Question ASA 8.3 : MSS dépassés - Les clients de HTTP ne peuvent pas parcourir à quelques sites Web

Contenu

Introduction

Ce document décrit une question qui se produit quand quelques sites Web ne sont pas accessibles par une appliance de sécurité adaptable (ASA) ce logiciel de version 8.3 ou ultérieures de passages.

La release ASA 7.0 introduit plusieurs nouvelles améliorations de la sécurité, l'un d'entre eux est des points finaux de TCP d'un vérifier qui adhèrent à la taille maximum annoncée de segment (MSS). Dans une session TCP normale, le client envoie un paquet SYN au serveur, avec la valeur MSS incluse dans les options TCP du paquet SYN. Le serveur, dès réception du paquet SYN, devrait identifier la valeur MSS envoyée par le client, puis envoyer sa propre valeur MSS dans le paquet SYN-ACK. Une fois que le client et le serveur sont tous deux informés de la valeur MSS de chacun, ni l'un ni l'autre pair ne devrait envoyer à l'autre un paquet plus grand que le MSS de ce pair.

Il a été observé que certains serveurs HTTP sur Internet ne respectent pas la valeur MSS publiée par le client. Le serveur HTTP envoie donc au client des paquets de données qui sont plus grands que la valeur MSS publiée. Avant version 7.0, on a permis ces paquets par l'ASA. Avec les améliorations de la sécurité incluses dans la version logicielle 7.0, ces paquets sont lâchés par défaut. Ce document est conçu pour aider l'administrateur d'appliance de sécurité adaptable Cisco dans le diagnostic de ce problème et l'implémentation d'un contournement pour permettre les paquets qui dépassent le MSS.

Référez-vous à la question PIX/ASA 7.X : MSS dépassés - Les clients de HTTP ne peuvent pas

parcourir à quelques sites Web pour la même configuration sur l'appliance de sécurité adaptable Cisco (ASA) avec des versions 8.2 et antérieures.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur une appliance de sécurité adaptable Cisco (ASA) ce logiciel de version 8.3 de passages.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Référez-vous au Conventions relatives aux conseils techniques Cisco pour les informations sur des conventions de document.

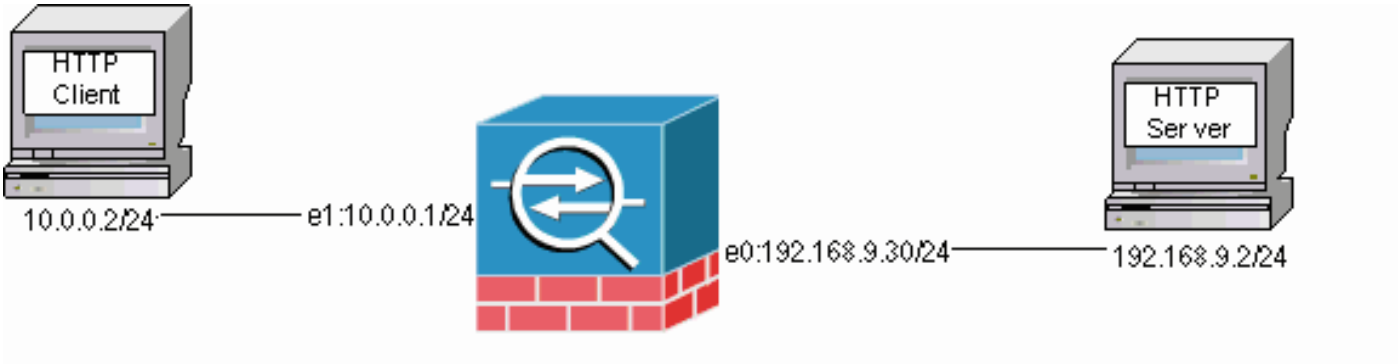
Configurez

Cette section vous présente les informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez le Command Lookup Tool (clients enregistrés seulement) pour trouver les informations complémentaires sur les commandes des utilisations de ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration ASA 8.3

Ces commandes de configuration sont ajoutées à une configuration par défaut ASA 8.3 afin de permettre au client de HTTP pour communiquer avec le serveur HTTP.

Configuration ASA 8.3
ASA(config)#**interface Ethernet0** ASA(config-if)#**speed 100** ASA(config-if)#**duplex full** ASA(config-if)#**nameif outside** ASA(config-if)#**security-level 0** ASA(config-if)#**ip address 192.168.9.30 255.255.255.0** ASA(config-if)#**exit** ASA(config)#**interface Ethernet1** ASA(config-if)#**speed 100** ASA(config-if)#**duplex full** ASA(config-if)#**nameif inside** ASA(config-if)#**security-level 100** ASA(config-if)#**ip address 10.0.0.1 255.255.255.0** ASA(config-if)#**exit** ASA(config)#**object network Inside-Network** ASA(config-obj)#**subnet 10.0.0.0 255.0.0.0** ASA(config)#**nat (inside,outside) source dynamic Inside-Network interface** ASA(config)#**route outside 0.0.0.0 0.0.0.0 192.168.9.2 1**

Dépannez

Si un site Web particulier n'est pas accessible par l'ASA, terminez-vous ces étapes pour dépanner. Vous le premier besoin de capturer les paquets de la connexion HTTP. Afin de collecter les paquets, les adresses IP appropriées du serveur HTTP et le client doivent être connus, aussi bien que l'adresse IP que le client est traduit à quand elle traverse l'ASA.

Dans le réseau d'exemple, le serveur HTTP est adressé chez 192.168.9.2, le client de HTTP est adressé chez 10.0.0.2, et les adresses du client de HTTP est traduites à 192.168.9.30 pendant que les paquets partent de l'interface extérieure. Vous pouvez employer la caractéristique de capture de l'appliance de sécurité adaptable Cisco (ASA) afin de collecter les paquets, ou vous pouvez utiliser une capture externe de paquet. Si vous avez l'intention d'utiliser la caractéristique de capture, l'administrateur peut également utiliser une nouvelle caractéristique de capture incluse dans la release 7.0 qui permet à l'administrateur pour capturer les paquets qui sont dus lâché à une anomalie de TCP.

Remarque: Certaines des commandes dans le bouclage de ces tables à une deuxième ligne due aux restrictions spatiales.

1. Définissez une paire de Listes d'accès qui identifient les paquets en tant qu'elles d'entrée et de sortie l'extérieur et les interfaces internes.
2. Activez la caractéristique de capture pour chacun des deux l'interface interne et externe. Activez également la capture pour les paquets MSS-dépassés parparticularité.
3. Effacez les compteurs accélérés de chemin de Sécurité (ASP) sur l'ASA.
4. Activez le déroutement syslogging au niveau de débogage envoyé à un hôte sur le réseau.
5. Initiez une session de HTTP du client de HTTP au serveur HTTP problématique, et collectez la sortie de Syslog et la sortie de ces commandes après que la connexion échoue.**show capture capture-à l'intérieur decapture-extérieur de show capturemss-capture de show captureaffichez la baisse d'aspRemarque:** Référez-vous au message du journal système 419001 pour plus d'informations sur ce message d'erreur.

Contournement

Implémentez un contournement maintenant que vous savez que l'ASA relâche les paquets qui

dépassent la valeur MSS annoncée par le client. Maintenez dans l'esprit que vous ne pourriez pas vouloir permettre à ces paquets pour atteindre le client en raison d'une mémoire tampon potentielle débordée sur le client. Si vous choisissez de permettre ces paquets par l'ASA, procédez à cette procédure de contournement.

Le cadre de stratégie modulaire (MPF) est une nouvelle caractéristique dans la release 7.0 qui est utilisée pour permettre ces paquets par l'ASA. Ce document n'est pas conçu pour détailler entièrement le MPF mais suggère plutôt les entités de configuration utilisées pour fonctionner autour du problème. Référez-vous au guide de configuration ASA 8.3 et au manuel de référence des commandes ASA 8.3 pour plus d'informations sur MPF et commandes l'unes des répertoriés dans cette section.

Un aperçu au contournement inclut l'identification du client et serveur de HTTP par l'intermédiaire d'une liste d'accès. Une fois que la liste d'accès est définie, un class map est créé et la liste d'accès est assignée au class map. Alors une carte de TCP est configurée et l'option de permettre les paquets qui dépassent le MSS est activée. Une fois que la carte et le class map de TCP sont définis, vous pouvez les ajouter à une carte de nouvelle ou existante stratégie. Une carte de stratégie est alors assignée à une stratégie de sécurité. Utilisez la commande de service-**stratégie** dans le mode de configuration de lancer une carte de stratégie globalement ou sur une interface. Ces paramètres de configuration sont ajoutés à l'appliance de sécurité adaptable Cisco (ASA) liste de 8.3 configurations. Après que vous créiez une carte de stratégie nommée "http-map1," cette configuration d'échantillon ajoute le class map à cette carte de stratégie.

Interface spécifique : Configuration MPF pour permettre les paquets qui dépassent MSS
ASA(config)#**access-list http-list2 permit tcp any host 192.168.9.2** ASA(config)# ASA#**configure terminal** ASA(config)# ASA(config)#**class-map http-map1** ASA(config-cmap)#**match access-list http-list2** ASA(config-cmap)#**exit** ASA(config)#**tcp-map mss-map** ASA(config-tcp-map)#**exceed-mss allow** ASA(config-tcp-map)#**exit** ASA(config)#**policy-map http-map1** ASA(config-pmap)#**class http-map1** ASA(config-pmap-c)#**set connection advanced-options mss-map** ASA(config-pmap-c)#**exit** ASA(config-pmap)#**exit** ASA(config)#**service-policy http-map1 interface outside** ASA#

Une fois que ces paramètres de configuration sont en place, on permet des paquets de 192.168.9.2 qui dépassent le MSS annoncé par le client par l'ASA. Il est important de noter que la liste d'accès utilisée dans le class map est conçue pour identifier le trafic sortant à 192.168.9.2. Le trafic sortant est examiné pour permettre à l'engine d'inspection pour extraire le MSS du paquet sortant de synchronisation. Par conséquent, il est impératif de configurer la liste d'accès avec la direction de la synchronisation à l'esprit. Si une règle plus dominante est exigée, vous pouvez remplacer l'**instruction de liste d'accès** dans cette section par une **instruction de liste d'accès** qui laisse tout, tel que l'**IP d'autorisation de la liste d'accès http-list2 tout** ou le **TCP d'autorisation de la liste d'accès http-list2 tout**. Souvenez-vous également que le tunnel VPN peut être lent si une grande valeur de TCP MSS est utilisée. Vous pouvez réduire le TCP MSS pour améliorer les performances.

Cet exemple aide à configurer globalement le trafic en entrée et en sortie dans l'ASA :

Configuration globale : Configuration MPF pour permettre les paquets qui dépassent MSS
ASA(config)#**access-list http-list2 permit tcp any host**

```
192.168.9.2 ASA(config)# ASA#configure terminal
ASA(config)# ASA(config)#class-map http-map1 ASA(config-
cmap)#match any ASA(config-cmap)#exit ASA(config)#tcp-
map mss-map ASA(config-tcp-map)#exceed-mss allow
ASA(config-tcp-map)#exit ASA(config)#policy-map http-
map1 ASA(config-pmap)#class http-map1 ASA(config-pmap-
c)#set connection advanced-options mss-map ASA(config-
pmap-c)#exit ASA(config-pmap)#exit ASA(config)#service-
policy http-map1 global ASA#
```

Vérifiez

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

Répétez les étapes dans la section de dépannage afin de vérifier que les modifications de configuration font ce qu'elles sont conçues pour faire.

Syslog d'une connexion réussie

```
%ASA-6-609001: Built local-host inside:10.0.0.2
%ASA-6-609001: Built local-host outside:192.168.9.2
%ASA-6-305011: Built dynamic TCP translation from
inside:10.0.0.2/58798
               to outside:192.168.9.30/1025
%ASA-6-302013: Built outbound TCP connection 13 for
outside:192.168.9.2/80
               (192.168.9.2/80) to inside:10.0.0.2/58798
(192.168.9.30/1025)
%ASA-5-304001: 10.0.0.2 Accessed URL 192.168.9.2:/

%ASA-6-302014: Teardown TCP connection 13 for
outside:192.168.9.2/80 to
               inside:10.0.0.2/58798 duration 0:00:01
bytes 6938 TCP FINs

!--- The connection is built and immediately !--- torn
down when the web content is retrieved.
```

Sortie des commandes show d'une connexion réussie

```
ASA#
ASA#show capture capture-inside 21 packets captured 1:
09:16:50.972392 10.0.0.2.58769 > 192.168.9.2.80: S
751781751:751781751(0) win 1840 <mss
460,sackOK,timestamp 110313116 0,nop,wscale 0> !--- The
advertised MSS of the client is 460 in packet #1.
However, !--- with th workaround in place, packets 7, 9,
11, 13, and 15 appear !--- on the inside trace, despite
the MSS>460. 2: 09:16:51.098536 192.168.9.2.80 >
10.0.0.2.58769: S 1305880751:1305880751(0) ack 751781752
win 8192 <mss 1380> 3: 09:16:51.098734 10.0.0.2.58769 >
192.168.9.2.80: . ack 1305880752 win 1840 4:
09:16:51.099009 10.0.0.2.58769 > 192.168.9.2.80: P
751781752:751781851(99) ack 1305880752 win 1840 5:
09:16:51.228412 192.168.9.2.80 > 10.0.0.2.58769: . ack
751781851 win 8192 6: 09:16:51.228641 192.168.9.2.80 >
10.0.0.2.58769: . ack 751781851 win 25840 7:
09:16:51.236254 192.168.9.2.80 > 10.0.0.2.58769: .
1305880752:1305882112(1360) ack 751781851 win 25840 8:
09:16:51.237704 10.0.0.2.58769 > 192.168.9.2.80: . ack
1305882112 win 4080 9: 09:16:51.243593 192.168.9.2.80 >
```

10.0.0.2.58769: P 1305882112:1305883472(**1360**) ack 751781851 win 25840 10: 09:16:51.243990 10.0.0.2.58769 > 192.168.9.2.80: . ack 1305883472 win 6800 11: 09:16:51.251009 192.168.9.2.80 > 10.0.0.2.58769: . 1305883472:1305884832(**1360**) ack 751781851 win 25840 12: 09:16:51.252428 10.0.0.2.58769 > 192.168.9.2.80: . ack 1305884832 win 9520 13: 09:16:51.258440 192.168.9.2.80 > 10.0.0.2.58769: P 1305884832:1305886192(**1360**) ack 751781851 win 25840 14: 09:16:51.258806 10.0.0.2.58769 > 192.168.9.2.80: . ack 1305886192 win 12240 15: 09:16:51.266130 192.168.9.2.80 > 10.0.0.2.58769: . 1305886192:1305887552(**1360**) ack 751781851 win 25840 16: 09:16:51.266145 192.168.9.2.80 > 10.0.0.2.58769: P 1305887552:1305887593(41) ack 751781851 win 25840 17: 09:16:51.266511 10.0.0.2.58769 > 192.168.9.2.80: . ack 1305887552 win 14960 18: 09:16:51.266542 10.0.0.2.58769 > 192.168.9.2.80: . ack 1305887593 win 14960 19: 09:16:51.267320 10.0.0.2.58769 > 192.168.9.2.80: F 751781851:751781851(0) ack 1305887593 win 14960 20: 09:16:51.411370 192.168.9.2.80 > 10.0.0.2.58769: F 1305887593:1305887593(0) ack 751781852 win 8192 21: 09:16:51.411554 10.0.0.2.58769 > 192.168.9.2.80: . ack 1305887594 win 14960 21 packets shown ASA# ASA# ASA#**show capture capture-outside** 21 packets captured 1: 09:16:50.972834 192.168.9.30.1024 > 192.168.9.2.80: S 1465558595:1465558595(0) win 1840 <mss 460,sackOK,timestamp 110313116 0,nop,wscale 0> 2: 09:16:51.098505 192.168.9.2.80 > 192.168.9.30.1024: S 466908058:466908058(0) ack 1465558596 win 8192 <mss 1460> 3: 09:16:51.098749 192.168.9.30.1024 > 192.168.9.2.80: . ack 466908059 win 1840 4: 09:16:51.099070 192.168.9.30.1024 > 192.168.9.2.80: P 1465558596:1465558695(99) ack 466908059 win 1840 5: 09:16:51.228397 192.168.9.2.80 > 192.168.9.30.1024: . ack 1465558695 win 8192 6: 09:16:51.228625 192.168.9.2.80 > 192.168.9.30.1024: . ack 1465558695 win 25840 7: 09:16:51.236224 192.168.9.2.80 > 192.168.9.30.1024: . 466908059:466909419(**1360** ack 1465558695 win 25840 8: 09:16:51.237719 192.168.9.30.1024 > 192.168.9.2.80: . ack 466909419 win 4080 9: 09:16:51.243578 192.168.9.2.80 > 192.168.9.30.1024: P 466909419:466910779(**1360**) ack 1465558695 win 25840 10: 09:16:51.244005 192.168.9.30.1024 > 192.168.9.2.80: . ack 466910779 win 6800 11: 09:16:51.250978 192.168.9.2.80 > 192.168.9.30.1024: . 466910779:466912139(**1360**) ack 1465558695 win 25840 12: 09:16:51.252443 192.168.9.30.1024 > 192.168.9.2.80: . ack 466912139 win 9520 13: 09:16:51.258424 192.168.9.2.80 > 192.168.9.30.1024: P 466912139:466913499(**1360**) ack 1465558695 win 25840 14: 09:16:51.258485 192.168.9.2.80 > 192.168.9.30.1024: P 466914859:466914900(41) ack 1465558695 win 25840 15: 09:16:51.258821 192.168.9.30.1024 > 192.168.9.2.80: . ack 466913499 win 12240 16: 09:16:51.266099 192.168.9.2.80 > 192.168.9.30.1024: . 466913499:466914859(**1360**) ack 1465558695 win 25840 17: 09:16:51.266526 192.168.9.30.1024 > 192.168.9.2.80: . ack 466914859 win 14960 18: 09:16:51.266557 192.168.9.30.1024 > 192.168.9.2.80: . ack 466914900 win 14960 19: 09:16:51.267335 192.168.9.30.1024 > 192.168.9.2.80: F 1465558695:1465558695(0) ack 466914900 win 14960 20: 09:16:51.411340 192.168.9.2.80 > 192.168.9.30.1024: F 466914900:466914900(0) ack 1465558696 win 8192 21:

```
09:16:51.411569 192.168.9.30.1024 > 192.168.9.2.80: .
ack 466914901 win 14960 21 packets shown ASA#
ASA(config)#show capture mss-capture 0 packets captured
0 packets shown ASA# ASA#show asp drop Frame drop: Flow
drop: ASA# !--- Both the show capture mss-capture and
the show asp drop !--- commands reveal that no packets
are dropped.
```

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Notes de terrain relatives aux produits de sécurité (appliance de sécurité adaptable Cisco y compris (ASA))
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems