ASA 8.3 Kwestie: MCS overschreden - HTTP-clients kunnen niet naar bepaalde websites bladeren

Inhoud

Inleiding

Dit document beschrijft een probleem dat zich voordoet wanneer bepaalde websites niet toegankelijk zijn via een adaptieve security applicatie (ASA) die versie 8.3 of later software uitvoert.

De ASA 7.0 release introduceert verschillende nieuwe beveiligingsverbeteringen, waaronder een controle van TCP-endpoints die voldoen aan de geadverteerde Maximum Segment Size (MSS). In een normale TCP-sessie, stuurt de client een SYN-pakket naar de server, met de MSS in de TCP-opties van het SYN-pakket. De server, na ontvangst van het SYN-pakket, moet de MSS-waarde herkennen die door de client is verstuurd en vervolgens zijn eigen MSS-waarde in het SYN-ACK-pakket verzenden. Zodra zowel de client als de server zich bewust zijn van elkaars MSS, zou geen van beide peer een pakket naar de andere moeten verzenden dat groter is dan MSS van dat peer.

Er is ontdekt dat er een paar HTTP servers op het internet zijn die niet voldoen aan de MSS die de client adverteert. Vervolgens stuurt de HTTP server gegevenspakketten naar de client die groter zijn dan de geadverteerde MSS. Voor release 7.0 waren deze pakketten toegestaan door de ASA. Indien de beveiligingsverbetering in de 7.0-softwarerelease is opgenomen, worden deze pakketten standaard verzonden. Dit document is ontwikkeld om de Cisco adaptieve security applicatie beheerder te helpen bij de diagnose van dit probleem en de implementatie van een werkruimte om pakketten toe te staan die de MSS overschrijden.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op een Cisco adaptieve security applicatie (ASA) die versie 8.3 van de software draait.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

In deze sectie wordt u voorzien van de informatie om de functies te configureren die in dit document worden beschreven.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:

ASA 8.3 configuratie

Deze configuratieopdrachten worden toegevoegd aan een ASA 8.3 standaard configuratie zodat de HTTP client kan communiceren met de HTTP server.

ASA 8.3 configuratie

```
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
```

Problemen oplossen

Als een bepaalde website niet via de ASA toegankelijk is, voltooi dan deze stappen om problemen op te lossen. U moet eerst de pakketten van de HTTP verbinding opnemen. Om de pakketten te verzamelen, moeten de relevante IP adressen van de HTTP server en client bekend zijn, zowel als het IP adres waar de client wordt vertaald wanneer deze de ASA passeert.

In het voorbeeldnetwerk, wordt de HTTP server benaderd op 192.168.9.2, wordt de HTTP client gericht op 10.0.0.2 en de HTTP client adressen worden vertaald naar 192.168.9.30 omdat pakketten de externe interface verlaten. U kunt de opnamefunctie van de Cisco adaptieve security applicatie (ASA) gebruiken om de pakketten te verzamelen, of u kunt een externe pakketvastlegging gebruiken. Als u de opnamefunctie wilt gebruiken, kan de beheerder ook een nieuwe opnamefunctie gebruiken die in de versie 7.0 inbegrepen is die de beheerder toestaat om pakketten op te nemen die wegens een anomalie van TCP worden gedropt.

Opmerking: Sommige opdrachten in deze tabellen worden op een tweede regel teruggebracht door ruimtelijke beperkingen.

1. Defineert een paar toegangslijsten die de pakketten identificeren aangezien zij de buitenkant en de binneninterfaces binnendringen.
2. Schakel de opnamefunctie in voor zowel de binnen- als de buitenkant. Schakel de opname ook in voor TCP-specifieke MSS-overtrokken pakketten.
3. Schakel de ASK-tellers (Accelerated Security Path) op de ASA uit.
4. Inschakelen van het opsluiten op het debug-niveau dat naar een host op het netwerk wordt verzonden.
5. Initieer een HTTP-sessie van de HTTP-client naar de problematische HTTP-server en verzamel de syfilminvoer en de output van deze opdrachten nadat de verbinding is verbroken.**gevangennemen binnen tonenopname buiten tonenvangenasfalt tonenOpmerking:** Raadpleeg [bericht 419001 voor](#) meer informatie over deze foutmelding.

Werken

Voer een tijdelijke oplossing in zodat u weet dat de ASA de pakketten laat vallen die de MSS waarde overschrijden die door de client wordt geadverteerd. Houd in gedachten dat u deze pakketten niet kunt toestaan om de client te bereiken wegens een potentiële bufferoverschrijding op de client. Als u deze pakketten door de ASA wilt laten doorlopen, gaat u met deze omwerkingsprocedure te werk.

Modular Policy Framework (MPF) is een nieuwe functie in de 7.0 release die gebruikt wordt om deze pakketten door de ASA te laten uitvoeren. Dit document is niet ontworpen om het Openbaar Ministerie volledig te gedetailleerd, maar suggereert eerder de configuratieentiteiten die gebruikt worden om rond het probleem te werken. Raadpleeg de [ASA 8.3 Configuration Guide](#) voor meer informatie over MPF.

Een overzicht van het traject omvat de identificatie van de HTTP-client en servers via een toegangslijst. Zodra de toegangslijst wordt gedefinieerd wordt er een class map aangemaakt en

wordt de toegangslijst toegewezen aan de class map. Vervolgens wordt een TCP-kaart ingesteld en is de optie om pakketten toe te staan die de MSS overschrijden ingeschakeld. Zodra de TCP kaart en class map worden gedefinieerd, kunt u ze toevoegen aan een nieuwe of bestaande beleidsplan. Vervolgens wordt een beleidsplan toegewezen aan een veiligheidsbeleid. Gebruik de opdracht **Service-beleid** in de configuratiemodus om een beleidskaart mondiaal of op een interface te activeren. Deze configuratieparameters worden toegevoegd aan de Cisco adaptieve security applicatie (ASA) 8.3 configuratielijst. Nadat je een beleidskaart maakte genaamd "http-map1", voegt deze voorbeeldconfiguratie de class map toe aan deze beleidsplanning.

Specifieke interface: MPF-configuratie om pakketten toe te staan die MSS overschrijden

```
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#
```

Nadat deze configuratieparameters zijn geïnstalleerd, zijn pakketten van 192.168.9.2 die de door de client geadverteerde MSS overschrijden, via de ASA toegestaan. Het is belangrijk op te merken dat de toegangslijst die in de class map wordt gebruikt, ontworpen is om uitgaande verkeer te identificeren naar 192.168.9.2. Het uitgaande verkeer wordt onderzocht om de inspectiemachine in staat te stellen de MSS uit het uitgaande SYN-pakket te halen. Daarom is het noodzakelijk om de toegangslijst met de richting van SYN in gedachten te configureren. Als er een meer wijdverspreide regel vereist is, kunt u de **access-list** verklaring in deze sectie vervangen met een **access-list** verklaring die alles toestaat, zoals **access-list2 vergunning ip om het even welke** of **access-list http-list2 vergunning** om het even welke of **toegang-lijst http-list2** vergunning. Denk er ook aan dat de VPN-tunnel langzaam kan zijn als een grote waarde van TCP MSS wordt gebruikt. U kunt TCP MSS verminderen om de prestaties te verbeteren.

Dit voorbeeld helpt om wereldwijd inkomende en uitgaande verkeer in de ASA te configureren:

Mondiale configuratie: MPF-configuratie om pakketten toe te staan die MSS overschrijden

```
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#
```

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Herhaal de stappen in het gedeelte Problemen oplossen om te controleren dat de configuratieveranderingen doen wat ze moeten doen.

Syslogs van een succesvolle verbinding

```
%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.
```

Uitvoer van showopdrachten vanuit een succesvolle verbinding

```
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.
```

Gerelateerde informatie

- Adaptieve security applicaties van Cisco ASA 5500 Series
- Security productmeldingen (inclusief Cisco adaptieve security applicatie (ASA)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems