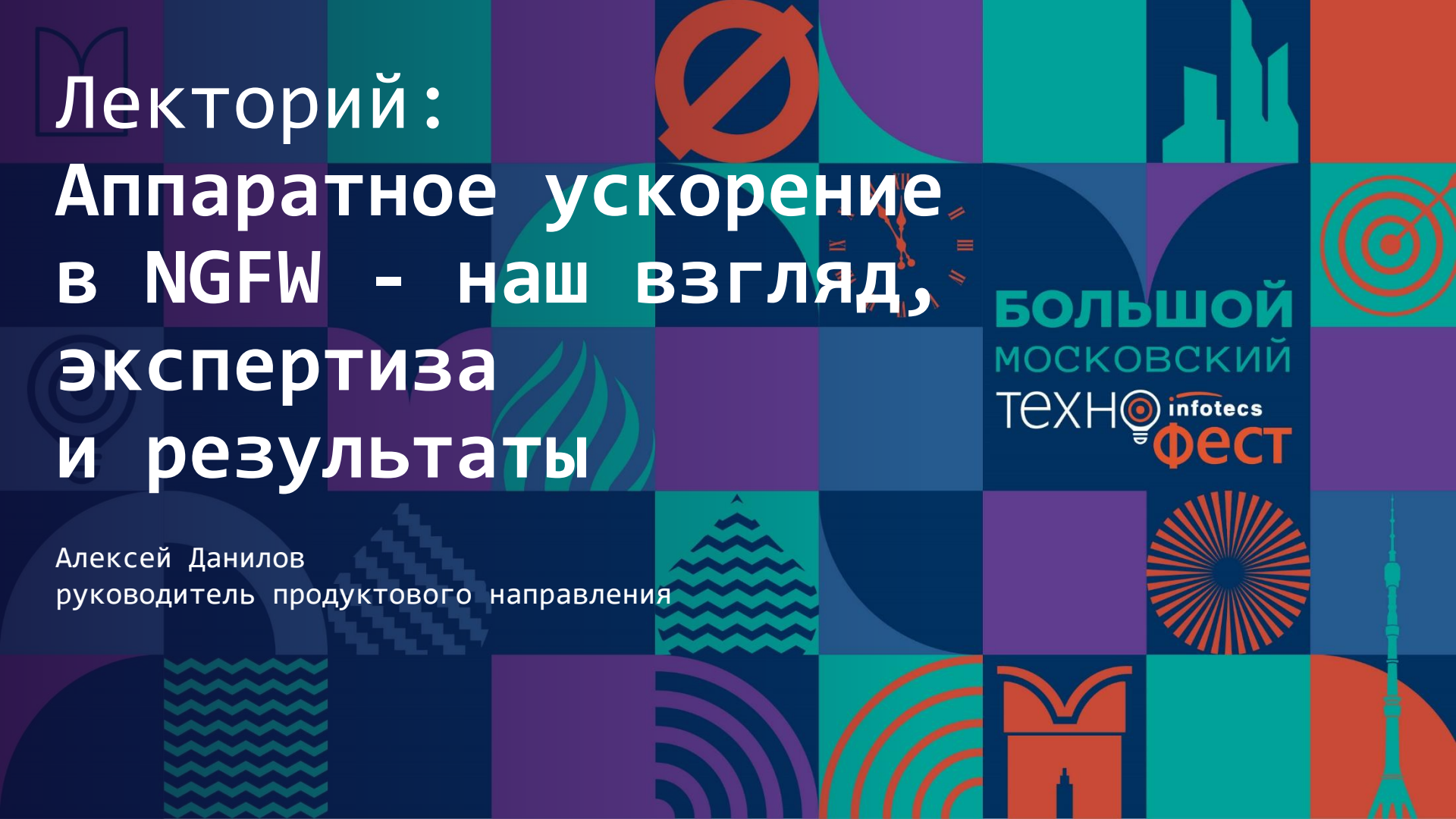
Лекторий:
Аппаратное ускорение в NGFW - наш взгляд, экспертиза и результаты

Алексей Данилов
руководитель продуктового направления



Чего достигло человечество к 2025 году

ТЕХНО infotecs ФЕСТ

О современной микроэлектронике

Основан на:
Дискретных компонентах

Частота:
1.024 Мгц

ПЗУ:
36 864 15-битных слов

ОЗУ:
2048 15-битных слов

Apollo Guidance Computer

Управлял командным и лунным модулями в ходе полётов по программе Аполлон

Имел **меньшую** производительность, чем

Основан на:
Cypress CYPD4225

Частота:
48 Мгц

ПЗУ:
8 КБайт

ОЗУ:
128 КБайт

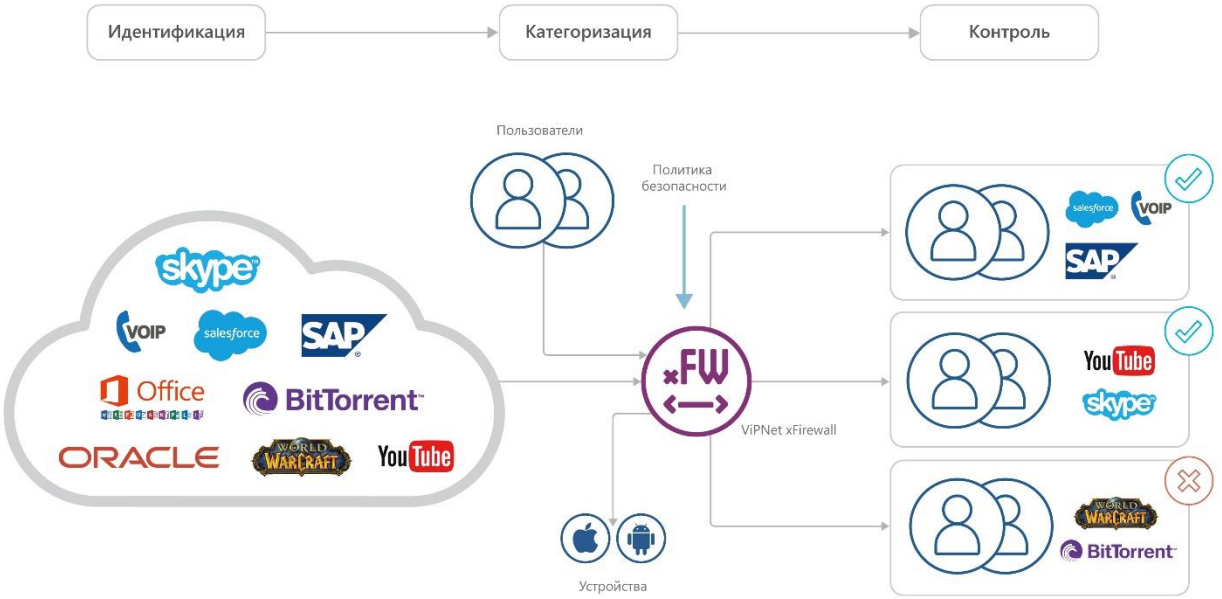
Зарядное устройство Anker USB-C, заряжает два телефона

В 563 раза быстрее

Полет на Луну 21 декабря 1968 года

NGFW глазами покупателя

Так представляется NGFW



Что такое NGFW с точки зрения «железа»

ТехноИнфотекс Фест

NGFW должен уметь

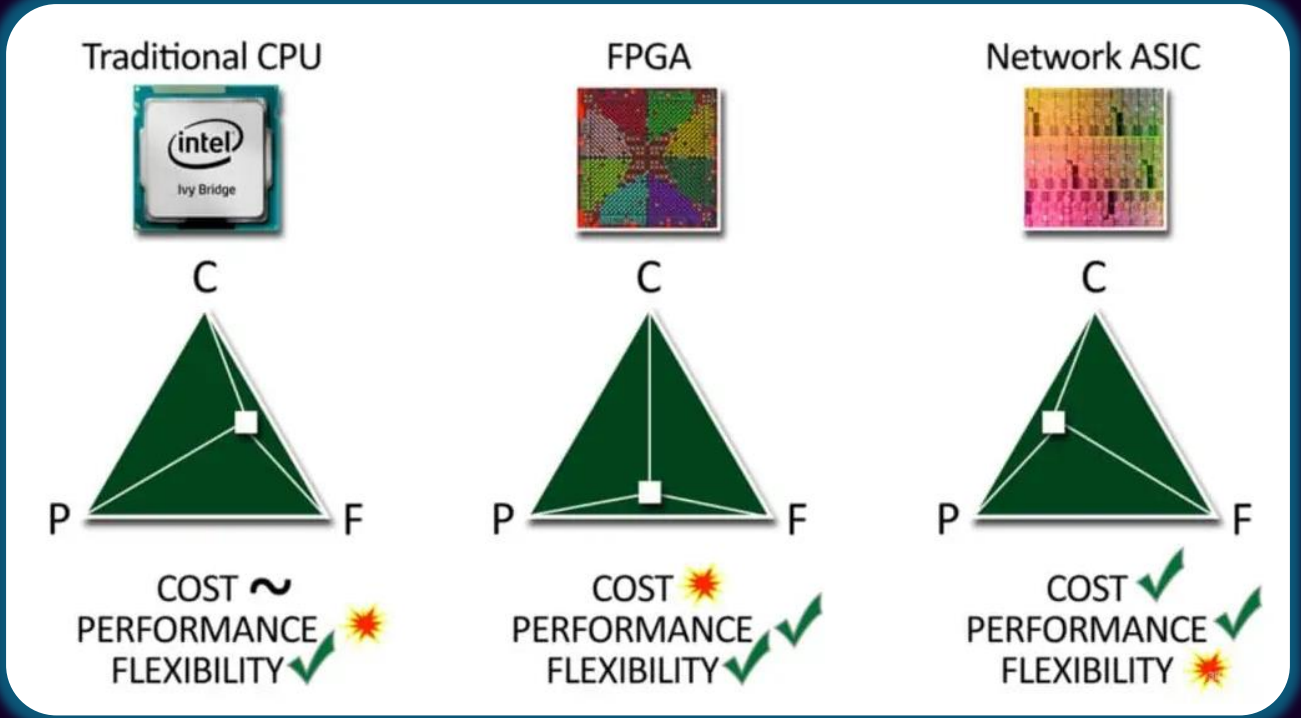
- Обрабатывать трафик на уровне L2-L4 (фильтрация по MAC, защита от DDoS, spoof-атак)
- Обеспечивать анализ на уровнях L4-L7:
  - Идентификация трафика приложений
  - Выявление атак сигнатурными и эвристическими методами (IPS, AntiVirus)
  - Анализировать содержимое трафика (URI, файлы и даже DLP)
- Анализироваться должен не ip-пакет, а сетевая сессия от старта до завершения.
- Расшифровывать трафик для анализа (SSL Inspection)
- Поддерживать I/O virtualization
- Поддерживать сетевые топологии: маршрутизация, в разрыв, коммутация, зеркалирование

NGFW - это еще и сетевое устройство

- Static routes
- BGP, MP-BGP
- OSPFv2, OSPFv3
- RIPv2
- IPv4 multicast routing
- BFD
- Redistribution
- DHCP
- DNS, DDNS
- ECMP
- LLDP
- GRE, VxLAN
- QoS

Виды аппаратных архитектур NGFW

Кратко


Traditional CPU
intel
Ivy Bridge
C
P
F
COST ~
PERFORMANCE
FLEXIBILITY
FPGA
C
P
F
COST
PERFORMANCE
FLEXIBILITY
Network ASIC
C
P
F
COST
PERFORMANCE
FLEXIBILITY

PA-5000 series

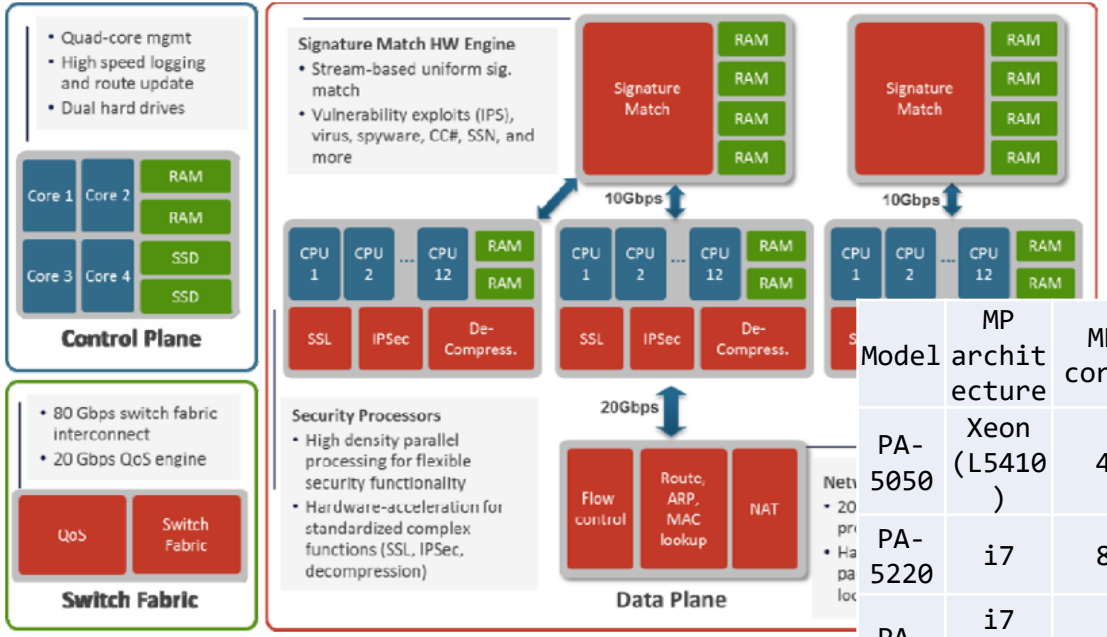
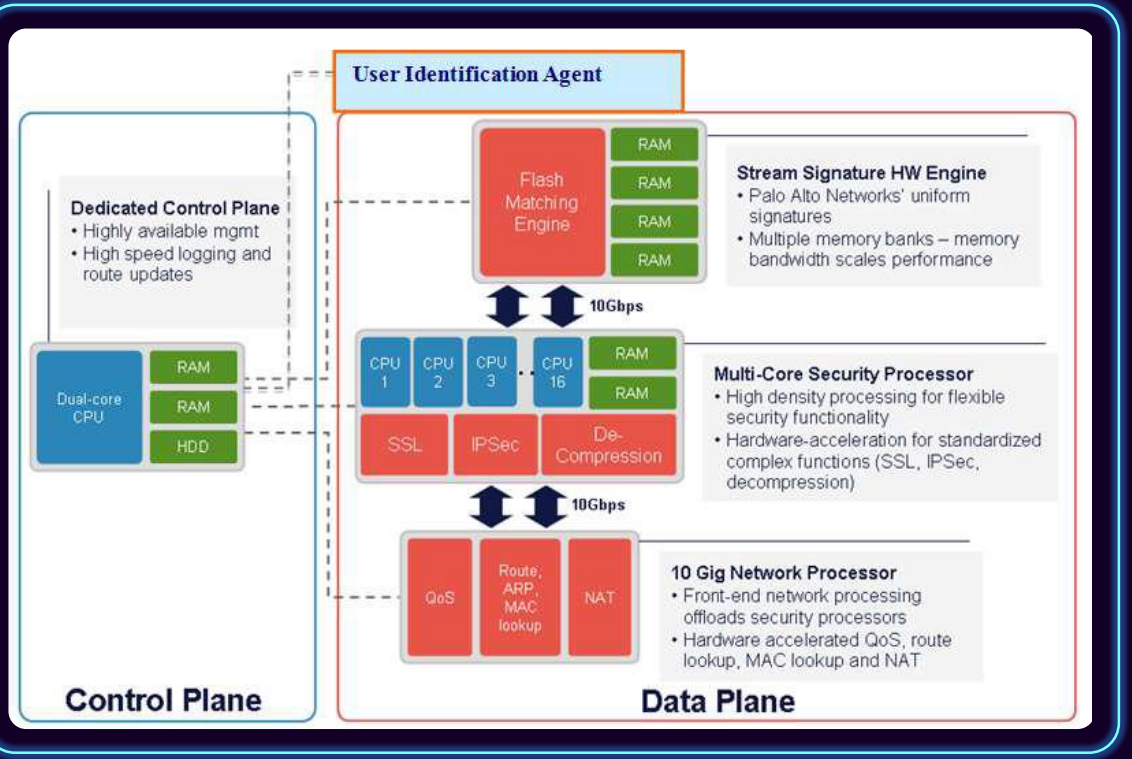


Image 3: PA-5000 Series hardware architecture.

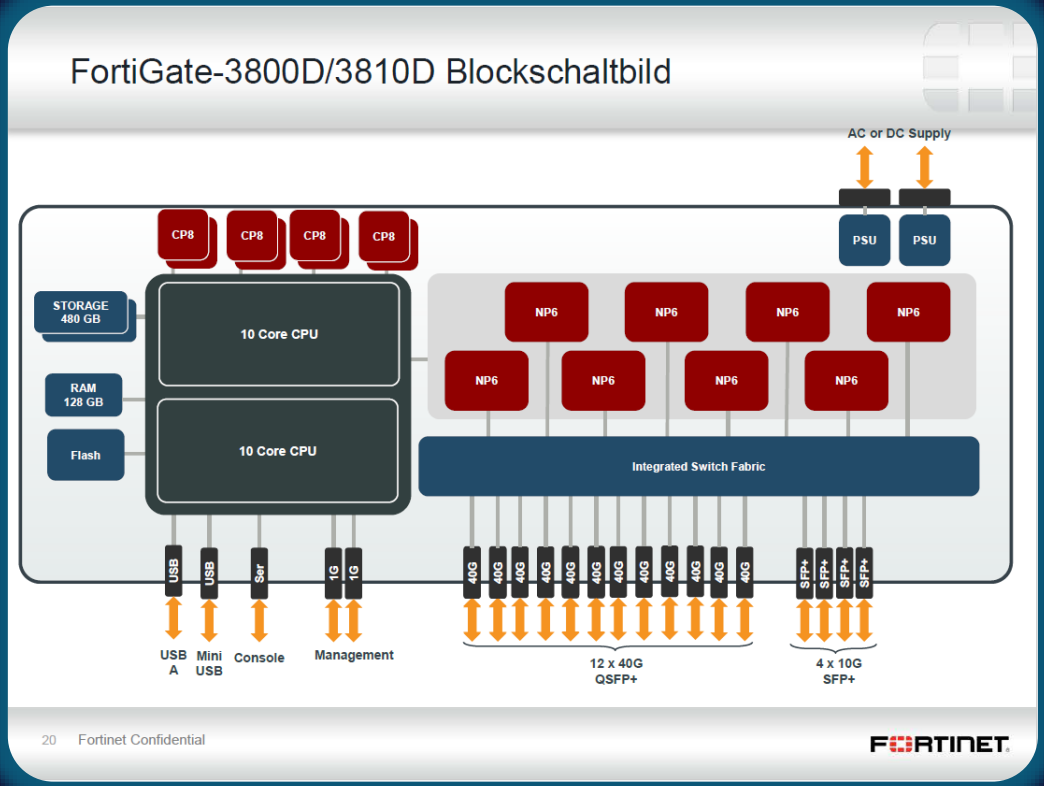
Model	MP architecture	MP cores	DP architecture	DP cores	DP Security	DP Signature	DP Network
PA-5050	Xeon (L5410)	4	CN5650	12	Cavium	FPGA	FPGA
PA-5220	i7	8	CN7885	40	Cavium	FPGA	FPGA
PA-7050	i7 (2715QE)	8	CN6880	32**	Cavium	FPGA	FPGA

PA-5200 series

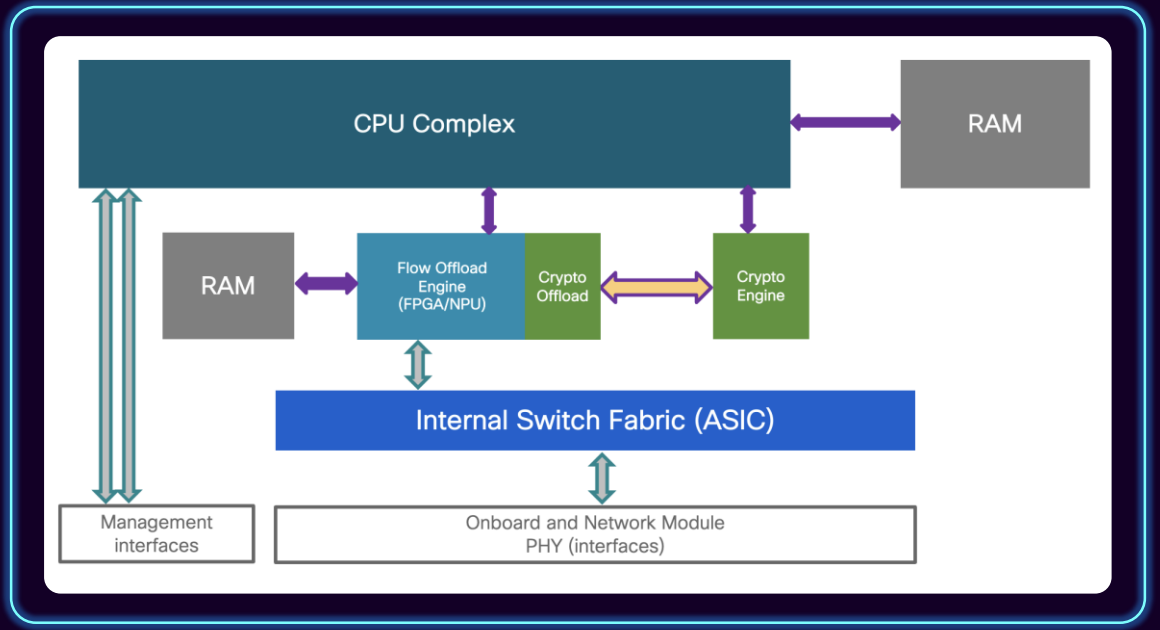


PA-5250: Processor: Cavium Octeon CN7890 MIPS64 (DP) / Intel Xeon D1567 (MP)

Fortigate


FortiGate-3800D/3810D Blockschaltbild
AC or DC Supply
PSU
PSU
CP8
CP8
CP8
CP8
STORAGE 480 GB
RAM 128 GB
Flash
10 Core CPU
10 Core CPU
NP6
NP6
NP6
NP6
NP6
NP6
NP6
NP6
Integrated Switch Fabric
USB
USB
Ser
1G
1G
40G
SFP+
USB A
Mini USB
Console
Management
12 x 40G QSFP+
4 x 10G SFP+
20
Fortinet Confidential
FORTINET

Cisco Secure Firewall



The 4200 Series appliances employ custom-built inline Field Programmable Gateway Array (FPGA) components to accelerate critical stateful inspection and cryptography functions directly within the data plane.

SmartNIC – Palo Alto

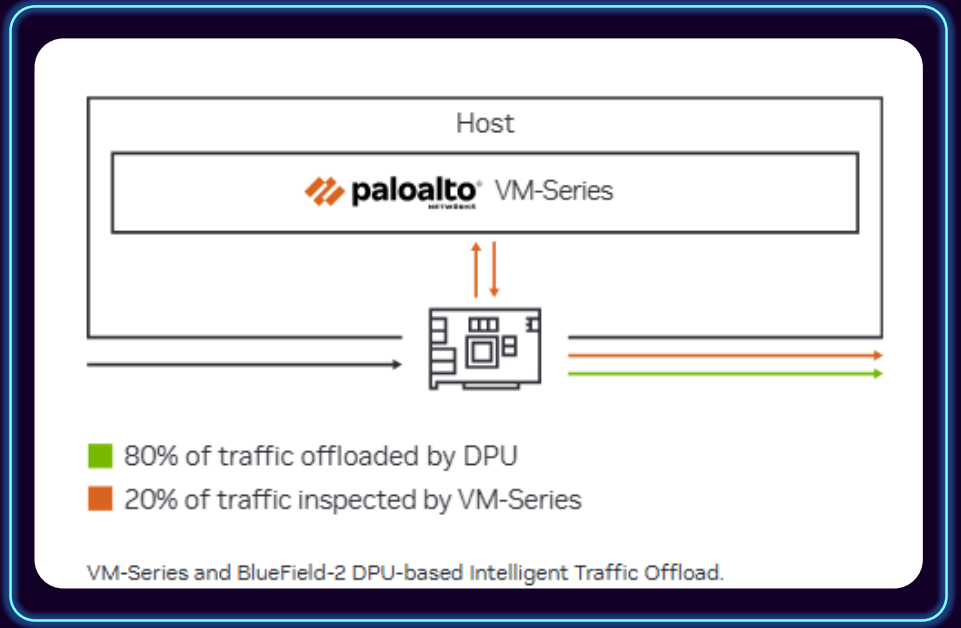
The current NVIDIA BlueField-2 DPU scalability limitations are as follows:

Session table capacity: 500,000 sessions

Session table update rate: 7000 sessions/second

Connections per second: 20,000

Offload hairpin rate: ~90 Gbps for 1500 byte packets



SmartNIC – Palo Alto

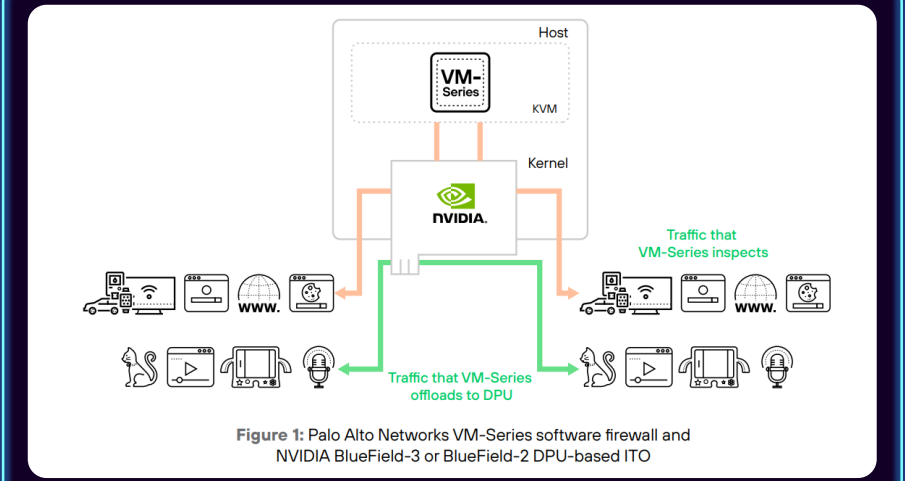


Figure 1: Palo Alto Networks VM-Series software firewall and NVIDIA BlueField-3 or BlueField-2 DPU-based ITO

The current NVIDIA BlueField-2 DPU scalability limitations are as follows:

Session table capacity: 500,000 sessions

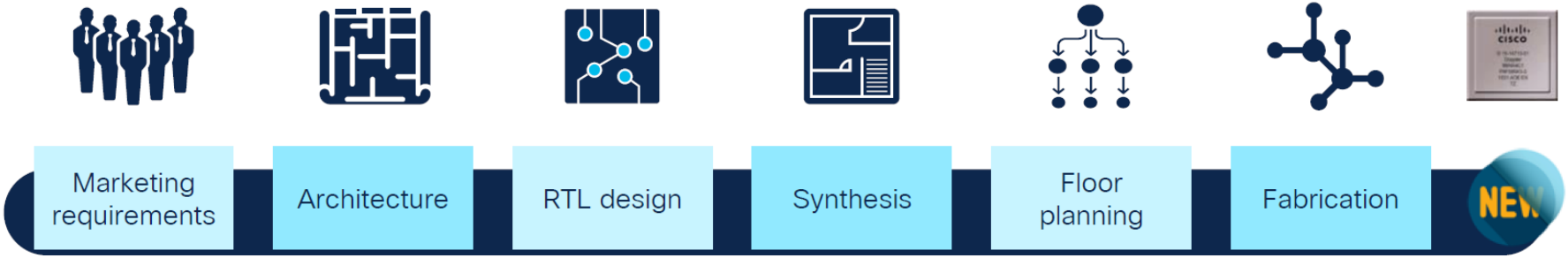
Session table update rate: 7000 sessions/second

Connections per second: 20,000

Offload hairpin rate: ~90 Gbps for 1500 byte packets

Заблуждения и мифы

ASIC - это дешево



Building a **new ASIC** takes a lot of **Time** and **Money**

Fortigate – это *ВСЕГДА* быстро

Key Benefits

- Single-session flow with 100 Gbps throughput needed for high-bandwidth internet2 sites.
- Millions of connections per second in hardware as required by high-demand e-commerce.
- Single-digit microsecond **latency** as called for by a financial exchange.

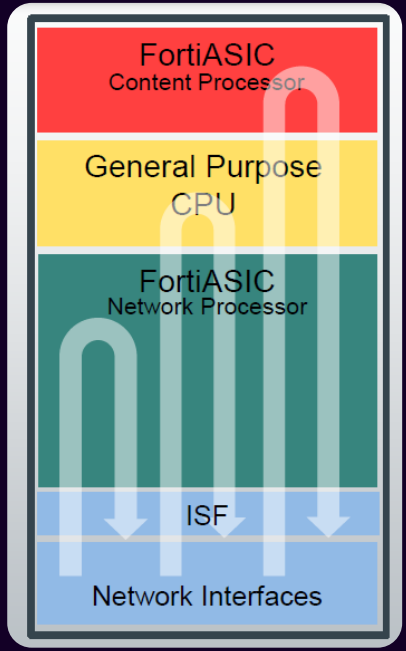
Use Cases

- Receive market data with the lowest required latency to avoid revenue loss
- Keep up with microbursts of traffic with high-speed packet forwarding
- Accelerate tens of millions of connections per second

NP7 Advantage

Specification	NP7 ASIC
Firewall	198 Gbps
IPsec VPN	55 Gbps
Threat Protection	15 Gbps
SSL Inspection	17 Gbps
Concurrent Sessions	12M
Sessions per second	750k

Based on the FortiGate 1800F series versus similar competitive products



Кто использует Intel, у того нет ускорения

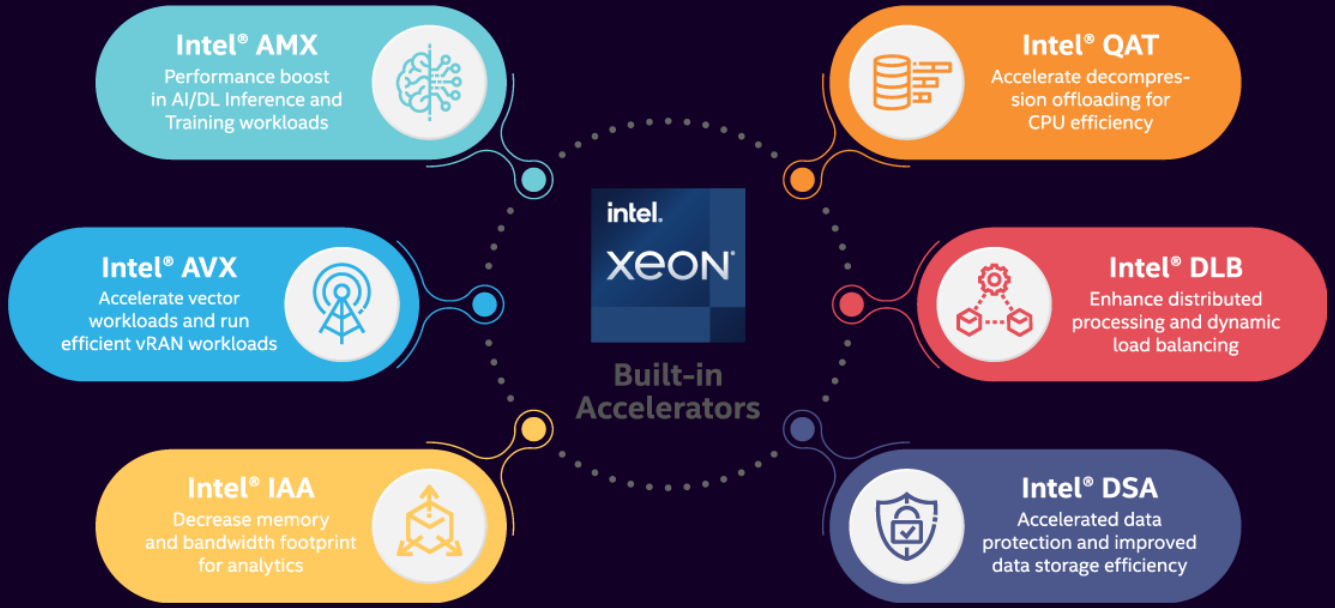
ТЕХНО infotecs ФЕСТ

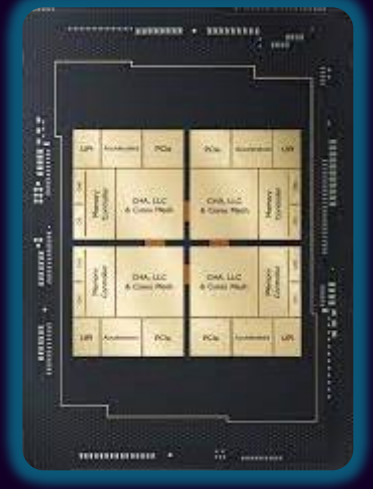
Intel® QuickAssist Technology (Intel® QAT)

Intel QAT is a technology for accelerating data encryption/decryption, public key cryptography for key exchange... This acceleration technology is integrated into 4th Gen Intel Xeon Scalable processors, supporting rates of **up to 400 Gbps for common cryptographic ciphers** and up to 160 Gbps verified compression.

Источник оценки	AES-256 CBC	AES-256 GCM
APNet`20 (1 ядро)	4,1 Гбит/с	20,7 Гбит/с
CU (1 ядро, 5000 Q2)	24 (65K) Гбит/с	41 (65K) Гбит/с

Кто использует Intel, у того нет ускорения

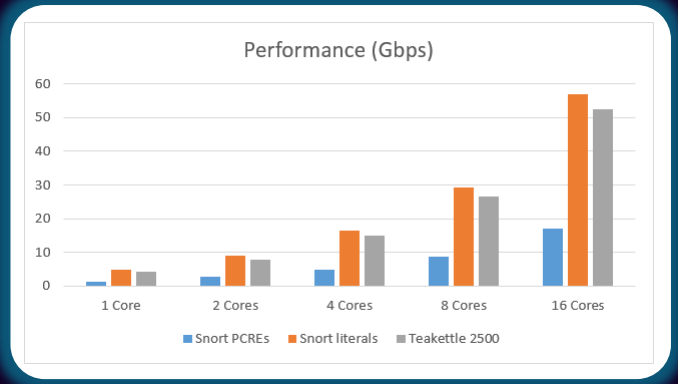




Кто использует Intel, у того нет ускорения

Hyperscan is a high-performance multiple regex matching library.

Hyperscan also takes advantage of the latest Intel® Advanced Vector Extensions 512 (Intel® AVX-512) vectorized bit manipulation instructions (vBMI) available on both the 3rd and 4th Gen Intel Xeon Scalable processors. It is suitable for usage scenarios such as DPI, IDS,IPS and firewalls, and has been deployed in network security solutions worldwide.

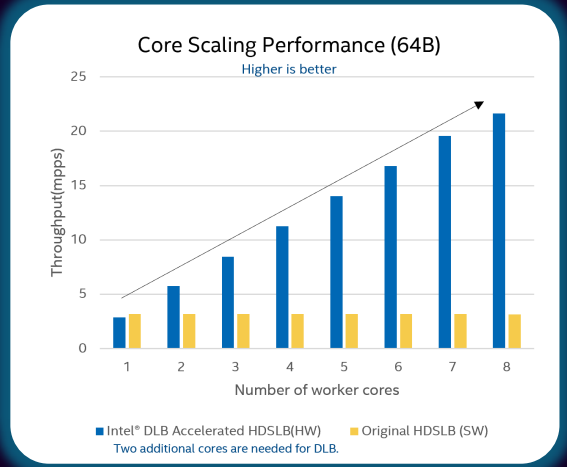


Xeon® processor E5-2699 v4 @ 2.20 GHz.

Кто использует Intel, у того нет ускорения

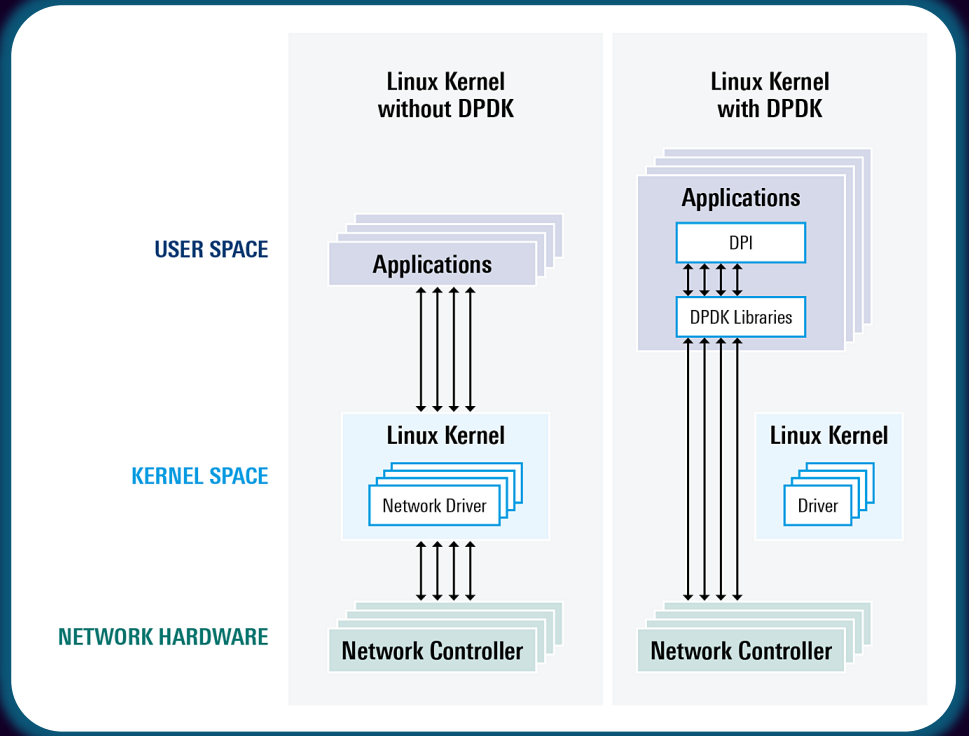
Intel Dynamic Load Balancer (DLB) is a hardware managed system of queues and arbiters connecting producers and consumers. These producers and consumers are typically software threads running on different cores or threads.

Intel DLB can be used to help alleviate the following potential system bottlenecks in NGFW: Elephant Flow, Slow Packets, Quaue Management



Почему мы используем стек Intel

Intel DPDK


Linux Kernel without DPDK
Linux Kernel with DPDK
USER SPACE
KERNEL SPACE
NETWORK HARDWARE
Applications
Linux Kernel
Network Driver
Network Controller
Applications
DPI
DPDK Libraries
Linux Kernel
Driver
Network Controller

Intel DPDK 40G

Test Results

Table 3: Test #1 Result

Frame Size (Bytes)	Line Rate[4x10G] (Mpps)	Frame Rate (Mpps)	% Line Rate
64	59.52	36.51	61.33
128	33.78	33.78	100
256	18.12	18.12	100
512	9.40	9.40	100
1024	4.79	4.79	100
1280	3.85	3.85	100
1518	3.25	3.25	100

Figure 4: Test #1 Result - RFC2544 zero packet loss test on 1x Intel® Ethernet Converged Network Adapter X710-DA4

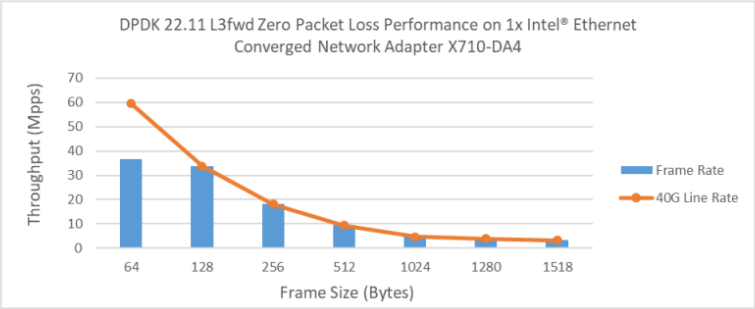
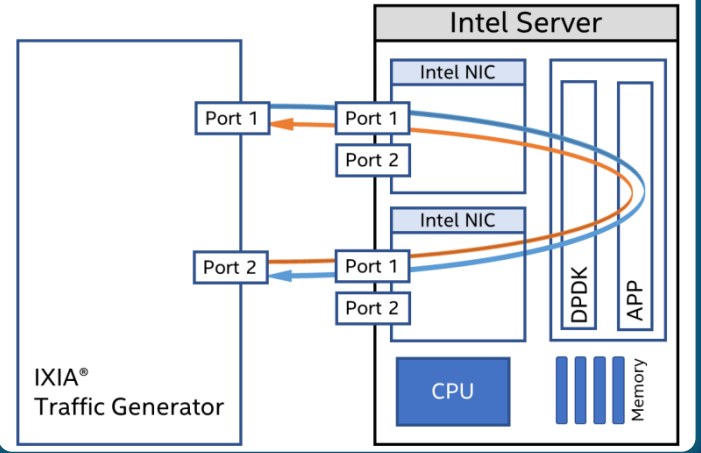


Figure 1: DPDK NIC performance test setup (1 port per NIC)



Выводы

Все используют ускорение

Те кто используют Intel используют аппаратное ускорение (блоки встроены в CPU, Network chips)

Те кто используют ASIC, FPGA ускоряют обработку в ряде сценариев, а не всегда

Важнее выяснять производительность NGFW в Ваших условиях, без оглядки на аппаратный состав

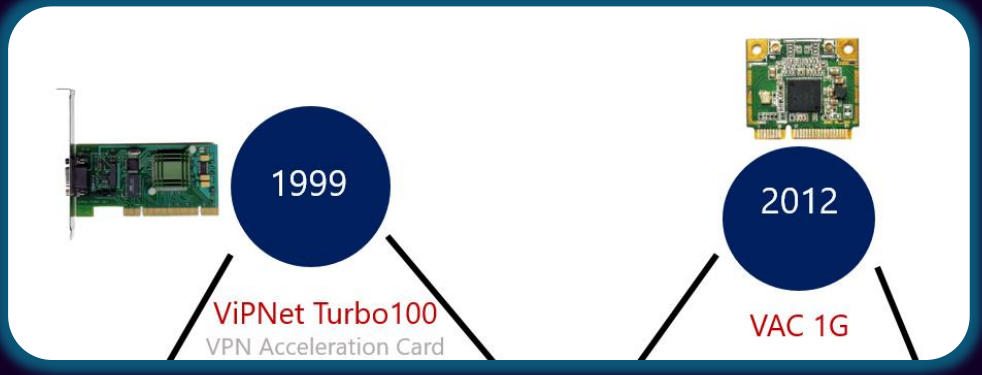
Наши планы в части аппаратного ускорения

Изучаем и используем все методы

Используем Intel и продолжаем изучать все их новые возможности

Изучаем и используем все методы

Используем FGPA (ускорение криптографии L2-10G, 100G)
и изучаем возможности использования для NGFW



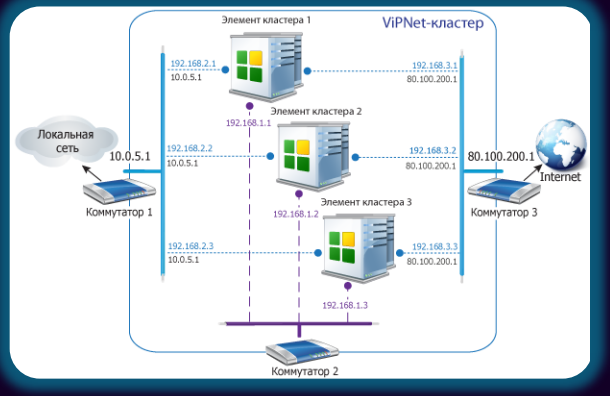
Изучаем и используем все методы

Изучали SmartNIC (санкционное давление) и продолжаем изучать

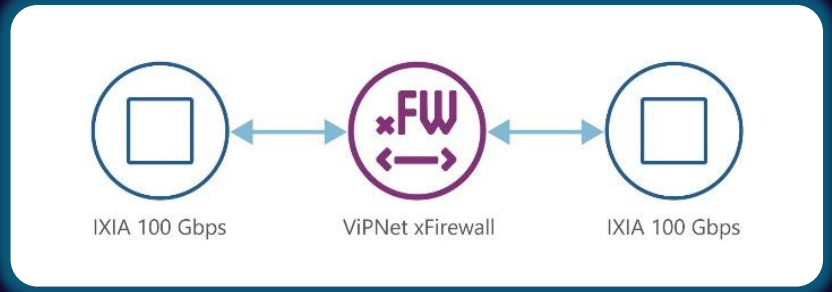
- B4COM tech SN1 SmartNIC (2x100 Гбит/с, ASIC Chelsio)
- Napatech F2070 (2x100 Гбит/с, FPGA+XeonD+16Гб DDR)
- Intel N2S-UPU01 (1x100 Гбит/с, Atom P5742, 16Гб eMMC)
- Lanner N2S NVIDIA BlueField DPU (2x100 Гбит/с, SWITCH+ARM)

Изучаем и используем все методы

Используем и продолжаем развивать механизмы горизонтального масштабирования (кластеризация А-А)



ViPNet Cluster 4.1 2013 год



Балансировка 2024 год

Сравнивайте потребительские качества

ТЕХНО infotecs ФЕСТ

Данные с сайтов нельзя сравнить

Диаметр Луны в 400 раз меньше диаметра Солнца. При этом Луна примерно в 400 раз ближе к Земле, чем к Солнцу. Поэтому с Земли Луна и Солнце кажутся примерно одинакового размера, и мы можем наблюдать солнечное затмение.

Данные с сайта

Исполнение	Производитель А	Производитель Б
Firewall, 1518 byte UDP (Мбит/сек)	1 600	3 800
AppControl, EMIX, (Мбит/сек)	395	2 200
NGFW (AppControl+IPS), (Мбит/сек)	40	1 000

Смеси трафика

Смесь крупного российского Enterprise

№ п/п	Протокол	Класс	Доля трафика по throughput, %	Доля трафика по CPS, %
1	HTTPS	WEB	25.22	7.24
2	HTTP	WEB	26.03	19.66
3	SAP	ENTERPRISE	3.15	3.22
4	CITRIX	ENTERPRISE	4.15	1.26
5	ORACLE	ENTERPRISE	2.02	0.92
6	SSH	ENTERPRISE	2.01	3.91
7	RDP	ENTERPRISE	5.24	1.26
8	LDAP	ENTERPRISE	1.96	6.09
9	SMB	FILE	10.96	0.57
10	NFS	FILE	1.89	2.87
11	MAPI	MAIL	2.87	7.47
12	POP3	MAIL	1.00	4.60
13	SMTP	MAIL	1.00	4.60
14	IMAP	MAIL	4.93	4.71
15	SIP	MEDIA/UDP	0.19	1.84
16	RTP	MEDIA/UDP	3.75	0.92
17	VIPNET	MEDIA/UDP	3.18	1.26
18	DNS	MEDIA/UDP	0.18	27.59

№	Приложение	Доля трафика, %
1.	Amazon S3	8,11
2.	AOL Instant Messenger	1,54
3.	BitTorrent	11,20
4.	Facebook	6,18
5.	Gmail	10,04
6.	Gtalk	5,02
7.	HTTP	19,07
8.	Simulated HTTPS	10,04
9.	SMTP	2,31
10.	SSH	0,51
11.	Oracle DB	0,5
12.	Twitter	3,47
13.	Yahoo Mail	10,04
14.	YouTube	11,97

Результаты измерений по единой методике

TRex
Realistic Traffic Generator

Исполнение	Производитель А	Производитель Б
Firewall, 1518 byte UDP (Мбит/сек)	1 640	1 916 (ограничение канала 1G)
AppControl, RuEntMIX, (Мбит/сек)	260,04	746,66
NGFW (AppControl+IPS), RuEntMIX, (Мбит/сек)	56,03	37,22

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA
NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ
GLOBAL DIGITAL SPACE
CISOCLUB
РУТОКЕН компания ПРАКТИВ
ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ
АВАНГАРД
PRinteg
АТБ ЭЛЕКТРОНИКА
infotecs {/-cademy}
merlion
УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС