

Инспектор сетевого фильтра NFI v1.1

Руководство пользователя

на 17 листах

Москва 2021г.

Контактная информация

127106, г. Москва, ул. Гостиничная, д.5Тел.: +7 (495) 988-92-25

E-mail: office@avsw.ru www.avsw.ru/about/contacts

Авторское право

ООО «AB Coфт» www.avsw.ru © 2010-2021 ООО «AB Coфт»

Версия документа

Март 20, 2021.

Настоящий документ является собственностью ООО «АВ Софт» (далее — «АВ Софт») и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения «АВ Софт».

СОДЕРЖАНИЕ

1	Термины и определения	4
2	Введение	6
2.1	Назначение и условия применения	6
2.2	Функциональные ограничения	6
3	Подготовка к работе	7
4	Описание операций	11
5	Нештатные ситуации	13
6	Интеграция с внешним SIEM	16

1 Термины и определения

В настоящем документе используются термины и определения, представленные в таблице .

Таблица 1. Термины и определения

№ п/п	Термин	Определение
1.	Bypass режим	Режим питания нагрузки сетевым напряжением в обход основной схемы системы бесперебойного питания

В настоящем документе используется перечень сокращений, представленный в таблице.

Таблица 2. Перечень сокращений

№ п/п	Сокращение	Расшифровка
1.	IPFW	Ipfirewall
2.	NFI	Network Filter Inspector
3.	NGFW	Next-Generation Firewall
4.	VGA	Video Graphics Array
5.	нсд	Несанкционированный доступ
6.	ПО	Программное обеспечение

2 Введение

Инспектор сетевого фильтра NFI (далее – NFI) является программным комплексом (далее – ПО) для контроля сетевого оборудования, включая межсетевые экраны нового поколения (NGFW), на предмет выявления компрометации и несанкционированного подключения к внешним ресурсам.

Область применения ПО включает в себя защиту информационной инфраструктуры от несанкционированного доступа (далее – НСД) сетевого оборудования во внешнюю сеть Интернет.

Уровень знаний пользователя ПО должен соответствовать уровню администратора ПО.

2.1 Назначение и условия применения

ПО предназначено для решения задач контроля подключений к внешним ресурсам сети Интернет со стороны сетевых устройств корпоративной или ведомственной сети, включая NFFW, в целях усиления безопасности информационной инфраструктуры организации.

ПО может использоваться как для контроля NGFW, так и в качестве самостоятельного межсетевого экрана.

2.2 Функциональные ограничения

В ПО присутствует ограничение на минимальное количество интерфейсов, которых должно быть не менее 4-х. Данное разграничение необходимо для удобного контроля проходящих пакетов. В случае, когда сетевых интерфейсов пять и более, NFI назначает NGFW1 и NGFW2 на интерфейсы по середине, интерфейсы с номером меньше половины от их количества работают аналогично интерфейсу LAN, а интерфейсы с номером больше половины от их количества работают аналогично интерфейсов назначается на 1 больше.

3 Подготовка к работе

Для подготовки NFI к работе необходимо выполнить следующую последовательность действий:

- Необходимо подключить кабель питания, консольный кабель VGA или COM кабель.
- Далее необходимо подключить кабели Ethernet к устройству в соответствии с их назначением по таблице 3 и схемой подключения портов на рисунке 1.

Таблица 3. Конфигурация сетевых портов

№ п/п	Порт	Назначение
1.	WAN (LAN1)	Выход в сеть Интернет
2.	NGFW1 (LAN2)	Оборот в кольцо NGFW (WAN)
3.	NGFW2 (LAN3)	Оборот в кольцо NGFW (LAN)
4.	LAN (LAN4)	Выход в локальную сеть

ИнтерензводеньраМН





Рисунок 1. Схема подключения портов NFI

- 3. Включить NFI. На экране загрузки получить IP адрес, выделенный NFI на интерфейсе WAN.
- Выполнить авторизацию в веб-интерфейсе NFI по полученному IP адресу из предыдущего пункта из компьютера, подключенного к локальной сети (LAN4) (Рисунок 2).

	линая панель						ŦŬ
Информация Сист	емы 🗲 🗢 😒	Интерфе	йсы			ŗ	• •
Имя	pfSense.localdomain	da WAN	•	1000baseT <full-dup< td=""><td>lex></td><td>192.168.10.144</td><td>ļ.</td></full-dup<>	lex>	192.168.10.144	ļ.
Пользователь	admin@192.168.10.234 (Local Database)	di LAN	0	autoselect		n/a	
Система	pfSense Идентификатор Устройства Netgate: 8b4186ab92c5478eafb4	LAN2	0	autoselect autoselect		n/a n/a	
SMART	Производитель: American Megatrends Inc. Версия:5.6.5 Дата Релиза: Fri Aug 31 2018	Графы Т WAN	рафика	3	🔵 wan (i) 😑 wan (out)	• •
Версия	2.4.4-RELEASE-p3 (илиб4) сделин Wed May 15 18:53:44 EDT 2019 Free50 11 2./RELEASE-p10 Система работает на последней верски. Информацию верски обновлена в Fri Dec 27 8:39:04 UTC 2019 ©					M-L	2.0k 0.0 -2.0k
Тип Процессора	Intel(R) Celeron(R) CPU J1900 @ 1.99GHz Current: 1992 MHz, Max: 1993 MHz 4 [Iboueccopu: 1 package(s) x 4 core(s)	48:42	49:00	49:20	49:40	50:00	-4.0k 50:20
	AES-NI CPU Crypto: No	LAN			🔵 lan (in) 🔴 lan (out)	1.0
Kernel PTI	Включен						
Аптайм	23 Hours 53 Minutes 59 Seconds						500m
Текущие дата/время	Fri Dec 27 8:50:19 UTC 2019						0.0
Серверы DNS	127.0.0.1192.168.10.90208.67.222.222						-500m
Последнее изменение конфигурации	Fri Dec 27 8:49:45 UTC 2019	48:42	49:00	49:20	49:40	50:00	-1.0 50:20
Размер таблицы соединений	0% (47/803000) Показать соединения	LAN2			2019-12-27 11:49	0 opt1 (out)	1.0
Использование MBUF	1% (10136/1000000)				opt1 (in) 0.00 opt1 (out) 0.00	B/s B/s	500m
Спелноя заглузка	0.09.0.12.0.15						l

Рисунок 2. Авторизация в NFI

5. Перейти во вкладку «Межсетевой экран» (Рисунок 3).

	ма 🗸 Интерфейсы	Межсетевой экран 🔫	Сервис
		NFI	
Статус / Приборн	ая панель	Алиасы	
		Виртуальные IPs	
Информация Системи	bl	Правила	
Имя	pfSense.localdomain	Расписания	١
Пользователь	admin@192.168.10.234	(LC Сетевая Трансляция Адрес	сов І
Система	pfSense Идентификатор Устро	Трафик Шейпер йст ън мендине.	L

Рисунок 3. Переход в NFI

6. Далее выбрать «NFI» (Рисунок 4).

SOFT	Система 🗸	Интерфейсы 🗸	Межсетевой экран 👻	Сервисы 🗕	VPN 🗸	Статус 🗕	Диагностика 🗸	Помощь 🗸	•
Межсетевой	і́ экран / Ň	IFI							0
Страница Авто	обновления								
Обно	вить 🗹 Авт	оматически обновля	ть вывод ниже						
Вывод									
Заблокиро	ванные	IP адреса	:						
ТСР трафик									
ICMP трафик									
UDP трафик									

Рисунок 4. Вкладка «Межсетевой экран/NFI

Назвачение Интерфейсов Группы Интерфейсов Беспроводное VLANы Qings PPPs GREs QIFs Cerease мосты LAGGs Интерфейс Сетевой порт	скорани си са	тема - Интерфейсы - Межсетевой экран - Сервисы - nterface Assignments	VPN ← Статус ← Диаг	ностика • Помощь •
Интерфейс Сетеюй порт VXAN Тарбо 000 9127 00 25.80) • LAN Tap6 000 9127 00 25.80) • * Yature LAN2 Tap6 100 9127 00 25.80) • * Yature LAN2 Tap6 100 9127 00 25.80) • * Yature Charge Tap2 00 9127 00 25.80) • * Yature	Назначение Интерфей	ив Группы Интерфейсов Беспроводное VLANы QinQs	PPPs GREs GIFs	Сетевые мосты LAGGs
WAN Туро (00.04 27.40.25.3e) LUN Typo (00.04 27.40.25.3e) LUN2 Typo (00.04 27.40.25.3e) LUN3 Typo (00.04 27.40.25.3e) LUN3 Typo (00.04 27.40.25.3e) Comparison Typo (00.04 27.40.25.3e) Writerpleikcuk, koto opuse Hacropoelski kak vinelus Miterpopeikca Iag (4), отображаться не будут. Typo (00.04 27.40.25.3e) Беспроводные интерфейса Iag (4), отображаться не будут. Беспроводные интерфейсы должны Какть созданы на вкладке «Беспроводная сеть», прежде чем они смогут быть назначены.	Интерфейс	Сетевой порт		
LNN Lgbs (00.91/27.80.25.b1) @ Ygburn LNN2 Lgb1 (00.91/27.80.25.a1) @ Ygburn LNN3 Lgb2 (00.91/27.80.25.b0) @ Ygburn Comparisoner @ Ygburn Writesphericus, xotopue настроены как члены интерфейса lag (4), отображаться не будут. @ School (4), отображаться не будут. Беспроводные интерфейсы должны быть созданы на вкладке «Беспроводная сеть», прежде чем они смогут быть назначены.	WAN	Igb0 (00:9f:27:e0:25:ae)	•	
LAN2 (уb1 (00 91/27 ию 25 ал) • € Узаино LAN3 (уb2 (00 91/27 ию 25 b0) • € Узаино Сохранение Интерфейсы, которые настроены как члены интерфейса lag (4), отображаться не будут. Беспровадные интерфейсы должны быть созданы на вкладие «Беспровадная сеть», прежде чем они смогут быть назначены.	LAN	igb3 (00:9f:27:e0:25:b1)	• 💼	Удалить
LAN3 (gbz (00.91/27.e0.25.50) т) удонито Сопранение Интерфейсы, которые настроены как члены интерфейса lag (4), отображаться не будут. Беспроводные интерфейсы должны быть созданы на вкладке «Беспроводная сеть», прежде чем они смогут быть назначены.	LAN2	igb1 (00:9f:27:e0:25:af)	• 💼	Удалить
Сопранение Интерфийсы, которые настроены как члены интерфейса lag (4), отображаться не будут. Беспроводные интерфейсы должны быть созданы на вкладке «Беспроводная сеть», прежде чем они смогут быть назначены.	LAN3	igb2 (00:9f:27:e0:25:b0)	• 💼	Удалить
	Интерфейсы, которые н Беспроводные интерфе	строены как члены интерфейса lag (4), отображаться не будут. сы должны быть созданы на вкладке «Беспроводная сеть», прежде чем с	ни смогут быть назначены.	

Рисунок 5. Настройка сетевых портов

 Проверить наличие доступа в Интернет на машине, которая подключена к NGFW со стороны локальной сети (Интерфейс LAN).

4 Описание операций

Описание интерфейсов по порядку прохождения сетевых пакетов представлено в таблице 4.

№ п/п	Интерфейс	Описание
1.	Интерфейс LAN	К данному интерфейсу подключается локальная
	(LAN4)	сеть, локальный маршрутизатор. Те IP адреса, на
		которые поступает запрос из этого интерфейса,
		заносятся в специальный список с разрешёнными
		IP адресами. Данный список включает в себя
		счетчик пакетов для данного IP адреса, а также
		время (в секундах), когда пакет был обработан.
2.	Интерфейс	К данному интерфейсу подключается NGFW.
	NGFW2 (LAN3)	Пакеты пришедшие с интерфейса LAN попадают
		на NGFW не претерпевая никаких изменений.
3.	Интерфейс	К данному интерфейсу подключается выход
	NGFW1 (LAN2)	NGFW. Пакеты, проходящие из этого
		интерфейса, должны фильтроваться на случай
		НСД со стороны межсетевого экрана. Для тех IP
		адресов, которые были найдены в ранее
		заведённом списке, прохождение пакета будет
		заблокировано.
4.	Интерфейс WAN	К данному интерфейсу подключается выход в
	(LAN1)	сеть Интернет. Пакеты на данном этапе уже
		отфильтрованы от НСД со стороны NGFW.

Таблица 4. Описание интерфейсов

Минимальные требования к техническим средствам представлены в таблице 5.

№ п/п	Характеристики оборудования	Требования
1.	Процессор	Intel Celeron J1000 или похожий.
		2 ядра, от 1 GHz
2.	Оперативная память	4 GB
3.	Жесткий диск	HDD 30 Гб
4.	Сетевая карта	4 порта 10/100BASE-Т(Х)

Таблица 5. Минимальные требования к техническим средствам

Для работы в диалоговом режиме используется экран дисплея, клавиатура и манипулятор типа «мышь».

Для поддержки графического режима необходимо наличие адаптер SVGA.

Входные данные хранятся на гибком и/или жестком дисках. Программа работает под управлением ОС FreeBSD.

5 Нештатные ситуации

Примеры возможных нештатных ситуаций, связанных с программным и аппаратным сбоем, а также порядок действий, приведены в таблице .

N⁰	Нештатная	Порялок лействий
п/п	ситуация	
1.	Отсутствует проверка сетевого трафика	 Проверить корректность настройки сетевых портов. Необходимо перейти в веб-интерфейс NFI и удостовериться, что отсутствует сообщение об ошибках. Необходимо проверить работоспособность NGFW.
2.	Потеря питания	При потере питания система NFI, то все сетевые порты автоматически переходит в режим Bypass (но в данном режиме контроля сетевого трафика не осуществляется).
3.	Потеря данных	Для восстановления данных в системе необходимо инициировать процедуру восстановления данных из резервной копии, которая осуществляется после каждого изменения в системе NFI.
4.	Потеря работоспособности	Использовать функцию пробуждения по сети.

Таблица 6. Порядок действий в нештатных ситуациях

№ п/п	Нештатная ситуация	Порядок действий
5.	Отключение NGFW	При отключении можно использовать NFI в качестве межсетевого экрана (требуется дополнительная настройка) с ограниченным функционалом.
6.	Несанкционированное вмешательство в данные	Отключить доступ во внешнюю сеть Интернет.

Для просмотра полной информации о заблокированных пакетах необходимо перейти во вкладку «Диагностика» далее «Командная строка» (Рисунок 6).

	Сервисы 👻	VPN 🕶	Статус -	Диагностика 🛨	Помощь 🕶	۵
WARNING: The 'admin' account password is set to the default value. Change the password	rd in the User Ma	anader		ARP таблица		
		anagon.		DNS 3anpoc		
				pfInfo		
Статус / Приборная панель				pfTop		
	Network	.		Аутентификация		
информация Системы 🥕 🕃 😒	Netgate	Services	And Support	Выключить Систе	ему	
				Заводские Настр	ойки	
				Захват Пакетов		
				Информация об с	ограничителе	
				Командная строк	a	
				Маршруты		
				Перезагрузка		
				Пинг		

Рисунок 6. Открытие командной строки

В открытой вкладке в поле «Command» необходимо вписать следующую команду:

cat /var/log/ipfw.log

Диагностика / Командная строка	0
Только для продвинутых пользователей Возможности, представленные здесь, могут быть опасны. Поддержка не оказывается. Используйте их на свой страх и риск.	
Выполнить Команду Оболочки	
cat /var/log/ipfw.log	
< 7 Выполнить » Очистить	

Рисунок 7. Выполнение команды командной строке

6 Интеграция с внешним SIEM

Для подключения к внешнему SIEM необходимо:

1. Перейти в графическом интерфейсе NFI во вкладку Статус

ы <mark>й Журнал / Настройки</mark> экран DHCP Аутентификация Портала Захвата IPsec PPP	Captive Portal CARP (аварийный переход) DNS Resolver IPsec Monitoring	орепVPN
жран DHCP Аутентификация Портала Захвата IPsec PPP	IPsec Monitoring	рузки OpenVPN
	NTP	
прования	OpenVPN UPnP & NAT-PM	
Показать записи журнала в обратном порядке (самые новые записи сверху)	Балансировщик Нагрузки График трафика	
50 Это число записей журнала, отображаемое на графическом интерфейсе. Он не вли курнала.	Интерфейсы Логи Пакетов Очереди	аписей в файлах
Bytes Размер файла журнала остаётся неизменным на циклической основе. Данное пол сурнала, и сколько записей может быть внутри журнала. По умолчанию данное зг зайпов журнала примерно 20	Герезагрузка Фильтра Приборная панель Сервисы	лим будет размер файла яет 500Кб, и таких
СВЕДЕНИЮ: Размер журнала будет изменён, когда в следующий раз файл журна величить размер файла журнала, сначала сохраните опции установок размера, а Курнала [°] далее ниже на данной странице.Имейти в виду, что увеличение данного аким образом использование диска значительно увеличится.	Системный Журнал Срок аренды DHCP Срок аренды DHCPv6 Шлюзы	бы немедленно зуя опцию "Сброс Файлов эго файла журнала,
	рования	рования рования ОрепVPN UPnP & NAT-PM Балансировщик Нагрузки График трафика UPnP & NAT-PM Балансировщик Нагрузки График трафика UPnP & NAT-PM Балансировщик Нагрузки График трафика UPnP & NAT-PM Балансировщик Нагрузки График трафика UPnP & NAT-PM Балансировщик Нагрузки График трафика UPnP & NAT-PM Балансировщик Нагрузки График трафика UPnP & NAT-PM Балансировщик Нагрузки График трафика UPnP & NAT-PM Балансировщик Нагрузки График трафика UPnP & NAT-PM Балансировщик Нагрузки График трафика UPnP & NAT-PM Балансировщик Нагрузки IPadvik Tpadvika UPnP & NAT-PM Falled

2. Далее «Системный журнал» (Настройки)

Статус / Систем	ный Журнал / Настройки 📀			
Система Межсетев NTP Настройки	эй экран DHCP Аутентификация Портала Захвата IPsec PPP VPN Балансировщик Нагрузки OpenVPN			
Общие Опции Журн	алирования			
Отобразить в прямом или обратном порядке	Показать записи журнала в обратном порядке (самые новые записи сверху)			
Записи Журнала Графического Интерфейса	50			
	Это число записей журнала, отображаемое на графическом интерфейсе. Он не влияет на количество актуальных записей в файлах журнала.			
Размер файла журнала	Bytes			
(в Байтах)	Размер файла журнала остаётся неизменным на циклической основе. Данное поле контролирует, насколько большим будет размер файла журнала, и сколько записей может быть внутри журнала. По умолчанию данное значение приблизительно составляет 500Кб, и таких файлов журнала примерно 20. К СВЕДЕНИЮ: Размер журнала будет изменён, когда в следующий раз файл журнала будет очищен или удалён. Чтобы немедленно увеличить размер файла журнала, сначала сохраните опции установок размера, а потом очистите все логи, используя опцию "Сброс Файлов Журнала" далее ниже на данной странице. Имейти в виду, что увеличение данного значения увеличит размер каждого файла журнала, таким образом использование диска значительно увеличтся. Пространство диска, используемое файлов журнала в данный момент:9.7МОставшееся пространство диска для файлов журнала:95G			
	таким образом использование диска значительно увеличится. Пространство диска, используемое файлов журнала в данный момент:9.7МОставшееся пространство диска для файлов журнала:95G			

3. В нижней части страницы выбрать опцию «Отправлять сообщения журнала на удаленный сервер syslog»

Опции Удалённого У	Курналирования				
Журналирование	e				
Адрес Источника	По умолчанию (любой) 🗸				
	Эта опция позволяет демону журналирования связываться с одним IP адресом, вместо всех IP адресов. Если выбран один IP, все удалённые серверы системного журнала должны быть этого типа IP. Чтобы использовать IPv4 и IPv6 удалённые серверы системного журнала, привяжите их ко всем интерфейсам.				
	К СВЕДЕНИЮ: Если IP адрес не может быть найден на выбранном интерфейсе, демон будет привязан ко всем адресам.				
IP Протокол	IPv4 v				
	Данная опция используется только при выборе выше не-дефолтного адреса в качестве источника. Данная опция всего лишь выражает предпочтение; Если IP адрес данного типа не найден на выбранном интерфейсе, будуе предпринята попытка использования другого типа.				
Серверы удалённого журнала	[IP[:port] [IP[:port]				
Содержание	✓ Bce				
Удалённого Сервера	🗆 Системные События				
Журнала	🗆 События Межсетевого Экрана				
	🗌 DNS-события (Резолвер/исходящий, Форвардер/dnsmasq, filterdns)				
	События DHCP (DHCP-демон, DHCP-ретрансляция, DHCP-клиент)				
	События РРР (клиент WAN PPPoE, клиент WAN L2TP, клиент WAN PPTP)				
	🗌 События Портала авторизации				
	События VPN (IPsec, OpenVPN, L2TP, PPPoE-сервер)				
	События монитора шлюза				
	События демона маршрутизации (RADVD, UPnP, RIP, OSPF, BGP)				
	События Балансировцика Нагрузки Сервера (relayd)				
	 События протокола Сетевого времени (демон NTP; клиент NTP) События беспроводной сети (hostapd) 				
	Системный Журнал отправляет датаграммы на порт 514 указанного удалённого сервера системного журнала, если не указан другой порт. Убедитесь в том, что настроен syslogd на удалённом сервере, чтобы принимать сообщения системного журнала от pfSense.				
	В Сохранение				

4. Ввести адрес сервера и отметить необходимые события