

VIPNet xFirewall – многогранная защита периметра

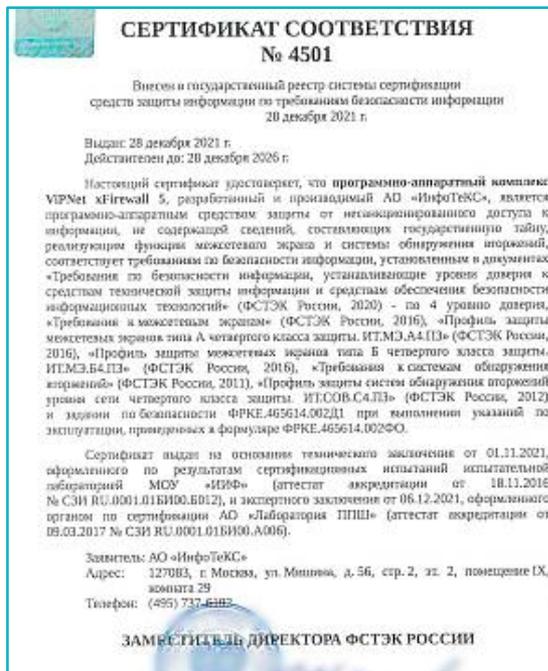


техно infotecs
2023 Фест
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Алексей Данилов

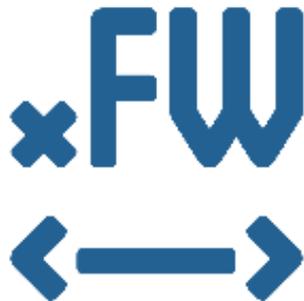
ViPNet xFirewall

Сертификат ФСТЭК



- 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)
- «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012)

Область применения



1 уровня включительно, в ИС общего пользования II класса 2.3.1 ViPNet xFirewall 5 ... предназначен для использования в государственных информационных системах до класса защищенности K1 включительно, на верхнем уровне (уровне диспетчерского управления) в автоматизированных системах управления производственными и технологическими процессами до класса защищенности K1 включительно, в ИС персональных данных для обеспечения уровня защищенности персональных данных до .

2.3.2 ViPNet xFirewall 5 может использоваться в указанных выше системах в том числе с целью выполнения базовых и адаптированных мер защиты информации в соответствии с требованиями, утвержденными приказами ФСТЭК России №17 от 11.02.2013, №31 от 14.03.2014, №21 от 18.02.2013 и №489 от 31.08.2010.

2.3.3 Также ViPNet xFirewall 5 может использоваться в автоматизированных системах управления, ИС и информационно-телекоммуникационных сетях, которые отнесены к значимым объектам критической информационной инфраструктуры (далее – КИИ) до категории значимости K1 в соответствии со статьей 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ.

Next-generation Firewall

Next-generation Firewall (NGFW)

Gartner®

Общепринято МЭ считать устройствами, реализующими технологию stateful packet inspection (SPI) сетевого трафика. МЭ разграничивает доступ на основе 5 параметров: адреса отправителя и получателя, порты отправителя и получателя, протокол L4.

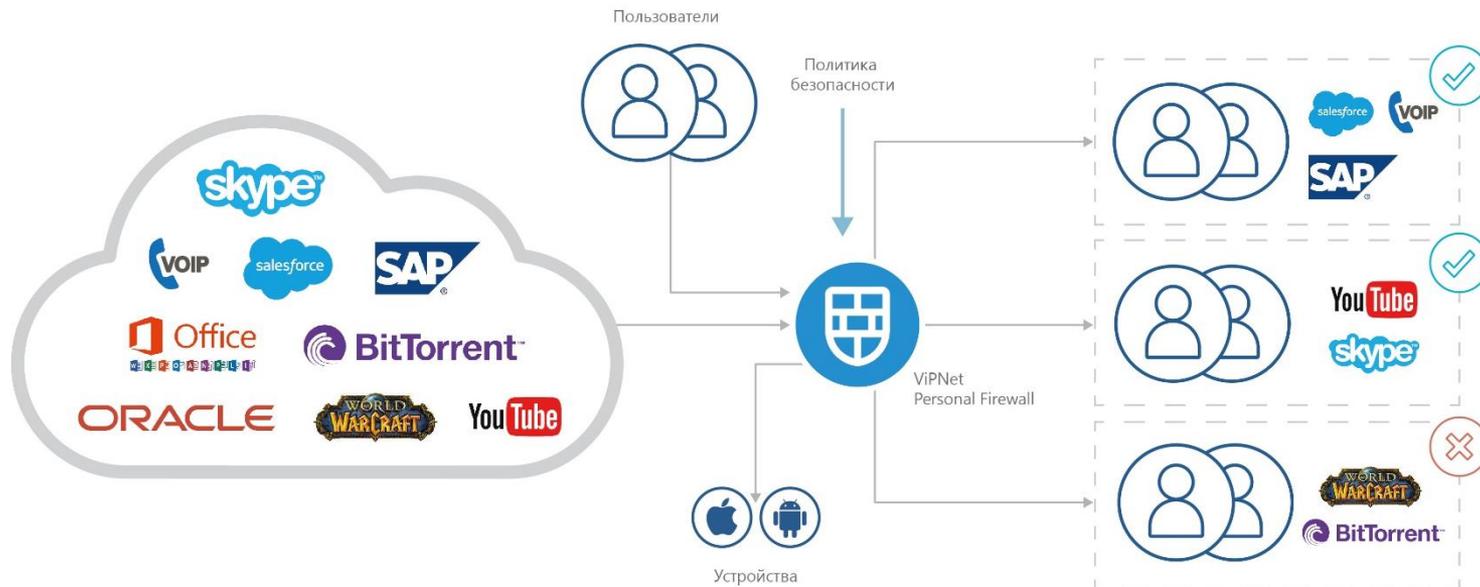
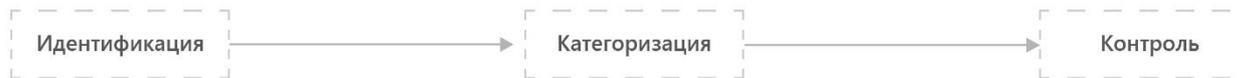


МЭ следующего поколения (NGFW) в дополнении к общепринятому разграничению доступа предоставляет возможности по выявлению и блокировке современных угроз, таких как: вредоносное ПО, атаки уровня приложений. Согласно определению Gartner NGFW должен состоять из:

- Стандартного МЭ SPI
- Встроенной системы предотвращения атак IPS
- Системы контроля приложений
- Extrafirewall intelligence

ViPNet xFirewall

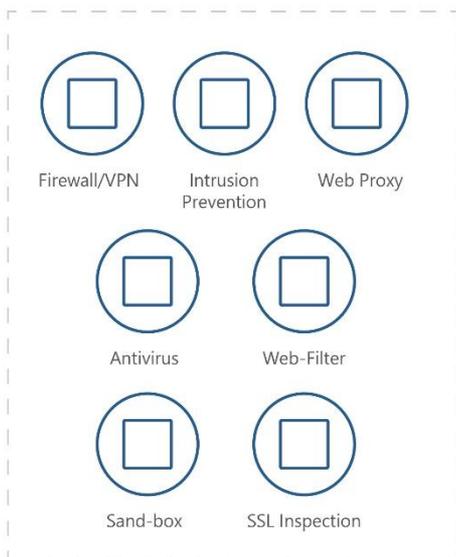
VIPNet xFirewall с первого взгляда



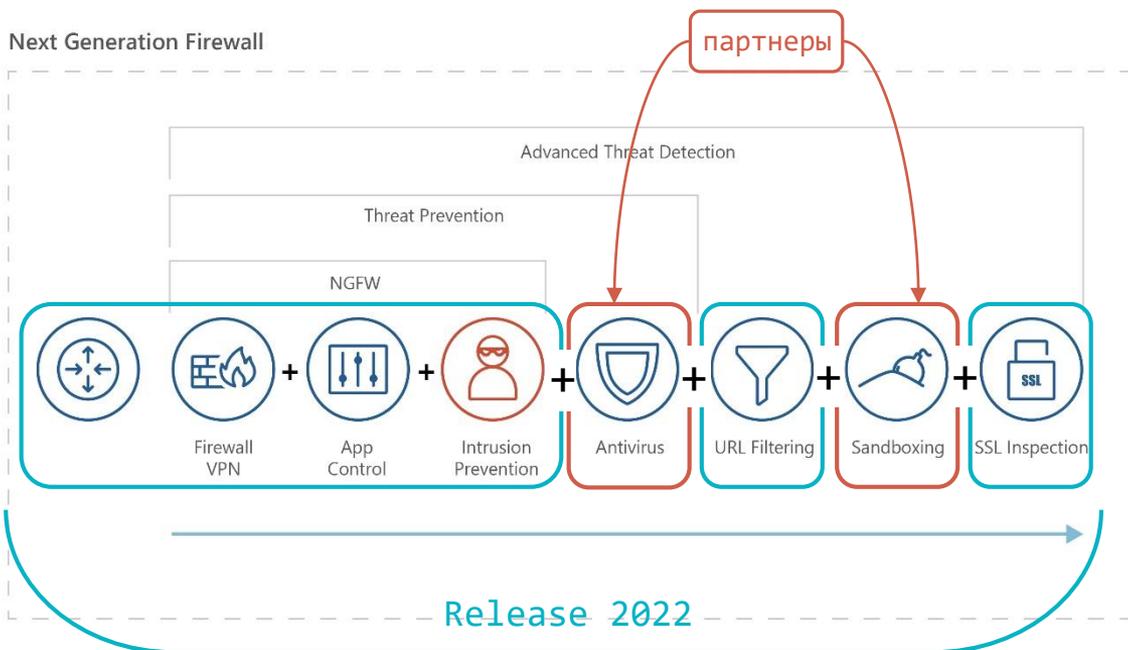
ViPNet xFirewall 2022

Next Generation Firewall

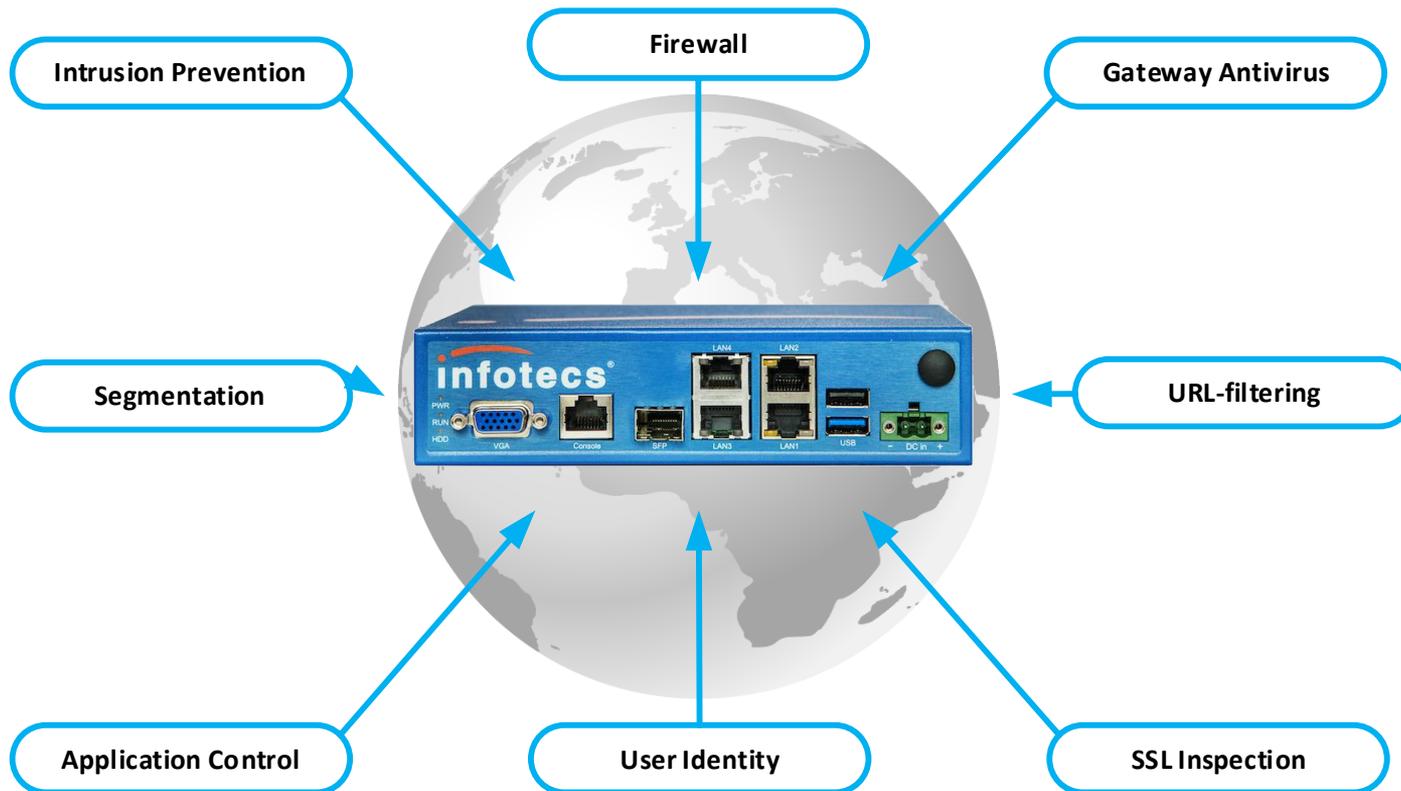
Standalone



Next Generation Firewall

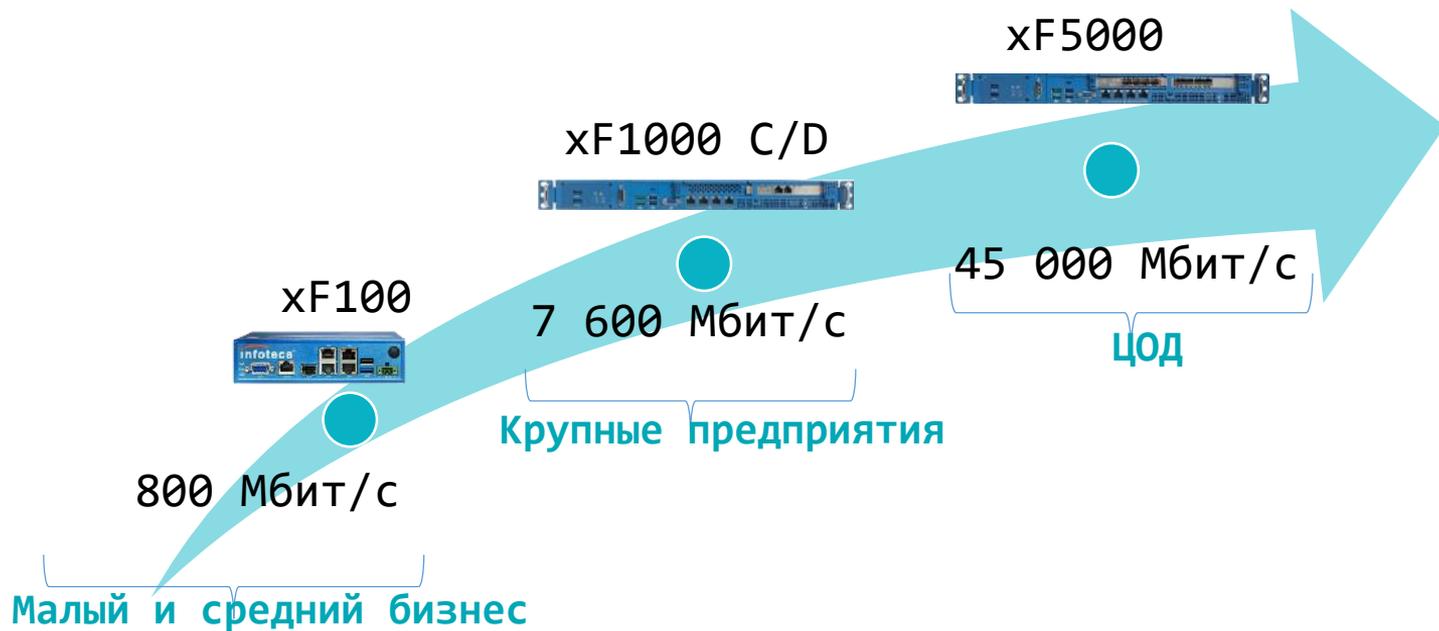


Что такое ViPNet xFirewall



Модельный ряд xFirewall

Тестирование по RFC-2544 UDP 1514 byte





Application Control – контроль приложений

Открыл порты 80/443 =
= Открыл всё!



more.tv – сериалы, фильмы и ТВ
Смотреть премьеры онлайн в HD

ЗАГРУЗИТЬ

Встроенные покупки



Строки: книги, подкасты
Читайте и слушайте

ЗАГРУЗИТЬ

Встроенные покупки



Prequel: Редактор Фото
Обработка, эффекты и фильтры

ЗАГРУЗИТЬ

Встроенные покупки



Artforintrovert
Саморазвитие с курсами-подкастами

ЗАГРУЗИТЬ

Встроенные покупки



LifeWheel цели, трекер
Цель - планы на день, приемы

ЗАГРУЗИТЬ

Встроенные покупки



InStories Reels & Stories
Сторис, AI аватары, ИИ

ЗАГРУЗИТЬ

Встроенные покупки



Google Фото
хранение фото и видео



Книги и аудиокниги MyBook
Читать и слушать книги удобно

ЗАГРУЗИТЬ

Встроенные покупки



Литрес: Книги и аудиокниги
Читай и Слушай онлайн

ЗАГРУЗИТЬ

Встроенные покупки



KION – оригинальный кинотеатр
Фильмы и мультфильмы онлайн

ЗАГРУЗИТЬ

Встроенные покупки



Облако Mail.ru: хранилище фото
Облачное хранение: диск и сейф

ЗАГРУЗИТЬ

Встроенные покупки



AppForType: текст на фото
Шаблоны для инстаграм сторис

ЗАГРУЗИТЬ

Встроенные покупки



Amiateka – сериалы онлайн
Сериалы и фильмы HD

ЗАГРУЗИТЬ

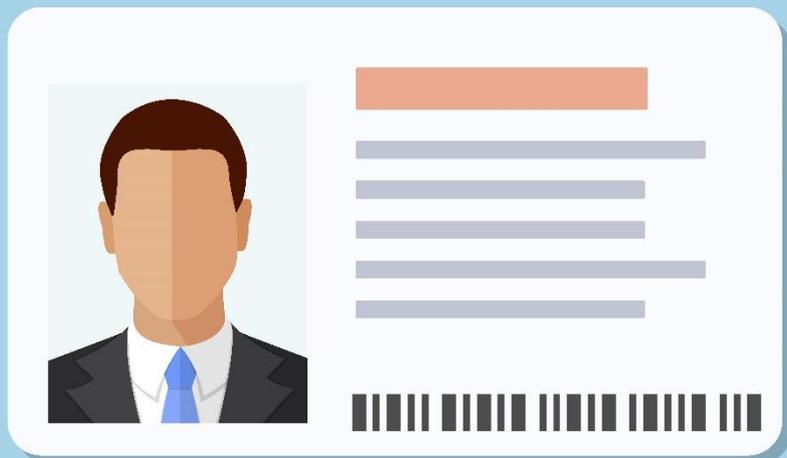
Встроенные покупки

Более 5000 приложений/протоколов

65 из категории «Социальные сети»

183 – потоковое видеовещание

- Palo Alto Networks – 3625 приложений
- Cisco – 3701 приложений



User Identity – идентификация пользователей

Интеграция с Microsoft AD

Без клиентская идентификация

- xFirewall использует технологическую учетную запись MS AD с ее помощью производится чтение EventLog
- Синхронизация с MS AD каждые 5 секунд
- Допустимое время отсутствия связи 1800 секунд

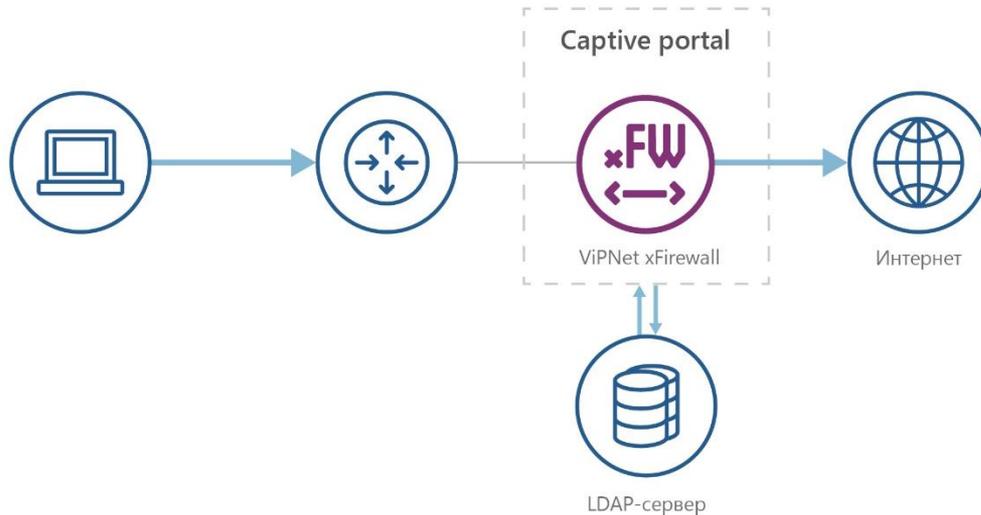
Использование учетных записей пользователей MS AD в правилах фильтрации

- Отсутствует потребность в «привязке» пользователей к ip-адресам
- Отсутствует потребность в «привязке» пользователей к устройствам



**BYOD – принеси
свое устройство
и работай**

Captive portal – аутентификация с помощью браузера



Идентификация пользователей, использующих Linux компьютеры, iPhone, iPad и Android-устройства

Предоставление контролируемого доступа подрядчикам, партнерам

Автоматическое перенаправление на Портал аутентификации – Captive Portal

Для таких пользователей можно создать политику с ограниченным доступом к ресурсам компании, потому что их устройства могут быть без средств защиты.



Intrusion Prevention - COB

Система предотвращения вторжений

Предотвращение вторжений включено

Поиск правил... Параметры Обновление базы ▾

Блокирующие

Правило предотвращения	Статус	Действие
▼ current_events (9)		
^ exploit (620)		
AM EXPLOIT iframe SRC JS XSS on IE test detected	Вкл	Блокировать
AM EXPLOIT Yahoo Widgets Engine 4.0.4 YDPCNTL.DLL ActiveX DoS attempt (short type)	Вкл	Блокировать
AM Exploit Firefox 46.0.1 - ASM.JS JIT-Spray Remote Code Execution	Вкл	Блокировать
AM EXPLOIT Yahoo Messenger 8.1.402 YVerInfo.dll 2007.8.26 buffer overflow exploit detected	Вкл	Блокировать
AM EXPLOIT CA Internet Security Suite 2008.0 ActiveX Control Arbitrary File Overwrite exploit detected	Вкл	Блокировать
AM EXPLOIT Facebook ImageUploader4.1.ocx FileMask DoS exploit detected	Вкл	Блокировать
AM EXPLOIT IBM DB2 Universal Database 9.1 FixPak 4a XML Query Buffer Overflow exploit detected	Вкл	Блокировать

Журнал регистрации IP-пакетов

Фильтр IP-пакетов ^

Признаки IP-пакетов

Пользователь сети: Любой ▾

Приложение: Любое ▾

Прикладной протокол: Любой ▾

Транспортный протокол: Все протоколы ▾

Сетевой интерфейс: Все сетевые интерфейсы ▾

Тип трафика: Весь трафик ▾

Тип IP-адреса: Любой ▾

Трансляция IP-пакетов: Все ▾

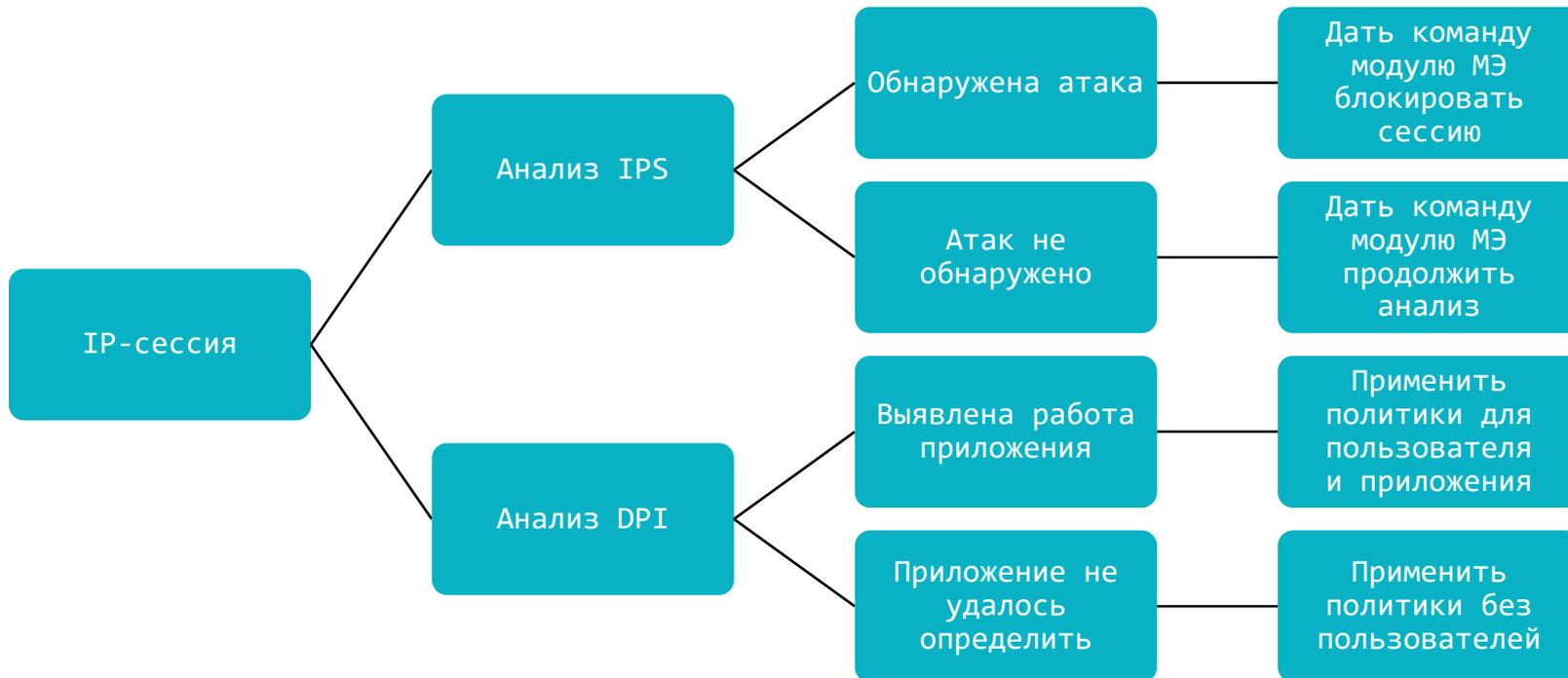
Событие: Блокированные IP-пакеты ▾

Группа правил IPS: Любая ▾

Правило IPS: Любое ▾

Найти **Восстановить значения по умолчанию**

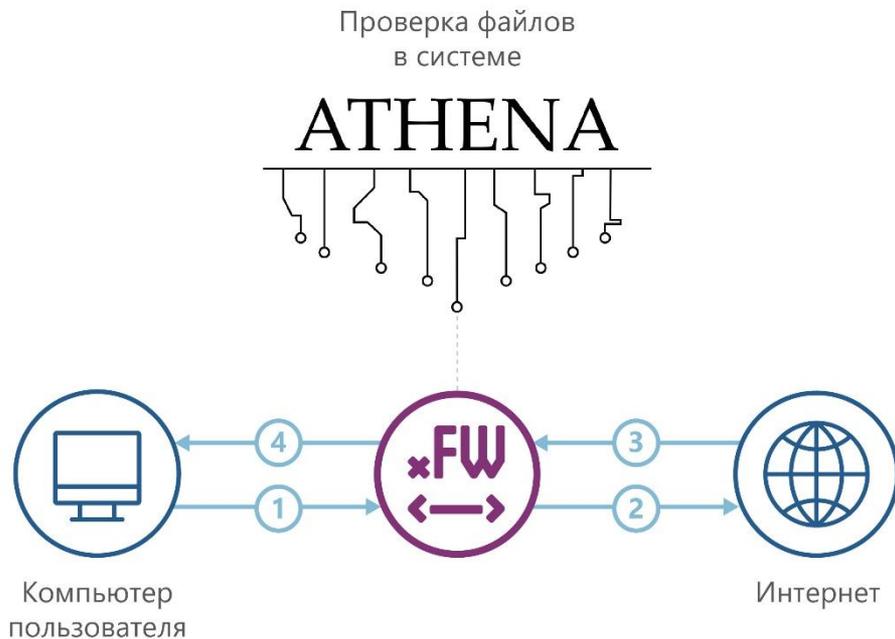
Порядок применения правил IPS





Gateway Antivirus – шлюзовой антивирус

Поддержка песочниц



- Тестировался сценарий проверки на содержание вредоносного контента файлов, загружаемых из сети Интернет в «песочницу» ATHENA через службу прокси-сервера xFirewall по протоколу ICAP
- Межсетевой экран VipNet xFirewall служит шлюзом между приложениями, функционирующими на узлах локальной сети, и внешними сетевыми ресурсами, к которым эти приложения обращаются (выполняет функции прокси-сервера)
- Система AVSOFT ATHENA работает на основе комбинации технологий мультисканера и «песочницы» для исследования файлов на подозрительное содержимое и поведение существенно повышает точность результата проверки



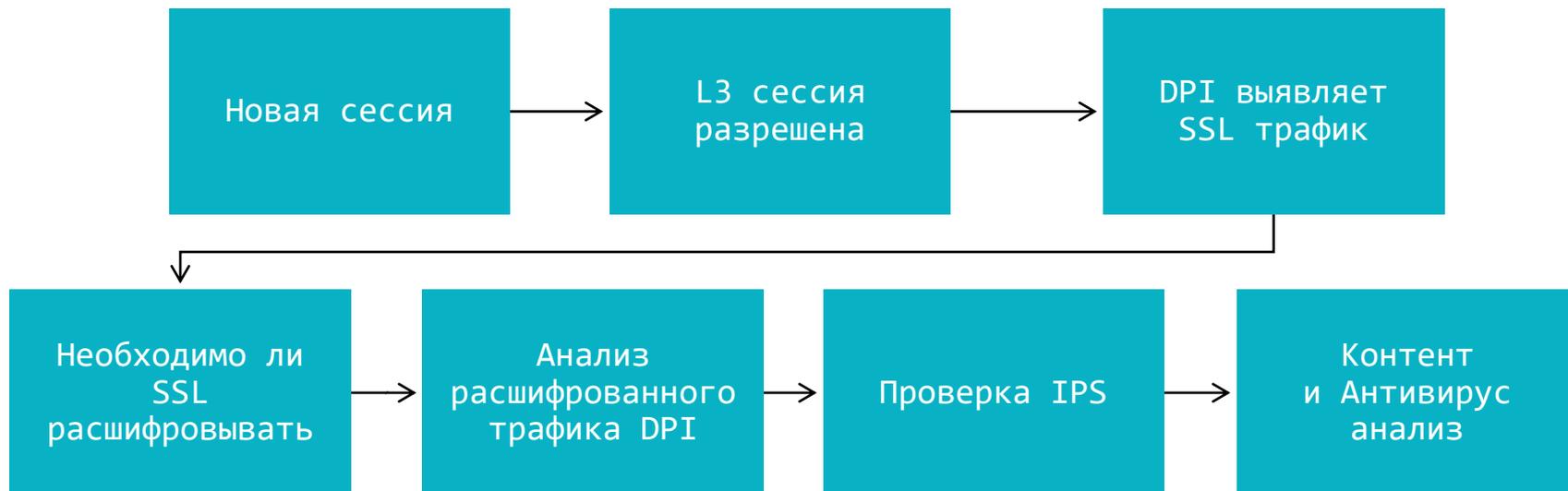
SSL Inspection – анализ SSL

Классификация SSL



- Разрешить тот SSL-трафик, который известен:
 - Yandex, Google, Facebook и тд
- Блокировать известный SSL запрещенных политикой приложений: социальные сети, мессенджеры и тд
- Запретить любой неизвестный SSL-трафик

Схема проверки трафика



Forward proxy decryption

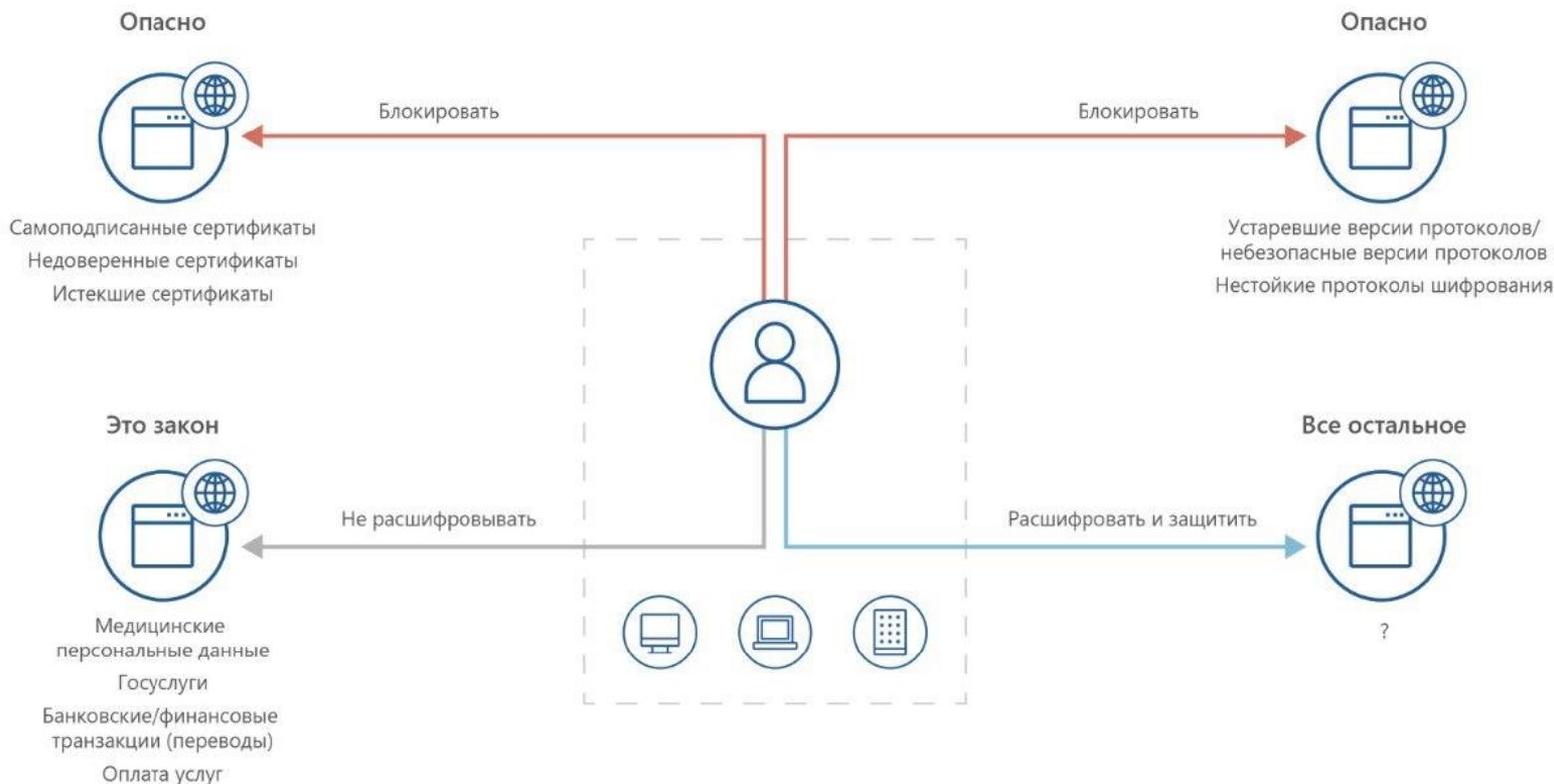
Корневой сертификат МСЭ (Firewall)

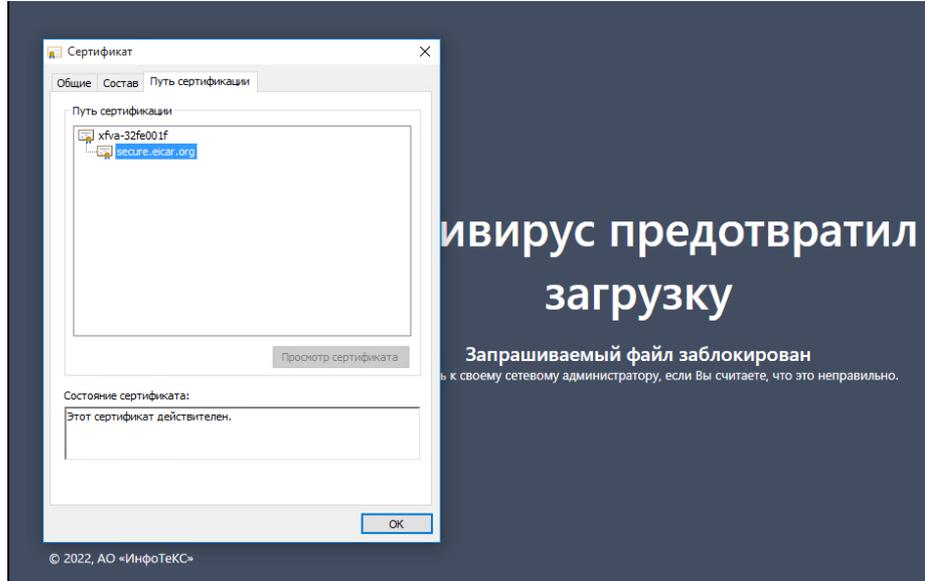


Клиент подтверждает корневой сертификат МСЭ



Лучшие практики SSL Inspection





Результат

Защита от неизвестных угроз

VIPNet xFirewall – повышает осведомленность



Максимальная
видимость –
фильтрация на 7
уровне ISO OSI



Защита от сетевых
атак – блокировка
аномалий,
запретных команд



Защита от
вирусных атак



Уменьшение
поверхности
атаки

Дорожная карта

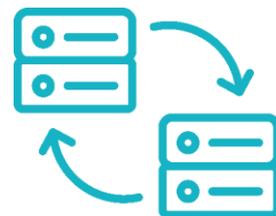
План разработки 2023



Рост скорости в ~10 раз



Поддержка протокола BGP



HA-Cluster



URL-фильтрация
по категориям



Поддержка PBR, DGD



Поддержка групп MS AD

техно infotecs
2023 Фест

Спасибо
за внимание!

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363