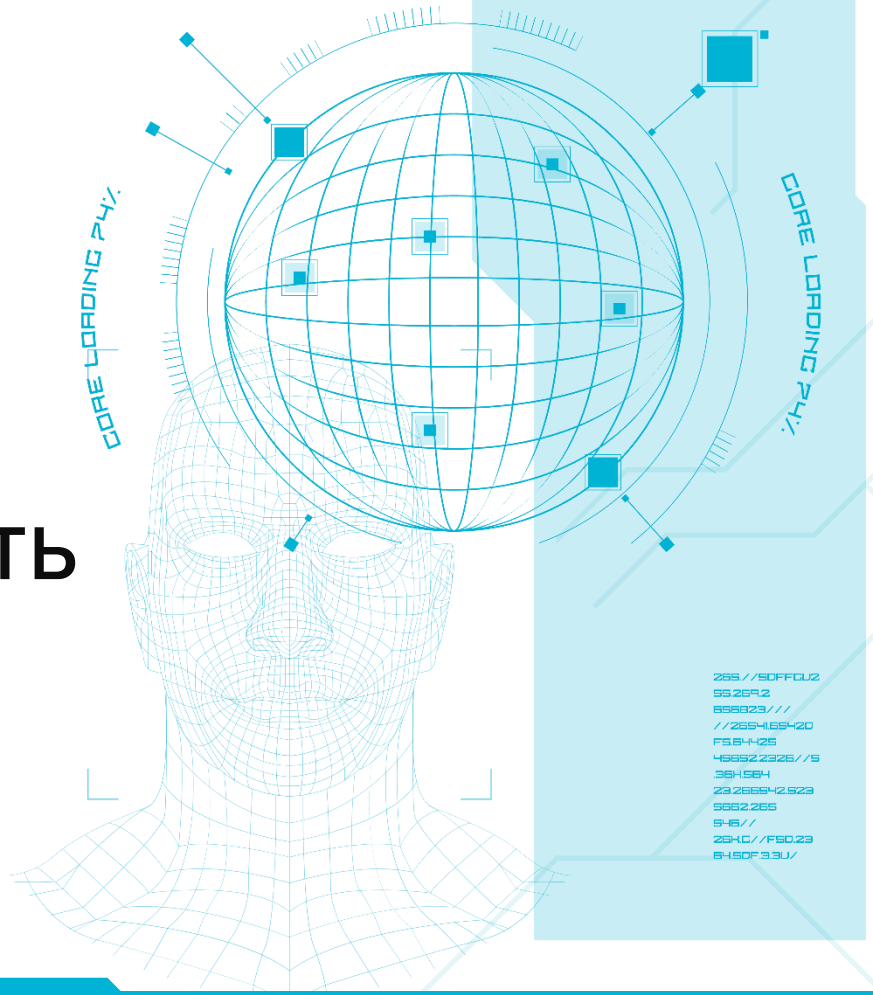
Алексей Данилов
руководитель продуктового направления

Декларации и реальные измерения производительности NGFW

Как сравнивать продукты по данным с сайтов?



2023 infotecs
ПАРТНЕРСКАЯ КОНФЕРЕНЦИЯ

2023 infotecs
ПАРТНЕРСКАЯ КОНФЕРЕНЦИЯ

У всех свои методики

Cisco	Palo Alto Networks	Check Point
Cisco uses a variety of testing methodologies in a lab environment to ensure the performance specifications we report are as close to real world as possible. Firewall performance is affected by many factors including network environment, packet sizes, packet type, TLS encryption, and more	Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions. † Threat Prevention throughput is measured with App-ID, IPS, antivirus, antispyware, WildFire, DNS Security, file blocking, and logging enabled, utilizing 64 KB HTTP/appmix transactions.	RFC 3511, 2544, 2647, 1242 Performance (Lab) Enterprise Test Conditions

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.

Методика NSS Labs открыта

По ней были протестированы все мировые лидеры рынка

Почему мы выбрали этот вариант

NSS Labs использует те же инструменты Ixia или конкурирующие Spirent.

Почему важен профиль трафика

UDP самый простой тест

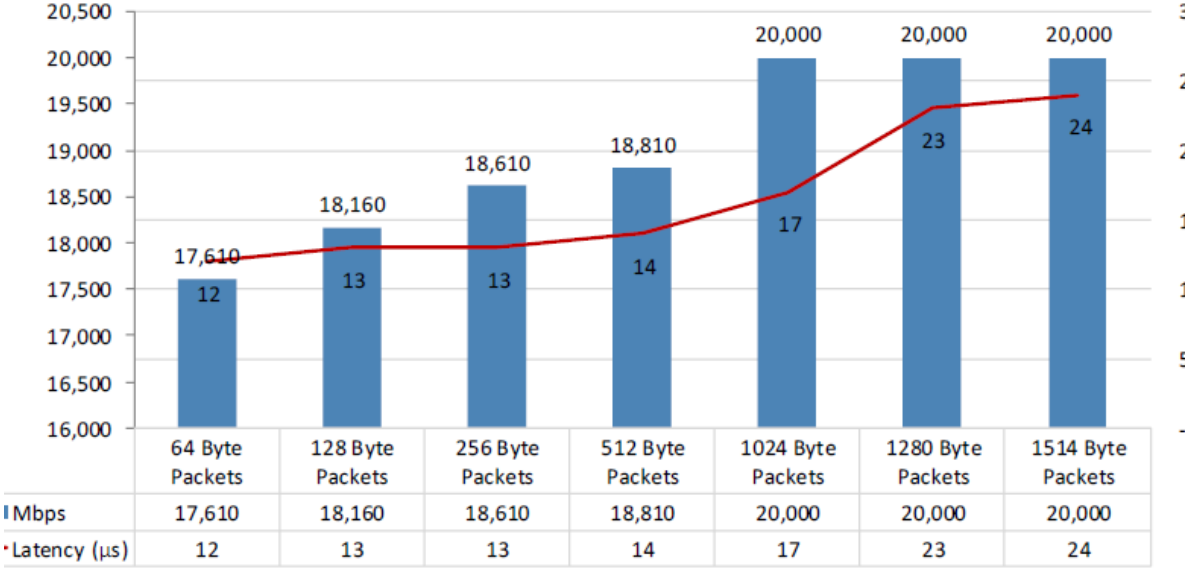


Figure 8 – Raw Packet Processing Performance (UDP Traffic)

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

UDP самый простой тест

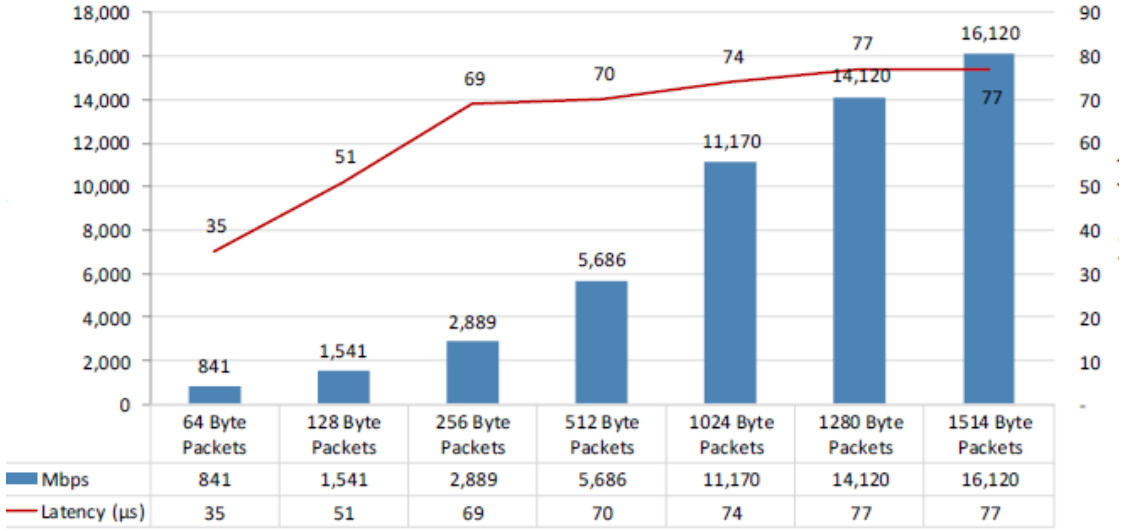


Figure 8 – Raw Packet Processing Performance (UDP Traffic)

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.

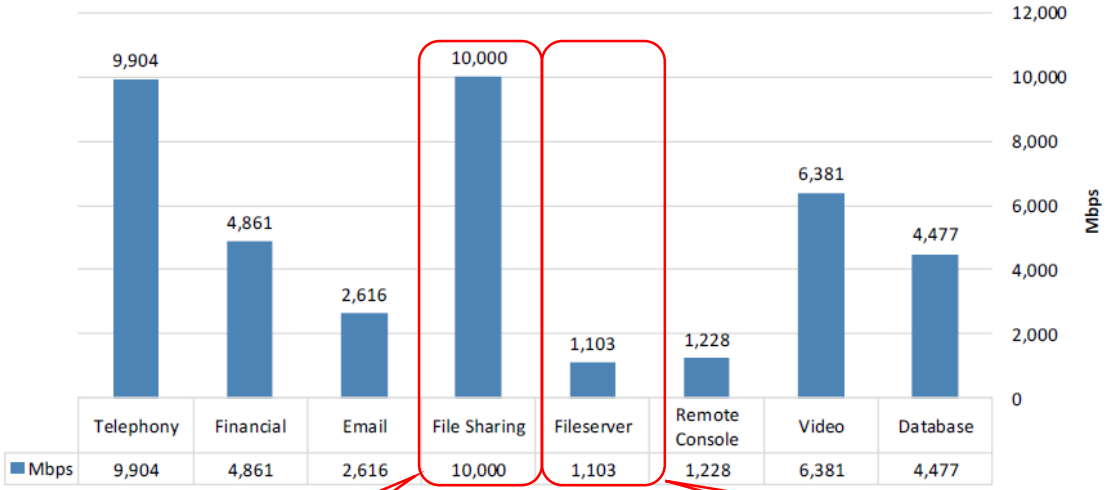


Figure 15 – Single Application Flows

FTP

SMB

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

Разные приложения – разная скорость

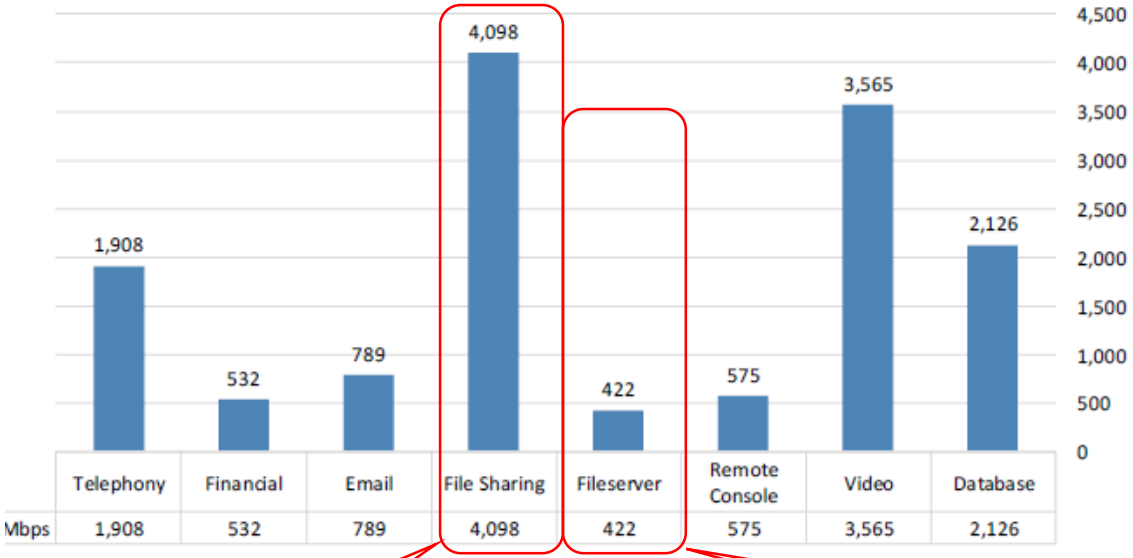


Figure 15 – Single Application Flows

FTP

SMB

Check Point Software Technologies 6500 Security Gateway R80.20

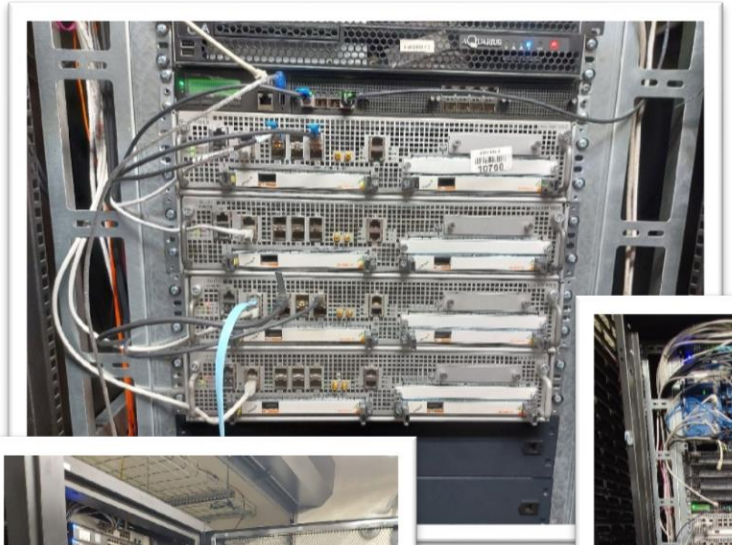
https://t.me/joinchat/CDUYdxTN_XHObkPRIyf9NA

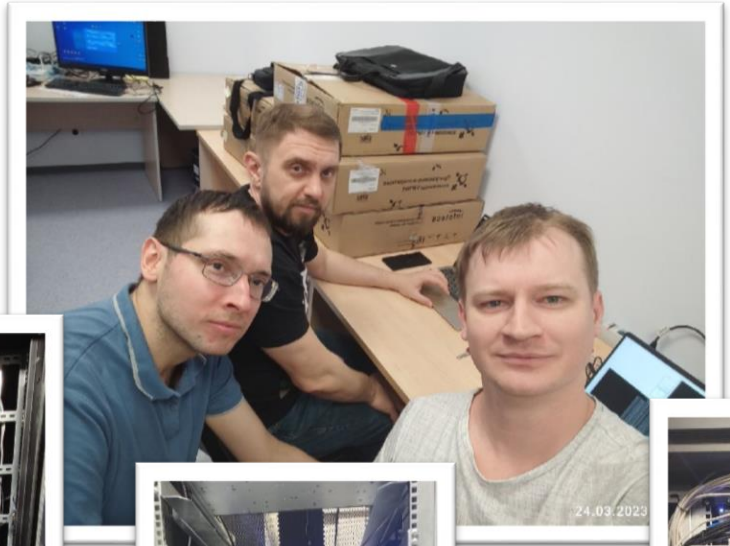
BDV 11:09:07 PM

самый идеальный по моему мнению тест - это использовать устройства типа Network TAP и при помощи них подавать свой реальный трафик в сети на несколько устройств разных производителей и смотреть как они загружаются от возложенных на них важных задач. так можно и песочницы и IPS и антивирусы и DLP тестировать.

в мире - те самые попугаи.
Пока что нет решения этой проблемы.

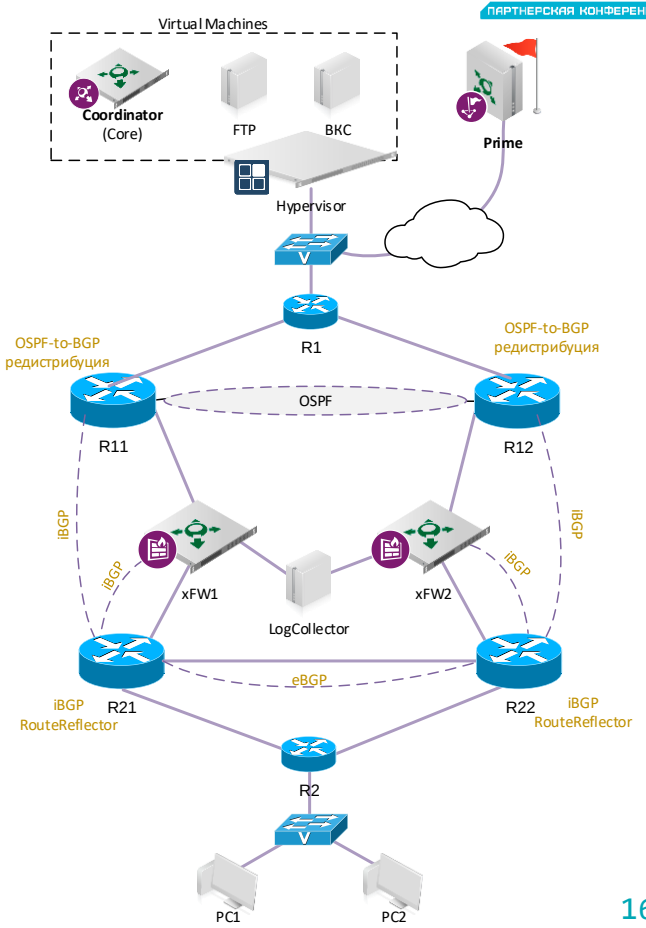
А в США в 1956 году джинсы стоили 5$




24.03.2023

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 остановил



Ближайшие мероприятия

21 сентября

Москва

Сравнительное тестирование по методике ИнфоТеКС

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

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

Данные с сайта

Исполнение	xF5000 Q2 ver. 5.6.0	UserGate E3000 ver. 6.1.9
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
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

Первые тесты

N	Метрика	Методика	ИнфоТеКС		UserGate E3000
			xF5 5000 Q2	Заявлено	Подтверждено
1.	МЭ, 1518 байт UDP (Мбит/сек)	P-P-UDP-Circuit	45 000	30 000	38 200
2.	МЭ (пакетов/сек)	P-P-UDP-Circuit	4 млн	не заявлено	4,4 млн
3.	Соединений в секунду	P-P-GENERIC-FIREWALL	85 000	127 000	259 000
4.	Обслуживаемых соединений	P-P-GENERIC-FIREWALL	9,9 млн	16 млн	16 млн
5.	МЭ, TCP (Мбит/сек)	P-P-TCP-40G	30 000	40 000	34 500

Тестирование

		Кол-во правил	Значение показателя, Gbps		Кол-во правил	Значение показателя, Gbps		Заявлено
			xF 5.6					
			NSS Labs	Заказчик		NSS Labs	Заказчик	
AppControl (Firewall+DPI), EMIX (Mbps)	P-P-AppMix	1	7,2	3,3	1	3,3	1,0	32
		51	6,8	3,2	51	3,1	1,0	
		101	6,6	3,0	101	3,1	1,0	
		501	6,4	2,3	501	UserGate искажает трафик	0,9	
		1001	5,5	1,7	1001	UserGate искажает трафик	0,8	
		11001	не проводился	0,3	11001	Отказ продукта	Отказ продукта	

		Кол-во правил	Значение показателя, Gbps		Кол-во правил	Значение показателя, Gbps		Заявлено, Gbps
			xF 5.6					
			NSS Labs	Заказчик		NSS Labs	Заказчик	
NGFW Throughput, EMIX (Mbps)	P-P-AppMix	1	1,2	0,7	1	0,6	0,6	3,9
		51	1,1	0,7	51	0,6	0,6	
		101	1,1	0,7	101	UserGate искажает трафик	0,6	
		501	1,1	0,7	501	UserGate искажает трафик	0,5	
		1001	1,1	0,6	1001	UserGate искажает трафик	0,5	
		11001	не проводился	0,2	11001	Отказ продукта	Отказ продукта	

TS Solution независимо протестировал

UserGate E1000 | E3000

Заказать

Производительность*

Межсетевой экран: до 30 Гб/с
Система обнаружения вторжений: до 1500 Мб/с
Advanced Threat Protection*: до 600 Мб/с
Потоковый антивирус*: до 600 Мб/с
Контроль Приложений L7: до 12 Гб/с
Антивирус с эвристическим анализом*: до 500 Мб/с

Размер организации*

[Купить UserGate у официального партнера. (tssolution.ru)]

2023 infotecs
ПАРТНЕРСКАЯ КОНФЕРЕНЦИЯ

Ответы на вопросы

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363

2023 infotecs
ПАРТНЕРСКАЯ КОНФЕРЕНЦИЯ

Спасибо за внимание!

При поддержке