

ViPNet xFirewall – многогранная защита периметра



техно infotecs
2023 Фест
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Алексей Данилов
Руководитель продуктового направления

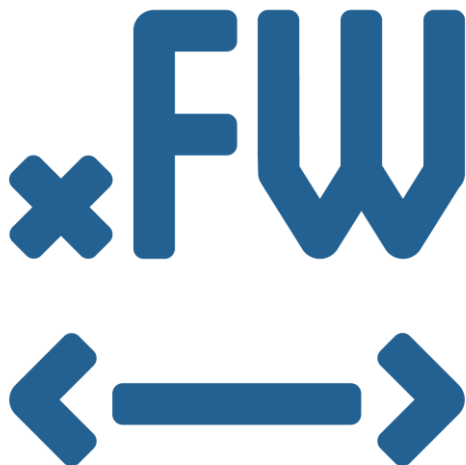
ViPNet xFirewall

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



2.3.1 ViPNet xFirewall 5 ... предназначен для использования в государственных информационных системах до класса защищенности К1 включительно, на верхнем уровне (уровне диспетчерского управления) в автоматизированных системах управления производственными и технологическими процессами до класса защищенности К1 включительно, в ИС персональных данных для обеспечения уровня защищенности персональных данных до 1 уровня включительно, в ИС общего пользования II класса.

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 К1 в соответствии со статьей 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ.

Next-generation Firewall

Next-generation Firewall (NGFW)

Gartner



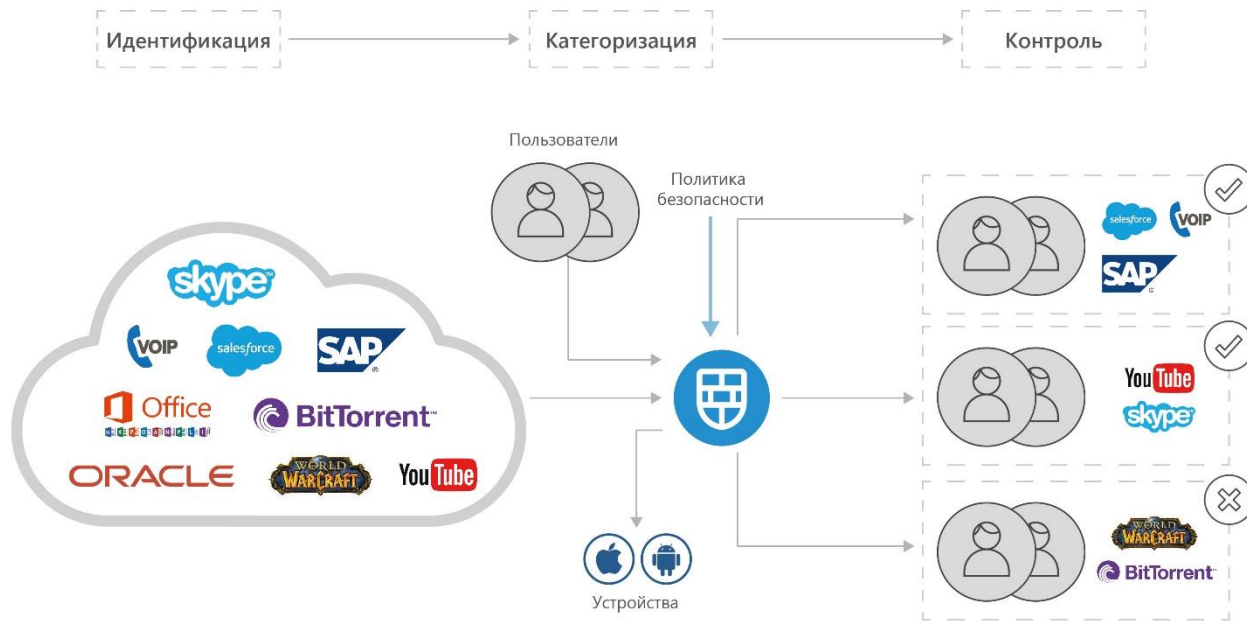
- Общепринято МЭ считать устройствами, реализующими технологию stateful packet inspection (SPI) сетевого трафика. МЭ разграничивает доступ на основе 5 параметров: адреса отправителя и получателя, порты отправителя и получателя, протокол L4.

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

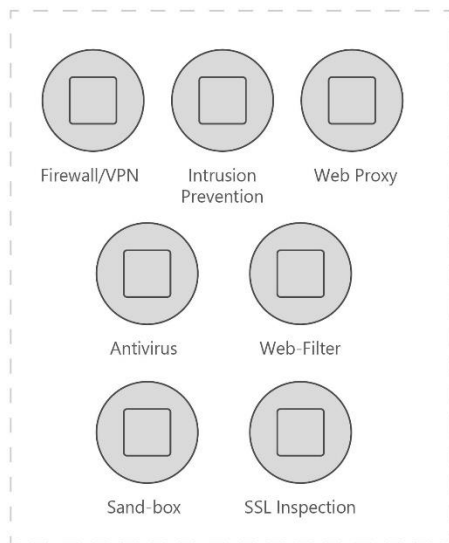
VIPNet xFirewall с первого взгляда



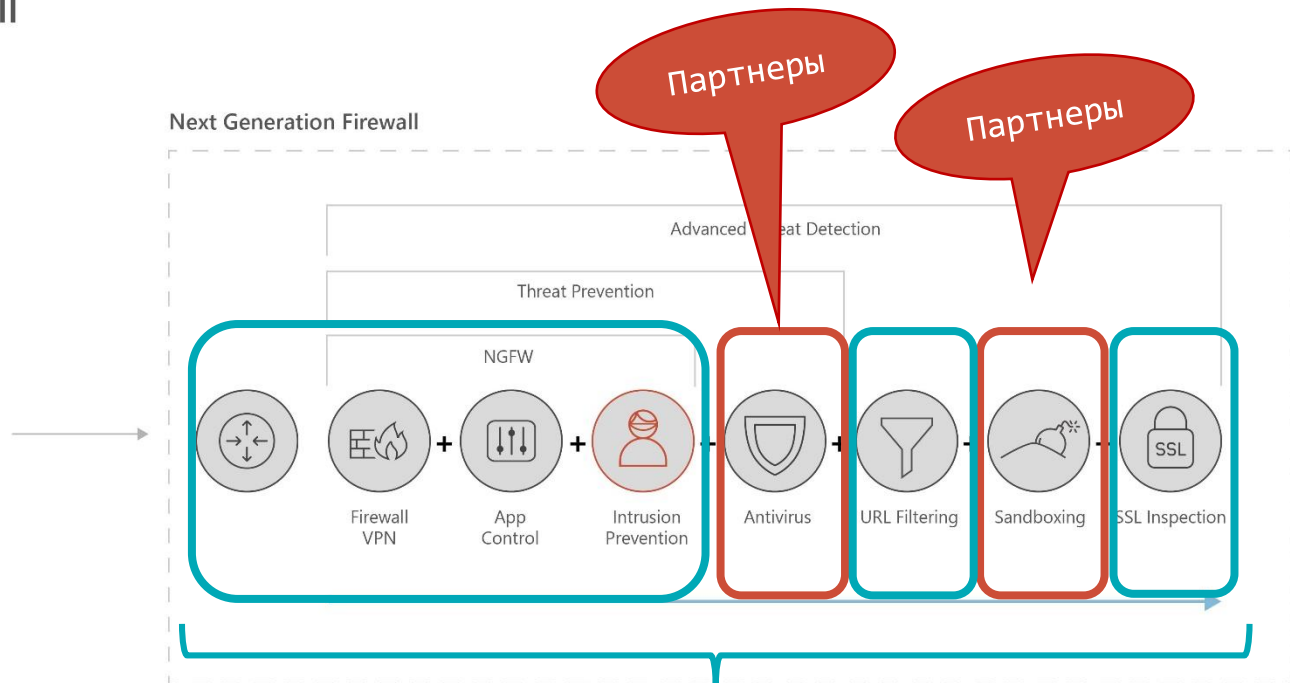
ViPNet xFirewall 2022

Next Generation Firewall

Standalone

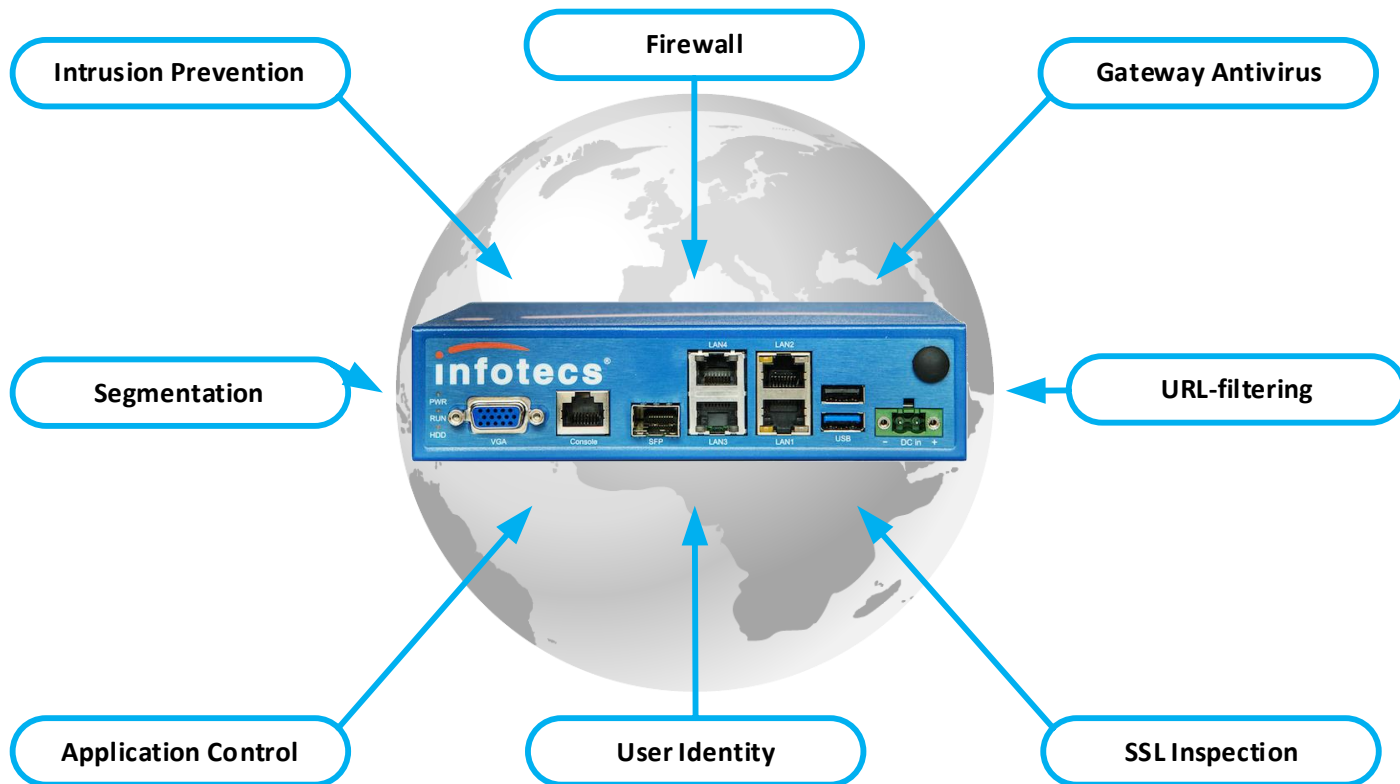


Next Generation Firewall



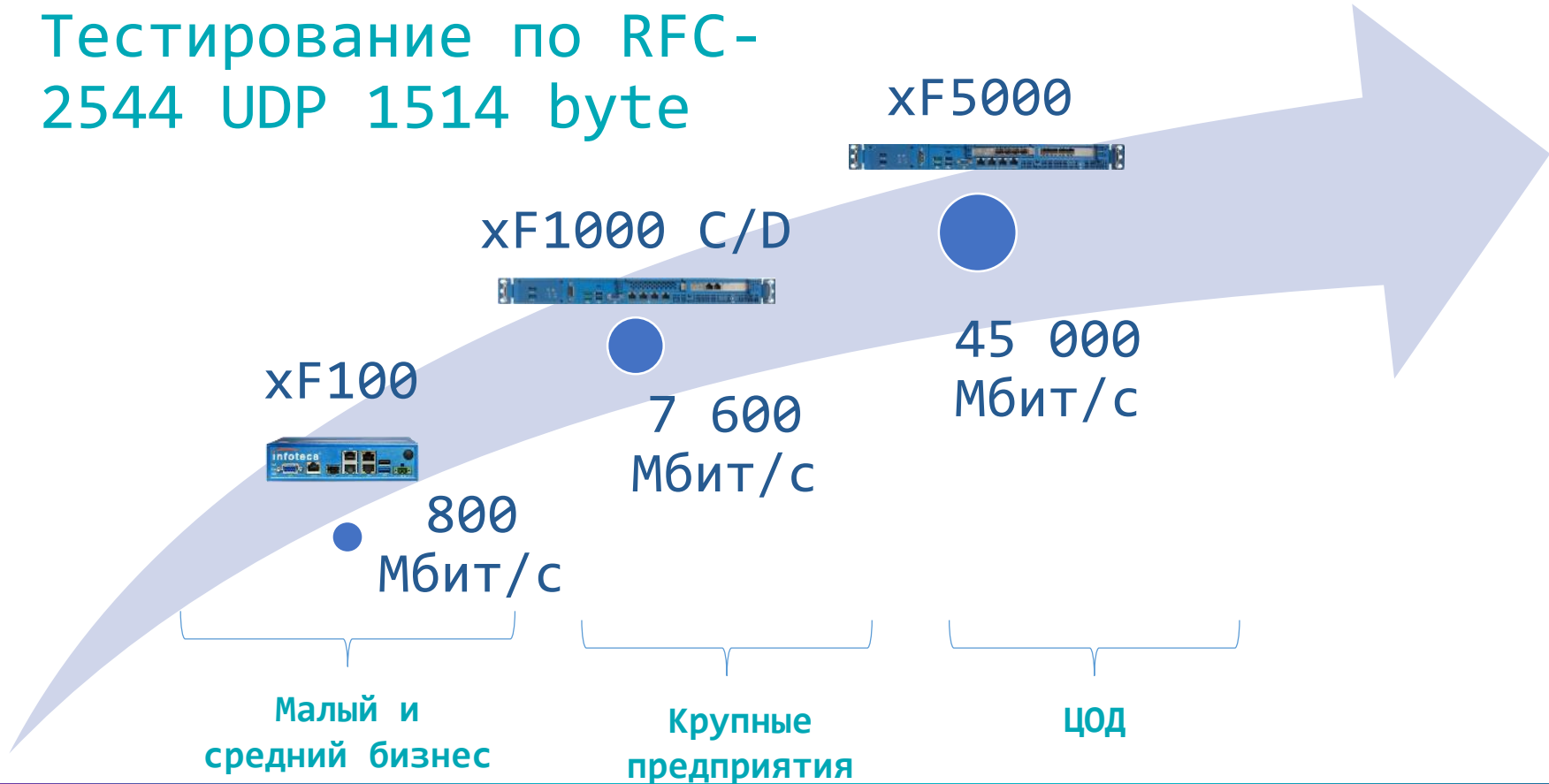
Release 2022

Что такое ViPNet xFirewall



Модельный ряд xFirewall

Тестирование по RFC-
2544 UDP 1514 byte

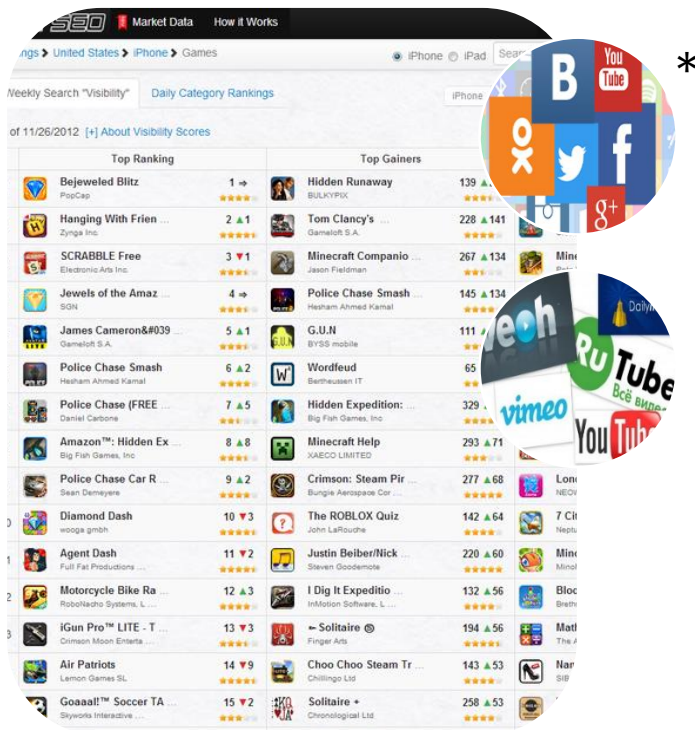


Application Control – контроль приложений



Открыл порты 80/443 == Открыл всё!

Более 5000 приложений/протоколов



The image shows a screenshot of an app store chart, likely from the App Store, displaying a list of top-ranking and top-gaining applications. The chart is titled "Weekly Search 'Visibility'" and "Daily Category Rankings". The top-ranking applications include "Bejeweled Blitz", "Hanging With Friends", "SCRABBLE Free", "Jewels of the Amazon", "James Cameron's Avatar: The Game", "Police Chase Smash", "Police Chase (FREE)", "Amazon™: Hidden Expeditions", "Police Chase Car Racing", "Diamond Dash", "Agent Dash", "Motorcycle Bike Racing", "iGun Pro™ LITE - The Game", "Air Patriots", and "Goaaaal™ Soccer Tactics". The top-gaining applications include "Hidden Runaway", "Tom Clancy's Splinter Cell: Blacklist", "Minecraft Companion", "Police Chase Smash", "G.U.N.", "Wordfeud", "Hidden Expedition: The Game", "Minecraft: Help", "Crimson: Steam Pirates", "The ROBLOX Quiz", "Justin Bieber/Nicki Minaj", "iDig It Expedition", "Solitaire", "Choo Choo Steam Train", and "Solitaire +". The chart is overlaid with a circular collage of social media icons (Blogger, YouTube, Instagram, Twitter, Facebook, Google+) and a collage of video streaming service logos (Tech, RuTube, Vimeo, YouTube, Beeline).

Top Ranking		Top Gainers	
Bejeweled Blitz	1	Hidden Runaway	139
Hanging With Friends	2	Tom Clancy's Splinter Cell: Blacklist	228
SCRABBLE Free	3	Minecraft Companion	267
Jewels of the Amazon	4	Police Chase Smash	145
James Cameron's Avatar: The Game	5	G.U.N.	111
Police Chase Smash	6	Wordfeud	65
Police Chase (FREE)	7	Hidden Expedition: The Game	329
Amazon™: Hidden Expeditions	8	Minecraft: Help	293
Police Chase Car Racing	9	Crimson: Steam Pirates	277
Diamond Dash	10	The ROBLOX Quiz	142
Agent Dash	11	Justin Bieber/Nicki Minaj	220
Motorcycle Bike Racing	12	iDig It Expedition	132
iGun Pro™ LITE - The Game	13	Solitaire	194
Air Patriots	14	Choo Choo Steam Train	143
Goaaaal™ Soccer Tactics	15	Solitaire +	258

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

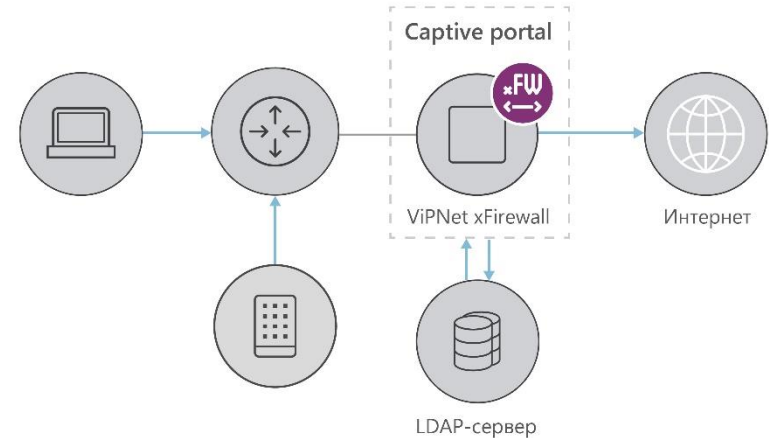




**BYOD –
принеси свое
устройство
и работай**

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 YDPCTL.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:

Приложение:

Прикладной протокол:

Транспортный протокол:

Сетевой интерфейс:

Тип трафика:

Тип IP-адреса:

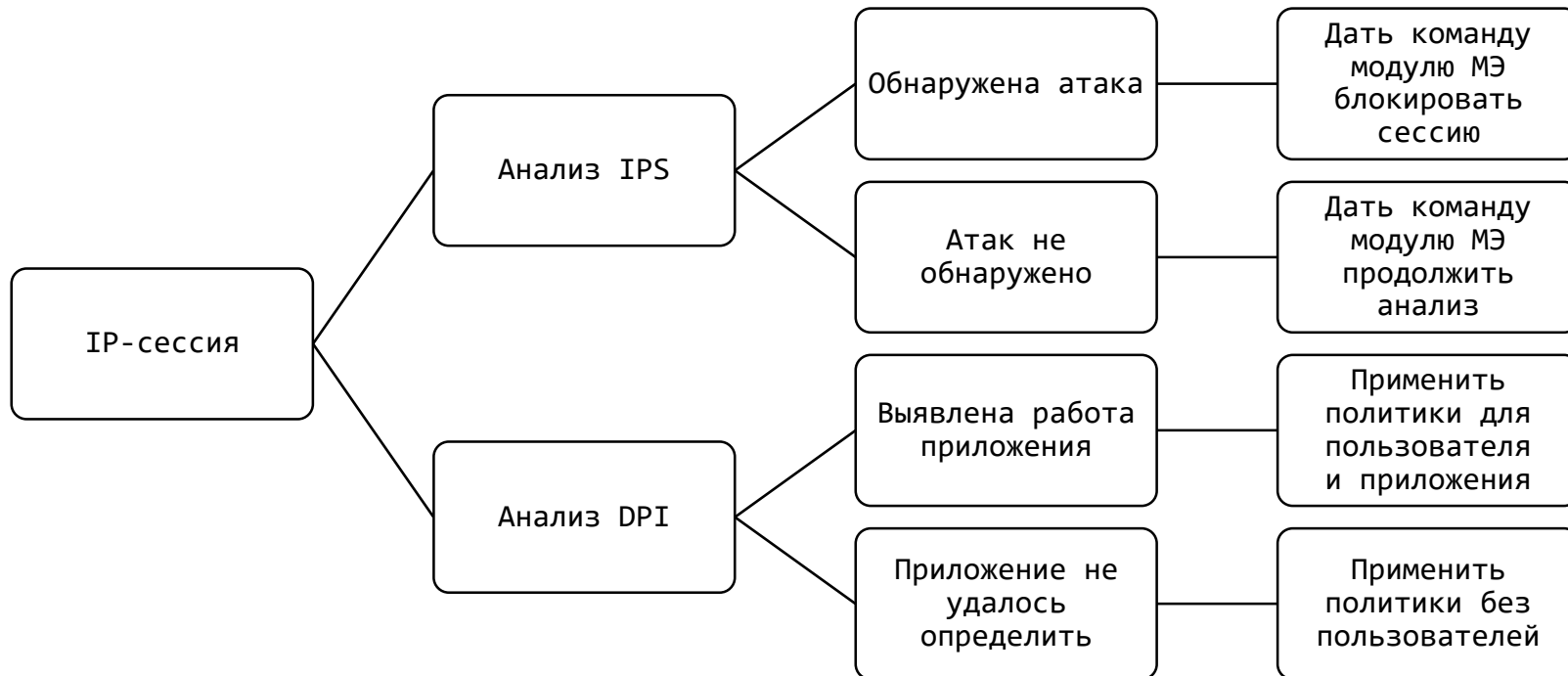
Трансляция IP-пакетов:

Событие:

Группа правил IPS:

Правило IPS:

Порядок применения правил IPS

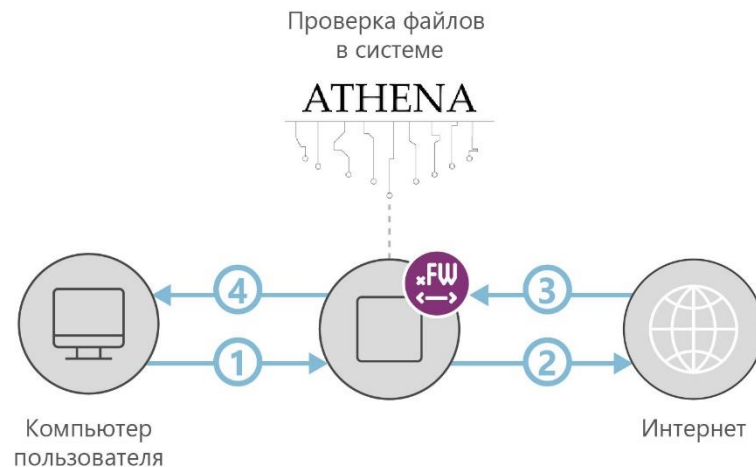


Gateway Antivirus – шлюзовой антивирус

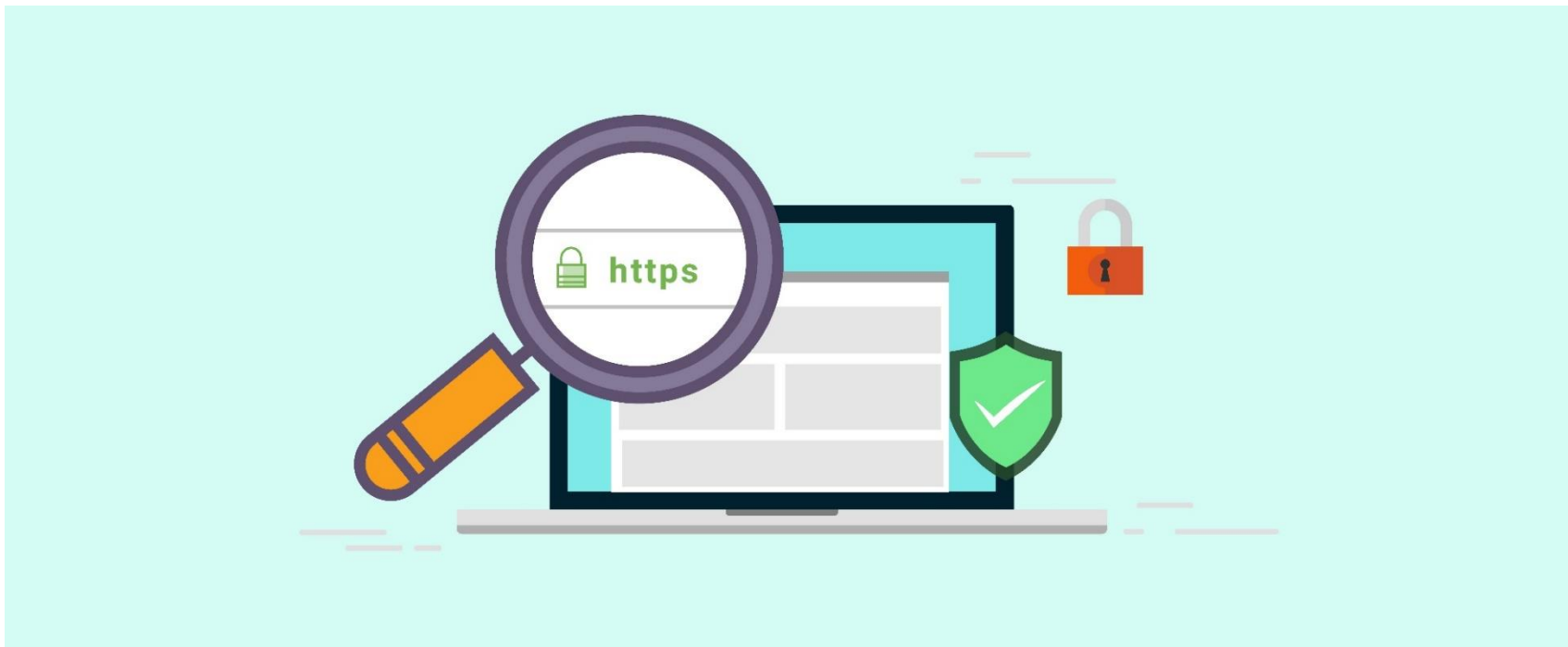


Поддержка песочниц

- 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

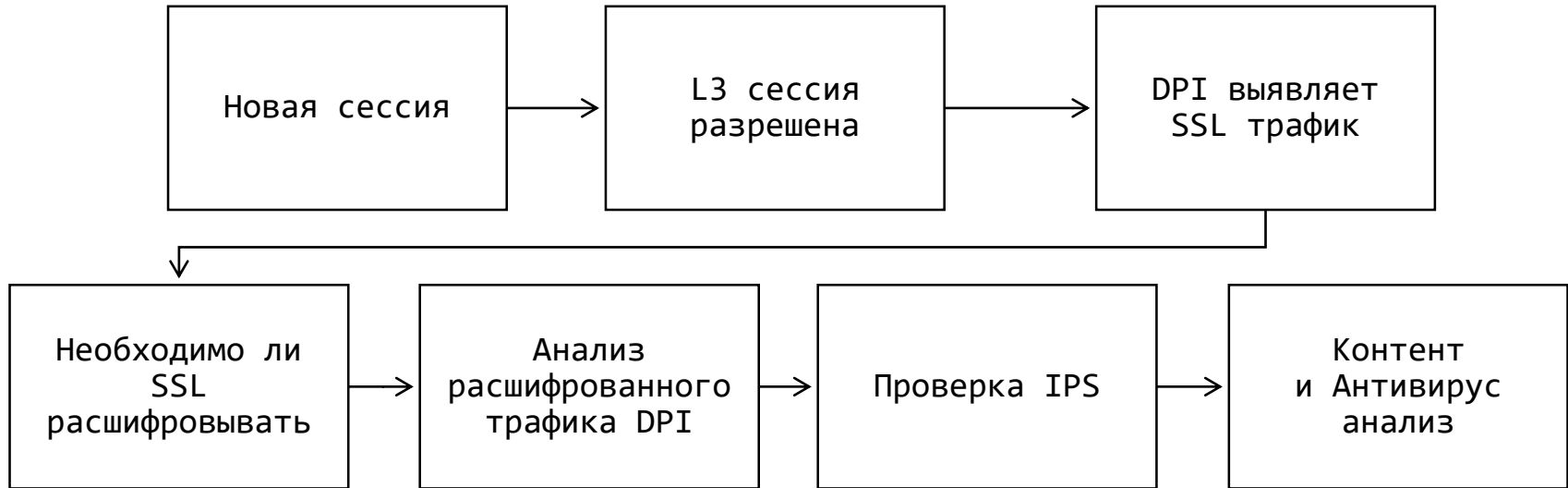


Классификация SSL

- 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

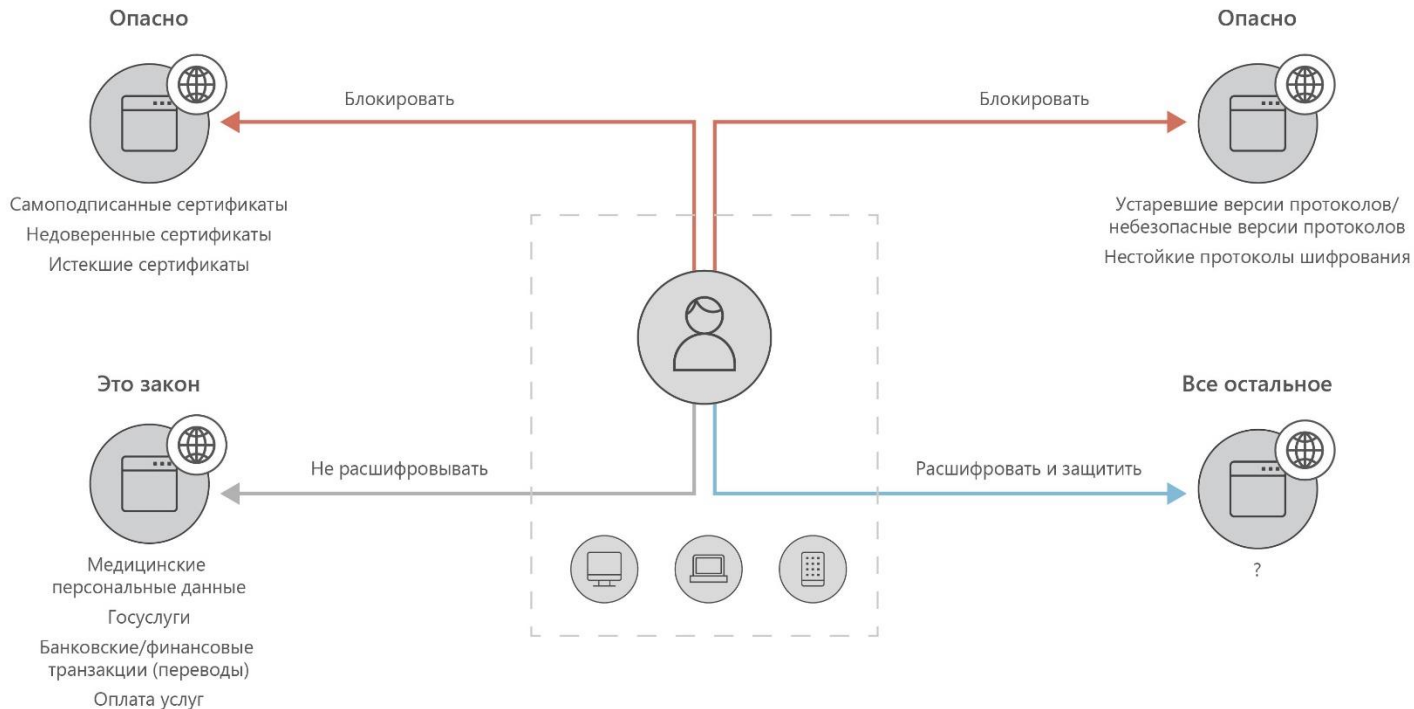
Корневой сертификат МСЭ (Firewall)



Клиент подтверждает корневой сертификат МСЭ



Лучшие практики SSL Inspection



Результат

Вирус предотвратил загрузку

Запрашиваемый файл заблокирован

Посмотреть сертификат

Состояние сертификата:
Этот сертификат действителен.

ОК

© 2022, АО «ИнфоТекс»

Защита от неизвестных угроз

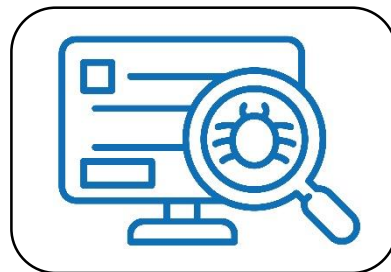
VIPNet xFirewall – повышает осведомленность



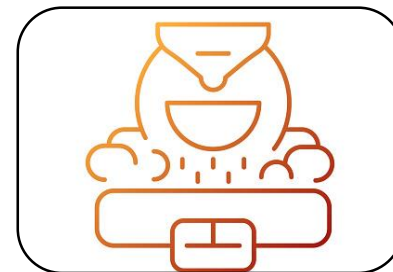
Максимальная
видимость –
фильтрация на 7
уровне ISO OSI



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



Спасибо за внимание!

Алексей Данилов
Руководитель направления
e-mail: danilov@infotecs.ru

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363