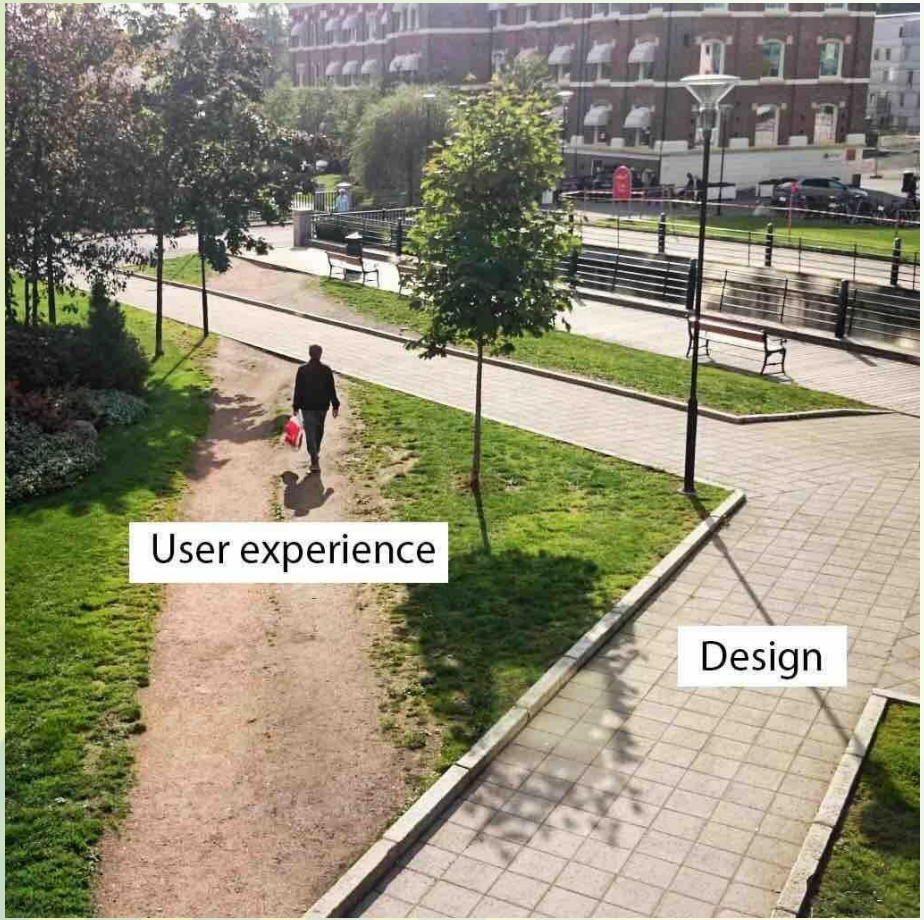
Концепция Zero Trust Networking

Denis Batrankov
Information Security Consultant
CISSP, CNSE, MVP Security

denis@paloaltonetworks.com

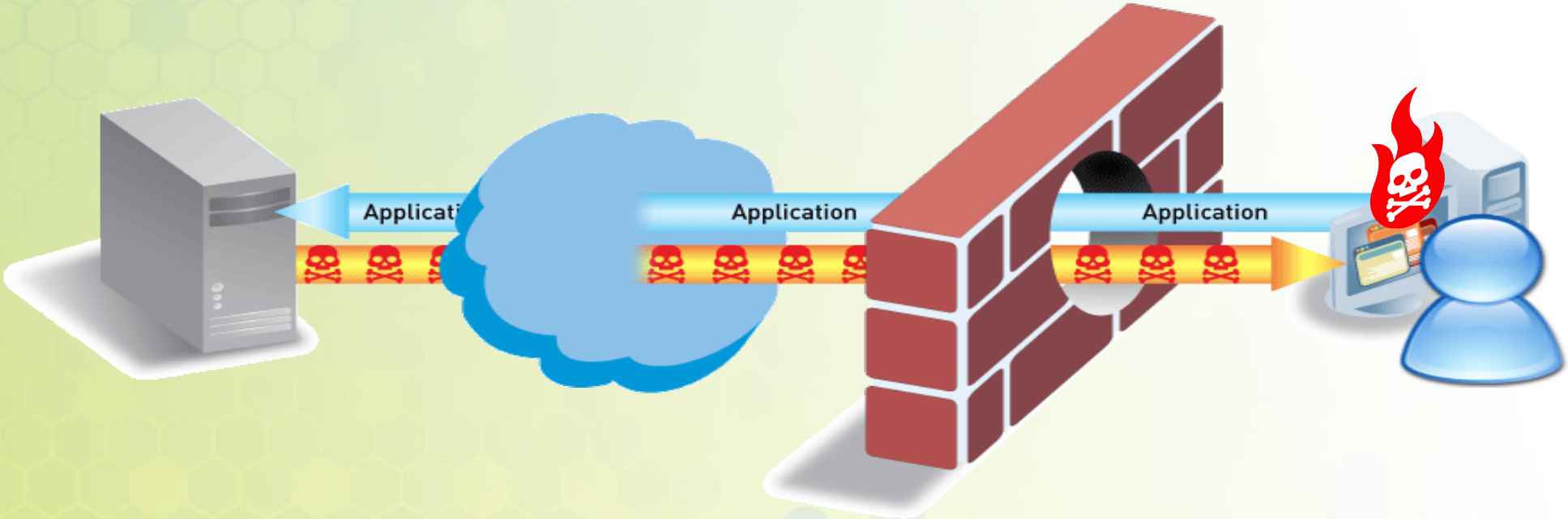
paloalto networks.

Действуют ли сотрудники как вы им говорите?



Придумано много способов обойти классические межсетевые экраны

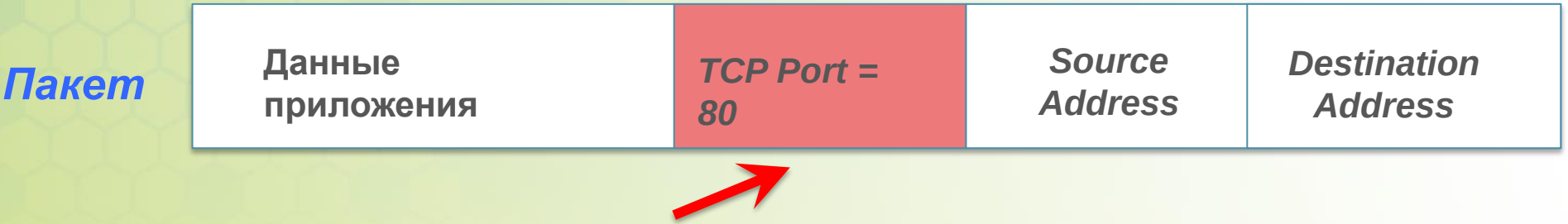
Сейчас сотрудник компании «сам» скачивает вредоносный код



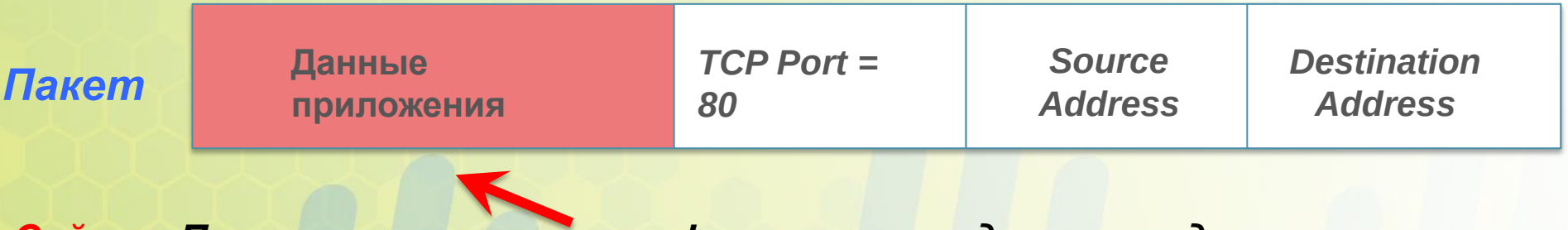
Установление обратного канала и скачивание дополнительного вредоносного ПО

paloalto networks

20 лет назад было достаточно проверять только поле «порт» в сетевом пакете



Последние 20 лет: *Приложение соответствовало номеру порта*
Например HTTP - это порт 80



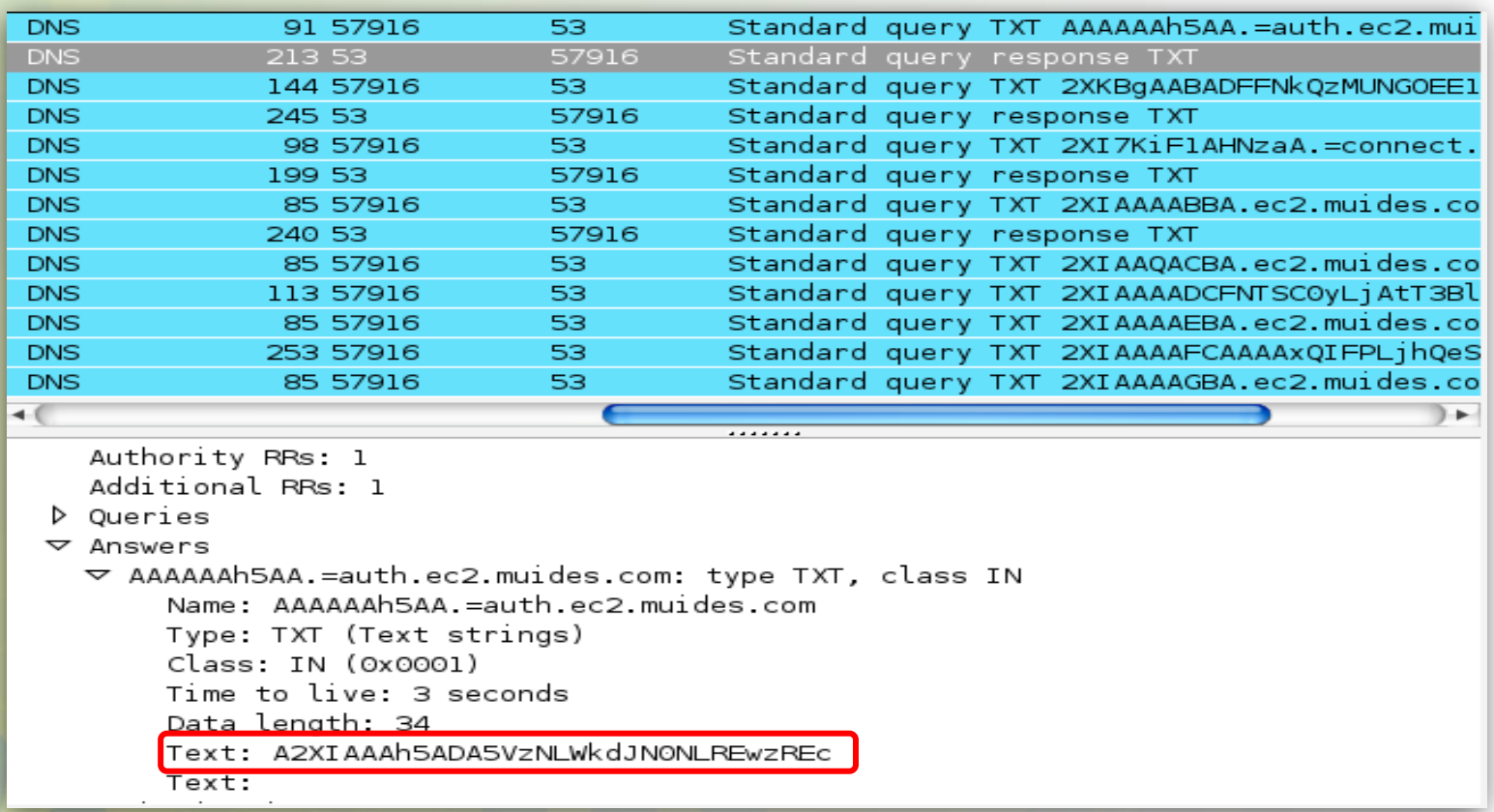
Сейчас: ***Приложение - это специфические передаваемые данные по сети***
Приложение flash = данные для анимации приложения Adobe Flash Player

paloalto networks

Пример из жизни: использование туннелирования поверх DNS

Примеры

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



Для обычного межсетевого экрана это DNS запросы
В реальности это туннели других приложений

paloalto networks

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

SSL для защиты данных или чтобы скрыть вредоносную активность?

paloalto networks

Текущая статистика:
SSL зашифрована треть трафика сети

А что прячется внутри SSL у вас?

paloalto networks

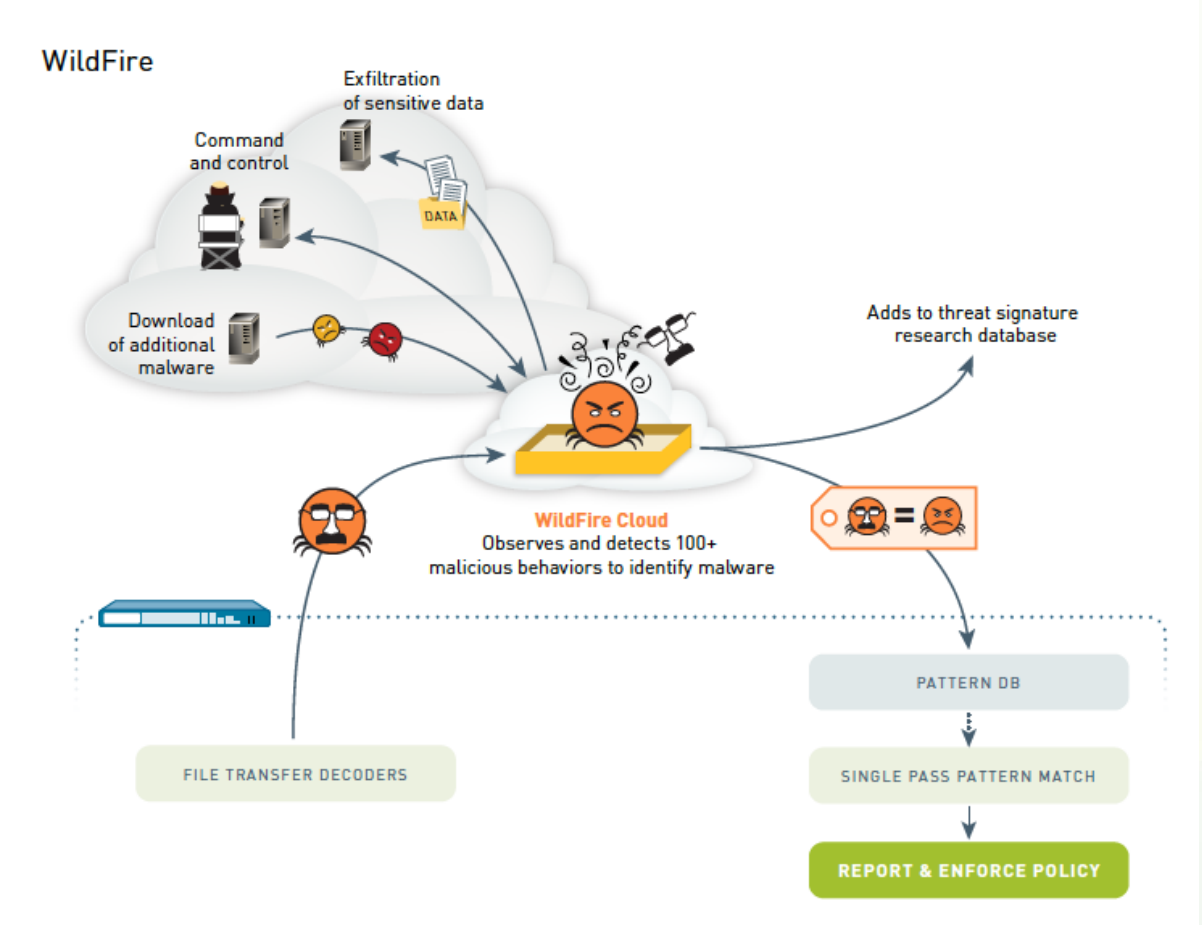
Почему традиционные антивирусы не справляются

- Целевое создание под компанию
- Полиморфизм
- Неизвестный еще никому код – нет сигнатуры

Сложно защититься

paloalto networks

Выход: своя автоматическая лаборатория анализа поведения - песочница



paloalto networks

ZERO TRUST NETWORKING

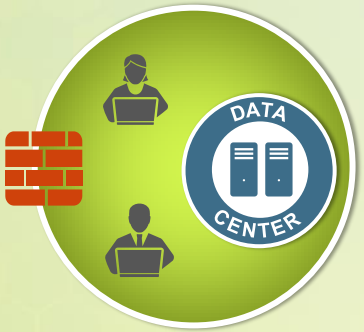
Эволюция подхода к построению корпоративной безопасности

paloalto networks

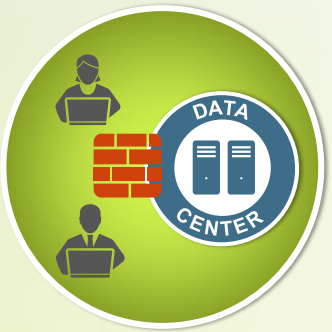
Что защищает архитектура Zero Trust

ОБНАРУЖИВАТЬ И **ПРЕДОТВРАЩАТЬ** УГРОЗЫ НА ВСЕХ УРОВНЯХ ИТ ИНФРАСТРУКТУРЫ

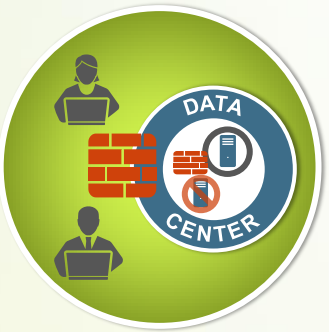
Мобильные устройства



Периметр



Внутри LAN



На периметре ЦОД и между VM

Внутри частного или публичного облака

paloalto networks

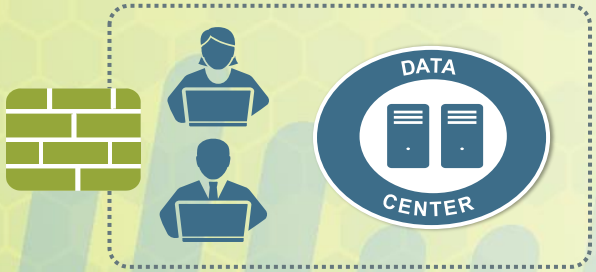
Периметр Интернет

Что было раньше

Цель

- Блокировать известные плохие порты, сигнатуры, IP и URL

- Защита сети от известных угроз
- Средства ИБ:
  - Для работы бизнеса можно только открыть порты
  - IPS для блокировки известного вредоносного кода и атак по сигнатурам
  - Блокировать известные и неподтвержденные URL
- Статический набор правил



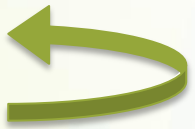
Что необходимо теперь

Цель

- Безопасная работа пользователей с приложениями с защитой от угроз «нулевого» дня

- Средства ИБ должны обеспечивать:
  - «Белые» и «черные» списки по приложениям и пользователям
  - «Песочница» для обнаружения неизвестного вредоносного ПО
  - Интегрированные политики для приложений, сигнатур угроз и URL

- Динамическая защита
  - Известный хороший
  - Известный плохой
  - Неизвестный



Замкнутый цикл (минуты)

paloalto networks

Периметр ЦОД (потоки трафика «север-юг»)

Что было раньше

Цель

- Защитить ЦОД от запрещенного трафика
- Политики базировались на:
  - Открытие/закрытие всех портов, поддерживаемых приложениями
  - IPS почти не применялся, либо как IDS
  - Меньше внимания исходящему трафику ЦОД
- Больше внимания соответствию регуляторам, чем защите от реальных угроз

Что необходимо теперь

Цель

- Защита ЦОД от любого скомпрометированного пользователя или вредоносного ПО. Пользователи более не являются доверенными
  - Политики используют:
    - «белые» списки: все участники взаимодействия известны, разрешены только необходимые функции соответствующим группам пользователей
  - Для разрешенного трафика использовать сканирование на все известные угрозы и локальную «песочницу» с целью своевременного обнаружения/блокирования атак
  - Применить строгие политики по приложениям для исходящего трафика, чтобы предотвратить утечку данных

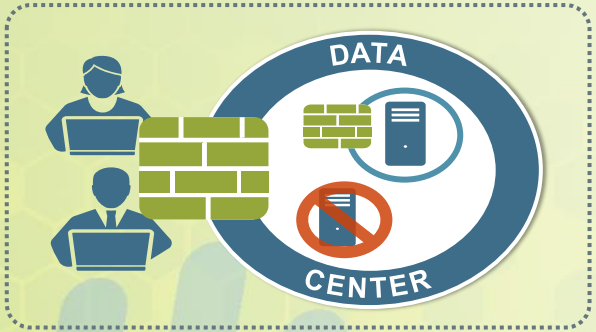
paloalto networks

Внутри ЦОД (потоки трафика «восток-запад»)

Что было раньше

Цель

- Защита виртуальных машин на уровне портов, которые используются приложениями
- Политики базировались на:
  - Открытие разрешенных портов между VM
  - IPS почти не применялся, либо как IDS



Что необходимо теперь

Цель

- Защита данных в ЦОД от любой скомпрометированной VM или вредоносного ПО. VM более не являются доверенными
- Прозрачное сегментирование и локализация трафика в пределах хоста
- Политики базируются на:
  - «белые» списки: все участники взаимодействия известны, разрешены только необходимые сервисы соответствующим VM на уровне приложений (а не портов)
- Динамические политики по атрибутам VM, автоматизация изменений, оркестрация
- Для разрешенного трафика использовать сканирование на все известные угрозы и локальную «песочницу» с целью своевременного обнаружения/блокирования атак и встроенного вредоносного ПО

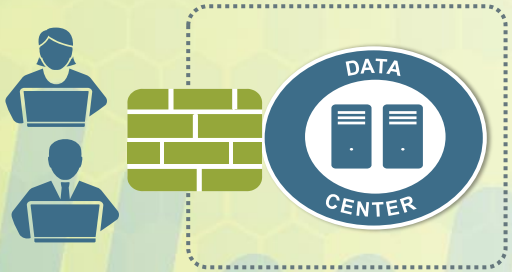
paloalto networks

Удаленные и мобильные пользователи

Что было раньше

Цель

- Remote VPN
- Обеспечить защищенный доступ пользователям извне
- Политики базировались на:
  - Создание шифрованных туннелей от устройств удаленных пользователей к VPN-концентратору в сети компании
  - После аутентификации пользователя – полный доступ к сегменту сети
  - Дополнительные средства защиты крайне ограничены



Что необходимо теперь

Цель

- Remote VPN с предотвращением вредоносного ПО и атак
- Обеспечить защищенный доступ пользователям извне безопасно для корпоративной сети
- Политики базируются на:
  - Проверка состояния мобильного устройства, чтобы убедиться, что оно безопасно для корпоративной сети
  - Проверка мобильного устройства на наличие вредоносного ПО
  - Шифрованный туннель для всего трафика
  - Использование User-ID для универсальных правил доступа, независимо от способа подключения
  - Полная инспекция всего трафика от мобильного устройства (к ЦОД, в Интернет) для обнаружения и блокирования вредоносной активности

paloalto networks

Предотвращение атак 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

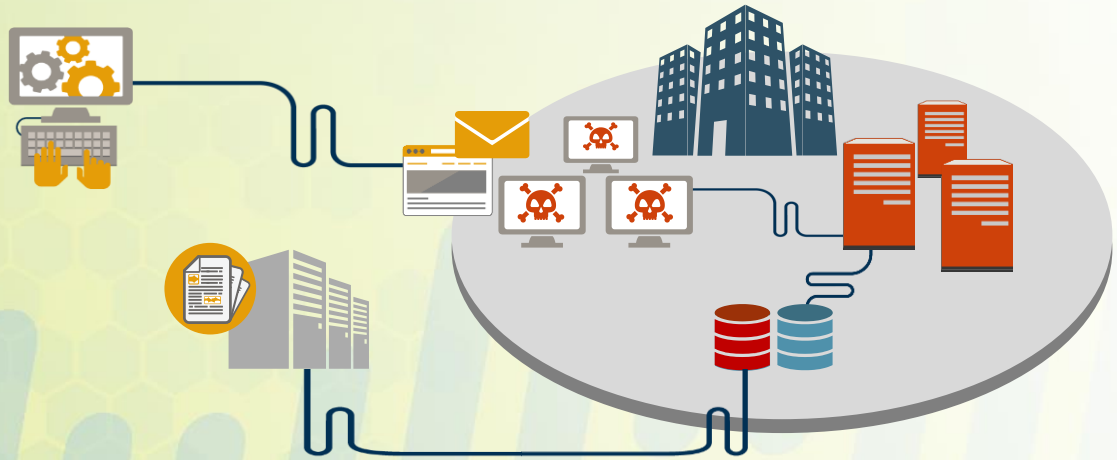
Next-Generation Firewall / GlobalProtect
- Создание зон безопасности с контролем доступа
- Инспекция трафика между зонами безопасности

WildFire
- 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

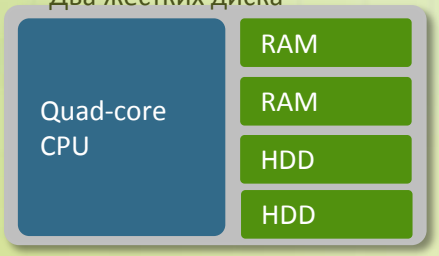
URL Filtering
- Блокирование исходящих соединений с вредоносными URL и IP



paloalto networks

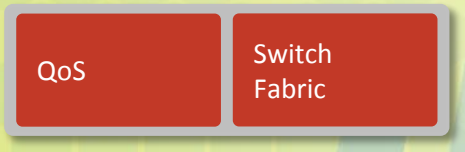
Аппаратная архитектура NGFW серии PA-5000 на базе Cavium, FPGA

- 4-ядерный ЦПУ управления
- Высокоскоростное журналирование и обновления таблиц маршрутизации
- Два жёстких диска



Control Plane

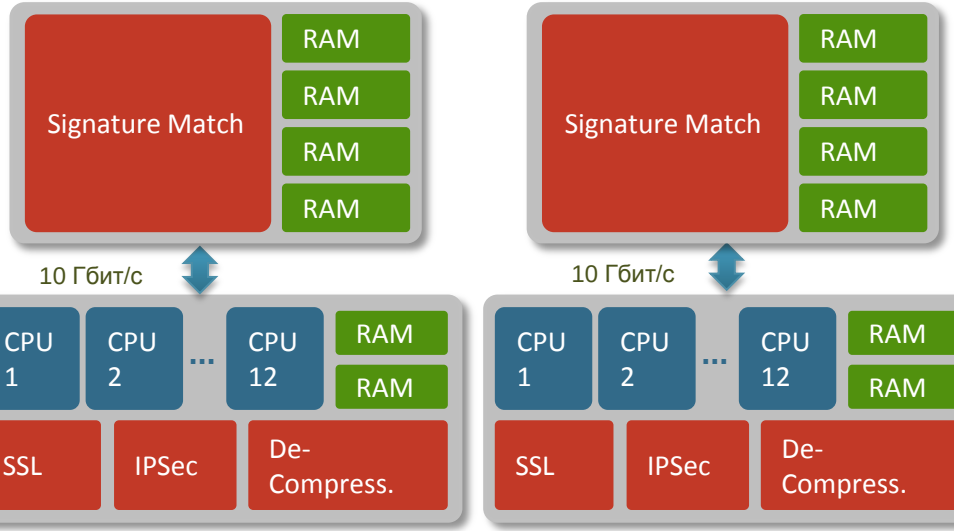
- 80 Гбит/с – производительность фабрики
- 20 Гбит/с – производительность QoS



Switch Fabric

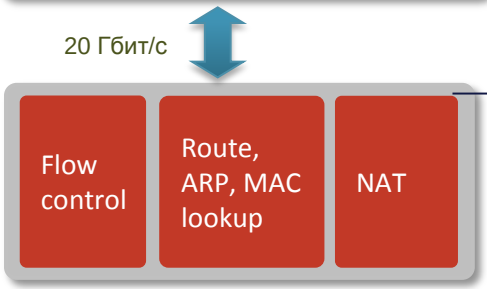
Сигнатурные интегральные схемы

- Потоковый анализ трафика
- Поиск уязвимостей (IPS), вирусов, шпионского ПО и пр.



Специализированные процессоры

- Многопоточная параллельная обработка, обеспечивающая множество функций безопасности
- Аппаратное ускорение ресурсоёмкого функционала (SSL, IPSec, разархивация)

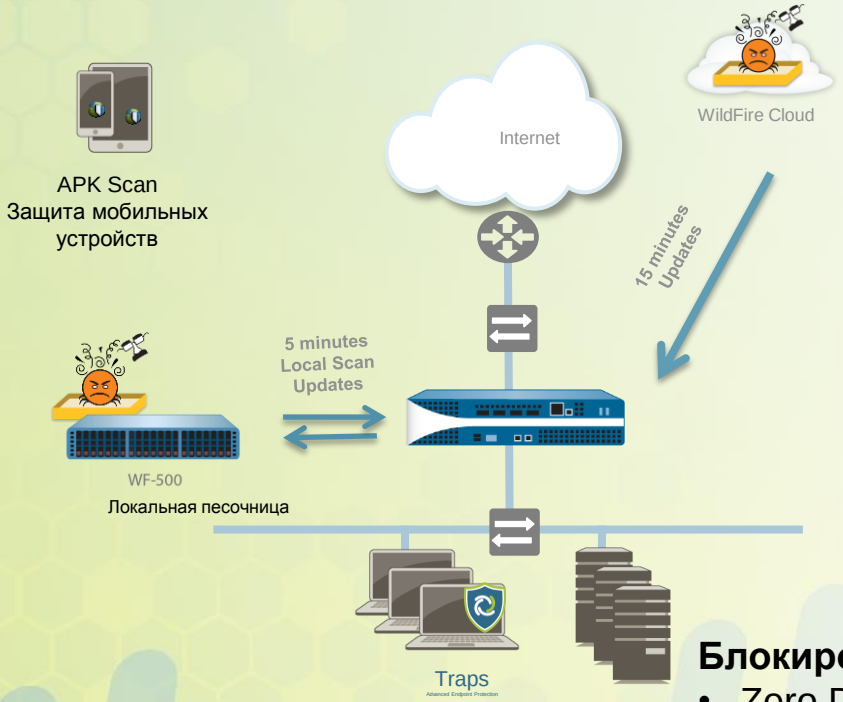


Data Plane

Сетевой процессор

- 20 Гбит/с – производительность сетевой обработки
- Аппаратное ускорение для поиска IP-маршрутов, MAC-адресов и функциональности NAT

Palo Alto Networks
платформа безопасности, где все сразу интегрировано и ускорено!



Блокировать на NGFW

- Все приложения
- Все пользователи User-ID
- Смотреть в SSL
- Сигнатуры IPS
- Сигнатуры антивируса
- Сигнатуры DNS
- Категории URL
- APT в локальной песочнице
- APT в облаке

Блокировать на хостах

- Zero Days
- Эксплойты
- Вредоносный код
- Без сигнатур!

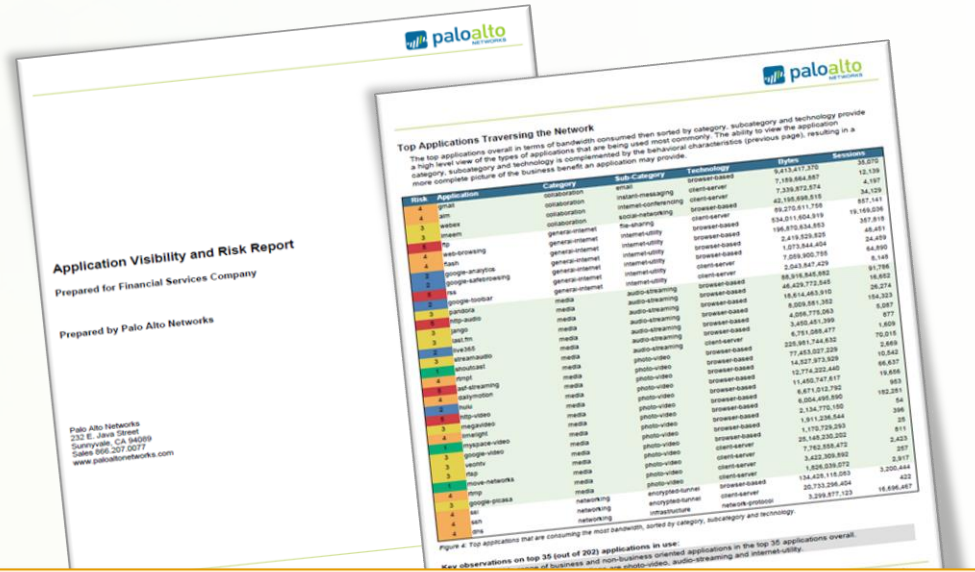
Сравните решение

- Palo Alto Networks
  - Встроенный функционал определения приложений
  - Все функции работают параллельно, а не последовательно
  - IPS
  - Wildfire – APT для всех протоколов
  - SSL и SSH расшифрование
  - Предотвращение на уровне сети
  - Предотвращение на хостах
  - Максимальная визуализация
  - Простая схема защиты в сети
  - Один производитель

Платформа Palo Alto Networks не создает пробок в сети

Обеспечиваем заданную производительность при всех включенных сервисах безопасности

С чего начать защиту Вашей 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!

Запрос по адресу Russia@paloaltonetworks.com

paloalto networks