Beheben von Störungen des Datenverkehrsflusses durch AnyConnect-Verbindungen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, was passiert, wenn ein AnyConnect-Client in genau einer Minute erneut eine Verbindung zur Adaptive Security Appliance (ASA) herstellt.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Verwandte Produkte

Diese Produkte wurden durch dieses Problem beeinflusst:

- ASA Version 9.17

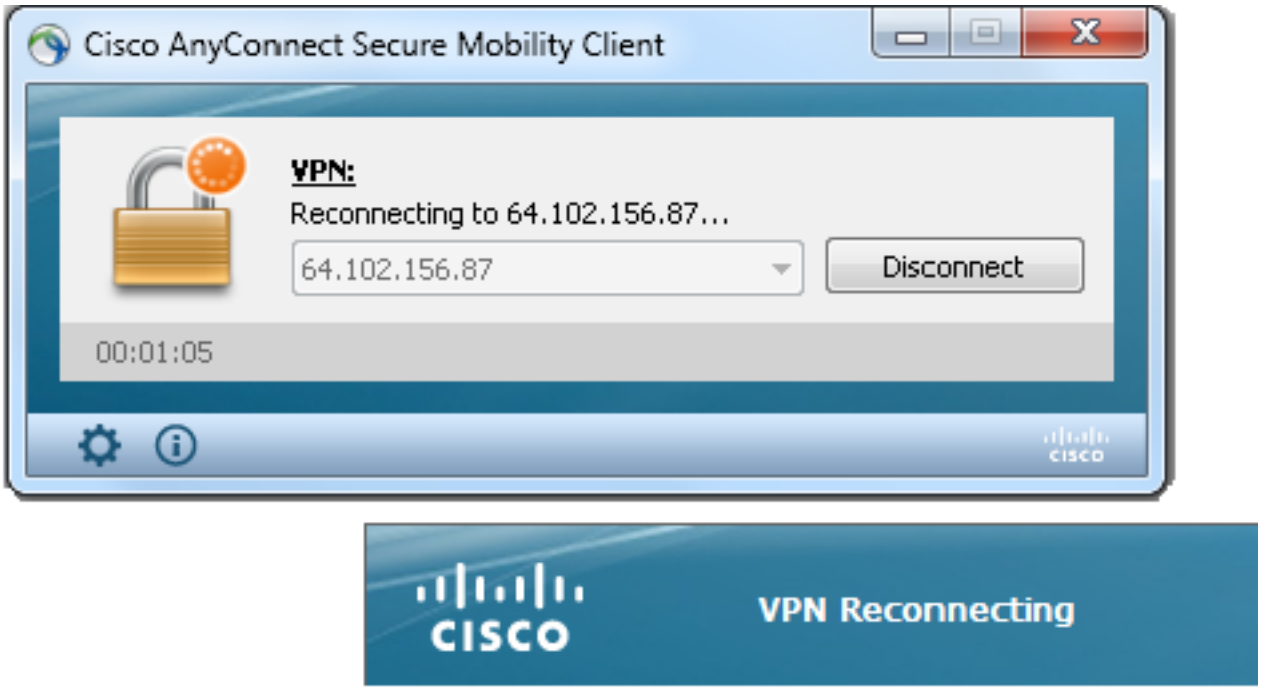
- AnyConnect-Client Version 4.10

Hintergrundinformationen

Wenn der AnyConnect-Client in genau einer Minute erneut eine Verbindung zur Adaptive Security Appliance (ASA) herstellt, können Benutzer erst wieder Datenverkehr über den TLS-Tunnel (Transport Layer Security) empfangen, wenn die Verbindung über AnyConnect wiederhergestellt ist. Dies hängt von einigen anderen Faktoren ab, die in diesem Dokument behandelt werden.

Symptome

In diesem Beispiel wird der AnyConnect-Client dargestellt, während er sich wieder mit der ASA verbindet.



Auf der ASA wird das folgende Syslog angezeigt:

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

Problembeschreibung

Diese Diagnose und Reporting Tool-Protokolle (DART) werden bei diesem Problem angezeigt:

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

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.


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

Ursachen

Die Ursache dieses Problems ist, dass kein Datagram Transport Layer Security (DTLS)-Tunnel erstellt wird. Dies kann zwei Gründe haben:

- DTLS ist irgendwo im Pfad blockiert
- Verwendung eines nicht standardmäßigen DTLS-Ports

DTLS ist irgendwo im Pfad blockiert

Seit ASA Version 9.x und AnyConnect Version 4.x wurde eine Optimierung in Form separater Maximum Transition Units (MTUs) eingeführt, die für TLS/DTLS zwischen dem Client/ASA ausgehandelt werden. Zuvor hatte der Client eine grobe MTU-Schätzung abgeleitet, die sowohl TLS als auch DTLS abdeckte und offensichtlich nicht optimal war. Nun berechnet ASA den Kapselungs-Overhead für TLS / DTLS und leitet die MTU-Werte entsprechend ab.

Solange DTLS aktiviert ist, wendet der Client die DTLS-MTU (in diesem Fall 1418) auf den VPN-Adapter an (der aktiviert ist, bevor der DTLS-Tunnel eingerichtet wird, und für die Durchsetzung von Routen / Filtern erforderlich ist), um eine optimale Leistung sicherzustellen. Wenn der DTLS-Tunnel an einem Punkt nicht hergestellt werden kann oder verworfen wird, führt der Client ein Failover auf TLS durch und passt die MTU auf dem virtuellen Adapter (VA) an den TLS-MTU-Wert an (hierfür ist eine erneute Verbindung auf Sitzungsebene erforderlich).

Auflösung

Um diesen sichtbaren Übergang von DTLS zu TLS zu vermeiden, kann der Administrator eine separate Tunnelgruppe für den reinen TLS-Zugriff für Benutzer konfigurieren, die Probleme mit der Einrichtung des DTLS-Tunnels haben (z. B. aufgrund von Firewall-Einschränkungen).

1. Die beste Option ist, den AnyConnect-MTU-Wert niedriger als die TLS-MTU festzulegen, die dann ausgehandelt wird.
   ```
   group-policy ac_users_group attributes
    webvpn
    anyconnect mtu 1300
   ```
   Dadurch sind die MTU-Werte von TLS und DTLS gleich. Erneute Verbindungen gibt es in diesem Fall nicht.
2. Die zweite Option ist die Ermöglichung von Fragmentierung.
   ```
   group-policy ac_users_group attributes
    webvpn
    anyconnect ssl df-bit-ignore enable
   ```
   Mit der Fragmentierung können große Pakete (deren Größe den MTU-Wert überschreitet) fragmentiert und durch den TLS-Tunnel gesendet werden.
3. Die dritte Option besteht darin, die maximale Segmentgröße (Maximum Segment Size, MSS) auf 1460 festzulegen, wie hier gezeigt:
   ```
   sysopt conn tcpmss 1460
   ```
   In diesem Fall kann die TLS-MTU 1427 (RC4/SHA1) betragen, was größer ist als die DTLS-MTU 1418 (AES/SHA1/LZS). Dadurch wird das Problem mit TCP von der ASA zum AnyConnect-Client (dank MSS) behoben, aber der große UDP-Datenverkehr von der ASA zum AnyConnect-Client kann darunter leiden, da er vom AnyConnect-Client aufgrund der niedrigeren MTU 1418 des AnyConnect-Clients verworfen werden kann. Wenn **sysopt conn tcpmss** geändert wird, kann dies andere Funktionen wie LAN-to-LAN (L2L) IPSec-VPN-Tunnel beeinträchtigen.

Workflow zum erneuten Verbinden

Angenommen, folgende Chiffren sind konfiguriert:

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

In diesem Fall laufen die folgenden Ereignisse ab:

- AnyConnect richtet einen übergeordneten Tunnel und einen TLS-Datentunnel mit AES256-SHA256 als SSL-Verschlüsselung ein.
- DTLS ist auf dem Pfad blockiert, und ein DTLS-Tunnel kann nicht eingerichtet werden.
- ASA teilt AnyConnect Parameter mit, einschließlich TLS- und DTLS-MTU-Werten (zwei separate Werte).
- DTLS-MTU ist standardmäßig 1418.
- Die TLS-MTU wird aus dem Wert **sysopt connect tcpmss berechnet (Standardwert ist 1380).** Die TLS-MTU wird folgendermaßen abgeleitet (wie aus der Ausgabe von **debug webvpn anyconnect ersichtlich):**

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

- AnyConnect aktiviert den VPN-Adapter und weist ihm eine **DTLS**-MTU zu, in Erwartung, dass eine Verbindung über DTLS hergestellt werden kann.
- Der AnyConnect-Client ist jetzt verbunden und der Benutzer besucht eine bestimmte Website.
- Der Browser sendet TCP SYN und setzt MSS = 1418-40 = 1378.
- Der HTTP-Server im Inneren der ASA sendet Pakete der Größe 1418.
- Die ASA kann sie nicht in den Tunnel einbinden und nicht fragmentieren, da für sie das DF-Bit (Do not Fragment) festgelegt ist.
- ASA druckt und verwirft Pakete aus dem Grund "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)
```

- Gleichzeitig sendet die ASA „ICMP Destination Unreachable, Fragmentation Needed“ an den Absender:

```
%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
```

- Wenn Internet Control Message Protocol (ICMP) erlaubt ist, überträgt der Absender verworfene Pakete erneut und alles funktioniert. Wenn ICMP blockiert wird, wird der Datenverkehr auf der ASA durch ein Blackhole unterbrochen.
- Nach mehreren erneuten Übertragungen erkennt die ASA, dass der DTLS-Tunnel nicht eingerichtet werden kann und dem VPN-Adapter ein neuer MTU-Wert zugewiesen werden muss.
- Der Zweck dieser erneuten Verbindung besteht darin, eine neue MTU zuzuweisen.

Weitere Informationen zum Verhalten bei erneuter Verbindung und zu Timern finden Sie unter

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.