IPsec FAQ: Por que é Avaya telefones já não capazes de conectar através do IPSec VPN após a upgrade de código no ASA?

Índice

Introdução

Este documento descreve um problema encontrado quando Avaya é distribuído em um sistema em que os telefones usam o cliente incorporado da segurança de protocolo do Internet (IPsec).

Por que é Avaya telefones já não capazes de conectar através do IPSEC VPN após a upgrade de código na ferramenta de segurança adaptável de Cisco (ASA)?

A fim compreender este problema, você precisa de compreender como o traversal da tradução de endereço de rede (NAT-T) e da descoberta NAT trabalhos (NAT-D). O processo NAT-D é compreendido destas etapas:

1. Detecta uns ou vários dispositivos NAT entre anfitriões do IPsec.
2. Identifica se o par apoia o NAT-T.
3. Negocia o uso do encapsulamento do User Datagram Protocol (UDP) dos pacotes de IPsec através dos dispositivos NAT no Internet Key Exchange (IKE).

NAT-D envia pica dos endereços IP de Um ou Mais Servidores Cisco ICM NT e das portas de ambos os pares IKE de cada extremidade à outro. Se o ambas as extremidades calcula aqueles pica e produza os mesmos resultados, eles sabem que não há nenhum NAT no meio. Pica são enviados como uma série de cargas úteis NAT-D. Cada payload contém uma mistura. No caso do múltiplo pica, cargas úteis múltiplas NAT-D são enviados. Normalmente, há somente duas cargas úteis NAT-D. As cargas úteis NAT-D são incluídas no terço e nos quartos pacotes do modo principal, e nos segundos e terceiros pacotes do modo assertivo. Desde que este exemplo usa um túnel de acesso remoto, é o modo assertivo.

Um dos detalhes incluídos nas cargas úteis NAT-D é o Vendor ID (VID). A troca dos VID entre ajudas dos pares determina a capacidade NAT-T do host remoto, como descrito na solicitação para comentários (RFC) 3947:

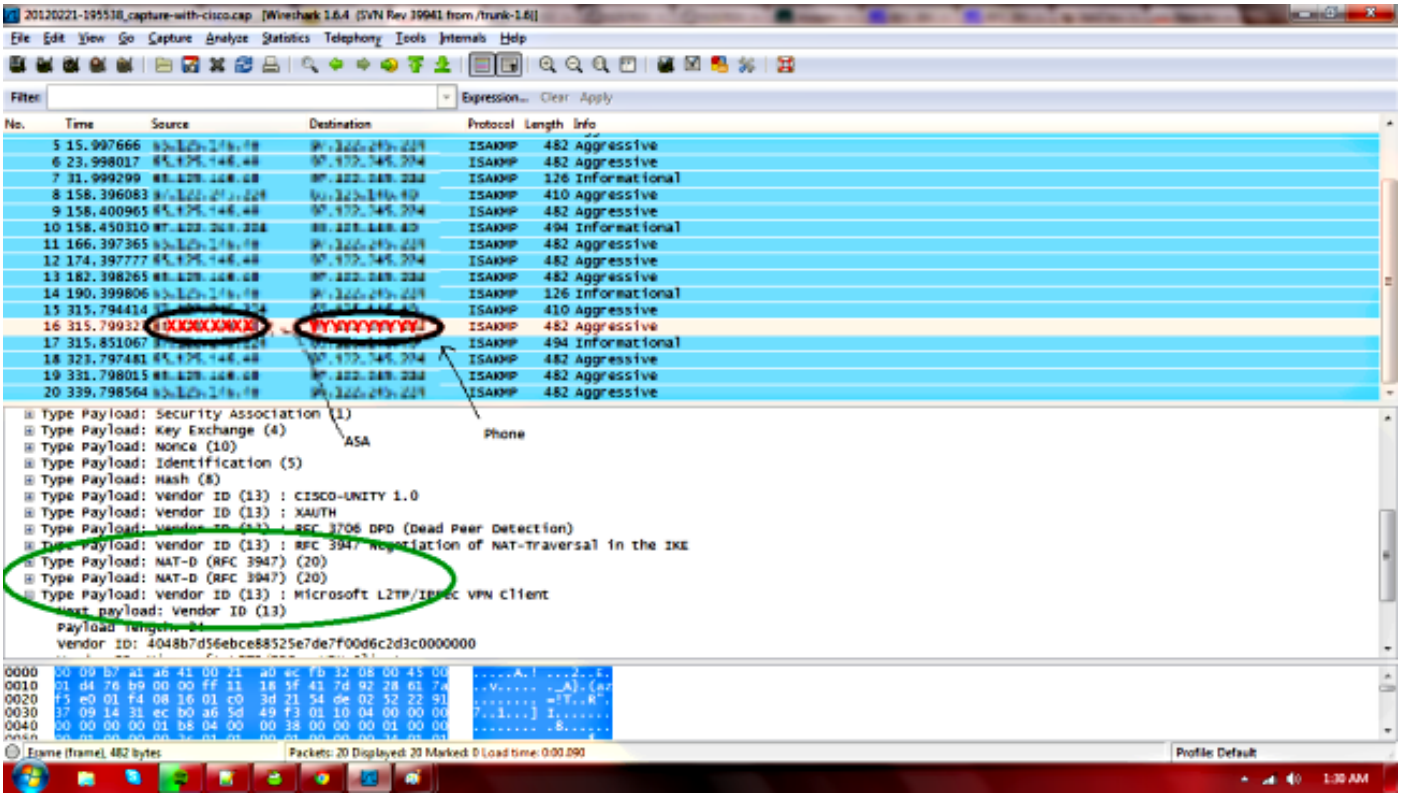
```
The format of the NAT-D packet is:

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.
```

A corrente aceitou o tipo de payload do payload NAT-D é 20. Se você olha debuga no ASA, você vê:

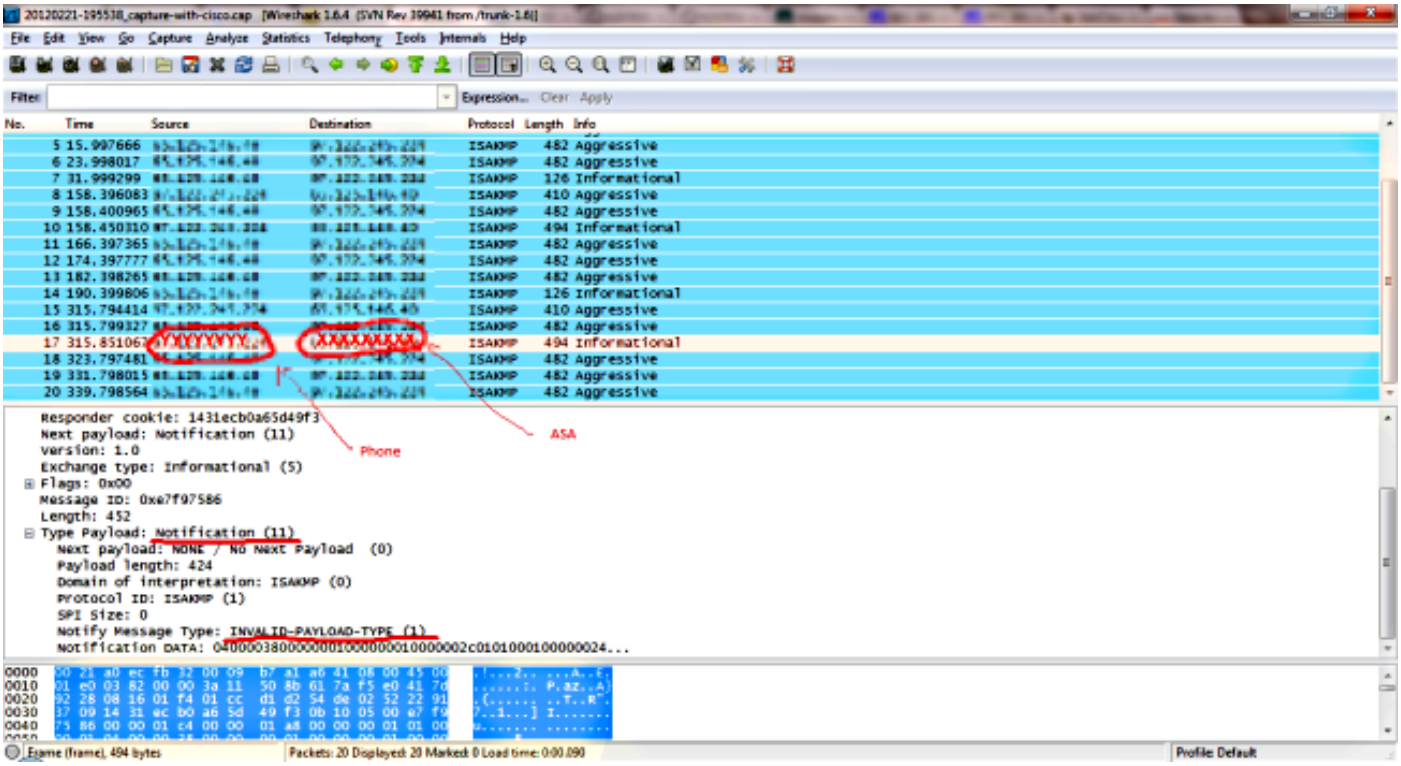
```
[IKEv1]IP = 192.168.96.120, IKE_DECODE RECEIVED Message (msgid=0) with payloads:
HDR + KE (4) + NONCE (10) + UNKNOWN (15), *** ERROR *** + UNKNOWN (15),
*** ERROR *** + NONE (0) total length : 232
```

Estão aqui os instantâneos das capturas de pacote de informação:

ASA a telefonar:



Telefone ao ASA:



Avaya não reconhece o payload 20, e o ASA não compreende o tipo de payload 15. A explicação para este comportamento é porque, em 2004, o mesmo RFC definiu o tipo de payload como 15. Consequentemente, desde 2004, os telefones de Avaya que usam este tipo de payload são já não em conformidade com RFC. Assim, por que trabalhou com mais velho codifica? Porque, como Avaya, algum do código mais velho (versão 8.0.x) ainda apoia o ID velho. Contudo, o código mais novo (versões 8.2.1+) é suposto para ser complacente com o valor novo RFC e não deve apoiar o payload type15. Todavia, você pode encontrar várias versões em torno desse payload imóvel type15 do apoio, que é o que causa o problema.

Necessidades de Avaya de fixar o firmware no telefone de modo que o cliente VPN incorporado use o paylod direito ID. Infelizmente, alguns outros telefones de Avaya, como o 46xx Series, estão já não na produção e não obterão um reparo. Neste caso, você precisa de obter o equipamento novo ou de precisá-lo de degradar o ASA a uma versão em que estava trabalhando. Obviamente esta última opção não está disponível se você promoveu a fim obter uma correção de bug no primeiro lugar. Alguma das versões de software de Cisco que trabalham com a necessidade mais velha do payload ID de ser relatado e da edição fixada naquelas versões.