Проблема с PIX/ASA 7.0: превышено допустимое значение MSS – HTTP-клиенты не могут просматривать определенные веб-сайты

Содержание

Введение

В данном документе описана проблема недоступности некоторых веб-сайтов через PIX или устройство адаптивной защиты (ASA) версии 7.0 или более поздних. В версии 7.0 представлено несколько новых усовершенствований в системе безопасности, одной из которых является проверка конечных точек TCP, соответствующих заявленному максимальному размеру сегмента (MSS; Maximum Segment Size). 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. Обменявшись сведениями о MSS, ни один одноранговый узел не должен отправлять другому пакет, размер которого больше MSS данного узла. Выяснилось, что существует несколько серверов HTTP в сети Интернет, которые не учитывают MSS, заявленный клиентом. Впоследствии, сервер HTTP отправляет клиенту пакеты данных, которые большие заявленных MSS. До выпуска версии 7.0 данным пакетам было разрешено проходить через устройство защиты PIX. При усовершенствовании безопасности в ПО версии 7.0, данные пакеты стали по умолчанию отбрасываться. Данный документ разработан для помощи администратору устройства защиты PIX/ASA в диагностике данной проблемы и реализации обходного пути, чтобы разрешить прохождение пакетов, превышающих MSS.

Предварительные условия

Требования

Для данного документа нет особых требований.

Используемые компоненты

Сведения в данном документе относятся к устройству защиты Cisco PIX 525 под управлением ПО версии 7.0.1.

Данные для документа были получены в специально созданных лабораторных условиях. Все устройства, используемые в этом документе, были запущены с чистой (заданной по умолчанию) конфигурацией. Если ваша сеть работает в реальных условиях, убедитесь, что вы понимаете потенциальное воздействие каждой команды.

Соответствующие продукты

Этот документ также может использоваться со следующими версиями программного и аппаратного обеспечения:

- На всех остальных платформах устройства защиты Cisco PIX используется версия 7.0. В данные платформы включены 515, 515E и 535.
- Все платформы Cisco ASA. В данные платформы включены 5510, 5520 и 5540.

Условные обозначения

Подробные сведения о применяемых в документе обозначениях см. в статье Условные обозначения, используемые в технической документации Cisco.

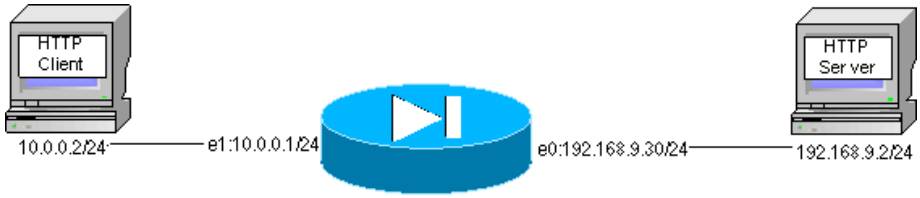
Настройка

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 данном документе используется следующая схема сети.



Настройка устройства защиты PIX версии 7.0

Эти команды конфигурации добавляются в конфигурацию PIX 7.0 по умолчанию, чтобы разрешить клиенту HTTP связываться с сервером HTTP.

Конфигурация PIX 7.0.1

```
pixfirewall(config)#interface Ethernet0
pixfirewall(config-if)#speed 100
pixfirewall(config-if)#duplex full
pixfirewall(config-if)#nameif outside
pixfirewall(config-if)#security-level 0
pixfirewall(config-if)#ip address 192.168.9.30 255.255.255.0
pixfirewall(config-if)#exit
pixfirewall(config)#interface Ethernet1
pixfirewall(config-if)#speed 100
pixfirewall(config-if)#duplex full
pixfirewall(config-if)#nameif inside
pixfirewall(config-if)#security-level 100
pixfirewall(config-if)#ip address 10.0.0.1 255.255.255.0
pixfirewall(config-if)#exit
pixfirewall(config)#global (outside) 1 interface
pixfirewall(config)#nat (inside) 1 10.0.0.0 255.0.0.0
pixfirewall(config)#route outside 0.0.0.0 0.0.0.0 192.168.9.2 1
```

Поиск и устранение неполадок

Если определенный веб-сайт недоступен через устройство защиты PIX/ASA, выполните следующие действия, чтобы устранить данную неполадку. Сначала захватите пакеты с соединения HTTP. Чтобы собрать пакеты, необходимо знать соответствующие IP-адреса сервера HTTP и клиента, а также IP-адрес, в который преобразовывается адрес клиента во время прохождения через устройство защиты PIX. 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 захвата устройства защиты PIX/ASA, чтобы собрать пакеты, или внешнее устройство захвата пакетов. 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. В следующих таблицах некоторые из команд записаны в двух строках из-за нехватки пространства.

1. Определите пару списков доступа, которые определяют пакеты, когда они входят и выходят на внешних и внутренних интерфейсах.

Конфигурация списка доступа для захвата пакетов
pixfirewall(config)#**access-list capture-list-in line 1 permitip host 10.0.0.2 host 192.168.9.2** pixfirewall(config)#**access-list capture-list-in line 2 permit ip host 192.168.9.2 host 10.0.0.2** pixfirewall(config)#**access-list capture-list-out line 1 permit ip host 192.168.9.30 host 192.168.9.2** pixfirewall(config)#**access-list capture-list-out line 2 permit ip host 192.168.9.2 host 192.168.9.30**

2. Включите функцию захвата для внешнего и внутреннего интерфейса. Также включите функцию захвата для пакетов с превышенным MSS конкретного TCP.

Конфигурация функции захвата для захвата пакетов
pixfirewall(config)#**capture capture-outside access-list capture-list-out packet-length 1518 interface outside** pixfirewall(config)#**capture capture-inside access-list capture-list-in packet-length 1518 interface inside** pixfirewall(config)#**capture mss-capture type asp-drop tcp-mss-exceeded packet-length 1518**

3. Обнулите счетчики пути ускоренной защиты (ASP) на устройстве защиты PIX.

Очистите статистики сброса ASP
pixfirewall(config)#**clear asp drop**

4. Активируйте системный журнал сообщений на уровне отладки для пакетов, отправленных к хосту в сети.

Активируйте регистрацию сообщений
pixfirewall(config)#**logging on** pixfirewall(config)#**logging host inside 10.0.0.2** pixfirewall(config)#**logging trap debug**

5. Инициируйте сеанс HTTP от клиента HTTP до проблемного сервера HTTP.

   Соберите данные регистрации и выходные данные команд после сбоя соединения.

- **show capture capture-inside**
- **show capture capture-outside**
- **show capture mss-capture**
- **show asp drop**

Системные журналы при неудачном подключении

```
%PIX-6-609001: Built local-host inside:10.0.0.2
%PIX-6-609001: Built local-host outside:192.168.9.2
%PIX-6-305011: Built dynamic TCP translation from inside:10.0.0.2/58565 to
outside:192.168.9.30/1024
%PIX-6-302013: Built outbound TCP connection 3 for outside:192.168.9.2/80
(192.168.9.2/80) to inside:10.0.0.2/58565 (192.168.9.30/1024)
%PIX-5-304001: 10.0.0.2 Accessed URL 192.168.9.2:/

!--- В нормальных условиях вы ожидаете
!--- увидеть мгновенный разрыв подключения
!--- после извлечения веб-контента с
!--- сервера HTTP. Если возникает данная проблема,
!--- пакеты данных с сервера HTTP отбрасываются на
!--- внешнем интерфейсе, а подключение
!--- остается, пока одна из сторон не сбросит это подключение
!--  или пока не истечет таймер неактивного соединения в устройстве защиты
!--- PIX. Таким образом, вы не сразу
!--- увидите сообщение системного журнала 302014 (разрыв TCP).



!--- В PIX версии 7.0.2 и более поздних, устройство защиты PIX
!--- использует системный журнал, если получает
!--- пакет, превышающий заявленный MSS. Системный журнал,
!--- используемый по умолчанию для уровня предупреждения, имеет следующий формат:


%PIX-4-419001: Dropping TCP packet from outside:192.168.9.2/80 to
inside:192.168.9.30/1025, reason: MSS exceeded, MSS 460, data 1440



!--- В ASA версии 7.0.2 и более поздних устройство защиты ASA
!--- использует системный журнал, если получает
!--- пакет, превышающий заявленный MSS. Системный журнал,
!--- используемый по умолчанию для уровня предупреждения, имеет следующий формат:


%ASA-4-419001: Dropping TCP packet from outside:192.168.9.2/80 to
inside:192.168.9.30/1025, reason: MSS exceeded, MSS 460, data 1440
```

Примечание. Дополнительные сведения об этом сообщении об ошибке см. в разделе Сообщения системного журнала 419001.

Выходные данные команд show при неудачном подключении

```
pixfirewall#show capture capture-inside
6 packets captured
  1: 08:59:59.362301 10.0.0.2.58565 > 192.168.9.2.80:
     S 3965932251:3965932251(0) win 1840 < mss 460,sackOK,timestamp
     110211948 0,nop,wscale 0>

!--- Заявленный MSS клиента составляет 460 в пакете #1.


  2: 08:59:59.552156 192.168.9.2.80 > 10.0.0.2.58565:
     S 1460644203:1460644203(0) ack 3965932252 win 8192 <mss 1380>
  3: 08:59:59.552354 10.0.0.2.58565 > 192.168.9.2.80: . ack 1460644204 win 1840
  4: 08:59:59.552629 10.0.0.2.58565 > 192.168.9.2.80:
     P 3965932252:3965932351(99) ack 1460644204 win 1840
  5: 08:59:59.725960 192.168.9.2.80 > 10.0.0.2.58565: . ack 3965932351 win 8192
  6: 08:59:59.726189 192.168.9.2.80 > 10.0.0.2.58565: . ack 3965932351 win 65340
6 packets shown
pixfirewall#
pixfirewall#
pixfirewall#show capture capture-outside
```

```
16 packets captured
  1: 08:59:59.362636 192.168.9.30.1024 > 192.168.9.2.80:
     S 473738107:473738107(0) win 1840 <mss 460,sackOK,timestamp
     110211948 0,nop,wscale 0>

!--- Заявленный MSS клиента составляет 460 в пакете #1.


  2: 08:59:59.552110 192.168.9.2.80 > 192.168.9.30.1024:
     S 314834194:314834194(0) ack 473738108 win 8192 <mss 1460>
  3: 08:59:59.552370 192.168.9.30.1024 > 192.168.9.2.80: . ack 314834195 win 1840
  4: 08:59:59.552675 192.168.9.30.1024 > 192.168.9.2.80:
     P 473738108:473738207(99) ack 314834195 win 1840
  5: 08:59:59.725945 192.168.9.2.80 > 192.168.9.30.1024: . ack 473738207 win 8192
  6: 08:59:59.726173 192.168.9.2.80 > 192.168.9.30.1024: . ack 473738207 win 65340

!--- В пакетах от 7 до 14 длина пакета превышает 460.
!--- Пакеты от 7 до 14 не прослеживаются в трассировке внутреннего захвата.
!--- Это означает, что они отбрасываются с помощью устройства защиты PIX.
!--- Пакеты от 7 до 14 также представлены в выходных данных
!--- команды show capture mss-capture.


  7: 08:59:59.734199 192.168.9.2.80 > 192.168.9.30.1024:
     . 314834195:314835647(1452) ack 473738207 win 65340
  8: 08:59:59.742072 192.168.9.2.80 > 192.168.9.30.1024:
     P 314835647:314837099(1452) ack 473738207 win 65340
  9: 08:59:59.757986 192.168.9.2.80 > 192.168.9.30.1024:
     . 314837099:314838551(1452) ack 473738207 win 65340
 10: 08:59:59.765661 192.168.9.2.80 > 192.168.9.30.1024:
     P 314838551:314840003(1452) ack 473738207 win 65340
 11: 08:59:59.771276 192.168.9.2.80 > 192.168.9.30.1024:
     P 314840003:314841035(1032) ack 473738207 win 65340
 12: 09:00:02.377604 192.168.9.2.80 > 192.168.9.30.1024:
     P 314834195:314835647(1452) ack 473738207 win 65340
 13: 09:00:07.452643 192.168.9.2.80 > 192.168.9.30.1024:
     P 314834195:314835647(1452) ack 473738207 win 65340
 14: 09:00:17.680049 192.168.9.2.80 > 192.168.9.30.1024:
     P 314834195:314835647(1452) ack 473738207 win 65340
 15: 09:00:29.670680 192.168.9.2.80 > 192.168.9.30.1024:
     F 314841035:314841035(0) ack 473738207 win 65340
 16: 09:00:29.670711 192.168.9.30.1024 > 192.168.9.2.80:
     P ack 314834195 win 1840
16 packets shown
pixfirewall#
pixfirewall#
pixfirewall(config)#show capture mss-capture
8 packets captured
  1: 08:59:59.734214 192.168.9.2.80 > 192.168.9.30.1024:
     . 314834195:314835647(1452) ack 473738207 win 65340
  2: 08:59:59.742086 192.168.9.2.80 > 192.168.9.30.1024:
     P 314835647:314837099(1452) ack 473738207 win 65340
  3: 08:59:59.758000 192.168.9.2.80 > 192.168.9.30.1024:
     . 314837099:314838551(1452) ack 473738207 win 65340
  4: 08:59:59.765673 192.168.9.2.80 > 192.168.9.30.1024:
     P 314838551:314840003(1452) ack 473738207 win 65340
  5: 08:59:59.771291 192.168.9.2.80 > 192.168.9.30.1024:
     P 314840003:314841035(1032) ack 473738207 win 65340
  6: 09:00:02.377619 192.168.9.2.80 > 192.168.9.30.1024:
     P 314834195:314835647(1452) ack 473738207 win 65340
  7: 09:00:07.452658 192.168.9.2.80 > 192.168.9.30.1024:
     P 314834195:314835647(1452) ack 473738207 win 65340
  8: 09:00:17.680063 192.168.9.2.80 > 192.168.9.30.1024:
     P 314834195:314835647(1452) ack 473738207 win 65340
8 packets shown
pixfirewall#
pixfirewall#
pixfirewall#show asp drop

Frame drop:
 TCP MSS was too large 8

Flow drop:
pixfirewall#

!--- Команда show asp drop показывает,
!--- что восемь пакетов были отброшены, так как
!--- TCP MSS слишком большой. Это подтверждает сведения, извлеченные из
!--- захватов пакетов.
```

Обходной путь

Теперь, когда известно, что устройство защиты PIX/ASA отбрасывает пакеты, превышающие значение MSS, заявленное клиентом, реализуйте обходной путь. Помните, что вам не обязательно, чтобы все пакеты достигли клиента, так как это может привести к переполнению буфера клиента. Выбрав разрешить прохождение всех пакетов через устройство защиты PIX/ASA, выполните следующую процедуру обходного пути. Чтобы разрешить прохождение пакетов через устройство защиты PIX, в версии 7.0 используется новая функция под названием Система модульных политик (MPF). В данном документе не предоставляется подробного описания MPF, а предлагаются записи конфигурации, которые используются для решения данной проблемы. Дополнительные сведения о MPF и командах, указанных в данной главе, см. в разделе Руководство по конфигурации PIX 7.0 и Справочник по командам PIX 7.0.

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 в режиме конфигурации **service-policy**, чтобы глобально активировать карту политики на внешнем интерфейсе. Данные параметры конфигурации добавляются в Список конфигураций PIX 7.0. После создания карты политики под названием http-map1, данная примерная конфигурация добавляет карту класса в карту политики.

Конфигурация MPF, чтобы разрешить прохождение пакетов, превышающих MSS

```
pixfirewall(config)#access-list http-list2 permit tcp any host 192.168.9.2
pixfirewall(config)#
pixfirewall#configure terminal
pixfirewall(config)#
pixfirewall(config)#class-map http-map1
pixfirewall(config-cmap)#match access-list http-list2
pixfirewall(config-cmap)#exit
pixfirewall(config)#tcp-map mss-map
pixfirewall(config-tcp-map)#exceed-mss allow
pixfirewall(config-tcp-map)#exit
pixfirewall(config)#policy-map http-map1
pixfirewall(config-pmap)#class http-map1
pixfirewall(config-pmap-c)#set connection advanced-options mss-map
pixfirewall(config-pmap-c)#exit
pixfirewall(config-pmap)#exit
pixfirewall(config)#service-policy http-map1 interface outside
pixfirewall#
```

После установки этих параметров конфигурации, пакеты из 192.168.9.2, превышающие заявленные клиентом MSS, могут проходить через устройство защиты PIX. 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 необходимо более общее правило, можно заменить утверждения списка доступа в данном разделе списком доступа, который разрешает все, например, **access-list http-list2 permit ip any any** или **access-list http-list2 permit tcp any any**. Также помните, что прохождение по туннелю VPN может быть замедлено из-за большого значения MSS TCP. Можно уменьшить MSS TCP, чтобы улучшить производительность.

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Повторите действия в разделе Устранение неполадок, чтобы убедиться, что изменения конфигурации выполняют свое предназначение.

Системные журналы при успешном подключении

```
%PIX-6-609001: Built local-host inside:10.0.0.2
%PIX-6-609001: Built local-host outside:192.168.9.2
%PIX-6-305011: Built dynamic TCP translation from inside:10.0.0.2/58798
               to outside:192.168.9.30/1025
```

```
%PIX-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)
%PIX-5-304001: 10.0.0.2 Accessed URL 192.168.9.2:/

%PIX-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

!--- Подключение создается и тут же прерывается,
!--- если извлекается веб-контент.
```

Выходные данные команд show при успешном подключении

```
pixfirewall#
pixfirewall#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>

!--- Заявленный MSS клиента составляет 460 в пакете #1.
!--- Однако с настроенным обходным путем пакеты 7, 9, 11, 13
!--- и 15 отображаются во внутренней трассировке, несмотря на 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
pixfirewall#
pixfirewall#
pixfirewall#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
pixfirewall#
pixfirewall(config)#show capture mss-capture
0 packets captured
0 packets shown
pixfirewall#
pixfirewall#show asp drop
```

```
Frame drop:

Flow drop:
pixfirewall#

!--- Команды show capture mss-capture
!--- и show asp drop отображают, что нет отброшенных пакетов.
```

Дополнительные сведения

- **ПО межсетевого экрана CiscoPIX**
- **Справочники по командам для межсетевого экрана Cisco Secure PIX**
- **Уведомления о продуктах безопасности (включая PIX)**
- **Запросы на комментарии RFC**
- **Cisco Systems – техническая поддержка и документация**

Дата генерации PDF файла: Jan 05, 2010

---

http://www.cisco.com/support/RU/customer/content/10/107636/pix-asa-70-browse.shtml

---