Problema de ASA 8.3: MSS excedido - Los clientes HTTP no pueden navegar a algunos sitios web

Contenido

Introducción

Este documento describe un problema que ocurre cuando algunos sitios Web no son accesibles a través de un Adaptive Security Appliance (ASA) que ejecuta software de la versión 8.3 o posterior.

La versión ASA 7.0 introduce varias mejoras de seguridad nuevas, una de las cuales es una comprobación de los terminales TCP que cumplen con el tamaño máximo de segmento (MSS) anunciado. En una sesión TCP normal, el cliente envía un paquete SYN al servidor, con el MSS incluido dentro de la opción TCP del paquete SYN. El servidor, tras la recepción del paquete SYN, debe reconocer el valor MSS enviado por el cliente y enviar su propio valor MSS en el paquete SYN-ACK. Una vez que el cliente y el servidor son conscientes del MSS de cada uno, ningún peer debe enviar un paquete al otro que sea mayor que el MSS de ese peer.

Se ha detectado que hay algunos servidores HTTP en Internet que no cumplen el MSS que anuncia el cliente. En consecuencia, el servidor HTTP envía paquetes de datos al cliente que son más grandes que el MSS anunciado. Antes de la versión 7.0, estos paquetes se permitían a través del ASA. Con la mejora de la seguridad incluida en la versión del software 7.0, estos paquetes se descartan de forma predeterminada. Este documento está diseñado para ayudar al administrador del dispositivo de seguridad adaptable de Cisco en el diagnóstico de este problema y la implementación de una solución alternativa para permitir los paquetes que exceden el MSS.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en un Cisco Adaptive Security Appliance (ASA) que ejecuta el software de la versión 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.

Configurar

En esta sección se presenta información para configurar las características que este documento describe.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Configuración de ASA 8.3

Estos comandos de configuración se agregan a una configuración predeterminada de ASA 8.3 para permitir que el cliente HTTP se comunique con el servidor HTTP.

Configuración de 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
```

Troubleshoot

Si un sitio web determinado no es accesible a través del ASA, complete estos pasos para resolver problemas. Primero debe capturar los paquetes de la conexión HTTP. Para recopilar los paquetes, es necesario conocer las direcciones IP relevantes del servidor HTTP y del cliente, así como la dirección IP a la que se traduce el cliente cuando atraviesa el ASA.

En la red de ejemplo, el servidor HTTP se dirige a 192.168.9.2, el cliente HTTP se dirige a 10.0.0.2 y las direcciones del cliente HTTP se traducen a 192.168.9.30 a medida que los paquetes salen de la interfaz externa. Puede utilizar la función de captura de Cisco Adaptive Security Appliance (ASA) para recopilar los paquetes o puede utilizar una captura de paquetes externa. Si pretende utilizar la función de captura, el administrador también puede utilizar una nueva función de captura incluida en la versión 7.0 que permite al administrador capturar paquetes que se descartan debido a una anomalía de TCP.

Nota: Algunos de los comandos de estas tablas se ajustan a una segunda línea debido a restricciones espaciales.

1. Defina un par de listas de acceso que identifiquen los paquetes a medida que ingresan y egresan las interfaces externa e interna.
2. Habilite la función de captura para la interfaz interna y externa. También habilite la captura para los paquetes MSS excedidos específicos de TCP.
3. Borre los contadores de la ruta de seguridad acelerada (ASP) en el ASA.
4. Habilite el registro del sistema de trampa en el nivel de depuración enviado a un host en la red.
5. Inicie una sesión HTTP del cliente HTTP al servidor HTTP problemático y recopile el resultado de syslog y el resultado de estos comandos después de que la conexión falle.**show capture capture capture-insideshow capture capture capture-outsideshow capture mss-captureshow asp dropNota:** Refiérase a Mensaje de Registro del Sistema 419001 para obtener más información sobre este mensaje de error.

Solución Aternativa

Implemente una solución alternativa ahora que sabe que ASA descarta los paquetes que exceden el valor MSS anunciado por el cliente. Tenga en cuenta que es posible que no desee permitir que estos paquetes lleguen al cliente debido a una posible saturación del búfer en el cliente. Si decide permitir estos paquetes a través del ASA, continúe con este procedimiento de solución alternativa.

Modular Policy Framework (MPF) es una nueva función de la versión 7.0 que se utiliza para permitir estos paquetes a través del ASA. Este documento no está diseñado para detallar completamente el MPF, sino más bien sugiere las entidades de configuración utilizadas para solucionar el problema. Refiérase a la Guía de Configuración de ASA 8.3 para obtener más información sobre MPF.

Una descripción general de la solución temporal incluye la identificación del cliente HTTP y los servidores a través de una lista de acceso. Una vez definida la lista de acceso, se crea un mapa de clase y la lista de acceso se asigna al mapa de clase. Luego se configura un mapa TCP y se habilita la opción para permitir paquetes que excedan el MSS. Una vez que se haya definido el mapa TCP y el mapa de clase, puede agregarlos a un mapa de política nuevo o existente. A continuación, se asigna un mapa de política a una política de seguridad. Utilice el comando

service-policy en el modo de configuración para activar un policy map globalmente o en una interfaz. Estos parámetros de configuración se agregan a la Lista de Configuración de Cisco Adaptive Security Appliance (ASA) 8.3. Después de crear un mapa de política denominado "http-map1", esta configuración de ejemplo agrega el mapa de clase a este mapa de política.

Interfaz específica: Configuración de MPF para Permitir Paquetes que Exceden 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#
```

Una vez que estos parámetros de configuración están en vigor, los paquetes de 192.168.9.2 que exceden el MSS anunciado por el cliente se permiten a través del ASA. Es importante tener en cuenta que la lista de acceso utilizada en el mapa de clase está diseñada para identificar el tráfico saliente a 192.168.9.2. El tráfico saliente se examina para permitir que el motor de inspección extraiga el MSS del paquete SYN saliente. Por lo tanto, es imprescindible configurar la lista de acceso teniendo en cuenta la dirección de SYN. Si se requiere una regla más generalizada, puede reemplazar la instrucción **access-list** en esta sección con una **lista de acceso** que lo permita todo, como **access-list http-list2 permit ip any** o **access-list http-list2 permit tcp any any**. También recuerde que el túnel VPN puede ser lento si se utiliza un gran valor de TCP MSS. Puede reducir el TCP MSS para mejorar el rendimiento.

Este ejemplo ayuda a configurar globalmente el tráfico entrante y saliente en el ASA:

Configuración global: Configuración de MPF para Permitir Paquetes que Exceden 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#
```

Verificación

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

Repita los pasos de la sección Solución de problemas para verificar que los cambios de configuración hagan lo que están diseñados para hacer.

Registros del sistema de una conexión correcta

```
%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.
```

Resultado de Comandos show de una Conexión Exitosa

```
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.
```

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Avisos de campo de productos de seguridad (incluido Cisco Adaptive Security Appliance (ASA))
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems