Обзор новых продуктов линейки ViPNet Endpoint Security. Свежий взгляд на классические подходы к защите Endpoint.

Пролог

Текущий состав линейки продуктов для защиты рабочих станций и серверов

ViPNet IDS HS
Система обнаружения вторжений

ViPNet SafeBoot
Средство доверенной загрузки

ViPNet Personal Firewall
Персональный межсетевой экран

ViPNet Client
VPN-Клиент, Межсетевой экран, Деловая почта

С другой стороны…

- Необходимо не только обнаруживать, но и блокировать/предотвращать атаки
- Необходимо централизованное управление всех продуктов линейки продуктов для защиты рабочих станций и серверов
- Необходимо классическое СЗИ от НСД для комплексного выполнения требований по построению различных автоматизированных систем

От знаний к реализации

Endpoint Protection

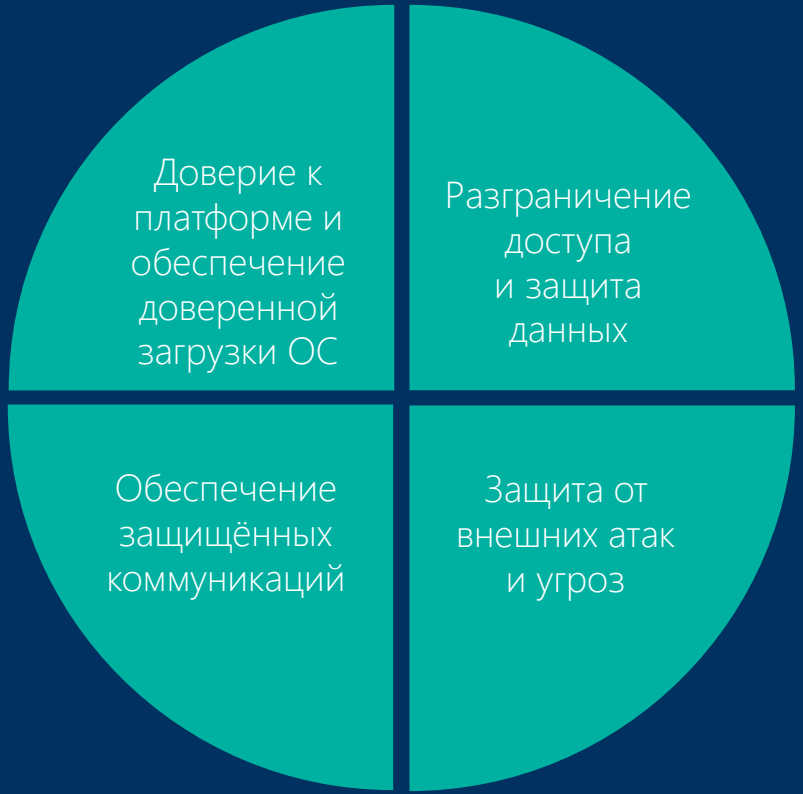
Классический Endpoint Protection	• знаем, что ищем (антивирус). Блокируем, что знаем (МЭ + HIPS), контролируем подключение устройств
Next Generation Endpoint Protection	• классический endpoint + модули по обнаружению и противодействию современным угрозам (ransomware, fileless-атаки, never-before-seen attacks) – Sandbox, Appcontrol, Memory Protection…
Endpoint Detection & Response	• NG EPP + возможность расследования инцидента и формирование реакции на инцидент (forensic)

«Российский Endpoint»

Средство защиты
от несанкционированного доступа

«Конечные устройства» – главная цель

Растущее количество атак и не доверенных аппаратных компонент



Пользователь - внутренний нарушитель, низкий уровень опыта

Удалённая работа, проведение приватных разговоров

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

ViPNet SafeBoot

ViPNet SafeBoot

Высокотехнологичный программный модуль доверенной загрузки, устанавливаемый в UEFI BIOS различных производителей. Предназначен для защиты компьютеров и серверов (в т.ч. и серверов виртуализации) от современных угроз НСД, связанных с загрузкой ОС и атак на сам BIOS.

Решаемые задачи ViPNet SafeBoot

ТЕХНО 2020 infotecs фест

Организация доверенной загрузки

Контроль целостности

- UEFI BIOS
- MBR
- Таблицы ACPI, SMBIOS, карты распределения памяти
- Файлов
- CMOS

Разграничение доступа

- Двухфакторная аутентификация
- Авторизация в AD/LDAP

Сертифицировано

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3823

Выдан 14 ноября 2017 г.
Действителен до 14 ноября 2020 г.

Настоящий сертификат удостоверяет, что **программный комплекс «Программный модуль доверенной загрузки ViPNet SafeBoot»**, разработанный и производимый ОАО «ИнфоТеКС» в соответствии с техническими условиями ФРКЕ.00180-01 97 01 ТУ, является программным средством доверенной загрузки уровня базовой системы ввода-вывода соответствует требованиям документов «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013) и «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты. ИТ.СДЗ.УБ2.ПЗ» (ФСТЭК России, 2013) при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00180-01 30 01 ФО.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004) - техническое заключение от 28.07.2017, экспертного заключения от 12.10.2017 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ОАО «ИнфоТеКС» (ИНН 7710013769)
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
Телефон: (495) 737-6192

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ООО «ЦБИ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В. Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
14 ноября 2017 г.

Сертифицирован по требованиям руководящих документов к средствам доверенной загрузки уровня базовой системы ввода-вывода второго класса и возможность использования в ИСПДн до УЗ1 включительно и в ГИС до 1-го класса защищенности включительно

ViPNet SafePoint

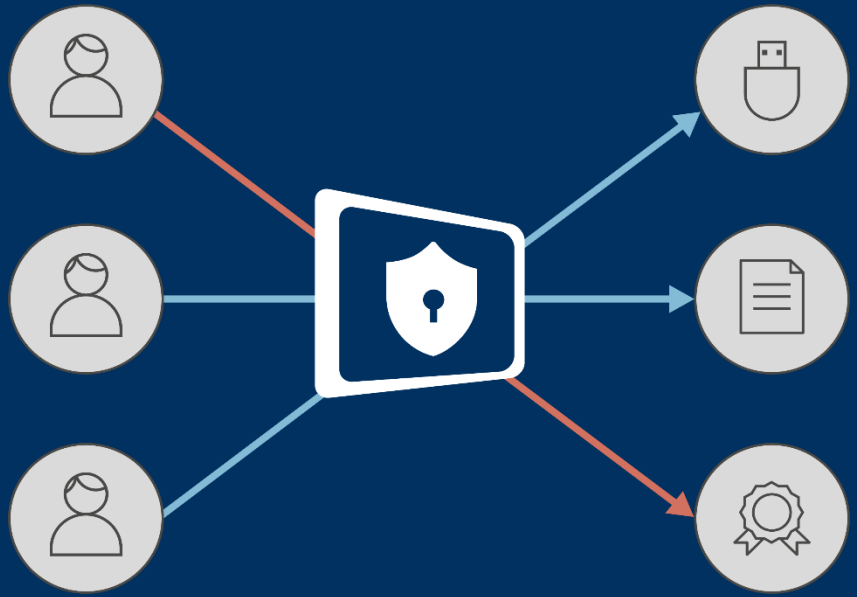
ViPNet SafePoint

Средство защиты информации от несанкционированного доступа, устанавливаемое на рабочие станции и сервера, предназначенное для мандатного и дискреционного разграничения доступа к критически важной информации.

Реализована разграничительная (пользователя к объектам) и разделительная (между пользователями) политика доступа, основанная на автоматической разметке создаваемых файлов.

Ключевая функциональность

- Двухфакторная аутентификация пользователей
- Поддержка USB-токенов и смарт-карт:
  - JaCarta ГОСТ
  - JaCarta PKI
  - JaCarta LT
  - Rutoken S
  - Rutoken Lite
  - Rutoken ЭЦП



Дискреционный контроль доступа пользователей

Разграничительная политика
на основе матрицы доступа

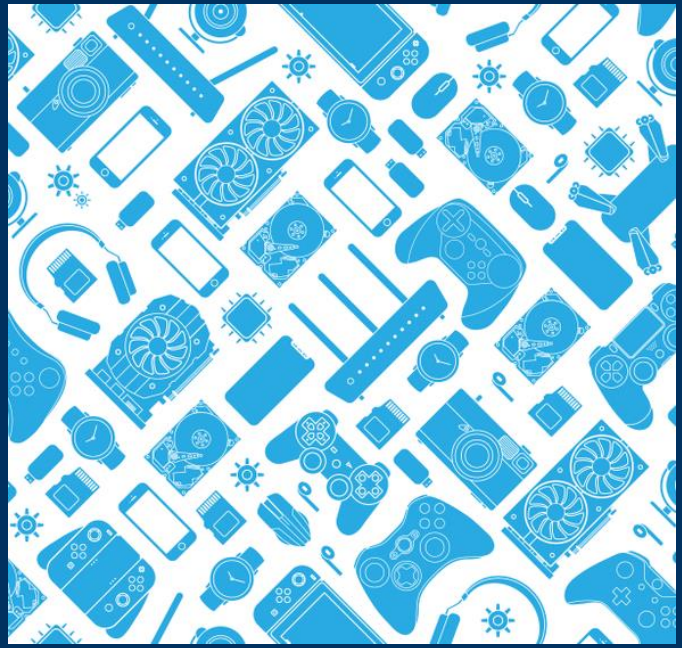
Мандатный контроль доступа пользователей и процессов

Разграничительная политика
на основе меток безопасности

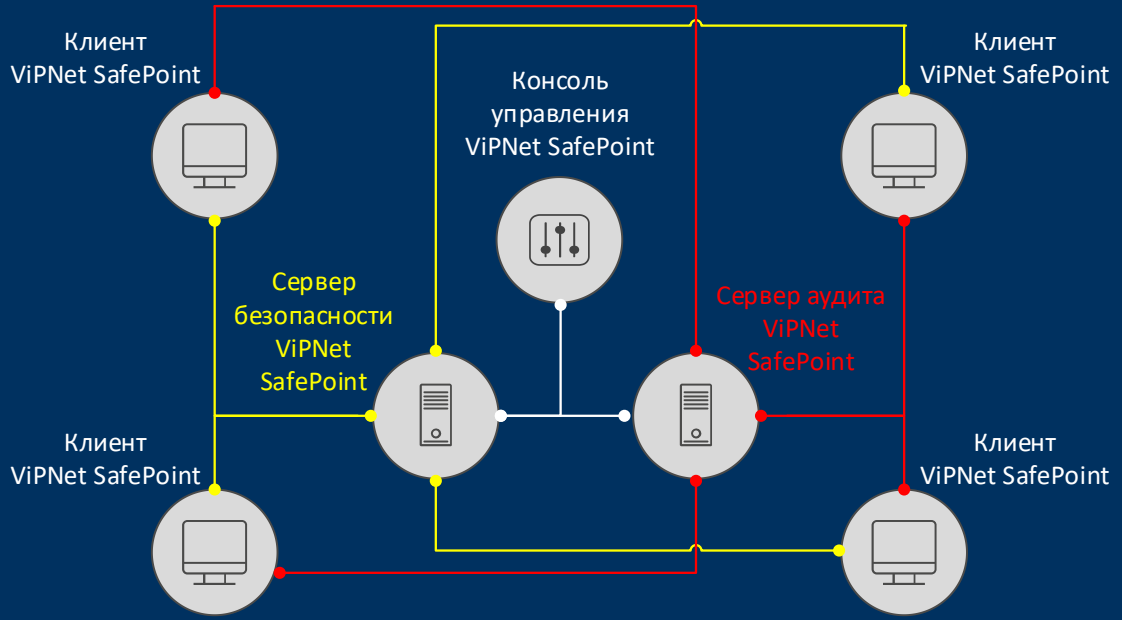
Замкнутая программная среда

- Защита от модификации запускаемых модулей
- Контроль запуска скриптов Active Scripts
- Контроль запуска задач

Контроль устройств



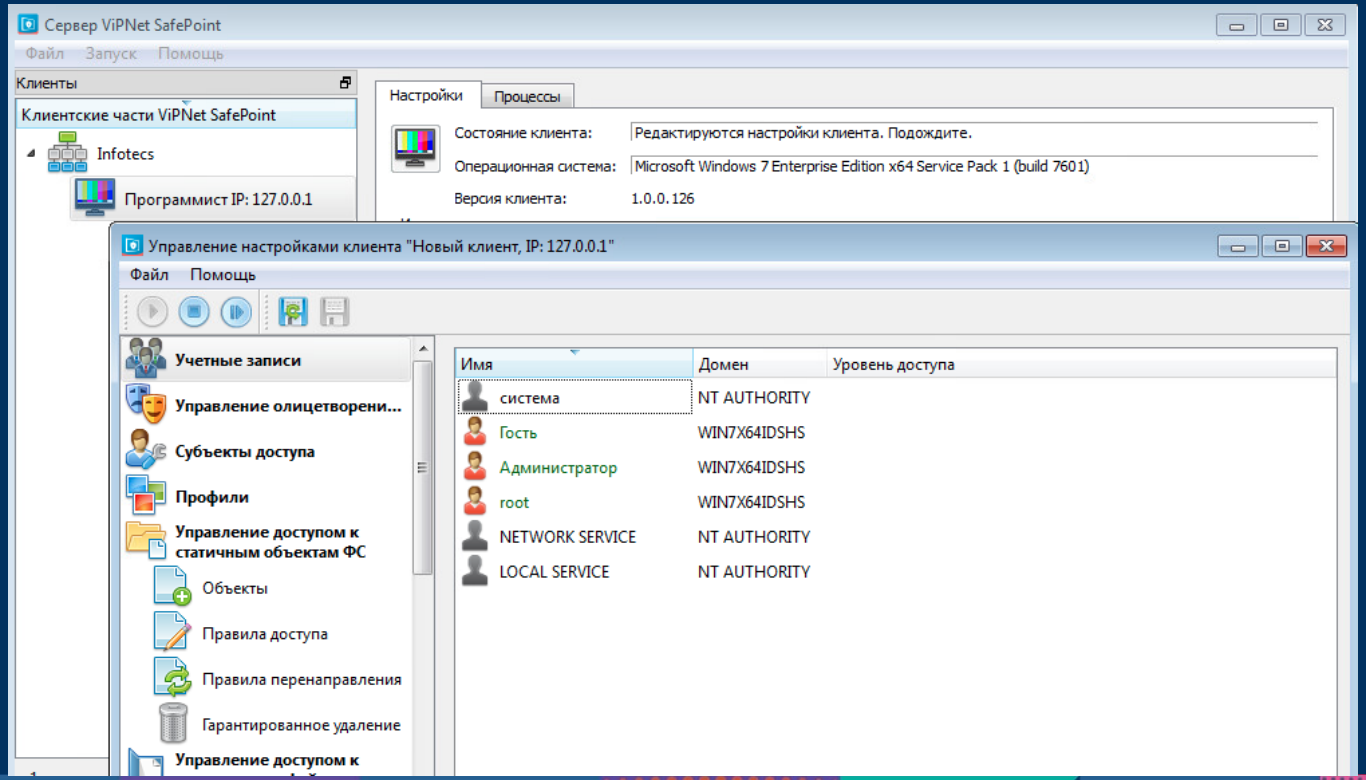
- Контроль и разграничения доступа к подключаемым внешним устройствам
- Разграничение доступа к принтерам



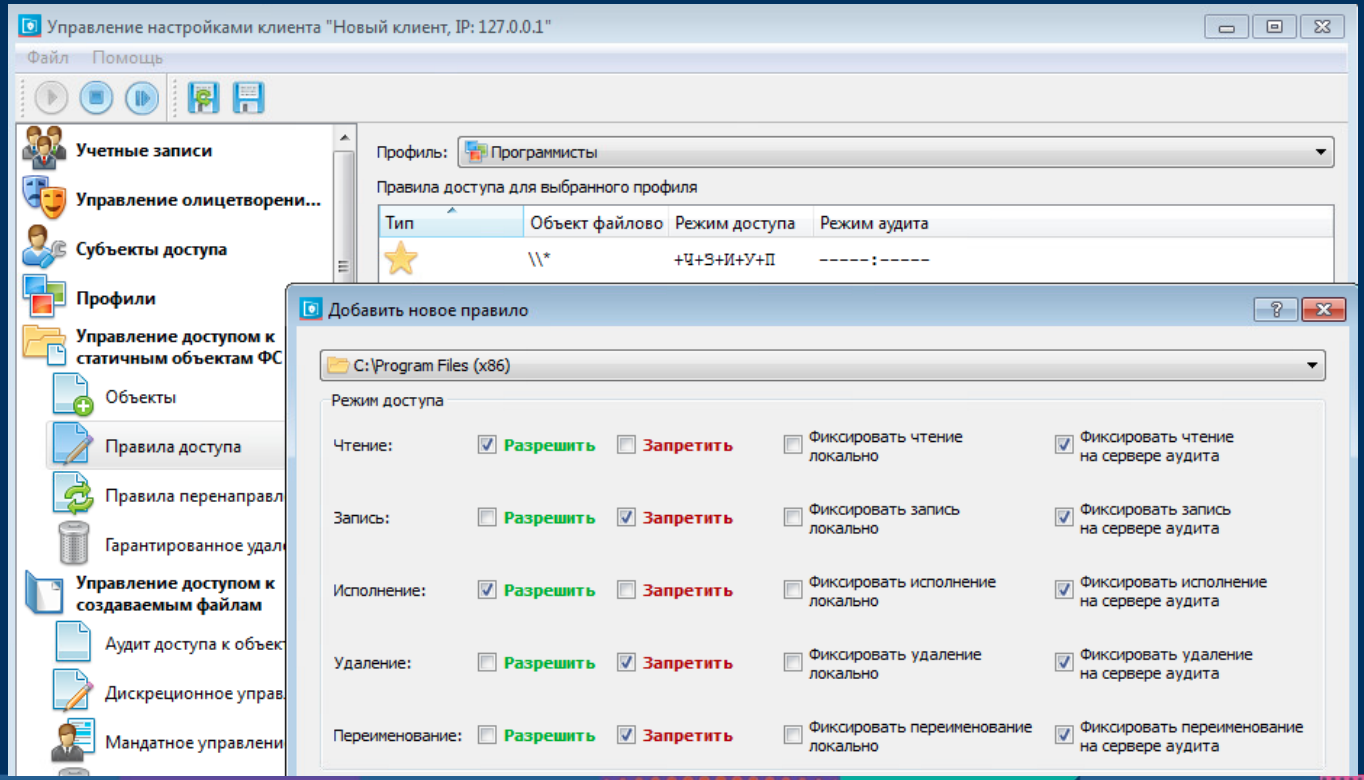
Архитектура ViPNet SafePoint

- Клиент
- Сервер безопасности
- Сервер аудита
- Консоль управления

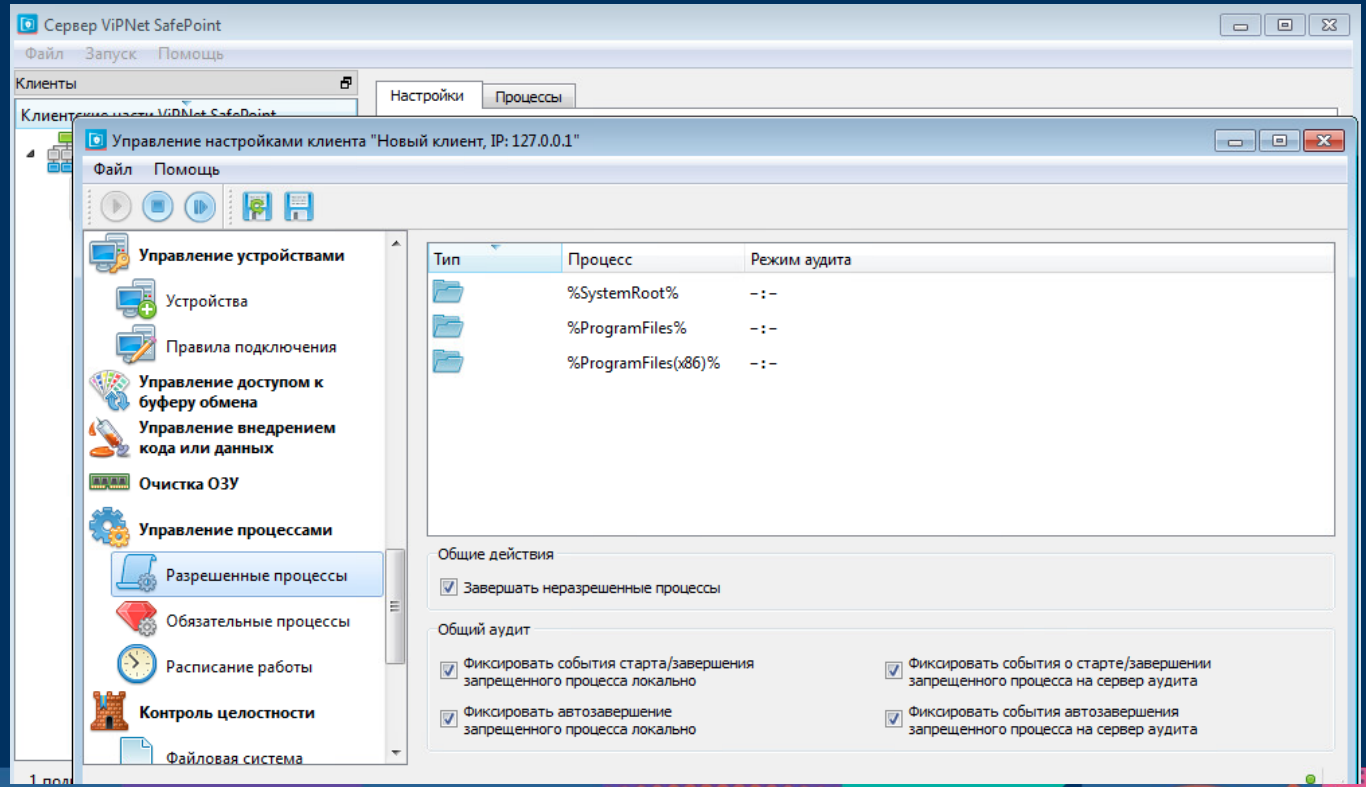
Интеграция с Active Directory



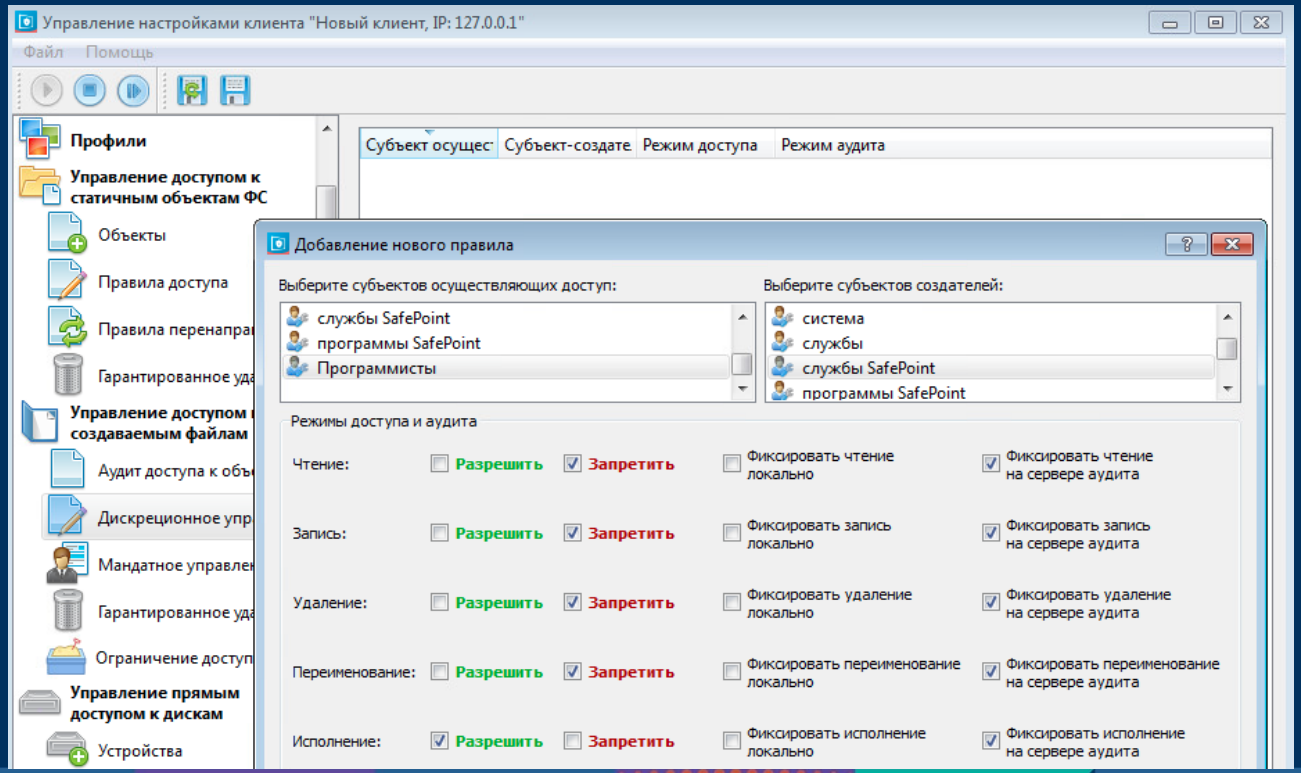
Создание правила доступа



Настройка разрешённых процессов



Дискреционное управление доступом



Ожидание по сертификации

Продукт передан на сертификацию по линии ФСТЭК России по требованиям к:

- 5 классу защищенности СВТ
- 4 классу защиты СКН (ИТ.СКН.П4.ПЗ)
- 4 классу ТДБ

ViPNet EndPoint Protection

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. Ключевыми модулями системы являются персональный межсетевой экран, система обнаружения и предотвращения вторжений, а также контроль приложений.

Обнаружение и предотвращение атак

Используем:

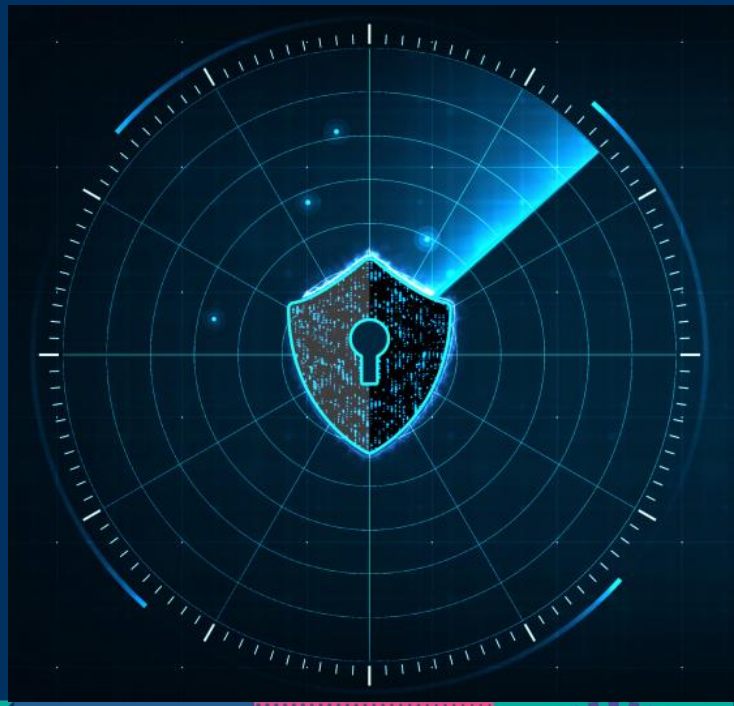
- Эвристический анализ
- Сигнатурный анализ

Следим за:

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

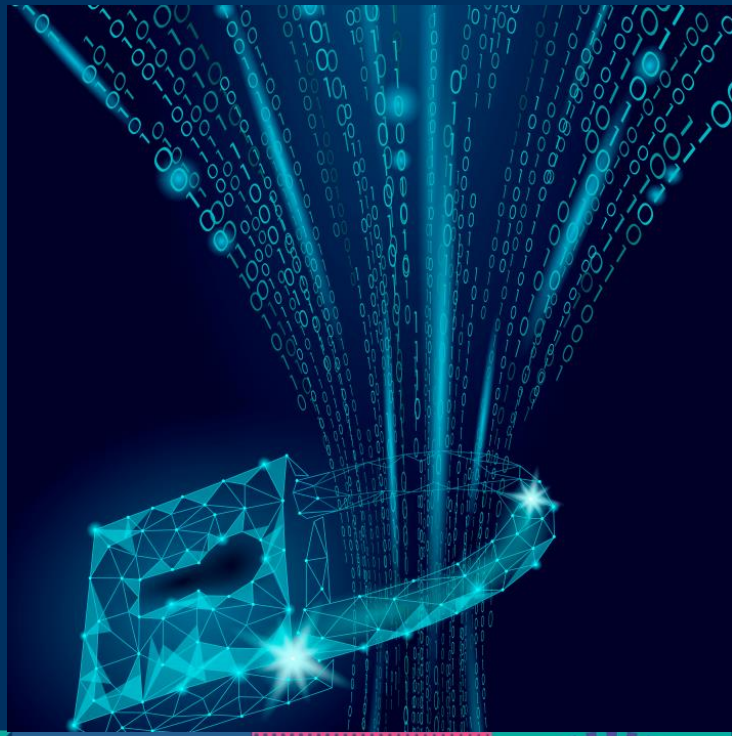
Блокируем:

- Подозрительный сетевой трафик
- Атакующие хосты



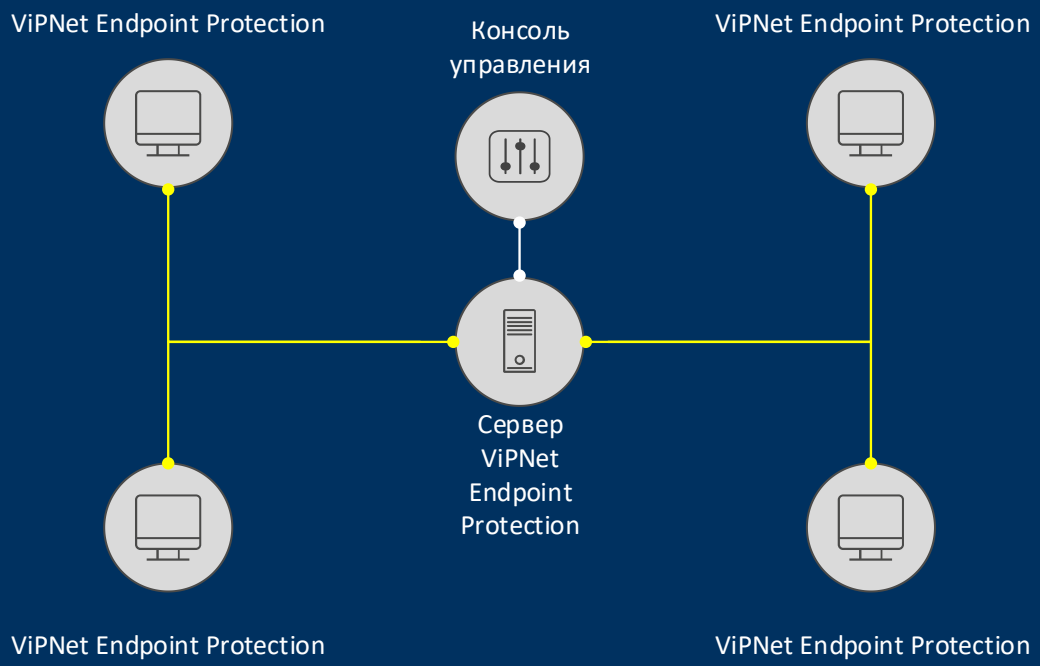
Межсетевое экранирование

- 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



Архитектура ViPNet Endpoint Protection

- Клиент
- Сервер
- Консоль управления

ViPNet EndPoint Protection Server — Администратор

Мониторинг
- Инфопанель
- События

Управление защитой
- Устройства
- Базы правил
- Учетные записи

Сервис
- Журналы
- Обнаружение аномалий

Конфигурация
- Параметры системы
- Передача данных
- Политика аудита

О программе
Выход

Инфопанель

Персональный межсетевой экран

Режим	Хосты
Полная блокировка трафика	0
Публичная сеть	0
Частная сеть	1
Защищенная сеть	0
Сетевой экран отключен	0
Всего	1

Контроль приложений

Режим	Хосты
Черный список - Блокировать	0
Черный список - Уведомлять	0
Белый список - Уведомлять	0
Белый список - Разрешать	1
Отключен	0
Всего	1

Обнаружение и предотвращение вторжений

Режим	Хосты
Усиленный	0
Базовый	1
Минимальный	0
Отключен	0
Всего	1

Запросы на подключение

Всего запросов 0

Доступно лицензий 24

Актуальность баз правил

1 устройств с актуальными базами правил

0 устройств ожидают обновления

0 не назначено

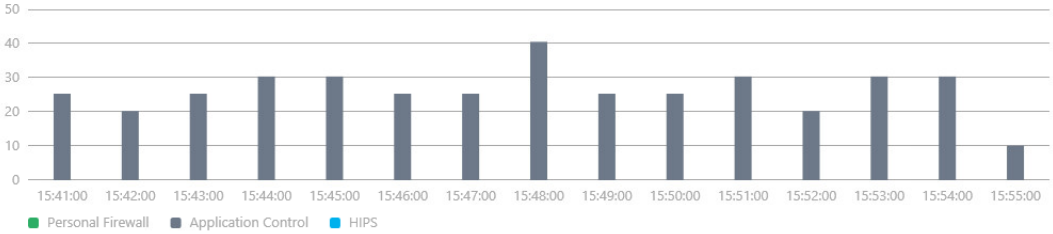
TIAS

Передача на IP **отключен**

Последний обмен **неизвестно**

Сводка событий

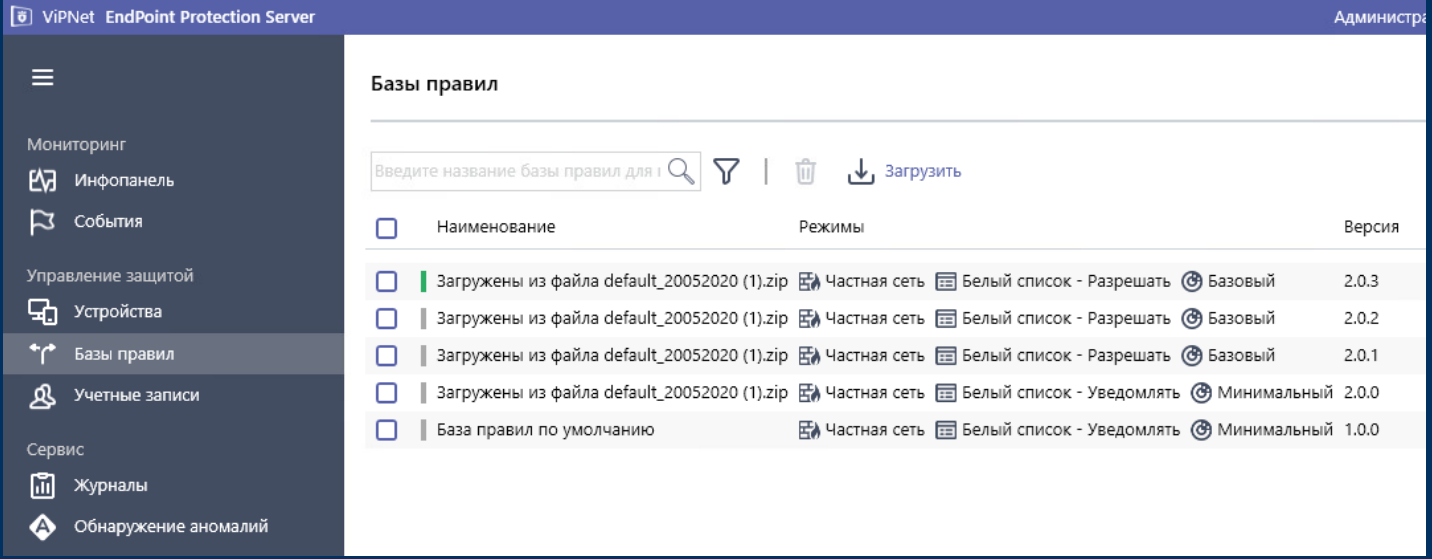
15 мин | 1 час | 4 часа | 8 часов



 | Версия ПО: 1.0.2.64494

ТЕХНО 2020 infotecs ФЕСТ

Консоль управления сервером



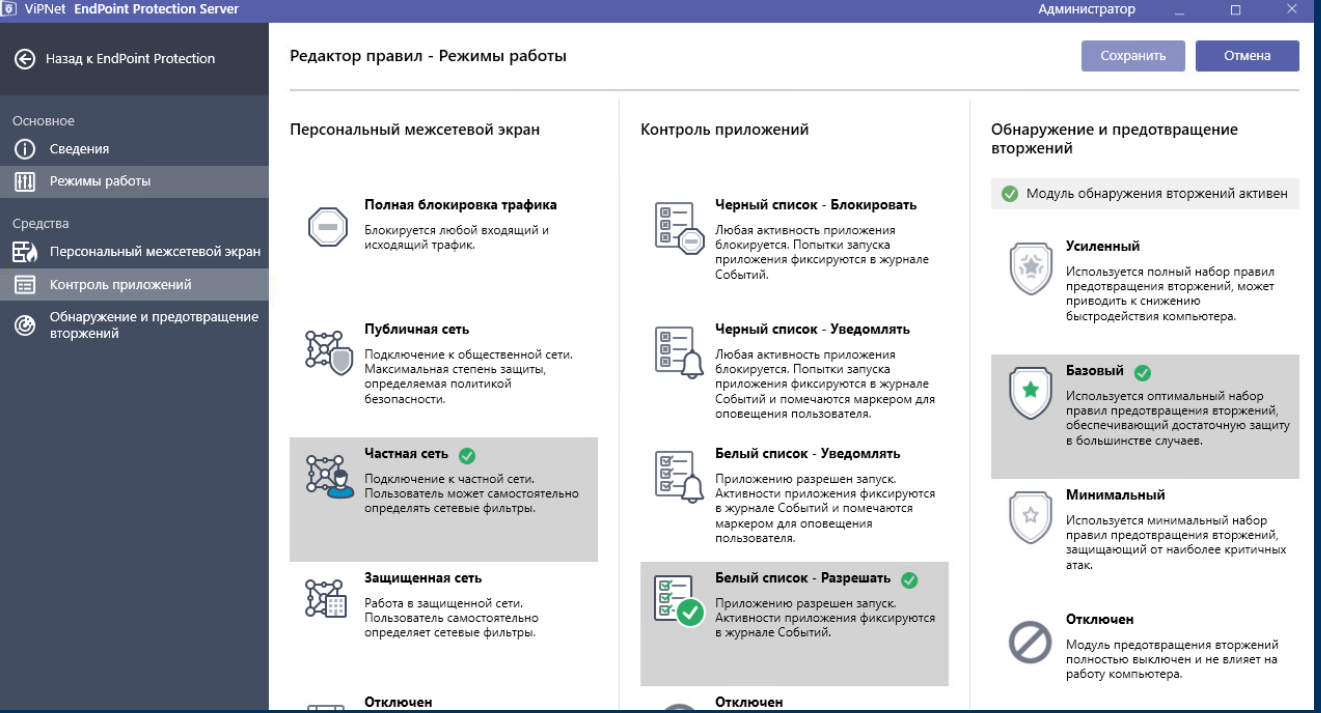
ТЕХНО 2020 infotecs ФЕСТ

Работаем по правилам!

EndPoint Protection работает по БРП

Состоит из:

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



ТЕХНО 2020 infotecs ФЕСТ

Настройки модулей – Режимы работы

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

Обнаружение и предотвращение вторжений

ТЕХНО 2020 infotecs ФЕСТ

Обнаружение вторжений активно всегда.

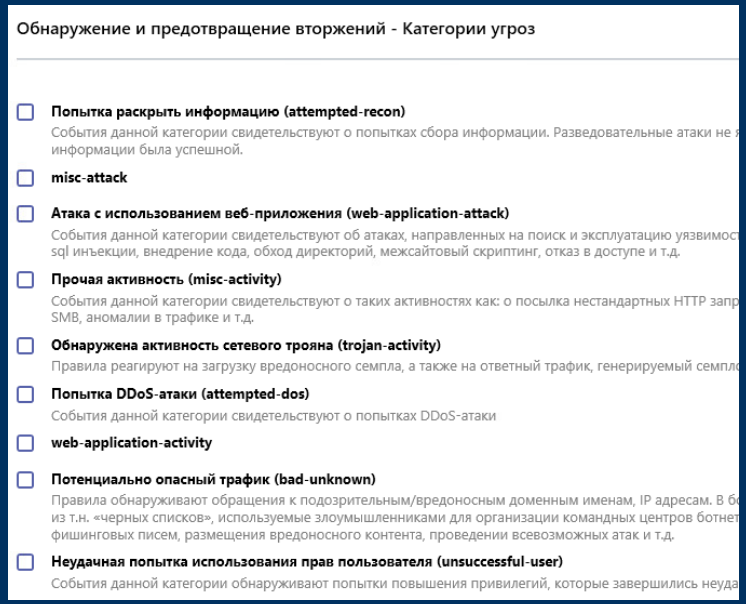
Механизмы работы схожи с ViPNet IDS HS:

- Загрузили БРП
- Назначили на группу агентов
- Агенты, получив БРП, мониторят события в соответствии с заданными политиками аудита

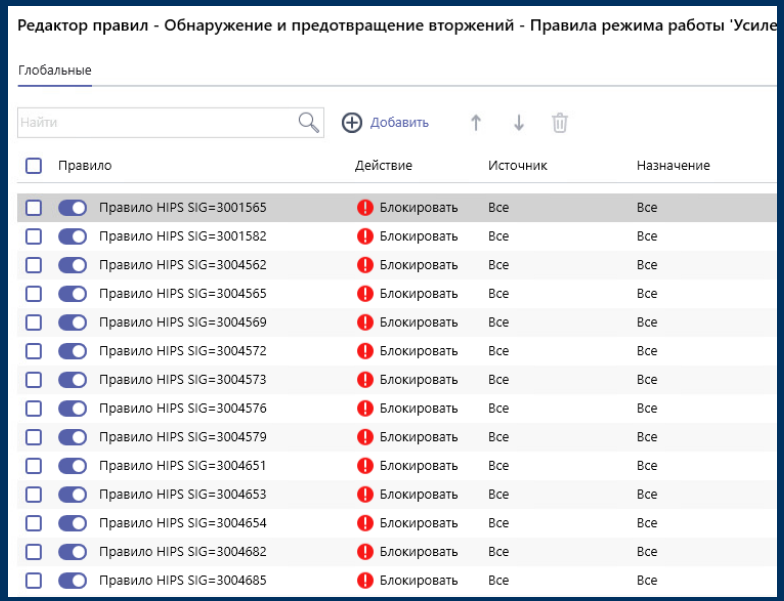
Предотвращение вторжений – имеется несколько уровней защиты – Усиленный, Базовый, Минимальный (разрабатывали совместно с ПМ)

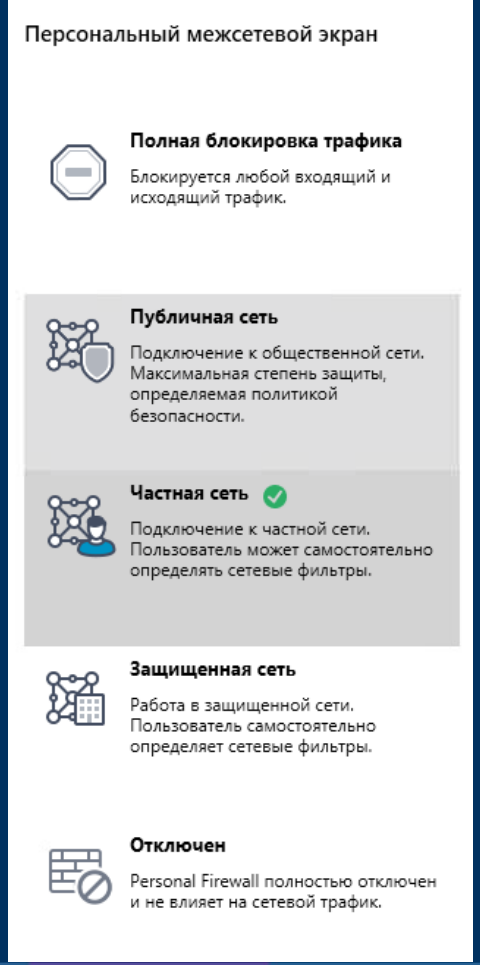
Предотвращение вторжений

По категориям угроз



По правилам



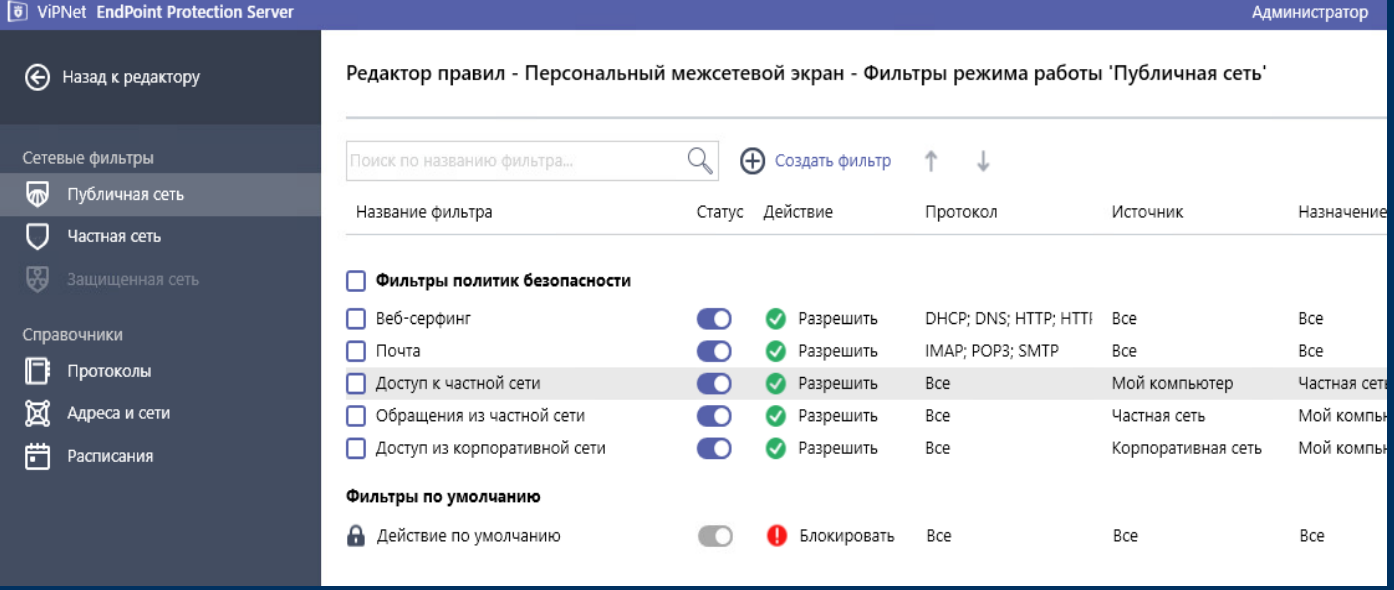


ТЕХНО 2020 infotecs фест

Межсетевой экран

Несколько режимов работы с преднастроенными фильтрами от производителя

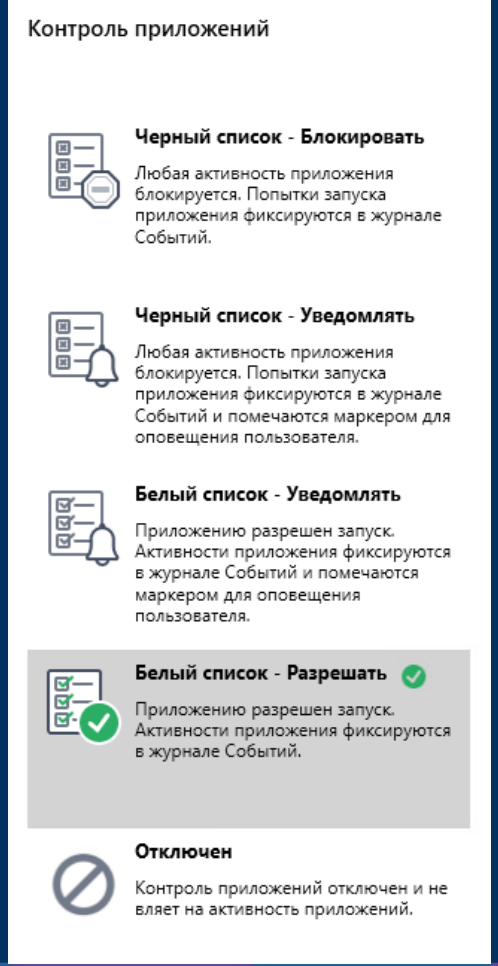
Администратор имеет возможность добавлять/изменять/удалять фильтры в режимах работы «Частная» и «Публичная сеть»



ТЕХНО infotecs 2020 ФЕСТ

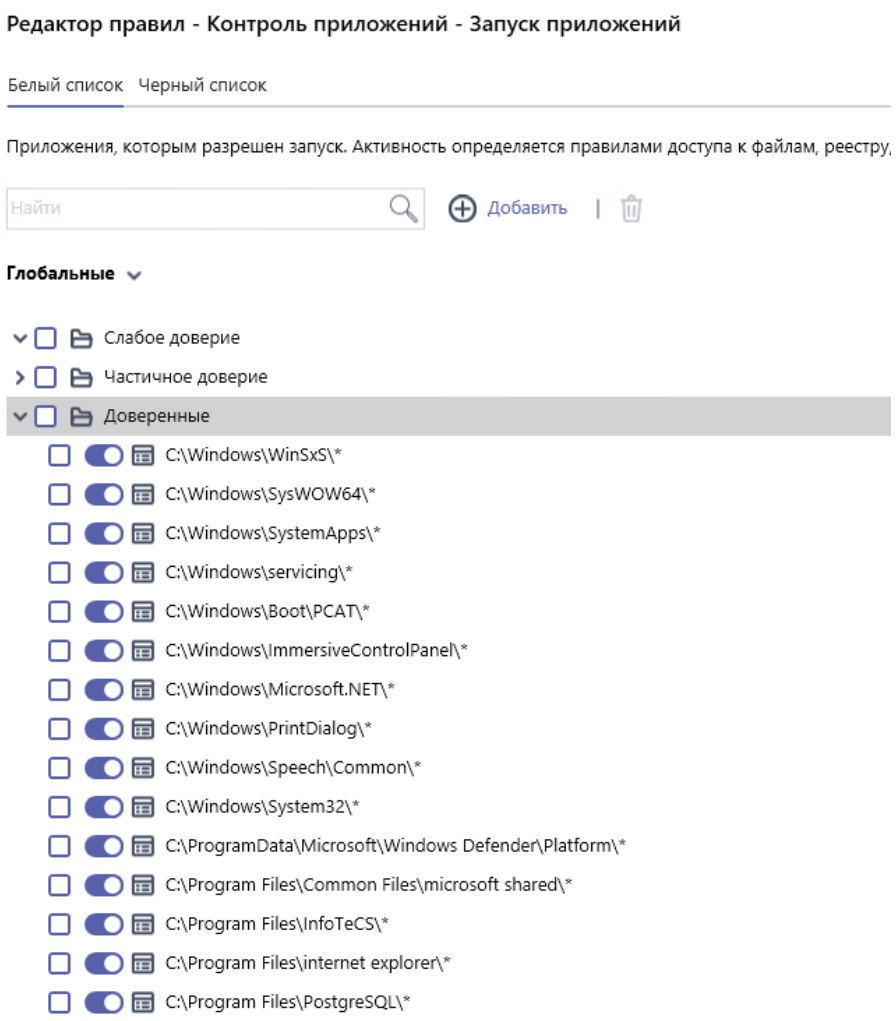
Межсетевой экран

Создание фильтров аналогично PFW, но т.к. это делается на сервере, имеется возможность рассылки на группы агентов с модулем персонального межсетевого экранирования



Контроль приложений

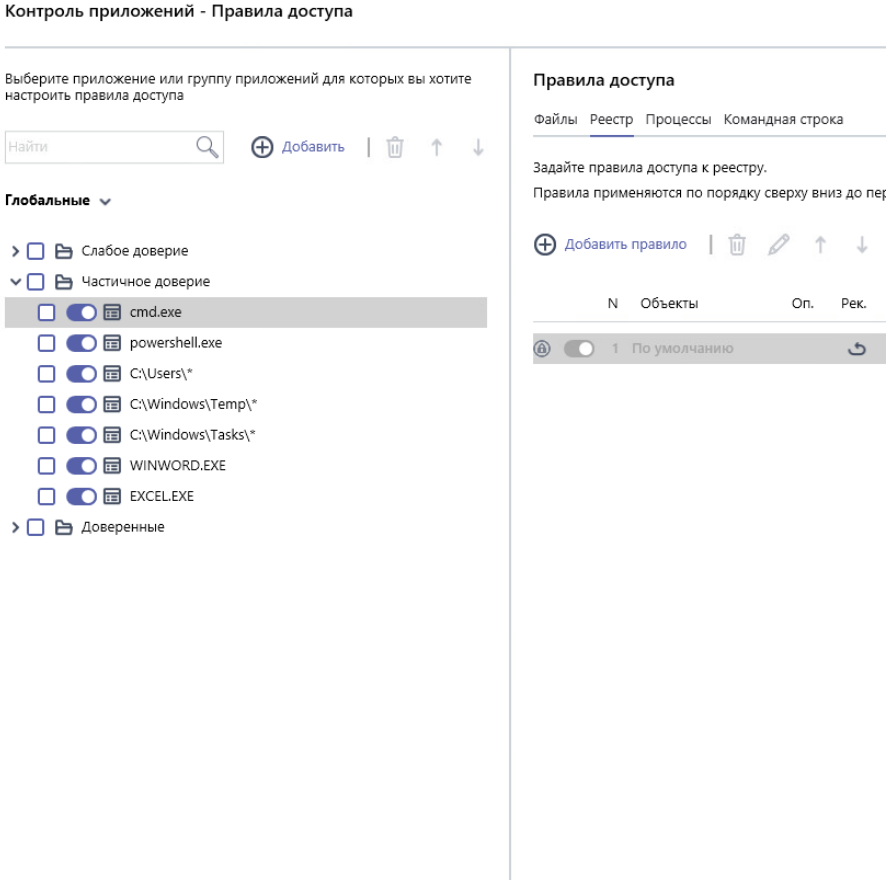
Возможность выбора режима работы Черного/Белого списка – с полной блокировкой или уведомлением о запуске



ТЕХНО infotecs 2020 ФЕСТ

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

Ещё немного о возможностях

- Возможность передачи данных из EPP в TIAS. Сейчас TIAS может обрабатывать ТОЛЬКО события системы обнаружения вторжений (исследования по работе с событиями от других модулей ведутся)
- Интеграция с Active Directory – для получения данных о хостах и распределения компьютеров и серверов в соответствии со структурой в AD
- Слежение за работой антивирусов Kaspersky Endpoint Security 11 для Windows или Dr.Web Desktop Security Suite 11 для Windows

Ожидание по сертификации

Продукт передан на сертификацию по линии ФСТЭК России по требованиям к:

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

Текущая концепция защиты рабочих станций

ТЕХНО 2020 infotecs ФЕСТ

ViPNet SafeBoot

Доверие к платформе и обеспечение доверенной загрузки ОС

Разграничение доступа и защита данных

ViPNet SafePoint

ViPNet Client 4U

Обеспечение защищённых коммуникаций

Защита от внешних атак и угроз

ViPNet EndPoint Protection

ТЕХНО 2020 infotecs Фест

Вопросы?

ТЕХНО 2020 infotecs Фест

Спасибо за внимание!