ASA 8.3 문제: MSS 초과 - HTTP 클라이언트가 일부 웹 사이트를 탐색할 수 없음

목차

소개

이 문서에서는 버전 8.3 이상을 실행하는 ASA(Adaptive Security Appliance)를 통해 일부 웹 사이트에 액세스할 수 없는 경우 발생하는 문제에 대해 설명합니다.

ASA 7.0 릴리스에서는 몇 가지 새로운 보안 개선 사항이 도입되었으며, 그 중 하나는 알려진 MSS(Maximum Segment Size)를 준수하는 TCP 엔드포인트를 확인하는 기능입니다. 일반 TCP 세션에서 클라이언트는 SYN 패킷의 TCP 옵션에 MSS가 포함된 SYN 패킷을 서버로 전송합니다. SYN 패킷을 받으면 서버는 클라이언트가 보낸 MSS 값을 인식한 다음 SYN-ACK 패킷에 고유한 MSS 값을 보내야 합니다. 클라이언트와 서버 모두 서로의 MSS를 인식하면 피어는 해당 피어의 MSS보다 큰 다른 피어로 패킷을 전송하지 않아야 합니다.

인터넷에 클라이언트가 광고하는 MSS를 준수하지 않는 몇 개의 HTTP 서버가 있다는 것을 발견했습니다. 그런 다음 HTTP 서버는 알려진 MSS보다 큰 클라이언트에 데이터 패킷을 전송합니다. 릴리스 7.0 이전에는 이러한 패킷이 ASA를 통해 허용되었습니다. 7.0 소프트웨어 릴리스에 포함된 보안 개선 사항을 통해 이러한 패킷은 기본적으로 삭제됩니다. 이 문서는 Cisco Adaptive Security Appliance 관리자가 이 문제를 진단하고 해결 방법을 구현하여 MSS를 초과하는 패킷을 허용하는 데 도움이 되도록 설계되었습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 버전 8.3 소프트웨어를 실행하는 Cisco ASA(Adaptive Security Appliance)를 기반

으로 합니다.

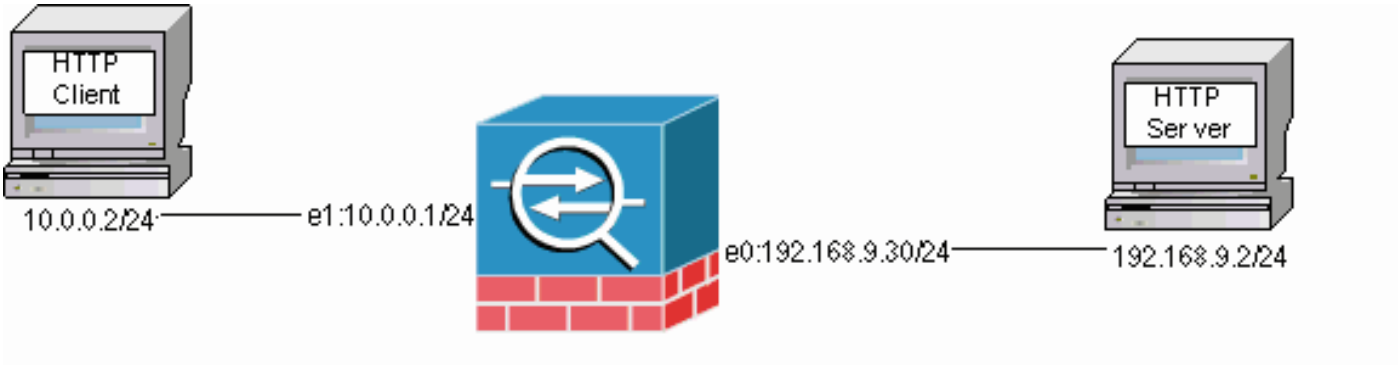
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 섹션에서는 이 문서에서 설명하는 기능을 구성하는 데 필요한 정보를 제공합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



ASA 8.3 컨피그레이션

이러한 컨피그레이션 명령은 HTTP 클라이언트가 HTTP 서버와 통신할 수 있도록 ASA 8.3 기본 컨피그레이션에 추가됩니다.

ASA 8.3 컨피그레이션

```
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
```

문제 해결

ASA를 통해 특정 웹 사이트에 액세스할 수 없는 경우 다음 단계를 완료하여 문제를 해결하십시오.

먼저 HTTP 연결에서 패킷을 캡처해야 합니다. 패킷을 수집하려면 HTTP 서버 및 클라이언트의 관련 IP 주소와 클라이언트가 ASA를 통과할 때 변환되는 IP 주소를 알아야 합니다.

예제 네트워크에서는 HTTP 서버가 192.168.9.2으로 주소가 지정되고, HTTP 클라이언트는 10.0.0.2으로 주소가 지정되며, 패킷이 외부 인터페이스를 떠날 때 HTTP 클라이언트 주소가 192.168.9.30으로 변환됩니다. Cisco ASA(Adaptive Security Appliance)의 캡처 기능을 사용하여 패킷을 수집하거나 외부 패킷 캡처를 활용할 수 있습니다. 캡처 기능을 사용하려는 경우 관리자는 7.0 릴리스에 포함된 새 캡처 기능을 사용하여 관리자가 TCP 이상 징후 때문에 삭제된 패킷을 캡처할 수 있습니다.

참고: 이러한 테이블의 일부 명령은 공간 제한으로 인해 두 번째 행으로 넘어갑니다.

1. 패킷을 인그레스(ingress) 및 이그레스(egress)할 때 패킷을 식별하는 액세스 목록 쌍을 정의합니다.
2. 내부 및 외부 인터페이스 모두에 대해 캡처 기능을 활성화합니다. 또한 TCP 특정 MSS 초과 패킷에 대한 캡처를 활성화합니다.
3. ASA에서 ASP(Accelerated Security Path) 카운터를 지웁니다.
4. 네트워크의 호스트로 전송된 디버그 레벨에서 트랩 syslog를 활성화합니다.
5. HTTP 클라이언트에서 문제가 있는 HTTP 서버로 HTTP 세션을 시작하고 연결 실패 후 syslog 출력 및 이러한 명령의 출력을 수집합니다.**캡처 캡처 내부 표시캡처 캡처 외부 표시show capture mss-captureasp 삭제 표시참고:** 이 오류 메시지에 대한 자세한 내용은 시스템 로그 메시지 419001을 참조하십시오.

해결 방법

ASA가 클라이언트에서 광고하는 MSS 값을 초과하는 패킷을 삭제한다는 사실을 알고 있는 경우 해결 방법을 구현합니다. 클라이언트에서 버퍼 오버런이 발생할 수 있으므로 이러한 패킷이 클라이언트에 도달하는 것을 허용하지 않을 수도 있습니다. ASA를 통해 이러한 패킷을 허용하도록 선택한 경우 이 해결 절차를 진행합니다.

MPF(Modular Policy Framework)는 7.0 릴리스의 새로운 기능으로, ASA를 통해 이러한 패킷을 허용하는 데 사용됩니다. 이 문서는 MPF를 완전히 자세히 설명하도록 설계되지 않았지만 문제를 해결하는 데 사용되는 구성 엔티티를 제안합니다. MPF에 대한 자세한 내용은 ASA 8.3 컨피그레이션 가이드를 참조하십시오.

해결 방법에 대한 개요에는 액세스 목록을 통한 HTTP 클라이언트 및 서버 식별이 포함됩니다. 액세스 목록이 정의되면 클래스 맵이 생성되고 액세스 목록이 클래스 맵에 할당됩니다. 그런 다음 TCP 맵이 구성되고 MSS를 초과하는 패킷을 허용하는 옵션이 활성화됩니다. TCP 맵 및 클래스 맵이 정의되면 새 정책 맵이나 기존 정책 맵에 추가할 수 있습니다. 그런 다음 정책 맵이 보안 정책에 할당됩니다. 컨피그레이션 모드에서 **service-policy** 명령을 사용하여 전역 또는 인터페이스에서 정책 맵을 활성화합니다. 이러한 컨피그레이션 매개변수는 Cisco ASA(Adaptive Security Appliance) 8.3 컨피그레이션 목록에 추가됩니다. "http-map1"이라는 정책 맵을 만든 후 이 샘플 컨피그레이션은 이 정책 맵에 클래스 맵을 추가합니다.

특정 인터페이스: MSS를 초과하는 패킷을 허용하는 MPF 구성

```
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#
```

이러한 컨피그레이션 매개변수가 구축되면 클라이언트에서 광고하는 MSS를 초과하는 192.168.9.2의 패킷이 ASA를 통해 허용됩니다. 클래스 맵에 사용되는 액세스 목록은 192.168.9.2에 대한 아웃바운드 트래픽을 식별하도록 설계되었습니다. 검사 엔진이 나가는 SYN 패킷에서 MSS를 추출할 수 있도록 아웃바운드 트래픽을 검사합니다. 따라서 SYN의 방향을 고려하여 액세스 목록을 구성해야 합니다. 좀 더 광범위한 규칙이 필요한 경우 이 섹션의 **access-list** 문을 access-list http-list2 permit ip any any 또는 **access-list http-list2 permit tcp any any와** 같은 모든 것을 허용하는 **access-list** 문**으로** 바꿀 수 있습니다. 또한 TCP MSS 값이 큰 경우 VPN 터널이 느릴 수 있습니다. TCP MSS를 줄여 성능을 향상시킬 수 있습니다.

이 예에서는 ASA에서 전역 인바운드 및 아웃바운드 트래픽을 구성하는 데 도움이 됩니다.

전역 구성: MSS를 초과하는 패킷을 허용하는 MPF 구성

```
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#
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

구성 변경이 의도한 대로 수행되는지 확인하려면 Troubleshoot(문제 해결) 섹션의 단계를 반복합니다.

성공적인 연결의 Syslog

```
%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.
```

성공적인 연결의 show 명령 출력

```
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.
```

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- 보안 제품 필드 알림(Cisco ASA(Adaptive Security Appliance) 포함)
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems