1. Настройка КМЭ в Центральном офисе
   1. Базовая конфигурация
2. Задать имя устройству:

|  |
| --- |
| *hostname cntr-fw* |

1. Выполнить следующие настройки на интерфейсе GigabitEthernet1/1:

|  |
| --- |
| *interface GigabitEthernet1/1*  *nameif INSIDE*  *security-level 100*  *ip address 192.168.10.1 255.255.255.0*  *description Inside Interface* |

1. Выполнить следующие настройки интерфейса GigabitEthernet1/2:

|  |
| --- |
| *interface GigabitEthernet1/2*  *shutdown* |

1. Выполнить следующие настройки интерфейса GigabitEthernet1/3:

|  |
| --- |
| *interface GigabitEthernet1/3*  *nameif ISP1*  *security-level 0*  *ip address 2.2.2.2 255.255.255.128*  *description ISP1 Interface* |

1. Выполнить следующие настройки интерфейса GigabitEthernet1/4:

|  |
| --- |
| *interface GigabitEthernet1/4*  *nameif ISP2*  *security-level 0*  *ip address 3.3.3.3 255.255.255.240*  *description ISP2 Interface* |

1. Выполнить следующие настройки:

|  |
| --- |
| *http server enable*  *http 192.168.0.0 255.255.0.0 INSIDE*  *ssh 192.168.0.0 255.255.0.0 INSIDE*  *ssh timeout 15*  *same-security-traffic permit inter-interface*  *same-security-traffic permit intra-interface* |

1. Для работы сервисов AAA на МЭ Cisco ASA необходимо выполнить следующие команды:

|  |
| --- |
| *username admin password <пароль локального пользователя> privilege 15*  *enable password <enable-пароль>*  *aaa authentication ssh console LOCAL*  *aaa authentication http console LOCAL*  *aaa authentication serial console LOCAL*  *aaa authentication enable console LOCAL*  *crypto key generate rsa modulus 1024* |

1. Обновить прошивку ASA и ASDM.

|  |
| --- |
| *show memory detail | include Max memory footprint*  *conf t*  *jumbo-frame reservation*  *wr*  *no jumbo-frame reservation*  *wr*  *copy tftp://192.168.7.55/asa961-lfbff-k8.SPA disk0:/asa961-lfbff-k8.SPA*  *copy tftp://192.168.7.55/asdm-761.bin disk0:/asdm-761.bin*  *boot system disk0:/asa961-lfbff-k8.SPA*  *boot system disk0:/asa952-lfbff-k8.SPA*  *asdm image disk0:/asdm-761.bin*  *wr*  *reload*  *sh run*  *sh running-config boot system*  *no boot system disk0:/asa952-lfbff-k8.SPA*  *sh running-config boot system*  *sh asdm image*  *delete disk0:/asa952-lfbff-k8.SPA*  *delete disk0:/asdm-752.bin*  *sh flash*  *wr*  *reload* |

1. Изменить количество отображаемых строк на 48 (по умолчанию 24):

|  |
| --- |
| *pager lines 48* |

1. Включить отображение ASA в прыжках traceroute:

|  |
| --- |
| *policy-map global\_policy*  *class class-default*  *set connection decrement-ttl* |

1. Настроить временные параметры:

|  |
| --- |
| *clock timezone EEST 2 0*  *clock summer-time EEDT recurring last Sun Mar 3:00 last Sun Oct 4:00 60* |

1. Настроить синхронизацию с NTP-серверами Internet:

|  |
| --- |
| *ntp server 88.147.254.232 source ISP1 prefer*  *ntp server 91.226.136.155 source ISP2* |

* 1. Настройка маршрутов и NAT

1. Настроить маршруты в Интернет для основного и резервного канала:

|  |
| --- |
| *route ISP1 0.0.0.0 0.0.0.0 2.2.2.1 10*  *route ISP2 0.0.0.0 0.0.0.0 3.3.3.1 1* |

1. Настроить проверку ISP1 через сайт 2ip.ru:

|  |
| --- |
| *route ISP1 178.63.151.224 255.255.255.255 2.2.2.1* |

1. Настроить проверку ISP2 через сайт ip.mail.ru:

|  |
| --- |
| *route ISP2 185.5.136.119 255.255.255.255 3.3.3.1* |

1. Настроить NAT для 2-х ISP:

|  |
| --- |
| *object network ISP1\_NAT*  *nat (any,ISP1) dynamic interface dns*  *object network ISP2\_NAT*  *nat (any,ISP2) dynamic interface dns* |

* 1. Конфигурация FirePower модуля

1. Проверить: установлены ли модули IPS, CXSC, или SFR:

|  |
| --- |
| *sh module all* |

Для корректной установки, данные модули необходимо удалить.

Если установлен модуль IPS, то удалить его при помощи команд:

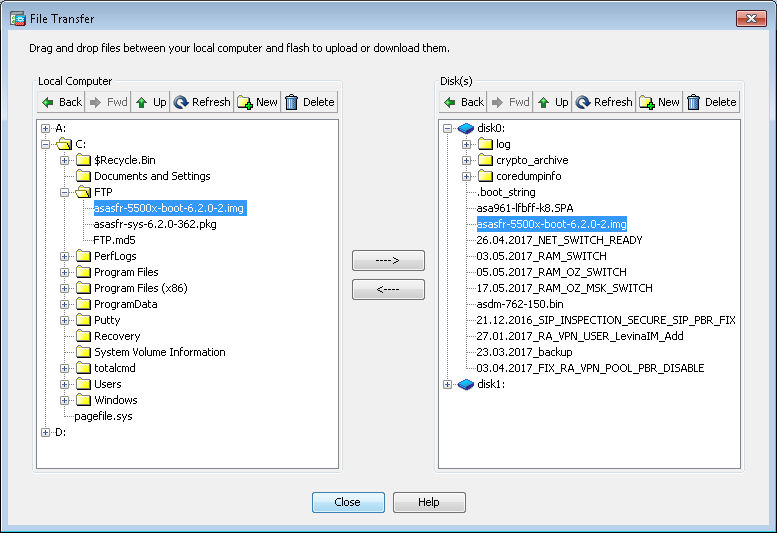
|  |
| --- |
| *sw-module module ips shutdown*  *sw-module module ips uninstall*  *reload* |

Если установлен модуль CXSC, то удалить его при помощи команд:

|  |
| --- |
| *sw-module module cxsc shutdown*  *sw-module module cxsc uninstall*  *reload* |

Если установлен модуль SFR, то удалить его при помощи команд:

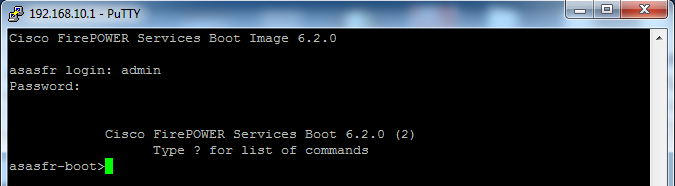
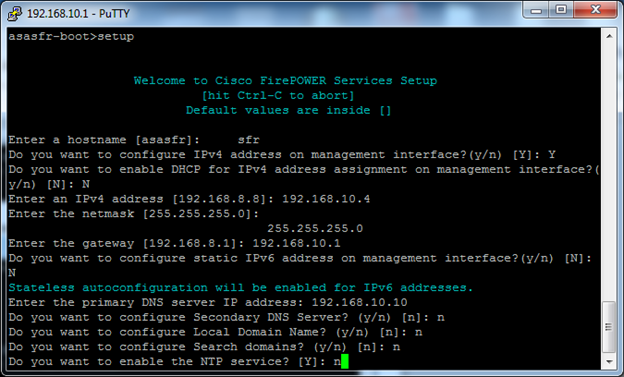
|  |
| --- |
| *sw-module module sfr uninstall* |

1. Скопировать на устройство загрузочный образ **asasfr-5500x-boot-6.2.0-2.img** через ASDM:  
     
   
2. Подключиться к ASA по ssh.
3. Ввести команду для указания расположения образа:

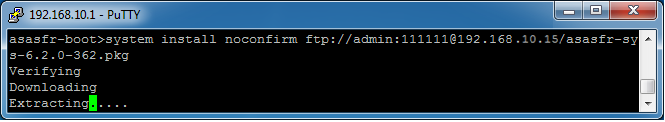
|  |
| --- |
| *sw-module module sfr recover configure image disk0:/asasfr-5500x-boot-6.2.0-2.img* |

1. Ввести команду для загрузки образа:

|  |
| --- |
| *sw-module module sfr recover boot* |

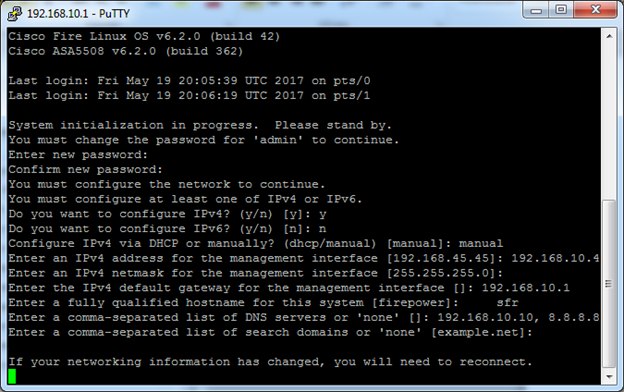
1. Процесс установки займёт примерно 7 минут. Проверять, закончилась ли установка или нет, можно с помощью команды ***session sfr console***. Если выдаётся сообщение с ошибкой – ждём. Если провалились в командную строку boot image, загрузка завершена успешно.  
   Первый вход в sfr console осуществляется не быстро, система может зависнуть минуты на 3.
2. В качестве логина вводим ***admin***, а в качестве пароля ***Admin123***  
   ******
3. Ввести команду ***setup*** и внести настройки:  
     
   ******
4. Ввести команду для загрузки образа:

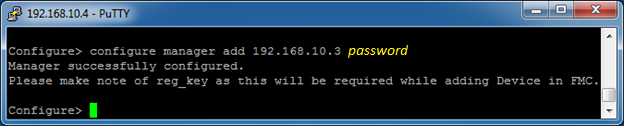
|  |
| --- |
| *system install noconfirm ftp://admin:111111@192.168.10.15/asasfr-sys-6.2.0-362.pkg* |

Закачка и установка образа займут примерно 15 минут.  
  


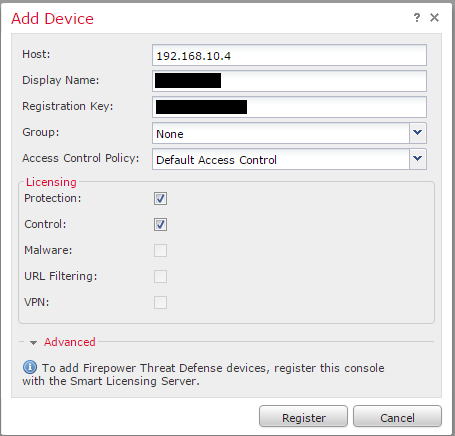
1. В конце установки система попросит нажать **«Enter»** для перезагрузки sfr-модуля.  
   Cisco ASA при этом не перезагружается.
2. После перезагрузки sfr-модуля, зайти в консоль sfr через команду ***session sfr console.***

Внимание! Первый вход осуществляется долго, консоль подвисает примерно на  
**35 минут** на сообщении *«Connected to module sfr. Escape character sequence is 'CTRL-^X'»***.** Не перезагружайте Cisco ASA, просто подождите пока не появится приглашение для входа.

В качестве логина ввести ***admin***, а в качестве пароля ***Admin123****.* Затем ввести настройки:  
  


1. Подключить sfr-модуль к к серверу Firepower Management Center (FMC).  
     
   Задаем параметры подключения на sfr-модуле:  
     
   

Задаем параметры подключения на сервере FMC:



* 1. Настройка дополнительных функций
     1. Настройка инспекции SIP

Инспекция SIP по умолчанию включена на Cisco ASA и проброс SIP работает даже без создания правил проброса в NAT, но она бесконтрольно пропускает SIP-трафик в обе стороны на любые адреса в Интернете.

Настроим инспекцию SIP с привязкой через access-list для работы с конкретным VOIP-шлюзом провайдера, остальной SIP-трафик из Интернет будет блокироваться:

|  |
| --- |
| *object network prov-sip-gw*  *host 5.5.5.5*  *description Provider VOIP-gateway*  *access-list sip\_inspection extended permit ip object-group SIP-GW prov-sip-gw*  *class-map inspection\_sip*  *match default-inspection-traffic*  *match access-list sip\_inspection*  *policy-map global\_policy*  *no class inspection\_default*  *no class sfr*  *class inspection\_sip*  *inspect sip*  *class inspection\_default*  *inspect dns preset\_dns\_map*  *inspect esmtp*  *inspect ftp*  *inspect h323 h225*  *inspect h323 ras*  *inspect ip-options*  *inspect netbios*  *inspect rsh*  *inspect rtsp*  *inspect skinny*  *inspect sqlnet*  *inspect sunrpc*  *inspect tftp*  *inspect xdmcp*  *class sfr*  *sfr fail-open*  *policy-map type inspect sip SIP\_MAP*  *parameters*  *max-forwards-validation action drop log*  *state-checking action drop-connection log*  *software-version action mask log*  *strict-header-validation action drop log*  *no traffic-non-sip*  *uri-non-sip action mask log*  *rtp-conformance enforce-payloadtype* |

Полезные команды для работы с SIP:

***show sip***  *-* показывает состояние регистрации sip-устройств

***show service-policy | i sip*** – показывает статистику по трафику, прошедшего через инспекцию SIP.

* + 1. Настройка уведомлений по событиям на сервер Syslog

Настроить уведомления на сервер syslog при возникновении определенных событий:

|  |
| --- |
| *logging list syslog message 113012*  *logging list syslog message 622001*  *logging host INSIDE 192.168.10.20*  *logging trap syslog*  *logging facility 16*  *logging device-id string CNTR-FW* |

Описание кодов событий:

***622001*** – события автоматического добавления и удаления маршрутов с SLA

***113012*** – события RA VPN подключений, и подключений к Cisco ASA по ssh