Corriger les interruptions de flux de trafic provoquées par les reconnexions AnyConnect

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés
- Produits connexes

Informations générales

Symptômes

Description du problème

Causes

- DTLS est bloqué quelque part sur le chemin
- Résolution

Reconnecter le workflow

Informations connexes

Introduction

Ce document décrit ce qui se passe lorsqu'un client AnyConnect se reconnecte à l'appliance de sécurité adaptatif (ASA) en exactement une minute.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

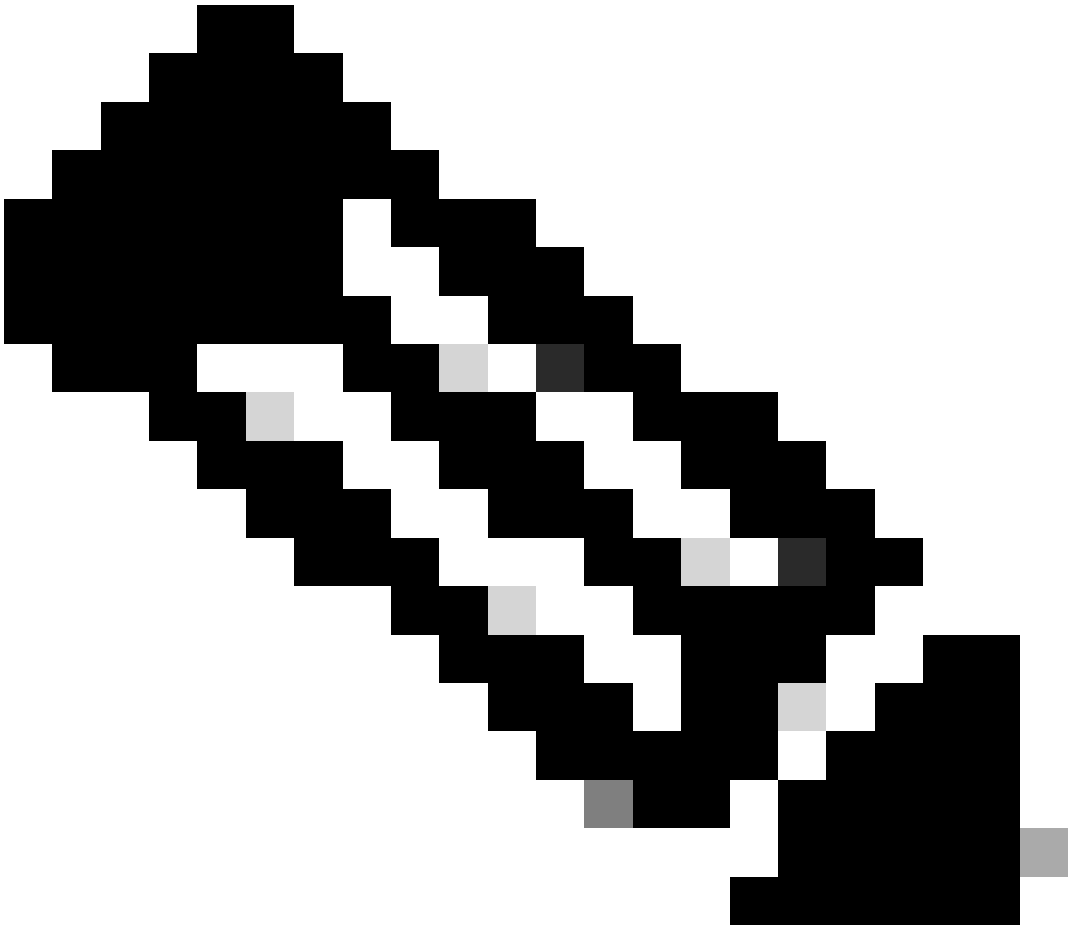
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Produits connexes

Ces produits ont été affectés par ce problème :

- ASA version 9.17
- Client AnyConnect version 4.10

Informations générales

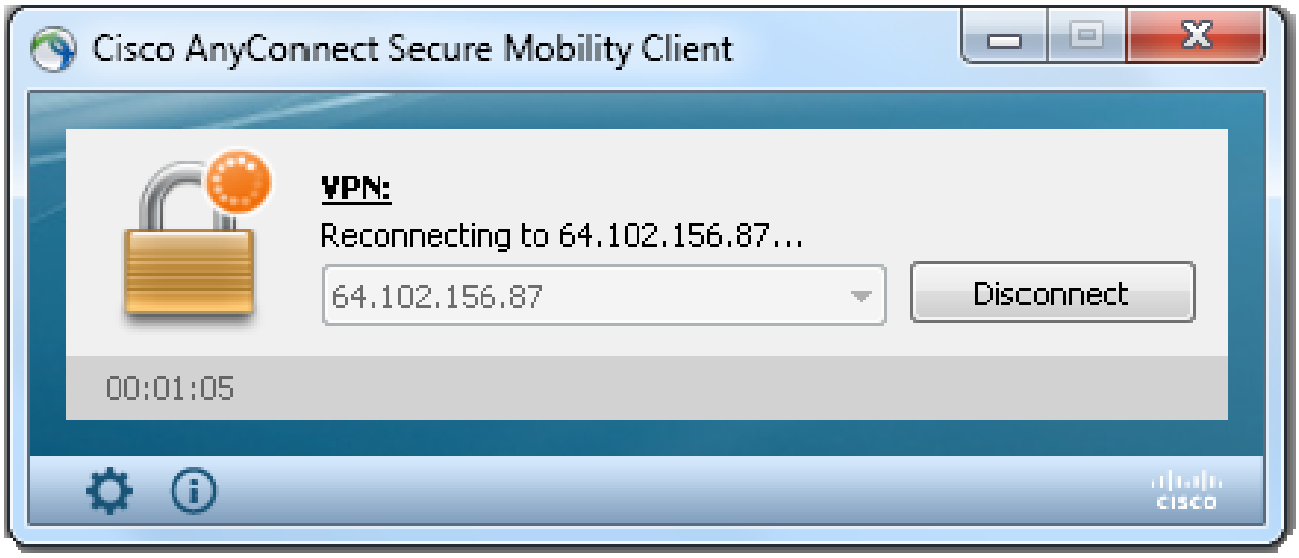


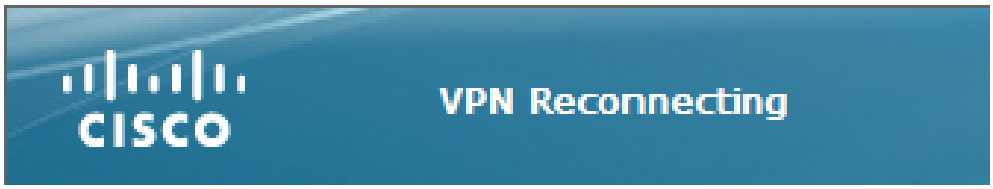
> Remarque : AnyConnect a été renommé Cisco Secure Client. Rien d'autre n'a changé, juste le nom, et le processus d'installation est le même.

Si le client AnyConnect se reconnecte à l'appareil de sécurité adaptatif (ASA) en exactement une minute, les utilisateurs ne peuvent pas recevoir de trafic sur le tunnel TLS (Transport Layer Security) tant qu'AnyConnect ne se reconnecte pas. Cela dépend de quelques autres facteurs qui sont discutés dans ce document.

Symptômes

Dans cet exemple, le client AnyConnect s'affiche lorsqu'il se reconnecte à l'ASA.





Ce syslog est visible sur l'ASA :

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

Description du problème

Les journaux DART (Diagnostics and Reporting Tool) suivants sont associés à ce problème :

<#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

La cause de ce problème est l'échec de la construction d'un tunnel DTLS (Datagram Transport Layer Security). Cela peut être dû à deux raisons :

- DTLS est bloqué quelque part sur le chemin.
- Utilisation d'un port DTLS autre que le port par défaut.

DTLS est bloqué quelque part sur le chemin

Depuis ASA version 9.x et AnyConnect version 4.x, une optimisation a été introduite sous la forme d'unités de transition maximales (MTU) distinctes négociées pour TLS/DTLS entre le client/ASA. Auparavant, le client avait calculé une MTU approximative qui couvrait à la fois les TLS et les DTLS et qui était manifestement moins qu'optimale. Maintenant, l'ASA calcule la surcharge d'encapsulation pour TLS/DTLS et dérive les valeurs MTU en conséquence.

Tant que DTLS est activé, le client applique la MTU DTLS (dans ce cas 1418) sur l'adaptateur VPN (qui est activé avant l'établissement du tunnel DTLS et est nécessaire pour l'application des routes/filtres), afin d'assurer des performances optimales. Si le tunnel DTLS ne peut pas être établi ou s'il est abandonné à un moment donné, le client bascule sur TLS et ajuste la MTU de la carte virtuelle (VA) à la valeur de MTU TLS (cela nécessite une reconnexion au niveau de la session).

Résolution

Afin d'éliminer cette transition visible de **DTLS > TLS**, l'administrateur peut configurer un groupe de tunnels séparé pour l'accès TLS uniquement pour les utilisateurs qui ont des problèmes avec l'établissement du tunnel DTLS (comme en raison des restrictions de pare-feu).

- La meilleure option consiste à définir la valeur de MTU AnyConnect sur une valeur inférieure à la MTU TLS, qui est ensuite négociée.

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

Les valeurs MTU TLS et DTLS sont donc égales. Les reconnexions ne sont pas visibles dans ce cas.

- La deuxième option consiste à autoriser la fragmentation.

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

Avec la fragmentation, les grands paquets (dont la taille dépasse la valeur MTU) peuvent être fragmentés et envoyés via le tunnel TLS.

- La troisième option consiste à définir la taille de segment maximale (MSS) sur 1460, comme indiqué ici :

```
sysopt conn tcpmss 1460
```

Dans ce cas, la MTU TLS peut être 1427 (RC4/SHA1), ce qui est supérieur à la MTU DTLS 1418 (AES/SHA1/LZS). Cela résout le problème avec TCP de l'ASA au client AnyConnect (grâce à MSS), mais un trafic UDP important de l'ASA au client AnyConnect peut en souffrir car il peut être abandonné par le client AnyConnect en raison de la MTU 1418 inférieure du client AnyConnect. Si sysopt conn tcpmss est modifié, il peut affecter d'autres fonctionnalités telles que les tunnels VPN IPSec LAN à LAN (L2L).

Reconnecter le workflow

Supposez que ces chiffrements sont configurés :

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

Cette séquence d'événements se déroule dans ce cas :

- AnyConnect établit un tunnel parent et un tunnel de données TLS avec AES256-SHA256 comme cryptage SSL.
- DTLS est bloqué dans le chemin et un tunnel DTLS ne peut pas être établi.
- ASA annonce des paramètres à AnyConnect, qui inclut les valeurs MTU TLS et DTLS, qui sont deux valeurs distinctes.
- DTLS MTU est 1418 par défaut.
- TLS MTU est calculé à partir de la valeur sysopt conn tcpmss (la valeur par défaut est 1380). Voici comment le MTU TLS est dérivé (comme vu à partir de la sortie debug webvpn anyconnect) :

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

- AnyConnect active l'adaptateur VPN et lui attribue le MTU DTLS en prévision de sa connexion via DTLS.
- Le client AnyConnect est maintenant connecté et l’utilisateur accède à un site Web particulier.
- Le navigateur envoie TCP SYN et définit MSS = 1418-40 = 1378.
- Le serveur HTTP à l'intérieur de l'ASA envoie des paquets de taille 1418.
- L'ASA ne peut pas les placer dans le tunnel et ne peut pas les fragmenter car ils ont le bit Ne pas fragmenter (DF) défini.
- ASA imprime et supprime les paquets avec la raison de suppression 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)

- En même temps, l'ASA envoie la destination ICMP inaccessible, fragmentation requise, à l'expéditeur :

```
%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 le protocole ICMP (Internet Control Message Protocol) est autorisé, l'expéditeur retransmet les paquets abandonnés et tout commence à fonctionner. Si ICMP est bloqué, le trafic est mis en trou noir sur l'ASA.

- Après plusieurs retransmissions, il comprend que le tunnel DTLS ne peut pas être établi et il doit réattribuer une nouvelle valeur MTU à l'adaptateur VPN.

- L'objectif de cette reconnexion est d'attribuer un nouveau MTU.

Pour plus d'informations sur le comportement et les minuteurs de reconnexion, consultez FAQ AnyConnect : Tunnels, Reconnect Behavior et Inactivity Timer

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.