



PT NGFW:

Новинки и новости



- 7 месяцев после старта
- Расширение линейки
- Новые функции 1.8
 - BFD
 - VPN
 - DHCP
 - BGP community
 - И другие важные изменения
- Дальнейшие планы

7 моделей

в линейке:
от 300 Мбит/с до 300 Гбит/с

4%

рынка межсетевых экранов России
в конце 2024г согласно
исследованию ЦСР



Выход
на международный рынок

100+

заказчиков выбрали PT NGFW для
защиты своей сети и уже
приобрели их себе

500+

устройств отгружено на
сегодняшний день

60 Гбит/с

в режиме IPS. Самый
производительный российский
межсетевой экран



**Мы слишком
производительные?**

PT NGFW 1005



NEW



Набор встроенных интерфейсов

- 4 × 1 Гбит/с RJ-45
- 1 × 1/10 Гбит/с SFP+

Роли сетевых портов

- Порт 1-3 – порты для пользовательского трафика
- Порт 4 – кластерный линк
- Порт 5 – выделенный интерфейс внеполосного управления
- Console – классический консольный порт

Разъёмы на обратной стороне

- Разъем блока питания (идёт в комплекте)
- VGA и USB – используется для АМДЗ в сертифицированных ФСТЭК версиях

PT NGFW 1020



NEW



Набор встроенных интерфейсов

- 4 × 1 Гбит/с RJ-45
- 4 × 1/10 Гбит/с SFP+

Роли сетевых портов

- Порт 3-8 – порты для пользовательского трафика
- Порт 2 – кластерный линк
- Порт 1 – выделенный интерфейс внеполосного управления
- Console – классический консольный порт
- Слоты для SIM-карт (для версии с LTE, позже)

Разъёмы на обратной стороне

- 2 разъема для блоков питания (идут в комплекте)
- VGA и USB – используется для АМДЗ в сертифицированных ФСТЭК версиях

Портфолио РТ NGFW



IPS,
Гбит/с

60

30

10

5

0,6

0,1

1 Гбит/с

10 Гбит/с

100 Гбит/с

300 Гбит/с



1005

1010



VM-1010

NEW

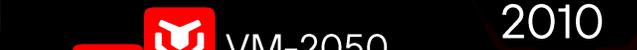


1020

1050



VM-1050



VM-2010

VM-2020

VM-2050



2010

2020

2050

3010

3040

FW+ L7

От филиала до ЦОД



	PT NGFW 1005	PT NGFW 1010	PT NGFW 1020	PT NGFW 1050
В режиме L4 FW + AppControl	1 Гбит/с	4 Гбит/с	8 Гбит/с	10 Гбит/с
В режиме IPS + AppControl	120 Мбит/с	600 Мбит/с	1,4 Гбит/с	4,5 Гбит/с
FW + IPS + AppControl + NAT + AV + URL- категоризация	100 Мбит/с	480 Мбит/с	1 Гбит/с	3,3 Гбит/с
	1,3 Mpps	1,3 Mpps	2 Mpps	3,2 Mpps

От филиала до ЦОД

	PT NGFW 2010	PT NGFW 2020	PT NGFW 2050	PT NGFW 3010	PT NGFW 3040
В режиме L4 FW + AppControl	80 Гбит/с	100 Гбит/с	140 Гбит/с	190 Гбит/с	300 Гбит/с
В режиме IPS + AppControl	12 Гбит/с	23 Гбит/с	32 Гбит/с	40 Гбит/с	60 Гбит/с
FW + IPS + AppControl + NAT + AV + URL- категоризация	10 Гбит/с	18 Гбит/с	25 Гбит/с	32 Гбит/с	47 Гбит/с
	7 Mpps	8,5 Mpps	12 Mpps	15 Mpps	20 Mpps



**Кто вы,
мистер ИКС?**

PT NGFW 3050



Элементная база

- 2 * Intel 8470N
- 16 * 64 GB RAM DDR5

Амбициозная цель

- 400+ Gb AppControl
- 100+ Gb IPS+AV+URL+NAT

Взрывной функциональный рост

Site-to-site VPN IPsec



- ✦ Routed based
- ✦ Совместим с любым другим межсетевым экраном
- ✦ Без ASIC и FPGA

Editing the IPsec tunnel ✕

General IKEv2 **IPsec**

Exchange methods

Encryption

AES-GCM-256 ✕ AES-GCM-128 ✕ AES-CBC-256 ✕ AES-CBC-128 ✕ ✕ ▾

Authentication

SHA-512 ✕ SHA-384 ✕ SHA-256 ✕ ✕ ▾

Key lifetime (s) 28800 ✕ From 0 to 604800 seconds, 0 is infinite

Key lifesize (KB) 4608000 ✕ From 0 to 2147483648 KB, 0 is infinite

Perfect Forward Secrecy

Local traffic selector ⓘ + 🔍 ☰ Peer traffic selector ⓘ + 🔍 ☰

🏠 0.0.0.0/0 🏠 0.0.0.0/0

Логика настройки S2S VPN



IPsec соединения

Основные IKEv2 IPsec

Состояние Включено

Общие

Название

Описание

Виртуальный туннельный интерфейс

Виртуальный роутер Зона безопасности

IP-адрес

IP-адрес и длина префикса (например, 192.168.80.10/32)

Force NAT-traversal Passive mode

Maximum transmission unit (MTU) Adjust TCP MSS

От 68 до 1500 Б

TCP maximum segment size (MSS) равен 1360 Б
Определяется автоматически по формуле: $MSS = MTU - 40$

IPsec соединения

Основные IKEv2 IPsec

Параметры шифрования

Шифрование

Аутентификация

Обмен ключами

Key lifetime (сек)

От 0 до 172800 секунд, 0 - бесконечность

Локальные параметры

Интерфейс

Тип локального ID Локальный ID

Pre-shared key

Удаленные параметры

Тип адреса Адрес

Тип удаленного ID Удаленный ID

Асимметричные pre-shared keys

Dead Peer Detection (DPD)

IPsec соединения

Основные IKEv2 IPsec

Параметры шифрования

Шифрование

Аутентификация

Key lifetime (сек) Key lifeseize (KB)

От 0 до 604800 секунд, 0 - бесконечность От 0 до 2147483648 KB, 0 - бесконечность

Perfect Forward Secrecy

Локальные трафик-селекторы Удаленные трафик-селекторы

Журналы IPSec



PT NGFW
Политики Объекты Устройства **Журналы** Параметры
↑ Отправить на устройства

- Трафик
- Расшифрование
- IPS
- Аудит
- Антивирус
- Аутентификация
- Политика аутентификации
- ICAP
- IPSec

IPSec logs

⌚ Последние 30 дней
🔍 Откл

📄 Экспорт в формате CSV
🔄 Обновить

^ Скрыть фильтры · 0

+ Добавить фильтр

Время создания записи	Событие	Описание	Название туннеля	Название виртуального к...	Название уст
04.07, 17:37:31	Соединение не удалось	Ошибка расшифровки	3xS1aeA0PX	XV3sQNRuFv	
04.07, 17:37:31	Соединение не удалось	Неподдерживаемая версия IKE	Yy9nXGEJl4	JTaNBdbjJD	
04.07, 17:37:31	Соединение не удалось	Некорректные трафик-селекторы	jqYtP0cgjl	nu8XfuVld1	
04.07, 17:37:31	Туннель активен		wl2WIUTh7u	5kcpPxtz6C	
04.07, 17:37:31	Соединение не удалось	Ошибка расшифровки	adLgJfqRjE	PkSYmiQM3U	
04.07, 17:37:31	Соединение не удалось	Неизвестный идентификатор peer	xmyjGctPXu	ZIHJRuC50u	
04.07, 17:37:31	Соединение не удалось	Неизвестный SPI	eVLpuaWd6F	68Nw5YiLN5	
04.07, 17:37:31	Соединение не удалось	Некорректное IKE сообщение	o3r8G0R7q6	XtjD11c36W	
04.07, 17:37:31	Соединение не удалось	Некорректное IKE сообщение	Te2f4us3cE	Cewx7g0Vm0	
04.07, 17:37:31	Соединение не удалось	Ошибка расшифровки	ZbSRPdH7WP	LHBURRFW52	
04.07, 17:37:31	Соединение не удалось	Некорректное IKE сообщение	uXSVPXTopl	Hg7WBDaaoZ	
04.07, 17:37:31	Соединение не удалось	Ошибка расшифровки	KsjXasdljZ	4sUUDBSAPd	
04.07, 17:37:31	Соединение не удалось	Неизвестный SPI	QZxA8P6VT1	vOSdXJrC2c	
04.07, 17:37:31	Соединение не удалось	Неподдерживаемая версия IKE	PXK3RVNPHF	NpwxCdP82p	
04.07, 17:37:31	Соединение не удалось	Не выбраны IKE параметры	m2QC8LrDOW	gj2CqrGYOc	
04.07, 17:37:31	Соединение не удалось	Некорректные трафик-селекторы	MeVv1dawHP	OWjtVWY1EB	
04.07, 17:37:31	Соединение не удалось	Некорректные трафик-селекторы	RpufgqUpKK	qWOCsyovDW	
04.07, 17:37:31	Соединение не удалось		KchoFC7MzE	Wkkcq6S1J5	
04.07, 17:37:31	Соединение не удалось	Не выбраны IPSec параметры	F6GfMdF1S9	Y4yqZBwGnb	

IPSec log

Общая информация

Время создания записи 04.07, 17:37:31	Название туннеля 3xS1aeA0PX	Название виртуального контекста XV3sQNRuFv
Событие Соединение не удалось	Локальный адрес ::ffff:251.206.214.197	Название устройства
Описание Ошибка расшифровки	Удаленный адрес www.dynamicvertical.net.	Серийный номер устройства serial number

IKE SA

IKEv2 шифрование AES-GCM-256	IKEv2 аутентификация SHA-1	IKEv2 обмен ключами DH-768 (group 1)
IKEv2 key lifetime 82	Локальный SPI 11	Удаленный SPI 72
IKE локальный адрес www.districtinterfaces.in...	IKE удаленный адрес www.forwardorchestrat...	

IPsec SA 1

Локальный SPI 475	Удаленный SPI 219	IPsec шифрование AES-GCM-128
IPsec key lifetime 6	IPsec key lifeseize (kb) 6	IPsec аутентификация MD5
ESP Локальный адрес ::ffff:247.163.48.79		ESP Удаленный адрес ::ffff:165.68.193.1

Удаленные трафик-селекторы
Порты: 80 - 1500
Порты: 80 - 1500
Протокол: 2

IPsec SA 2

Локальный SPI 10	Удаленный SPI 174	IPsec шифрование AES-CBC-256
IPsec key lifetime 6	IPsec key lifeseize (kb) 6	IPsec аутентификация MD5



Совместимость

- Cisco ASA, routers
- Check Point
- Fortinet
- Juniper
- Palo Alto
- strongSwan
- VyOS
- ...





Цифры*

HTTP response size 64kb (aes-gcm-256)



1010	500 Mb/s
1050	3 Gb/s
2010	10,5 Gb/s
2020	17,9 Gb/s
2050	24,3 Gb/s
3010	35,2 Gb/s
3040	47,7 Gb/s

*Предварительные тесты. В релизах 1.8.x планируется оптимизация производительности

Кластер

Повышение управляемости

Общие | Кластеры > Cluster-1

Изменить

Общие

Название	Cluster-1
Состояние	● Ok
Configuration state	● In sync
Тип	Кластер A/S
Описание	
Использовать виртуальный MAC-адрес для интерфейсов	Отключено
Preemption	Отключено

Устройства

Узел	Название устройства	Connection state	State in cluster	Состояния устройства обновлены	Версия продукта
1.	LAB-Debian-nafw-node-1	● Подключено	● Active	06.05.2025, 12:29:02	1.7.0
2.	LAB-Debian-nafw-node-2	● Отключено	● Standby	06.05.2025, 12:29:02	1.7.0

Изменение кластера

Название

Cluster-1

Тип

Кластер A/S

Описание

Использовать виртуальный MAC-адрес для интерфейсов

Preemption

Устройства

Узел	Название	Connection st...	State in cluster	IP-адрес MG...	Модель	Серий-
1.	LAB-Debia...	● Подкл...	● Active	10.13.107.34	PT-VM	001
2.	LAB-Debia...	● Подкл...	● Standby	10.13.107.35	PT-VM	002

Узел 1

Priority

5

Sync-link IP address

192.168.250.1

Sync-link port

5650

1 — самый высокий, 10 — самый низкий

Например, 192.168.100.50

От 1 до 65535

Узел 2

Priority

6

Sync-link IP address

192.168.250.2

Sync-link port

5650

1 — самый высокий, 10 — самый низкий

Например, 192.168.100.51

От 1 до 65535

Сохранить

Отмена

Кластер

Статусы в UI

Общие | Кластеры > Cluster-1

[Изменить](#)

Общие

Название	Cluster-1
Состояние	● Degraded
Configuration state	● In sync
Тип	Кластер A/S
Описание	
Использовать виртуальный MAC-адрес для интерфейсов	Отключено
Preemption	Отключено

Устройства

Узел	Название устройства	Connection state	State in cluster	Версия продукта	Версия компо...
1.	LAB-Debian-ngfw-node-1	● Отключено	● Unknown	1.7.0	2.0.0.12001
2.	LAB-Debian-ngfw-node-2	● Подключено	● Active	1.7.0	2.0.0.12001

Общие | Кластеры > Cluster-1

[Изменить](#)

Общие

Название	Cluster-1
Состояние	● Down
Configuration state	● In sync
Тип	Кластер A/S
Описание	
Использовать виртуальный MAC-адрес для интерфейсов	Отключено
Preemption	Отключено

Устройства

Узел	Название устройства	Connection state	State in cluster	Версия продукта
1.	LAB-Debian-ngfw-node-1	● Подключено	● Suspended	1.7.0
2.	LAB-Debian-ngfw-node-2	● Отключено	● Unknown	1.7.0

Кластер

Редактирование состава кластера

- Возможность создания кластера, в котором состоит только один NGFW
- Удаление узла из уже созданного кластера, например
- Добавление узла к уже созданному кластеру
- Удаление кластера с сохранением конфигурации на один из узлов

Изменение кластера

Название: Cluster-1 ✕ Тип: Кластер A/S ▾

Описание:

Использовать виртуальный MAC-адрес

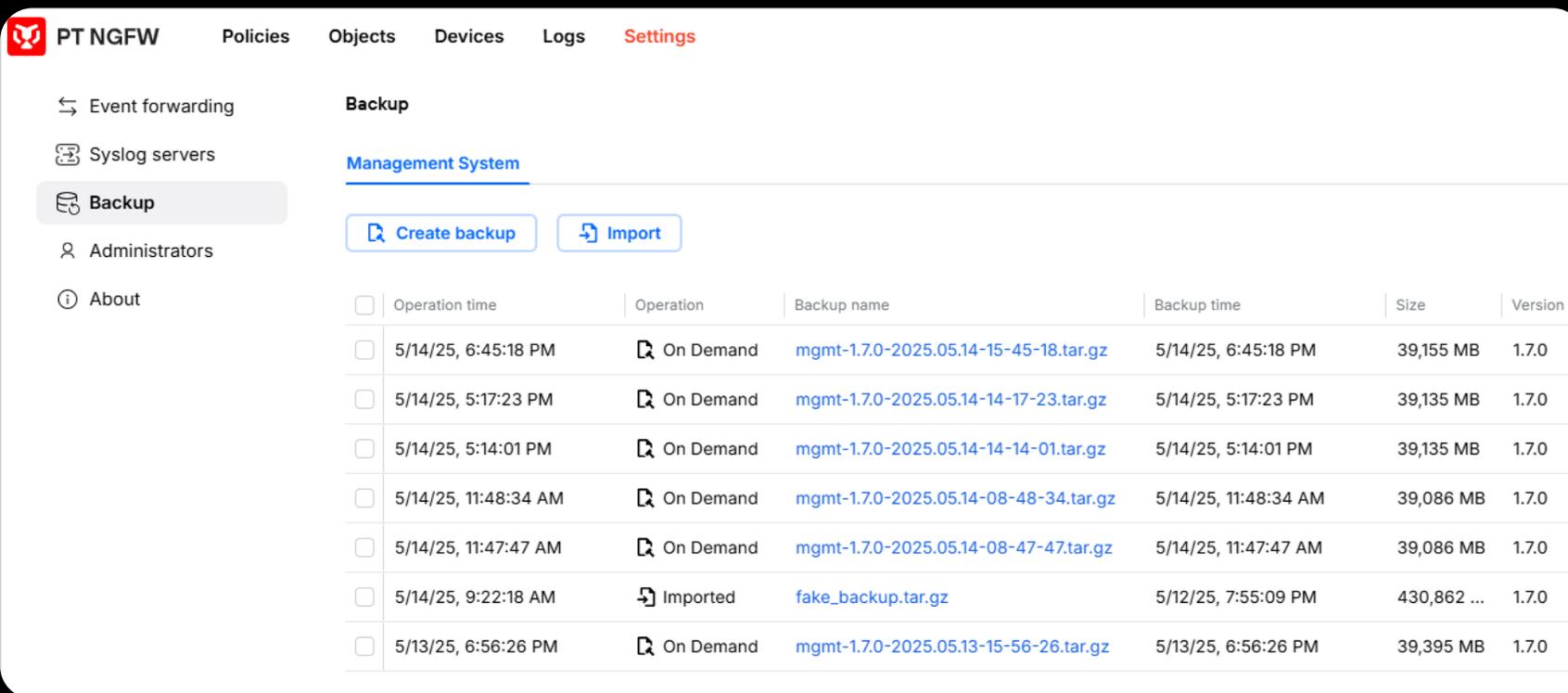
Приоритетное замещение

Устройства + Добавить

Узел	Название	Состояние по...	Состояние в кластере	Адрес MGMT	Мод
1.	LAB-Debian-ngfw-0	● Подкл...	● Активный	10.13.107.34	pt-n
2.	LAB-Debian-ngfw-2	● Подкл...		10.13.107.35	pt-n

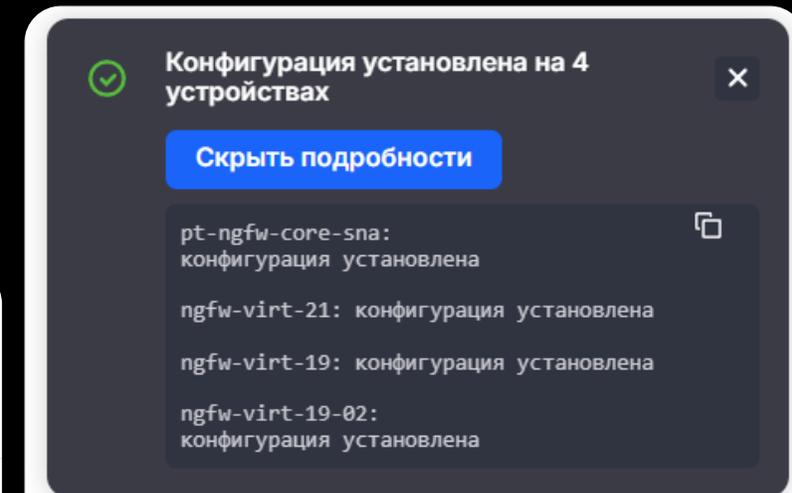
Удобство администрирования

- Бэкапирование в UI
- Гранулярный контроль применения конфигурации



The screenshot shows the PT NGFW web interface. The top navigation bar includes 'Policies', 'Objects', 'Devices', 'Logs', and 'Settings'. The left sidebar has 'Event forwarding', 'Syslog servers', 'Backup', 'Administrators', and 'About'. The main content area is titled 'Backup' and 'Management System'. It features 'Create backup' and 'Import' buttons. Below is a table of backup operations.

<input type="checkbox"/>	Operation time	Operation	Backup name	Backup time	Size	Version
<input type="checkbox"/>	5/14/25, 6:45:18 PM	On Demand	mgmt-1.7.0-2025.05.14-15-45-18.tar.gz	5/14/25, 6:45:18 PM	39,155 MB	1.7.0
<input type="checkbox"/>	5/14/25, 5:17:23 PM	On Demand	mgmt-1.7.0-2025.05.14-14-17-23.tar.gz	5/14/25, 5:17:23 PM	39,135 MB	1.7.0
<input type="checkbox"/>	5/14/25, 5:14:01 PM	On Demand	mgmt-1.7.0-2025.05.14-14-14-01.tar.gz	5/14/25, 5:14:01 PM	39,135 MB	1.7.0
<input type="checkbox"/>	5/14/25, 11:48:34 AM	On Demand	mgmt-1.7.0-2025.05.14-08-48-34.tar.gz	5/14/25, 11:48:34 AM	39,086 MB	1.7.0
<input type="checkbox"/>	5/14/25, 11:47:47 AM	On Demand	mgmt-1.7.0-2025.05.14-08-47-47.tar.gz	5/14/25, 11:47:47 AM	39,086 MB	1.7.0
<input type="checkbox"/>	5/14/25, 9:22:18 AM	Imported	fake_backup.tar.gz	5/12/25, 7:55:09 PM	430,862 ...	1.7.0
<input type="checkbox"/>	5/13/25, 6:56:26 PM	On Demand	mgmt-1.7.0-2025.05.13-15-56-26.tar.gz	5/13/25, 6:56:26 PM	39,395 MB	1.7.0



Конфигурация установлена на 4 устройствах

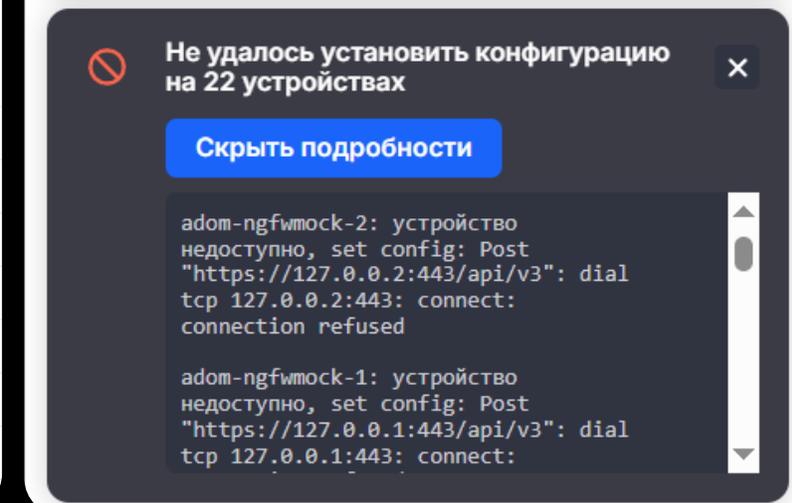
Скрыть подробности

pt-ngfw-core-sna: конфигурация установлена

ngfw-virt-21: конфигурация установлена

ngfw-virt-19: конфигурация установлена

ngfw-virt-19-02: конфигурация установлена



Не удалось установить конфигурацию на 22 устройствах

Скрыть подробности

```
adom-ngfwmock-2: устройство недоступно, set config: Post "https://127.0.0.2:443/api/v3": dial tcp 127.0.0.2:443: connect: connection refused
```

```
adom-ngfwmock-1: устройство недоступно, set config: Post "https://127.0.0.1:443/api/v3": dial tcp 127.0.0.1:443: connect:
```

ICAP



- Редактирование в UI
- Разные ICAP серверы для RESPMODE, REQMODE
- Режим мониторинга
- Выбор действия в случае недоступности сервера
- Совместимость с PT Sandbox и другими ICAP совместимыми продуктами

Новый профиль ICAP ✕

[Общие](#) [Модификация запроса](#) [Модификация ответа](#)

Группа устройств

⌵

Название

✕

Описание

ICAP



Новый профиль ICAP



Общие Модификация запроса Модификация ответа

Состояние

Включено

Сервер ICAP

PT-Sandbox

URI

/scanrequest

Журналирование

Режим мониторинга ⓘ

Действие при ошибке

Пропускать Блокировать

Тип контента

🔍 Search 🗑 Remove all + Добавить

📁 Documents

Все

Выбранные · 34



* Любой

> Archives · 16

▼ Documents · 34

abw
AbiWord document

azw
Amazon Kindle eBook format

CSV
Comma-separated values (CSV)

Новый профиль ICAP



Общие Модификация запроса Модификация ответа

Состояние

Включено

Сервер ICAP

PT-Sandbox

URI

/scanresponse

Журналирование

Режим мониторинга ⓘ

Действие при ошибке

Пропускать Блокировать

Тип контента

🔍 Search 🗑 Remove all + Добавить

📁 Archives

📁 Documents

📄 air
Adobe AIR Installation Package File

📄 btapp
uTorrent App

📄 apk
Android Package Kit (Android Application Package)

📄 deb
Debian software package file

Все

Выбранные · 54



* Любой

> Archives · 16

> Documents · 34

> Encrypted · 1

▼ Executables · 18

air
Adobe AIR Installation Package ...

apk

ICAP



Редактирование сервера ICAP



Название

PT-Sandbox



Группа устройств

Global



Описание

Подключение

Тип адреса

IP-адрес FQDN

IP-адрес

10.13.107.33



Например, 192.168.100.50

Порт

1344



От 1 до 65535

Подключений, макс.

100



От 1 до 1000

Попыток подключений, макс.

1



От 1 до 5

Тайм-аут подключения, мс

500



От 100 до 60000 миллисекунд

Тайм-аут ожидания вердикта, с

30



От 1 до 900 секунд

URI

URI или описание

+ Добавить

<input type="checkbox"/>	URI	Описание
<input type="checkbox"/>	/scanrequest	reqmode блокирующий режим
<input type="checkbox"/>	/scanresponse	respmode блокирующий режим

Изменение правила безопасности



Условия срабатывания

Зона источника

+ Добавить

* Любой

Адрес источника

+ Добавить

* Любой

Пользователь (источник)

+ Добавить

* Любой

Зона назначения

+ Добавить

* Любой

Адрес назначения

+ Добавить

* Любой

Приложение · 2

+ Добавить

http

web-browsing

Категории URL

+ Добавить

* Любая

Сервис

+ Добавить

* Любой

Действие при срабатывании

Действие

Разрешить

Профили безопасности · 1

+ Добавить

ICAP ICAP

Нет

✓ DLP-Sandbox

PT Sandbox all modes

ICAP



PT NGFW Политики Объекты Устройства **Журналы** Параметры

Трафик
Расшифрование
IPS
Аудит
Антивирус
Аутентификация
Политика аутентификации
ICAP
IPSec

ICAP logs

[Экспорт в формате CSV](#) [Обновить](#)

Скрыть фильтры · 0

[+](#) Добавить фильтр

Время создания з...	Действие	Категория контен...	Тип контента	URL	Имя файла	URI ICAP-сервера
04.07, 17:37:31	Заблокировать	Other	sh	https://vk.com	file.txt	icap://icap1.com/r...
04.07, 17:37:31	Разрешить	Documents	php	https://vk.com	file.txt	icap://icap1.com/r...
04.07, 17:37:31	Разрешить	Other	7z	https://vk.com	file.txt	icap://icap1.com/r...
04.07, 17:37:31	Разрешить	Archives	cab	https://vk.com	file.txt	icap://icap2.com/...
04.07, 17:37:31	Заблокировать	Other	midi	https://vk.com	file.txt	icap://icap2.com/...
04.07, 17:37:31	Разрешить	Archives	json	https://vk.com	file.txt	icap://icap1.com/r...
04.07, 17:37:31	Разрешить	Executable	yaml	https://vk.com	file.txt	icap://icap1.com/r...
04.07, 17:37:31	Заблокировать	Archives	7z	https://vk.com	file.txt	icap://icap2.com/...
04.07, 17:37:31	Заблокировать	Archives	7z	https://vk.com	file.txt	icap://icap1.com/r...
04.07, 17:37:31	Заблокировать	Archives	sh	https://vk.com	file.txt	icap://icap1.com/r...

BFD

- Классический и multihop
- Для статических маршрутов
- Для протоколов динамической маршрутизации



Новый профиль BFD ✕

Состояние
 Включено

Название

Латинские буквы, цифры или специальные символы: точка ("."), дефис ("-"), знак подчеркивания ("_"). От 1 до 63 символов

Описание

Режим
 Активный Пассивный

Желаемый минимальный интервал отправки пакетов (мс) <input type="text" value="1000"/> ✕ <small>От 100 до 2000. Значение по умолчанию 1000</small>	Необходимый минимальный интервал получения пакетов (мс) <input type="text" value="1000"/> ✕ <small>От 100 до 2000. Значение по умолчанию 1000</small>
--	--

Макс. число пропущенных пакетов
 ✕
От 2 до 50. Значение по умолчанию 3

Планы на релиз 1.9*

*Планы могут измениться без предварительного уведомления

Policy based routing

- **Квалификаторы**
 - Zone
 - Interface
 - Source address (user/group позднее)
 - Service
 - Type of service (позднее)
- **Действия**
 - No PBR
 - Drop
 - Forward
 - Out Interface
 - Changed next hop
 - Monitor (позднее)
- Совместимость с логированием политик фильтрации трафика

New PBR rule

Rule properties **Match conditions** Action on match

Source

Type

Zone Interface

Source interface [+ Add](#)

Add at least one interface

Source address [+ Add](#)

* Any

Destination

Destination address [+ Add](#)

* Any

Service & Application

Service [+ Add](#)

* Any

[Save](#) [Cancel](#)



Планы на релиз 1.9

- Индивидуальные таймауты для разных сессий
- Floating static route, включая работу с административной дистанцией и совместимость с BFD
- Синхронизация статусов интерфейсов в vWire
- Graceful restart и синхронизация таблиц маршрутизации
- TCP Dump на dataplane интерфейсах
- Loopback интерфейс
- Расширение функций CLI
- Расширение функций S2S VPN
- Расширение функций поиска по таблицам
- Расширение базы промышленных протоколов



Дополнительные материалы



[Даташит](#)



[Рoadmap](#)



[Условия тест-драйва](#)



[Архитектура сетевой безопасности предприятия](#)



[Отчет о тестировании независимой лабораторией BI.ZONE](#)



[Статья инженера PT NGFW «Как добиться 5+ Гбит/с от виртуального NGFW»](#)



[Курс по эксплуатации PT NGFW](#)