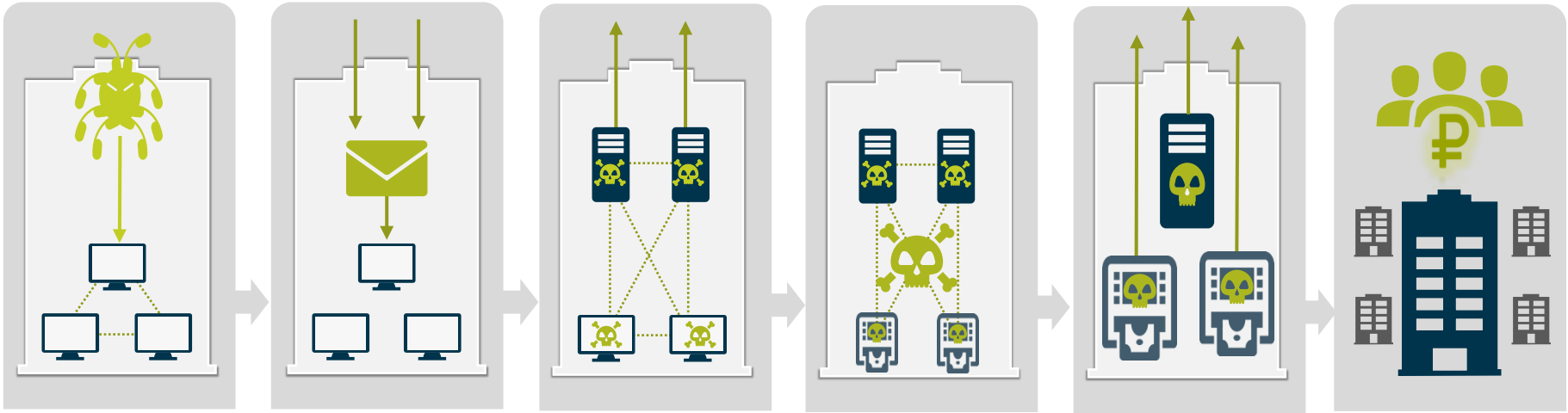
Palo Alto Networks
платформа для защиты от современных атак

Защита от краж данных по скрытым каналам
Защита от APT
Защита мобильных устройств
Защита виртуализации
Защита ЦОД
Построение VPN IPSEC/SSL VPN

Денис Батранков
+7 915 2414101
dbatrankov@paloaltonetworks.com

АТАКА ANUNAK

Успешно получен доступ внутрь корпоративных сетей более чем 50 банков.
Украдено более 1 млрд. рублей с 2013 по 2014 год из банков в России



Инфицирование через drive-by-download: Andromeda и Pony трояны через Neutrino Exploit Kit

Поддельные письма с вредоносными вложениями от имени ЦБ РФ

Использование существующих ботнетов для распространения нового кода

Доступ к банкоматам из специализированных сегментов, которые должны быть изолированными,

Снятие денег из банкоматов и через Интернет-кошельки, напр. Yandex Money

Подтверждено, что было захвачено 52 банкомата. Кража более 1 млрд. рублей.

Элементы атаки

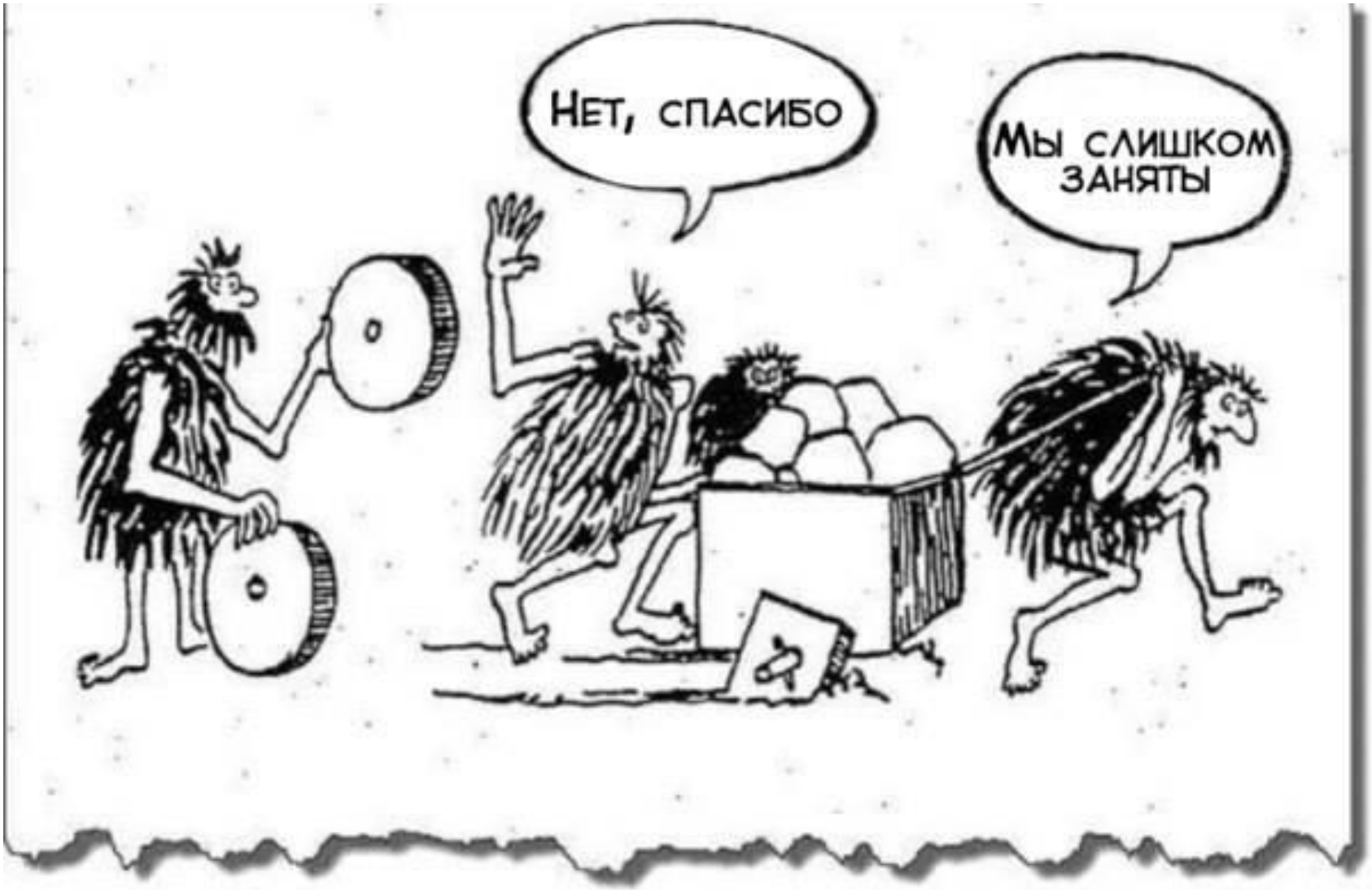
http://securityaffairs.co/wordpress/31405/cyber-crime/apt-anunak-steals-millions-from-banks.html
http://www.group-ib.com/files/Anunak_APT_against_financial_institutions.pdf

paloalto NETWORKS

ОБЩИЕ ЧЕРТЫ ВЗЛОМАННЫХ СЕТЕЙ

- ✓ Классический «портовый» межсетевой экран версия 1.0
- ✓ Статический IPS (или даже IDS)
- ✓ Устаревшие технологии на базе прокси серверов
- ✓ Классический антивирус на ПК (лучший из top10)

Зачем мне NGFW?



paloalto NETWORKS

Приложения изменились и используют сложные схемы подключения по сети

paloalto NETWORKS

Сетевые приложения изменились

- Apps ≠ Ports
  - 368 приложений в Applipedia используют **динамические** TCP/UPD порты (18,5%)
  - 352 приложений могут **туннелировать** другие приложения (18%)
  - 740 используют **шифрование** для сокрытия контента (37%)
  - 11% вредоносных сессий **бот-сетей** идентифицируются в трафике как “unknown tcp/udp”

https://applipedia.paloaltonetworks.com/

paloalto NETWORKS

Межсетевые экраны не изменились

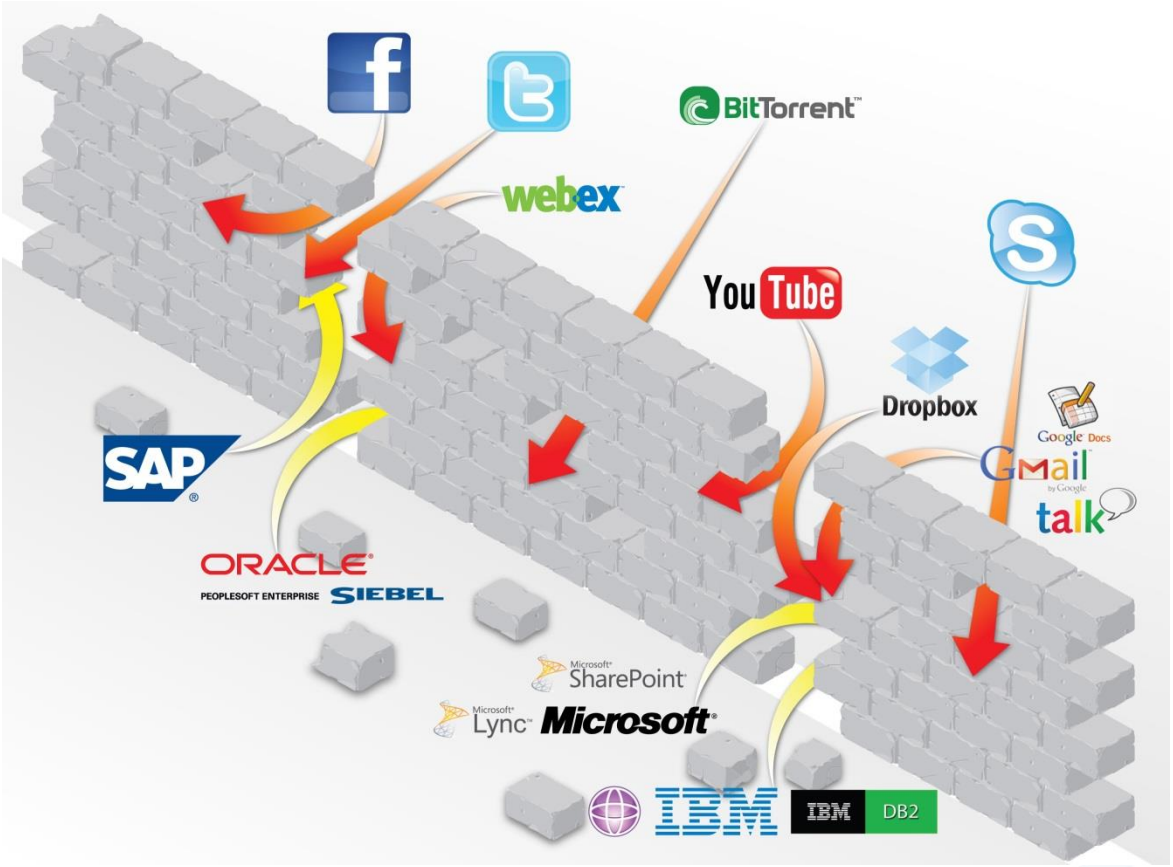
Межсетевые экраны не изменились

Политики межсетевых экранов базируются на контроле:

- Портов
- IP адресов
- Протоколов

НО…приложения изменились

- Порты ≠ Приложения
- IP-адреса ≠ Пользователи
- Пакеты ≠ Контент



Новый межсетевой экран должен восстановить контроль

paloalto NETWORKS

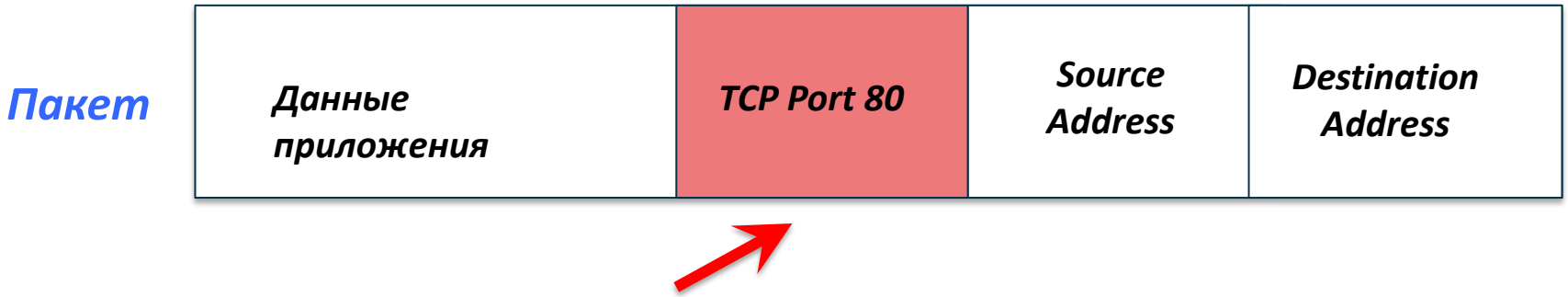
Пример

Разрешить MS Lync? Запросто!

1434(UDP), 5060, 5061, 444, 135, 5062, 8057, 8058, 5063, 57501-65535, 80, 443, 8080, 4443, 8060, 8061, 5086, 5087, 5064, 5072, 5070, 5067, 5068, 5081, 5082, 5065, 49152-57500(TCP/UDP), 5073, 5075, 5076, 5066, 5071, 8404, 5080, 448, 445, 881, 5041

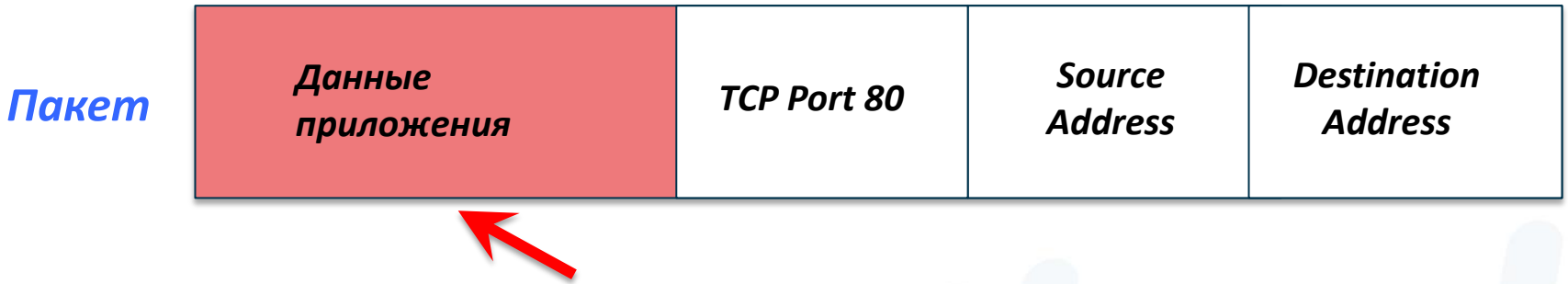
А как разрешить bittorent?

Какую часть сетевого пакета надо проверять?



Традиционно:

Приложение = номер порта (напр., HTTP = 80)



Новое определение:

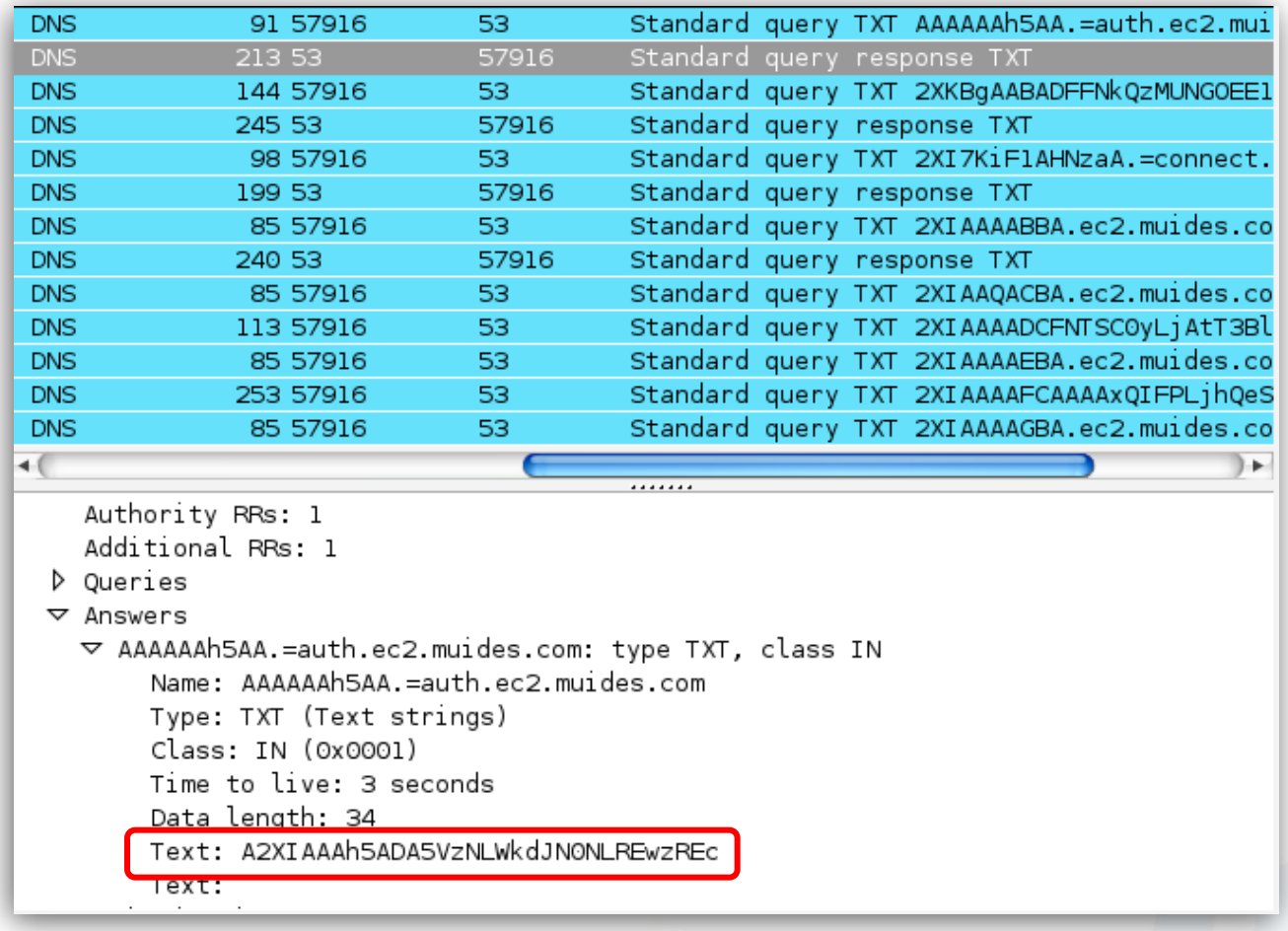
Приложение = Специфические передаваемые данные

flash = данные для анимации внутри браузера от Adobe

Туннелирование поверх DNS

Примеры

- tcp-over-dns
- dns2tcp
- Iodine
- Heyoka
- OzymanDNS
- NSTX



Использование рекурсивных запросов для передачи инкапсулированных сообщений по TCP в запросах удаленному DNS серверу и ответах клиенту

Что Вы видите со старым FW?

NGFW: Вашей сетью пользуется 200-300 приложений

Отчет о приложениях удивляет многих заказчиков

5	ares	general-internet	file-sharing	peer-to-peer	1,872	5
5	gnutella	general-internet	file-sharing	peer-to-peer	1,252	1
5	neonet	general-internet	file-sharing	peer-to-peer	160	1
4	web-browsing	general-internet	internet-utility	browser-based	10,161,886,439,519	196,005,508
4	flash	general-internet	internet-utility	browser-based	2,018,785,960,346	3,747,484
4	web-crawler	general-internet	internet-utility	browser-based	129,821,100,429	673,530
4	apple-appstore	general-internet	internet-utility	client-server	127,123,732,506	5,959
5	rss	general-internet	internet-utility	client-server	35,994,266,661	360,473
4	opera-mini	general-internet	internet-utility	client-server	765,112,718	1,647
4	google-desktop	general-internet	internet-utility	client-server	1,416,110	170
4	atom	general-internet	internet-utility	client-server	1,109,456	10
4	mobile-me	general-internet	internet-utility	browser-based	321,114	24
5	http-audio	media	audio-streaming	browser-based	382,876,698,144	97,357
4	pandora-tv	media	audio-streaming	browser-based	6,763,818	154
4	tagoo	media	audio-streaming	browser-based	21,864	5
4	poker-stars	media	gaming	browser-based	15,314	1
4	source-engine	media	gaming	client-server	142	1
5	http-video	media	photo-video	browser-based	1,400,772,539,442	173,541
5	youtube-base	media	photo-video	browser-based	563,165,794,217	281,304
4	rtmpt	media	photo-video	browser-based	118,638,696,267	4,104,013
4	rtmp	media	photo-video	browser-based	55,688,672,985	3,203
5	vimeo	media	photo-video	browser-based	49,067,440,021	44,625
5	asf-streaming	media	photo-video	browser-based	48,324,709,116	140
4	youtube-uploading	media	photo-video	browser-based	21,274,471,687	95,209
4	youtube-safety-mode	media	photo-video	browser-based	4,362,694,616	1,147
4	rtmpe	media	photo-video	browser-based	3,882,960,101	1,251
4	justin.tv	media	photo-video	browser-based	1,114,697,163	707
4	limelight	media	photo-video	browser-based	651,630,285	5,118
4	dailymotion	media	photo-video	browser-based	92,181,486	1,401

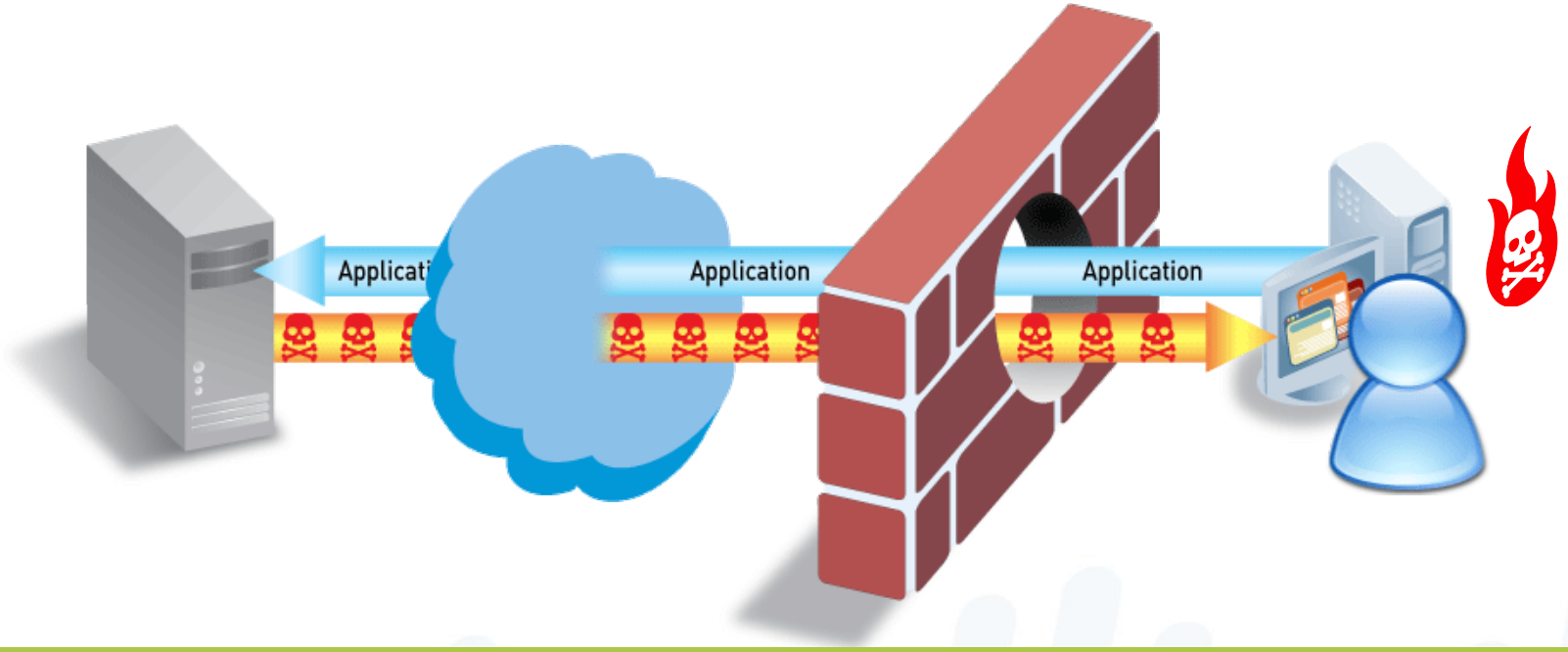
Приложения являются источником рисков

Приложения сами могут быть “угрозами”

- P2P file sharing, туннельные приложения, анонимайзеры, мультимедиа, TOR, Bitcoin

Приложения могут способствовать распространению угроз

- Основные угрозы – это угрозы уровня приложений

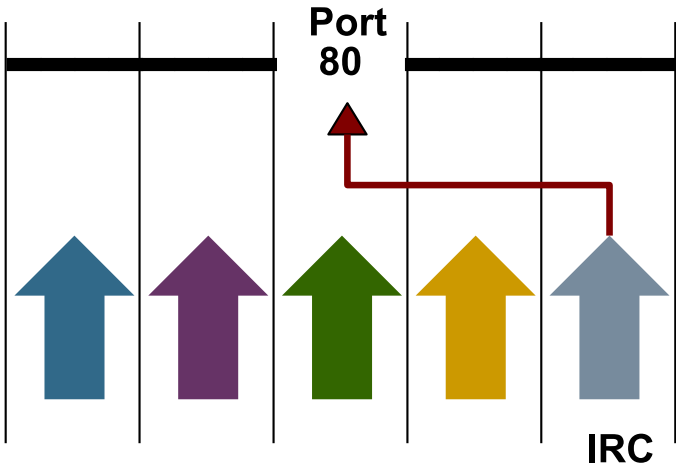


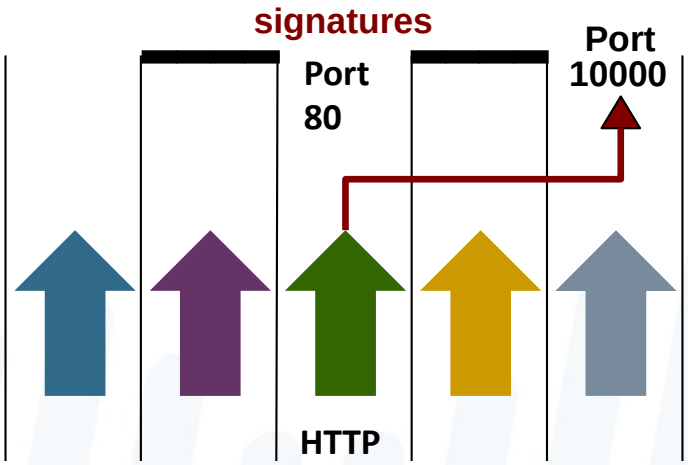
Приложения и угрозы уровня приложений создают бреши в системе безопасности

paloalto NETWORKS

Техники уклонения от защиты развиваются

1. Распространение вредоносного ПО или нелегитимного трафика через открытые порты
   - нестандартное использование стандартных портов
   - создание новых специализированных протоколов для атаки
2. Использование стандартных протоколов на нестандартных портах – уклонение от сигнатурного сканирования





paloalto NETWORKS

Две стороны одного протокола SSL

Good?

Bad?

BlackPOS

facebook

ultrasurf

webex
powering real-time meetings on the web

Citadel

Aurora

salesforce.com
Success On Demand.™

TDL-4

Tor

Rustock

Dropbox

Poison IVY

Ramnit

APT1

SSL для защиты данных или чтобы скрыть вредоносную активность?

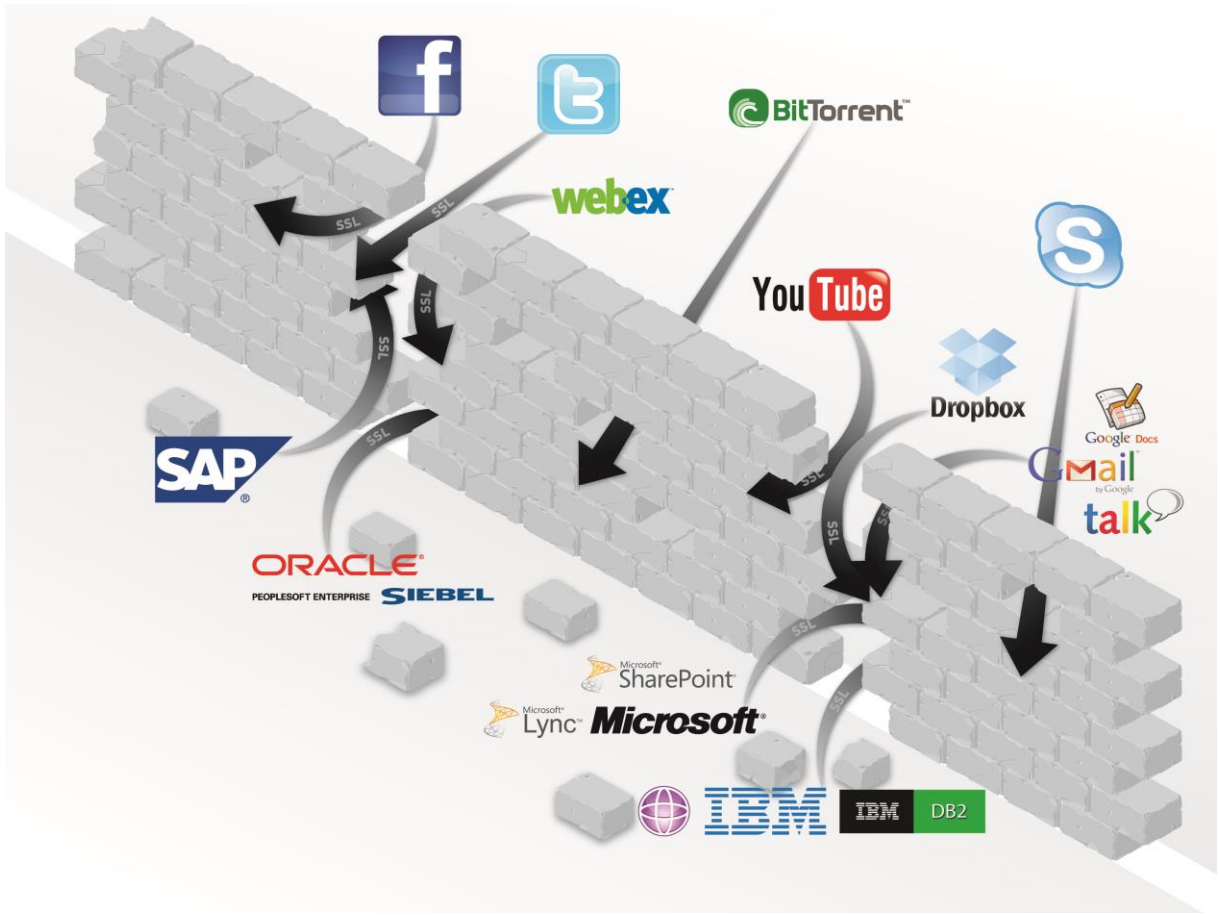
paloalto NETWORKS

SSL зашифрована треть трафика сети

Доверяй, но проверяй!

paloalto NETWORKS

Что сотрудники передают через зашифрованные каналы?



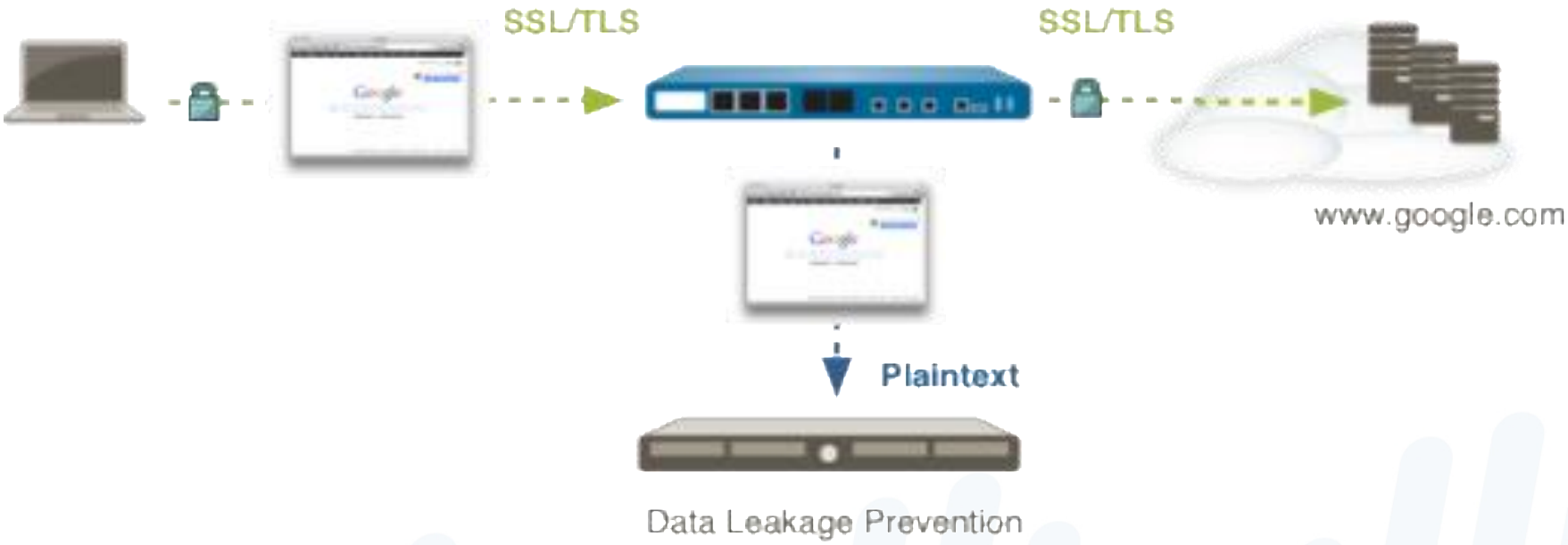
Применение шифрования:

- **SSL**
- **Специальные протоколы шифрования**

paloalto NETWORKS

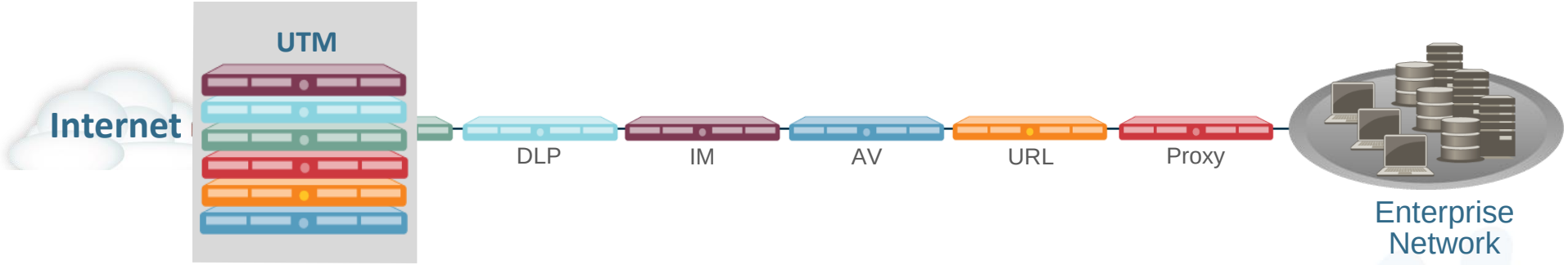
Схема работы расшифрования SSL/SSH

- После расшифрования трафик будет проверен и он может быть также отослан на внешний зеркальный порт (например во внешний DLP)



«Помощники» межсетевого экрана не помогают!

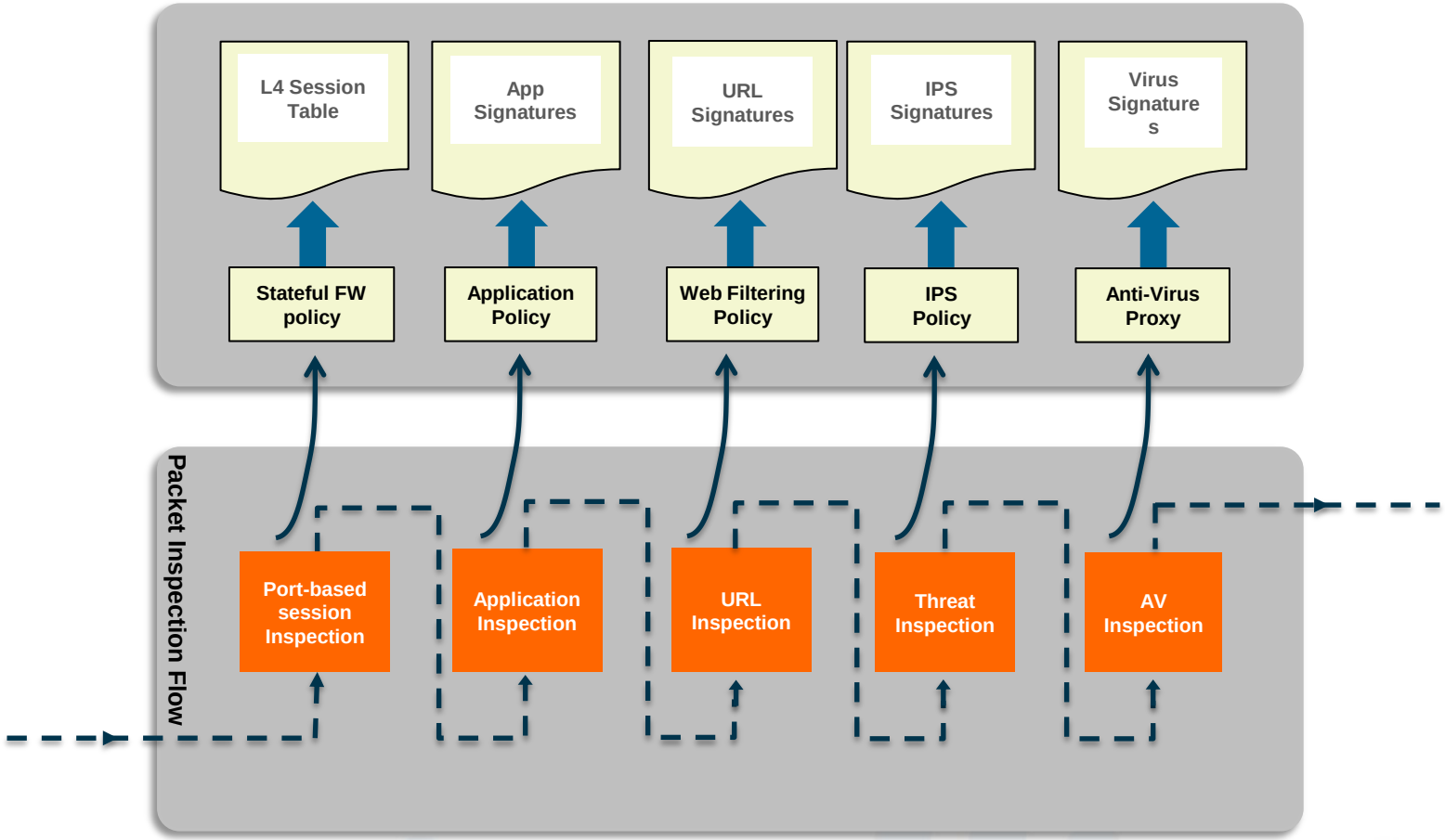
- Сложная топология и нет «прозрачной» интеграции
- «Помощники» межсетевого экрана не имеют полного представления о трафике – нет корреляции
- Дорогостоящее и дорогое в обслуживании решение



- Использование UTM - отдельных функциональных модулей в одном устройстве делает его ОЧЕНЬ медленным

paloalto NETWORKS

Почему подход UTM не работает



Повышаем безопасность = хуже производительность

Традиционная безопасность

- Каждая новая коробка для безопасности снижает производительность
- IPS чаще всех получают жалобы
- Идут трения между ИТ и безопасностью

paloalto NETWORKS

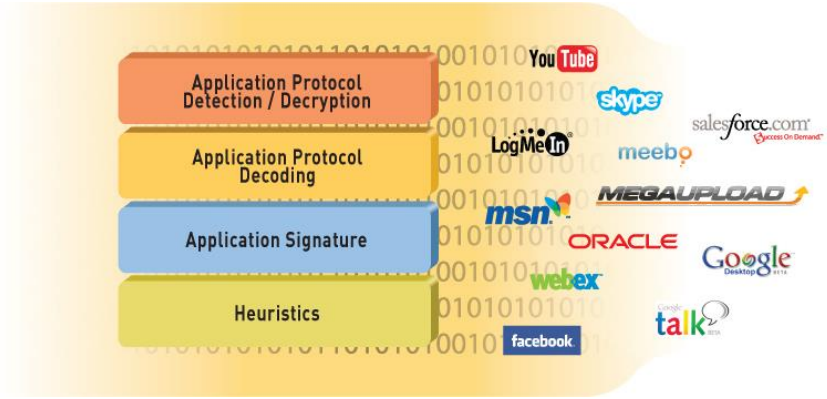
Межсетевой экран нового поколения Palo Alto Networks

аппаратное устройство спроектированное для работы при всех включенных функциях безопасности

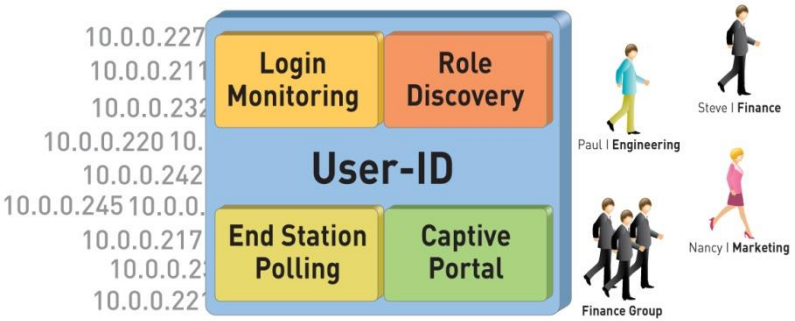
paloalto NETWORKS

Инновационные технологии Palo Alto Networks

App-ID™
Идентификация приложений



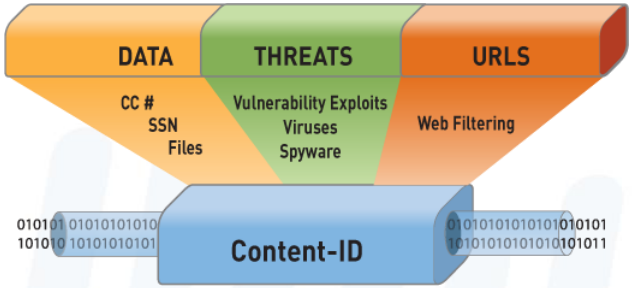
User-ID™
Идентификация пользователей



Content-ID™

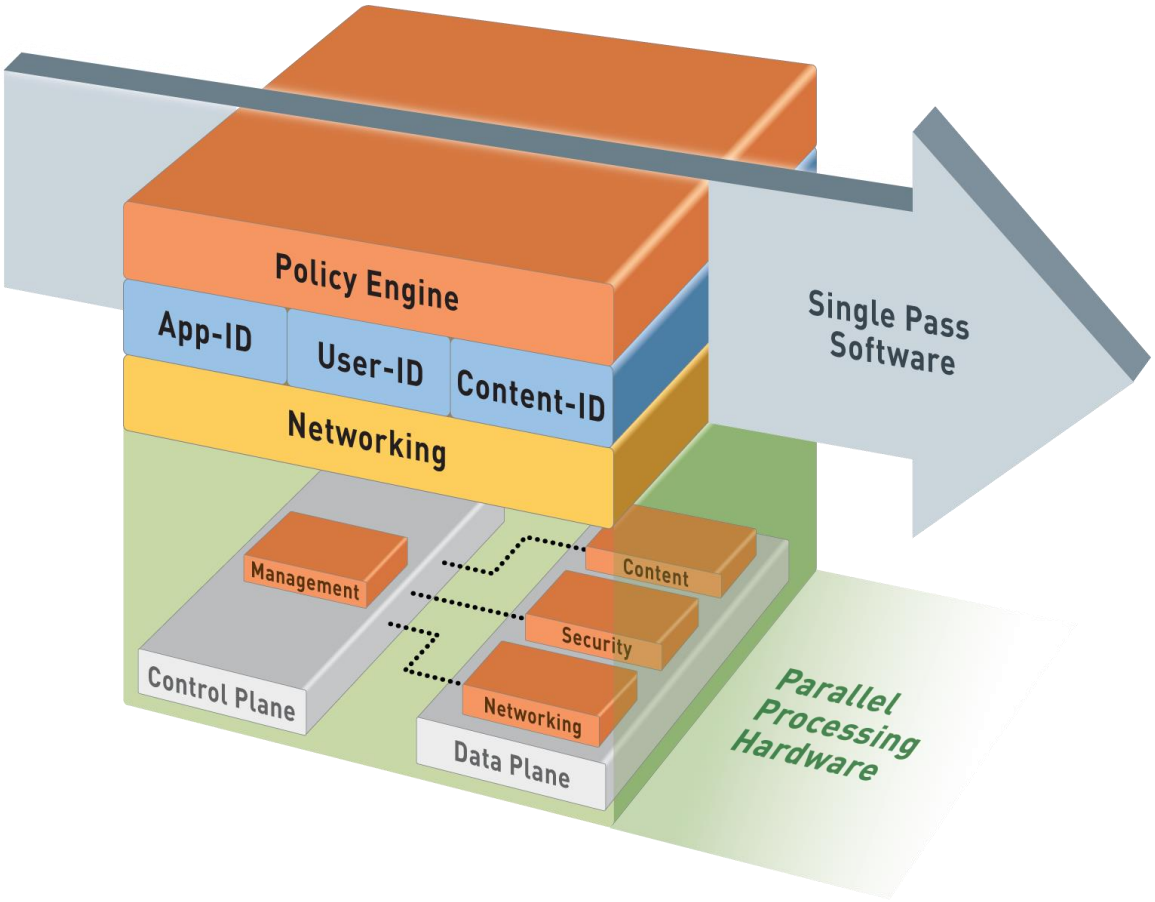
Контроль данных

+ SSL decryption



paloalto NETWORKS

Архитектура однопроходной параллельной обработки



Один проход

- Каждый пакет сканируется только один раз
- При сканировании одновременно определяется:
  - Приложение
  - Пользователь/группа
  - Контент – угрозы, URL и т.д.

Параллельная обработка

- Специализированное аппаратное обеспечение для каждой задачи
- Разделение Data plane и Control plane

До 200 Гбит/с, низкая задержка

paloalto NETWORKS

Архитектура на примере PA-5000

- 40+ процессоров
- 30+ Гб RAM
- Разделенные платы управления и передачи данных (Management Plane/Data Plane)
- 20 Гбит/с детект приложений
- 10 Гбит/с с всем включенным
- 4 миллиона одновременных сессий

Control Plane

- Highly available mgmt
- High speed logging and route update
- Dual hard drives

Quad-core CPU

RAM

RAM

HDD

HDD

Switch Fabric

- 80 Gbps switch fabric interconnect
- 20 Gbps QoS engine

QoS

Switch Fabric

Data Plane

Signature Match HW Engine

- Stream-based uniform sig. match
- Vulnerability, spyware, CC#, SSN, and more

Signature Match

RAM

RAM

RAM

RAM

Signature Match

RAM

RAM

RAM

RAM

10Gbps

10Gbps

CPU 1

CPU 2

...

CPU 12

RAM

RAM

SSL

IPSec

Compress.

CPU 1

CPU 2

...

CPU 12

RAM

RAM

SSL

IPSec

De-Compress.

20Gbps

Security Processors

- High density parallel processing for flexible security functionality
- Hardware-acceleration for standardized complex functions (SSL, IPSec, decompression)

Flow control

Route, ARP, MAC lookup

NAT

Network Processor

- 20 Gbps front-end network processing
- Hardware accelerated per-packet route lookup, MAC lookup and NAT

paloalto NETWORKS

Gartner: NGFW – ваш следующий IPS

IPS is Dead – Migrate to Next-Generation Firewalls

The world of stand-alone IPS products will soon be gone, as IPS functionality becomes integrated as a standard feature of Next-Generation Firewalls. Threats target applications, and enterprises struggle to control modern applications with existing security infrastructure. The current landscape dictates a new set of requirements for comprehensive intrusion prevention, and Palo Alto Networks next-generation firewalls deliver, where IPS products cannot:

Requirement	Palo Alto Networks	Traditional IPS
Control Applications	Over 900 applications	Can only treat a few "bad" applications like threats
Scan allowed traffic for threats	Yes, 1000s of signatures	Yes, 1000s of signatures
Real-world, Multi-Gbps Performance	Yes	Depends on the vendor, but oftentimes, no
Research and Support	Class-leading – more Microsoft vulnerabilities discovered than any IPS vendor (6 in the last 6 months)	Lots of noise, little action – the best in-house IPS research team discovered 3 Microsoft vulnerabilities in the last 6 months. Some haven't done anything for 2 years.

Furthermore, because Palo Alto Networks next-generation firewalls have superior port density, covering multiple segments is much easier, and cost-effective than stand-alone IPS.

Industry experts understand all of these new requirements, and have begun recommending that enterprises transition from standalone IPS to next-generation firewalls – read Gartner's note, **"Defining the Next-Generation Firewall."** Complete the form on the right to download a copy of the report. (*Note: All fields are required*)

Download FREE Report

Gartner's "Defining the Next-Generation Firewall"

Complete the form below to download the report.

First Name:

Last Name:

Company:

Title:

Phone:

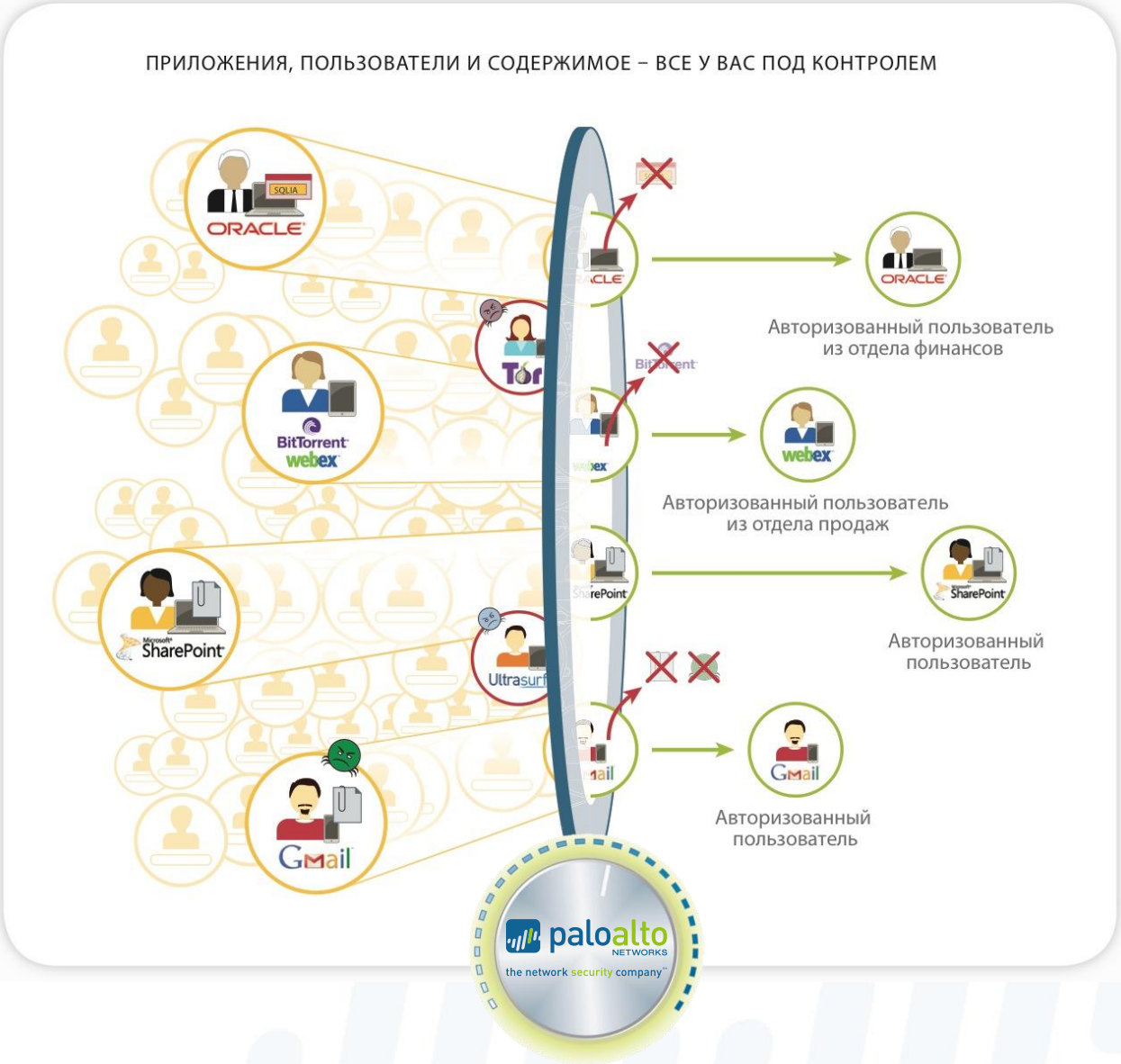
E-mail:

State: Select State

Country: Select Country

SUBMIT

NGFW: гарантированная производительность при всех включенных функциях безопасности



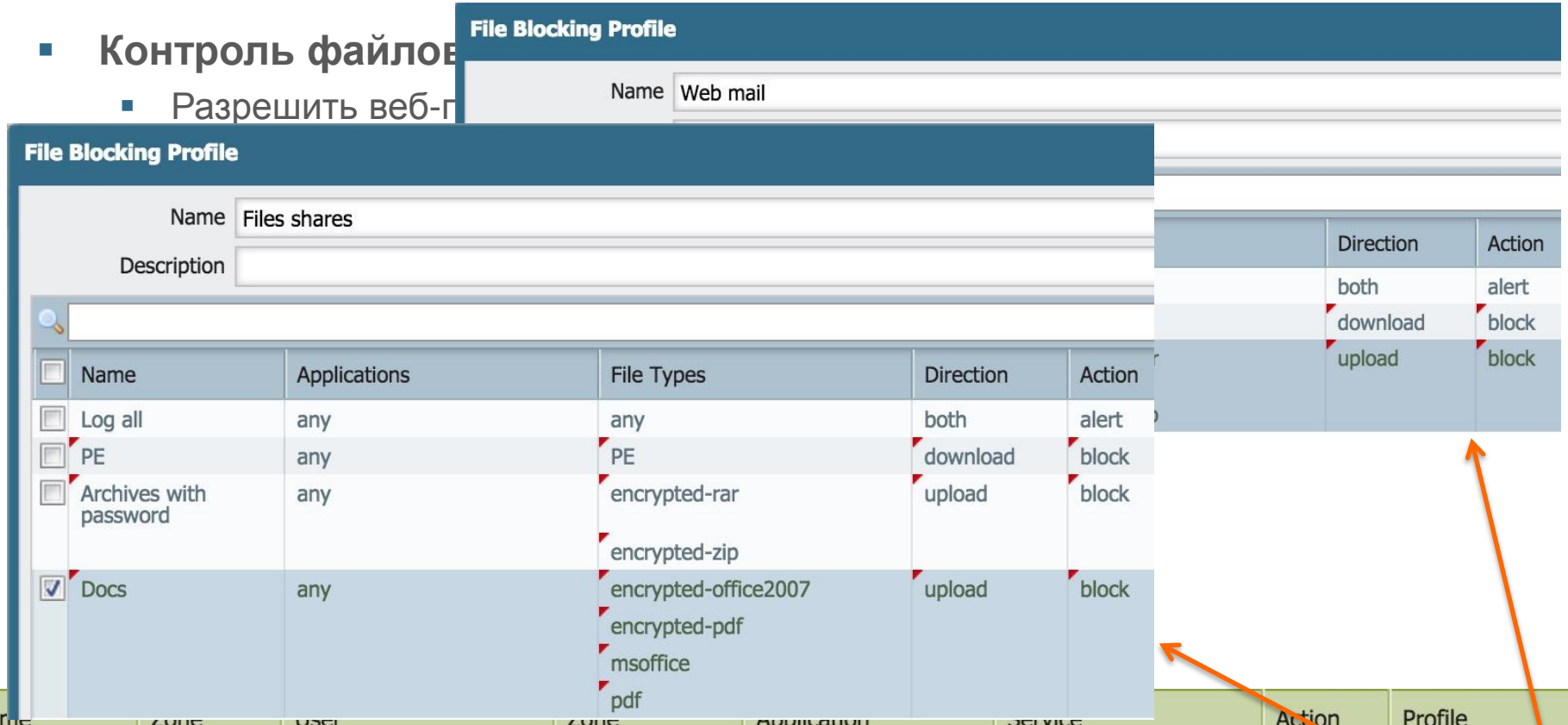
- **Единая политика безопасности**
- **Идентификация, контроль и безопасное разрешение приложений (App-ID) для каждого пользователя/группы (User-ID)**
- **Расшифрование входящего/исходящего SSL/SSH**
- **Обнаружение известных и неизвестных угроз в режиме реального времени (Content-ID)**
- **Высокая пропускная способность, низкие задержки**
- **Простота и большое количество вариантов внедрения**

Примеры решения задач с помощью NGFW

paloalto NETWORKS
the network security company™

Пример 1

- **Контроль файлов**
  - Разрешить веб-п



Name	Zone	User	Zone	Application	Service	Action	Profile
Secure web-...	L3-...	corp\internet	L3-Untr...	web mail	service-https	Allow	
Other web-mail	L3-...	any	L3-Untr...	web mail	any	Deny	
Cloud file sha...	L3-...	corp\vip_internet	L3-Untr...	Cloud file sharing	service-http service-https	Allow	

Пример 2

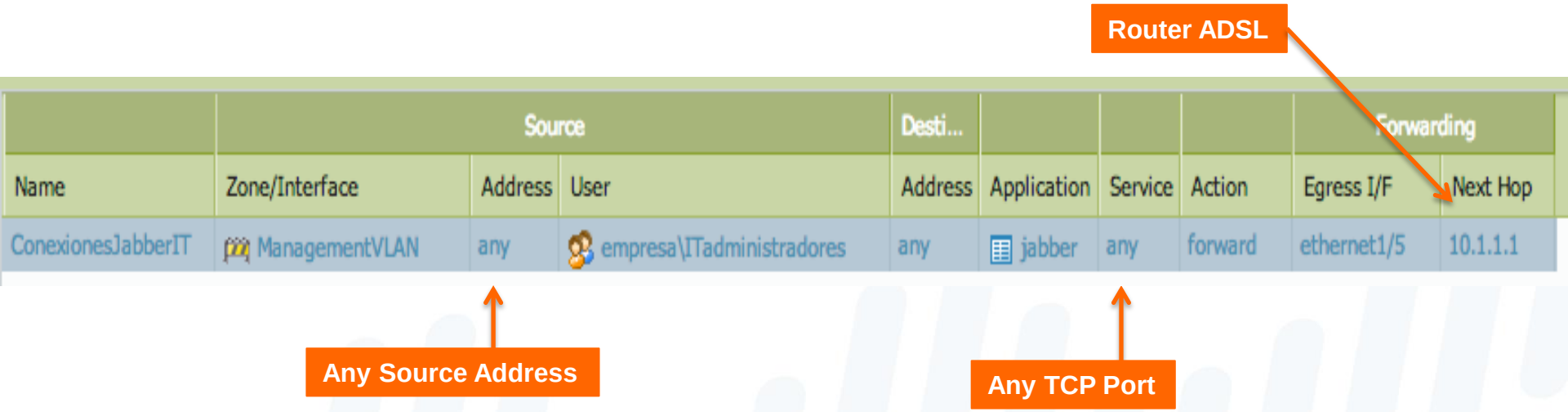
- **Маркировка трафика lync-voice по классу gold CoS в MPLS WAN**
  - В Компании X есть множество филиалов, соединенных поверх MPLS VPN. Оператор обеспечивает классы сервиса (CoS) и администратор хочет маркировать голосовые сессии Lync согласно golden CoS
  - Но администратор хочет сохранить передачу файлов через Lync как best-effort CoS

DSCP Marking by application
Mark only lync-voice application with DSCP EF to become gold CoS. Don't do that for lync-file-transfer

	Source				
Name	Address	User	Application	Action	Options
lyncVoiceGold	any	any	ms-lync-audio	✓	QoS
lyncFileTransfer	any	any	ms-lync-file-transfer	✓	

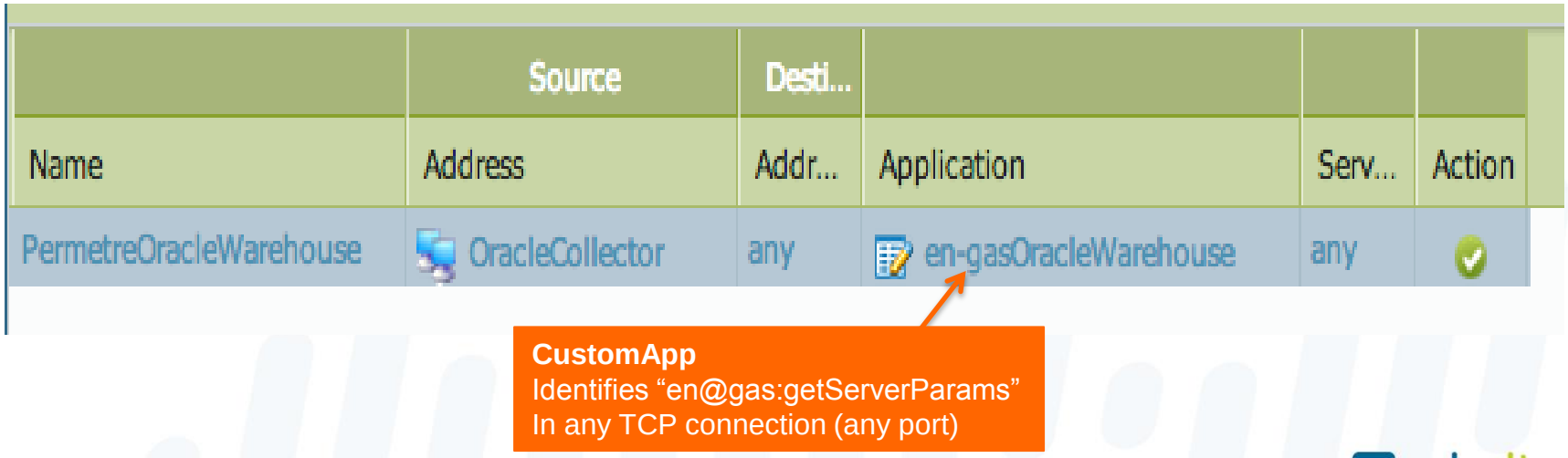
Пример 3

- **Перенаправление по политике трафика jabber для IT администраторов**
  - Филиал Компании X подключен к ГО с использованием MPLS VPN. В филиале работают разработчики ПО, которые передают через jabber большие объемы кода, перегружая VPN.
  - В филиале установили новый маршрутизатор ADSL. МЭ должен перенаправлять весь траффик jabber (независимо от TCP порта) от пользователей группы ITadministrators (независимо от IP источника) в сторону ADSL маршрутизатора.



Пример 4

- **«Самописное» приложение OracleWarehouse connector**
  - Компании En@gas требуется разместить в ЦОД сервер для сбора данных с 300 объектов АСУ ТП, распределенных территориально поверх MPLS IP/VPN.
  - Сбор данных будет осуществляться программой OracleWarehose connector. К сожалению, сложно определить место расположения всех 300 объектов и соответствующие TCP порты, которые они публикуют коннектору.
  - Но зато сессии легко идентифицировать по TCP payload, который начинается с charString “**en@gas:getServerParams**”



Обзор аппаратной архитектуры и линейки оборудования NGFW Palo Alto Networks

paloalto NETWORKS
the network security company™

Семейство платформ Palo Alto Networks

PA-5060

20 Гбит/с FW/10 Гбит/с предотвращение атак/4,000,000 сессий

4 SFP+ (10 Gig), 8 SFP (1 Gig), 12 RJ-45 gigabit

PA-5050

10 Гбит/с FW/5 Гбит/с предотвращение атак /2,000,000 сессий

4 SFP+ (10 Gig), 8 SFP (1 Gig), 12 RJ-45 gigabit

PA-5020

5 Гбит/с FW/2 Гбит/с предотвращение атак /1,000,000 сессий

8 SFP, 12 RJ-45 gigabit

PA-3060

4 Gbps FW

2 Gbps threat prevention

500,000 sessions

8 copper gigabit

8 SFP interfaces, 2 SFP+ (10GE)

PA-3050

4 Gbps FW

2 Gbps threat prevention

500,000 sessions

12 copper gigabit

8 SFP interfaces

PA-3020

2 Gbps FW

1 Gbps threat prevention

250,000 sessions

12 copper gigabit

8 SFP interfaces

VM Series

(ESXi/NSX/SDX/AWS/KVM)

до 1 Gbps FW

до 600 Mbps threat prevention

до 250,000 sessions

Гостевая машина или в режиме гипервизора

PA-500

250 Мбит/с FW/100 Мбит/с предотвращение атак /64,000 сессий

8 copper gigabit

PA-200

100 Мбит/с FW/50 Мбит/с предотвращение атак/64,000 сессий

4 copper gigabit

PA-7080 - самый производительный в мире NGFW !!

	PA-7050 NPC	PA-7050 System	PA-7080 System
NGFW (L3-L7) Gbps	20	**120**	**200**
Threat Prev. Gbps	10+	**60+**	**100+**
Матрица коммутации		1.2 Тбит	1.2 Тбит
Встроенная система логирования		4x1TB HDD = 2TB RAID1	4x1TB HDD = 2TB RAID1

- Лицензирование и техническая поддержка на шасси
- Линейное масштабирование производительности
- Снижение стоимости за защищенный Гбит
- Интерфейсы 10 и 40 Гбит

Функции операционной системы

Идентификация и контроль приложений, пользователей и защита от угроз дополняются следующим функционалом:

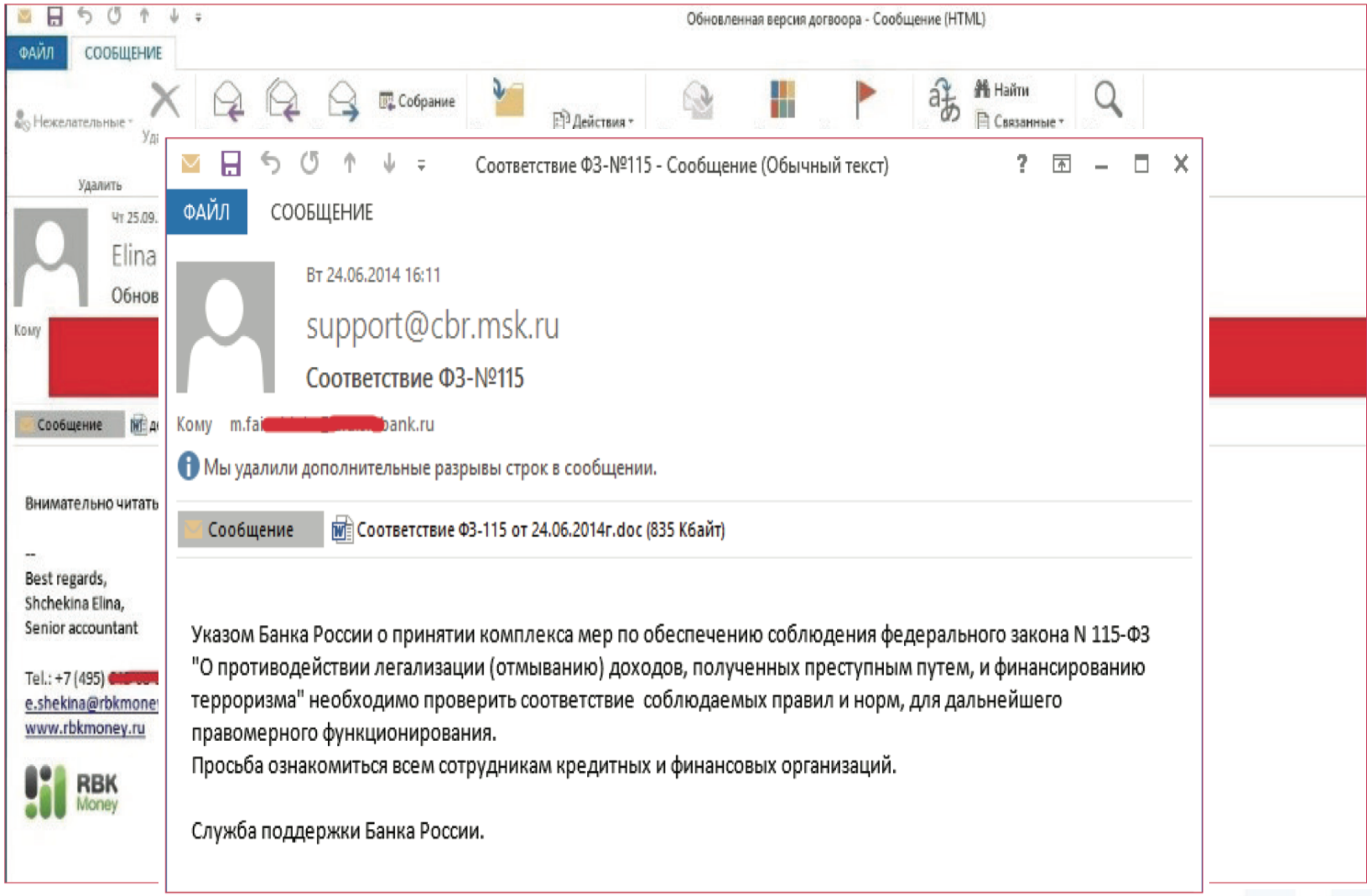
- Network
  - Динамическая маршрутизация (BGP, OSPF, RIPv2)
  - Режим мониторинга – подключение к SPAN-порту
  - Прозрачный (L1) / L2 / L3 режимы
  - Маршрутизация по политикам (PBF)
  - IPv6
  - PortChannel (LACP)
  - ECMP и балансировка нагрузки
- VPN
  - Site-to-site IPSec VPN
  - SSL VPN (GlobalProtect)
- Функционал QoS
  - Приоритезация, обеспечение максимальной/гарантированной полосы
  - Возможна привязка к пользователям, приложениям, интерфейсам, зонам и т.д.
  - Мониторинг полосы в режиме реального времени
- Зоновый подход
  - Все интерфейсы включаются в зоны безопасности для упрощения настройки политик
- Отказоустойчивость
  - Active/active, active/passive
  - Синхронизация конфигурации
  - Синхронизация сессий на L7
  - Path, link и HA мониторинг
- Виртуальные системы
  - Настройка нескольких межсетевых экранов в одном устройстве (серии PA-7000/5000/3000)
- Простое и гибкое управление
  - CLI, Web, Panorama, SNMP, Syslog, NetFlow, интеграция с SIEM/SIM

paloalto NETWORKS

Построение защиты от современных угроз и целенаправленных атак (APT)

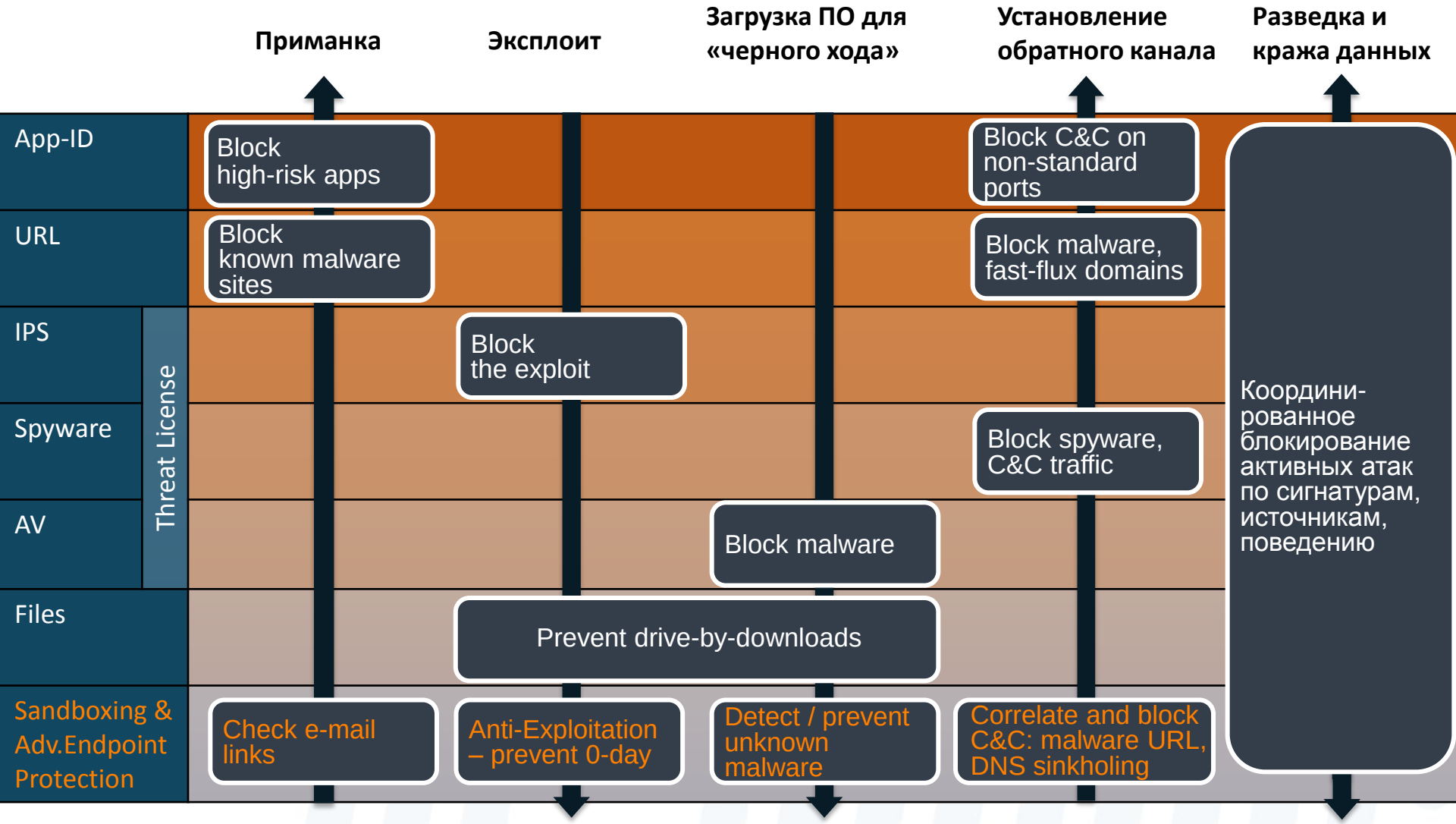
paloalto NETWORKS
the network security company™

Anunak – письмо с вредоносным вложением



paloalto NETWORKS

Технологии Palo Alto Networks, применяемые для защиты от современных угроз

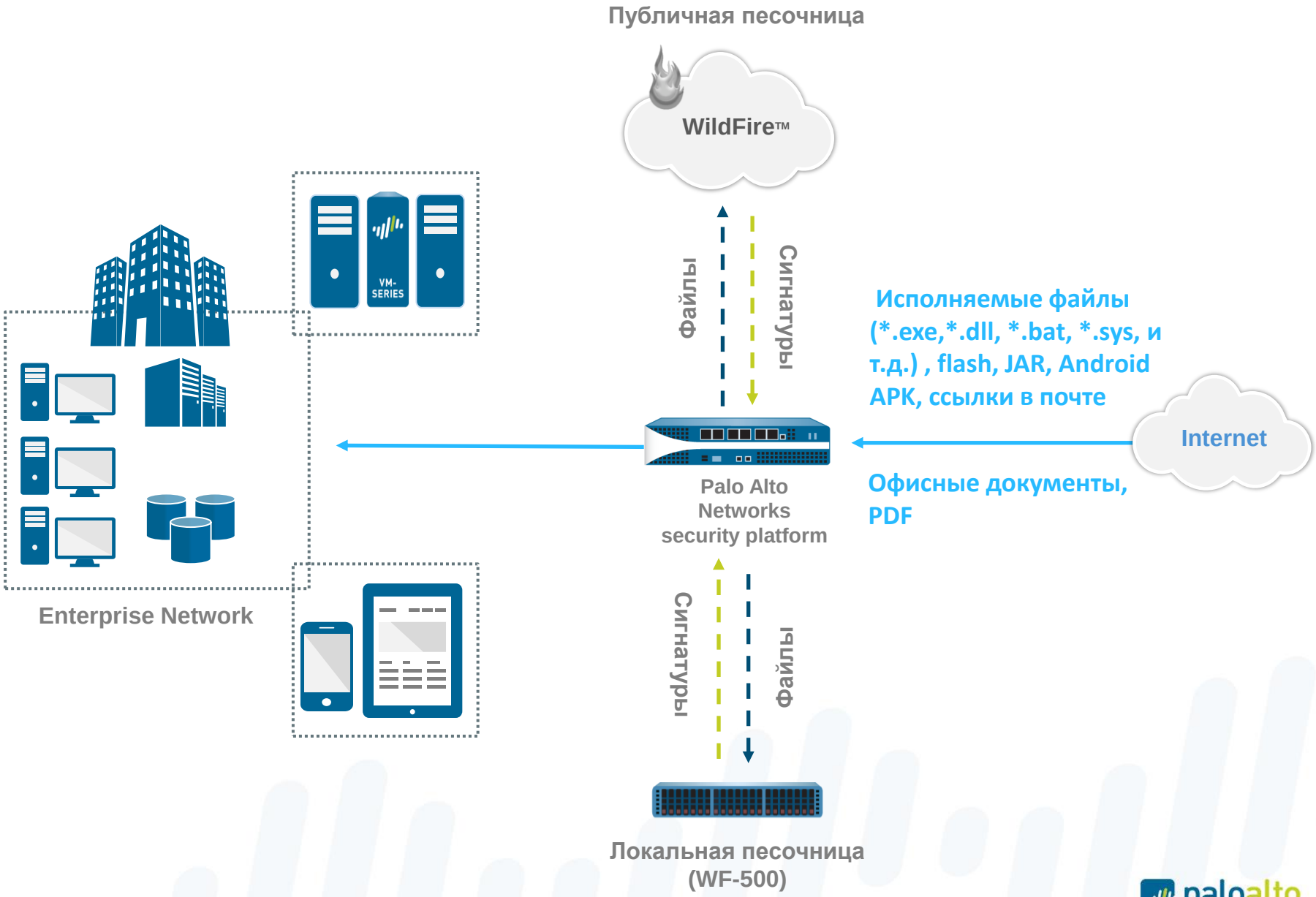


Антивирусы **не справляются** со скоростью появления новых видов вредоносного ПО и не могут заблокировать эксплойты

Что делать: при нажатии на ссылку, каждому новому нажавшему генерируется новый совершенно код вируса?

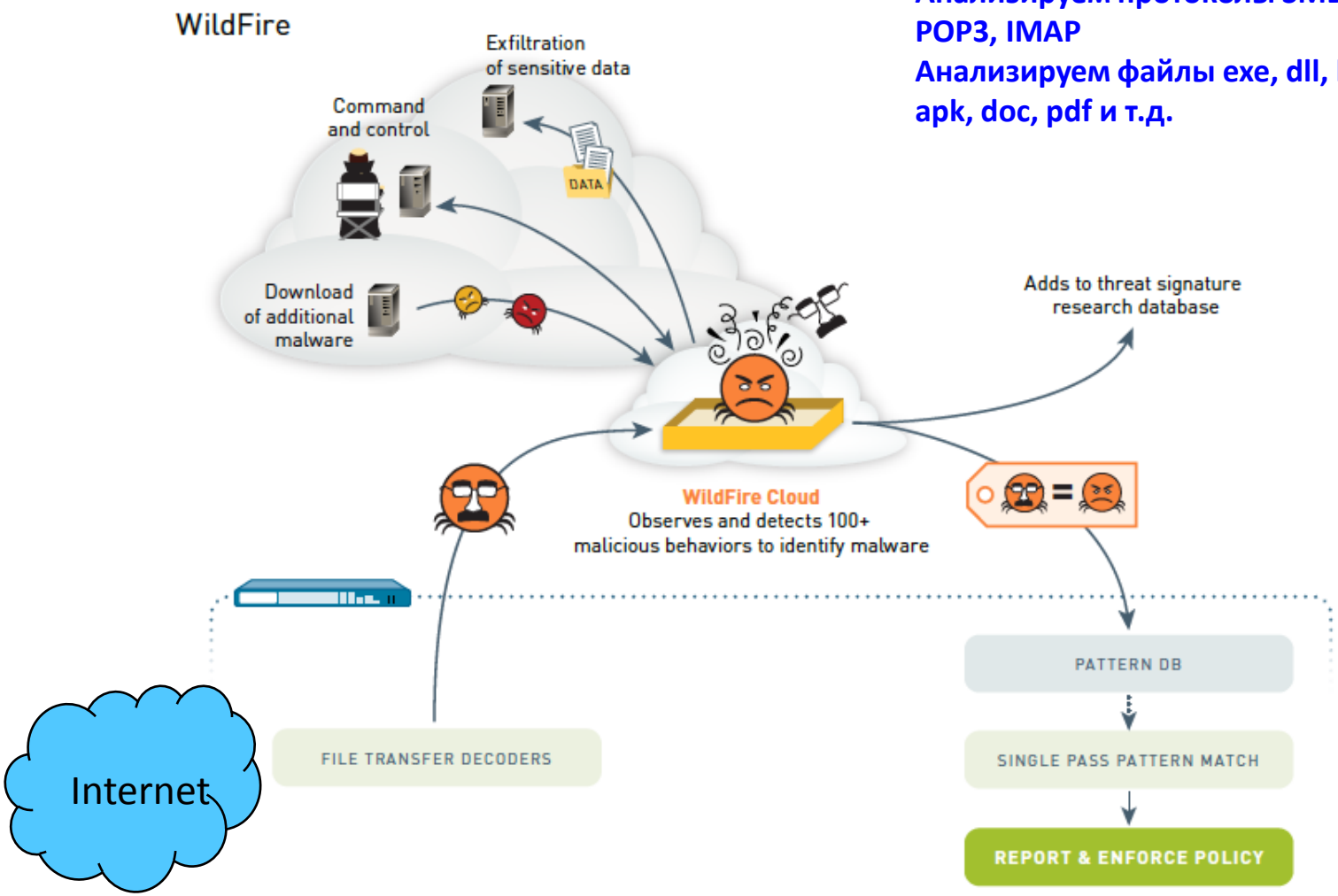
paloalto NETWORKS

Wildfire – защита от неизвестных угроз на уровне сети



Анализируем поведение. Технология WildFire

Анализируем протоколы SMB, FTP, HTTP, SMTP, POP3, IMAP
Анализируем файлы exe, dll, bat, sys, flash, jar, apk, doc, pdf и т.д.



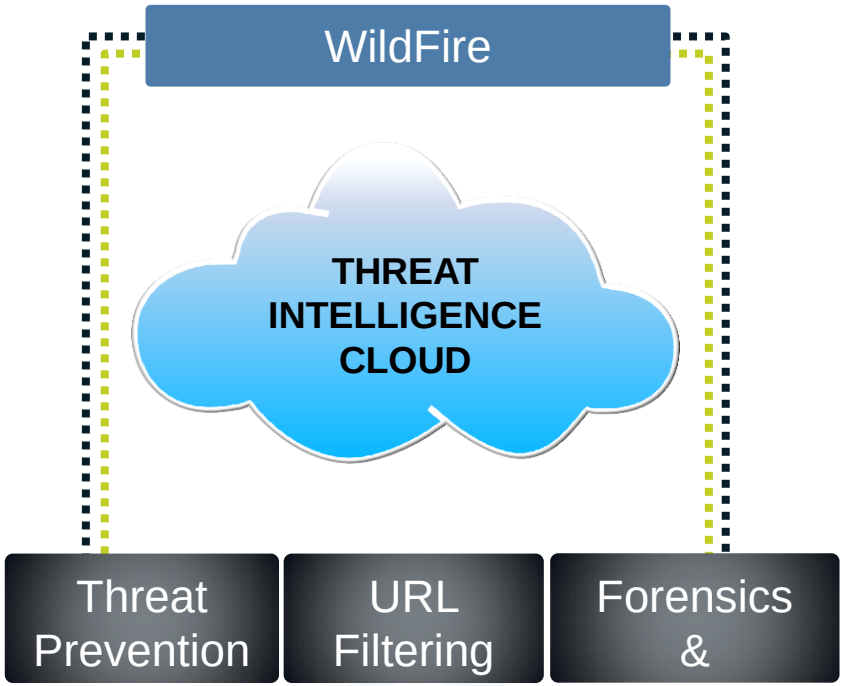
Сервис Wildfire в цифрах

7,500+
корпоративных клиентов сервиса в мире

31,000+
NGFW – сенсоры и источники файлов

5-15 мин.
время реакции Wildfire на новую угрозу

120,000
сигнатур безопасности каждые 15 мин.



до 330,000+
вариантов вредоносов закрывает 1 сигнатура (≠ hash, URL)

150,000
сигнатур DNS и URL каждые 15 мин.

до 77.5%
вредоносов неизвестны другим AV (VirusTotal)

60+ Ext. Feeds
AV концорциум, и др.

paloalto NETWORKS

Wildfire: Remote Access Trojan (RAT) в Arcom

- WildFire обнаружил целенаправленную атаку на крупную производственную компанию в центральной Азии
- Вредоносное ПО было предназначено для промышленного шпионажа и кражи данных
  - Строит обратный канал
  - Принимает более 40 команд от центра управления
- Было отправлено как фишинговое электронное письмо
  - “The end of Syrian President Bashar al-Assad.exe”
- Не использовался внешний упаковщик
  - Обычно для целенаправленных атак

- Для маскировки код инжектировался в браузер по умолчанию и notepad.exe
- Command&Control в Ливан

Решение для защиты хостов нового поколения: Palo Alto Networks TRAPS

paloalto NETWORKS
the network security company™

Блокирует базовые техники – а не конкретные угрозы

Фундаментально другой подход от Palo Alto Networks

Уязвимости и эксплойты

Тысячи в год

Техники эксплуатации

Всего 2-4 техники в год

Вредоносное ПО

Миллионы в год

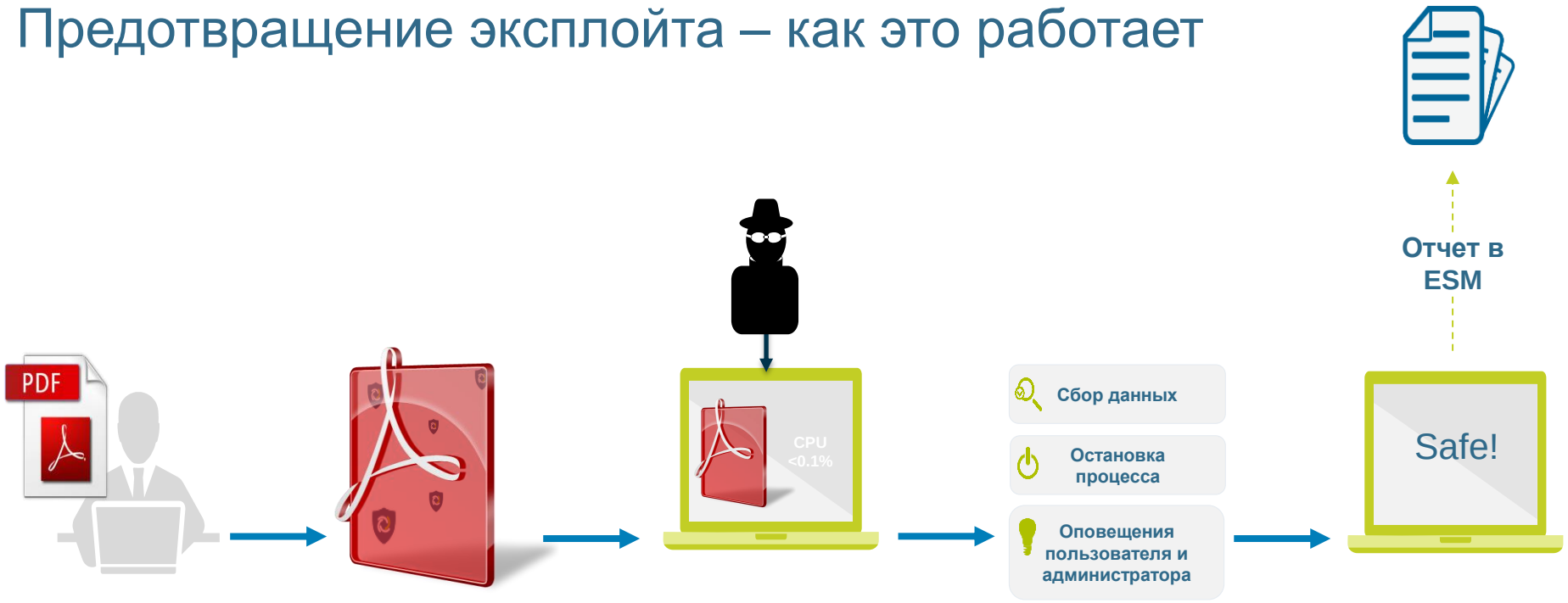
Техники работы вредоносного ПО

Всего 10-100 в год

Теперь предотвращение возможно!

paloalto NETWORKS

Предотвращение эксплойта – как это работает



Пользователь открывает документ

Traps прозрачно инжектирует ловушки в процессы

Процесс защищен, так как при попытке использования эксплойта срабатывает ловушка

Traps выполняет действия только в момент срабатывания ловушки

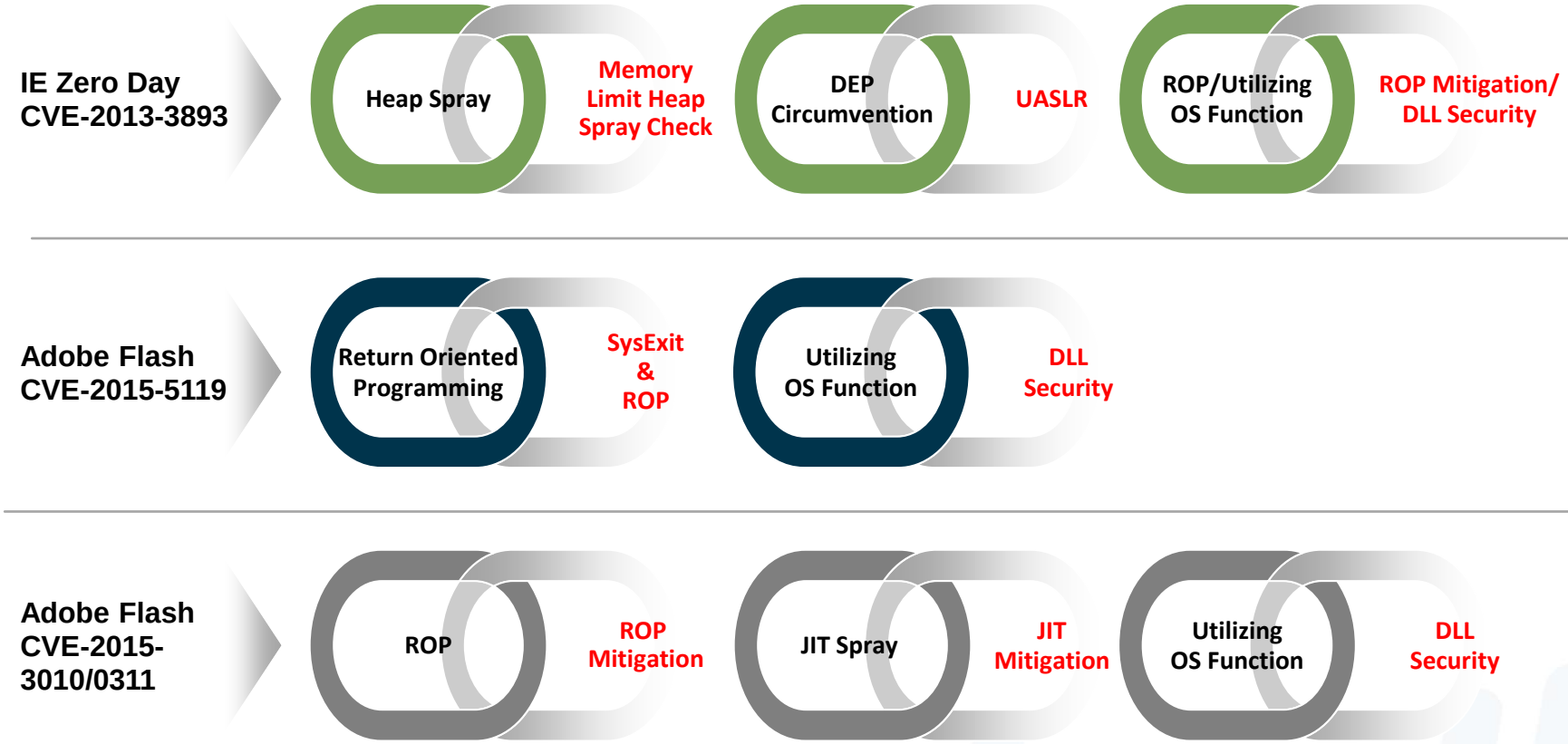
Атака остановлена до исполнения вредоносного кода

При попытке использования уязвимости срабатывает ловушка и процесс останавливается еще до запуска вредоносного кода.
Лечение / карантин не требуется!

paloalto NETWORKS

Предотвращение завтрашних эксплойтов сегодня

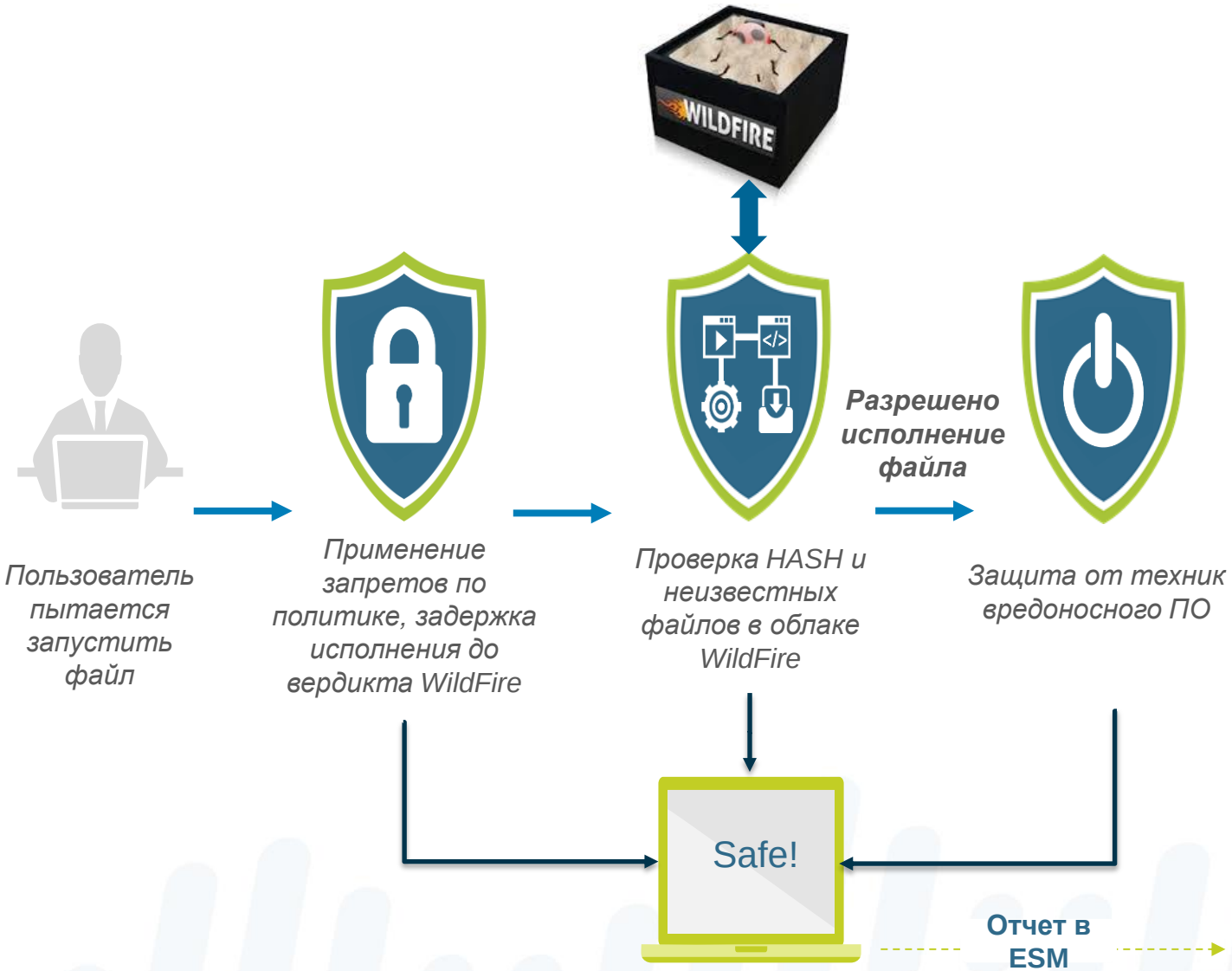
Новые 0-day эксплойты используют старые техники (2-5 в цепочке)



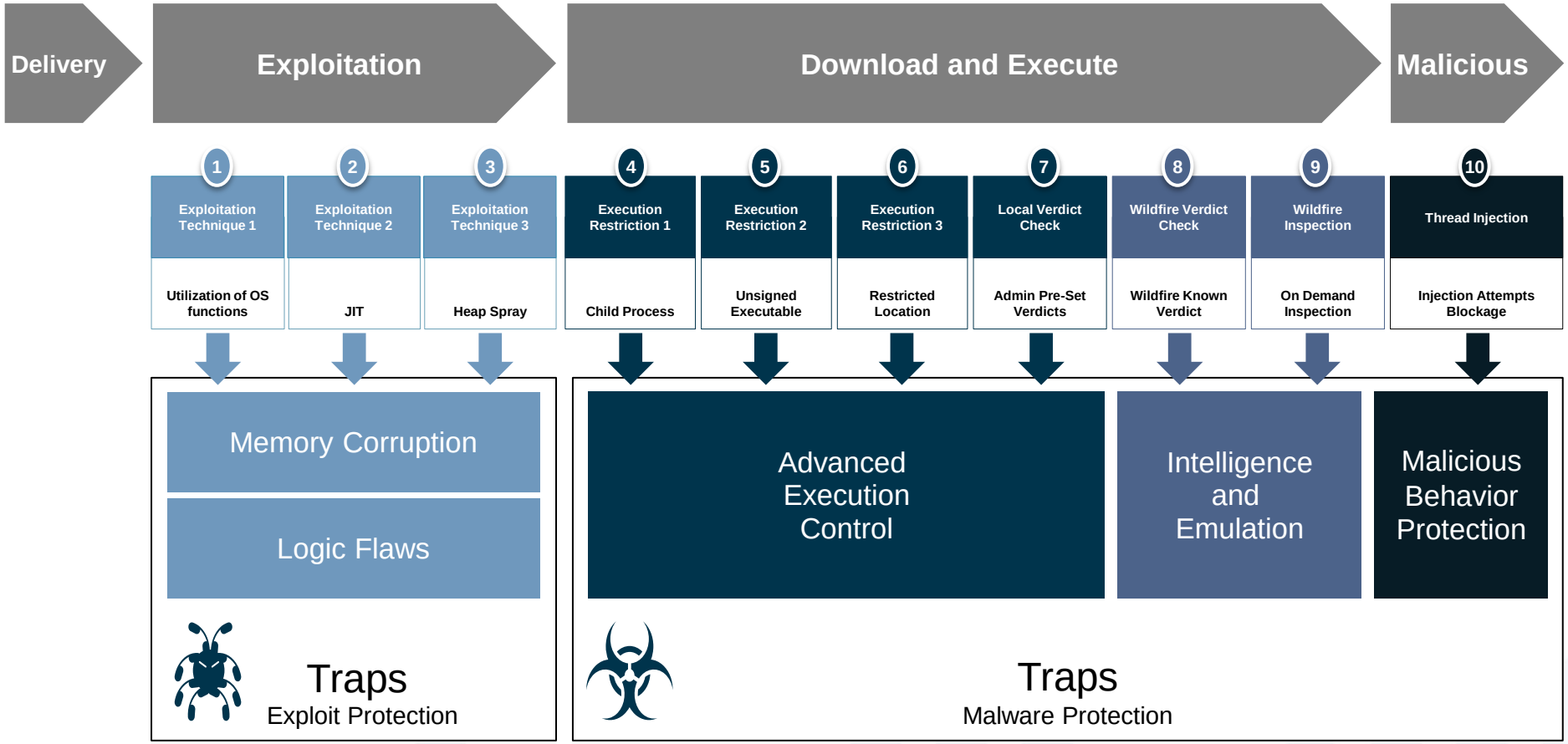
Блокирование хотя бы одной техники останавливает атаку целиком

paloalto NETWORKS

Защита от вредоносного ПО – как это работает



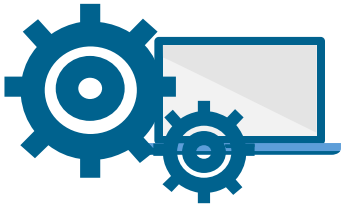
Пример: технологии Traps на разных этапах атаки



Системные требования

Все платформы и приложения на базе Windows

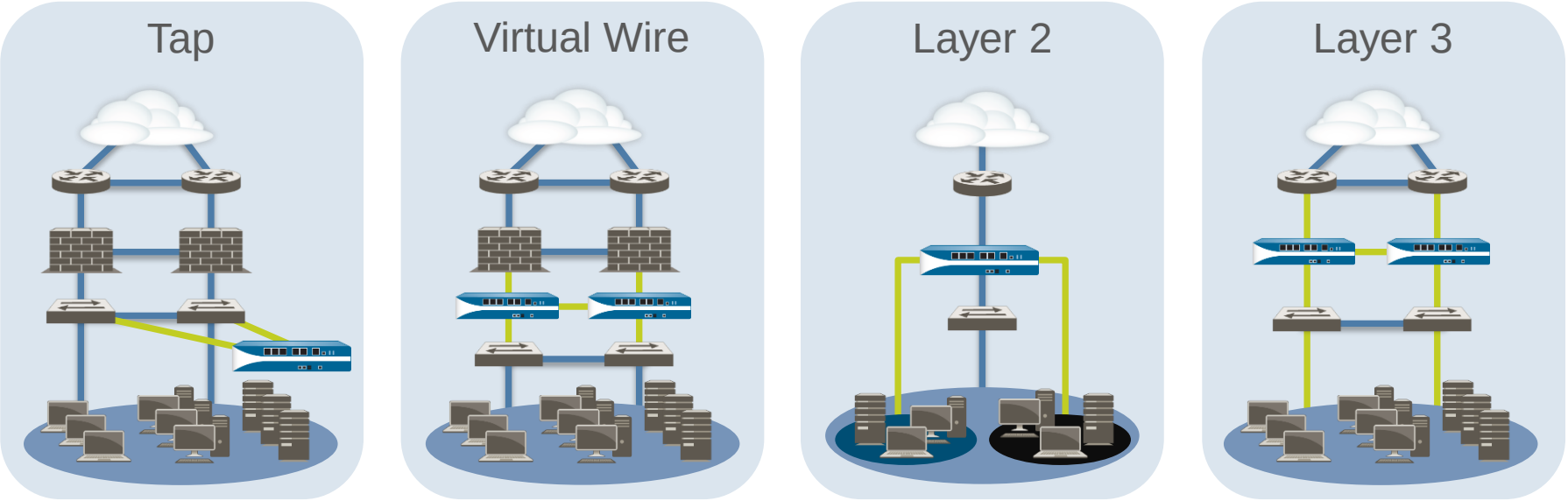
- Desktops, Servers, Terminals, VM, VDI
- ICS SCADA and POS
- XP, SP3- Windows 8.1, 32-bit & 64-bit, Windows Servers 2003 – 2015



Потребляемые ресурсы

- ~25 MB RAM
- 0.1% CPU в момент старта процесса
- I/O – очень низко
- Доступ в сеть только после предотвращения

Интеграция NGFW в сетевую инфраструктуру



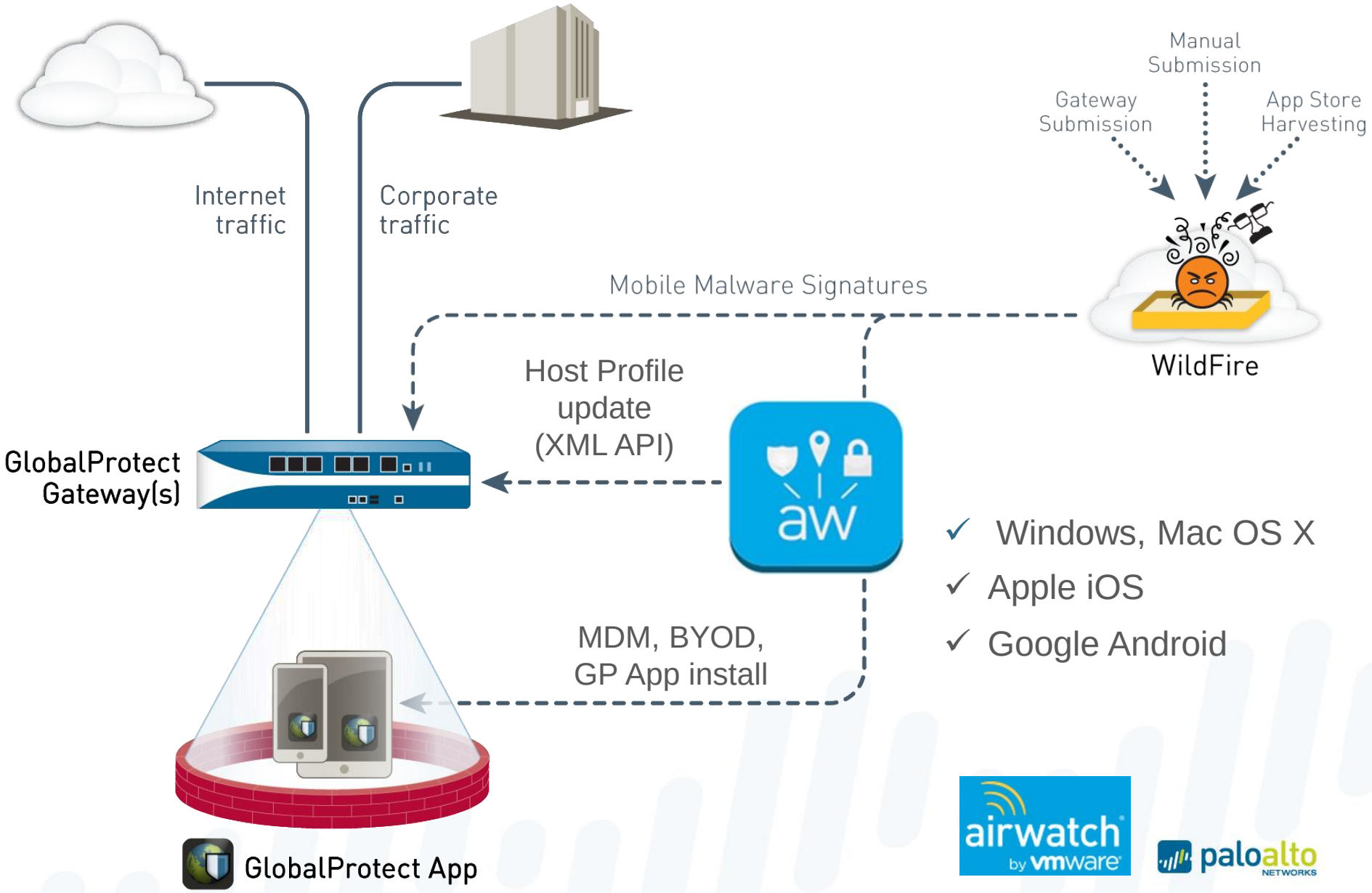
- Tap режим - SPAN порт свитча для аудита или обзора приложений в сети
- Virtual Wire - для прозрачного контроля и сохранения текущей топологии
- На 2 уровне OSI идеально для фильтрации между VLAN
- На 3 уровне OSI меняем портовые МЭ и HTTP прокси на NGFW

OSPF RIP BGP PBF PIM-SM/SMM IGMP IPv6 NAT VLAN LACP VPN QoS

- Виртуальные системы, кластер A/A, A/P

paloalto NETWORKS

Защищенный мобильный/удаленный доступ в ЦОД: GlobalProtect + AirWatch

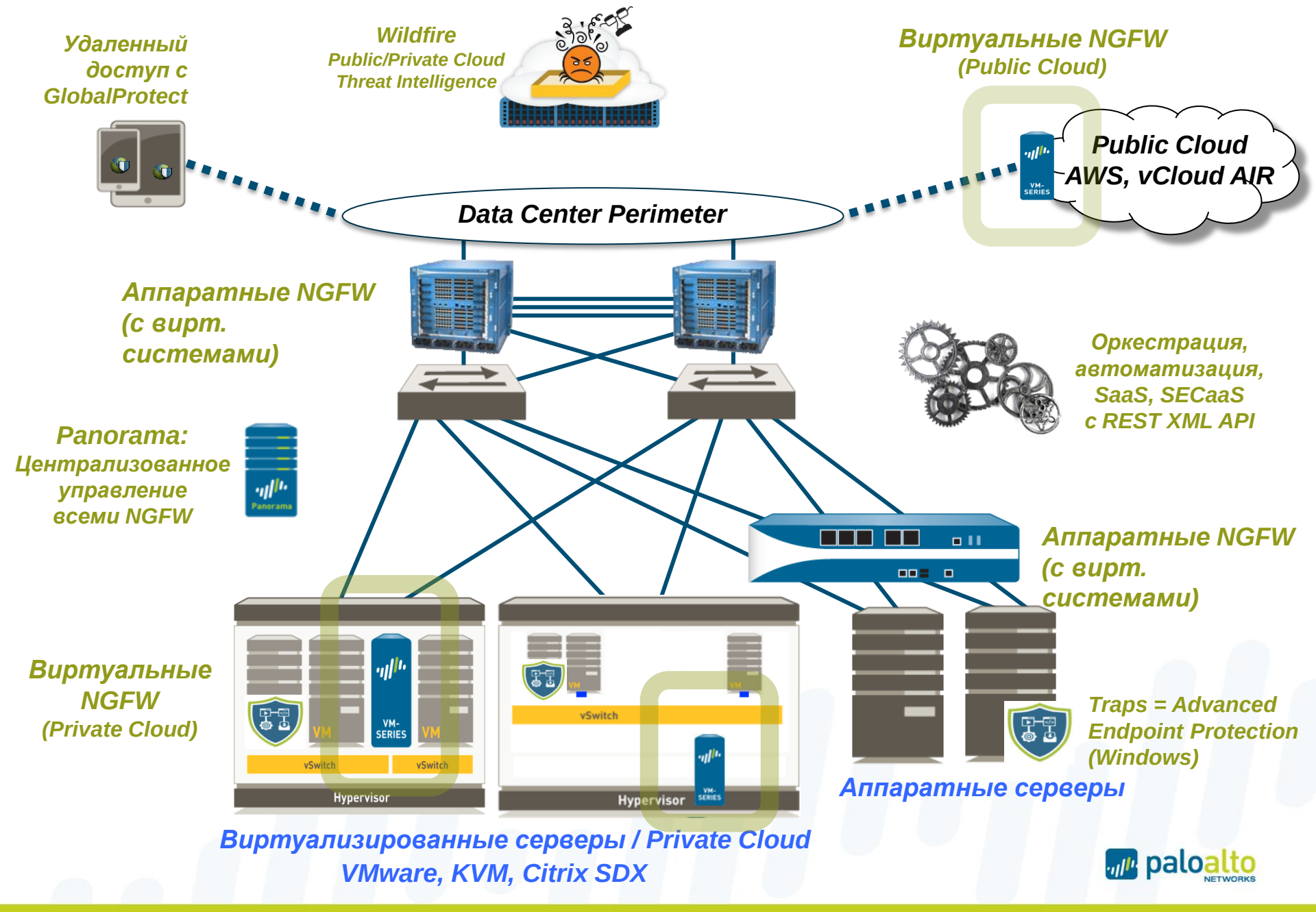


- ✓ Windows, Mac OS X
- ✓ Apple iOS
- ✓ Google Android

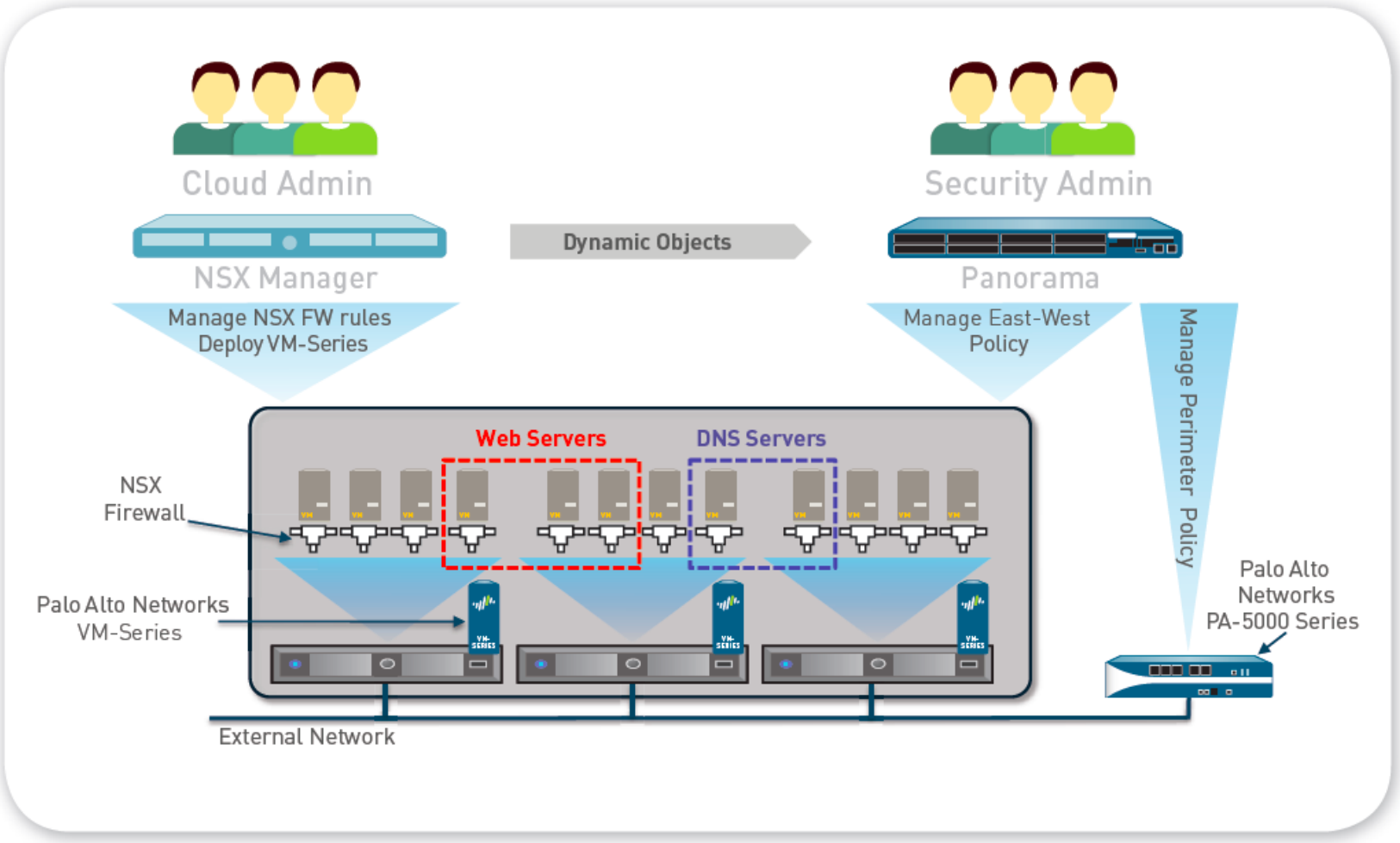
airwatch by vmware

paloalto NETWORKS

Экосистема Palo Alto Networks для защиты ЦОД



Защита виртуальных ЦОД:
Palo Alto Networks NGFW + VMware NSX



Пример крупнейшего внедрения NGFW + VMware NSX

How Columbia Sportswear enhances security with 'software defined data centre' approach

American retailer will save millions of dollars by swapping physical infrastructure for software managed systems

By Matthew Finnegan | Computerworld UK | Published 09:05, 01 April 15

http://www.computerworlduk.com/news/infrastructure/how-columbia-sportswear-will-enhances-security-with-software-defined-data-centre-approach-3606103/

Networking

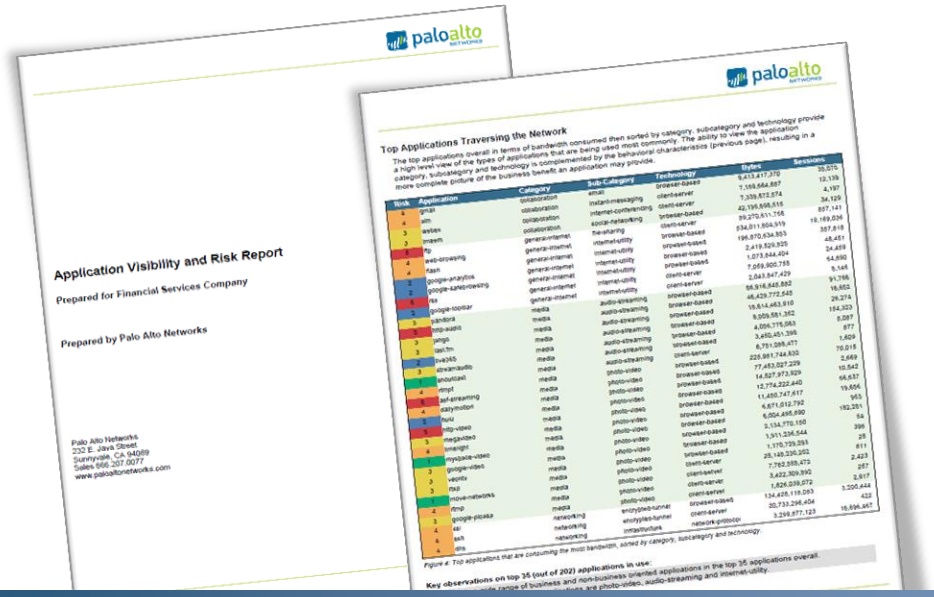
Security and micro-segmentation is one of the compelling adoption arguments for SDDC

By Networks Asia staff | Wednesday, August 27, 2014 - 08:54

http://www.networksasia.net/article/security-and-micro-segmentation-one-compelling-adoption-arguments-sddc.1409100853

paloalto NETWORKS

С чего начать защиту Вашей корпоративной и технологической сети?



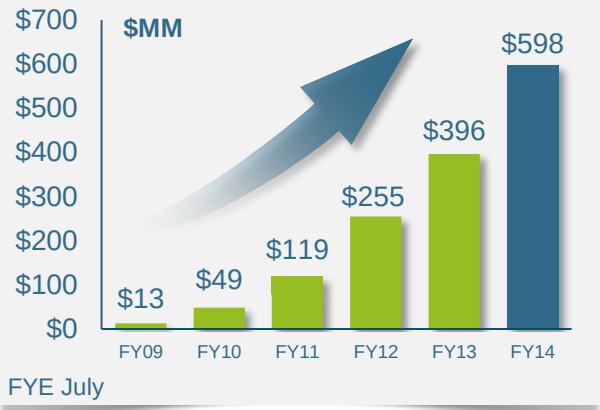
Отчет Palo Alto Networks Application Visibility Report (AVR):

- Обратитесь к нам для проведения бесплатного тестирования
- Установите МЭ Palo Alto Networks в Вашей сети в режиме анализа SPAN или виртуального провода / L2 / L3
- Мы покажем, какие приложения и угрозы в ней есть!

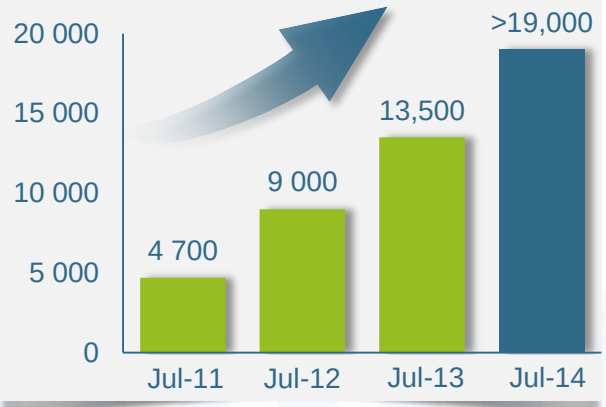
Palo Alto Networks – общая информация

Общие сведения о компании
Основана в 2005 году; первая отгрузка в 2007 Изобрела Next-Generation Firewall (NGFW)
В России и СНГ с 2010 года. Крупнейшие заказчики: Ростелеком, МТС, МЧС, РЖД, Росатом, Транснефть, Еврохим, СГК, KPMG, Казахтелеком, и др.
Офис и сервисный склад в г. Москва
Сертификация ФСТЭК по РД МЭ, НДВ, СОВ, 1 уровень защищенности персональных данных и гос. систем. Сертификат в ОАЦ РБ осенью 2015
Лидер Гартнер в категории межсетевых экранов нового поколения (4 года подряд)
1,500+ сотрудников в мире

Оборот



Количество заказчиков



Платформа безопасности нового поколения

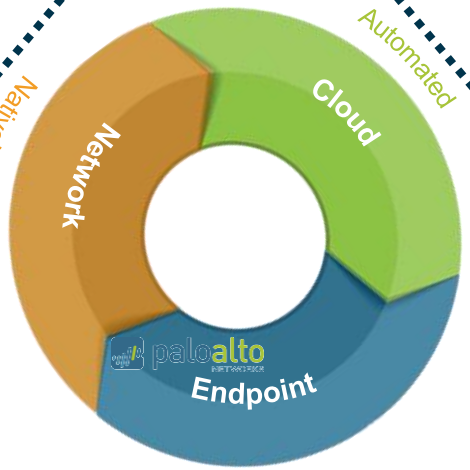
Palo Alto Networks
Next-Generation Threat Cloud

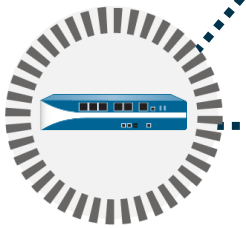
Next-Generation Threat Cloud

- Анализ подозрительных файлов в облаке
- Распространение сигнатур безопасности на МЭ

Next-Generation Firewall

- Инспекция трафика
- Контроль приложений и пользователей
- Защита от угроз 0-ого дня
- Блокировка угроз и вирусов на уровне сети





Palo Alto Networks
Next-Generation Firewall

Next-Generation Endpoint

- Инспекция процессов и файлов
- Защиты от известных и неизвестных угроз
- Защиты стационарных, виртуальных и мобильных пользователей
- Интеграция с облачной защитой от угроз

Palo Alto Networks
Next-Generation Endpoint

paloalto NETWORKS

Платформа Palo Alto Networks не создает пробок в сети

Обеспечиваем заданную производительность при всех включенных сервисах безопасности