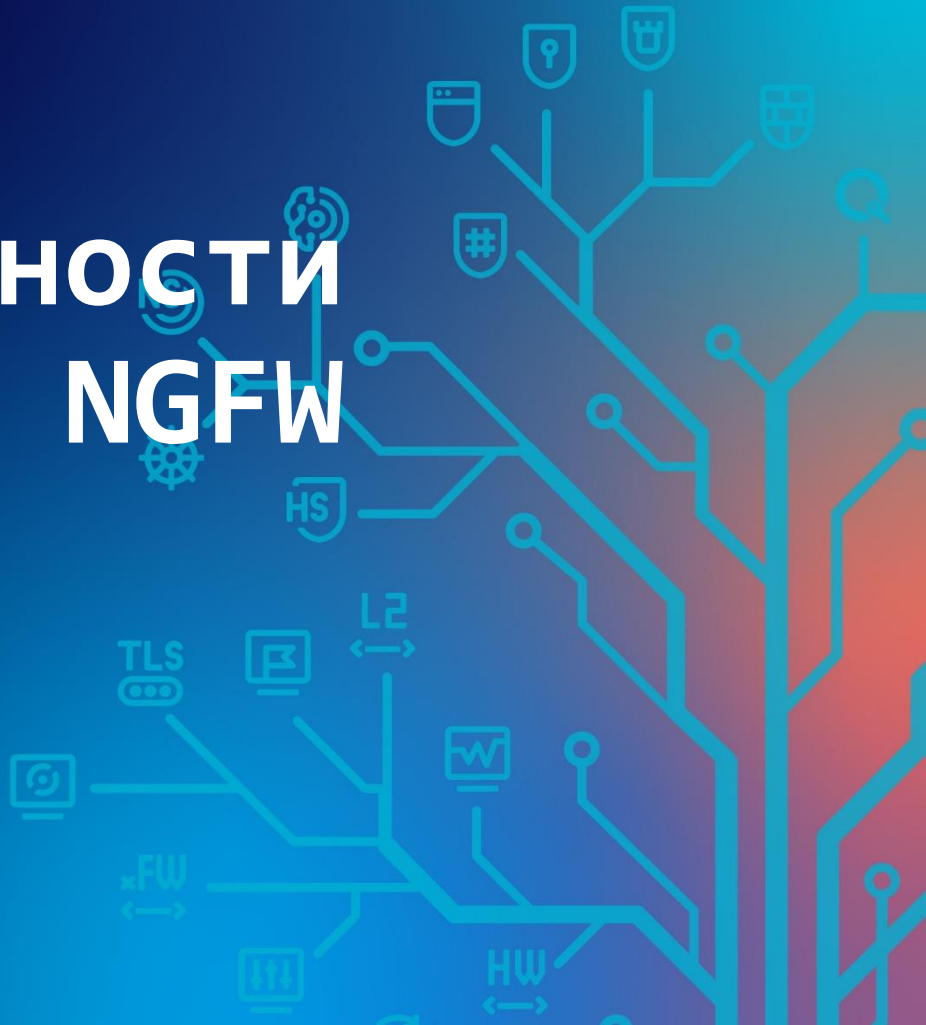
Шлюзы безопасности ViPNet класса NGFW

Алексей Данилов



NGFW

Next-Generation Firewall (NGFW)

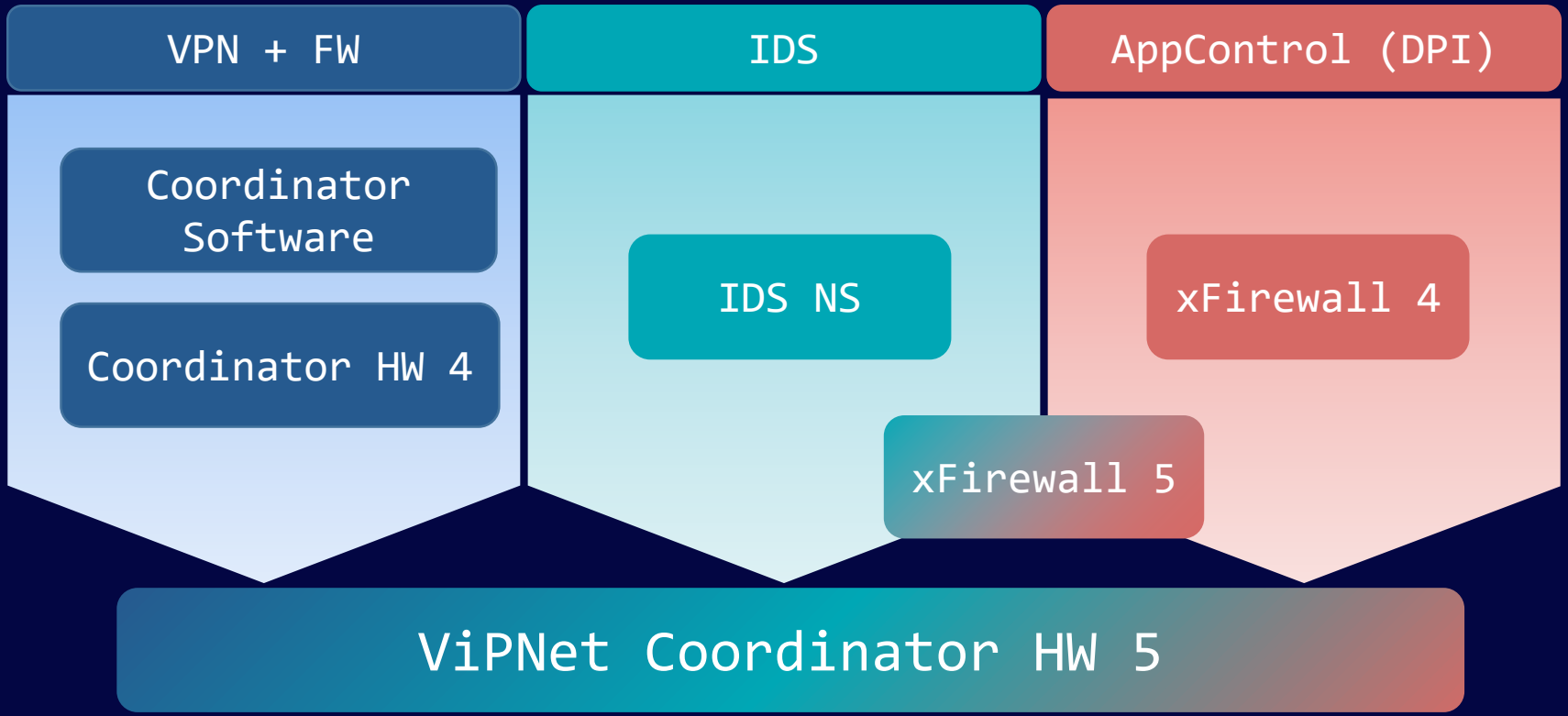
Gartner

МЭ следующего поколения (NGFW) в дополнении к общепринятому разграничению доступа предоставляет возможности по выявлению и блокировке современных угроз, таких как: вредоносное ПО, атаки уровня приложений.

Согласно определению Gartner NGFW должен состоять из:

- стандартный МЭ SPI
- встроенная система IPS
- система контроля приложений
- Дополнительная информация об угрозах

Шлюзы безопасности ViPNet



Два NGFW в портфолио

xFirewall, Coordinator HW 5

ФСТЭК России

- Межсетевой экран тип «А» и тип «Б» 4 класса
- СОВ уровня сети 4 класса
- 4-й уровень доверия средств защиты информации
- Многофункциональный межсетевой экран уровня сети NEW

Coordinator HW 5

ФСБ России

- СКЗИ класса КС1-КС3
- Межсетевой экран 4 класса

Минцифры России

- В реестре российского ПО

Основные модули безопасности

Application Control

IDS/IPS

VPN

Аутентификация пользователей

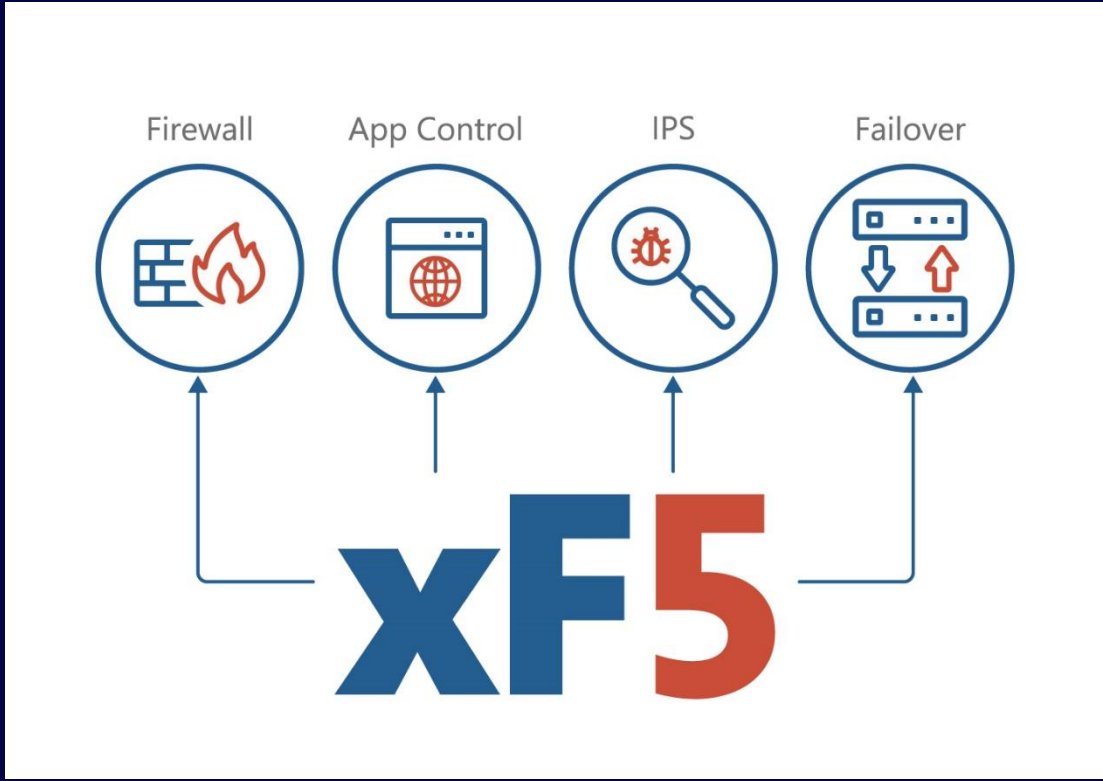
Фильтрация по URL

Инспектирование TLS

Антивирус

Антиспам

ViPNet xFirewall 5



Модельный ряд xFirewall

Тестирование по RFC-2544 UDP 1514 byte

xF65000

xF5000

xF1000 C/D

xF100

76 000 Мбит/с

45 000 Мбит/с

7 600 Мбит/с

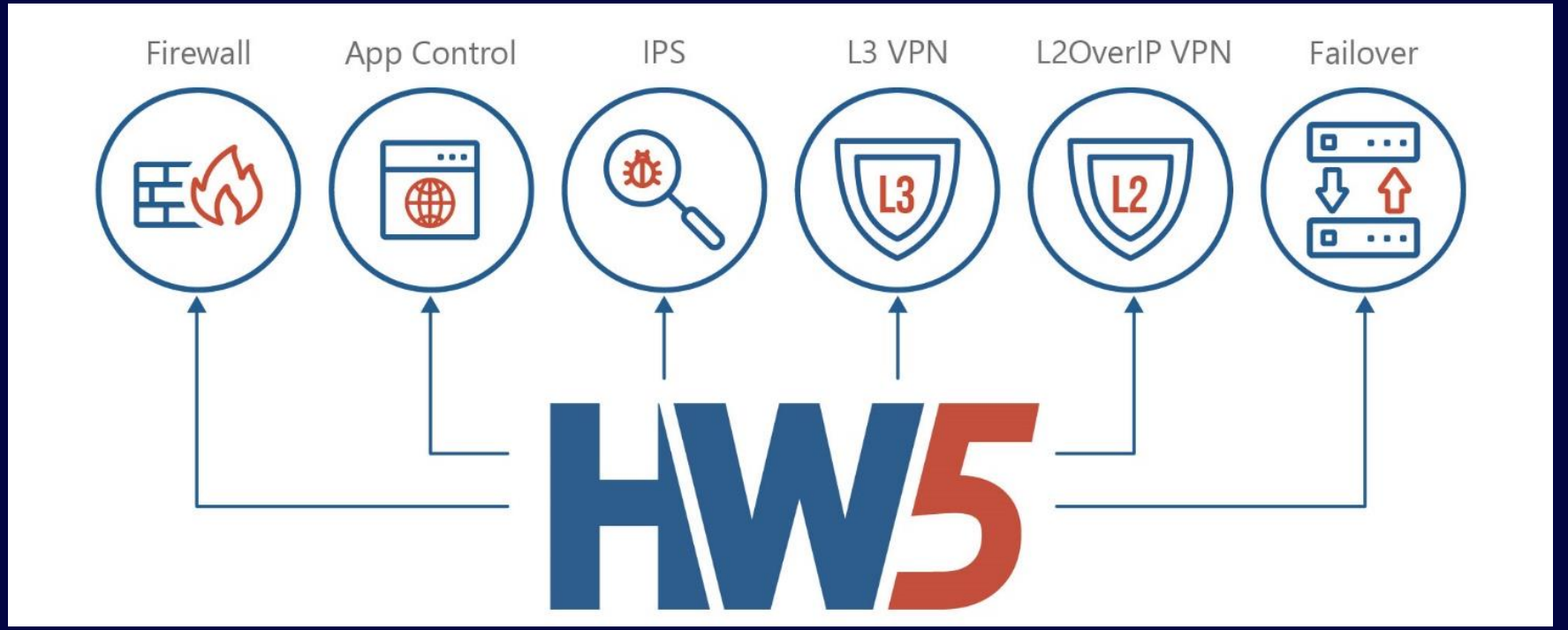
1 600 Мбит/с

Малый и средний бизнес

Крупные предприятия

ЦОД

ViPNet Coordinator HW 5



ViPNet Coordinator HW

Тестирование VPN по RFC-2544 UDP 1514 byte

ViPNet xFirewall версии 5.6.4

Что нового в 5.6.4

1. Улучшенный механизм SSL/TLS-инспекции
2. Расширение возможностей агрегированных интерфейсов
3. Улучшенный пользовательский интерфейс
4. Поддержка новых аппаратных платформ

Что нового в 5.6.4

5 RADIUS-аутентификация для SSH-подключений

6 Сброс к заводским настройкам

7 Повышена скорость и стабильность отправки CEF-сообщений

8 Исправление ошибок

xF100 Q1/Q2

6 сетевых интерфейсов:

- 4 x 1 Гбит/сек RJ45
- 2 x 1 Гбит/сек SFP

Незначительно повысилась производительность

Производительность

Исполнение	xF100 N1	xF100 Q1/Q2
Firewall, 1518 Байт UDP (Мбит/сек)	722	**1 600**
Firewall, TCP Multistream (Мбит/сек)	600	**1 380**
AppControl (Firewall+DPI), (Мбит/сек)	180	**395**
NGFW (FW+DPI+IPS) (Мбит/сек)	13	**40**
NGFW+SSL Inspection (1МБ)	32	50
Firewall Throughput (UDP 64 Байт)	79 000	**137 000**
Connections per Second	10 000	**18 000**
Concurrent Connections	149 993	499 994

Производительность

Исполнение	xF1000 Q7/Q8	xF5000 Q2
Firewall, 1518 Байт UDP (Мбит/сек)	7 600	51 000
Firewall, TCP Multistream (Мбит/сек)	11 000	33 000
AppControl (Firewall+DPI), (Мбит/сек)	2 600	7 800
NGFW (FW+DPI+IPS) (Мбит/сек)	480	1 300
NGFW+SSL Inspection (1МБ)	480	1 300
Firewall Throughput (UDP 64 Байт)	2 200 000	4 000 000
Connections per Second	53 000	106 000
Concurrent Connections	4 999 000	29 999 990

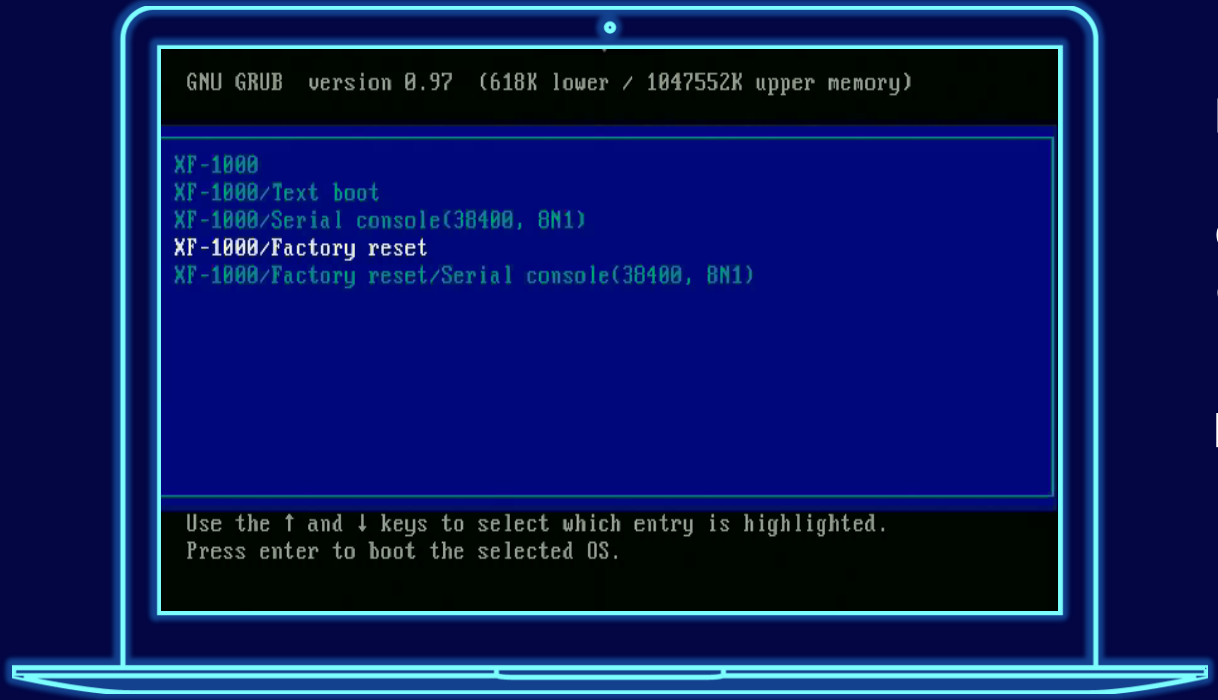
Radius-аутентификация

- Чтобы пользователь подключался к ViPNet xFirewall в режиме администратора, установите значение атрибута shell:priv-lvl равным 15.
- При другом значении атрибута shell:priv-lvl или при его отсутствии подключение будет выполняться в режиме пользователя.

Возможность возврата к предыдущей версии ViPNet xFirewall

В ViPNet xFirewall добавлена возможность возврата ПО к версии 5.4.0

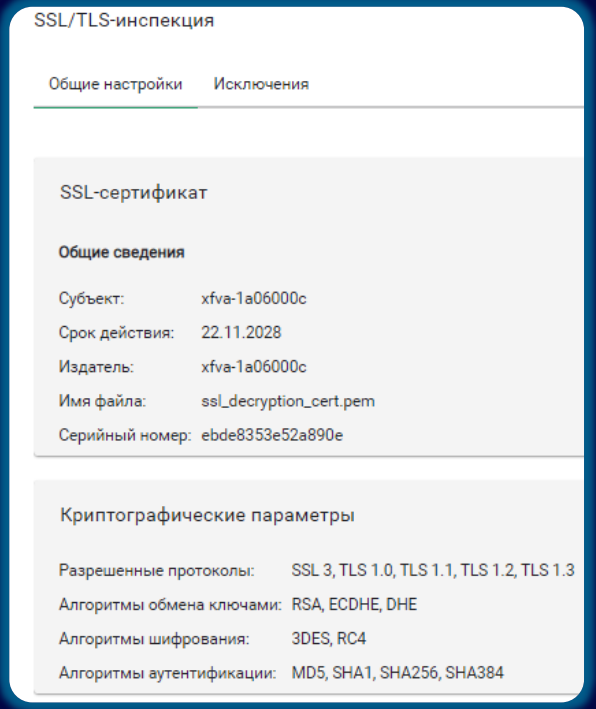
Сброс к заводским настройкам



В строке Are you sure you want to execute this command and delete key? Введите

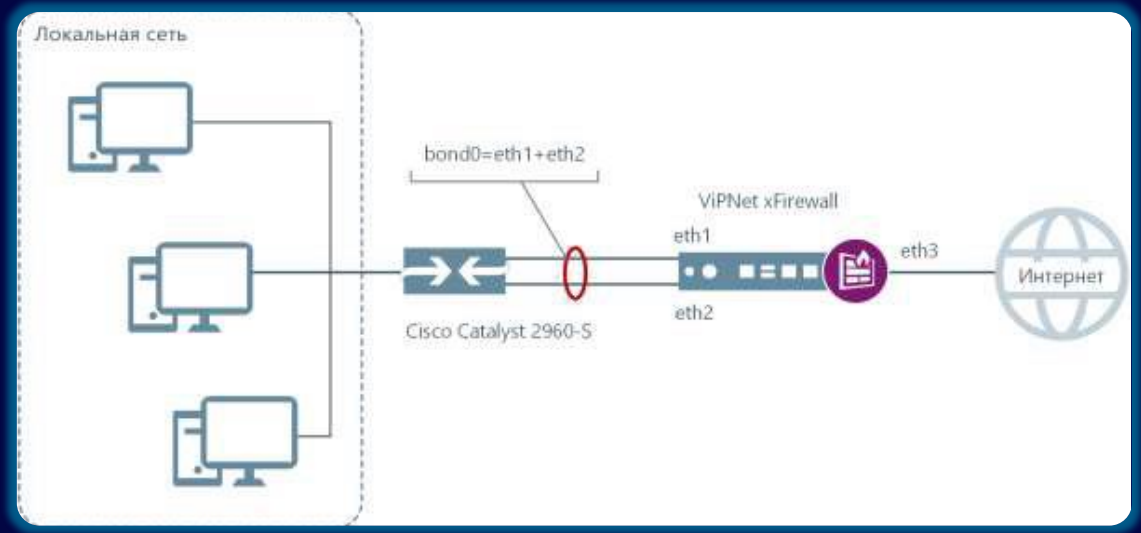
Delete нажмите Enter.

Улучшения SSL Inspection



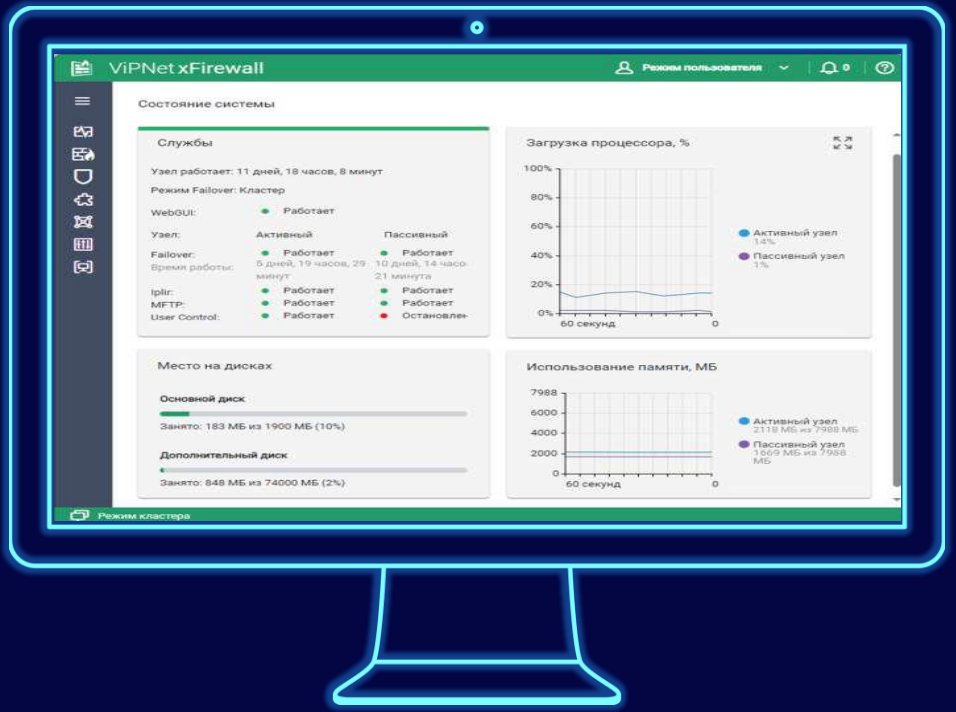
- Добавлена поддержка расшифровывания протокола TLS 1.3
- Добавлена возможность инспекции трафика HTTP/2
- Добавлены настройки доверия к сертификатам ресурсов:
  - проверка срока действия сертификатов;
  - проверка полей сертификата, определяющих его использование (key usage, extended key usage);
  - проверка самоподписанных сертификатов.
- Исключать из инспекции веб-ресурсы, используя их альтернативные имена (SAN – Subject Alternative Names) и поддомены (wildcard).

Агрегация интерфейсов



- Ранее вы могли включать в состав агрегированного интерфейса только до трех подчиненных физических. Теперь это ограничение снято.
- Максимальное количество агрегированных интерфейсов увеличено до 8.

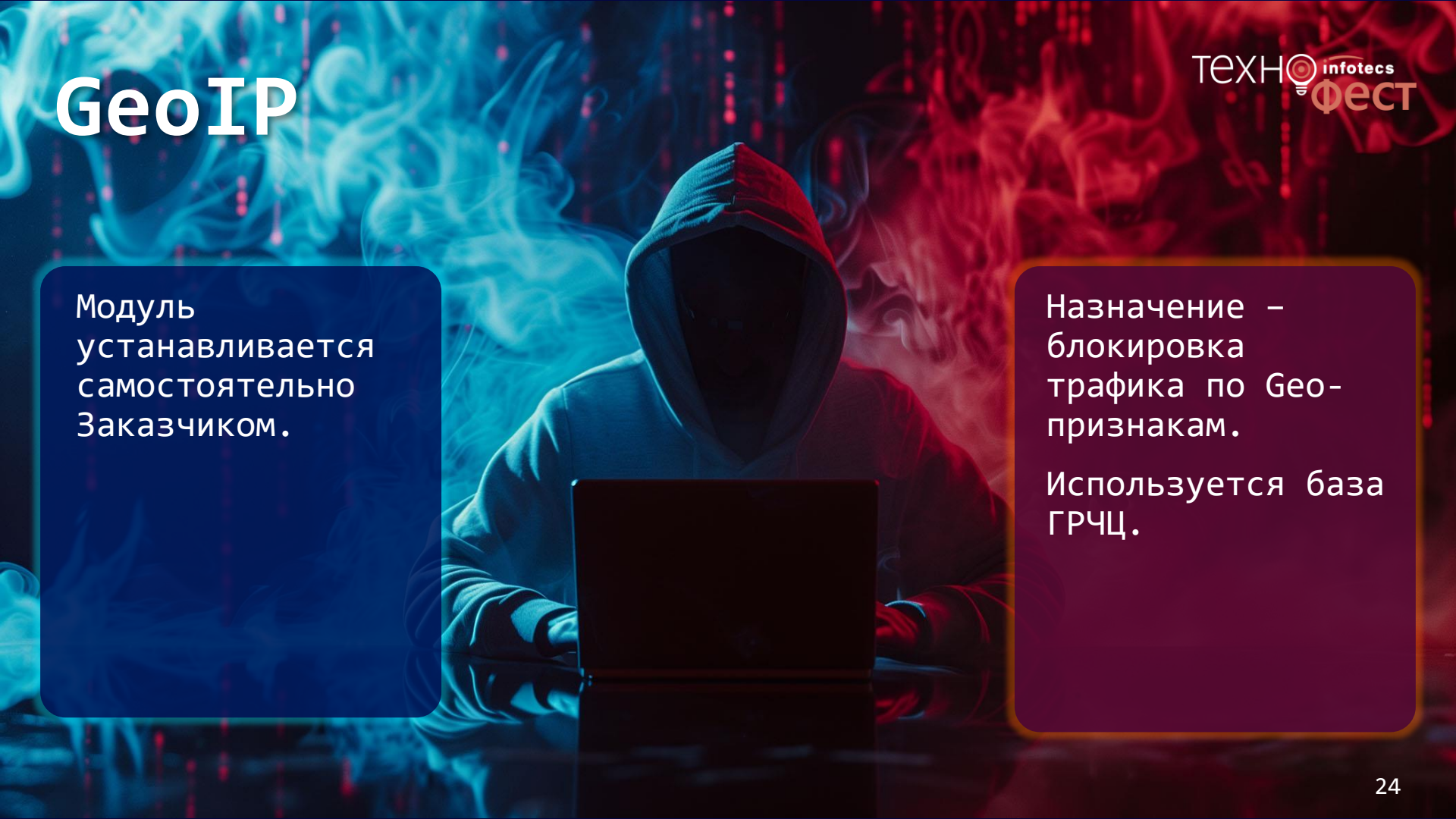
Изменен вывод контролируемых параметров



Теперь отображается относительная загрузка CPU, а максимальная загрузка всех ядер принята за 100%.

ViPNet xFirewall Add-ons

GeoIP



Модуль устанавливается самостоятельно Заказчиком.

Назначение – блокировка трафика по Geo-признакам.

Используется база ГРЧЦ.

Принципы GeoIP-фильтрации трафика

Модуль GeoIP-фильтрации

Модуль ViPNet xFirewall, позволяющий разграничивать доступ на основе геолокации. Блокирует входящий трафик из заданных регионов.

Первый этап анализа трафика

Это снижает долю трафика, анализируемого DPI, IPS, что повышает эффективность межсетевого экрана.

Белый список

Можно исключить из GeoIP-фильтрации отдельные IP-адреса или подсети.

Next

Прошедший GeoIP-фильтрацию трафик обрабатывается другими подсистемами межсетевого экрана.

ViPNet xFirewall
xF65000
Межсетевой экран
для защиты ЦОДов

Исполнение xF65000

- 2U платформа производства Аквариус
- 4 x 1Gb RJ-45
- 4 x 1Gb SFP
- 8 x 10Gb SFP+
- 2 БП

Новые возможности

1

Высокая производительность
85 тыс. правил
DPI+IPS без деградации

2

HA-Cluster
Синхронизация сессий

Переключение за 1 сек

3

Динамическая маршрутизация
BGP
OSPF

4

Шлюзовой антивирус
Прокси-сервер
Поддержка ICAP

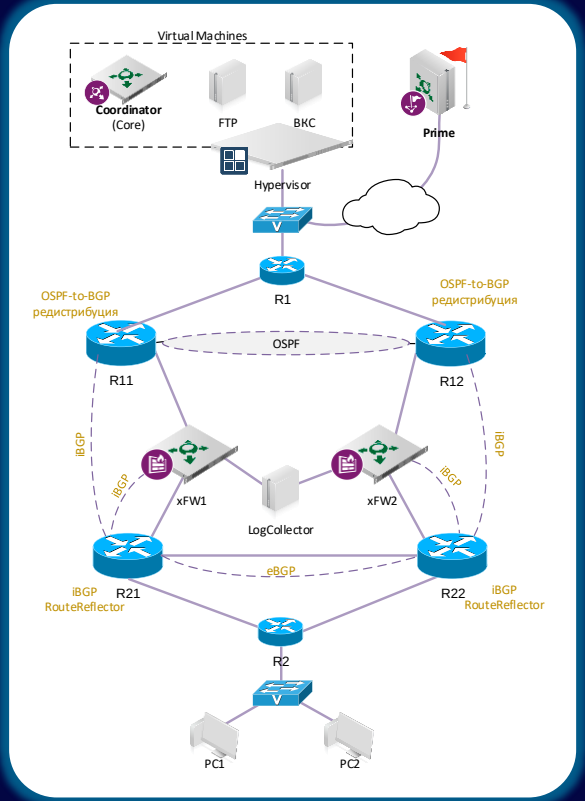
5

Резервирование
2 блока питания

Поддержка BFD

BGP. Моделирование переключения кластера

- Отключение питания активной ноды xFW1
- Проверить изменение таблицы маршрутизации на xFW1
- Проверить трассировку с PC1 до тестового сервиса (сервер BKC\FTP). Выведен список хопов через R11 и R21
- На узле PC1 видео-поток не остановился
- Включение питания активной ноды xFW 2
- Проверить изменение таблицы маршрутизации на xFW1
- Проверить трассировку с PC1 до тестового сервиса (сервер BKC\FTP). Выведен список хопов через R11 и R21
- На узле PC1 видео-поток не остановился



Сравнение производительности

Checkpoint 28000

Firewall	Next Gen Firewall
145 Гбит/сек	51,5 Гбит/сек

ViPNet xFirewall xF65000

Firewall	Next Gen Firewall
76 Гбит/сек	60 Гбит/сек

HW 5

Требования по сертификации

инфотекс

ФСБ России

- СКЗИ класса КС1-КС3
- Межсетевой экран 4 класса

ФСТЭК России

- Межсетевой экран тип «А» и тип «Б» 4 класса
- СОВ уровня сети 4 класса
- 4-й уровень доверия средств защиты информации
- Многофункциональный межсетевой экран уровня сети NEW

Минцифры России

- В реестре российского ПО

VPN с ГОСТ шифрованием

- VPN-шлюз сетевого уровня (L3 VPN)
- VPN-шлюз канального уровня (L2OverIP VPN)
- Remote Access VPN (ViPNet Client)
- «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018) NEW
- ГОСТ 28147-89 для обратной совместимости
- IPlir 6 – протокол безопасности сетевого уровня NEW

Многофункциональный МЭ

Аппаратные платформы

инфотекс

HW50

HW100

Малые офисы и филиалы

HW1000

HW1000 C

HW1000 D

Предприятия среднего бизнеса

HW2000

HW5000

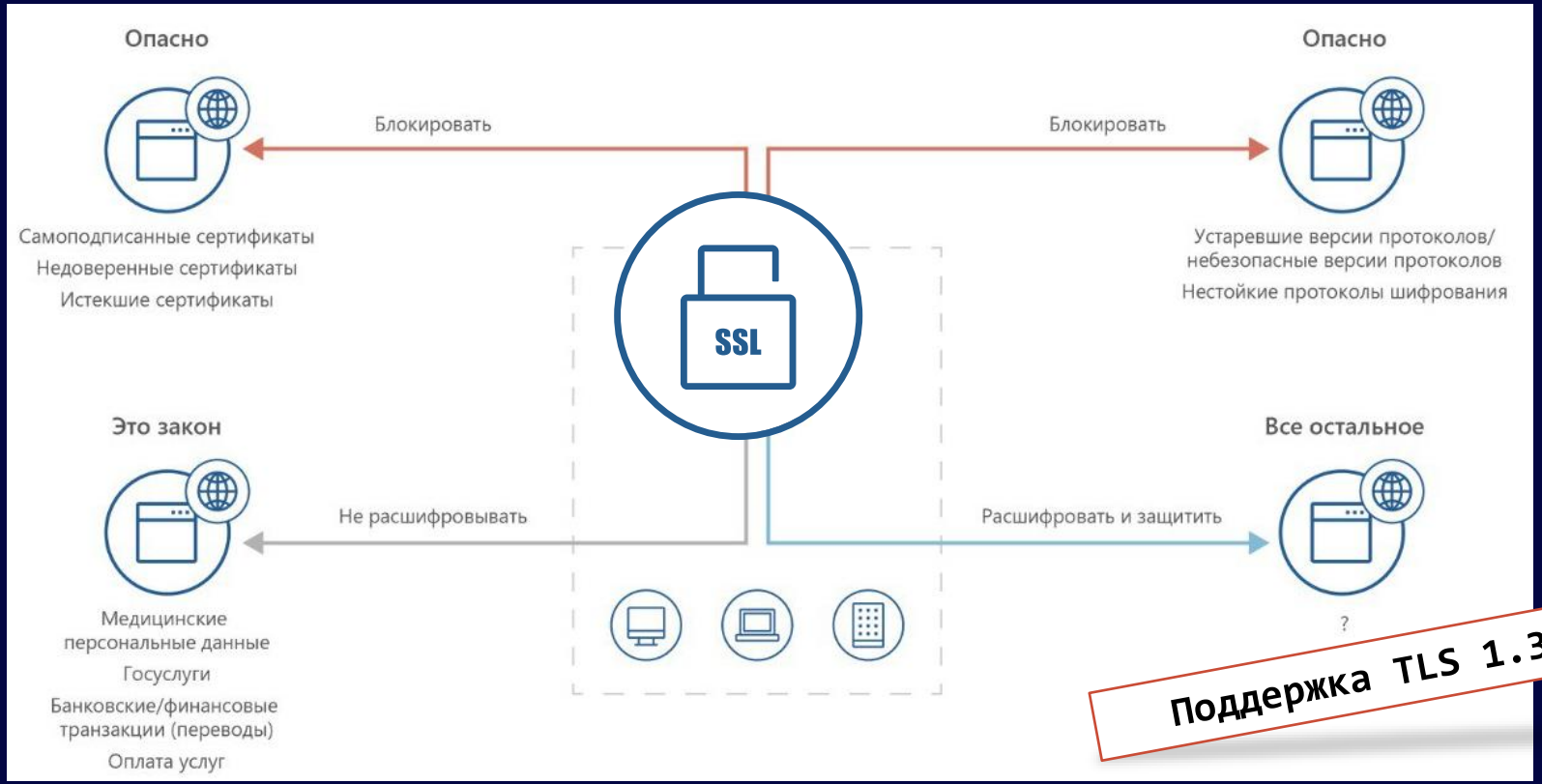
Крупные предприятия, ЦОД

ViPNet Coordinator HW 5.4/5.5

- SSL/TLS-инспекция
- URL-фильтрация
- Блокировка по GEO-IP
- Встроенный антивирус
- Проверка состояния связи между шлюзами
- Локальные учетные записи + новая роль
- Интеграция ViPNet SafeBoot

Идет сертификация

SSL/TLS-инспекция



Источник баз URL-категорий

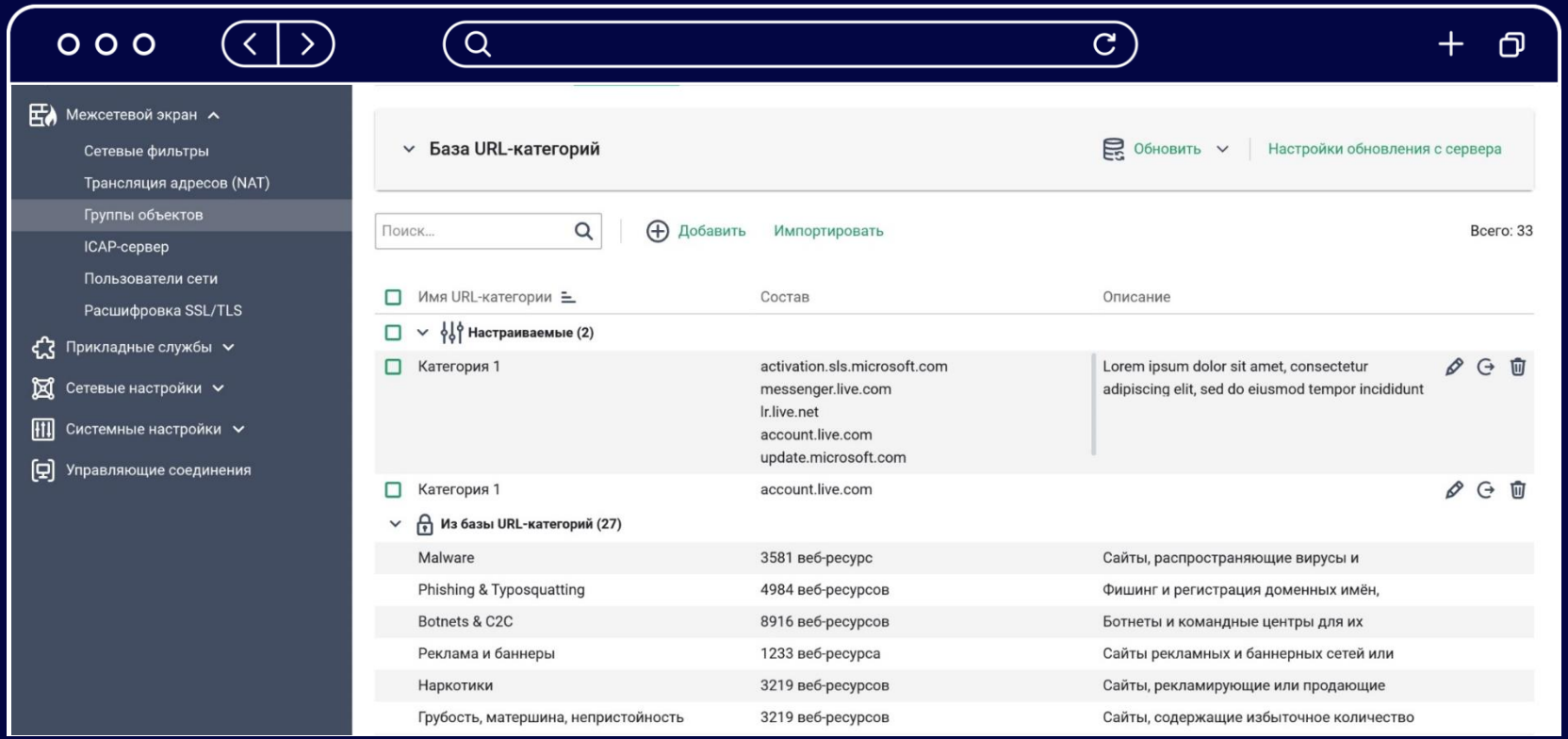
инфотекс

~100 млн веб-ресурсов

80 категорий

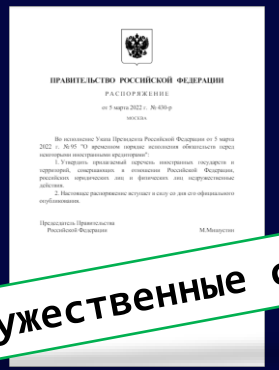
+15% ежемесячный прирост базы

URL-фильтрация

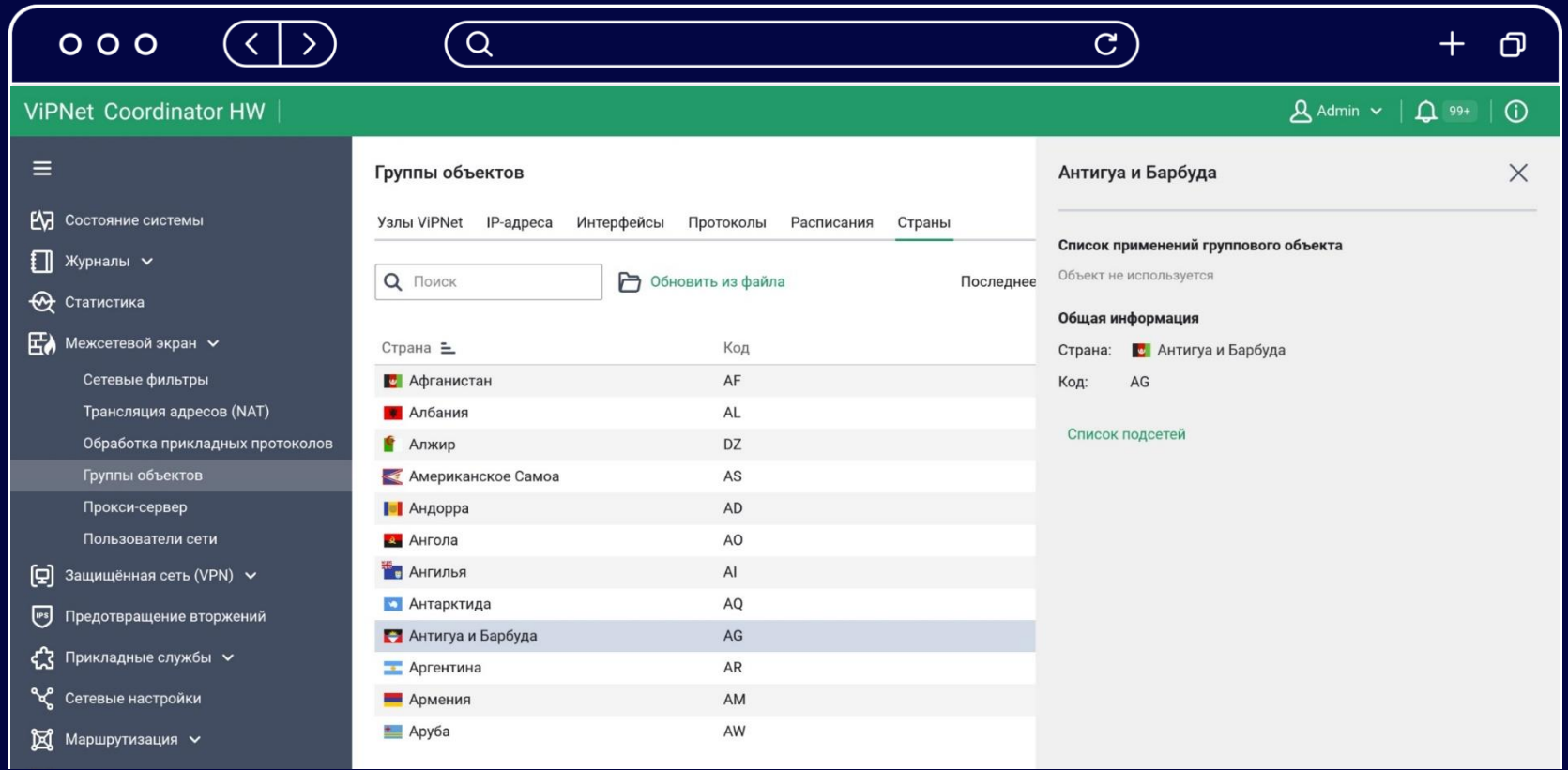


Блокировка по GEO-IP

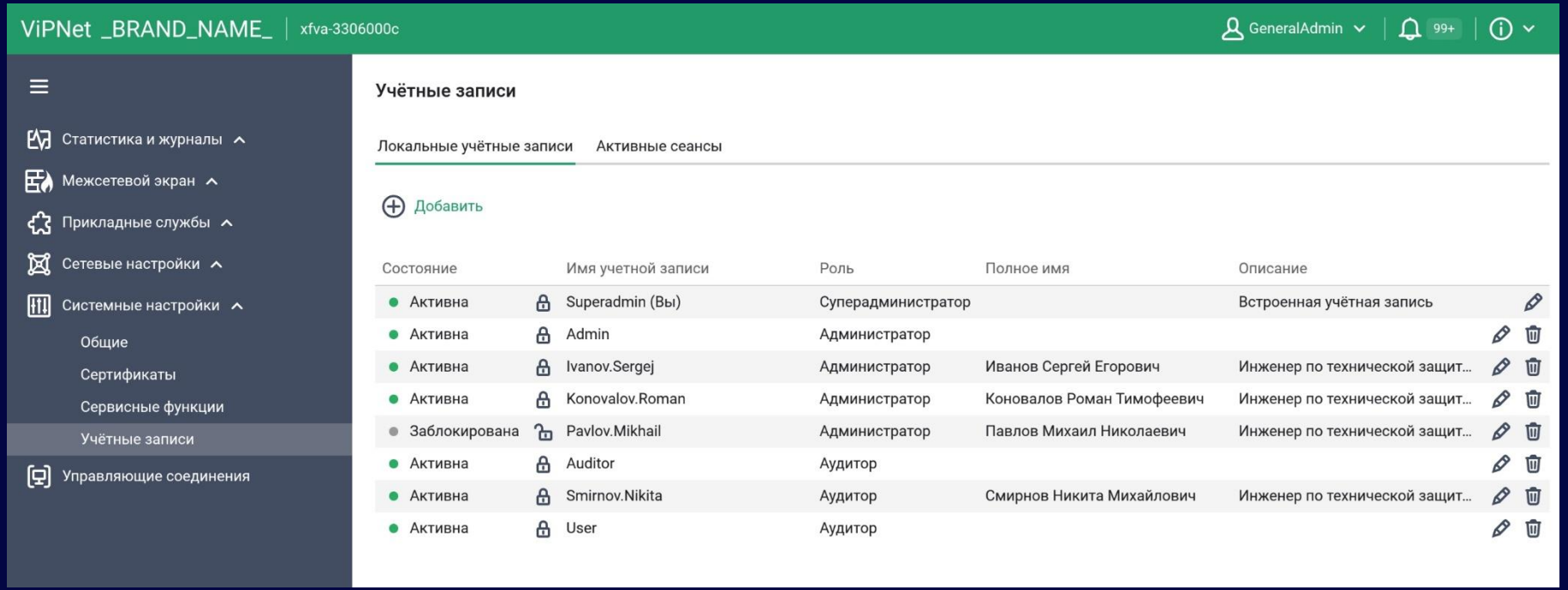
- Фильтрация трафика на основе данных о географической принадлежности отправителей
- Использование доверенной базы геолокации IP-адресов на базе «Главного радиочастотного центра» (ФГУП «ГРЧЦ»)



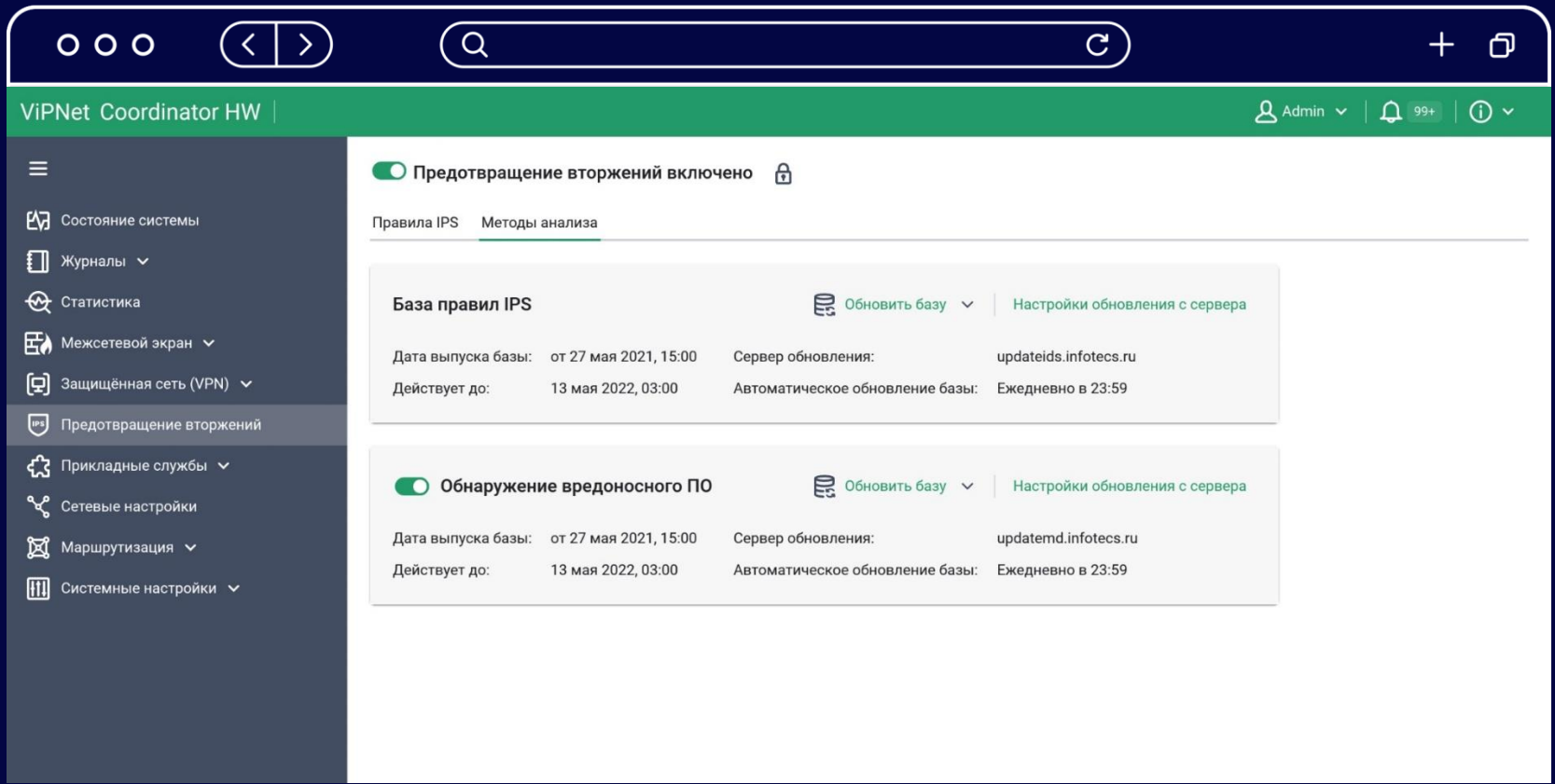
Блокировка по GEO-IP



Локальные учетные записи



Обнаружение вредоносного ПО



Спасибо за внимание!

Подписывайтесь на наши соцсети

https://vk.com/infotecs_news

https://t.me/infotecs_news