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 ésos 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:

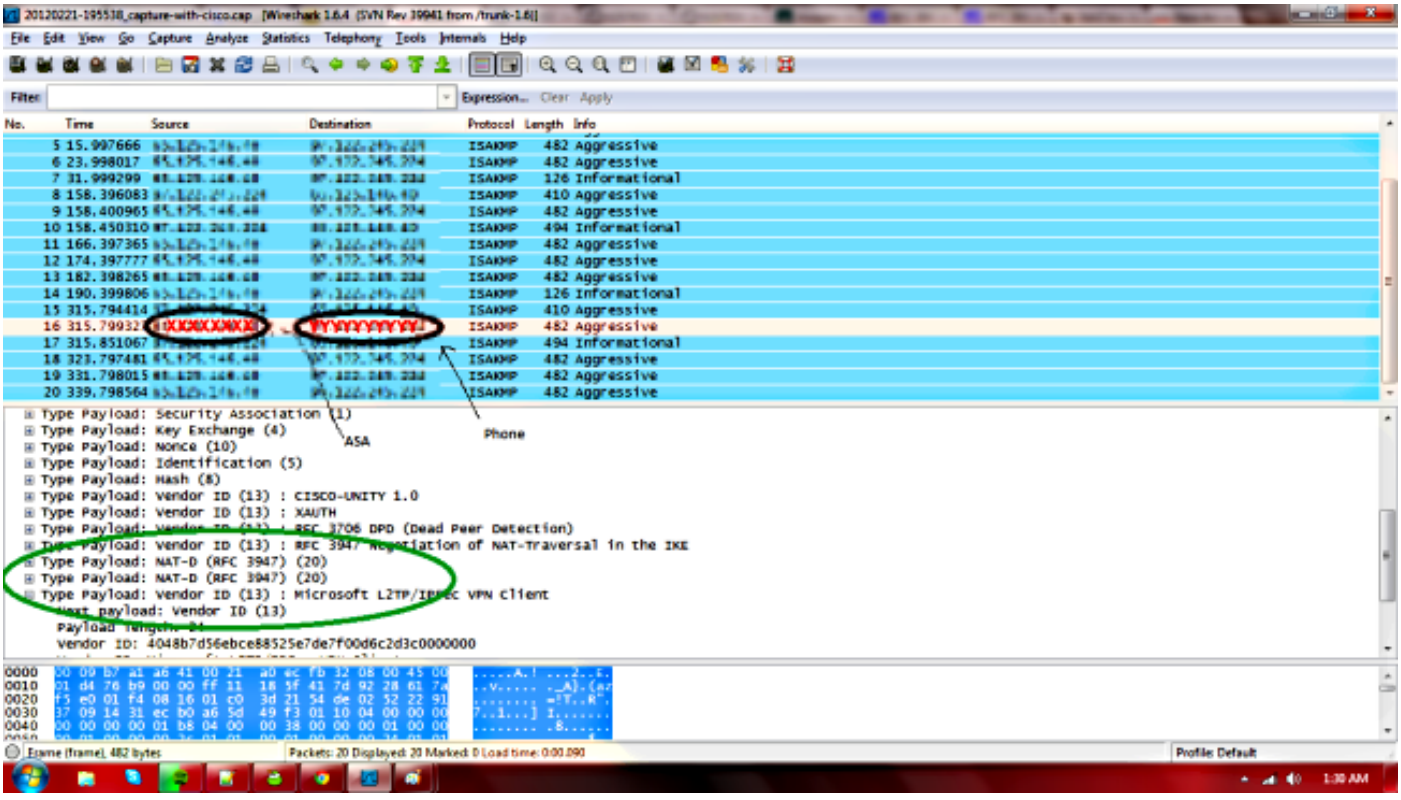
```
The format of the NAT-D packet is:

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:

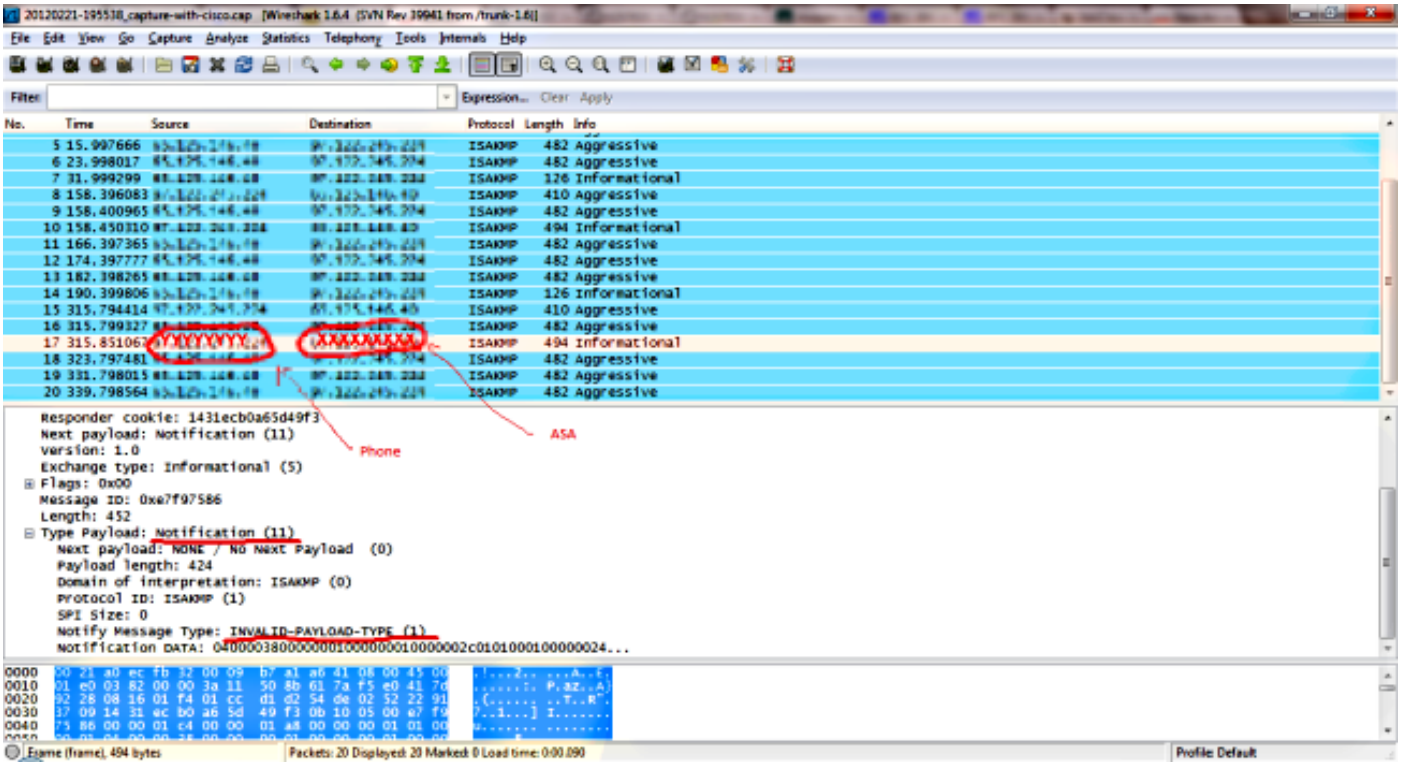
```
[IKEv1]IP = 192.168.96.120, IKE_DECODE RECEIVED Message (msgid=0) with payloads:
HDR + KE (4) + NONCE (10) + UNKNOWN (15), *** ERROR *** + UNKNOWN (15),
*** ERROR *** + NONE (0) total length : 232
```

Aquí están las fotos de las capturas de paquetes:

ASA a llamar por teléfono:



Teléfono al ASA:



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 paylod 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.