

VIPNet xFirewall – НОВЫЕ ВОЗМОЖНОСТИ

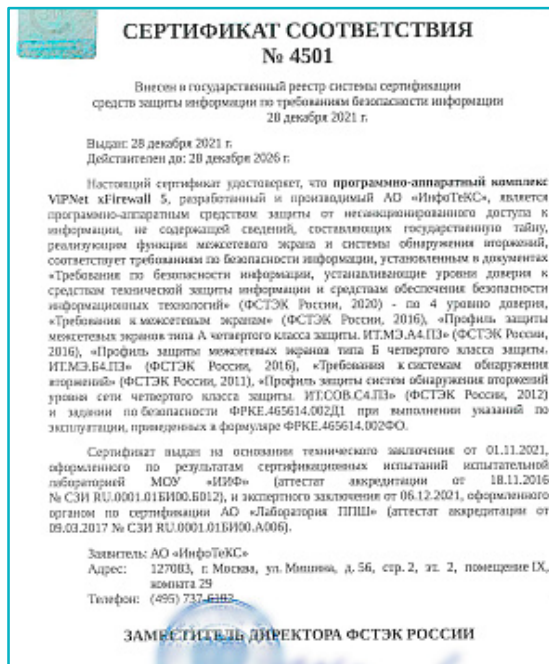


техно infotecs
2024 ФЕСТ
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Алексей Данилов

ViPNet xFirewall

Сертификат 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



1 уровня включительно, в ИС общего пользования II класса 2.3.1 ViPNet xFirewall 5 ... предназначен для использования в государственных информационных системах до класса защищенности K1 включительно, на верхнем уровне (уровне диспетчерского управления) в автоматизированных системах управления производственными и технологическими процессами до класса защищенности K1 включительно, в ИС персональных данных для обеспечения уровня защищенности персональных данных до .

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 K1 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.

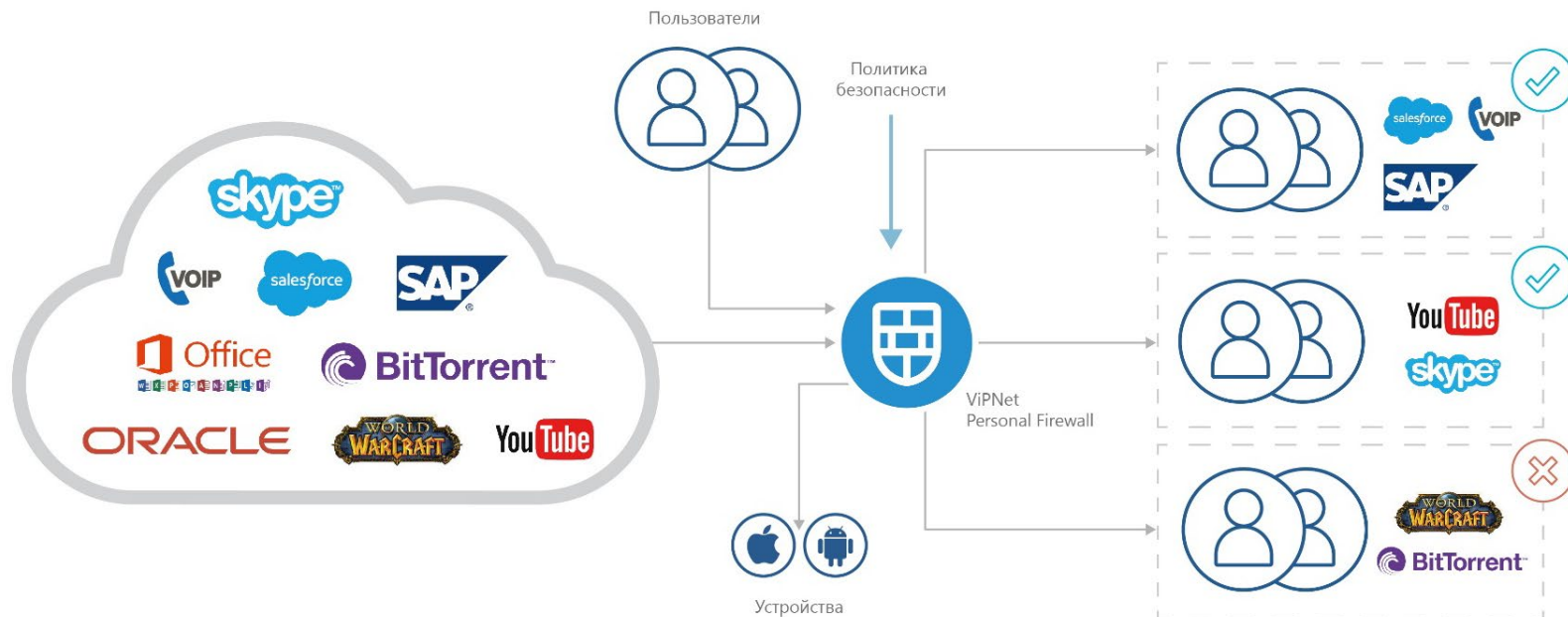


МЭ следующего поколения (NGFW) в дополнении к общепринятому разграничению доступа предоставляет возможности по выявлению и блокировке современных угроз, таких как: вредоносное ПО, атаки уровня приложений. Согласно определению Gartner NGFW должен состоять из:

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

ViPNet xFirewall

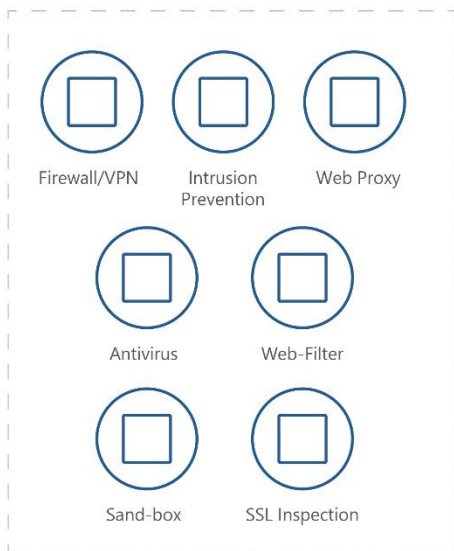
ViPNet xFirewall с первого взгляда



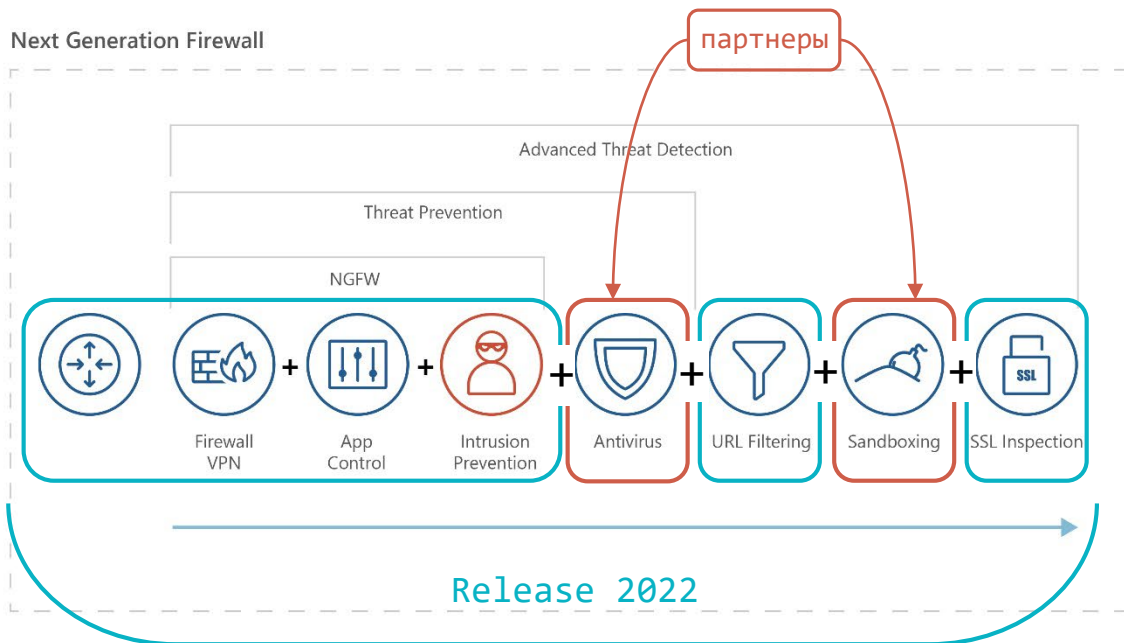
ViPNet xFirewall 2022

Next Generation Firewall

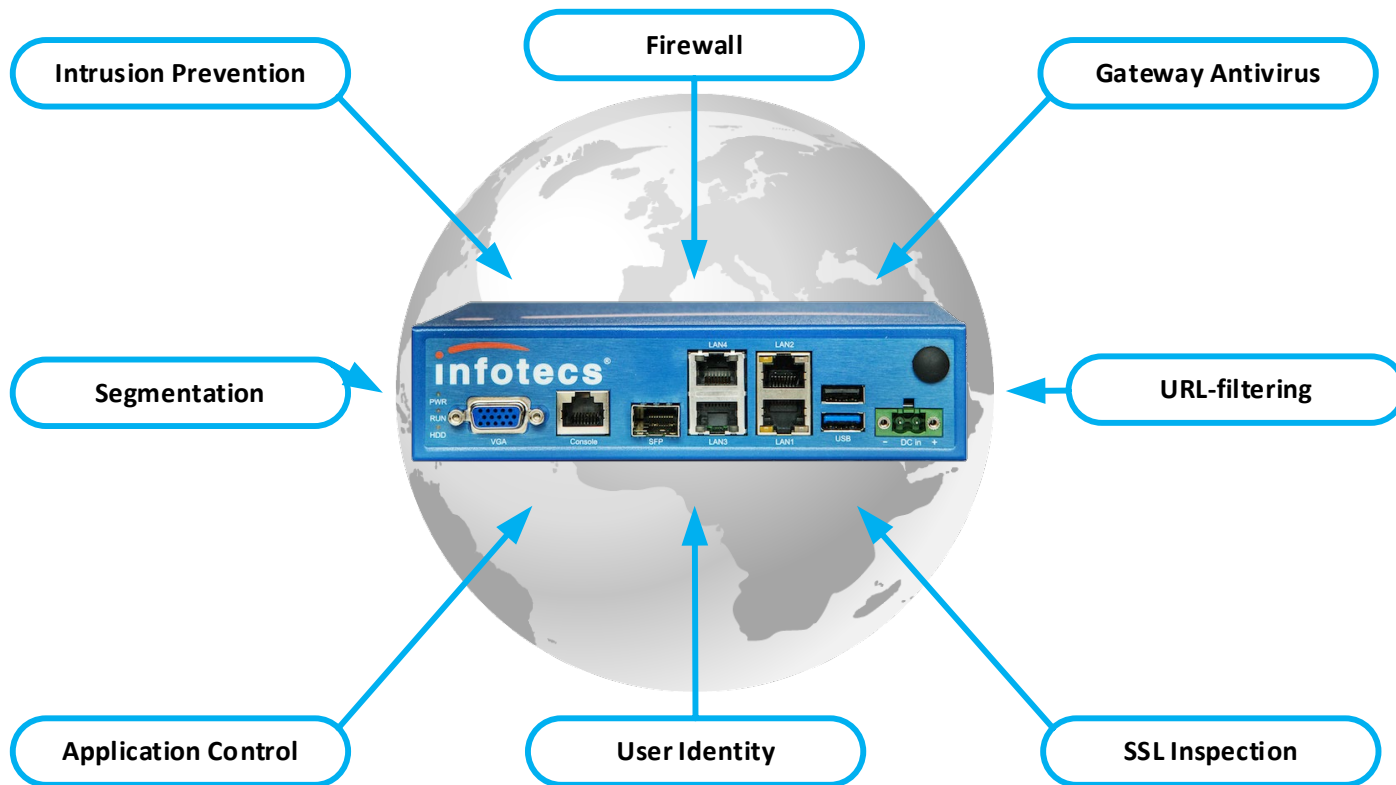
Standalone



Next Generation Firewall

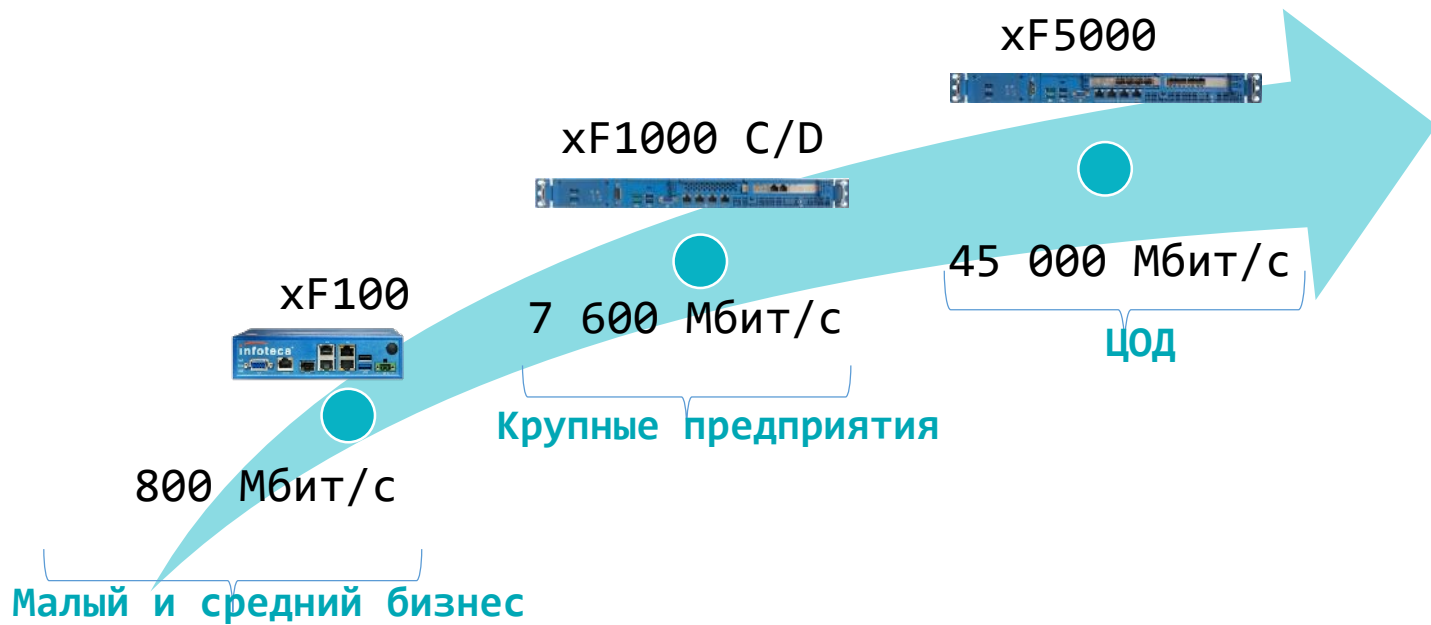


Что такое ViPNet xFirewall



Модельный ряд xFirewall














Тестирование по RFC-2544 UDP 1514 byte





Application Control – контроль приложений

Открыл порты 80/443 =
= Открыл всё!

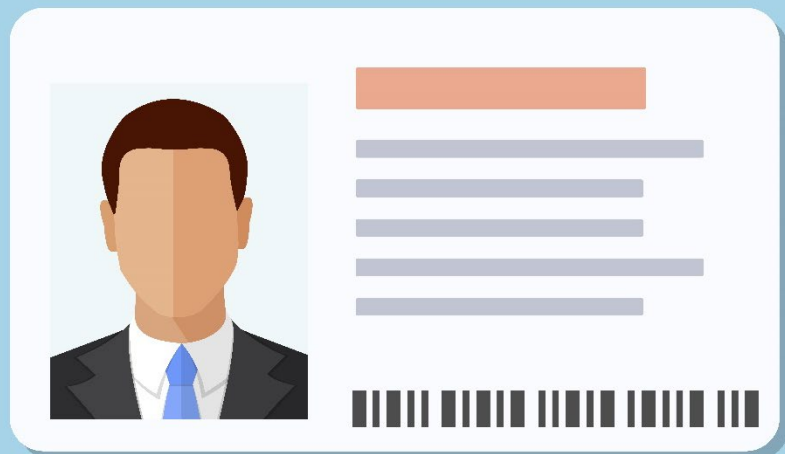
	<p>more.tv – сериалы, фильмы и ТВ Смотреть премьеры онлайн в HD</p>		<p>Книги и аудиокниги MyBook Читать и слушать книги удобно</p>
	<p>Строки: книги, подкасты Читайте и слушайте</p>		<p>Литрес: Книги и аудиокниги Читай и Слушай онлайн</p>
	<p>Prequel: Редактор Фото Обработка, эффекты и фильтры</p>		<p>KION – оригинальный кинотеатр Фильмы и мультфильмы онлайн</p>
	<p>Artforintrovert Саморазвитие с курсами-подкастами</p>		<p>Облако Mail.ru: хранилище фото Облачное хранение: диск и сейф</p>
	<p>LifeWheel цели, трекеры Цель - планы на день, приемы</p>		<p>AppForType: текст на фото Шаблоны для инстаграм сторис</p>
	<p>InStories Reels & Stories Сторис, AI аватары, ИИ</p>		<p>Amiateka – сериалы онлайн Сериалы и фильмы HD</p>
	<p>Google Фото хранение фото и видео</p>		

Более 5000 приложений/протоколов

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 клиентской идентификации



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



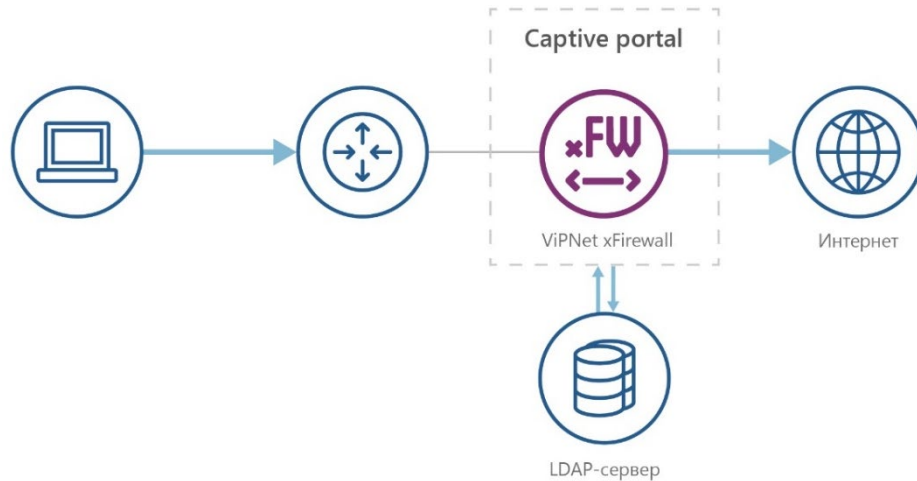
Отсутствует потребность в «привязке» пользователей к ip-адресам



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 YDPCNTL.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 ▾

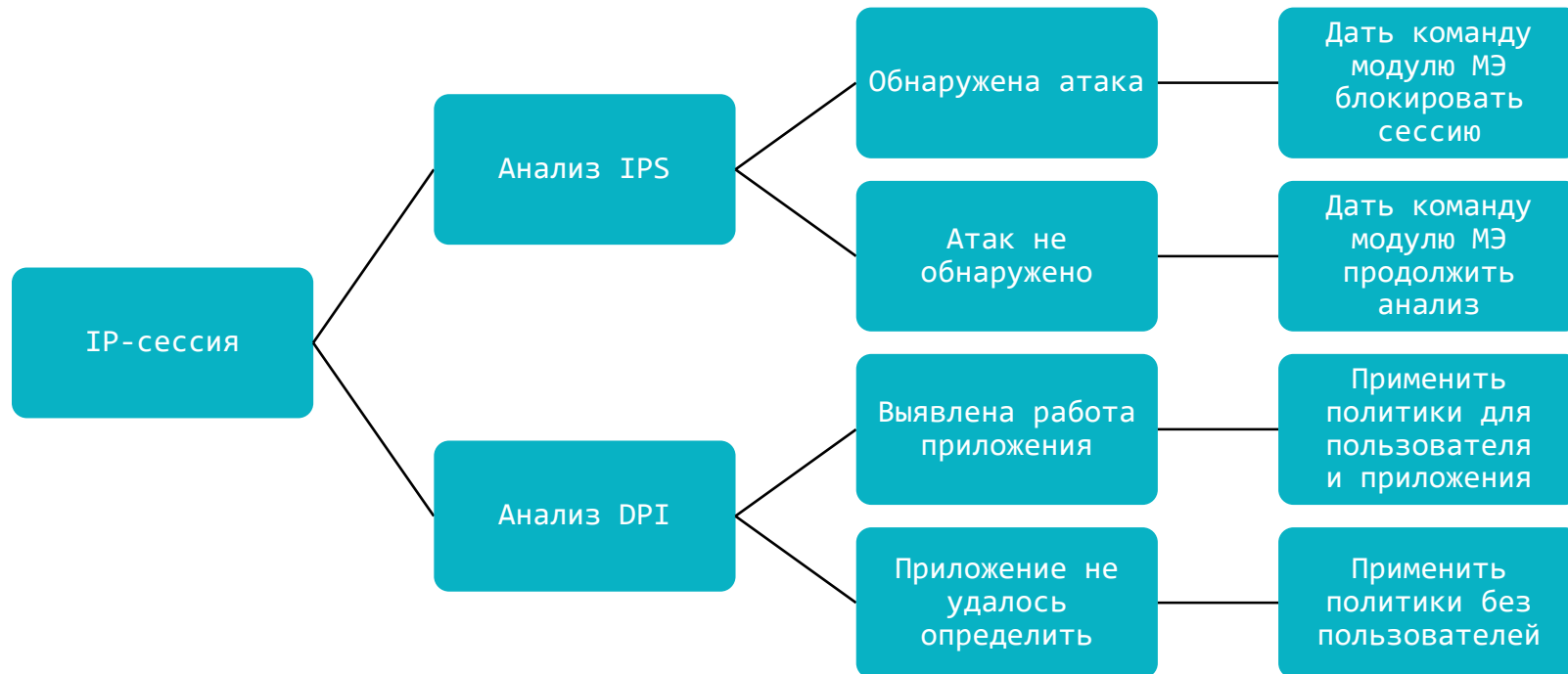
Событие: Блокированные IP-пакеты ▾

Группа правил IPS: Любая ▾

Правило IPS: Любое ▾

Найти **Восстановить значения по умолчанию**

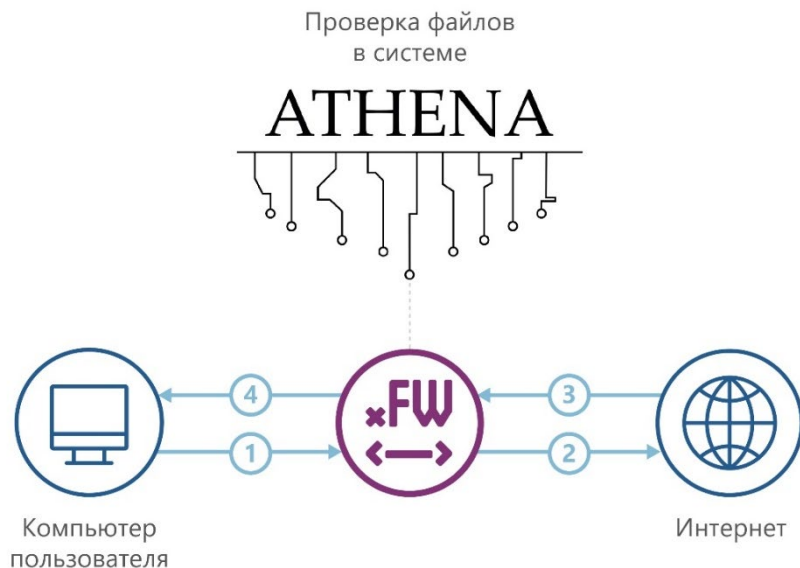
Порядок применения правил IPS





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.

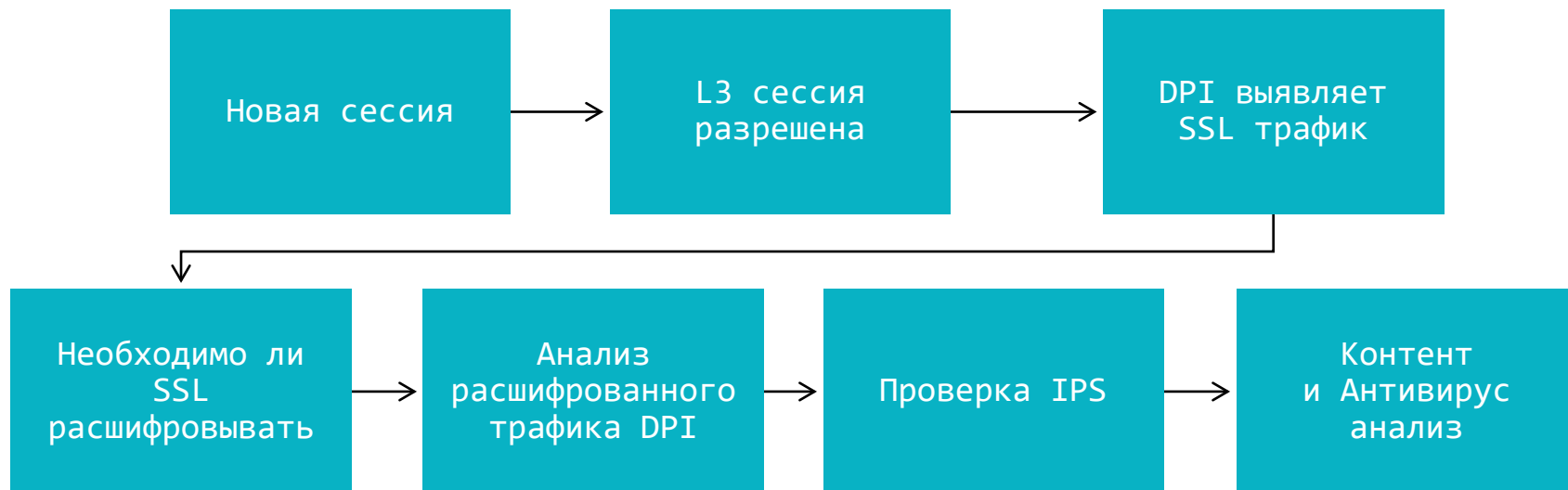


Блокировать известный SSL запрещенных политикой приложений: социальные сети, мессенджеры и тд.



Запретить любой неизвестный SSL-трафик

Схема проверки трафика



Forward proxy decryption

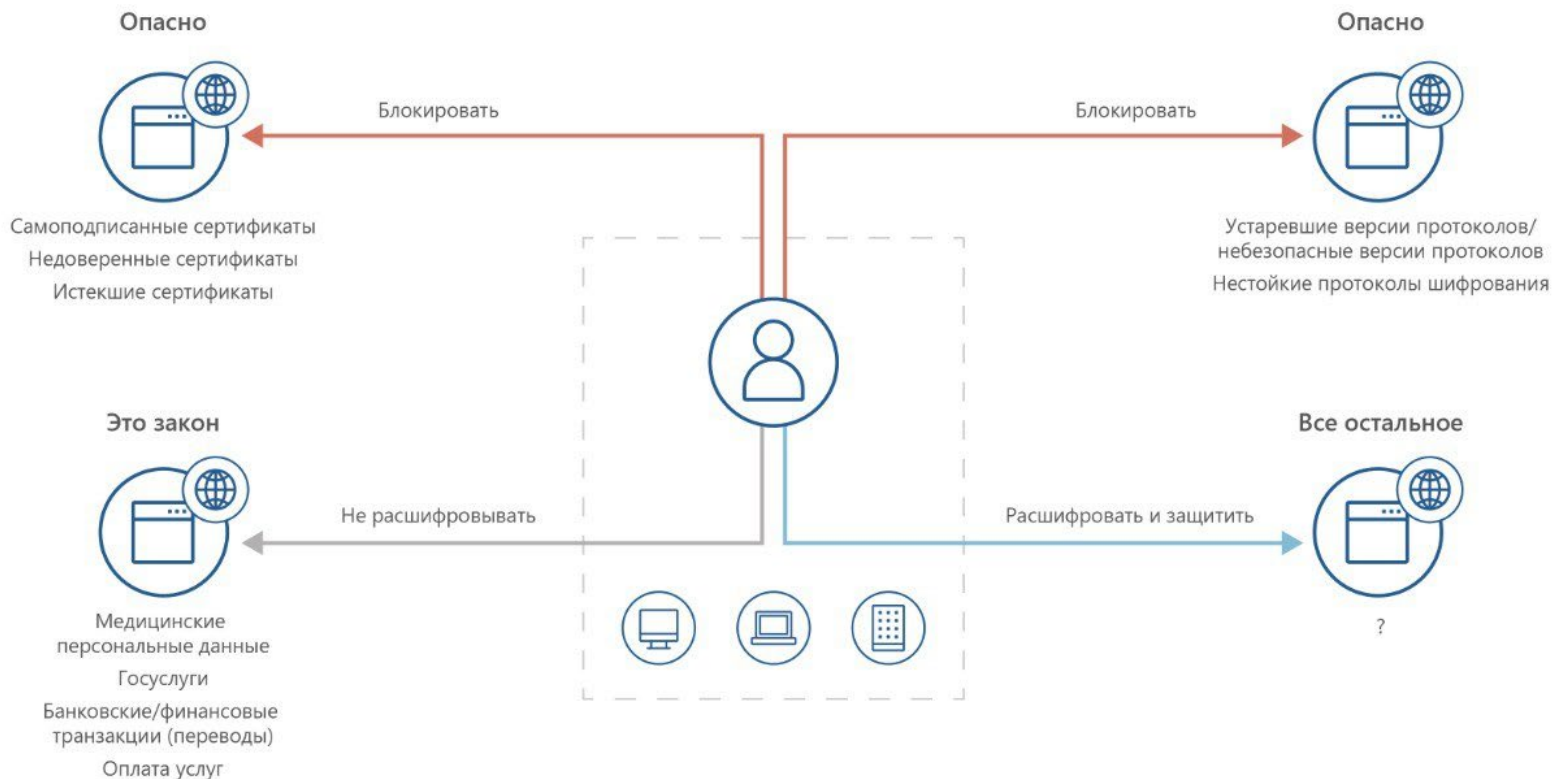
Корневой сертификат МСЭ (Firewall)

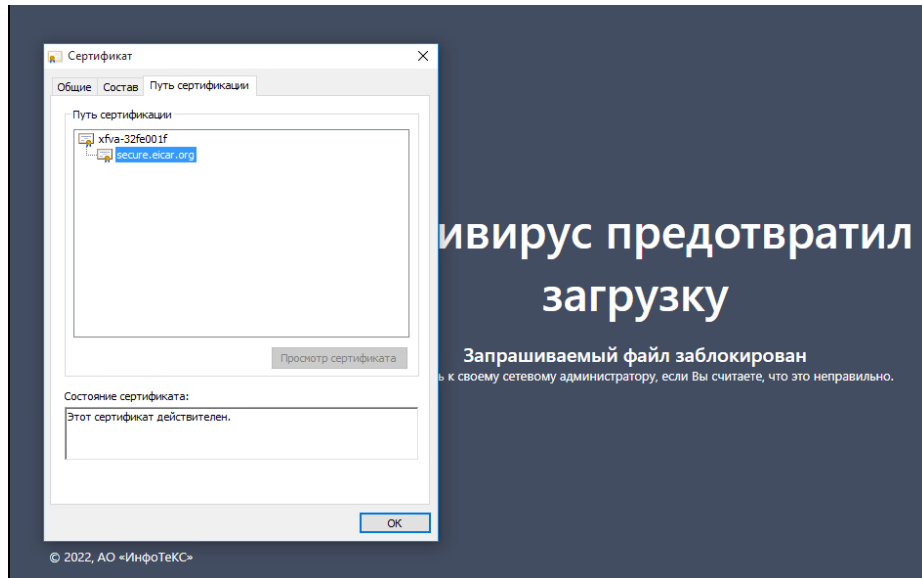


Клиент подтверждает корневой сертификат МСЭ



Лучшие практики SSL Inspection





Результат

Защита от неизвестных угроз

КАК СРАВНИВАТЬ ИНФОРМАЦИЮ ИЗ ЛИСТОВОК?

Покупатели считают, что их вводят в заблуждение

А на сайте обещали другое



Зато порция большая

У всех свои методики

Cisco



¹ Throughput measured with 1500B User Datagram Protocol (UDP) traffic measured under ideal test conditions.

[Cisco Firepower 4100 Series Data Sheet - Cisco](#)

Palo Alto



* Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions.

[downloadResource \(paloaltonetworks.com\)](#)

Check Point



RFC 3511, 2544, 2647, 1242 (Lab),
Firewall 1518B UDP (Gbps)

[Check Point 26000 Security Gateway Datasheet](#)

Что такое «идеальные условия»

Производительность тем выше, чем легче задача



- UDP проще, чем TCP: нужно отслеживать меньше состояний
- Самый большой возможный размер пакета (обычно Jumbo frames):
 - Меньше соединений для передачи того же объема данных
 - Меньше заголовков пакетов для разбора



- Максимальное количество соединений:
 - Открыть много соединений
 - Передавать мало или совсем не передавать данных
 - Не закрывайте соединения



- Максимальное количество новых соединений в секунду:
 - Используйте много очень маленьких соединений
 - Передавать мало или совсем не передавать данных
 - Закрывайте соединения как можно быстрее

Почему никто не тестирует все варианты

Слишком долго и дорого – за это будут платить покупатели



Если в продукте 26 функций, то оценка влияния каждой на производительность приводит к 67 млн. уникальных тестов.
(с) Cisco



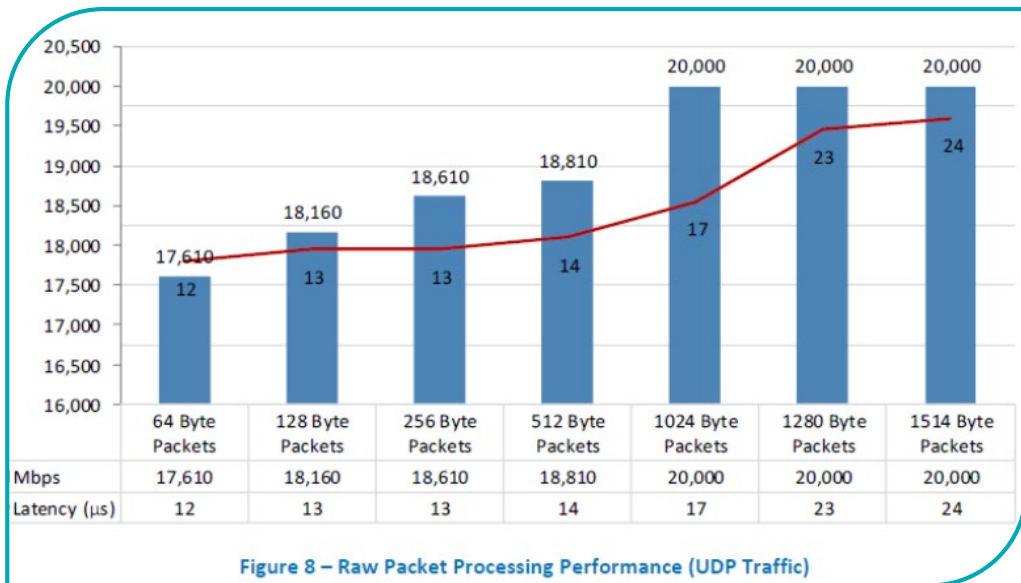
Нужно быть экспертом, чтобы понимать результаты всех этих тестов.



Покупателю нужно изучить все результаты и собрать из них комбинацию своих, чтобы потом ее протестировать и понять что будет у покупателя.

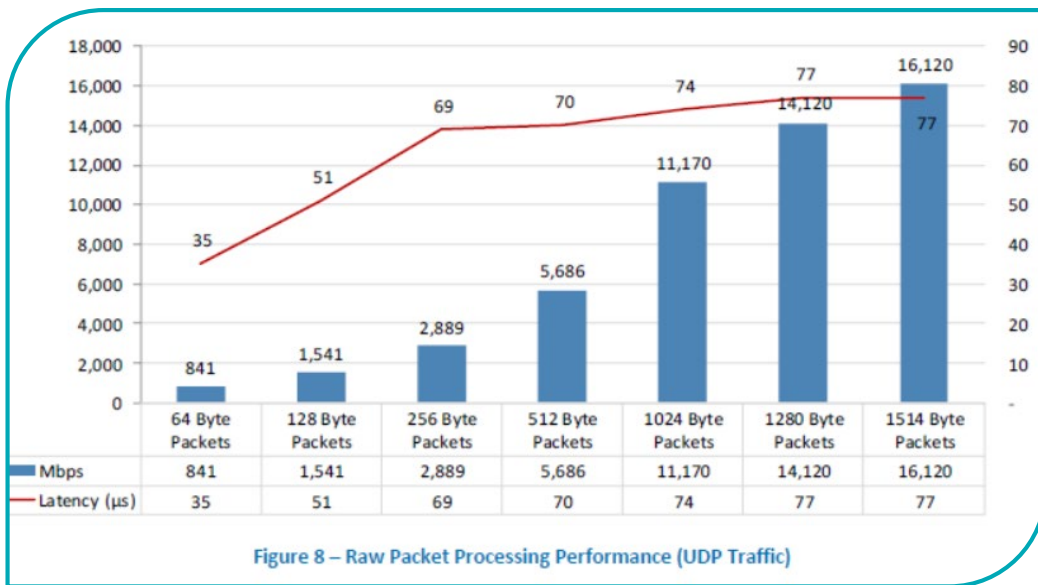
ПОЧЕМУ ВАЖЕН ПРОФИЛЬ ТРАФИКА ?

UDP самый простой тест



Palo Alto Networks
PA-5220 PAN-OS 8.1.6-h2

UDP самый простой тест



Check Point Software
Technologies 6500
Security Gateway
R80.20

Разные приложения – разная скорость

These tests measured the performance of the device with single application flows. For details about single application flow testing, see the NSS Labs Next Generation Firewall Test Methodology v9.0, available at www.nsslabs.com.

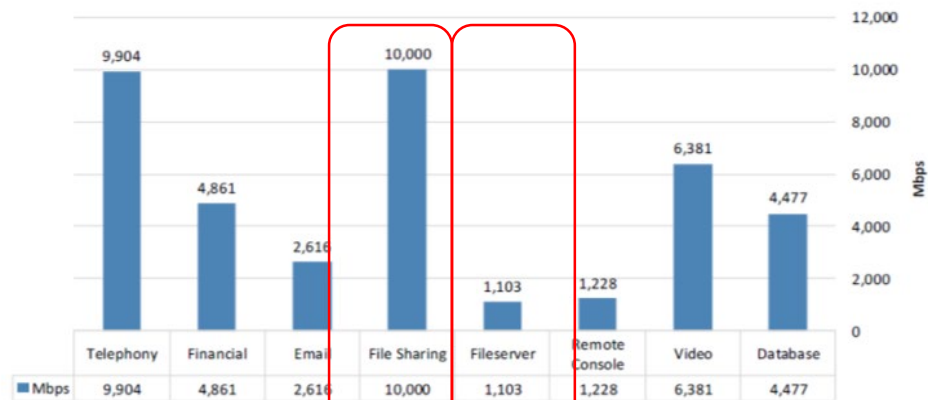


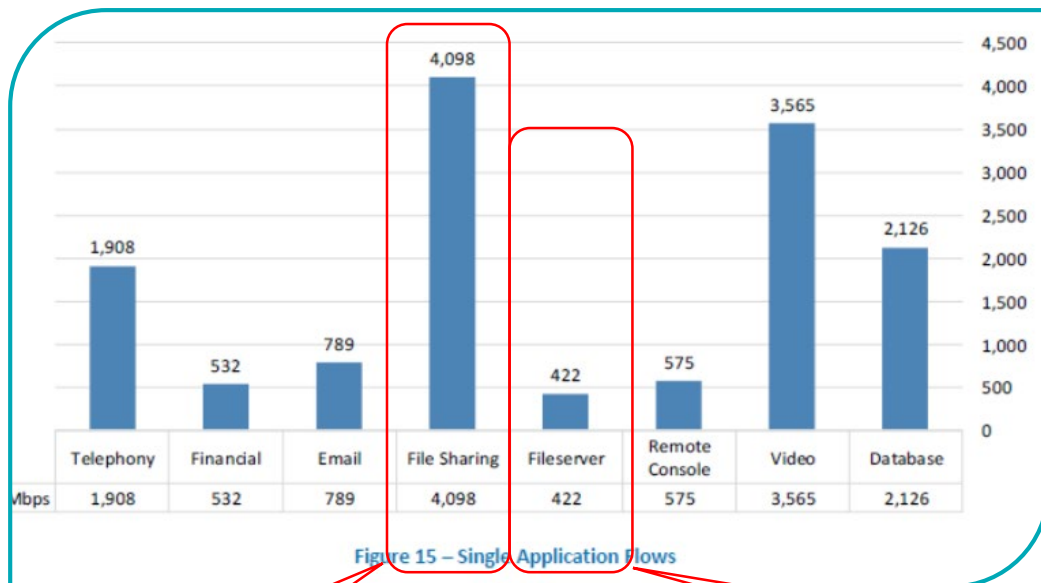
Figure 15 – Single Application Flows

Palo Alto Networks
PA-5220 PAN-OS
8.1.6-h2

FTP

SMB

Разные приложения – разная скорость



Check Point Software
Technologies 6500
Security Gateway
R80.20

FTP

SMB

Профиль трафика влияет на производительность драматически

Changing the traffic profile from HTTP to an Enterprise Mix and running it through the IPS engine:



- HTTP 44%, Bittorrent 22%, IMAP v4 16%, FTP 9%, SMTP 9%

This is Cisco's generic Multiprotocol test and is very similar to all the Internet multiprotocol standards.

Даже HTTP у всех разный

HTTP – хороший базовый уровень для тестов “real world”

Cisco

1024B HTTP Test (256KB Object)

This number is to compare with other vendors at a 256KB object size. It uses a larger and commonly tested packet size for every simulated session. With the protocol overhead, the average frame size is around 1024 bytes. This represents typical production conditions for most firewall deployments.

Palo Alto
Networks

Note: Results were measured on PAN-OS 11.0.

* Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP appmix transactions.

Check Point

	Enterprise Test	Preferred Testing Conditions
Protocols	Typical blend of HTTP, SMTP, HTTPS, DNS, FTP and other protocols derived from research conducted over hundreds of customer environments	HTTP only
Content Types	Realistic blend	Page loads only

СРАВНИТЕЛЬНОЕ ТЕСТИРОВАНИЕ ПО МЕТОДИКЕ ИнфоТеКС

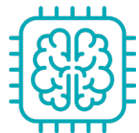
Как мы тестируем



Методики ИнфоТеКС основаны на публичных



RFC-2544, RFC 9411
(Benchmarking Methodology for Network
Security Device Performance)



Методики NSS Labs - NextGeneration Firewall (NGFW)

Чем мы тестируем



Система тестирования производительности, функционала и совместимости сетей и сетевых приложений. Компактное 2-слотовое шасси Ixia XM2.



Решение PerfectStorm ONE компании Ixia представляет собой компактный программно-аппаратный комплекс (ПАК), предназначенный для тестирования систем сетевой безопасности и других сетевых средств реалистичным трафиком атак, приложений и сервисов на уровнях 4–7 модели OSI.

Тесты по методикам и реальность

Самая жесткая методика
по RFC 9411

Реальный заказчик



Кол-во правил **максимум 562**



Кол-во правил в 2022
году было около 5 тыс.,
а в 2023 году стало
10 461

Профиль трафика

По методике NSS Labs

№	Приложение	Доля трафика, %
1.	Amazon S3	7,73
2.	AOL Instant Messenger	1,16
3.	BitTorrent	10,82
4.	Facebook	5,8
5.	FTP	5
6.	Gmail	9,66
7.	Gtalk	4,64
8.	HTTP	18,69
9.	Simulated HTTPS	9,66
10.	SMTP	1,93
11.	SSH	0,29
12.	Oracle DB	0,28
13.	Twitter	3,09
14.	Yahoo Mail	9,66
15.	YouTube	11,59

Реальный заказчик

№	Приложение	Доля трафика, %
1.	Citrix	5,8
2.	DNS	0,3
3.	Dropbox Sync-Get	7,2
4.	HTTP Text_1	5,8
5.	HTTP VE	8,7
6.	HTTPS Dropbox	19
7.	MAX Bandwidth HTTP_	4,4
8.	RDP	0,4
9.	SMB Client File Download	43,9
10.	SNMP_1	4,5
11.		
12.		
13.		
14.		
15.		

Журналирование

Самая жесткая методика
по RFC 9411

Реальный заказчик



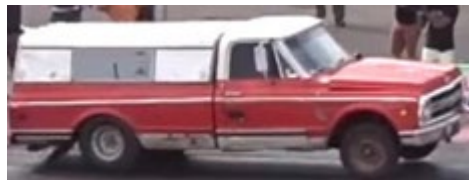
Logging and reporting
MUST be enabled



Должно быть включено
журналирование всего

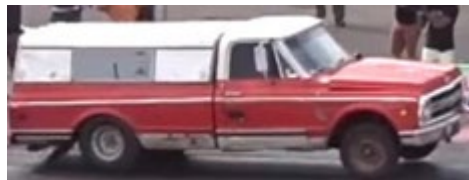
ТЕСТИРОВАНИЕ В ИДЕАЛЬНЫХ УСЛОВИЯХ

Данные с сайта



Исполнение	Производитель А	Производитель Б
Firewall, 1518 byte UDP (Mbps)	до 45 000	До 30 000
Firewall Throughput (Packets Per Second)	4 000 000	----
Firewall, TCP Multistream (Mbps)	30 000	40 000

Данные с сайта



Исполнение	Производитель А	Производитель Б
AppControl (Firewall+DPI) (Mbps)	7 800	32 000
NGFW Througput (Mbps)	1 531	3 900
Connections per Second	85 000	127 000
Concurrent Connections	9 900 000	16 000 000

Казалось бы, победитель известен до старта



Тест «Идеальные условия»

	Производитель А	Производитель Б
МЭ, 1518 байт UDP	45 Гбит/сек	38,2 Гбит/сек
МЭ (пакетов/сек)	4 млн	4,4 млн
Соединений в секунду	85 000	259 000
МЭ, TCP	30 Гбит/сек	34,5 Гбит/сек

ТЕСТИРОВАНИЕ ПО МЕТОДИКЕ NSS LABS

Трафик NSS Labs EMIX

Кол-во правил	Производитель А	Производитель Б
1 правило	7,2 Гбит/сек	3,3 Гбит/сек
101 правило	6,6 Гбит/сек	3,1 Гбит/сек
1001 правило	5,5 Гбит/сек	Тест не пройден

ТЕСТИРОВАНИЕ ПО МЕТОДИКЕ ЗАКАЗЧИКА

Условия Заказчика

Кол-во правил	Производитель А	Производитель Б
1 правило	700 Мбит/сек	600 Мбит/сек
1001 правило	600 Мбит/сек	500 Мбит/сек
11001 правило	200 Мбит/сек	Тест не пройден

Победителя определяет финиш



ПОДВЕДЕМ ИТОГИ

Данные на сайтах верные!

Но получены по разным методикам

2 Результаты получены на основании методики АО «ИнфоТеКС». Результаты получены для релиза 5.6.0.»

Скорость передачи данных измерена по собственной методике, которая может быть предоставлена по запросу.

Требуйте предоставить методики измерений... если готовы в них разбираться, либо...

BANANA VS APPLE



100 GRAMS

- PROTEIN : 1.2GM
- CARBS : 27.2GM
- FAT : 0.3GM
- CALORIE : 116



100 GRAMS

- PROTEIN : 0.2GM
- FIBER : 3.2GM
- WATER : 86%
- CALORIE : 59

**Сравнивать
нужно
в равных
условиях**

Как сравнить производительность

Единая
методика



Максимально идентичные
настройки всех испытуемых



Единый профиль трафика



Единый инструмент
нагрузочного тестирования

техно infotecs
2024 Фест

Спасибо
за внимание!

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363