Проблема ASA 8. 3: Клиенты MSS Exceeded - HTTP не могут посещать некоторые веб-сайты

Содержание

Введение

Этот документ описывает проблему, которая происходит, когда некоторые веб-сайты не доступны через Устройство адаптивной защиты (ASA), которое выполняет версию 8.3 или более позднее программное обеспечение.

Выпуск ASA 7.0 представляет несколько новых улучшений безопасности, одно из которых является проверкой для оконечных точек TCP, которые придерживаются Размера Сегмента объявленного максимума (MSS). В обычном сеансе TCP, клиент отправляет пакет SYN на сервер вместе с MSS, включенным в параметры TCP пакета SYN. Серверу после получения пакета SYN необходимо определить значение MSS, отправленное клиентом, а потом отправить свое собственное значение MSS в пакете SYN-ACK. Однажды и клиент и сервер знают о MSS друг друга, никакой узел не должен передавать пакет к другому, который больше, чем MSS того узла.

Обнаружение было сделано этим существует несколько серверов HTTP в Интернете, которые не соблюдают MSS, который объявляет клиент. Впоследствии, сервер HTTP передает пакеты данных клиенту, которые больше, чем объявленный MSS. Перед выпуском 7.0 эти пакеты были позволены через ASA. При усовершенствовании безопасности в ПО версии 7.0, данные пакеты стали по умолчанию отбрасываться. Этот документ разработан, чтобы помочь администратору устройства адаптивной защиты Cisco в диагнозе этой проблемы и реализации обходного пути позволять пакеты, которые превышают MSS.

См. PIX/ASA 7. X Проблем: Превышенный MSS - Клиенты HTTP не Может Перейти к

Некоторым веб-сайтам об одинаковой конфигурации на устройстве адаптивной защиты Cisco (ASA) с версиями 8.2 и ранее.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на устройстве адаптивной защиты Cisco (ASA), который выполняет программное обеспечение версии 8.3.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

См. Cisco Technical Tips Conventions для получения информации об условных обозначениях в документации.

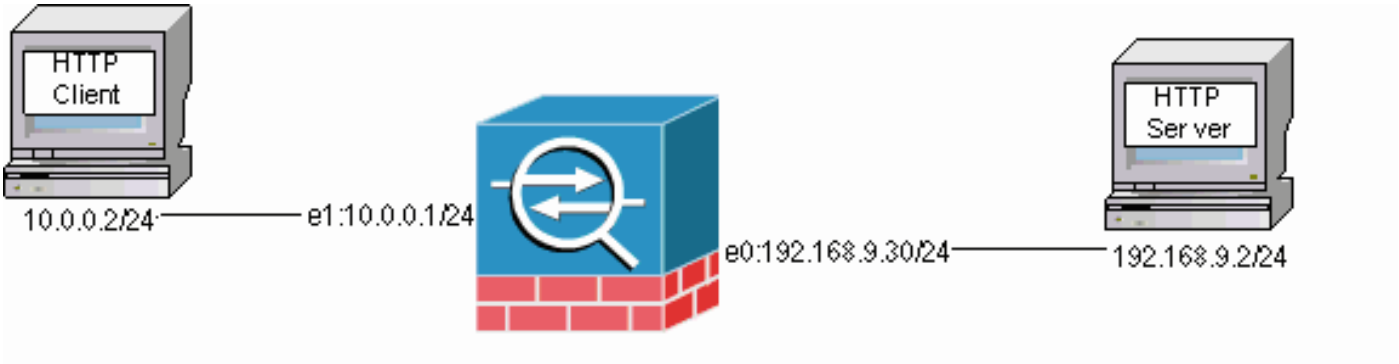
Настройка

В данном разделе содержится информация о настройке функций, описанных в этом документе.

Примечание: Для поиска дополнительных сведений о командах в данном документе используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



Конфигурация

ASA 8. 3

Эти команды настройки добавлены к конфигурации по умолчанию ASA 8.3, чтобы позволить клиенту HTTP связываться с сервером HTTP.

Конфигурация ASA 8. 3
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**

Устранение неполадок

Если определенный веб-сайт не доступен через ASA, выполните эти шаги для устранения проблем. Сначала захватите пакеты с соединения HTTP. Для сбора пакетов соответствующие IP-адреса сервера HTTP и клиента должны быть известны, а также IP-адрес, что клиент преобразован в то, когда это пересекает ASA.

В этом примере сети сервер HTTP имеет адрес 192.168.9.2, клиент HTTP имеет адрес 10.0.0.2, и адреса клиента HTTP преобразуются в 192.168.9.30, когда пакеты покидают внешний интерфейс. Можно использовать функцию перехвата устройства адаптивной защиты Cisco (ASA) для сбора пакетов, или можно использовать внешний захват пакета. При выборе функции захвата, администратор также может использовать новую функцию захвата в версии 7.0, которая позволяет захватывать пакеты, отброшенные из-за ненормальной работы TCP.

Примечание: Некоторые команды в этих таблицах переносятся к второй линии из-за пространственных ограничений.

1. Определите пару списков доступа, которые определяют пакеты как их вход и выход внутренние и внешние интерфейсы.
2. Включите функцию захвата для внешнего и внутреннего интерфейса. Также включите функцию захвата для пакетов с превышенным MSS конкретного TCP.
3. Очистите счетчики Ускоренного пути безопасности (ASP) на ASA.
4. Активируйте системный журнал сообщений на уровне отладки для пакетов, отправленных к хосту в сети.
5. Инициируйте сеанс HTTP от клиента HTTP до проблематичного сервера HTTP и соберите вывод системного журнала и выходные данные от этих команд после сбоев соединения.**show capture capture-insideshow capture capture-outsideshow capture mss-captureshow asp dropПримечание:** Дополнительные сведения об этом сообщении об ошибке см. в разделе Сообщения системного журнала 419001.

Обходной путь

Внедрите обходной путь теперь, когда вы знаете, что ASA отбрасывает пакеты, которые

превышают значение MSS, объявленное клиентом. Помните, что вам не обязательно, чтобы все пакеты достигли клиента, так как это может привести к переполнению буфера клиента. Если вы принимаете решение позволить эти пакеты через ASA, продолжить эту обходную процедуру.

Модульная система политик (MPF) является новой характеристикой в этих 7.0 выпусках, которые используются для разрешения этих пакетов через ASA. В данном документе не предоставляется подробного описания MPF, а предлагаются записи конфигурации, которые используются для решения данной проблемы. См. руководство по конфигурации ASA 8.3 и Справочник по командам ASA 8.3 для получения дополнительной информации о MPF и любой из команд, перечисленных в этом разделе.

В обзор обходного пути включена идентификация клиента HTTP и серверов через список доступа. Когда список доступа определен, создается карта класса, и для нее назначается список доступа. После этого настраивается карта tcp и активируется разрешение прохождения пакетов, которые превышают MSS. Когда карта tcp и карта класса определены, можно добавить их в новую или существующую карту политики. После этого карта политики назначается для политики безопасности. Используйте **команду service-policy** в режиме конфигурации для активации карты политик глобально или на интерфейсе. Эти параметры конфигурации добавлены к устройству адаптивной защиты Cisco (ASA) 8.3 Списков Конфигурации. После создания карты политики под названием http-map1, данная примерная конфигурация добавляет карту класса в карту политики.

Определенный интерфейс: Конфигурация MPF, чтобы разрешить прохождение пакетов, превышающих MSS
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#

Как только эти параметры конфигурации существуют, пакеты от 192.168.9.2, которые превышают MSS, объявленный клиентом, позволены через ASA. Важно отметить, что список доступа, который используется в карте класса, разработан для определения исходящего трафика для 192.168.9.2. Исходящий трафик рассматривается, чтобы разрешить модулю проверки извлекать MSS в исходящем пакете SYN. Таким образом, необходимо настраивать список доступа, учитывая направление SYN. Если более распространяющееся правило требуется, можно заменить **оператор access-list** в этом разделе с **оператором access-list**, который разрешает все, такое как **permit ip any any http-list2 access-list**, или **http-list2 access-list разрешают tcp любого любой**. Также помните, что прохождение по туннелю VPN может быть замедлено из-за большого значения MSS TCP. Можно уменьшить MSS TCP, чтобы улучшить производительность.

Данный пример помогает настраивать глобально входящий и исходящий трафик в ASA:

Глобальная конфигурация: Конфигурация MPF, чтобы разрешить прохождение пакетов, превышающих MSS

```
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#
```

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Повторите шаги в раздел Устранения неполадок, чтобы проверить, что изменения конфигурации делают то, что они разработаны, чтобы сделать.

Системные журналы при успешном подключении

```
%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.
```

Выходные данные команд show при успешном подключении

```
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.
```

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Уведомления о дефекте для специалистов по продуктам безопасности (включая устройство адаптивной защиты Cisco (ASA))
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация