ASA 8.3問題：超出MSS - HTTP客戶端無法瀏覽某些網站

目錄

簡介

本文描述運行8.3版或更高版本軟體的自適應安全裝置(ASA)無法訪問某些網站時出現的問題。

ASA 7.0版本引入了幾個新的安全增強功能，其中一個功能是檢查符合通告的最大資料段大小(MSS)的TCP端點。 在正常TCP作業階段中，使用者端會將SYN封包傳送到伺服器，而MSS包含在SYN封包的TCP選項中。收到SYN封包後，伺服器應識別使用者端傳送的MSS值，然後在SYN-ACK封包中傳送其自己的MSS值。一旦使用者端和伺服器都知道彼此的MSS，對等點都不應將大於對等MSS的封包傳送到對方。

發現Internet上有幾台HTTP伺服器不執行客戶端通告的MSS。隨後，HTTP伺服器向客戶端傳送大於通告MSS的資料包。在7.0版之前，允許這些資料包通過ASA。由於7.0軟體版本包含安全增強功能，因此預設會捨棄這些封包。本文檔旨在協助思科自適應安全裝置管理員診斷此問題，並實施允許超過MSS的資料包的解決方法。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據執行8.3版軟體的思科調適型安全裝置(ASA)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

本節提供用於設定本檔案中所述功能的資訊。

網路圖表

本檔案會使用以下網路設定：

ASA 8.3配置

這些配置命令將新增到ASA 8.3預設配置中，以允許HTTP客戶端與HTTP伺服器通訊。

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
```

疑難排解

如果無法通過ASA訪問特定網站，請完成以下步驟進行故障排除。首先需要從HTTP連線捕獲資料包。為了收集資料包，需要知道HTTP伺服器和客戶端的相關IP地址，以及客戶端通過ASA時轉換為的IP地址。

在示例網路中，HTTP伺服器地址為192.168.9.2,HTTP客戶端地址為10.0.0.2，並且HTTP客戶端地址在資料包離開外部介面時轉換為192.168.9.30。您可以使用思科自適應安全裝置(ASA)的捕獲功能來收集資料包，也可以使用外部資料包捕獲。如果您打算使用捕獲功能，管理員還可以利用7.0版中包含的新捕獲功能，該功能允許管理員捕獲由於TCP異常而丟棄的資料包。

注意：由於空間限制，這些表格中的某些命令會換到第二行。

1. 定義一對存取清單，用於在封包輸入和輸出外部和內部介面時識別封包。
2. 為內部和外部介面啟用捕獲功能。還為TCP特定的MSS超出封包啟用擷取。
3. 清除ASA上的加速安全路徑(ASP)計數器。
4. 在傳送到網路上的主機的調試級別啟用陷阱系統日誌記錄。
5. 啟動從HTTP客戶端到有問題的HTTP伺服器的HTTP會話，並在連線失敗後收集系統日誌輸出和這些命令的輸出。**show capture capture-insideshow capture capture-outsideshow capture mss-captureshow asp drop註：有關**此錯誤消息的詳細資訊，請參閱系統日誌消息41901。

因應措施

既然您已知道ASA丟棄超出客戶端通告的MSS值的資料包，請實施解決方法。請記住，您可能不想允許這些封包到達使用者端，因為使用者端上可能存在緩衝區溢位。如果選擇允許這些資料包通過ASA，請繼續執行此解決過程。

模組化策略框架(MPF)是7.0版本中的一項新功能，用於允許這些資料包通過ASA。本文檔並非旨在全面詳述MPF，而是建議用於解決該問題的配置實體。有關MPF的詳細資訊，請參閱ASA 8.3配置指南。

解決方法的概述包括通過訪問清單標識HTTP客戶端和伺服器。定義訪問清單後，將建立類對映並將訪問清單分配給類對映。然後設定一個TCP映像，並啟用允許超過MSS的封包的選項。定義TCP對映和類對映後，可以將它們新增到新的或現有的策略對映中。然後將策略對映分配給安全策略。在配置模式下使用**service-policy**命令以全域性方式或在介面上啟用策略對映。這些配置引數將新增到思科自適應安全裝置(ASA)8.3配置清單中。建立名為「http-map1」的策略對映後，此示例配置將類對映新增到此策略對映中。

特定介面：允許超過MSS的封包的MPF組態

```
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#
```

一旦這些配置引數到位，來自192.168.9.2且超出客戶端通告的MSS的資料包就可以通過ASA了。必須注意的是，類對映中使用的訪問清單旨在標識發往192.168.9.2的出站流量。檢查出站流量以允許檢測引擎從出站SYN資料包提取MSS。因此，必須考慮使用SYN的方向來設定存取清單。如果需要更普遍的規則，可以用允許所有內容的**access-list**語句替換本節中的**access-list**語句，例如**access-list http-list2 permit ip any any**或**access-list http-list2 permit tcp any**。另請記住，如果使用大量TCP MSS，VPN通道可能會變慢。您可以降低TCP MSS以改善效能。

此示例有助於在ASA中全域性配置入站和出站流量：

全域性配置：允許超過MSS的封包的MPF組態

```
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#
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

重複疑難排解一節中的步驟，以驗證組態變更是否執行其所設計的工作。

來自成功連線的系統日誌

```
%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.
```

成功連線中的show命令輸出

```
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.
> 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.
```

相關資訊

- Cisco ASA 5500系列調適型安全裝置
- 安全產品現場通知(包括思科自適應安全裝置(ASA))
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems