Защита Угрозы FirePOWER Настройки взаимодействует в Режиме маршрутизации

Содержание

Введение

Этот документ описывает конфигурацию, проверку и фоновую работу Встроенного Парного Интерфейса на устройстве Защиты угрозы FirePOWER (FTD).

Предварительные условия

Требования

Нет определенных требований для этого документа.

Используемые компоненты

- ASA5512-X, выполняющий код 6.1.0 FTD. x
- Центр управления FirePOWER (FMC), работающий 6.1.0. x

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.

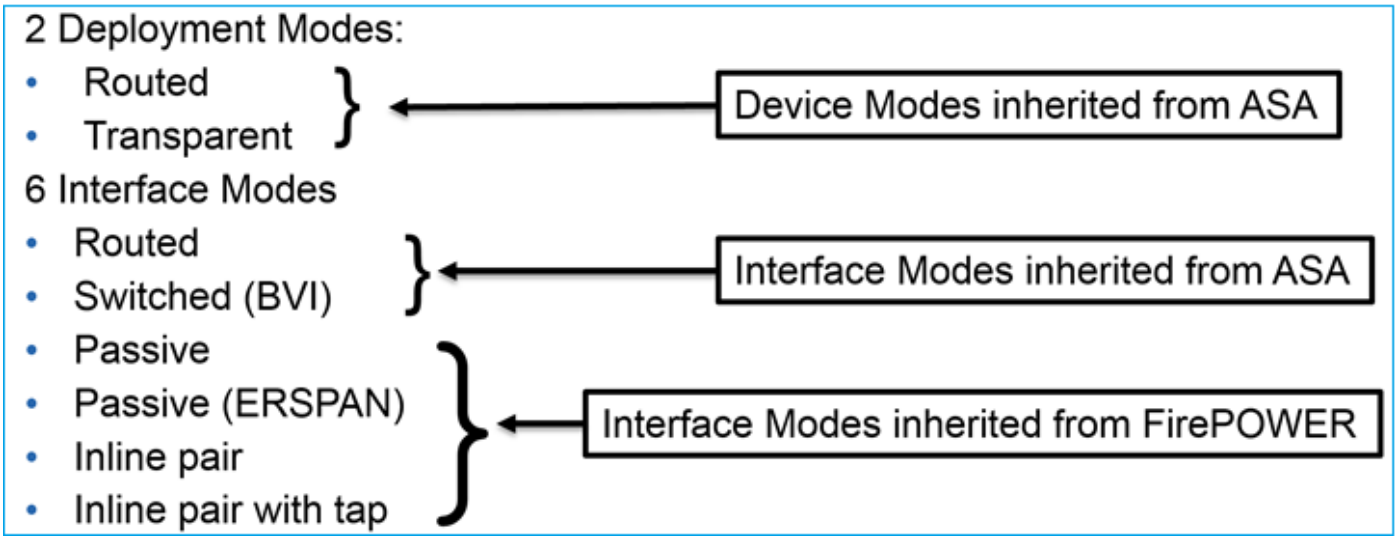
Родственные продукты

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

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR2100, FPR4100, FPR9300
- VMware (ESXi), Веб-сервисы Amazon (AWS), клавиатура/Видео/Мышь (KVM)
- Программный код FTD 6.2.x и позже.

Общие сведения

FTD предоставляет два режима Развертываний и шесть Интерфейсных режимов как показано в следующем образе:



Примечание: Можно смешать интерфейсные режимы на одиночном устройстве FTD.

Глобальный обзор различных развертываний FTD и интерфейсных режимов:

Режим интерфейса FTD	Режим Развертываний FTD	Описание	Трафик может быть отброшен
Направленный	Направленный	Полные проверки механизма и механизма Фырканья LINA	Да
Коммутируемый	Прозрачный	Полные проверки механизма и механизма Фырканья LINA	Да

Встроенная пара	Направленный или прозрачный	Частичный механизм LINA и полные проверки механизма Фырканья	Да
Встроенная пара с ответвителем	Направленный или прозрачный	Частичный механизм LINA и полные проверки механизма Фырканья	Нет
Пассивный	Направленный или прозрачный	Частичный механизм LINA и полные проверки механизма Фырканья	Нет
Пассивный (ERSPAN)	Направленный	Частичный механизм LINA и полные проверки механизма Фырканья	Нет

Настройка

Схема сети

Настройте маршрутизируемый интерфейс и подинтерфейс

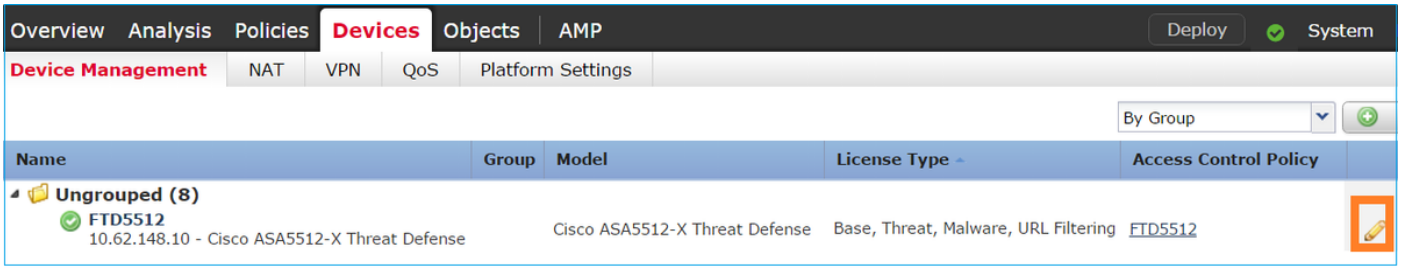
Настройте подинтерфейс G0/0.201 и интерфейсный G0/1 согласно следующим требованиям:

Interface	G0/0.201	G0/1
Name	Внутри	СНАРУЖИ
Зона безопасности	INSIDE_ZONE	OUTSIDE_ZONE
Описание	ВНУТРЕННИЙ	ВНЕШНИЙ
ID интерфейса Sub	201	-
Идентификатор VLAN	201	-
IPv4	192.168.201.1/24	192.168.202.1/24
Дуплекс/Скорость	Auto	Auto

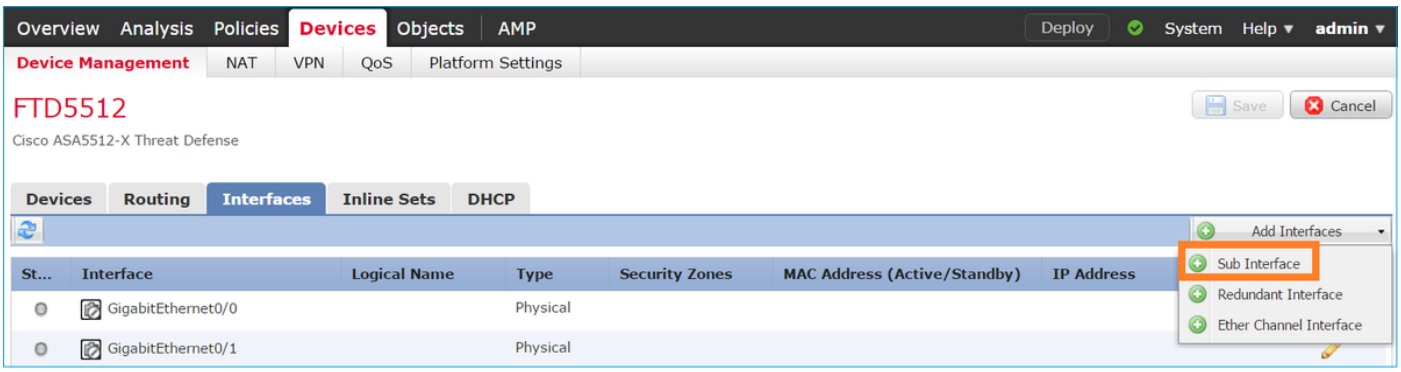
Решение

Шаг 1. Настройте логический интерфейс

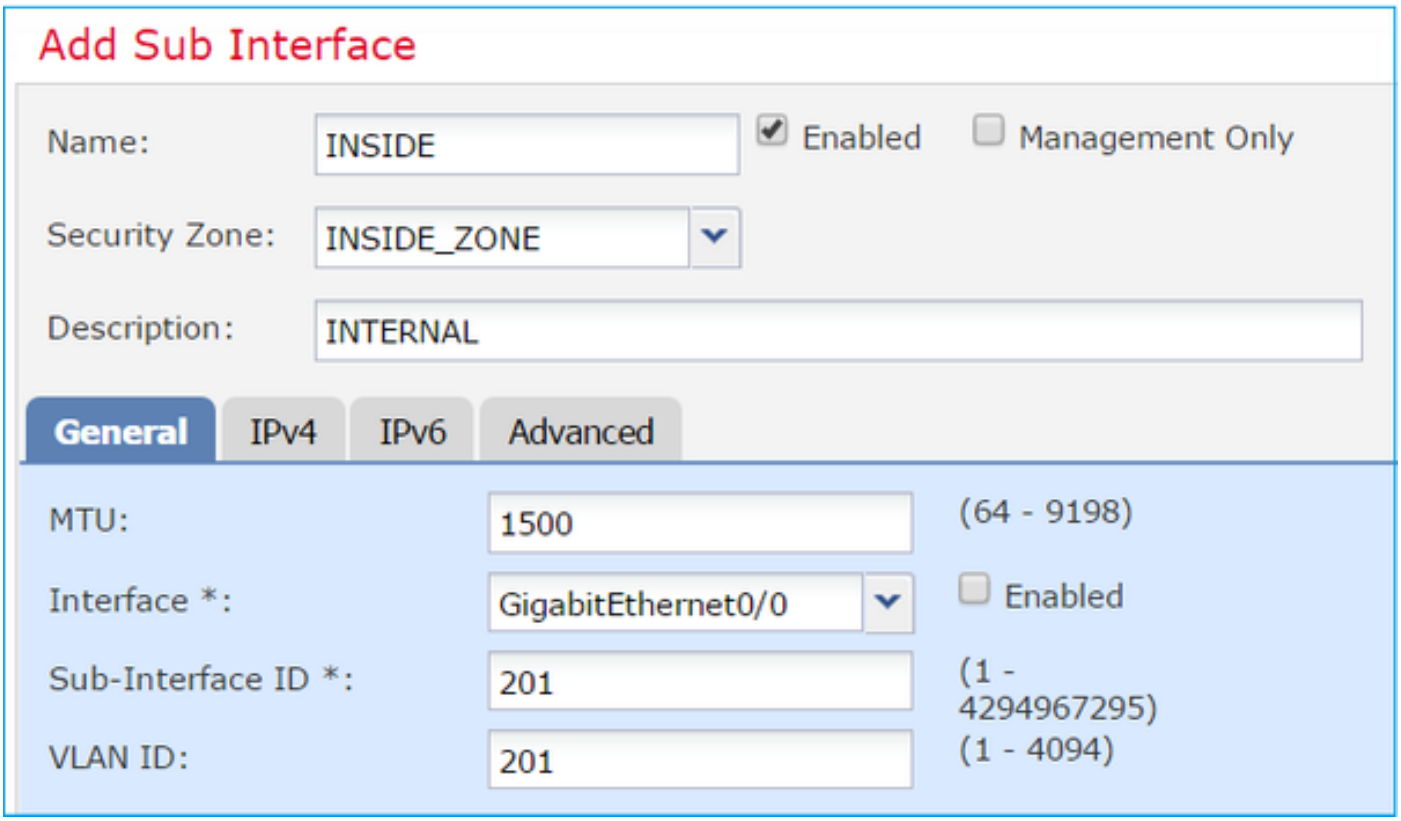
Перейдите к **Устройствам> Управление устройствами,** выберите соответствующее устройство и выберите **Значок редактирования**:



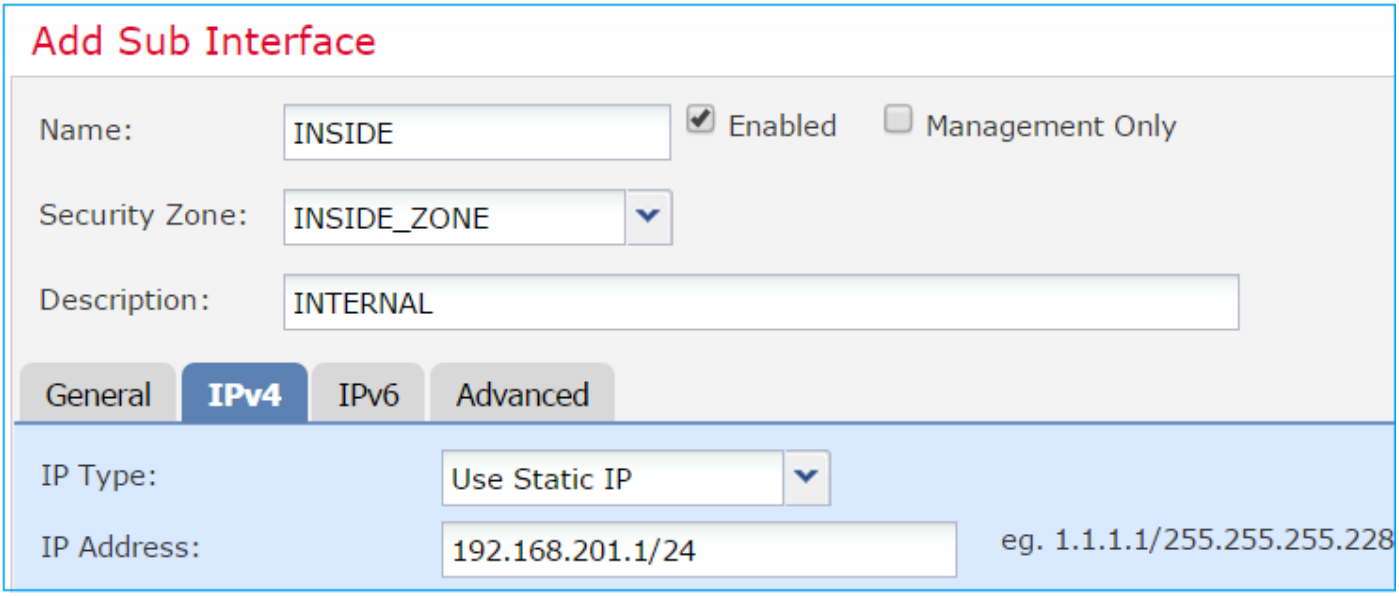
Выберите **Add Interfaces> Sub Interface**:



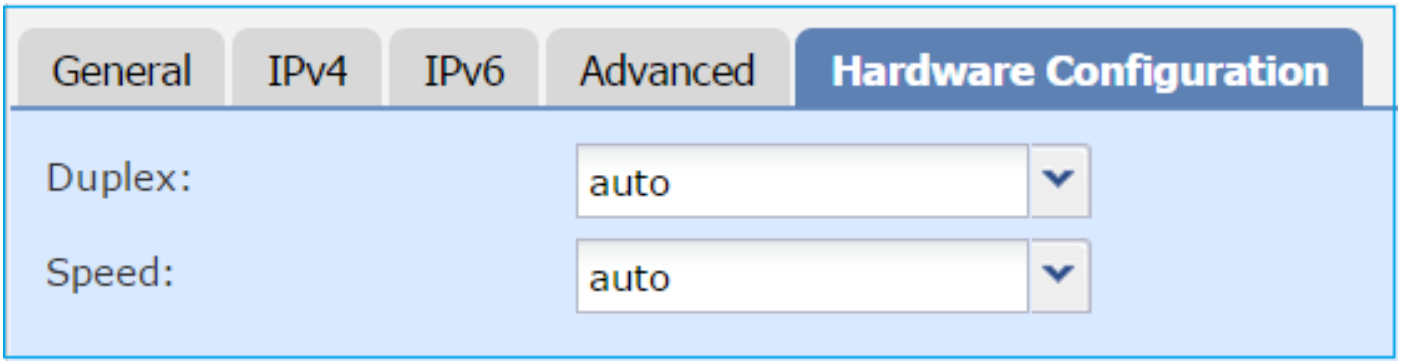
Настройте параметры настройки подинтерфейса согласно требованиям:



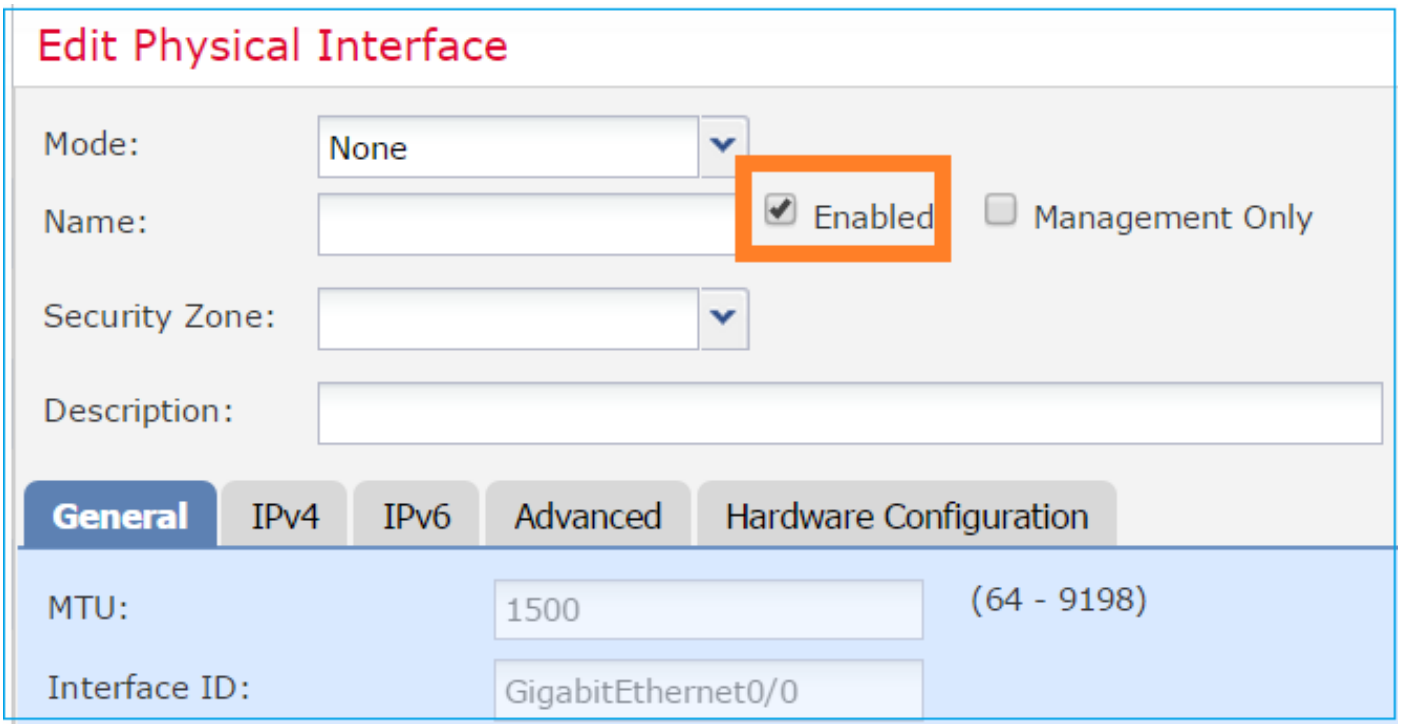
Интерфейсные параметры настройки IP:



Под физическим интерфейсом (GigabitEthernet0/0) задают дуплекс и Параметры настройки скорости:

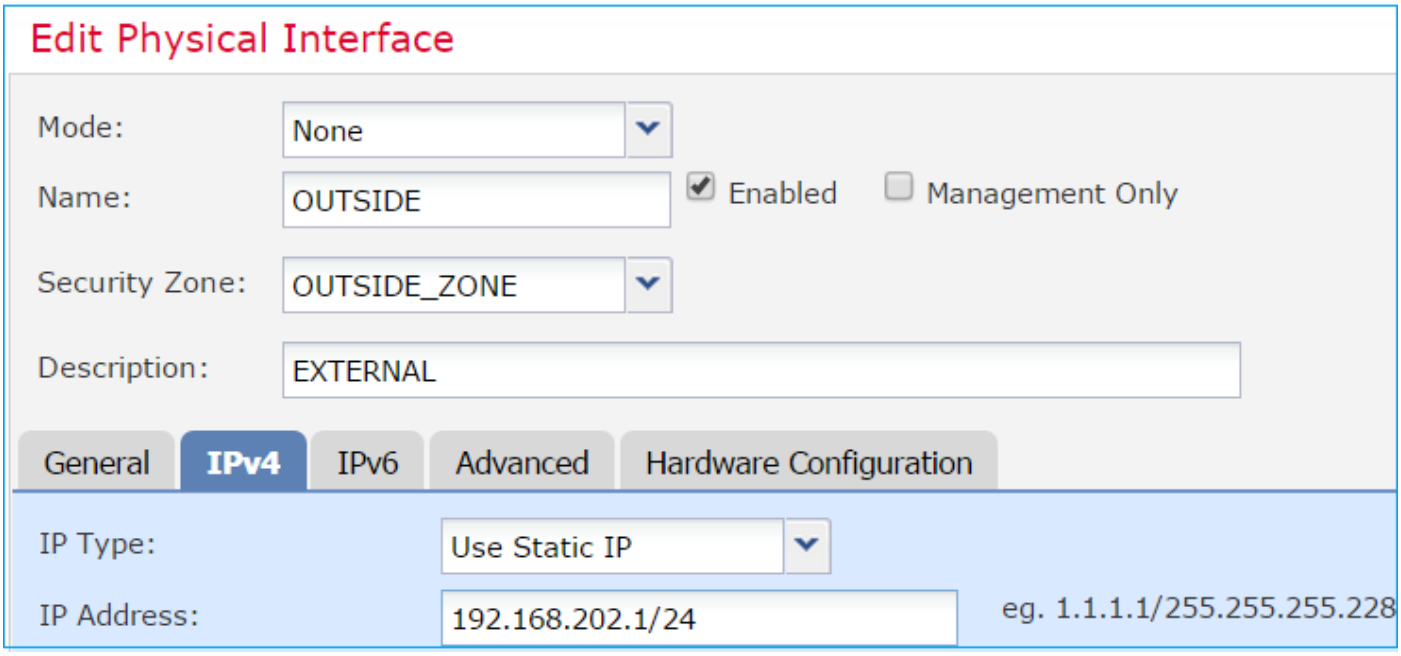


Включите физический интерфейс (G0/0 в этом случае):



Шаг 2. Настройте физический интерфейс

Отредактируйте физический интерфейс GigabitEthernet0/1 согласно требованиям:

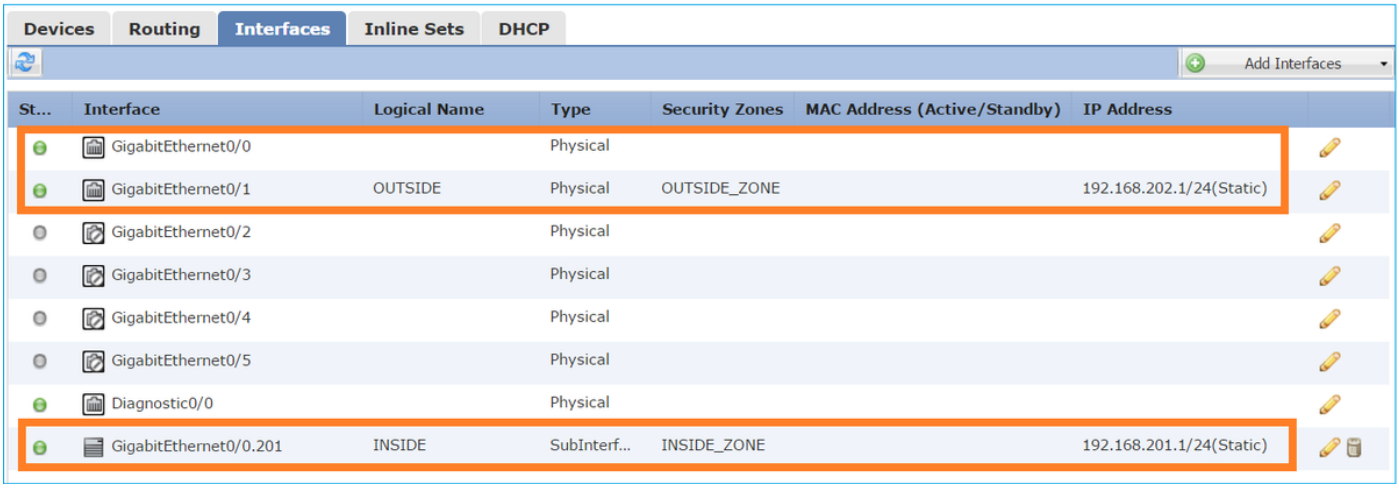


- Для Маршрутизируемого интерфейса Режим: **Нет**
- Название эквивалентно **nameif** интерфейса ASA
- На FTD все интерфейсы имеют уровень безопасности = 0
- **same-security-traffic** не применим на FTD. Трафик между интерфейсами FTD (предает земле), и прикрепление (intra) позволен по умолчанию

Выберите **Save** и **Deploy.**

Проверка

От GUI FMC:

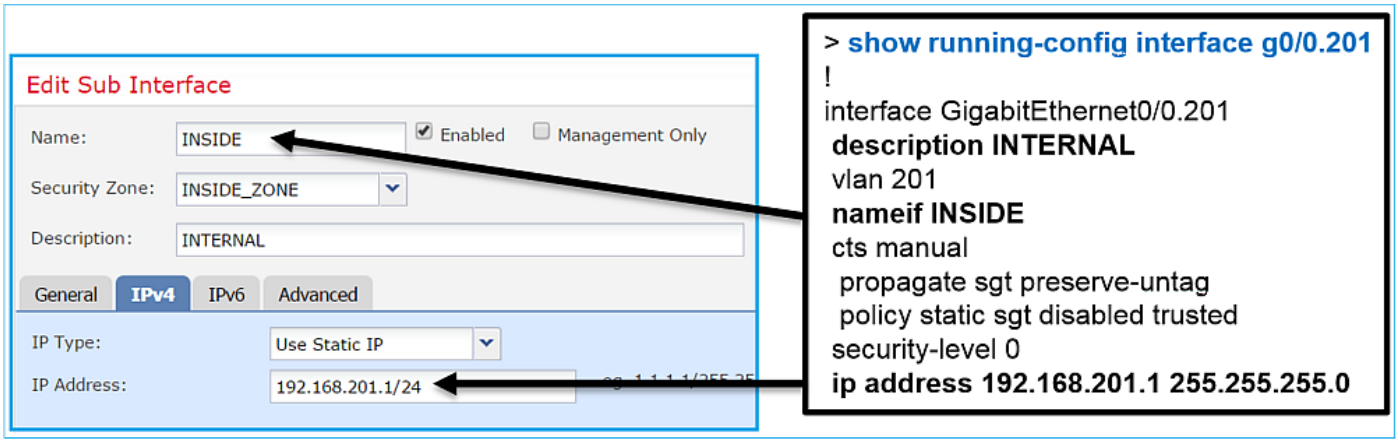


От CLI FTD:

```
> show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES unset  up                    up
GigabitEthernet0/0.201     192.168.201.1   YES manual up                    up
GigabitEthernet0/1         192.168.202.1   YES manual up                    up
GigabitEthernet0/2         unassigned      YES unset  administratively down down
GigabitEthernet0/3         unassigned      YES unset  administratively down down
GigabitEthernet0/4         unassigned      YES unset  administratively down down
GigabitEthernet0/5         unassigned      YES unset  administratively down down
Internal-Control0/0        127.0.1.1       YES unset  up                    up
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
Management0/0              unassigned      YES unset  up                    up
```

```
> show ip
System IP Addresses:
Interface                Name                IP address      Subnet mask     Method
GigabitEthernet0/0.201   INSIDE              192.168.201.1   255.255.255.0   manual
GigabitEthernet0/1       OUTSIDE             192.168.202.1   255.255.255.0   manual
Current IP Addresses:
Interface                Name                IP address      Subnet mask     Method
GigabitEthernet0/0.201   INSIDE              192.168.201.1   255.255.255.0   manual
GigabitEthernet0/1       OUTSIDE             192.168.202.1   255.255.255.0   manual
```

GUI FMC и корреляция CLI FTD:




```
> show interface g0/0.201
Interface GigabitEthernet0/0.201 "INSIDE", is up, line protocol is up
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        VLAN identifier 201
        Description: INTERNAL
        MAC address a89d.21ce.fdea, MTU 1500
        IP address 192.168.201.1, subnet mask 255.255.255.0
  Traffic Statistics for "INSIDE":
        1 packets input, 28 bytes
        1 packets output, 28 bytes
        0 packets dropped
> show interface g0/1
Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
        Input flow control is unsupported, output flow control is off
        Description: EXTERNAL
        MAC address a89d.21ce.fde7, MTU 1500
        IP address 192.168.202.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        1 packets output, 64 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 12 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (511/511)
        output queue (blocks free curr/low): hardware (511/511)
  Traffic Statistics for "OUTSIDE":
        0 packets input, 0 bytes
        0 packets output, 0 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,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

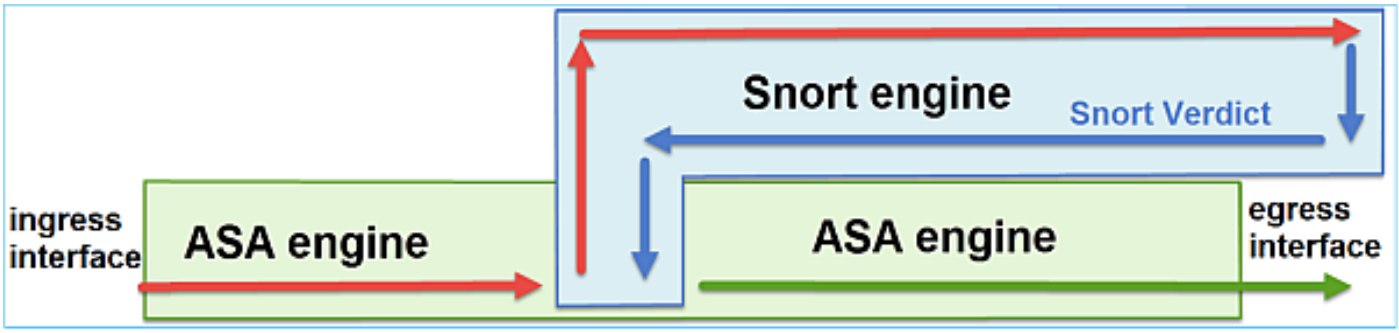
Операция маршрутизируемого интерфейса FTD

Проверьте пакетную обработку FTD, когда будут использоваться Маршрутизируемые интерфейсы.

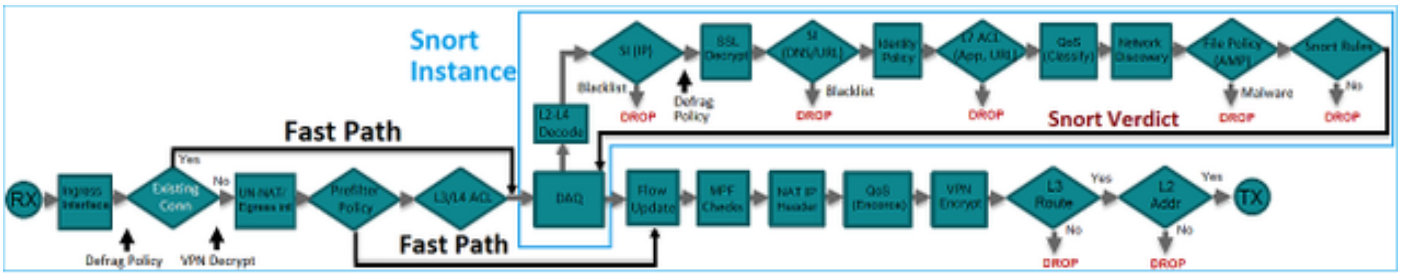
Решение

Обзор архитектуры FTD

Общий обзор плоскости данных FTD:



Следующее изображение показывает некоторые проверки, которые происходят в каждом механизме:



Ключевые точки

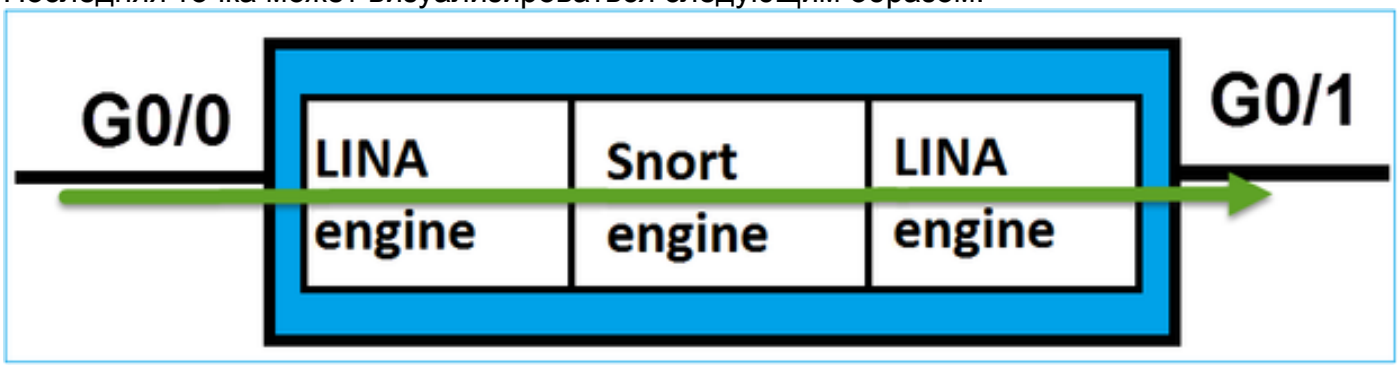
- Нижние проверки соответствуют FTD LINA Путь данных механизма
- Проверки в синем поле соответствуют экземпляру механизма Фырканья FTD

Обзор маршрутизируемого интерфейса FTD

- Доступный только в **Направленных** Развертываниях
- Традиционные **развертывания межсетевого экрана L3**
- Один или более физических или логические (VLAN) маршрутизируемые интерфейсы
- Позволяет функциям как NAT или Протоколы динамической маршрутизации быть настроенными
- Пакеты переданы на основе **Поиска маршрута**, и следующий переход решен на основе

Поиска ARP
- Фактический трафик **может быть отброшен**
- **Полные** проверки **механизма LINA** применены наряду с **полными** проверками **механизма Фырканья**

Последняя точка может визуализироваться следующим образом:



Проверка

Отследите пакет на маршрутизируемом интерфейсе FTD

Схема сети

Используйте пакетного трассировщика со следующими параметрами для наблюдения прикладной политики:

Входной интерфейс	Внутри
Протокол/Сервис	Порт TCP 80
IP-адрес отправителя	192.168.201.100
IP-адрес назначения	192.168.202.100

Решение

Когда Маршрутизируемый интерфейс используется, пакет обработан похожим способом к

классическому Маршрутизируемому интерфейсу ASA. Проверки как Поиск маршрута, Модульная система политик (MPF), NAT, поиск ARP и т.д. имеет место в Пути данных механизма LINA. Кроме того, если Политика контроля доступа требует так, пакет осмотрен механизмом Фырканья (один из экземпляров Фырканья), где вердикт (Черный список, Белый список) генерируется и возвратился назад к механизму LINA:

```
> packet-tracer input INSIDE tcp 192.168.201.100 11111 192.168.202.100 80

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.202.100 using egress ifc OUTSIDE

Phase: 2
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 268437505
access-list CSM_FW_ACL_ remark rule-id 268437505: ACCESS POLICY: FTD5512 -
Defau

                  lt/1
access-list CSM_FW_ACL_ remark rule-id 268437505: L4 RULE: DEFAULT ACTION RULE
Additional Information:
 This packet will be sent to snort for additional processing where a verdict
wil

                l be reached

Phase: 3
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map class-default
 match any
policy-map global_policy
 class class-default
 set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 11336, packet dispatched to next module

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

>
```

Примечание: В фазе 4 пакет проверен против карты TCP под названием UM_STATIC_TCP_MAP. Это - Карта TCP по умолчанию на FTD.

```
firepower# show run all tcp-map
!
tcp-map UM_STATIC_TCP_MAP
 no check-retransmission
 no checksum-verification
 exceed-mss allow
 queue-limit 0 timeout 4
 reserved-bits allow
 syn-data allow
 synack-data drop
 invalid-ack drop
 seq-past-window drop
 tcp-options range 6 7 allow
 tcp-options range 9 18 allow
 tcp-options range 20 255 allow
 tcp-options selective-ack allow
 tcp-options timestamp allow
 tcp-options window-scale allow
 tcp-options mss allow
 tcp-options md5 clear
 ttl-evasion-protection
 urgent-flag allow
 window-variation allow-connection
!
>
```

Дополнительные сведения

- Руководство по конфигурации защиты угрозы FirePOWER Cisco для менеджера устройств FirePOWER, версии 6.1
- Установка и Обновление Защиты Угрозы FirePOWER на ASA 55xx-X устройства
- Работа с перехватами Защиты угрозы FirePOWER (FTD) и пакетным трассировщиком
- Cisco Systems – техническая поддержка и документация