El cliente de AnyConnect vuelve a conectar cada minuto que cause una interrupción en el flujo de tráfico

Contenido

[Introducción](#)
[Componentes Afectados](#)
[Síntomas](#)
[Descripción de problemas](#)
[Causas](#)
[Los DTL se bloquean en alguna parte en la trayectoria](#)
[Resolución](#)
[Uso de un puerto del no valor por defecto DTL](#)
[Resolución](#)
[Vuelva a conectar el flujo de trabajo](#)
[Advertencias](#)
[Información Relacionada](#)

Introducción

Este documento discute el escenario específico donde el cliente de AnyConnect pudo volver a conectar al dispositivo de seguridad adaptante (ASA) en exactamente un minuto. Los usuarios no pudieron poder recibir el tráfico sobre el túnel de Transport Layer Security (TLS) hasta que AnyConnect vuelva a conectar. Esto es dependiente sobre algunos otros factores que se discutan en este documento.

Componentes Afectados

- Versión 9.0 ASA o versión 9.1
- 3.0 o versión 3.1 de la versión de cliente de AnyConnect

Síntomas

En este ejemplo, muestran el cliente de AnyConnect mientras que vuelve a conectar al ASA.

Este Syslog se ve en el ASA:

```
%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111>
```

```
Transmitting large packet 1418 (threshold 1347).
```

Descripción de problemas

Estos registros de los diagnósticos y de la herramienta de informe (DARDO) se ven con este problema:

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

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

La causa de este problema es el error construir un túnel de la Seguridad de la capa de transporte de datagrama (DTL). Esto podía estar debido a dos razones:

- Los DTL se bloquean en alguna parte en la trayectoria
- Uso de un puerto del no valor por defecto DTL

Los DTL se bloquean en alguna parte en la trayectoria

A partir de la versión 9.x ASA y de la versión 3.x de AnyConnect, una optimización se ha introducido bajo la forma de unidades máximas distintas de la transición (MTU) que se negocian para TLS/DTLS entre el client/ASA. Previamente, el cliente derivó un cálculo aproximado MTU que cubrió ambos TLS/DTLS y era obviamente menos que óptimo. Ahora, el ASA computa la tara de encapsulación para ambos TLS/DTLS y deriva los valores MTU por consiguiente.

Mientras se habiliten los DTL, el cliente aplica los DTL MTU (en este caso 1418) en el adaptador VPN (se habilita que antes de que el túnel DTL se establezca y sea necesario para las rutas/la aplicación de los filtros), para asegurar el rendimiento óptimo. Si el túnel DTL no puede ser establecido o se cae en algún momento, el cliente falla encima a TLS y ajusta el MTU en el adaptador virtual (VA) al valor de TLS MTU (éste requiere un nivel de la sesión vuelve a conectar).

Resolución

Para eliminar esta transición visible de los DTL > TLS, el administrador pueden configurar un grupo del túnel diferente para el acceso de TLS solamente para los usuarios que tienen problema con el establecimiento del túnel DTL (tal como debido a las restricciones del Firewall).

1. La mejor opción es fijar el valor de AnyConnect MTU para ser más baja que TLS MTU, que entonces se negocia.`group-policy ac_users_group attributes`
   `webvpn`
   `anyconnect mtu 1300` Esto hace los valores de TLS y DTL MTU iguales. Las reconexiones no se consideran en este caso.
2. La segunda opción es permitir la fragmentación. `group-policy ac_users_group attributes`
   `webvpn`
   `anyconnect ssl df-bit-ignore enable`Con la fragmentación, los paquetes grandes (cuyo tamaño excede el valor MTU) se pueden hacer fragmentos y enviar a través del túnel de TLS.
3. La tercera opción es fijar el Maximum Segment Size (MSS) a 1460 como sigue:`sysopt conn tcpmss 1460` En este caso, TLS MTU será 1427 (RC4/SHA1) que es más grande que los DTL MTU 1418 (AES/SHA1/LZS). Esto debe resolver el problema con el TCP del ASA al cliente de AnyConnect (gracias al MSS), pero el tráfico grande UDP del ASA al cliente de AnyConnect pudo sufrir de esto pues será caído por el cliente de AnyConnect debido al cliente más bajo MTU 1418 de AnyConnect. Si se modifican los **tcpmss conec del sysopt**, puede ser que afecte a las otras funciones tales como túneles del IPSec VPN del LAN a LAN (L2L).

Uso de un puerto del no valor por defecto DTL

Otra causa potencial para el incidente DTL está habilitando los DTL en un puerto no valor por defecto después de que se habilite el WebVPN (por ejemplo, cuando el **webvpn habilita** se ingresa el comando **exterior**). Esto es debido al Id. de bug Cisco CSCuh61321 y se ha visto en la versión 9.x donde el ASA avanza el puerto no valor por defecto al cliente, pero continúa escuchando el puerto predeterminado. Por lo tanto, los DTL no se construyen y AnyConnect vuelve a conectar.

```
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:*
```

Después de que se establezca el túnel de TLS, el cliente intenta establecer los DTL hace un túnel al puerto 444 como se esperaba:

La orden de los comandos que llevan al problema y a los socketes acelerados de la tabla de la trayectoria de la Seguridad (ASP) abiertos es:

1. Comience con los socketes del WebVPN no habilitados.
```
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. Cambie el puerto de TLS a 444 y habilite el 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. Cambie los DTL viran hacia el lado de babor 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: El puerto del socket DTL sigue siendo 443. ¡En este momento los clientes de AnyConnect establecen los DTL a 444 sin embargo!

Resolución

La solución alternativa para este problema es seguir la orden de:

1. Inhabilite el WebVPN.
2. Ingrese el puerto DTL.
3. Habilite el WebVPN.

Este comportamiento no existe en las versiones de la versión 8.4.x, adonde los socketes DTL consiguen actualizados con los puertos configurados inmediatamente después que se ingresa la configuración:

Versión 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
```

Vuelva a conectar el flujo de trabajo

Suponga que estas cifras están configuradas:

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

Esta Secuencia de eventos ocurre en este caso:

- AnyConnect establece un túnel del padre y un túnel de los datos de TLS con el RC4-SHA como la encripción de SSL.
- Los DTL se bloquean en la trayectoria y un túnel DTL no puede ser establecido.
- El ASA anuncia los parámetros a AnyConnect, que incluye los valores de TLS y DTL MTU, que son dos valores separados.
- Los DTL MTU son 1418 por abandono.
- TLS MTU se calcula del valor de los **tcpmss conec del sysopt** (el valor por defecto es 1380). Éste es cómo se deriva TLS MTU (según lo visto del **anyconnect del webvpn del debug** hecho salir):

  ```
  1380 - 5 (TLS header) - 8 (CSTP) - 0 (padding) - 20 (HASH) = 1347
  ```
- AnyConnect trae el adaptador VPN para arriba y le asigna **DTL** MTU en la anticipación que podrá conectar vía los DTL.
- El cliente de AnyConnect ahora está conectado y el usuario va a un sitio web determinado.
- El navegador envía TCP SYN y fija MSS = 1418-40 = 1378 en él.
- El servidor HTTP en el interior del ASA envía los paquetes de talla 1418.
- El ASA no puede ponerlos en el túnel y no puede hacer fragmentos de ellos pues tienen el

conjunto de bits del don't fragment (DF).

- Impresiones ASA`%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111> Transmitting large packet 1418 (threshold 1347)`y paquetes de los descensos con la razón del descenso MP-SVC-ninguno-fragmento-ASP.
- Al mismo tiempo el ASA envía el destino ICMP inalcanzable, fragmentación necesaria el remitente:

```
    %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
```

- Si se permite el Internet Control Message Protocol (ICMP), después el remitente retransmite los paquetes perdidos y todo comienza a trabajar. Si se bloquea el ICMP, después el tráfico blackholed en el ASA.
- Después de que varios retransmitan entiende que el túnel DTL no puede ser establecido y necesita reasignar un nuevo valor MTU al adaptador VPN.
- El propósito de esto vuelve a conectar es asignar un nuevo MTU.

Para más información encendido vuelva a conectar el comportamiento y los temporizadores, ven AnyConnect FAQ: Los túneles, vuelven a conectar el comportamiento, y el temporizador de inactividad

Advertencias

El Id. de bug Cisco CSCuh61321 AC 3.1:ASA dirige incorrectamente los DTL alternos vira hacia el lado de babor, las causas vuelve a conectar

Información Relacionada

- AnyConnect FAQ: Los túneles, vuelven a conectar el comportamiento, y el temporizador de inactividad
- Soporte Técnico y Documentación - Cisco Systems