Fix Traffic Flow Disruptions Caused by AnyConnect Reconnections

Contents

Introduction

This document describes what happens when an AnyConnect client reconnects to the Adaptive Security Appliance (ASA) in exactly one minute.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Related Products

These products were affected by this problem:

- ASA Release 9.17
- AnyConnect Client Release 4.10

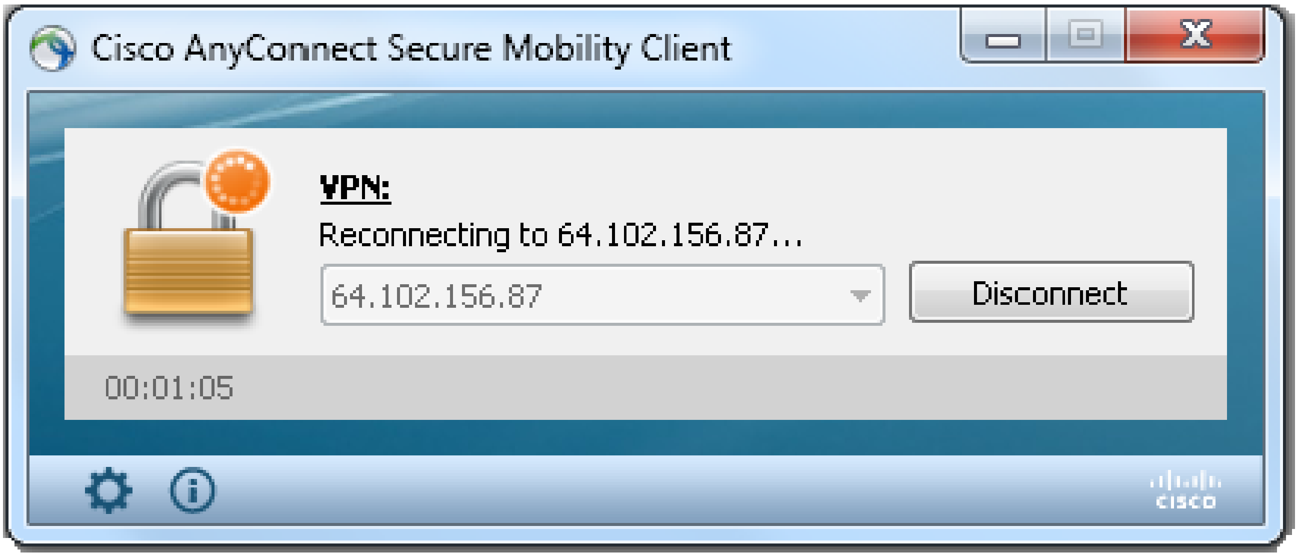
Background Information

Note: AnyConnect has been rebranded to Cisco Secure Client. Nothing else changed, just the name, and the installation process is the same.

If AnyConnect client reconnects to the Adaptive Security Appliance (ASA) in exactly one minute, users cannot receive traffic over the Transport Layer Security (TLS) tunnel until AnyConnect reconnects. This is dependent upon a few other factors which are discussed in this document.

Symptoms

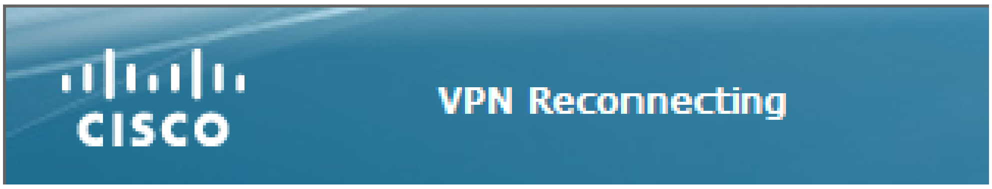
In this example, the AnyConnect client is shown as it reconnects to the ASA.



Reconnecting to 64.102.156.87...

64.102.156.87

00:01:05



VPN Reconnecting

This syslog is seen on the ASA:

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

Problem Description

These Diagnostics and Reporting Tool (DART) logs are seen with this issue:

<#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.




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

Causes

The cause of this issue is the failure to build a Datagram Transport Layer Security (DTLS) tunnel. This could be because of two reasons:

- DTLS is blocked somewhere in the path.
- Use of a non-default DTLS port.

DTLS is Blocked Somewhere in the Path

As of ASA Release 9.x and AnyConnect Release 4.x, an optimization has been introduced in the form of distinct Maximum Transition Units (MTUs) that are negotiated for TLS/DTLS between the client/ASA. Previously, the client derived a rough estimate MTU which covered both TLS/DTLS and was obviously less than optimal. Now, the ASA computes the encapsulation overhead for both TLS/DTLS and derives the MTU values accordingly.

As long as DTLS is enabled, the client applies the DTLS MTU (in this case 1418) on the VPN adapter (which is enabled before the DTLS tunnel is established and is needed for routes/filters enforcement), to ensure optimum performance. If the DTLS tunnel cannot be established or it is dropped at some point, the client fails over to TLS and adjusts the MTU on the virtual adapter (VA) to the TLS MTU value (this requires a session level reconnect).

Resolution

In order to eliminate this visible transition of **DTLS > TLS**, the administrator can configure a separate tunnel group for TLS only access for users that have trouble with the establishment of the DTLS tunnel (such as due to firewall restrictions).

1. The best option is to set the AnyConnect MTU value to be lower than the TLS MTU, which is then negotiated.

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

   This makes TLS and DTLS MTU values equal. Reconnections are not seen in this case.

2. The second option is to allow fragmentation.

   ```
   group-policy ac_users_group attributes
    webvpn
     anyconnect ssl df-bit-ignore enable
   ```

   With fragmentation, large packets (whose size exceeds the MTU value) can be fragmented and sent through the TLS tunnel.

3. The third option is to set the Maximum Segment Size (MSS) to 1460 shown here:

   ```
   sysopt conn tcpmss 1460
   ```

   In this case, the TLS MTU can be 1427 (RC4/SHA1) which is larger than the DTLS MTU 1418 (AES/SHA1/LZS). This resolves the issue with TCP from the ASA to the AnyConnect client (thanks to MSS), but large UDP traffic from the ASA to the AnyConnect client can suffer from this as it can be dropped by the AnyConnect client due to the lower AnyConnect client MTU 1418. If sysopt conn tcpmss is modified, it can affect other features such as LAN-to-LAN (L2L) IPSec VPN tunnels.

Reconnect Workflow

Suppose that these ciphers are configured:

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

This sequence of events takes place in this case:

- AnyConnect establishes a parent tunnel and a TLS data tunnel with AES256-SHA256 as the SSL encryption.

- DTLS is blocked in the path and a DTLS tunnel cannot be established.
- ASA announces parameters to AnyConnect, which includes TLS and DTLS MTU values, which are two separate values.
- DTLS MTU is 1418 by default.
- TLS MTU is calculated from the sysopt conn tcpmss value (default is 1380). This is how the TLS MTU is derived (as seen from the debug webvpn anyconnect output):

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

- AnyConnect brings the VPN adapter up and assigns DTLS MTU to it in anticipation that it can connect via DTLS.
- The AnyConnect client is now connected and the user goes to a particular website.
- The browser sends TCP SYN and sets MSS = 1418-40 = 1378 in it.
- The HTTP-server on the inside of the ASA sends packets of size 1418.
- The ASA cannot put them into the tunnel and cannot fragment them as they have Do not Fragment (DF) bit set.
- ASA prints and drops packets with mp-svc-no-fragment-ASP drop reason.

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

- At the same time, the ASA sends ICMP Destination Unreachable, Fragmentation Needed, to the sender:

```
%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
```

- If Internet Control Message Protocol (ICMP) is allowed, then the sender retransmits dropped packets and everything starts to work. If ICMP is blocked, then traffic is blackholed on the ASA.
- After several retransmits, it understands that the DTLS tunnel cannot be established and it needs to reassign a new MTU value to the VPN adapter.
- The purpose of this reconnect is to assign a new MTU.

For more information on reconnect behavior and timers, see AnyConnect FAQ: Tunnels, Reconnect Behavior, and the Inactivity Timer

Related Information

- Cisco Technical Support & Downloads