ASA 8.3-Problem: MSS übertroffen - HTTP-Clients können nicht zu einigen Websites wechseln

Inhalt

Einführung

Dieses Dokument beschreibt ein Problem, das auftritt, wenn auf einige Websites nicht über eine Adaptive Security Appliance (ASA) zugegriffen werden kann, die Version 8.3 oder höher ausführt.

Die ASA 7.0-Version bietet eine Reihe neuer Sicherheitsverbesserungen, darunter eine Überprüfung auf TCP-Endpunkte, die der angegebenen maximalen Segmentgröße (MSS) entsprechen. In einer normalen TCP-Sitzung sendet der Client ein SYN-Paket an den Server, wobei die MSS in den TCP-Optionen des SYN-Pakets enthalten ist. Der Server sollte nach Erhalt des SYN-Pakets den vom Client gesendeten MSS-Wert erkennen und dann seinen eigenen MSS-Wert im SYN-ACK-Paket senden. Sobald sowohl der Client als auch der Server die MSS des anderen kennen, sollte keiner der Peers ein Paket an den anderen senden, das größer ist als die MSS des Peers.

Es wurde festgestellt, dass es im Internet einige HTTP-Server gibt, die die vom Client angekündigte MSS nicht einhalten. Anschließend sendet der HTTP-Server Datenpakete an den Client, die größer als die angegebene MSS sind. Vor Version 7.0 waren diese Pakete über die ASA zugelassen. Wenn die Sicherheitsverbesserungen in der Softwareversion 7.0 enthalten sind, werden diese Pakete standardmäßig verworfen. Dieses Dokument soll den Administrator der Cisco Adaptive Security Appliance bei der Diagnose dieses Problems und der Implementierung einer Lösung unterstützen, um Pakete zuzulassen, die die MSS überschreiten.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einer Cisco Adaptive Security Appliance (ASA), auf der Version 8.3 Software ausgeführt wird.

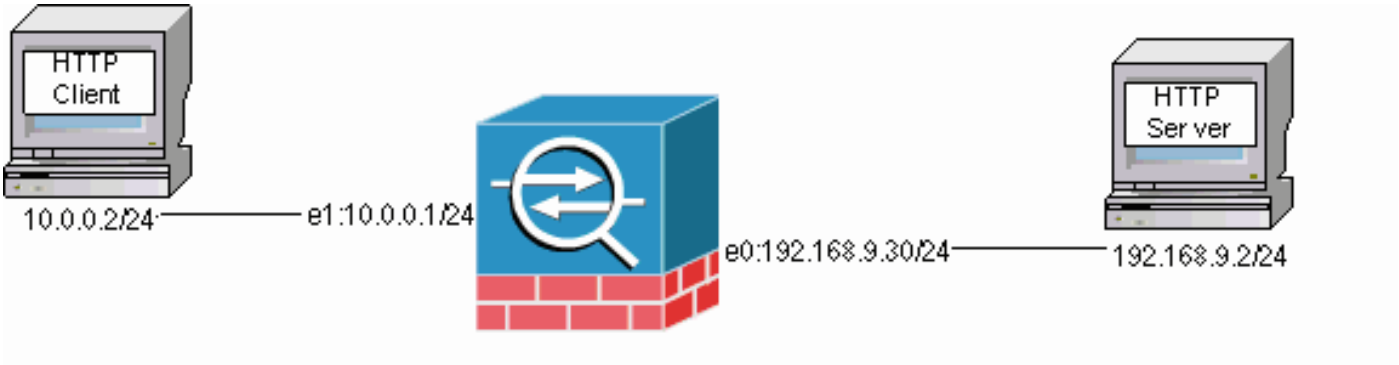
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



ASA 8.3-Konfiguration

Diese Konfigurationsbefehle werden einer ASA 8.3-Standardkonfiguration hinzugefügt, damit der HTTP-Client mit dem HTTP-Server kommunizieren kann.

ASA 8.3-Konfiguration

```
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
```

Fehlerbehebung

Wenn auf eine bestimmte Website nicht über die ASA zugegriffen werden kann, führen Sie die folgenden Schritte aus, um eine Fehlerbehebung durchzuführen. Zuerst müssen Sie die Pakete von der HTTP-Verbindung erfassen. Um die Pakete zu erfassen, müssen die relevanten IP-Adressen des HTTP-Servers und -Clients sowie die IP-Adresse bekannt sein, in die der Client übersetzt wird, wenn er die ASA passiert.

Im Beispielnetzwerk wird der HTTP-Server unter 192.168.9.2 adressiert, der HTTP-Client unter 10.0.0.2 adressiert und die HTTP-Client-Adressen in 192.168.9.30 übersetzt, da Pakete die externe Schnittstelle verlassen. Sie können die Erfassungsfunktion der Cisco Adaptive Security Appliance (ASA) verwenden, um die Pakete zu erfassen, oder Sie können eine externe Paketerfassung verwenden. Wenn Sie die Erfassungsfunktion verwenden möchten, kann der Administrator auch eine neue Erfassungsfunktion in der Version 7.0 verwenden, mit der der Administrator Pakete erfassen kann, die aufgrund einer TCP-Anomalie verworfen wurden.

Hinweis: Einige der Befehle in diesen Tabellen werden aufgrund räumlicher Einschränkungen in eine zweite Zeile eingefügt.

1. Definieren Sie zwei Zugriffslisten, die die Pakete beim Ein- und Ausgang der Außen- und Innenschnittstellen identifizieren.
2. Aktivieren Sie die Erfassungsfunktion für die interne und die externe Schnittstelle. Aktivieren Sie außerdem die Erfassung für TCP-spezifische MSS-überschreitende Pakete.
3. Löschen Sie die ASP-Zähler (Accelerated Security Path) auf der ASA.
4. Aktivieren Sie die Syslogging-Trap-Protokollierung auf der Debugebene, die an einen Host im Netzwerk gesendet wird.
5. Initiieren Sie eine HTTP-Sitzung vom HTTP-Client zum problematischen HTTP-Server, und sammeln Sie die Syslog-Ausgabe und die Ausgabe dieser Befehle, nachdem die Verbindung fehlschlägt.**Show Capture InsideShow Capture-AußenMSS-Erfassung anzeigenshow asp dropHinweis:** Weitere Informationen zu dieser Fehlermeldung finden Sie in der Systemprotokollmeldung 419001.

Problemumgehung

Implementieren Sie jetzt eine Problemumgehung, da Sie wissen, dass die ASA die Pakete verwirft, die den vom Client angegebenen MSS-Wert überschreiten. Beachten Sie, dass Sie diese Pakete aufgrund eines potenziellen Pufferüberlaufs auf dem Client möglicherweise nicht auf den Client zugreifen dürfen. Wenn Sie diese Pakete über die ASA zulassen möchten, fahren Sie mit diesem Workaround fort.

Das modulare Richtlinien-Framework (MPF) ist eine neue Funktion in der Version 7.0, mit der diese Pakete über die ASA zugelassen werden. Dieses Dokument ist nicht vollständig auf den MPF ausgerichtet, sondern bietet einen Vorschlag für die zur Problemumgehung verwendeten Konfigurationseinheiten. Weitere Informationen zu MPF finden Sie im ASA 8.3-Konfigurationshandbuch.

Eine Übersicht zur Problemumgehung beinhaltet die Identifizierung des HTTP-Clients und der Server über eine Zugriffsliste. Nach der Definition der Zugriffsliste wird eine Klassenzuordnung

erstellt und der Klassenzuordnung die Zugriffsliste zugewiesen. Anschließend wird eine TCP-Zuordnung konfiguriert und die Option aktiviert, Pakete, die die MSS überschreiten, zuzulassen. Wenn die TCP-Zuordnung und die Klassenzuordnung definiert sind, können Sie sie einer neuen oder einer vorhandenen Richtlinienzuordnung hinzufügen. Eine Richtlinienzuordnung wird dann einer Sicherheitsrichtlinie zugewiesen. Verwenden Sie den **Service-Policy**-Befehl im Konfigurationsmodus, um eine Richtlinienzuordnung global oder auf einer Schnittstelle zu aktivieren. Diese Konfigurationsparameter werden der Konfigurationsliste der Cisco Adaptive Security Appliance (ASA) 8.3 hinzugefügt. Nachdem Sie eine Richtlinienzuordnung mit dem Namen "http-map1" erstellt haben, fügt diese Beispielkonfiguration dieser Richtlinienzuordnung die Klassenzuordnung hinzu.

Spezifische Schnittstelle: MPF-Konfiguration zum Zulassen von Paketen, die MSS überschreiten

```
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#
```

Sobald diese Konfigurationsparameter vorhanden sind, sind Pakete ab 192.168.9.2, die die vom Client angegebene MSS überschreiten, über die ASA zulässig. Beachten Sie, dass die in der Klassenzuordnung verwendete Zugriffsliste so konzipiert ist, dass ausgehender Datenverkehr an 192.168.9.2 identifiziert wird. Der ausgehende Datenverkehr wird geprüft, damit die Prüfungs-Engine die MSS aus dem ausgehenden SYN-Paket extrahieren kann. Aus diesem Grund ist es zwingend erforderlich, die Zugriffsliste unter Berücksichtigung der Richtung des SYN zu konfigurieren. Wenn eine umfassendere Regel erforderlich ist, können Sie die **Zugriffslistenanweisung** in diesem Abschnitt durch eine **Zugriffslistenanweisung** ersetzen, die alles zulässt, z. B. **Zugriffsliste http-list2 permit ip any any any any** or **access-list http-list2 permit tcp any**. Denken Sie auch daran, dass der VPN-Tunnel langsam sein kann, wenn ein großer Wert von TCP-MSS verwendet wird. Sie können die TCP-MSS reduzieren, um die Leistung zu verbessern.

Dieses Beispiel hilft bei der Konfiguration des globalen ein- und ausgehenden Datenverkehrs in der ASA:

Globale Konfiguration: MPF-Konfiguration zum Zulassen von Paketen, die MSS überschreiten

```
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#
```

Überprüfen

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Wiederholen Sie die Schritte im Abschnitt Fehlerbehebung, um sicherzustellen, dass die Konfigurationsänderungen die von ihnen festgelegten Aufgaben erfüllen.

Syslogs von einer erfolgreichen Verbindung

```
%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.
```

Ausgabe von show Commands aus einer erfolgreichen Verbindung

```
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.
```

Zugehörige Informationen

- Cisco Adaptive Security Appliances der Serie ASA 5500
- Problemhinweise zu Sicherheitsprodukten (einschließlich Cisco Adaptive Security Appliance (ASA))
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems