Межсетевые экраны нового поколения Palo Alto Networks

paloalto NETWORKS

the network security company™

О компании Palo Alto Networks

- Palo Alto Networks - это **Network Security Company**
- Команда мирового класса с богатейшим опытом в области безопасности и сетевых технологий
  - Основана в 2005 году, первый заказчик – июль 2007 года
- Специализация на межсетевых экранах нового поколения, способных распознавать и контролировать 1900+ приложениями
  - Межсетевой экран – ключевой элемент инфраструктуры сетевой безопасности
  - Использует инновационные технологии: App-ID™, User-ID™, Content-ID™, WildFire™
- 10 000+ корпоративных заказчиков в 100+ странах мира, 40+ из которых внедрили решение стоимостью более $1 000 000
  - Одно из самых успешных размещений на Нью-Йоркской фондовой бирже (PANW)
  - Устойчивый рост в течение 9 последних кварталов

Независимые тесты и рекомендации

2014 Magic Quadrant for Enterprise Network Firewalls

Figure 1. Magic Quadrant for Enterprise Network Firewalls

Source: Gartner (April 2014)

Решения Palo Alto Networks протестированы как NGFW и IPS и рекомендованы NSS Labs.

Palo Alto Networks в России

- Более 4 лет на российском рынке
- 50+ текущих крупнейших корпоративных и государственных заказчиков, в т.ч.

Ростелеком (Электронное Правительство), МТС, МЧС, РЖД, Аэроэкспресс Еврохим, СГК, Банк Авангард, СДМ Банк, СМП Банк, KPMG, ФАС и т.д.;

- Локальный офис, большой пул демо-оборудования старших моделей
- Развитая экосистема партнеров (Gold, Platinum)
- Тех. поддержка 24 x 7 x 365, склад RMA в РФ
- 2 авторизованных учебных центра, курсы на русском языке каждые 2 мес.

Сертификат ФСТЭК и НДВ на МЭ и IPS (PA-5000/2000/500):

- АС класса защищенности до 1Г включительно;
- ИСПДн до 1 уровня защищённости включительно (соответствие 152-ФЗ, ППРФ-1119, приказу ФСТЭК № 21).

Анализ приложений в корпоративных сетях

Application Usage & Threat Report

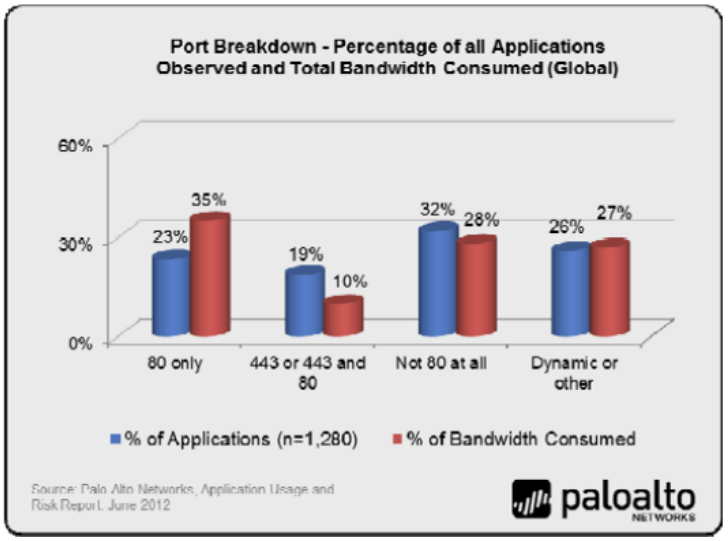
paloalto NETWORKS

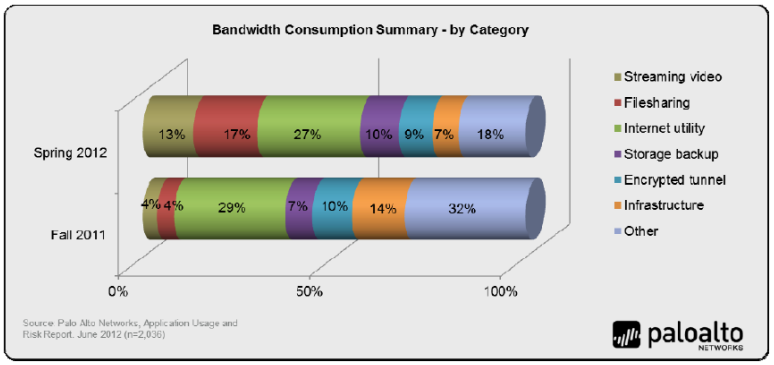
www.paloaltonetworks.com/aur

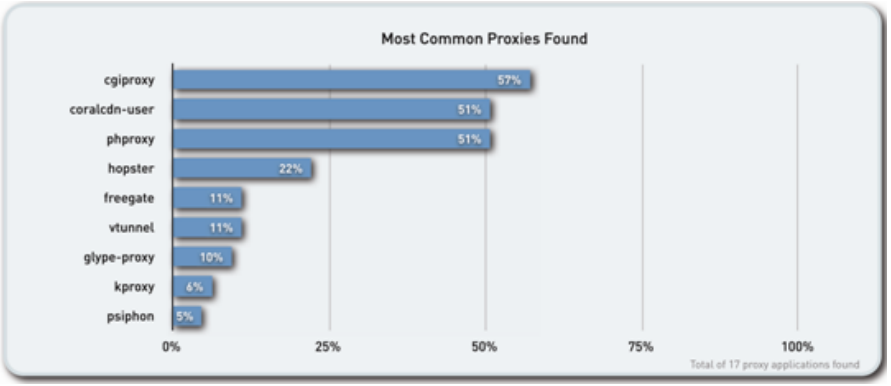
www.paloaltonetworks.com/app-usage-risk-report-visualization

Контроля приложений нет

- Анализ трафика 2000+ организаций: что происходит в современной сети?
  - 68% приложений (бизнес и пользовательских) для работы используют порты 80 и 443 или динамические порты, в т.ч. потоковое видео (13% пропускной способности)
  - Приложения, помогающие обойти политики безопасности, доступны каждому (бесплатные прокси – 81%, удаленный доступ к рабочему столу 95%, SSL туннели)
  - Очень широко распространены файл-обменные сети (P2P – 87%; браузерные)
  - 80+ социальных сетей (растет число, функциональность, нагрузка на сеть)





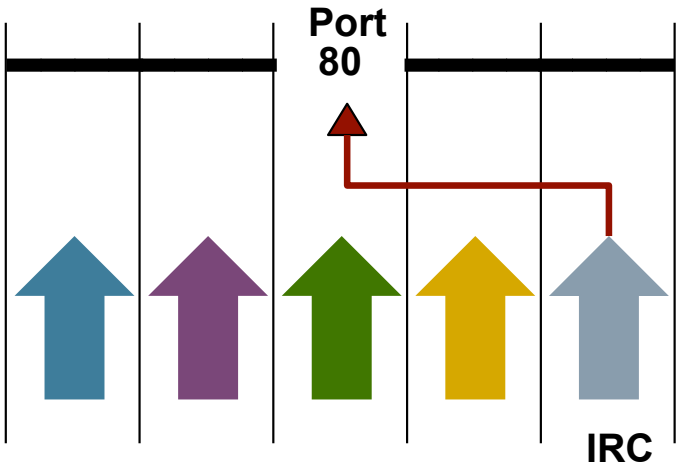


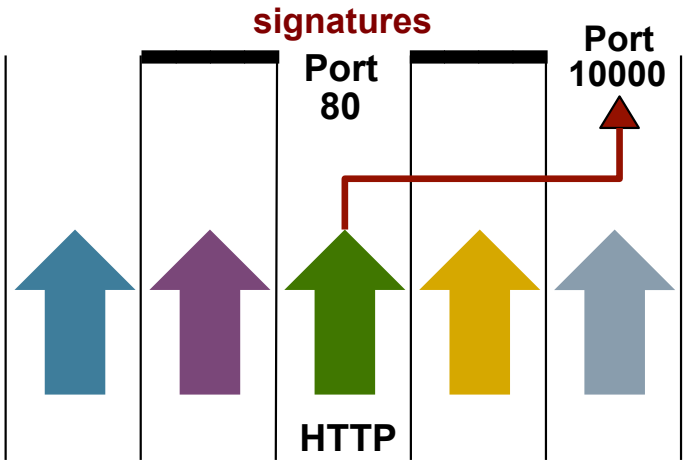
Риски использования таких приложений: непрерывность бизнеса, потери данных, продуктивность, финансовые затраты

paloalto NETWORKS

Техники уклонения от средств защиты

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



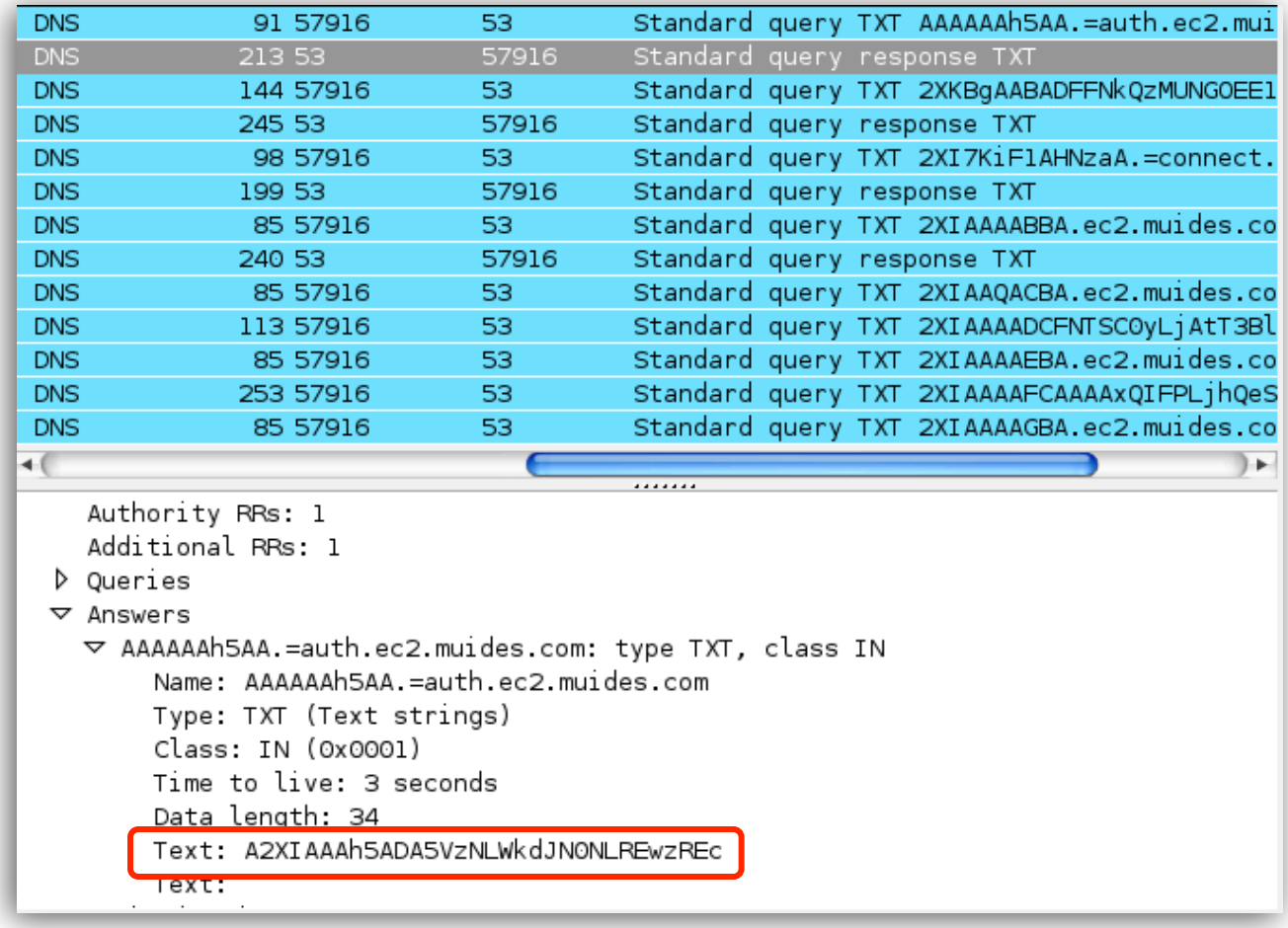


paloalto NETWORKS

Использование туннелирования поверх DNS

Примеры

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



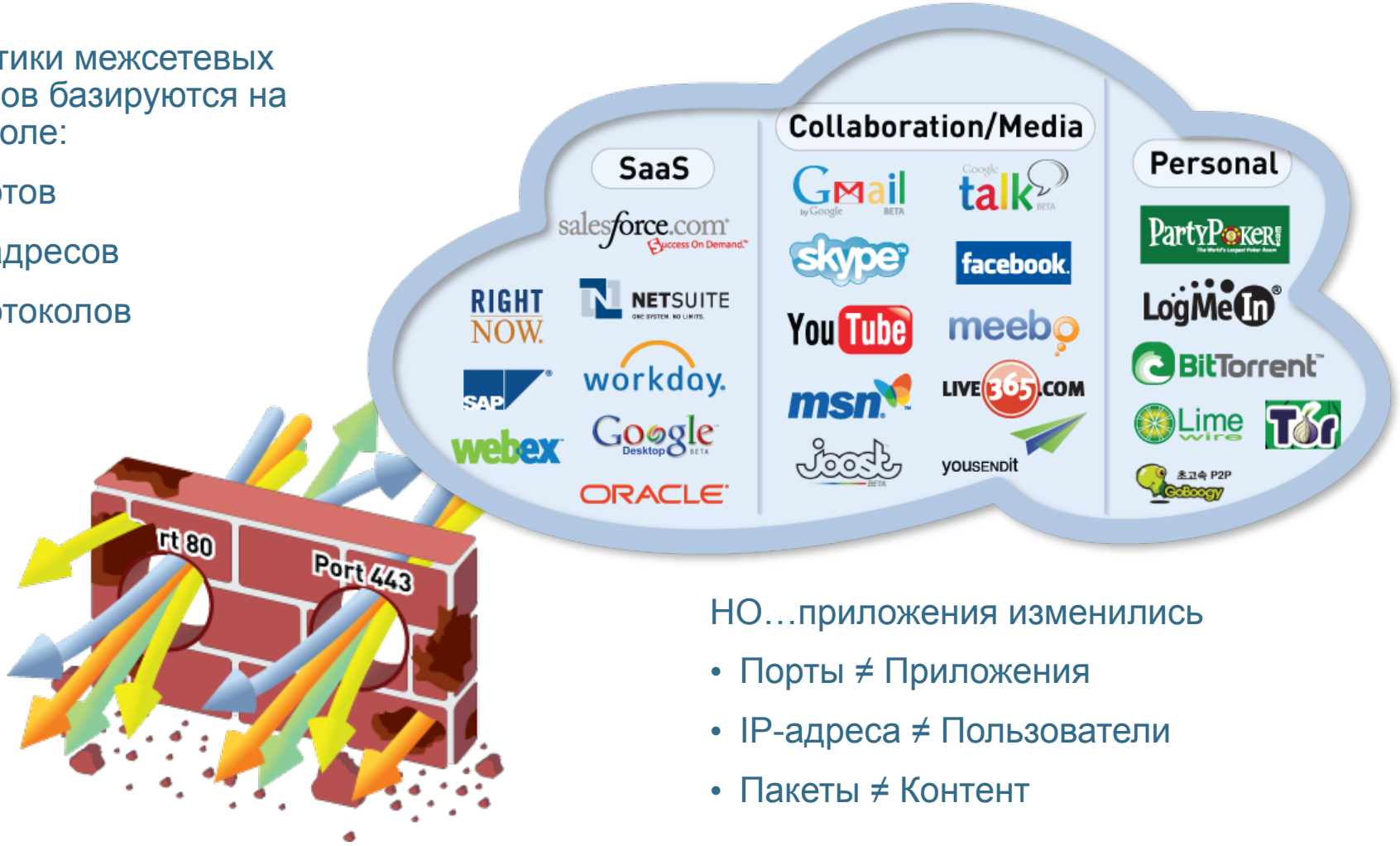
Использование рекурсивных запросов для передачи инкапсулированных сообщений по TCP в запросах удаленному DNS серверу и ответах клиенту

paloalto NETWORKS

Приложения изменились, а межсетевые экраны традиционных вендоров - нет

Политики межсетевых экранов базируются на контроле:

- Портов
- IP-адресов
- Протоколов



НО…приложения изменились

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

Межсетевой экран должен восстановить контроль над сетью

paloalto NETWORKS

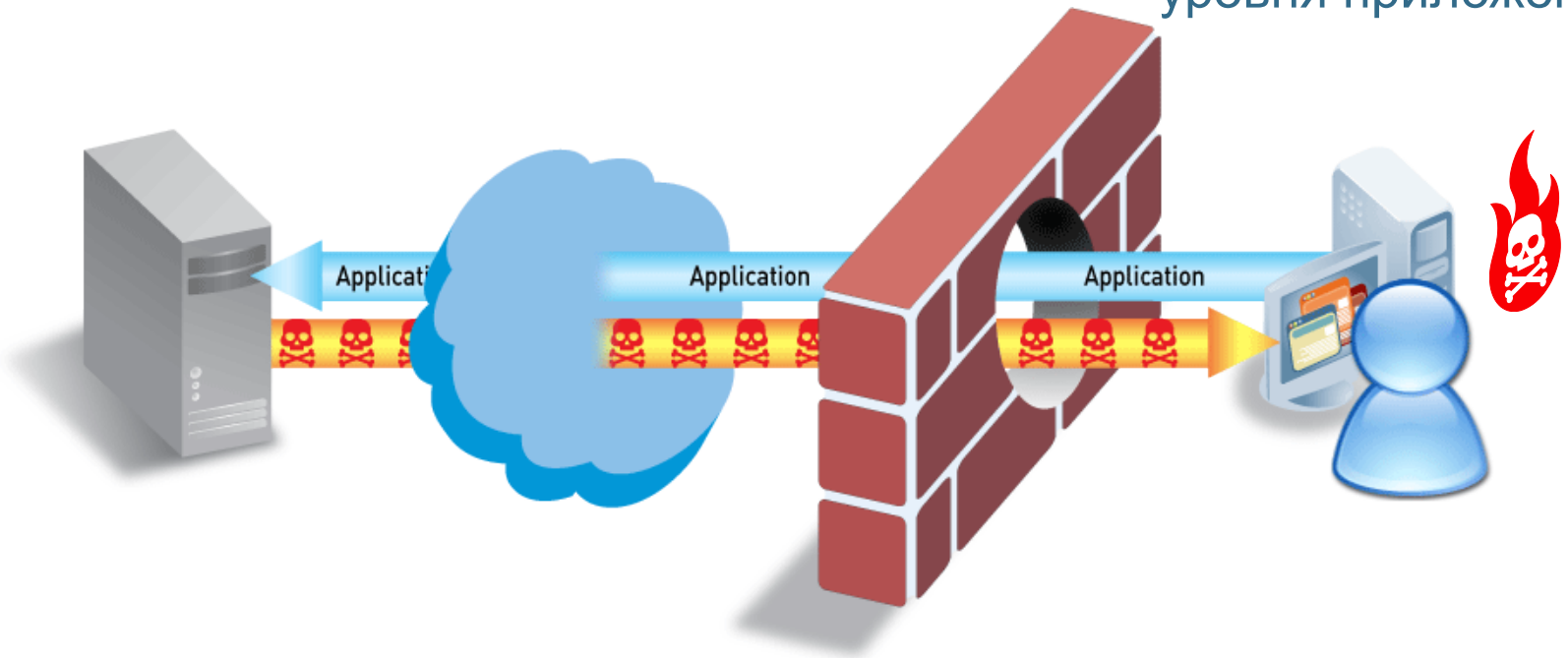
Приложения являются источником рисков

Приложения сами могут быть “угрозами”

- P2P file sharing, туннельные приложения, анонимайзеры, мультимедиа

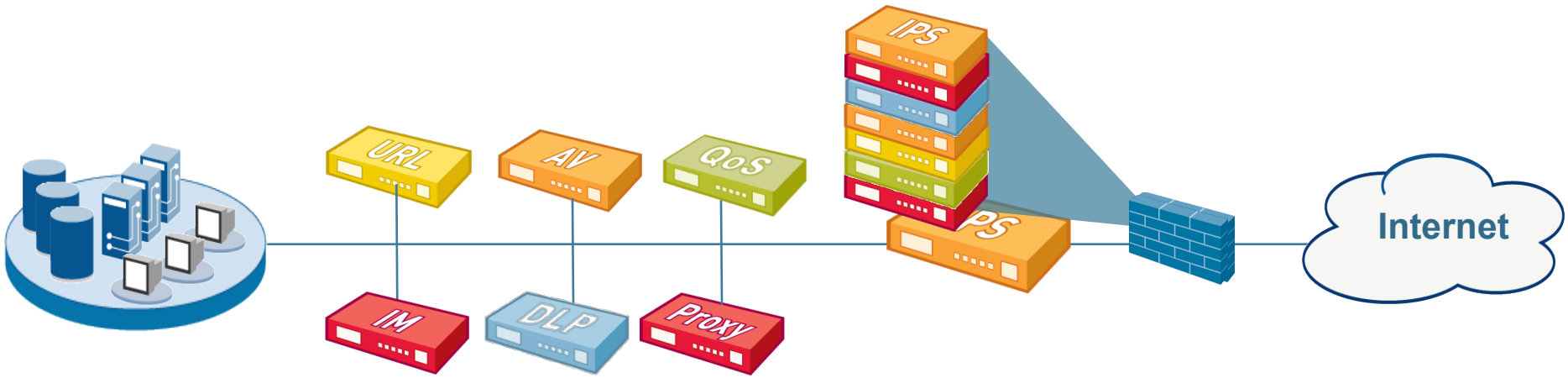
Приложения могут способствовать распространению угроз

- Qualys Top 20 уязвимостей: основные угрозы – это угрозы уровня приложений



Приложения и угрозы уровня приложений создают бреши в системе безопасности

«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 отдельных функциональных модулей в одном устройстве (UTM) делает его ОЧЕНЬ медленным

paloalto NETWORKS

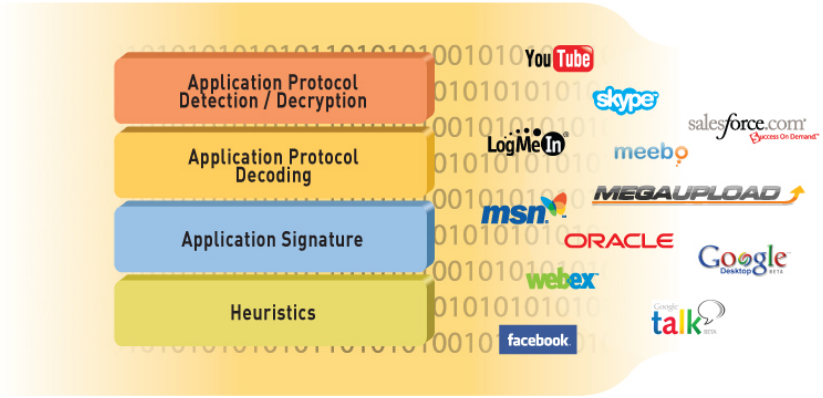
Межсетевой экран нового поколения

paloalto NETWORKS

Технологии идентификации изменили межсетевой экран

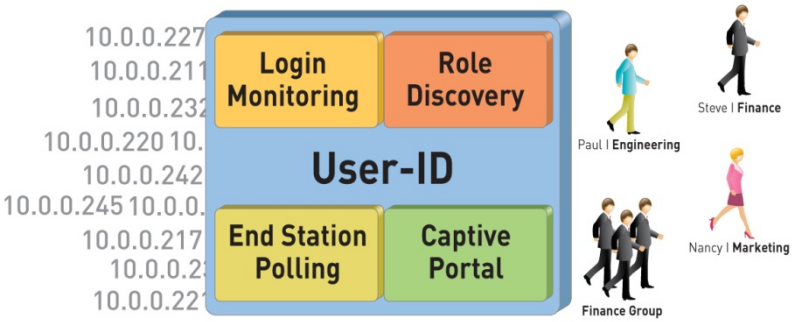
App-ID™

Идентификация приложений



User-ID™

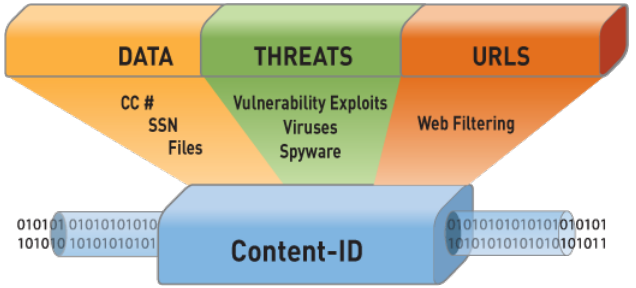
Идентификация пользователей



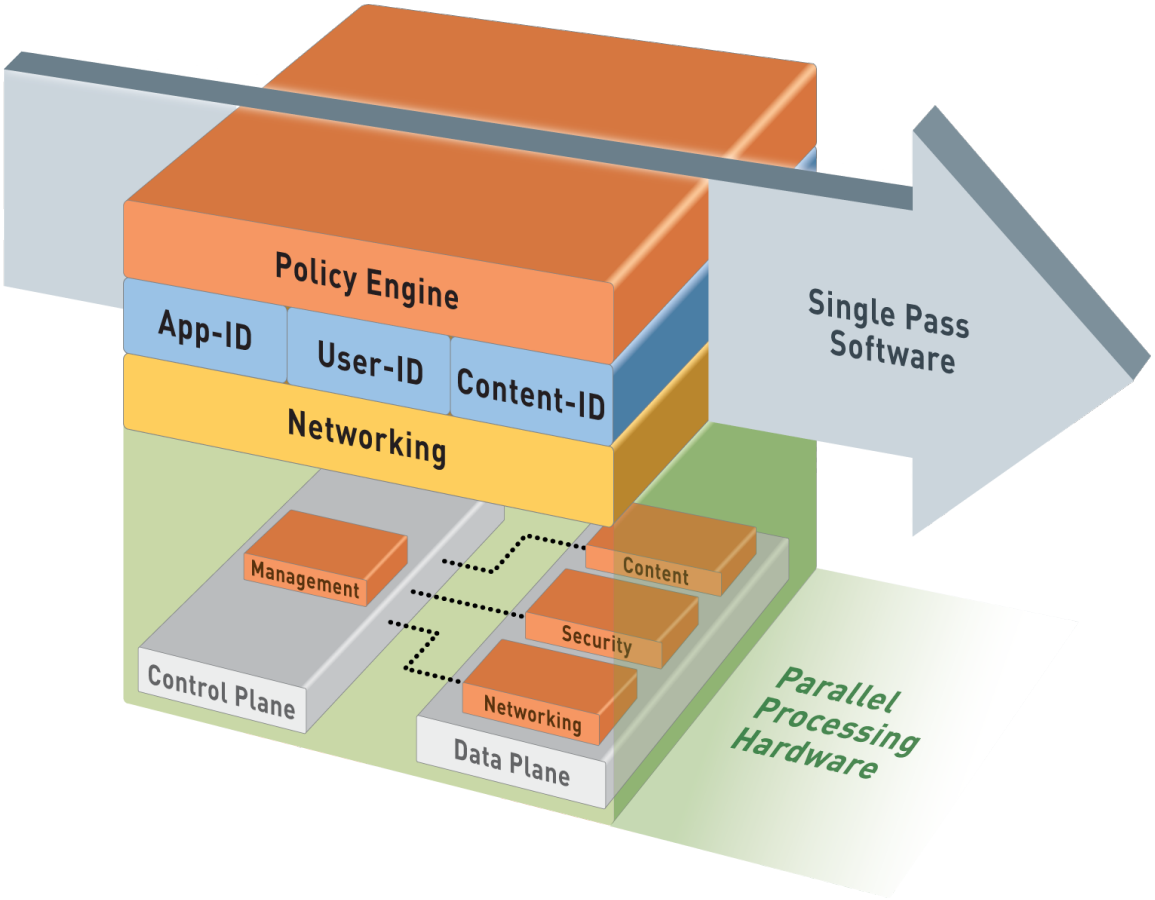
Content-ID™

Контроль данных +

SSL расшифровка



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.

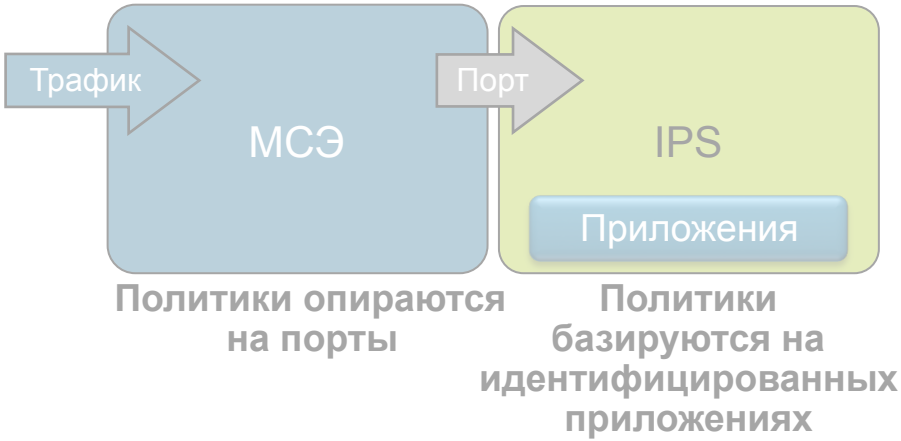
Параллельная обработка

Специализированное аппаратное обеспечение для каждой задачи

Разделение Data plane и Control plane

•До 20 Гбит/с, низкая задержка

Почему идентификация и контроль над приложениями должны быть на межсетевом экране



Контроль над приложениями как надстройка

- Портовый МСЭ + Контроль приложений (IPS) = две политики
- Приложения как угрозы
  - Искать и блокировать только то, что задано в явном виде

Последствия

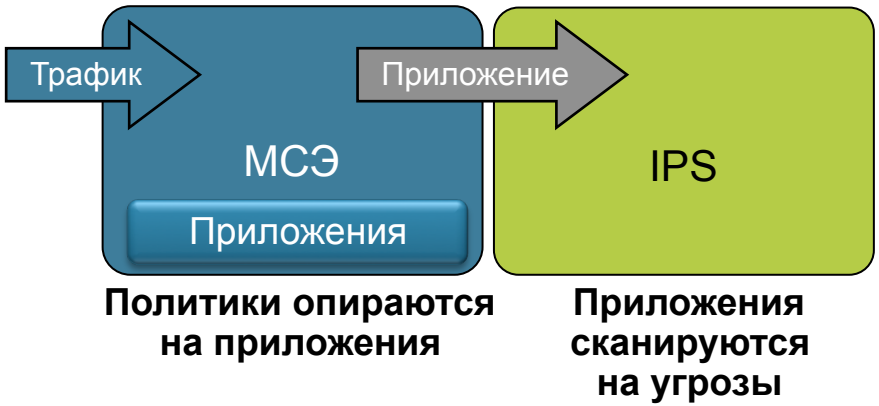
- Разрешение / запрет доступа к сети базируются на неполной информации
- Нельзя «безопасно разрешить» приложения
- Два хранилища некоррелируемых логов

Контроль приложений Межсетевыми Экранами Нового Поколения

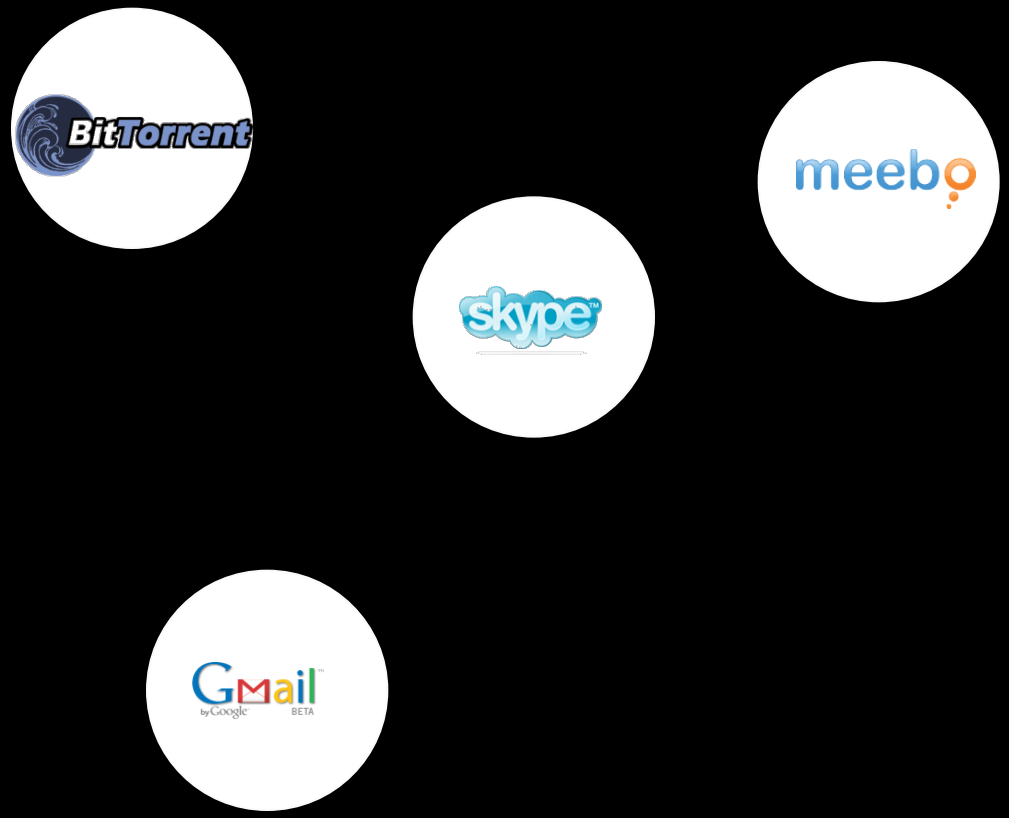
- Контроль над приложениями интегрирован в межсетевой экран = единая политика
- Идентификация приложений независимо от порта, постоянно и для всего трафика

Последствия

- Разрешение / запрет доступа к сети опираются на информацию о приложении
- Можно «безопасно разрешить» приложения



Что Вы видите… с портовым МСЭ + надстройкой IPS для распознавания приложений



Что Вы видите с полноценным Межсетевым Экраном Нового Поколения

Как строится современная целенаправленная атака на корпоративную сеть?

paloalto NETWORKS

Ключевые этапы современной сетевой атаки

1

Приманка

Завлечь использовать специальное ПО, открыть файл или перейти на веб-сайт с вредоносами

2

Эксплоит

Зараженный контент использует уязвимости установленного ПО без ведома пользователя

3

Загрузка ПО для «черного хода»

В фоне загружается и устанавливается второй вредонос

4

Установление обратного канала

Вредонос устанавливает исходящее подключение для связи с злоумышленником

5

Разведка и кража данных

Удаленный злоумышленник имеет доступ внутри сети и проводит атаку

Рекомендуемый комплексный подход к предотвращению угроз

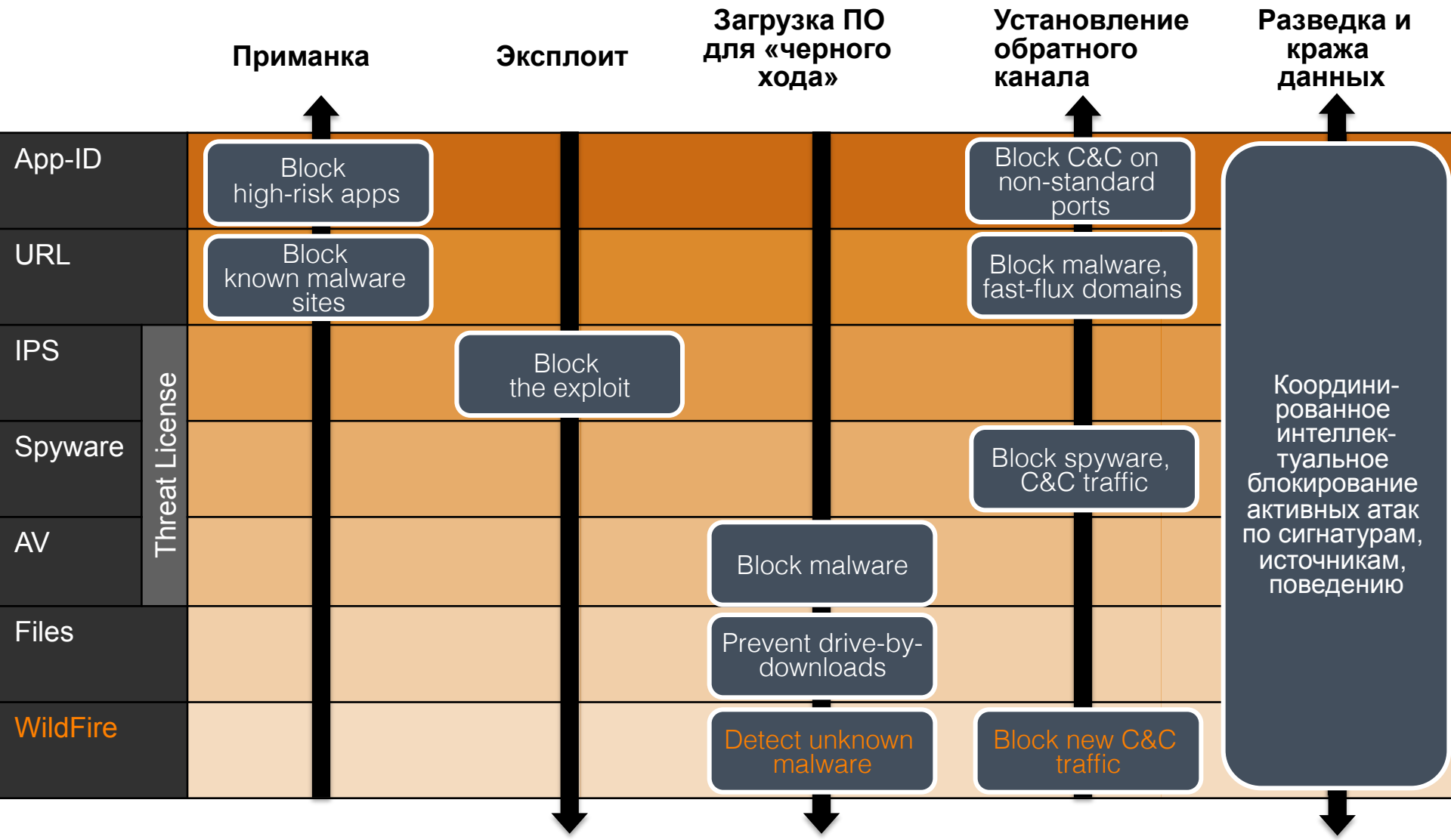
Приложения	Участники сетевого обмена	Известные угрозы	Неизвестные угрозы
• Визуализация и контроль приложений для всего трафика, по всем портам, все время	• Контроль трафика источников и назначений с учетом риска	• Блокировать эксплоиты, вредоносы, шпионское ПО и опасные файлы	• Автоматически определять и блокировать новые и измененные угрозы

Снижение риска

• Уменьшить площадь атаки • Контроль вектора угроз • Контроль методов, используемых для сокрытия угроз	• Блокировать известные сайты с вредоносами • Дешифрация SSL для сайтов с высоким риском • Обнаружить трафик к C&C серверам	• IPS, протестированный и рекомендованный NSS Labs • Потоковое сканирование на миллионы сигнатур • Блокирование угроз независимо от портов	• Анализ неизвестных файлов сервисом WildFire • Визуализация и контроль трафика неизвестных приложений • Поведенческий анализ

paloalto NETWORKS

Технологии Palo Alto Networks, применяемые для защиты от современных угроз



Анализ современного вредоносного ПО

Modern Malware Review

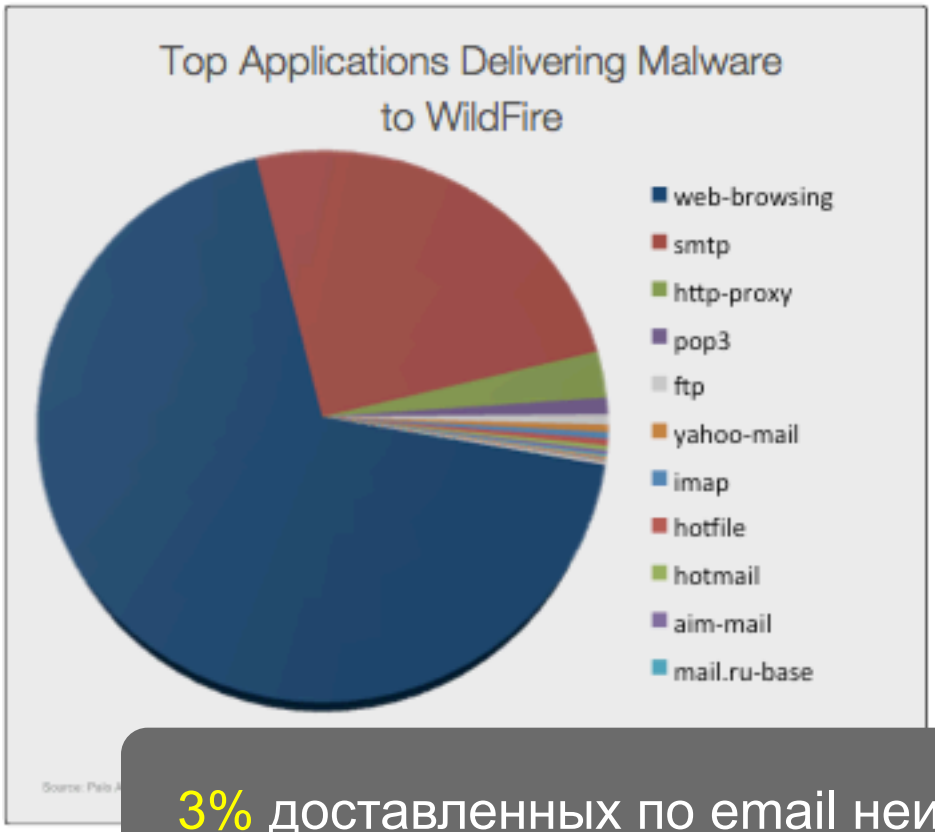
paloalto NETWORKS

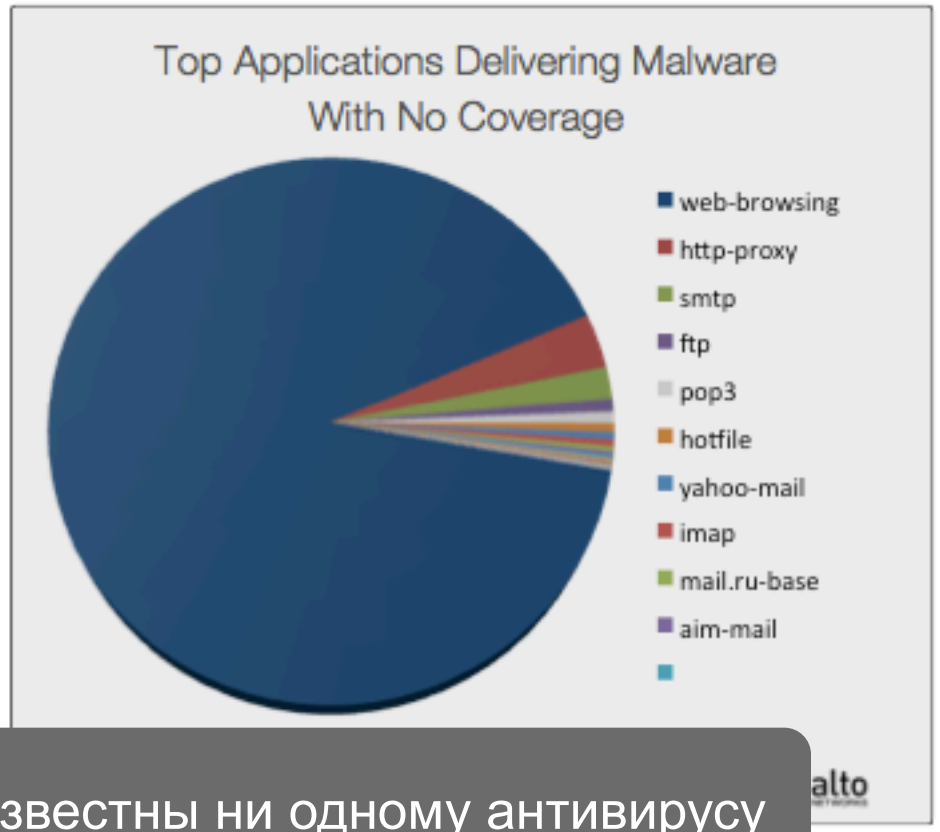
www.paloaltonetworks.com/mmr

Статистика заражений по приложениям

3 месяца анализа данных 1,000+ корпоративных сетей.

Веб-трафик – основной источник неизвестных вредоносов





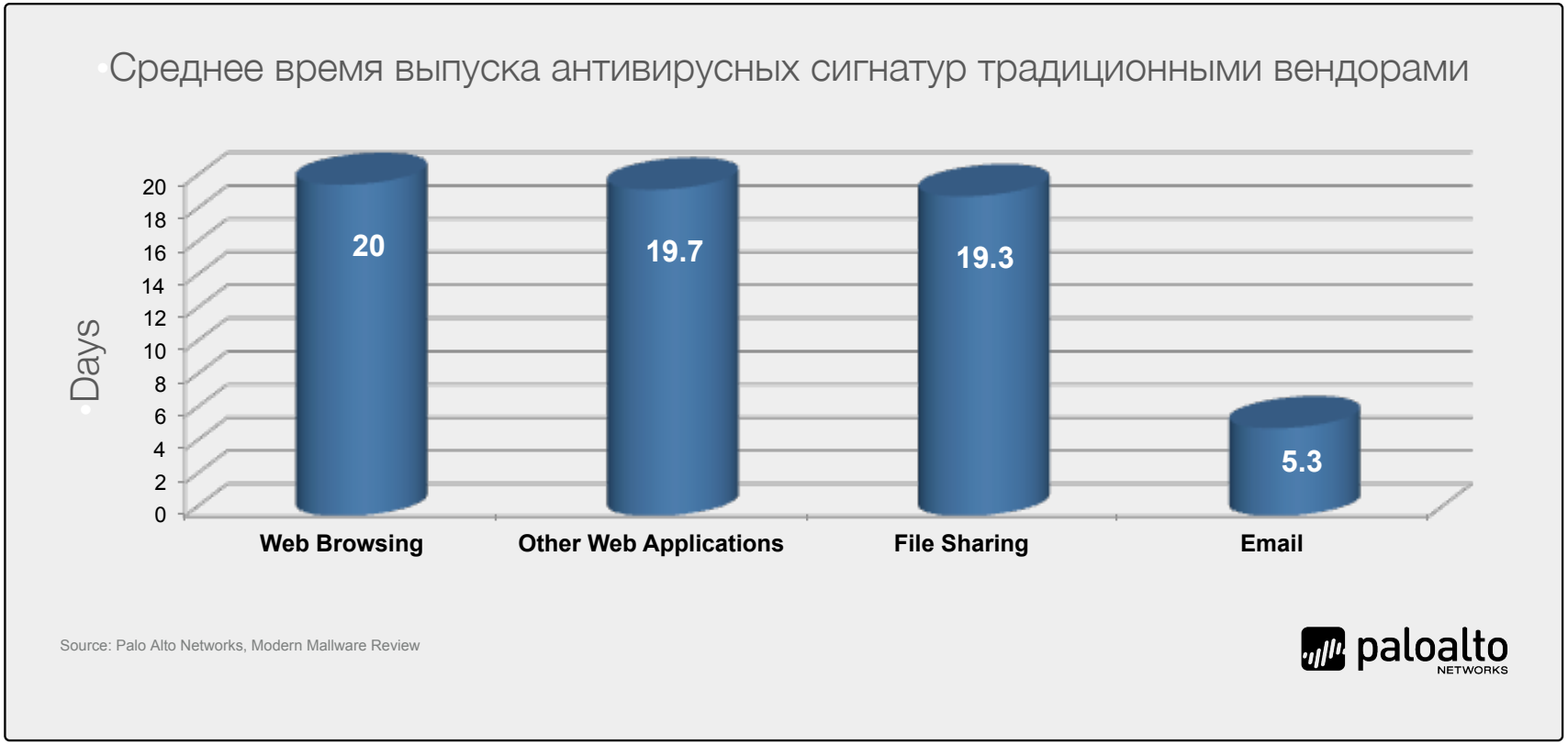
3% доставленных по email неизвестны ни одному антивирусу

vs.

Более 50% новых вредоносов доставлены через веб-браузинг

Покрытие новых вредоносов антивирусами

В среднем традиционные антивирусы в 4 раза дольше выпускают сигнатуры для новых вредоносов, распространяемых с использованием приложений, отличных от E-mail

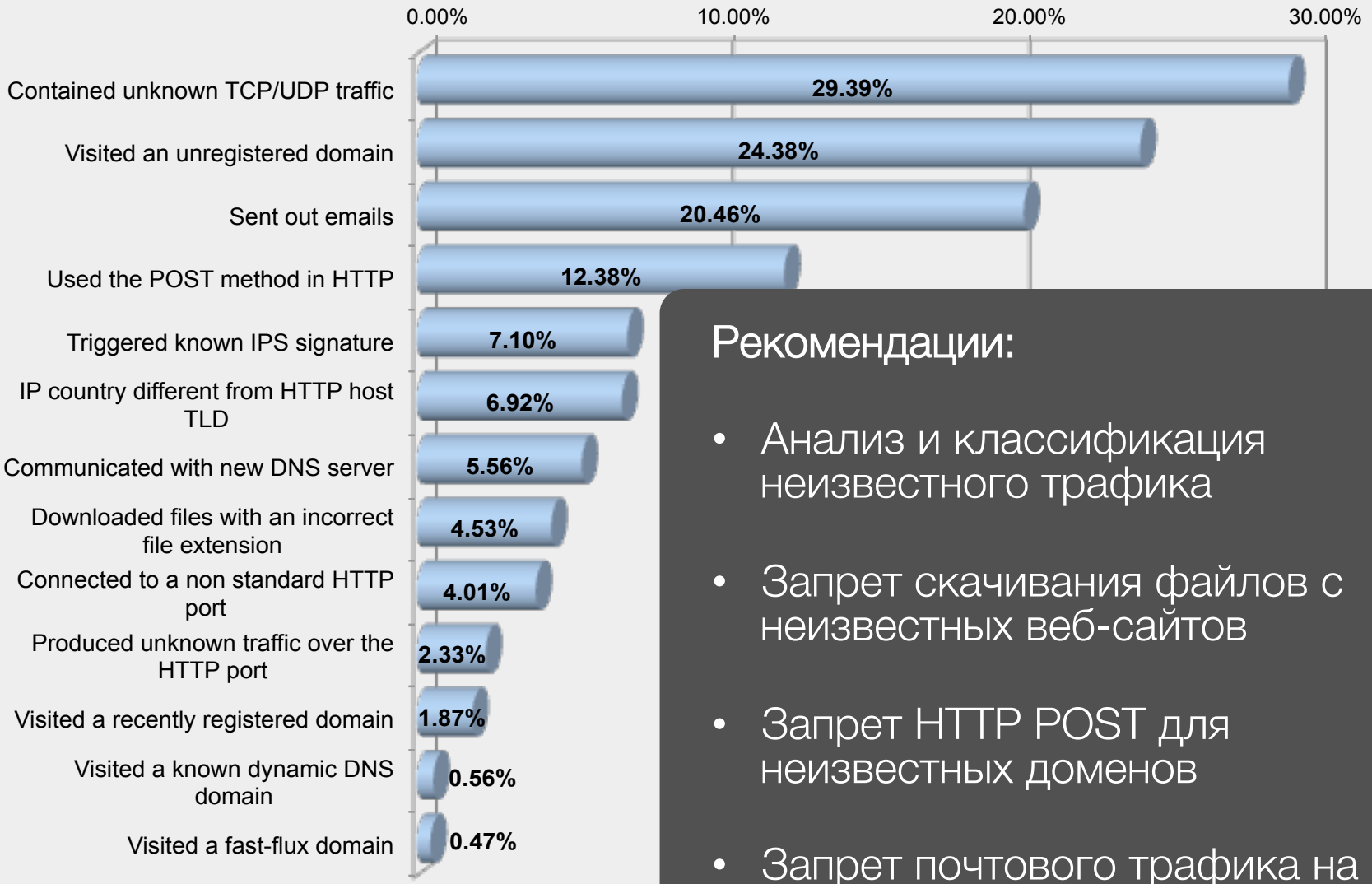


Source: Palo Alto Networks, Modern Mallware Review

paloalto NETWORKS

paloalto NETWORKS

Наиболее часто обнаруживаемое сетевое поведение вредоносов

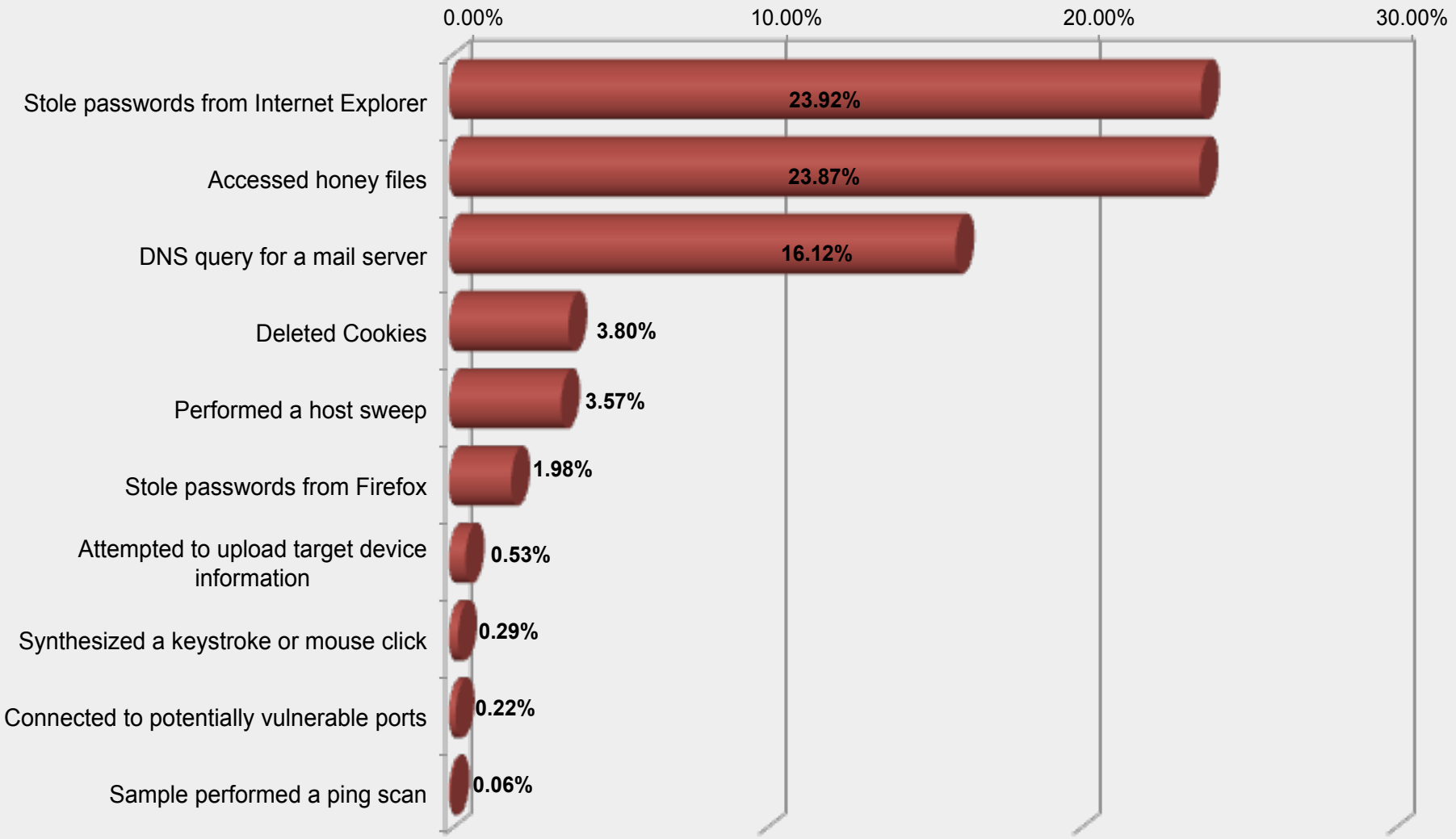


Рекомендации:

- Анализ и классификация неизвестного трафика
- Запрет скачивания файлов с неизвестных веб-сайтов
- Запрет HTTP POST для неизвестных доменов
- Запрет почтового трафика на некорпоративные серверы

Source: Palo Alto Networks, WildFire Malware Report

Наиболее часто обнаруживаемое поведение вредоносов, связанное со взломом и кражей данных



paloalto NETWORKS

Использование вредоносами нестандартных портов

FTP – самое проникающее приложение при заражениях

- Для 95% новых вредоносов, доставленных по FTP, так и не были выпущены антивирусные сигнатуры.
- 97% FTP-сессий при заражении использовали нестандартные порты (237 разных портов).

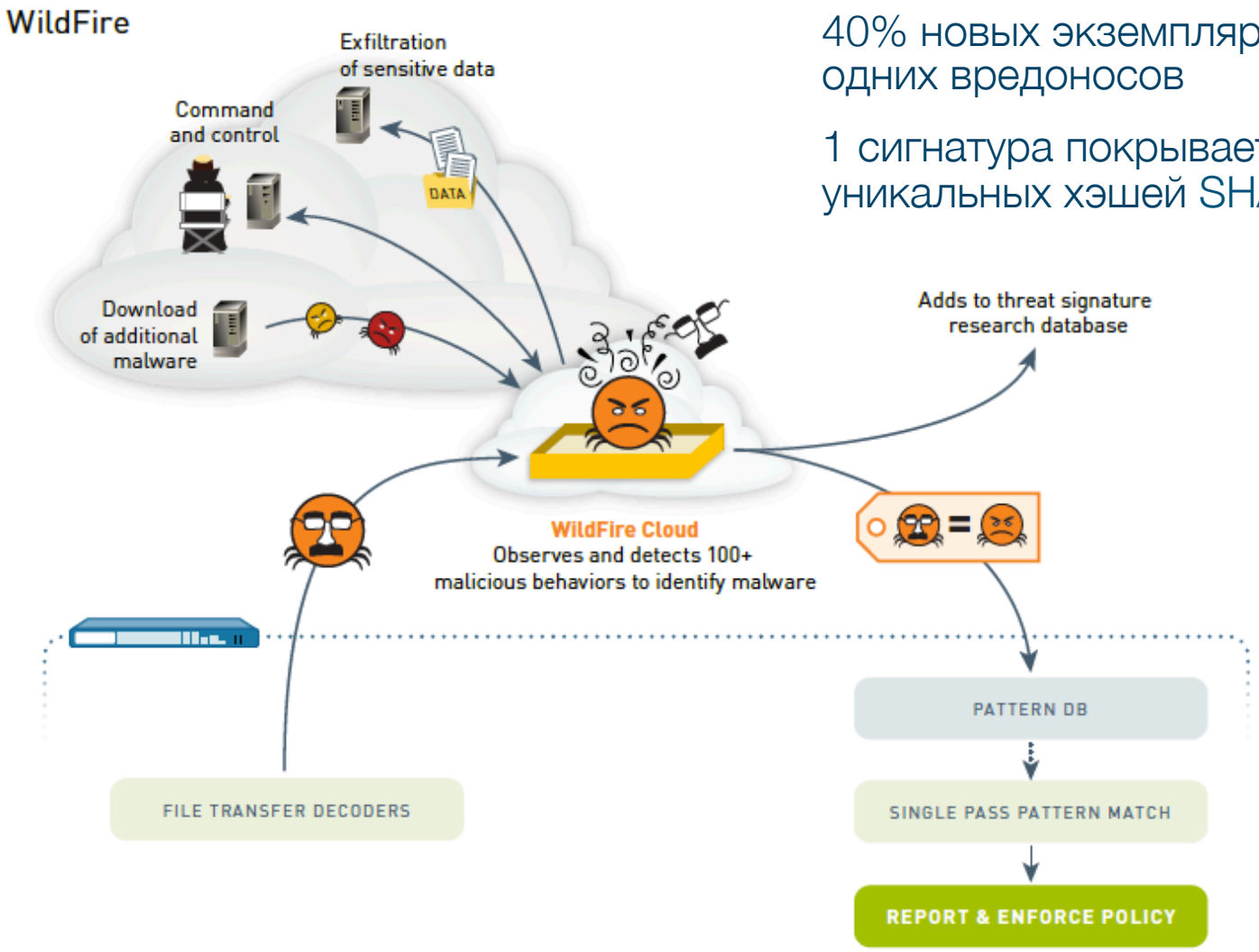
Web-browsing доставил больше вредоносов, но был менее проникающим

- 10% вредоносов доставлено с использованием 90 нестандартных портов

WildFire – облачный сервис обнаружения вредоносного ПО «нулевого дня»

paloalto NETWORKS

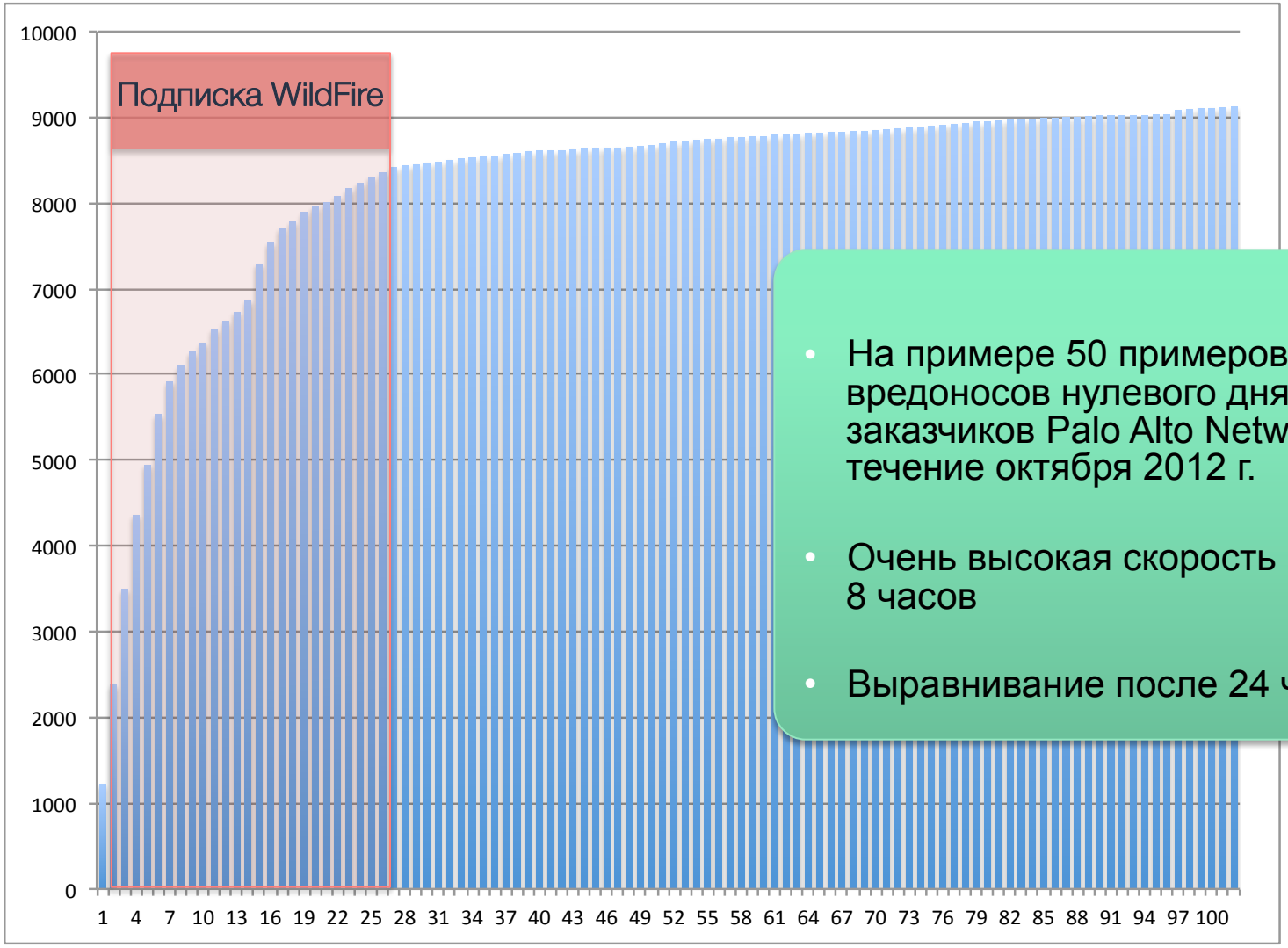
Как работает сервис WildFire



40% новых экземпляров – вариации одних вредоносов

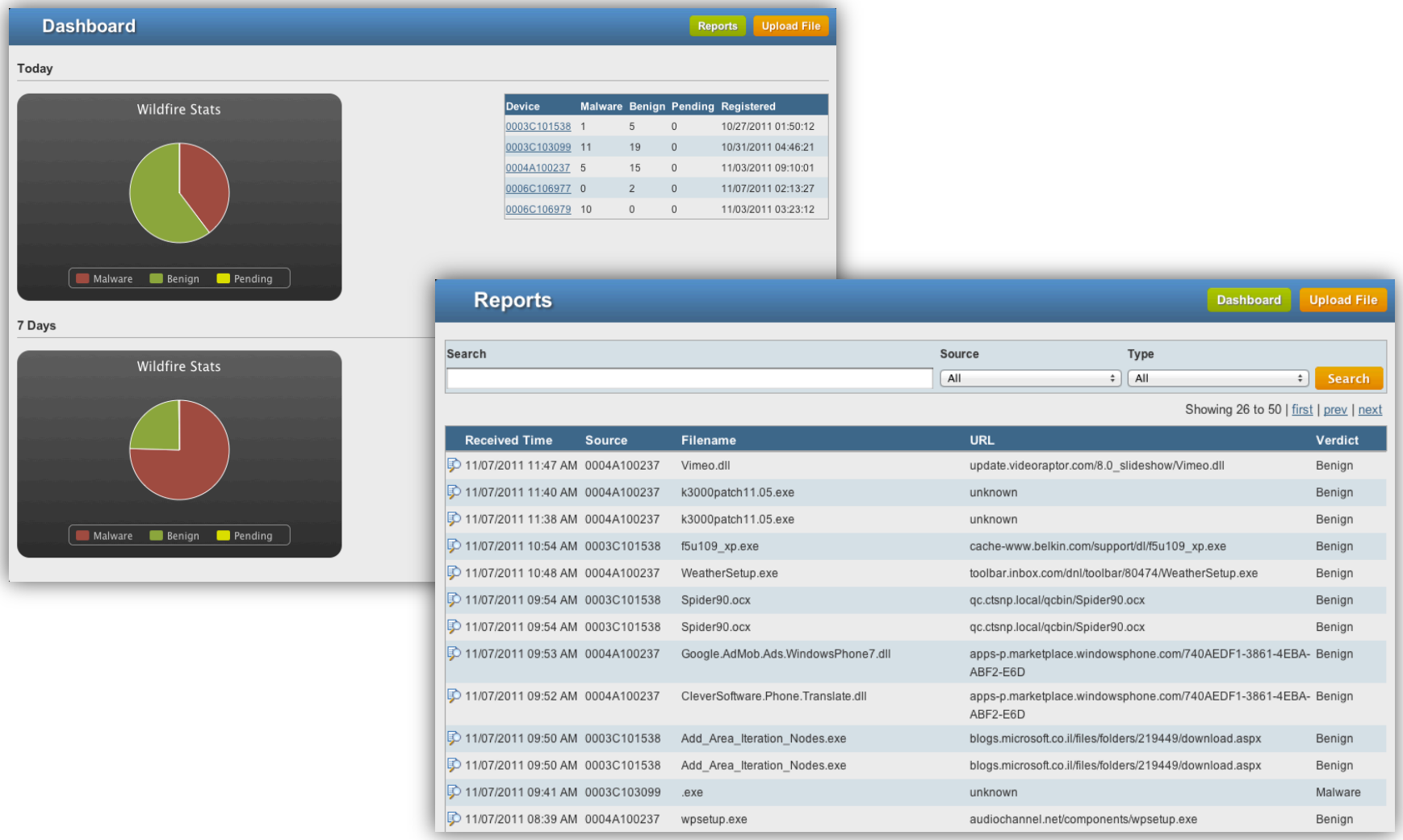
1 сигнатура покрывает до 1500+ уникальных хэшей SHA

Распространение вредоносного ПО нулевого дня



- На примере 50 примеров вредоносов нулевого дня в сетях заказчиков Palo Alto Networks в течение октября 2012 г.
- Очень высокая скорость в первые 8 часов
- Выравнивание после 24 часов

Веб-портал WildFire



Пример детального отчета о вредоносном файле

Общая информация

Имя файла, hash, URL, source & destination, вердикт (вредонос или нет), приложение

Filename:	transcript.scr		
SHA256:	4f325b6b63cf7c0daf8ca3ed72a182f05c6fe2d19f1991bce45723697571ad61		
URL:	unknown		
User:	unknown	**Received:**	11/4/2011 9:06:49 PM
Source:	133.5.184.202 :110	**Destination:**	133.6.215.213 :39887
Hostname/Mgmt. IP:	PA-2050	**Application:**	pop3
Verdict:	Malware	Virus Coverage Information	

Вердикт

Покрытие AV

Результаты анализа поведения

Список подозрительных действий, выполненных файлом в «песочнице»

Created an executable file in Windows folder
Stole saved user passwords from Internet Explorer
Created or modified files
Spawned new processes
Masqueraded as a Windows system program
Modified Windows registries
Modified registries or system configuration to enable auto start capablity
Accessed honey files
Changed security settings of Internet Explorer
Changed the proxy settings for Internet Explorer
Modified the network connections setting for Internet Explorer
Sent out emails

Анализ 100+ видов поведения. Одни безвредны сами по себе, другие используются только вредоносами.

paloalto NETWORKS

Семейство платформ и функционал операционной системы

paloalto NETWORKS

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-3050

4 Gbps FW
2 Gbps threat prevention
500,000 sessions
12 copper gigabit
8 SFP interfaces

PA-3020

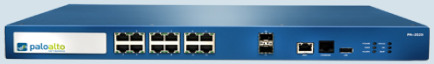
2 Gbps FW
1 Gbps threat prevention
250,000 sessions
12 copper gigabit
8 SFP interfaces

VM Series (VMware)
VM-100, 200, 300

до 1 Gbps FW
до 1 Gbps threat prevention
до 250,000 sessions
9 VMNICs (L1/L2/L3/Tap)
4094 L2/L3 sub-interfaces

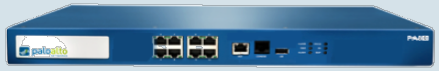
PA-2050

- 1 Гбит/с FW/500 Мбит/с предотвращение атак/ 250,000 сессий
- 4 SFP, 16 RJ-45 gigabit



PA-2020

- 500 Мбит/с FW/200 Мбит/с предотвращение атак / 125,000 сессий
- 2 SFP, 12 RJ-45 gigabit



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

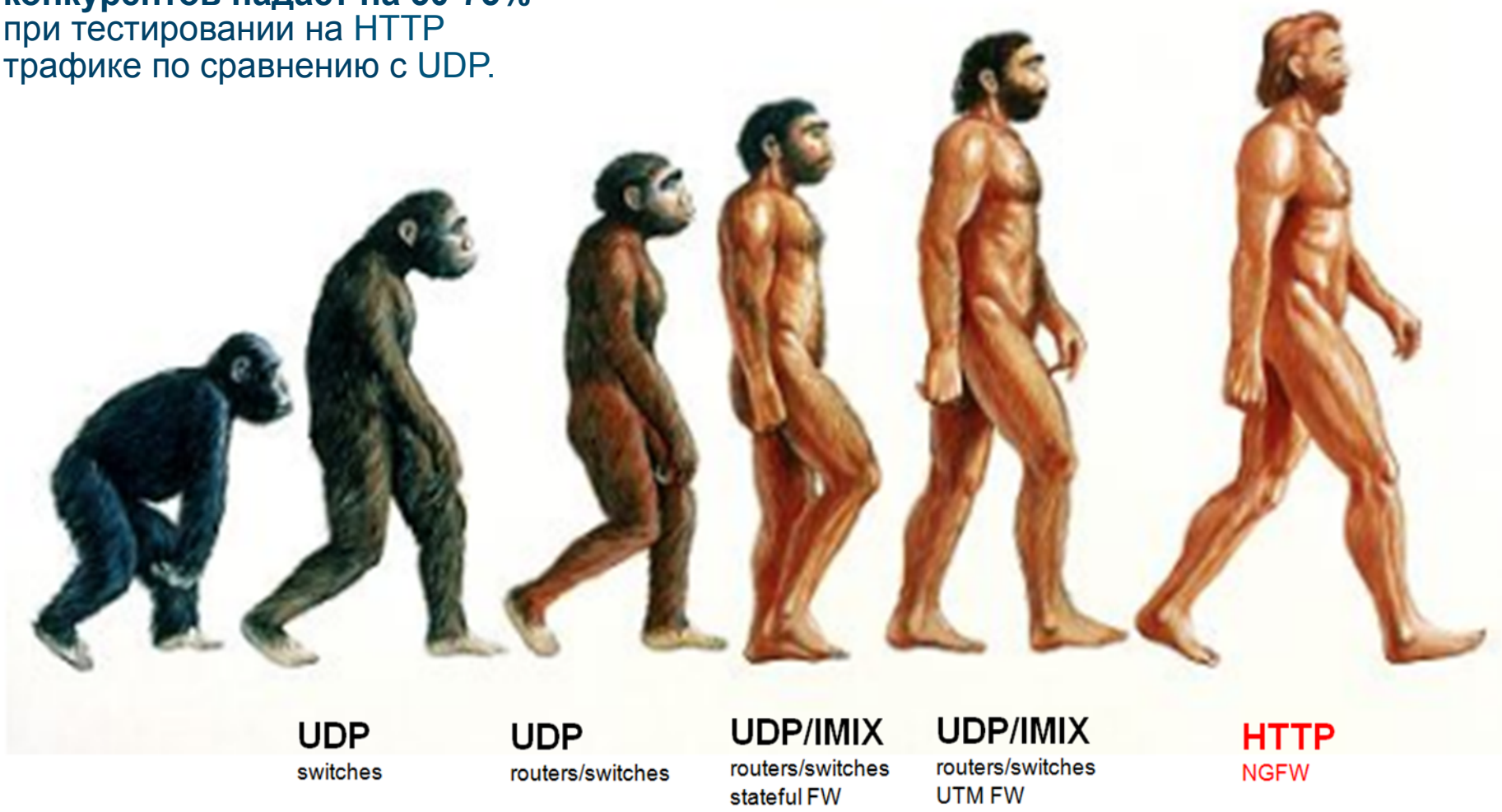
Архитектура межсетевого экрана нового поколения Palo Alto Networks

- Более 40 процессоров
- Более 30 Гб RAM
- Разделение высокопроизводительного Data Plane и Control Plane
- Производительность межсетевого экрана – 20 Гбит/с
- Производительность защиты от угроз – 10 Гбит/с
- 4 000 000 одновременных сессий

Почему правильнее измерять производительность на HTTP трафике?

Согласно тестам NSS Labs **производительность решений конкурентов падает на 50-75%** при тестировании на HTTP трафике по сравнению с UDP.

Все наши данные о производительности – результаты тестов на HTTP.



Основной функционал операционной системы

Идентификация и контроль приложений, пользователей и контента дополняются следующим функционалом

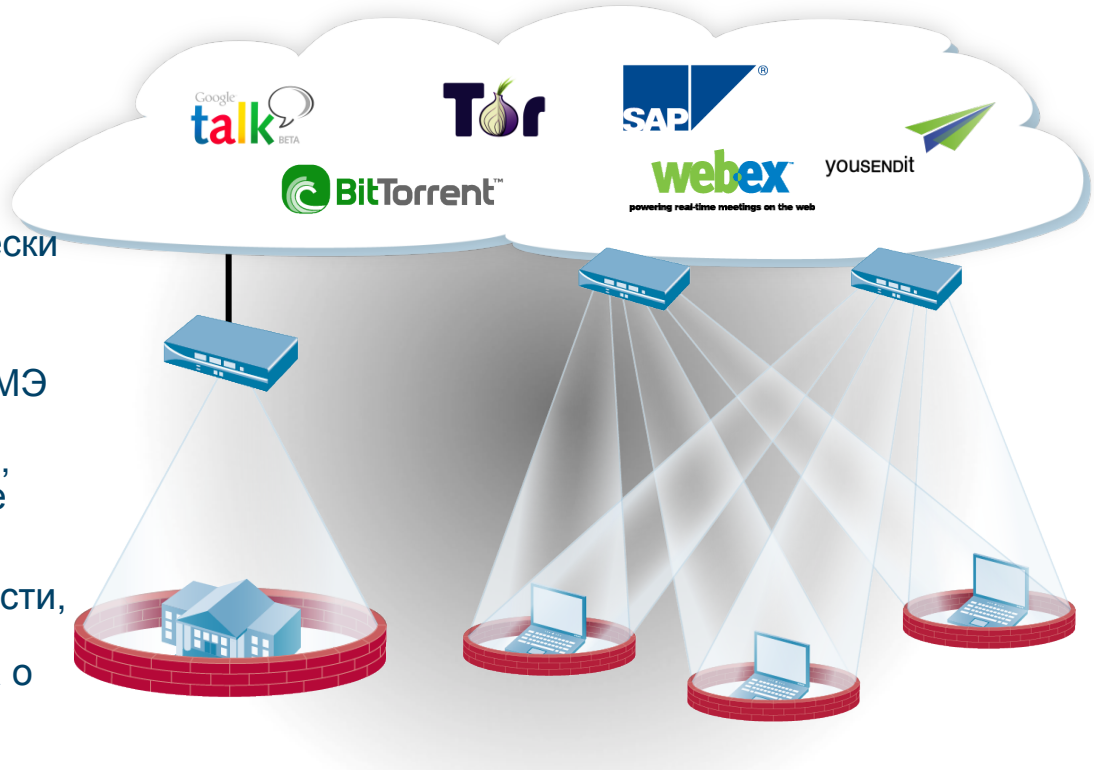
- Network
  - Динамическая маршрутизация (BGP, OSPF, RIPv2)
  - Режим мониторинга – подключение к SPAN-порту
  - Прозрачный (L1) / L2 / L3 режимы
  - Маршрутизация по политикам (PBF)
  - IPv6
- VPN
  - Site-to-site IPSec VPN
  - SSL VPN (GlobalProtect)
- Функционал QoS
  - Приоритезация, обеспечение 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 (кроме PA-200, VM-series)
  - Path, link и HA мониторинг
- Виртуальные системы
  - Настройка нескольких межсетевых экранов в одном устройстве (серии PA-5000, PA-3000 и PA-2000)
- Простое и гибкое управление
  - CLI, Web, Panorama, SNMP, Syslog, NetFlow, интеграция с SIEM/SIM

Global Protect

paloalto NETWORKS

Функционал GlobalProtect

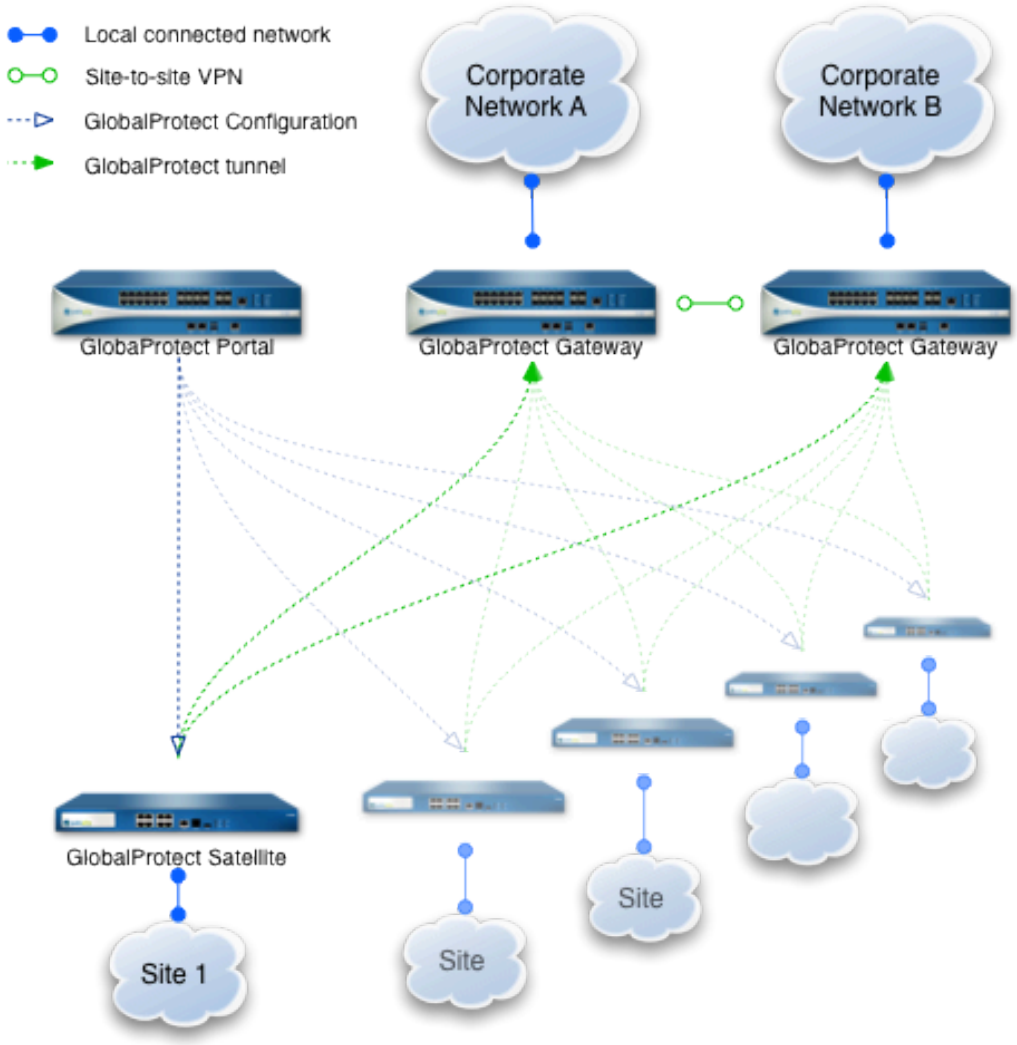
- Пользователи никогда не работают “off-network” независимо от их местоположения
- Межсетевые экраны образуют «облако» сетевой безопасности
- Как это работает:
  - Программный агент определяет местоположение клиента (внутри корпоративной сети или нет)
  - Если клиент находится вне корпоративной сети, то автоматически устанавливается IPsec/SSL VPN соединение к ближайшему МЭ
  - Агент также может предоставлять МЭ информацию о состоянии безопасности клиента (тип клиента, установленные патчи, шифрование диска, антивирус и т.д.)
  - МЭ применяет политики безопасности, основанные на App-ID, User-ID, Content-ID и информации от агента о соответствии АРМ пользователя корпоративным требованиям



Доступны клиенты GlobalProtect для настольных и мобильных ОС

- Windows, Mac OS X
- Для Apple iOS в App Store
- Для Android в Google Play
- Автоматическое или ручное подключение

Легкое развертывание Large Scale VPN с GlobalProtect



1 GP Portal в HQ/DC

Несколько GP Gateways в HQ/DCs

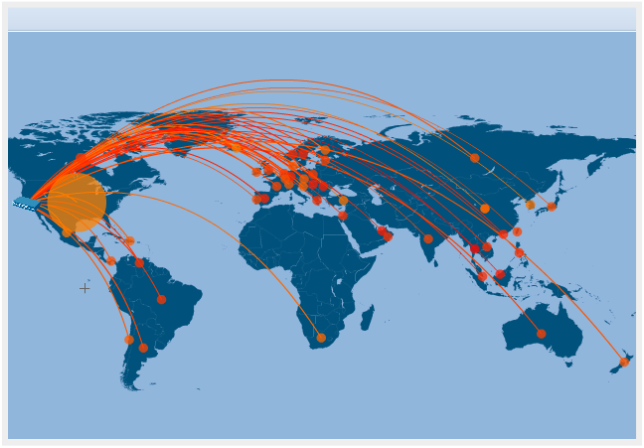
Сотни/тысячи GP Satellites в филиалах и мини-офисах с простой настройкой – достаточно только подключения к Интернет/ WAN

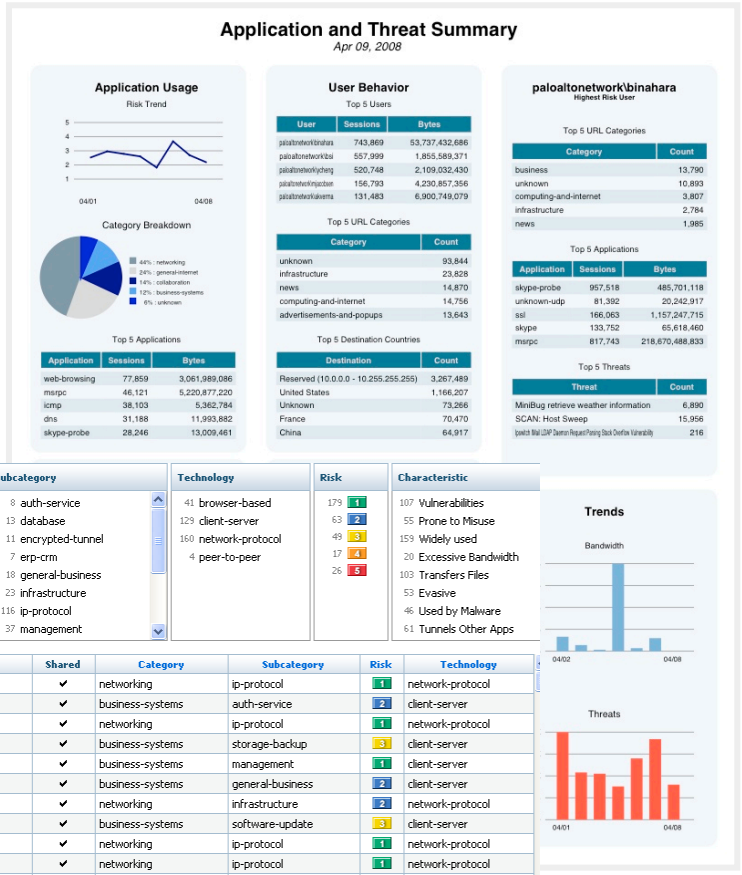
Управление

paloalto NETWORKS

Средства управления, отчетности и интеграции

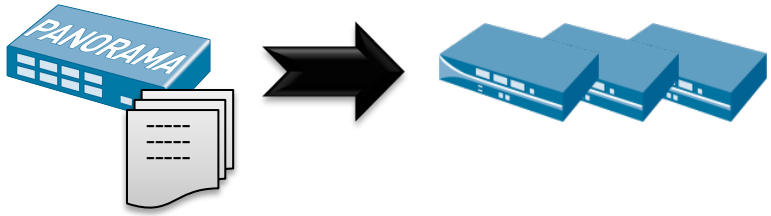
- Web GUI, SSH, XML API
- Централизованное управление – ПО Panorama + M-100
- Богатая отчетность из коробки
- Отправка логов по Syslog, SNMP
- Интеграция с ПО оркестрации
- Интеграция с SEIM/SIM (например, HP ArcSight, Symantec SIM)



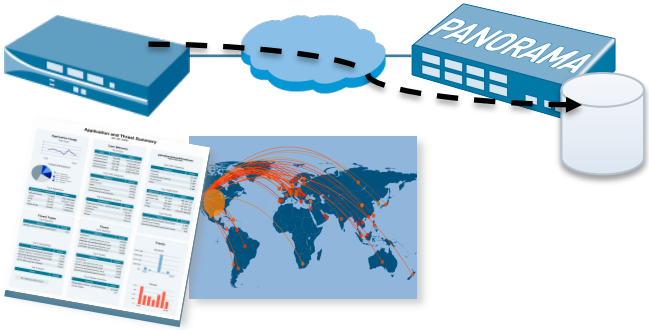


Централизованное управление с использованием ПО Panorama

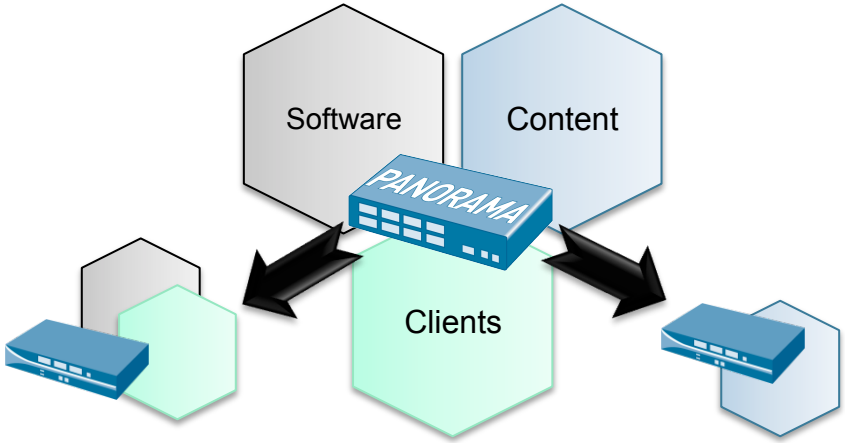
- Централизованная настройка



- Централизованное логирование и отчетность



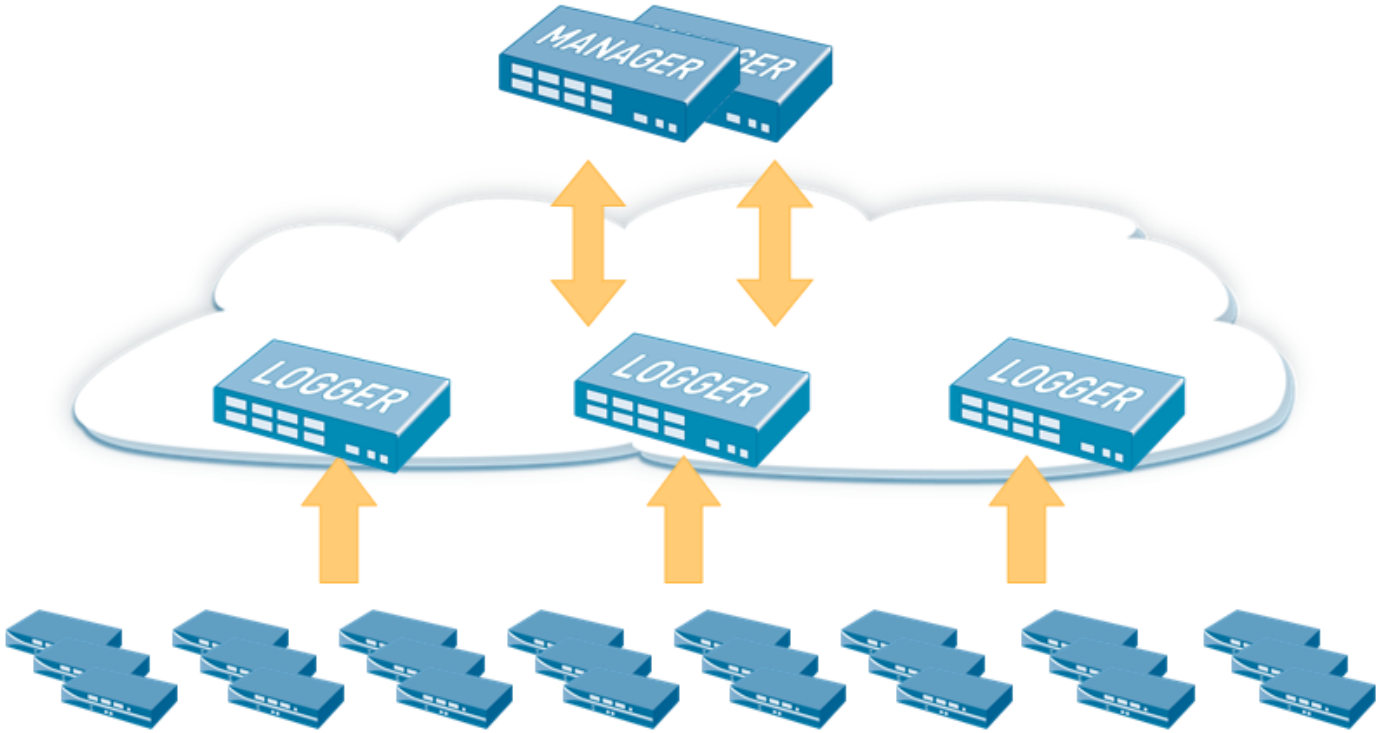
- Централизованное обновление



- Ролевое администрирование

paloalto NETWORKS

Распределенная система централизованного управления и сбора логов – устройства M-100



Экономия пропускной способности каналов WAN за счет агрегации в логов в удаленных объектах

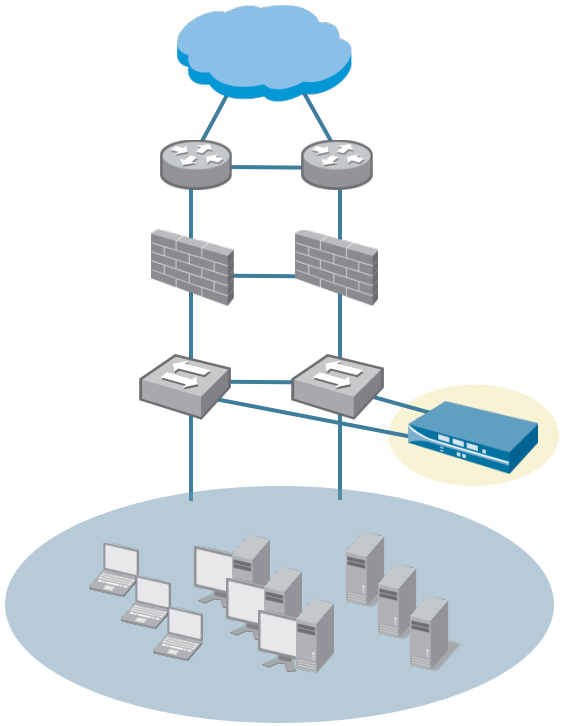
paloalto NETWORKS

Дизайн сетей на базе продуктов Palo Alto Networks

paloalto NETWORKS

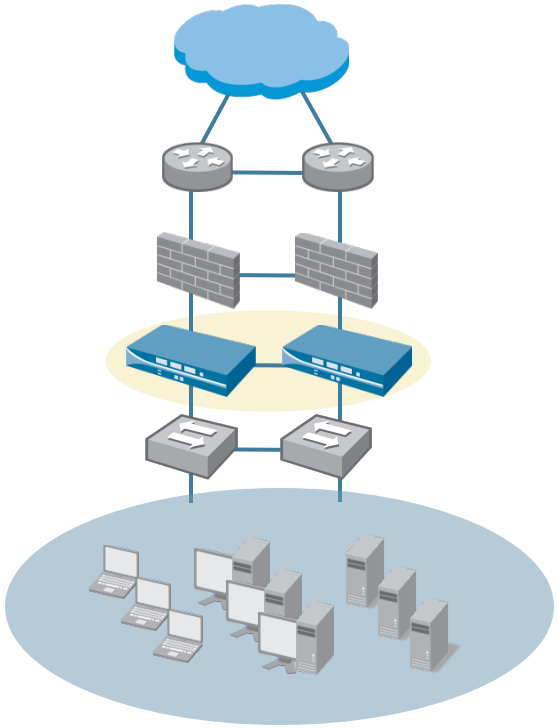
Этапы внедрения в сети

Мониторинг



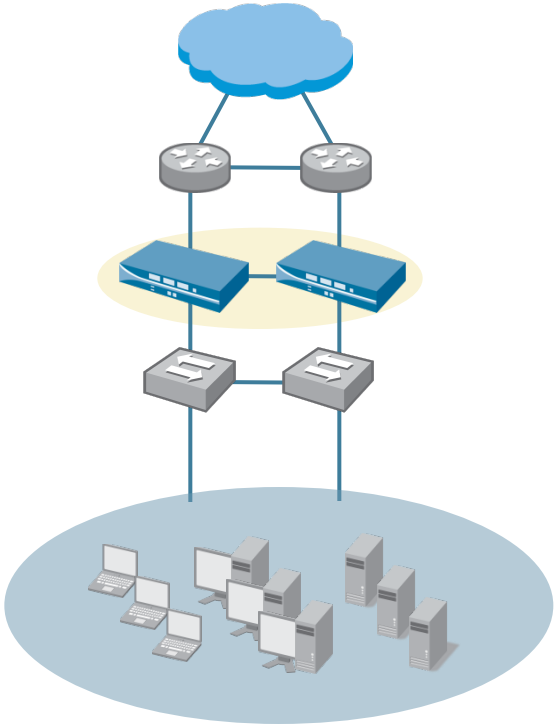
- Мониторинг без вмешательства в работу сети

Прозрачный In-Line



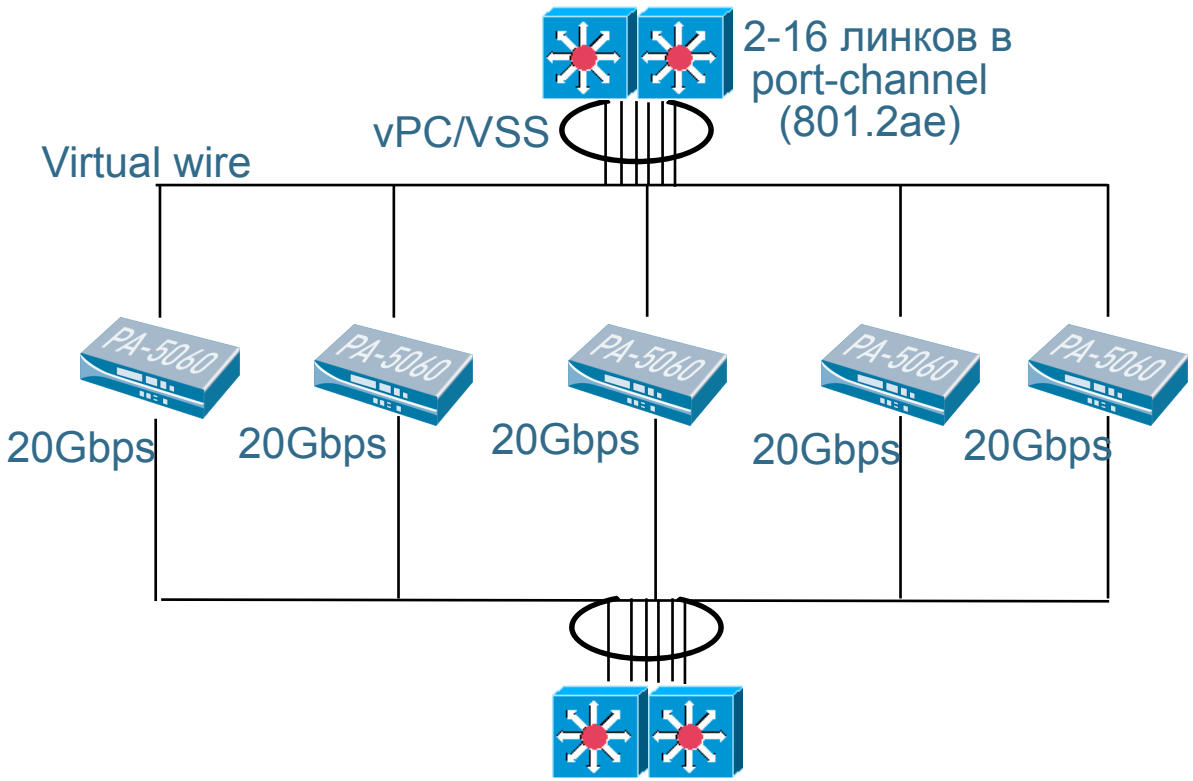
- Функции защиты от угроз
- IPS + AV + URL фильтрации

Взамен существующего



- Вместо Firewall (и других устройств)
- Firewall + IPS + AV + URL фильтрация + SSL-дешифрация

Масштабирование до 320Гбит/с



Если нужно больше 20 Гбит/с:

- Необходимы коммутаторы с поддержкой Port-Channel или Link-aggregation
- Коммутаторы в режиме L2/L3
- Необходимо обеспечить симметричную маршрутизацию
- Каждый линк инспектируется Palo Alto Networks в режиме Virtual-Wire
- Масштабирование за счет добавления большего числа устройств PAN без переконфигурации
- Задержка от 17 мкс.

VM-series – межсетевой экран нового поколения для защиты среды виртуализации VMware

paloalto NETWORKS

VM-series: назначение и реализация

VM-series – **межсетевой экран нового поколения**, который обеспечивает применение инновационных технологий Palo Alto Networks в среде виртуализации, включая:

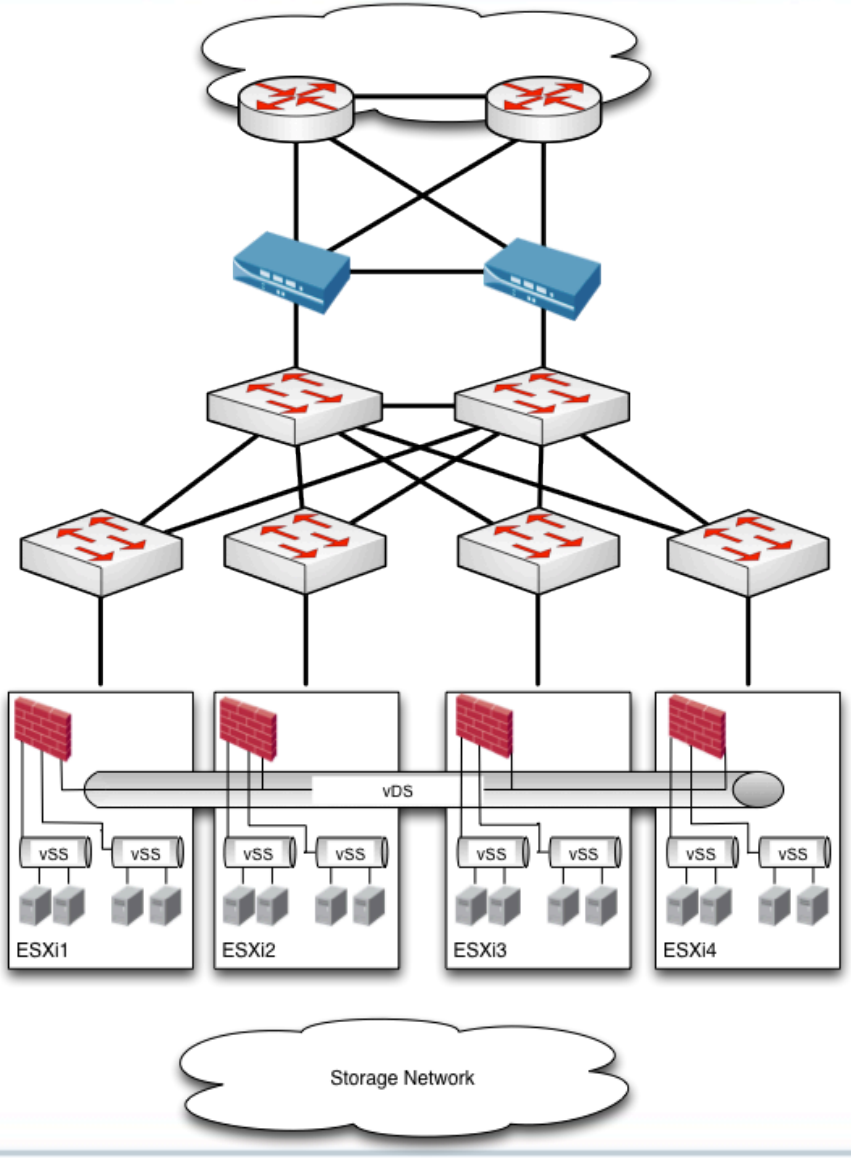
- App-ID
- User-ID
- Content-ID (IPS, AV/AS, WildFire, URL-фильтрацию, блокировку файлов)

Это **ключевое отличие Palo Alto Networks VM-series от виртуальных портовых МЭ**, таких как vShield.

VM-series реализован как гостевая виртуальная машина (VMware virtual appliance), исполняемая гипервизором ESXi и подключаемая к защищаемым сегментам сети (PGs, VLANs), организованным на базе виртуальных коммутаторов vSwitch/Nexus 1000v.

VM-series обеспечивает контроль, инспекцию и визуализацию трафика между виртуальными машинами.

Архитектура виртуализированного ЦОД



Software Stack

Security Management

Network Management

Systems Management

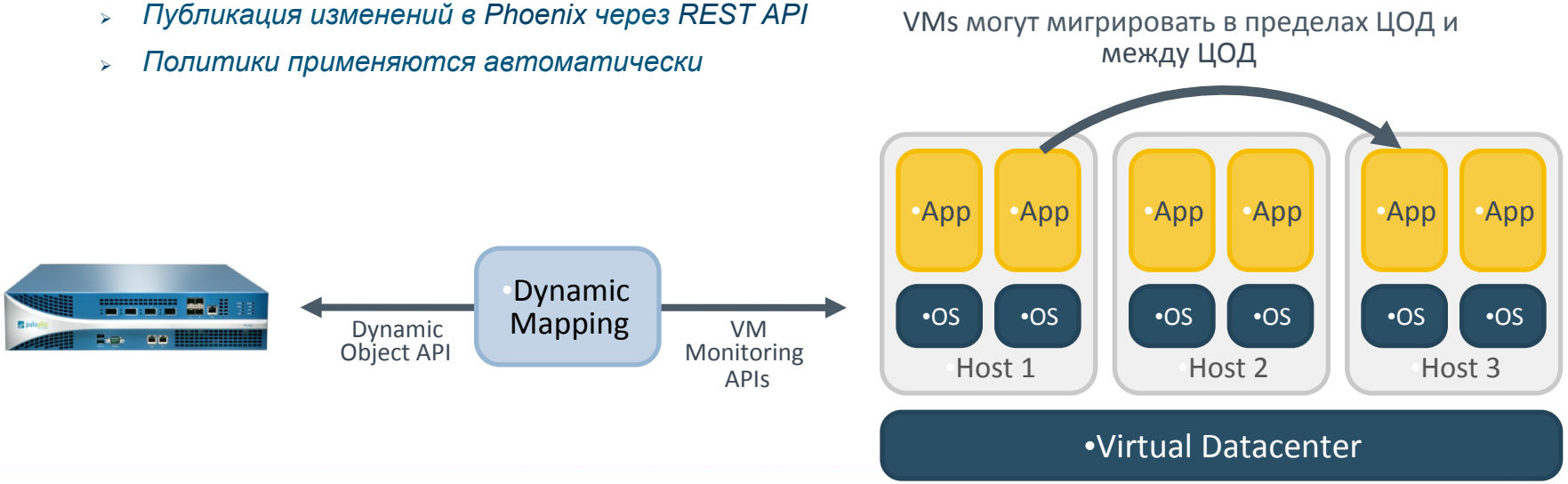
Storage Management

•Virtualization Management

•Orchestration

Использование динамических адресных объектов для отслеживания виртуальных машин (VM-UID)

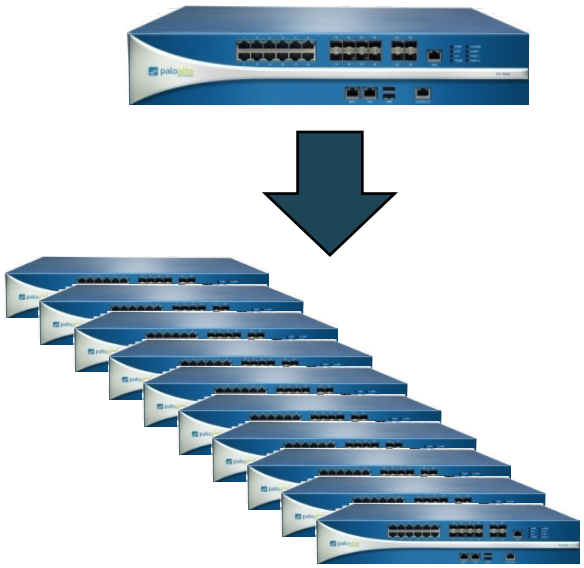
- Изменения, вносимые в среде виртуализации, происходят чаще, чем в политиках безопасности.
- Централизованный подход создания политик по зонам обеспечивает их применение независимо от места расположения и адресации виртуальных машин.
- В случаях, когда зоны неприменимы,
  - Динамический адресный объект отражает изменения IP-адреса виртуальной машины и позволяет политике безопасности «следовать» за ней
    - *Мониторинг изменений через vSphere API*
    - *Публикация изменений в Phoenix через REST API*
    - *Политики применяются автоматически*

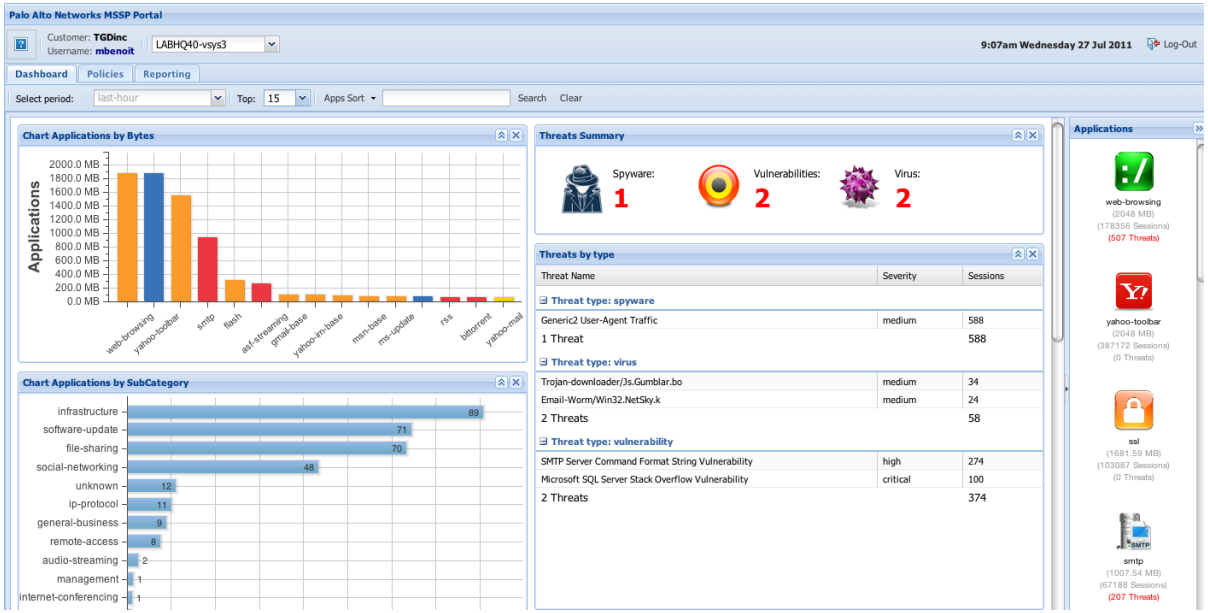


Безопасность как сервис – решения для Managed Security Service Provider (MSSP)

paloalto NETWORKS

Инструменты для MSSP





- До 225 виртуальных систем на одном устройстве
- Архитектура с Shared gateway
- Автоматизация и управление через XML API
- WebService SDK для создания и кастомизации портала управления услугами
- Интеграция со сторонним ПО оркестрации

Пример бизнес модели

Пакеты	Basic	Standard	Advanced
Отчеты	★	★	★
Защита от угроз (IPS, Сетевой AV)		★	★
Фильтрация контента (App, DLP)			★
Фильтрация URL (опция)		☆	☆

1. Организация пилотной инсталляции
2. Пользователям высылается бесплатный отчет
3. Привлечение пользователей
4. Масштабирование решения

the network security company™