



техно infotecs
2020 ФЕСТ

ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

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

Доверие к платформе и обеспечение доверенной загрузки ОС

Разграничение доступа и защита данных

Пользователь - внутренний нарушитель, низкий уровень опыта

Удалённая работа, проведение частных разговоров

Обеспечение защищённых коммуникаций

Защита от внешних атак и угроз

Malware, Ransomware, 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.



Организация доверенной загрузки

Контроль целостности

Разграничение доступа

UEFI BIOS

MBR

Таблицы ACPI,
SMBIOS, карты
распределения
памяти

Файлов

CMOS

Двухфакторная
аутентификация

Авторизация
в AD/LDAP

Сертифицировано



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

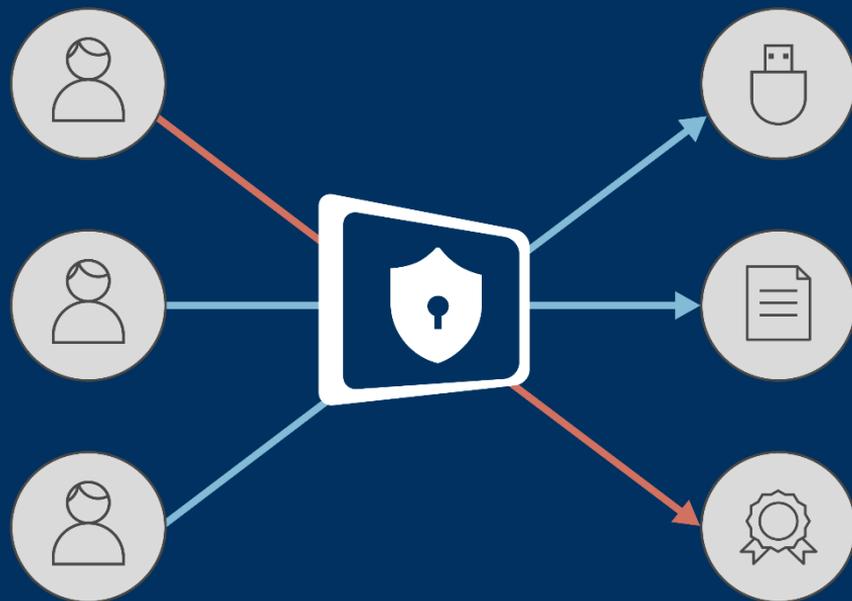
Средство защиты информации от несанкционированного доступа, устанавливаемое на рабочие станции и сервера, предназначенное для мандатного и дискреционного разграничения доступа к критически важной информации.

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

Ключевая функциональность

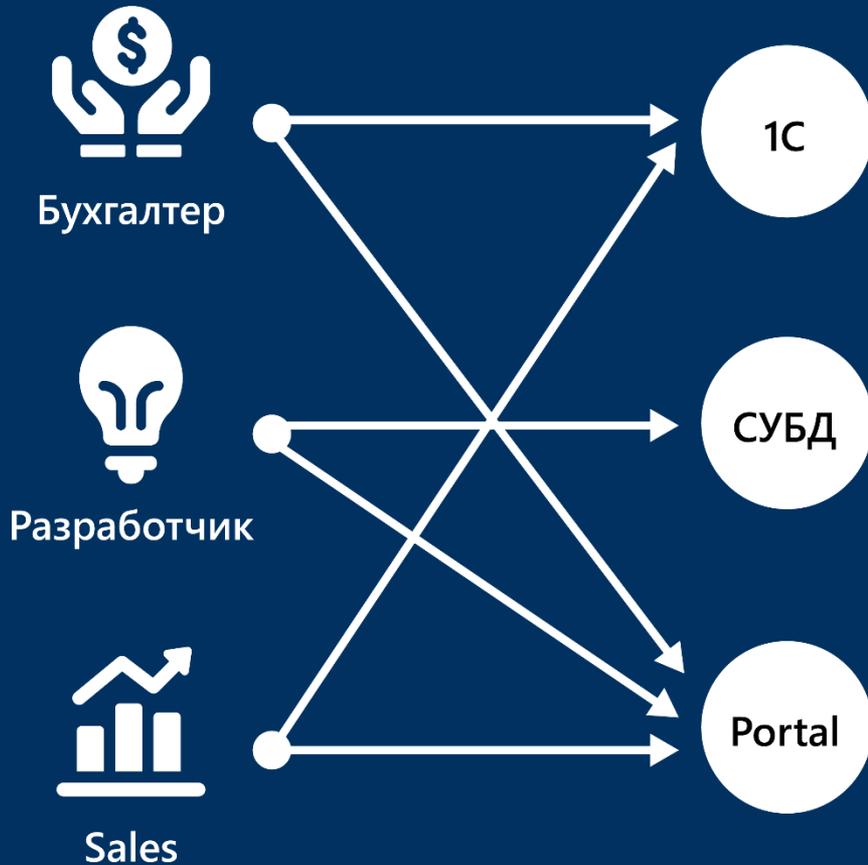
- Двухфакторная аутентификация пользователей
- Поддержка USB-токенов и смарт-карт:
 - JaCarta ГОСТ
 - JaCarta PKI
 - JaCarta LT
 - Rutoken S
 - Rutoken Lite
 - Rutoken ЭЦП





Дискреционный контроль
доступа пользователей

Разграничительная политика
на основе матрицы доступа



Мандатный контроль
доступа пользователей
и процессов

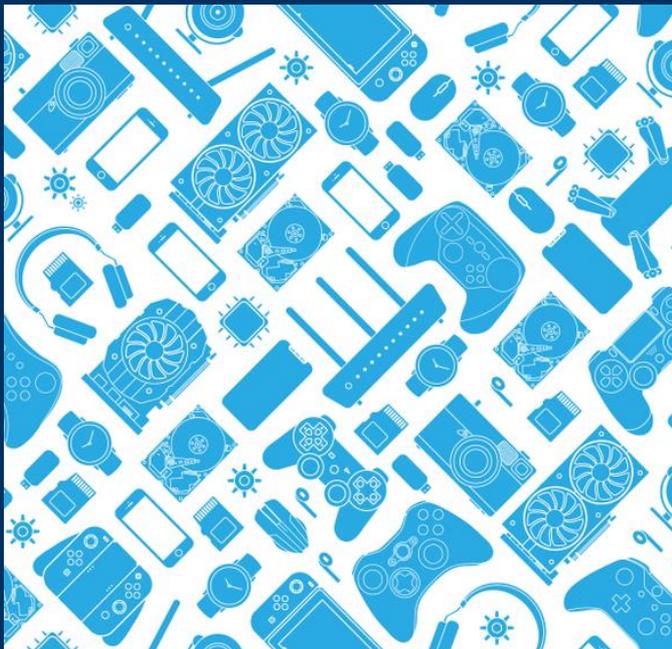
Разграничительная политика
на основе меток безопасности

Замкнутая программная среда



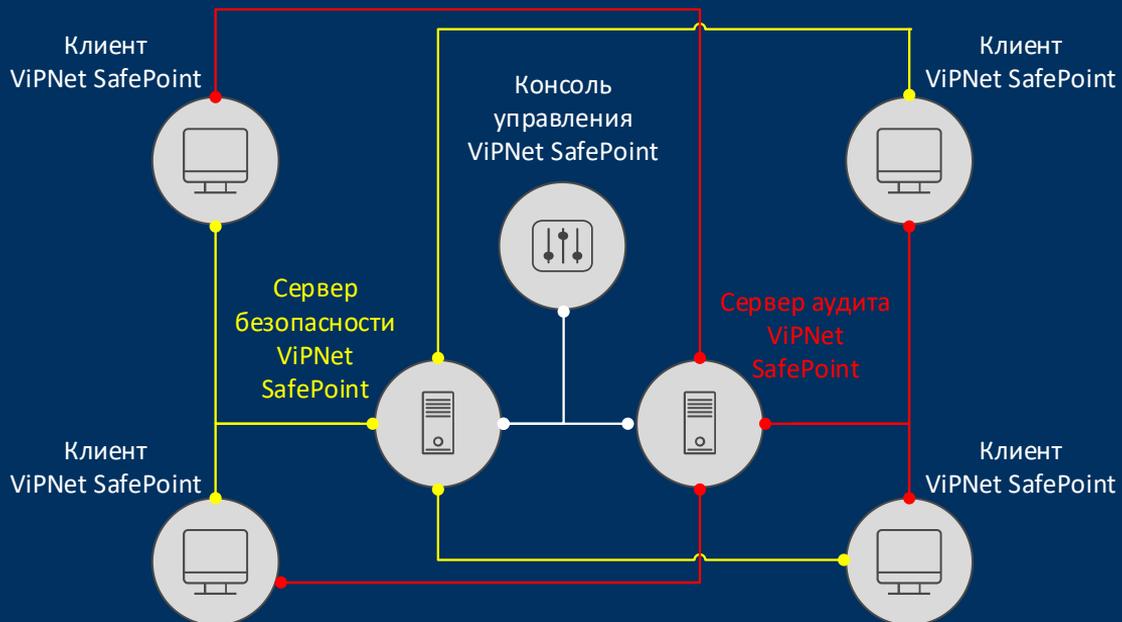
- Защита от модификации запускаемых модулей
- Контроль запуска скриптов Active Scripts
- Контроль запуска задач

Контроль устройств



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





Архитектура ViPNet SafePoint

- Клиент
- Сервер безопасности ViPNet SafePoint
- Сервер аудита ViPNet SafePoint
- Консоль управления ViPNet SafePoint

Интеграция с Active Directory

The screenshot displays the VIPNet SafePoint management console. The main window, titled "Сервер VIPNet SafePoint", shows a tree view of clients under the "Infotecs" organization. A specific client, "Программист IP: 127.0.0.1", is selected, and its settings are displayed in the main pane. The settings include the client's status, operating system (Microsoft Windows 7 Enterprise Edition x64 Service Pack 1), and version (1.0.0.126).

A secondary window, titled "Управление настройками клиента 'Новый клиент, IP: 127.0.0.1'", is open in the foreground. It shows a list of users and their access levels. The list is as follows:

Имя	Домен	Уровень доступа
система	NT AUTHORITY	
Гость	WIN7X64IDSHS	
Администратор	WIN7X64IDSHS	
root	WIN7X64IDSHS	
NETWORK SERVICE	NT AUTHORITY	
LOCAL SERVICE	NT AUTHORITY	

Создание правила доступа

Управление настройками клиента "Новый клиент, IP: 127.0.0.1"

Профиль: Программисты

Правила доступа для выбранного профиля

Тип	Объект файлово	Режим доступа	Режим аудита
★	*	+Ц+Э+И+У+П	-----

Добавить новое правило

C:\Program Files (x86)

Режим доступа

Чтение:	<input checked="" type="checkbox"/> Разрешить	<input type="checkbox"/> Запретить	<input type="checkbox"/> Фиксировать чтение локально	<input checked="" type="checkbox"/> Фиксировать чтение на сервере аудита
Запись:	<input type="checkbox"/> Разрешить	<input checked="" type="checkbox"/> Запретить	<input type="checkbox"/> Фиксировать запись локально	<input checked="" type="checkbox"/> Фиксировать запись на сервере аудита
Исполнение:	<input checked="" type="checkbox"/> Разрешить	<input type="checkbox"/> Запретить	<input type="checkbox"/> Фиксировать исполнение локально	<input checked="" type="checkbox"/> Фиксировать исполнение на сервере аудита
Удаление:	<input type="checkbox"/> Разрешить	<input checked="" type="checkbox"/> Запретить	<input type="checkbox"/> Фиксировать удаление локально	<input checked="" type="checkbox"/> Фиксировать удаление на сервере аудита
Переименование:	<input type="checkbox"/> Разрешить	<input checked="" type="checkbox"/> Запретить	<input type="checkbox"/> Фиксировать переименование локально	<input checked="" type="checkbox"/> Фиксировать переименование на сервере аудита

Настройка разрешённых процессов

Сервер VipNet SafePoint

Клиенты

Настройки Процессы

Управление настройками клиента "Новый клиент, IP: 127.0.0.1"

Файл Помощь

Управление устройствами

- Устройства
- Правила подключения

Управление доступом к буферу обмена

Управление внедрением кода или данных

Очистка ОЗУ

Управление процессами

- Разрешенные процессы**
- Обязательные процессы
- Расписание работы

Контроль целостности

- Файловая система

Тип	Процесс	Режим аудита
Папка	%SystemRoot%	- :-
Папка	%ProgramFiles%	- :-
Папка	%ProgramFiles(x86)%	- :-

Общие действия

- Завершать неразрешенные процессы

Общий аудит

- Фиксировать события старта/завершения запрещенного процесса локально
- Фиксировать события автозавершения запрещенного процесса локально
- Фиксировать события о старте/завершении запрещенного процесса на сервер аудита
- Фиксировать события автозавершения запрещенного процесса на сервер аудита

Дискреционное управление доступом

The screenshot displays the Windows Firewall rule configuration interface. The main window is titled "Управление настройками клиента 'Новый клиент, IP: 127.0.0.1'". A sub-window titled "Добавление нового правила" is open, showing the configuration for a new rule. The rule is named "Субъект-создате" and is currently in the "Режим доступа" (Access Mode) tab.

The "Выберите субъектов осуществляющих доступ:" (Select subjects to grant access to) list includes:

- службы SafePoint
- программы SafePoint
- Программисты

The "Выберите субъектов создателей:" (Select subjects to create rules for) list includes:

- система
- службы
- службы SafePoint
- программы SafePoint

The "Режимы доступа и аудита" (Access and audit modes) section is configured as follows:

Режим	Разрешить	Запретить	Фиксировать локально	Фиксировать на сервере аудита
Чтение:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Запись:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Удаление:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Переименование:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Исполнение:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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:

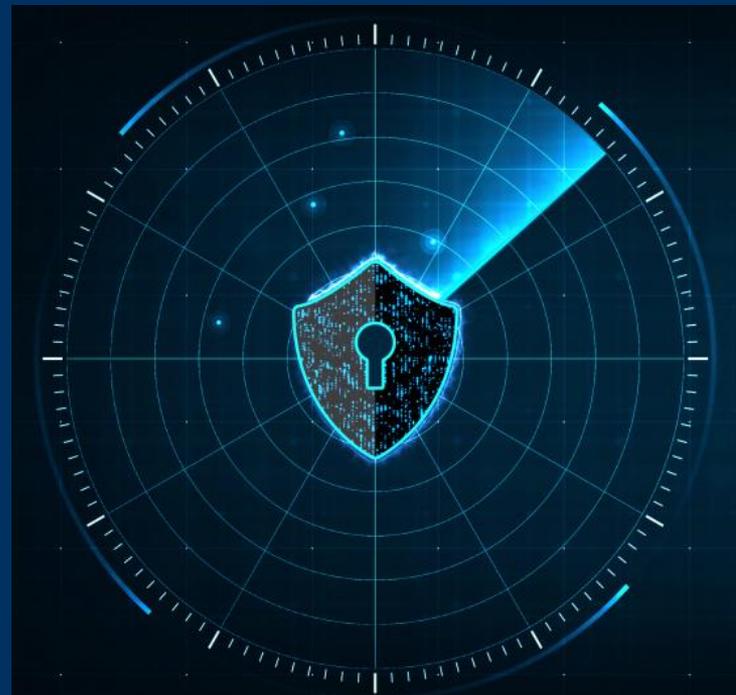
- Эвристический анализ
- Сигнатурный анализ

Следим за:

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

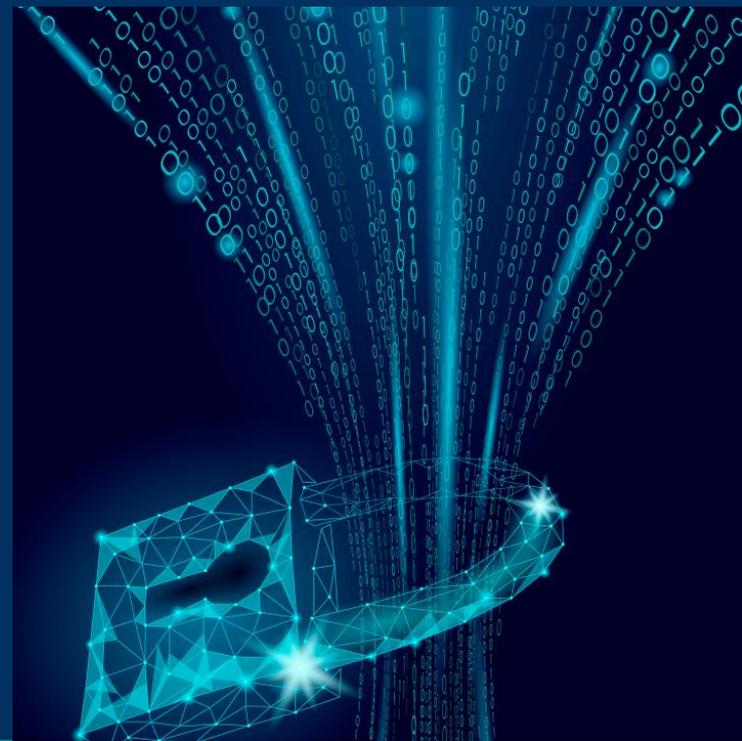
Блокируем:

- Подозрительный сетевой трафик
- Атакующие хосты



Межсетевое экранирование

- Фильтрация трафика Ipv4 и Ipv6
- Работа сетевых фильтров по расписанию
- Наличие предустановленных 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

WHITELIST

BLACKLIST



ViPNet Endpoint Protection



Консоль
управления



Сервер
ViPNet
Endpoint
Protection

ViPNet Endpoint Protection



ViPNet Endpoint Protection

ViPNet Endpoint Protection

Архитектура ViPNet Endpoint Protection

- Клиент
- Сервер
- Консоль управления

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

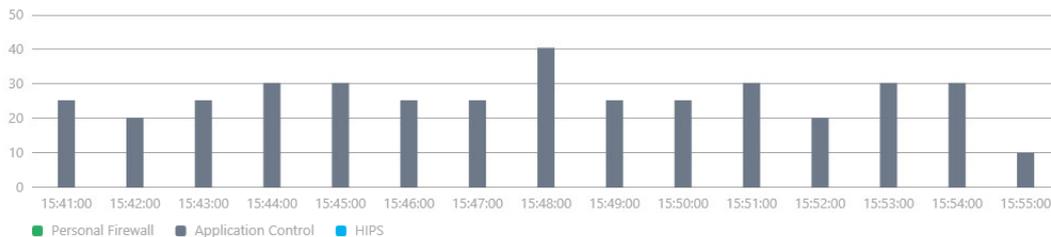
1 устройств с актуальными базами правил
 0 устройств ожидают обновления
 0 не назначено

TIAS

⚠ Передача на IP отключен
 ✅ Последний обмен неизвестно

Сводка событий

15 мин 1 час 4 часа 8 часов



Консоль
управления
сервером

Базы правил

Введите название базы правил для | 🔍 | 🗑️ | 📄 Загрузить

<input type="checkbox"/>	Наименование	Режимы	Версия
<input type="checkbox"/>	Загружены из файла default_20052020 (1).zip	Частная сеть Белый список - Разрешать Базовый	2.0.3
<input type="checkbox"/>	Загружены из файла default_20052020 (1).zip	Частная сеть Белый список - Разрешать Базовый	2.0.2
<input type="checkbox"/>	Загружены из файла default_20052020 (1).zip	Частная сеть Белый список - Разрешать Базовый	2.0.1
<input type="checkbox"/>	Загружены из файла default_20052020 (1).zip	Частная сеть Белый список - Уведомлять Минимальный	2.0.0
<input type="checkbox"/>	База правил по умолчанию	Частная сеть Белый список - Уведомлять Минимальный	1.0.0

Работаем по правилам!

EndPoint Protection работает по БРП

Состоит из:

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

← Назад к EndPoint Protection

Основное

- Сведения
- Режимы работы**
- Средства
- Персональный межсетевой экран
- Контроль приложений
- Обнаружение и предотвращение вторжений

Редактор правил - Режимы работы

Сохранить Отмена

Персональный межсетевой экран

- Полная блокировка трафика**
Блокируется любой входящий и исходящий трафик.
- Публичная сеть**
Подключение к общественной сети. Максимальная степень защиты, определяемая политикой безопасности.
- Частная сеть** ✓
Подключение к частной сети. Пользователь может самостоятельно определять сетевые фильтры.
- Защищенная сеть**
Работа в защищенной сети. Пользователь самостоятельно определяет сетевые фильтры.
- Отключен**

Контроль приложений

- Черный список - Блокировать**
Любая активность приложения блокируется. Попытки запуска приложения фиксируются в журнале Событий.
- Черный список - Уведомлять**
Любая активность приложения блокируется. Попытки запуска приложения фиксируются в журнале Событий и помечаются маркером для оповещения пользователя.
- Белый список - Уведомлять**
Приложению разрешен запуск. Активности приложения фиксируются в журнале Событий и помечаются маркером для оповещения пользователя.
- Белый список - Разрешать** ✓
Приложению разрешен запуск. Активности приложения фиксируются в журнале Событий.
- Отключен**

Обнаружение и предотвращение вторжений

- ✓ Модуль обнаружения вторжений активен
- Усиленный**
Используется полный набор правил предотвращения вторжений, может приводить к снижению быстродействия компьютера.
- Базовый** ✓
Используется оптимальный набор правил предотвращения вторжений, обеспечивающий достаточную защиту в большинстве случаев.
- Минимальный**
Используется минимальный набор правил предотвращения вторжений, защищающий от наиболее критичных атак.
- Отключен**
Модуль предотвращения вторжений полностью выключен и не влияет на работу компьютера.



Настройки модулей –
Режимы работы

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



✔ Модуль обнаружения вторжений активен



Усиленный

Используется полный набор правил предотвращения вторжений, может приводить к снижению быстродействия компьютера.



Базовый ✔

Используется оптимальный набор правил предотвращения вторжений, обеспечивающий достаточную защиту в большинстве случаев.



Минимальный

Используется минимальный набор правил предотвращения вторжений, защищающий от наиболее критичных атак.



Отключен

Модуль предотвращения вторжений полностью выключен и не влияет на работу компьютера.

Обнаружение и предотвращение вторжений

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

Обнаружение и предотвращение вторжений - Категории угроз

- Попытка раскрыть информацию (attempted-recon)**
События данной категории свидетельствуют о попытках сбора информации. Разведывательные атаки на информацию были успешной.
- misc-attack**
- Атака с использованием веб-приложения (web-application-attack)**
События данной категории свидетельствуют об атаках, направленных на поиск и эксплуатацию уязвимостей: sql инъекции, внедрение кода, обход директорий, межсайтовый скриптинг, отказ в доступе и т.д.
- Прочая активность (misc-activity)**
События данной категории свидетельствуют о таких активностях как: отправка нестандартных HTTP запросов, SMB, аномалии в трафике и т.д.
- Обнаружена активность сетевого трояна (trojan-activity)**
Правила реагируют на загрузку вредоносного семпла, а также на ответный трафик, генерируемый семплом.
- Попытка DDoS-атаки (attempted-dos)**
События данной категории свидетельствуют о попытках DDoS-атаки
- web-application-activity**
- Потенциально опасный трафик (bad-unknown)**
Правила обнаруживают обращения к подозрительным/вредоносным доменным именам, IP адресам. В базе т.н. «черных списков», используемые злоумышленниками для организации командных центров ботнетов, фишинговых писем, размещения вредоносного контента, проведении всевозможных атак и т.д.
- Неудачная попытка использования прав пользователя (unsuccessful-user)**
События данной категории обнаруживают попытки повышения привилегий, которые завершились неудачно.

По правилам

Редактор правил - Обнаружение и предотвращение вторжений - Правила режима работы 'Усиление'

Глобальные

Найти 🔍 ➕ Добавить ↑ ↓ 🗑️

<input type="checkbox"/>	Правило	Действие	Источник	Назначение
<input checked="" type="checkbox"/>	Правило HIPS SIG=3001565	❗ Блокировать	Все	Все
<input type="checkbox"/>	Правило HIPS SIG=3001582	❗ Блокировать	Все	Все
<input type="checkbox"/>	Правило HIPS SIG=3004562	❗ Блокировать	Все	Все
<input type="checkbox"/>	Правило HIPS SIG=3004565	❗ Блокировать	Все	Все
<input type="checkbox"/>	Правило HIPS SIG=3004569	❗ Блокировать	Все	Все
<input type="checkbox"/>	Правило HIPS SIG=3004572	❗ Блокировать	Все	Все
<input type="checkbox"/>	Правило HIPS SIG=3004573	❗ Блокировать	Все	Все
<input type="checkbox"/>	Правило HIPS SIG=3004576	❗ Блокировать	Все	Все
<input type="checkbox"/>	Правило HIPS SIG=3004579	❗ Блокировать	Все	Все
<input type="checkbox"/>	Правило HIPS SIG=3004651	❗ Блокировать	Все	Все
<input type="checkbox"/>	Правило HIPS SIG=3004653	❗ Блокировать	Все	Все
<input type="checkbox"/>	Правило HIPS SIG=3004654	❗ Блокировать	Все	Все
<input type="checkbox"/>	Правило HIPS SIG=3004682	❗ Блокировать	Все	Все
<input type="checkbox"/>	Правило HIPS SIG=3004685	❗ Блокировать	Все	Все



Полная блокировка трафика

Блокируется любой входящий и исходящий трафик.



Публичная сеть

Подключение к общественной сети. Максимальная степень защиты, определяемая политикой безопасности.



Частная сеть

Подключение к частной сети. Пользователь может самостоятельно определять сетевые фильтры.



Защищенная сеть

Работа в защищенной сети. Пользователь самостоятельно определяет сетевые фильтры.



Отключен

Personal Firewall полностью отключен и не влияет на сетевой трафик.

Межсетевой экран

Несколько режимов работы с предустановленными фильтрами от производителя

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

Назад к редактору

Сетевые фильтры

- Публичная сеть
- Частная сеть
- Защищенная сеть

Справочники

- Протоколы
- Адреса и сети
- Расписания

Редактор правил - Персональный межсетевой экран - Фильтры режима работы 'Публичная сеть'

Поиск по названию фильтра...

+ Создать фильтр ↑ ↓

Название фильтра	Статус	Действие	Протокол	Источник	Назначение
Фильтры политик безопасности					
<input type="checkbox"/> Веб-серфинг	<input checked="" type="checkbox"/>	Разрешить	DHCP; DNS; HTTP; HTTP	Все	Все
<input type="checkbox"/> Почта	<input checked="" type="checkbox"/>	Разрешить	IMAP; POP3; SMTP	Все	Все
<input type="checkbox"/> Доступ к частной сети	<input checked="" type="checkbox"/>	Разрешить	Все	Мой компьютер	Частная сеть
<input type="checkbox"/> Обращения из частной сети	<input checked="" type="checkbox"/>	Разрешить	Все	Частная сеть	Мой компьютер
<input type="checkbox"/> Доступ из корпоративной сети	<input checked="" type="checkbox"/>	Разрешить	Все	Корпоративная сеть	Мой компьютер
Фильтры по умолчанию					
<input checked="" type="checkbox"/> Действие по умолчанию	<input type="checkbox"/>	Блокировать	Все	Все	Все

Межсетевой экран

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



Черный список - Блокировать

Любая активность приложения блокируется. Попытки запуска приложения фиксируются в журнале Событий.



Черный список - Уведомлять

Любая активность приложения блокируется. Попытки запуска приложения фиксируются в журнале Событий и помечаются маркером для оповещения пользователя.



Белый список - Уведомлять

Приложению разрешен запуск. Активности приложения фиксируются в журнале Событий и помечаются маркером для оповещения пользователя.



Белый список - Разрешать ✔

Приложению разрешен запуск. Активности приложения фиксируются в журнале Событий.



Отключен

Контроль приложений отключен и не влияет на активность приложений.

Контроль приложений

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

Приложения, которым разрешен запуск. Активность определяется правилами доступа к файлам, реестру,

Найти   [Добавить](#) | 

Глобальные ▾

 Слабое доверие

 Частичное доверие

 Доверенные

-  C:\Windows\WinSxS*
-  C:\Windows\SysWOW64*
-  C:\Windows\SystemApps*
-  C:\Windows\servicing*
-  C:\Windows\Boot\PCAT*
-  C:\Windows\ImmersiveControlPanel*
-  C:\Windows\Microsoft.NET*
-  C:\Windows\PrintDialog*
-  C:\Windows\Speech\Common*
-  C:\Windows\System32*
-  C:\ProgramData\Microsoft\Windows Defender\Platform*
-  C:\Program Files\Common Files\microsoft shared*
-  C:\Program Files\InfoTeCS*
-  C:\Program Files\internet explorer*
-  C:\Program Files\PostgreSQL*

Контроль приложений

Возможность формирования
Белых и Чёрных списков



Контроль приложений - Правила доступа

Выберите приложение или группу приложений для которых вы хотите настроить правила доступа

Найти  Добавить |   

Глобальные ▾

> Слабое доверие

▾ Частичное доверие

cmd.exe

powershell.exe

C:\Users*

C:\Windows\Temp*

C:\Windows\Tasks*

WINWORD.EXE

EXCELE.EXE

> Доверенные

Правила доступа

Файлы Реестр Процессы Командная строка

Задайте правила доступа к реестру.

Правила применяются по порядку сверху вниз до пер

 Добавить правило |    

N Объекты Оп. Рек.

 1 По умолчанию 

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



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 infotecs
2020 ФЕСТ

Вопросы?



ТЕХНО infotecs
2020 Фест

Спасибо
за внимание!