Problema do ASA 8.3: MSS excedido - Os clientes HTTP não podem navegar para alguns sites

Contents

Introduction

Este documento descreve um problema que ocorre quando alguns sites não são acessíveis por meio de um mecanismo de segurança adaptável (ASA) que executa a versão 8.3 ou posterior do software.

A versão ASA 7.0 introduz vários novos aprimoramentos de segurança, um dos quais é uma verificação para endpoints TCP que aderem ao tamanho máximo de segmento (MSS) anunciado. Em uma sessão de TCP normal, o cliente envia um pacote SYN ao servidor com o MSS incluído dentro das opções de TCP do pacote SYN. O servidor, após receber o pacote SYN, deverá reconhecer o valor do MSS enviado pelo cliente e, então, enviar seu próprio valor de MSS no pacote SYN-ACK. Quando o cliente e o servidor estiverem cientes do MSS de cada um, nem o peer deverá enviar um pacote para outro que seja maior do que o MSS desse peer.

Um descoberta foi realizada que há alguns servidores HTTP na Internet que não honram o MSS que o cliente anuncia. Subsequentemente, o servidor HTTP envia pacotes de dados ao cliente que é maior que o MSS anunciado. Antes da versão 7.0, esses pacotes eram permitidos pelo ASA. Com o aprimoramento da segurança incluído na versão 7.0 do software, estes pacotes foram reduzidos por padrão. Este documento foi projetado para auxiliar o administrador do Cisco Adaptive Security Appliance no diagnóstico desse problema e na implementação de uma solução alternativa para permitir os pacotes que excedem o MSS.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas em um Cisco Adaptive Security Appliance (ASA) que executa o software versão 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

Esta seção apresenta informações para configurar as características que este documento descreve.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configuração do ASA 8.3

Esses comandos de configuração são adicionados a uma configuração padrão do ASA 8.3 para permitir que o cliente HTTP se comunique com o servidor HTTP.

Configuração do 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

Se um site específico não estiver acessível através do ASA, faça o seguinte para solucionar o problema. Primeiro você precisa capturar os pacotes da conexão HTTP. Para coletar os pacotes, os endereços IP relevantes do servidor HTTP e do cliente precisam ser conhecidos, bem como o endereço IP para o qual o cliente é convertido quando atravessa o ASA.

No exemplo de rede, o servidor HTTP é endereçado em 192.168.9.2, o cliente HTTP é endereçado em 10.0.0.2 e os endereços de cliente HTTP são convertidos em 192.168.9.30 à medida que os pacotes deixam a interface externa. Você pode usar o recurso de captura do Cisco Adaptive Security Appliance (ASA) para coletar os pacotes ou pode utilizar uma captura de pacote externo. Se você pretende usar o recurso de captura, o administrador também pode utilizar um novo recurso de captura incluído na versão 7.0 que permite ao administrador capturar pacotes que são descartados devido a uma anomalia TCP.

Observação: alguns dos comandos nestas tabelas são finalizados para uma segunda linha devido a restrições espaciais.

1. Defina um par de listas de acesso que identifique os pacotes à medida que eles ingressam e saem das interfaces externa e interna.
2. Ative o recurso de captura para a interface interna e externa. Ative também a captura de pacotes excedidos pelo MSS específico do TCP.
3. Limpe os contadores do ASP (Accelerated Security Path) no ASA.
4. Ative o trap syslogging no nível de depuração enviado a um host na rede.
5. Inicie uma sessão HTTP do cliente HTTP para o servidor HTTP problemático e colete a saída do syslog e a saída desses comandos depois que a conexão falhar.**show capture capture-insideshow capture capture-outsideshow capture mss-captureshow asp dropObservação:** consulte a Mensagem de log do sistema 419001 para obter mais informações sobre essa mensagem de erro.

Solução

Implemente uma solução agora que você sabe que o ASA descarta os pacotes que excedem o valor do MSS anunciado pelo cliente. Lembre-se de que talvez você não queira permitir que esses pacotes cheguem ao cliente devido a uma possível sobrecarga de buffer no cliente. Se você optar por permitir esses pacotes através do ASA, continue com este procedimento alternativo.

O Modular Policy Framework (MPF) é um novo recurso na versão 7.0 usado para permitir esses pacotes através do ASA. Este documento não foi projetado para detalhar totalmente o MPF, mas sugere as entidades de configuração usadas para resolver o problema. Consulte o Guia de configuração do ASA 8.3 para obter mais informações sobre o MPF.

Uma visão geral da solução inclui a identificação do cliente HTTP e dos servidores através de uma lista de acesso. Uma vez definida a lista de acesso, um mapa de classe é criado e a lista de acesso é atribuída ao mapa de classe. Em seguida, um mapa TCP é configurado e a opção para permitir pacotes que excedem o MSS é ativada. Depois que o mapa TCP e o mapa de classes forem definidos, você poderá adicioná-los a um mapa de políticas novo ou existente. Um mapa de política é então atribuído a uma política de segurança. Use o comando **service-policy** no modo de configuração para ativar um mapa de políticas globalmente ou em uma interface. Esses

parâmetros de configuração são adicionados à lista de configuração do Cisco Adaptive Security Appliance (ASA) 8.3. Depois de criar um mapa de política chamado "http-map1", essa configuração de exemplo adiciona o mapa de classes a esse mapa de política.

Interface específica: Configuração do MPF para permitir pacotes que excedem o 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#
```

Quando esses parâmetros de configuração estiverem em vigor, os pacotes de 192.168.9.2 que excederem o MSS anunciado pelo cliente serão permitidos através do ASA. É importante observar que a lista de acesso usada no mapa de classes é projetada para identificar o tráfego de saída para 192.168.9.2. O tráfego de saída é examinado para permitir que o mecanismo de inspeção extraia o MSS do pacote SYN de saída. Portanto, é imperativo configurar a lista de acesso com a direção do SYN em mente. Se uma regra mais difundida for necessária, você poderá substituir a instrução **access-list** nesta seção por uma instrução **access-list** que permita tudo, como **access-list http-list2 permit ip any any** ou **access-list http-list2 permit tcp any any**. Lembre-se também de que o túnel VPN pode ser lento se um grande valor de TCP MSS for usado. Você pode reduzir o TCP MSS para melhorar o desempenho.

Este exemplo ajuda a configurar globalmente o tráfego de entrada e saída no ASA:

Configuração global: Configuração do MPF para permitir pacotes que excedem o 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#
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente.

Repita as etapas da seção Solução de problemas para verificar se as alterações de configuração fazem o que foram projetadas para fazer.

Syslogs de uma conexão bem-sucedida

```
%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.
```

Saída dos comandos show de uma conexão bem-sucedida

```
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.
```

Informações Relacionadas

- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Avisos de campo de produtos de segurança (incluindo Cisco Adaptive Security Appliance (ASA))
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems