O cliente de AnyConnect reconecta cada minuto que causa um rompimento no fluxo de tráfego

Índice

Introdução

Este documento discute a encenação específica onde o cliente de AnyConnect pôde reconectar à ferramenta de segurança adaptável (ASA) em exatamente um minuto. Os usuários não puderam poder receber o tráfego sobre o túnel do Transport Layer Security (TLS) até que AnyConnect reconecte. Isto é dependente de alguns outros fatores que são discutidos neste documento.

Componentes afetados

- Liberação 9.0 ASA ou liberação 9.1
- 3.0 da versão cliente de AnyConnect ou liberação 3.1

Sintomas

Neste exemplo, o cliente de AnyConnect é mostrado enquanto reconecta ao ASA.

Este Syslog é visto no ASA:

```
%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111>
Transmitting large packet 1418 (threshold 1347).
```

Descrição do problema

Estes logs dos diagnósticos e da ferramenta de relatório (DARDO) são considerados com esta edição:

```
****************************************

Date         : 11/16/2013
Time         : 01:28:50
Type         : Warning
Source       : acvpnagent

Description : Reconfigure reason code 16:
New MTU configuration.

****************************************

Date         : 11/16/2013
Time         : 01:28:50
Type         : Information
Source       : acvpnagent

Description : The entire VPN connection is being reconfigured.

****************************************

Date         : 11/16/2013
Time         : 01:28:51
Type         : Information
Source       : acvpnui

Description : Message type information sent to the user:
Reconnecting to 10.1.1.2...

****************************************

Date         : 11/16/2013
Time         : 01:28:51
Type         : Warning
Source       : acvpnagent

Description : A new MTU needs to be applied to the VPN network interface.
Disabling and re-enabling the Virtual Adapter. Applications utilizing the
private network may need to be restarted.


****************************************
```

Causas

A causa desta edição é a falha construir um túnel da Segurança da camada de transporte de datagram (DTL). Isto podia ser devido a duas razões:

- Os DTL são obstruídos em algum lugar no trajeto
- Uso de uma porta não-padrão DTL

Os DTL são obstruídos em algum lugar no trajeto

Até à data do ASA libere a liberação 3.x 9.x e de AnyConnect, uma otimização foi introduzido sob a forma das unidades máximas distintas da transição (MTU) que são negociadas para TLS/DTLS

entre o client/ASA. Previamente, o cliente derivou uma estimativa bruta MTU que cobrisse ambos os TLS/DTLS e fosse obviamente menos do que ótimo. Agora, o ASA computa a carga adicional de encapsulamento para ambos os TLS/DTLS e deriva os valores MTU em conformidade.

Enquanto os DTL são permitidos, o cliente aplica os DTL MTU (neste caso 1418) no adaptador de VPN (que é permitido antes que o túnel DTL esteja estabelecido e precisado para rotas/aplicação dos filtros), para assegurar o desempenho ideal. Se o túnel DTL não pode ser estabelecido ou está deixado cair em algum momento, o cliente falha sobre ao TLS e ajusta o MTU no adaptador virtual (VA) ao valor TLS MTU (este exige um nível da sessão reconecta).

Resolução

A fim eliminar esta transição visível dos DTL > o TLS, o administrador podem configurar um grupo do túnel separado para o acesso TLS somente para os usuários que têm o problema com o estabelecimento do túnel DTL (tal como devido às restrições de firewall).

1. A melhor opção é ajustar o valor de AnyConnect MTU para ser mais baixa do que o TLS MTU, que é negociado então.`group-policy ac_users_group attributes`
   `webvpn`
   `anyconnect mtu 1300` Isto faz os valores TLS e DTL MTU iguais. As reconexões não são consideradas neste caso.
2. A segunda opção é permitir a fragmentação. `group-policy ac_users_group attributes`
   `webvpn`
   `anyconnect ssl df-bit-ignore enable`Com fragmentação, os grandes pacotes (cujo o tamanho excede o valor MTU) podem ser fragmentados e enviado através do túnel TLS.
3. A terceira opção é ajustar o Maximum Segment Size (MSS) a 1460 como segue:`sysopt conn tcpmss 1460` Neste caso, o TLS MTU será 1427 (RC4/SHA1) que é maior do que os DTL MTU 1418 (AES/SHA1/LZS). Isto deve resolver a edição com o TCP do ASA ao cliente de AnyConnect (agradecimentos ao MSS), mas o grande tráfego UDP do ASA ao cliente de AnyConnect pôde sofrer deste porque será deixado cair pelo cliente de AnyConnect devido ao cliente mais baixo MTU 1418 de AnyConnect. Se os **tcpmss conexão do sysopt** são alterados, pôde afetar outros recursos tais como túneis do IPSec VPN do LAN para LAN (L2L).

Uso de uma porta não-padrão DTL

Uma outra causa potencial para a falha DTL está permitindo DTL em uma porta não-padrão depois que o WebVPN é permitido (por exemplo, quando o **webvpn permite o** comando **exterior** está incorporado). Isto é devido à identificação de bug Cisco CSCuh61321 e foi visto na liberação 9.x onde o ASA empurra a porta não-padrão para o cliente, mas continua a escutar a porta padrão. Consequentemente, os DTL não são construídos e AnyConnect reconecta.

```
webvpn
 port 444
 enable outside
 dtls port 444
 anyconnect enable

ciscoasa(config-webvpn)# show asp table socket
```

```
Protocol  Socket    State      Local Address             Foreign Address
SSL       0001fc08  LISTEN     172.16.11.1:444           0.0.0.0:*

DTLS      00020dc8  LISTEN     172.16.11.1:443           0.0.0.0:*
```

Depois que o túnel TLS é estabelecido, o cliente tenta estabelecer os DTL escava um túnel à porta 444 como esperado:

A ordem dos comandos que conduzem ao problema e aos soquetes acelerados da tabela do trajeto da Segurança (ASP) abertos é:

1. Comece com os soquetes WebVPN não permitidos.
```
ciscoasa(config)# show run webvpn
webvpn
 anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
 anyconnect enable


ciscoasa(config)# show asp table socket
Protocol  Socket    State      Local Address             Foreign Address
ciscoasa(config)#
```
2. Mude a porta TLS a 444 e permita o WebVPN.
```
ciscoasa(config-webvpn)# show run webvpn
webvpn
 port 444
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
 anyconnect enable


ciscoasa(config-webvpn)# show asp tabl socket
Protocol  Socket    State      Local Address             Foreign Address
SSL       0001fc08  LISTEN     172.16.11.1:444           0.0.0.0:*
DTLS      00020dc8  LISTEN     172.16.11.1:443           0.0.0.0:*
```
3. Mude os DTL movem a 444.
```
ciscoasa(config-webvpn)# dtls port 444
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# show run webvpn
webvpn
 port 444
 enable outside
 dtls port 444
 anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
 anyconnect enable

ciscoasa(config-webvpn)# show asp table socket


Protocol  Socket    State      Local Address             Foreign Address
SSL       0001fc08  LISTEN     172.16.11.1:444           0.0.0.0:*
DTLS      00020dc8  LISTEN     172.16.11.1:443           0.0.0.0:*
```

   Nota: A porta do soquete DTL é ainda 443. Neste momento os clientes de AnyConnect estabelecem DTL a 444 embora!

Resolução

A ação alternativa para este problema é seguir a ordem de:

1. Desabilite o WebVPN.

2. Entre na porta DTL.
3. Permita o WebVPN.

Este comportamento não existe nas versões da liberação 8.4.x, aonde os soquetes DTL obtêm actualizados com as portas configuradas imediatamente depois que a configuração é incorporada:

Liberação 8.4.6 ASA:

```
ciscoasa(config-webvpn)# port 444
ciscoasa(config-webvpn)# enable outside
ciscoasa(config-webvpn)# show asp table socket

Protocol Socket Local Address Foreign Address State
SSL 0000bf2f 172.16.11.1:444 0.0.0.0:* LISTEN
DTLS 0000d5df 172.16.11.1:443 0.0.0.0:* LISTEN

ciscoasa(config-webvpn)# dtls port 444
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# show asp table socket

Protocol Socket Local Address Foreign Address State
SSL 0000bf2f 172.16.11.1:444 0.0.0.0:* LISTEN
DTLS 0000eb5f 172.16.11.1:444 0.0.0.0:* LISTEN << changed immediately
```

Reconecte trabalhos

Supõe que estas cifras estão configuradas:

```
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1
```

Esta sequência de evento ocorre neste caso:

- AnyConnect estabelece um túnel do pai e uns dados TLS escavam um túnel com o RC4-SHA como a criptografia SSL.
- Os DTL são obstruídos no trajeto e um túnel DTL não pode ser estabelecido.
- O ASA anuncia parâmetros a AnyConnect, que inclui os valores TLS e DTL MTU, que são dois valores separados.
- OS DTL MTU são 1418 à revelia.
- O TLS MTU é calculado do valor dos **tcpmss conexão do sysopt** (o padrão é 1380). Isto é como o TLS MTU é derivado (como visto do **anyconnect do webvpn debugar** output):
  `1380 - 5 (TLS header) - 8 (CSTP) - 0 (padding) - 20 (HASH) = 1347`
- AnyConnect traz o adaptador de VPN acima e atribui-lhe **DTL** MTU na antecipação que poderá conectar através dos DTL.
- O cliente de AnyConnect é conectado agora e o usuário vai a um Web site particular.
- O navegador envia TCP SYN e ajusta-se MSS = 1418-40 = 1378 nele.
- O Server do HTTP no interior do ASA envia pacotes do tamanho 1418.
- O ASA não pode pô-los no túnel e não pode fragmentá-los porque têm don't fragment (DF) o jogo do bit.
- Cópias ASA`%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111> Transmitting large packet 1418 (threshold 1347)`e pacotes das gotas com razão da gota MP-SVC-nenhum-fragmento-ASP.
- Ao mesmo tempo o ASA envia o destino ICMP inacessível, fragmentação necessária o remetente:

```
    %ASA-6-602101: PMTU-D packet 1418 bytes greater than effective mtu 1347,
dest_addr=10.10.10.1, src_addr=10.48.66.200, prot=TCP
```

- Se o Internet Control Message Protocol (ICMP) é permitido, a seguir o remetente retransmite pacotes descartado e tudo começa trabalhar. Se o ICMP é obstruído, a seguir o tráfego blackholed no ASA.
- Depois que diversos retransmitem compreende que o túnel DTL não pode ser estabelecido e precisa de atribuir novamente um valor novo MTU ao adaptador de VPN.
- A finalidade desta reconecta é atribuir um MTU novo.

Para obter mais informações sobre de reconecte o comportamento e os temporizadores, veem AnyConnect FAQ: Os túneis, reconectam o comportamento, e o temporizador de inatividade

Caveats

A identificação de bug Cisco CSCuh61321 AC 3.1:ASA segura incorretamente DTL alternativos move, causas reconecta

Informações Relacionadas

- AnyConnect FAQ: Os túneis, reconectam o comportamento, e o temporizador de inatividade
- Suporte Técnico e Documentação - Cisco Systems