ViPNet EndPoint Protection

Иван Кадыков

Пролог

«Болезни» последних 5ти лет

«Конечные устройства» – главная цель

Растущее количество атак и не доверенных аппаратных компонент

Удалённая работа, проведение приватных разговоров

Пользователь - внутренний нарушитель, низкий уровень опыта

Malware, Ransomeware, Fileless & Never-seen-before attacks

Состав продуктовой линейки на начало 2020 г.

ViPNet SafeBoot
Средство доверенной загрузки

ViPNet IDS HS
Система обнаружения вторжений

ViPNet Personal Firewall
Персональный межсетевой экран

ViPNet Client
VPN-Клиент, Межсетевой экран, Деловая почта

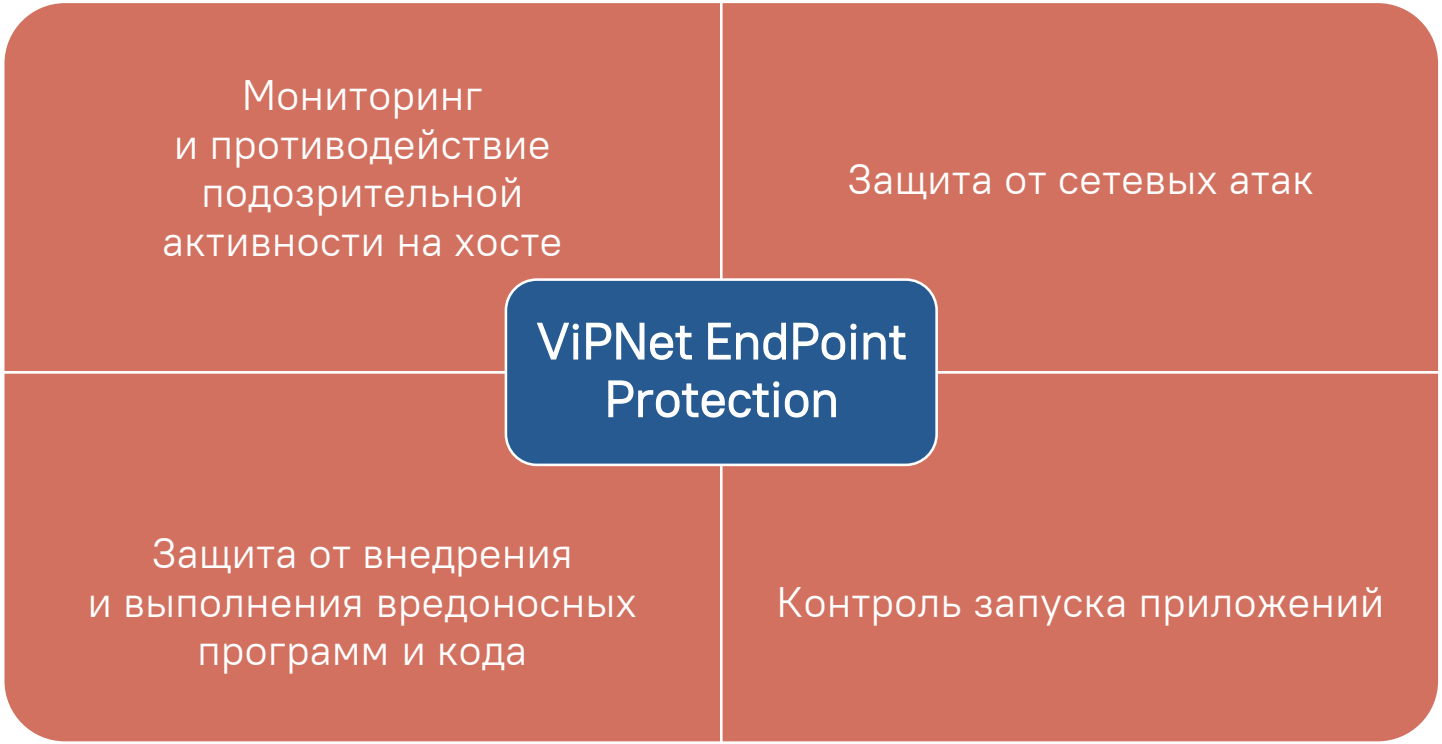
Наш новый продукт

ViPNet EndPoint Protection

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

Модули продукта

Решаемые задачи



Функциональность модулей и архитектура

Обнаружение и предотвращение атак

Используем:

- Эвристический анализ
- Сигнатурный анализ

Следим за:

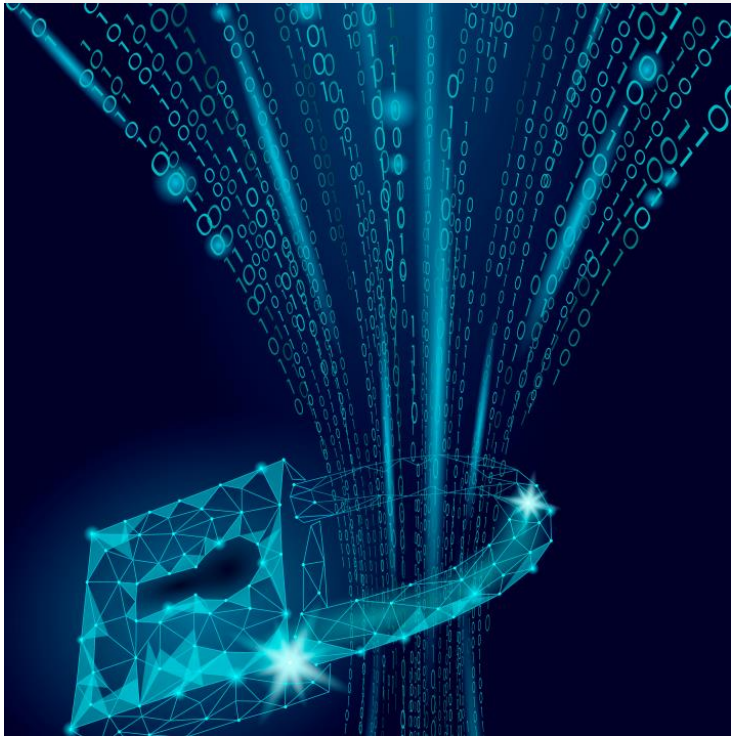
- Системными журналами Windows
- Журналами и логами приложений
- Изменениями в файловой системе и реестре
- Сетевым трафиком

Блокируем

- Подозрительный сетевой трафик
- Атакующие хосты

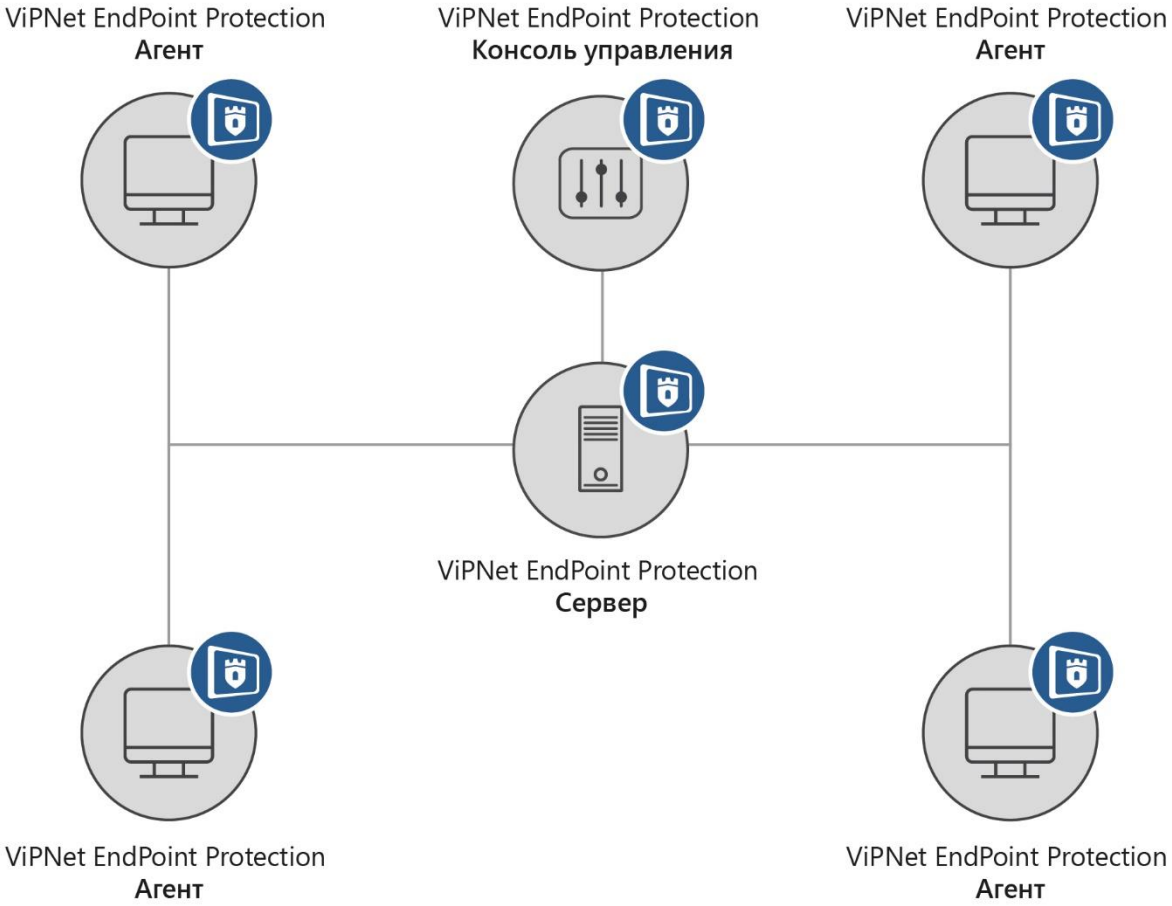
Межсетевое экранирование

- Фильтрация трафика Ipv4 и Ipv6
- Работа сетевых фильтров по расписанию
- Наличие преднастроенных фильтров
- Создание фильтров для определённых групп хостов
- Создание правил фильтрации из журнала трафика



Контроль приложений

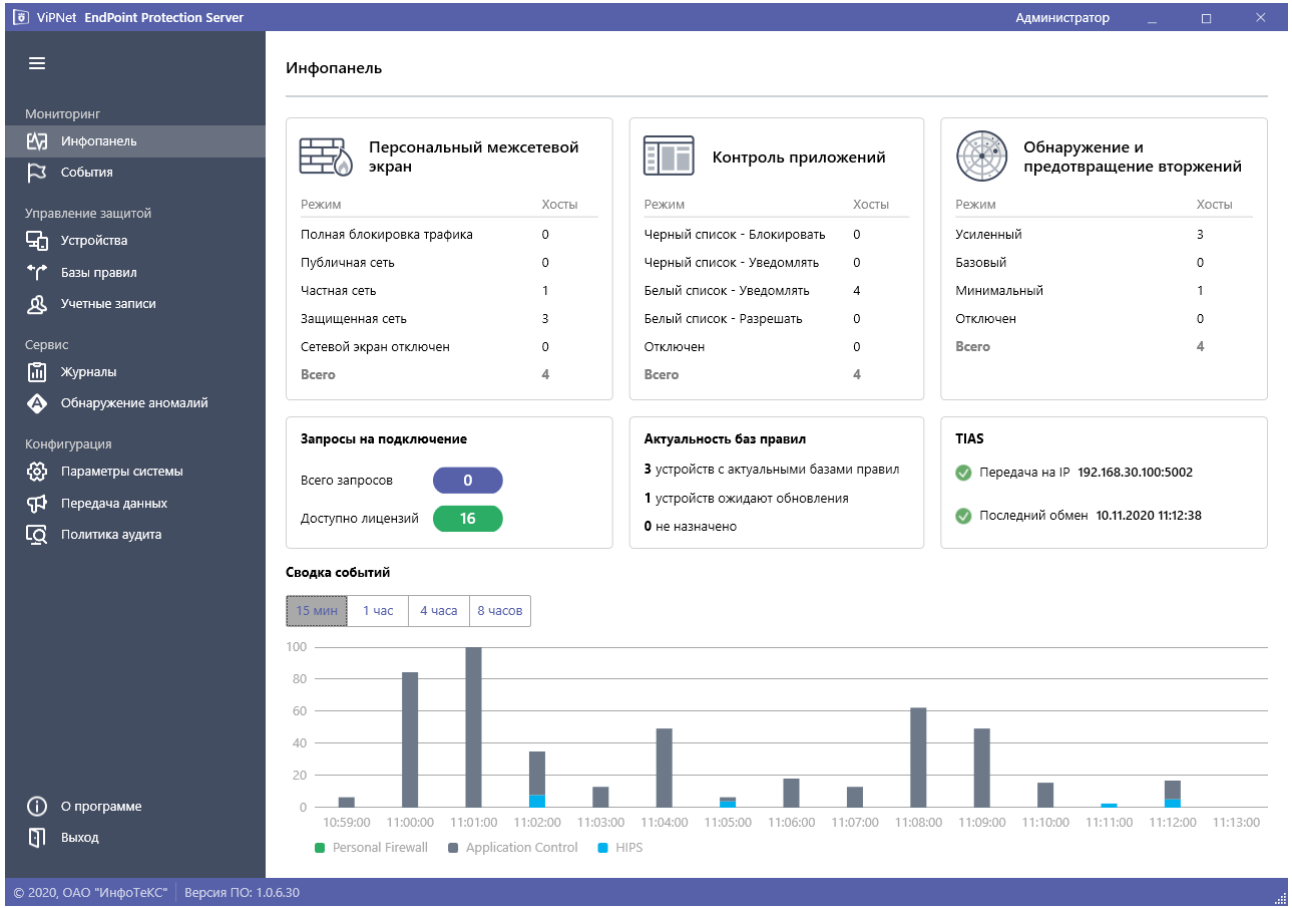
- Контроль запуска программ с использованием Чёрных и Белых списков программного обеспечения
- Анализ командной строки
- Защита файлов
- Защита реестра
- Контроль запуска программ, DLL-модулей, драйверов
- Контроль сетевой активности приложений



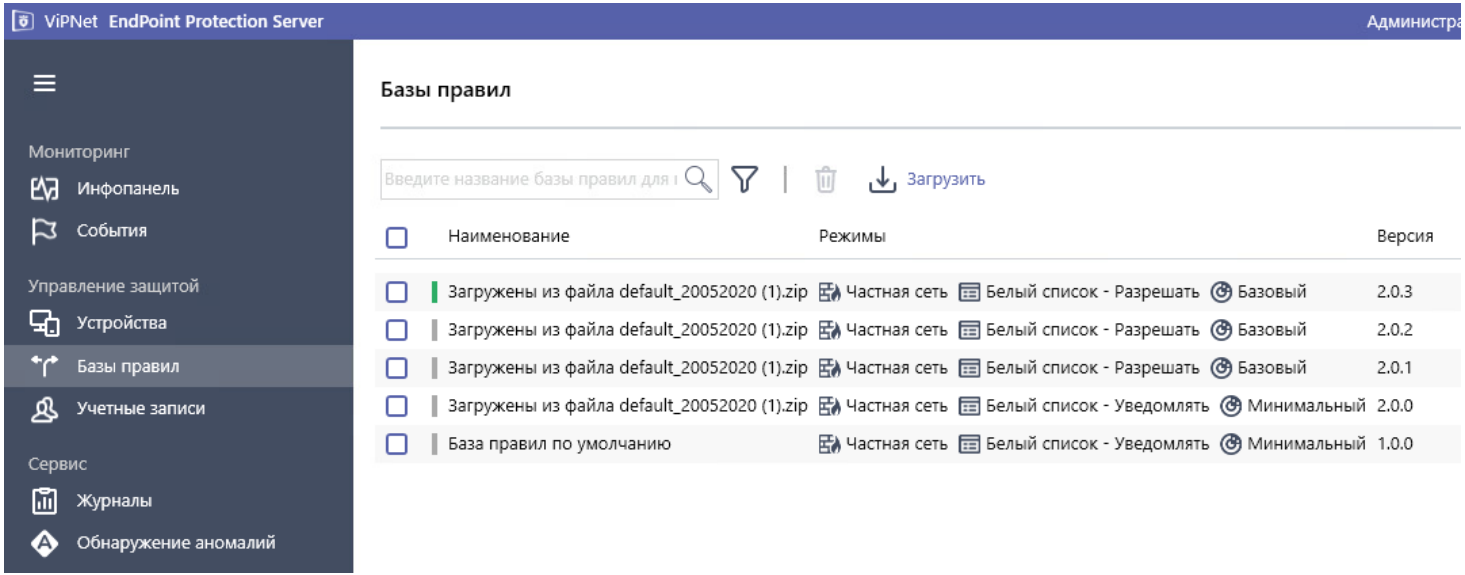
- Агент
- Сервер
- Консоль управления

Как всё работает

Консоль управления сервером



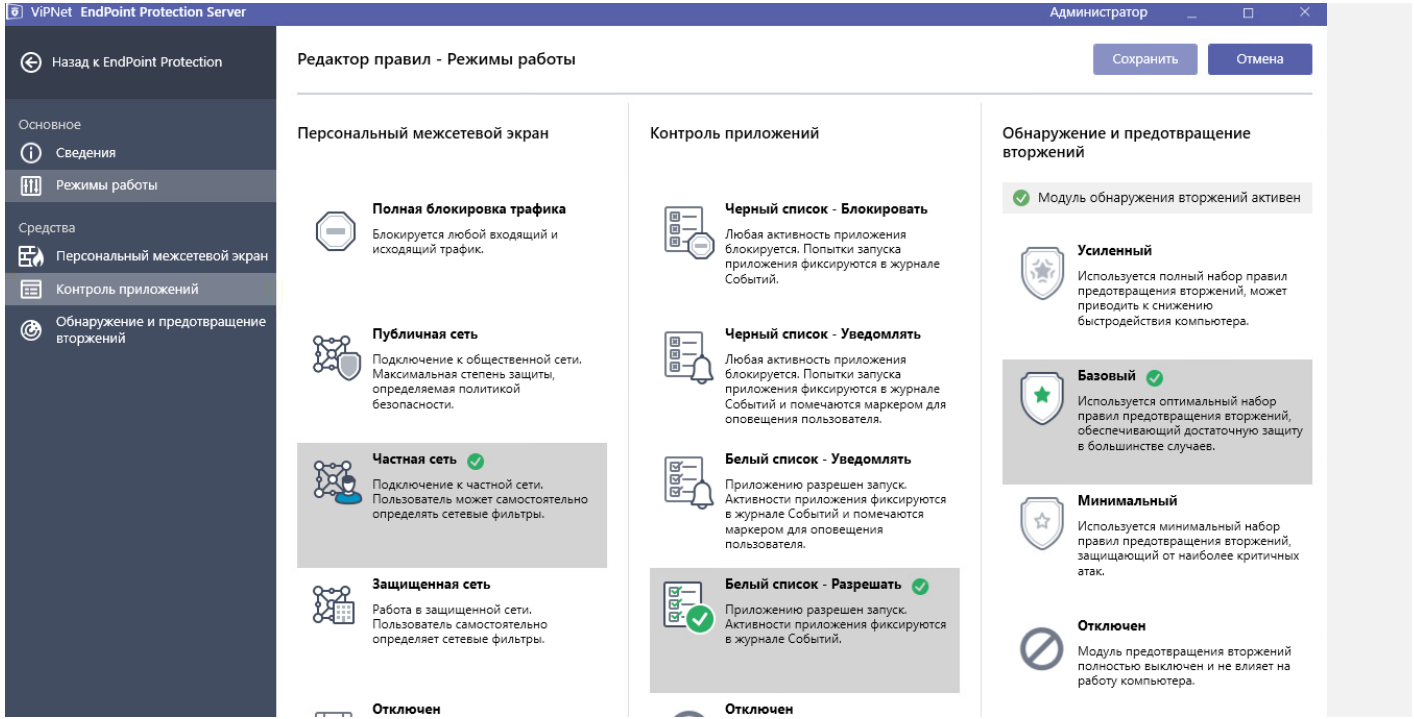
Базы правил (БРП)



БРП разрабатываются совместно с дочерней компанией «Перспективный мониторинг» и состоят из:

- Правил системы обнаружения и предотвращения вторжений
- Фильтров Межсетевого экрана
- Списков ПО для Чёрного и Белого списка

Настройки модулей – режимы работы



Администратор может использовать предоставленные нами режимы работы модулей или сам настроить режимы работы модулей.

Обнаружение и предотвращение вторжений

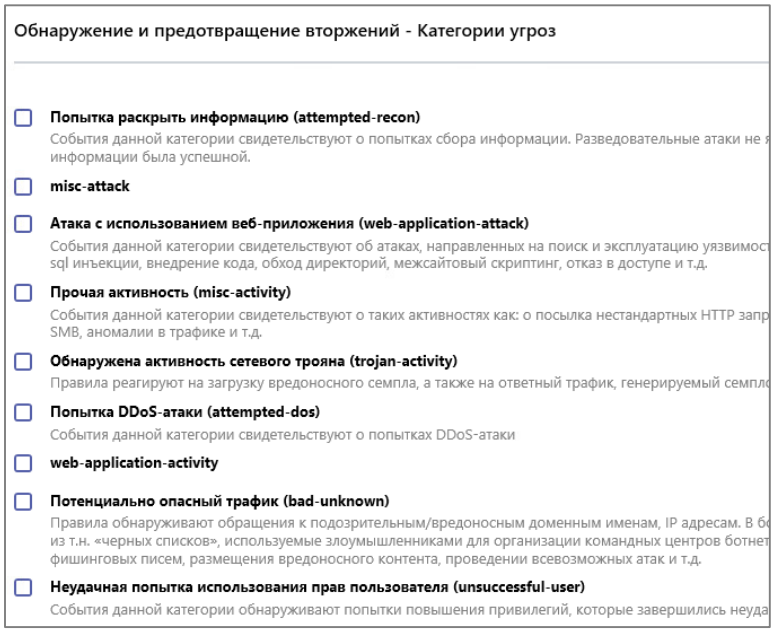
Обнаружение вторжений активно всегда.

Механизмы работы схожи с ViPNet IDS HS:

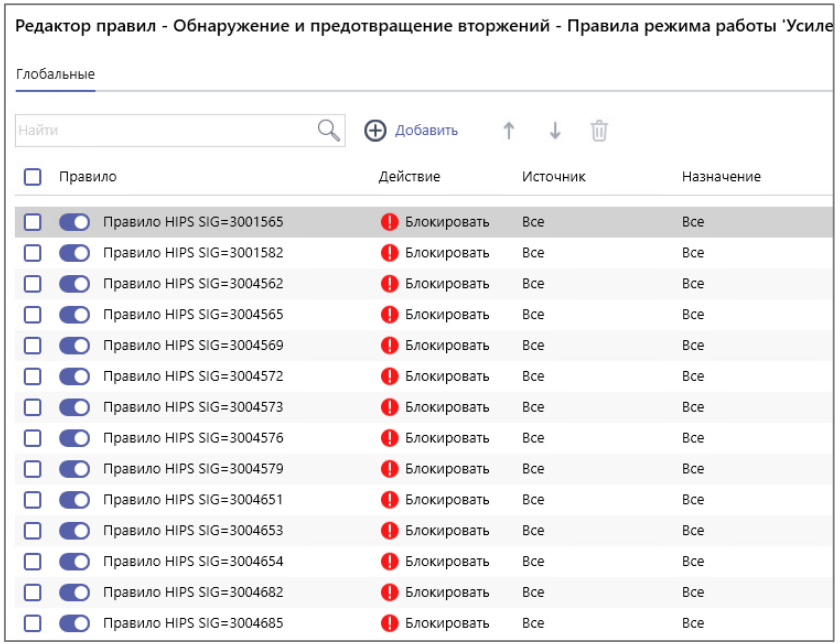
1. Загрузили БРП
2. Назначили на группу агентов
3. Агенты, получив БРП, мониторят события в соответствии с заданными политиками аудита

Предотвращение вторжений – имеется несколько уровней защиты – Усиленный, Базовый, Минимальный (разрабатывали совместно с ПМ)

Предотвращение вторжений



По категориям угроз



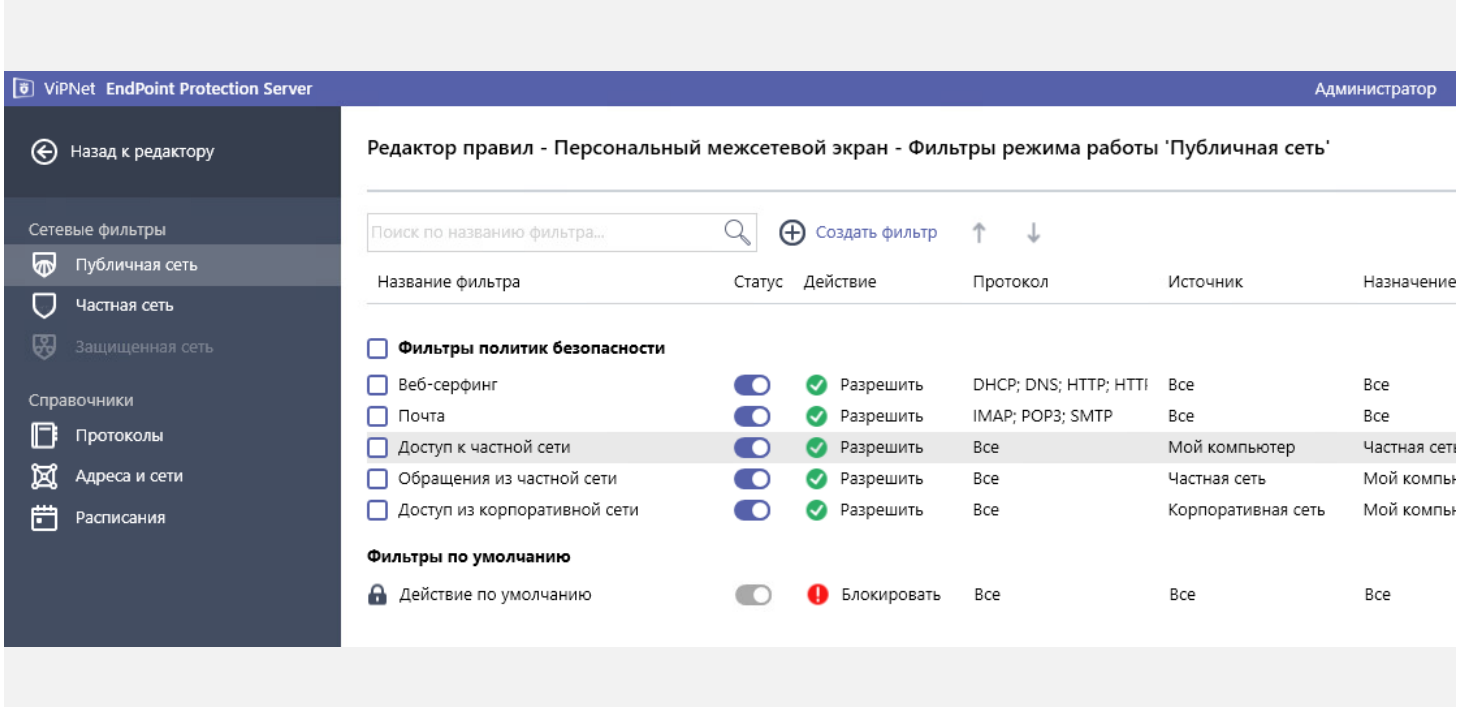
По правилам

Межсетевой экран

Несколько режимов работы
с преднастроенными фильтрами
от производителя

Администратор имеет возможность
добавлять/изменять/удалять
фильтры в режимах работы
«Частная сеть» и «Публичная сеть»

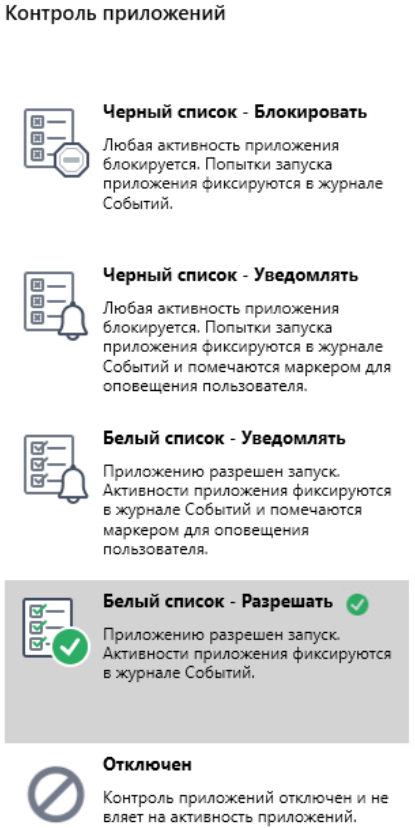
Межсетевой экран



Создание фильтров аналогично PFW, но т.к. это делается на сервере, имеется возможность рассылки на группы агентов.

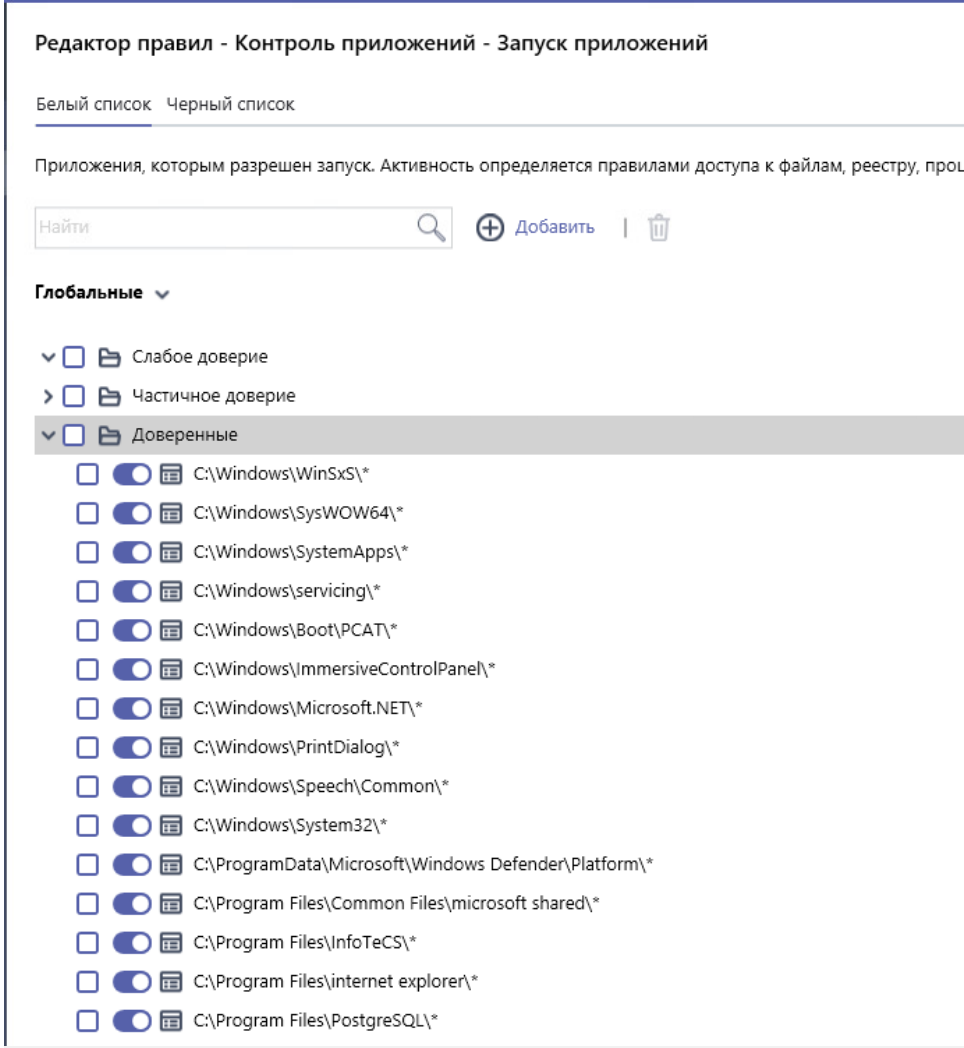
Контроль приложений

Возможность выбора режима работы Черного/Белого списка – с полной блокировкой или уведомлением о запуске



Контроль приложений

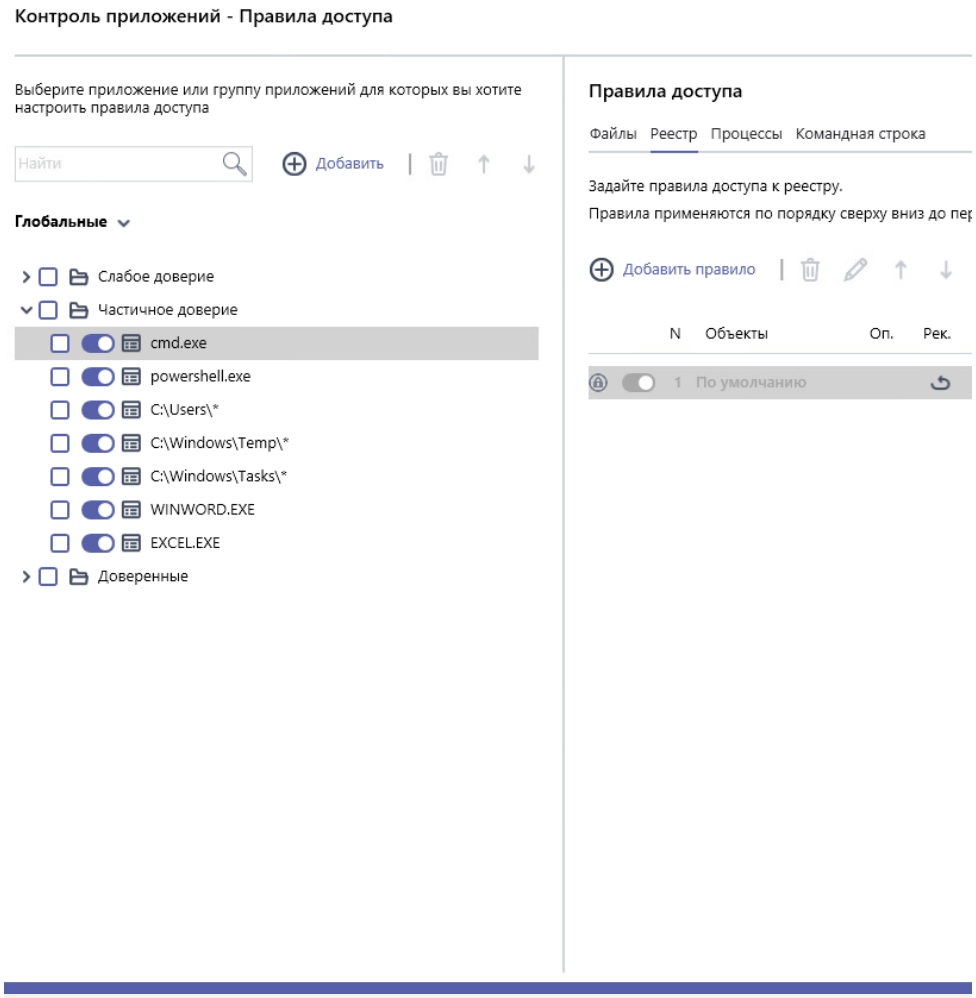
Возможность формирования Белых и Чёрных списков.



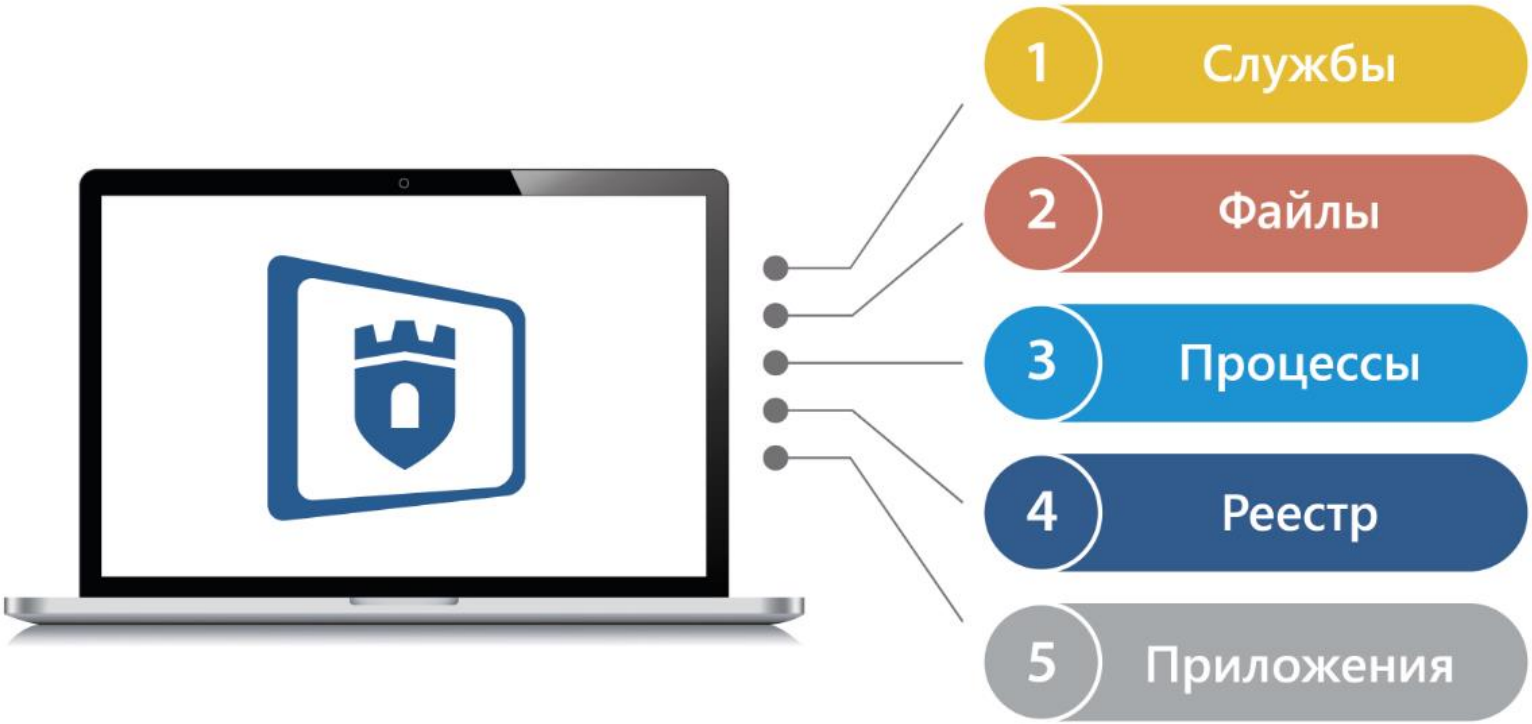
Контроль приложений
Правила доступа

Возможность создания правил доступа для приложений к следующим объектам:

- Файлам
- Реестру
- Процессам
- Командной строке

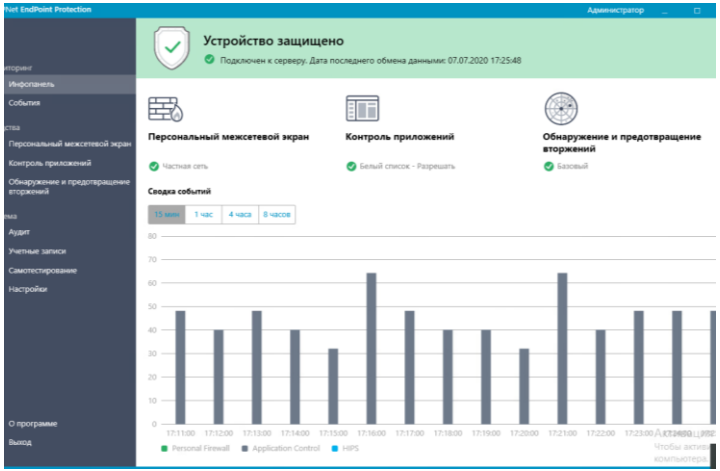


Полная защита

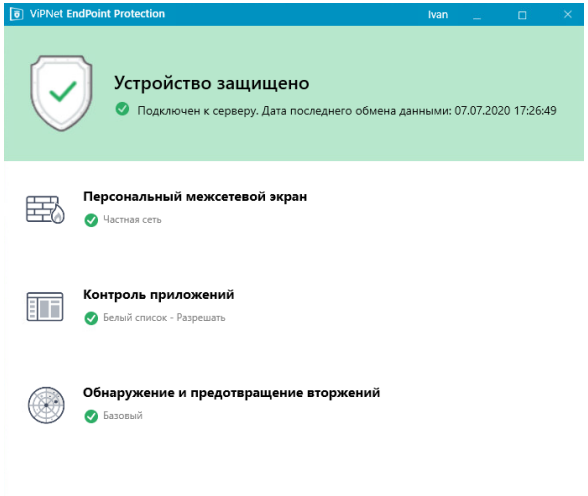


Это только кратко про сервер ViPNet EndPoint Protection, а есть ещё…

А есть ещё агент…



… на котором администратор может локально изменять настройки…



… а доверенный пользователь только менять режим работы для себя

Поддерживаемые ОС

- Microsoft Windows 10 (64-разрядная)
- Microsoft Windows 8.1 (64-разрядная)
- Microsoft Windows Server 2012 R2 (Standard или Datacenter)
- Microsoft Windows Server 2016 (Standard или Datacenter)

Ожидание по сертификации

Продукт передан на сертификацию по линии

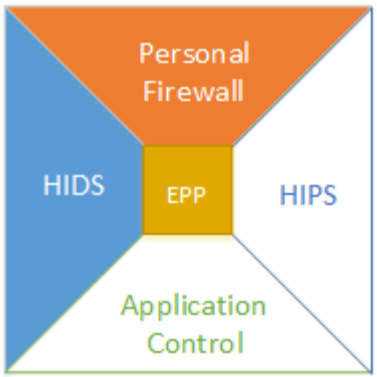
ФСТЭК России по требованиям к:

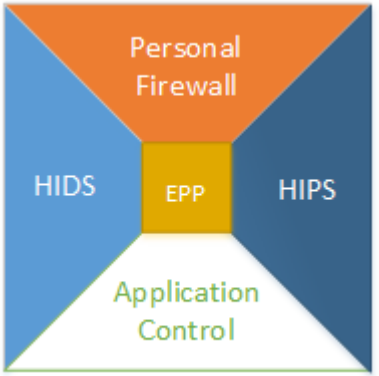
- Системам обнаружения вторжений уровня узла 4 класс ИТ.СОВ.У4.ПЗ
- Межсетевым экранам типа В класса 4 (ИТ.МЭ.В4.ПЗ)
- 4 классу ТДБ

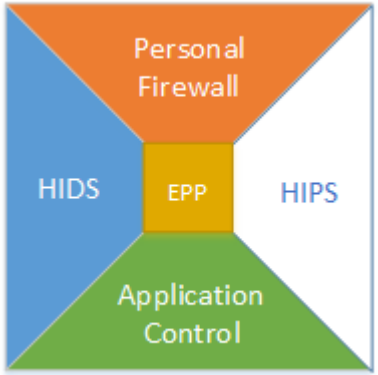
Схема лицензирования

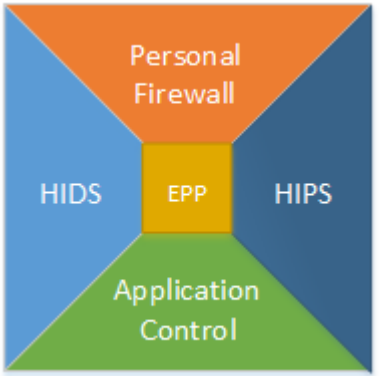
Модульный продукт

- Пользователь может сам выбрать нужный набор модулей в зависимости от имеющихся задач и бюджета









Лицензирование

Лицензия устанавливается на ViPNet EPP Сервер и определяет:

- MAX-количество защищаемых узлов, которые разрешено подключить серверу.
- Срок скачивания баз правил и загрузки баз правил на ViPNet EPP Сервер.
- Максимальную версию ViPNet EPP Сервер, до которой возможно обновление.
- Вариант разрешенных модулей одинаковый для всех защищаемых узлов:
  - Personal Firewall + HIDS.
  - Personal Firewall + HIDS + HIPS.
  - Personal Firewall + HIDS + HIPS + Application Control.

ЛИЦЕНЗИЯ

Состояние:	Лицензия активирована
Идентификатор лицензии:	1818468/1/1-EPP
Дата окончания обновления баз правил:	25.03.2021
Дата окончания действия лицензии:	02.10.2020

ДОСТУПНЫЕ МОДУЛИ	ВСЕГО	ИСПОЛЬЗОВАНО	ОСТАЛОСЬ
HIDS	25	1	24
Personal Firewall	25	1	24
Application Control	25	1	24
HIPS	25	1	24

Перспективы развития

Что дальше?

- Агент для Linux:
  - Astra Linux Special Edition 1.6 релиз «Смоленск»
  - Ред ОС 7.2
  - АльтЛинукс 8 СП
- Возможность управления ViPNet SafeBoot
- Расширение возможностей модуля эвристики (аномальные запуски системных утилит, перехват системных вызовов, сканирование памяти для отслеживания code injection и fileless атак)
- WebControl
- Интеграция с ViPNet Client 4U

Вместо эпилога

Текущая концепция защиты рабочих станций

ViPNet SafeBoot

ViPNet Client 4U

ViPNet SafePoint

ViPNet EndPoint Protection

Вопросы?

Иван Кадыков,
руководитель направления
Ivan.Kadykov@infotecs.ru

infotecs

Спасибо
за внимание!