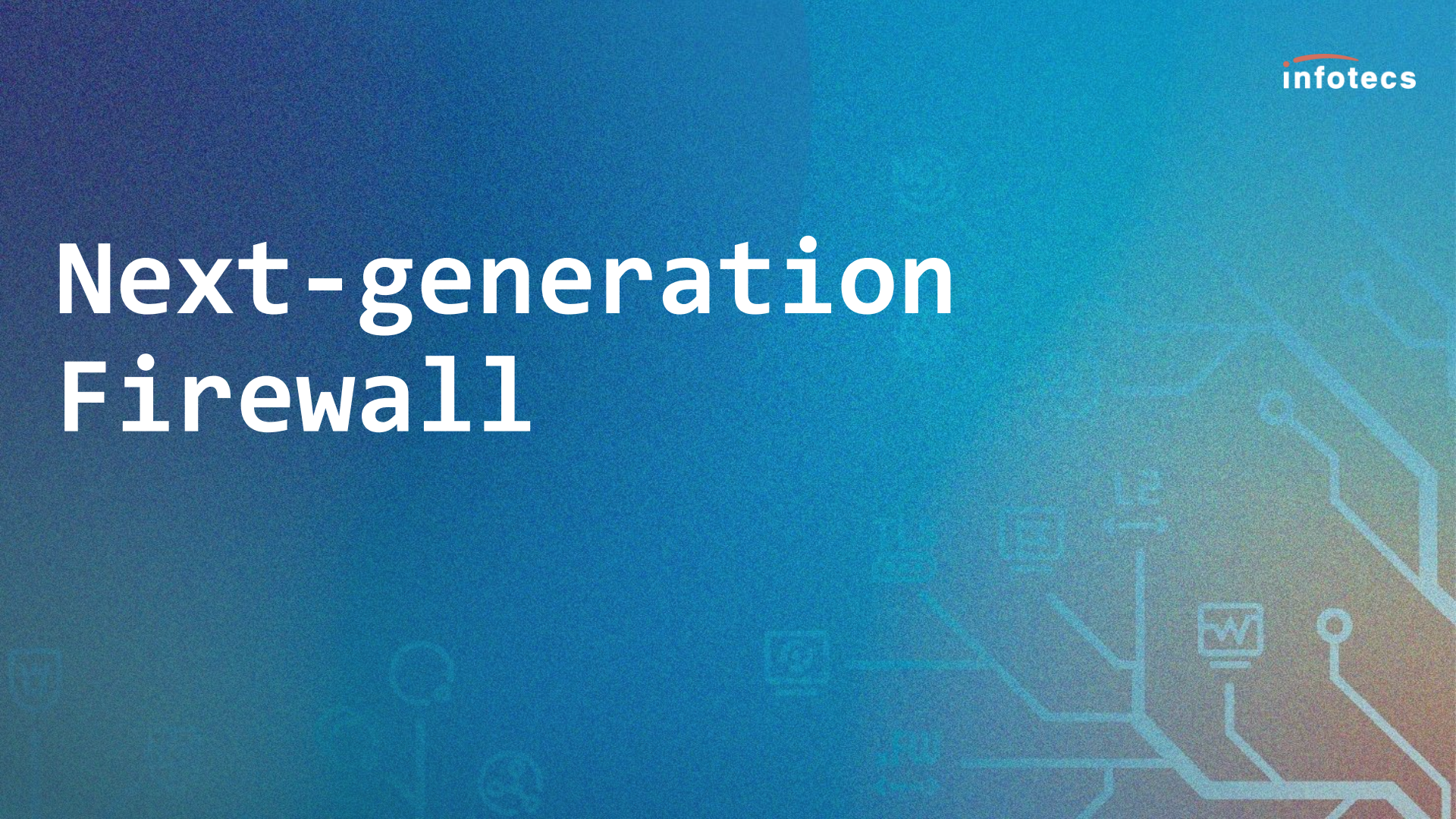
ViPNet xFirewall 5.6.2: новые возможности

Алексей Данилов

infotecs

infotecs

Next-generation Firewall



Next-Generation Firewall (NGFW)

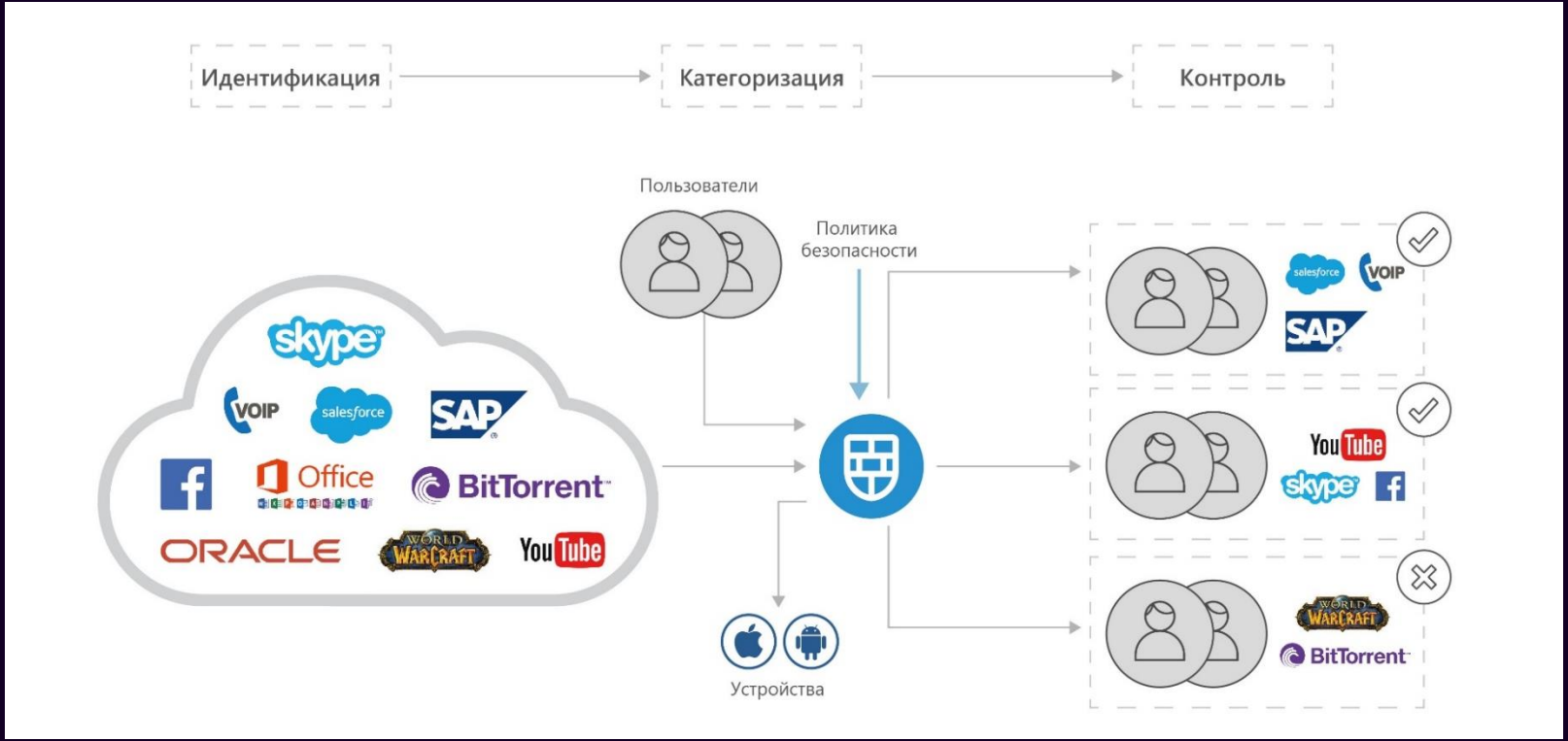
Gartner

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

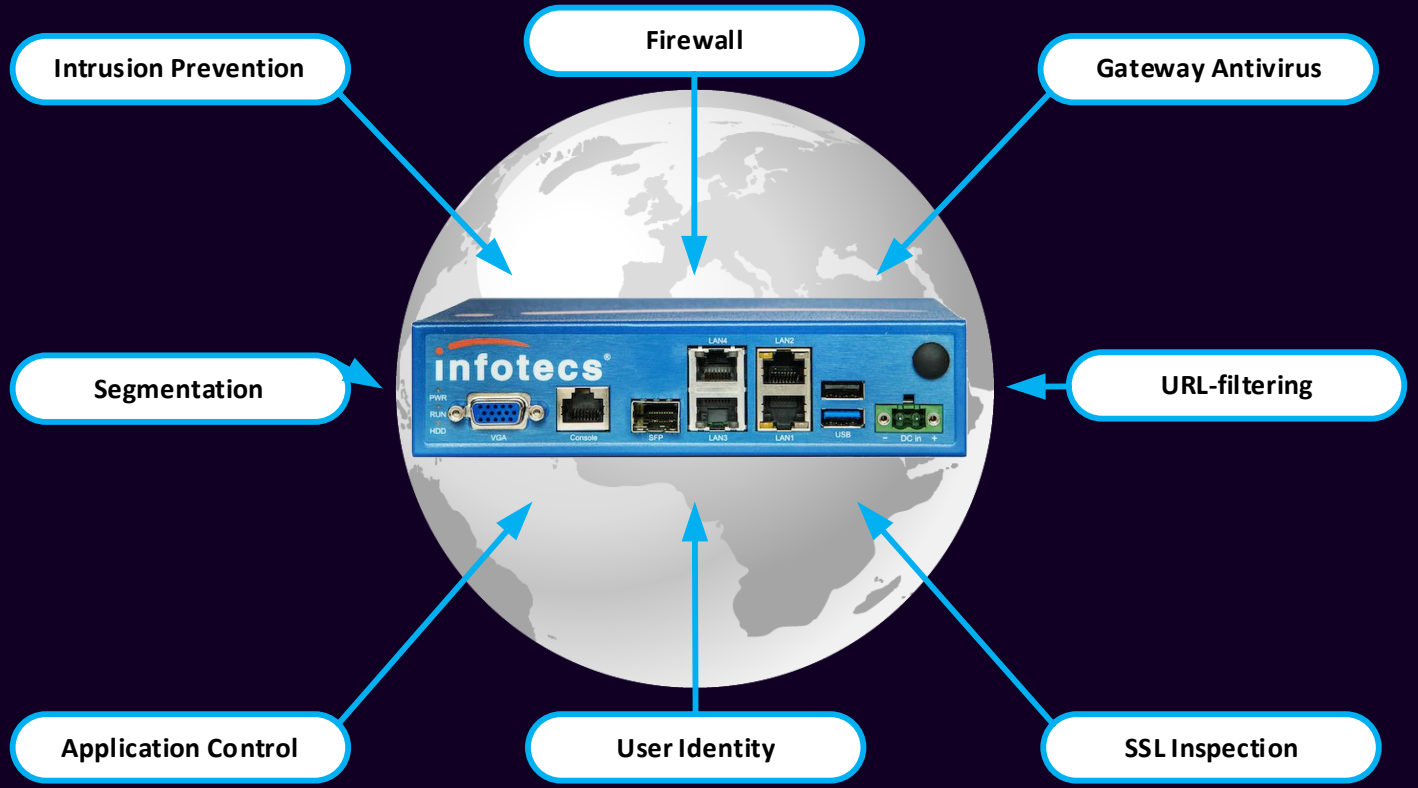
NGFW с первого взгляда



infotecs

ViPNet xFirewall

Что такое 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 задании по безопасности ФРКЕ.465614.002Д1 при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.465614.002ФО.

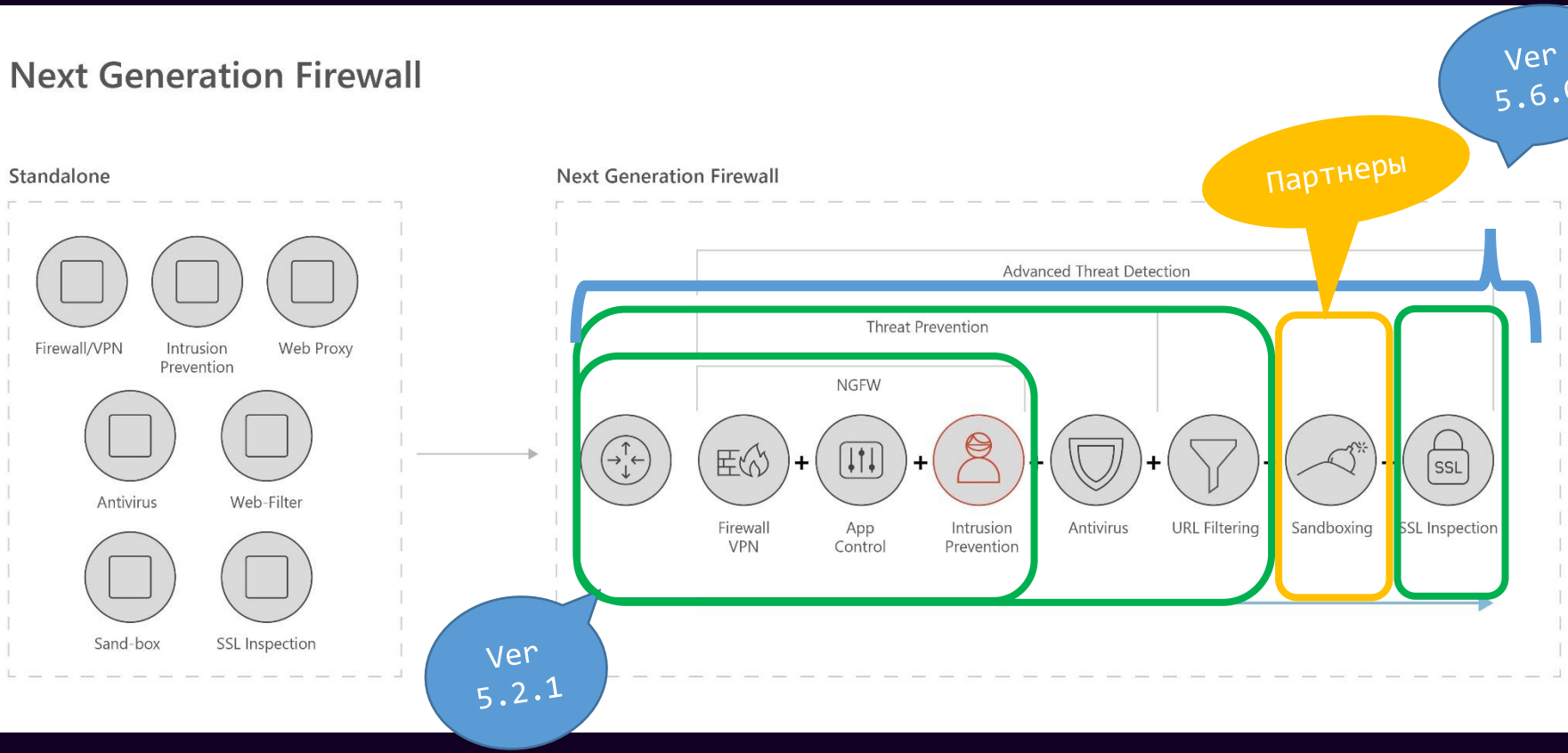
Сертификат выдан на основании технического заключения от 01.11.2021, оформленного по результатам сертификационных испытаний испытательной лабораторией МОУ «ИЗФ» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 06.12.2021, оформленного органом по сертификации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

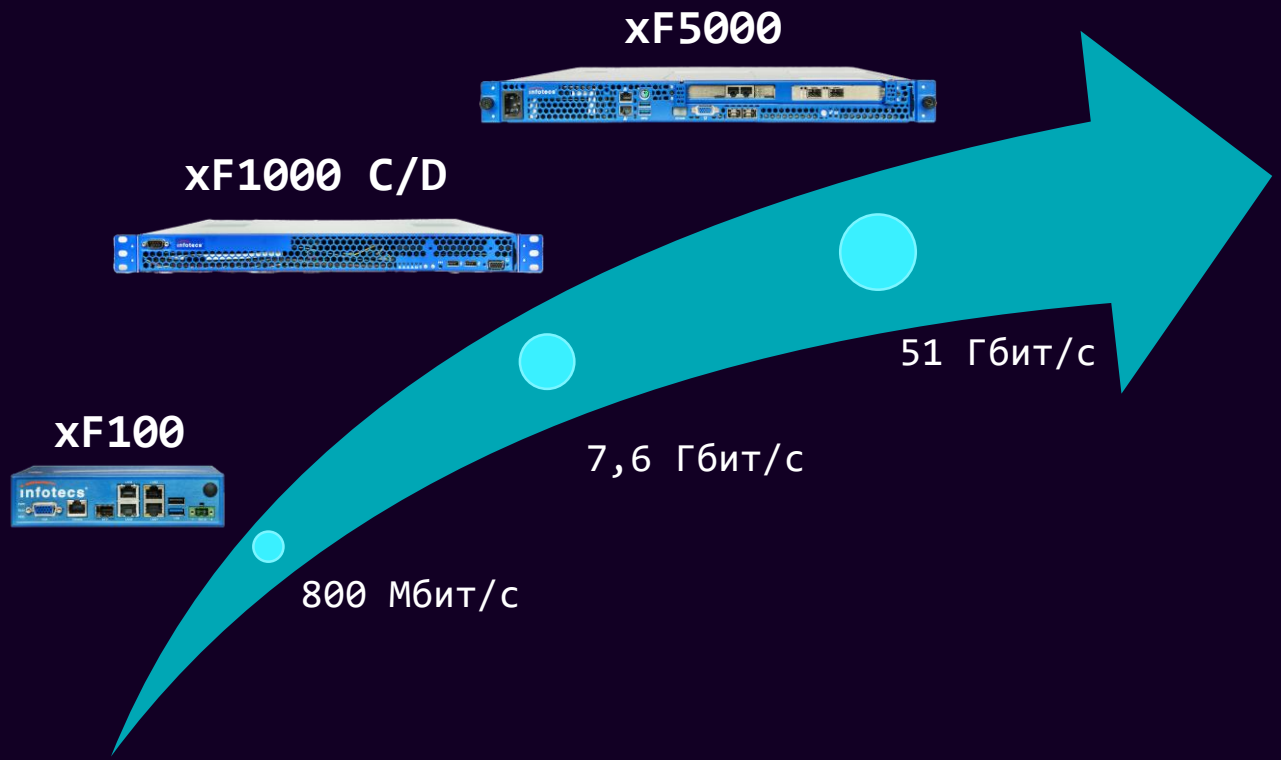
- Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020)» - по 4 уровню доверия
- «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых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



Релиз 5.6.0

ViPNet xFirewall. Платформы



SSL Inspection – анализ SSL

Классификация SSL

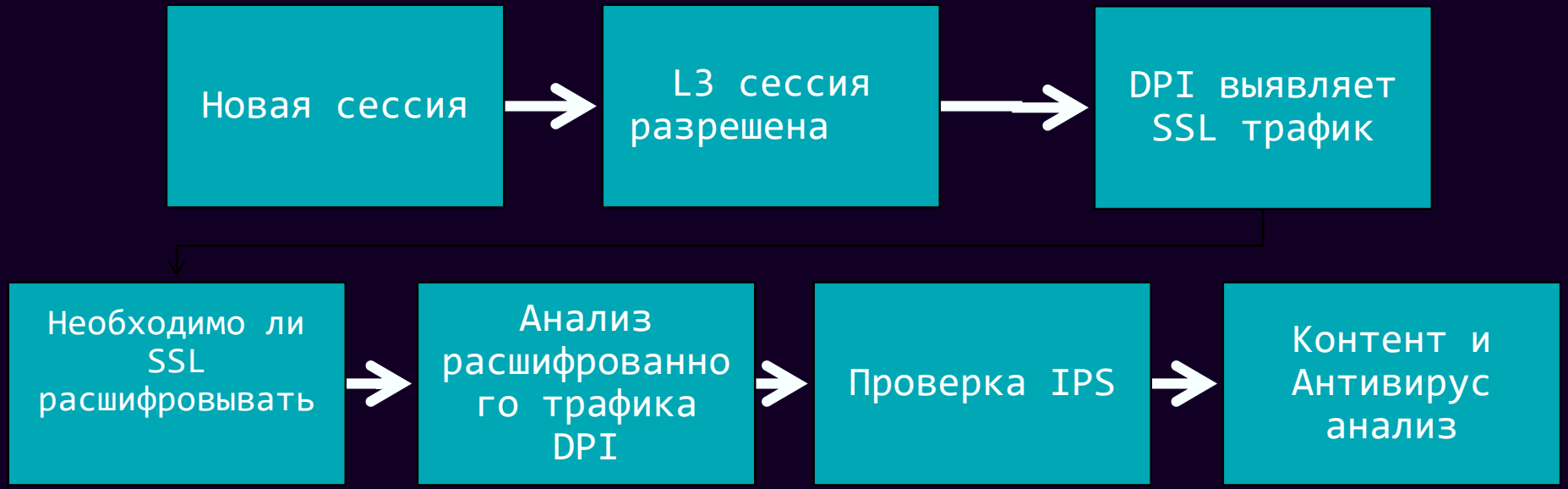
- Разрешить тот SSL трафик, который известен:

  Yandex, Rutube, VK и тд

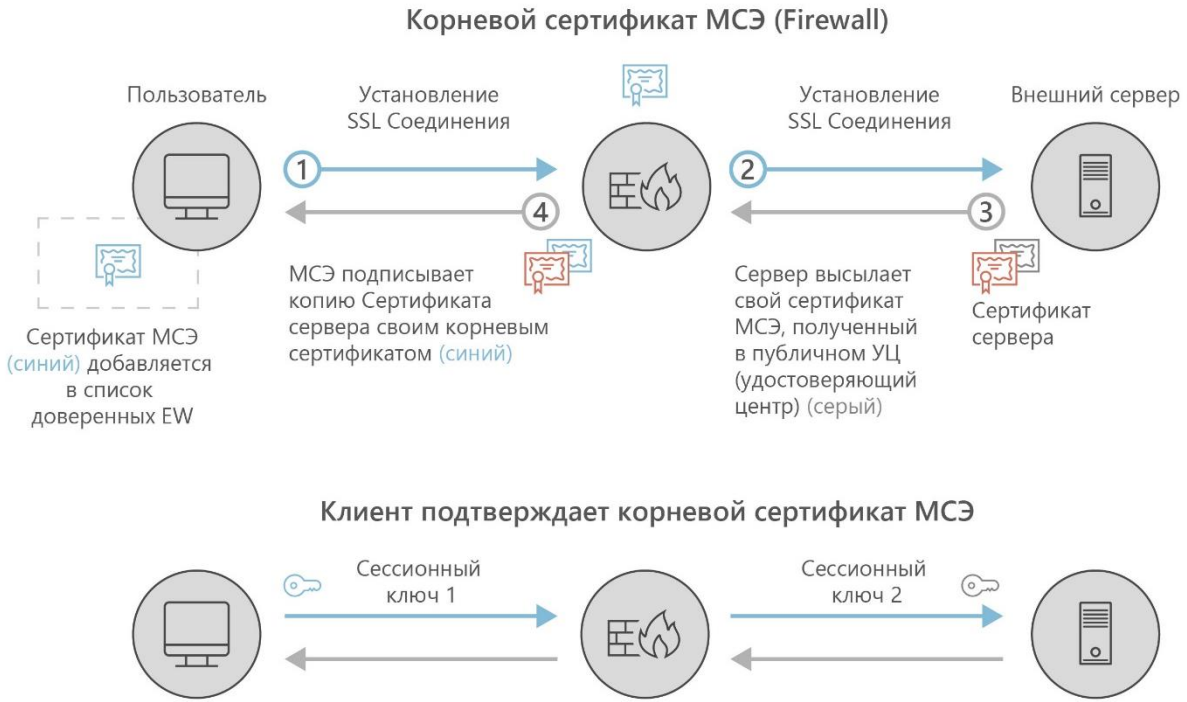
- Блокировать известный SSL запрещенных политикой приложений: Социальные сети, мессенджеры и тд

- Запретить любой неизвестный SSL трафик

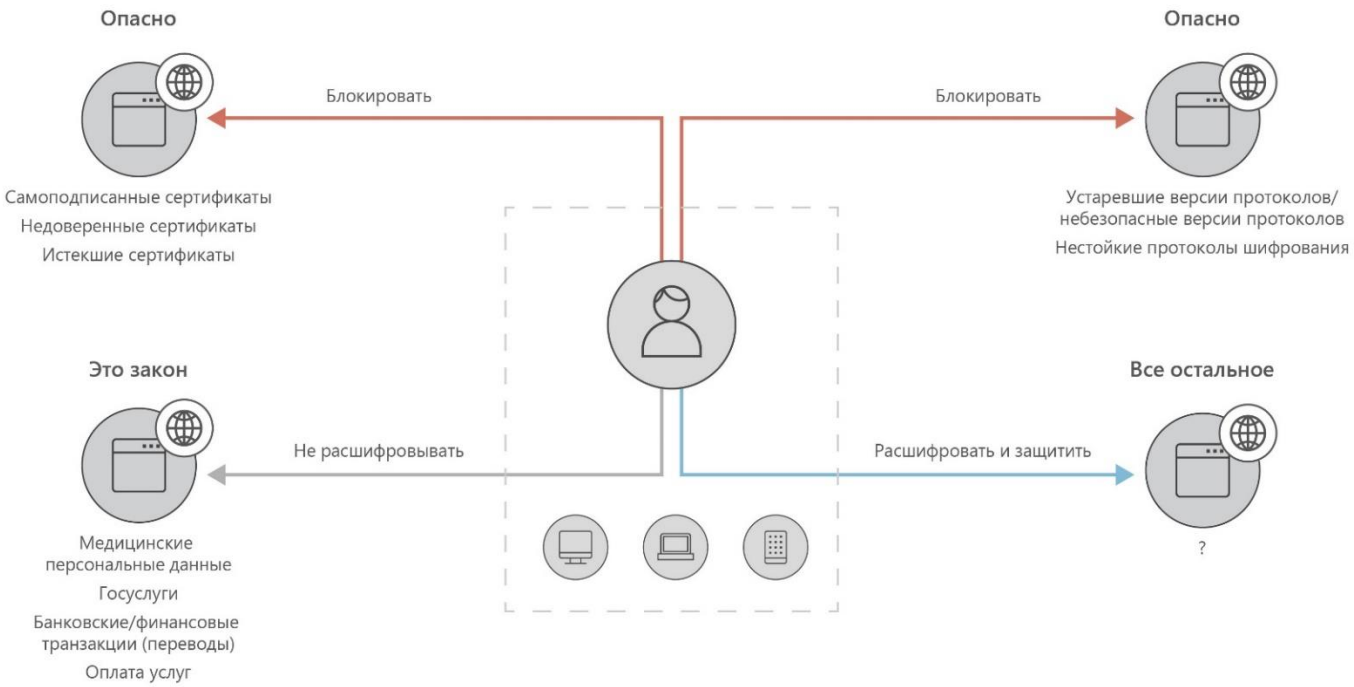
Схема проверки трафика



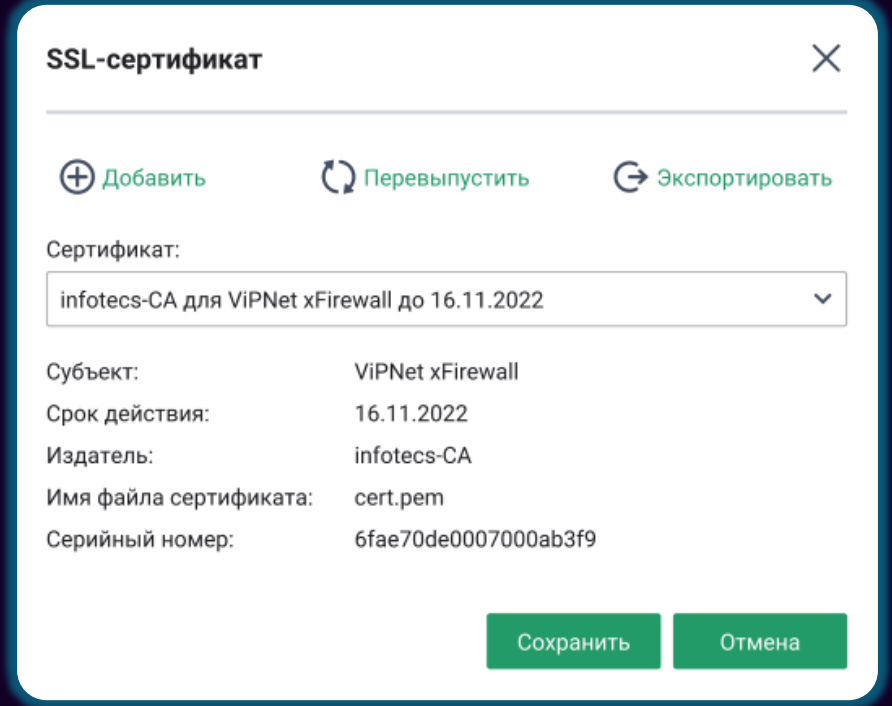
Forward proxy decryption

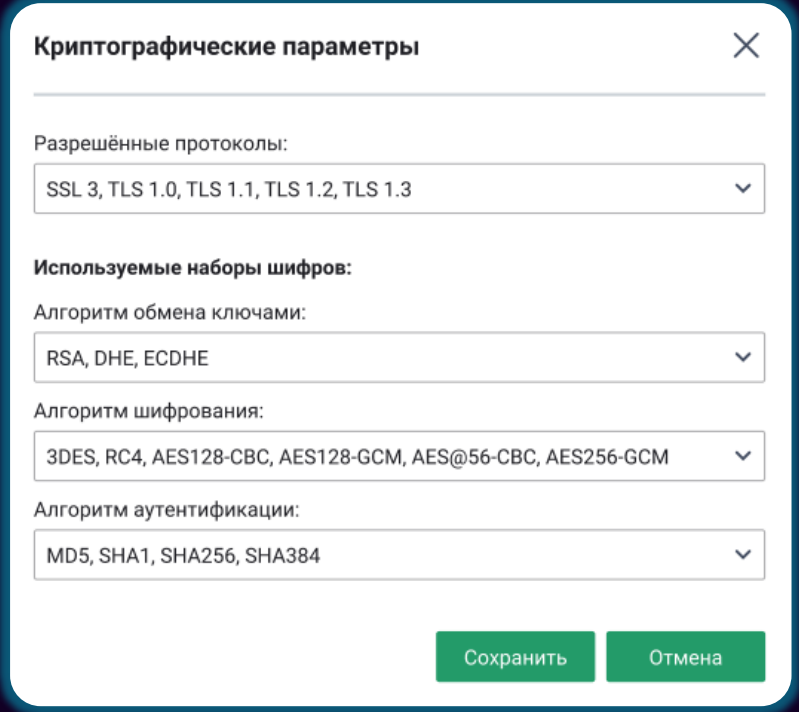


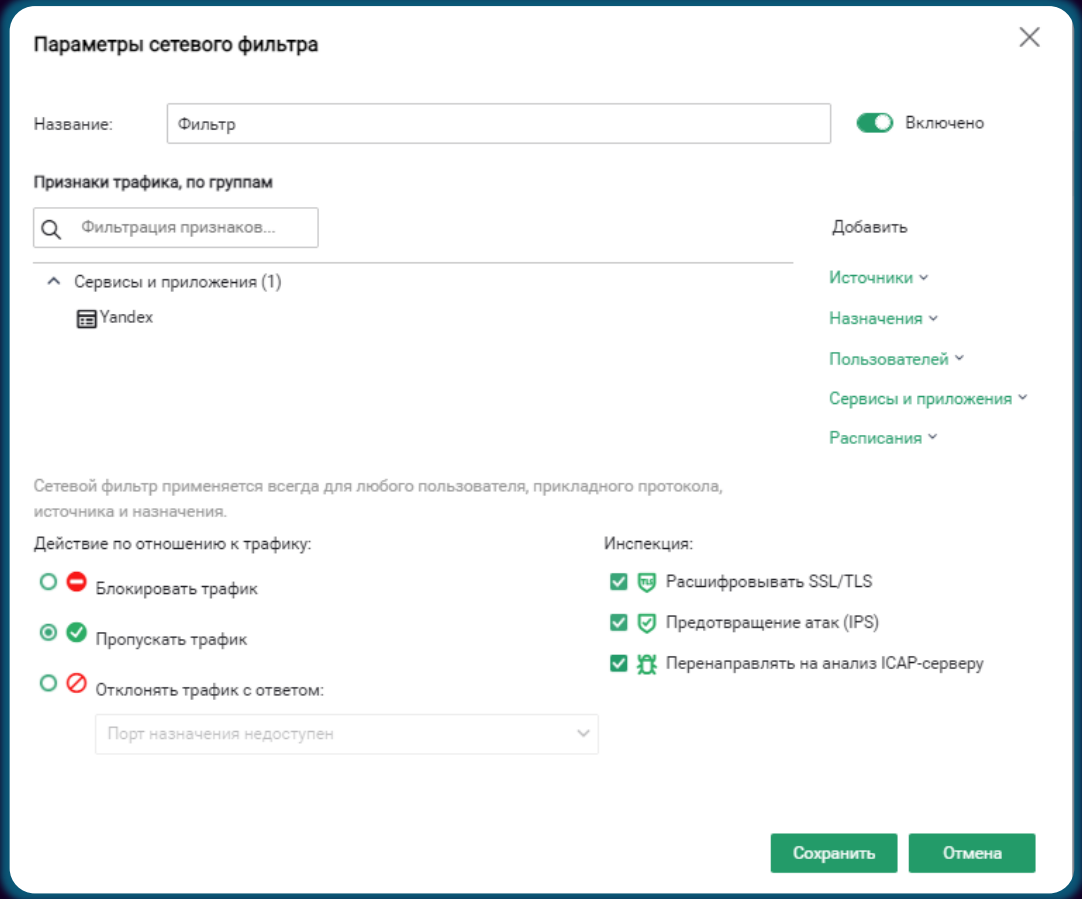
Лучшие практики SSL Inspection



SSL Inspection

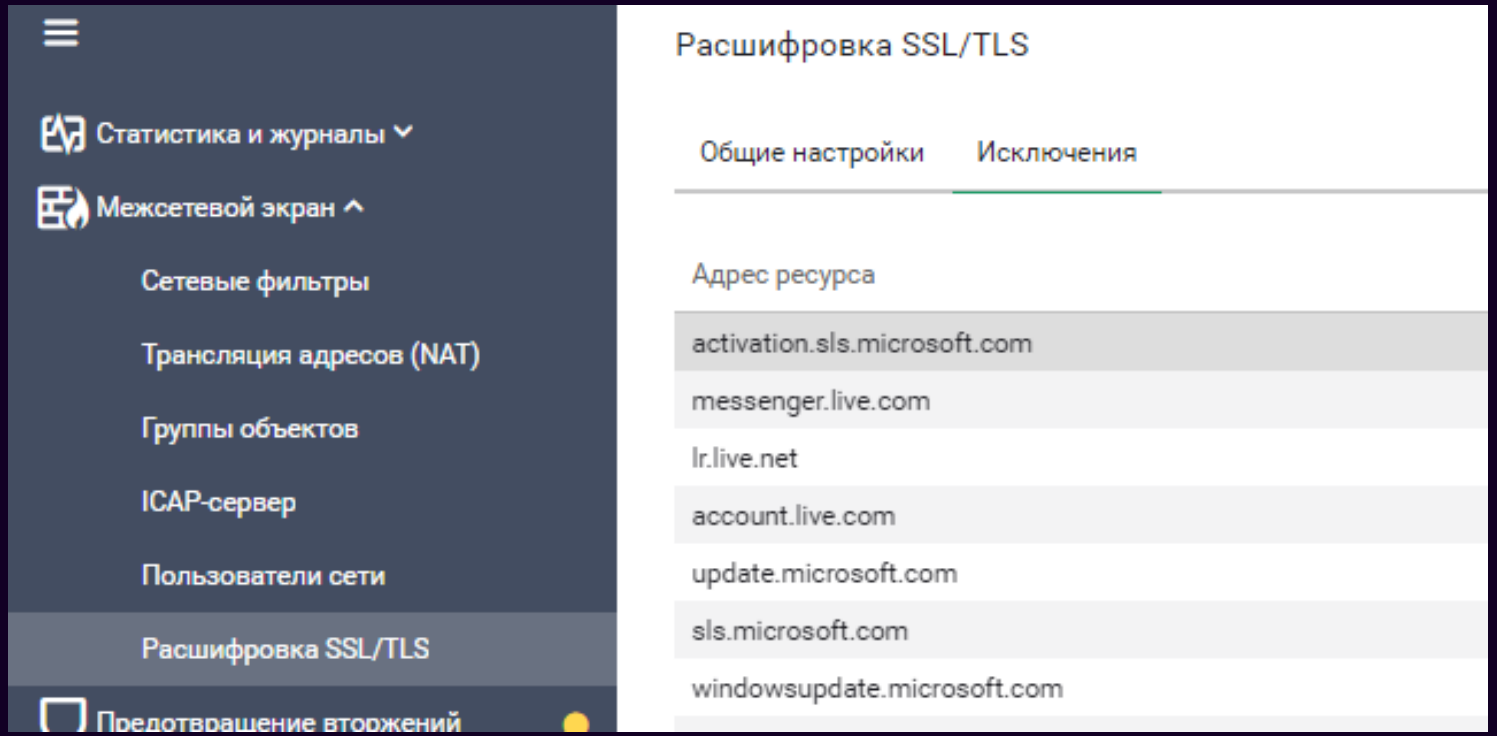




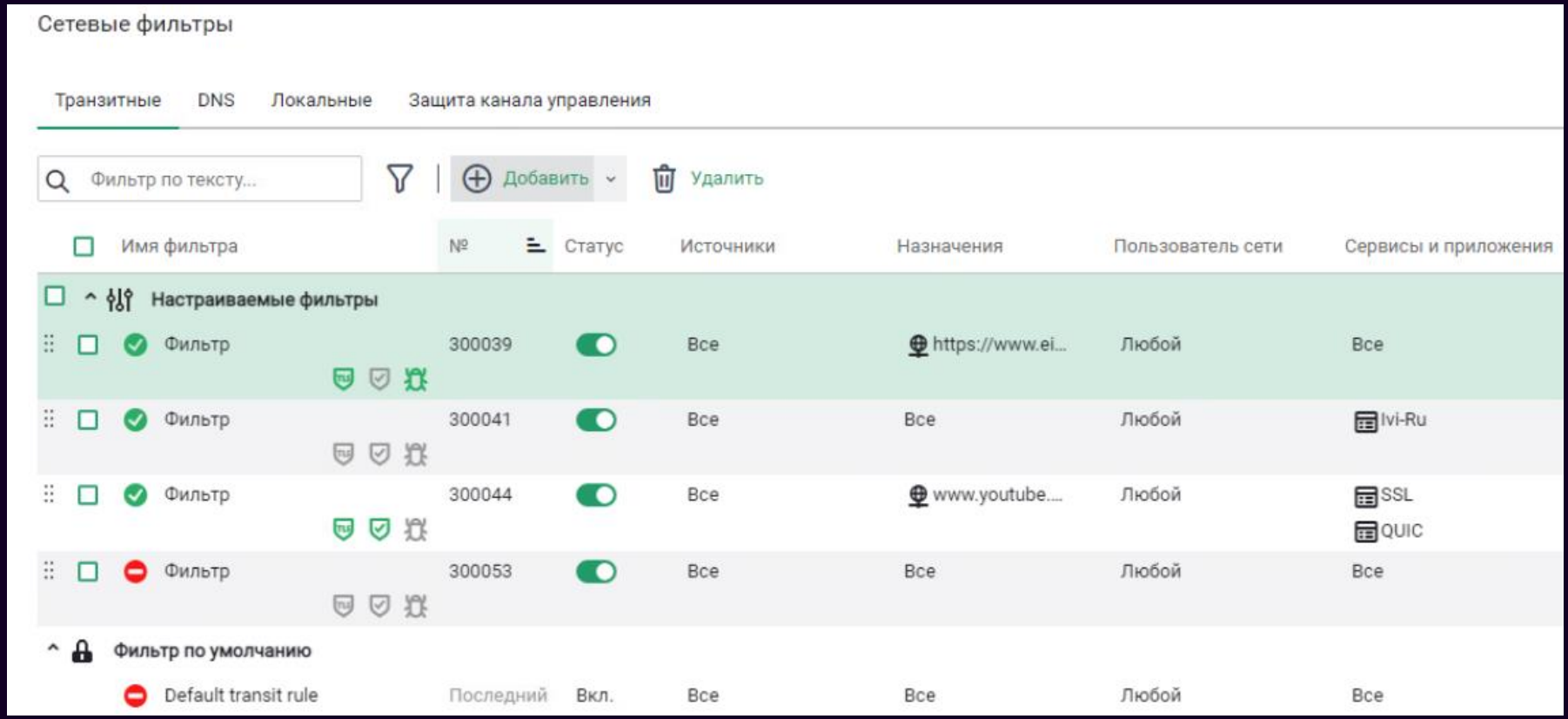


SSL Inspection

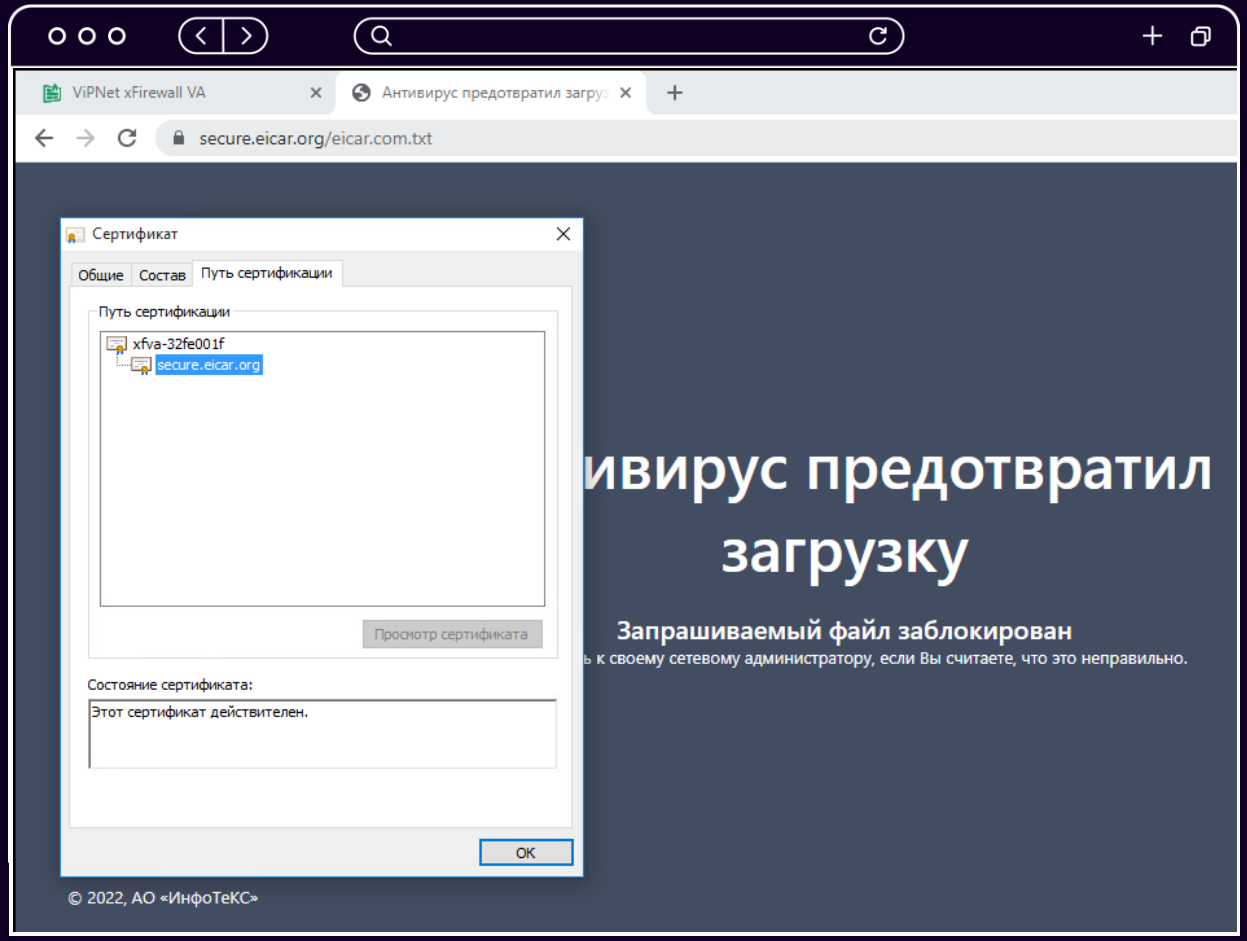
Исключения были и будут



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»

Блокировка источников повышенной сетевой нагрузки

Directly to black hole

Обработка списков блокировки имеет приоритет перед остальными правилами межсетевого экрана

- 1 раз в минуту ищем заблокированные пакеты
- Если от какого-то адреса регистрируется множество заблокированных пакетов – **по умолчанию 10 пакетов**, то этот адрес включается в список блокировки
- Все адреса из списка блокировки **блокируются на 1800 секунд**
- Адрес удаляется из списка, если отсутствует его сетевая активность

В чем задача и польза

На тестах Заказчика xF1000 C обрабатывал 920 Мбит/сек нагрузки и блокировал 2.5 Гбит/сек DoS атаку.

Задача – защитить ПАК от DDoS и DoS атак и сохранить управляемость

Польза – еще и сети заказчиков стали **немного** защищать от атак

Новые возможности

Что нового в 5.6.2

1. Улучшенный механизм SSL/TLS-инспекции
2. Расширение возможностей агрегированных интерфейсов
3. Улучшенный пользовательский интерфейс
4. Поддержка новых аппаратных платформ

Что нового в 5.6.2

5 RADIUS-аутентификация для SSH-подключений

6 Сброс к заводским настройкам

7 Повышена скорость и стабильность отправки CEF-сообщений

8 Исправление ошибок

xF100 Q1/Q2

- Размеры корпуса (ШхВхГ)- 250 x 44 x 227,6 мм
- 6 сетевых интерфейсов:
  - 4 x 1 Гбит/сек RJ45
  - 2 x 1 Гбит/сек SFP
- Незначительно повысилась производительность

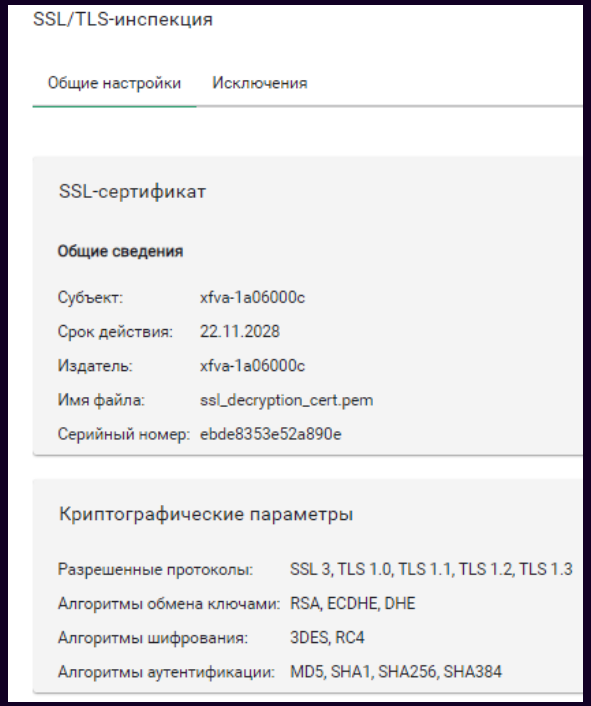
Производительность

Исполнение	xF100 N1	xF100 Q1/Q2
Firewall, 1518 Байт UDP (Мбит/сек)	722	**1 600**
Firewall, TCP Multistream (Мбит/сек)	600	**1 380**
AppControl (Firewall+DPI), (Мбит/сек)	180	**395**
NGFW (FW+DPI+IPS) (Мбит/сек)	13	**40**
NGFW+SSL Inspection (1МБ)	32	50
Firewall Throughput (UDP 64 Байт)	79 000	**137 000**
Connections per Second	10 000	**18 000**
Concurrent Connections	149 993	499 994

Производительность

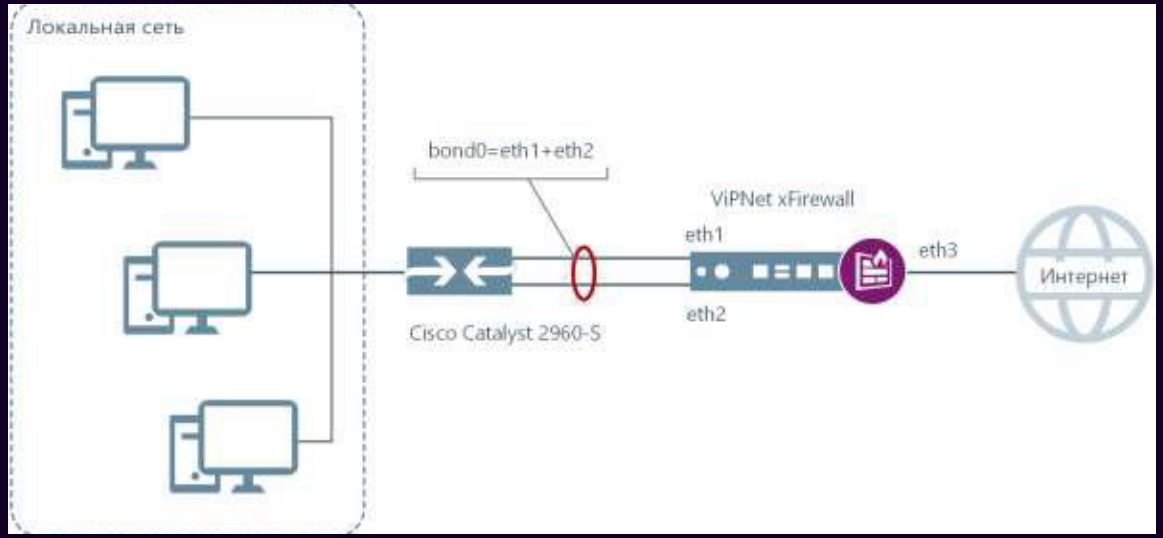
Исполнение	xF1000 Q7/Q8	xF5000 Q2
Firewall, 1518 Байт UDP (Мбит/сек)	7 600	51 000
Firewall, TCP Multistream (Мбит/сек)	11 000	33 000
AppControl (Firewall+DPI), (Мбит/сек)	2 600	7 800
NGFW (FW+DPI+IPS) (Мбит/сек)	480	1 300
NGFW+SSL Inspection (1МБ)	480	1 300
Firewall Throughput (UDP 64 Байт)	2 200 000	4 000 000
Connections per Second	53 000	106 000
Concurrent Connections	4 999 000	29 999 990

Улучшения SSL Inspection



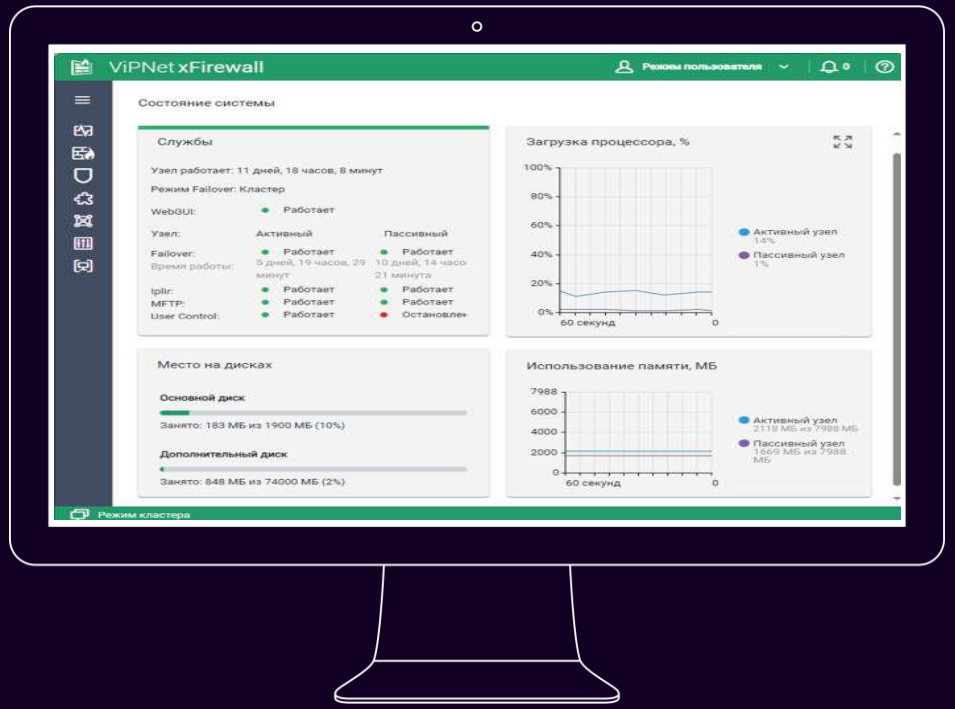
- Добавлена поддержка расшифровывания протокола TLS 1.3
- Добавлена возможность инспекции трафика HTTP/2
- Добавлены настройки доверия к сертификатам ресурсов:
  - проверка срока действия сертификатов;
  - проверка полей сертификата, определяющих его использование (key usage, extended key usage);
  - проверка самоподписанных сертификатов.
- Исключать из инспекции веб-ресурсы, используя их альтернативные имена (SAN – Subject Alternative Names) и поддомены (wildcard).

Агрегация интерфейсов



- Ранее вы могли включать в состав агрегированного интерфейса только до трех подчиненных физических. Теперь это ограничение снято.
- Максимальное количество агрегированных интерфейсов увеличено до 8.

Изменен вывод контролируемых параметров



Теперь отображается относительная загрузка CPU, а максимальная загрузка всех ядер принята за 100%.

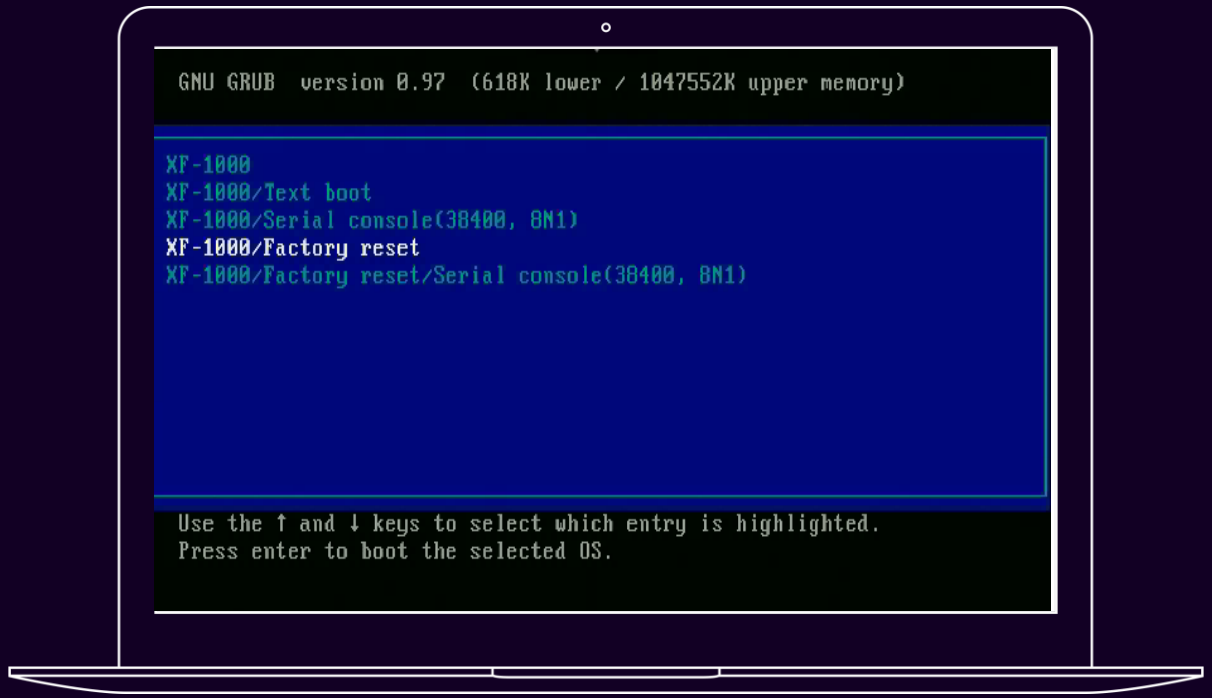
Radius-аутентификация

- Чтобы пользователь подключался к ViPNet xFirewall в режиме администратора, установите значение атрибута shell:priv-lvl равным 15.
- При другом значении атрибута shell:priv-lvl или при его отсутствии подключение будет выполняться в режиме пользователя.

Возможность возврата к предыдущей версии ViPNet xFirewall

В ViPNet xFirewall добавлена возможность возврата ПО к версии 5.4.0

Сброс к заводским настройкам



В строке Are you sure you want to execute this command and delete key? Введите

Delete нажмите Enter.

ViPNet xFirewall Add-ons

GeoIP

Модуль устанавливается самостоятельно Заказчиком.

Назначение – блокировка трафика по Geo-признакам.

Используется база ГРЧЦ.

Принципы GeoIP-фильтрации трафика

infotecs

Модуль GeoIP-фильтрации

Модуль ViPNet xFirewall, позволяющий разграничивать доступ на основе геолокации. Блокирует входящий трафик из заданных регионов.

Первый этап анализа трафика

Это снижает долю трафика, анализируемого DPI, IPS, что повышает эффективность межсетевого экрана.

Белый список

Можно исключить из GeoIP-фильтрации отдельные IP-адреса или подсети.

Next

Прошедший GeoIP-фильтрацию трафик обрабатывается другими подсистемами межсетевого экрана.

ViPNet xFirewall
xF65000
Межсетевой экран
для защиты ЦОДов

xFirewall исполнение xF65000

- 2U платформа производства Аквариус
- 4 x 1Gb RJ-45
- 4 x 1Gb SFP
- 8 x 10Gb SFP+
- 2 БП

Новые возможности

1

Высокая производительность
85 тыс. правил
DPI+IPS без деградации

2

HA-Cluster
Синхронизация сессий

Переключение за 1 сек

3

Динамическая маршрутизация
BGP
OSPF

4

Шлюзовой антивирус
Прокси-сервер
Поддержка ICAP

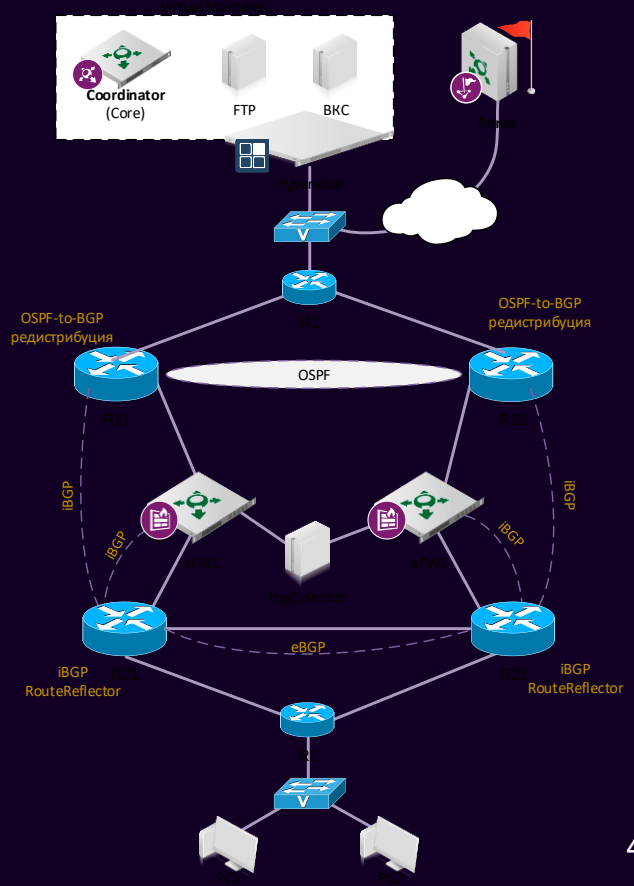
5

Резервирование
2 блока питания

Поддержка BFD

BGP. Моделирование переключения кластера

- Отключение питания активной ноды xFW1
- Проверить изменение таблицы маршрутизации на xFW1
- Проверить трассировку с PC1 до тестового сервиса (сервер BKC\FTP). Выведен список хопов через R11 и R21
- На узле PC1 видео-поток не остановился
- Включение питания активной ноды xFW 2
- Проверить изменение таблицы маршрутизации на xFW1
- Проверить трассировку с PC1 до тестового сервиса (сервер BKC\FTP). Выведен список хопов через R11 и R21
- На узле PC1 видео-поток не остановился



Сравнение производительности

Checkpoint 28000

Firewall	Next Gen Firewall
• 145 Гбит/сек	• 51,5 Гбит/сек

ViPNet xFirewall xF65000

Firewall	Next Gen Firewall
• 76 Гбит/сек	• 60 Гбит/сек

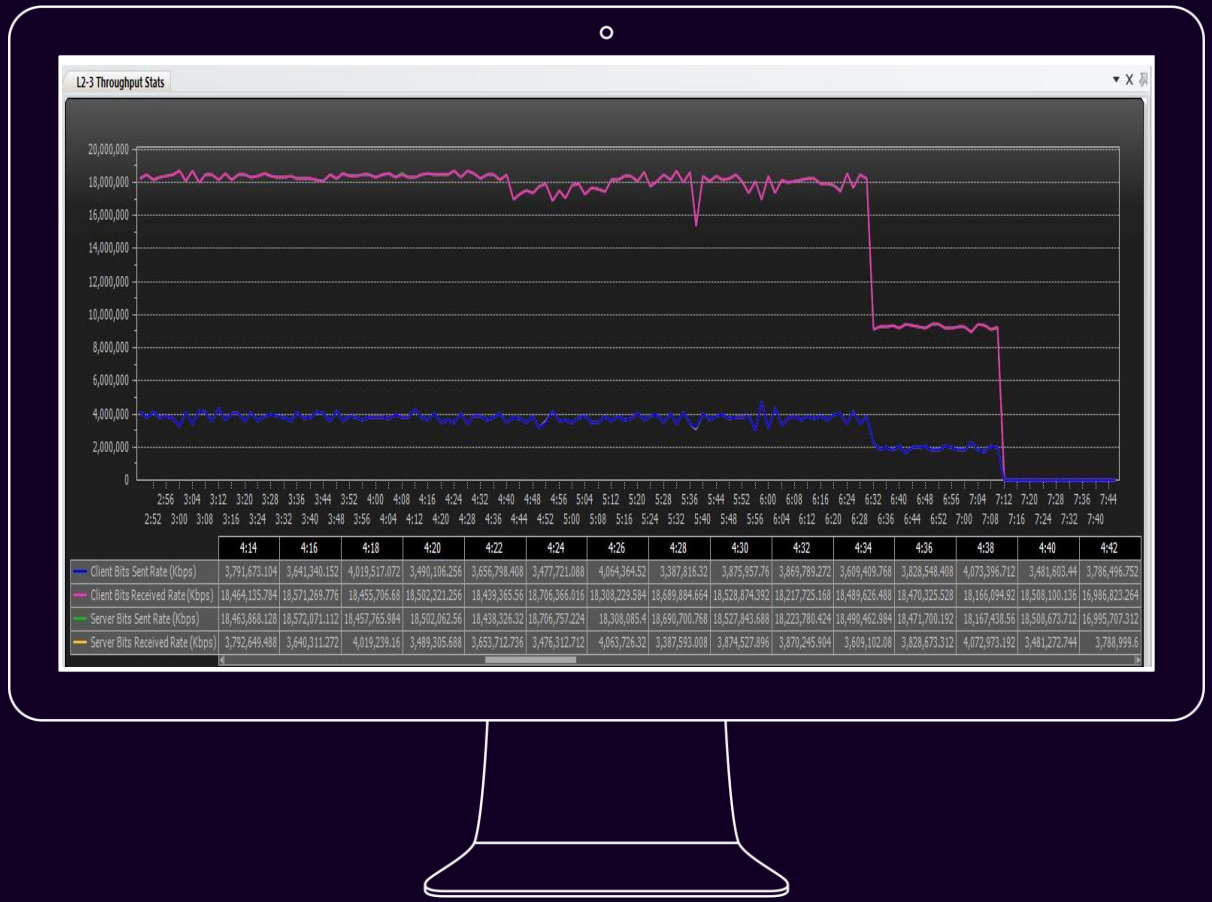
Производительность

Условия тестирования

Протокол/Приложение	Порт	Доля Throughput, %
HTTPS	TCP/443	32,26
SMB/CIFS (MS DS)	TCP/445	30,48
HTTP	TCP/80	5,37
Citrix	TCP/1494	6,94
RDP	TCP/3389	1,4
DNS	UDP/53	0,3
SNMP	UDP/161	1
Syslog	UDP/514	6,89
MS SQL	TCP/1433	9,7
Имитация VNC	TCP/8080	5,66

Проведенные тесты

Номер теста	Характеристика набора правил				Ожидаемая пропускная способность, не менее, Гбит/с	Зафиксированы результаты, Гбит/с
	Количество правил, не менее	Срабатывающее правило	IPS	DPI		
1	85 000	все	нет	да	20	22
2	85 000	все	да	да	10	12
3	85 000	последнее	нет	да	20	22
4	85 000	последнее	да	да	10	12

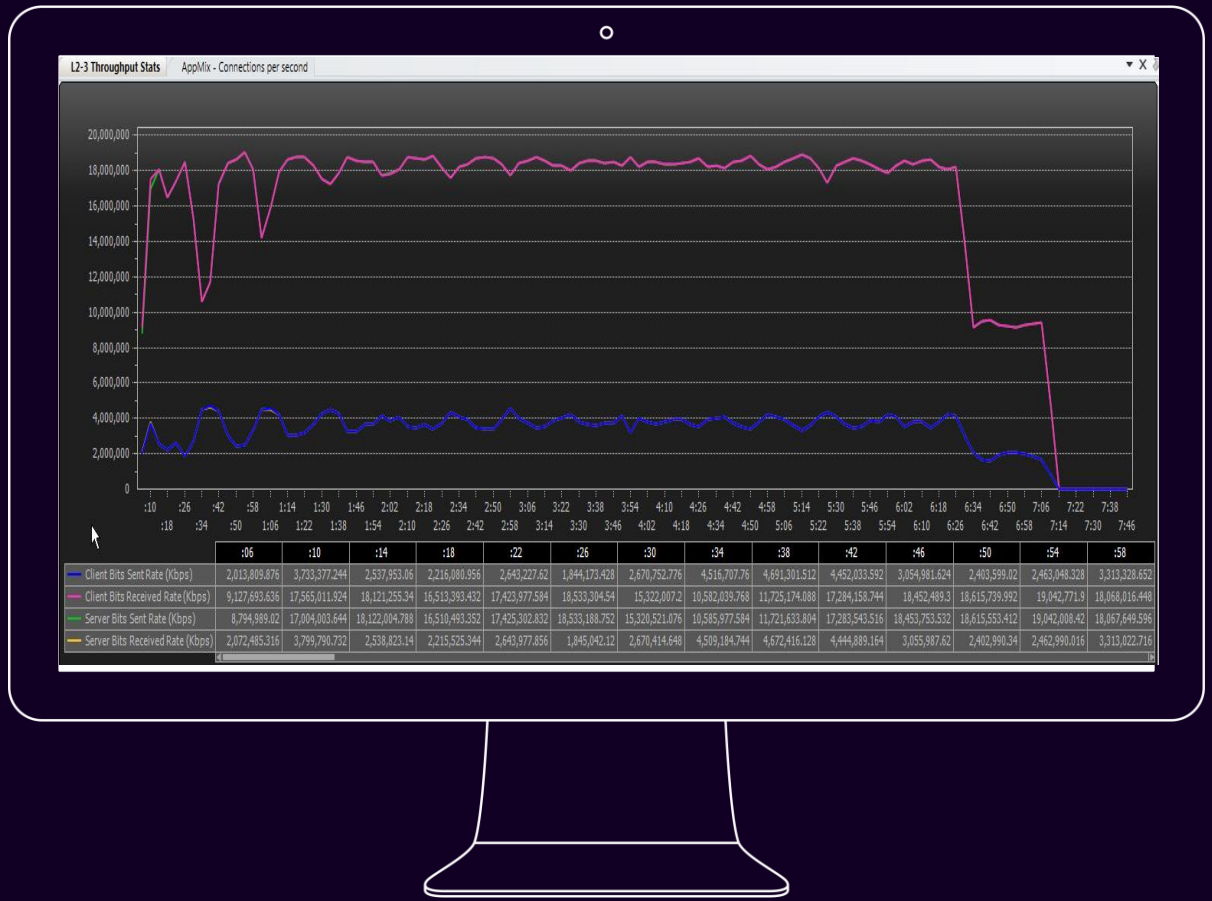


	4:14	4:16	4:18	4:20	4:22	4:24	4:26	4:28	4:30	4:32	4:34	4:36	4:38	4:40	4:42
Client Bits Sent Rate (Kbps)	3,791,673.104	3,641,340.152	4,019,517.072	3,490,106.256	3,656,798.408	3,477,721.088	4,064,364.52	3,387,816.32	3,875,957.76	3,869,789.272	3,609,409.768	3,828,548.408	4,073,396.712	3,481,603.44	3,786,496.752
Client Bits Received Rate (Kbps)	18,464,135.784	18,571,269.776	18,455,706.68	18,502,321.256	18,439,365.56	18,706,366.016	18,308,229.584	18,689,894.664	18,528,874.392	18,217,725.168	18,489,626.488	18,470,325.528	18,166,094.92	18,508,100.136	16,986,823.264
Server Bits Sent Rate (Kbps)	18,463,868.128	18,572,071.112	18,457,765.984	18,502,062.56	18,438,326.32	18,706,757.224	18,308,085.4	18,690,700.768	18,527,843.688	18,223,780.424	18,490,462.984	18,471,700.192	18,167,438.56	18,508,673.712	16,995,707.312
Server Bits Received Rate (Kbps)	3,792,649.488	3,640,311.272	4,019,239.16	3,489,305.688	3,653,712.736	3,476,312.712	4,063,726.32	3,387,593.008	3,874,527.896	3,870,245.904	3,609,102.08	3,828,673.312	4,072,973.192	3,481,272.744	3,788,999.6

График теста №1

График теста №2

	5:34	5:38	5:42	5:46	5:50	5:54	5:58	6:02	6:06	6:10	6:14	6:18	6:22	6:26
Client Bits Sent Rate (Kbps)	2,402,467.44	2,684,556.652	2,720,825.78	2,629,699.276	2,568,169.636	2,904,204.392	2,688,693.692	2,686,762.296	2,486,396.964	2,760,101.076	2,611,524.396	2,718,202.768	2,425,156.348	2,616,753.728
Client Bits Received Rate (Kbps)	12,859,651.412	13,446,219.088	12,943,874.736	12,763,770.824	12,725,219.728	11,682,801.132	12,935,113.276	13,754,359.88	12,450,880.444	13,240,390.736	12,474,129.324	12,902,042.852	12,266,218.616	13,274,975.188
Server Bits Sent Rate (Kbps)	12,856,312.604	13,446,678.748	12,938,347.444	12,761,757.828	12,723,342.932	11,678,862.884	12,933,230.24	13,749,975.064	12,447,477.276	13,235,814.64	12,468,318.452	12,901,911.632	12,262,395.004	13,274,054.412
Server Bits Received Rate (Kbps)	2,402,920.356	2,684,896.524	2,716,137.724	2,628,462.84	2,563,625.68	2,903,890.872	2,690,059.252	2,687,642.444	2,485,279.136	2,755,799.704	2,610,362.924	2,720,082.148	2,422,233.652	2,615,842.696



	:06	:10	:14	:18	:22	:26	:30	:34	:38	:42	:46	:50	:54	:58
Client Bits Sent Rate (Kbps)	2,013,809.876	3,733,377.244	2,537,953.06	2,216,080.956	2,643,227.62	1,844,173.428	2,670,752.776	4,516,707.76	4,691,301.512	4,452,033.592	3,054,981.624	2,403,599.02	2,463,048.328	3,313,328.652
Client Bits Received Rate (Kbps)	9,127,693.636	17,565,011.924	18,121,255.34	16,513,393.432	17,423,977.584	18,533,304.54	15,322,007.2	10,582,039.768	11,725,174.088	17,284,158.744	18,452,489.3	18,615,739.992	19,042,771.9	18,068,016.448
Server Bits Sent Rate (Kbps)	8,794,989.02	17,004,003.644	18,122,004.788	16,510,493.352	17,425,302.832	18,533,188.752	15,320,521.076	10,585,977.584	11,721,633.804	17,283,543.516	18,453,753.532	18,615,553.412	19,042,008.42	18,067,649.596
Server Bits Received Rate (Kbps)	2,072,485.316	3,799,790.732	2,538,823.14	2,215,525.344	2,643,977.856	1,845,042.12	2,670,414.648	4,509,184.744	4,672,416.128	4,444,889.164	3,055,987.62	2,402,990.34	2,462,990.016	3,313,022.716

График теста №3

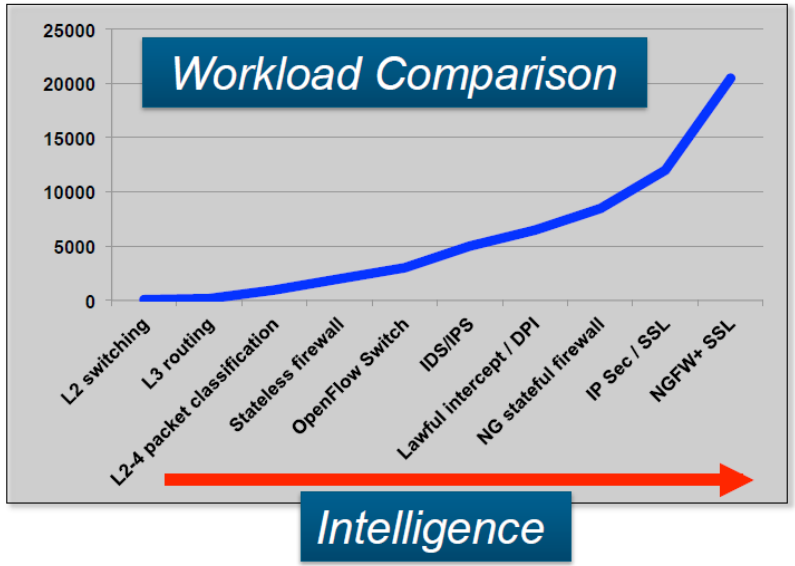
	:10	:14	:18	:22	:26	:30	:34	:38	:42	:46	:50	:54	:58	1:02
Client Bits Sent Rate (Kbps)	507,116.408	461,821.108	513,871.924	774,745.616	953,436.172	925,991.432	1,221,324.896	1,286,399.62	1,525,297.936	1,734,121.816	2,313,988.364	2,456,650.152	2,268,742.704	2,496,589.896
Client Bits Received Rate (Kbps)	1,262,810.668	1,722,143.936	2,870,245.02	6,463,853.532	10,105,433.136	8,533,951.06	10,698,603.368	8,434,513.44	8,885,096.036	10,777,928.772	12,871,577.948	14,116,601.364	11,275,245.708	12,763,806.064
Server Bits Sent Rate (Kbps)	1,262,484.72	1,722,366.872	2,871,600.792	6,464,097.624	10,102,546.336	8,531,644.908	10,694,985.18	8,438,115.64	8,883,335.416	10,781,082.072	12,870,581.848	14,115,385.02	11,271,670.984	12,762,894.244
Server Bits Received Rate (Kbps)	505,588.596	462,701.588	514,451.084	774,597.068	953,723.172	926,033.424	1,226,075.08	1,288,399.584	1,525,975.24	1,734,699.808	2,313,596.208	2,456,894.54	2,268,054.02	2,497,102.292

График теста №4

Производительность NGFW

Потребность в производительности

Function	Cycles required
L2 switching	75
L3 routing	200
L2-4 packet classification	1,000
Stateful firewall	2,000
OpenFlow Switch	3,000
IDS/IPS	5,000
Lawful intercept / DPI	6,500
NG stateful firewall	8,500
IP Sec / SSL	12,000
NGFW+ SSL	20,500

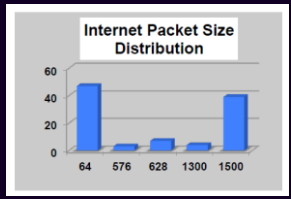


NGFW+SSL Inspection требуют в 10 раз больше вычислительной мощности по сравнению с обычным МЭ.

Что может процесс Intel в NGFW

Intel Xeon 5645

- • 6 cores @ 2.4 Ghz
- • 14.4 billion instructions per second



Instructions Required for line rate operation @ 10 Gbps

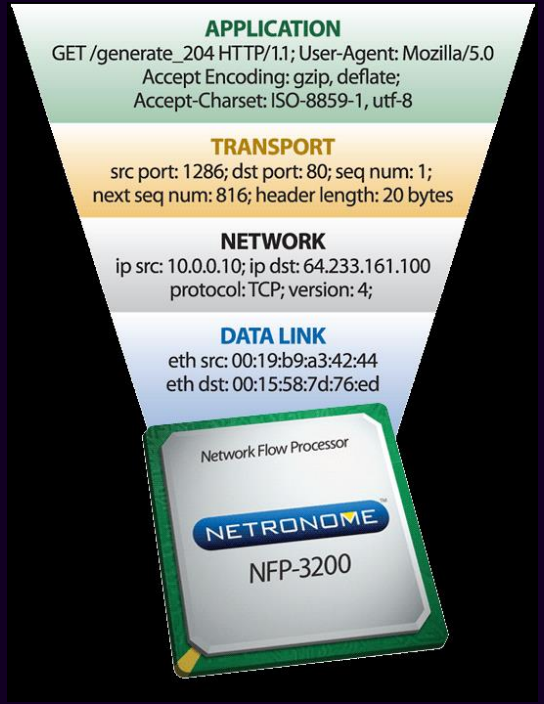
Packet Size	L2 switching	L3 routing	L2-L4 classification	Stateful firewall	IDS/IPS	Lawful Intercept / DPI	NG stateful firewall	IP Sec / SSL	NGFW + SSL
64	1.12 B	2.98 B	14.9 B	29.8 B	74.4 B	96.7 B	126.5 B	178.6 B	305.1 B
128	633 M	1.69 B	8.5 B	16.9 B	42.3 B	54.9 B	71.8 B	101.4 B	173.1 B
256	340 M	906 M	4.5 B	9.1 B	22.6 B	29.4 B	38.5 B	54.3 B	92.8 B
440	204 M	543 M	2.7 B	5.4 B	13.6 B	17.7 B	23.1 B	32.6 B	55.7 B
512	176M	470 M	2.4 B	4.7 B	11.7 B	15.3 B	19.9 B	28.2 B	48.2 B
1024	143 M	383 M	1.9 B	3.8 B	9.6 B	12.5 B	16.3 B	23.0 B	39.3 B
1500	61 M	163 M	813 M	1.6 B	4.1 B	5.3 B	6.9 B	9.8 B	16.7 B

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

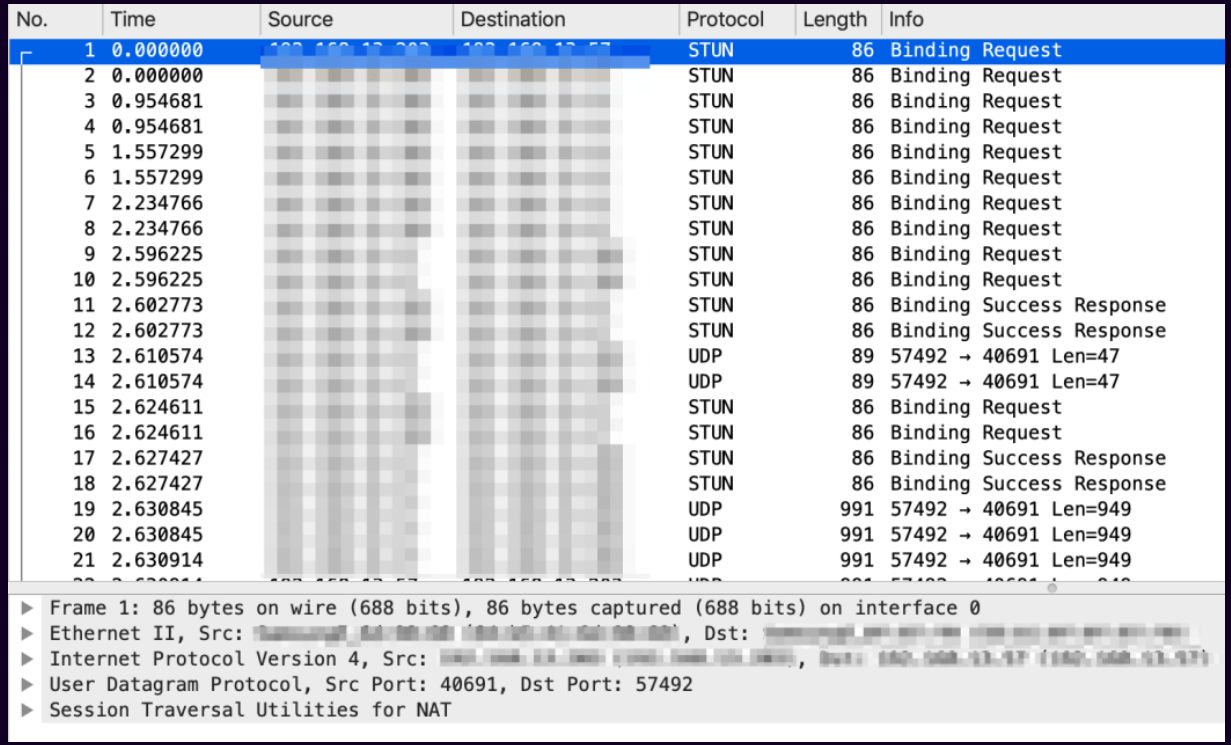
L7 сессия – приложение - L4+L6+L7 = 40 + 1500 байт



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.



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

Что влияет на производительность

CPU →

- Elephant flows
- Распределение нагрузки между CPU
- Connection per second

Memory →

- Количество политик и/или правил
- Кол-во одновременно обслуживаемых сессий

Скорость и/или пропускная способность →

- Тип трафика (HTTP или EMIX)
- Включенные функции (расшифровка SSL, IPS, DPI, Антивирус и т.д.)
- Доступность свободных ресурсов: CPU, RAM

Покупатели считают, что их вводят в заблуждение

А на сайте обещали другое

Зато порция большая

UDP самый простой тест

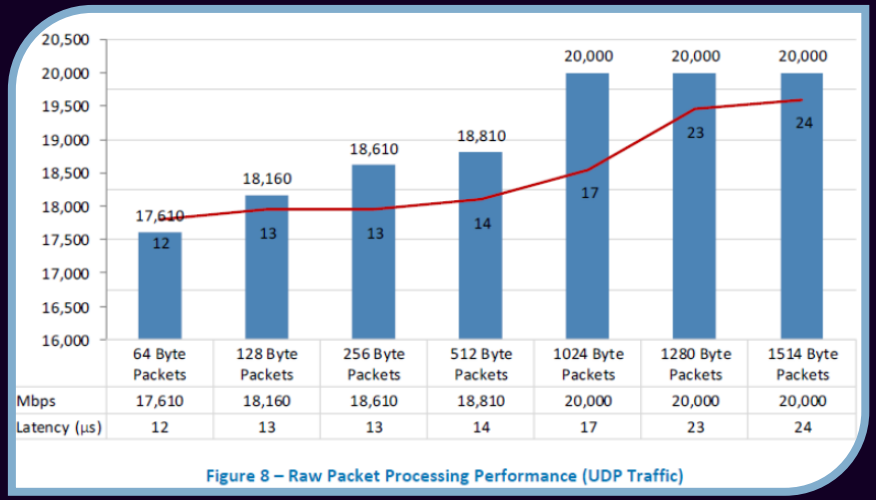
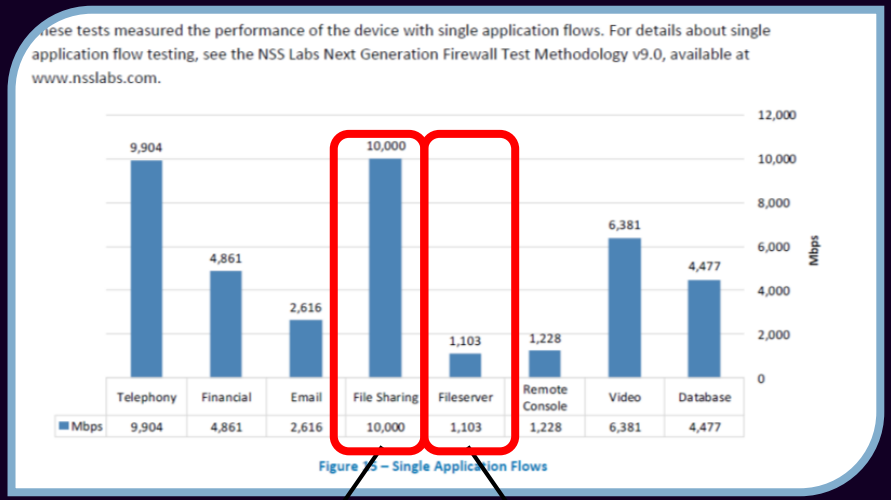


Figure 8 – Raw Packet Processing Performance (UDP Traffic)

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

Разные приложения – разная скорость



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


У вас прекрасные результаты!
Как вы их достигли?
Мы просто неправильно считаем

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

Кол-во правил **максимум 562**

Реальный заказчик

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

Профиль трафика

infotecs

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

infotecs

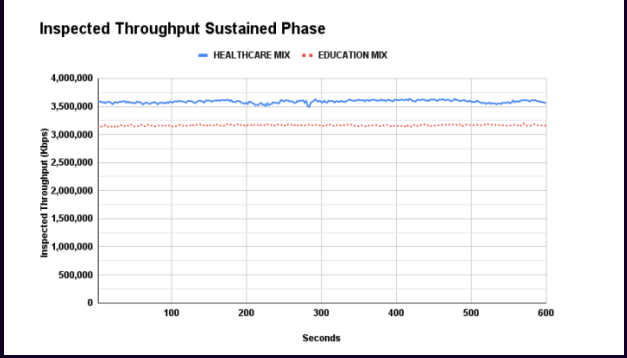
Самая жесткая методика по RFC 9411

Реальный заказчик

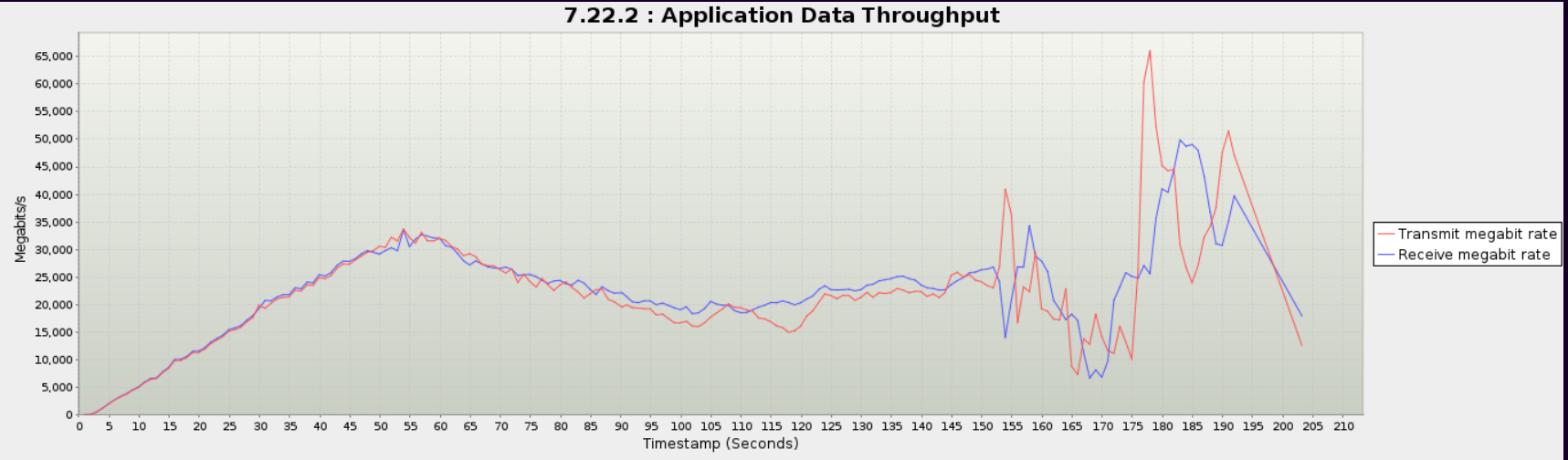
Logging and reporting MUST be enabled

Должно быть включено журналирование всего

Продолжительность теста



The minimum RECOMMENDED time duration for the sustain phase is 300 seconds.



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

Казалось бы, победитель известен до старта

Тест «Идеальные условия»

infotecs

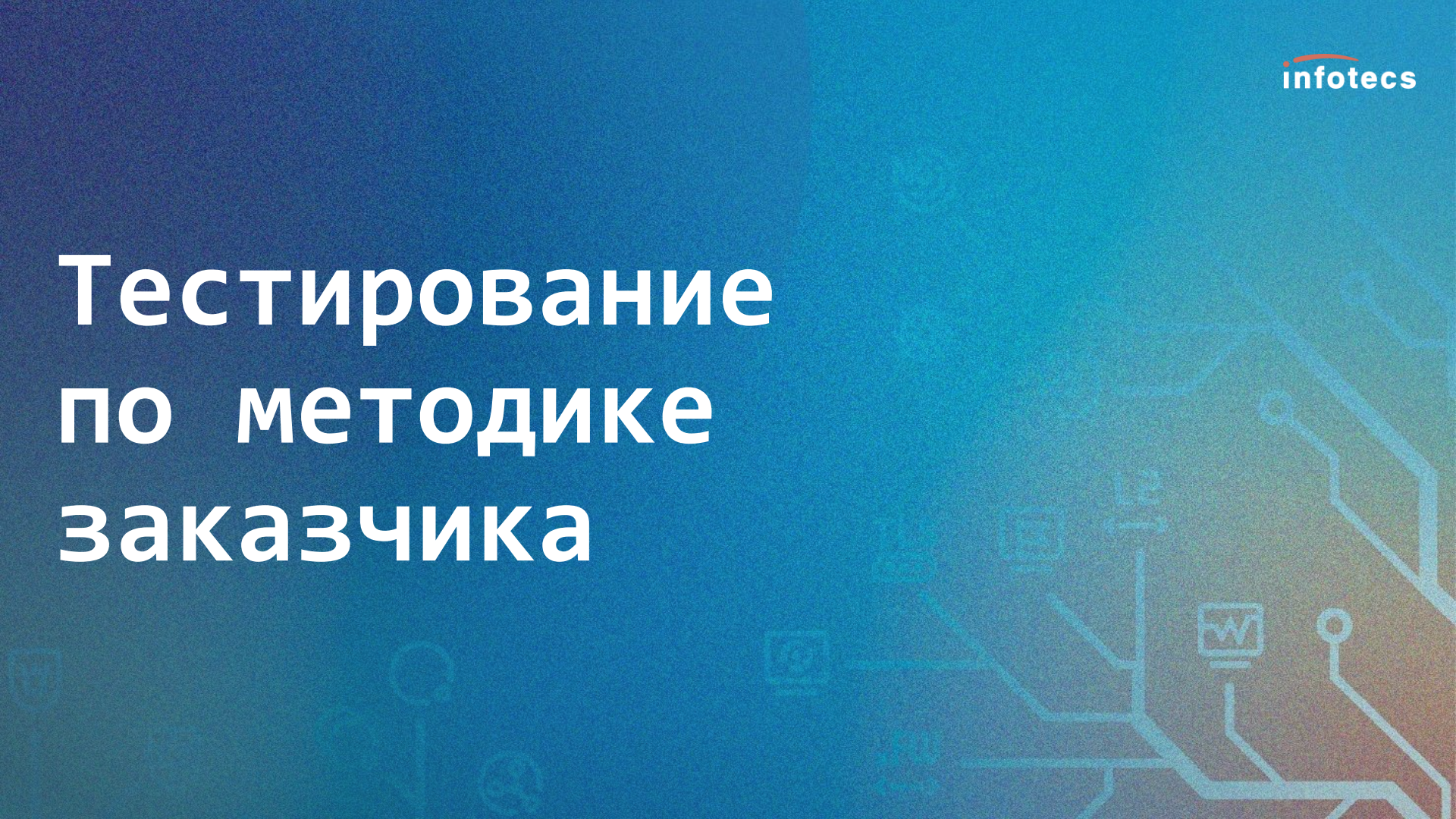
	Производитель А	Производитель Б
МЭ, 1518 байт UDP	45 Гбит/сек	38,2 Гбит/сек
МЭ (пакетов/сек)	4 млн	4,4 млн
Соединений в секунду	85 000	259 000
МЭ, TCP	30 Гбит/сек	34,5 Гбит/сек

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

infotecs

Спасибо за внимание!