Le client d'AnyConnect rebranche chaque minute qui entraîne une interruption dans la circulation

Contenu

Introduction

Ce document discute le scénario spécifique où le client d'AnyConnect pourrait rebrancher à l'appliance de sécurité adaptable (ASA) en exactement une minute. Les utilisateurs ne pourraient pas pouvoir recevoir le trafic au-dessus du tunnel de Transport Layer Security (TLS) jusqu'à ce qu'AnyConnect rebranche. Ce dépend de quelques autres facteurs qui sont discutés dans ce document.

Composants affectés

- Version 9.0 ou version 9.1 ASA
- Version 3.0 ou version 3.1 de client d'AnyConnect

Symptômes

Dans cet exemple, le client d'AnyConnect est affiché pendant qu'il rebranche à l'ASA.

Ce Syslog est vu 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

Ces logs de diagnostics et d'outil de génération de rapports (DART) sont vus avec cette question :

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

Date        : 11/16/2013
Time        : 01:28:50
Type        : Warning
Source      : acvpnagent

Description : Reconfigure reason code 16:
New MTU configuration.

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

Date        : 11/16/2013
Time        : 01:28:50
Type        : Information
Source      : acvpnagent

Description : The entire VPN connection is being reconfigured.

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

Date        : 11/16/2013
Time        : 01:28:51
Type        : Information
Source      : acvpnui

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

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

Date        : 11/16/2013
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 cette question est le manque de construire un tunnel du Transport Layer Security de datagramme (DTLS). Ceci a pu être pour deux raisons :

- DTLS est bloqué quelque part dans le chemin
- Utilisation d'un port du non-par défaut DTLS

DTLS est bloqué quelque part dans le chemin

En date de la version 9.x ASA et de la release 3.x d'AnyConnect, une optimisation a été introduite sous forme d'unités maximum distinctes de transition (mtu) qui sont négociées pour TLS/DTLS entre le client/ASA. Précédemment, le client a dérivé un MTU d'évaluation grossière qui a couvert les deux TLS/DTLS et était évidemment moins qu'optimal. Maintenant, l'ASA calcule le temps système d'encapsulation pour les deux TLS/DTLS et dérive les valeurs de MTU en conséquence.

Tant que DTLS est activé, le client applique le MTU DTLS (dans ce cas 1418) sur l'adaptateur VPN (qui est activé avant que le tunnel DTLS soit établi et soit nécessaire pour des artères/application de filtres), pour assurer la performance optimale. Si le tunnel DTLS ne peut pas être établi ou il est lâché à un certain point, le client bascule au TLS et ajuste le MTU sur l'adaptateur virtuel (VA) à la valeur de MTU de TLS (ceci exige un niveau de session rebranchent).

Résolution

Afin d'éliminer cette transition visible de DTLS > TLS, l'administrateur peuvent configurer un groupe distinct de tunnel pour l'accès de TLS seulement pour les utilisateurs qui ont des ennuis avec l'établissement du tunnel DTLS (tel qu'en raison des restrictions de Pare-feu).

1. La meilleure option est de placer la valeur de MTU d'AnyConnect pour être inférieure au MTU de TLS, qui est alors négocié.`group-policy ac_users_group attributes`
   `webvpn`
   `anyconnect mtu 1300` Ceci rend le TLS et les valeurs de MTU DTLS égaux. Des reconnexions ne sont pas vues dans ce cas.
2. La deuxième option est de permettre la fragmentation. `group-policy ac_users_group attributes`
   `webvpn`
   `anyconnect ssl df-bit-ignore enable`Avec la fragmentation, de grands paquets (dont la taille dépasse la valeur de MTU) peuvent être fragmentés et envoyés par le TLS percent un tunnel.
3. La troisième option est de placer la taille maximum de segment (MSS) à 1460 comme suit :`sysopt conn tcpmss 1460` Dans ce cas, le MTU de TLS sera 1427 (RC4/SHA1) qui est plus grand que le MTU 1418 (AES/SHA1/LZS) DTLS. Ceci devrait résoudre le problème avec le TCP de l'ASA au client d'AnyConnect (grâce à MSS), mais le grand trafic UDP de l'ASA au client d'AnyConnect pourrait souffrir de ceci car il sera abandonné par le client d'AnyConnect dû au MTU inférieur 1418 de client d'AnyConnect. Si des **tcpmss conn. de sysopt** est modifiés, il pourrait affecter d'autres caractéristiques telles que des tunnels VPN d'IPSec de l'entre réseaux locaux (L2L).

Utilisation d'un port du Non-par défaut DTLS

Une autre cause potentielle pour la panne DTLS active DTLS sur un port de non-par défaut après que le webvpn soit activé (par exemple, quand le **webvpn enable en dehors de la** commande est entré). C'est dû à l'ID de bogue Cisco CSCuh61321 et a été vu dans la release 9.x où l'ASA pousse le port de non-par défaut au client, mais continue à écouter le port par défaut. En conséquence, le DTLS n'est pas construit et AnyConnect rebranche.

```
webvpn
 port 444
 enable outside
```

```
 dtls port 444
 anyconnect enable

ciscoasa(config-webvpn)# show asp table socket


Protocol  Socket    State      Local Address             Foreign Address
SSL       0001fc08  LISTEN     172.16.11.1:444           0.0.0.0:*

DTLS      00020dc8  LISTEN     172.16.11.1:443           0.0.0.0:*
```

Après que le tunnel de TLS soit établi, les tentatives de client d'établir le tunnel DTLS au port 444 comme prévus :

La commande des commandes qui mènent au problème et aux sockets accélérés de table de chemin de Sécurité (ASP) ouverts est :

1. Début avec les sockets de webvpn non activés.
```
ciscoasa(config)# show run webvpn
webvpn
 anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
 anyconnect enable


ciscoasa(config)# show asp table socket
Protocol  Socket    State      Local Address             Foreign Address
ciscoasa(config)#
```
2. Le TLS de modification met en communication à 444 et active le webvpn.
```
ciscoasa(config-webvpn)# show run webvpn
webvpn
 port 444
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
 anyconnect enable


ciscoasa(config-webvpn)# show asp tabl socket
Protocol  Socket    State      Local Address             Foreign Address
SSL       0001fc08  LISTEN     172.16.11.1:444           0.0.0.0:*
DTLS      00020dc8  LISTEN     172.16.11.1:443           0.0.0.0:*
```
3. Changez le port DTLS à 444.
```
ciscoasa(config-webvpn)# dtls port 444
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# show run webvpn
webvpn
 port 444
 enable outside
 dtls port 444
 anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
 anyconnect enable

ciscoasa(config-webvpn)# show asp table socket


Protocol  Socket    State      Local Address             Foreign Address
SSL       0001fc08  LISTEN     172.16.11.1:444           0.0.0.0:*
DTLS      00020dc8  LISTEN     172.16.11.1:443           0.0.0.0:*
```

   Remarque: Le port de socket DTLS est toujours 443. En ce moment les clients d'AnyConnect établissent DTLS à 444 cependant !

Résolution

Le contournement pour ce problème est de suivre la commande de :

1. Désactivez le webvpn.
2. Entrez dans le port DTLS.
3. Activez le webvpn.

Ce comportement n'existe pas dans des versions de la release 8.4.x, où les sockets DTLS obtiennent mis à jour avec les ports configurés juste après que la configuration est écrite :

Version 8.4.6 ASA :

```
ciscoasa(config-webvpn)# port 444
ciscoasa(config-webvpn)# enable outside
ciscoasa(config-webvpn)# show asp table socket

Protocol Socket Local Address Foreign Address State
SSL 0000bf2f 172.16.11.1:444 0.0.0.0:* LISTEN
DTLS 0000d5df 172.16.11.1:443 0.0.0.0:* LISTEN

ciscoasa(config-webvpn)# dtls port 444
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# show asp table socket

Protocol Socket Local Address Foreign Address State
SSL 0000bf2f 172.16.11.1:444 0.0.0.0:* LISTEN
DTLS 0000eb5f 172.16.11.1:444 0.0.0.0:* LISTEN << changed immediately
```

Rebranchez le processus

Supposez que ces chiffrements sont configurés :

```
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1
```

Cette séquence d'opérations a lieu dans ce cas :

- AnyConnect établit un tunnel de parent et un tunnel de données de TLS avec RC4-SHA comme ssl encryption.
- DTLS est bloqué dans le chemin et un tunnel DTLS ne peut pas être établi.
- L'ASA annonce des paramètres à AnyConnect, qui inclut le TLS et les valeurs de MTU DTLS, qui sont deux valeurs distinctes.
- Le MTU DTLS est 1418 par défaut.
- Le MTU de TLS est calculé à partir de la valeur de **tcpmss conn. de sysopt** (le par défaut est 1380). C'est comment le MTU de TLS est dérivé (comme vu de l'**anyconnect de debug webvpn** sorti) :
  `1380 - 5 (TLS header) - 8 (CSTP) - 0 (padding) - 20 (HASH) = 1347`
- AnyConnect apporte l'adaptateur VPN et lui assigne le MTU **DTLS** d'avance qu'il pourra se connecter par l'intermédiaire de DTLS.
- Le client d'AnyConnect est maintenant connecté et l'utilisateur va à un site Web particulier.
- Le navigateur envoie la synchronisation de TCP et place MSS = 1418-40 = 1378 dans lui.
- Le serveur HTTP sur l'intérieur de l'ASA envoie des paquets de la taille 1418.
- L'ASA ne peut pas les mettre dans le tunnel et ne peut pas les fragmenter car ils font placer le bit du Don't Fragment (DF).
- Copies ASA`%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111> Transmitting large packet 1418 (threshold 1347)`et paquets de baisses avec la raison de

baisse de MP-svc-aucun-fragment-ASP.

- En même temps l'ASA envoie la destination ICMP inaccessible, fragmentation requise 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 on permet le Protocole ICMP (Internet Control Message Protocol), alors l'expéditeur retransmet les paquets lâchés et tout des débuts pour fonctionner. Si l'ICMP est bloqué, alors le trafic blackholed sur l'ASA.
- Après que plusieurs les retransmette il comprend que le tunnel DTLS ne peut pas être établi et il doit réaffecter une nouvelle valeur de MTU à l'adaptateur VPN.
- Le but de ceci rebranchent est d'assigner un nouveau MTU.

Pour plus d'informations sur rebranchez le comportement et les temporisateurs, voient la Foire aux questions d'AnyConnect : Les tunnels, rebranchent le comportement, et le temporisateur d'inactivité

Mises en garde

Le courant alternatif 3.1:ASA de l'ID de bogue Cisco CSCuh61321 manipule inexactement le port alternatif DTLS, des causes rebranchent

Informations connexes

- Foire aux questions d'AnyConnect : Les tunnels, rebranchent le comportement, et le temporisateur d'inactivité
- Support et documentation techniques - Cisco Systems