Работа с перехватами Защиты угрозы FirePOWER (FTD) и пакетным трассировщиком

Содержание

Введение

Этот документ описывает, как работать с перехватами Защиты угрозы FirePOWER (FTD) и Утилитами Packet Tracer.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

- ASA5515X, выполняющий код 6.1.0 FTD (создают 330),
- FPR4110, выполняющий код 6.2.2 FTD (создают 81),
- Центр управления FirePOWER (FMC), работающий 6.1.0 (создают 330),
- Центр управления FirePOWER (FMC), работающий 6.2.2 (создают 81),

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

Общие сведения

Захваты пакета являются одним из обычно используемых средств устранения проблем. Варианты использования захватов пакета:

- Доказать, что пакет поступает в устройство
- Доказать, что пакет оставляет устройство
- Доказать, что пакет отброшен устройством (например, отбрасывания ASP)

Настройка

Предварительные условия

Требования

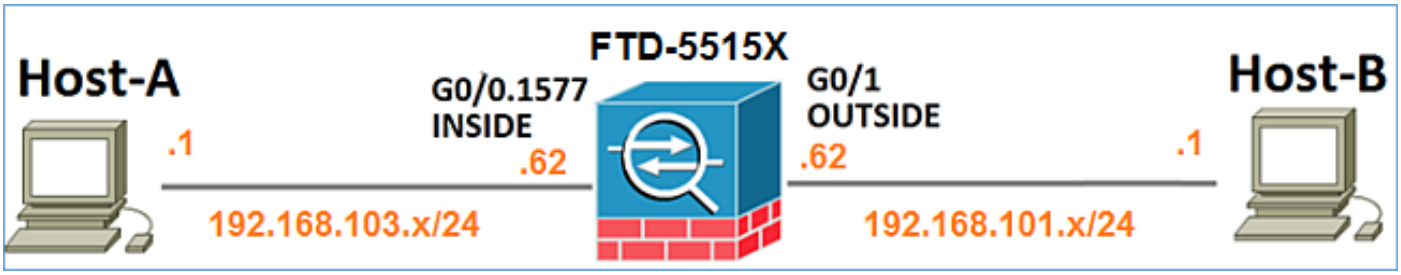
Для этого документа отсутствуют особые требования.

Используемые компоненты

- ASA5515-X рабочее программное обеспечение FTD 6.1.0
- FPR4110, выполняющий программное обеспечение FTD 6.2.2
- FS4000, выполняющий программное обеспечение FMC 6.2.2

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

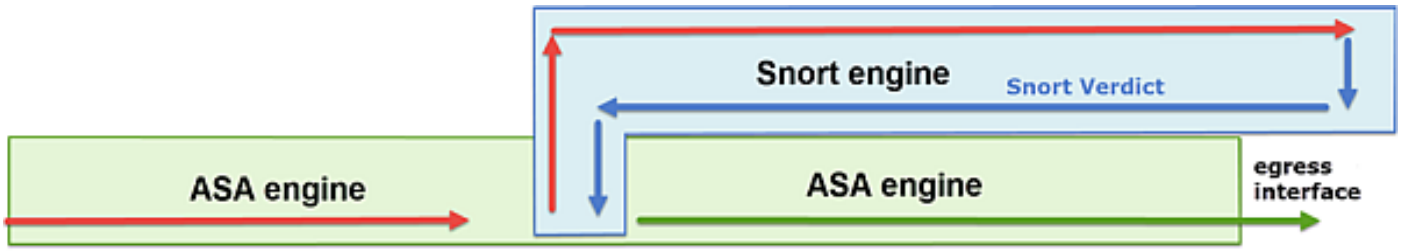
Схема сети



Общие сведения

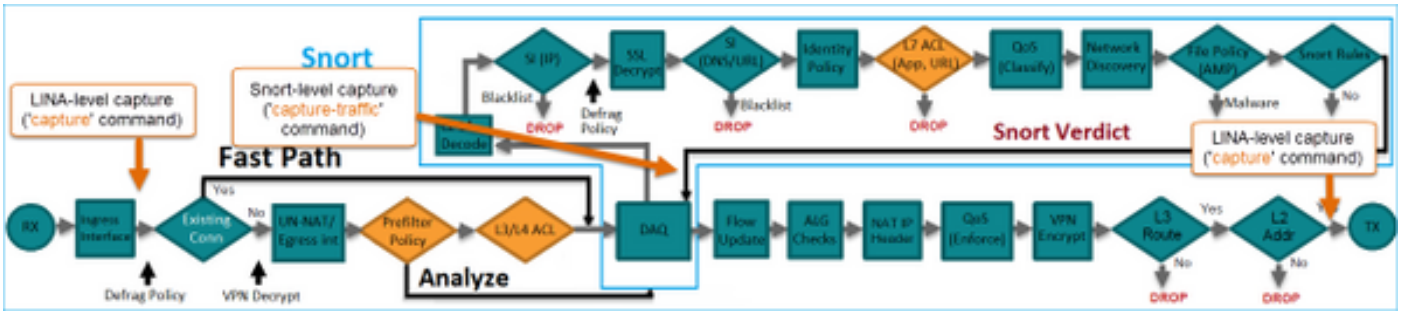
Пакетная обработка FTD

Пакетная обработка FTD может визуализироваться следующим образом:



1. Пакет вводит входной интерфейс, и это обрабатывается механизмом LINA.
2. Если политика требует, чтобы пакет был осмотрен механизмом Фырканья.
3. Механизм фырканья выносит вердикт (например, белый список, черный список) для пакета.
4. Механизм LINA отбрасывает или передает пакет на основе вердикта Фырканья.

На основе вышеупомянутой архитектуры перехваты FTD могут быть взяты на 2 других местах:



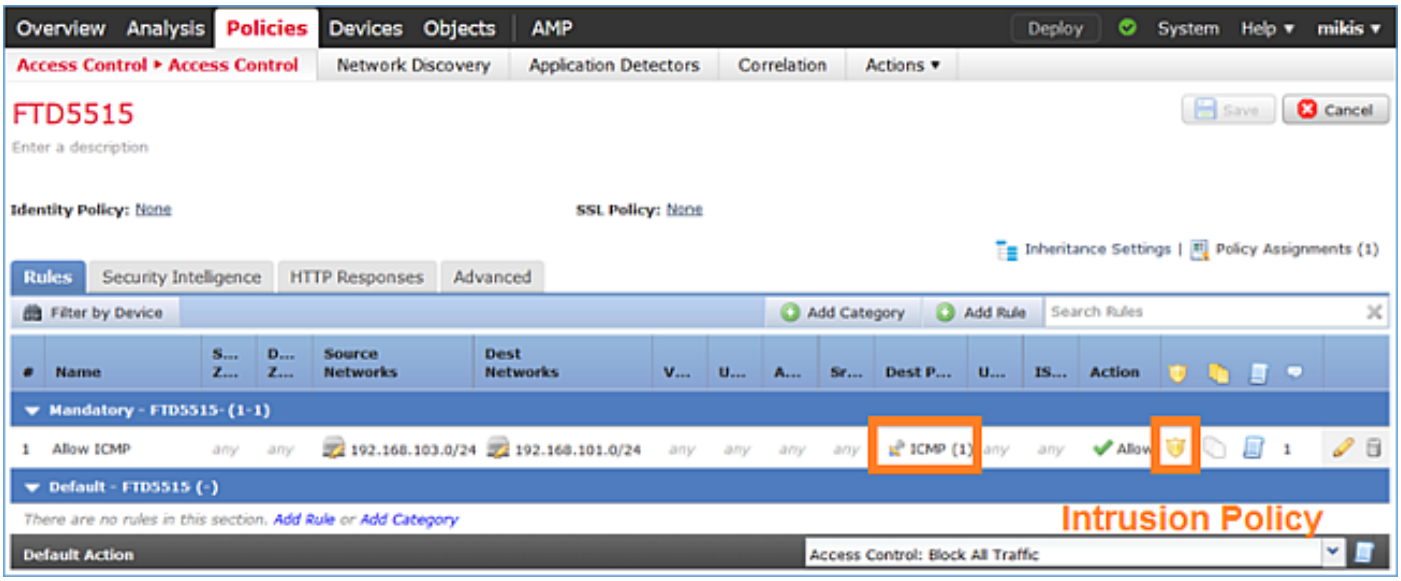
Настройка

Работайте с перехватами механизма Фырканья

Предварительные условия

Существует Политика контроля доступа (ACP), примененная на FTD, который позволяет

трафику ICMP проходить. Политика имеет также примененную Политику Проникновения:



Требования

1. Включите перехват на FTD CLISH режим, не используя фильтра.
2. Эхо-запрос через FTD и проверку перехват выведен.

Решение

Шаг 1. Вход в систему к консоли FTD или SSH к br1 взаимодействуют и включают перехват на FTD CLISH режим, не используя фильтра.

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

На FTD 6.0.x команда:

```
> system support capture-traffic
```

Шаг 2. Эхо-запрос через FTD и проверку перехват выведен.

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
12:52:34.749945 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0,
seq 1, length 80
12:52:34.749945 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq
1, length 80
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0,
seq 2, length 80
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq
2, length 80
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0,
seq 3, length 80
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq
3, length 80
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0,
seq 4, length 80
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq
4, length 80
^C<- to exit press CTRL + C
```

Работайте с перехватами механизма фырканья

Требования

1. Включите перехват на FTD CLISH режим с помощью фильтра для IP 192.168.101.1.
2. Эхо-запрос через FTD и проверку перехват выведен.

Решение

Шаг 1. Включите перехват на FTD CLISH режим с помощью фильтра для IP 192.168.101.1.

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
```

```
Options: host 192.168.101.1
```

Шаг 2. Эхо-запрос через FTD и проверку перехват вывел:

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: host 192.168.101.1
```

Можно использовать**-n** опцию для наблюдения хостов и номеров портов в числовом формате. Например, вышеупомянутый перехват покажут как:

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -n host 192.168.101.1
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 0, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 1, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 2, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 3, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 4, length 80
```

Примеры фильтра tcpdump

Пример 1

Перехватывать IP Src или IP Dst = 192.168.101.1 и порт Src или порт Dst = TCP/UDP 23:

```
Options: -n host 192.168.101.1 and port 23
```

Пример 2

Перехватывать IP Src = 192.168.101.1 и порт Src = TCP/UDP 23:

```
Options: -n src 192.168.101.1 and src port 23
```

Пример 3

Перехватывать IP Src = 192.168.101.1 и порт Src = TCP 23:

```
Options: -n src 192.168.101.1 and tcp and src port 23
```

Пример 4

Перехватывать IP Src = 192.168.101.1 и видеть, что MAC-адрес пакетов добавляет 'e' опцию:

```
Options: -ne src 192.168.101.1
17:57:48.709954 6c:41:6a:a1:2b:f6 > a8:9d:21:93:22:90, ethertype IPv4 (0x0800), length 58:
192.168.101.1.23 > 192.168.103.1.25420: Flags [S.], seq 3694888749, ack 1562083610, win 8192,
options [mss 1380], length 0
```

Пример 5

Выходить после получения 10 пакетов:

```
Options: -n -c 10 src 192.168.101.1
18:03:12.749945 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 3758037348, win 32768,
length 0
18:03:12.749945 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 1, win 32768, length
2
18:03:12.949932 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 1, win 32768, length
10
18:03:13.249971 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 3, win 32768, length 0
18:03:13.249971 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 3, win 32768, length
2
18:03:13.279969 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 5, win 32768, length 0
18:03:13.279969 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 5, win 32768, length
10
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 0
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 7, win 32768, length
12
18:03:13.349972 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 9, win 32768, length 0
```

Пример 6

Записать перехват в файл с названием capture.pcap и скопировать его через FTP к удаленному серверу:

```
Options: -w capture.pcap host 192.168.101.1 CTRL + C <- to stop the capture
> file copy 10.229.22.136 ftp / capture.pcap
Enter password for ftp@10.229.22.136:
Copying capture.pcap
Copy successful.

>
```

Работайте с FTD LINA перехваты механизма

Требования

1. Включите 2 перехвата на FTD использование следующих фильтров:

IP-адрес отправителя	192.168.103.1
IP-адрес назначения	192.168.101.1
Протокол	ICMP
Interface	Внутри
IP-адрес отправителя	192.168.103.1
IP-адрес назначения	192.168.101.1
Протокол	ICMP
Interface	СНАРУЖИ

2. Эхо-запрос от Хоста A (192.168.103.1) Хост B (192.168.101.1) и проверка перехваты.

Решение

Шаг 1. Включение перехватов:

```
> capture CAPI interface INSIDE match icmp host 192.168.103.1 host 192.168.101.1
> capture CAPO interface OUTSIDE match icmp host 192.168.101.1 host 192.168.103.1
```

Шаг 2. Проверка перехватов с помощью CLI.

Эхо-запрос от хоста A до хоста B:


```
> show capture
capture CAPI type raw-data interface INSIDE [Capturing - 752 bytes]
  match icmp host 192.168.103.1 host 192.168.101.1
capture CAPO type raw-data interface OUTSIDE [Capturing - 720 bytes]
  match icmp host 192.168.101.1 host 192.168.103.1
```

2 перехвата имеют другие размеры из-за заголовка Dot1Q на Внутреннем интерфейсе. Это можно показать в следующем результате:

```
> show capture CAPI
8 packets captured
   1: 17:24:09.122338 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   2: 17:24:09.123071 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
```

```
   3: 17:24:10.121392 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   4: 17:24:10.122018 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   5: 17:24:11.119714 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   6: 17:24:11.120324 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   7: 17:24:12.133660 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   8: 17:24:12.134239 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
8 packets shown
```

```
> show capture CAPO
8 packets captured
   1: 17:24:09.122765  192.168.103.1 > 192.168.101.1: icmp: echo request
   2: 17:24:09.122994  192.168.101.1 > 192.168.103.1: icmp: echo reply
   3: 17:24:10.121728  192.168.103.1 > 192.168.101.1: icmp: echo request
   4: 17:24:10.121957  192.168.101.1 > 192.168.103.1: icmp: echo reply
   5: 17:24:11.120034  192.168.103.1 > 192.168.101.1: icmp: echo request
   6: 17:24:11.120263  192.168.101.1 > 192.168.103.1: icmp: echo reply
   7: 17:24:12.133980  192.168.103.1 > 192.168.101.1: icmp: echo request
   8: 17:24:12.134194  192.168.101.1 > 192.168.103.1: icmp: echo reply
8 packets shown
```

Работайте с FTD LINA Перехваты Механизма – Экспорт Перехват через HTTP

Требования

Экспортируйте перехваты, взятые в предыдущем сценарии с помощью браузера.

Решение

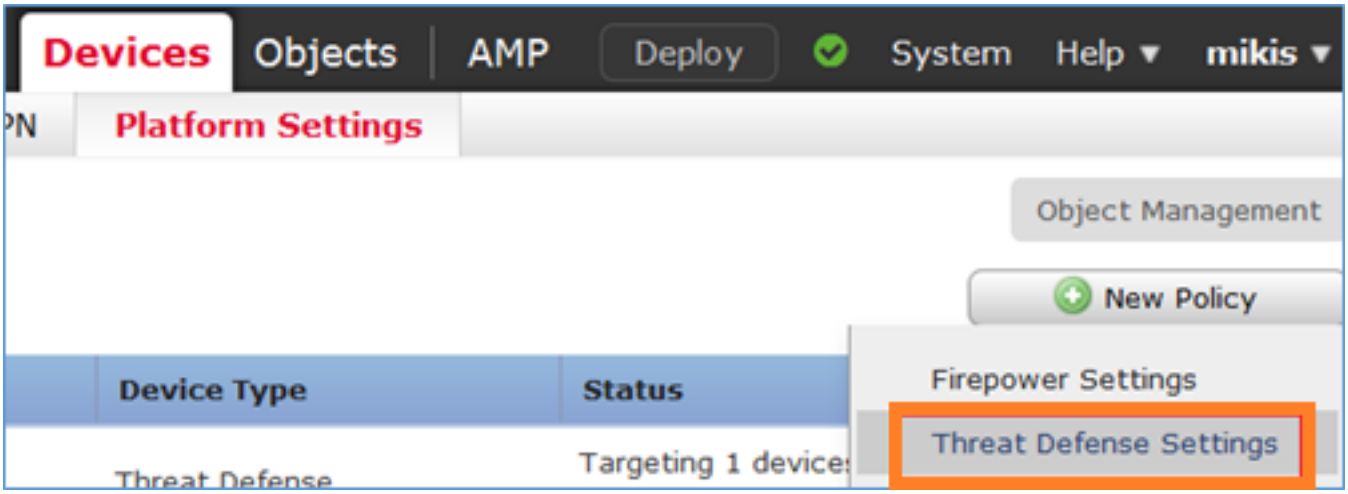
Для экспортирования перехватов с помощью браузера существует потребность к:

1. Включите сервер HTTPS.
2. Предоставьте доступ HTTPS.

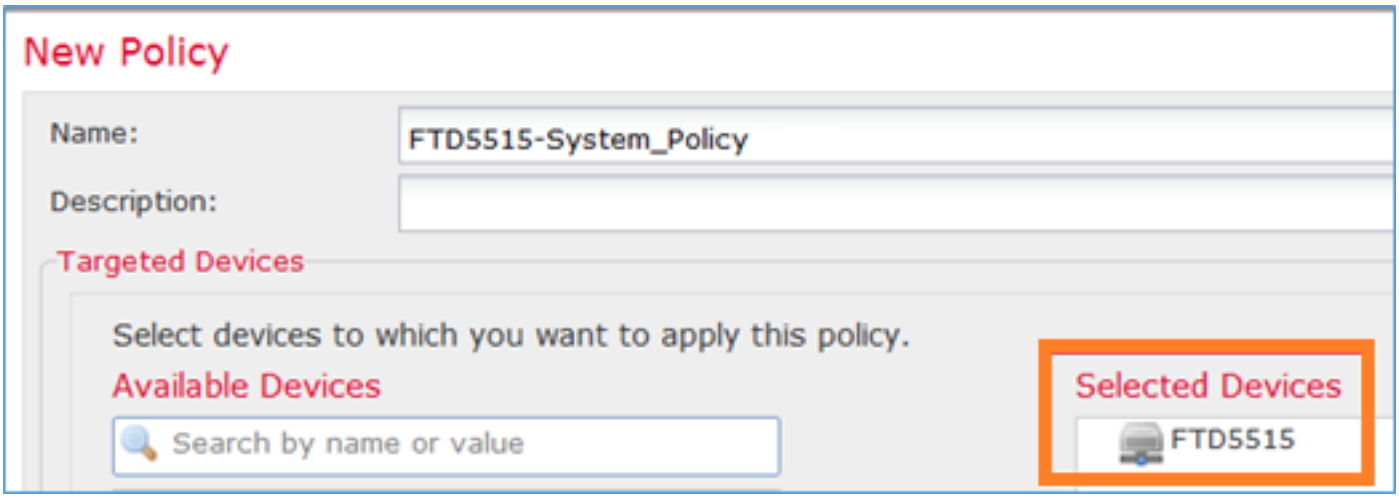
По умолчанию сервер HTTPS отключен, и никакой доступ не предоставлен:

```
> show running-config http

>
```

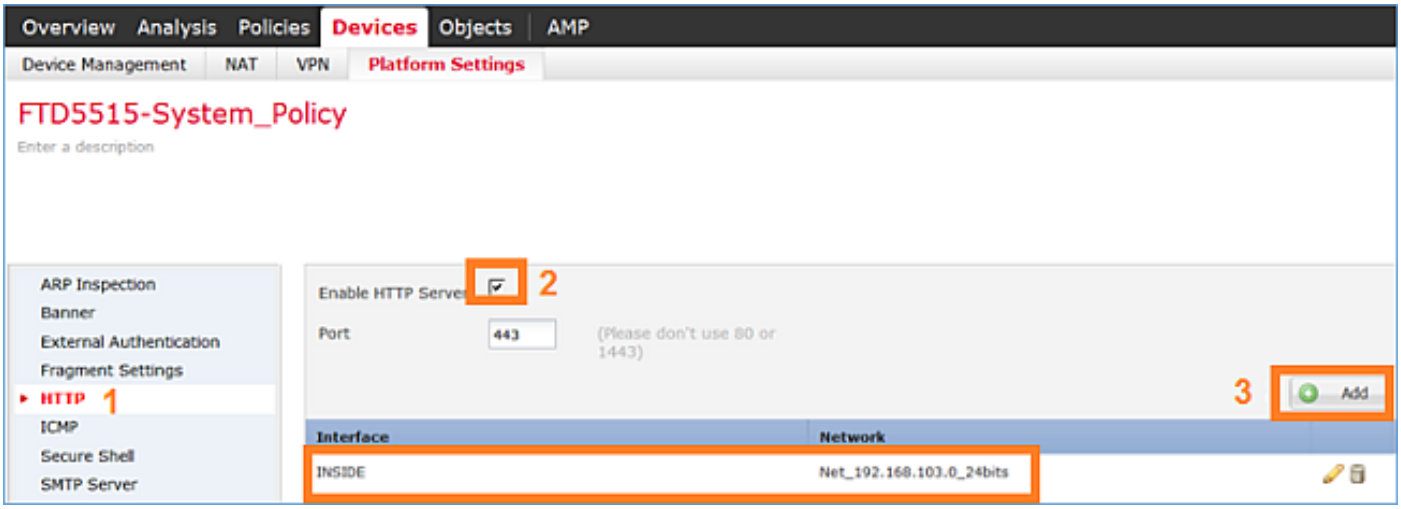
Шаг 1. Перейдите к **Устройствам> Параметры настройки Платформы,** щелкните **по New Policy** и выберите **Threat Defense Settings:**



Задайте название Политики и Адресата устройства:



Шаг 2. Включите сервер HTTPS и добавьте сеть, что вы хотите быть разрешенными обратиться к устройству FTD по HTTPS:



Сохраните и **развернитесь.**

Во время внедрения политики можно включить **http отладки**, чтобы видеть, что запускается сервис HTTP:

```
> debug http 255
```

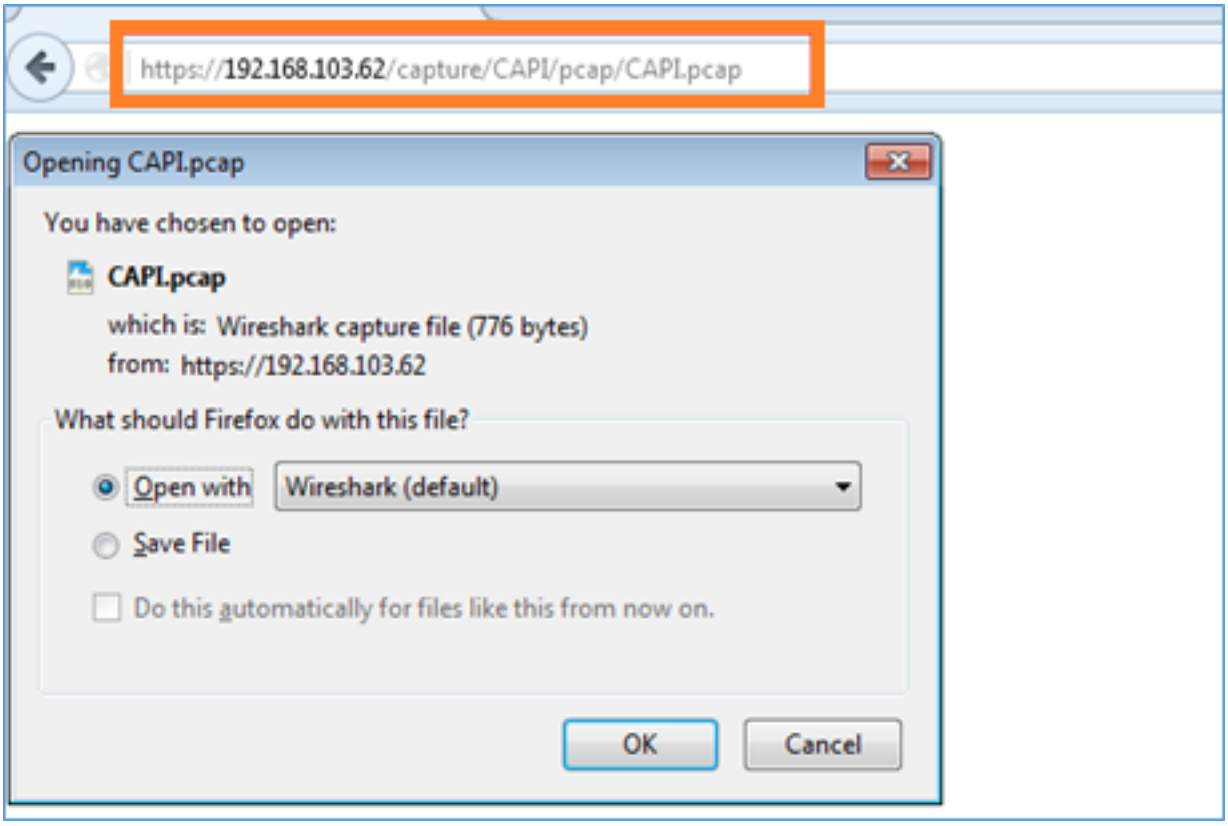
```
debug http enabled at level 255.
http_enable: Enabling HTTP server
HTTP server starting.
```

Результат на CLI FTD:

```
> unebug all
> show run http
http server enable http 192.168.103.0 255.255.255.0 INSIDE
```

Откройте браузер на Хосте A (192.168.103.1) и используйте следующий URL для загрузки первого перехвата:

https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap

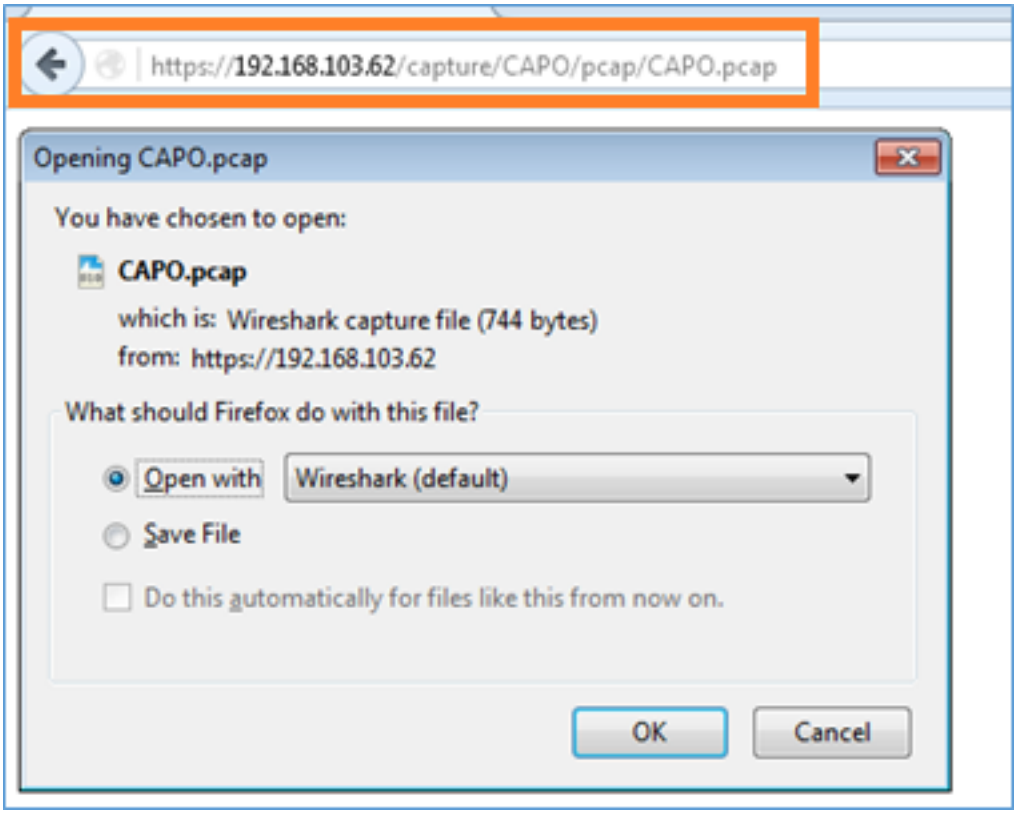


Для ссылки

https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	IP интерфейса данных FTD, где включен сервер HTTP
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	Название перехвата FTD
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	Название файла, который будет загружен

Для второго перехвата:

https://192.168.103.62/capture/CAPO/pcap/CAPO.pcap



Работайте с FTD LINA Перехваты Механизма – Экспорт Перехват через FTP/TFTP/SCP

Требования

Экспортируйте перехваты, взятые в предыдущих сценариях с помощью протоколов FTP/TFTP/SCP.

Решение

Экспортирование перехвата к серверу FTP:

```
firepower# copy /pcap capture:CAPI ftp://ftp_username:ftp_password@192.168.78.73/CAPI.pcap

Source capture name [CAPI]?

Address or name of remote host [192.168.78.73]?

Destination username [ftp_username]?

Destination password [ftp_password]?
```

```
Destination filename [CAPI.pcap]?
!!!!!!
114 packets copied in 0.170 secs
firepower#
```

Экспортирование перехвата к серверу TFTP:

```
firepower# copy /pcap capture:CAPI tftp://192.168.78.73

Source capture name [CAPI]?

Address or name of remote host [192.168.78.73]?

Destination filename [CAPI]?
!!!!!!!!!!!!!!!!
346 packets copied in 0.90 secs

firepower#
```

Экспортирование перехвата к серверу SCP:

```
firepower# copy /pcap capture:CAPI scp://scp_username:scp_password@192.168.78.55

Source capture name [CAPI]?

Address or name of remote host [192.168.78.55]?

Destination username [scp_username]?

Destination filename [CAPI]?
The authenticity of host '192.168.78.55 (192.168.78.55)' can't be established.
RSA key fingerprint is
<cb:ca:9f:e9:3c:ef:e2:4f:20:f5:60:21:81:0a:85:f9:02:0d:0e:98:d0:9b:6c:dc:f9:af:49:9e:39:36:96:33
>(SHA256).
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.78.55' (SHA256) to the list of known hosts.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
454 packets copied in 3.950 secs (151 packets/sec)

firepower#
```

Работайте с FTD LINA, перехваты механизма – отслеживают пакет реального трафика

Требования

Включите перехват на FTD использование следующих фильтров:

IP-адрес отправителя	192.168.103.1
IP-адрес назначения	192.168.101.1
Протокол	ICMP

Interface	Внутри
Пакетное отслеживание	да
Количество отслеживания пакетов	100

Эхо-запрос от Хоста A (192.168.103.1) Хост B (192.168.101.1) и проверка перехваты.

Решение

Отслеживание действительного пакета может быть очень полезно для устранения проблем проблем с подключением. Это позволяет видеть все внутренние проверки, которые проходит пакет. Добавьте '**подробные** ключевые слова' **трассировки** и задайте сумму пакетов, что вы хотите быть отслеженными. По умолчанию FTD отслеживает первые 50 входящих пакетов.

В этом случае включите перехват с подробностью трассировки для первых 100 пакетов, которые FTD получает на Внутреннем интерфейсе:

```
> capture CAPI2 interface INSIDE trace detail trace-count 100 match icmp host 192.168.103.1 host 192.168.101.1
```

Эхо-запрос от Хоста A до Хоста B и проверки результат:

```
C:\Users\cisco>ping 192.168.101.1

Pinging 192.168.101.1 with 32 bytes of data:
Reply from 192.168.101.1: bytes=32 time=2ms TTL=255
Reply from 192.168.101.1: bytes=32 time=2ms TTL=255
Reply from 192.168.101.1: bytes=32 time=2ms TTL=255
Reply from 192.168.101.1: bytes=32 time=8ms TTL=255
```

Захваченные пакеты:

```
> show capture CAPI2
8 packets captured
   1: 18:08:04.232989  802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   2: 18:08:04.234622  802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   3: 18:08:05.223941  802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   4: 18:08:05.224872  802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   5: 18:08:06.222309  802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   6: 18:08:06.223148  802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
   7: 18:08:07.220752  802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
   8: 18:08:07.221561  802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
8 packets shown
```

Следующий результат показывает трассировку первого пакета. Содержательные части:

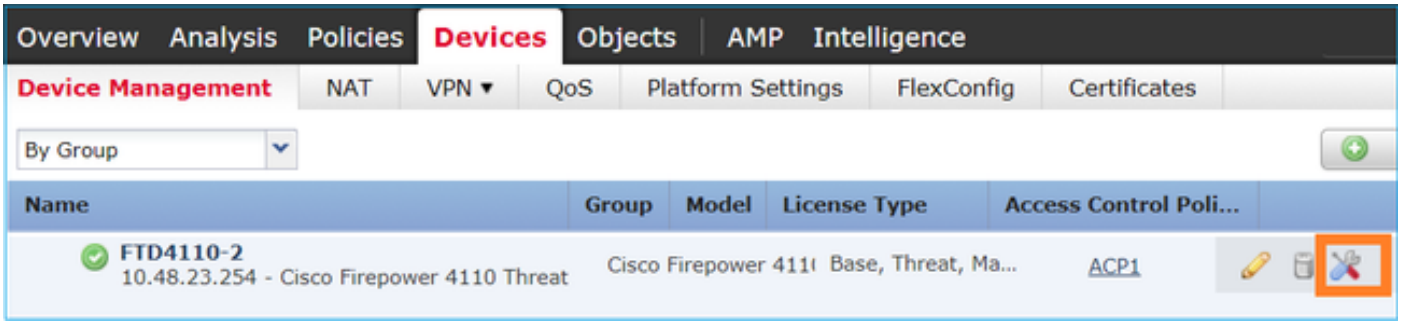
- Фаза 12, где может быть замечен 'прямой поток'. Это - Массив Отправки механизма LINA (эффективно внутренний заказ операций)
- Фаза 13, где FTD передает пакет для Фырканья экземпляра

- Фаза 14, где замечен Вердикт Фырканья

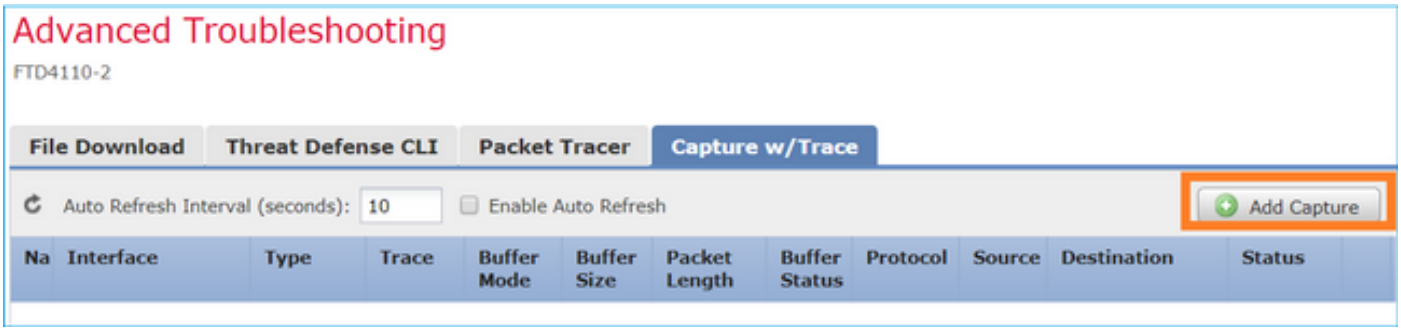
```
> show capture CAPI2 packet-number 1 trace detail
8 packets captured
   1: 18:08:04.232989 000c.2998.3fec a89d.2193.2293 0x8100 Length: 78
      802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request (ttl 128, id 3346)
Phase: 1
Type: CAPTURE
... output omitted ...

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 195, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_snort
snp_fp_inspect_icmp
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_inspect_icmp
snp_fp_snort
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Phase: 13
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

... output omitted ...

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow

1 packet shown
>
```

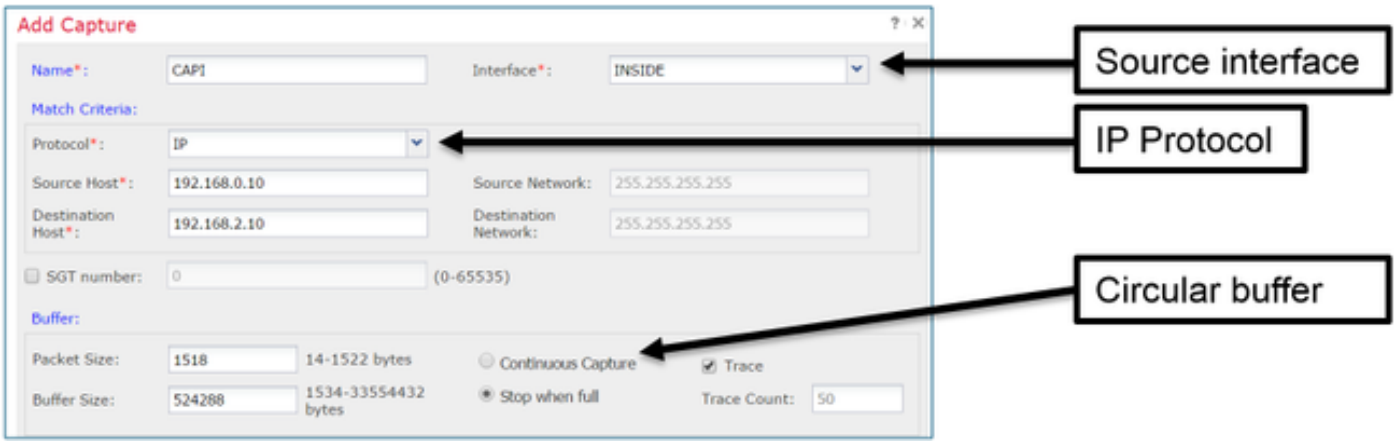
Программное средство перехвата в пост6.2 версиях программного обеспечения FMC

В FMC 6.2.x присваивают версию новому мастеру захвата пакета, был представлен. Перейдите к **Устройствам> Управление устройствами** и выберите значок **Устранения неполадок**. Затем выберите **Advanced Troubleshooting** и наконец **Перехват w/Trace.**



Выберите **Add Capture** для создания перехвата FTD:



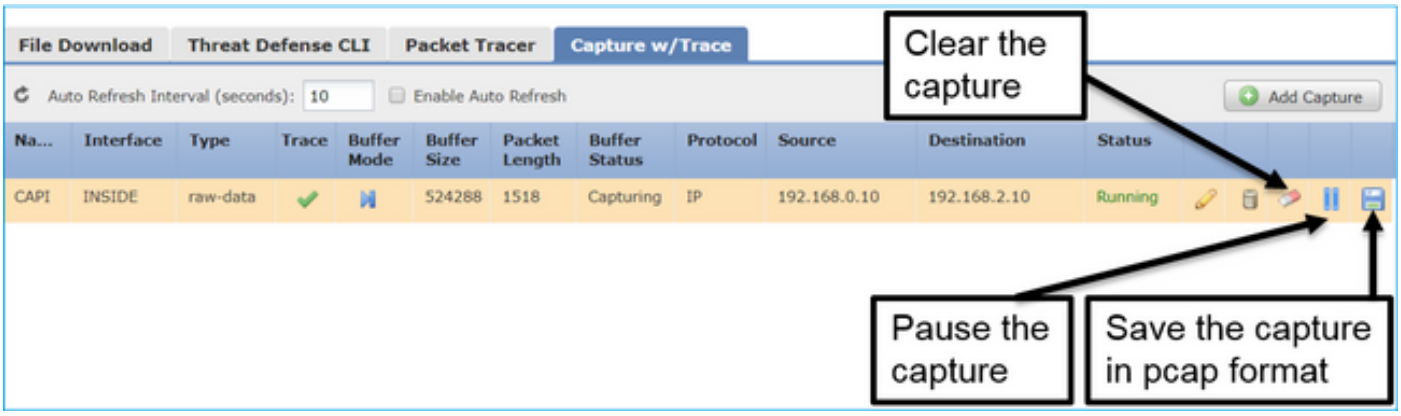


Текущие ограничения UI FMC

- Не может задать порты Src и Dst
- Только с основными Протоколами "IP" можно совпасть
- Не может включить перехват для Отбрасываний ASP механизма LINA

Обходной путь – использует CLI FTD.

Как только вы применяете перехват от UI FMC, перехват работает:

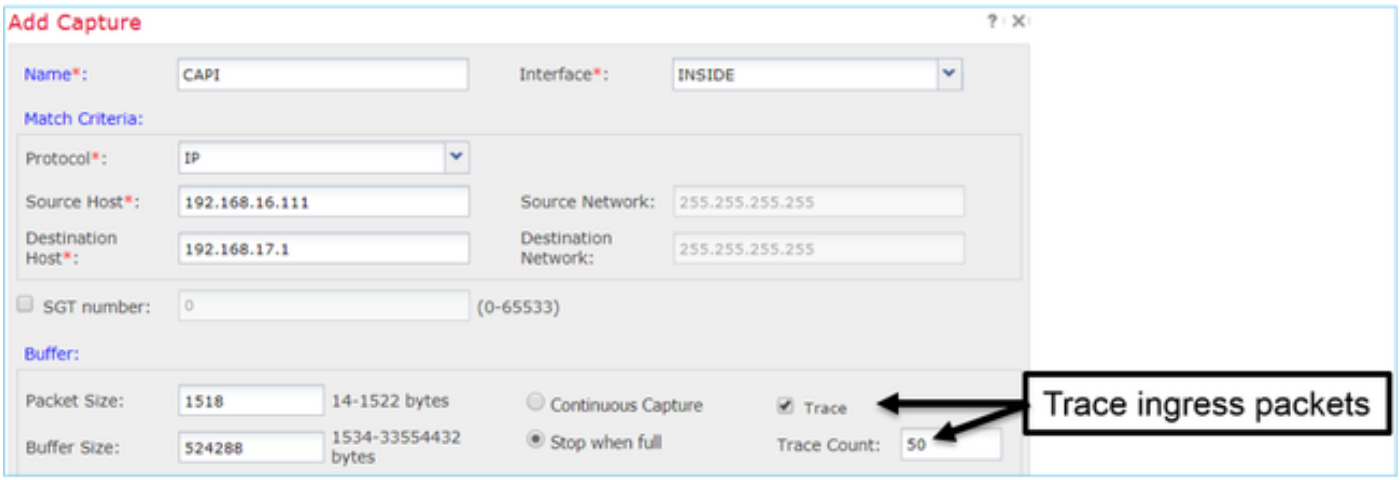


Перехват на CLI FTD:

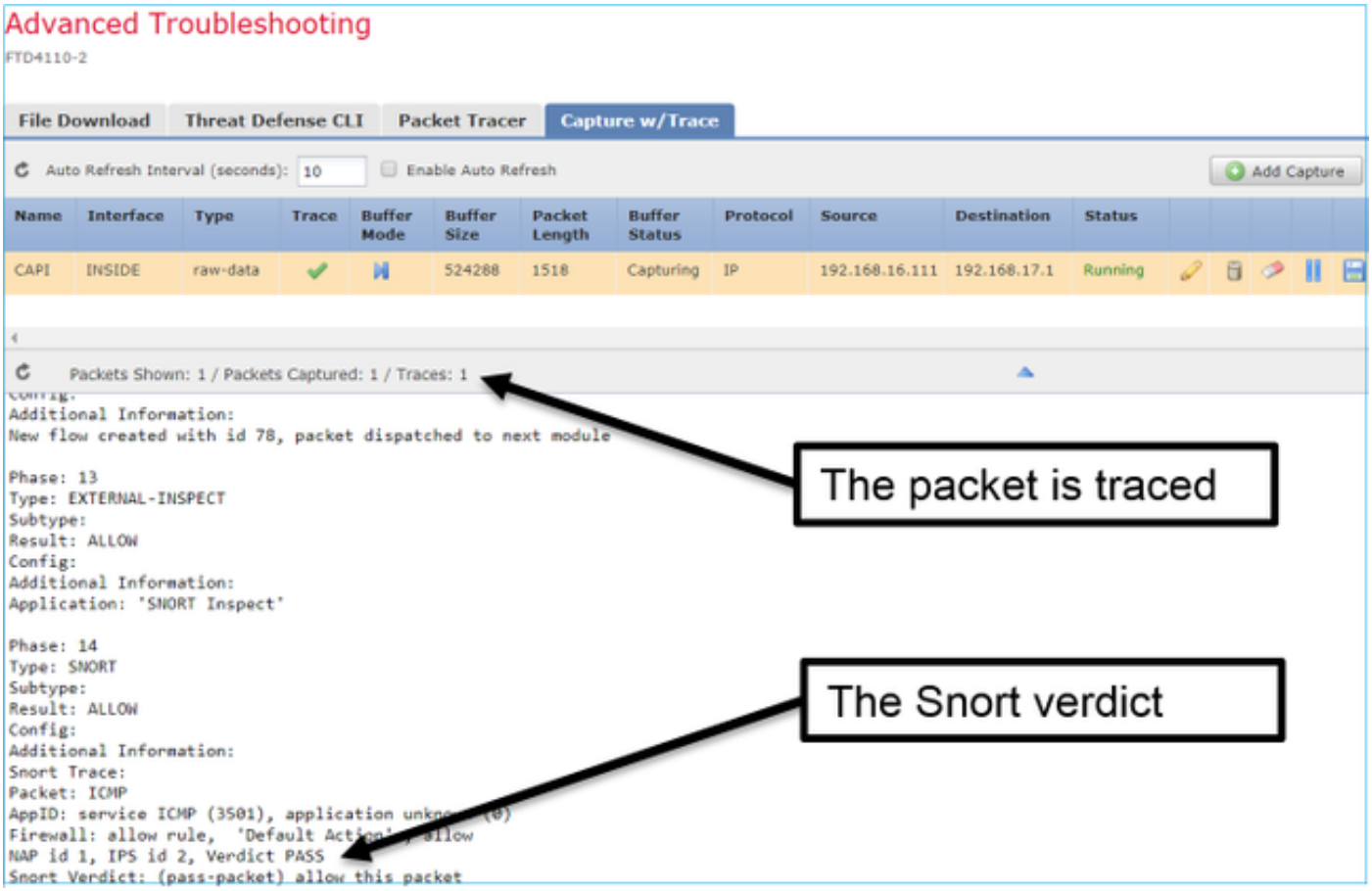
```
> show capture
capture CAPI%intf=INSIDE% type raw-data trace interface INSIDE [Capturing - 0 bytes]
  match ip host 192.168.0.10 host 192.168.2.10
>
```

Отследите действительный пакет на пост6.2 FMC

На FMC 6.2.x **Перехват w/Trace** мастер позволяет перехватывать и отслеживать действительные пакеты на FTD:



Можно проверить отслеженный пакет в UI FMC:



Утилита Packet Tracer FTD

Требования

Используйте Утилиту Packet Tracer для следующего потока и проверьте, как пакет будет обрабатываться внутренне:

Входной интерфейс	Внутри
Протокол	Эхо-запрос протокола ICMP
IP-адрес отправителя	192.168.103.1
IP-адрес назначения	192.168.101.1

Решение

Пакетный Трассировщик будет генерировать **действительный пакет.** Как это может быть замечено ниже пакета, предмет для Фырканья контроля. Перехват, взятый в то же время на уровне Фырканья **(трафик перехвата)**, показывает эхо-запрос протокола ICMP:

```
> packet-tracer input INSIDE icmp 192.168.103.1 8 0 192.168.101.1

Phase: 1
Type: CAPTURE
```

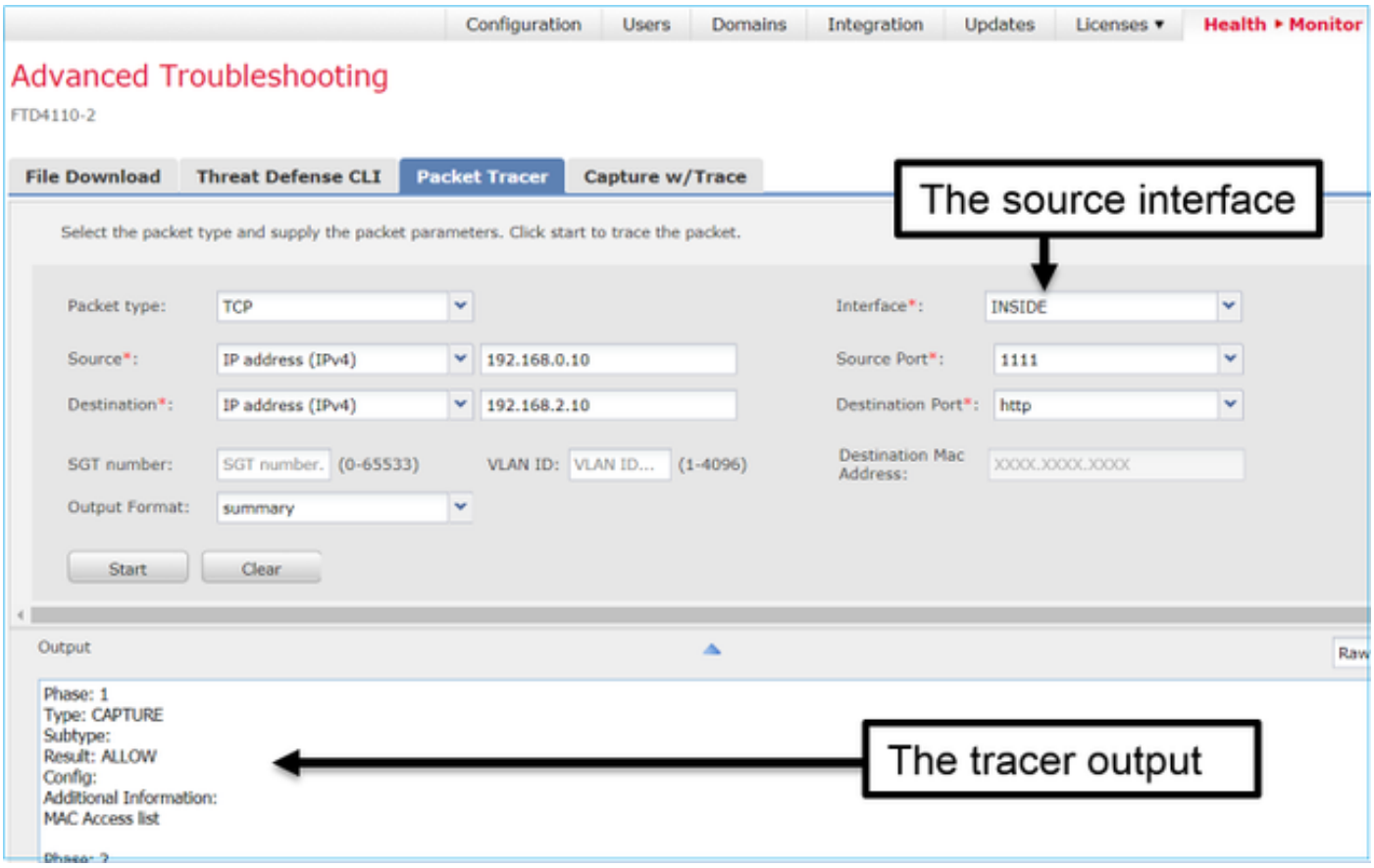
```
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.101.1 using egress ifc  OUTSIDE

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip 192.168.103.0 255.255.255.0 192.168.101.0
255.255.255.0 rule-id 268436482 event-log both
access-list CSM_FW_ACL_ remark rule-id 268436482: ACCESS POLICY: FTD5515 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268436482: L4 RULE: Allow ICMP
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached

... output omitted ...

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 203, packet dispatched to next module

Phase: 13
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: allow rule, id 268440225, allow
NAP id 2, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet

Result: input-interface: INSIDE input-status: up input-line-status: up output-interface: OUTSIDE
output-status: up output-line-status: up Action: allow >
```

Перехват уровня фырканья во время теста пакетного трассировщика показывает действительный пакет:

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - management0
  1 - Router

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -n
13:27:11.939755 IP 192.168.103.1 > 192.168.101.1: ICMP echo request, id 0, seq 0, length 8
```

Пакетное программное средство UI трассировщика в пост6.2 версиях программного обеспечения FMC

В FMC 6.2.x присваивают версию **Пакетному** программному средству UI **Трассировщика**, был представлен. Программное средство доступно таким же образом как программное средство перехвата и позволяет вам выполнять Пакетный Трассировщик на FTD от UI FMC:



Дополнительные сведения

- Справочник по командам защиты угрозы FirePOWER
- Примечания релиза системы FirePOWER, версия 6.1.0
- Руководство по конфигурации защиты угрозы FirePOWER Cisco для менеджера устройств FirePOWER, версии 6.1
- Cisco Systems – техническая поддержка и документация