Работа с перехватами FTD и Пакетным трассировщиком

Содержание

Введение
Используемые компоненты
Топология
Пакетная обработка FTD
Работа с перехватами механизма Фырканья
Работа с перехватами механизма Фырканья (с фильтрами tcpdump)
Примеры фильтра tcpdump
Работа с перехватами Механизма ASA FTD
Работа с перехватами Механизма ASA FTD? Экспортирование перехвата с помощью HTTP
Работа с перехватами Механизма ASA FTD? Экспортирование перехвата с помощью FTP/TFTP/SCP
Работа с перехватами Механизма ASA FTD? Отслеживание пакета
Использование утилиты packet-tracer FTD
Дополнительная документация

Введение

Этот документ описывает, как работать с перехватами Защиты угрозы огневой мощи (FTD) и утилитами пакетного трассировщика.

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 ASA)

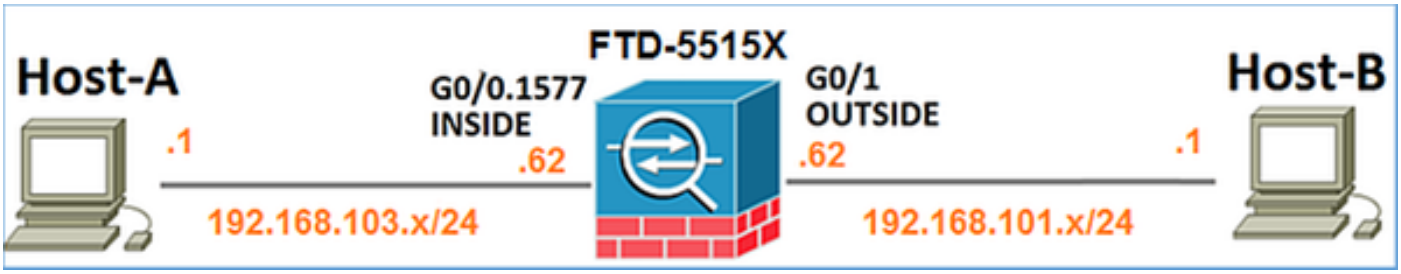
На пакетах FTD может быть перехвачен двумя механизмами:

1. Механизм ASA
2. Механизм фырканья

Используемые компоненты

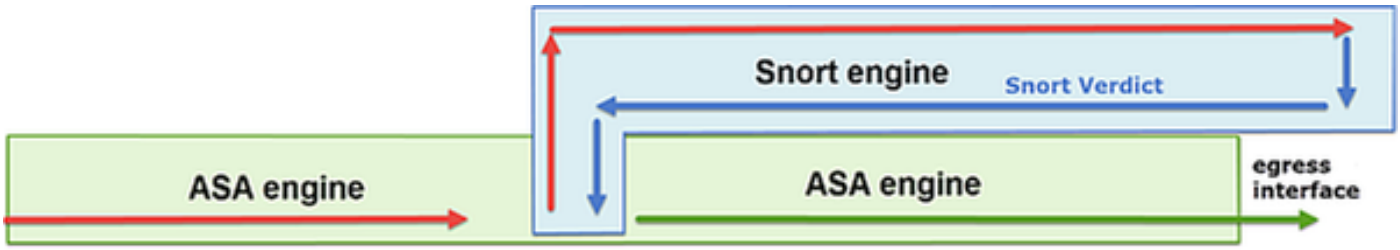
- ASA5515X, выполняющий код 6.1.0 FTD (создают 330),
- Центр управления огневой мощи (FMC), работающий 6.1.0 (создают 330),

Топология



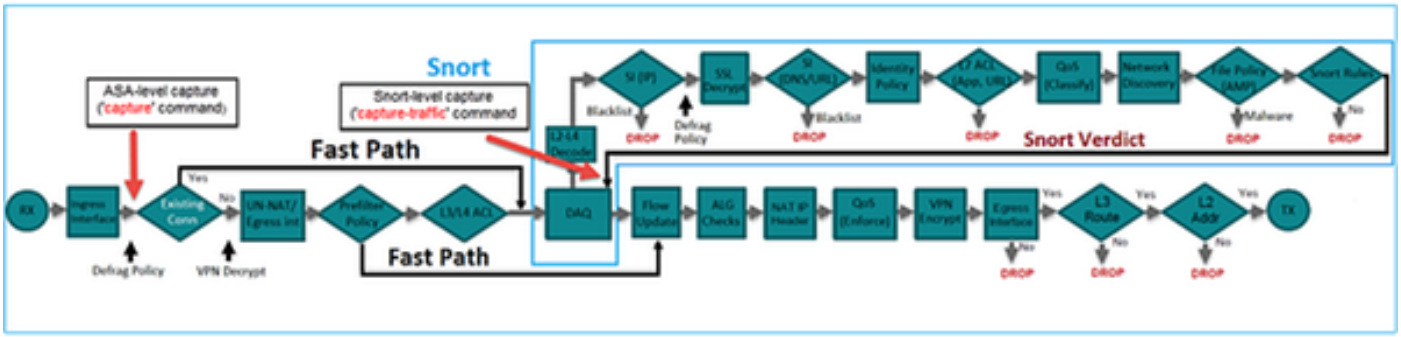
Пакетная обработка FTD

Пакетная обработка FTD может визуализироваться следующим образом:



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

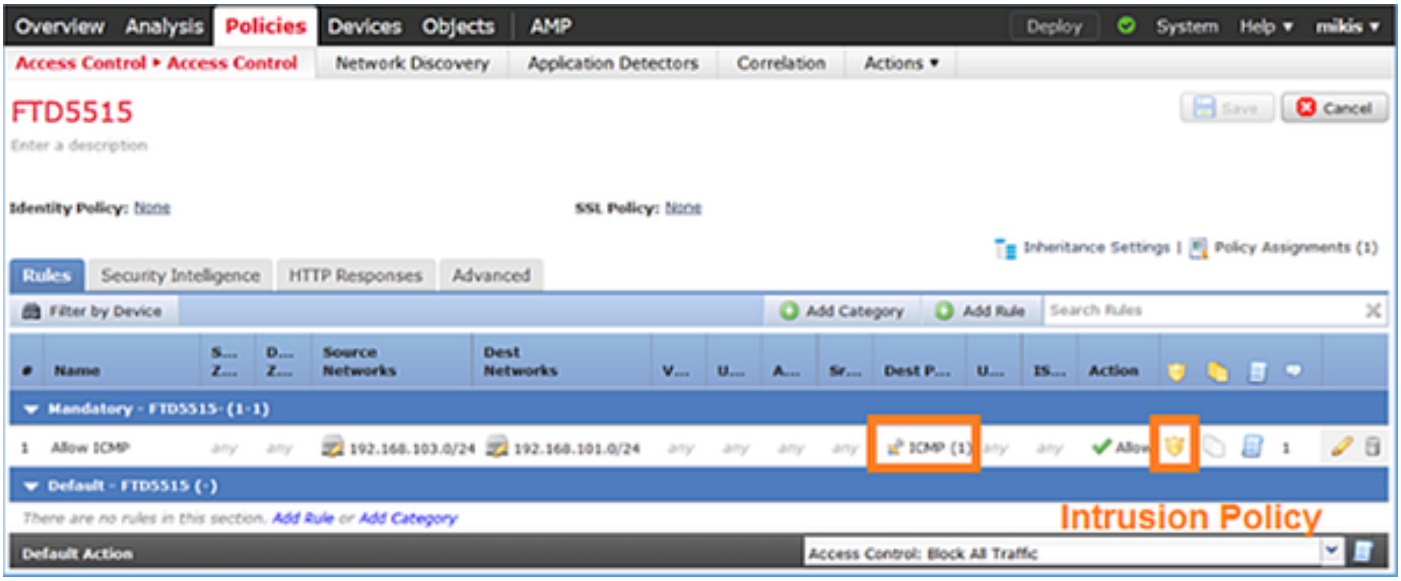
На основе вышеупомянутой архитектуры перехваты FTD могут быть взяты на 2 других местах:



Работа 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-trafficPlease choose domain to capture traffic from: 0 - br1 1 - RouterSelection?
1Please 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-trafficPlease choose domain to capture traffic from: 0 - br1 1 - RouterSelection?
1Please 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 8012:52:34.749945 IP olab-vl647-gw.cisco.com > olab-vl603-
gw.cisco.com: ICMP echo reply, id 0, seq 1, length 8012:52:34.759955 IP olab-vl603-gw.cisco.com
> olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 2, length 8012:52:34.759955 IP olab-
vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 2, length
8012:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0,
seq 3, length 8012:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo
reply, id 0, seq 3, length 8012:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-
gw.cisco.com: ICMP echo request, id 0, seq 4, length 8012:52:34.759955 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
```

Работа с перехватами механизма Фырканья (с фильтрами tcpdump)

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-trafficPlease choose domain to capture traffic from: 0 - br1 1 - RouterSelection?
1Please 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:

```
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq
0, length 8013:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo
reply, id 3, seq 1, length 8013:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-
gw.cisco.com: ICMP echo reply, id 3, seq 2, length 8013:28:36.079982 IP olab-vl647-gw.cisco.com
> olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 3, length 8013:28:36.079982 IP olab-vl647-
gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 4, length 80
```

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

```
> capture-trafficPlease choose domain to capture traffic from: 0 - br1 1 - RouterSelection?
1Please specify tcpdump options desired.(or enter '?' for a list of supported options)Options: -
n host 192.168.101.113:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq
0, length 8013:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 1,
length 8013:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 2, length
8013:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 3, length
8013:29:59.599959 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 192.168.101.117:57:48.709954 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 192.168.101.118:03:12.749945 IP 192.168.101.1.23 > 192.168.103.1.27287:
Flags [.], ack 3758037348, win 32768, length 018:03:12.749945 IP 192.168.101.1.23 >
192.168.103.1.27287: Flags [P.], ack 1, win 32768, length 218:03:12.949932 IP 192.168.101.1.23 >
192.168.103.1.27287: Flags [P.], ack 1, win 32768, length 1018:03:13.249971 IP 192.168.101.1.23
> 192.168.103.1.27287: Flags [.], ack 3, win 32768, length 018:03:13.249971 IP 192.168.101.1.23
> 192.168.103.1.27287: Flags [P.], ack 3, win 32768, length 218:03:13.279969 IP 192.168.101.1.23
> 192.168.103.1.27287: Flags [.], ack 5, win 32768, length 018:03:13.279969 IP 192.168.101.1.23
> 192.168.103.1.27287: Flags [P.], ack 5, win 32768, length 1018:03:13.309966 IP
192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 018:03:13.309966 IP
192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 7, win 32768, length 1218:03:13.349972
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 192.168.101.1CTRL + C <- to stop the capture> system file copy
10.229.22.136 ftp / capture.pcapEnter password for ftp@10.229.22.136:Copying capture.pcapCopy
successful.>
```

Работа с перехватами Механизма ASA FTD

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

Интерфейс СНАРУЖИ

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

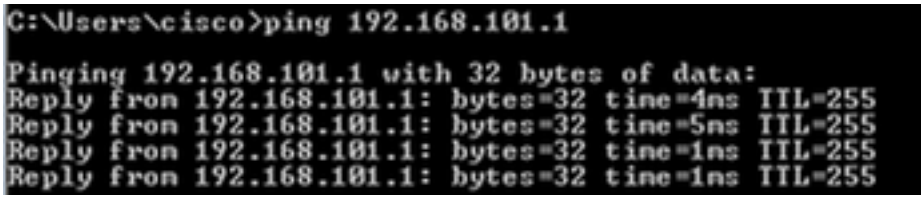
Решение

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 capturecapture CAPI type raw-data interface INSIDE [Capturing - 752 bytes] match icmp host 192.168.103.1 host 192.168.101.1capture 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 CAPI8 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 reply8 packets shown > show capture CAPO8 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 reply8 packets shown
```

Работа с перехватами Механизма ASA FTD? Экспортирование перехвата с помощью HTTP

Требования

Экспортируйте перехваты, взятые в предыдущем сценарии с помощью браузера

Решение

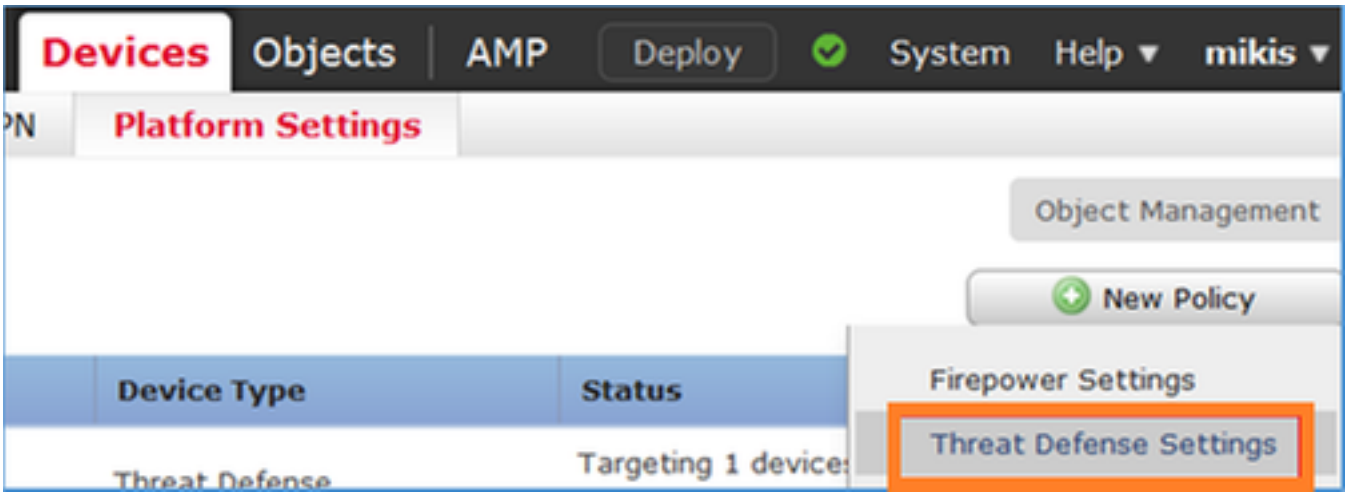
Для экспортирования перехватов с помощью браузера существует потребность к:

1. Включите сервер HTTPS
2. Предоставьте доступ HTTPS

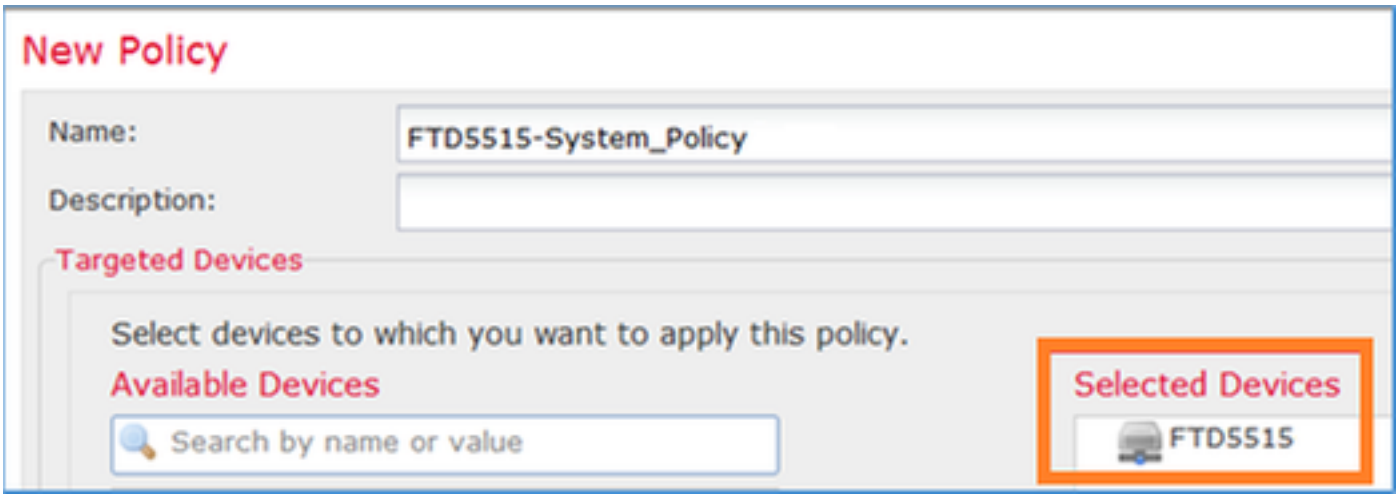
По умолчанию сервер HTTPS отключен, и никакой доступ не предоставлен:

```
> show running-config http
>
```

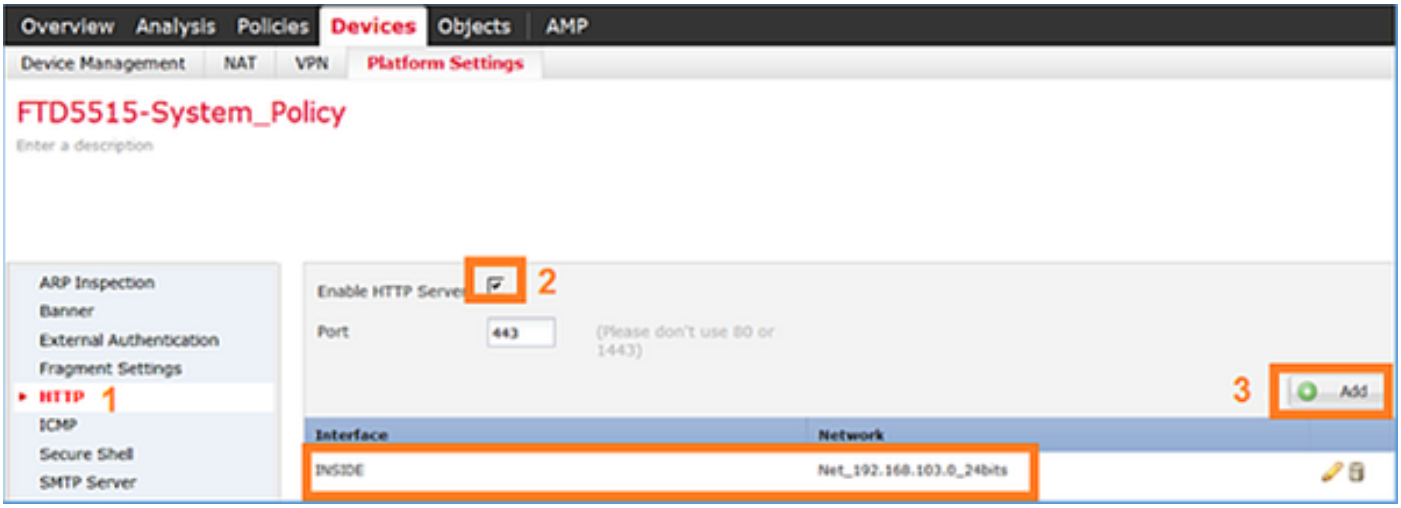
Шаг 1: Перейдите к **Устройствам> Параметры настройки Платформы,** щелкните **по New Policy** и выберите **Threat Defense Settings:**



Задайте название Политики и Адресата устройства:



Шаг 2: Включите сервер HTTPS и добавьте сеть, которой нужно позволить обратиться к устройству FTD по HTTPS:



Сохраните и **развернитесь**

Совет

При развертывании политики, можно включить **http отладки**, чтобы видеть, что запускается сервис HTTP:

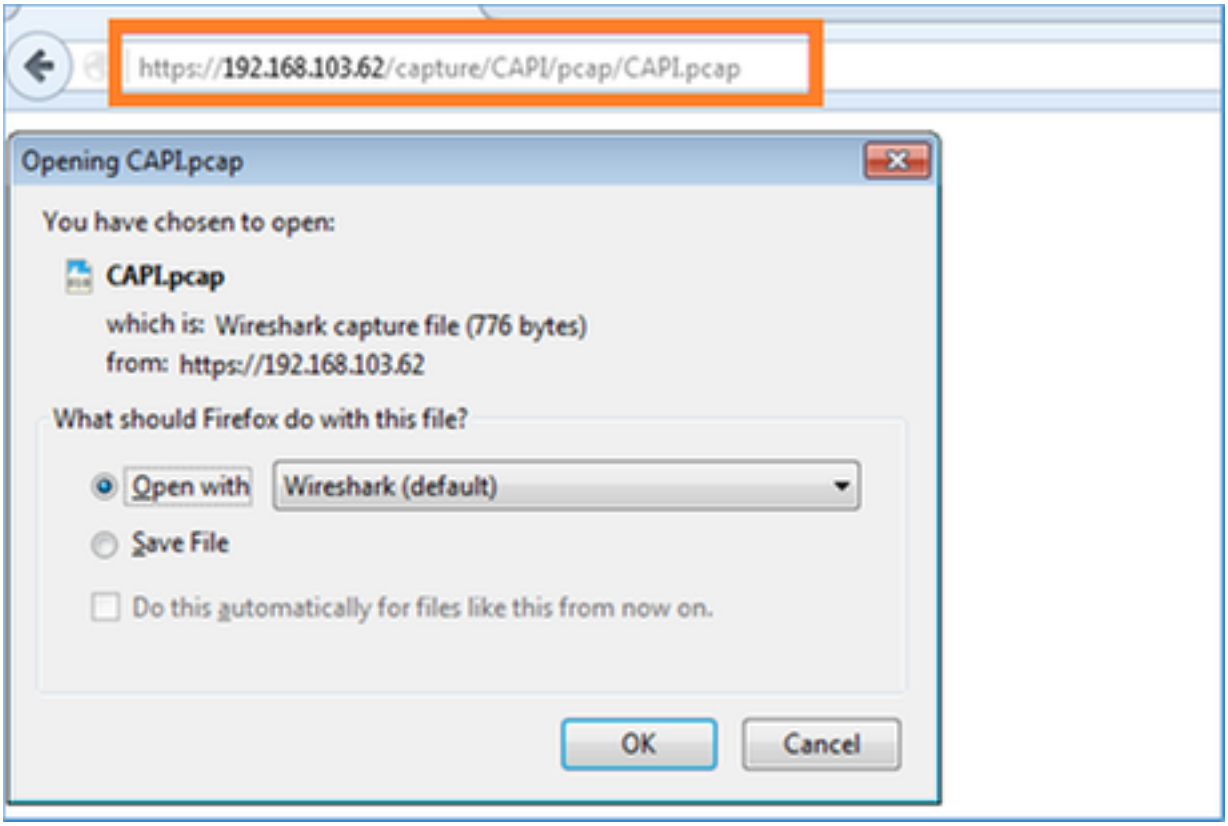
```
> debug http 255debug http enabled at level 255.http_enable: Enabling HTTP serverHTTP server starting.
```

Вот результат на CLI FTD:

```
> unebug all> show run httphttp server enablehttp 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

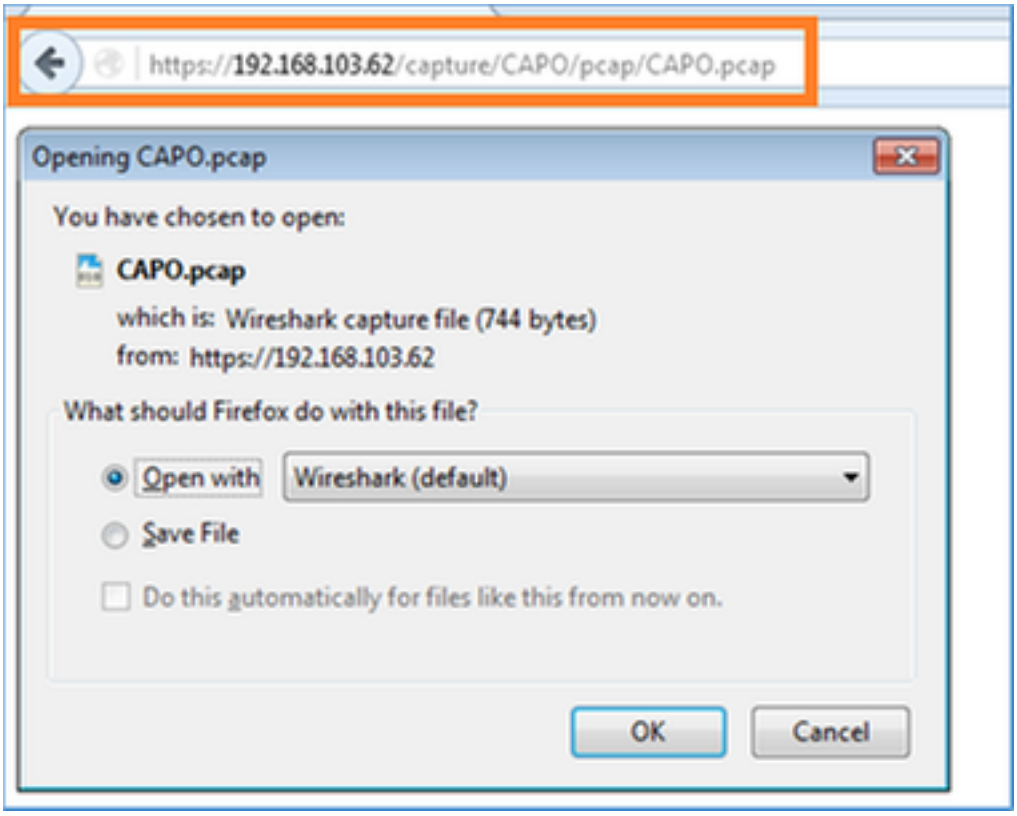


Для ссылки

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



Работа с перехватами Механизма ASA FTD? Экспортирование перехвата с помощью 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.pcapSource
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://192.168.78.73Source 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@192.168.78.55Source 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)? yesWarning: Permanently added
'192.168.78.55' (SHA256) to the list of known
hosts.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!454
packets copied in 3.950 secs (151 packets/sec)
firepower#
```

Работа с перехватами Механизма ASA FTD? Отслеживание пакета

Требования

Включите перехват на FTD использование следующих фильтров:

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

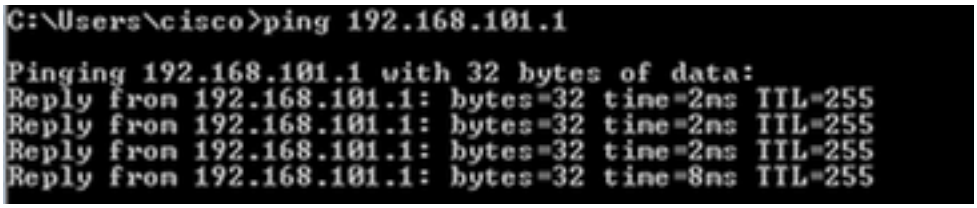
Решение

Отслеживание действительного пакета может быть очень полезно для устранения проблем проблем с подключением. Это позволяет видеть все внутренние проверки, которые проходит пакет. Добавить? **подробность трассировки**? ключевые слова и задают сумму пакетов, которые будут отслежены. 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:



Вот захваченные пакеты:

```
> show capture CAPI28 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 reply8 packets shown
```

Вот трассировка первого пакета. Содержательные части:

- Фаза 12, где может быть замечен 'прямой поток'. Это - Массив Отправки Механизма ASA (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 detail8 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: 1Type: CAPTURE... output omitted
...Phase: 12Type: FLOW-CREATIONSubtype:Result: ALLOWConfig:Additional Information:New flow
created with id 195, packet dispatched to next moduleModule information for forward flow
...snp_fp_inspect_ip_optionssnp_fp_snortsnp_fp_inspect_icmpsnp_fp_adjacencysnp_fp_fragmentsnp_ifc_stat Module information for reverse flow
...snp_fp_inspect_ip_optionssnp_fp_inspect_icmpsnp_fp_snortsnp_fp_adjacencysnp_fp_fragmentsnp_ifc_stat Phase: 13Type: EXTERNAL-INSPECTSubtype:Result: ALLOWConfig:Additional
Information:Application: 'SNORT Inspect' Phase: 14Type: SNORTSubtype:Result:
ALLOWConfig:Additional Information:Snort Verdict: (pass-packet) allow this packet... output
omitted ...Result:input-interface: OUTSIDEinput-status: upinput-line-status: upoutput-interface:
OUTSIDEoutput-status: upoutput-line-status: upAction: allow 1 packet shown>
```

Использование утилиты 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, но перехват на Механизме Фырканья показывает, что действительный пакет фактически не передается через него:

```
> packet-tracer input INSIDE icmp 192.168.103.1 8 0 192.168.101.1 Phase: 1Type:
CAPTURESubtype:Result: ALLOWConfig:Additional Information:MAC Access list Phase: 2Type: ACCESS-
LISTSubtype:Result: ALLOWConfig:Implicit RuleAdditional Information:MAC Access list Phase:
3Type: ROUTE-LOOKUPSubtype: Resolve Egress InterfaceResult: ALLOWConfig:Additional
Information:found next-hop 192.168.101.1 using egress ifc OUTSIDE Phase: 4Type: ACCESS-
LISTSubtype: logResult: ALLOWConfig:access-group CSM_FW_ACL_ globalaccess-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 bothaccess-list CSM_FW_ACL_ remark rule-id 268436482: ACCESS POLICY: FTD5515 -
Mandatory/1access-list CSM_FW_ACL_ remark rule-id 268436482: L4 RULE: Allow ICMPAdditional
Information: This packet will be sent to snort for additional processing where a verdict will be
reached ... output omitted ... Phase: 12Type: FLOW-CREATIONSubtype:Result:
ALLOWConfig:Additional Information:New flow created with id 203, packet dispatched to next
module Result:input-interface: INSIDEinput-status: upinput-line-status: upoutput-interface:
OUTSIDEoutput-status: upoutput-line-status: upAction: allow >
```

Дополнительная документация

Справочник по командам защиты угрозы огневой мощи

Примечания релиза системы огневой мощи, версия 6.1.0

Руководство по конфигурации защиты угрозы огневой мощи Cisco для менеджера устройств огневой мощи, версии 6.1