Защита Угрозы Огневой мощи Настройки взаимодействует во Встроено-парном режиме

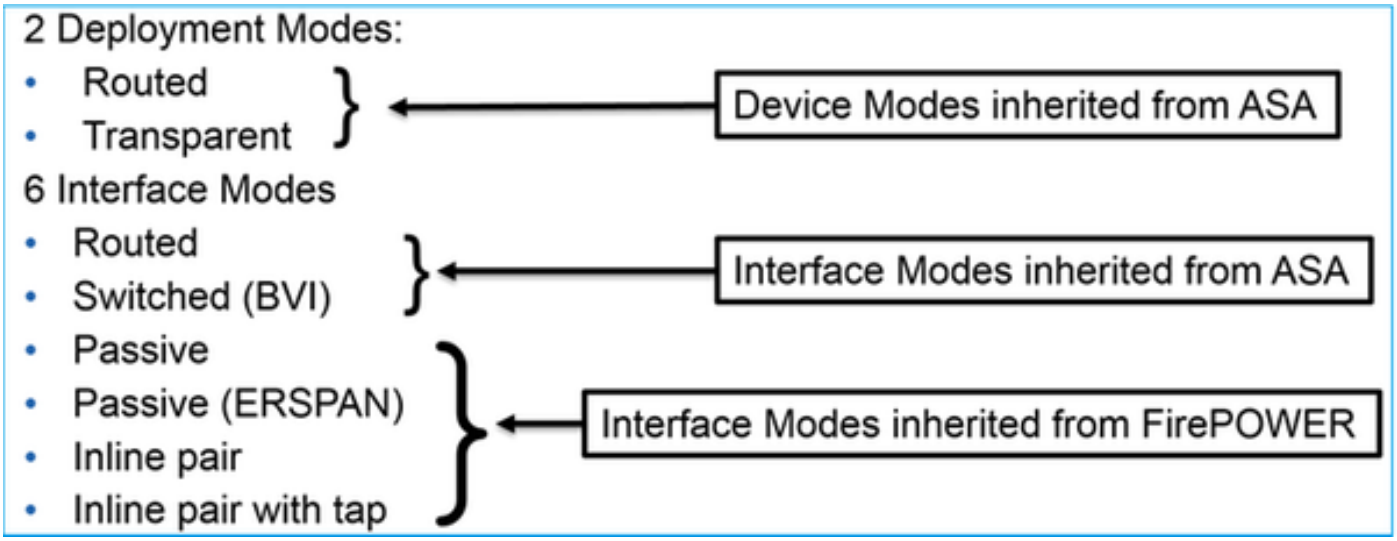
Содержание

Введение

Защита угрозы огневой мощи (FTD) является унифицированным образом программного обеспечения, который может быть установлен на следующих платформах:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR4100, FPR9300
- VMware (ESXi)
- Веб-сервисы Amazon (AWS)
- KVM
- Модуль комплекта маршрутизаторов ISR

FTD предоставляет 2 режима Развертываний и 6 Интерфейсных режимов



Примечание: Можно смешать интерфейсные режимы на sigle FTD устройство

Вот глобальный обзор различных развертываний FTD и интерфейсных режимов:

Режим интерфейса FTD	Режим Развертываний FTD	Описание	Трафик может быть отброшен
Направленный	Направленный	Полные проверки механизма ASA и механизма Фырканья	Да
Коммутируемый	Прозрачный	Полные проверки механизма ASA и механизма Фырканья	Да
Встроенная пара	Направленный или прозрачный	Частичный механизм ASA и полные проверки механизма Фырканья	Да
Встроенная пара с ответвителем	Направленный или прозрачный	Частичный механизм ASA и полные проверки механизма Фырканья	Нет
Пассивный	Направленный или прозрачный	Частичный механизм ASA и полные проверки механизма Фырканья	Нет
Пассивный (ERSPAN)	Направленный	Частичный механизм ASA и полные проверки механизма Фырканья	Нет

Цель

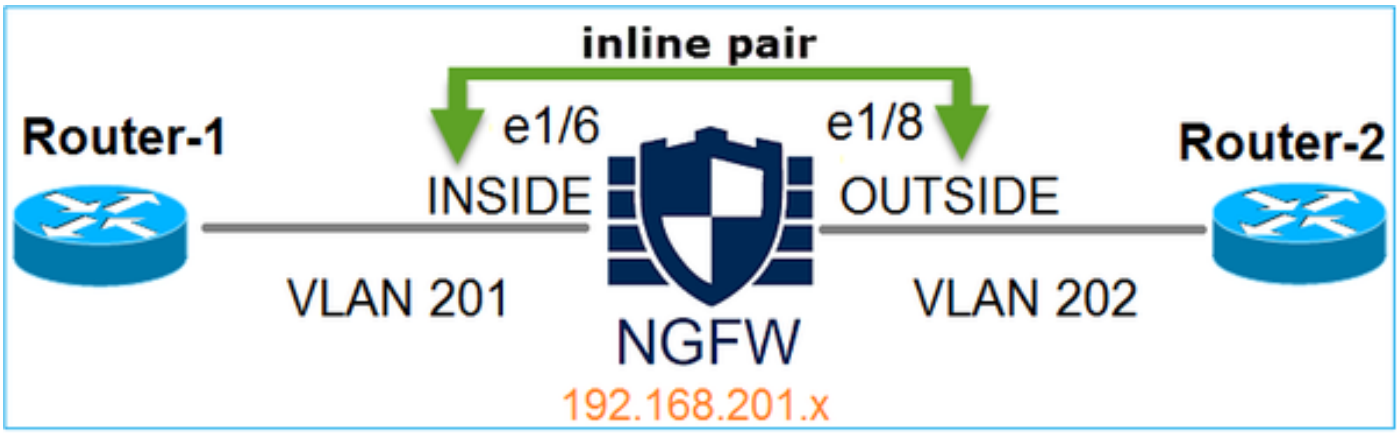
Цель этого документа к:

- Продемонстрируйте конфигурацию и использование Встроено-парного интерфейса FTD

Используемые компоненты

- Огневая мощь 4150 выполнений код 6.1.0 FTD. x
- Центр управления огневой мощи (FMC), работающий 6.1.0. x

Топология



Настройка Встроенный парный интерфейс на FTD

Требование

Настройте e1/6 физических интерфейсов и e1/8 во Встроенном Парном Режиме на следующие требования:

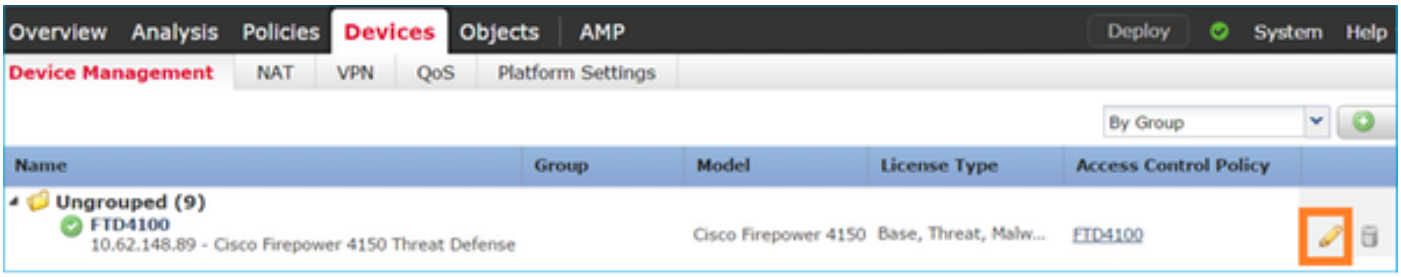
Интерфейс	e1/6	e1/8
Name	ВНУТРИ	СНАРУЖИ
Зона безопасности	INSIDE_ZONE	OUTSIDE_ZONE
Встроенное Определенное имя	Inline-Pair-1	
Встроенный MTU набора	1500	
FailSafe	Включенный	
Распространитесь состояние канала	Включенный	

Решение

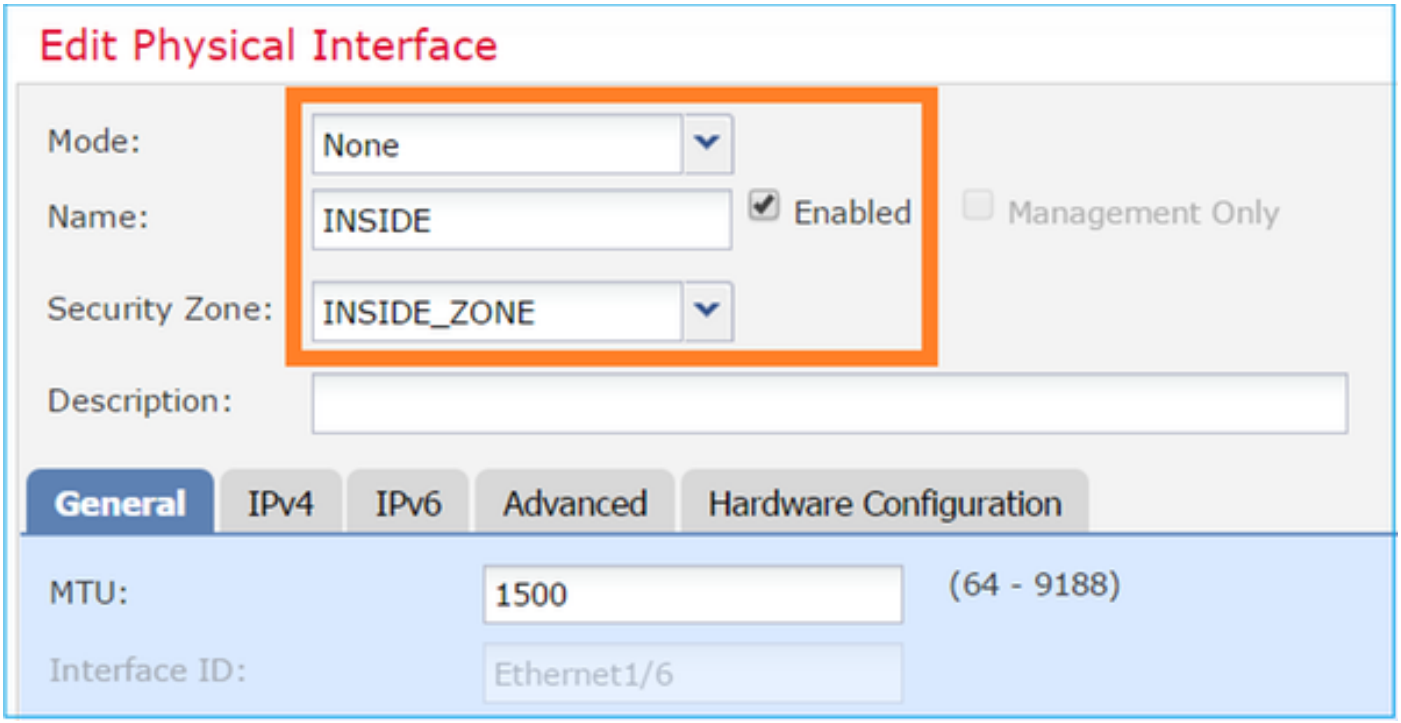
Шаг 1? Настройка отдельные интерфейсы

Перейдите к **Устройствам> Управление устройствами,** выберите соответствующее

устройство и щелкните **по Значку редактирования**:

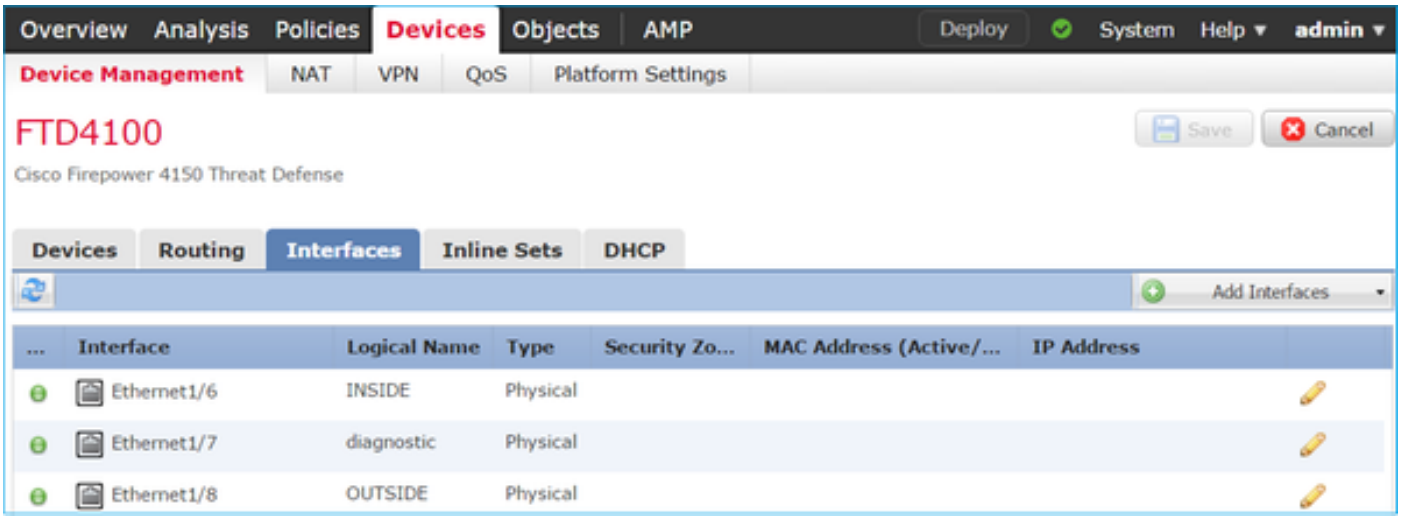


Задайте название и включите интерфейс:



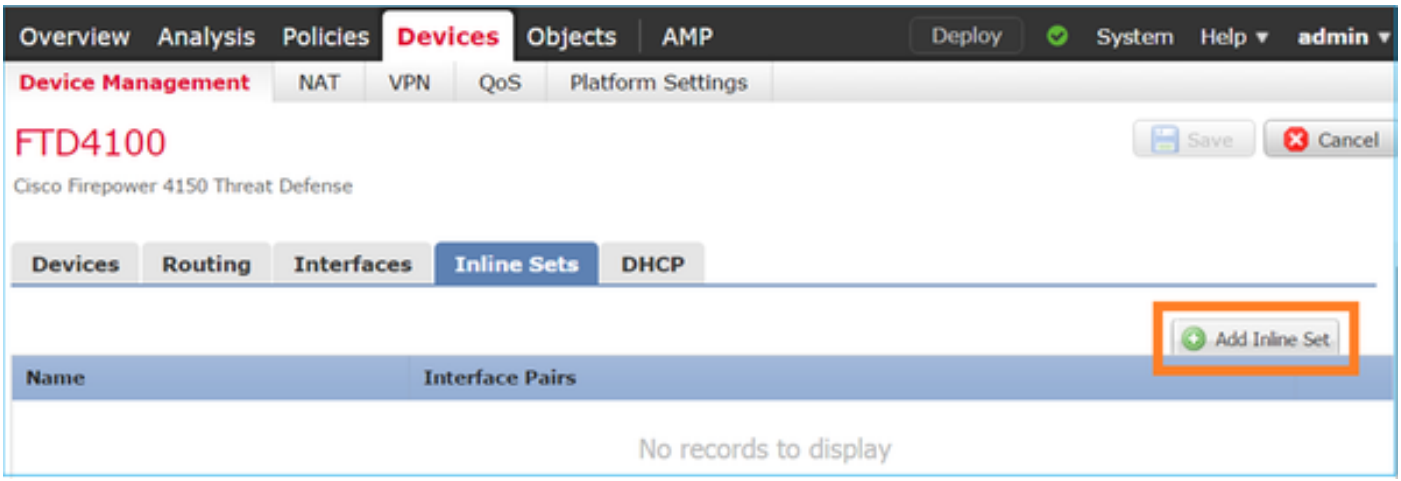
Название будет **nameif** интерфейса

Так же для интерфейсного Ethernet1/8. Окончательный результат:

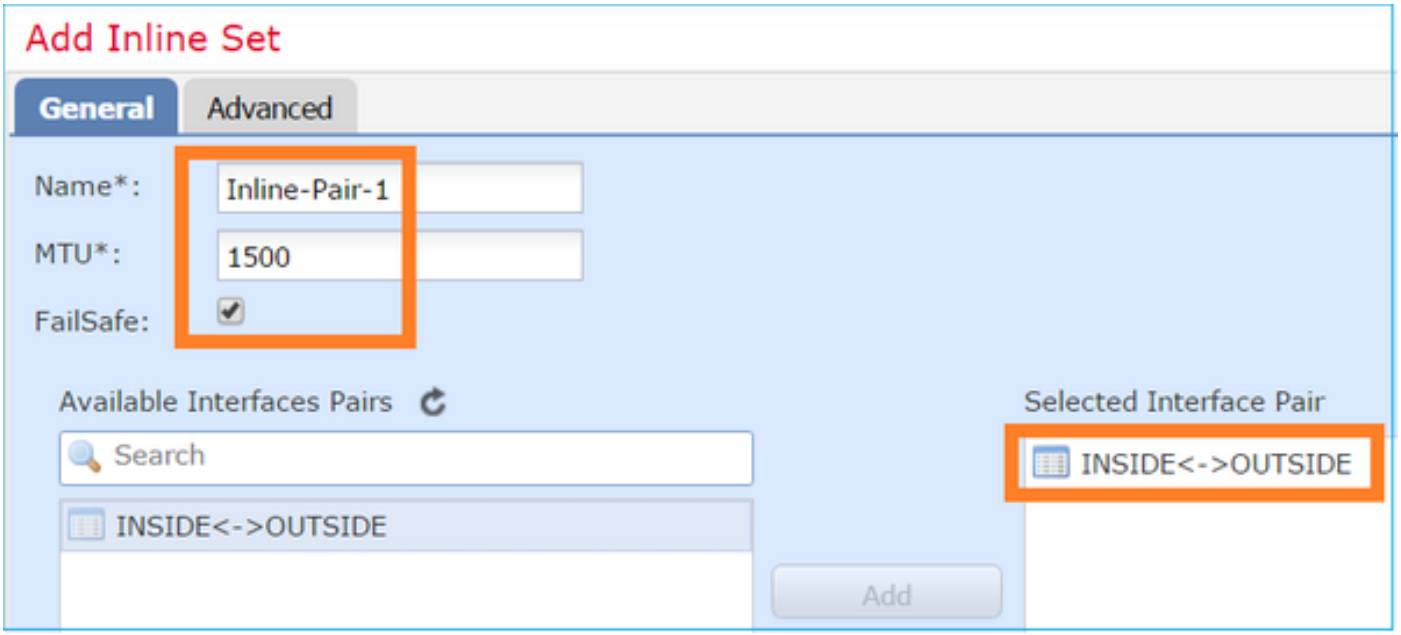


Шаг 2? Настройка встроенная пара

Перейдите к вкладке **Inline Sets** и щелкните **по Add Inline Set**:

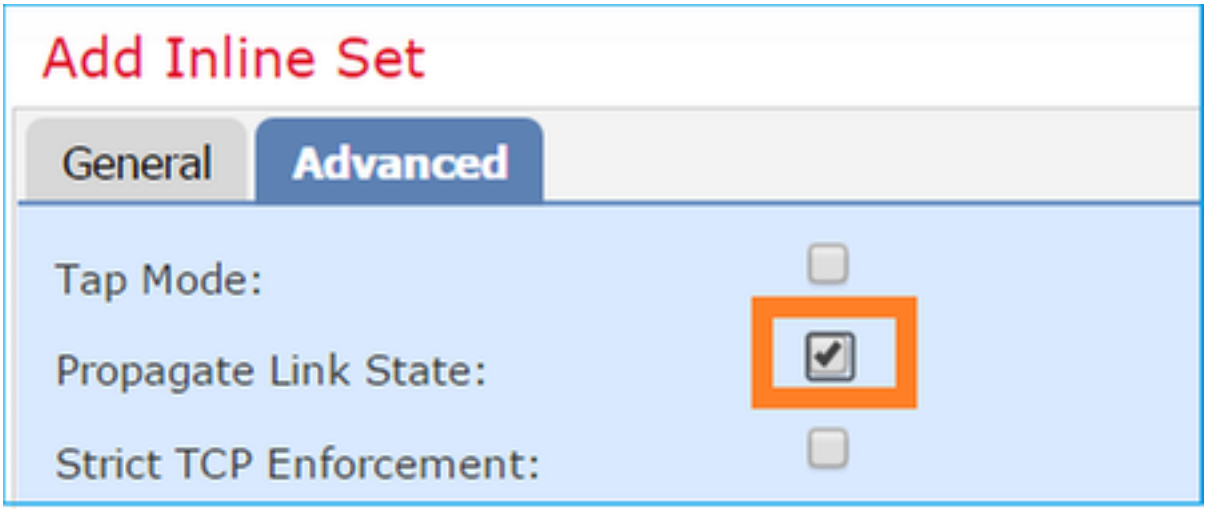


Настройте параметры настройки на требования:



Отказоустойчивый позволяет трафику проходить через встроенную пару, неосмотренную в случае, если интерфейсные буферы полны (как правило, замеченный, когда устройство перегружено, или механизм Фырканья перегружен). Интерфейсный размер буфера динамично выделен.

Включить? **Распространиться состояние канала**? параметр:



Когда один из интерфейсов во встроенном наборе выключается, распространение состояния канала автоматически переводит второй интерфейс в нерабочее состояние во встроенной интерфейсной паре.

Сохраните изменения и **Развернитесь**

Проверка Встроенной Парной конфигурации интерфейса

Проверьте Встроенную Парную конфигурацию от CLI FTD

Решение

Вход в систему к CLI FTD и проверяет Встроенную Парную конфигурацию:

```
> show inline-set

Inline-set Inline-Pair-1
 Mtu is 1500 bytes
 Failsafe mode is on/activated
 Failsecure mode is off
 Tap mode is off
 Propagate-link-state option is on
 hardware-bypass mode is disabled
 Interface-Pair[1]:
   Interface: Ethernet1/6 "INSIDE"
     Current-Status: UP
   Interface: Ethernet1/8 "OUTSIDE"
     Current-Status: UP
   Bridge Group ID: 509
>
```

Примечание: ID Группы мостов является значением, другим, чем 0. Если Режим Ответвителя идет тогда, это 0

Интерфейс и информация об имени:

```
> show nameif
Interface              Name                   Security
Ethernet1/6            INSIDE                 0
Ethernet1/7            diagnostic             0
Ethernet1/8            OUTSIDE                0
>
```

Проверка интерфейсного статуса:

```
> show interface ip brief
Interface                  IP-Address     OK? Method Status                Protocol
Internal-Data0/0           unassigned     YES unset up                     up
Internal-Data0/1           unassigned     YES unset up                     up
Internal-Data0/2           169.254.1.1    YES unset up                     up
Ethernet1/6                unassigned     YES unset up                     up
Ethernet1/7                unassigned     YES unset up                     up
Ethernet1/8                unassigned     YES unset up                     up
```

Проверка информации о физическом интерфейсе:

```
> show interface e1/6
Interface Ethernet1/6 "INSIDE", is up, line protocol is up
 Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
       MAC address 5897.bdb9.770e, MTU 1500
       IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1
       IP address unassigned
 Traffic Statistics for "INSIDE":
       468 packets input, 47627 bytes
       12 packets output, 4750 bytes
       1 packets dropped
     1 minute input rate 0 pkts/sec, 200 bytes/sec
     1 minute output rate 0 pkts/sec, 7 bytes/sec
     1 minute drop rate, 0 pkts/sec
     5 minute input rate 0 pkts/sec, 96 bytes/sec
     5 minute output rate 0 pkts/sec, 8 bytes/sec
     5 minute drop rate, 0 pkts/sec
>show interface e1/8
Interface Ethernet1/8 "OUTSIDE", is up, line protocol is up
 Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
       MAC address 5897.bdb9.774d, MTU 1500
       IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1
       IP address unassigned
 Traffic Statistics for "OUTSIDE":
       12 packets input, 4486 bytes
       470 packets output, 54089 bytes
       0 packets dropped
     1 minute input rate 0 pkts/sec, 7 bytes/sec
     1 minute output rate 0 pkts/sec, 212 bytes/sec
     1 minute drop rate, 0 pkts/sec
     5 minute input rate 0 pkts/sec, 7 bytes/sec
```

```
      5 minute output rate 0 pkts/sec, 106 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

Проверка FTD Встроенная Парная интерфейсная операция

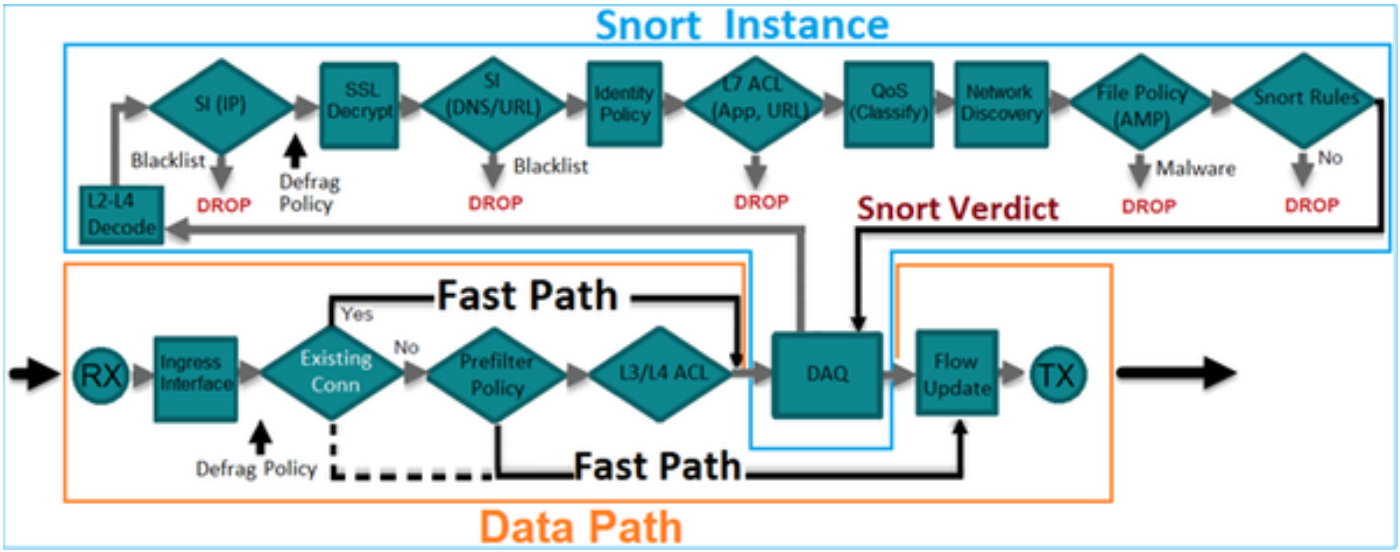
Этот раздел покрывает следующие проверки проверки для проверки Встроенной Парной операции:

- Проверка 1? Использование пакетного трассировщика
- Проверка 2? Включение перехвата с трассировкой и передача пакета SYN/ACK TCP через Встроенную Пару
- Проверка 3? Мониторинг трафика FTD с помощью отладки механизма межсетевого экрана
- Проверка 4? Проверка функциональности Распространения Состояния канала
- Проверка 5? Статическая NAT Настройка

Решение

Обзор архитектуры

Когда 2 интерфейса FTD работают во Встроено-парном режиме, пакет обрабатывается следующим образом:

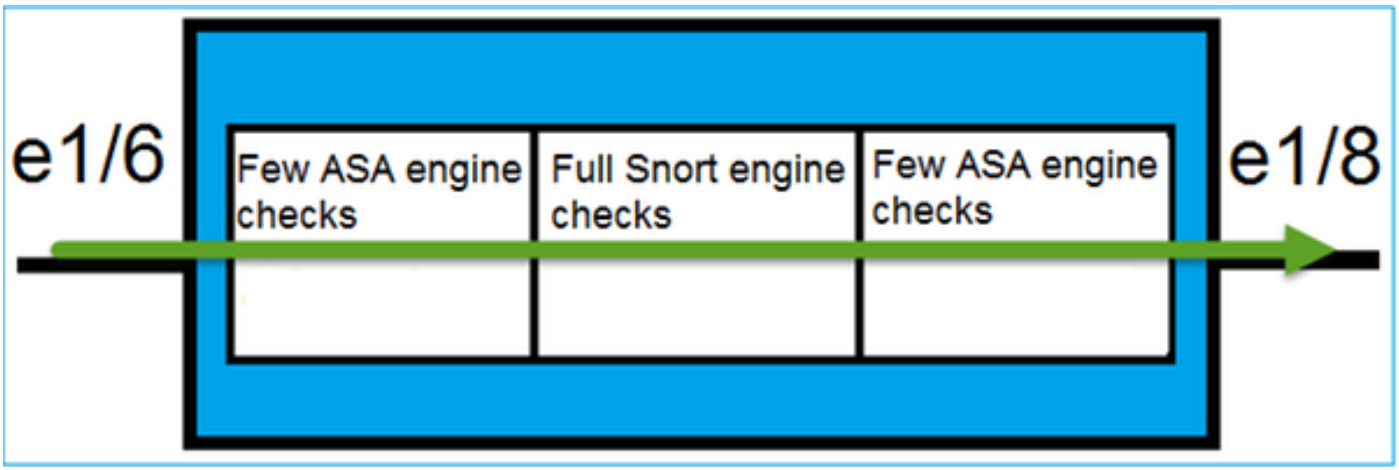


Примечание: Только физические интерфейсы могут быть участниками Встроенного парного набора

Теоретические сведения

- При настройке Встроенной Пары внутренне соединены 2 Физических интерфейса
- Подобный **классике встраивают IPS**
- Доступный в **Направленных** или **Прозрачных** режимах **Развертываний**
- Большинство функций механизма ASA (NAT, Маршрутизация, ACL L3/L4 и т.д.) не **доступно** для потоков, проходящих Встроенную Пару
- Транзитный трафик **может быть отброшен**
- **Немного** проверок **механизма ASA** применены наряду с **полными** проверками **механизма Фырканья**

Последняя точка может визуализироваться следующим образом:



Проверка 1? Использование пакетного трассировщика

Вот выходные данные packet-tracer, эмулирующие пакет, пересекающий встроенную пару с выделенными интересными моментами:

```
> packet-tracer input INSIDE tcp 192.168.201.50 1111 192.168.202.50 80

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 3
Type: ACCESS-LIST
```

```
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD4100 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: DEFAULT ACTION RULE
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 4
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Ingress interface INSIDE is in NGIPS inline mode.
Egress interface OUTSIDE is determined by inline-set configuration

Phase: 5
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 106, packet dispatched to next module

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
Action: allow

>
```

Проверка 2? Передача пакетов SYN/ACK TCP через Встроенную Пару

Можно генерировать пакеты SYN/ACK TCP с помощью пакетной утилиты обработки как Scapy. Следующий синтаксис будет генерировать 3 пакета с включенными флагами SYN/ACK:

```
root@KALI:~# scapyINFO: Can't import python gnuplot wrapper . Won't be able to plot.WARNING: No route found for IPv6 destination :: (no default route?)Welcome to Scapy (2.2.0)>>> conf.iface='eth0'>>> packet = IP(dst="192.168.201.60")/TCP(flags="SA",dport=80)>>> syn_ack=[]>>> for i in range(0,3): # Send 3 packets... syn_ack.extend(packet)...>>> send(syn_ack)
```

Включите следующий перехват на CLI FTD и передайте немного пакетов SYN/ACK TCP:

```
> capture CAPI interface INSIDE trace match ip host 192.168.201.60 any
>capture CAPO interface OUTSIDE match ip host 192.168.201.60 any
>
```

После передачи пакетов через FTD вы видите соединение, которое было создано:

```
> show conn detail
1 in use, 34 most used
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       b - TCP state-bypass or nailed,
```

```
      C - CTIQBE media, c - cluster centralized,
      D - DNS, d - dump, E - outside back connection, e - semi-distributed,
      F - initiator FIN, f - responder FIN,
      G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
      i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
      k - Skinny media, M - SMTP data, m - SIP media, N - inspected by Snort, n - GUP
      O - responder data, P - inside back connection,
      q - SQL*Net data, R - initiator acknowledged FIN,
      R - UDP SUNRPC, r - responder acknowledged FIN,
      T - SIP, t - SIP transient, U - up,
      V - VPN orphan, v - M3UA W - WAAS,
      w - secondary domain backup,
      X - inspected by service module,
      x - per session, Y - director stub flow, y - backup stub flow,
      Z - Scansafe redirection, z - forwarding stub flow

TCP Inline-Pair-1:OUTSIDE(OUTSIDE): 192.168.201.60/80 Inline-Pair-1:INSIDE(INSIDE):
192.168.201.50/20,
   flags b N, idle 13s, uptime 13s, timeout 1h0m, bytes 0

>
```

- **b флаг:** классический ASA отбросил бы незапрашиваемый пакет SYN/ACK, пока не был включен обход состояния TCP. Интерфейс FTD во Встроенном Парном режиме обрабатывает TCP - подключение в транзитном режиме состояния TCP и doesn? t отбрасывают пакеты TCP тот Дон? t принадлежат существующим соединениям
- **Флаг N:** пакет будет осмотрен механизмом Фырканья FTD

Перехваты доказывают вышеупомянутое, так как вы видите, что эти 3 пакета пересекают FTD:

```
> show capture CAPI

3 packets captured

  1: 15:27:54.327146      192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
  2: 15:27:54.330000      192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
  3: 15:27:54.332517      192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3 packets shown
>
```

3 пакета, выходящие из устройства FTD:

```
> show capture CAPO

3 packets captured

  1: 15:27:54.327299      192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
  2: 15:27:54.330030      192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
  3: 15:27:54.332548      192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3 packets shown
>
```

Отслеживание первого пакета перехвата показывает некоторые дополнительные сведения как вердикт механизма Фырканья:

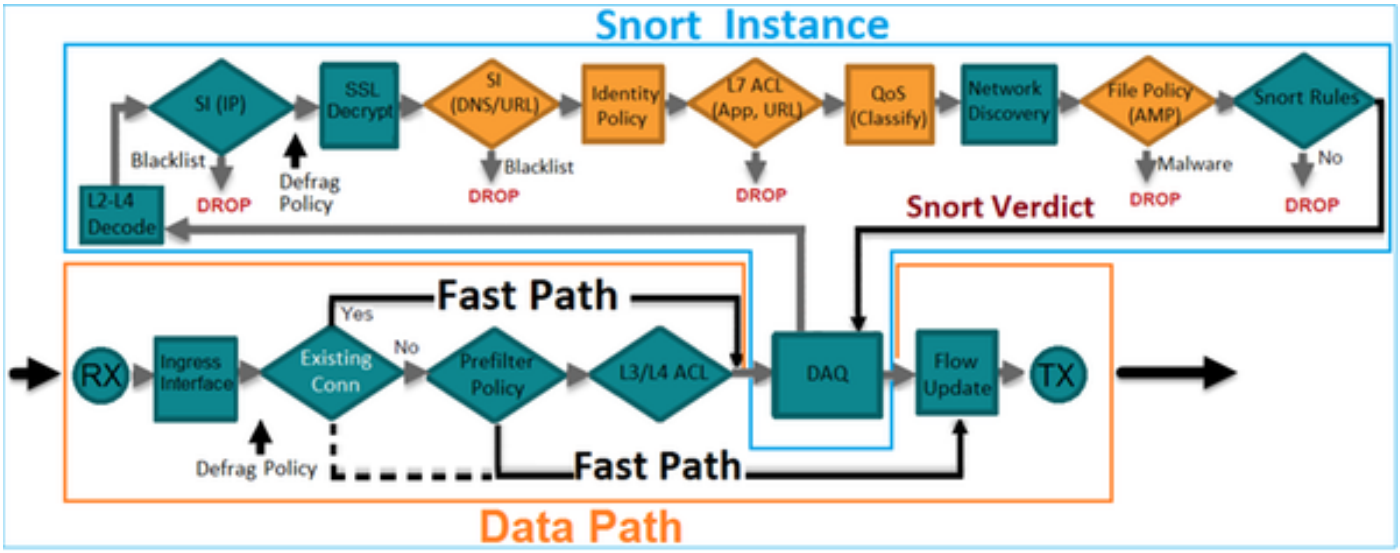
```
> show capture CAPI packet-number 1 trace3 packets captured 1: 15:27:54.327146 192.168.201.50.20
> 192.168.201.60.80: S 0:0(0) ack 0 win 8192Phase: 1Type: CAPTURESubtype:Result:
ALLOWConfig:Additional Information:MAC Access listPhase: 2Type: ACCESS-LISTSubtype:Result:
ALLOWConfig:Implicit RuleAdditional Information:MAC Access listPhase: 3Type: NGIPS-MODESubtype:
ngips-modeResult: ALLOWConfig:Additional Information:The flow ingressed an interface configured
for NGIPS mode and NGIPS services will be appliedPhase: 4Type: ACCESS-LISTSubtype: logResult:
ALLOWConfig:access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced permit ip any any
rule-id 268438528access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD4100 -
Default/1access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: DEFAULT ACTION
RULEAdditional Information: This packet will be sent to snort for additional processing where a
verdict will be reachedPhase: 5Type: NGIPS-EGRESS-INTERFACE-LOOKUPSubtype: Resolve Egress
InterfaceResult: ALLOWConfig:Additional Information:Ingress interface INSIDE is in NGIPS inline
mode.Egress interface OUTSIDE is determined by inline-set configurationPhase: 6Type: FLOW-
CREATIONSubtype:Result: ALLOWConfig:Additional Information:New flow created with id 282, packet
dispatched to next modulePhase: 7Type: EXTERNAL-INSPECTSubtype:Result: ALLOWConfig:Additional
Information:Application: 'SNORT Inspect'Phase: 8Type: SNORTSubtype:Result:
ALLOWConfig:Additional Information:Snort Verdict: (pass-packet) allow this packetPhase: 9Type:
CAPTURESubtype:Result: ALLOWConfig:Additional Information:MAC Access listResult:input-interface:
OUTSIDEinput-status: upinput-line-status: upAction: allow1 packet shown>
```

Отслеживание второго захваченного пакета показывает, что пакет совпадает с существующим соединением, таким образом, это обходит проверку ACL, но все еще осмотрено механизмом Фырканья:

```
> show capture CAPI packet-number 2 trace3 packets captured 2: 15:27:54.330000 192.168.201.50.20
> 192.168.201.60.80: S 0:0(0) ack 0 win 8192Phase: 1Type: CAPTURESubtype:Result:
ALLOWConfig:Additional Information:MAC Access listPhase: 2Type: ACCESS-LISTSubtype:Result:
ALLOWConfig:Implicit RuleAdditional Information:MAC Access listPhase: 3Type: FLOW-
LOOKUPSubtype:Result: ALLOWConfig:Additional Information:Found flow with id 282, using existing
flowPhase: 4Type: EXTERNAL-INSPECTSubtype:Result: ALLOWConfig:Additional
Information:Application: 'SNORT Inspect'Phase: 5Type: SNORTSubtype:Result:
ALLOWConfig:Additional Information:Snort Verdict: (pass-packet) allow this packetPhase: 6Type:
CAPTURESubtype:Result: ALLOWConfig:Additional Information:MAC Access listResult:input-interface:
OUTSIDEinput-status: upinput-line-status: upAction: allow1 packet shown>
```

Проверка 3? Механизм межсетевого экрана отлаживает для Позволенного трафика

Механизм межсетевого экрана отлаживает выполнения против отдельных компонентов Механизма Фырканья FTD как Политика контроля доступа:



При передаче пакетов SYN/ACK TCP через Встроенную Пару вы видите в выходных данных отладки:

```
> system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address: 192.168.201.60
Please specify a server port: 80
Monitoring firewall engine debug messages

192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 New session
192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 using HW or preset rule order 3, id 268438528
action Allow and prefilter rule 0
192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 allow action
192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 Deleting session
```

Проверка 4? Проверка распространения состояния канала

Включите буфер, входящий в систему FTD, и завершите работу порта коммутатора, связанного с интерфейсом e1/6. На CLI FTD необходимо видеть, что выключились оба интерфейса:

```
> show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
Internal-Data0/0           unassigned      YES unset up                     up
Internal-Data0/1           unassigned      YES unset up                     up
Internal-Data0/2           169.254.1.1     YES unset up                     up
Ethernet1/6                unassigned      YES unset down                   down
Ethernet1/7                unassigned      YES unset up                     up
Ethernet1/8                unassigned      YES unset administratively down up
>
```

Журналы FTD показывают:

```
> show logging

Jan 03 2017 15:53:19: %ASA-4-411002: Line protocol on Interface Ethernet1/6, changed state to
down
Jan 03 2017 15:53:19: %ASA-4-411004: Interface OUTSIDE, changed state to administratively down
Jan 03 2017 15:53:19: %ASA-4-411004: Interface Ethernet1/8, changed state to administratively
down
Jan 03 2017 15:53:19: %ASA-4-812005: Link-State-Propagation activated on inline-pair due to
failure of interface Ethernet1/6(INSIDE) bringing down pair interface Ethernet1/8(OUTSIDE)
>
```

Статус встроенного набора показывает состояние 2 интерфейсных участников:

```
> show inline-set

Inline-set Inline-Pair-1
 Mtu is 1500 bytes
 Failsafe mode is on/activated
 Failsecure mode is off
 Tap mode is off
 Propagate-link-state option is on
 hardware-bypass mode is disabled
 Interface-Pair[1]:
   Interface: Ethernet1/6 "INSIDE"
     Current-Status: Down(Propagate-Link-State-Activated)
   Interface: Ethernet1/8 "OUTSIDE"
     Current-Status: Down(Down-By-Propagate-Link-State)
   Bridge Group ID: 509
>
```

Обратите внимание на различие в статусе 2 интерфейсов:

```
> show interface e1/6
Interface Ethernet1/6 "INSIDE", is down, line protocol is down
 Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
       MAC address 5897.bdb9.770e, MTU 1500
       IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1
       Propagate-Link-State-Activated
       IP address unassigned
 Traffic Statistics for "INSIDE":
       3393 packets input, 234923 bytes
       120 packets output, 49174 bytes
       1 packets dropped
     1 minute input rate 0 pkts/sec, 0 bytes/sec
     1 minute output rate 0 pkts/sec, 0 bytes/sec
     1 minute drop rate, 0 pkts/sec
     5 minute input rate 0 pkts/sec, 6 bytes/sec
     5 minute output rate 0 pkts/sec, 3 bytes/sec
     5 minute drop rate, 0 pkts/sec
>
```

И для интерфейса Ethernet1/8:

```
> show interface e1/8
Interface Ethernet1/8 "OUTSIDE", is administratively down, line protocol is up
 Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
       MAC address 5897.bdb9.774d, MTU 1500
       IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1
```

```
        Down-By-Propagate-Link-State
        IP address unassigned
 Traffic Statistics for "OUTSIDE":
        120 packets input, 46664 bytes
        3391 packets output, 298455 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec, 0 bytes/sec
      1 minute output rate 0 pkts/sec, 0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec, 3 bytes/sec
      5 minute output rate 0 pkts/sec, 8 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

После реактивирования порта коммутатора журналы FTD показывают:

```
> show logging
...
Jan 03 2017 15:59:35: %ASA-4-411001: Line protocol on Interface Ethernet1/6, changed state to up
Jan 03 2017 15:59:35: %ASA-4-411003: Interface Ethernet1/8, changed state to administratively up
Jan 03 2017 15:59:35: %ASA-4-411003: Interface OUTSIDE, changed state to administratively up
Jan 03 2017 15:59:35: %ASA-4-812006: Link-State-Propagation de-activated on inline-pair due to
recovery of interface Ethernet1/6(INSIDE) bringing up pair interface Ethernet1/8(OUTSIDE)
>
```

Проверка 5? Статическая NAT Настройка

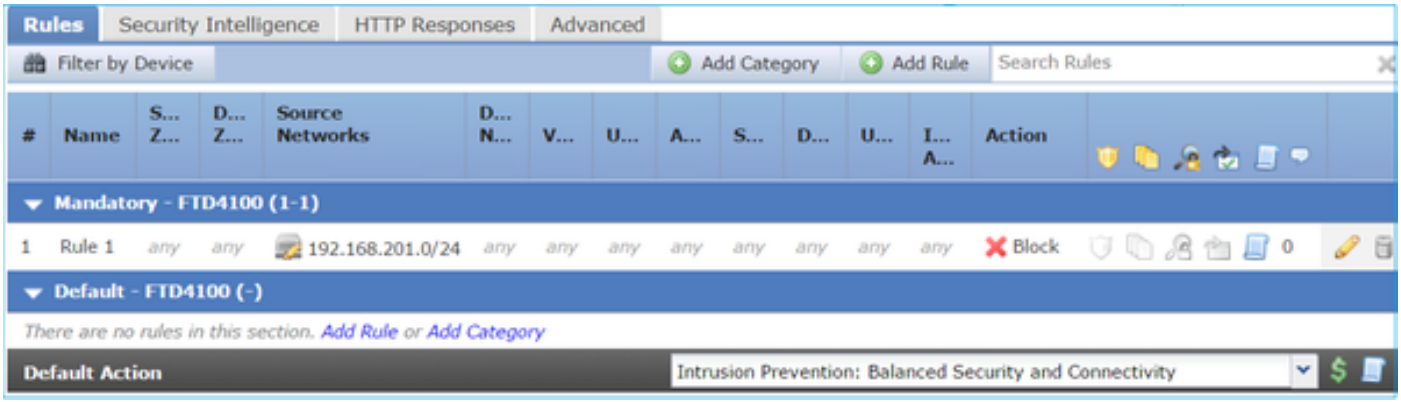
Решение

NAT не поддерживается для интерфейсов, работающих во встроенном, встроенном ответвителе или пассивных режимах:

http://www.cisco. com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Network_Address_Translation__NAT__for_Threat_Defense.html

Блокирование пакета на Встроенном Парном интерфейсном режиме

Создайте Правило блокировки как следующее, передайте трафик через FTD Встроенная Пара и наблюдайте поведение:



Решение

Включите перехват с трассировкой и передайте пакеты SYN/ACK через FTD Встроенная Пара. Трафик заблокирован:

```
> show capturecapture CAPI type raw-data trace interface INSIDE [Capturing - 210 bytes] match ip host 192.168.201.60 anycapture CAPO type raw-data interface OUTSIDE [Capturing - 0 bytes] match ip host 192.168.201.60 any
```

Отслеживание пакета показывает:

```
> show capture CAPI packet-number 1 trace

3 packets captured

  1: 16:12:55.785085       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
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: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 4
Type: ACCESS-LIST
Subtype: log
```

```
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600
event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD4100 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: Rule 1
Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule


1 packet shown
```

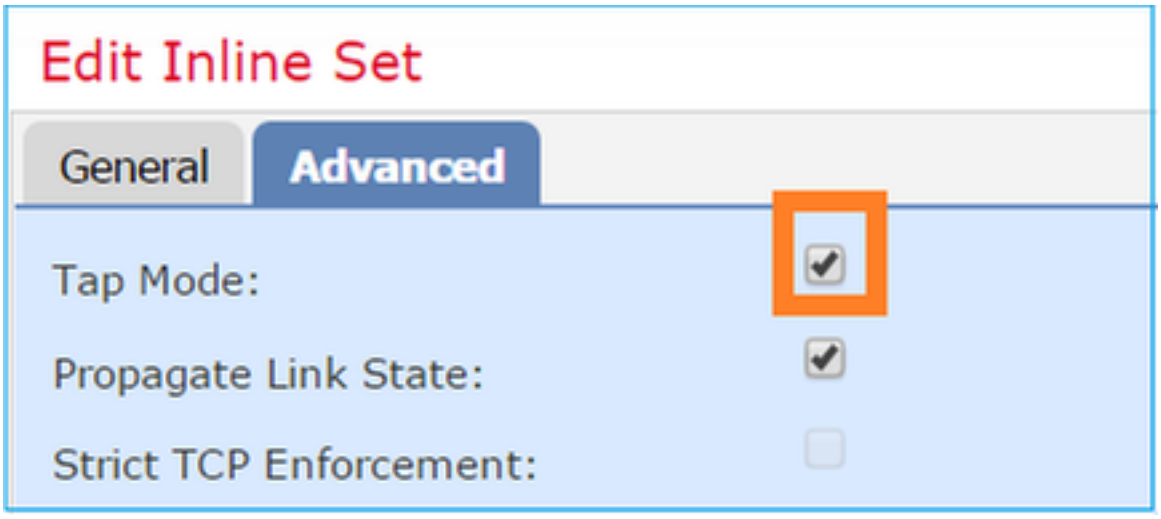
В вышеупомянутой трассировке можно заметить, что пакет был отброшен механизмом ASA FTD и не был передан к механизму Фырканья FTD.

Настройка Встроенный Парный режим с Ответвителем

Включите режим Ответвителя на Встроенной Паре

Решение

Перейдите к **Устройствам> Управление устройствами> Встроенные Наборы**, отредактируйте Встроенную Пару, щелкните **по Вкладке Дополнительно** и включите **Режим Ответвителя**:



Проверка

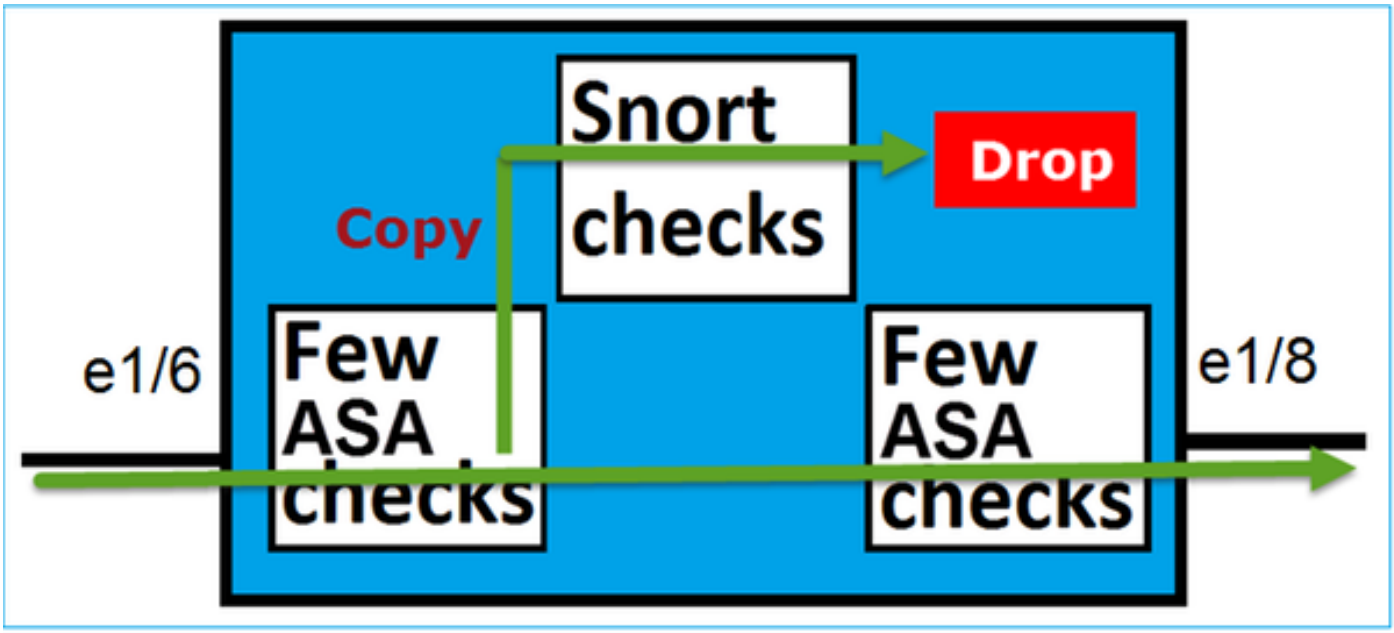
```
> show inline-setInline-set Inline-Pair-1 Mtu is 1500 bytes Failsafe mode is on/activated
Failsecure mode is off Tap mode is on Propagate-link-state option is on hardware-bypass mode is
disabled Interface-Pair[1]: Interface: Ethernet1/6 "INSIDE" Current-Status: UP Interface:
Ethernet1/8 "OUTSIDE" Current-Status: UP Bridge Group ID: 0>
```

Проверка FTD Встроенная Пара с операцией интерфейса Ответвителя

Теоретические сведения

- При настройке Встроенной Пары с Ответвителем внутренне соединены 2 физических интерфейса
- Доступный в **Направленных** или **Прозрачных** режимах **Развертываний**
- **Большинство функций механизма ASA** (NAT, Маршрутизация, ACL L3/L4 и т.д.) **не доступно** для потоков, проходящих Встроенную Пару
- Фактический трафик **не может быть отброшен**
- **Немного** проверок **механизма ASA** применены наряду с **полными** проверками **механизма Фырканья к копии фактического трафика**

Последняя точка может визуализироваться следующим образом:



Встроенная Пара с Режимом Ответвителя не отбрасывает транзитный трафик. Отслеживание пакета подтверждает это:

```
> show capture CAPI packet-number 2 trace3 packets captured 2: 13:34:30.685084 192.168.201.50.20
> 192.168.201.60.80: S 0:0(0) win 8192Phase: 1Type: CAPTURESubtype:Result:
ALLOWConfig:Additional Information:MAC Access listPhase: 2Type: ACCESS-LISTSubtype:Result:
ALLOWConfig:Implicit RuleAdditional Information:MAC Access listPhase: 3Type: NGIPS-MODESubtype:
ngips-modeResult: ALLOWConfig:Additional Information:The flow ingressed an interface configured
for NGIPS mode and NGIPS services will be appliedPhase: 4Type: ACCESS-LISTSubtype: logResult:
WOULD HAVE DROPPEDConfig:access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced deny ip
192.168.201.0 255.255.255.0 any rule-id 268441600 event-log flow-startaccess-list CSM_FW_ACL_
remark rule-id 268441600: ACCESS POLICY: FTD4100 - Mandatory/1access-list CSM_FW_ACL_ remark
rule-id 268441600: L4 RULE: Rule 1Additional Information:Result:input-interface: INSIDEinput-
status: upinput-line-status: upAction: Access-list would have dropped,but packet forwarded due
to inline-tap1 packet shown
>
```

Сравнение: встроенная пара по сравнению со встроенной парой с ответвителем

	Встроенная пара	Встроенная пара с Ответвителем
покажите встроенный набор	> покажите встроенный набор Встроенный набор Inline-Pair-1 Mtu составляет 1500 байтов Отказоустойчивый режим включен Режим Failsecure выключен Коснитесь режим выключен Опция распространяться-состояния-канала идет аппаратный транзитный режим отключен Интерфейсно-парный [1]: Интерфейс : Ethernet1/6 "ВНУТРИ" Текущий статус: _____ включен Интерфейс : Ethernet1/8 "СНАРУЖИ" Текущий статус: _____ включен ID группы мостов: 509	> покажите встроенный набор Встроенный набор Inline-Pair-1 Mtu составляет 1500 байтов Отказоустойчивый режим включен Режим Failsecure выключен Коснитесь режим идет Опция распространяться-состояния-ка идет аппаратный транзитный режим отключе Интерфейсно-парный [1]: Интерфейс : Ethernet1/6 "ВНУТРИ" Текущий статус: _____ включен Интерфейс : Ethernet1/8 "СНАРУЖИ" Текущий статус: _____ включен ID группы мостов: 0
show interface	> > e1/6 show interface Интерфейсный Ethernet1/6 "ВНУТРИ", подключен, протокол линии связи подключен Аппаратными средствами является EtherSVI, BW 1000 Мбит/с, DLY 1000 мкс MAC-адрес 5897.bdb9.770e, MTU 1500 Интерфейсный Режим IPS: встроенный, Встроенный Набор: Inline-Pair-1 IP-адрес неприсвоенным Статистика трафика для "ВНУТРИ": 3957 пакетных вводов, 264913 байтов 144 пакетных выходных данных, 58664 байта 4 пакета понизились	> > e1/6 show interface Интерфейсный Ethernet1/6 "ВНУТРИ", подключен, протокол линии связи подкл Аппаратными средствами является EtherSVI, BW 1000 Мбит/с, DLY 1000 мк MAC-адрес 5897.bdb9.770e, MTU 15 Интерфейсный Режим IPS: встроен ответвитель, Встроенный Набор: Inline- IP-адрес неприсвоенным Статистика трафика для "ВНУТРИ": 24 пакетных ввода, 1378 байтов 0 пакетных выходных данных, 0 бай 24 пакета понизились Скорость входного потока 1 минуты

	Скорость входного потока 1 минуты 0 pkts/сек., 26 байтов/сек. 1 скорость выхода в минуту 0 pkts/сек., 7 байтов/сек. Уровень сброса 1 минуты, 0 pkts/сек. 5-минутная скорость входного потока 0 pkts/сек., 28 байтов/сек. 5 скоростей выхода в минуту 0 pkts/сек., 9 байтов/сек. 5-минутный уровень сброса, 0 pkts/сек. **>e1/8 show interface** Интерфейсный Ethernet1/8 "СНАРУЖИ", подключен, протокол линии связи подключен Аппаратными средствами является EtherSVI, BW 1000 Мбит/с, DLY 1000 мкс MAC-адрес 5897.bdb9.774d, MTU 1500 Интерфейсный Режим IPS: **встроенный**, Встроенный Набор: Inline-Pair-1 IP-адрес неприсвоенным Статистика трафика для "СНАРУЖИ": 144 пакетных ввода, 55634 байта 3954 пакетных выходных данных, 339987 байтов 0 пакетов понизились Скорость входного потока 1 минуты 0 pkts/сек., 7 байтов/сек. 1 скорость выхода в минуту 0 pkts/сек., 37 байтов/сек. Уровень сброса 1 минуты, 0 pkts/сек. 5-минутная скорость входного потока 0 pkts/сек., 8 байтов/сек. 5 скоростей выхода в минуту 0 pkts/сек., 39 байтов/сек. 5-минутный уровень сброса, 0 pkts/сек. > **> трассировка пакетного номера 1 CAPI show capture** Перехвачены 3 пакета 1: 16:12:55.785085 192.168.201.50.20> 192.168.201.60.80: S 0:0 (0) ack 0 побед 8192 Этап 1 Введите : ПЕРЕХВАТ Подтип: Результат: ПОЗВОЛИТЬ Config: Дополнительные сведения: Список доступа MAC Этап 2 Введите : ACCESS-LIST Подтип:	pkts/сек., 0 байтов/сек. 1 скорость выхода в минуту 0 pkts/се байтов/сек. Уровень сброса 1 минуты, 0 pkts/сек. 5-минутная скорость входного потока pkts/сек., 0 байтов/сек. 5 скоростей выхода в минуту 0 pkts/с байтов/сек. 5-минутный уровень сброса, 0 pkts/се **>e1/8 show interface** Интерфейсный Ethernet1/8 "СНАРУЖИ" подключен, протокол линии связи подкл Аппаратными средствами является EtherSVI, BW 1000 Мбит/с, DLY 1000 мк MAC-адрес 5897.bdb9.774d, MTU 15 Интерфейсный Режим IPS: **встроен ответвитель**, Встроенный Набор: Inline- IP-адрес неприсвоенным Статистика трафика для "СНАРУЖИ": 1 пакетный ввод, 441 байт 0 пакетных выходных данных, 0 бай 1 пакет понизился Скорость входного потока 1 минуты pkts/сек., 0 байтов/сек. 1 скорость выхода в минуту 0 pkts/се байтов/сек. Уровень сброса 1 минуты, 0 pkts/сек. 5-минутная скорость входного потока pkts/сек., 0 байтов/сек. 5 скоростей выхода в минуту 0 pkts/с байтов/сек. 5-минутный уровень сброса, 0 pkts/се > **> трассировка пакетного номера 1 CAPI show capture** Перехвачены 3 пакета 1: 16:56:02.631437 192.168.201.50.2 192.168.201.60.80: S 0:0 (0) победа 8192 Этап 1 Введите : ПЕРЕХВАТ Подтип: Результат: ПОЗВОЛИТЬ Config: Дополнительные сведения: Список доступа MAC Этап 2 Введите : ACCESS-LIST Подтип:
Пакетная обработка через **Правило блокировки**		

Результат: ПОЗВОЛИТЬ
Config:
Неявное правило
Дополнительные сведения:
Список доступа MAC

Стадия 3
Введите : NGIPS-РЕЖИМ
Подтип: ngips-режим
Результат: ПОЗВОЛИТЬ
Config:
Дополнительные сведения:
Поток ingressed интерфейс, настроенный для режима NGIPS и сервисов NGIPS, будет применен

Этап 4
Введите : ACCESS-LIST
Подтип: журнал
Результат: ОТБРАСЫВАНИЕ
Config:
access-group глобальный CSM_FW_ACL_
access-list усовершенствованные CSM_FW_ACL_ запрещают ip 192.168.201.0 255.255.255.0 любых идентификаторов правила 268441600 event-log, запускается поток
access-list CSM_FW_ACL_ отмечает идентификатор правила 268441600: ПОЛИТИКА ДОСТУПА: FTD4100 - Обязательный/1
access-list CSM_FW_ACL_ отмечает идентификатор правила 268441600: ПРАВИЛО L4: Правило 1
Дополнительные сведения:

Результат:
input-interface: ВНУТРИ
входной статус: _____ включен
статус входной линии: _____ включен
Действие: отбрасывание
Причина отбрасывания: (acl-drop) Поток запрещен настроенным правилом

1 показанный пакет
>

Результат: ПОЗВОЛИТЬ
Config:
Неявное правило
Дополнительные сведения:
Список доступа MAC

Стадия 3
Введите : NGIPS-РЕЖИМ
Подтип: ngips-режим
Результат: ПОЗВОЛИТЬ
Config:
Дополнительные сведения:
Поток ingressed интерфейс, настроенны для режима NGIPS и сервисов NGIPS, б применен

Этап 4
Введите : ACCESS-LIST
Подтип: журнал
Результат: WOULD HAVE ПОНИЗИЛСЯ
Config:
access-group глобальный CSM_FW_ACL
access-list усовершенствованные CSM_FW_ACL_ запрещают ip 192.168.2 255.255.255.0 любых идентификаторов правила 268441600 event-log, запускает поток
access-list CSM_FW_ACL_ отмечает идентификатор правила 268441600: ПОЛИТИКА ДОСТУПА: FTD4100 - Обязательный/1
access-list CSM_FW_ACL_ отмечает идентификатор правила 268441600: ПРАВИЛО L4: Правило 1
Дополнительные сведения:

Результат:
input-interface: ВНУТРИ
входной статус: _____ включен
статус входной линии: _____ включе
Действие: Access-list понизился бы, но передал из-за встроенного ответвителя

1 показанный пакет
>

Сводка

- При использовании Встроенного Парного режима пакет идет в основном через механизм Фырканья FTD.
- TCP - подключения обрабатываются в транзитном режиме состояния TCP
- С точки зрения механизма ASA FTD применяется политика ACL
- Когда Встроенный Парный Режим используется, пакеты могут быть заблокированы, так как они обработаны встроенные
- Когда Режиму Ответвителя включают, копия пакета осмотрена и отброшена внутренне, в то время как фактический трафик проходит FTD немодифицированный

Дополнительная документация

Огневая мощь Cisco NGFW