



**Инструкция по развертыванию
программного комплекса
«Инспектор сетевого фильтра NFI»**

Москва

2021

АННОТАЦИЯ

Данный документ содержит самую актуальную информацию, касающуюся установки продукта «Инспектор сетевого фильтра NFI». Рекомендуется внимательно изучить его, прежде чем приступать к развертыванию программного продукта.

Оглавление

Общие сведения	4
Список используемых сокращений	4
Требование к виртуальной среде	5
Требования к аппаратному обеспечению	5
Проверка совместимости	6
Подготовка к развертыванию программного комплекса	6
Развертывание и конфигурация программного комплекса	6
Схема организации сети с использованием устройства NFI.....	8

Общие сведения

Программный комплекс «Инспектор сетевого фильтра NFI» предназначен для использования в локальных информационных сетях в целях обеспечения контроля и защиты любого сетевого оборудования, используемого в рамках целевой локальной сети, включая межсетевые экраны нового поколения (NGFW).

Программный комплекс «Инспектор сетевого фильтра NFI» поставляется в виде виртуального образа для виртуальной машины VMware ESXI.

Список используемых сокращений

LAN (Local Area Network) – локальная вычислительная сеть. Компьютерная сеть, соединяющая компьютеры на небольшой территории, такой как частные дома, офисные здания и комплексы, учебные заведения, предприятия, офисы. Наиболее часто для построения локальных сетей используются такие технологии, как Ethernet и Wi-Fi.

OVA (Open Virtual Appliance) – пакет, который представляет собой файл архива TAR с внутренним каталогом OVF.

OVF (Open Virtualization Format) – открытый стандарт для хранения и распространения виртуальных машин. Стандарт описывает открытый, переносимый, расширяемый формат для распространения образов виртуальных машин. Стандарт OVF не привязан к какой-либо реализации гипервизора или аппаратной архитектуре.

NGFW (Next-Generation Firewall) – Межсетевые экраны нового поколения – представляют собой интегрированные платформы сетевой безопасности, в которых традиционные брандмауэры сочетаются с другими сетевыми решениями для фильтрации трафика, такими как системы глубокого анализа трафика Deep Packet Inspection (DPI), система предотвращения вторжений (IPS) и др.

VMware ESXI – программный продукт для виртуализации уровня предприятия. Является встроенным гипервизором, не требует наличия на машине установленной операционной системы. Гипервизор ESXi позволяет разделить ресурсы физического компьютера на логические разделы,

называемые виртуальными машинами. Включает в себя средства управления виртуальными машинами и ресурсами. Предъявляет определённый набор требований к аппаратному обеспечению.

WAN (Wide Area Network, WAN) – компьютерная сеть, охватывающая большие территории и включающая большое число узлов, возможно находящиеся в различных городах и странах. В рамках настоящего документа подразумевает любые внешние интернет-сети и соединения.

Требование к виртуальной среде

Минимальные требования: специализированный аппаратный гипервизор VMware ESXI версия 6.0.

Рекомендованные требования: специализированный аппаратный гипервизор VMware ESXI версия 7.0.

Требования к аппаратному обеспечению

Необходимые требования к аппаратному обеспечению:

- Поддержка виртуализации со стороны материнской платы и процессора;
- Поддержка многоядерных 64-х разрядных процессоров x86. Для поддержки 64-битных виртуальных машин на базах процессоров x64 – возможность включения поддержки аппаратной виртуализации (Intel VT-x или AMD RVI);
- **CPU:** 2 ядра (минимально);
- **Оперативная память (RAM):** 4 GB (минимально), 8 GB (рекомендовано);
- **BIOS:** поддержка NX/XD для CPU;
- **Сетевые контроллеры (минимально):** один Gigabit-контроллер или один Ethernet-контроллер;
- Наличие жесткого диска для развертывания программного комплекса «Система защиты сетевого оборудования NFI».

Проверка совместимости

Таблица проверки совместимости специализированного аппаратного гипервизора VMware ESXi версий 6.0+ с аппаратными комплексами доступна по адресу: <https://www.vmware.com/resources/compatibility/search.php>.

Подготовка к развертыванию программного комплекса

Программный комплекс «Инспектор сетевого фильтра NFI» поставляется в виде образов для виртуальной машины VMware ESXi. Для работы с образами программного комплекса необходимо:

1. Получить доступ к облачному репозиторию-хранилищу файлов ООО «АВ Софт»;
2. Авторизоваться в облачном хранилище с помощью логина и пароля;
3. Выгрузить локально файлы в формате .ovf и .vmdk, содержащие виртуальные образы программного комплекса;
4. Развернуть на целевом оборудовании необходимое программное окружение (см. раздел «Требования к виртуальной среде»).

Развертывание и конфигурация программного комплекса

Для развертывания программного комплекса «Инспектор сетевого фильтра NFI» необходимо выполнить следующие действия:

1. Запустить VMware ESXi.
2. Добавить образ виртуальной машины.

Для этого необходимо выполнить следующие действия:

- выбрать раздел «Virtual Machines»;
- в указанном разделе выбрать и нажать пункт «Create / Register VM»;
- выбрать опцию «Deploy a virtual machine from an OVF or OVA file»;
- ввести имя виртуальной машины и добавить загруженные из репозитория файлы в формате .ovf и .vmdk;
- выбрать носитель информации;

- в разделе «Deployment options» необходимо назначить «port group». «Port group» назначается для каждого интерфейса.

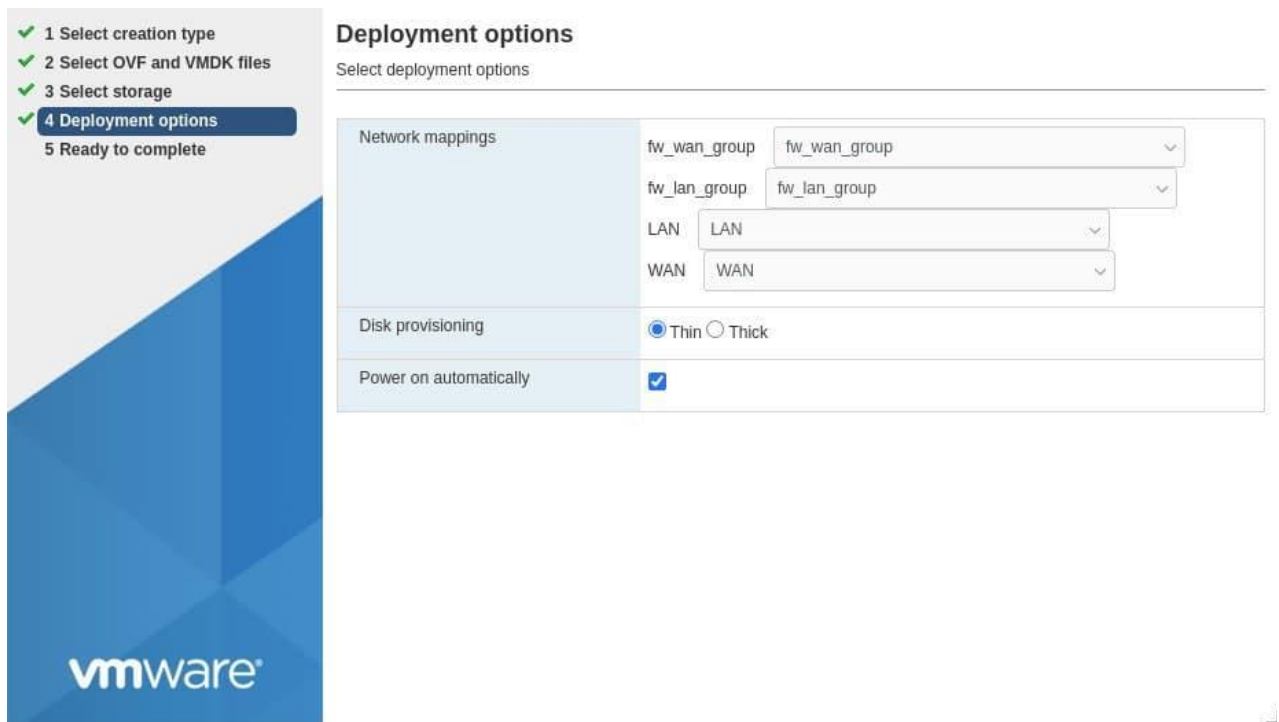


Рисунок 1 Настройки раздела «Deployment options»

Пояснения по настройкам раздела «Deployment options»:

LAN – соединение частной сети с программным комплексом NFI;

fw_lan_group – соединение программного комплекса NFI со входом в NGFW;

fw_wan_group – соединение выхода из NGFW с программным комплексом NFI;

WAN – соединение программного комплекса NFI с глобальной сетью Интернет.

Схема организации сети с использованием устройства NFI

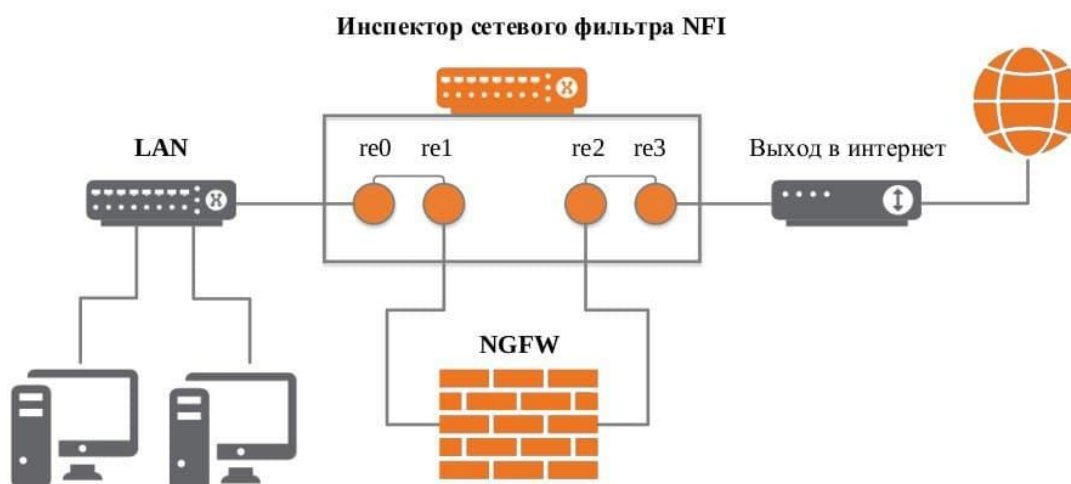


Рисунок 2 Схема организации сети с использованием NFI

Пояснения по схеме организации сети:

LAN соединяется с программным комплексом NFI посредством интерфейса re0.

Интерфейс re1 программного комплекса NFI соединяется посредством fw_lan_group со входом в NGFW.

Интерфейс re2 программного комплекса NFI соединяется посредством fw_wan_group с выходом из NGFW.

WAN соединяется с программным комплексом NFI посредством интерфейса re3 NFI.

Указанная выше схема организации сетевого взаимодействия позволяет:

1. Транслировать сетевой трафик на программный комплекс NFI.
2. Выявлять и блокировать несанкционированный (деструктивный) трафик.
3. Выявлять и блокировать доступ во всемирную глобальную сеть от скомпрометированных сетевых устройств.
4. Транслировать во всемирную глобальную сеть только «очищенный» трафик или трафик, отвечающий определенным параметрам.