Конфигурация Управляющего доступ к FTD (HTTPS и SSH) через FMC

Содержание

Введение

Этот документ описывает конфигурацию управляющего доступ к Защите угрозы огневой мощи (FTD) (HTTPS и SSH) через Центр управления Firesight (FMC).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание технологии Огневой мощи
- Базовые знания о ASA (устройство адаптивной безопасности)
- Знание Управляющего доступ на ASA через HTTPS и SSH (Secure Shell)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Образ Защиты Угрозы Огневой мощи Устройства адаптивной защиты (ASA) для ASA

(5506X/5506H-X/5506W-X, 5508-X ASA, 5516-X ASA), который работает на версии программного обеспечения 6.0.1 и выше
- Образ Защиты Угрозы Огневой мощи ASA для ASA (5515-X, 5525-X ASA, 5545-X ASA, 5555-X ASA, 5585-X ASA), который работает на версии программного обеспечения 6.0.1 и выше
- Версия 6.0.1 Центра управления огневой мощи (FMC) и выше

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

С началом Защиты угрозы огневой мощи (FTD) вся связанная конфигурация ASA сделана на GUI.

На устройствах FTD, работающих под управлением ПО версии 6.0.1, обращаются к CLI диагностики ASA, поскольку вы вводите **диагностического cli поддержки системы**. Однако на устройствах FTD, работающих под управлением ПО версии 6.1.0, CLI сходится, и все команды ASA настроены на CLISH.

```
Cisco Fire Linux OS v6.0.1 (build 37)
Cisco Firepower Threat Defense for VMWare v6.0.1 (build 1213)

>                                                    CLISH
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> en
Password:
firepower#                                           DIAGNOSTIC CLI
```

Для получения управляющего доступ непосредственно от внешней сети, необходимо настроить управляющего доступ через HTTPS или SSH. Этот документ предоставляет необходимую конфигурацию, требуемую получать управляющего доступ по SSH или HTTPS внешне.

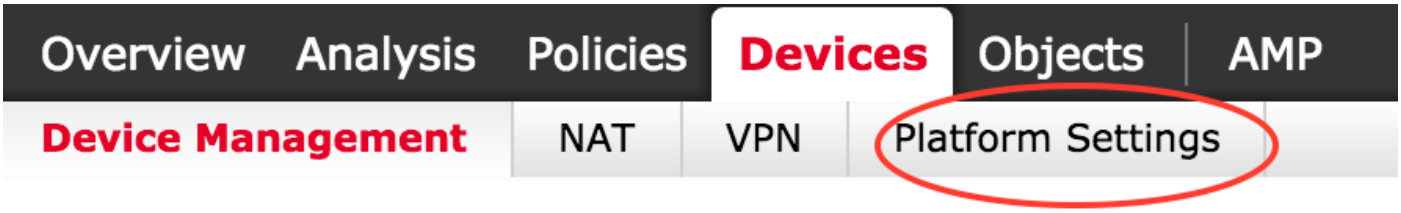
> **Примечание:** На устройствах FTD, работающих под управлением ПО версии 6.0.1, к CLI не может обратиться локальный пользователь, внешняя проверка подлинности должна быть настроена для аутентификации пользователей. В то время как внешняя проверка подлинности требуется для всех других пользователей, Однако на устройствах FTD, работающих под управлением ПО версии 6.1.0, к CLI обращается пользователь **локального администратора**

> **Примечание:** На устройствах FTD, работающих под управлением ПО версии 6.0.1, диагностический CLI не непосредственно доступен по IP, который настроен для **br1** FTD. Однако на устройствах FTD, работающих под управлением ПО версии 6.1.0, установившийся CLI доступен по любому интерфейсу, настроенному для

управляющего доступ, однако, интерфейс должен быть настроен с IP-адресом.

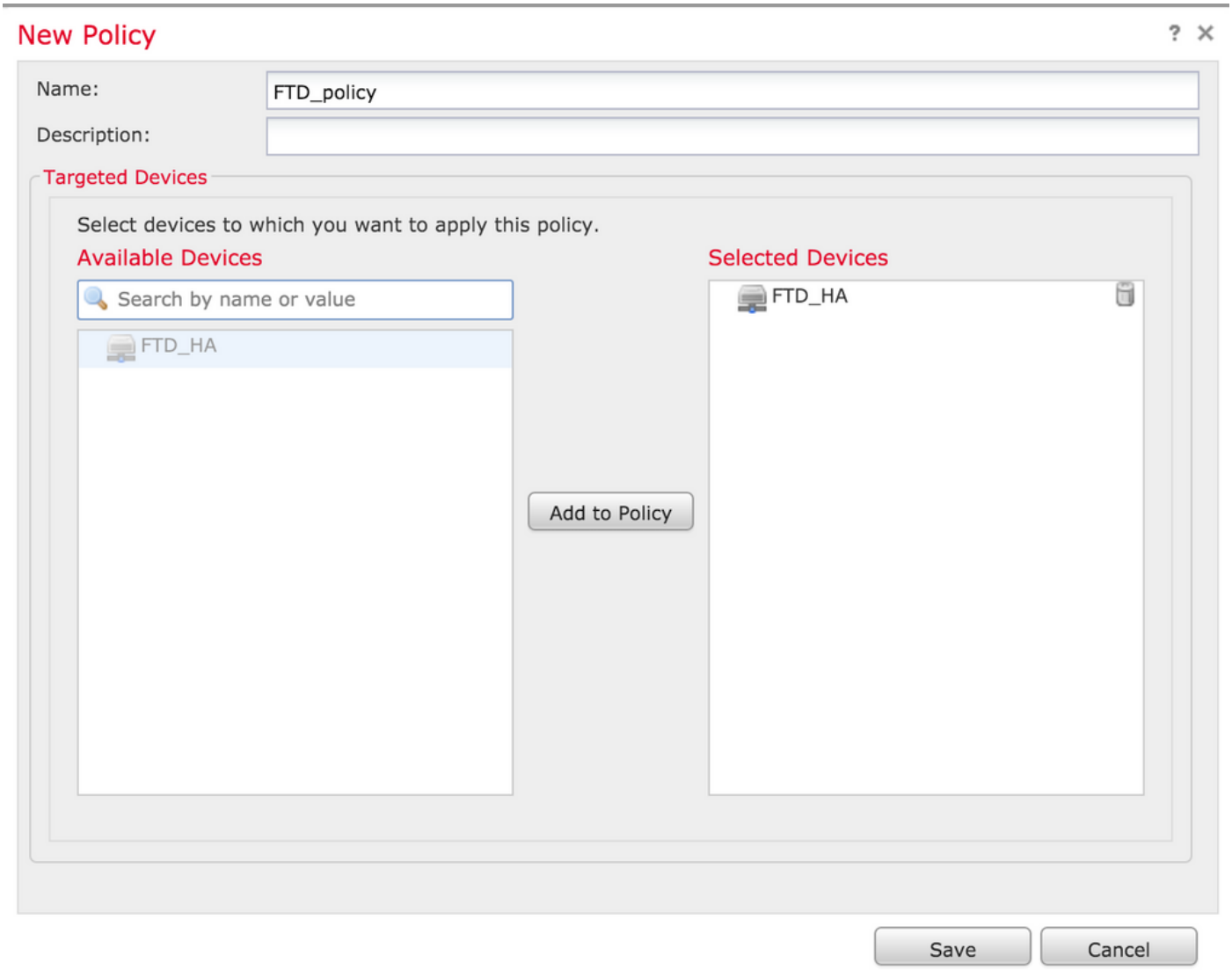
Настройка

Вся связанная конфигурация Управляющего доступ настроена, поскольку вы перешли к вкладке **Platform Settings** в **Устройствах**, как показано в образе:



Или отредактируйте политику, которая существует, поскольку вы щелкаете по значку карандаша или создаете новую политику FTD, поскольку вы нажимаете **Новую кнопку Policy** и выбираете тип как **Параметры настройки Защиты Угрозы**, как показано в образе:

Выберите устройство FTD, чтобы применить эту политику и нажать **Save**, как показано в образе:



Настройте управляющего доступ

Это эти четыре главных действия, взятые для настройки Управляющего доступ.

Шаг 1. Настройте IP на Интерфейсе FTD через GUI FMC.

Настройте IP на интерфейсе, по которому FTD доступен через SSH или HTTPS. Отредактируйте интерфейсы, которые существуют , поскольку вы перешли к вкладке **Interfaces** FTD.

> **Примечание:** На устройствах FTD, работающих под управлением ПО версии 6.0.1, стандартный интерфейс управления на FTD является интерфейсом diagnostic0/0. Однако на устройствах FTD, работающих под управлением ПО версии 6.1.0, всем доступе управления поддержкой интерфейсов кроме диагностического интерфейса.

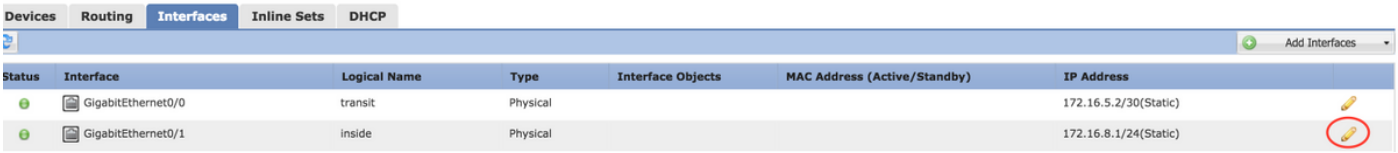
Существует шесть шагов для настройки диагностического интерфейса.

Шаг 1. Перейдите к **Устройству> Управление устройствами.**

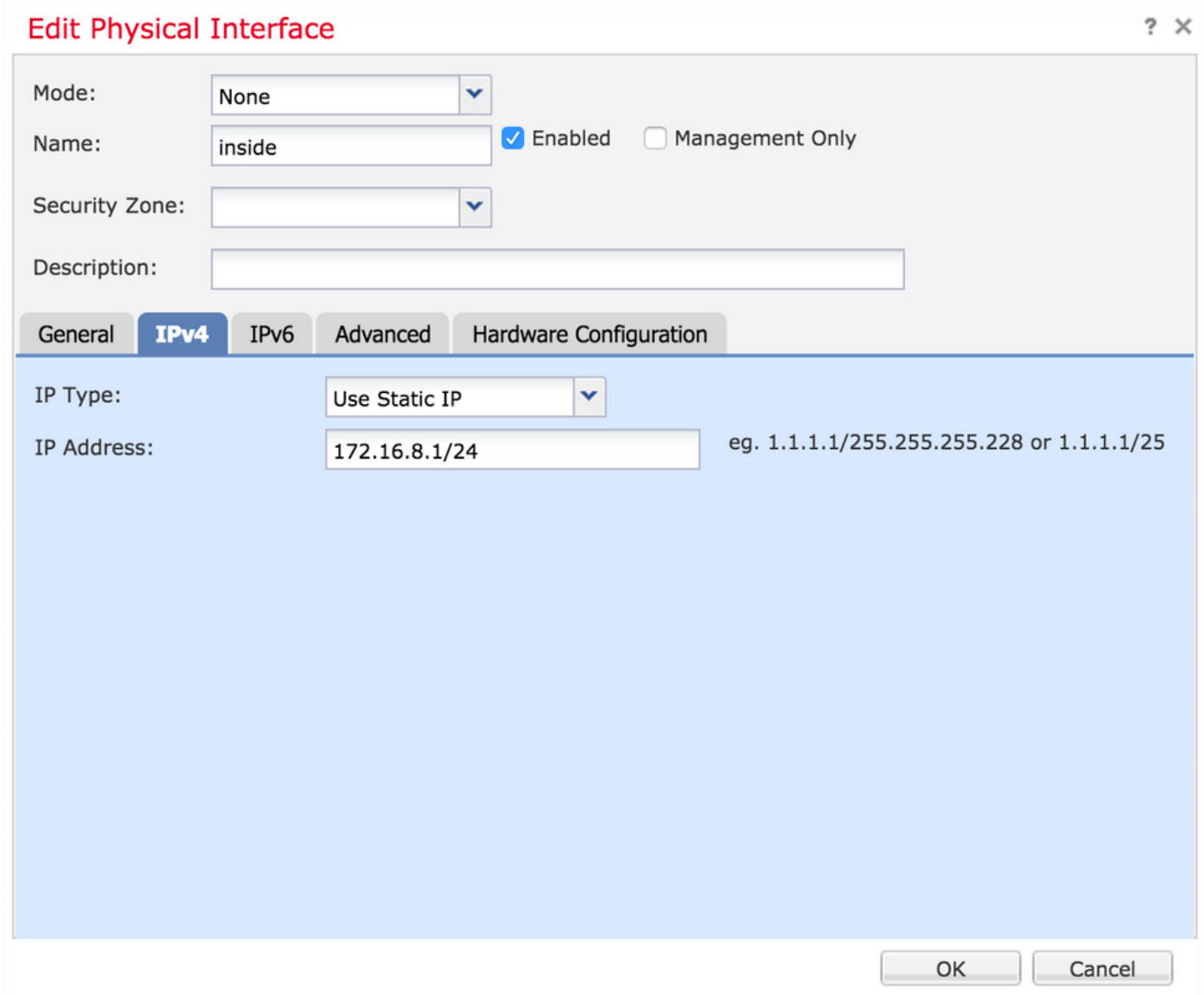
Шаг 2. Выберите Device или FTD HA Cluster.

Шаг 3. Перейдите к вкладке **Interfaces**.

Шаг 4. . Нажмите **значок карандаша** для настройки интерфейса для получения управляющего доступ, как показано в образе:



Шаг 5. . Выберите **флажок enable** для включения интерфейсов. Перейдите к **вкладке Ipv4**, выберите IP Type в качестве **помех или DHCP**. Теперь введите IP-адрес для Интерфейса и **нажмите OK**, как показано в образе:



Шаг 6. Нажмите **Save** и затем разверните политику на FTD.

Примечание: Диагностический интерфейс не может использоваться для доступа к

Установившемуся CLI по SSH на устройствах с версией программного обеспечения 6.1.0

Шаг 2. Настройте внешнюю проверку подлинности.

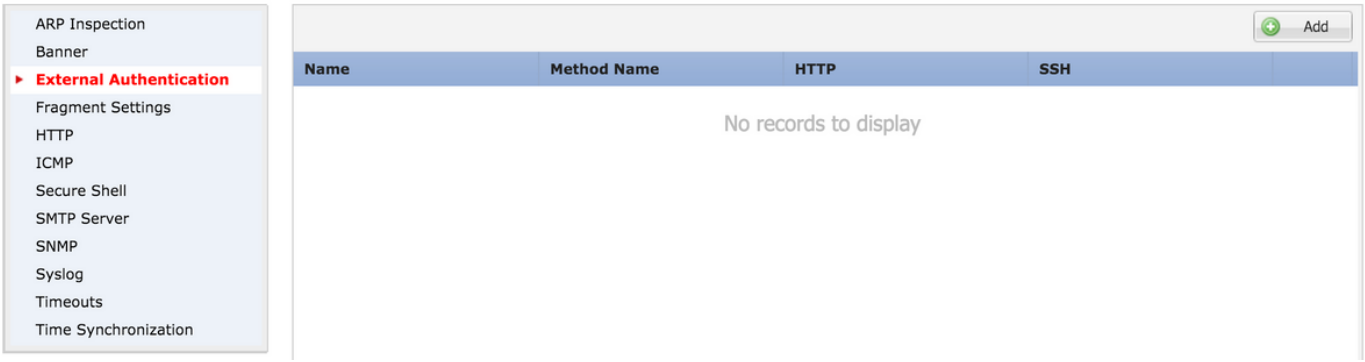
Внешняя проверка подлинности упрощает интеграцию FTD к Active Directory или серверу RADIUS для проверки подлинности пользователя. Это - обязательное действие, потому что у локально настроенных пользователей нет прямого доступа к диагностическому CLI. К диагностическому CLI и GUI обращаются только пользователи, которые аутентифицируются через Протокол LDAP или RADIUS.

Существует 6 шагов для настройки Внешней проверки подлинности.

Шаг 1. Перейдите к **Устройствам> Параметры настройки Платформы.**

Шаг 2. Или отредактируйте политику, которая существует, поскольку вы щелкаете по значку карандаша или создаете новую политику FTD, поскольку вы нажимаете **Новую кнопку Policy** и выбираете тип как **Параметры настройки Защиты Угрозы.**

Шаг 3. Перейдите к вкладке **External Authentication**, как показано в образе:



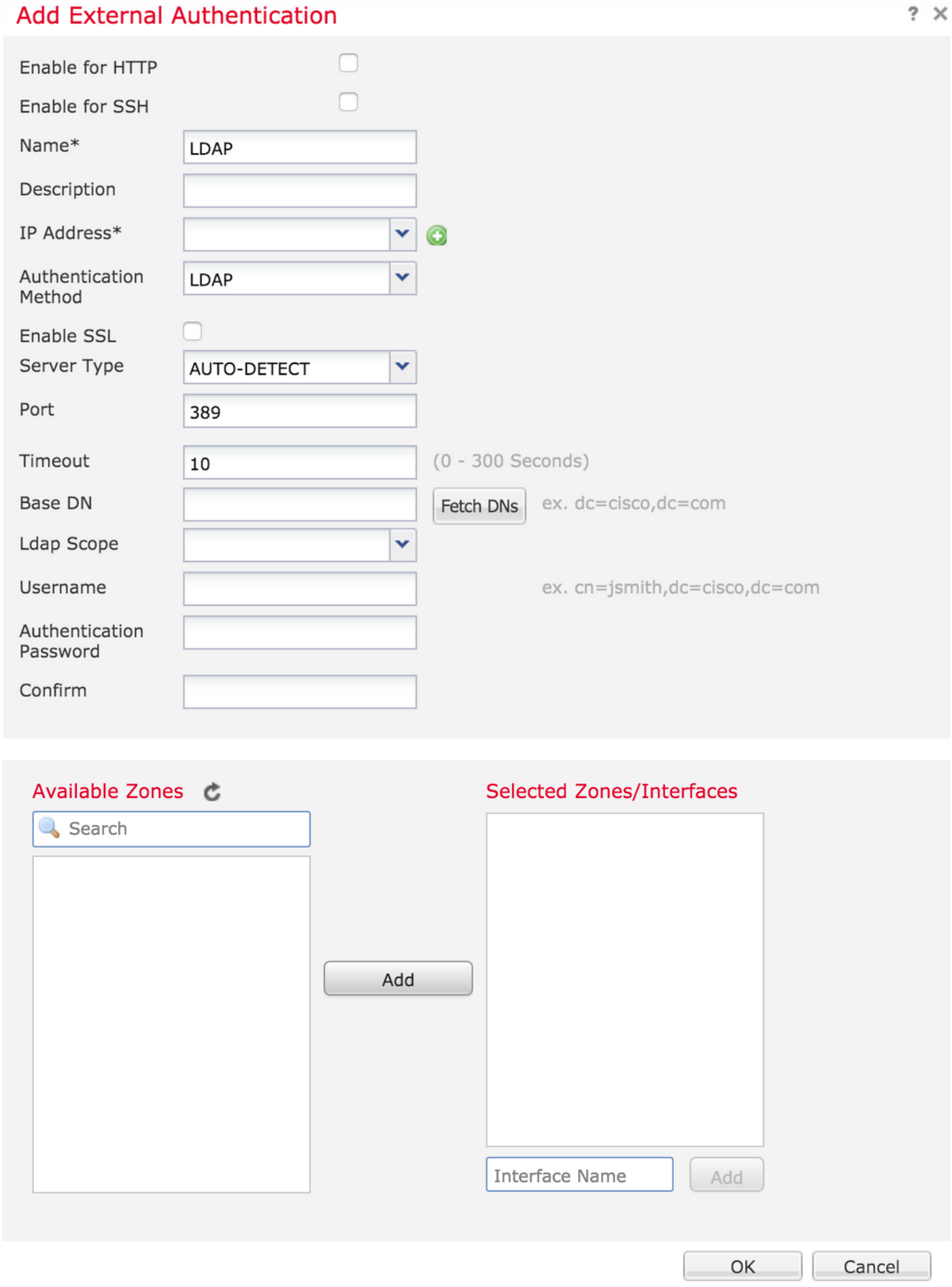
Шаг 4. . Поскольку вы щелкаете **по Add**, диалоговое окно появляется как показано в образе:

- **Включите для HTTP** - Позволяют этой опции предоставить , обращаются к FTD по HTTPS.
- **Включите для SSH** - Позволяют этой опции предоставить, обращаются к FTD по SSH.
- **Название** - Вводит имя для Соединения LDAP.
- **Описание-** Введите дополнительное описание для объекта External Authentication.
- **IP-адрес-** Введите сетевой объект, который хранит IP Внешнего сервера проверки подлинности. Если нет никакого сетевого объекта , настроен, создают новый путем щелчка **(+)** значок.

- **Выберите метод аутентификации** RADIUS или Протокол LDAP для аутентификации.
- **Включите SSL** - Позволяют этой опции зашифровать Трафик аутентификации.
- **Тип сервера** - Выбирает Тип сервера. Известными типами сервера является Active Directory MS, Sun, OpenLDAP и Novell. По умолчанию опция собирается автоматически обнаружить тип сервера.
- **Порт** - Введите порт, по которому имеет место аутентификация.
- **Таймаут** - Вводит значение таймаута для запросов аутентификации.
- **Основной DN** - Вводит основной DN для обеспечения области, в которой должен присутствовать пользователь.
- **Область LDAP** - Выбирает область LDAP для взгляда. Область в том же уровне или смотреть в поддереве.
- **Имя пользователя** - Вводит имя пользователя для привязки с каталогом LDAP.
- **пароль для проверки подлинности** - вводит пароль для этого пользователя.
- **Подтвердите** - Повторно вводят пароль.
- **Доступные Интерфейсы** - список доступных интерфейсов на FTD отображен.
- **Выбранные зоны и интерфейсы** - Это показывает список интерфейсов, по которым от сервера проверки подлинности обращаются.

Для Проверки подлинности RADIUS нет никакого DN Ядра типа сервера или Области LDAP. Портом является ПОРТ RADIUS 1645.

Тайна - Вводит секретный ключ для RADIUS.



Шаг 5. . Как только конфигурация реализована, нажмите **OK.**

Шаг 6. Сохраните политику и Разверните ее на устройстве Защиты Угрозы Огневой мощи.

Примечание: Внешняя проверка подлинности не может использоваться для доступа к Установившемуся CLI по SSH на устройствах с версией программного обеспечения 6.1.0

Шаг 3. Настройте доступ SSH.

SSH предоставляет прямой доступ к установившемуся CLI. Используйте эту опцию, чтобы непосредственно обратиться к CLI и выполнить команды отладки. В этом разделе описывается настроить SSH для доступа к CLI FTD.

Примечание: На устройствах FTD, работающих под управлением ПО версии 6.0.1, конфигурация SSH на Параметрах настройки Платформы предоставляет доступ к диагностическому CLI непосредственно а не CLISH. Необходимо соединиться с IP-адресом, настроенным на **br1** для доступа к CLISH. Однако на устройствах FTD, работающих под управлением ПО версии 6.1.0, все интерфейсы перешли к установившемуся CLI, когда обращено по SSH

Существует 6 шагов для настройки SSH на ASA

На 6.0.1 устройствах только:

Эти шаги выполнены на устройствах FTD с версией программного обеспечения меньше чем 6.1.0 и больше, чем 6.0.1. На 6.1.0 устройствах эти параметры наследованы от ОС.

Шаг 1. Перейдите к **Устройствам> Параметры настройки Платформы.**

Шаг 2. Или отредактируйте политику, которая существует, поскольку вы щелкаете по значку карандаша или создаете новую Политику в области обороны Угрозы Огневой мощи, поскольку вы нажимаете **Новую кнопку Policy** и выбираете тип как **Параметры настройки Защиты Угрозы.**

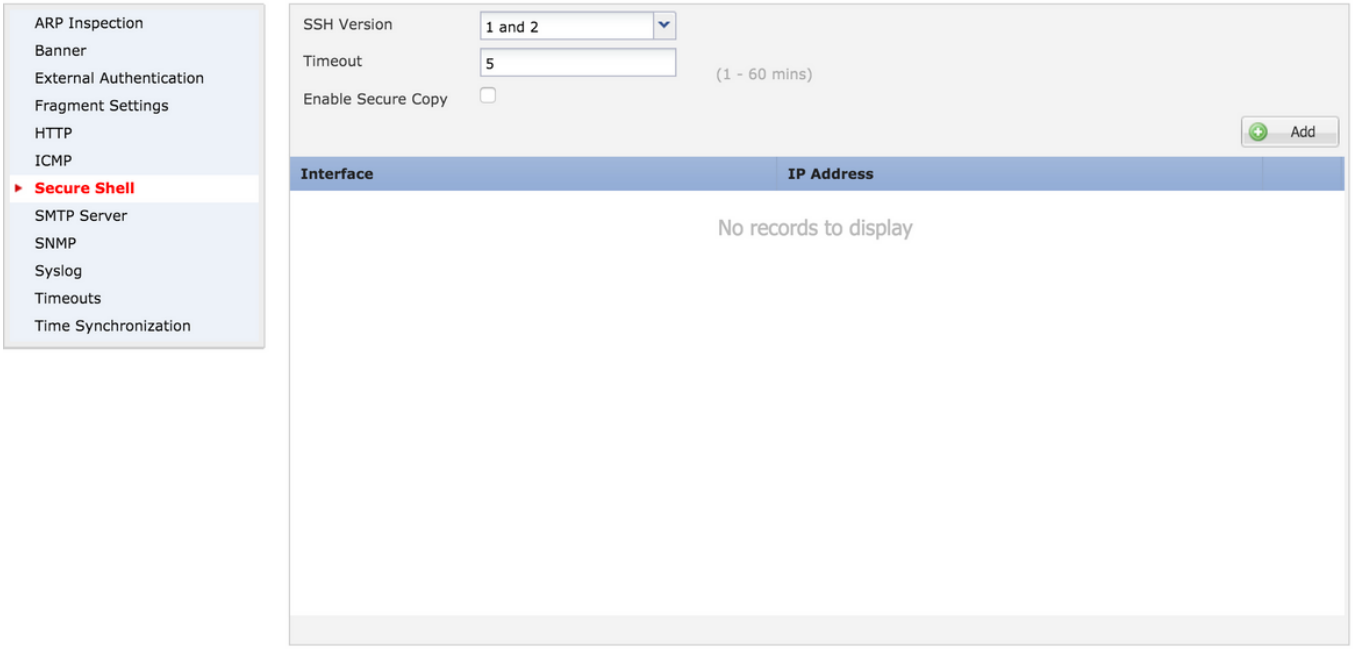
Шаг 3. Перейдите к Разделу **Secure Shell**. Страница появляется, как показано в образе:

Версия SSH: Выберите версию SSH для включения на ASA. Существует три опции:

- **1:** Включите только версию SSH 1
- **2:** Включите только версию SSH 2
- **1 и 2:** Включите обе версии SSH 1 и 2

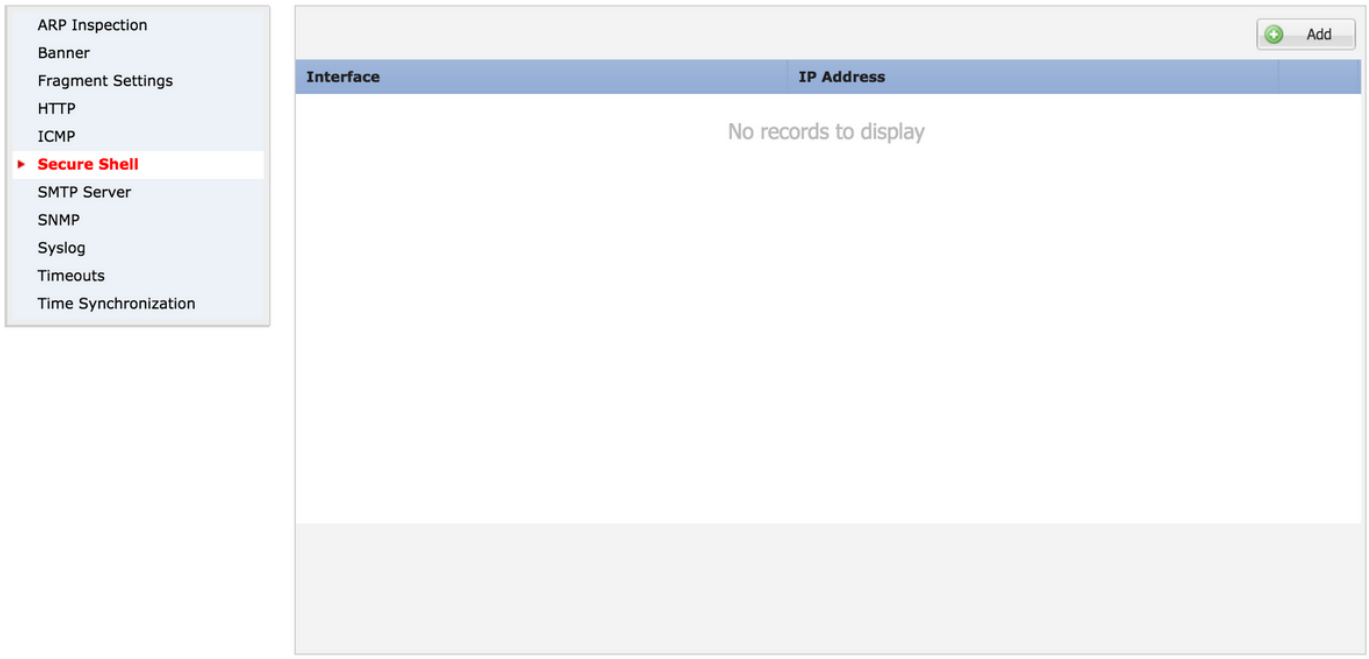
Таймаут: Введите желаемую задержку SSH в минутах.

Включите Безопасную Копию - Позволяют этой опции настроить устройство для разрешения соединений Протокола SCP и действия как сервер SCP.



На 6.0.1 и 6.1.0 устройствах:

Эти шаги настроены для ограничения управляющего доступ через SSH к определенным интерфейсам и к определенным IP-адресам.

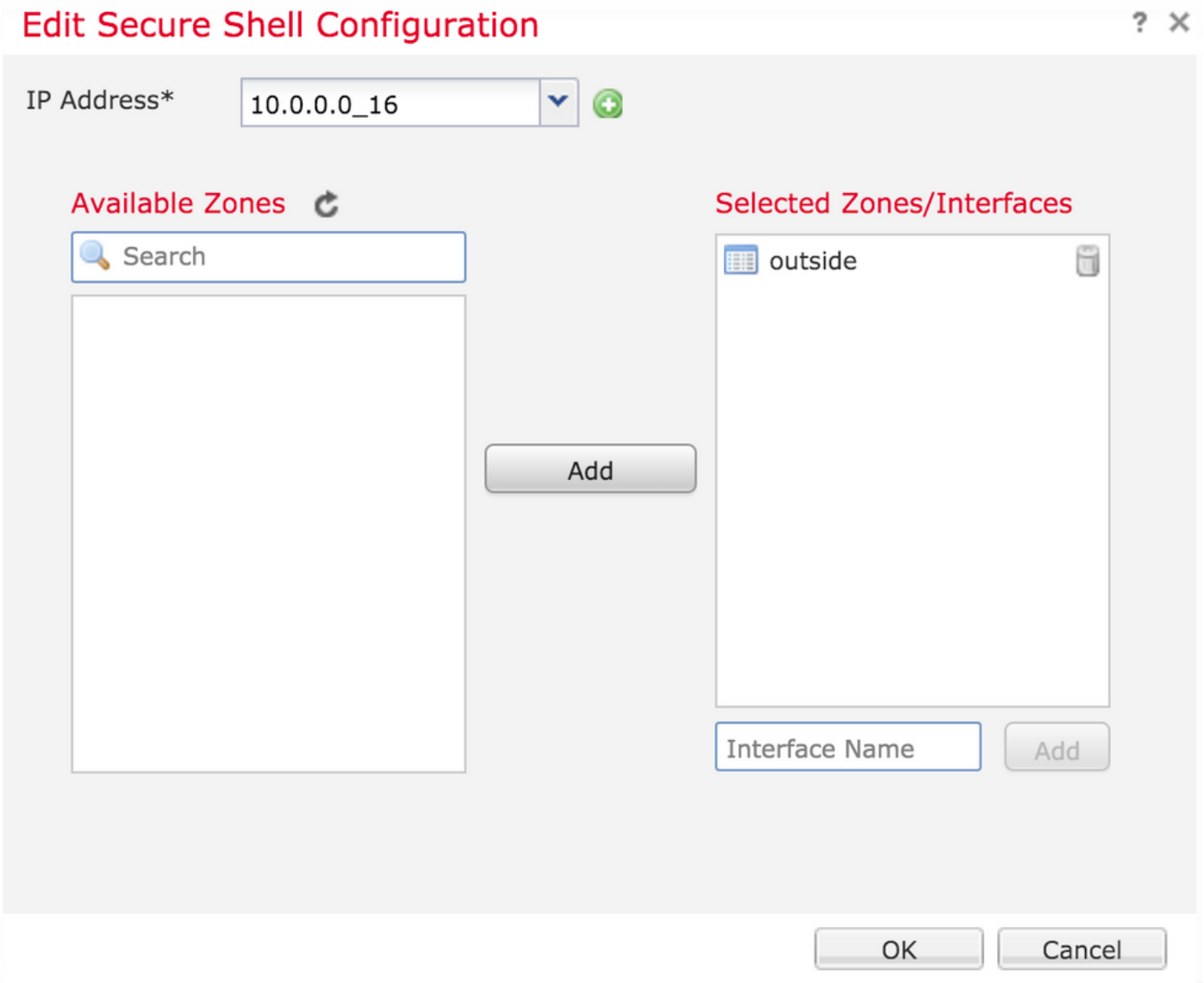


Шаг 1. **Нажмите Add** и настройте эти опции:

IP-адрес: Выберите сетевой объект, который содержит подсети, которым позволяют обратиться к CLI по SSH. Если сетевой объект не присутствует, создайте тот, поскольку вы щелкаете **(+)** значок.

Выбранные Зоны/интерфейсы: Выберите зоны или интерфейсы, по которым от сервера SSH обращаются.

Шаг 2. **Нажмите OK**, как показано в образе:



Конфигурация для SSH просматривается в установившемся CLI (CLI Диагностики ASA в 6.0.1 устройствах) использующий эту команду.

```
> show running-config ssh
ssh 172.16.8.0 255.255.255.0 inside
```

Шаг 3. Как только конфигурация SSH сделана, нажмите **Save** и затем разверните политику на FTD.

Шаг 4. . Настройте доступ HTTPS.

Для включения доступа HTTPS к одному или более интерфейсам перейдите к разделу **HTTP** в параметрах настройки платформы. Доступ HTTPS в частности полезен для загрузки захватов пакета от диагностического безопасного веб-интерфейса непосредственно для анализа.

Существует 6 шагов для настройки доступа HTTPS.

Шаг 1. Перейдите к **Устройствам> Параметры настройки Платформы**

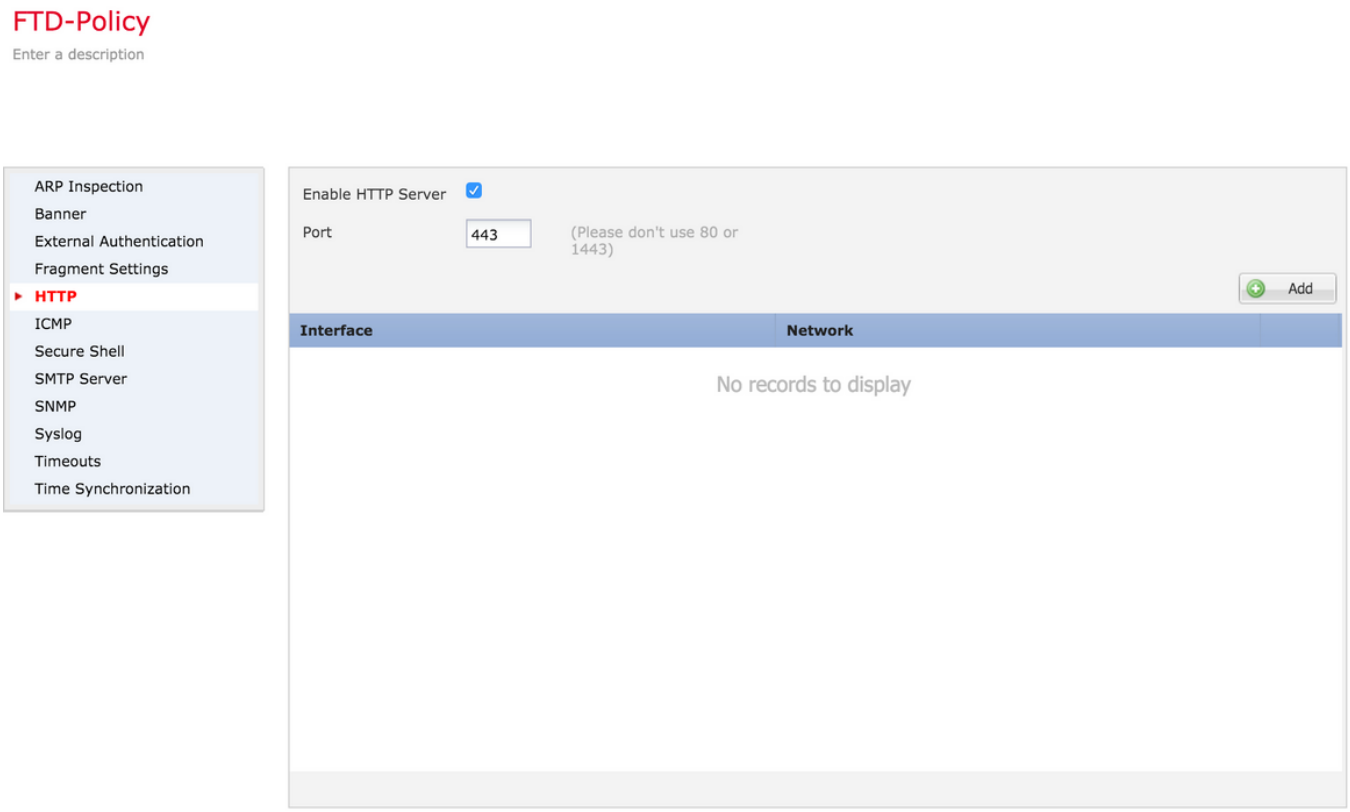
Шаг 2. Или отредактируйте политику параметров настройки платформы, которая

существует, поскольку вы нажимаете **значок карандаша** около политики или создаете новую политику FTD, как вы нажимаете **New Policy**. Выберите тип как **Защиту Угрозы Огневой мощи.**

Шаг 3. Поскольку вы перешли к разделу **HTTP**, страница появляется как показано в образе.

Включите сервер HTTP: Позвольте этой опции сделать для включения сервера HTTP на FTD.

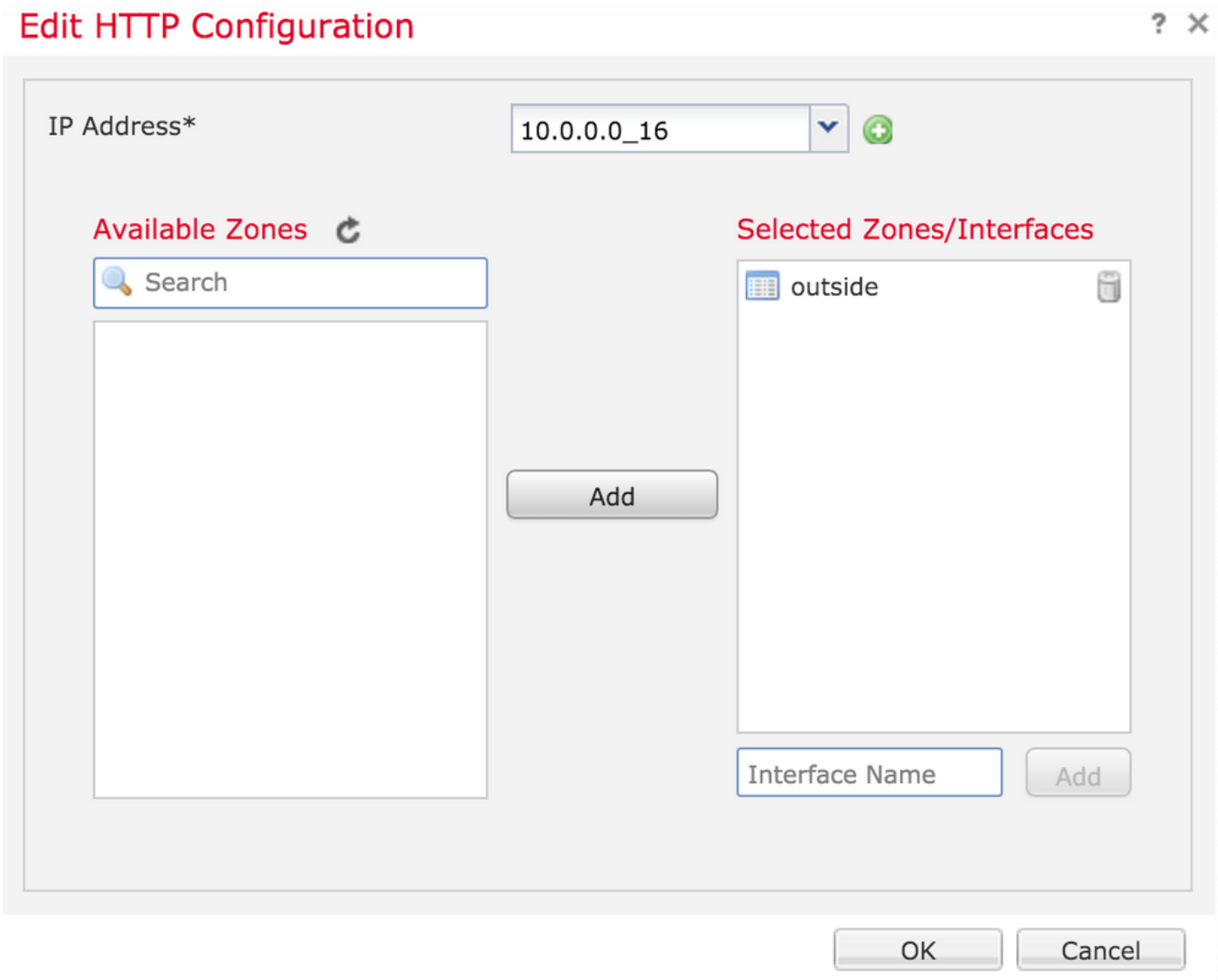
Порт: Выберите порт, на котором FTD принимает подключения управления.



Шаг 4. . **Нажмите Add** и apage появляется как показано в образе:

IP-адрес- Введите подсети, которым позволяют иметь доступ HTTPS к диагностическому интерфейсу. Если сетевой объект не присутствует, создают тот с помощью **(+)** опция.

Выбранный zones/Interfaces- Подобный SSH, конфигурации HTTPS нужно было настроить интерфейс, по которому это доступно через HTTPS. Выберите зоны или интерфейс, по которому к FTD нужно обратиться через HTTPS.



Конфигурация для HTTPS просматривается в установившемся CLI (CLI Диагностики ASA в 6.0.1 устройствах) использующий эту команду.

```
> show running-config http
http 172.16.8.0 255.255.255.0 inside
```

Шаг 5. . Как только необходимая конфигурация сделана, выбирают **OK.**

Шаг 6. Как только вся необходимая информация была введена, нажимают **Save** и затем развертывают политику на устройстве.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Это основные шаги для того, чтобы решить проблему управляющего доступ на FTD.

Шаг 1. Гарантируйте, что интерфейс включен и настроен с IP-адресом.

Шаг 2. Гарантируйте, что Внешняя проверка подлинности работает согласно конфигурации и ее достижимость от соответствующего интерфейса, заданного в разделе **Внешней проверки подлинности Параметров настройки Платформы**.

Шаг 3. Гарантируйте, что маршрутизация на FTD точна. В версии программного обеспечения 6.0.1 FTD перейдите к **диагностическому cli поддержки системы.** Выполните **show route** команд и **только для управления show route** для наблюдения маршрутов для FTD и интерфейсов управления соответственно.

В версии программного обеспечения 6.1.0 FTD, выполненной команды непосредственно в установившемся CLI.

Дополнительные сведения

- Краткое руководство по началу работы защиты угрозы огневой мощи Cisco для ASA
- Cisco Systems – техническая поддержка и документация