# ViPNet xFirewall 5.6.0: новые возможности шлюза безопасности

Алексей Данилов
Руководитель направления
Отдел развития продуктов ИнфоТеКС

# Next-generation Firewall

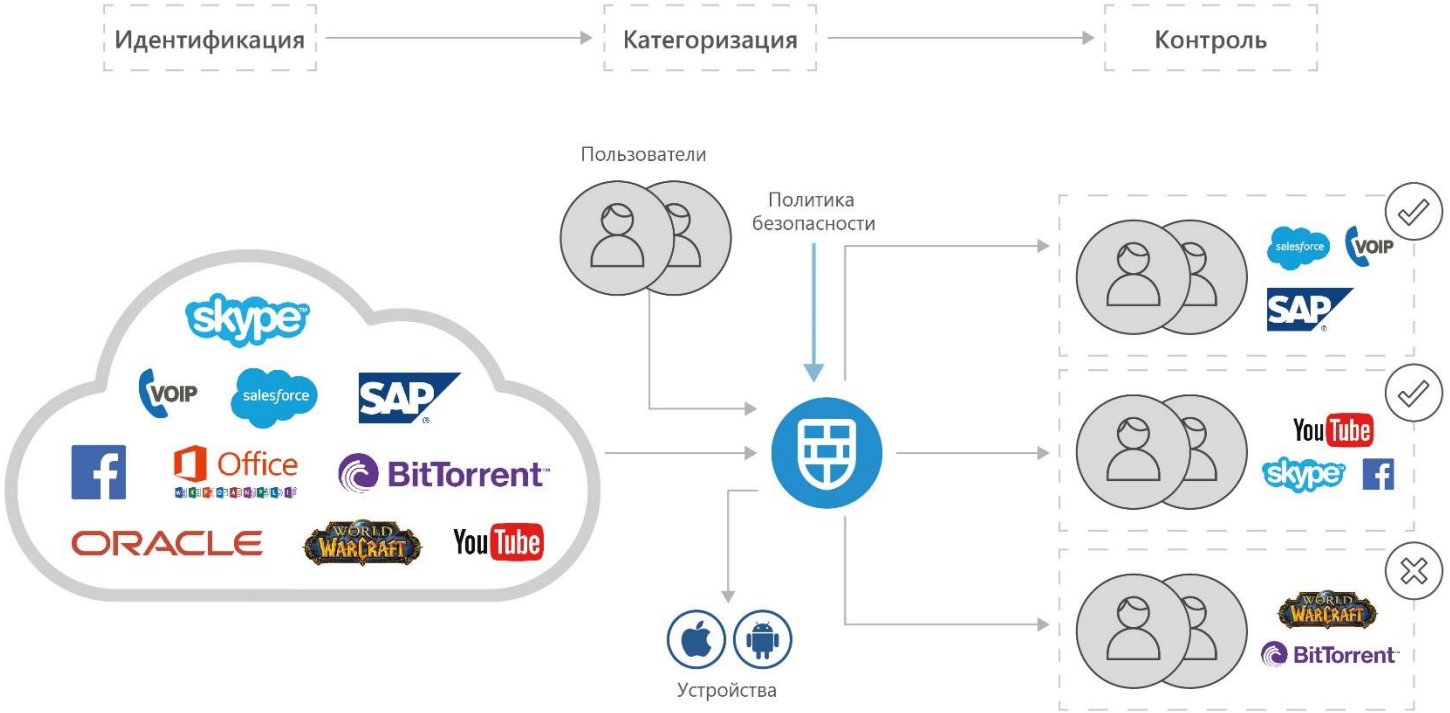
# Next-Generation Firewall (NGFW)


- Общепринято МЭ считать устройства, реализующие 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:

- Стандартный МЭ SPI
- Встроенная система предотвращения атак IPS
- Система контроля приложений
- Extrafirewall intelligence

# NGFW с первого взгляда



# ViPNet xFirewall

# 7 задач

Знать что охранять

Управлять доступом

Защитить от сетевых атак

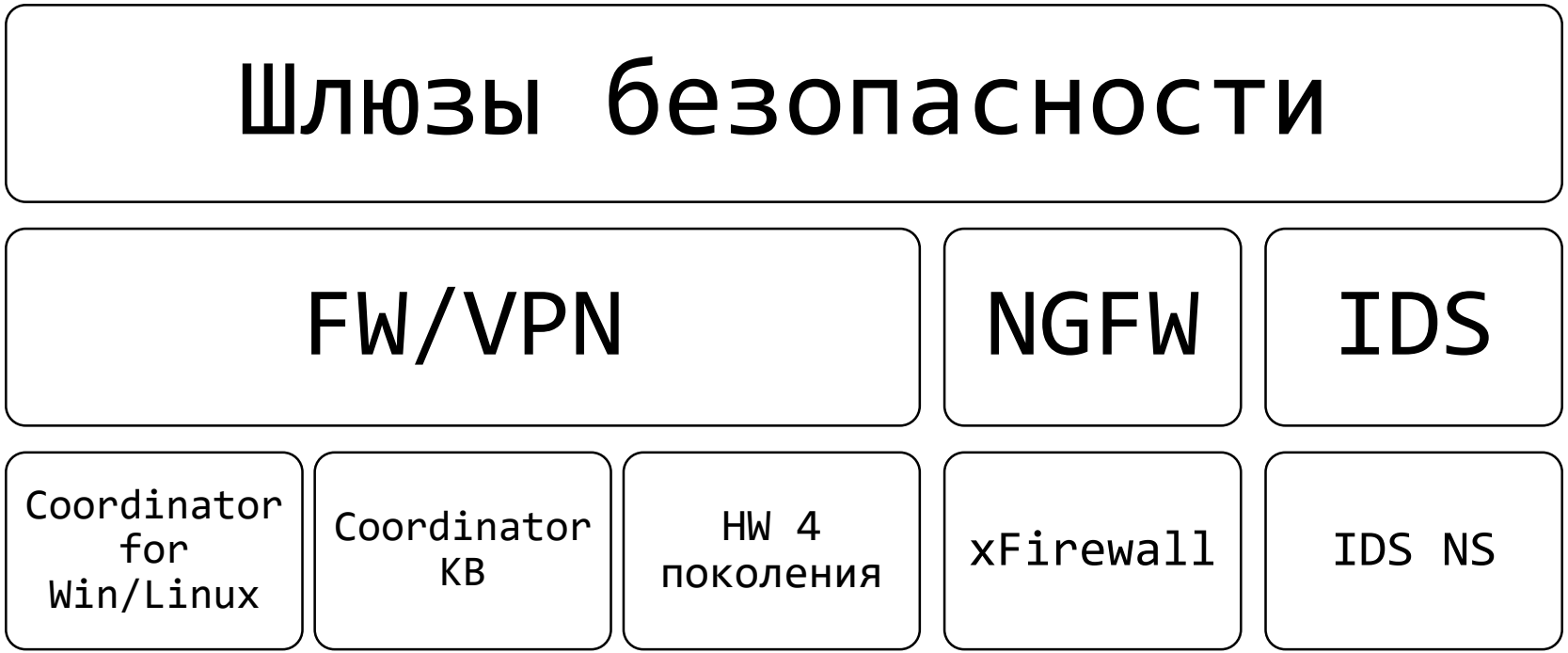
Реализовать BYOD

Защитить от вирусов

Что делать с SSL

Защита от неизвестных угроз

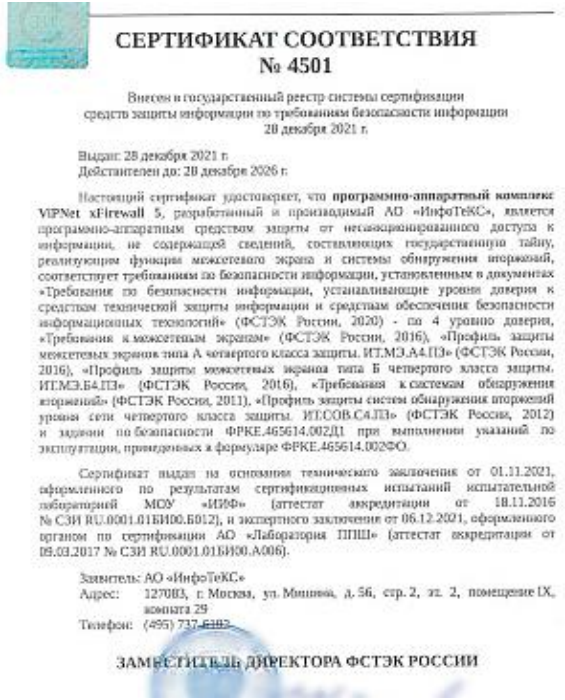
# ViPNet xFirewall



# Что такое ViPNet xFirewall

| | | |
|---|---|---|
| Сетевая платформа в составе: | Межсетевой экран | Сетевой экран приложений - DPI |
| Система предотвращения вторжений | Шлюзовой антивирус | Интеграция с Active Directory |

# Сертификат ФСТЭК



**СЕРТИФИКАТ СООТВЕТСТВИЯ**
**№ 4501**

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 20 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 задании 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).

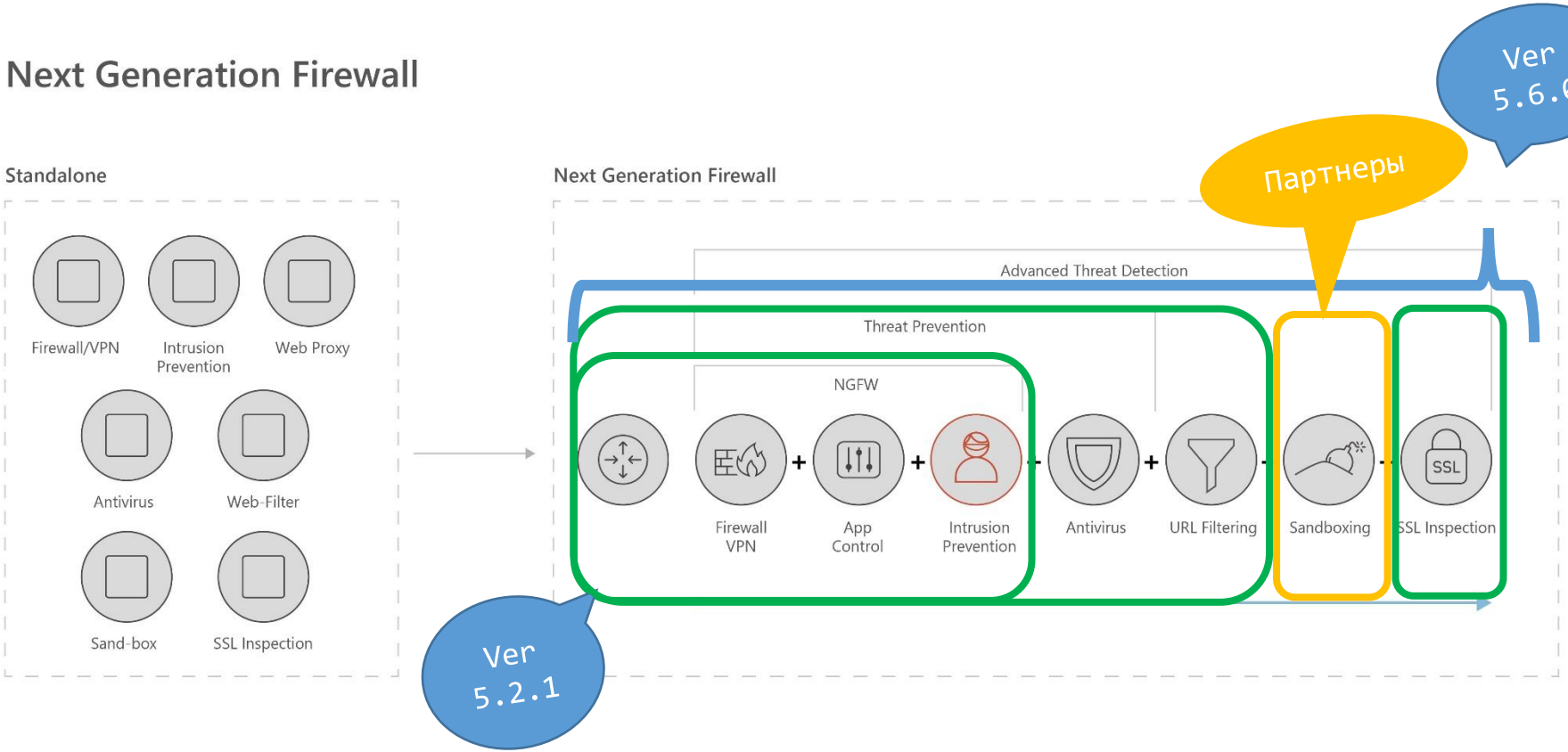
Заявитель: АО «ИнфоТеКС»
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX, комната 29
Телефон: (495) 737-6192

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)

# ViPNet xFirewall 5.6.0

## Next Generation Firewall



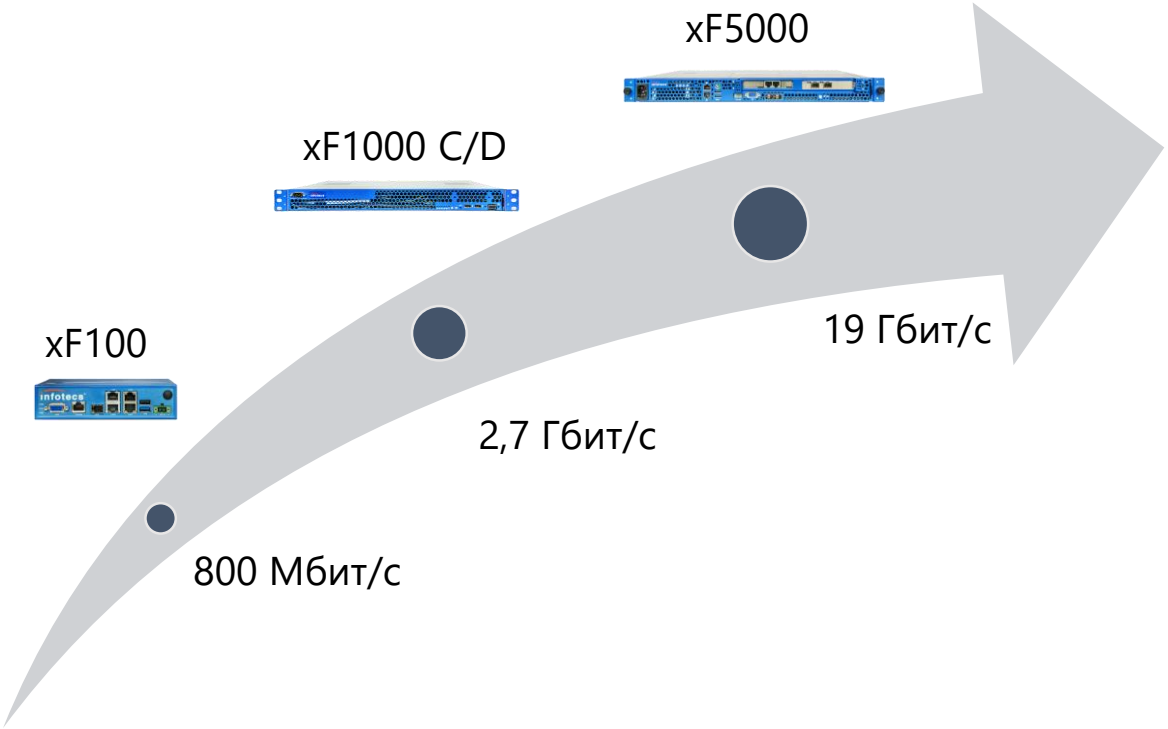
# Что нового в 5 поколении продукта

- 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

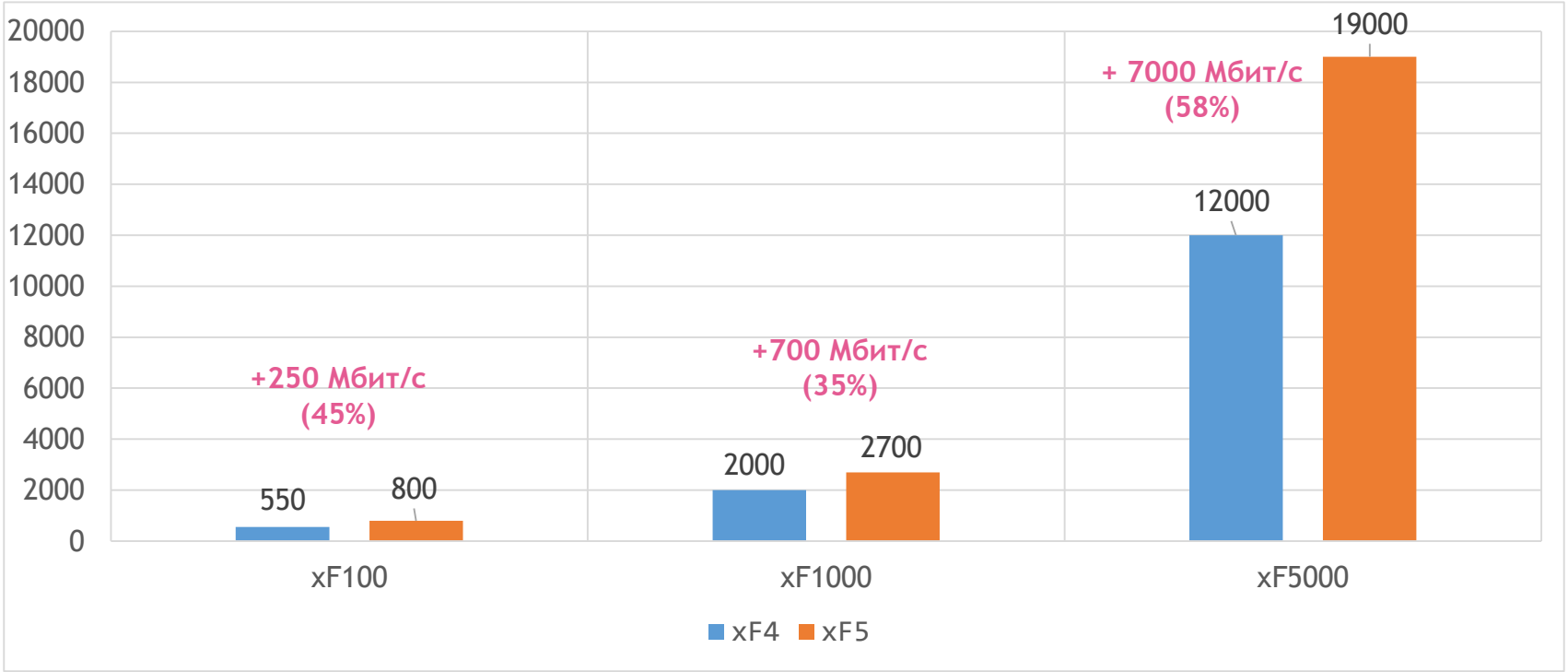
# Что нового в 5 поколении продукта

- 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 ТОРП
- SSL Inspection

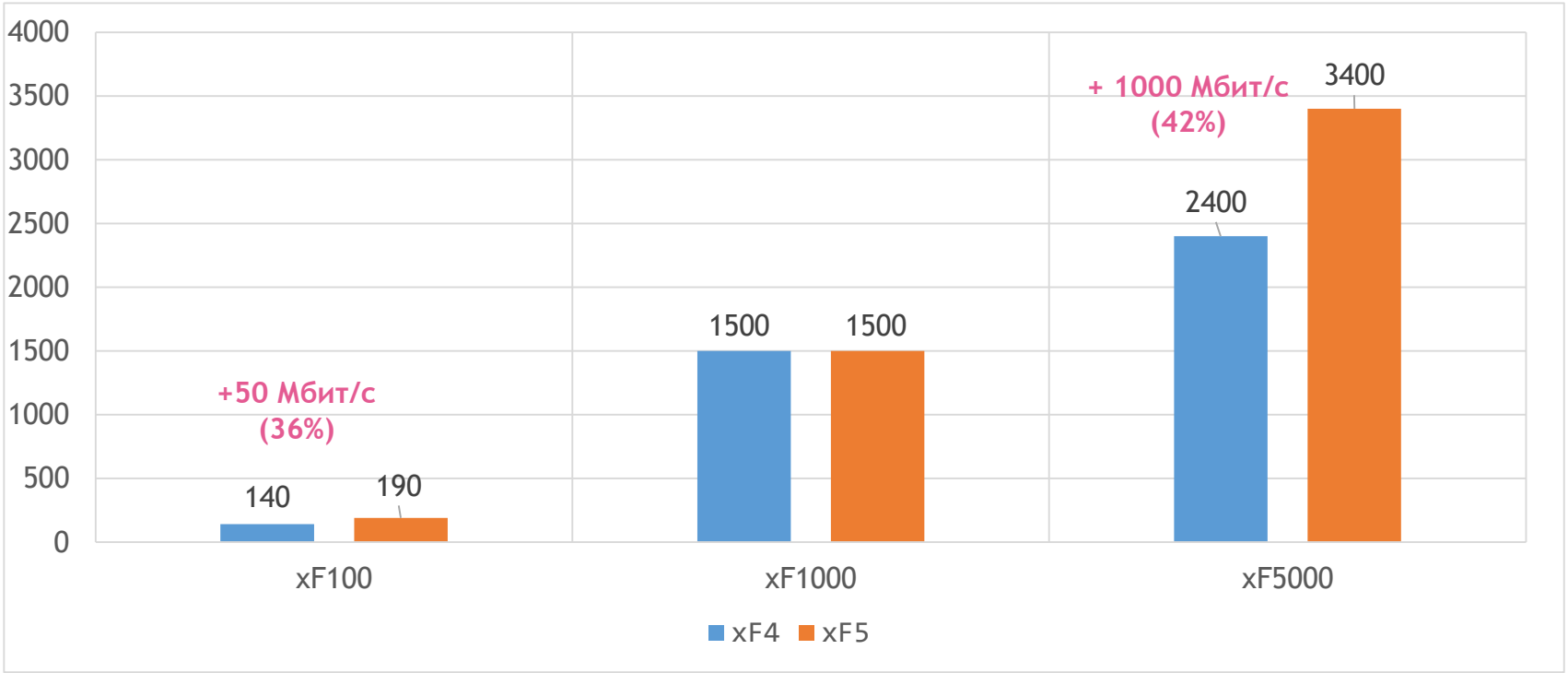
# ViPNet xFirewall. Платформы



# 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

# Знать что охранять

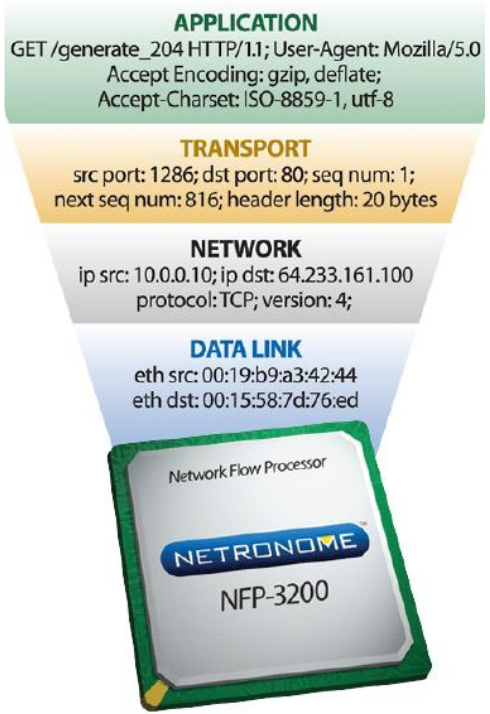

- Открыл порты 80/443 == Открыл всЁ!

# Что такое сессия

L3-L4 сессия – TCP/UDP – 40 байт для анализа

| Flow Definition Fields |
| --- |
| Ingress Interface |
| Ethernet Source MAC Address |
| Ethernet Destination MAC Address |
| Ethertype |
| VLAN ID |
| Source IP Address |
| Destination IP Address |
| IP Protocol |
| TCP/UDP Source Port |
| TCP/UDP Destination Port |
| ICMP Type/Code |

L7 сессия – приложение - L4+L6+L7 ~1500 байт

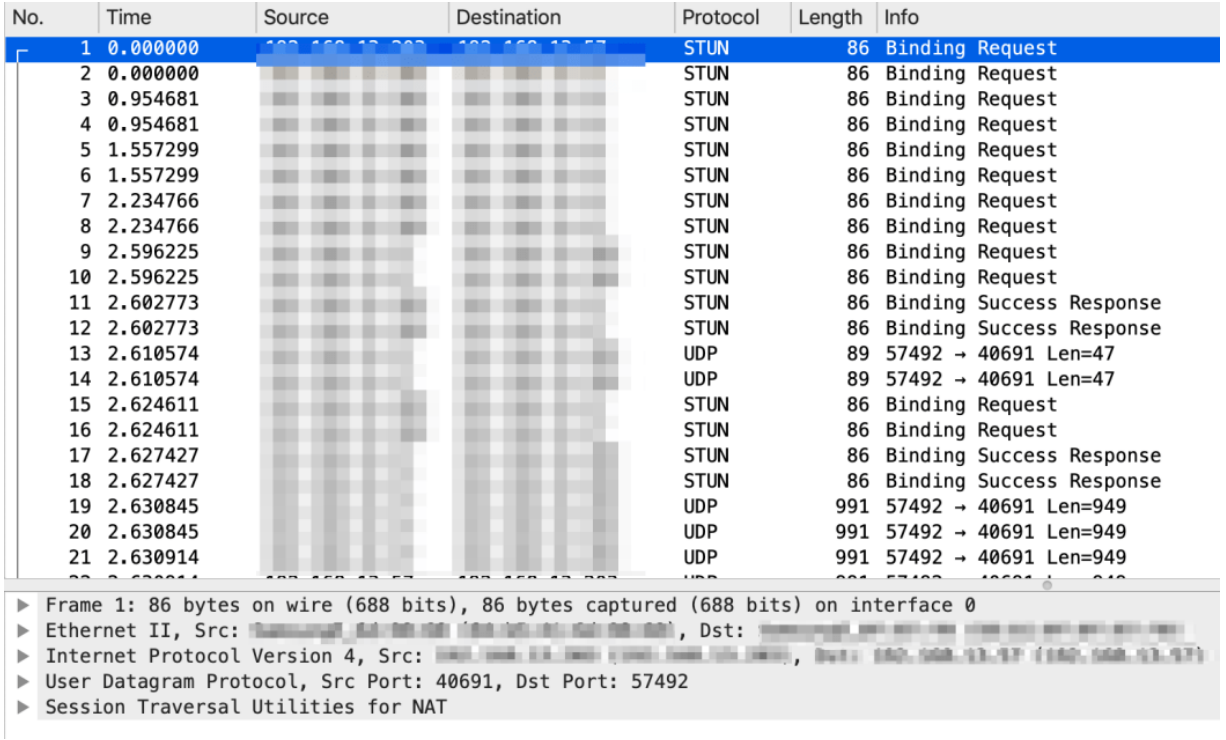


# Как WhatsApp устанавливает сессию

Для установления соединения WhatsApp использует прокол туннелирования STUN и нужно захватить 13 пакетов, чтобы правильно определить приложение.

Facebook WhatsApp/Messenger, Google Hangout/Duo/Meet тоже используют STUN.

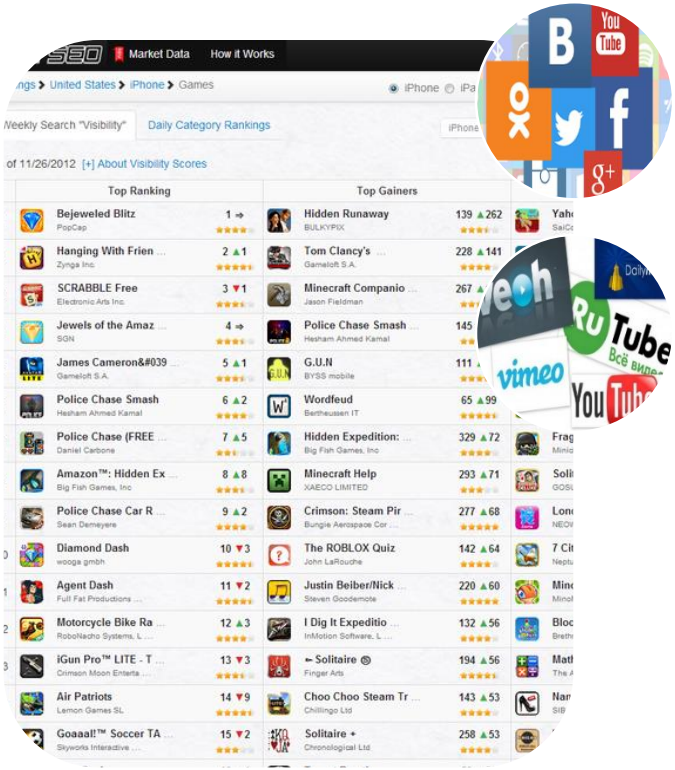
BattleNet, Facetime, Microsoft Teams, Odnoklassniki, Signal, Skype, Snapchat, Steam, Telegram, Twitch, Viber,VK, Webex, Yandex Telemost



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | [redacted] | [redacted] | STUN | 86 | Binding Request |
| 2 | 0.000000 | [redacted] | [redacted] | STUN | 86 | Binding Request |
| 3 | 0.954681 | [redacted] | [redacted] | STUN | 86 | Binding Request |
| 4 | 0.954681 | [redacted] | [redacted] | STUN | 86 | Binding Request |
| 5 | 1.557299 | [redacted] | [redacted] | STUN | 86 | Binding Request |
| 6 | 1.557299 | [redacted] | [redacted] | STUN | 86 | Binding Request |
| 7 | 2.234766 | [redacted] | [redacted] | STUN | 86 | Binding Request |
| 8 | 2.234766 | [redacted] | [redacted] | STUN | 86 | Binding Request |
| 9 | 2.596225 | [redacted] | [redacted] | STUN | 86 | Binding Request |
| 10 | 2.596225 | [redacted] | [redacted] | STUN | 86 | Binding Request |
| 11 | 2.602773 | [redacted] | [redacted] | STUN | 86 | Binding Success Response |
| 12 | 2.602773 | [redacted] | [redacted] | STUN | 86 | Binding Success Response |
| 13 | 2.610574 | [redacted] | [redacted] | UDP | 89 | 57492 → 40691 Len=47 |
| 14 | 2.610574 | [redacted] | [redacted] | UDP | 89 | 57492 → 40691 Len=47 |
| 15 | 2.624611 | [redacted] | [redacted] | STUN | 86 | Binding Request |
| 16 | 2.624611 | [redacted] | [redacted] | STUN | 86 | Binding Request |
| 17 | 2.627427 | [redacted] | [redacted] | STUN | 86 | Binding Success Response |
| 18 | 2.627427 | [redacted] | [redacted] | STUN | 86 | Binding Success Response |
| 19 | 2.630845 | [redacted] | [redacted] | UDP | 991 | 57492 → 40691 Len=949 |
| 20 | 2.630845 | [redacted] | [redacted] | UDP | 991 | 57492 → 40691 Len=949 |
| 21 | 2.630914 | [redacted] | [redacted] | UDP | 991 | 57492 → 40691 Len=949 |

▶ Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
▶ Ethernet II, Src: [redacted], Dst: [redacted]
▶ Internet Protocol Version 4, Src: [redacted]
▶ User Datagram Protocol, Src Port: 40691, Dst Port: 57492
▶ Session Traversal Utilities for NAT

# Более 5000 приложений/протоколов




65 из категории «Социальные сети»

183 – потоковое видеовещание

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

# Управлять доступом

# 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

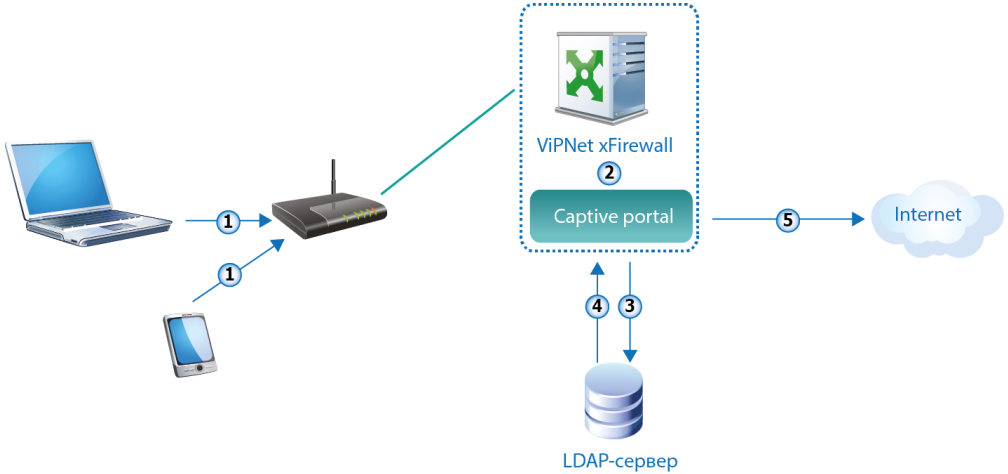
Использование учетных записей пользователей MS AD в правилах фильтрации

- 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

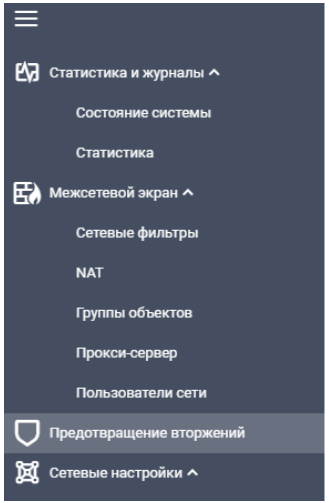
- Идентификация пользователей, использующих Linux компьютеры, iPhone, iPad и Android-устройства
- Предоставление контролируемого доступа подрядчикам, партнерам
- Автоматическое перенаправление на Портал аутентификации – Captive Portal

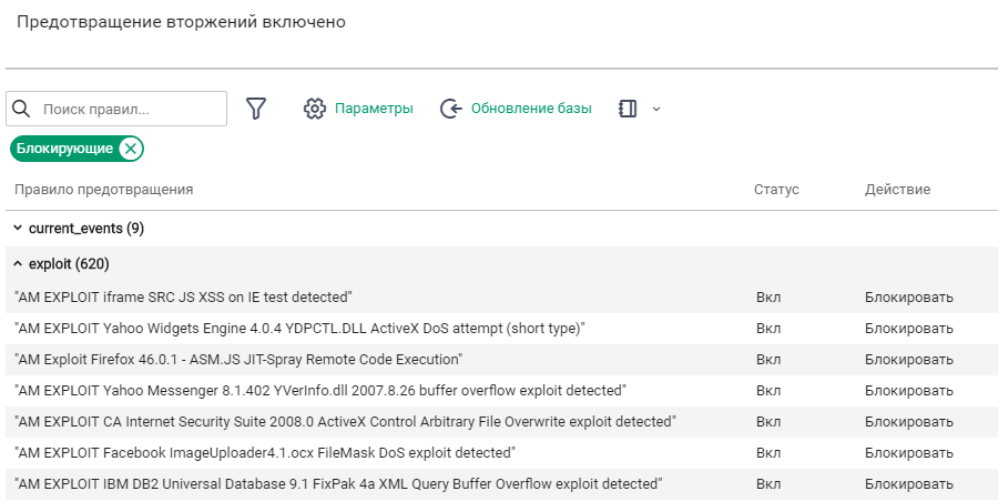


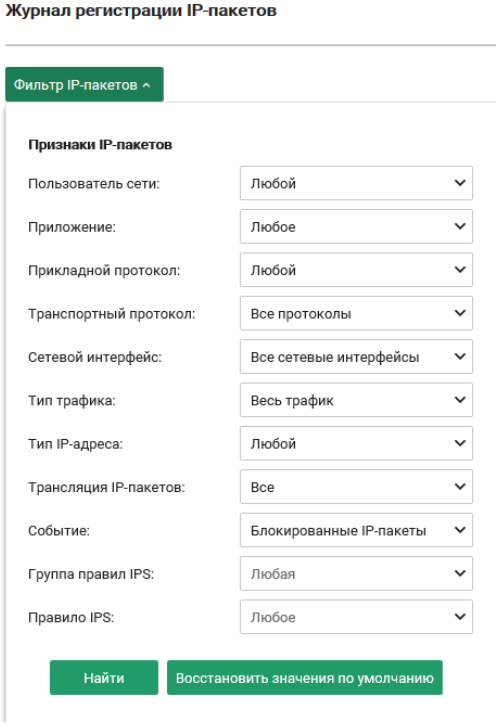

Для таких пользователей можно создать политику с ограниченным доступом к ресурсам компании, потому что их устройства могут быть без средств защиты.

# №3 – Защита от сетевых атак

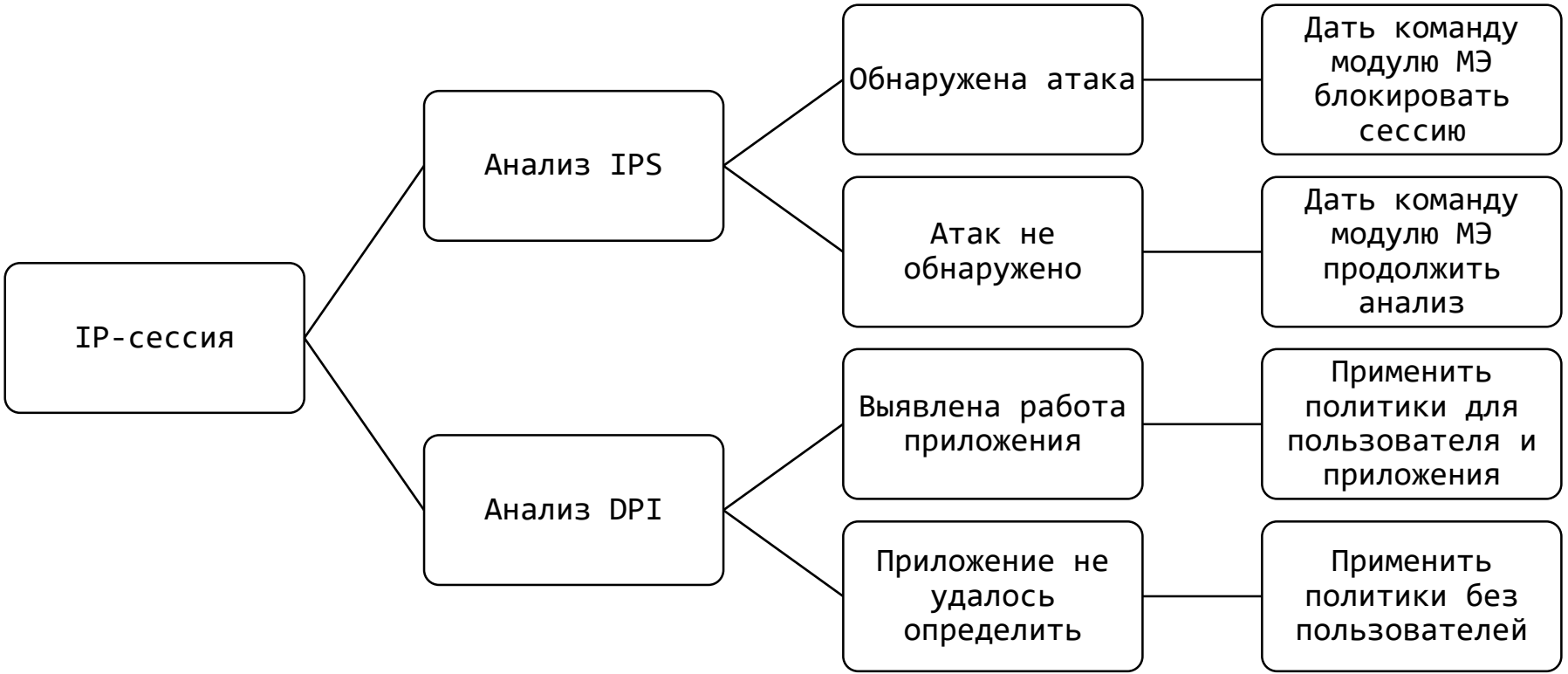
# Система предотвращения вторжений



# Порядок применения правил IPS



# №5 – Защита от вирусов

# Поддержка песочниц

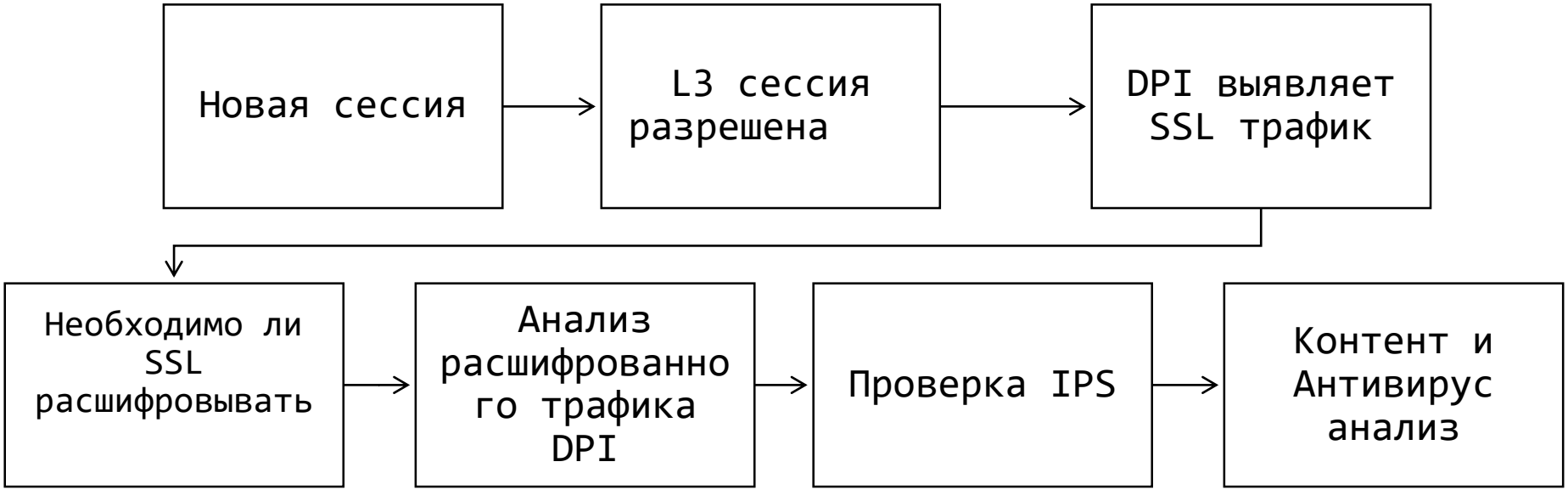
- Тестировался сценарий проверки на содержание вредоносного контента файлов, загружаемых из сети Интернет в «песочницу» ATHENA через службу прокси-сервера xFirewall по протоколу ICAP.
- Межсетевой экран ViPNet xFirewall служит шлюзом между приложениями, функционирующими на узлах локальной сети, и внешними 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.

# №6 – Что делать с SSL

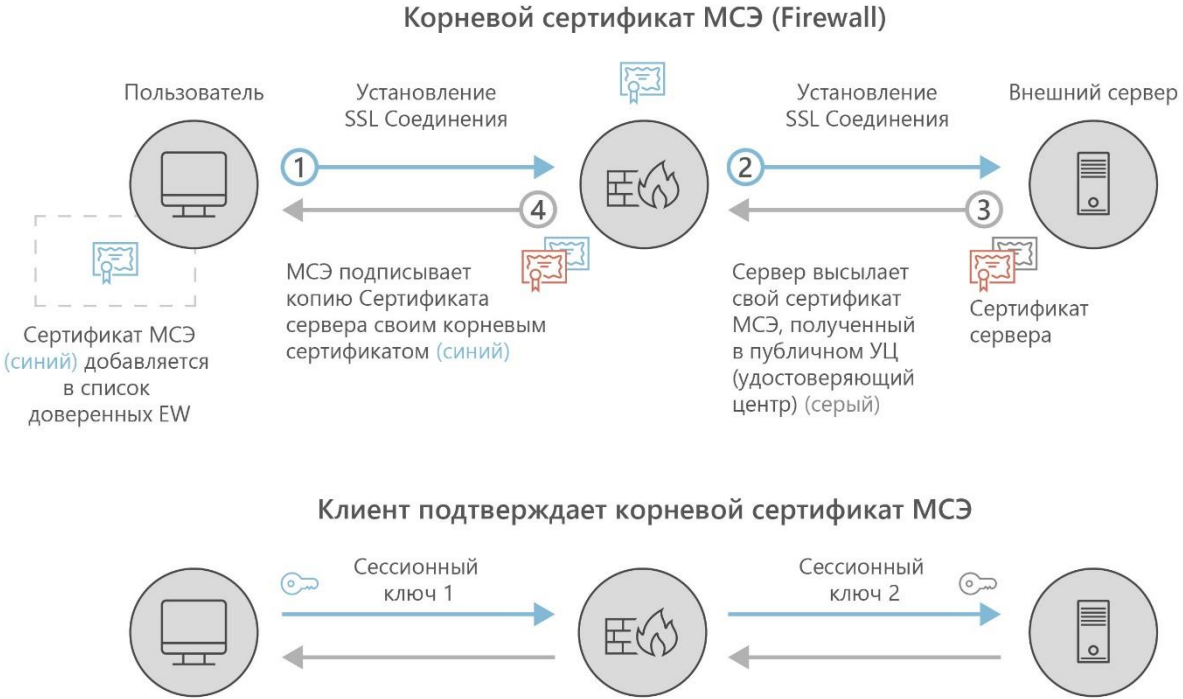
# Классификация SSL

- 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

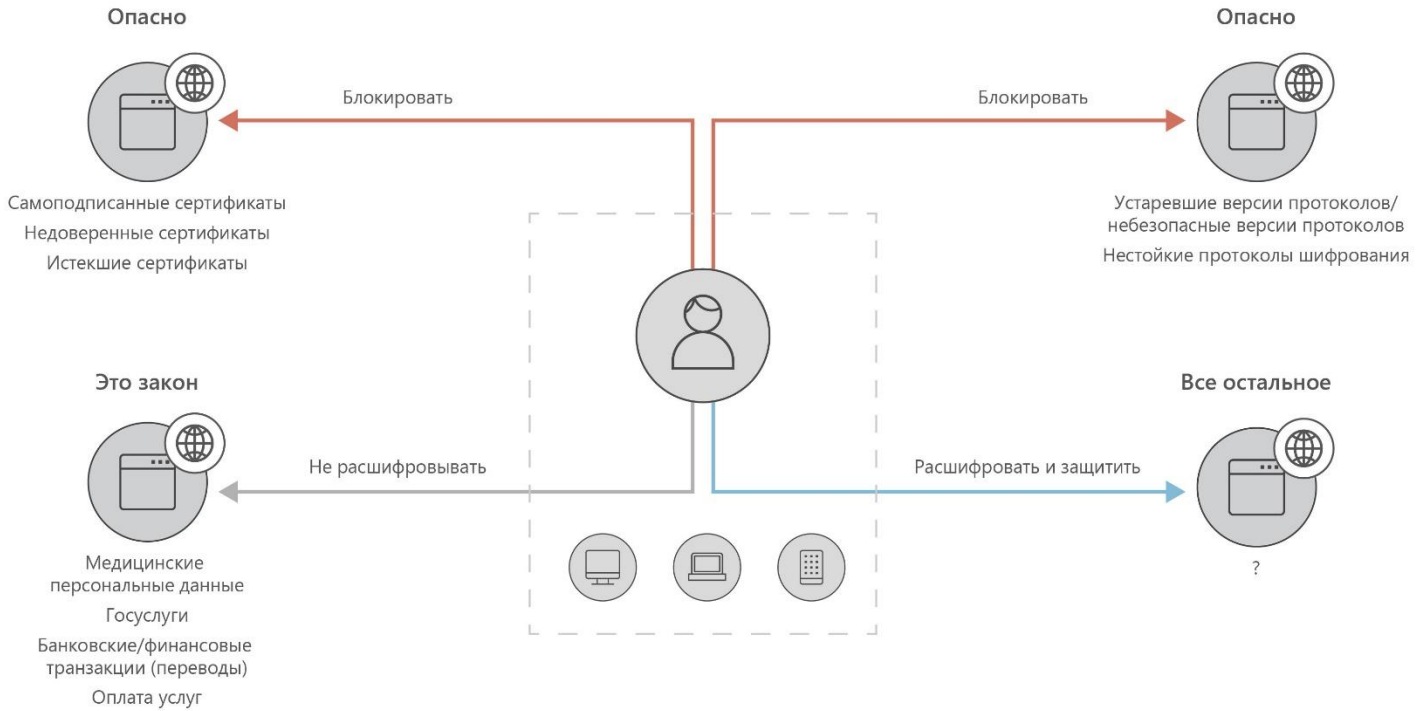
# Схема проверки трафика



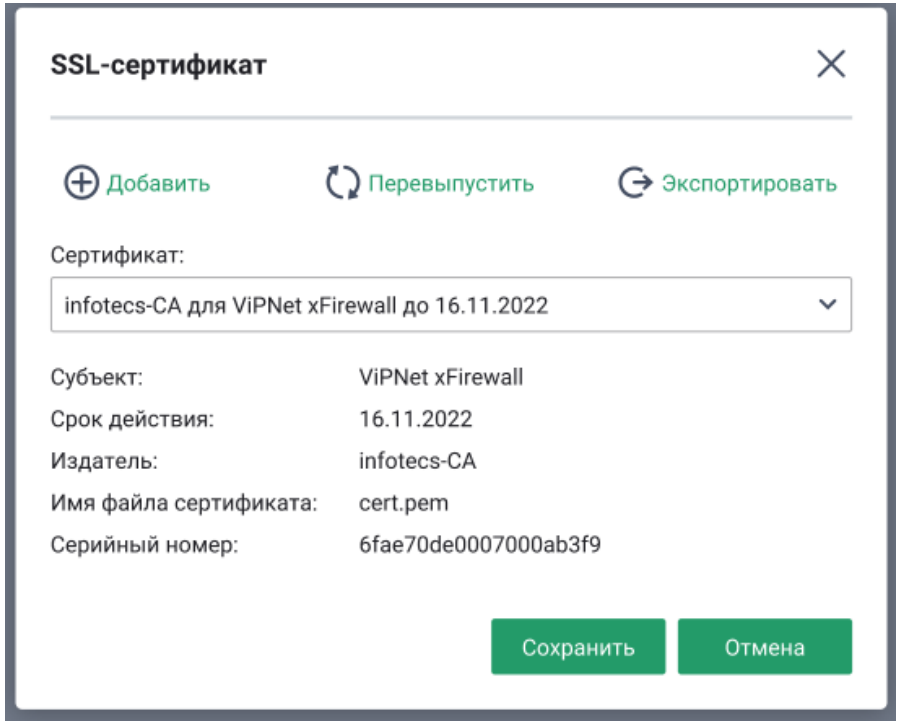
# Forward proxy decryption

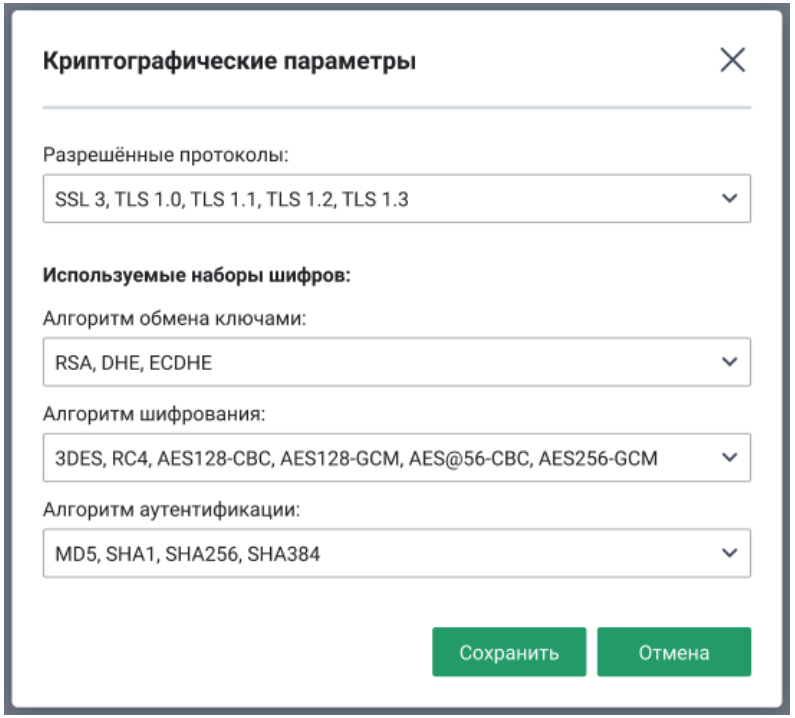


# Лучшие практики SSL Inspection

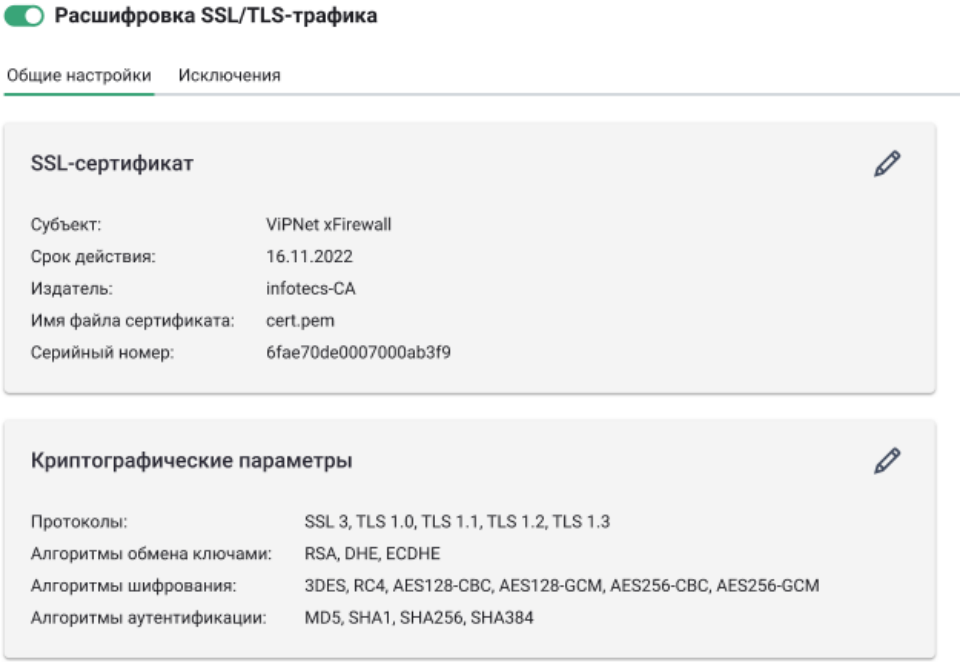


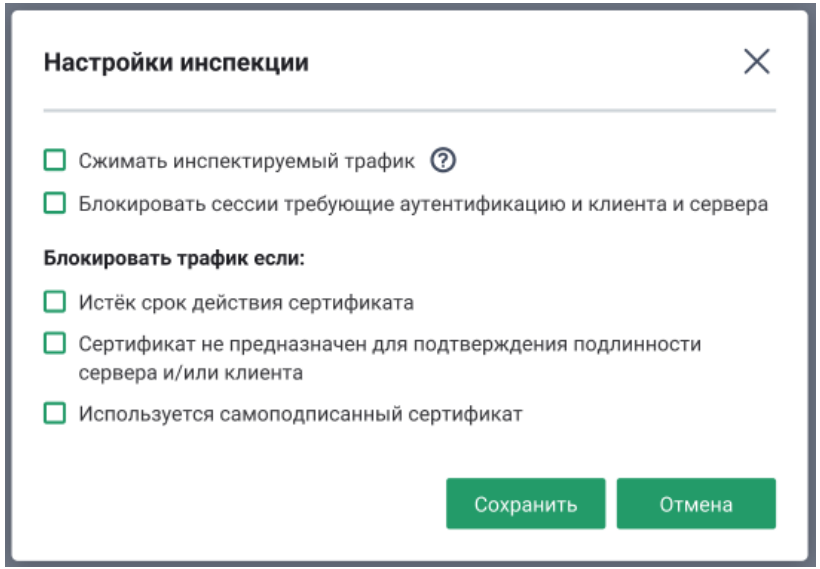
# SSL Inspection



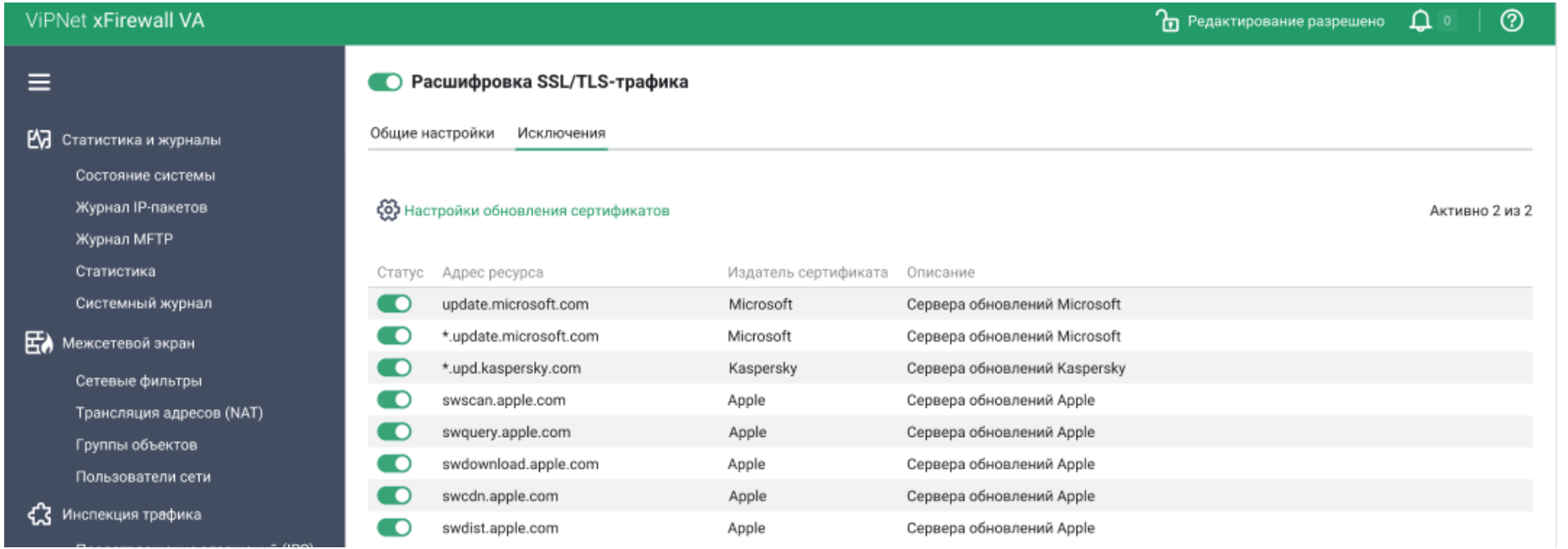



# SSL Inspection

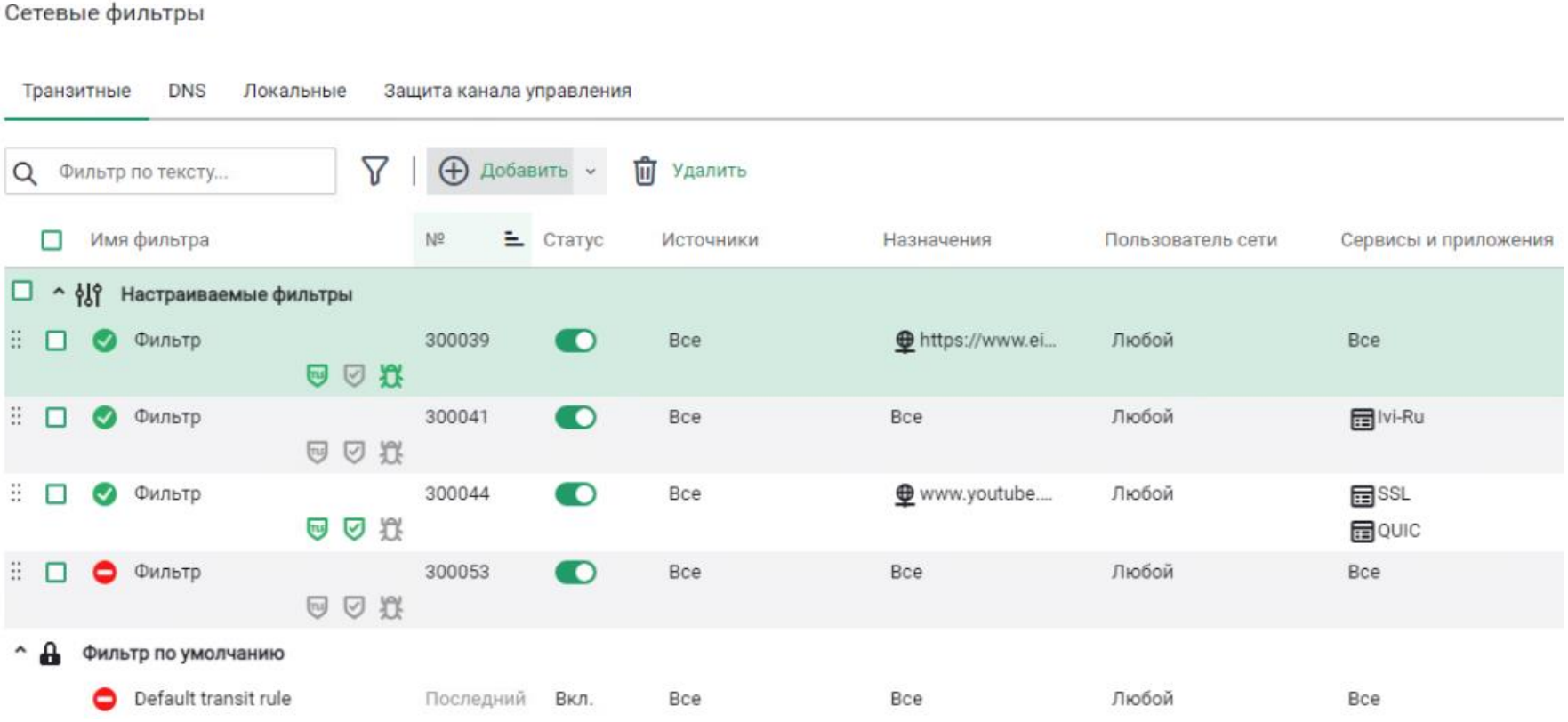


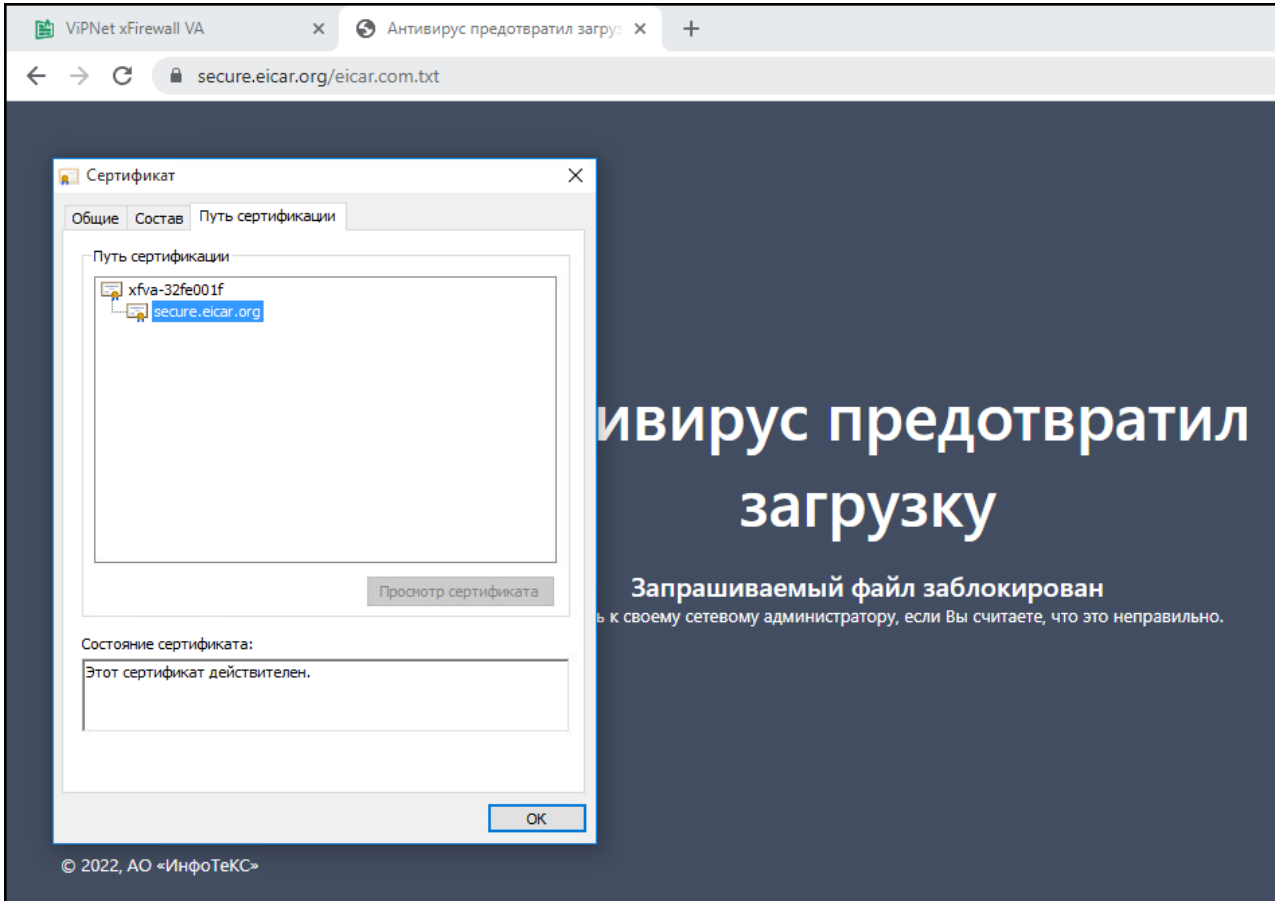
# Исключения были и будут



# Создаем правило инспекции



# 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»

# Производительность SSL Inspection

| Исполнение | AppControl (DPI), Mbps | AppControl + IPS, Mbps | AppControl +SSL | AppControl+ IPS+SSL, Mbps |
|---|---|---|---|---|
| xF1000 C/D | 1 482 | 983 | 829 | 260 |
| xF5000 | 9 100 | 4 170 | 1 373 | 615 |

Оценка производительности инспекции SSL/TLS соединений осуществляется методом измерения показателей передачи HTTPS-трафика через объект тестирования. Измерение производительности может проводиться на фоне передачи вредоносного трафика, который должен отфильтровываться контентными фильтрами и антивирусной проверкой.

# №7 – 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

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow