Verhelpen van de doorstroming van het verkeer als gevolg van AnyConnect-verbindingen

Inhoud

Inleiding

In dit document wordt beschreven wat er gebeurt wanneer een AnyConnect-client binnen precies een minuut opnieuw verbinding maakt met de adaptieve security applicatie (ASA).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Verwante producten

Deze producten werden door dit probleem beïnvloed:

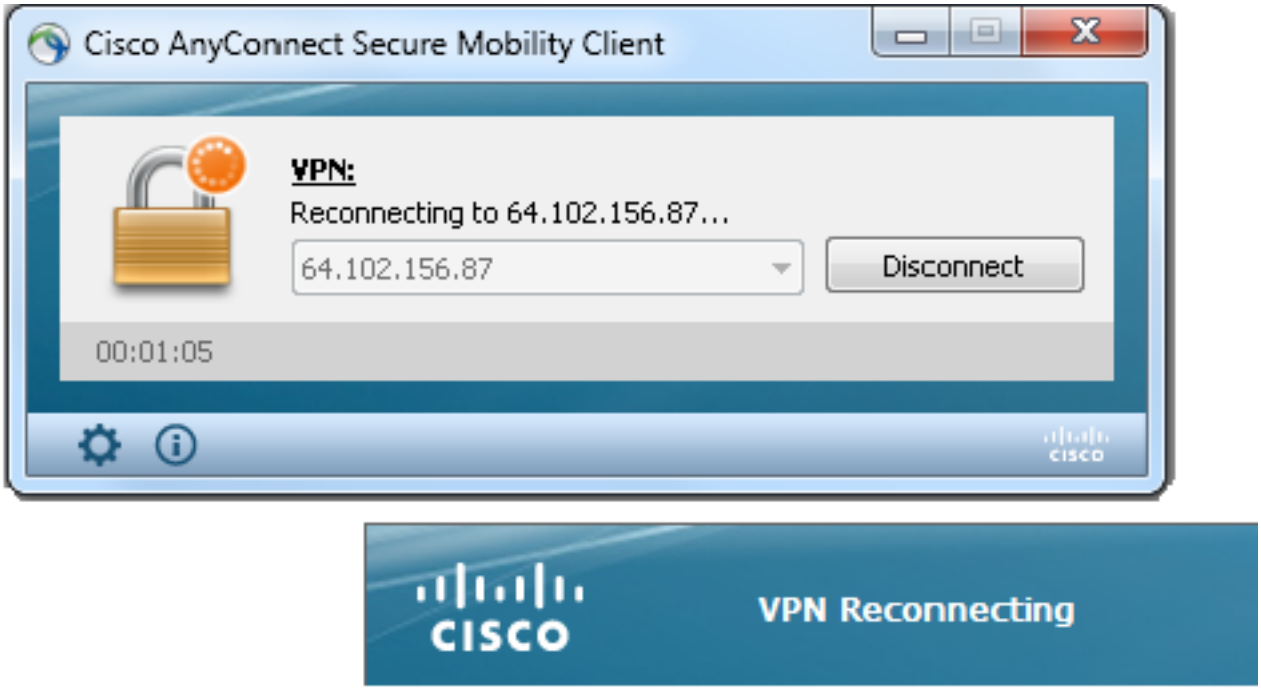
- ASA release 9.17
- AnyConnect-clientrelease 4.10

Achtergrondinformatie

Als AnyConnect-client binnen precies een minuut opnieuw verbinding maakt met de adaptieve security applicatie (ASA), kunnen gebruikers geen verkeer ontvangen via de TLS-tunnel (Transport Layer Security) totdat AnyConnect opnieuw verbinding maakt. Dat hangt af van een paar andere factoren die in dit document worden besproken.

Symptomen

In dit voorbeeld wordt de AnyConnect-client weergegeven wanneer deze opnieuw verbinding maakt met de ASA.



Deze syslog is te zien op de ASA:

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

Probleembeschrijving

Deze diagnostische en Reporting Gereedschapslogs (DART) worden met dit probleem gezien:

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

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.


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

Oorzaken

De oorzaak van dit probleem is het falen om een DTLS-tunnel (Datagram Transport Layer Security) te bouwen. Dit kan zijn om twee redenen:

- DTLS is ergens op het pad geblokkeerd
- Gebruik van een niet-standaard DTLS-poort

DTLS wordt ergens in het pad geblokkeerd

Sinds ASA release 9.x en AnyConnect release 4.x is er een optimalisatie geïntroduceerd in de vorm van verschillende Maximum Transition Units (MTU's) die voor TLS/DTLS worden onderhandeld tussen de client/ASA. Vroeger leidde de klant een ruwe schatting MTU af die zowel TLS/DTLS omvatte als duidelijk minder dan optimaal was. Nu, berekent ASA de inkapselingsoverheadkosten voor zowel TLS/DTLS en leidt dienovereenkomstig de waarden MTU af.

Zolang DTLS is ingeschakeld, past de client de DTLS MTU (in dit geval 1418) toe op de VPN-adapter (die is ingeschakeld voordat de DTLS-tunnel is geopend en die nodig is voor het afdwingen van routes/filters) om optimale prestaties te garanderen. Als de DTLS-tunnel niet kan worden ingesteld of op een bepaald moment wordt verbroken, reageert de client niet op TLS en past de MTU op de virtuele adapter (VA) aan de TLS MTU-waarde aan (hiervoor moet opnieuw worden verbonden op sessieniveau).

Resolutie

Om deze zichtbare overgang van DTLS > TLS te elimineren, kan de beheerder een afzonderlijke tunnelgroep configureren voor TLS-alleen-toegang voor gebruikers die problemen hebben met de instelling van de DTLS-tunnel (zoals vanwege firewallbeperkingen).

1. De beste optie is om de AnyConnect MTU-waarde lager in te stellen dan de TLS MTU, die vervolgens wordt onderhandeld.
   ```
   group-policy ac_users_group attributes
    webvpn
    anyconnect mtu 1300
   ```
   Dit maakt TLS en DTLS MTU waarden gelijk. In dit geval zijn geen reconnecties te zien.
2. De tweede optie is fragmentatie toe te staan.
   ```
   group-policy ac_users_group attributes
    webvpn
    anyconnect ssl df-bit-ignore enable
   ```
   Met fragmentatie kunnen grote pakketten (waarvan de grootte de MTU-waarde overschrijdt) worden gefragmenteerd en via de TLS-tunnel worden verzonden.
3. De derde optie is om de maximale segmentgrootte (MSS) in te stellen op 1460 zoals hier weergegeven:
   ```
   sysopt conn tcpmss 1460
   ```
   In dit geval kan TLS MTU 1427 (RC4/SHA1) zijn, wat groter is dan DTLS MTU 1418 (AES/SHA1/LZS). Hiermee lost u het probleem op met TCP van de ASA naar de AnyConnect-client (dankzij MSS), maar een groot UDP-verkeer van de ASA naar de AnyConnect-client kan hier last van hebben, omdat het kan worden gedropt door de AnyConnect-client als gevolg van de lagere AnyConnect-client MTU 1418. Als **sysopt-conn tcpms** wordt gewijzigd, kan dit invloed hebben op andere functies zoals LAN-to-LAN (L2L) IPSec VPN-tunnels.

Werkstroom opnieuw verbinden

Stel dat deze algoritmen zijn geconfigureerd:

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

Deze opeenvolging van gebeurtenissen vindt in dit geval plaats:

- AnyConnect maakt een oudertunnel en een TLS-gegevenstunnel met AES256-SHA256 als SSL-encryptie.
- DTLS is geblokkeerd in het pad en er kan geen DTLS-tunnel worden gemaakt.
- ASA kondigt parameters aan voor AnyConnect, die TLS- en DTLS MTU-waarden bevat, die twee afzonderlijke waarden zijn.
- DTLS MTU is standaard 1418.
- TLS MTU wordt berekend uit de **sysopt conn tcpms-**waarde (standaard is 1380). Dit is hoe de TLS MTU wordt afgeleid (zoals te zien is op de **debug webvpn anyconnect** uitvoer):

  ```
  1380 - 5 (TLS header) - 8 (CSTP) - 0 (padding) - 20 (HASH) = 1347
  ```
- AnyConnect brengt de VPN-adapter omhoog en wijst **DTLS** MTU eraan toe in afwachting van de verbinding via DTLS.
- De AnyConnect-client is nu verbonden en de gebruiker gaat naar een bepaalde website.

- De browser verstuurt TCP SYN en stelt MSS = 1418-40 = 1378 in.
- De HTTP-server binnen de ASA verstuurt pakketten met de grootte 1418.
- ASA kan hen niet in de tunnel zetten en kan hen niet fragmenteren aangezien zij geen Fragment (DF) beetjereeks hebben.
- ASA drukt pakketten af met mp-svc-no-fragment-ASP reden.

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

- Tezelfdertijd verzendt ASA Onbereikbare Bestemming ICMP, Vereiste Fragmentation naar de afzender:

  ```
  %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
  ```

- Als Internet Control Message Protocol (ICMP) is toegestaan, stuurt de afzender gedropte pakketten opnieuw over en begint alles te werken. Als ICMP is geblokkeerd, is er verkeer geblokkeerd via de ASA.
- Na verschillende herverzendingen begrijpt de Commissie dat de DTLS-tunnel niet kan worden opgezet en moet ze een nieuwe MTU-waarde aan de VPN-adapter toewijzen.
- Het doel van deze nieuwe verbinding is om een nieuwe MTU toe te wijzen.

Zie voor meer informatie over gedrag en timers bij opnieuw verbinden

Gerelateerde informatie

- Cisco technische ondersteuning en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.