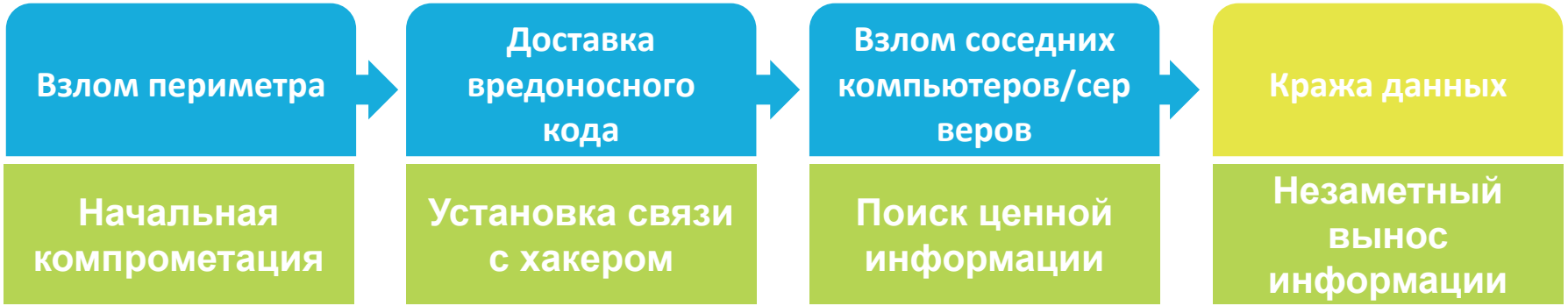
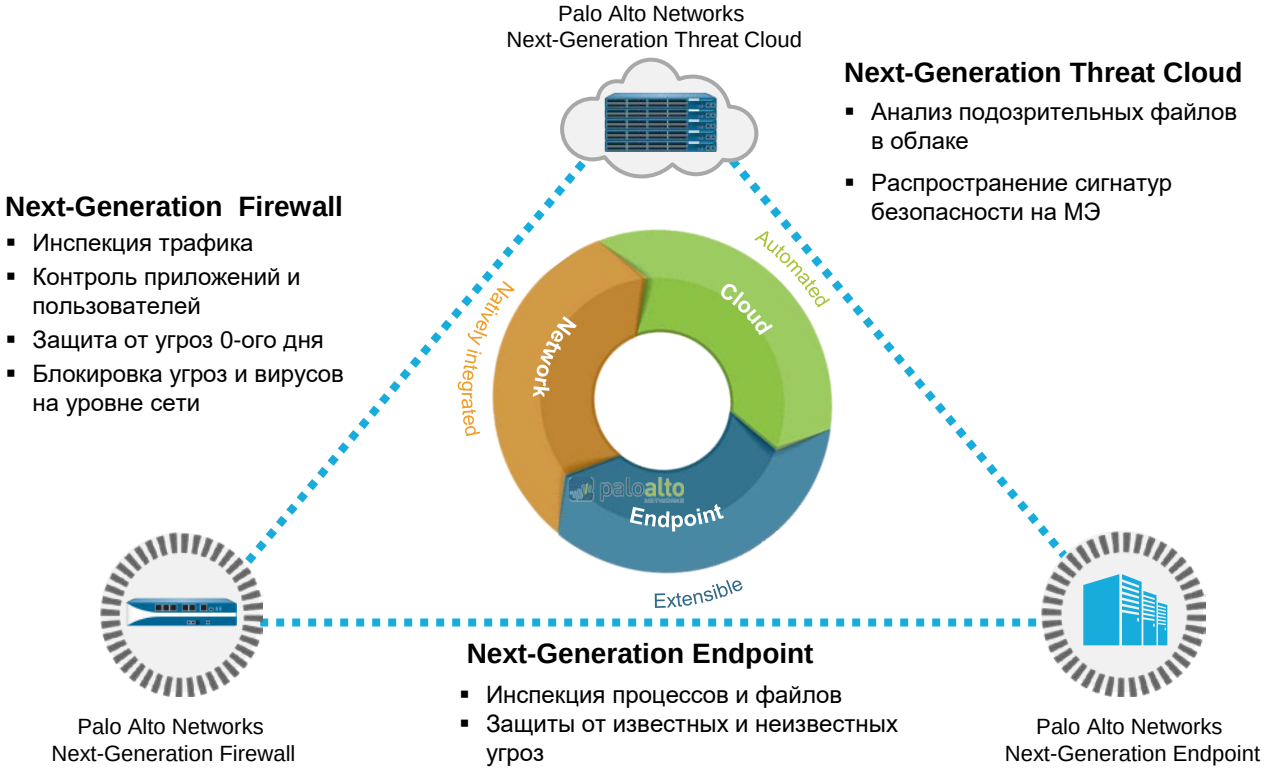
Лучшие практики и рекомендации по противодействию целевым кибератакам от Palo Alto Networks

Евгений Кутумин
Консультант по информационной безопасности Palo Alto Networks

Этапы развития целевых кибератак (APT)

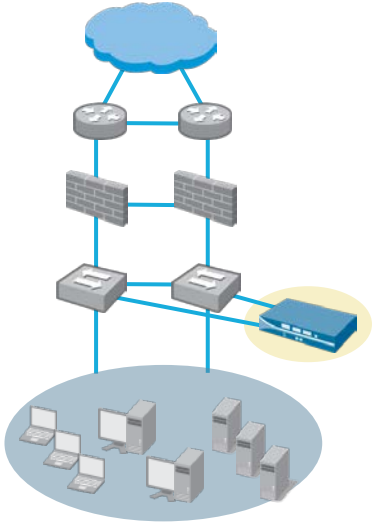


Как защищаться от *APT с* ***помощью*** *Palo Alto Networks*



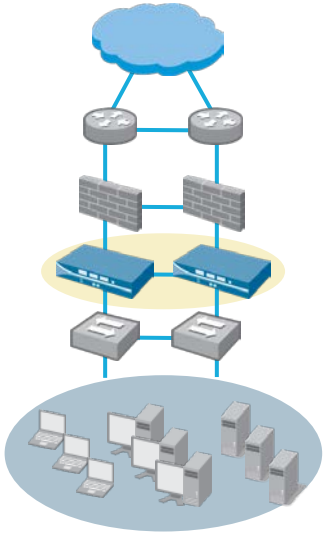
1-ый этап – интегрировать NGFW в сеть

Мониторинг



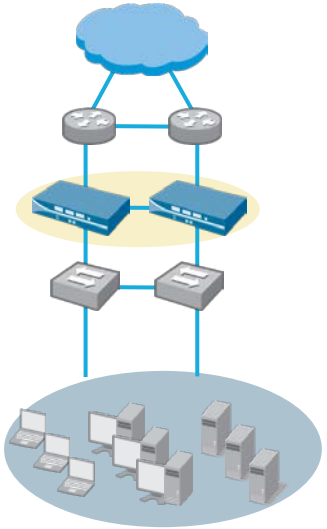
- **Мониторинг без вмешательства в работу сети (режим IDS)**

Прозрачный In-Line



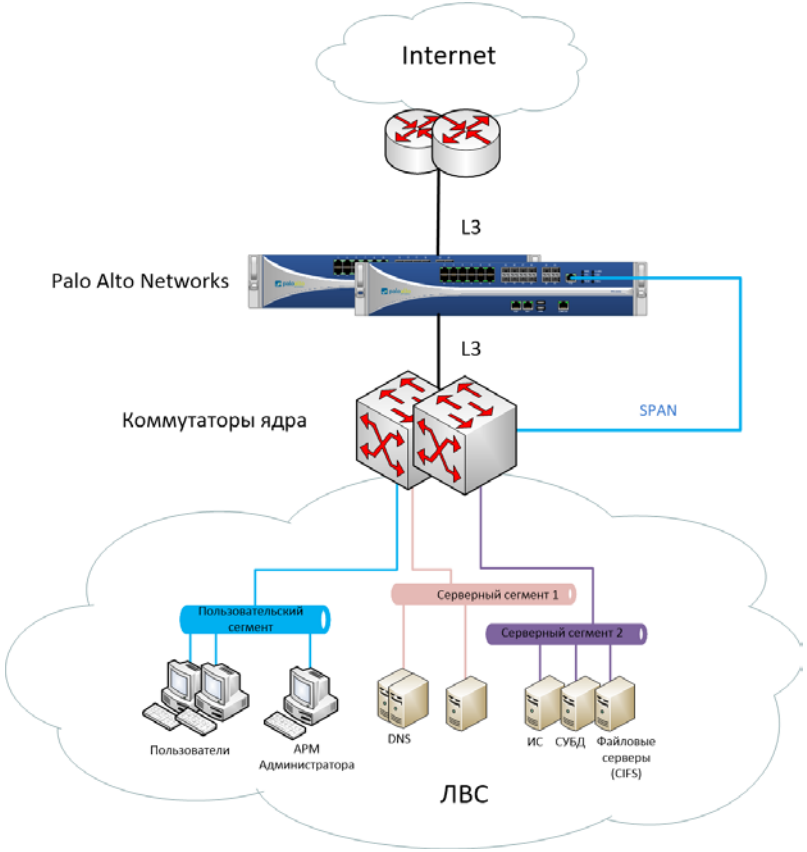
- **Функции защиты от угроз**
- **FW+IPS + AV + AntiSpy+ URL фильтрации+SSL**

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



*2-**ой этап – применить контроль приложений + дешифрования** SSL*

Что Вы видите с портовым МСЭ

Визуализация с NGFW

Протокол SSL – это хорошо или плохо?

Good?

facebook

webex
powering real-time meetings on the web

Citadel

salesforce.com
Success On Demand.™

TDL-4

Rustock

Dropbox

Ramnit

BlackPOS

Bad?

ultrasurf

Aurora

Tor

Poison IVY

APT1

Текущая статистика:
SSL зашифрована треть трафика сети

А что прячется внутри SSL у вас?

3-ий этап – контроль пользователей и написание политик нулевого доверия

- Интеграция с Active Directory для контроля пользователей в домене;
- Captive Portal для пользователей не в домене и для гостевого Wi-Fi.

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	

Самописные приложения???

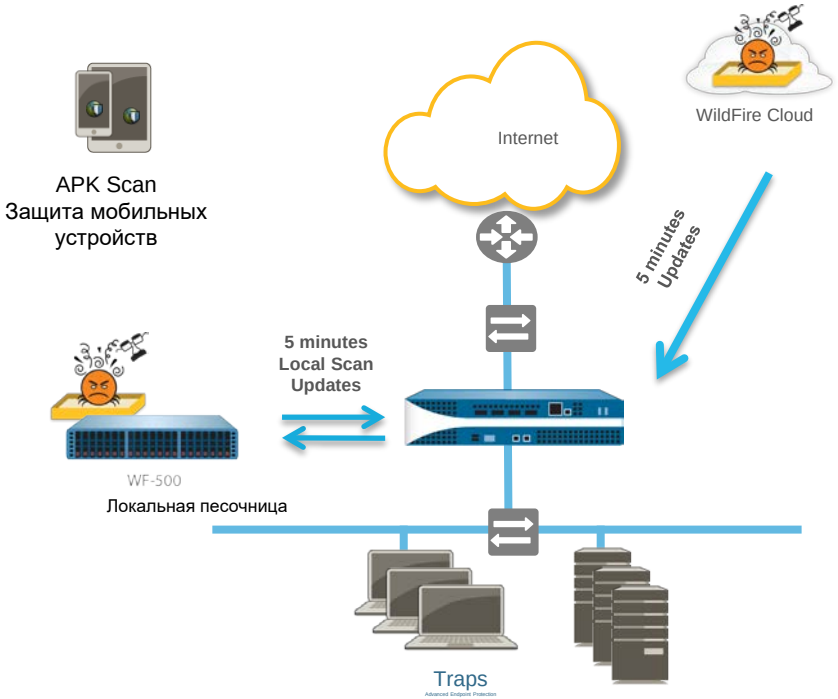
Если в сети есть самописные приложения, которые будут работать через NGFW, то для осуществления должного уровня сетевой безопасности за счет использования методологии Zero-Trust (модель нулеого доверия) необходимо создать на МЭ кастомные сигнатуры приложений.

4-ый этап применить контроль данных для разрешенный приложений

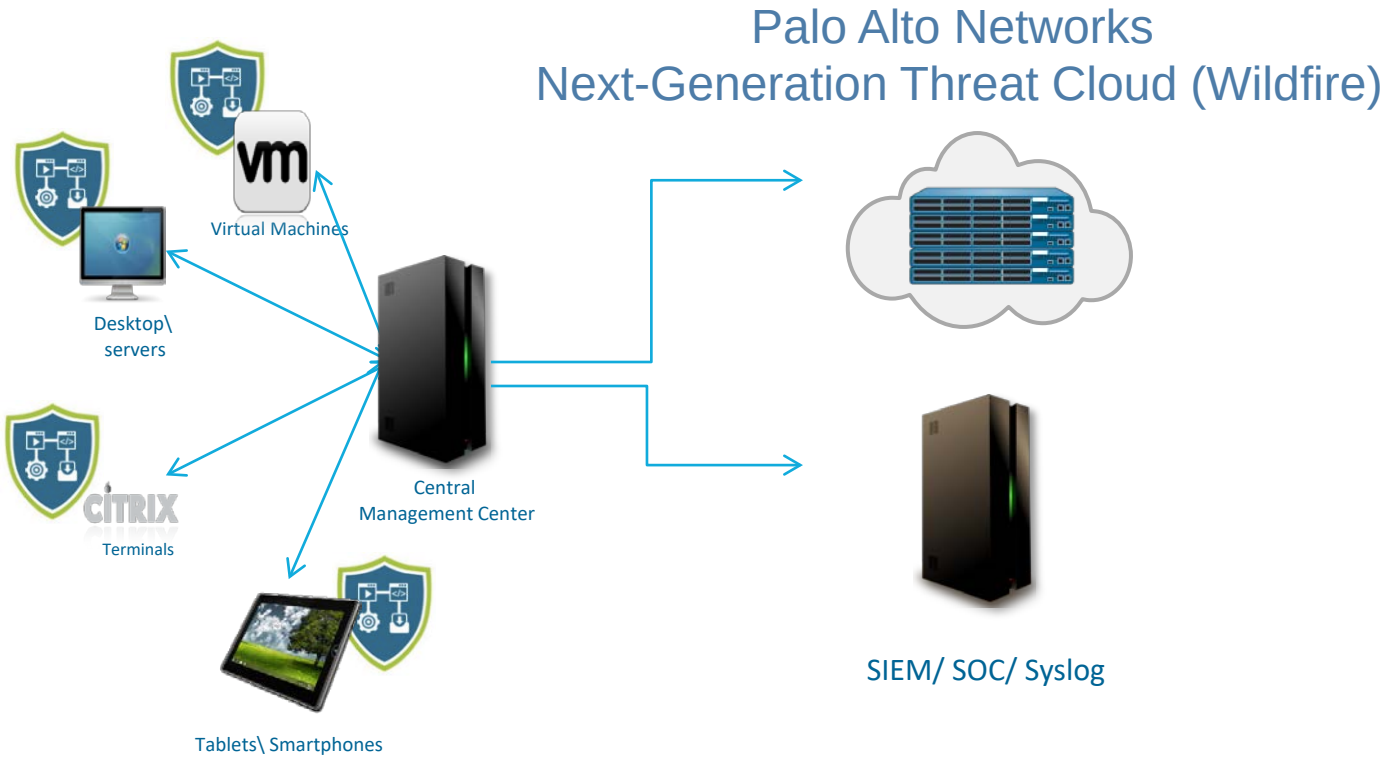
- URL фильтрация по категориям (Категории Malware – запретить, Unknown – continue/запретить, остальные категории по усмотрению администратора);
- Запретить скачивать исполняемые файлов с неизвестных категорий URL;
- **Защита от вирусов (включить AV);**
- **Защита от уязвимостей (включить IPS);**
- **Защиты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

4-ый этап применить контроль данных

- Применить защиту от неизвестных угроз с помощью поведенческого анализа



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

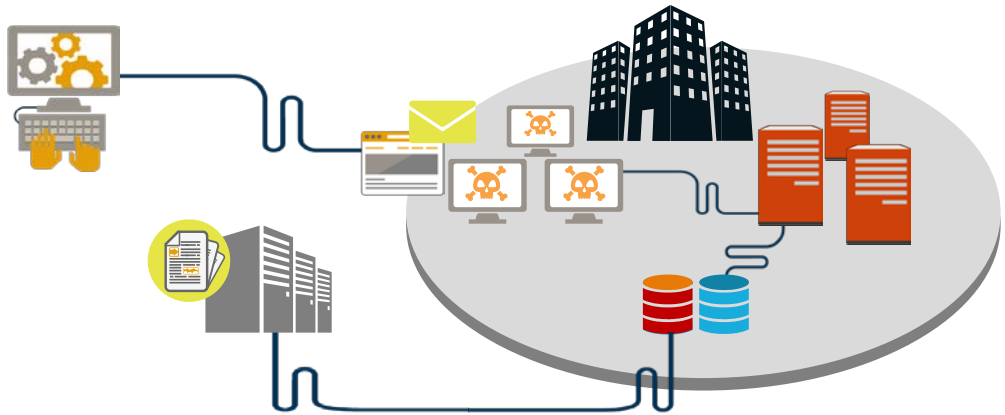
Next-Generation Firewall / GlobalProtect
- Создание зон безопасности с контролем доступа
- Инспекция трафика между зонами безопасности

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 URL и IP




paloalto
NETWORKS®