# Что такое NGFW и как их выбирать?


Виталий Беличко
Ведущий менеджер продуктов

# История развития МЭ

# Next-Generation Firewall (NGFW)

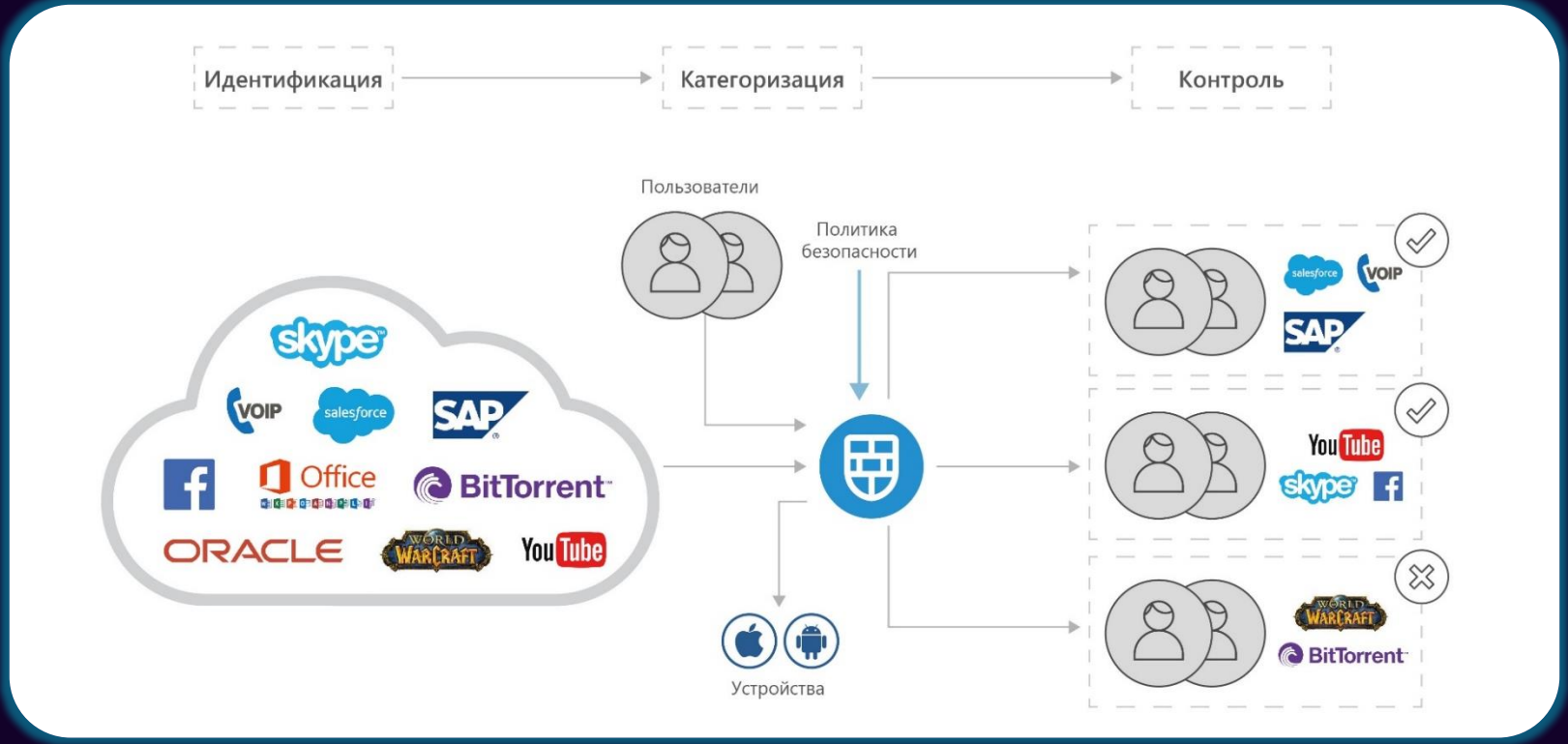
Gartner

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



# Основные модули безопасности

**Application Control**

**IDS/IPS**

**VPN**

**Аутентификация пользователей**

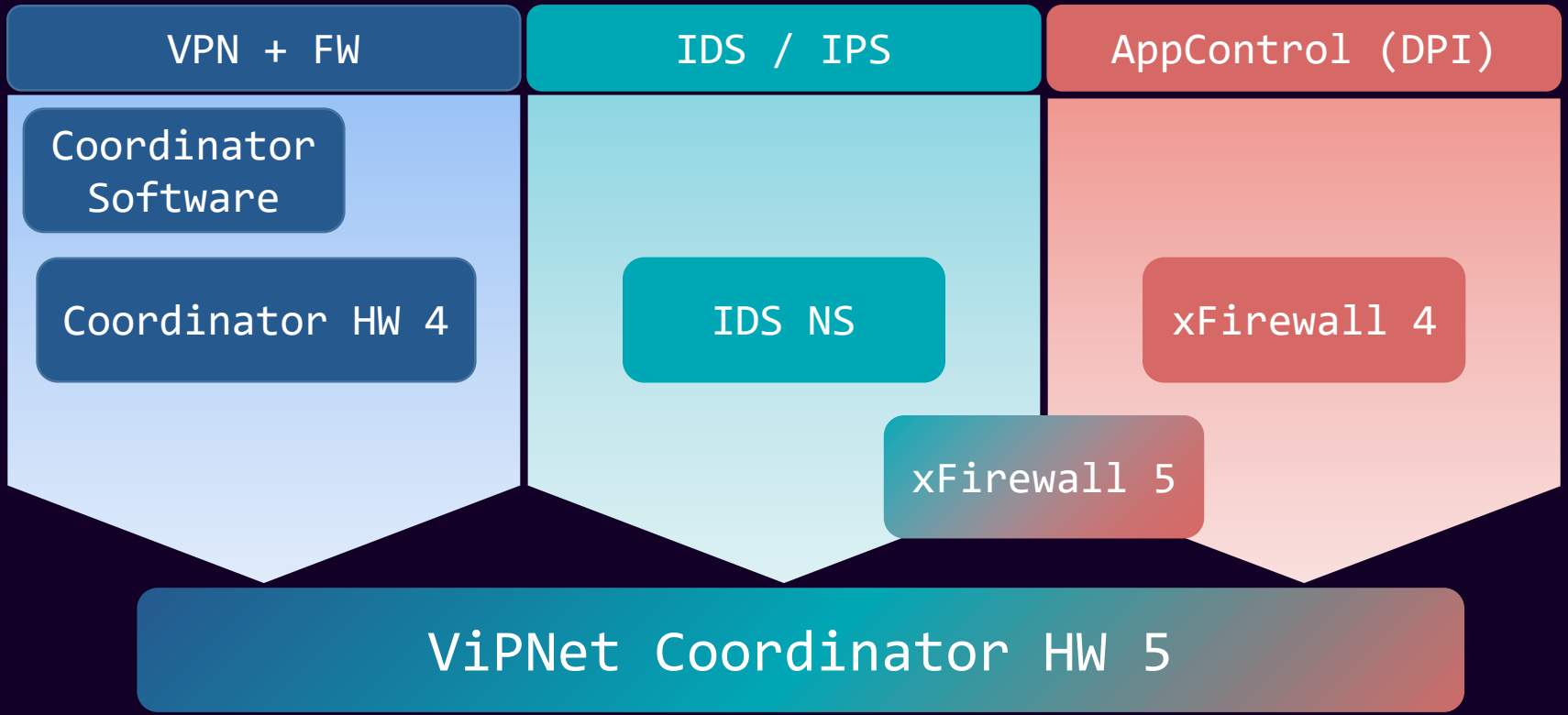
**Фильтрация по URL**

Инспектирование TLS

**Антивирус**

Антиспам

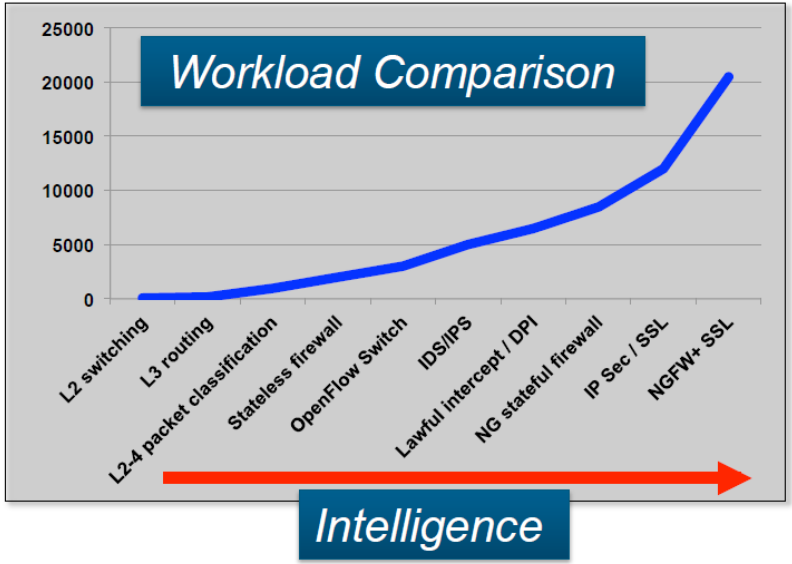
# Шлюзы безопасности ViPNet



# 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 |



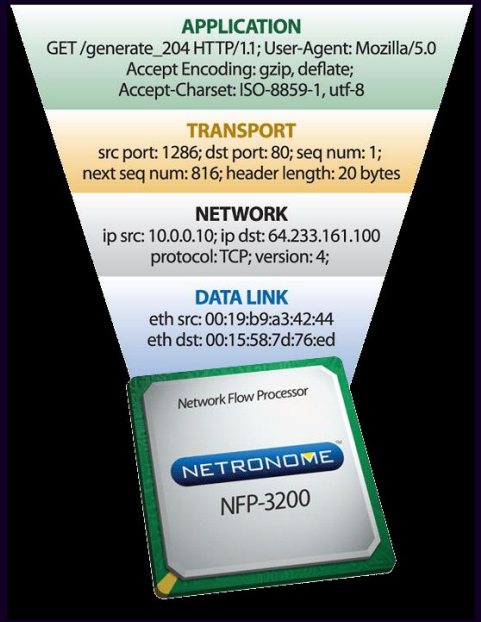

NGFW+SSL Inspection требуют в 10 раз больше вычислительной мощности по сравнению с обычным МЭ.

# Что 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 |

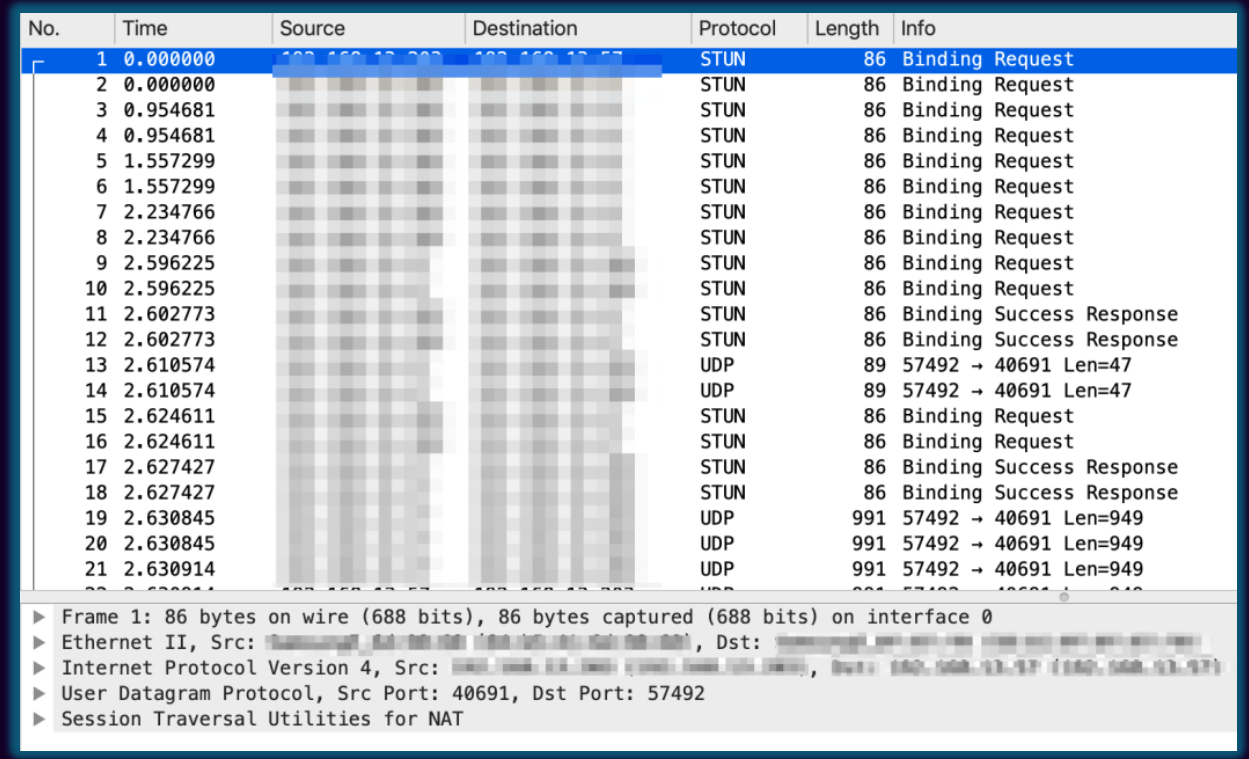
L7 сессия – приложение - L4+L6+L7 = 40 + 1500 байт



# 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 |

▶ 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

# 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

# Как сравнивать информацию из листовок?

# 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 (c) 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

# UDP самый простой тест

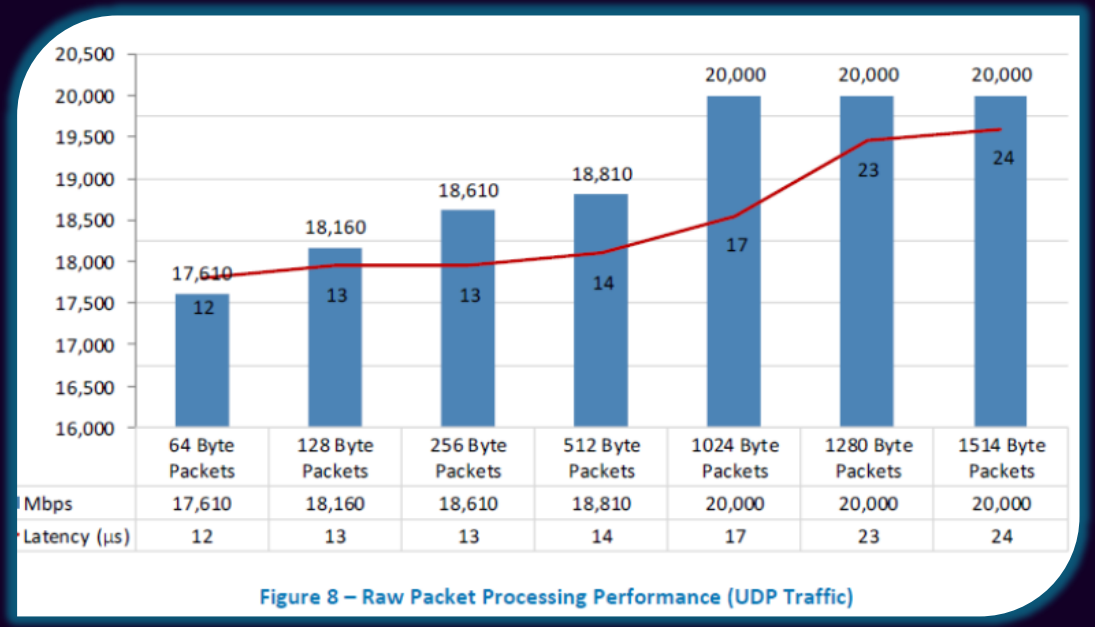



Figure 8 – Raw Packet Processing Performance (UDP Traffic)

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

# UDP самый простой тест

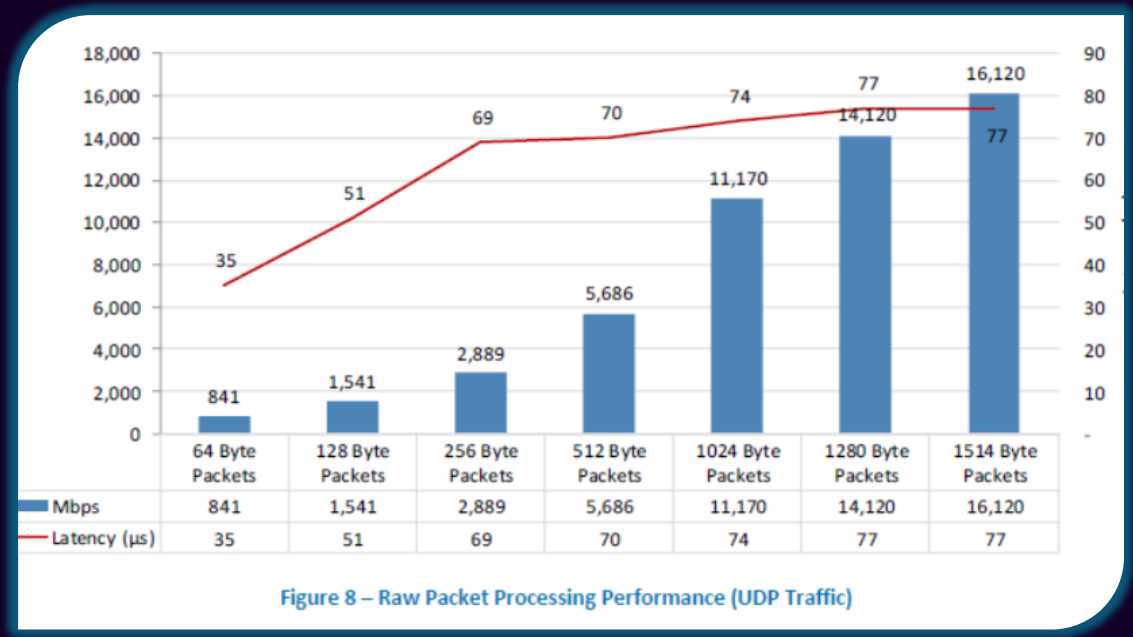
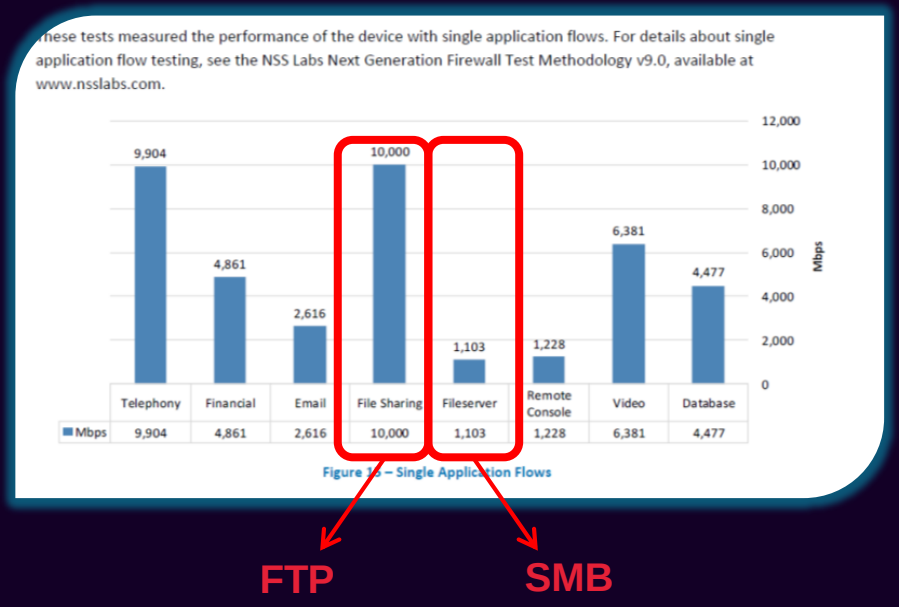



Figure 8 – Raw Packet Processing Performance (UDP Traffic)

Check Point Software Technologies 6500 Security Gateway R80.20

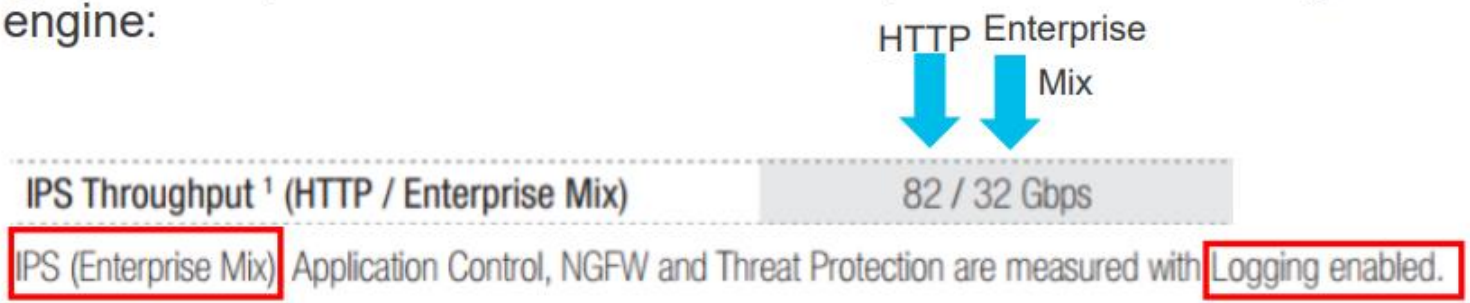
# Разные приложения – разная скорость




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

# 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 |

# 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 есть готовность в них разбираться, либо…**

# 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.

# 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 |

# ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного