

ViPNet xFirewall 5.6.0: НОВЫЕ ВОЗМОЖНОСТИ ШЛЮЗА БЕЗОПАСНОСТИ

Алексей Данилов
Руководитель направления
Отдел развития продуктов ИнфоТекС



Next-generation Firewall

Next-Generation Firewall (NGFW)

Gartner®

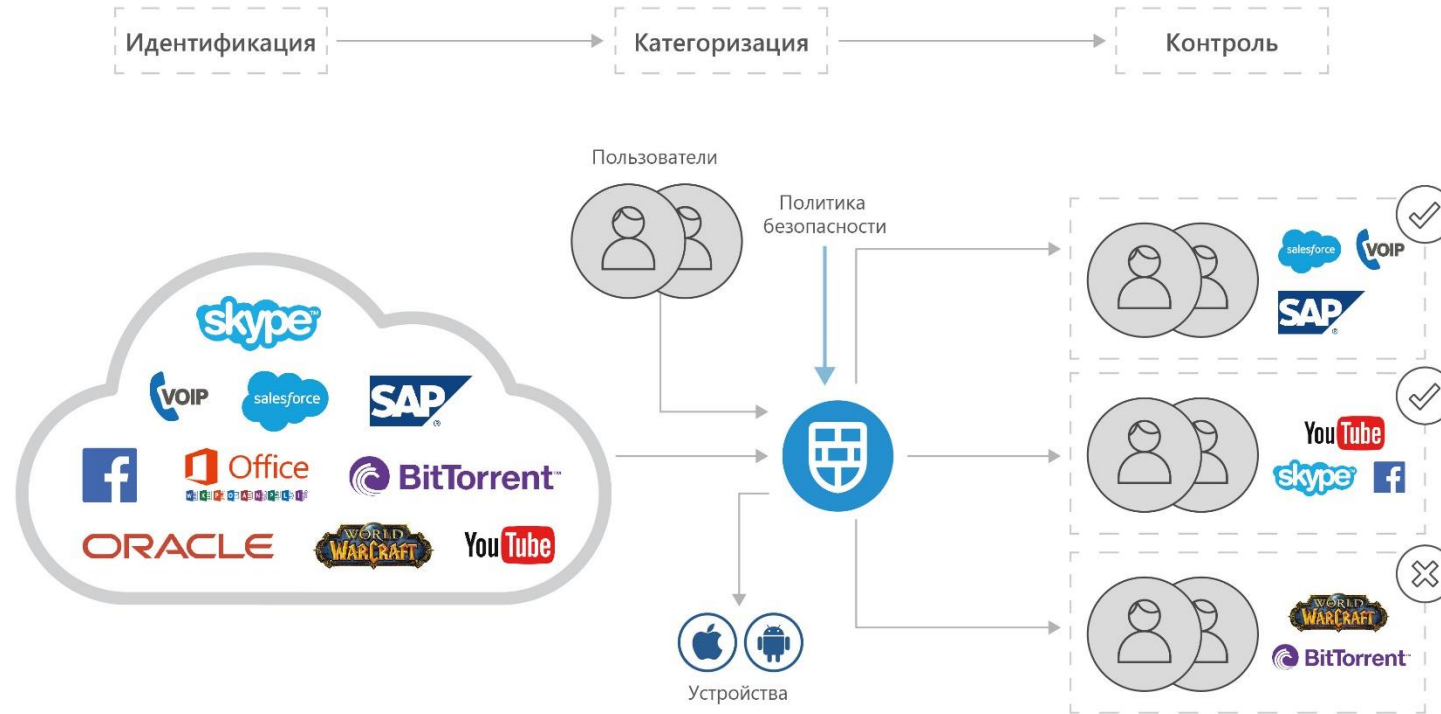


- Общепринято МЭ считать устройства, реализующие технологию stateful packet inspection (SPI) сетевого трафика. МЭ разграничивает доступ на основе 5 параметров: адреса отправителя и получателя, порты отправителя и получателя, протокол L4.

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

Шлюзы безопасности

FW/VPN

NGFW

IDS

Coordinator
for
Win/Linux

Coordinator
KB

HW 4
поколения

xFirewall

IDS NS

Что такое ViPNet xFirewall

Сетевая
платформа в
составе:

Межсетевой
экран

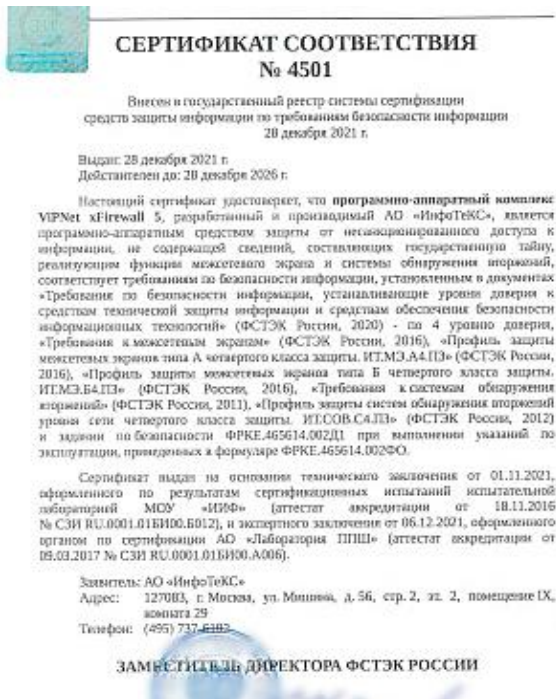
Сетевой экран
приложений -
DPI

Система
предотвращения
вторжений

Шлюзовой
антивирус

Интеграция с
Active Directory

Сертификат ФСТЭК

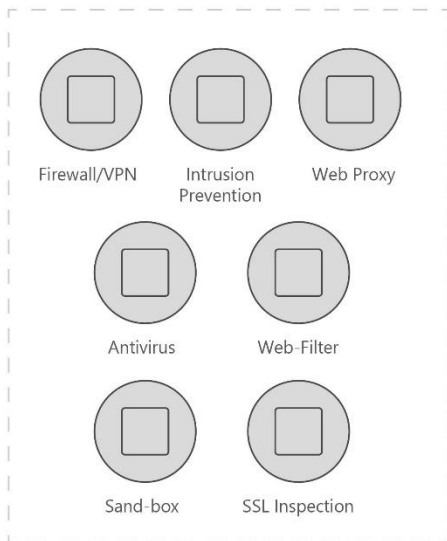


- Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020)» - по 4 уровню доверия
- «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых 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)

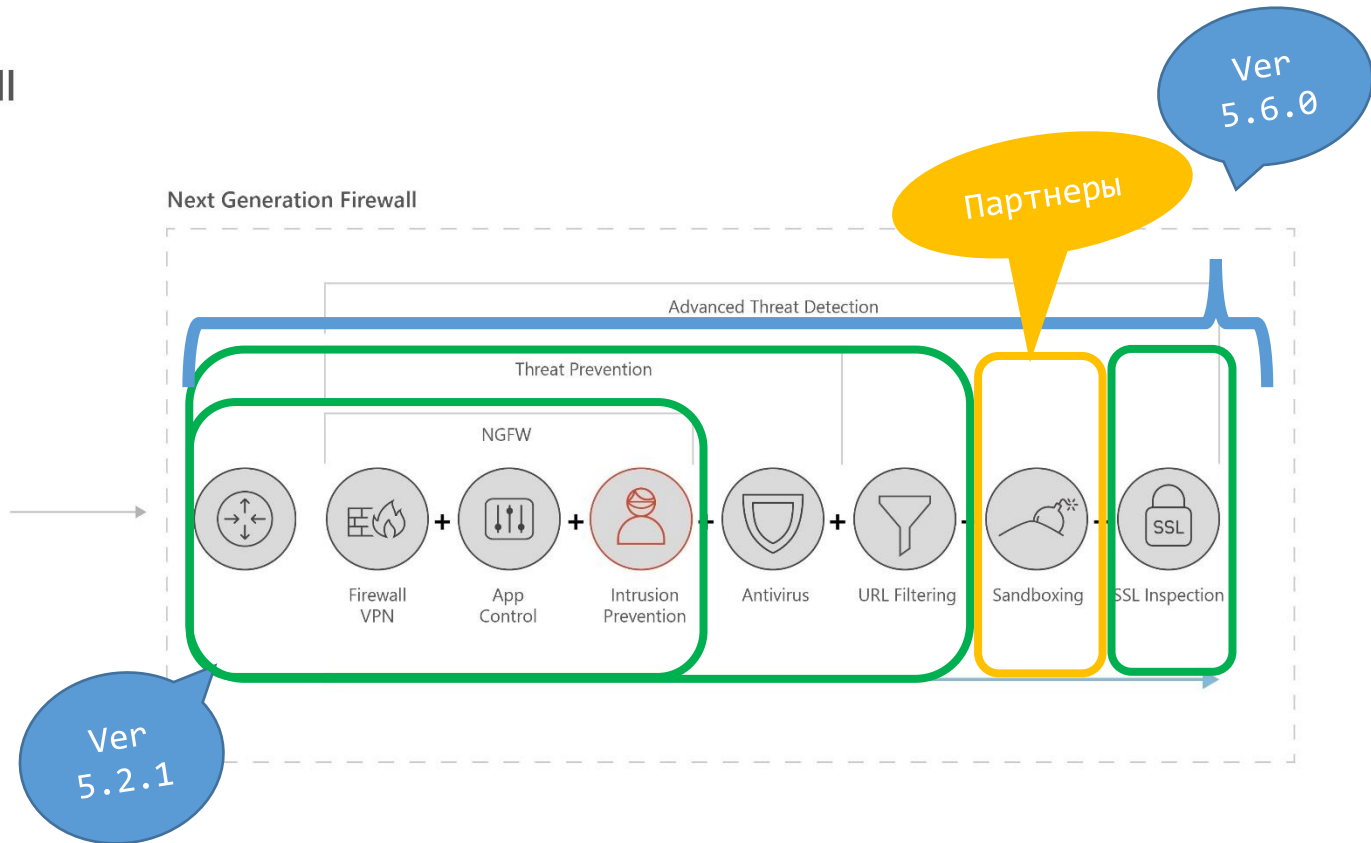
ViPNet xFirewall 5.6.0

Next Generation Firewall

Standalone



Next Generation Firewall



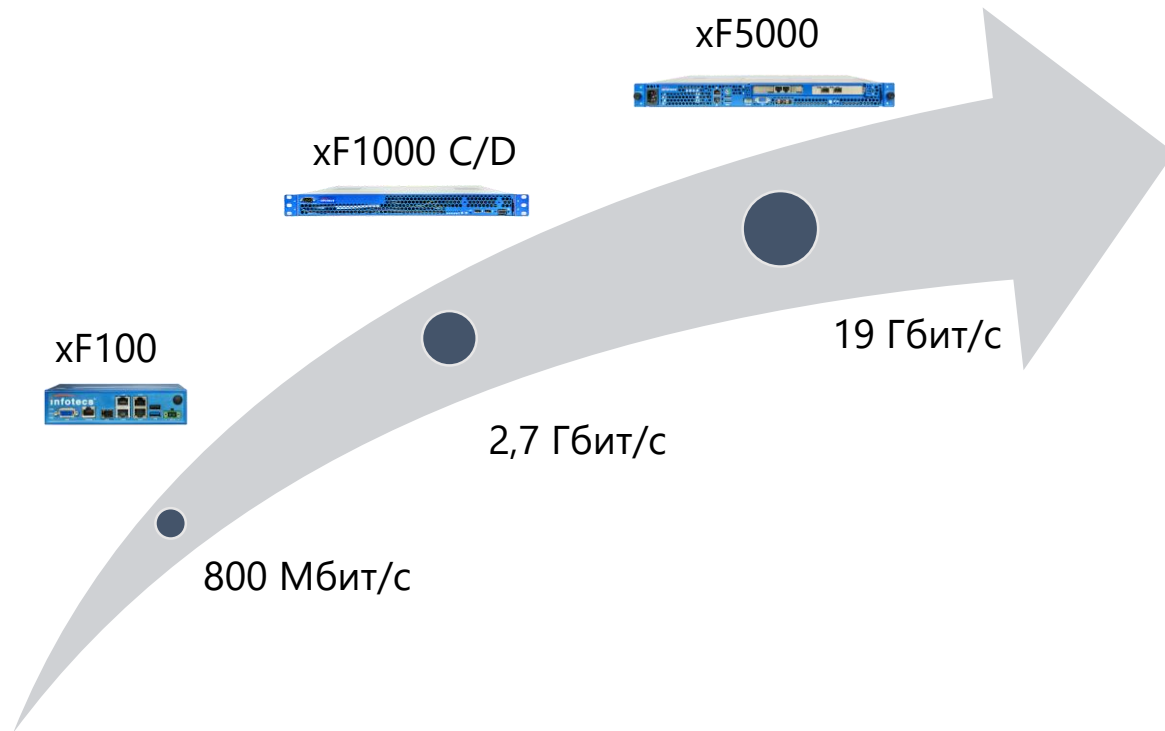
Что нового в 5 поколении продукта

- 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

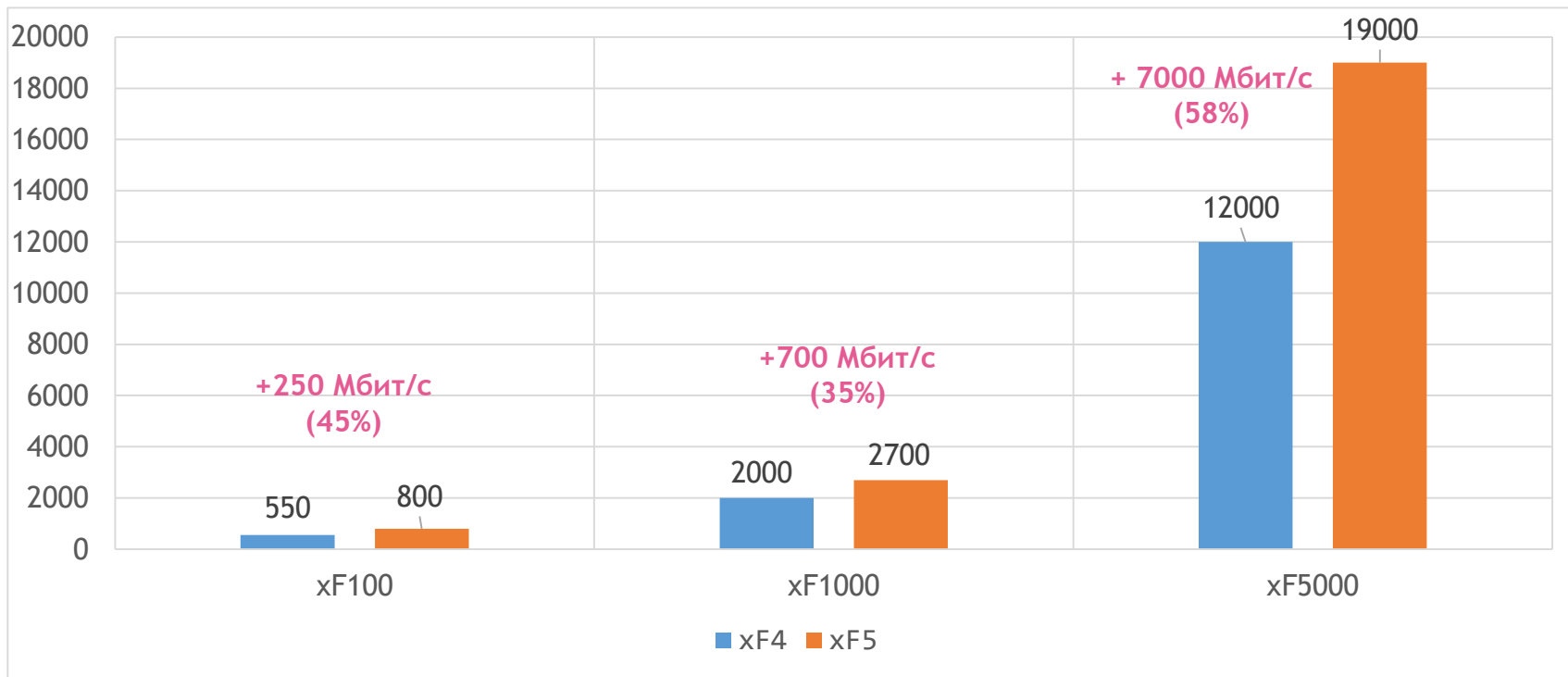
Что нового в 5 поколении продукта

- 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 TOPP
- SSL Inspection

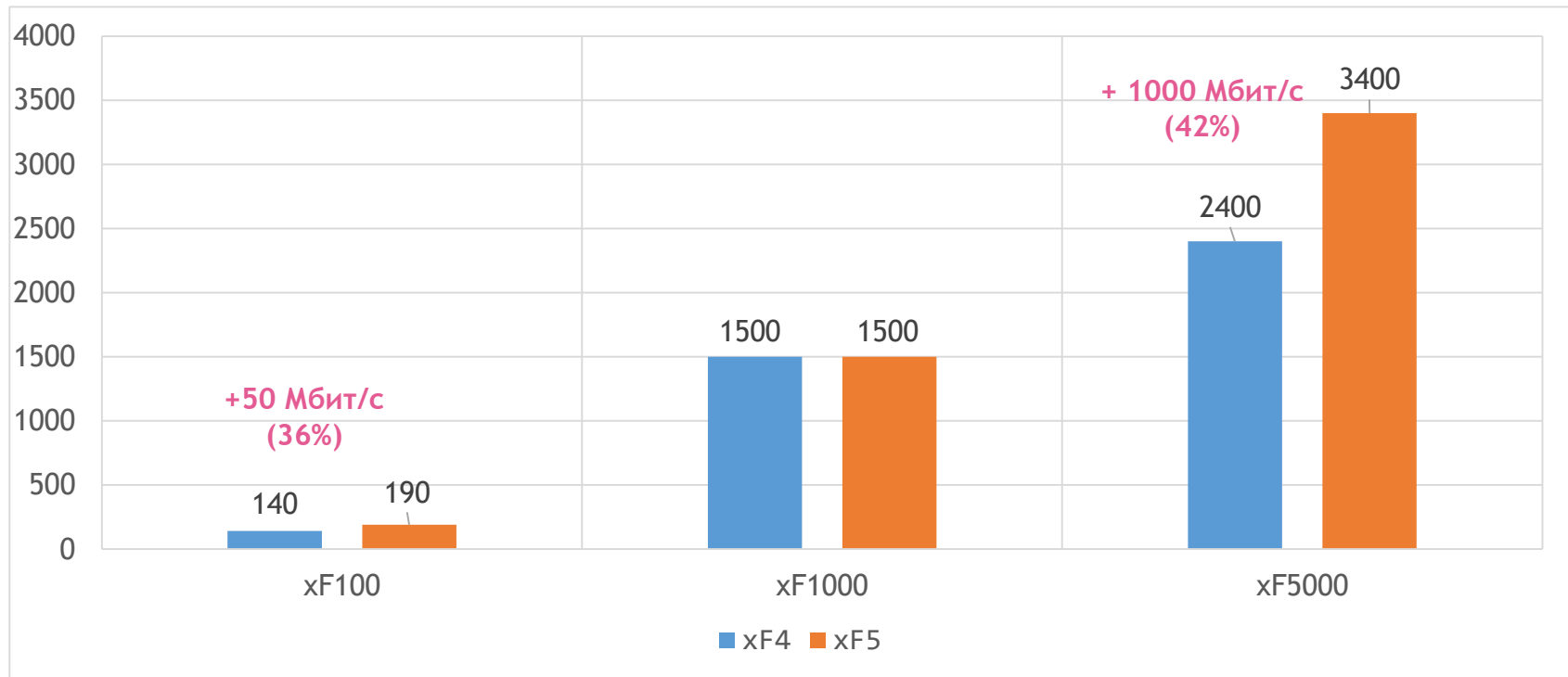
VIPNet xFirewall. Платформы



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.

$3,4 \text{ Gb} / 6000 \text{ users} = 0,56 \text{ Mbps/user}$

Знать что охранять



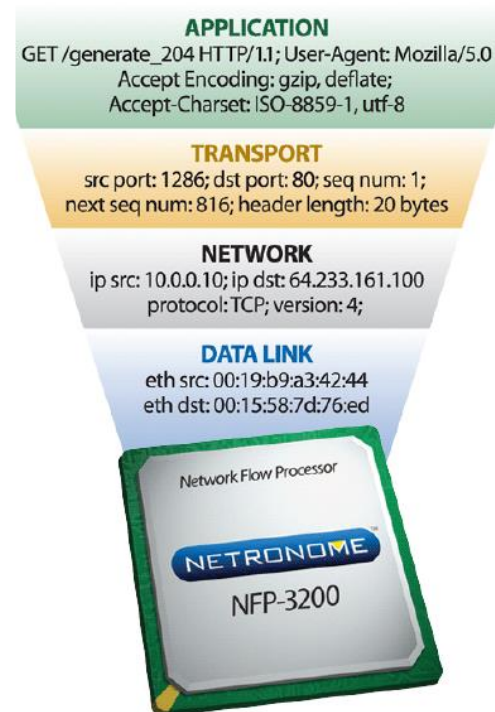
- Открыл порты 80/443 == Открыл всё!

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	192.168.12.202	192.168.12.57	STUN	86	Binding Request
2	0.000000			STUN	86	Binding Request
3	0.954681			STUN	86	Binding Request
4	0.954681			STUN	86	Binding Request
5	1.557299			STUN	86	Binding Request
6	1.557299			STUN	86	Binding Request
7	2.234766			STUN	86	Binding Request
8	2.234766			STUN	86	Binding Request
9	2.596225			STUN	86	Binding Request
10	2.596225			STUN	86	Binding Request
11	2.602773			STUN	86	Binding Success Response
12	2.602773			STUN	86	Binding Success Response
13	2.610574			UDP	89	57492 → 40691 Len=47
14	2.610574			UDP	89	57492 → 40691 Len=47
15	2.624611			STUN	86	Binding Request
16	2.624611			STUN	86	Binding Request
17	2.627427			STUN	86	Binding Success Response
18	2.627427			STUN	86	Binding Success Response
19	2.630845			UDP	991	57492 → 40691 Len=949
20	2.630845			UDP	991	57492 → 40691 Len=949
21	2.630914			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: [MAC], Dst: [MAC]
▶ Internet Protocol Version 4, Src: [IP], Dst: [IP]
▶ User Datagram Protocol, Src Port: 40691, Dst Port: 57492
▶ Session Traversal Utilities for NAT

Более 5000 приложений/протоколов

Top Ranking		Top Gainers	
Bejeweled Blitz	1	Hidden Runaway	139 ▲ 262
Hanging With Friends	2 ▲ 1	Tom Clancy's Splinter Cell	228 ▲ 141
SCRABBLE Free	3 ▼ 1	Minecraft Companion	267 ▲ 4
Jewels of the Amazon	4	Police Chase Smash	145
James Cameron & #039; Avatar	5 ▲ 1	G.U.N.	111 ▲
Police Chase Smash	6 ▲ 2	Wordfeud	65 ▲ 99
Police Chase (FREE)	7 ▲ 5	Hidden Expedition	329 ▲ 72
Amazon™: Hidden Expeditions	8 ▲ 8	Minecraft Help	293 ▲ 71
Police Chase Car Rally	9 ▲ 2	Crimson: Steam Pirates	277 ▲ 68
Diamond Dash	10 ▼ 3	The ROBLOX Quiz	142 ▲ 64
Agent Dash	11 ▼ 2	Justin Bieber/Nicki Minaj	220 ▲ 60
Motorcycle Bike Rally	12 ▲ 3	I Dig It Expedition	132 ▲ 56
iGun Pro™ LITE - T	13 ▼ 3	Solitaire	194 ▲ 56
Air Patriots	14 ▼ 9	Choo Choo Steam Train	143 ▲ 53
Goaaal!™ Soccer Tactics	15 ▼ 2	Solitaire	258 ▲ 53

65 из категории «Социальные сети»

183 – потоковое видеовещание

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



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

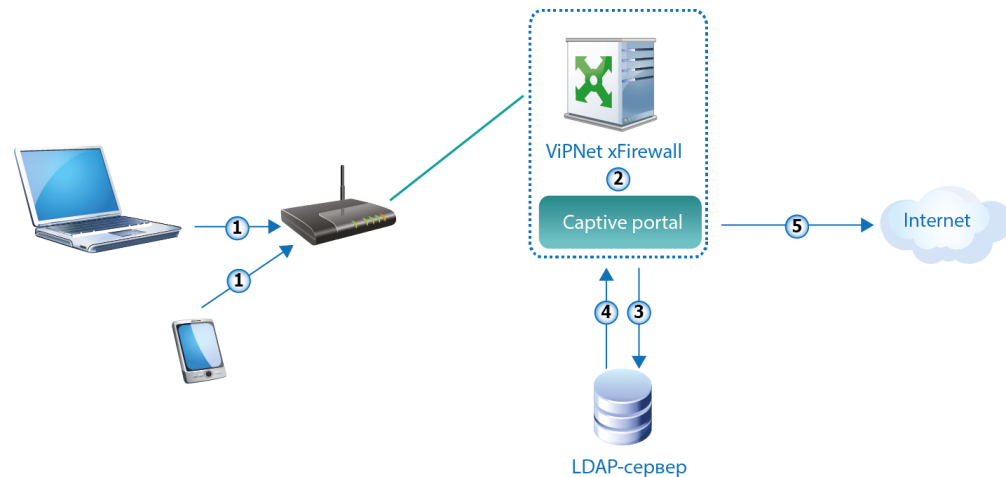


BYOD – принеси свое устройство и работай



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.



Система предотвращения вторжений

- Статистика и журналы ^
- Состояние системы
- Статистика
- Межсетевой экран ^
- Сетевые фильтры
- NAT
- Группы объектов
- Прокси-сервер
- Пользователи сети
- Предотвращение вторжений
- Сетевые настройки ^

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 ^

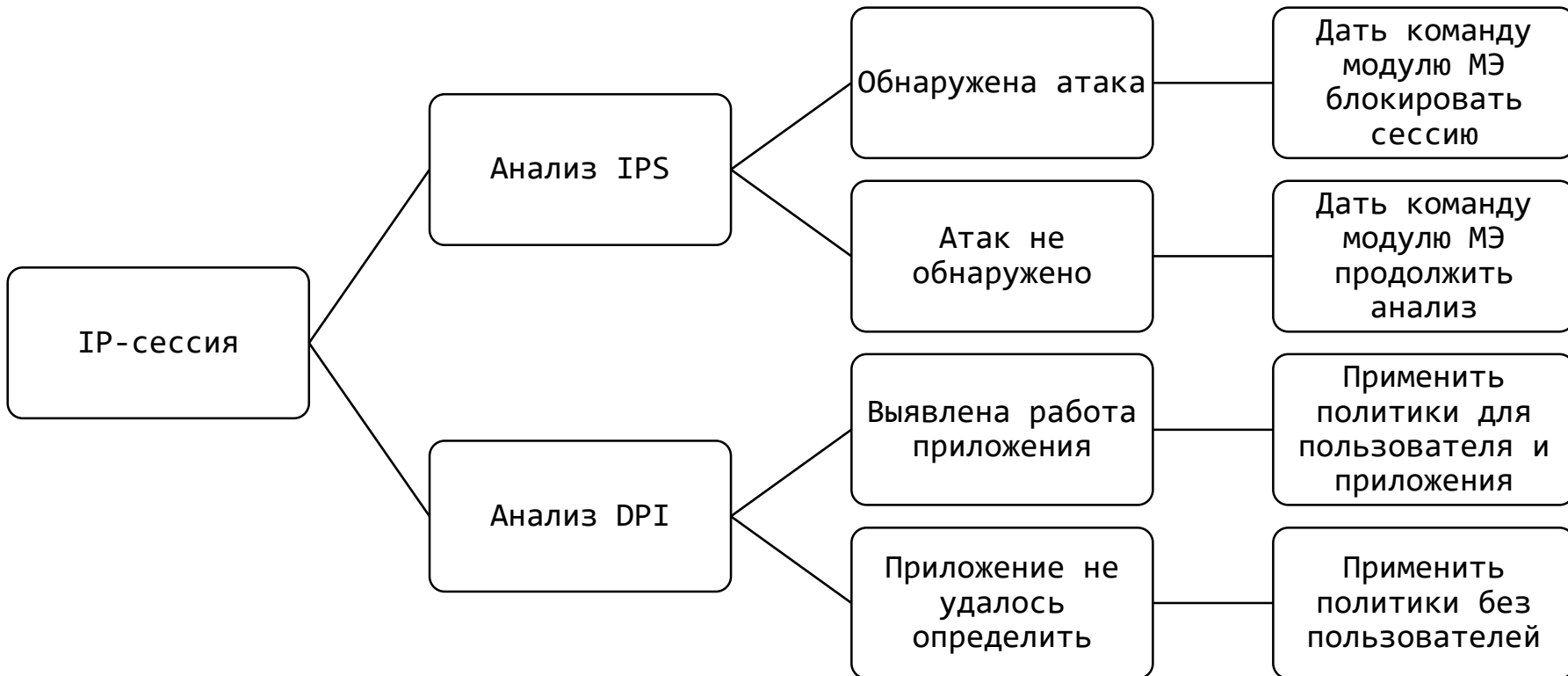
Признаки IP-пакетов

Пользователь сети:	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



№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

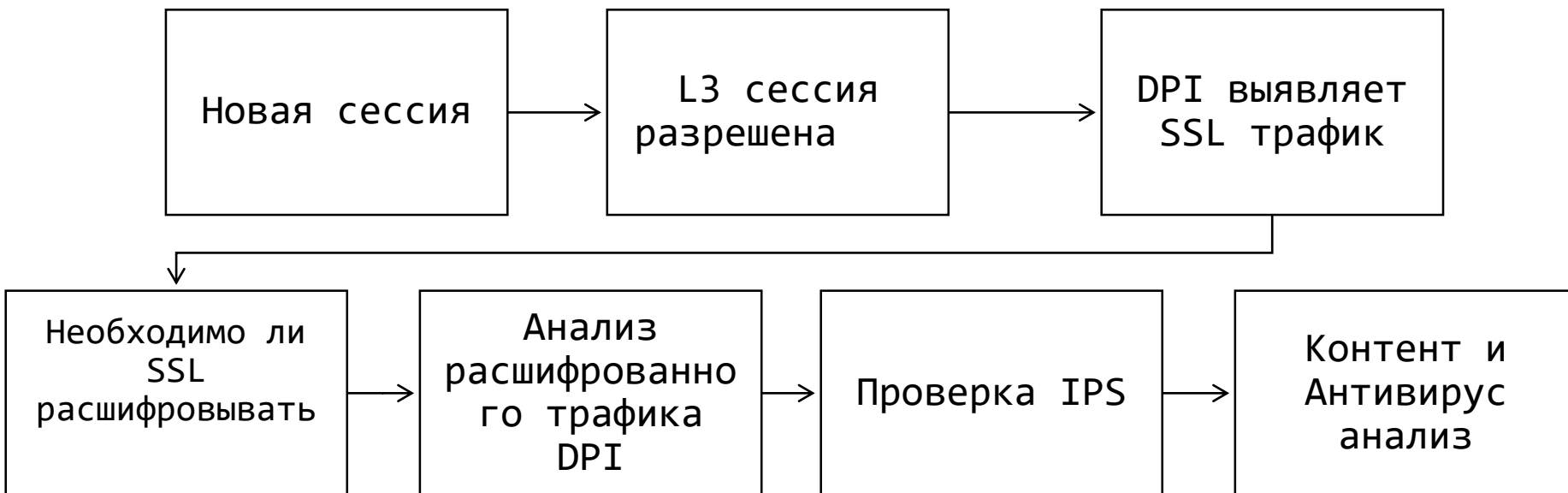


Классификация SSL



- 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

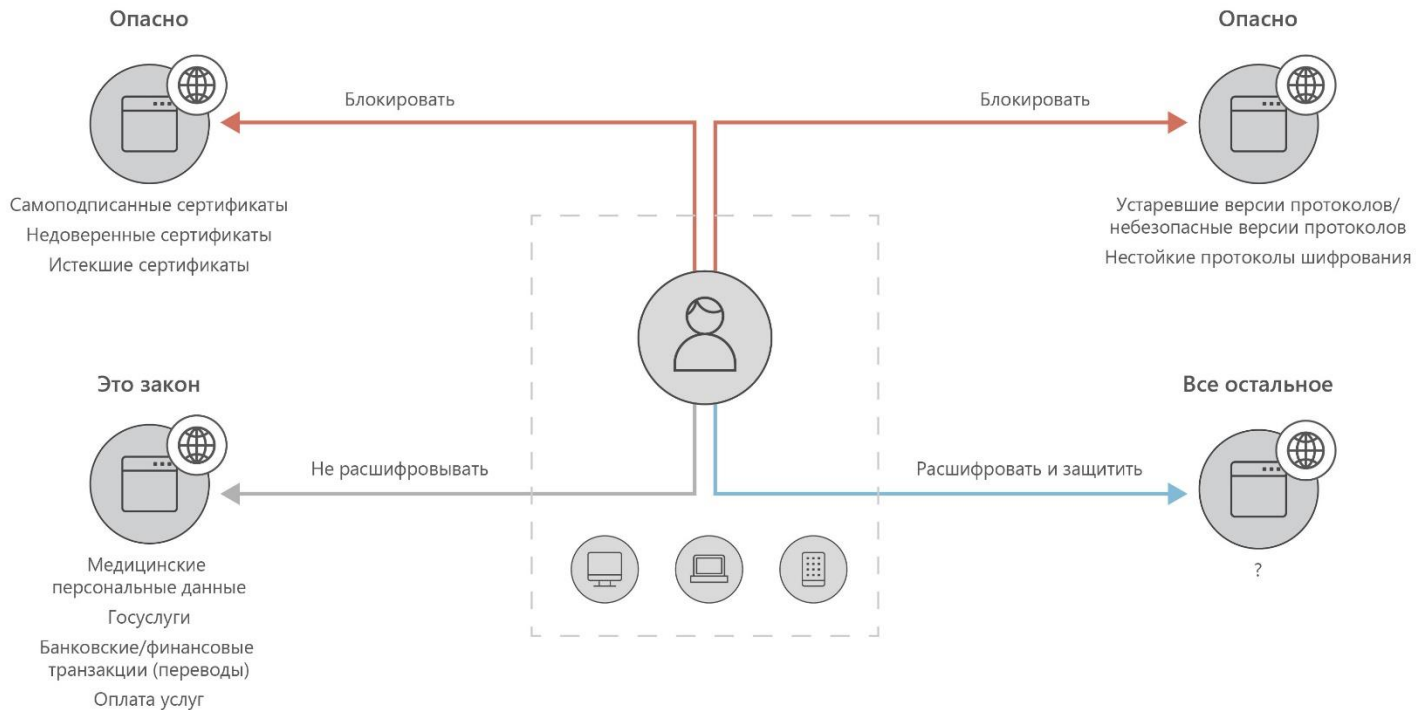
Корневой сертификат МСЭ (Firewall)



Клиент подтверждает корневой сертификат МСЭ



Лучшие практики SSL Inspection



SSL Inspection

SSL-сертификат ✕

⊕ Добавить 🔄 Перевыпустить 📤 Экспортировать

Сертификат:

Субъект:	ViPNet xFirewall
Срок действия:	16.11.2022
Издатель:	infotecs-CA
Имя файла сертификата:	cert.pem
Серийный номер:	6fae70de0007000ab3f9

Сохранить Отмена

Криптографические параметры ✕

Разрешённые протоколы:

Используемые наборы шифров:

Алгоритм обмена ключами:

Алгоритм шифрования:

Алгоритм аутентификации:

Сохранить Отмена

SSL Inspection

Расшифровка SSL/TLS-трафика

Общие настройки Исключения


SSL-сертификат

Субъект: VIPNet xFirewall
Срок действия: 16.11.2022
Издатель: infotecs-CA
Имя файла сертификата: cert.pem
Серийный номер: 6fae70de0007000ab3f9

Криптографические параметры

Протоколы: SSL 3, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3
Алгоритмы обмена ключами: RSA, DHE, ECDHE
Алгоритмы шифрования: 3DES, RC4, AES128-CBC, AES128-GCM, AES256-CBC, AES256-GCM
Алгоритмы аутентификации: MD5, SHA1, SHA256, SHA384

Настройки инспекции

- Сжимать inspected трафик 
- Блокировать сессии требующие аутентификацию и клиента и сервера

Блокировать трафик если:

- Истёк срок действия сертификата
- Сертификат не предназначен для подтверждения подлинности сервера и/или клиента
- Используется самоподписанный сертификат

Сохранить

Отмена

Исключения были и будут

VIPNet xFirewall VA 🔒 Редактирование разрешено 0 | ?

☰

📊 Статистика и журналы

- Состояние системы
- Журнал IP-пакетов
- Журнал MFTP
- Статистика
- Системный журнал

🔗 Межсетевой экран

- Сетевые фильтры
- Трансляция адресов (NAT)
- Группы объектов
- Пользователи сети

⚙️ Инспекция трафика

🔴 Расшифровка SSL/TLS-трафика

Общие настройки | Исключения

⚙️ Настройки обновления сертификатов Активно 2 из 2

Статус	Адрес ресурса	Издатель сертификата	Описание
🔴	update.microsoft.com	Microsoft	Сервера обновлений Microsoft
🔴	*.update.microsoft.com	Microsoft	Сервера обновлений Microsoft
🔴	*.upd.kaspersky.com	Kaspersky	Сервера обновлений Kaspersky
🔴	swscan.apple.com	Apple	Сервера обновлений Apple
🔴	swquery.apple.com	Apple	Сервера обновлений Apple
🔴	swdownload.apple.com	Apple	Сервера обновлений Apple
🔴	swcdn.apple.com	Apple	Сервера обновлений Apple
🔴	swdist.apple.com	Apple	Сервера обновлений Apple

Создаем правило инспекции

Сетевые фильтры

Транзитные DNS Локальные Защита канала управления

Фильтр по тексту... | | Добавить | Удалить

<input type="checkbox"/>	Имя фильтра	№	Статус	Источники	Назначения	Пользователь сети	Сервисы и приложения
<input type="checkbox"/>	Настраиваемые фильтры						
<input type="checkbox"/>	Фильтр	300039		Все	https://www.ei...	Любой	Все
<input type="checkbox"/>	Фильтр	300041		Все	Все	Любой	Ivi-Ru
<input type="checkbox"/>	Фильтр	300044		Все	www.youtube...	Любой	SSL QUIC
<input type="checkbox"/>	Фильтр	300053		Все	Все	Любой	Все
<input type="checkbox"/>	Фильтр по умолчанию						
<input type="checkbox"/>	Default transit rule	Последний	Вкл.	Все	Все	Любой	Все

Результат

ВиPNет xFirewall VA x Антивирус предотвратил загрузку x +

← → ↻ 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»

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