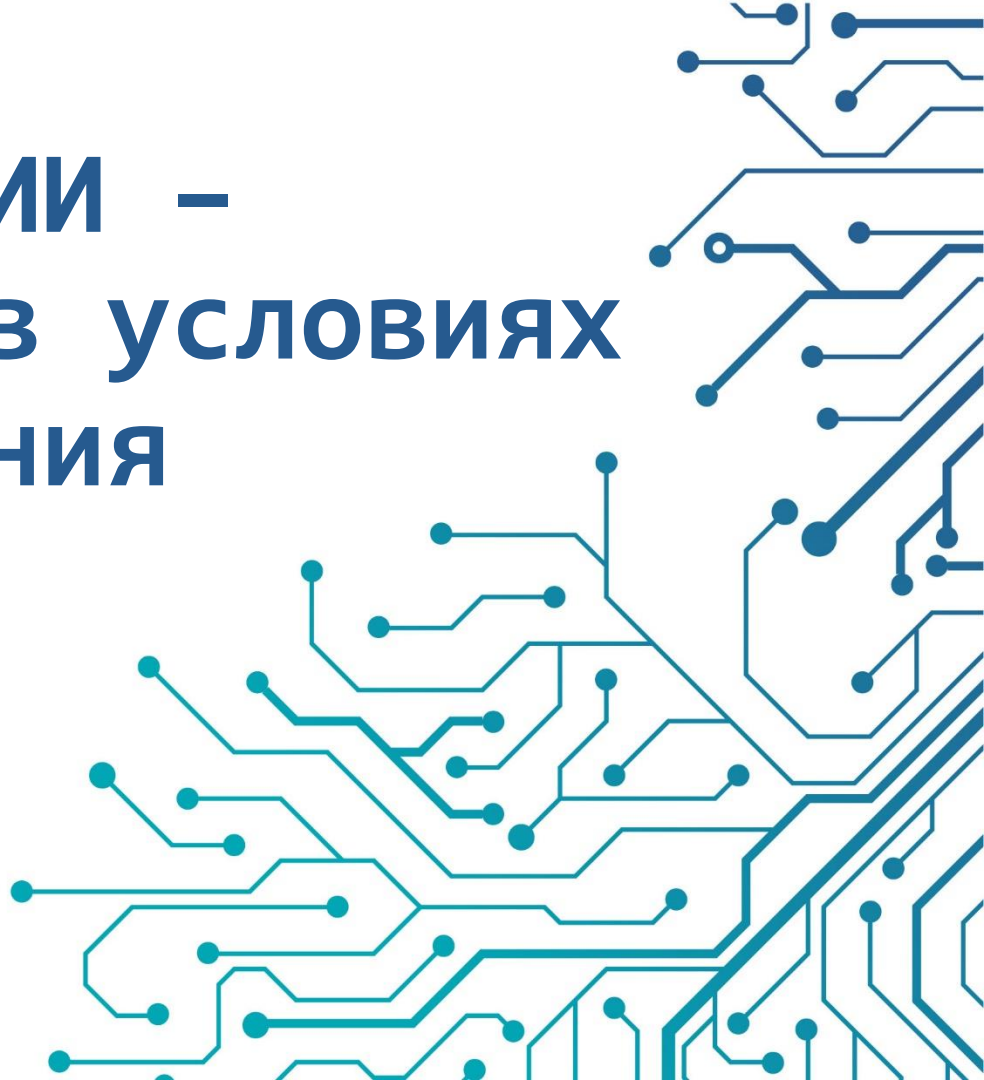


ГИС, ИСПДн, КИИ – чем защищать в условиях импортозамещения

Алексей Данилов
Руководитель направления
Отдел развития продуктов ИнфоТеКС



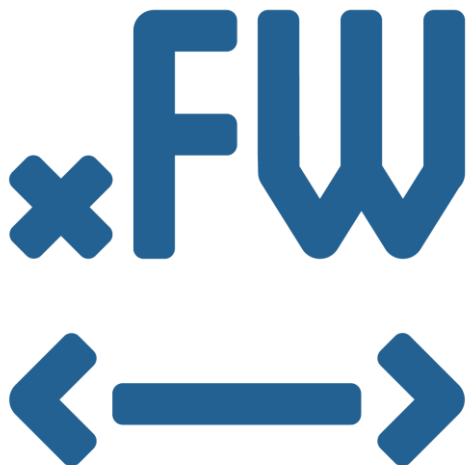


ViPNet xFirewall

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)

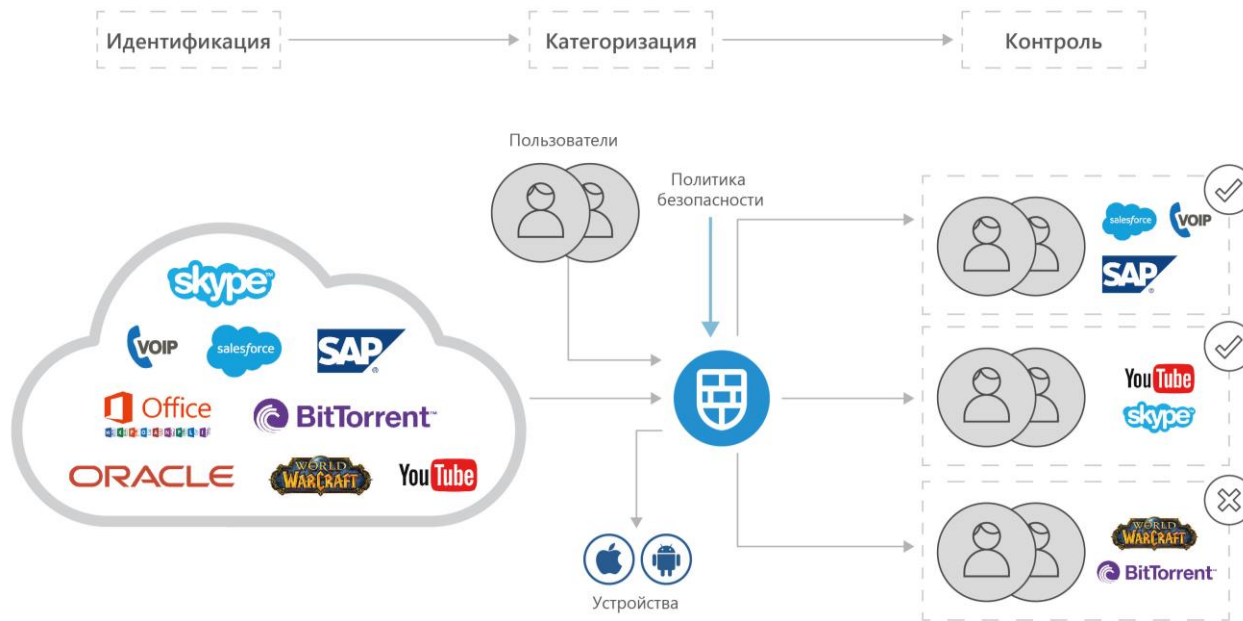


2.3.1 ViPNet xFirewall 5 ... предназначен для использования в государственных информационных системах до класса защищенности К1 включительно, на верхнем уровне (уровне диспетчерского управления) в автоматизированных системах управления производственными и технологическими процессами до класса защищенности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

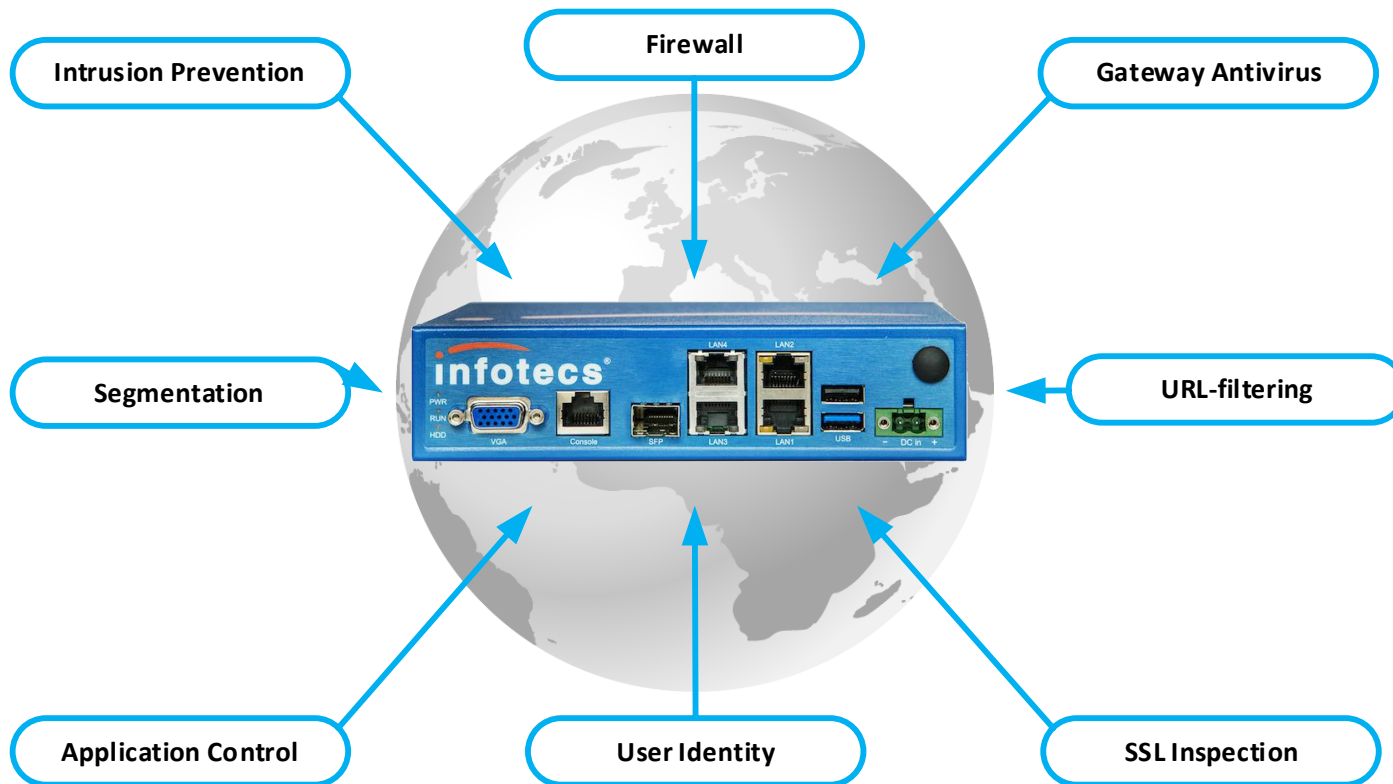
2.3.2 ViPNet xFirewall 5 может использоваться в указанных выше системах в том числе с целью выполнения базовых и адаптированных мер защиты информации в соответствии с требованиями, утвержденными приказами ФСТЭК России №17 от 11.02.2013, №31 от 14.03.2014, №21 от 18.02.2013 и №489 от 31.08.2010.

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

VIPNet xFirewall с первого взгляда



Что такое ViPNet xFirewall



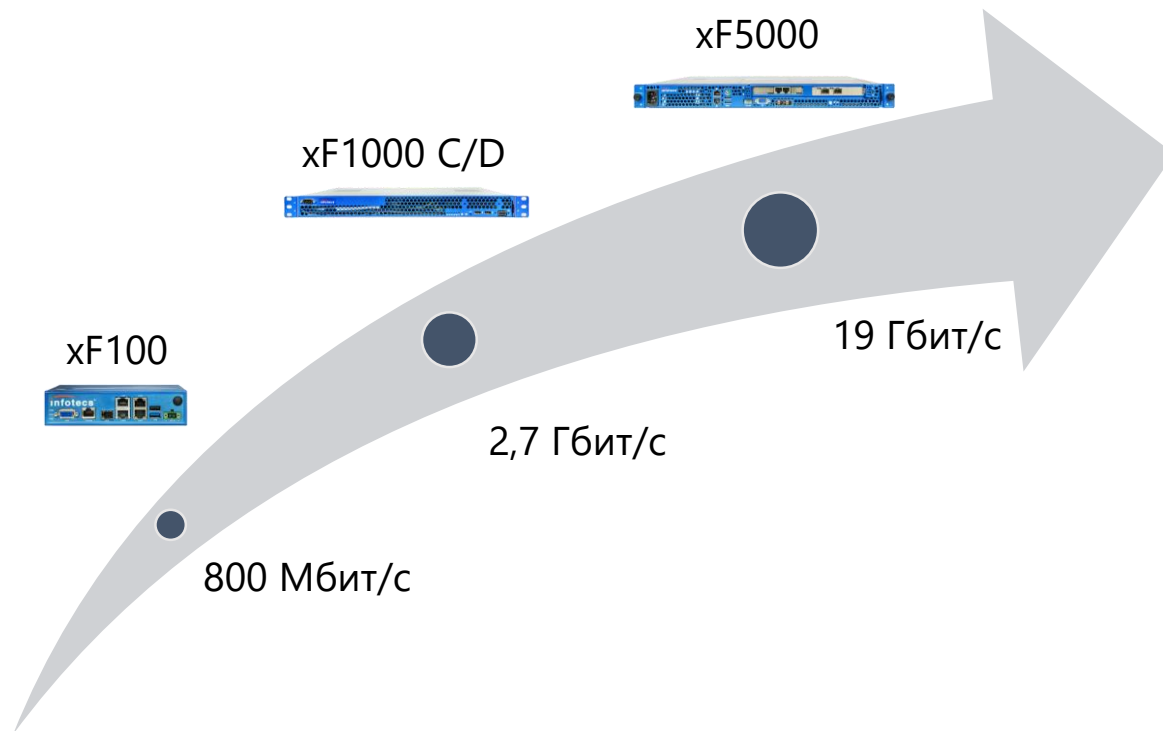
Что нового в 5 поколении продукта

- Система предотвращения вторжений IPS:
 - Реализована система предотвращения вторжений – IPS
 - Реализовано взаимодействие с ViPNet TIAS
 - Расширены базы решающих правил
 - Обновление базы правил IPS через прокси сервер
 - Добавлена возможность перехода к описанию правила IPS, соответствующего событию, зарегистрированному в журнале IP-пакетов.
- Улучшения МСЭ
 - Блокировка доступа к поддоменам DNS
 - Protection Tools – автоматическая блокировка источников повышенной нагрузки
 - Работа с несколькими контроллерами доменов MS AD
- Новый web-UI

Что нового в 5 поколении продукта

- Расширение возможностей failover
 - Поддержка dhcp-relay
 - Поддержка DHCP-сервера
- Улучшение возможностей мониторинга
 - Экспорт журнала пакетов в формате CEF по syslog
 - Информация о сработавших правилах в журнале IP-пакетов
 - Управление уровнем важности событий, регистрируемых в системном журнале
 - Поддержка SNMPv3
 - Мониторинг пассивного узла кластера по протоколу SNMP
 - Поддержка протокола Netflow v9
- Поддержка новых аппаратных платформ из TOPP
- SSL Inspection

VIPNet xFirewall. Платформы



Повышена производительность

В зависимости от типа платформы и типа теста производительность повышена на 35-58%

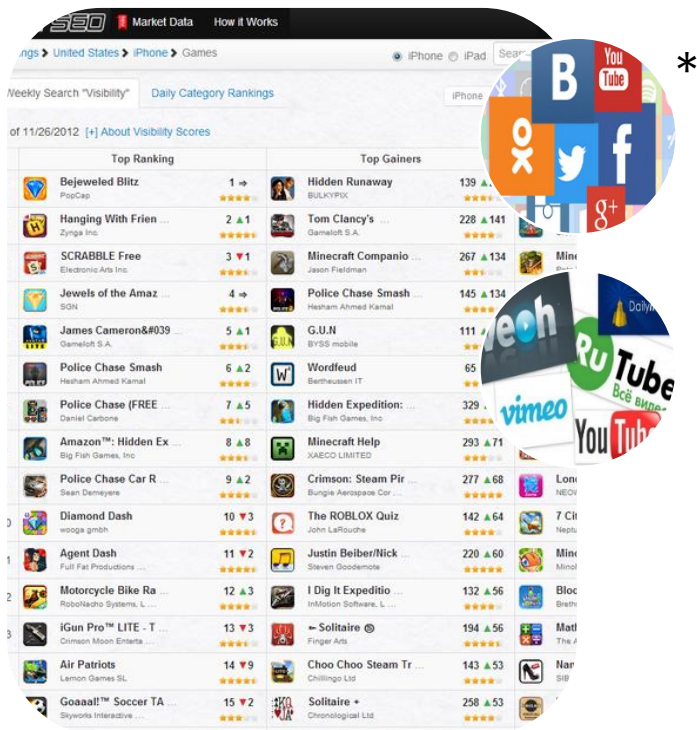


Application Control – контроль приложений



Открыл порты 80/443 == Открыл всё!

Более 5000 приложений/протоколов



The image shows a screenshot of an app store's 'Daily Category Rankings' for the 'Games' category on an iPhone. The page is titled 'Weekly Search "visibility" Daily Category Rankings' and is dated 'of 11/26/2012'. It features two columns: 'Top Ranking' and 'Top Gainers'. The 'Top Ranking' column lists apps like '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 Expedition', 'Police Chase Car Racing', 'Diamond Dash', 'Agent Dash', 'Motorcycle Bike Racing', 'iGun Pro™ LITE - The Game', and 'Air Patriots'. The 'Top Gainers' column lists apps like 'Hidden Runaway', 'Tom Clancy's Splinter Cell: Chaos Theory', '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', and 'Solitaire+'. Overlaid on the right side of the screenshot are several social media icons: a large blue 'B' for Blogger, a red 'You Tube' logo, a blue Twitter bird, a blue Facebook 'f', a red and white Google Plus 'g+', a blue and white Vimeo logo, a green and white RuTube logo, and a red and white YouTube logo. A black asterisk is placed to the right of the Blogger icon.

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

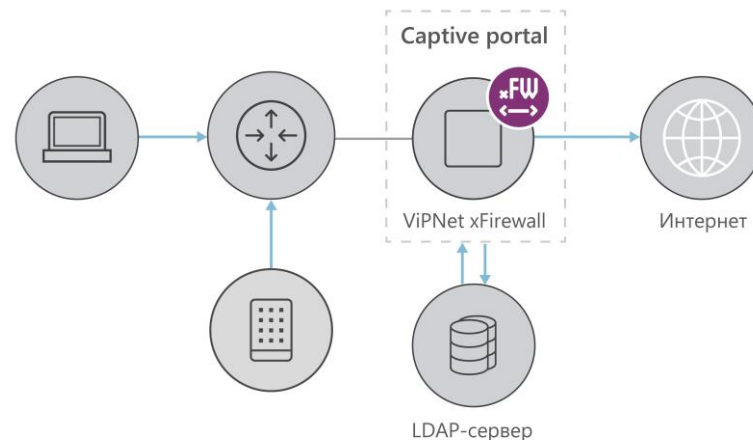




**BYOD –
принеси свое
устройство
и работай**

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.

A graphic illustration for an Intrusion Detection and Prevention System. It features a central figure of a person in a dark suit pointing their right index finger towards the viewer. The background is a dark blue gradient with a grid of hexagonal icons. Some icons show a padlock (both locked and unlocked) and a magnifying glass. Overlaid on this background is the text "INTRUSION DETECTION AND PREVENTION SYSTEM" in large, bold, white, sans-serif capital letters with a slight blue glow and drop shadow.

INTRUSION DETECTION AND PREVENTION SYSTEM

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 YDPCTLDLL 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:

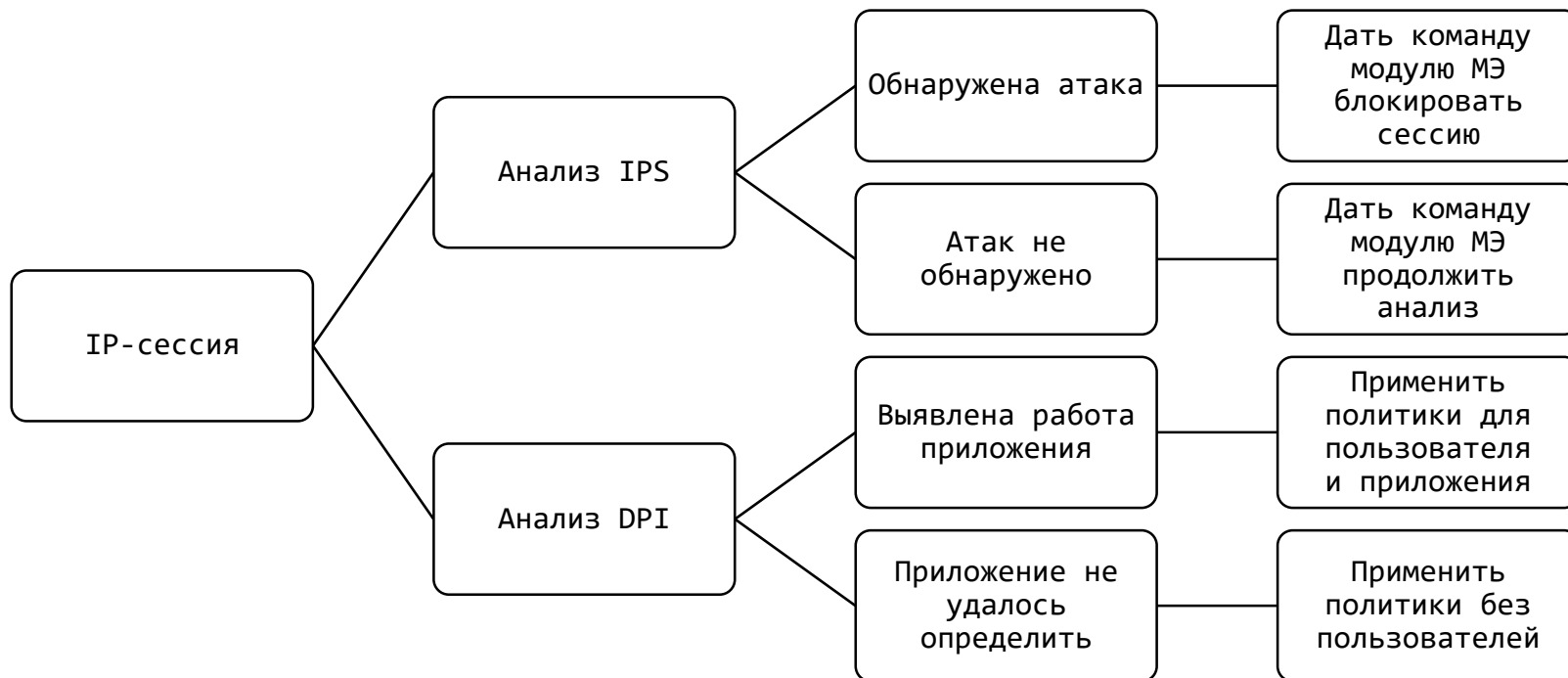
Трансляция IP-пакетов:

Событие:

Группа правил IPS:

Правило IPS:

Порядок применения правил IPS

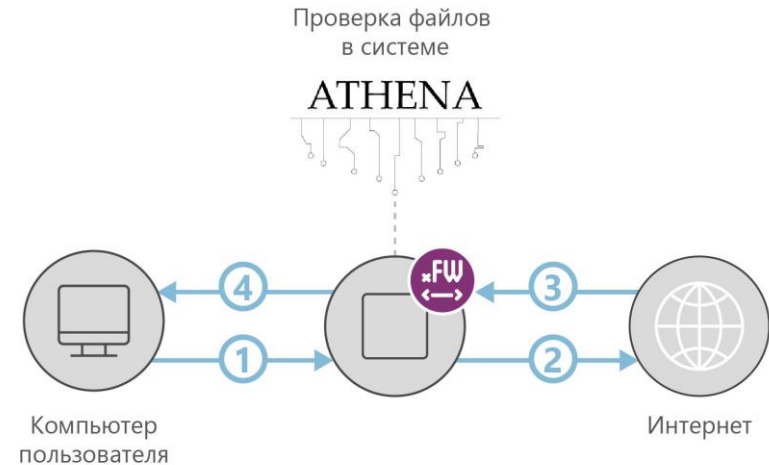


Gateway Antivirus – ШЛЮЗОВОЙ антивирус



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

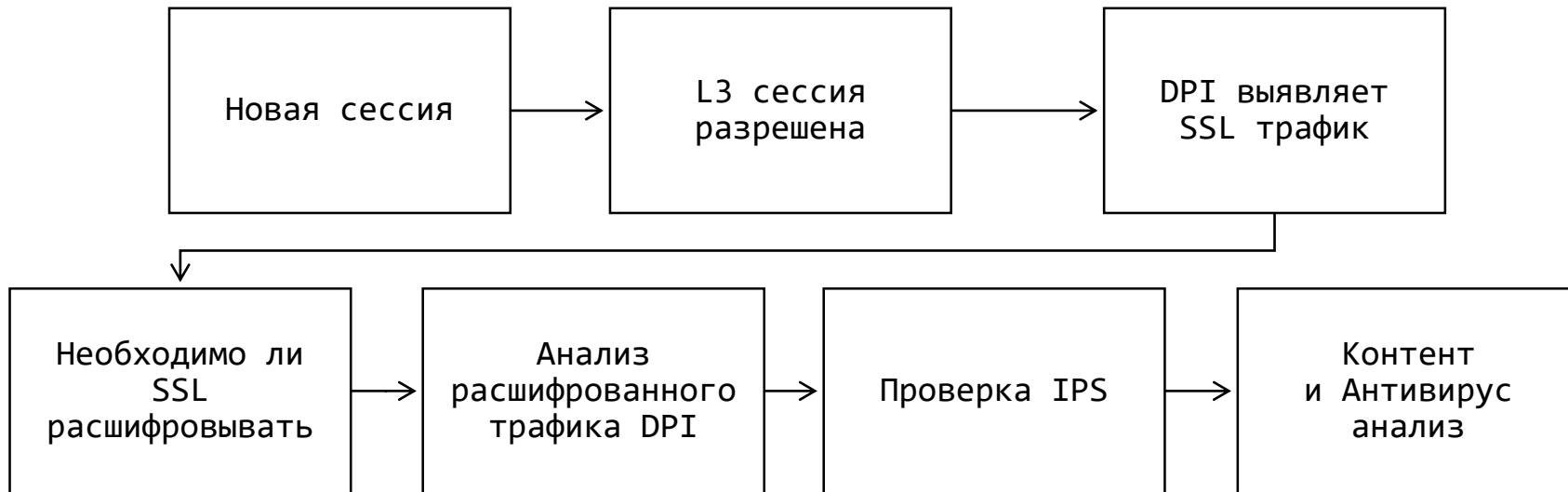


Классификация SSL

- 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

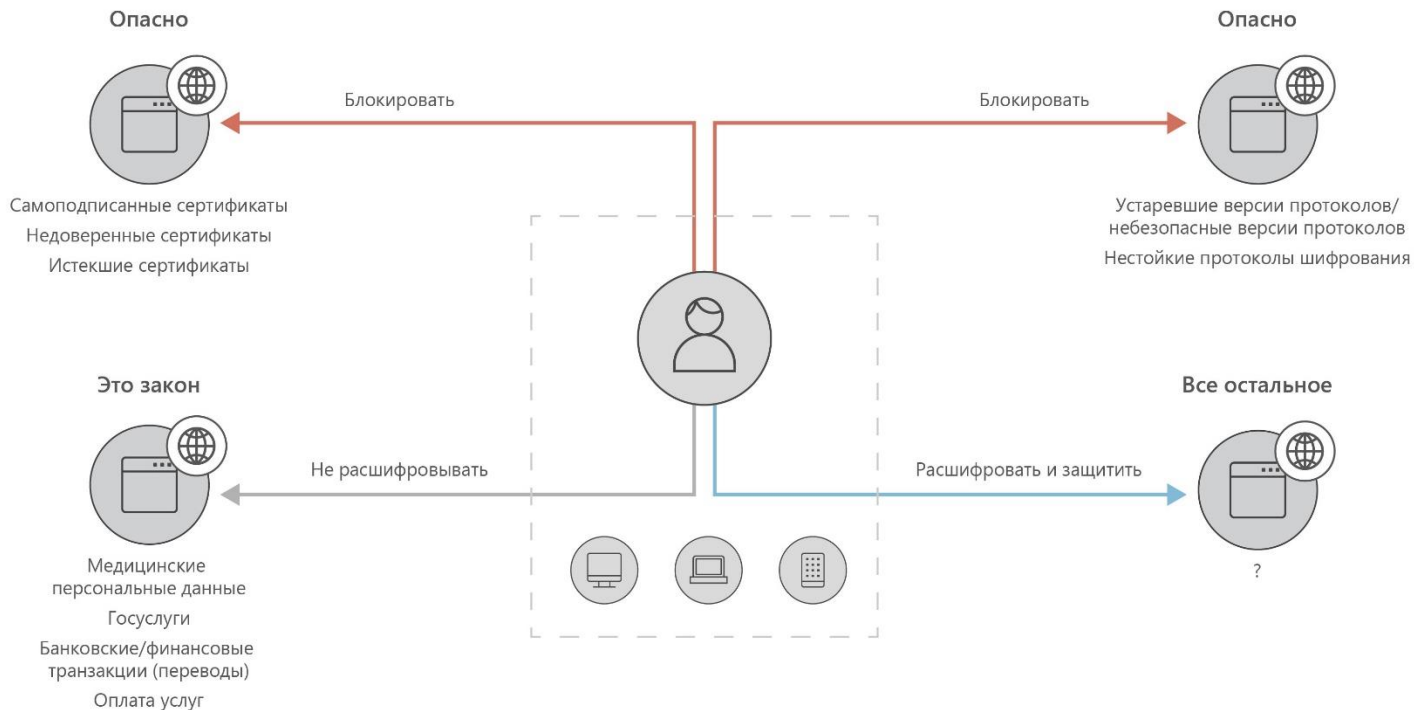
Корневой сертификат МСЭ (Firewall)



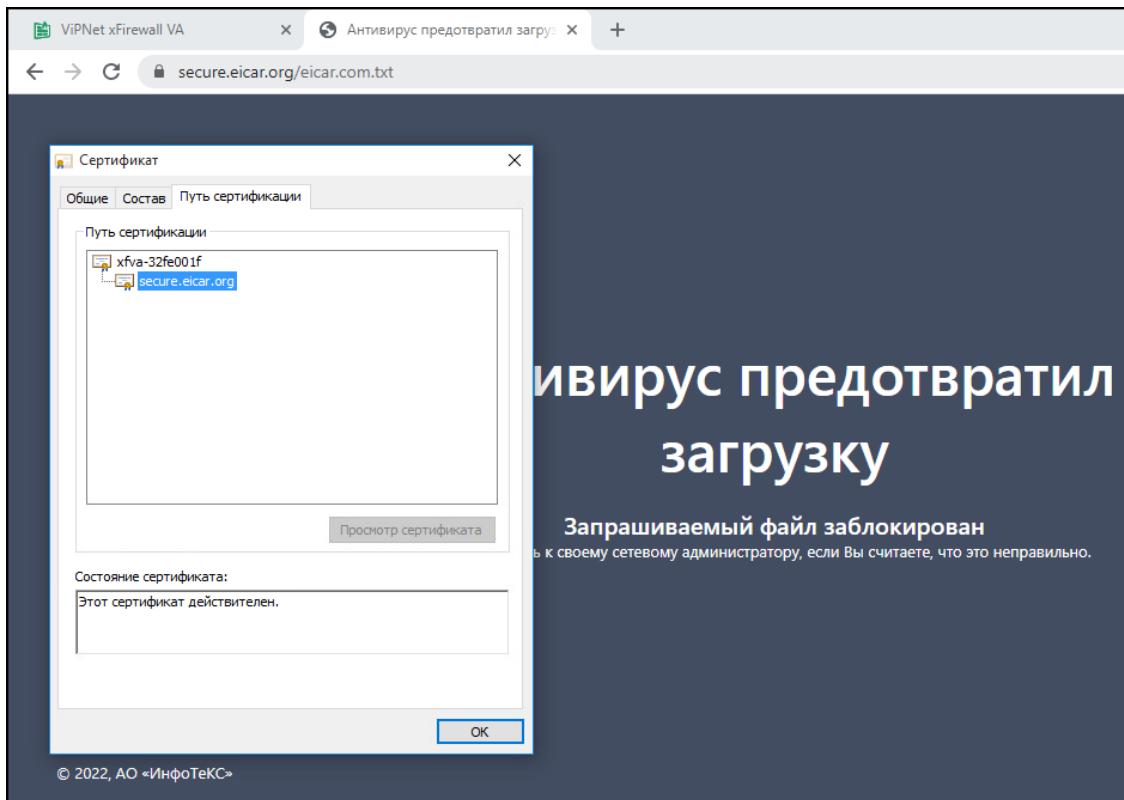
Клиент подтверждает корневой сертификат МСЭ



Лучшие практики SSL Inspection



Результат



ВиPNет xFirewall VA Антивирус предотвратил загрузку

← → ↻ secure.eicar.org/eicar.com.txt

Сертификат

Общие Состав Путь сертификации

Путь сертификации

- xfva-32fe001f
 - secure.eicar.org

Просмотр сертификата

Состояние сертификата:

Этот сертификат действителен.


ОК

Антивирус предотвратил загрузку

Запрашиваемый файл заблокирован

Обратитесь к своему сетевому администратору, если Вы считаете, что это неправильно.

© 2022, АО «ИнфоТекс»

A dark silhouette of a person wearing a hooded sweatshirt is centered on the left side of the slide. The background is a dark teal color filled with a pattern of white binary digits (0s and 1s) and some small square icons, creating a digital or data-themed atmosphere.

Защита от неизвестных угроз

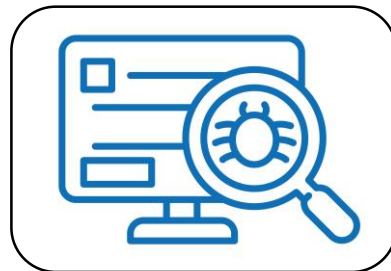
VIPNet xFirewall - повышает осведомленность



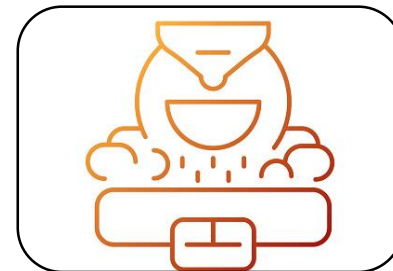
Максимальная
видимость -
фильтрация на 7
уровне ISO OSI



Защита от сетевых
атак - блокировка
аномалий, запретных
команд



Защита от вирусных
атак



Уменьшение
поверхности атаки



Спасибо за внимание!

Алексей Данилов

Руководитель направления

e-mail: danilov@infotecs.ru

Подписывайтесь на наши соцсети

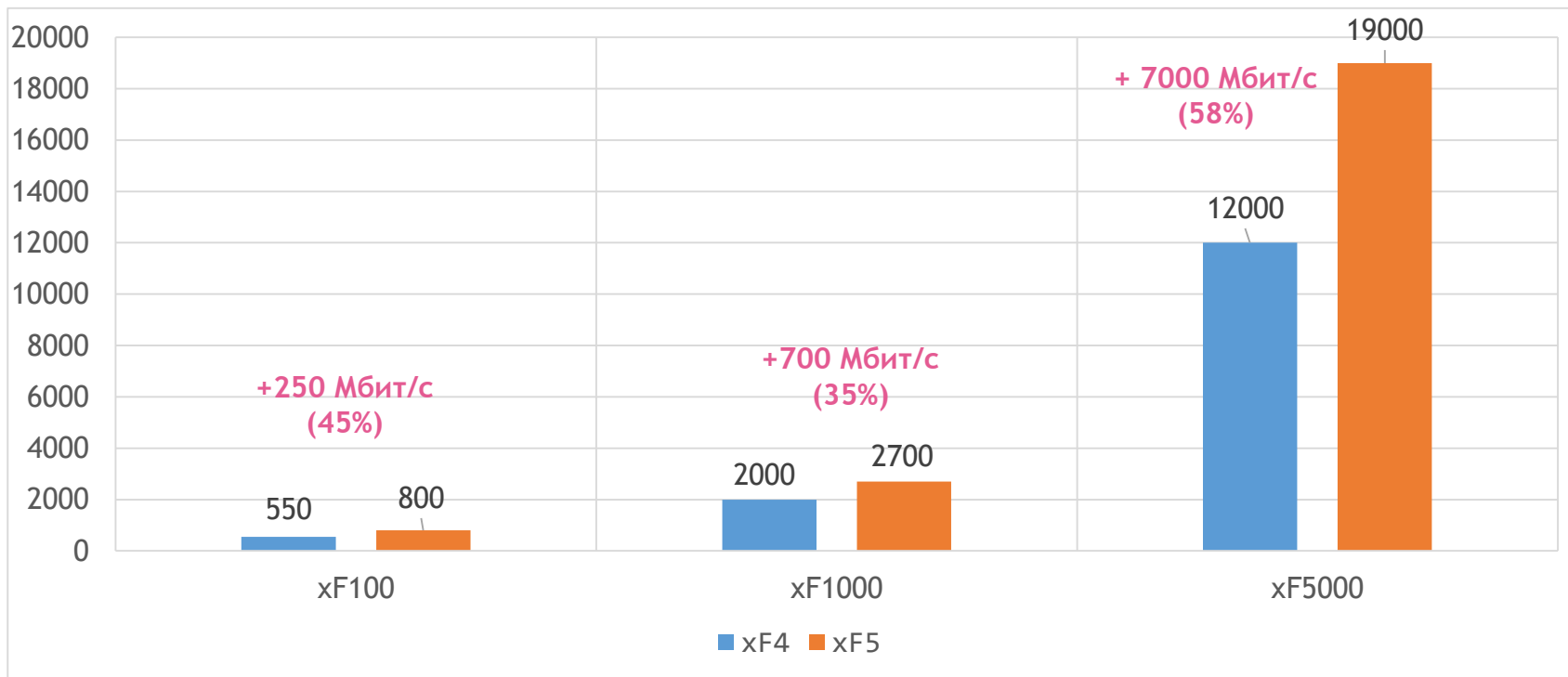


https://vk.com/infotecs_news

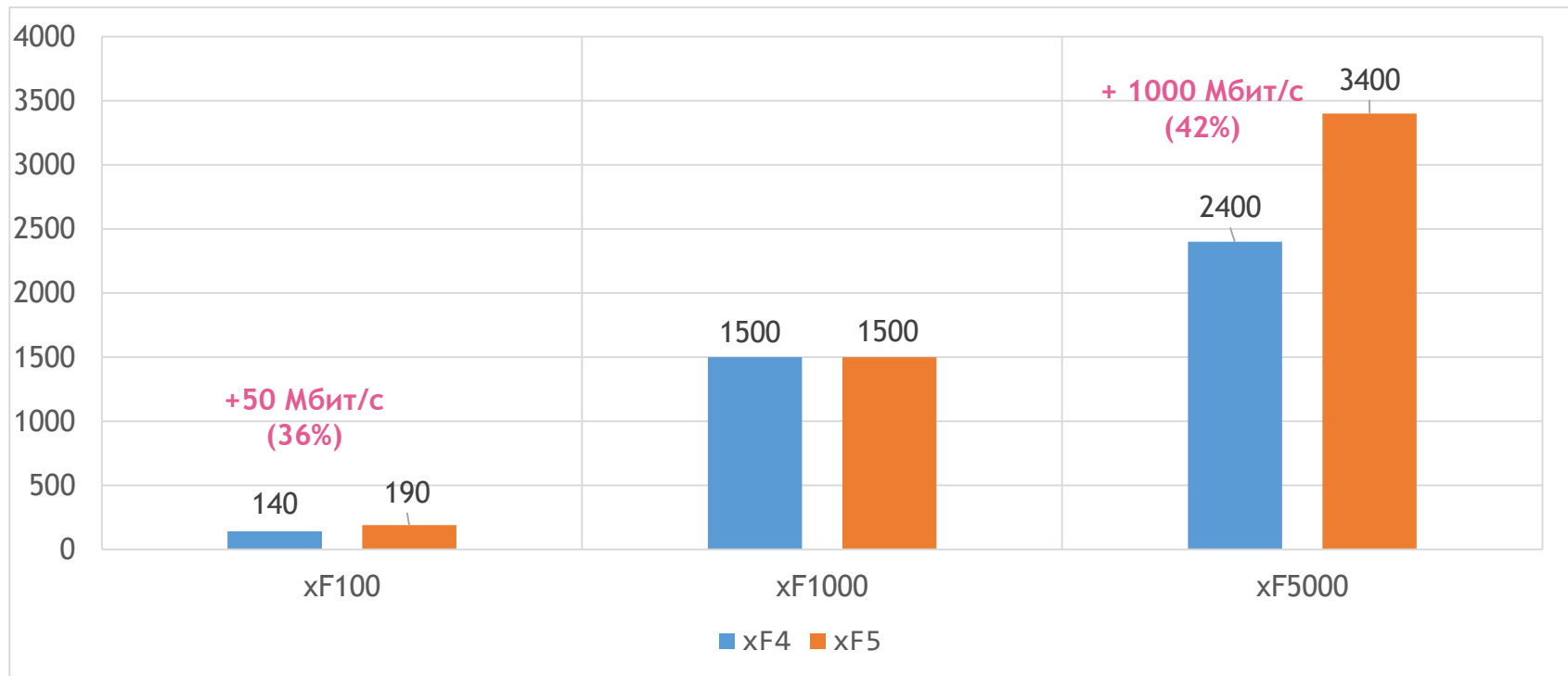


https://t.me/infotecs_news

Производительность МЭ (UDP)



Производительность Application Control



Производительность

Исполнение	xF100	xF1000 C/D	xF5000
Firewall, 1518 byte UDP (Mbps)	800	2 700	19 000
Firewall, TCP Multistream (Mbps)	720	2 700	9 300
AppControl (Firewall+DPI)(Mbps)	190	1 500	3 400
Firewall Throughput (64 bytes packets Per Second)	90 000	1 300 000	4 000 000
Connections per Second	2 500	20 000	50 000
Concurrent Connections	148 500	990 000	9 900 000
Users	~ 100	~ 1000	~ 6000

Max UDP > Max TCP > NGFW

BitTorrent, HTTP, HTTP(s), Oracle DB, SMTP, SSH и др.

3,4 Gb/ 6000 users = 0,56 Mbps/user