МЕЖСЕТЕВЫЕ ЭКРАНЫ CISCO ASA (FIREWALL)

Особенности внедрения, октябрь 2016

Межсетевые экраны нового поколения NGFW ASA 5500-X с сервисами FirePOWER

CCIE# 27142

Алексей Николаев
e-mail: al@learncisco.ru
Web: LearnCisco.Ru

Межсетевые экраны нового поколения NGFW Cisco ASA 5500-X:

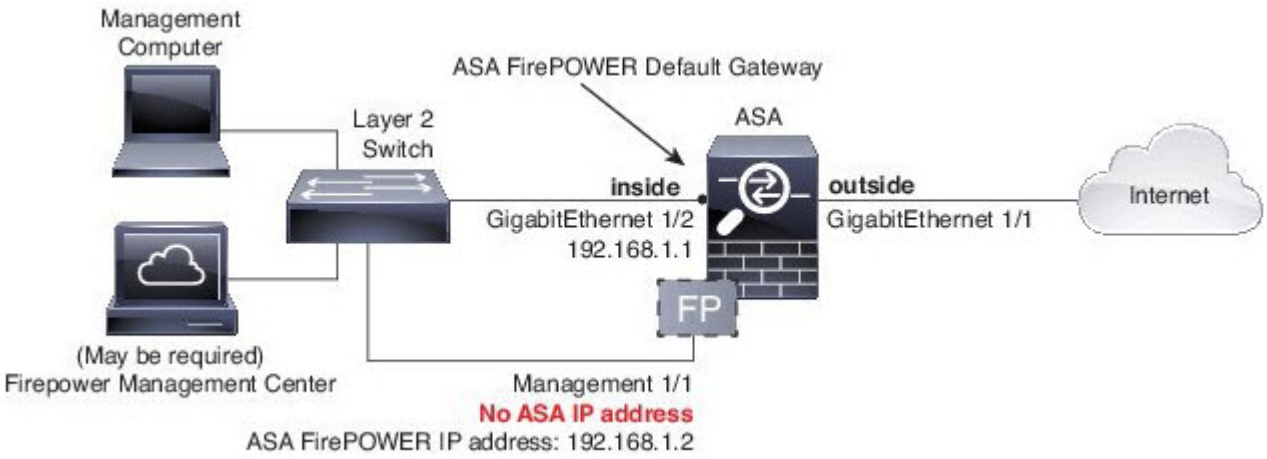
- **Две реализации ПО**
  - Классическая OS для **ASA** и отдельная OS для **модуля FirePOWER** (FirePOWER Services 6.1).
    - Для младших моделей возможно единое управление через ASDM (ASA и ключевые настройки FirePOWER)
    - Раздельные политики и объекты для ASA и модуля FirePOWER
  - Единый унифицированный образ **F**irePOWER **T**hreat **D**efense (**FTD**) для ASA и модуля FirePOWER
    - Для локального управления вместо ASDM используется **Firepower Device Manager**, не требующий Java
    - Единые политики и объекты (FirePOWER Threat Defense 6.1).
    - Для перехода на FTD требуется полный re-image устройства.

Межсетевые экраны нового поколения NGFW Cisco ASA 5500-X:

- **Системы управления для NGFW ASA 5500-X**
  - **Централизованная система управления**
    - **Firepower Management Center (FMC)**
    - Самый полный функционал, но требуется аппаратное устройство, либо виртуальный образ и покупка лицензии
  - **Cisco ASDM (встроенный)**
    - Для управления функциями ASA
    - Поддерживает основные функции FirePOWER
    - Java-зависимый
  - **Firepower Device Manager (встроенный в FTD)**
    - Для единого FTD образа
    - Java не используется

Межсетевые экраны нового поколения NGFW Cisco ASA 5500-X:

❑ Рекомендованная схема внедрения NGFW ASA 5500-X

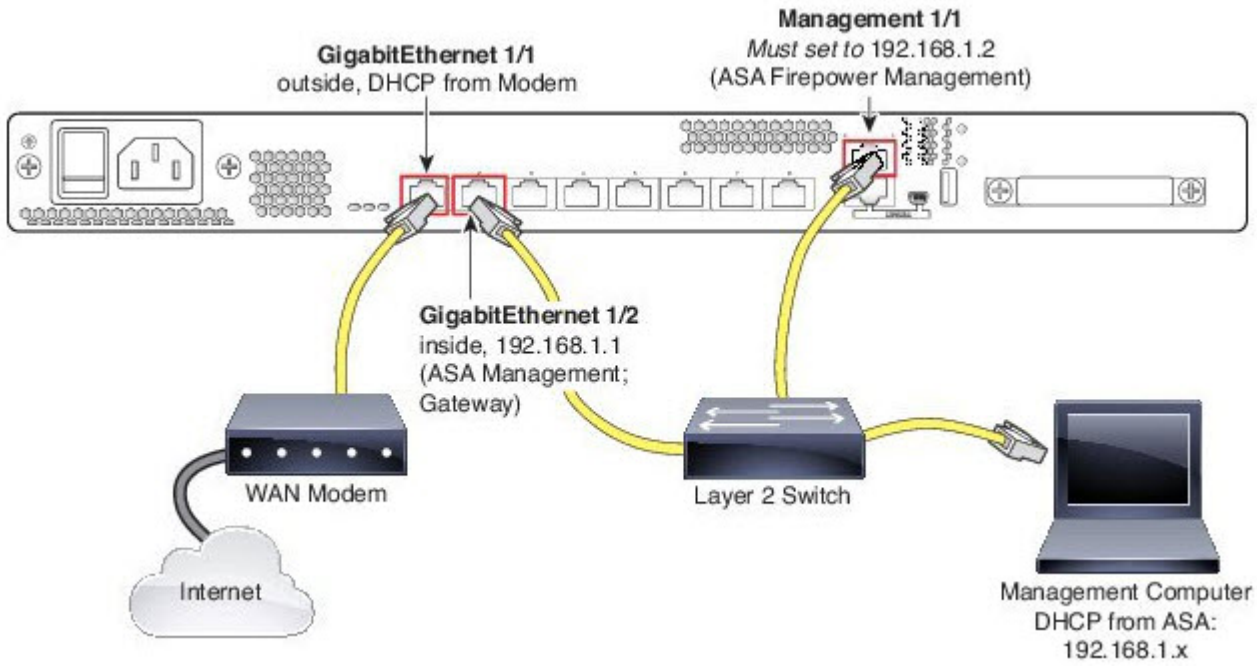


❑ Конфигурация ASA 5500-X «по умолчанию»

- Разрешен трафик **inside → outside**
- **IP адрес** на интерфейсе **outside** получается по **DHCP**
- Включен **DHCP сервер** для клиентов на интерфейсе **inside**
- Разрешен доступ через **ASDM** на интерфейсе **inside**
- Интерфейс **Management 1/1** только для встроенного **FirePOWER модуля** (не надо ничего конфигурировать на нем через ASA! Все только через FirePOWER)

Межсетевые экраны нового поколения NGFW Cisco ASA 5500-X:

- **Рекомендованная схема внедрения NGFW ASA 5500-X**



Межсетевые экраны нового поколения NGFW Cisco ASA 5500-X:

❑ Рекомендации по внедрения NGFW ASA 5500-X

- Для полноценной работы ASDM в Windows 10 необходима версия FirePOWER **6.1** и старше
- В FTD пока поддерживается только один тип VPN - Site-to-Site с pre-shared keys, без сертификатов.
- Если требуется полный функционал ASA, включая SSL/Web VPN, то лучше пока не мигрировать на FTD
- Если же более интересен функционал FirePOWER и достаточно Site-to-Site VPN, то имеет смысл перейти на единый образ FTD

Межсетевые экраны нового поколения NGFW Cisco ASA 5500-X:

- **Запуск и настройка NGFW ASA 5500-X с сервисами FirePOWER будут подробно рассмотрены во втором томе видео курса:**

  «Настройка межсетевых экранов Cisco ASA и PIX», Том II

- **Обзор межсетевых экранов нового поколения NGFW ASA 5500-X с сервисами FirePOWER и начало работы с ними уже включены в первый том видео курса:**

  «Настройка межсетевых экранов Cisco ASA и PIX», Том I

- **Полезные ссылки** (на примере ASA 5506-X / 5508-X / 5516-X)

  http://www.cisco.com/go/asa5506x-welcome
  http://www.cisco.com/go/asa5506x-install
  http://www.cisco.com/go/asa5506x-quick

  http://www.cisco.com/go/asa5508x-welcome
  http://www.cisco.com/go/asa5508x-install
  http://www.cisco.com/go/asa5508x-quick