Инспектор сетевого фильтра NFI

Описание процессов, обеспечивающих поддержание жизненного цикла v 1.2

Москва

2021г.

Контактная информация

127106, г. Москва, ул. Гостиничная, д.5

Тел.: +7 (495) 988-92-25

E-mail: office@avsw.ru

www.avsw.ru/about/contacts

Авторское право

Версия документа

Апрель 19, 2021

Оглавление

1. Термины и определения

В настоящем документе используются термины и определения, представленные в Таблица 1.

Таблица 1 Термины и определения

№	Термин	Определение
1.	LAN	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
2.	OVA	Пакет, который представляет собой файл архива TAR с внутренним каталогом OVF
3.	OVF	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
4.	NGFW	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, система предотвращения вторжений и др.

№	Термин	Определение
5.	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
6.	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
7.	USB flash drive	Запоминающее устройство, использующее в качестве носителя флэш-память, и подключаемое к компьютеру или иному считывающему устройству по интерфейсу USB

2. Сокращения

В настоящем документе используется перечень сокращений, представленный в Таблица 2.

Таблица 2 Перечень сокращений

№	Сокращение	Значение
1.	LAN	Local Area Network
2.	OVA	Open Virtual Appliance
3.	OVF	Open Virtualization Format
4.	NGFW	Next-Generation Firewall, NGFW
5.	NFI	Network Filter Inspector
6.	WAN	Wide Area Network
7.	ПК	Программный комплекс
8.	USB	Universal Serial Bus
9.	ПО	Программное обеспечение

3. 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.

3.1. ПО, необходимое для функционирования ПК

ПОК предназначен для функционирования на ПЭВМ с архитектурой Intel x86_84.

Требования к аппаратному обеспечению описаны в Таблица 3.

Таблица 3 Требования к аппаратному обеспечению

Характеристики	Минимальные требования
CPU	2 ядра
BIOS	Поддержка NX/XD для CPU
Оперативная память	4 GB (минимально) 8 GB (рекомендовано)
Сетевые контроллеры	Один Gigabit-контроллер или один Ethernet-контроллер
Жесткий диск	Наличие жесткого диска для развертывания программного комплекса «Система защиты сетевого оборудования NFI»
VMware ESXI	Специализированный аппаратный гипервизор VMware ESXI версия 6.0 (минимально) Специализированный аппаратный гипервизор VMware ESXI версия 7.0 (рекомендовано)

Виртуализация	Поддержка виртуализации со стороны материнской платы и процессора Возможность включения поддержки аппаратной виртуализации (Intel VT-x или AMD RVI)

3.2. Языки программирования, на которых написан ПК

Код Программного комплекса «Инспектор сетевого фильтра NFI» реализован с помощью: C, C++, PHP, Bash.

4. Процессы, обеспечивающие поддержание жизненного цикла

Поддержание жизненного цикла ПК «Инспектор сетевого фильтра NFI» осуществляется за счет сопровождения комплекса, включающего в себя следующие сервисные процессы:

1. Поставка и настройка программного комплекса (первичная и в процесс эксплуатации);
2. Техническая поддержка пользователей;
3. Проведение обновления программного комплекса.

Сопровождение ПК необходимо для:

- Обеспечения гарантий корректного функционирования ПК и дальнейшего развития её функционала;
- Отсутствия простоя в работе по причине невозможности функционирования ПК (аварийная ситуация, ошибки в работе и т.п.).

Программный комплекс «Инспектор сетевого фильтра NFI» распространяется по проприетарной модели (закрытый исходный код). Конечный пользователь получает неисключительную лицензию на программный продукт.

4.1. Требования к квалификации пользователей

Работа с программным комплексом «Инспектор сетевого фильтра NFI» должна осуществляться в соответствии с Руководством пользователя.

Требования к специалисту, сопровождающего ПК «Инспектор сетевого фильтра NFI»:

1. Наличие опыта работы по настройке сетевых протоколов, сетевого оборудования;
2. Знание PfSense;
3. Наличие опыта работы по настройке сети;
4. Наличие опыта работы с NGFW, с FreeBSD, VMware;
5. Знание топологии сети;
6. Компетентность в вопросах кибербезопасности.

4.2. Обновление программного комплекса

Устранение неисправностей, не влияющих на общую работоспособность ПК «Инспектор сетевого фильтра NFI» выполняется разработчиком в новых версиях, клиент только осуществляет обновление ПК в соответствии с инструкцией по обновлению ПК.

Устранение критических неисправностей, влияющих на общую работоспособность ПК «Инспектор сетевого фильтра NFI» выполняется разработчиком в максимально короткие сроки. Каких-либо действий, требующих специальной квалификации, со стороны клиента выполнять не требуется, клиент производит только установку готового обновления в соответствии с инструкцией по обновлению ПК.

В целях безопасности, установка обновленной версии ПК «Инспектор сетевого фильтра NFI» производится со съемного носителя.

Подготовка съемного носителя:

1. Используйте съемный носитель USB (USB flash drive). Рекомендуется использовать съемный носитель с поддержкой интерфейса USB 3.0. Рекомендуемая емкость носителя составляет 2 ГБ (или больше).
2. Отформатируйте съемный USB-носитель в файловой системе FAT32.
3. Скопируйте на USB-носитель заранее загруженный архив с обновлением. Архив должен быть в формате .TAR.

Установка обновления со съемного носителя:

1. Подключите съёмный носитель к USB-порту устройства NFI.

2. На главном экране консоли pfsense необходимо выбрать пункт 8 – «Shell».

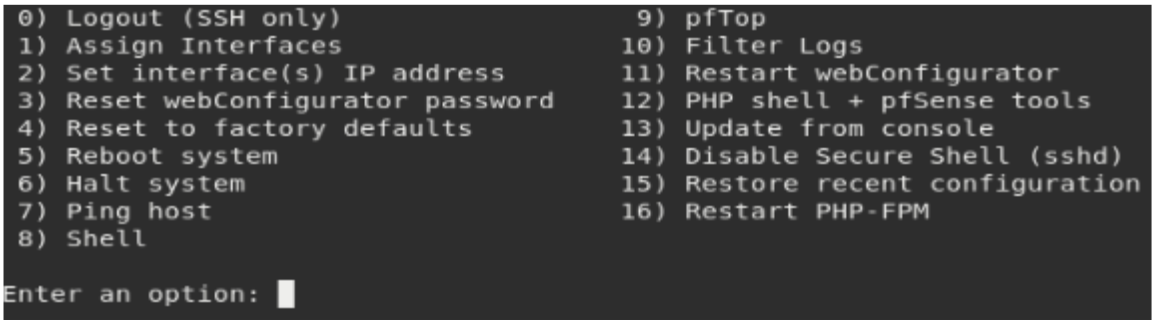

Рисунок 1Вывод консоли

3. С помощью команды gpart list | less найти имя первого раздела подключенного носителя (в описании нужного устройства в списке Providers первая строка, Name).

Рисунок 2 Описание подключенного носителя

4. Создать каталог, в который будет примонтирован носитель:
   mkdir /mnt/nfi;
5. Примонтировать носитель в папке /mnt с помощью команды:
   *mount_msdosfs /dev/*имя первого раздела носителя */mnt/nfi;*
6. Перейти в каталог с архивом:
   cd /mnt/flash;
7. Разархивировать файл nfi.tar.gz:
   tar -xvf ./nfi.tar.gz;
8. Создать каталог с файлами модуля:
   mkdir /usr/src/nfi;
9. Скопировать файлы из носителя в каталог nfi:
   cp -r /mnt/flash/ /usr/src/nfi/;*
10. Запустить скрипт install.sh:
    sh /usr/src/nfi/install.sh;

11. В консоли будет выведено сообщение об успешной установке:

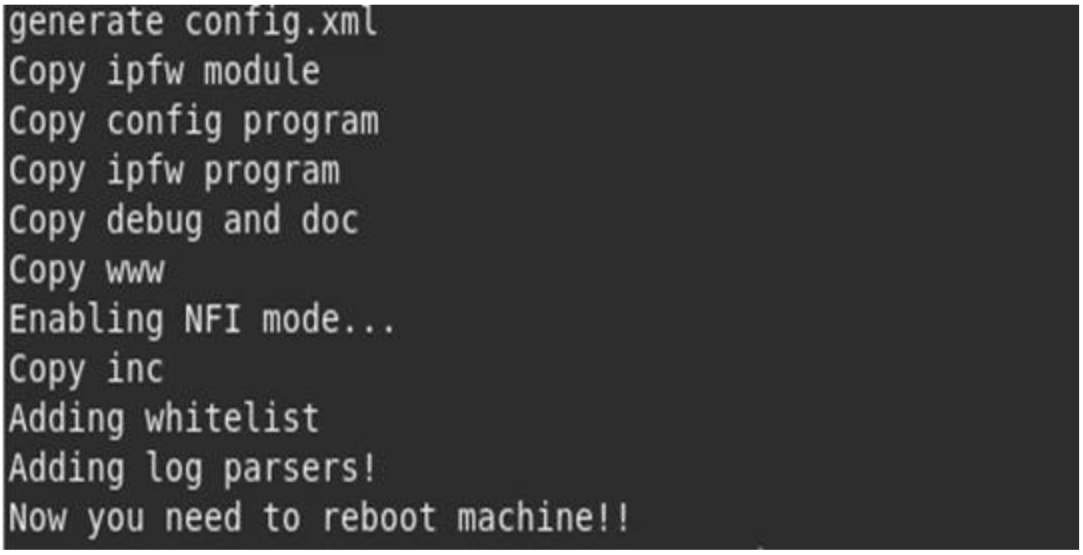

Рисунок 3 Вывод скрипта

12. Перезапустите устройство NFI;
13. Проверьте, что интерфейсы NFI назначены корректно.

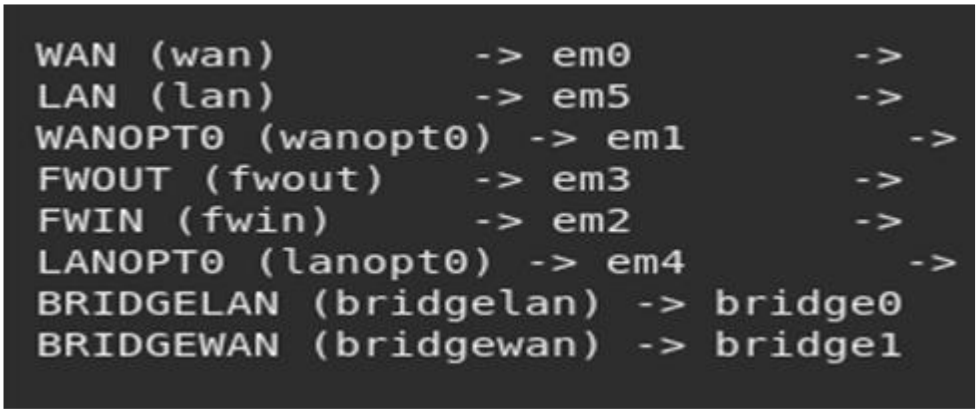

Рисунок 4 Назначение сетевых интерфейсов

4.3. Техническая поддержка пользователей

В рамках технической поддержки программного комплекса оказываются следующие услуги:

- Помощь в установке;
- Помощь в настройке и администрировании;
- Помощь в установке обновлений;
- Помощь в поиске и устранении проблем в случае некорректной установки обновления;
- Пояснение функционала модулей программного комплекса, помощь в эксплуатации;

– Общие консультации по выбору серверного программного обеспечения для обеспечения более высокой производительности работы программного комплекса.

В случае выявления каких-либо неисправностей в работе ПК «Инспектор сетевого фильтра NFI» необходимо сообщить об этом факте одним из способов (в порядке уменьшения приоритета):

– На адрес электронной почты office@avsw.ru;
– По телефону: +7 (495) 651-92-45.

4.3.1. Требования к квалификации специалистов тех. поддержки

Требования к специалистам, обеспечивающим техническую поддержку и развитие ПК:

1. Наличие опыта работы по настройке сетевых протоколов, сетевого оборудования;
2. Знание PfSense;
3. Наличие опыта работы по настройке сети;
4. Наличие опыта работы с NGFW, с FreeBSD, VMware;
5. Знание топологии сети;
6. Наличие опыта по развертыванию и настройке ПК «Инспектор сетевого фильтра NFI»;
7. Компетентность в вопросах кибербезопасности.