ASA 8.3 问题：超出 MSS - HTTP 客户端无法浏览到某些网站

Contents

Introduction

本文档将说明一个在无法通过运行 8.3 版本或更高版本软件的自适应安全设备 (ASA) 访问某些网站时发生的问题。

ASA 7.0 版本引入了若干项新的安全增强功能，其中一项功能是检查遵循所通告最大分段大小 (MSS) 的 TCP 终端。在正常的 TCP 会话中，客户端会将 SYN 数据包发送到服务器（MSS 包含在 SYN 数据包的 TCP 选项内）。收到 SYN 数据包时，服务器应识别客户端发送的 MSS 值，然后在 SYN-ACK 数据包中发送它自己的 MSS 值。客户端和服务器获悉彼此的 MSS 之后，两个对等体都不应该向对方发送大于对等体的 MSS 的数据包。

已发现 Internet 上有一些 HTTP 服务器不遵从客户端通告的 MSS。随后，该 HTTP 服务器会将大于所通告的 MSS 的数据包发送到客户端。在 7.0 版本之前，系统会允许这些数据包通过 ASA。使用 7.0 软件版本中包含的安全增强功能，默认情况下这些数据包会被丢弃。本文档旨在帮助思科自适应安全设备管理员诊断此问题，并通过实施解决方法来允许超过 MSS 的数据包通过。

有关运行 8.2 及以前版本软件的思科自适应安全设备 (ASA) 上的相同配置，请参阅 PIX/ASA 7.X 问题：超出 MSS - HTTP 无法浏览某些网站。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

本文档中的信息以运行 8.3 版本软件的思科自适应安全设备 (ASA) 为基础。

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.

Conventions

关于文件规则的信息，请参见Cisco技术提示规则。

Configure

本部分提供了用于配置本文档所述功能的信息。

Note: 使用命令查找工具（仅限注册用户）可查找有关本文档所用命令的其他信息。

Network Diagram

本文档使用以下网络设置：

ASA 8.3 配置

这些配置命令已添加到 ASA 8.3 默认配置中，以允许 HTTP 客户端与 HTTP 服务器通信。

ASA 8.3 配置

```
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

如果无法通过 ASA 访问某个特定的网站，请完成这些步骤以排除故障。您首先需要从 HTTP 连接获取数据包。为了收集数据包，需要知道 HTTP 服务器和客户端的相关 IP 地址，以及当客户端通过 ASA 时被转换成的 IP 地址。

在示例网络中，HTTP 服务器地址被指定为 192.168.9.2，HTTP 客户端地址被指定为 10.0.0.2，并且在数据包离开外部接口时，HTTP 客户端地址会转换为 192.168.9.30。要收集数据包，您既可以使用思科自适应安全设备 (ASA) 的捕获功能，也可以使用外部数据包捕获功能。如果打算使用捕获功能，管理员还可以使用 7.0 版本中包含的新捕获功能，该功能允许管理员捕获因 TCP 异常而丢弃的数据包。

Note: 由于空间限制，这些表格中的部分命令会自动换行到第二行。

1. 定义一对在数据包出入内外部接口时对这些数据包进行识别的访问列表。
2. 对内部接口和外部接口均启用捕获功能。并且对 TCP 特定的超过 MSS 的数据包启用捕获。
3. 清除 ASA 上的加速安全路径 (ASP) 计数器。
4. 允许将调试级别的陷井系统日志记录消息发送到网络中的主机。
5. 从 HTTP 客户端向有问题的 HTTP 服务器发起 HTTP 会话，当连接失败后，收集 syslog 输出和这些命令的输出。**show capture capture-insideshow capture capture-outsideshow capture mss-captureshow asp dropNote:** 有关此错误消息的详细信息，请参阅系统日志消息 419001。

解决方法

在知道 ASA 会丢弃超过客户端通告的 MSS 值的数据包后，下一步是实施解决方法。请记住，由于客户端上可能发生缓冲区溢出，因此您可能不希望允许这些数据包到达客户端。如果选择允许这些数据包通过 ASA，请继续执行此解决方法操作步骤。

模块化策略框架 (MPF) 是 7.0 版本中的一个新功能，用于允许这些数据包通过 ASA。本文档并不旨在详细介绍 MPF，而是就用于解决问题的配置实体提出建议。有关 MPF 和此部分列出的命令的更多信息，请参阅 ASA 8.3 配置指南和 ASA 8.3 命令参考手册。

解决方法概述包括通过访问列表识别 HTTP 客户端和服务器。在定义访问列表后，系统将创建类映射，并将访问列表分配到此类映射。然后系统将配置 TCP 映射，并且启用允许超出 MSS 的数据包通过的选项。在定义 TCP 映射和类映射后，您可以将其添加到新的或现有的策略映射中。然后，系统会将策略映射分配给安全策略。在配置模式下使用 **service-policy 命令**，从全局或在某个接口上激活策略映射。这些配置参数会被添加到思科自适应安全设备 (ASA) 8.3 配置列表。在您创建名为“http-map1”的策略映射之后，此配置示例会将类映射添加到此策略映射中。

特定接口：允许超出 MSS 的数据包的 MPF 配置

```
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#
```

设置好这些配置参数后，系统将允许来自 192.168.9.2 的超出客户端通告的 MSS 的数据包通过 ASA。请注意，类映射中使用的访问列表旨在识别流向 192.168.9.2 的出站流量。出站数据流会受到检查以允许检测引擎从传出 SYN 数据包提取 MSS。因此，配置访问列表时必须谨记 SYN 的方向。如果需要一个更加普遍的规则，您可以用允许一切数据通过的**访问列表语句**替换此部分中的**访问列表语句**，例如 **access-list http-list2 permit ip any any** 或 **access-list http-list2 permit tcp any any**。此外，请记住，如果使用的 TCP MSS 值较大，VPN 隧道可能会变得很慢。可以减小 TCP MSS 来改进性能。

此示例可帮助在 ASA 中全局配置入站和出站流量：

全局配置：允许超出 MSS 的数据包的 MPF 配置

```
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#
```

Verify

本部分提供的信息可帮助您确认您的配置是否可正常运行。

重复故障排除部分所述的步骤，以验证配置更改是否执行其预期应执行的操作。

来自成功连接的 Syslog 消息

```
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#
```

来自成功连接的 show 命令输出

```
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.
```

Related Information

- Cisco ASA 5500 系列自适应安全设备
- 安全产品现场通告（包括思科自适应安全设备 (ASA)）
- 请求注解 (RFC)