Problème ASA 8.3 : MSS dépassé - Les clients HTTP ne peuvent pas accéder à certains sites Web

Contenu

Introduction

Ce document décrit un problème qui se produit lorsque certains sites Web ne sont pas accessibles via un appareil de sécurité adaptatif (ASA) qui exécute la version 8.3 ou ultérieure du logiciel.

La version ASA 7.0 introduit plusieurs nouvelles améliorations en matière de sécurité, dont l'une consiste à vérifier les points de terminaison TCP qui respectent la taille maximale de segment (MSS) annoncée. 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 la version 7.0, ces paquets étaient autorisés via 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 du dispositif de sécurité adaptatif Cisco à diagnostiquer ce problème et à mettre en oeuvre une solution de contournement permettant les paquets qui dépassent le MSS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur un dispositif de sécurité adaptatif (ASA) Cisco qui exécute le logiciel version 8.3.

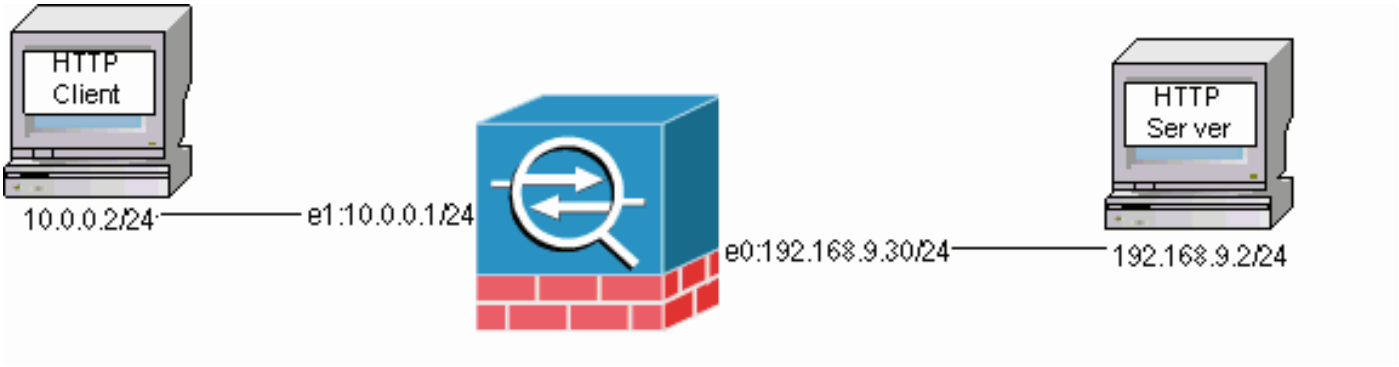
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Cette section vous présente les informations pour configurer les fonctionnalités décrites dans 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 HTTP de 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
```

Dépannage

Si un site Web particulier n'est pas accessible via l'ASA, procédez comme suit pour résoudre les problèmes. Vous devez d'abord capturer les paquets à partir de la connexion HTTP. Afin de collecter les paquets, les adresses IP pertinentes du serveur et du client HTTP doivent être connues, ainsi que l'adresse IP vers laquelle le client est traduit lorsqu'il traverse l'ASA.

Dans l'exemple de réseau, le serveur HTTP est adressé à 192.168.9.2, le client HTTP est adressé à 10.0.0.2 et les adresses du client HTTP sont traduites en 192.168.9.30 lorsque les paquets quittent l'interface externe. Vous pouvez utiliser la fonction de capture de l'appliance de sécurité adaptative (ASA) de Cisco afin de collecter les paquets, ou utiliser une capture de paquets externe. Si vous avez l'intention d'utiliser la fonctionnalité de capture, l'administrateur peut également utiliser une nouvelle fonctionnalité de capture incluse dans la version 7.0 qui permet à l'administrateur de capturer les paquets abandonnés en raison d'une anomalie TCP.

Remarque : certaines des commandes de ces tables sont renvoyées à une deuxième ligne en raison de restrictions d'espace.

1. Définissez une paire de listes d’accès qui identifient les paquets lorsqu’ils entrent et sortent des interfaces externe et interne.
2. Activez la fonction de capture pour l'interface interne et externe. Activez également la capture pour les paquets MSS spécifiques au protocole TCP.
3. Effacez les compteurs ASP (Accelerated Security Path) sur l'ASA.
4. Activez la journalisation des déroutements au niveau de débogage envoyé à un hôte sur le réseau.
5. Lancez une session HTTP du client HTTP vers le serveur HTTP problématique, et collectez la sortie syslog et la sortie de ces commandes après l'échec de la connexion.**show capture-insideshow capture-outsideshow capture mss-captureshow asp dropRemarque :** Référez-vous à Message du journal système 419001 pour plus d'informations sur ce message d'erreur.

Solution de contournement

Implémentez une solution de contournement maintenant que vous savez que l'ASA abandonne les paquets qui dépassent la valeur MSS annoncée par le client. Gardez à l'esprit que vous pouvez ne pas autoriser ces paquets à atteindre le client en raison d'un dépassement de tampon potentiel sur le client. Si vous choisissez d'autoriser ces paquets via l'ASA, poursuivez la procédure de contournement.

MPF (Modular Policy Framework) est une nouvelle fonctionnalité de la version 7.0 qui est utilisée pour autoriser ces paquets via l'ASA. Ce document n'est pas conçu pour décrire en détail le protocole MPF, mais suggère plutôt les entités de configuration utilisées pour contourner le problème. Référez-vous au Guide de configuration ASA 8.3 pour plus d'informations sur MPF.

Une présentation de la solution de contournement inclut l'identification du client et des serveurs HTTP via une liste d'accès. Une fois la liste d'accès définie, une carte de classe est créée et la liste d'accès est affectée à la carte de classe. Ensuite, une carte TCP est configurée et l'option

permettant d'autoriser les paquets qui dépassent le MSS est activée. Une fois la carte TCP et la carte de classe définies, vous pouvez les ajouter à une carte de stratégie nouvelle ou existante. Une carte de stratégie est ensuite affectée à une stratégie de sécurité. Utilisez la commande **service-policy** en mode de configuration pour activer une carte de stratégie globalement ou sur une interface. Ces paramètres de configuration sont ajoutés à la liste de configuration de Cisco Adaptive Security Appliance (ASA) 8.3. Après avoir créé une carte de stratégie nommée « http-map1 », cet exemple de configuration ajoute la carte de classe à cette carte de stratégie.

Interface spécifique : Configuration MPF pour autoriser les paquets dépassant 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 ces paramètres de configuration en place, les paquets de 192.168.9.2 qui dépassent le MSS annoncé par le client sont autorisés via l'ASA. Il est important de noter que la liste d'accès utilisée dans la carte de classe est conçue pour identifier le trafic sortant vers 192.168.9.2. Le trafic sortant est examiné pour permettre au moteur d'inspection d'extraire le MSS du paquet SYN sortant. Par conséquent, il est impératif de configurer la liste d'accès en gardant à l'esprit la direction du SYN. Si une règle plus généralisée est requise, vous pouvez remplacer l'instruction **access-list** de cette section par une instruction **access-list** qui autorise tout, comme **access-list http-list2 permit ip any any** ou **access-list http-list2 permit tcp any**. Souvenez-vous également que le tunnel VPN peut être lent si une grande valeur de TCP MSS est utilisée. Vous pouvez réduire le MSS TCP pour améliorer les performances.

Cet exemple aide à configurer le trafic entrant et sortant global dans l'ASA :

Configuration globale : Configuration MPF pour autoriser les paquets dépassant 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#

Vérification

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

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

Syslogs 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 à partir 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.
> 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 7517
win 25840 7: 09:16:51.236254 192.168.9.2.80 > 10.0.0.2.58769: . 1305880752:1305882112(1360) ack 7517818
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
- Avis sur le terrain des produits de sécurité (y compris Cisco Adaptive Security Appliance (ASA))
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems