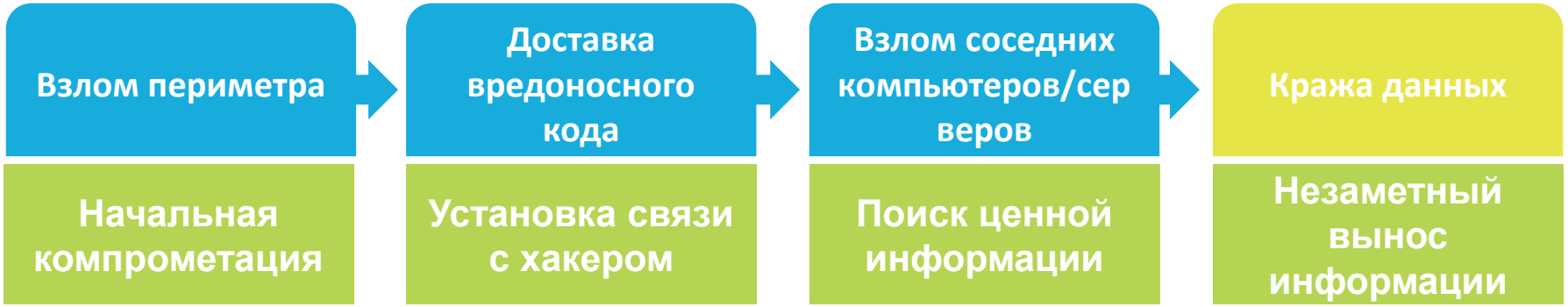
Лучшие практики и рекомендации по противодействию целевым кибератакам от Palo Alto Networks + обзор новой ОС 8.0

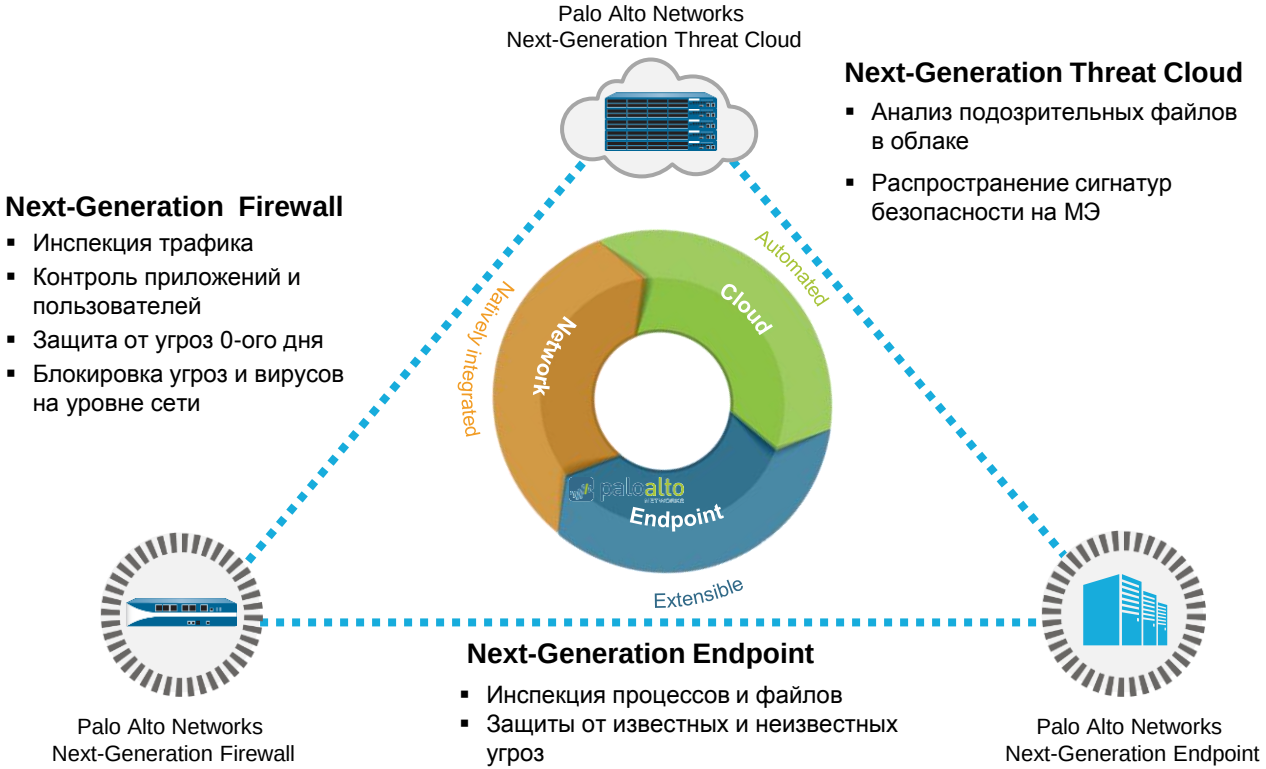
Евгений Кутумин
Консультант по информационной безопасности Palo Alto Networks

Этапы развития целевых кибератак (APT)



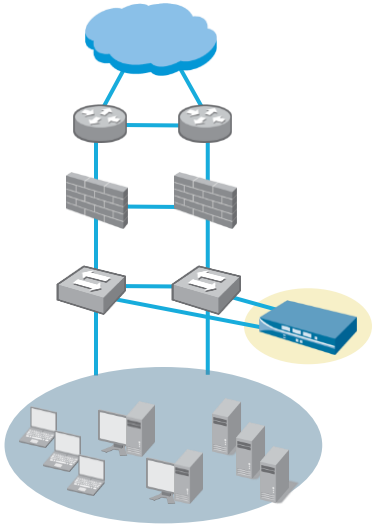
 ©2014, Palo Alto Networks. Confidential and Proprietary.

Как защищаться от APT с помощью платформы Palo Alto Networks



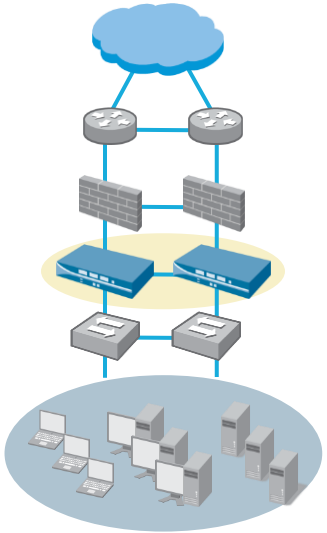
1-ый этап – интегрировать NGFW в сеть

Мониторинг



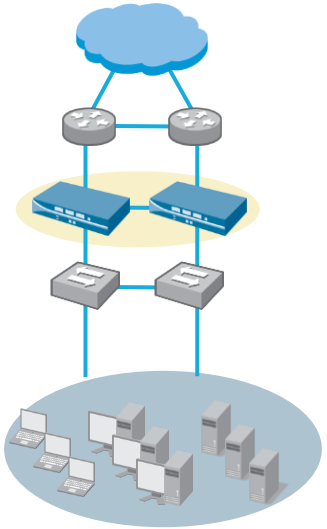
- Мониторинг без вмешательства в работу сети (режим IDS)

Прозрачный In-Line



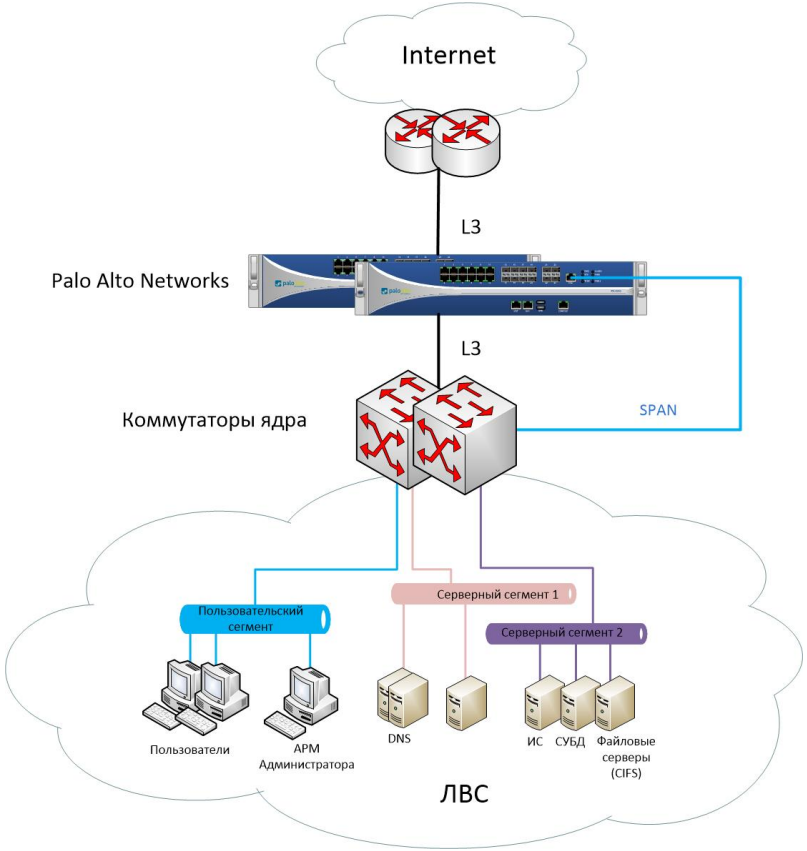
- Функции защиты от угроз
- FW+IPS + AV + AntiSpy+ URL фильтрации+SSL

Сегментация/Защита периметра (L3/L2)



- Эшелонированная защита/замена текущего FW
- Firewall + IPS + AV + URL фильтрация + SSL-дешифрация

1-ый этап – интегрировать NGFW в сеть. Пример

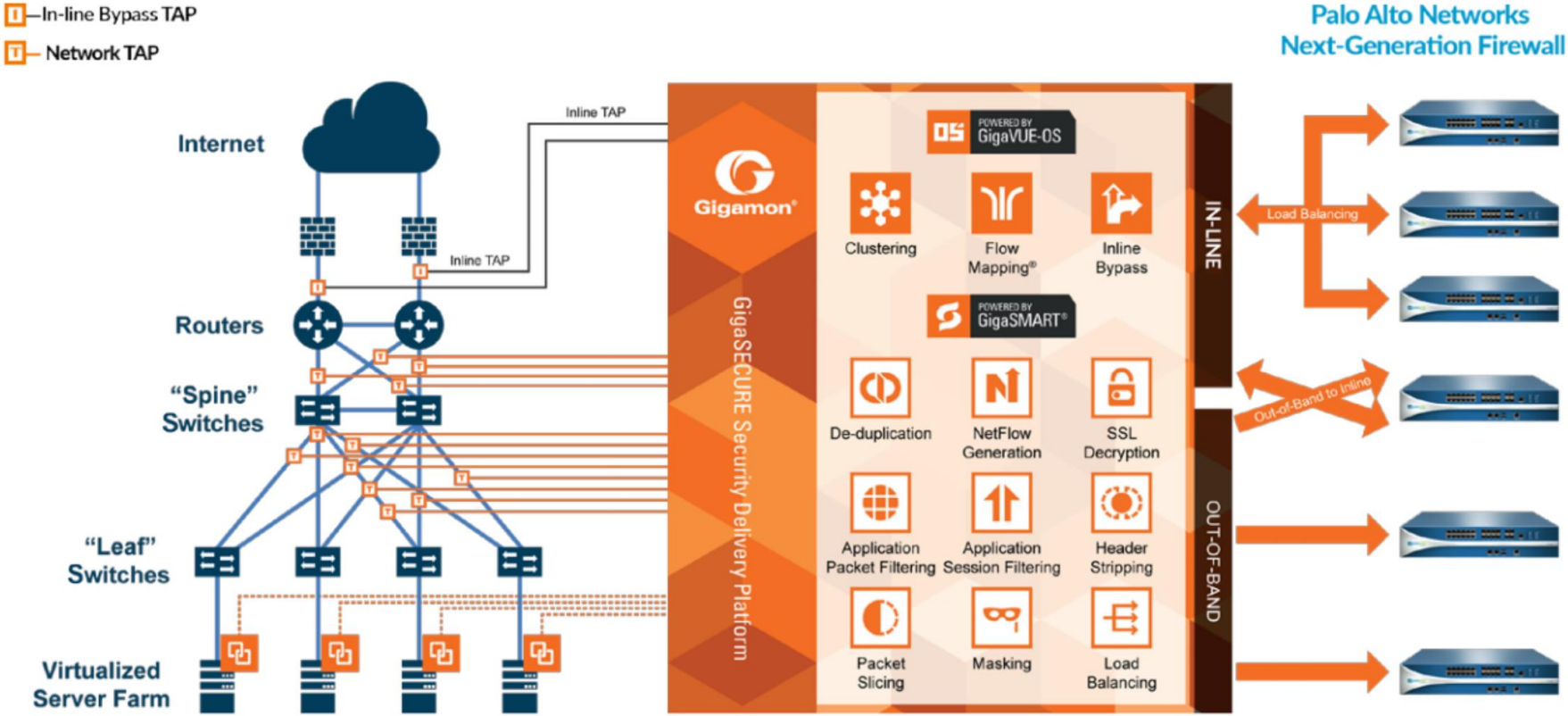


 © 2015, Palo Alto Networks. Confidential and Proprietary.

Что делать если SPAN-ы заняты???

 © 2015, Palo Alto Networks. Confidential and Proprietary.

Что делать если SPAN-ы заняты???



 © 2015, Palo Alto Networks. Confidential and Proprietary.

2-ой этап – применить контроль приложений + дешифрования SSL

 © 2015, Palo Alto Networks. Confidential and Proprietary.

Что Вы видите с портовым МСЭ

Визуализация с NGFW

Протокол SSL – это хорошо или плохо?

Good?

Bad?

BlackPOS

facebook

webex
powering real-time meetings on the web

ultrasurf

Citadel

Aurora

salesforce.com
Success On Demand.™

TDL-4

Tor

Rustock

Dropbox

Poison IVY

Ramnit

APT1

3-ий этап – контроль пользователей и написание политик нулевого доверия (Zero Trust)

- Разрешаем в явном виде хороший трафик и блокируем все остальное;
- Интеграция с Active Directory для контроля пользователей в домене;
- Captive Portal для пользователей не в домене и для гостевого Wi-Fi;
- Заставить работать приложения по стандартным портам/доверенным портам.

Name	Zone	User	Zone	Application	Service	Action	Profile
Internet VIP	LAN	CORP\VIP_Internet	Internet	VIP apps	application-default	Allow	
Bad stuff	LAN	any	Internet	Known bad apps Unknown apps	any	Deny	
Internet users	LAN	CORP\Internet CORP\VIP_Internet	Internet	Known good apps	application-default	Allow	
Other web	LAN	CORP\Internet CORP\VIP_Internet	Internet	any	service-http service-https	Allow	
Deny other	LAN	any	Internet	any	any	Deny	

 ©2014, Palo Alto Networks. Confidential and Proprietary.

Самописные приложения???

Если в сети есть самописные приложения, которые будут работать через NGFW, то для осуществления должного уровня сетевой безопасности за счет использования методологии Zero-Trust (модель нулевого доверия) необходимо создать на МЭ кастомные сигнатуры приложений.

 ©2014, Palo Alto Networks. Confidential and Proprietary.

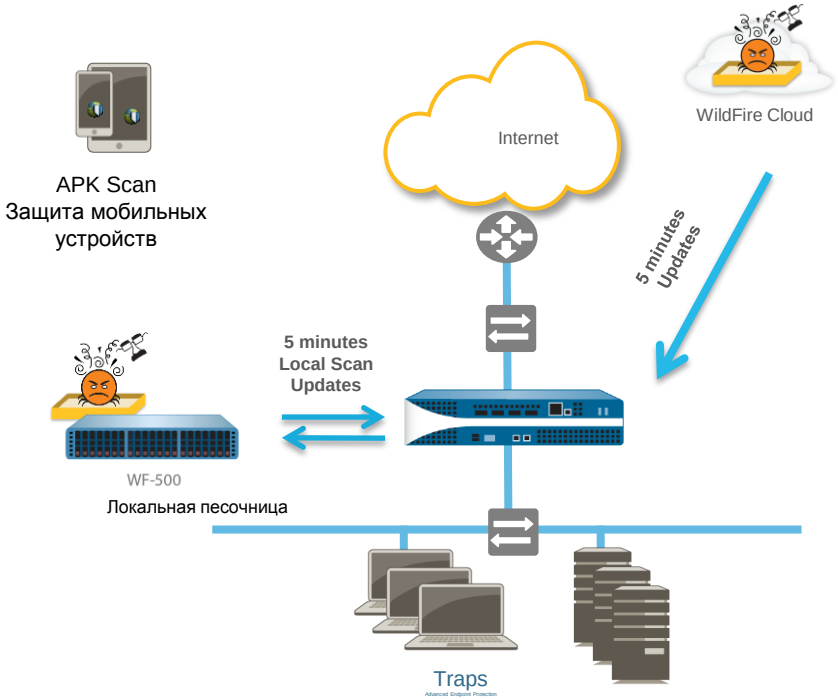
4-ый этап применить контроль данных для разрешенный приложений

- URL фильтрация по категориям (Категории Malware – запретить, Unknown – continue/запретить, остальные категории по усмотрению администратора);
- Запретить скачивать исполняемые файлов с неизвестных категорий URL;
- **Защита от вирусов (включить AV);**
- **Защита от уязвимостей (включить IPS);**
- **Защиты от ботнетов и шпиоского ПО (включить AntiSpy);**
- **Применить контроль DNS запросов (DNS Sinkholing);**
- ***Защита от DDoS (уровня приложений).***

 ©2014, Palo Alto Networks. Confidential and Proprietary.

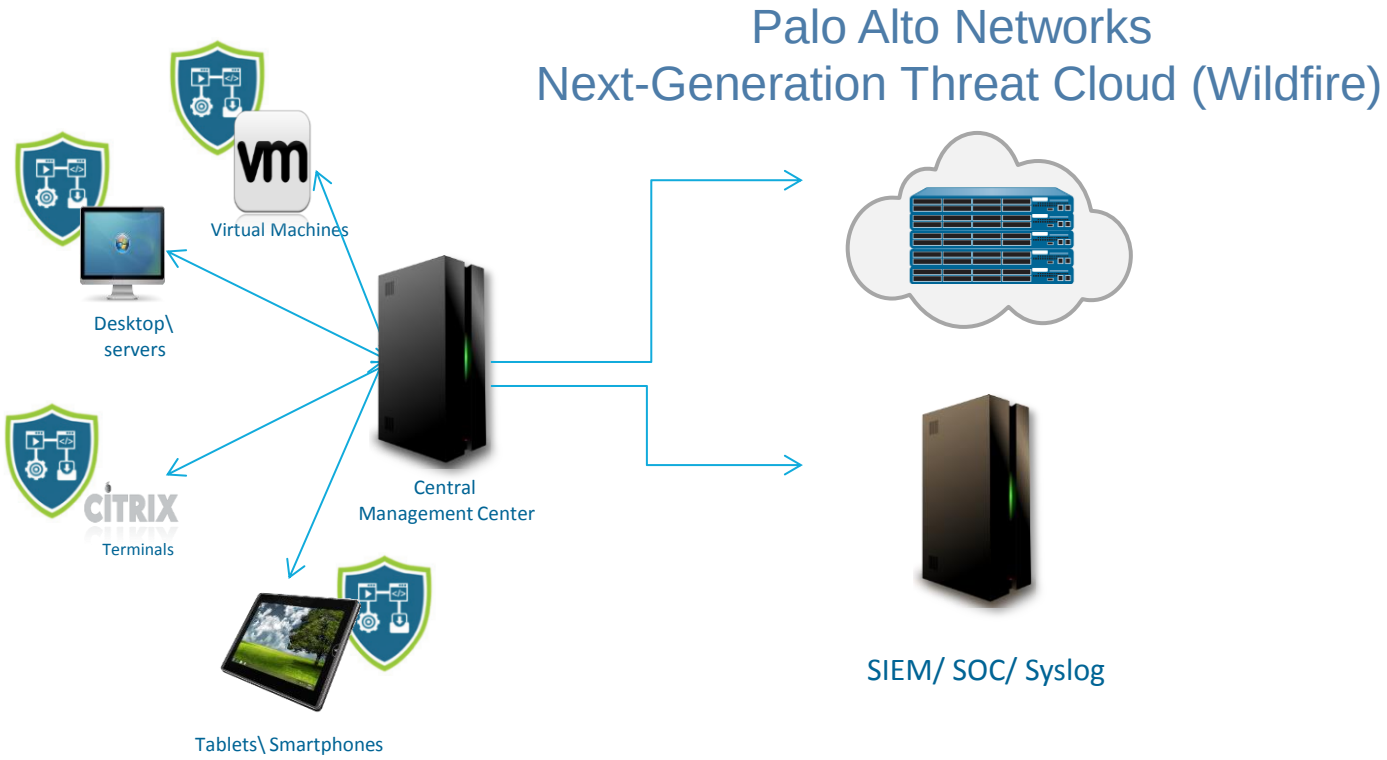
4-ый этап защититься от неизвестных угроз и вирусов

- Применить защиту от неизвестных угроз с помощью поведенческого анализа



 ©2014, Palo Alto Networks. Confidential and Proprietary.

5-ый этап – защитить рабочие станции



Предотвращение на различных стадиях

Проникновение сквозь периметр

Next-Generation Firewall / GlobalProtect
- Визуализация всего трафика, включая SSL
- Блокирование приложений с высоким уровнем риска
- Блокирование файлов по типам

Threat Prevention
- Блокирование известных эксплойтов, malware и трафика command-and-control

URL Filtering
- Борьба с социальным инжинирингом и блокирование вредоносных URLs и IP

WildFire
- Отправка входящих файлов и вложенных ссылок в наше или частное облако для инспекции
- Обнаружение новых угроз
- Автоматизированная глобальная доставка обновлений

Доставка эксплойта

Traps / WildFire
- Блокирование известных и неизвестных эксплойтов и вирусов
- Предоставление детальной информации об атаках

Продвижение по сети

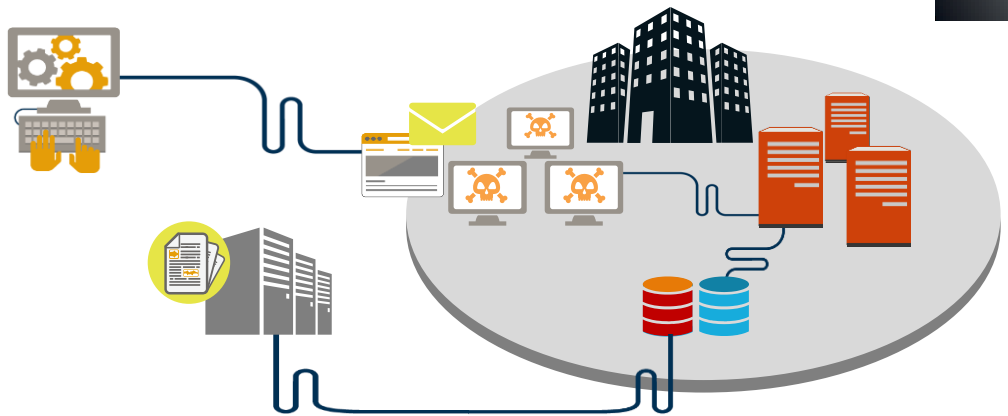
Next-Generation Firewall / GlobalProtect
- Создание зон безопасности с контролем доступа
- Инспекция трафика между зонами безопасности

WildFire + Traps
- Обнаружение новых угроз внутри сети, а не только на входе

Кража данных

Threat Prevention
- Блокирование исходящего трафика command-and-control
- Блокирование отправки файлов
- Мониторинг DNS

URL Filtering
- Блокирование исходящих соединений с вредоносными/неизвестным URL и IP



Новые платформы и новая ОС 8.0

 ©2014, Palo Alto Networks. Confidential and Proprietary.

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

VM Series

(VMware: ESXi + NSX)

Hyper-V, KVM, Azure, AWS)

до 1 Gbps FW

до 600 Mbps threat prevention

до 250,000 sessions

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

Спецификации серии PA-5200

PA-5260

- 72 Gbps App-ID
- 30 Gbps Threat Prevention
- 21 Gbps IPSec VPN
- 32,000,000 сессий
- (4) 40G/100G QSFP28
- (16) 1G/10G SFP/SFP+
- (4) 100/1000/10G Copper

PA-5250

- 35 Gbps App-ID
- 20 Gbps Threat Prevention
- 14 Gbps IPSec VPN
- 8,000,000 сессий
- (4) 40G/100G QSFP28
- (16) 1G/10G SFP/SFP+
- (4) 100/1000/10G Copper

PA-5220

- 18 Gbps App-ID
- 9 Gbps Threat Prevention
- 5 Gbps IPSec VPN
- 4,000,000 сессий
- (4) 40G QSFP+
- (16) 1G/10G SFP/SFP+
- (4) 100/1000/10G Copper

- Горячая замена кулеров и блоков питания
- Двойные системные SSD (240GB) и двойные HDD для логов (2TB)
- Выделенные интерфейсы для HA и управления
- 3U, крепление к 2- и 4-опорным стойкам
- Охлаждение Front to back со сменными фильтрами

** Производительность на основе HTTP-трафика с размером транзакции 64K*

 © 2017 Palo Alto Networks, Inc. Confidential and Proprietary.

Спецификации серии PA-800

PA-850

- 1.9 Gbps App-ID
- 780 Mbps Threat Prevention
- 192,000 сессий
- (4) 10/100/1000 Copper
- (4) SFP, (4) SFP+ или 8 SFP

PA-820

- 940 Mbps App-ID
- 610 Mbps Threat Prevention
- 128,000 сессий
- (4) 10/100/1000 Copper
- (8) SFP

- 1U стоечное шасси
- Двойные блоки питания с горячей заменой (PA-850)
- 240GB SSD
- Выделенный порт управления
- Консольные порты RJ-45 и Micro USB
- Выделенные интерфейсы для HA

 © 2017 Palo Alto Networks, Inc. Confidential and Proprietary.

Спецификация PA-220

PA-220

500 Mbps App-ID
170 Mbps Threat Prevention
64,000 сессий
(8) Портов 1G Copper Ethernet

- Нет движущихся частей
- Двойные адаптеры питания (опция)
- 32GB SSD (EMMC)
- Выделенный порт управления
- Консольные порты RJ-45 и Micro USB
- Полная поддержка HA (Active/Passive с синхронизацией сессий и Active/Active)
- Для вертикального крепления к стене или горизонтальной установки

 © 2017 Palo Alto Networks, Inc. Confidential and Proprietary.

PA-7000 SERIES

NEW

PA-5200 SERIES

PA-5000 SERIES

PA-3000 SERIES

PA-800 SERIES

PA-500

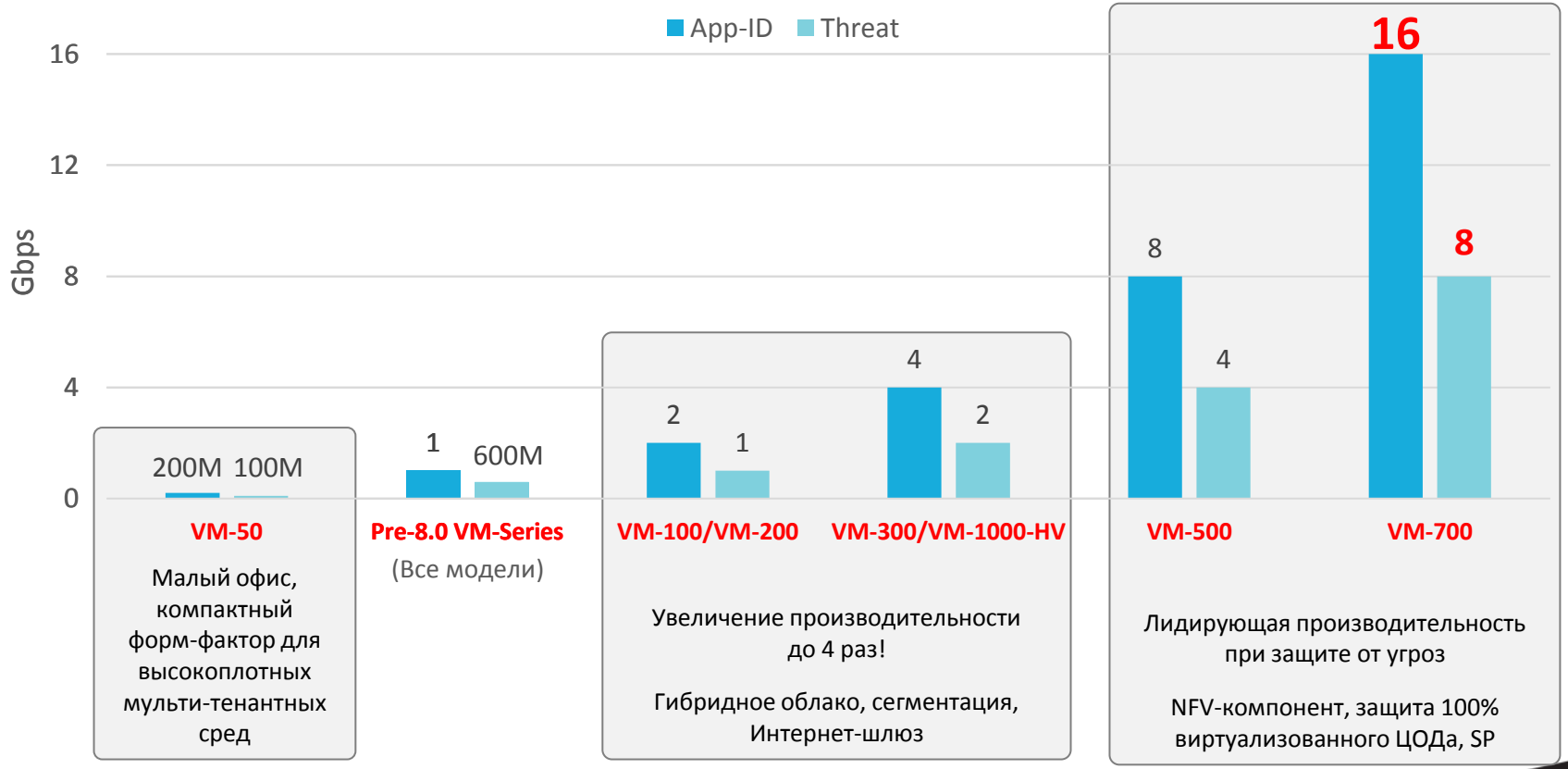
NEW

PA-220

PA-200

NEW

Новое портфолио vNGFW



 © 2017 Palo Alto Networks, Inc. Confidential and Proprietary.

Неполный список новых feature ОС 8.0

- **App-ID**
  - Поддержка IPv6 ALG
  - **Детальный ACC для SaaS**
  - **Контроль non-IP протоколов**
  - Улучшенный ACC
  - 3 новых App-ID каждую неделю
- **User-ID**
  - Поддержка SAML 2.0
  - **БД логов User-ID в веб-интерфейсе**
  - Panorama в качестве редистрибьюции мапинга пользователей
  - Увеличение максимального числа групп
- **Content-ID**
  - Защита от фишинга логина/пароля
  - Автоматические C2-сгинатуры
  - Фиды плохих IP
  - **5-минутные обновления категорий Phising и Malware в PAN-DB**
  - Глобально уникальные Threat IDs
  - Сбор телеметрии по угрозам
- **GlobalProtect**
  - GP 4.0 с поддержкой IPv6
  - **Clienless VPN**
- **Виртуализация**
  - Шаблоны действий интеграции VM-series b NSX в Panorama
  - **Улучшенная производительность VM-серии**
  - **VM bootstrapping**
- **Сетевые функции**
  - **Инспекция туннелей (GRE, AH IPsec, etc.)**
  - Поддержка MP-BGP
  - Удаление маршрута на основе мониторинга пути
  - Анонсирование роутера IPv6 для DNS
  - Повышенные буферы IKE peer
  - Защита от Multipath TCP
  - Улучшения в части DoS защиты
- **Расшифрование**
  - Perfect Forward Secrecy для инспекции входящего трафика
  - Управляемый список исключений
- **Управление**
  - NetFlow на PA-7000
  - Отправка логов PA-7000 на Panorama
  - **Отправка логов по HTTP/HTTPS**
  - Авто-тэгирование Src IP / Dst IP
  - Улучшения SNMP
  - **Индивидуальные commit и откаты конфигруций**
- **Panorama**
  - **Отчеты и аналитика в 30 раз быстрее**
  - **Сбор логов и корреляция логов из Traps**
  - **24Тб для хранения логова для одной Panorama VM**
  - Использование всех интерфейсов Panorama (M-100 и M-500)

Контакты "ДиалогНаука"

Телефон: +7 (495) 980-67-76 (доб. 128,129)

E-mail: marketing@dialognauka.ru