.4 (SVN Rev 39941 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
5	15.997666	85.129.178.78	85.129.219.229	ISAKMP	482	Aggressive
6	23.998017	85.129.178.78	85.129.219.229	ISAKMP	482	Aggressive
7	31.998299	85.129.178.78	85.129.219.229	ISAKMP	126	Informational
8	158.396083	85.129.178.78	85.129.219.229	ISAKMP	410	Aggressive
9	158.400965	85.129.178.78	85.129.219.229	ISAKMP	482	Aggressive
10	158.450310	85.129.178.78	85.129.219.229	ISAKMP	494	Informational
11	166.397365	85.129.178.78	85.129.219.229	ISAKMP	482	Aggressive
12	174.397777	85.129.178.78	85.129.219.229	ISAKMP	482	Aggressive
13	182.398265	85.129.178.78	85.129.219.229	ISAKMP	482	Aggressive
14	190.399806	85.129.178.78	85.129.219.229	ISAKMP	126	Informational
15	315.794414	85.129.178.78	85.129.219.229	ISAKMP	410	Aggressive
16	315.799327	85.129.178.78	85.129.219.229	ISAKMP	482	Aggressive
17	315.851067	XXXXXXXXXX	XXXXXXXXXX	ISAKMP	494	Informational
18	323.797481	85.129.178.78	85.129.219.229	ISAKMP	482	Aggressive
19	331.798015	85.129.178.78	85.129.219.229	ISAKMP	482	Aggressive
20	339.798564	85.129.178.78	85.129.219.229	ISAKMP	482	Aggressive

Responder cookie: 1431ecb0a65d49f3
 Next payload: Notification (11)
 version: 1.0
 Exchange type: Informational (5)
 Flags: 0x00
 Message ID: 0xe7f97586
 Length: 452
 Type Payload: Notification (11)
 Next payload: NONE / No Next Payload (0)
 Payload length: 424
 Domain of interpretation: ISAKMP (0)
 Protocol ID: ISAKMP (1)
 SPI size: 0
 Notify Message Type: INVALID-PAYLOAD-TYPE (1)
 Notify Message DATA: 0400003800000001000000010000002c0101000100000024...

0000 50 21 a0 ec fb 32 00 09 b7 a1 a6 41 08 00 45 00
 0010 01 e0 03 82 00 00 3a 11 50 8b 61 7a f5 e0 41 7d
 0020 92 28 08 16 01 f4 01 cc 01 62 54 6e 02 32 22 91
 0030 37 09 14 31 ec 00 a8 5d 49 f3 0b 10 05 00 67 f9
 0040 7a 86 00 00 01 e4 00 00 01 a8 00 00 00 01 03 00
 0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Epine (frame), 494 bytes | Packets: 20 Displayed: 20 Marked: 0 Load time: 0:00.090 | Profile: Default

El Avaya no reconoce el payload 20, y el ASA no entiende el tipo de carga útil 15. La explicación para este comportamiento es porque, en 2004, el mismo RFC definió el tipo de carga útil como 15. Por lo tanto, desde 2004, los teléfonos del Avaya que utilizan este tipo de carga útil son no más conforme a RFC. ¿Así pues, por qué trabajó con más viejo cifró? Porque, como el Avaya, algo del más viejo código (versión 8.0.x) todavía soporta el ID viejo. Sin embargo, el más nuevo código (versiones 8.2.1+) se supone para ser obediente con el nuevo valor RFC y no debe soportar el payload type15. No obstante, usted puede encontrar las diversas versiones alrededor de ese payload inmóvil type15 del soporte, que es qué causa el problema.

Necesidades del Avaya de reparar el firmware en el teléfono de modo que el cliente VPN incorporado utilice el payload correcto ID. Desafortunadamente, algunos otros teléfonos del Avaya, como las 46xx Series, están no más en la producción y no conseguirán un arreglo. En este caso, usted necesita obtener el nuevo equipo o necesitar retroceder el ASA a una versión en la cual trabajaba. Esta última opción no está obviamente disponible si usted actualizó para conseguir un arreglo del bug en el primer lugar. Ninguno de las versiones de software de Cisco que trabajan con la más vieja necesidad del payload ID de ser señalado y del problema reparado en esas versiones.