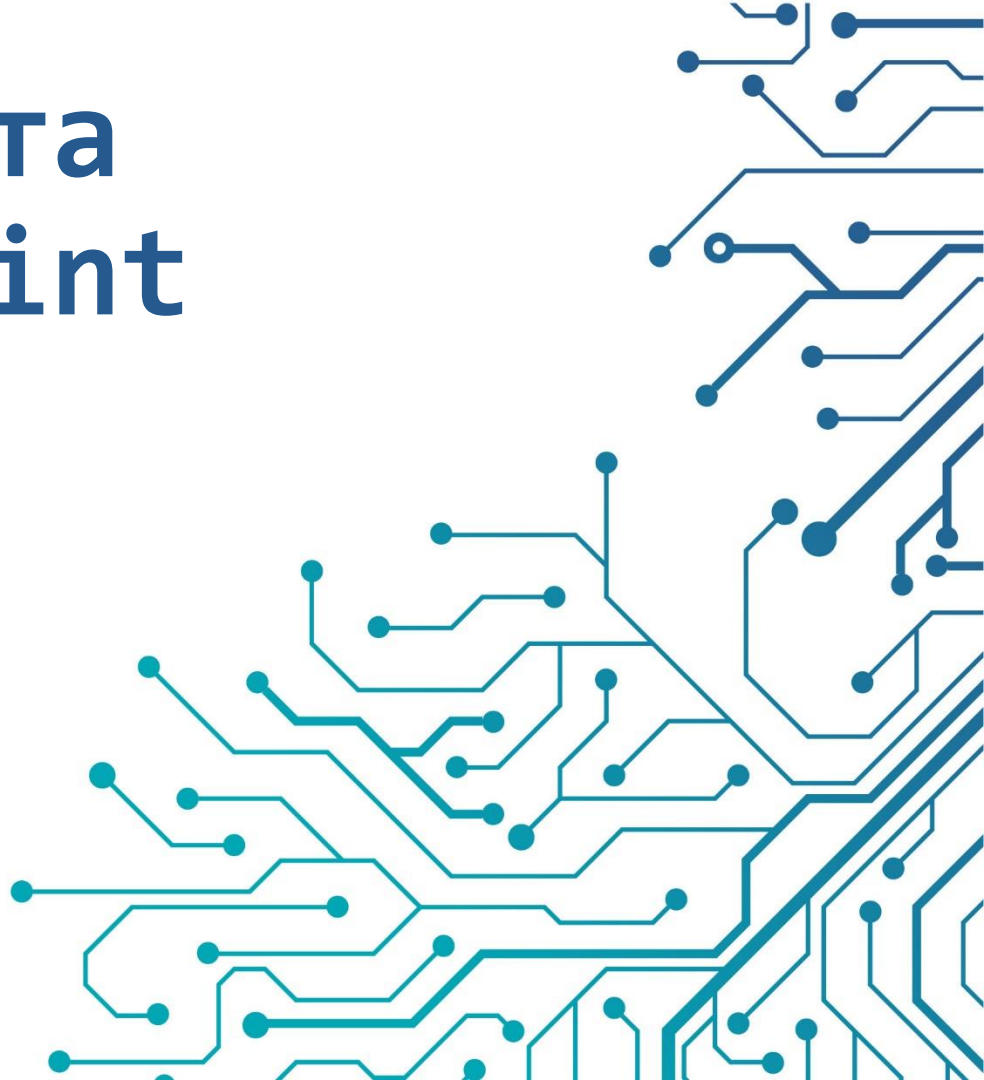
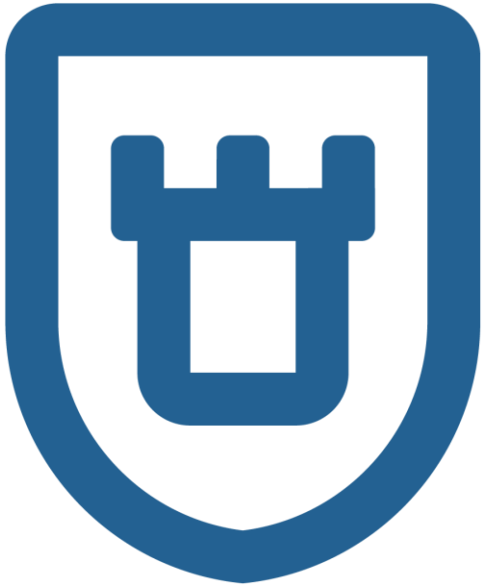
Обзор продукта ViPNet EndPoint Protection версия 1.6

Кадыков Иван

infotecs





ViPNet EndPoint Protection

Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых», «бесфайловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия.

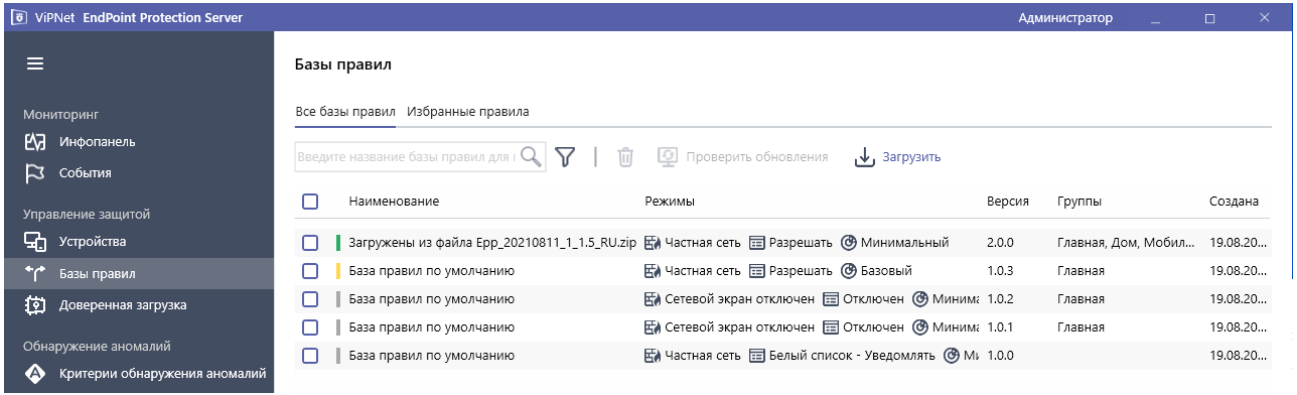
Защитные механизмы

ViPNet EndPoint Protection – комбинирование методов защиты

- Сигнатурные методы защиты:
  - правила белого/чёрного списка
  - правила для HIDS/HIPS
  - фильтры межсетевого экрана
- Эвристические методы защиты:
  - Поведенческий анализ
  - Эвристический антивирус (NGAV - бессигнатурный)
  - Математические модели построенные при помощи искусственного интеллекта
- Средства мониторинга и передача событий для последующего анализа

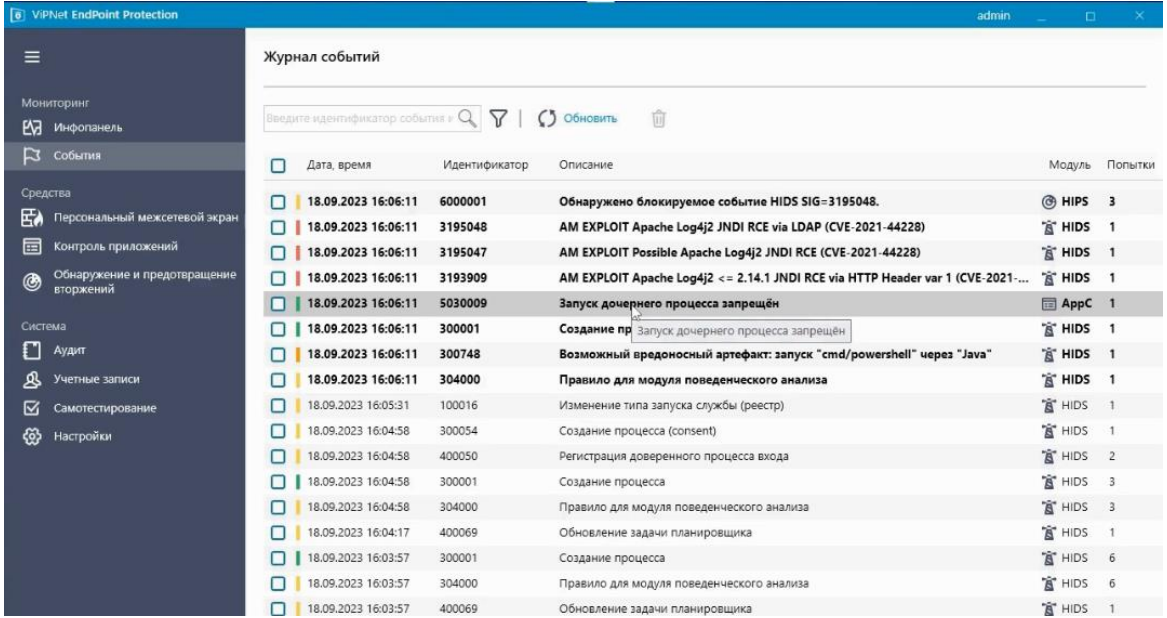
Работаем по правилам и моделям!

EndPoint Protection работает по БРП



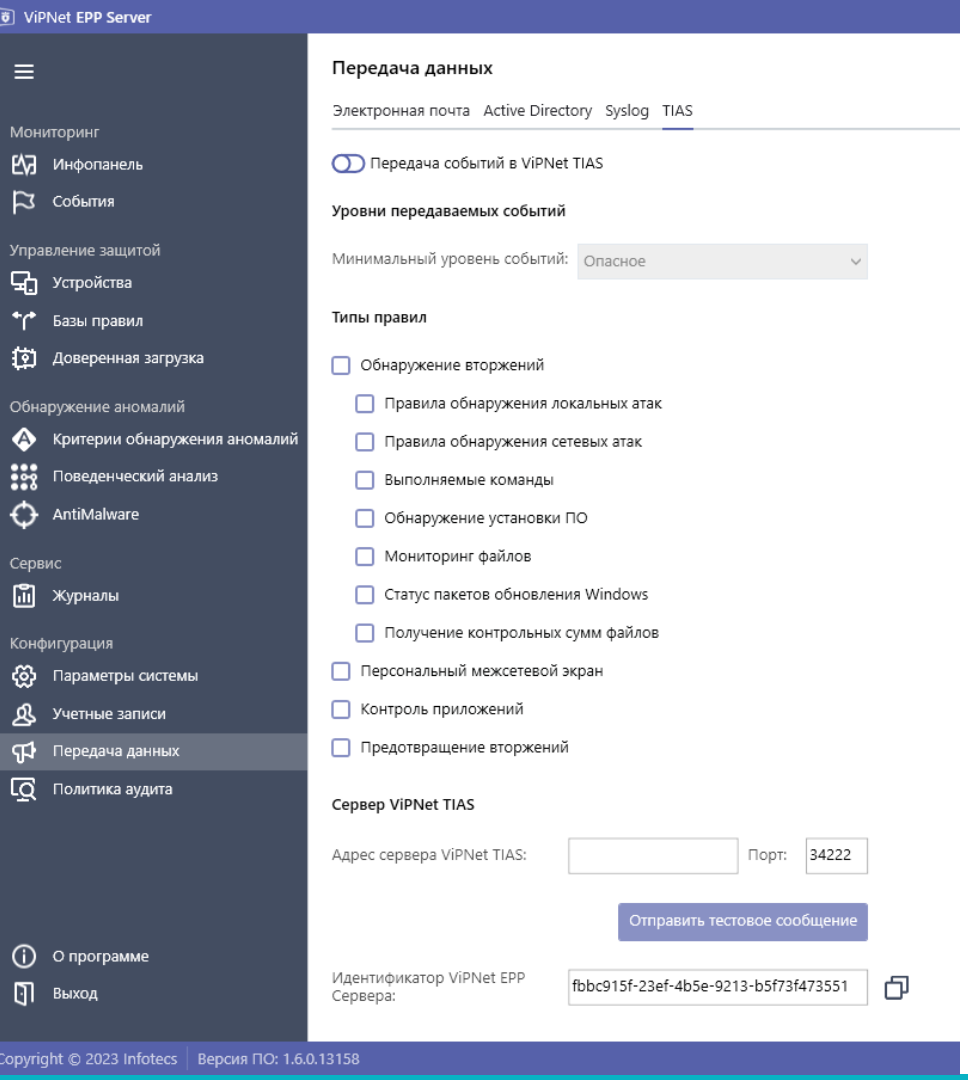
Состоит из:

- Правил системы обнаружения и предотвращения вторжений
- Фильтров Межсетевого экрана
- Списков ПО для Черного и Белого списка
- Эвристический движок Anti-malware
- Модель обнаружения аномального поведения системных утилит



Мы всё видим

Все события с хостов собираются на сервере и выводятся на экран для администратора ИБ

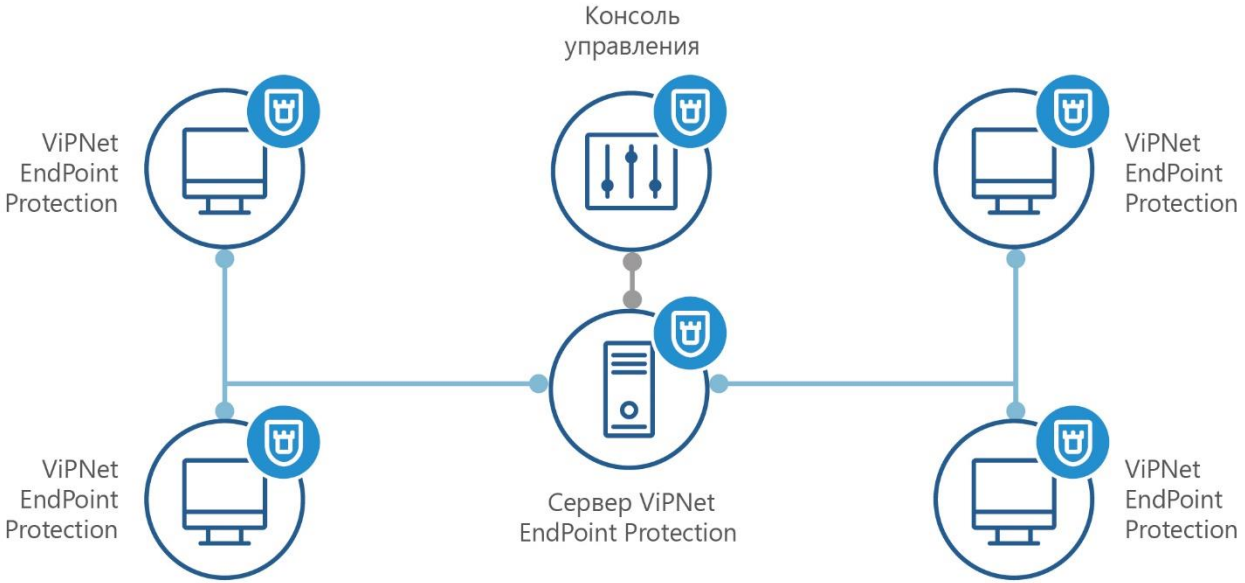


Передача событий

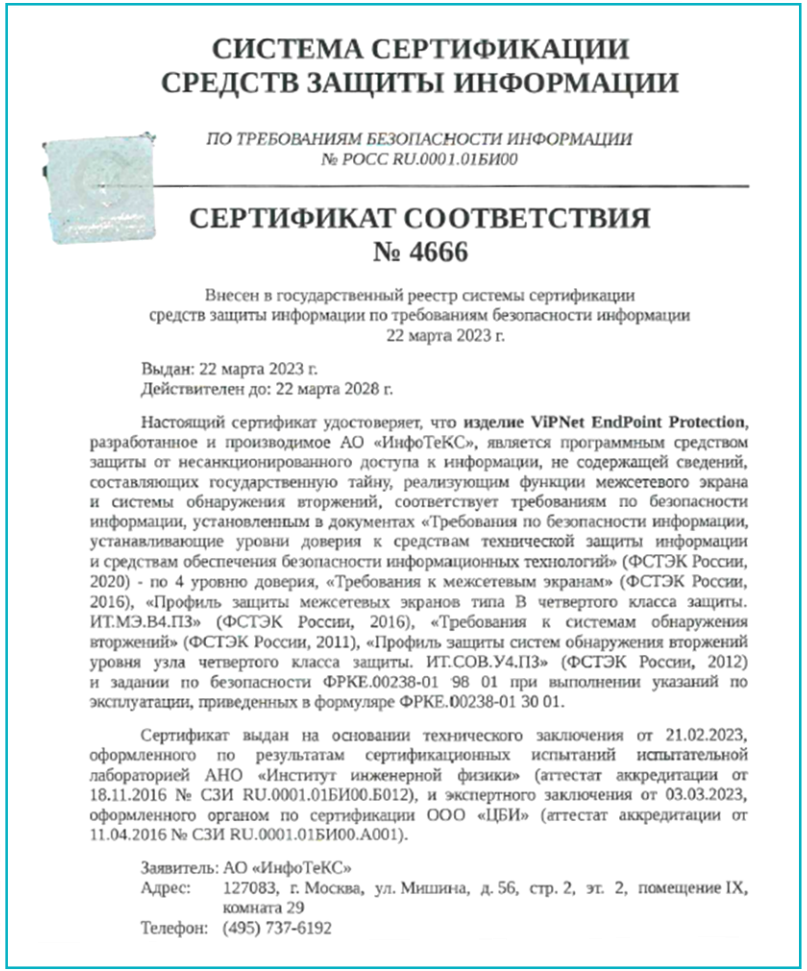
Все события могут передаваться в:

- ViPNet TIAS
- В любую SIEM

Архитектура ViPNet EndPoint Protection



- Клиент
- Сервер
- Консоль управления



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4666

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
22 марта 2023 г.

Выдан: 22 марта 2023 г.
Действителен до: 22 марта 2028 г.

Настоящий сертификат удостоверяет, что **изделие ViPNet EndPoint Protection**, разработанное и производимое АО «ИнфоТеКС», является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции межсетевого экрана и системы обнаружения 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 В четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ» (ФСТЭК России, 2012) и задании по безопасности ФРКЕ.00238-01 98 01 при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00238-01 30 01.

Сертификат выдан на основании технического заключения от 21.02.2023, оформленного по результатам сертификационных испытаний испытательной лабораторией АНО «Институт инженерной физики» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 03.03.2023, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001).

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

Сертифицировано!

- Межсетевой экран тип В класс 4
- Система обнаружения вторжений У4
- 4 класс ТДБ

Таблица 1 – Реализация ViPNet EPP мер по защите информации

№ п/п	Содержание меры по обеспечению безопасности в [1], [2] и ее условное обозначение	Содержание меры по обеспечению безопасности в [3], [7] и ее условное обозначение
1.	ИАФ.1* Идентификация и аутентификация пользователей, являющихся работниками оператора	ИАФ.1* Идентификация и аутентификация пользователей и инициируемых ими процессов
2.	ИАФ.3* Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	ИАФ.3* Управление идентификаторами
3.	ИАФ.4* Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	ИАФ.4* Управление средствами аутентификации
4.	ИАФ.5* Защита обратной связи при вводе аутентификационной информации	В [3], [7] отсутствует соответствующая мера
5.	УПД.1* Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	УПД.1* Управление учетными записями пользователей
6.	УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	УПД.2 Реализация модели управления доступом
7.	УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между	ЗИС.6 Управление сетевыми потоками

Меры прописаны в правилах пользования

На картинке представлена лишь часть мер прописанных в документе

Версия 1.6
Что нового?

Сервер под Linux!

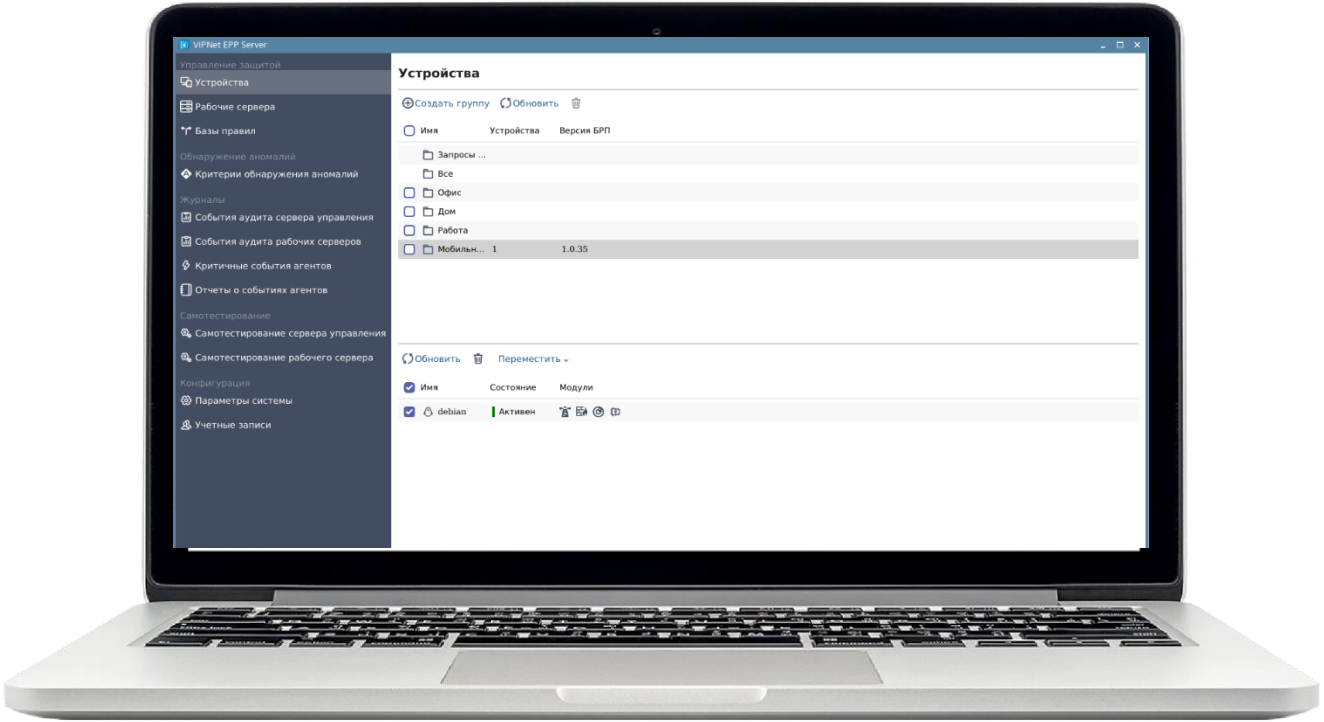
Разработан компонент ViPNet EndPoint Protection Server под Astra Linux Special Edition 1.7.4

Пока реализована возможность управление следующими модулями:

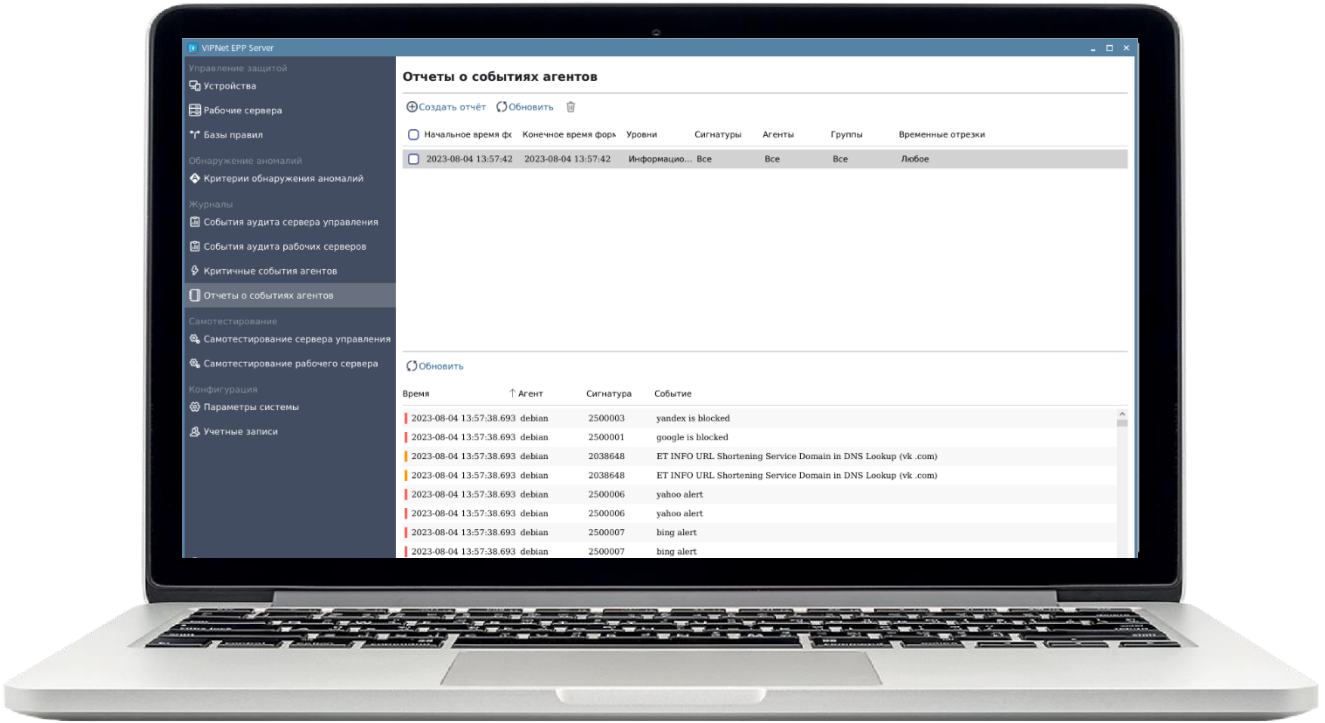
- Персональный межсетевой экран
- Модуль обнаружения и предотвращения вторжений
- Модуль обнаружения аномалий в части обнаружения с помощью критериев

Так же реализована возможность отслеживания работы антивирусов.

Управление устройствами



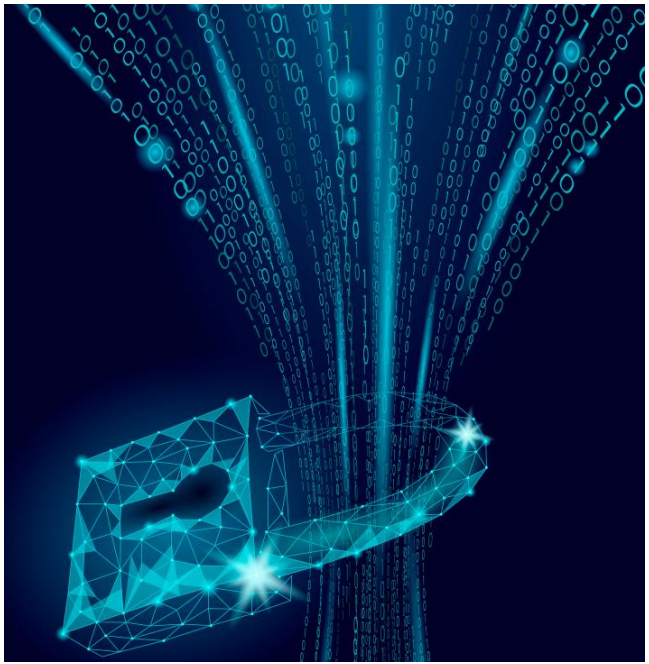
События от агентов



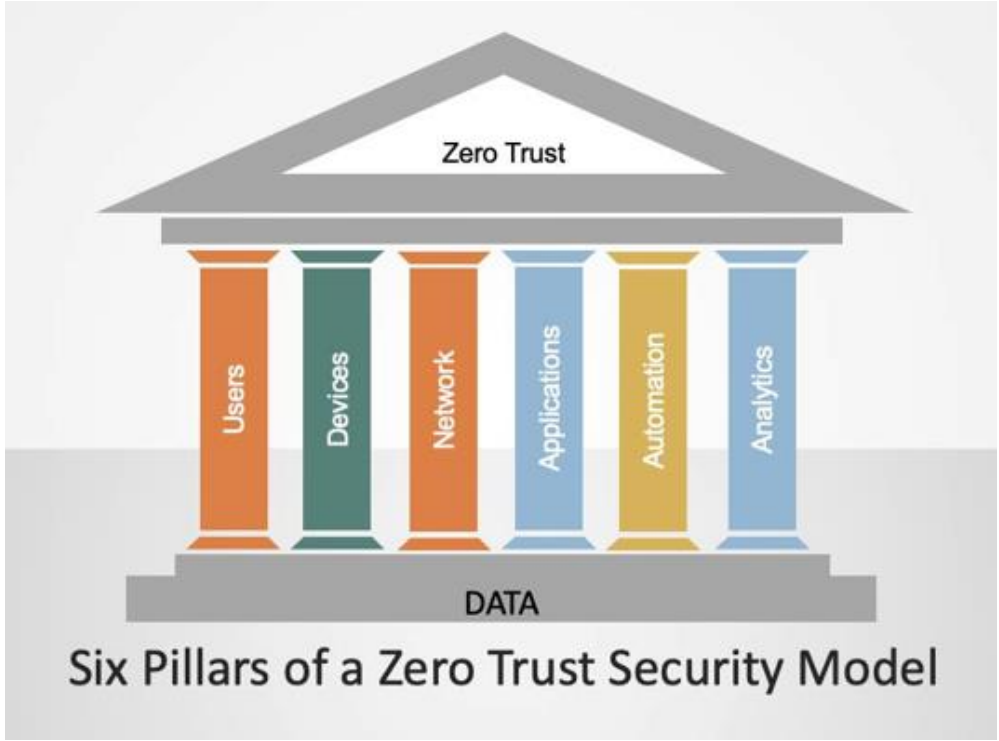
Изменения в модуле межсетевого экрана

Добавились новые возможности:

- Стек технологий ZTNA
- Интеграция с Client 4U
- Добавление\Редактирование\Удаление фильтров защищённой сети из локальной консоли ViPNet EndPoint Protection (агент)



Что такое Zero Trust?

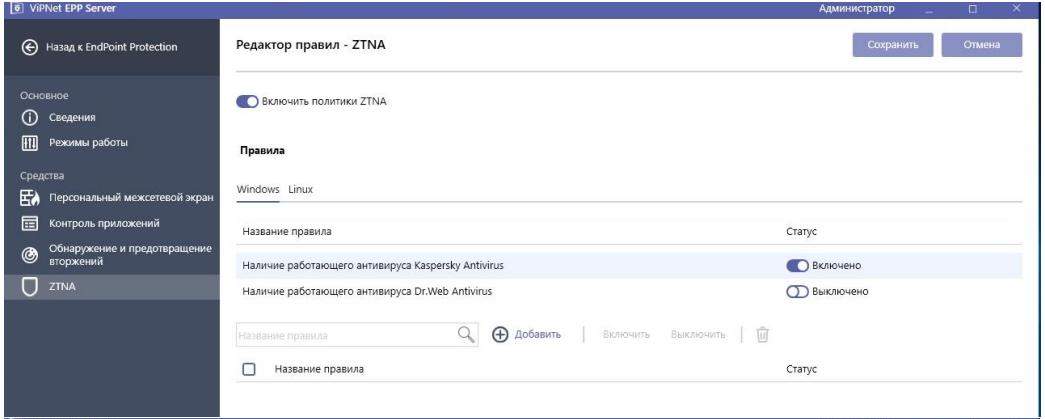


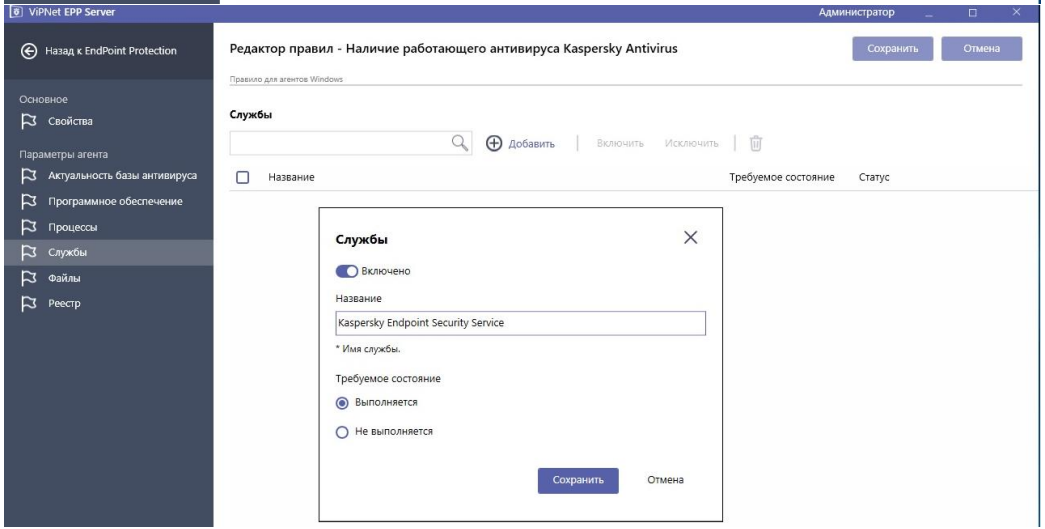
Six Pillars of a Zero Trust Security Model

Zero Trust (ZT) или «нулевое доверие» – набор постоянно развивающихся концепций и идей, направленных на принятие точных решений о доступе субъекта к объекту с минимальными привилегиями для каждого запроса доступа.

Что уже реализовано

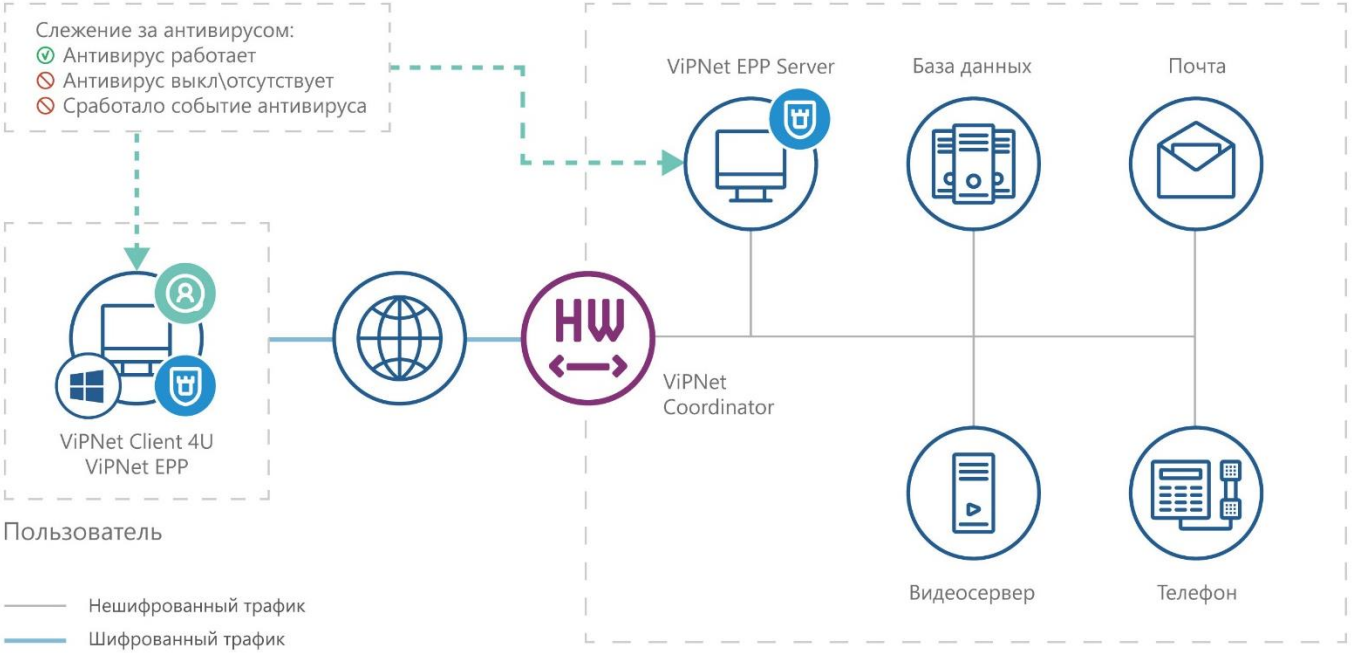
- Проверка соответствия хоста на наличие необходимого/требуемого ПО, обновлений ПО, запущенных процессов, обновление антивирусных баз и т.д.
- Блокировка входа в защищенную сеть ViPNet при несоответствии устройства политикам ZTNA, информирование пользователя об этом.



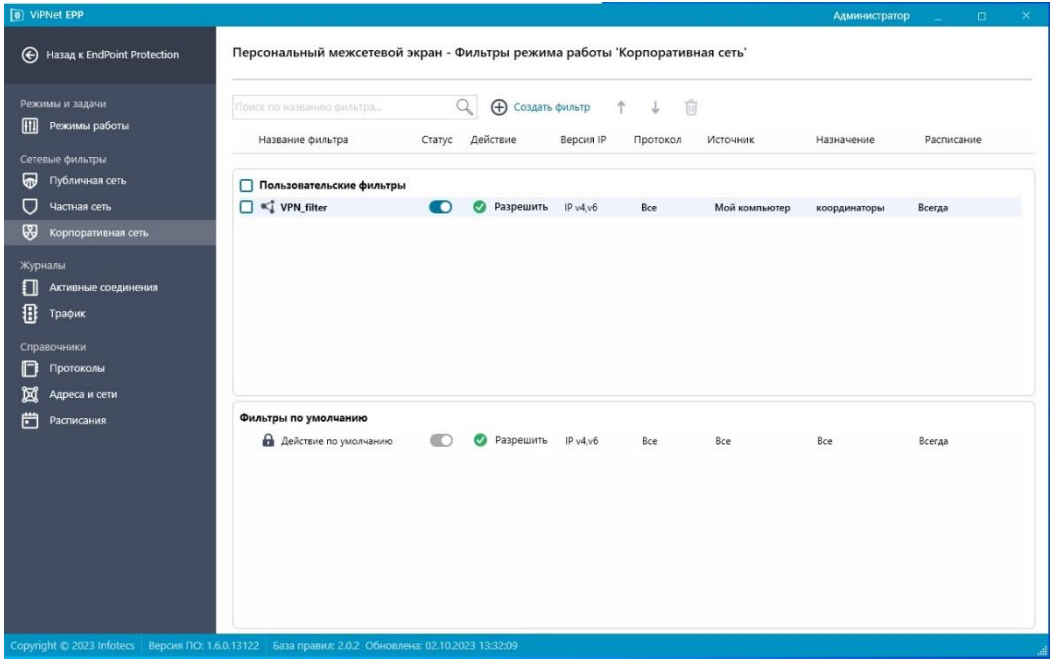


Редактирование правил ZTNA

ZTNA «в картинках»



Создание фильтров защищённой сети

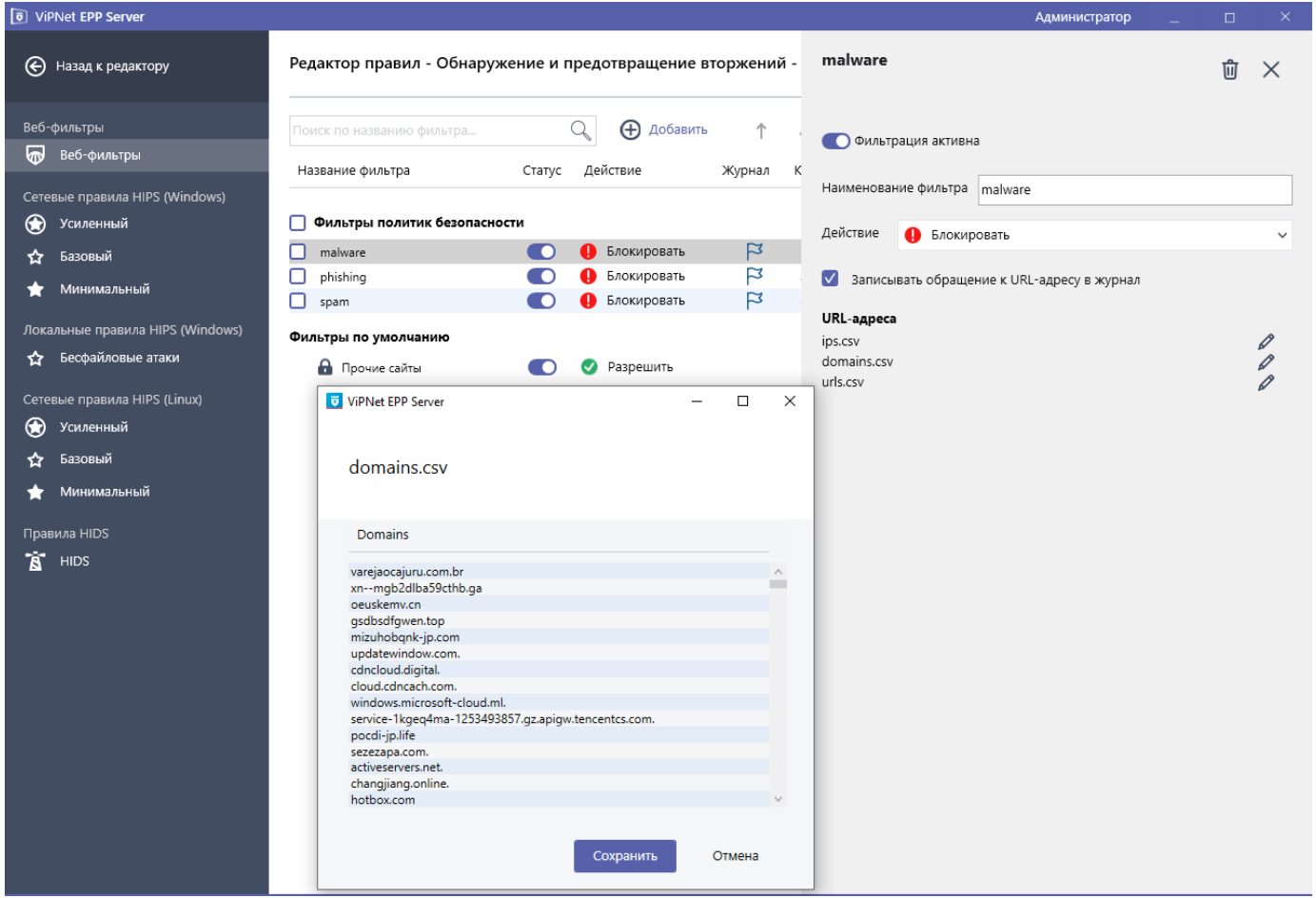


Используя UI ViPNet EndPoint Protection agent можно создавать пользовательские фильтры защищённой сети для ViPNet Client 4U

Изменения в модуле системы обнаружения и предотвращения вторжений

- TLS – инспекция – возможность расшифровывания трафика проходящего через модули ViPNet EndPoint Protection. База «bad URL» поставляется в рамках БРП, обновляется регулярно

- SafeBrowsing – безопасный сёрфинг в интернете (веб-фильтрация)



Как это выглядит

Fileless attacks

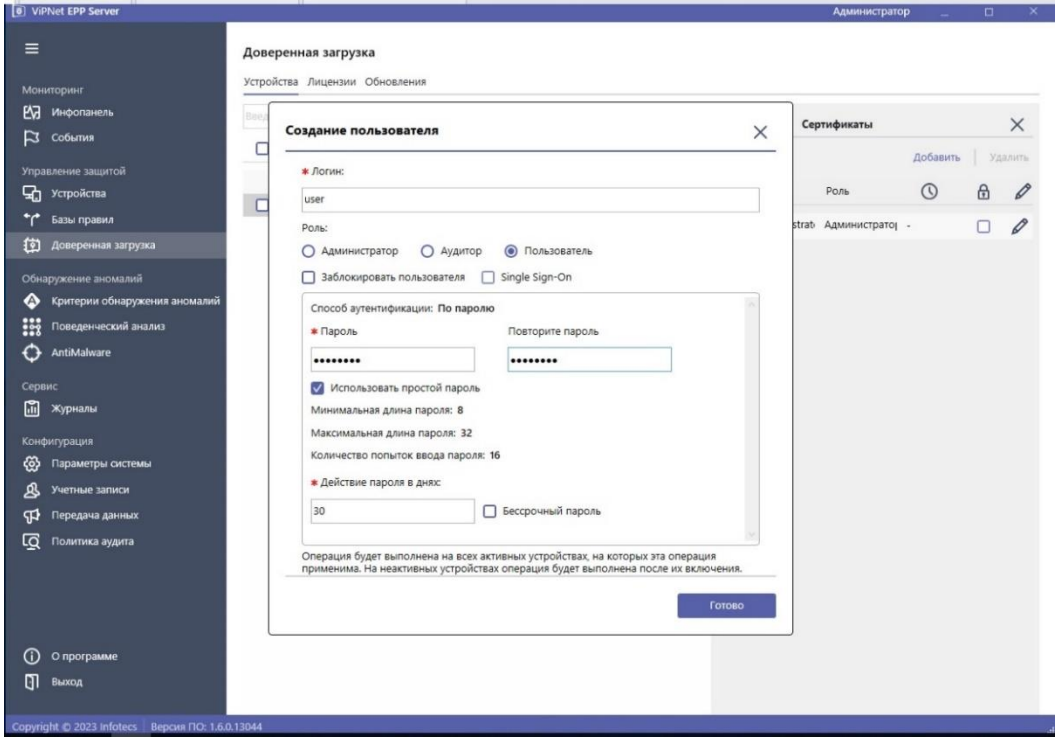
Внедрение новых
техник предотвращения бесфайловых
атак:

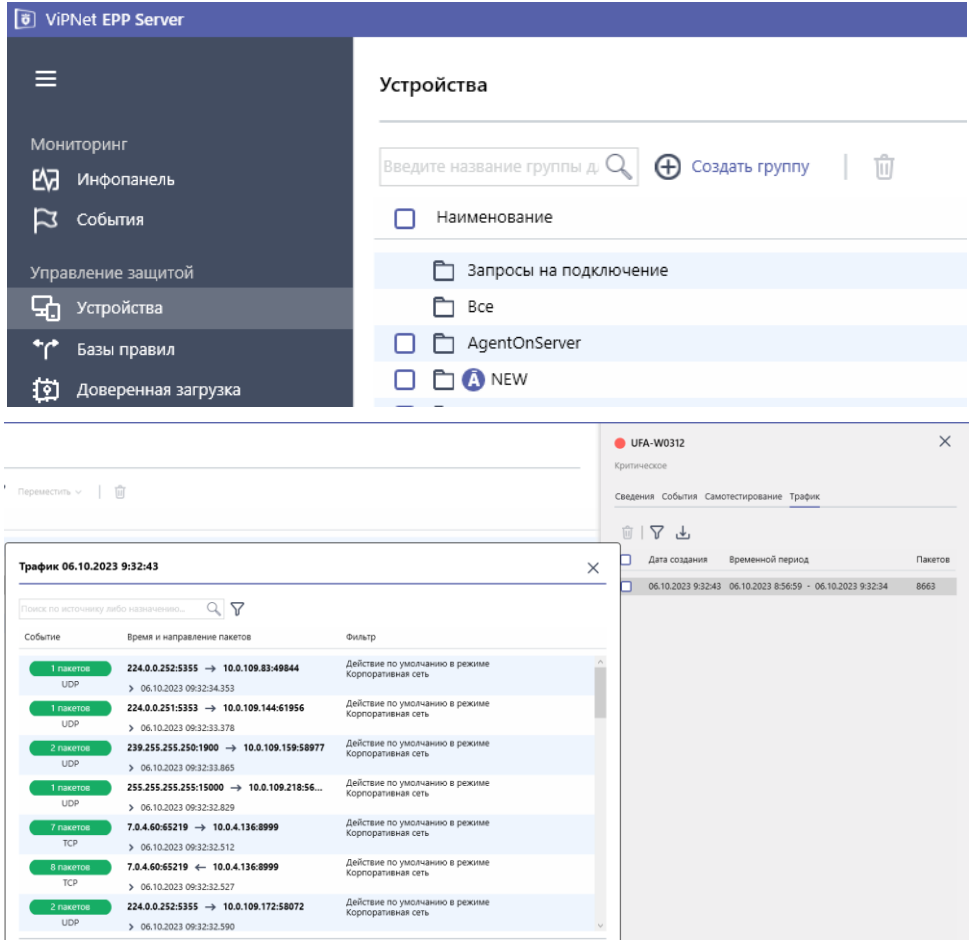
- Hollowed / replaced
- Doppelganger

Управление ViPNet SafeBoot

Дополнительные механизмы удалённого управления ViPNet SafeBoot:

- Обновление МДЗ
- Управление пользователями
- Установка корневых сертификатов

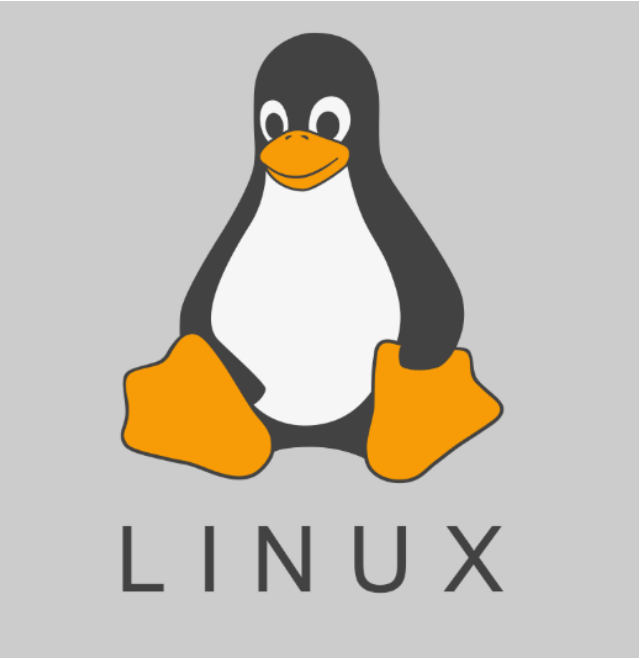




И ещё добавили…

- Автоматическое подключение защищаемых узлов к ViPNet EPP Сервер
- Запрос журнала регистрации трафика с ViPNet EPP

Поддержка новых ОС Linux



Astra Linux Special Edition 1.7.4

Альт СП Рабочая станция релиз 10

Альт Рабочая станция 10.1

РЕД ОС 7.3.2 «Муром» Рабочая станция

РЕД ОС 7.3.3 «Муром» Рабочая станция

infotecs

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363