Corregir las interrupciones del flujo de tráfico causadas por las reconexiones de AnyConnect

Contenido

Introducción

Este documento describe qué sucede cuando un cliente AnyConnect se vuelve a conectar al dispositivo de seguridad adaptable (ASA) en exactamente un minuto.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

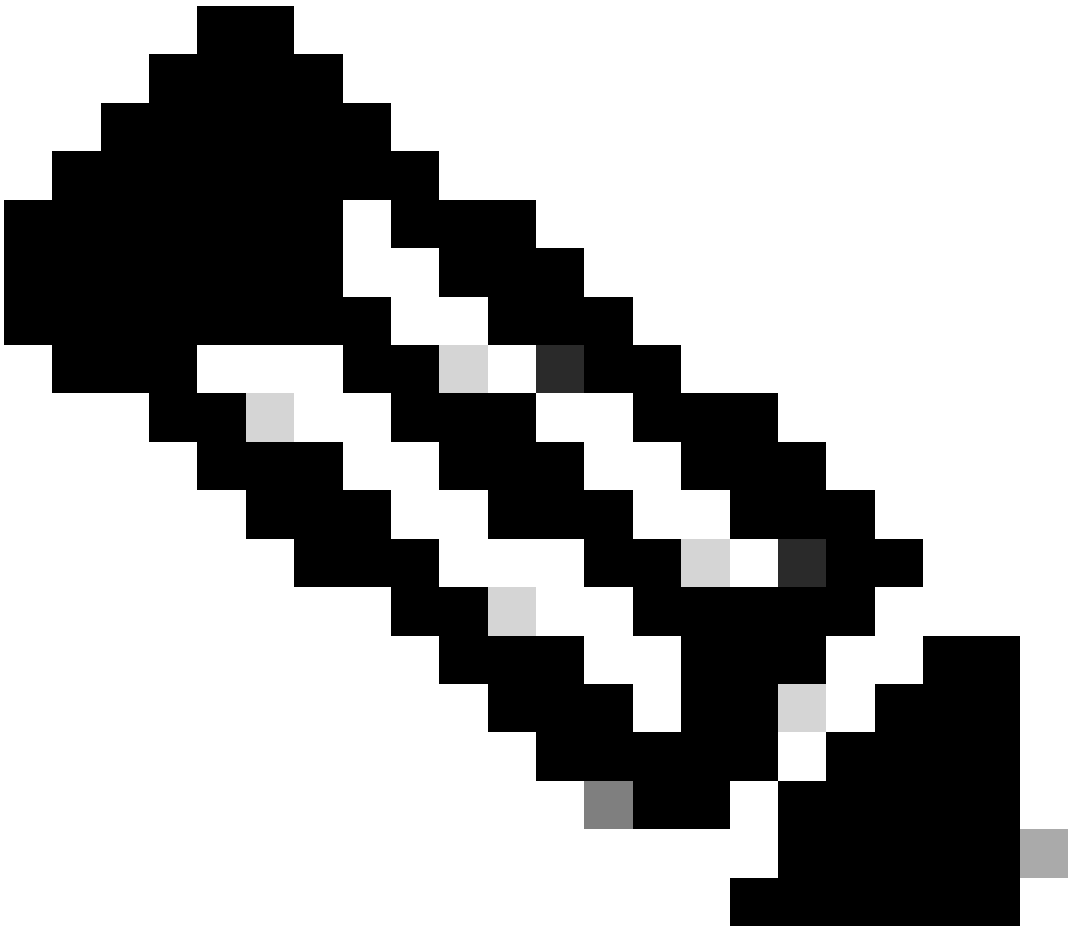
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Estos productos se vieron afectados por este problema:

- ASA versión 9.17
- Cliente AnyConnect versión 4.10

Antecedentes

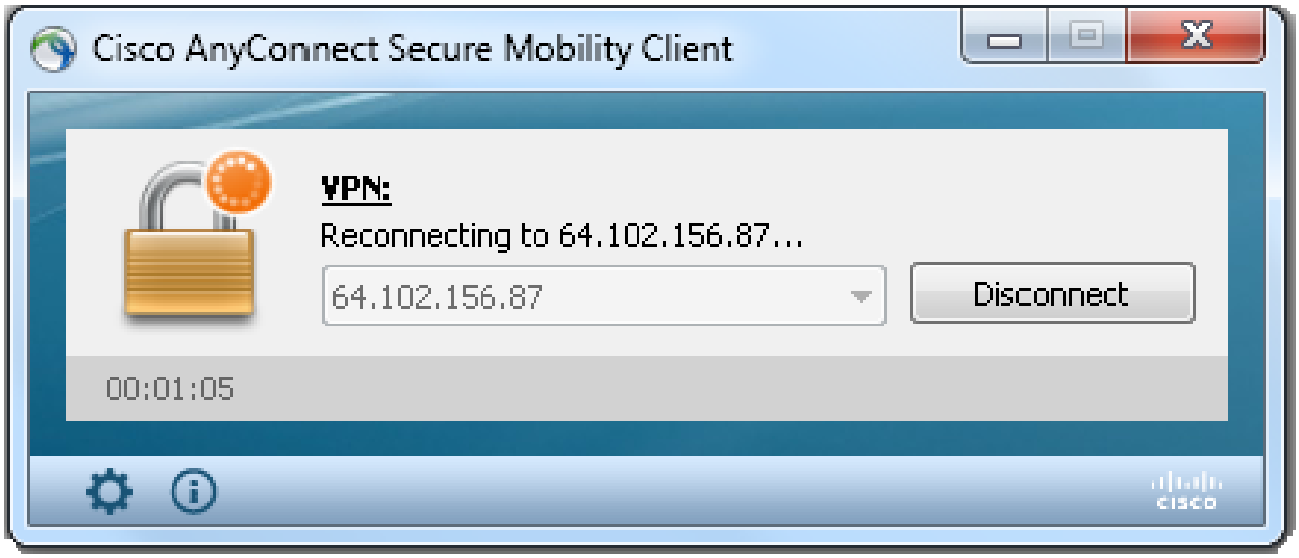


> Nota: AnyConnect se ha cambiado a Cisco Secure Client. Nada más cambió, solo el nombre, y el proceso de instalación es el mismo.

Si el cliente AnyConnect se vuelve a conectar al dispositivo de seguridad adaptable (ASA) en exactamente un minuto, los usuarios no podrán recibir tráfico a través del túnel de seguridad de la capa de transporte (TLS) hasta que AnyConnect se vuelva a conectar. Esto depende de algunos otros factores que se discuten en este documento.

Síntomas

En este ejemplo, se muestra el cliente AnyConnect cuando se vuelve a conectar al ASA.



Este syslog se ve en 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 diagnóstico y Reporting herramientas (DART) se ven con este problema:

<#root>

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

Date         : 11/16/2022
Time         : 01:28:50
Type         : Warning
Source       : acvpnagent

Description : Reconfigure reason code 16:

New MTU configuration.


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

Date         : 11/16/2022
Time         : 01:28:50
```

```
Type        : Information
Source      : acvpnagent

Description : The entire VPN connection is being reconfigured.

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

Date        : 11/16/2022
Time        : 01:28:51
Type        : Information
Source      : acvpnui

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

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

Date        : 11/16/2022
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 la falla al construir un túnel de seguridad de la capa de transporte del datagrama (DTLS). Esto puede deberse a dos razones:

- DTLS está bloqueado en algún lugar de la ruta.
- Uso de un puerto DTLS no predeterminado.

DTLS está bloqueado en algún lugar del trayecto

A partir de ASA Release 9.x y AnyConnect Release 4.x, se ha introducido una optimización en forma de unidades de transición máxima (MTU) distintas que se negocian para TLS/DTLS entre el cliente/ASA. Anteriormente, el cliente obtenía una MTU aproximada que cubría tanto TLS/DTLS y era obviamente inferior a la óptima. Ahora, ASA calcula la sobrecarga de encapsulación para TLS/DTLS y deriva los valores de MTU en consecuencia.

Mientras DTLS esté habilitado, el cliente aplica la MTU DTLS (en este caso, 1418) en el adaptador VPN (que está habilitado antes de que se establezca el túnel DTLS y es necesario para la aplicación de rutas/filtros), para garantizar un rendimiento óptimo. Si el túnel DTLS no se

puede establecer o se descarta en algún momento, el cliente conmuta por error a TLS y ajusta la MTU en el adaptador virtual (VA) al valor de MTU de TLS (esto requiere una reconexión de nivel de sesión).

Resolución

Para eliminar esta transición visible de DTLS > TLS, el administrador puede configurar un grupo de túnel independiente para el acceso TLS solamente para los usuarios que tienen problemas con el establecimiento del túnel DTLS (por ejemplo, debido a las restricciones del firewall).

1. La mejor opción es establecer el valor de MTU de AnyConnect en menor que la MTU de TLS, que se negocia a continuación.

```
group-policy ac_users_group attributes
 webvpn
  anyconnect mtu 1300
```

   Esto hace que los valores de MTU TLS y DTLS sean iguales. En este caso no se ven reconexiones.

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 de MTU) se pueden fragmentar y enviar a través del túnel TLS.

3. La tercera opción es establecer el tamaño máximo de segmento (MSS) en 1460, como se muestra a continuación:

```
sysopt conn tcpmss 1460
```

   En este caso, la MTU de TLS puede ser 1427 (RC4/SHA1), que es mayor que la MTU de DTLS 1418 (AES/SHA1/LZS). Esto resuelve el problema con el TCP del ASA al cliente AnyConnect (gracias a MSS), pero el gran tráfico UDP del ASA al cliente AnyConnect puede sufrir esto ya que puede ser descartado por el cliente AnyConnect debido a la menor MTU del cliente AnyConnect 1418. Si se modifica sysopt conn tcpmss, puede afectar a otras funciones como los túneles VPN IPSec de LAN a LAN (L2L).

Volver a conectar flujo de trabajo

Suponga que estos cifrados están configurados:

```
ssl cipher tlsv1.2 custom AES256-SHA256 AES128-SHA256 DHE-RSA-AES256-SHA256
```

Esta secuencia de eventos tiene lugar en este caso:

- AnyConnect establece un túnel principal y un túnel de datos TLS con AES256-SHA256 como cifrado SSL.
- DTLS está bloqueado en la ruta y no se puede establecer un túnel DTLS.
- ASA anuncia los parámetros a AnyConnect, que incluye los valores de MTU de TLS y DTLS, que son dos valores independientes.
- La MTU de DTLS es 1418 de forma predeterminada.
- La MTU de TLS se calcula a partir del valor tcpmss de sysopt conn (el valor predeterminado es 1380). Así es como se deriva la MTU de TLS (como se observa en el resultado de debug webvpn anyconnect):

```
1380 - 5 (TLS header) - 8 (CSTP) - 0 (padding) - 20 (HASH) = 1347
```

- AnyConnect activa el adaptador VPN y le asigna la MTU DTLS en previsión de que pueda conectarse a través de DTLS.
- El cliente AnyConnect ahora está conectado y el usuario va a un sitio web en particular.
- El navegador envía TCP SYN y establece MSS = 1418-40 = 1378 en él.
- El servidor HTTP en el interior del ASA envía paquetes del tamaño 1418.
- El ASA no puede colocarlos en el túnel y no puede fragmentarlos porque tienen configurado el bit Do not Fragment (DF).
- ASA imprime y descarta paquetes con el motivo de la caída mp-svc-no-fragment-ASP.

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

- Al mismo tiempo, ASA envía el mensaje ICMP Destination Unreachable, Fragmentation Needed (Destino inalcanzable, fragmentación necesaria) al 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 protocolo de mensajes de control de Internet (ICMP), el remitente retransmite los paquetes descartados y todo comienza a funcionar. Si el ICMP está bloqueado, el tráfico está agujereado en el ASA.
- Después de varias retransmisiones, entiende que el túnel DTLS no se puede establecer y necesita reasignar un nuevo valor de MTU al adaptador VPN.
- El propósito de esta reconexión es asignar una nueva MTU.

Para obtener más información sobre el comportamiento de reconexión y los temporizadores, consulte Preguntas frecuentes de AnyConnect: túneles, comportamiento de reconexión y el temporizador de inactividad

Información Relacionada

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).