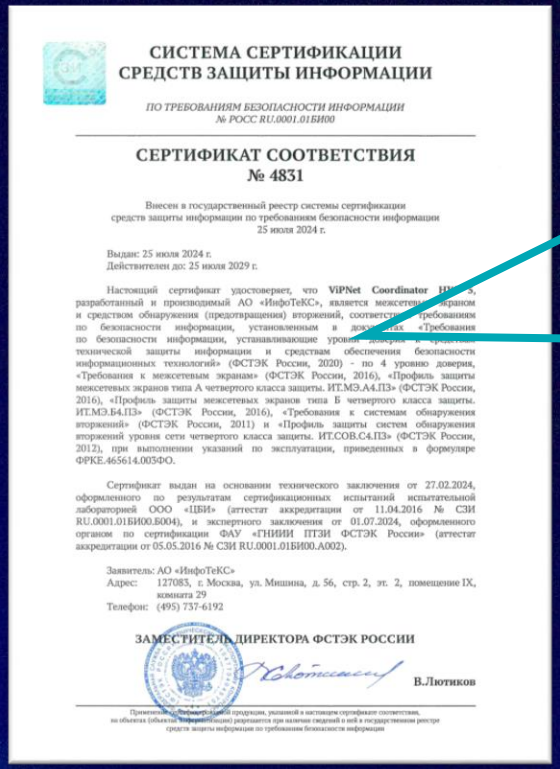
ViPNet Coordinator HW 5 – новое поколение шлюзов безопасности

Виталий Беличко
Ведущий менеджер продуктов

ViPNet Coordinator HW 5

Типовая схема применения HW 5

Сертификат ФСТЭК России (МЭ и СОВ)



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4831

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
25 июля 2024 г.

Выдан: 25 июля 2024 г.
Действителен до: 25 июля 2029 г.

Настоящий сертификат удостоверяет, что **ViPNet Coordinator HW 5**, разработанный и производимый АО «ИнфоТеКС», является межсетевым экраном и средством обнаружения (предотвращения) вторжений, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012), при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.465614.003ФО.

Сертификат выдан на основании технического заключения от 27.02.2024, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004), и экспертного заключения от 01.07.2024, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «ИнфоТеКС»
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX, комната 29
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение (использование) данной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4831

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
25 июля 2024 г.

Выдан: 25 июля 2024 г.
Действителен до: 25 июля 2029 г.

Настоящий сертификат удостоверяет, что **ViPNet Coordinator HW 5**, разработанный и производимый АО «ИнфоТеКС», является межсетевым экраном и средством обнаружения (предотвращения) вторжений, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012), при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.465614.003ФО.

Сертификат ФСБ России (СКЗИ КС3)

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4972 от "30" августа 2024 г.

Действителен до "30" августа 2027 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программно-аппаратный комплекс ViPNet Coordinator HW 5 (исполнения: ViPNet Coordinator HW50 на аппаратных платформах: HW50 N1, HW50 N2, HW50 N3, HW50 N4; ViPNet Coordinator HW100 на аппаратных платформах: HW100 N1, HW100 N2, HW100 N3; ViPNet Coordinator HW1000 на аппаратных платформах: HW1000 Q4, HW1000 Q7; ViPNet Coordinator HW1000 C на аппаратных платформах: HW1000 Q5, HW1000 Q8; ViPNet Coordinator HW1000 D на аппаратных платформах: HW1000 Q6, HW1000 Q9; ViPNet Coordinator HW2000 на аппаратных платформах: HW2000 Q4, HW2000 Q5; ViPNet Coodinator HW5000 на аппаратных платформах: HW5000 Q1, HW5000 Q2) в комплектации согласно формуляру ФРКЕ.465614.003ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3 и может использоваться для криптографической защиты (шифрование и имитозащита данных, передаваемых в IP-пакетах по общим сетям передачи данных) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов продукции №№ 1056А-000501, 1056Б-000501, 1056В-000501, 1056В1-000501, 1056В2-000501, 1056Г-000501, 1056Д-000501.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.465614.003ТУ, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.465614.003ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России О.В. Скрябин

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4972 от "30" августа 2024 г.

Действителен до "30" августа 2027 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программно-аппаратный комплекс ViPNet Coordinator HW 5 (исполнения: ViPNet Coordinator HW50 на аппаратных платформах: HW50 N1, HW50 N2, HW50 N3, HW50 N4; ViPNet Coordinator HW100 на аппаратных платформах: HW100 N1, HW100 N2, HW100 N3; ViPNet Coordinator HW1000 на аппаратных платформах: HW1000 Q4, HW1000 Q7; ViPNet Coordinator HW1000 C на аппаратных платформах: HW1000 Q5, HW1000 Q8; ViPNet Coordinator HW1000 D на аппаратных платформах: HW1000 Q6, HW1000 Q9; ViPNet Coordinator HW2000 на аппаратных платформах: HW2000 Q4, HW2000 Q5; ViPNet Coodinator HW5000 на аппаратных платформах: HW5000 Q1, HW5000 Q2) в комплектации согласно формуляру ФРКЕ.465614.003ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3 и может использоваться для криптографической защиты (шифрование и имитозащита данных, передаваемых в IP-пакетах по общим сетям передачи данных) информации, не содержащей сведений, составляющих государственную тайну.

Требования по сертификации

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

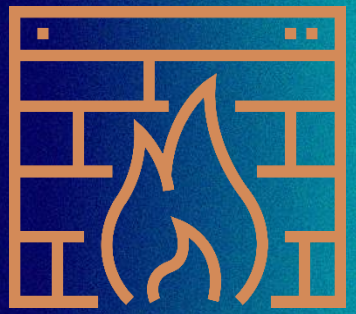
Минцифры России и Минпромторг России
- В реестре российского ПО и реестре РЭП

Минцифры России

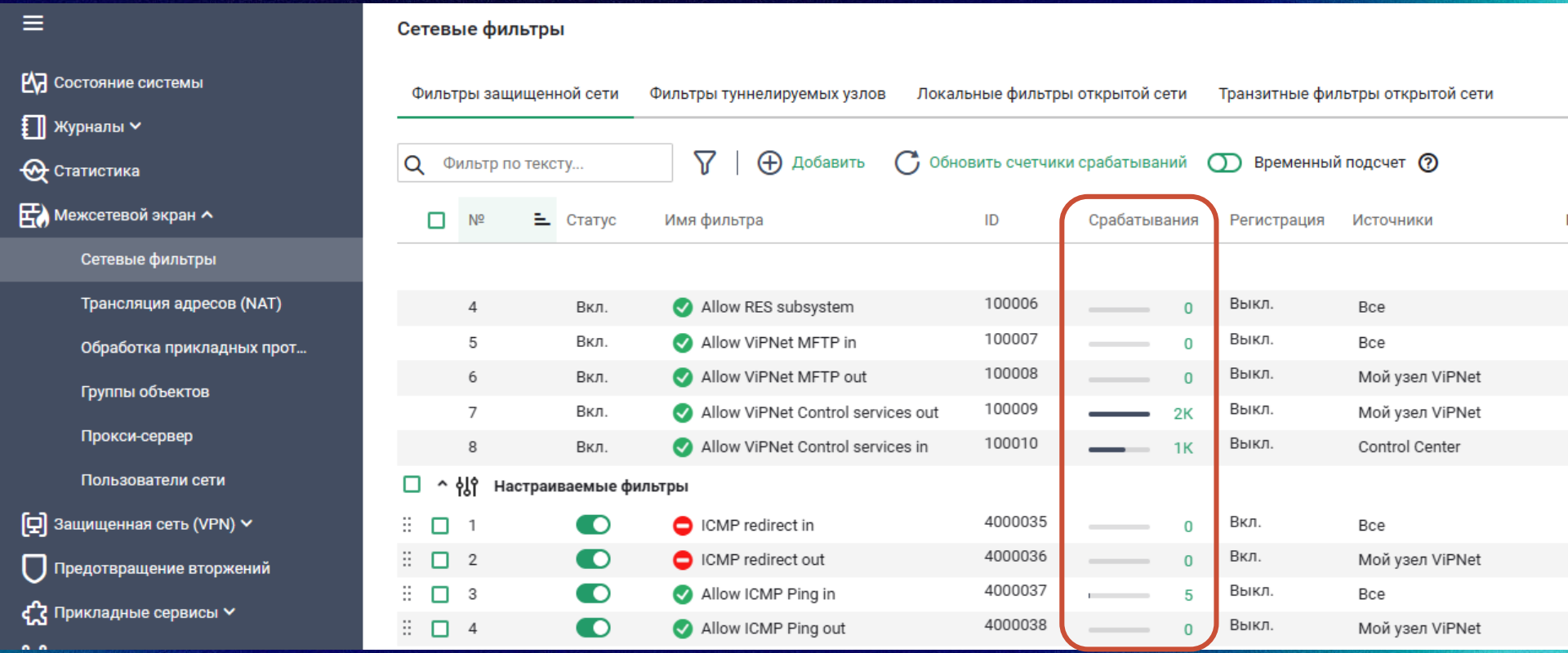
МИНПРОМТОРГ РОССИИ

Межсетевое экранирование

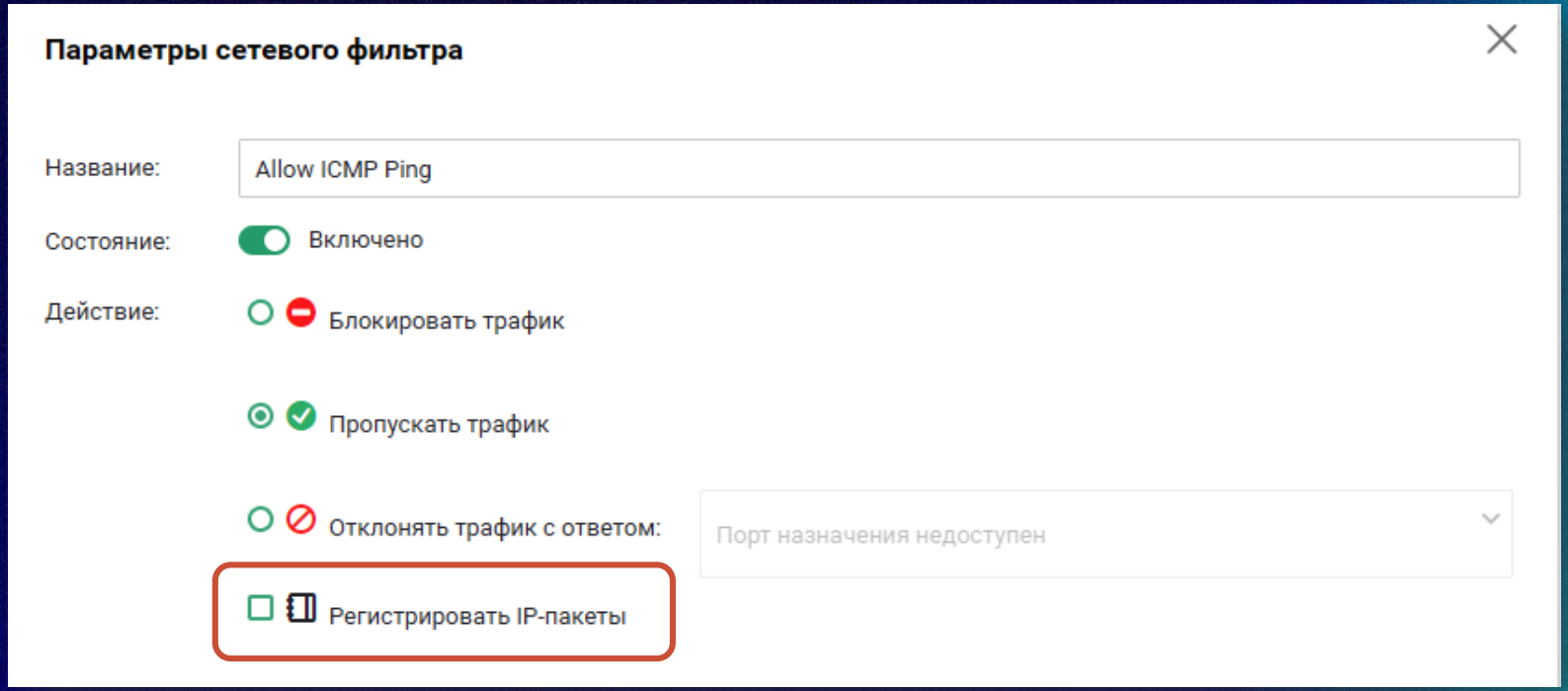
- Внедрение технологии DPI (контроль приложений)
- Идентификация пользователей с использованием:
  - Microsoft Active Directory
  - Captive Portal с LDAP каталогом
- Повышение производительности МЭ
- Идентификация правил МЭ
- Счетчики срабатывания правил МЭ



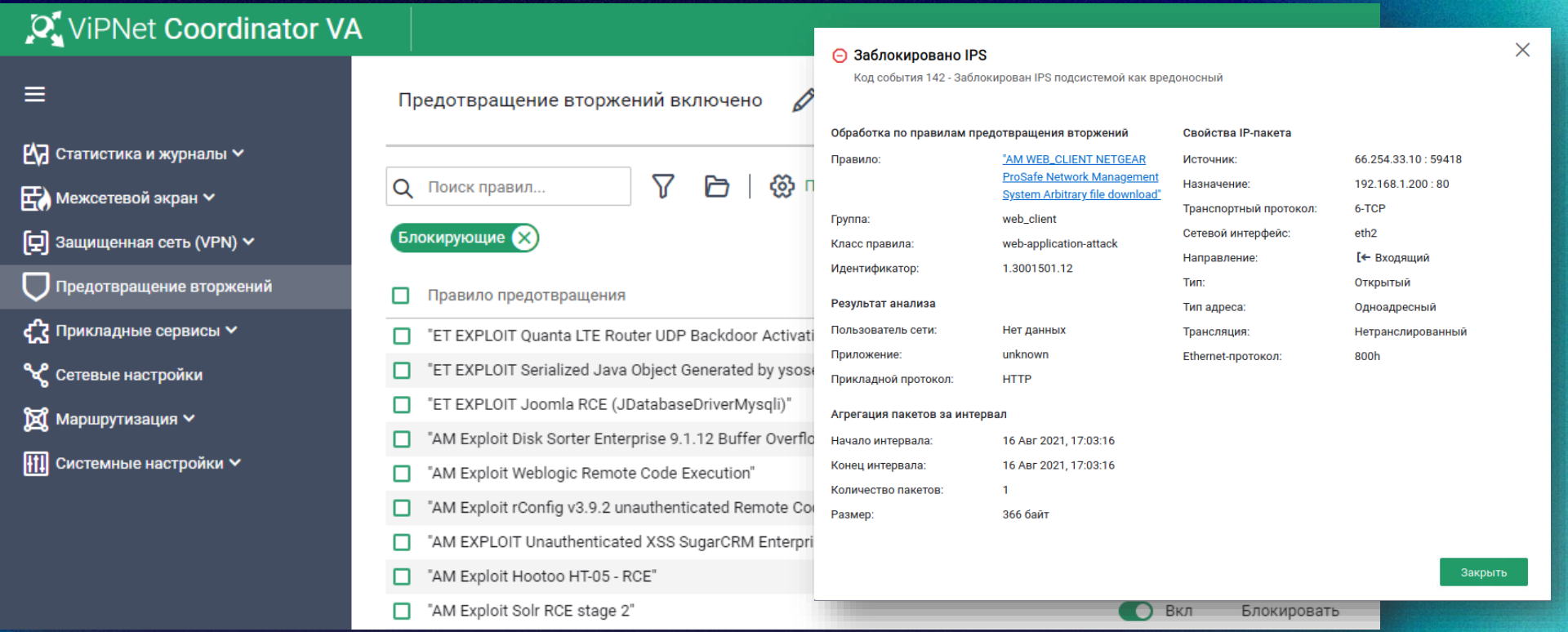
Счетчики срабатывания правил МЭ



Выборочное логирование правил МЭ



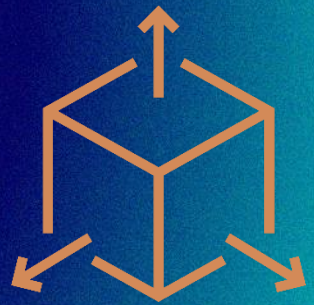
Предотвращение вторжений (IPS)



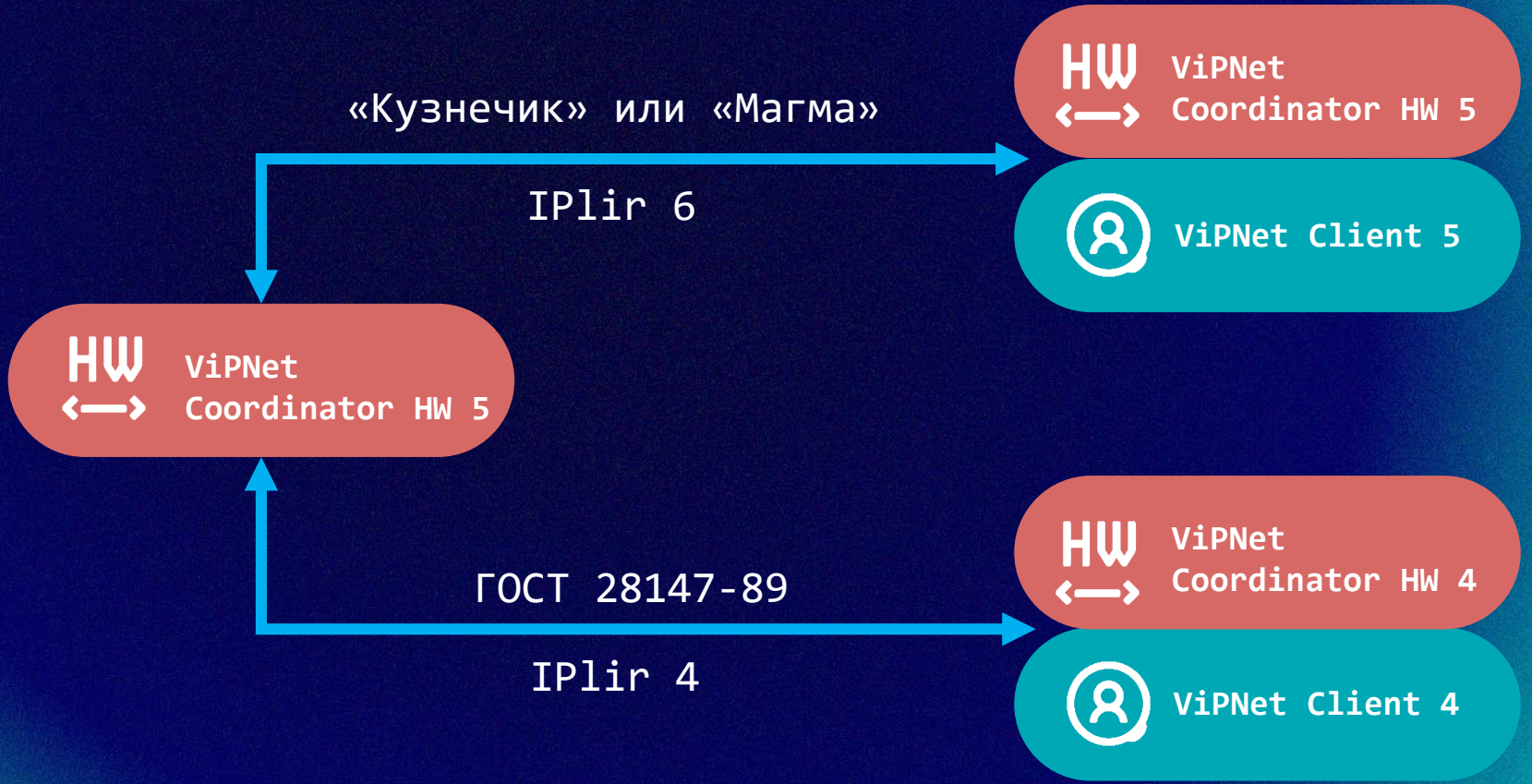
Криптография (VPN)

- «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- ГОСТ 28147-89 для обратной совместимости
- IPlir 6 – протокол безопасности сетевого уровня

ТК 26 Р 1323565.1.034-2020 «Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня»

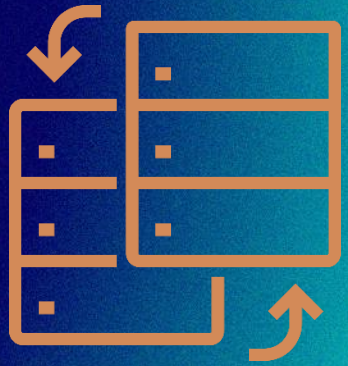


Обратная совместимость



Кластер высокой доступности

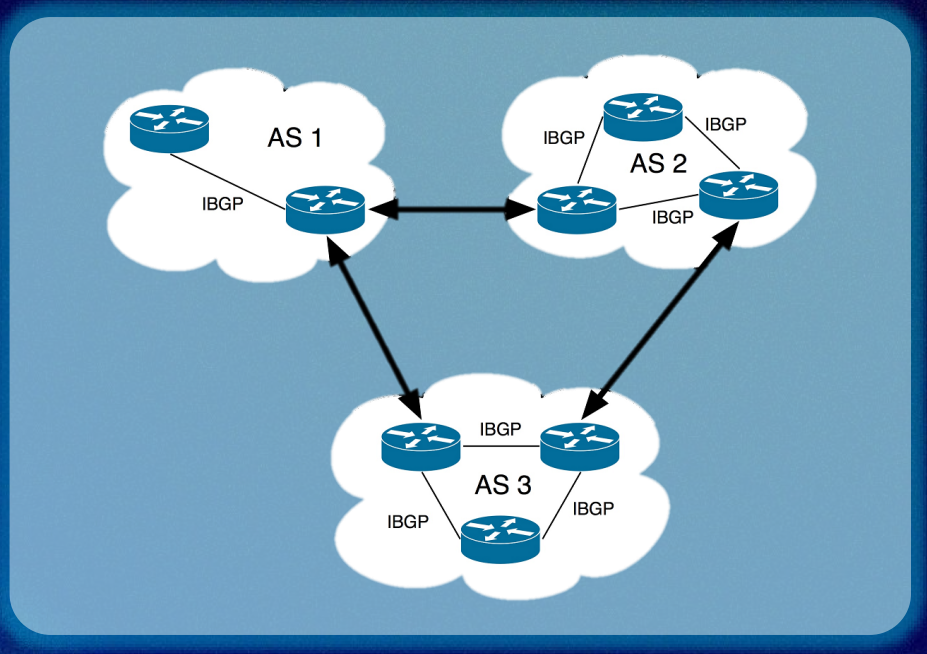
- Быстрое переключение кластера по потере связи и питания
- Синхронизация сессий МЭ в кластере
- Виртуальный MAC-адрес для кластера
- Синхронизация времени пассивного узла кластера
- Минимальное время переключения кластера сократилось до 1 секунды



Сетевые функции

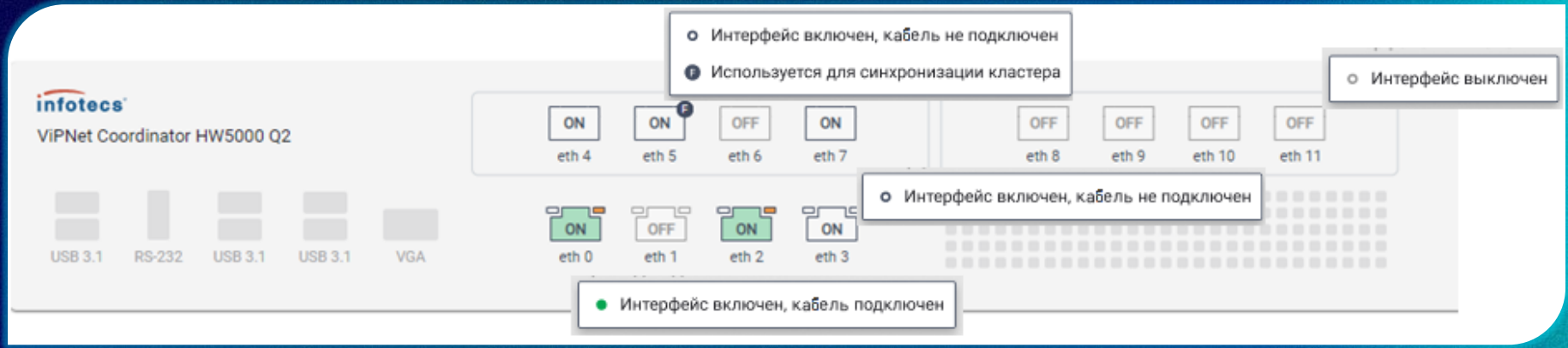
- Расширенная статическая маршрутизация (Policy based routing)
- Динамическая маршрутизации (OSPF, BGP)
- Поддержка VLAN
- Агрегирование сетевых интерфейсов (802.3ad, LACP)
- Поддержка Jumbo-кадров и Path MTU Discovery
- Приоритизация трафика (QoS, ToS, DiffServ)
- Встроенный DCHP-, DNS-, NTP-сервер
- SNMP, Syslog, Syslog (CEF), SSH, HTTPS

Поддержка протокола BGP



- Создание BGP-окружения или встраивание узла в существующее
- Получение и использование маршрутов по протоколу BGP
- Анонсирование и перераспределение маршрутов
- Балансировка трафика (ECMP, UCMP)

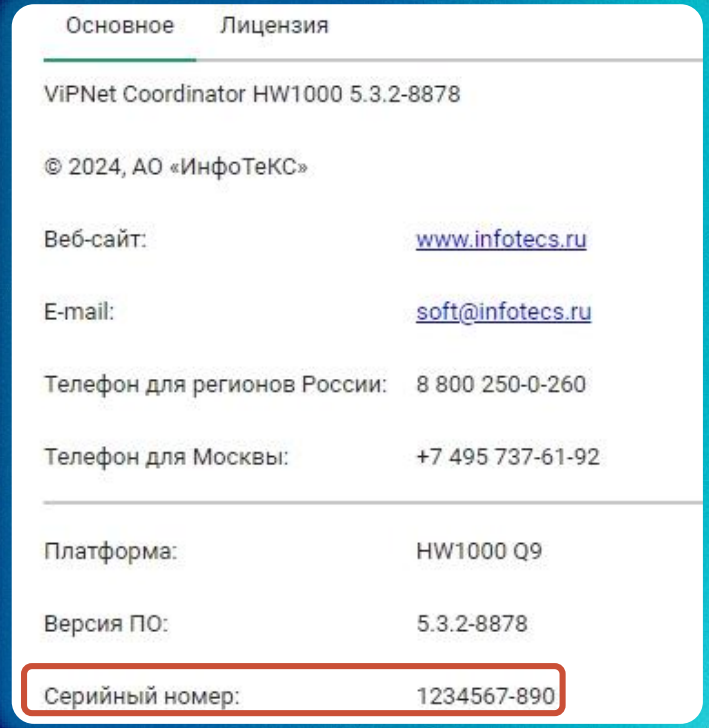
Визуализация сетевых интерфейсов



Серийный номер платформы

- Добавление серийного номера при производстве и пользователем самостоятельно
- Отображение в CLI, WebUI
- Передача данных по SNMP

```
HW1000Q9-node-1# version
Product: ViPNet Coordinator HW
Platform: HW1000 Q9
Serial number: 1234567-890
License: HW1000 D
Software version: 5.3.2-8878
```



Новая система управления

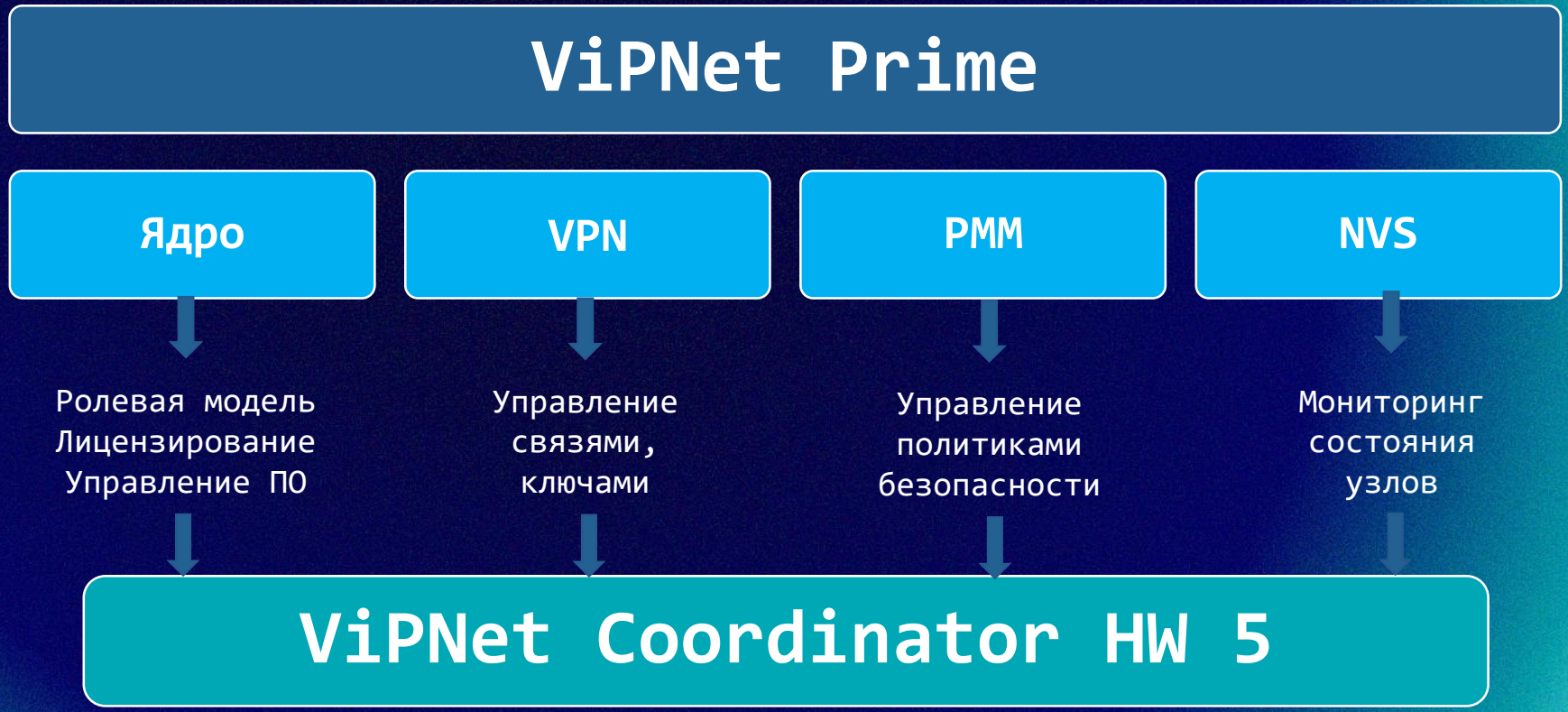
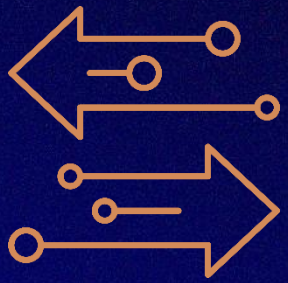


Схема лицензирования

Изменение ролевой модели

ViPNet Coordinator HW 4

- Пользователь
- Администратор узла
- Администратор группы узлов
- Администратор сети



ViPNet Coordinator HW 5

Локальные учетные записи:

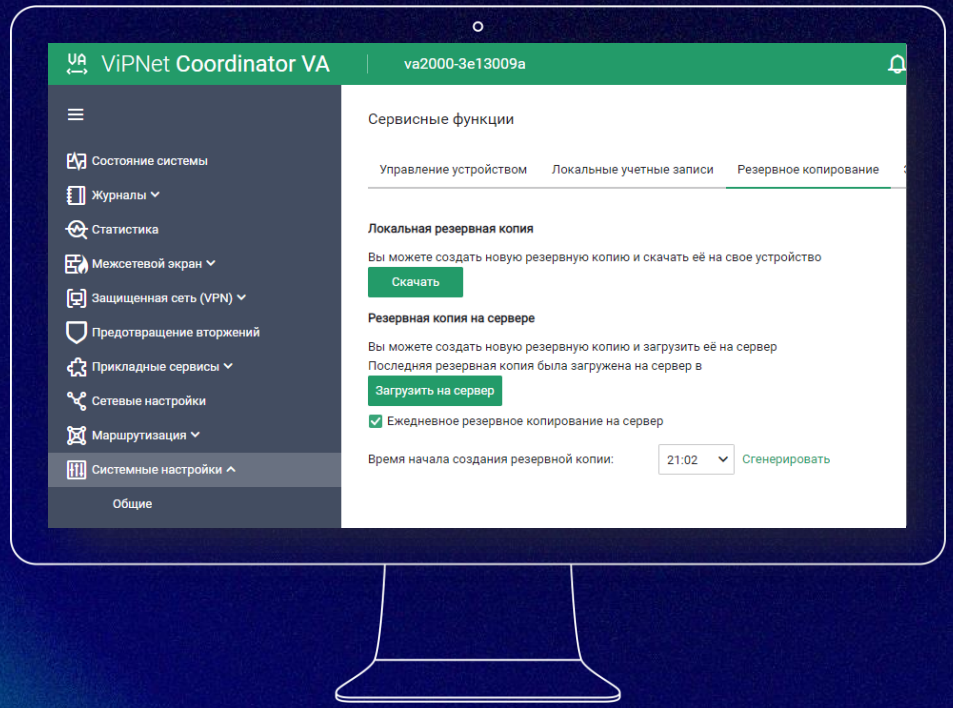
- Администратор
- Пользователь (Аудитор)

+

Централизованные учетные записи:

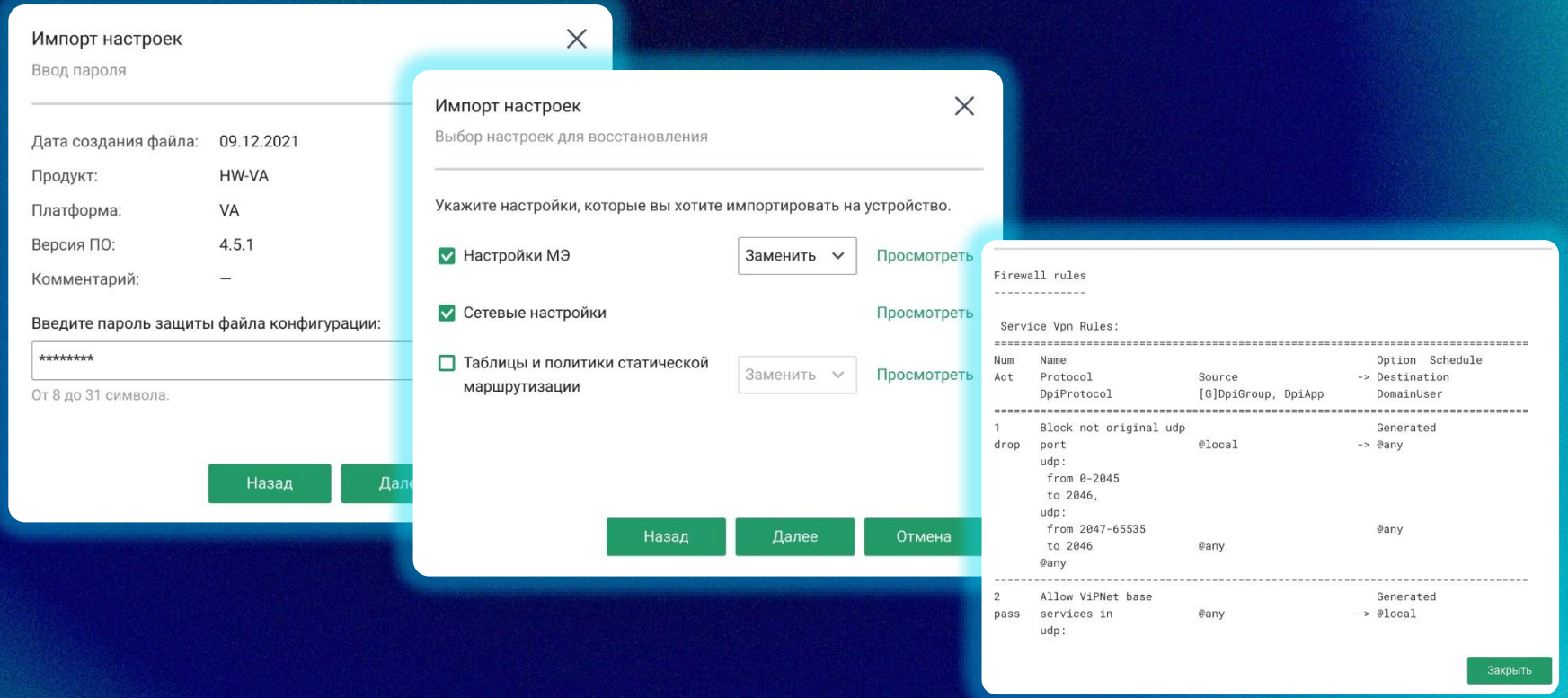
- Неограниченное количество
- Администратор/Аудитор
- Single Sign-On (SSO)

Резервное копирование



- Локальный экспорт на USB
- Удаленный экспорт через WebUI
- Выгрузка на сервер Prime

Перенос настроек с любой платформы



Аппаратные платформы

HW50

HW100

Малые офисы и филиалы

HW1000

HW1000 C

HW1000 D

Предприятия среднего бизнеса

HW2000

HW5000

Крупные предприятия, ЦОД

Поддержка аппаратных платформ

ViPNet Coordinator HW50

- HW50 N1*/N2*/N3*/N4*
- HW50 A1 DEV

ViPNet Coordinator HW100

- HW100 N1/N2/N3
- HW100 Q1/Q2 NEW

ViPNet Coordinator HW2000

- HW2000 Q4
- HW2000 Q5

ViPNet Coordinator HW1000

- HW1000 Q4*/Q5/Q6
- HW1000 Q7/Q8/Q9

ViPNet Coordinator HW5000

- HW5000 Q1
- HW5000 Q2

* - режим BASE only

HW100 Q1/Q2

- 4x 1G RJ-45 / 2x 1G SFP
- 2x USB, Console, VGA
- Внешний БП
- 250 x 44 x 227 ШхВхГ (мм)
- 1,9 кг

- VPN – 400 Мбит/с
- FW – 1400[BOND] Мбит/с

HW50 A1 DEV

- 3x 1G RJ-45
- 2x USB, Console, HDMI
- Внешний БП
- 150 x 150 x 40 ШхВхГ(мм)
- 400 г

- VPN – 250 Мбит/с
- FW – 700 Мбит/с

HW10 F1 DEV

- 3x 1G RJ-45
- 2x USB, HDMI
- Внешний БП, Type-C
- 95 x 30 x 68 ШхВхГ (мм)
- 260 г

- VPN – 35 Мбит/с
- FW – 200 Мбит/с

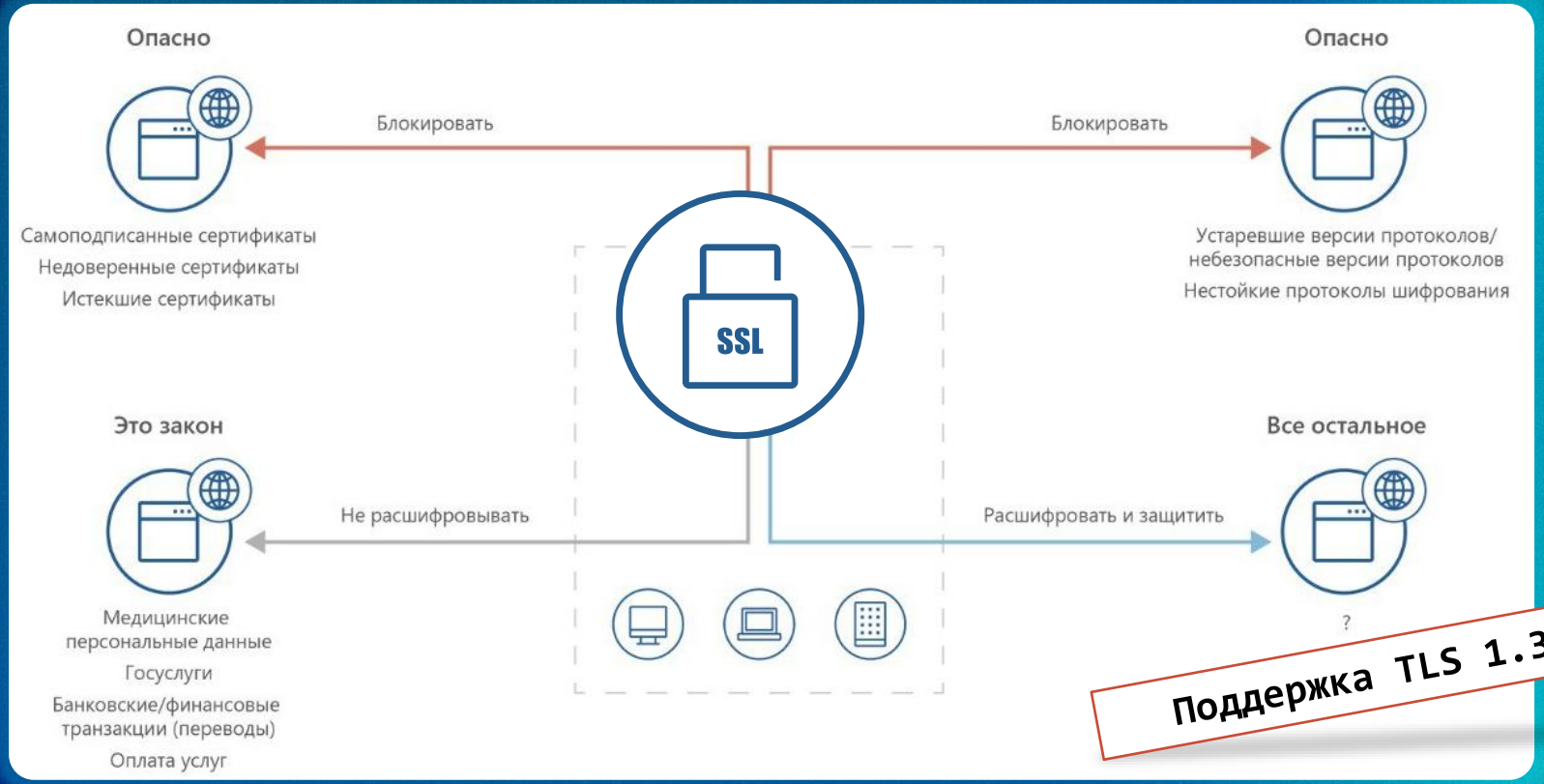
ViPNet Coordinator VA 5

Поддерживаемые гипервизоры:

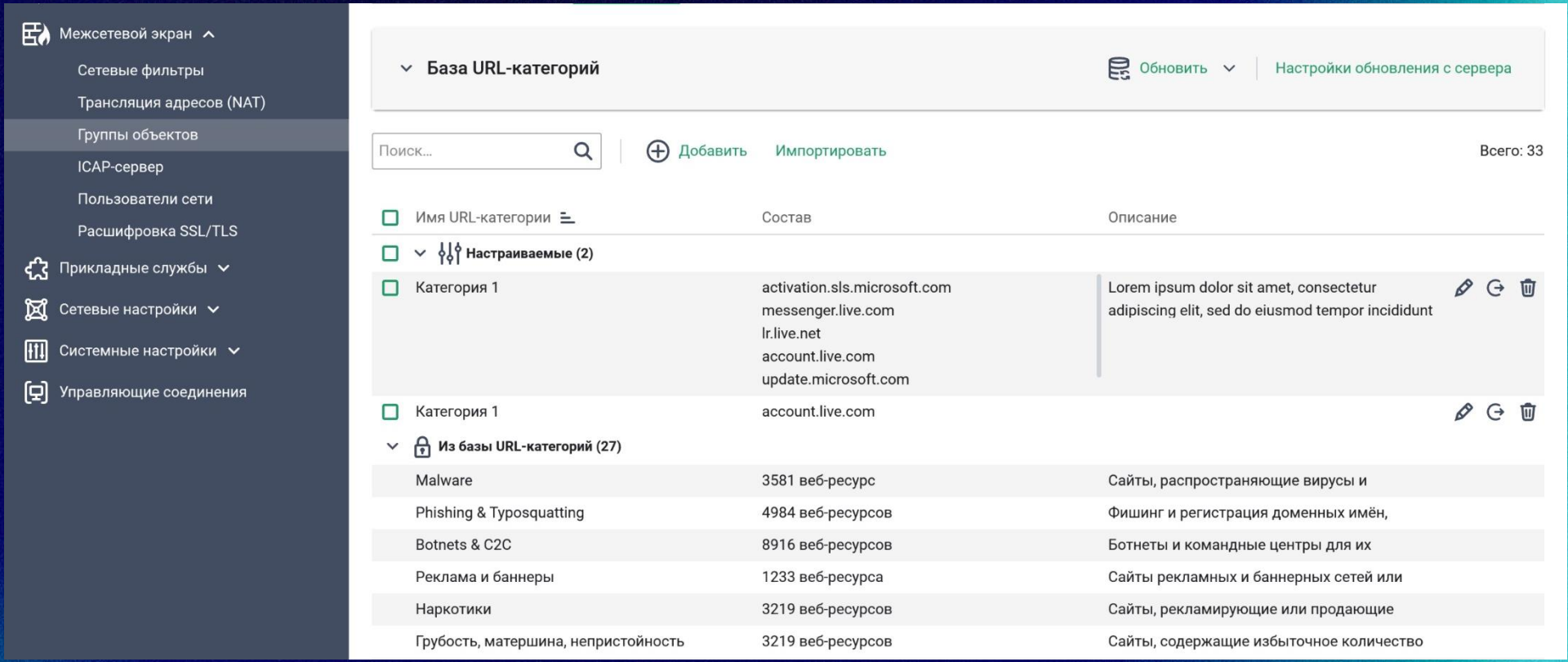
- KVM, QEMU-KVM и Proxmox VE
- Астра Брест, zVirt, SharxBase
- VMware ESXi
- VMware Workstation
- Microsoft Hyper-V Server
- Oracle VM Server
- Oracle VM VirtualBox

Планы развития

SSL/TLS-инспекция



URL-фильтрация



Источник баз URL-категорий

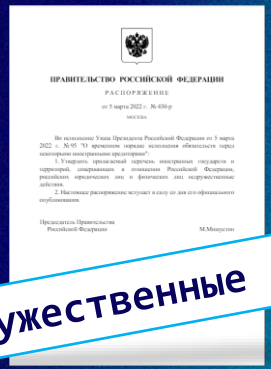
~85 млн веб-ресурсов

80 категорий

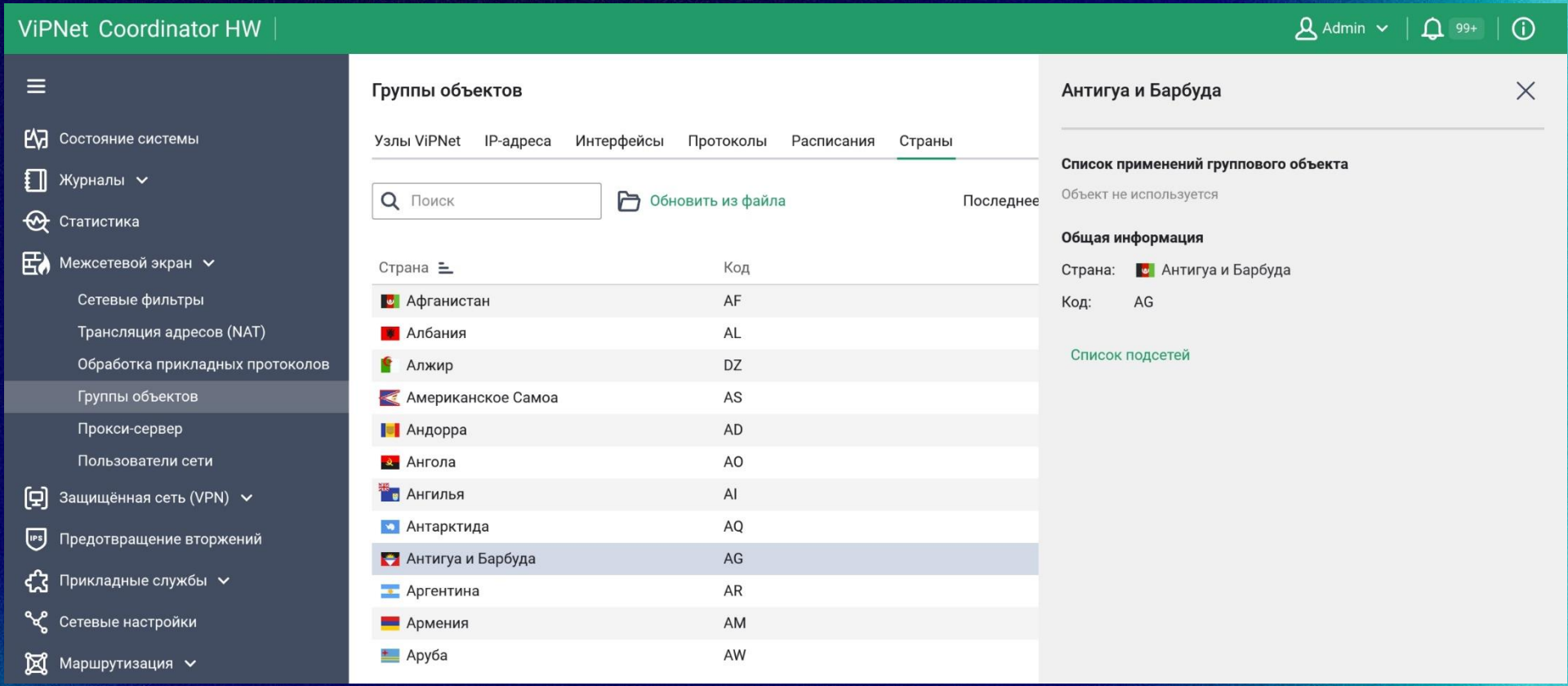
+15% ежемесячный прирост базы

Блокировка по GEO-IP

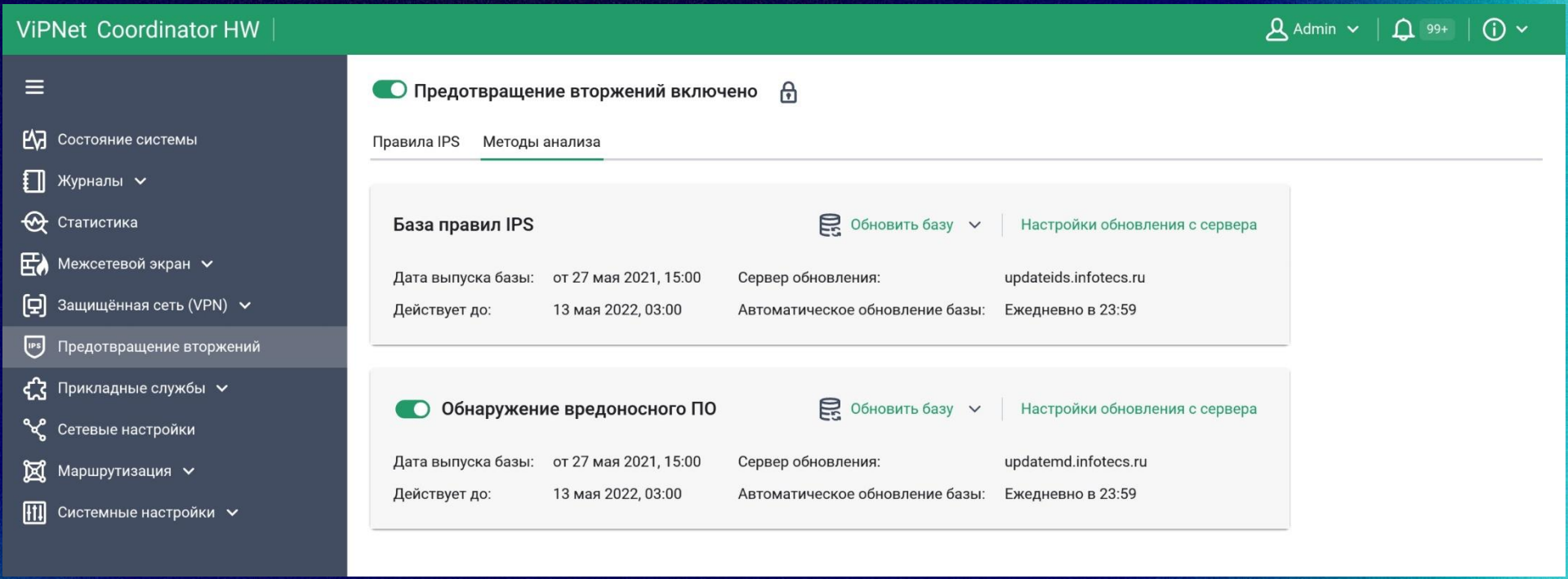
- Фильтрация трафика на основе данных о географической принадлежности отправителей
- Использование доверенной базы геолокации IP-адресов на базе «Главного радиочастотного центра» (ФГУП «ГРЧЦ»)



Блокировка по GEO-IP



Обнаружение вредоносного ПО



Журнал сетевых сессий

- Состояние системы
- Журналы
  - Журнал аудита
  - Журнал IP-пакетов
  - Журнал сессий
  - Журнал СКЗИ
  - Журнал MFTP
  - Журнал DNS-запросов
  - Системный журнал
- Статистика
- Межсетевой экран
- Защищённая сеть (VPN)
- Предотвращение вторжений
- Прикладные службы
- Сетевые настройки
- Маршрутизация
- Системные настройки

Журнал сессий

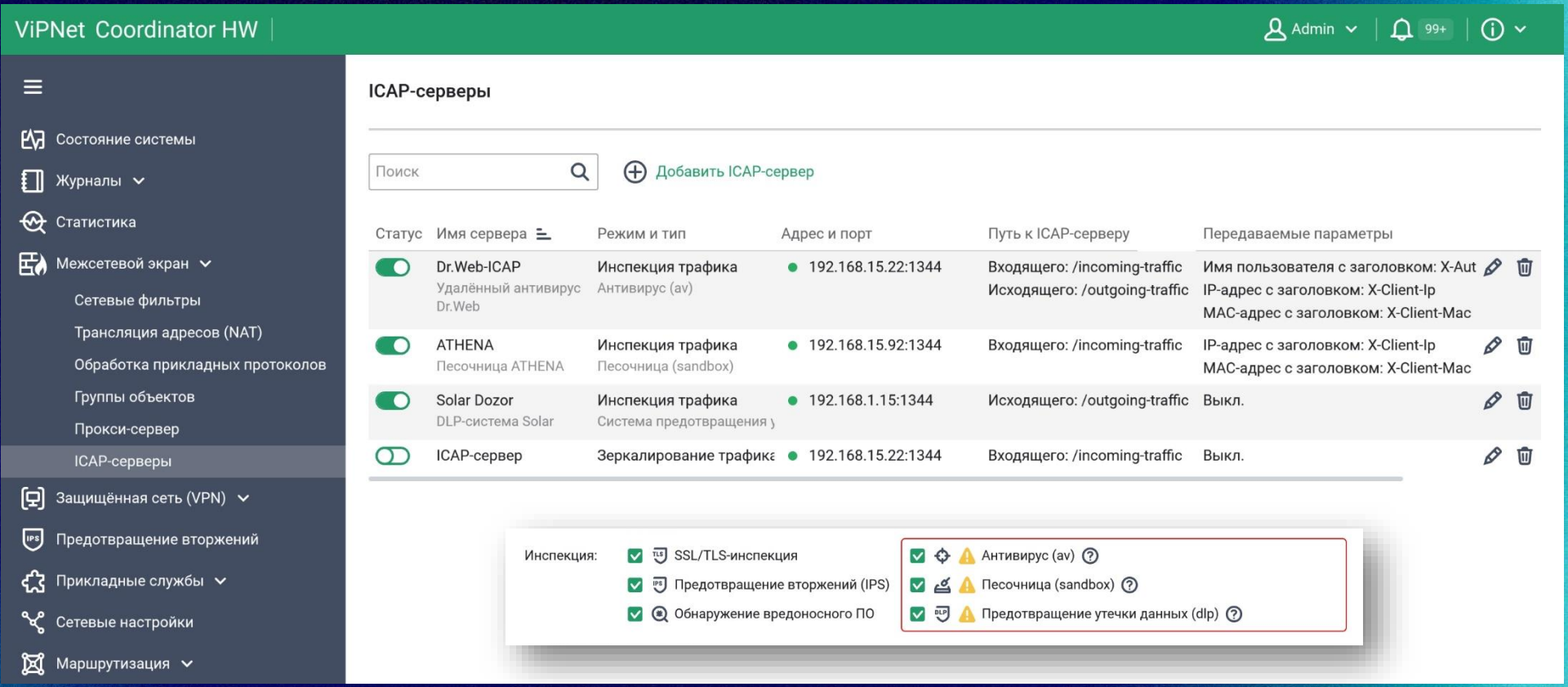
Поиск

Результат фильтрации за последний час, с 20.06.2024 13:39:41

Показано: 37

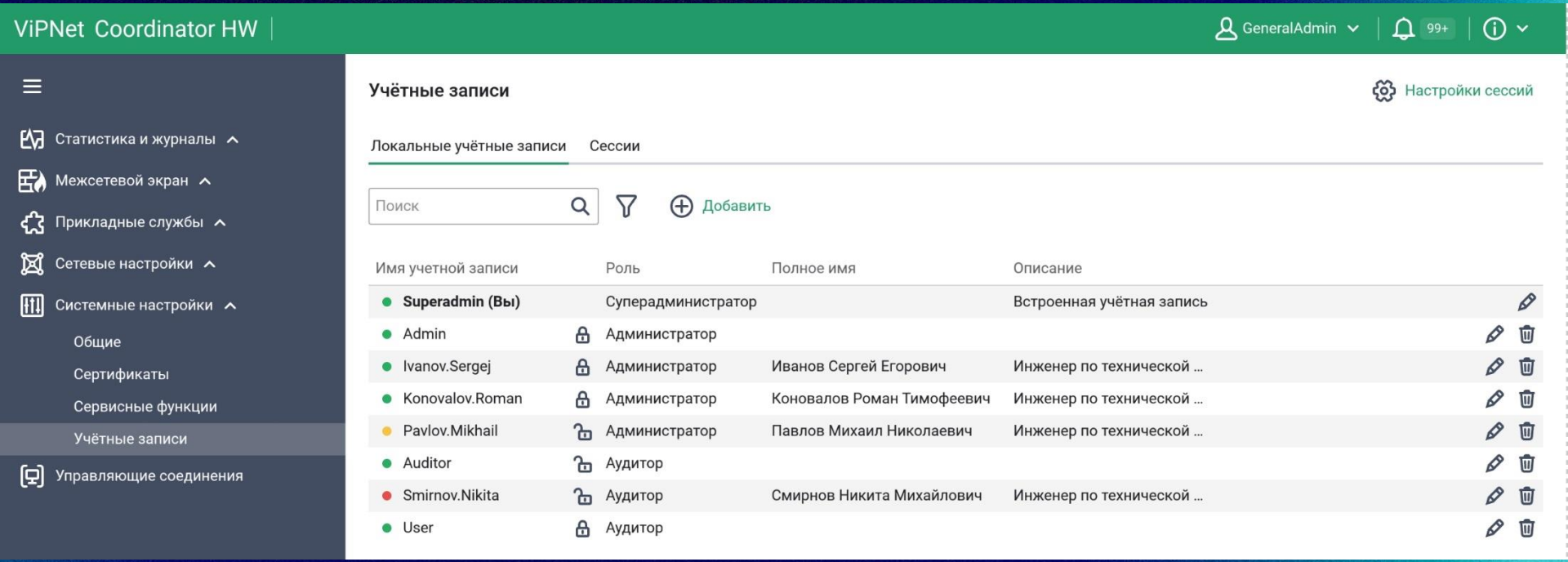
Дата и время	Завершение	Состояние	Источник	Назначение	Пользователь сети	Протокол	URL
2020.06.11 16:45:31	17:55:31	Завершена	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com https://example.com/blog https://example.com/blog https://example.com/blog https://example.com/blog
2020.06.11 16:45:31	2020.06.12 13:23:54	Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog
2020.06.11 16:45:31	—	Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog
2020.06.11 16:45:31	—	Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog
2020.06.11 16:45:31	—	Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog
2020.06.11 16:45:31	—	Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog
2020.06.11 16:45:31	—	Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog
2020.06.11 16:45:31	—	Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog

Расширение возможностей ICAP



Локальные учетные записи

- новая роль «Сетевой администратор»



ViPNet Coordinator HW 5.4

- SSL/TLS-инспекция
- URL-фильтрация
- Блокировка по GEO-IP
- Обнаружение вредоносного ПО
- Расширение возможностей ICAP
- Журнал сетевых сессий
- Локальные учетные записи + новая роль
- Интеграция ViPNet SafeBoot

В разработке

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного