Problema ASA 8.3: MSS excedido - Los clientes HTTP no pueden hojear 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 nuevas mejoras de la seguridad, uno de los cuales es una comprobación para los Puntos finales de TCP que se adhieren al máximo anunciado del tamaño del segmento (MSS). 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 fueron permitidos con el ASA. Con la mejora de la seguridad incluida en la versión del software 7.0, estos paquetes se descartan de forma predeterminada. Este documento se diseña para ayudar al administrador adaptante del dispositivo de seguridad de Cisco en la diagnosis de este problema y la implementación de una solución alternativa para permitir los paquetes que exceden el MSS.

Refiera al problema del PIX/ASA 7.X: MSS excedido - Los clientes HTTP no pueden hojear a algunos sitios web para la misma configuración en el dispositivo de seguridad adaptante de Cisco (ASA) con las versiones 8.2 y anterior.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en un dispositivo de seguridad adaptante de Cisco (ASA) ese software de la versión 8.3 de los funcionamientos.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Refiera a los convenios de los consejos técnicos de Cisco para la información sobre las convenciones sobre documentos.

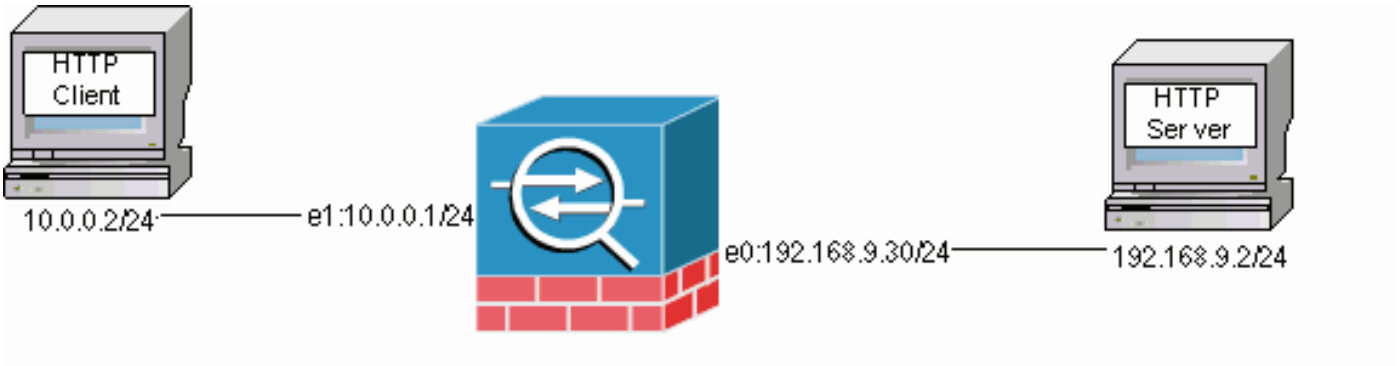
Configurar

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

Nota: Utilice la herramienta de búsqueda de comandos (clientes registrados solamente) para encontrar la información adicional en los comandos las aplicaciones de este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración ASA 8.3

Agregan a estos comandos configuration a una configuración predeterminada ASA 8.3 para permitir que el cliente HTTP comunique con el servidor HTTP.

Configuración 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
```

Troubleshooting

Si un sitio web determinado no es accesible con el ASA, complete estos pasos para resolver problemas. Usted primero necesita capturar los paquetes de la conexión HTTP. Para recoger los paquetes, los IP Addresses relevantes del servidor HTTP y el cliente necesitan ser conocidos, así como la dirección IP que traducen al cliente a cuando atraviesa el ASA.

En la red de muestra, el servidor HTTP se dirige en 192.168.9.2, el cliente HTTP se dirige en 10.0.0.2, y los direccionamientos del cliente HTTP se traducen a 192.168.9.30 mientras que los paquetes salen de la interfaz exterior. Usted puede utilizar la característica de la captura del dispositivo de seguridad adaptante de Cisco (ASA) para recoger los paquetes, o usted puede utilizar a una captura de paquetes externa. Si usted se prepone utilizar la característica de la captura, el administrador puede también utilizar una nueva característica de la captura incluida en la versión 7.0 que permite que el administrador capture los paquetes que son caído debido a una anomalía de TCP.

Nota: Algunos de los comandos en el abrigo de estas tablas a una segunda línea debido a las restricciones espaciales.

1. Defina un par de Listas de acceso que identifiquen los paquetes como él ingreso y salida el exterior y las interfaces interiores.
2. Habilite la característica de la captura para ambos las interfaces interior y exterior. También habilite la captura para los paquetes MSS-excedidos TCP-específicos.
3. Borre los contadores acelerados de la trayectoria de la Seguridad (ASP) en el ASA.
4. Habilite el syslogging del desvío en el nivel de debug enviado a un host en la red.
5. Inicie HTTP session del cliente HTTP al servidor HTTP problemático, y recoja la salida de Syslog y la salida de estos comandos después de que la conexión falle.**muestre la captura captura-dentro demuestre el captura-exterior de la capturamuestre la mss-captura de la capturamuestre el descenso ASPNota:** Refiera al mensaje del registro del sistema 419001 para más información sobre este mensaje de error.

Solución Aternativa

Implemente un workaround ahora que usted sabe que el ASA cae los paquetes que exceden el valor MSS de divulgación por el cliente. Tenga presente que usted puede ser que no quiera permitir que estos paquetes alcancen al cliente debido a una saturación del búfer potencial en el cliente. Si usted elige permitir estos paquetes con el ASA, proceda con este procedimiento de solución alternativa.

El Marco de políticas modular (MPF) es una nueva función en la versión 7.0 que se utiliza para permitir estos paquetes con el ASA. Este documento no se diseña para detallar completamente el MPF sino sugiere bastante las entidades de configuración usadas para trabajar alrededor del problema. Refiera a la guía de configuración ASA 8.3 y al manual de referencia de comandos ASA 8.3 para más información sobre el MPF y los comandos uces de los enumerados en esta sección.

Una descripción a la solución alternativa incluye la identificación del cliente HTTP y de los servidores vía una lista de acceso. Una vez que se define la lista de acceso, se crea una correspondencia de la clase y la lista de acceso se asigna a la correspondencia de la clase. Entonces una correspondencia TCP se configura y la opción para permitir los paquetes que exceden el MSS se habilita. Una vez que se definen la correspondencia TCP y la correspondencia de la clase, usted puede agregarlas de la política existente a una correspondencia nueva o. Una correspondencia de políticas entonces se asigna a una política de seguridad. Utilice el **comando service-policy** en el modo de configuración de activar una correspondencia de políticas global o en una interfaz. Estos parámetros de la configuración se agregan al dispositivo de seguridad adaptante de Cisco (ASA) lista de 8.3 configuraciones. Después de que usted cree una correspondencia de políticas nombrada el "http-map1," esta configuración de muestra agrega la correspondencia de la clase a esta correspondencia de políticas.

Interfaz específica: Configuración MPF para permitir los paquetes que exceden el 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 la configuración existen, los paquetes de 192.168.9.2 que exceden el MSS de divulgación por el cliente se permiten con el ASA. Es importante observar que la lista de acceso usada en la correspondencia de la clase está diseñada para identificar el tráfico

saliente a 192.168.9.2. El tráfico saliente se examina para permitir que el motor del examen extraiga el MSS del paquete SYN saliente. Por lo tanto, es imprescindible configurar la lista de acceso con la dirección del SYN en la mente. Si se requiere una regla más penetrante, usted puede substituir la **sentencia de lista de acceso** en esta sección por una **sentencia de lista de acceso** que permita todo, tal como **IP del permiso de la lista de acceso http-list2 cualquier** o **permiso tcp de la lista de acceso http-list2 cualquier**. También recuerde que el túnel VPN puede ser lento si un valor grande de TCP MSS se utiliza. Usted puede reducir TCP MSS para mejorar el funcionamiento.

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

Configuración global: Configuración MPF para permitir los paquetes que exceden el 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.

Relance los pasos en la sección del Troubleshooting para verificar que los cambios de configuración hacen lo que se diseñan para hacer.

Syslog de una conexión satisfactoria

```
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#
```

Resultados del comando show de una conexión satisfactoria

```
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.
```

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Field Notice de seguridad del producto (dispositivo de seguridad adaptante incluyendo de Cisco (ASA))
- Solicitudes de Comentarios (RFC)