ViPNet xFirewall – многогранная защита периметра

Алексей Данилов
Руководитель направления
Отдел развития продуктов ИнфоТеКС

ViPNet xFirewall

Сертификат ФСТЭК

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4501

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 28 декабря 2021 г.

Выдан: 28 декабря 2021 г.
Действителен до: 28 декабря 2026 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс** ViPNet xFirewall 5, разработанный и производимый АО «ИнфоТеКС», является программно-аппаратным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции межсетевого экрана и системы обнаружения вторжений, соответствует требованиям по безопасности информации, установленным в документах «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) и задачи по безопасности ФРКЕ.465614.002Д1 при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.465614.002ФО.

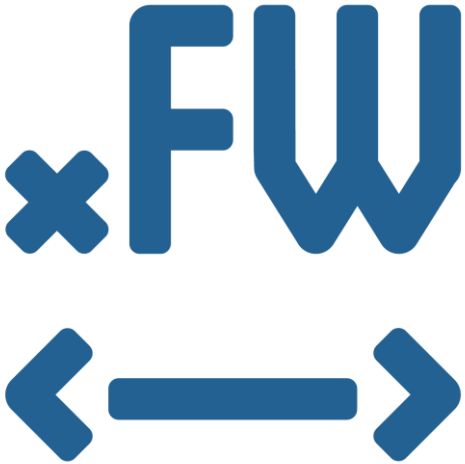
Сертификат выдан на основании технического заключения от 01.11.2021, оформленного по результатам сертификационных испытаний испытательной лабораторией МОУ «ИИФ» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 06.12.2021, оформленного органом по сертификации АО «Лаборатория ППШ» (аттестат аккредитации от 09.03.2017 № СЗИ RU.0001.01БИ00.А006).

Заявитель: АО «ИнфоТеКС»
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX, комната 29
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

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

Next-generation Firewall

Next-generation Firewall (NGFW)

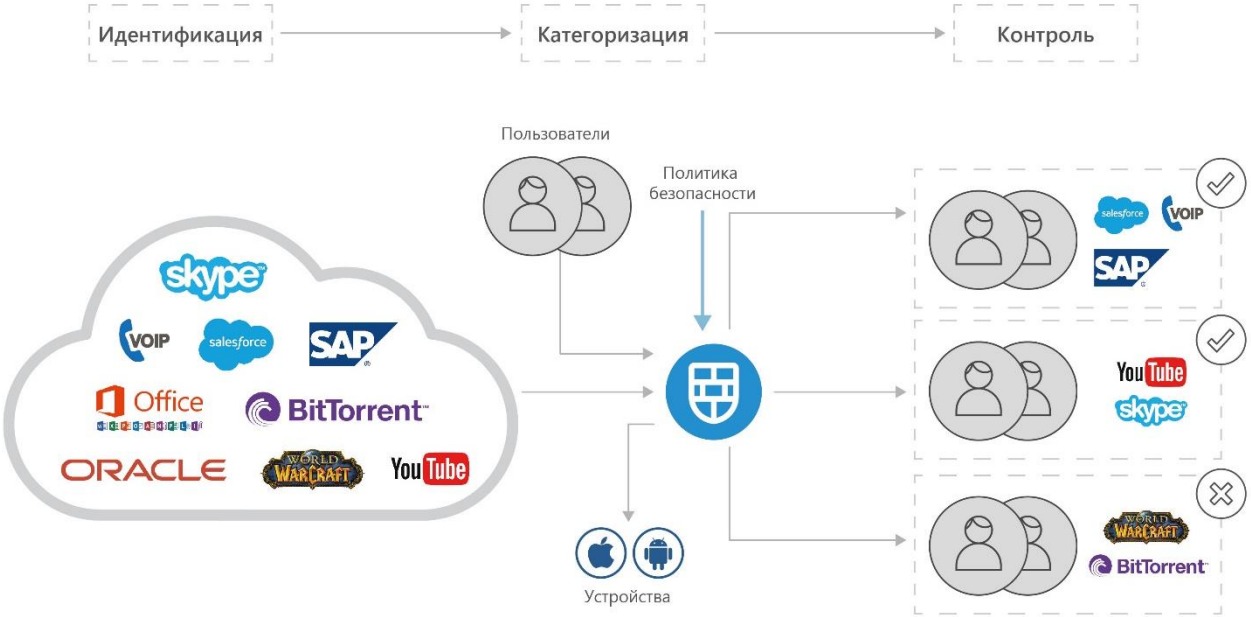
- Общепринято МЭ считать устройствами, реализующими технологию stateful packet inspection (SPI) сетевого трафика. МЭ разграничивает доступ на основе 5 параметров: адреса отправителя и получателя, порты отправителя и получателя, протокол L4.

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:

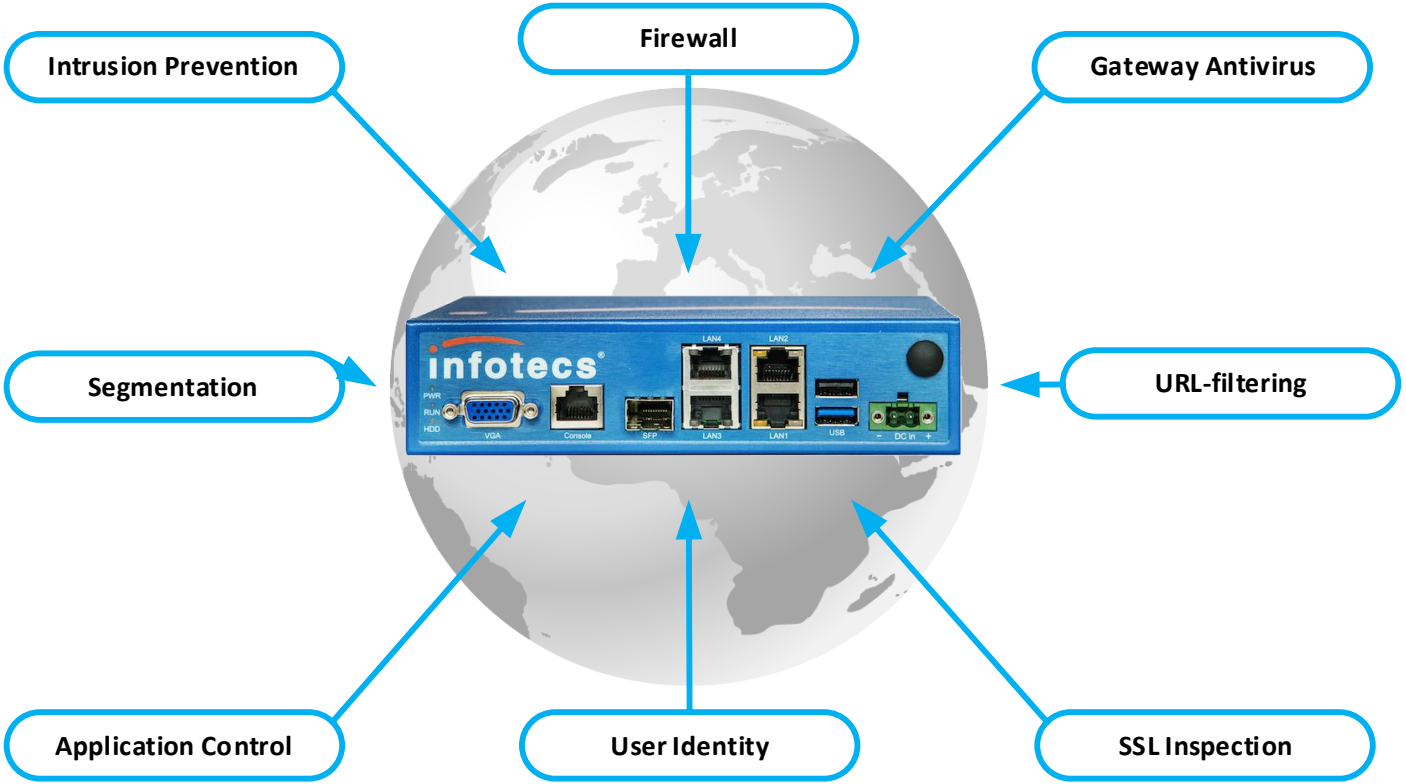
- Стандартного МЭ SPI
- Встроенной системы предотвращения атак IPS
- Системы контроля приложений
- Extrafirewall intelligence

ViPNet xFirewall

ViPNet xFirewall
с первого взгляда



Что такое ViPNet xFirewall



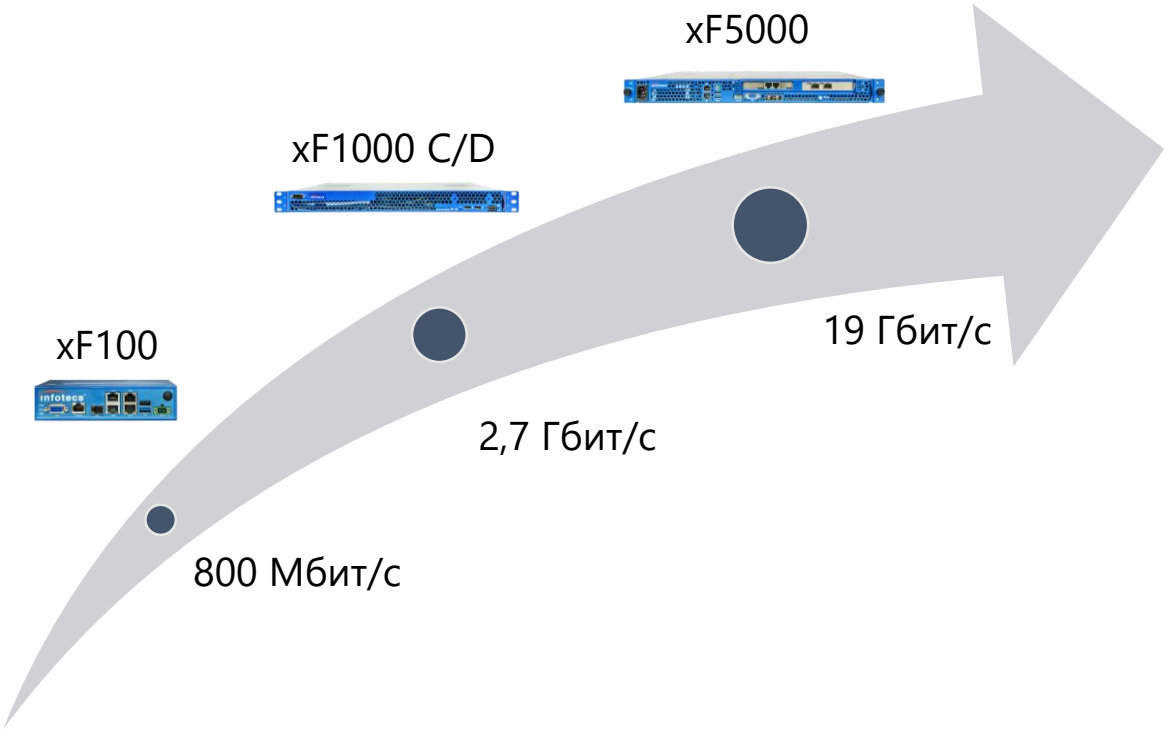
Что нового в 5-м поколении продукта

- **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-м 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 ТОРП**
- **SSL Inspection**

ViPNet xFirewall. Платформы



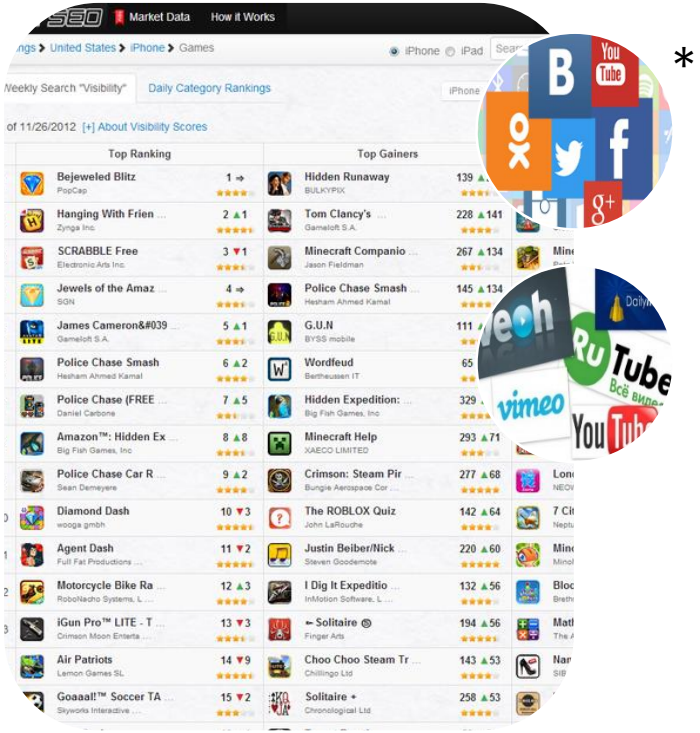
Повышена производительность

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



*

65 из категории «Социальные сети»

183 – потоковое видеовещание

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

*компания Meta признана в России экстремисткой организацией

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

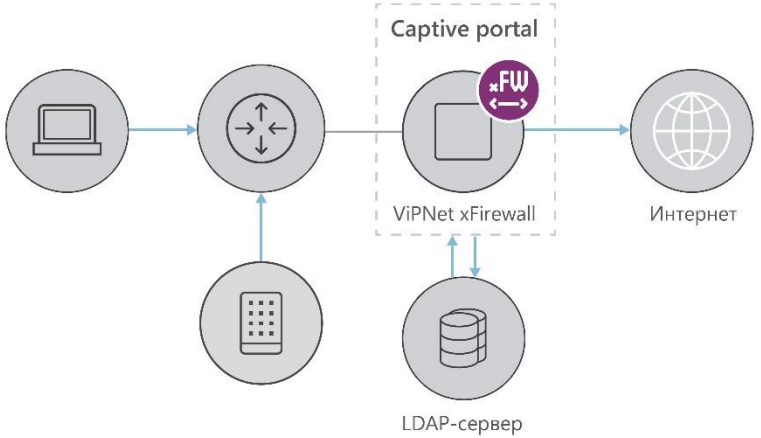
Использование учетных записей пользователей MS AD в правилах фильтрации

- 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

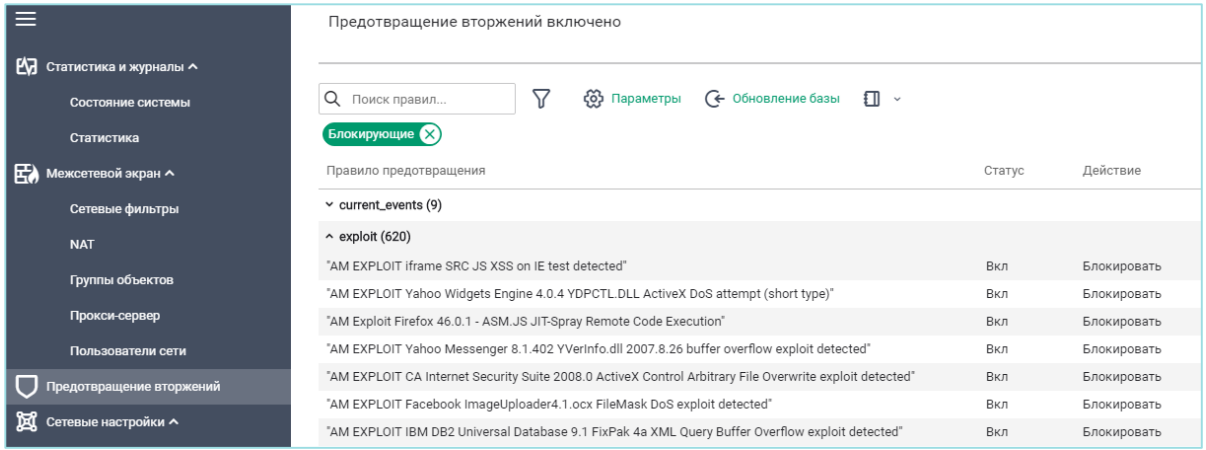
- Идентификация пользователей, использующих Linux компьютеры, iPhone, iPad и Android-устройства
- Предоставление контролируемого доступа подрядчикам, партнерам
- Автоматическое перенаправление на Портал аутентификации – Captive Portal

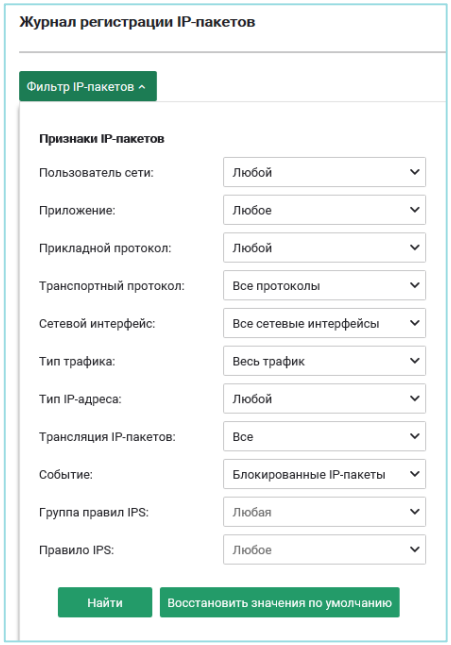


Для таких пользователей можно создать политику с ограниченным доступом к ресурсам компании, потому что их устройства могут быть без средств защиты.

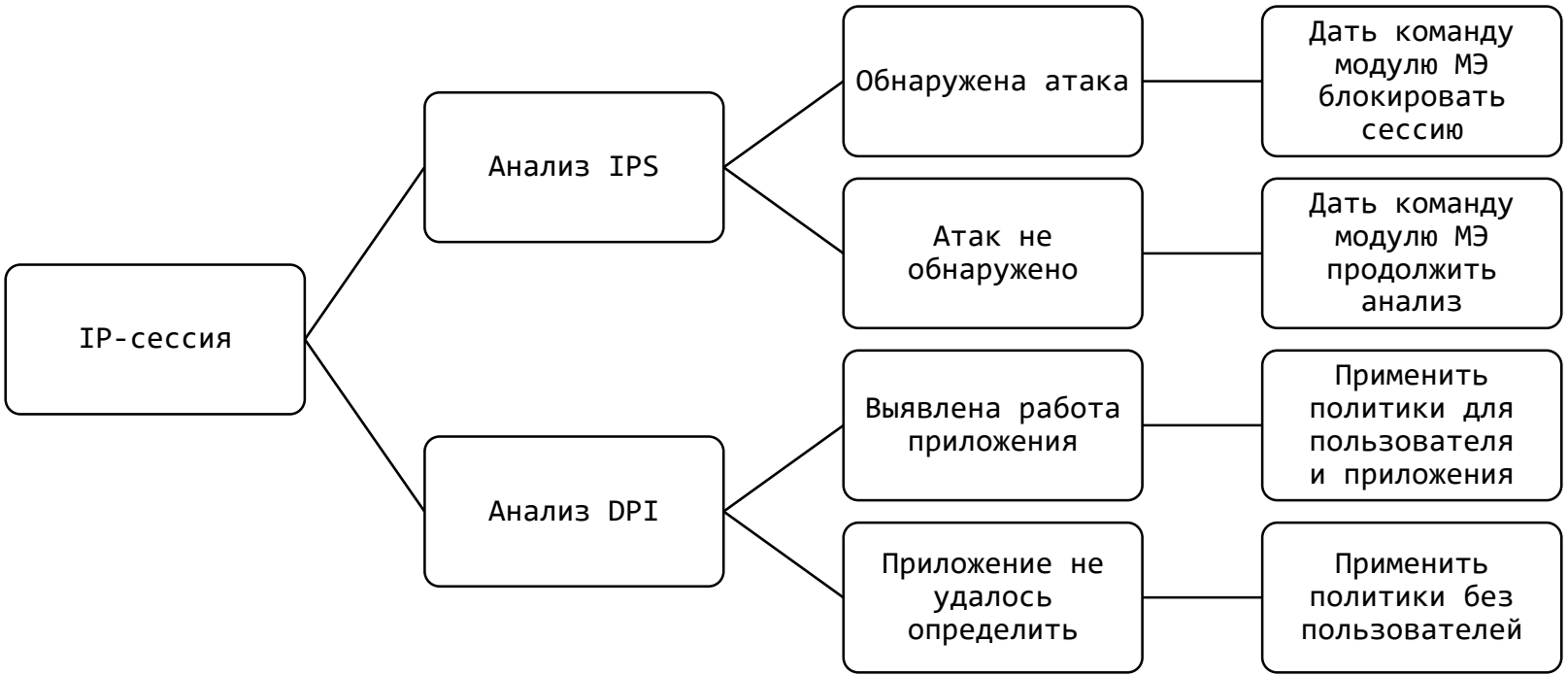
Intrusion Prevention - СОВ

Система предотвращения вторжений





Порядок применения правил IPS



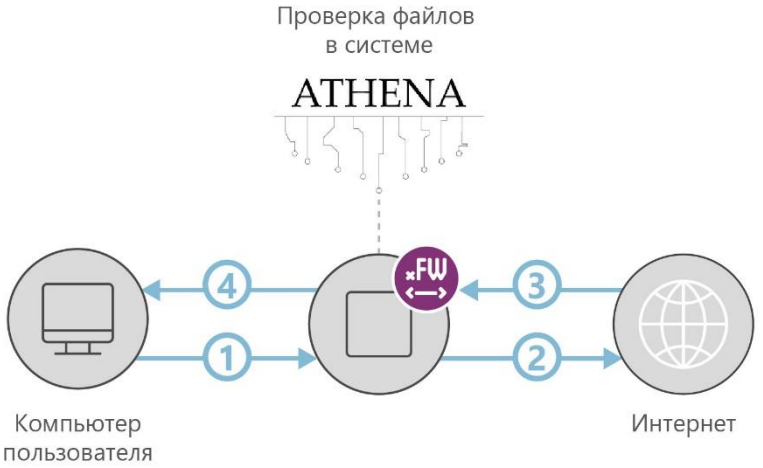
Gateway Antivirus – шлюзовой антивирус

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

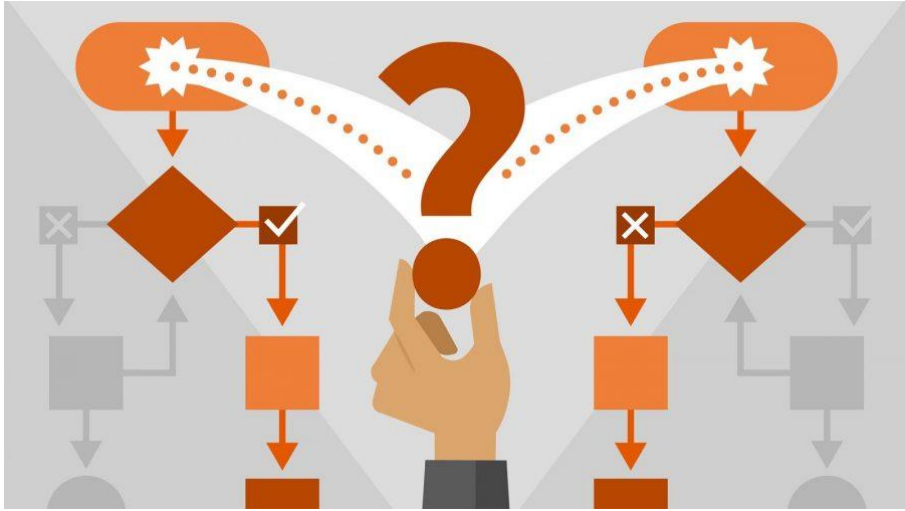
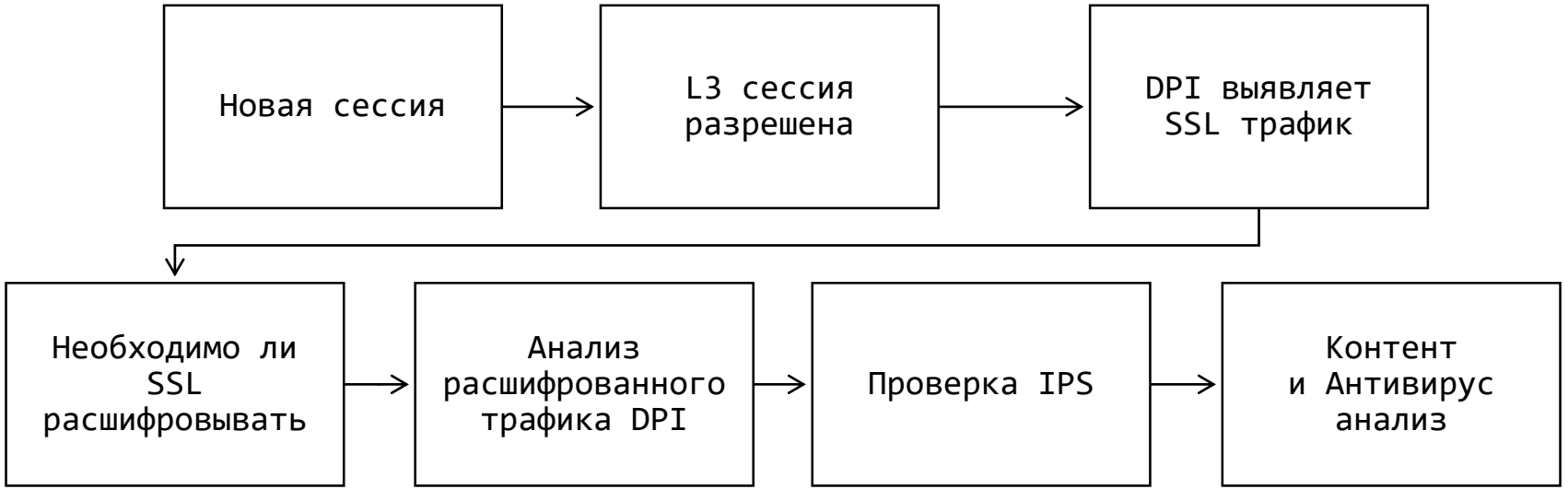
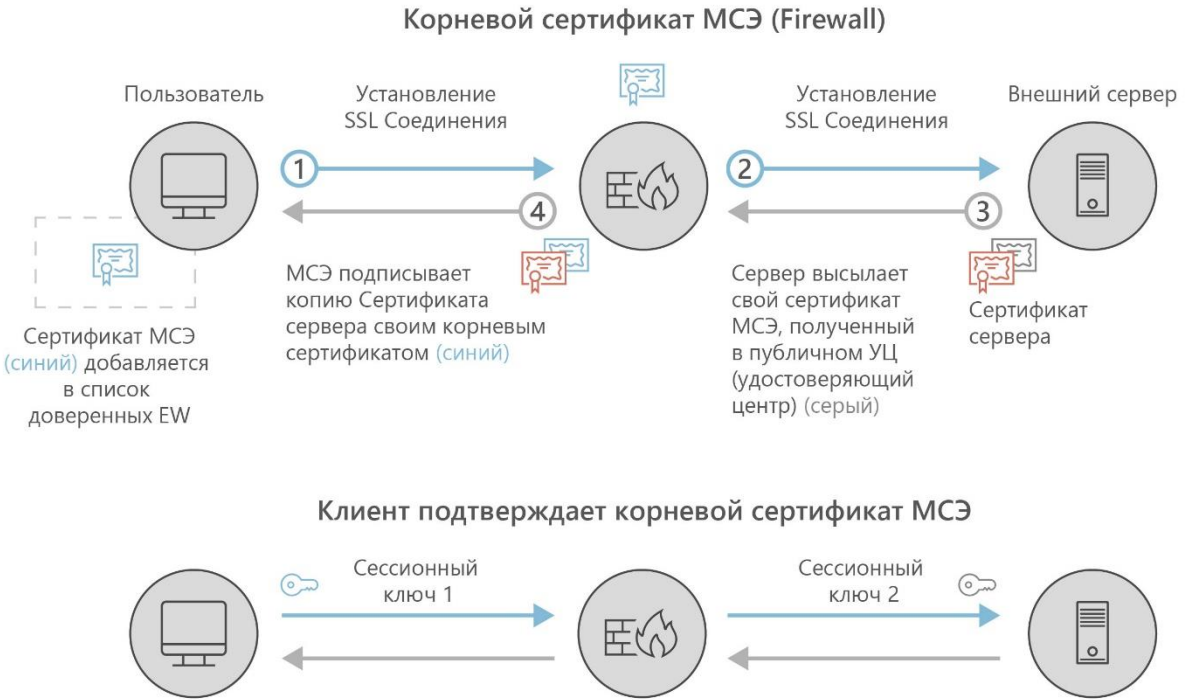


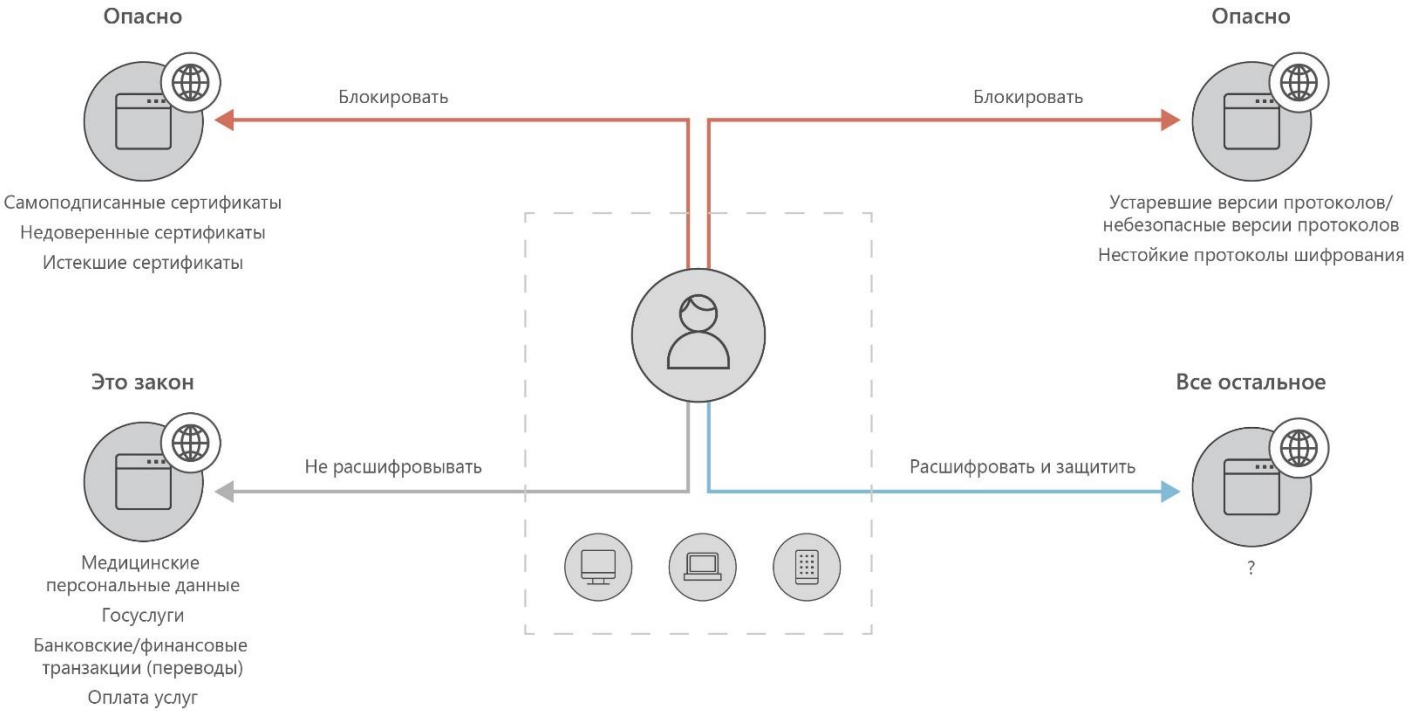
Схема проверки трафика



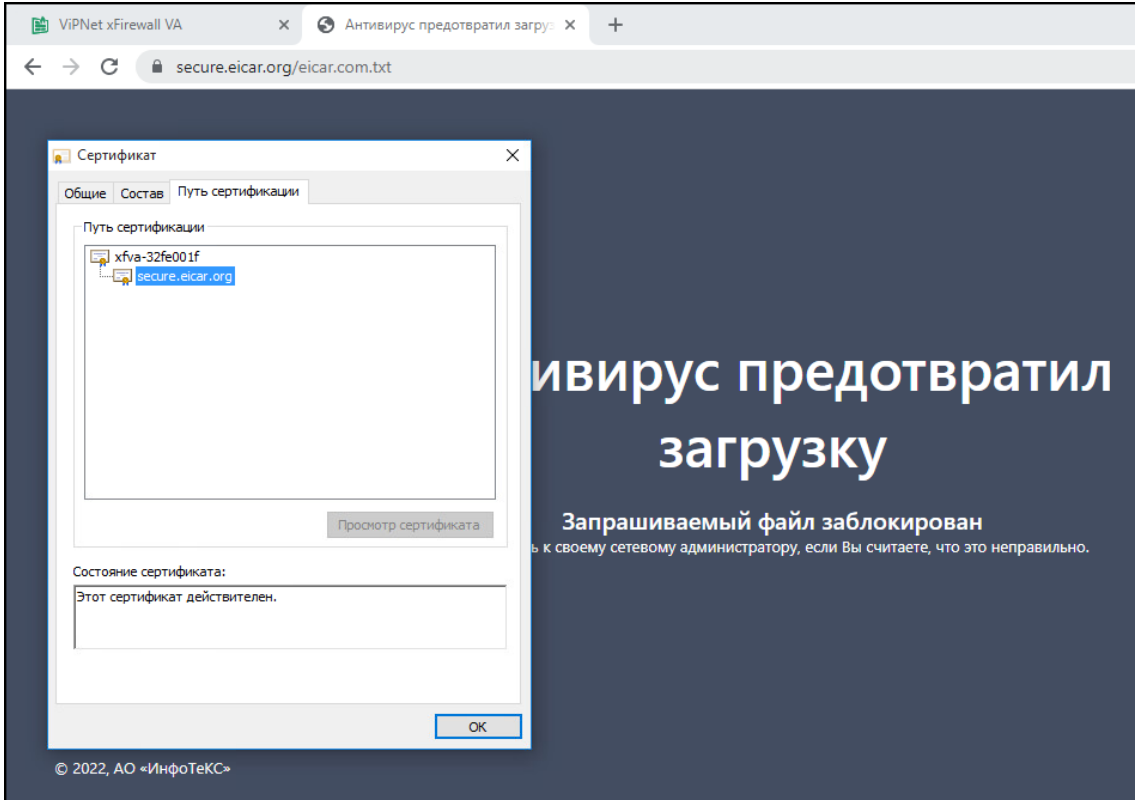
Forward proxy decryption



Лучшие практики SSL Inspection

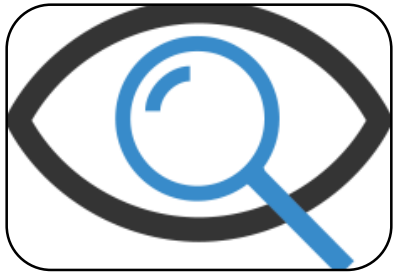


Результат


ViPNet xFirewall VA
Антивирус предотвратил загру
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.
OK
ивирус предотвратил загрузку
Запрашиваемый файл заблокирован
к своему сетевому администратору, если Вы считаете, что это неправильно.
© 2022, АО «ИнфоТеКС»

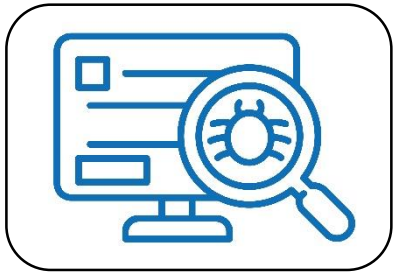
Защита от неизвестных угроз

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

ТЕХНО 2022 infotecs ФЕСТ

Спасибо за внимание!

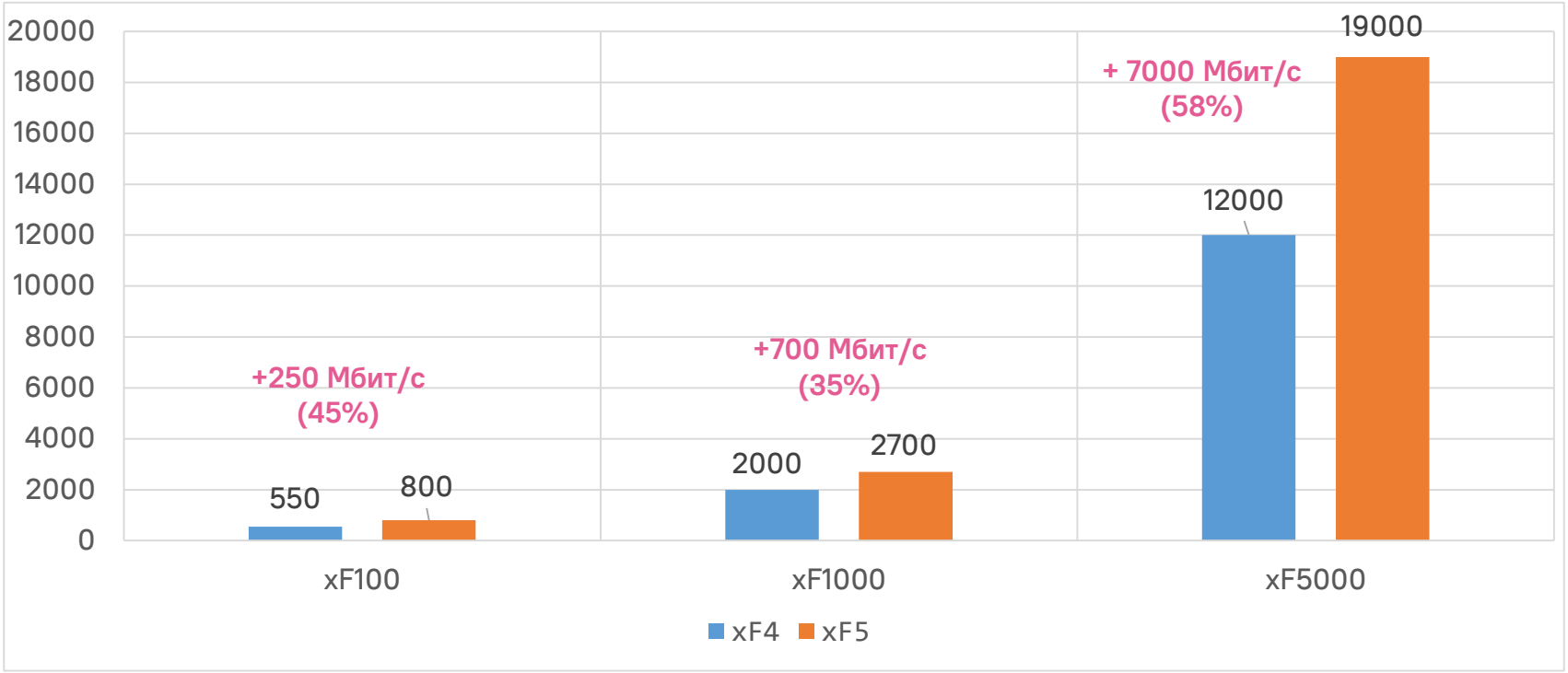
Алексей Данилов
Руководитель направления
e-mail: danilov@infotecs.ru

Подписывайтесь на наши соцсети

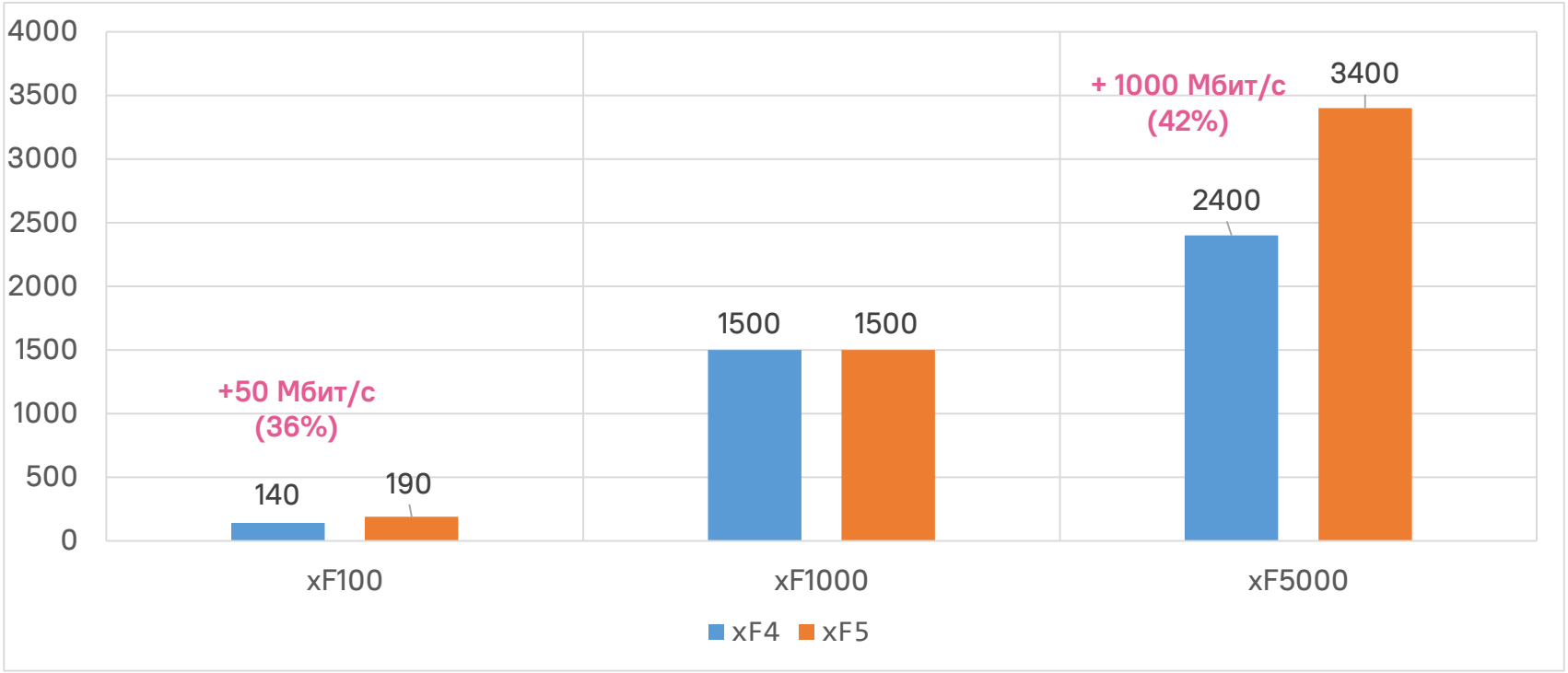
https://vk.com/infotecs_news

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