# Какие вопросы чаще всего задают вендору при выборе решения по информационной безопасности

**Уральский форум по информационной безопасности финансовых организаций**

Денис Батранков
Russia@paloaltonetworks.com
twitter @batrankov

paloalto NETWORKS®

# АТАКА ANUNAK

Успешно получен доступ внутрь корпоративных сетей более чем 50 банков

Как атаковали:

- 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 проникновения в банк
- Снятие денег из банкоматов и через Интернет-кошельки

Подтверждено, что было под удаленным управлением 52 банкомата

Украдено более 1 млрд. рублей с 2013 по 2014 год из банков в России

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

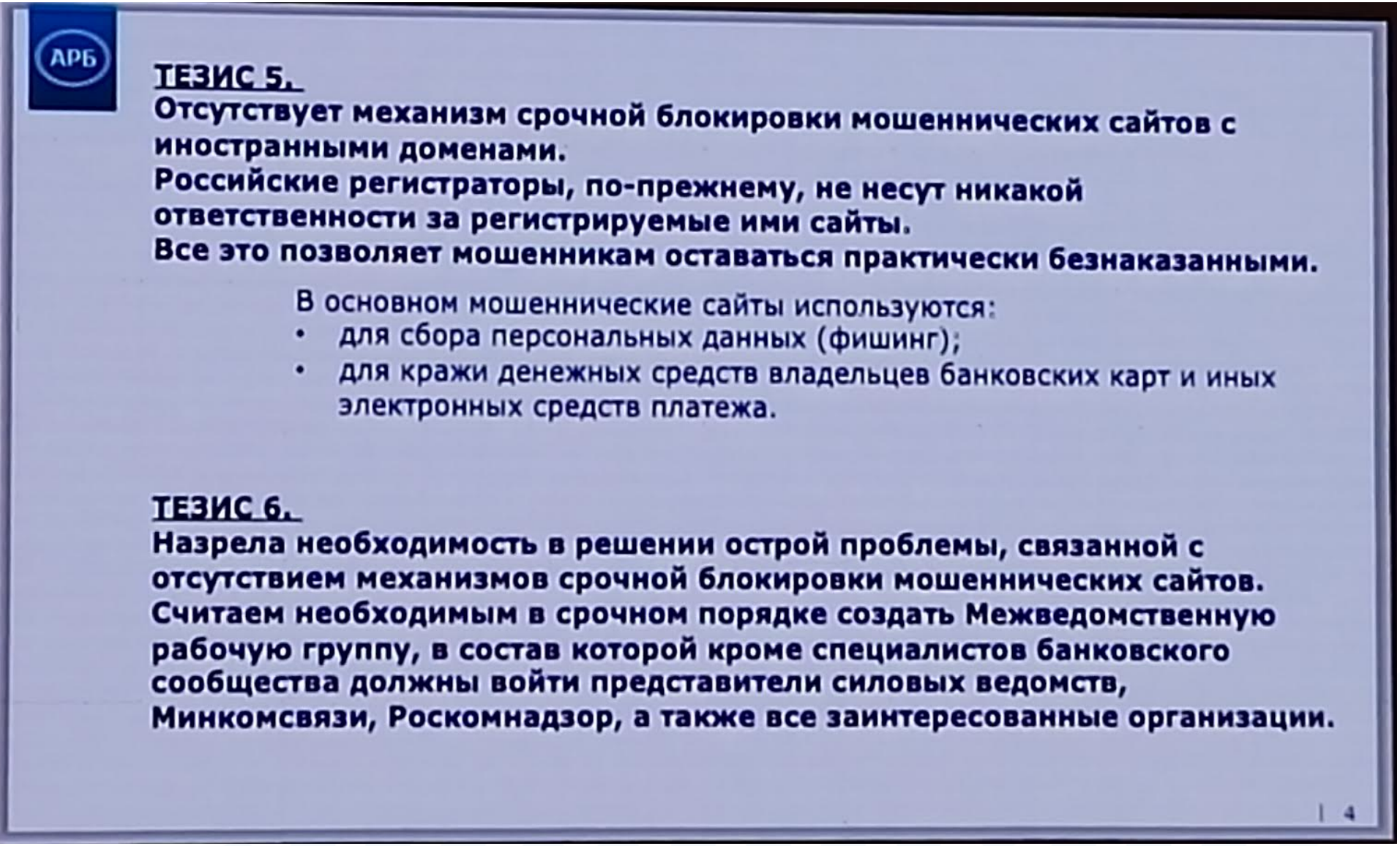
# Везде была защита, но не помогла:

- ✓ Классический «портовый» межсетевой экран
- ✓ Системы предотвращения атак (IPS)
- ✓ Технологии на базе HTTP прокси серверов
- ✓ Классический антивирус на ПК (лучший из top10)

paloalto NETWORKS

# Почему?

# На конференции мы обсуждали это:



АРБ

**ТЕЗИС 5.**

**Отсутствует механизм срочной блокировки мошеннических сайтов с иностранными доменами.**
**Российские регистраторы, по-прежнему, не несут никакой ответственности за регистрируемые ими сайты.**
**Все это позволяет мошенникам оставаться практически безнаказанными.**

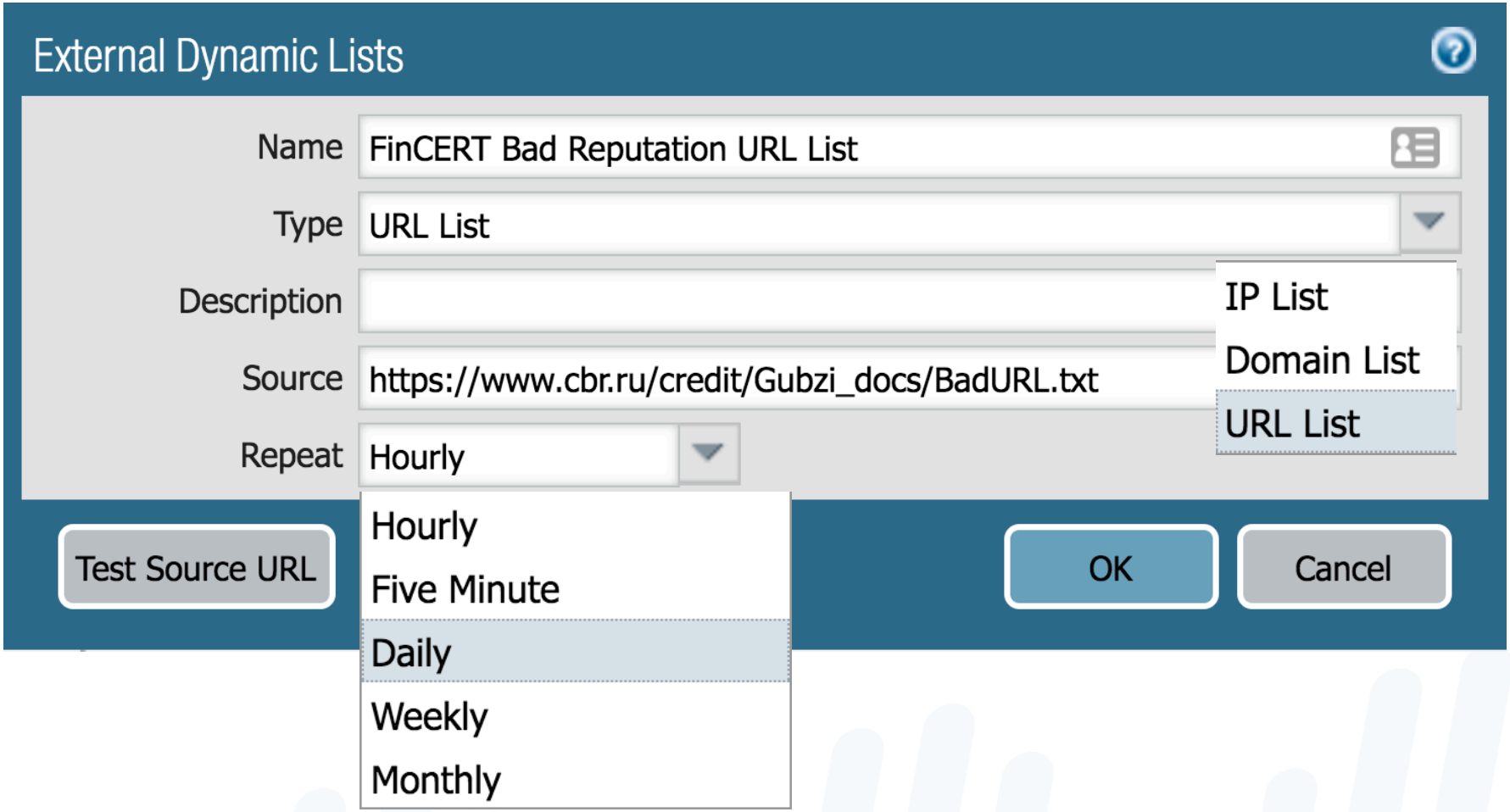
В основном мошеннические сайты используются:
- для сбора персональных данных (фишинг);
- для кражи денежных средств владельцев банковских карт и иных электронных средств платежа.

**ТЕЗИС 6.**

**Назрела необходимость в решении острой проблемы, связанной с отсутствием механизмов срочной блокировки мошеннических сайтов.**
**Считаем необходимым в срочном порядке создать Межведомственную рабочую группу, в состав которой кроме специалистов банковского сообщества должны войти представители силовых ведомств, Минкомсвязи, Роскомнадзор, а также все заинтересованные организации.**

4

# Предлагаю механизм. Межсетевой экран может подгрузить список IP, URL, доменных имен с сервера ФинЦЕРТ из текстового файла и сразу заблокировать доступ




Скачивает этот список автоматически

www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/external-dynamic-list.html

# Threat Intelligence:

Как решение блокирует обратный канал от зараженных пользователей и серверов к внешнему серверу управления злоумышленника (command & control)?

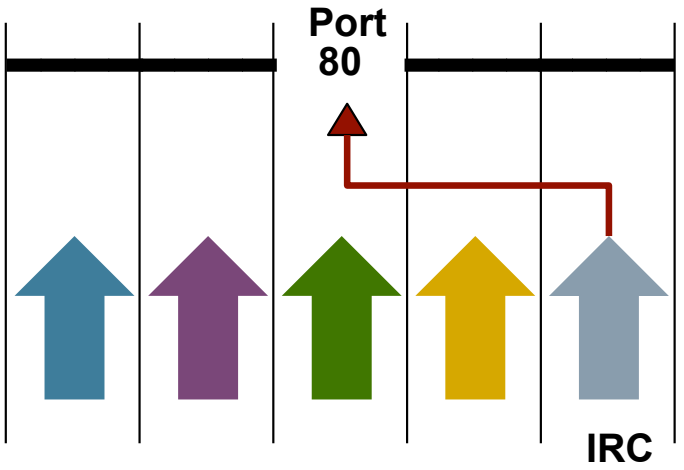
# DNS Sinkholing:

Как выполняется блокирование DNS запросов к C&C серверами?

Что вендор говорит про fast-flux?

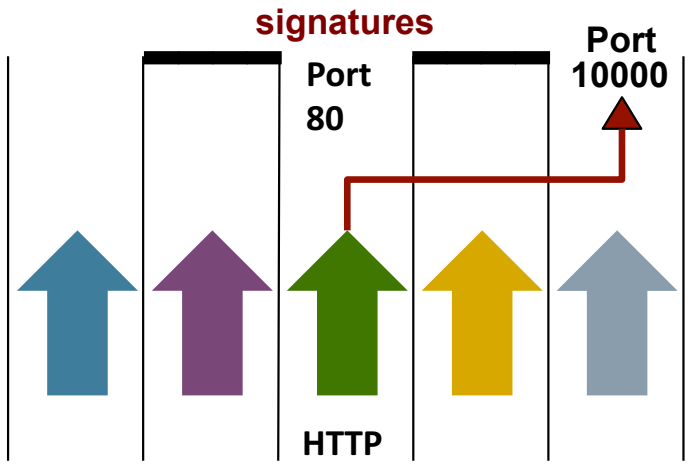
# Техники уклонения от IPS/IDS и Firewall

1. Распространение вредоносного ПО или нелегитимного трафика через открытые порты
   - нестандартное использование стандартных портов
   - создание новых специализированных протоколов для атаки



# Техники уклонения от IPS/IDS и Firewall

2. Использование стандартных протоколов на нестандартных портах – уклонение от сигнатурного сканирования



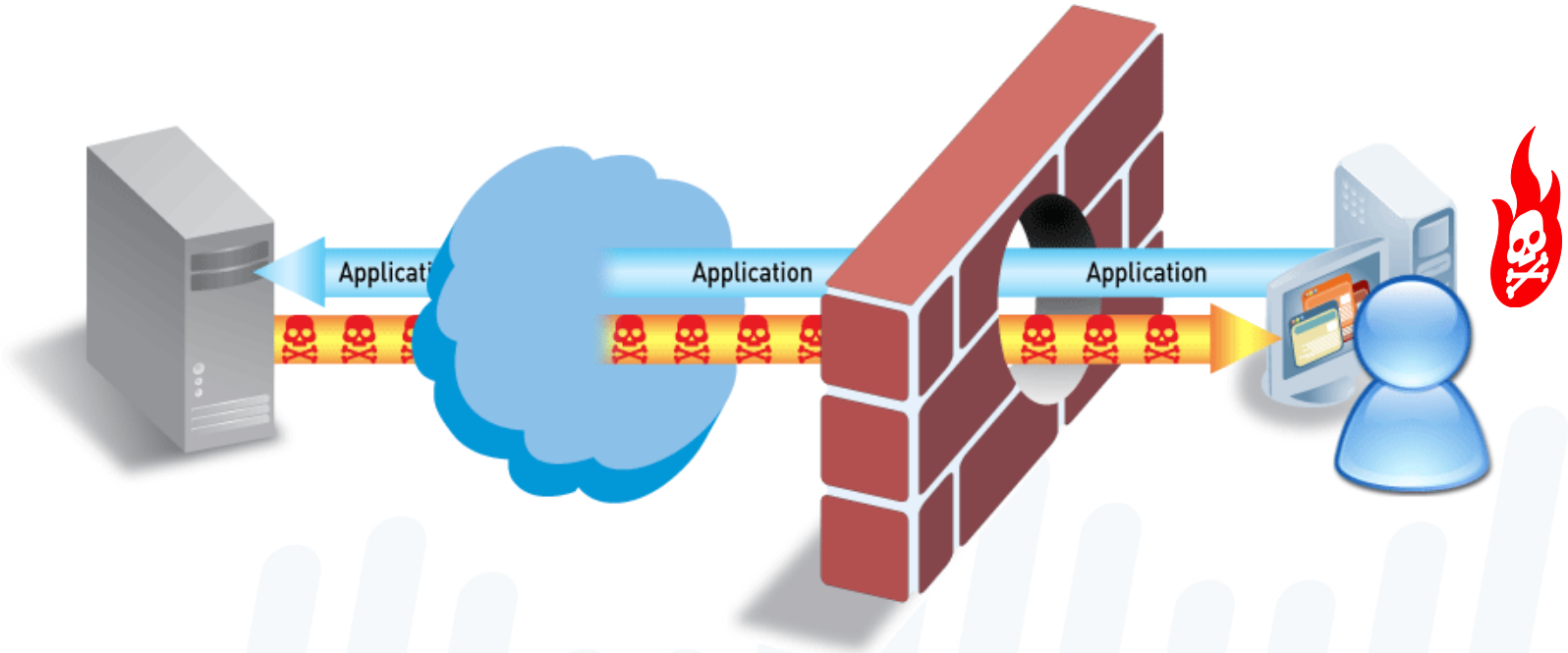
# Даже стандартные приложения являются источником рисков

## Приложения могут быть “несанкционированными”

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

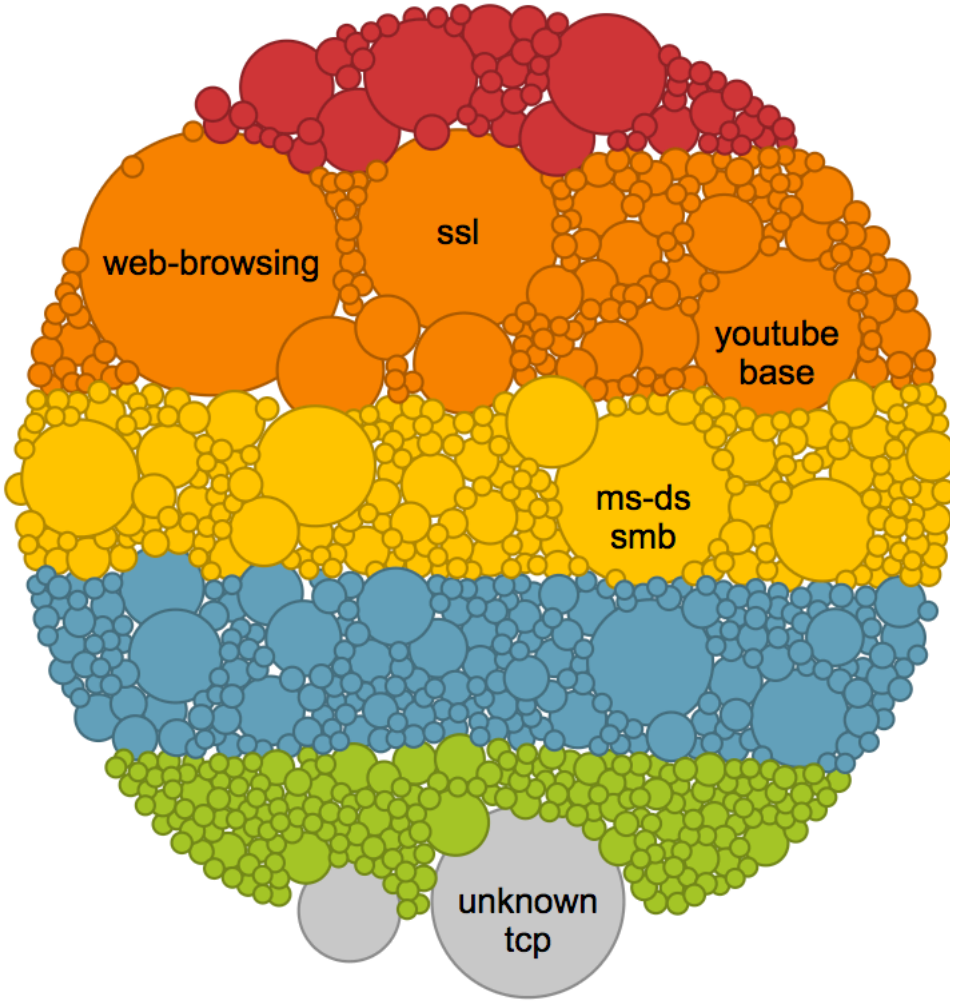
## Угрозы есть внутри приложений

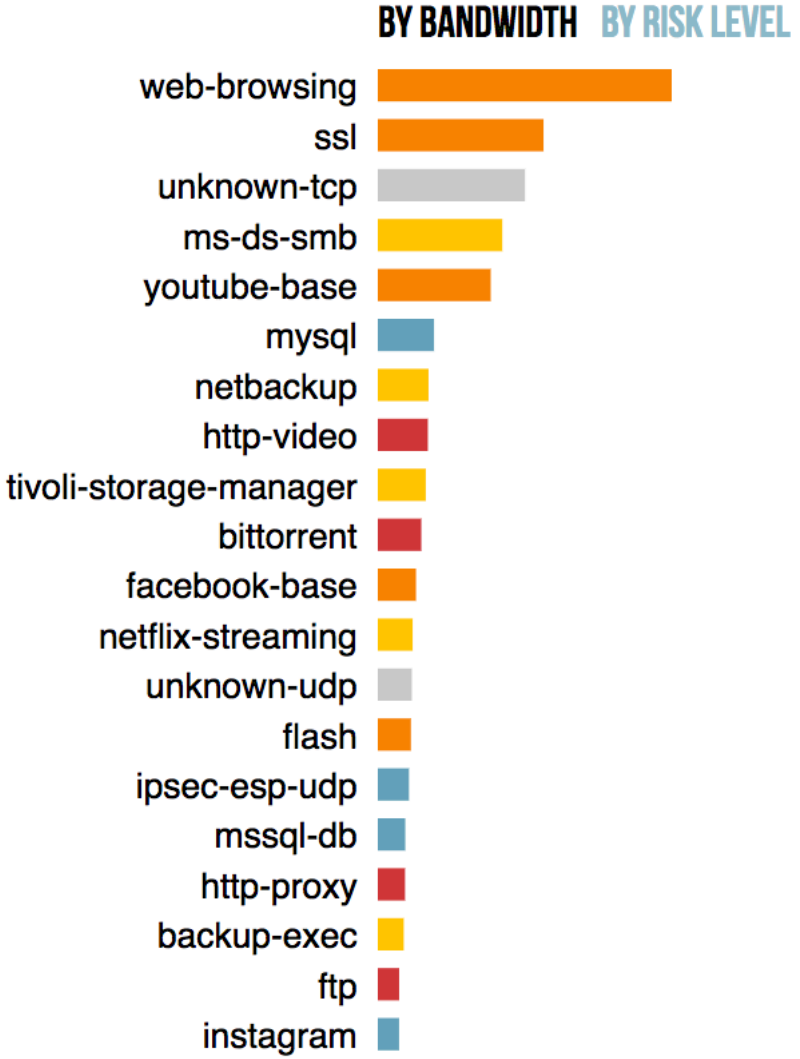
- Угрозы переместились на уровень приложений – система защиты еще на уровне сети




paloalto NETWORKS

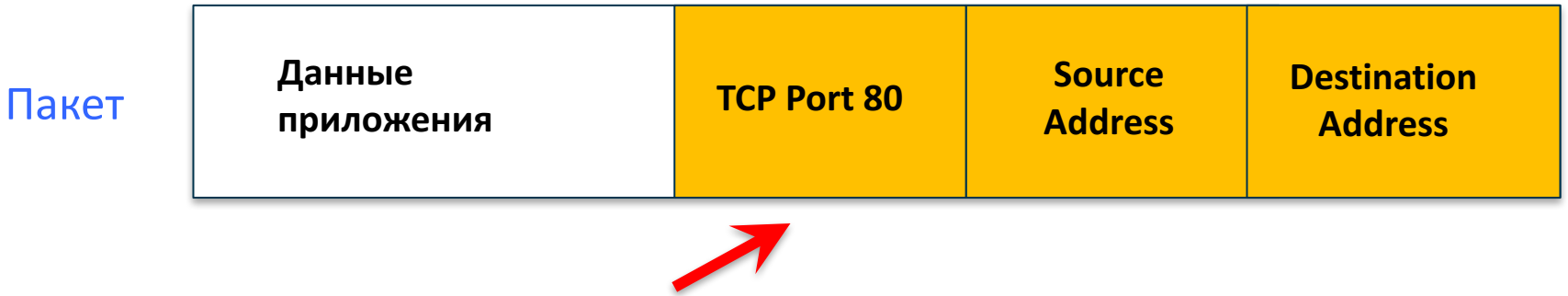
# Через периметр компании проходит 200-300 разных приложений



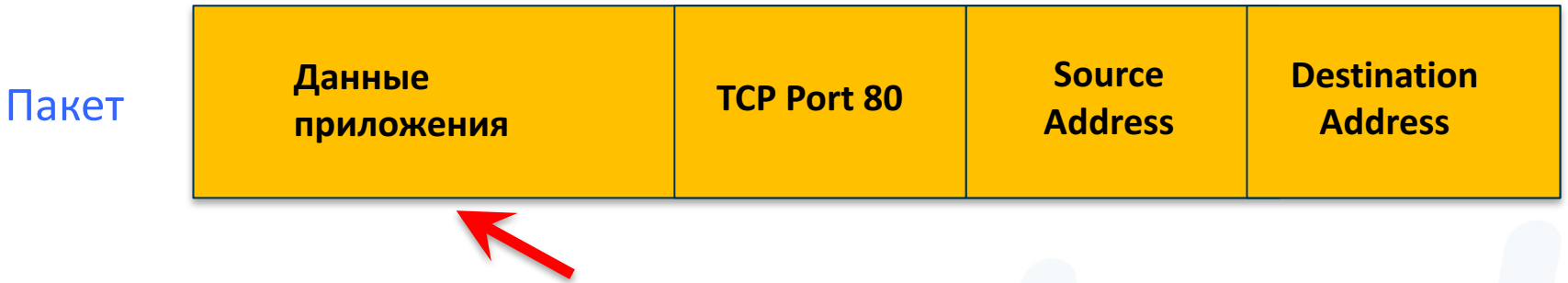




paloalto NETWORKS

# Как отличает приложения ваш межсетевой экран?




Критерий: Порт – традиционно обозначал приложение (HTTP = порт 80). А что будет, если приложение использует нестандартный порт?




Нужно добавить новый критерий проверки: данные приложения
Приложение использует специфические передаваемые данные и по ним его можно определить вне зависимости от порта
flash = данные для анимации внутри браузера от Adobe

paloalto NETWORKS

Анализируя данные, мы начинаем идентифицировать приложения вне зависимости от порта.

Например: другого способа определить в трафике Skype, TeamViewer, TOR, Bittorent не существует.

paloalto NETWORKS

# Может ли система защиты определять динамические приложения?

Например: Skype, TeamViewer, TOR, Bittorent.

# Может ли система защиты
# - и видеть приложения
# - и блокировать приложения?

Пример: если skype блокировать один способ подключения, то он находит другие методы, обходя текущие блокировки

paloalto NETWORKS

# Может ли система защиты определять приложения по их нестандартным портам?

Например:  POP3 по порту 10000

# Адаптируется ли аналитика средства защиты, если приложение использует нестандартный порт?

Например: FTP по 80 порту

# Квалификаторы Firewall и UTM

По каким критериям мы принимаем решение о потоке трафика?

**rule1**

- Если совпал source, destination, port
- Действие

**rule2**

- Если совпал source, destination, port
- Действие

**rule3**

- Если совпал source, destination, port
- Действие

# Квалификаторы NGFW Palo Alto Networks

По каким критериям мы принимаем решение о потоке трафика?

**rule1**

- Если совпал source, destination, port, приложение, URL, пользователь
- Действие

**rule2**

- Если совпал source, destination, port, приложение, URL, пользователь
- Действие

**rule3**

- Если совпал source, destination, port, приложение, URL, пользователь
- Действие

Есть разница?

paloalto NETWORKS

# Является ли приложение квалификатором в вашем межсетевом экране?

# User-ID: Как вы распознаете пользователя на входе в сеть?

**Пользователь = SOURCE IP + SOURCE PORT в каждый момент времени**

1) Соответствие пользователь-IP-порт получаем из :

- активная аутентификация (Captive Portal, локальный агент)
- пассивная идентификация
- активная идентификация

2) user-group-mapping

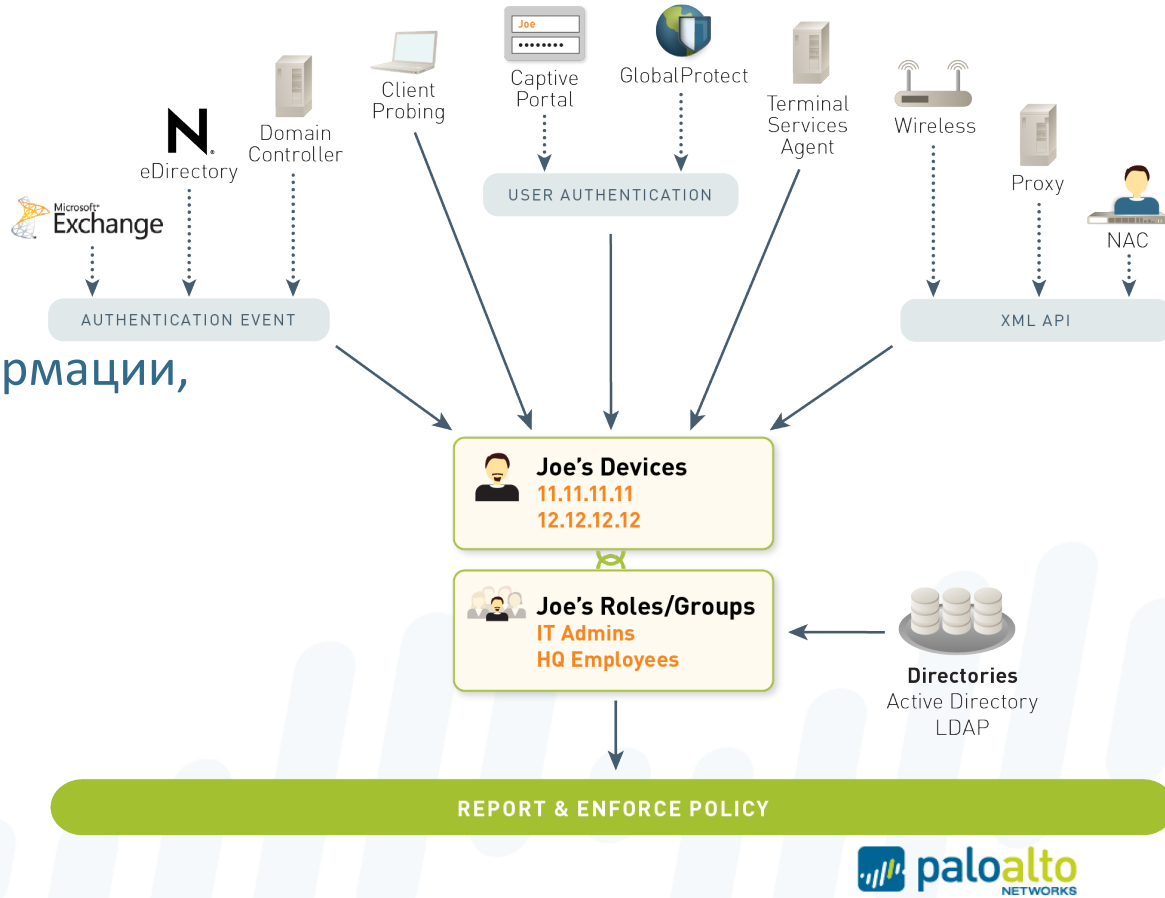
Чем больше источников информации,

тем лучше:

MS AD, сетевые ресурсы,

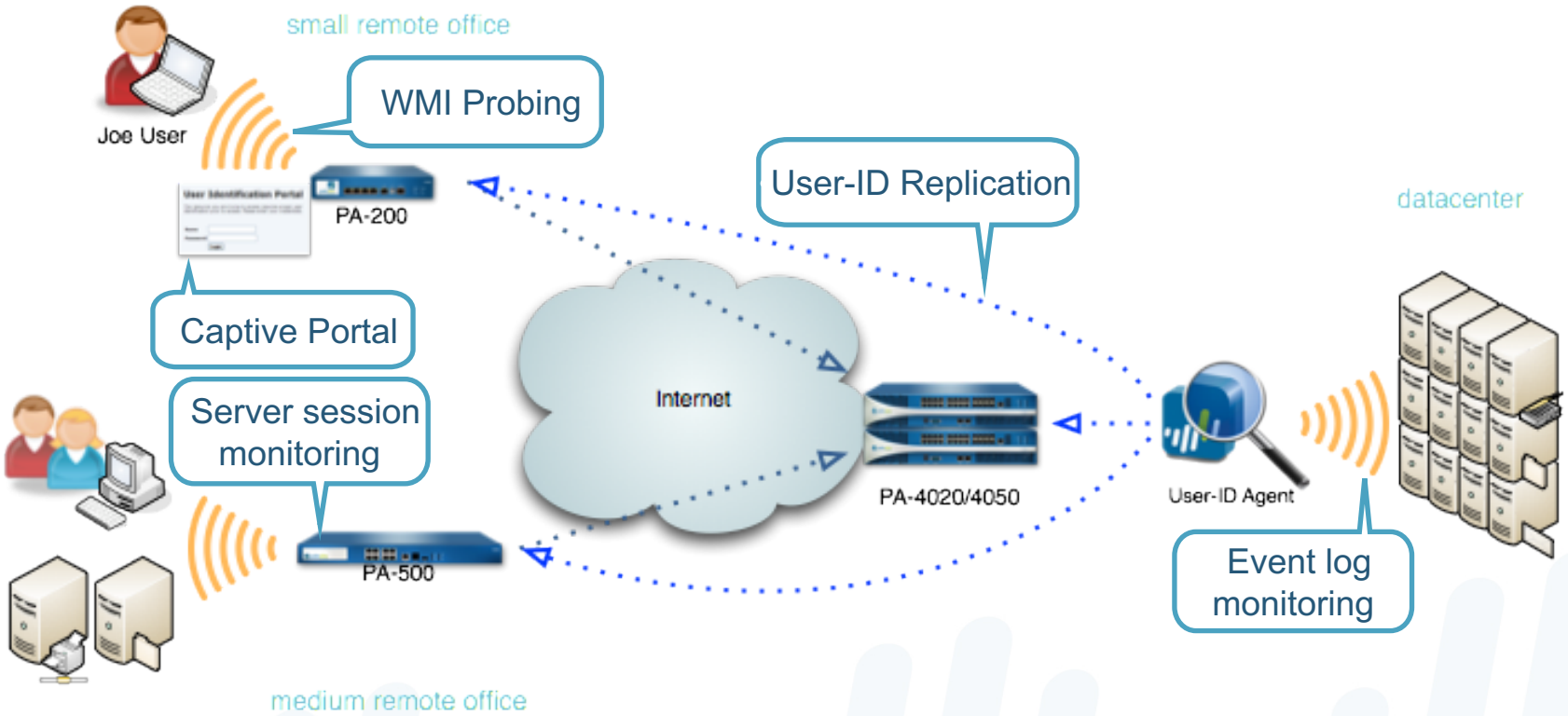
VDI, Wi-Fi, NAC,

SSL VPN, BYOD, …



# User-ID в распределенной сети очень полезна

Совмещение активной и пассивной аутентификации/идентификации, агентской и безагентской схемы, репликация данных User-ID между NGFW



# Из каких источников средство защиты берет соответствие конкретного пользователя и его текущего IP?

Например: из журналов Active Directory

# Сегментация сети

- Почему не смотреть свой же трафик внутри?
- Разделите сеть на зоны и контролируйте приложения и угрозы внутри и заражения станций

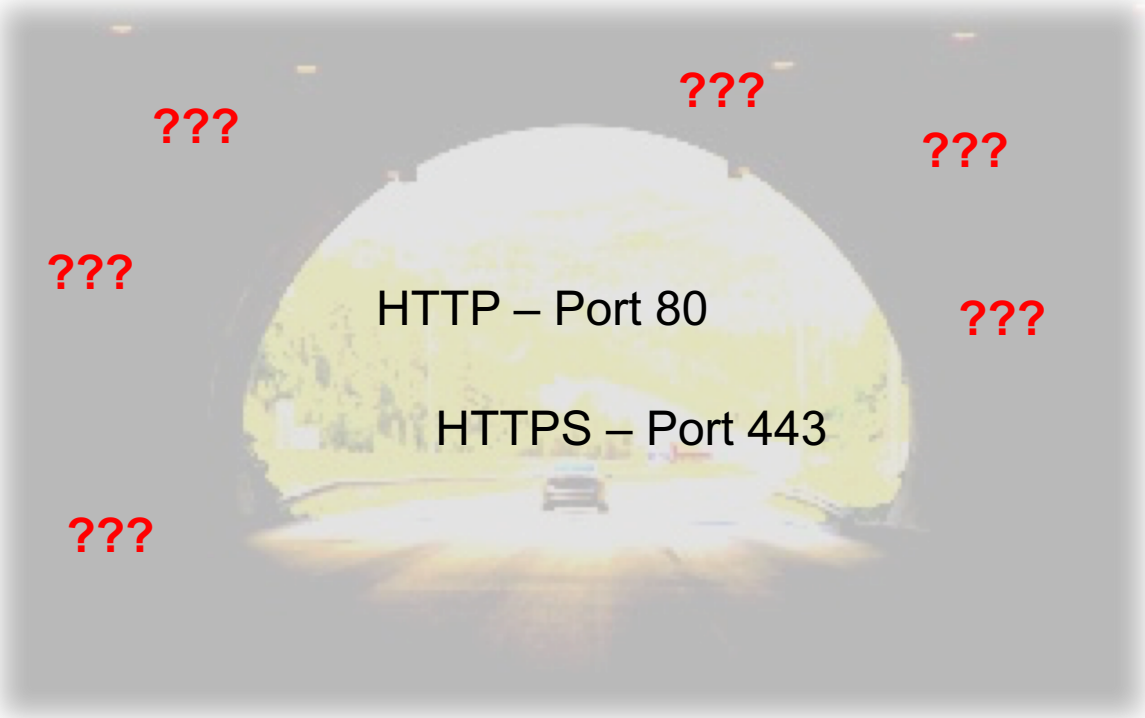
Пример: В атаке ANUNAK взломав компьютер сотрудника банка, следующим этапом проникали в банкоматы по RDP, потому что не было внутренней сегментации

# Хватит ли производительности устройства защиты на внутренний трафик между сегментами?

Например: вы хотите проверять приложения, вирусы и атаки на суммарной скорости 10Гбит/с

# У вас 200-300 приложений в сети. Сколько из них вы защищаете сегодня?

## Чаще всего защита только HTTP и SMTP




Фокус на HTTP/SMTP оставляет злоумышленнику доступным большой арсенал атак по другим приложениям.
Проверяете ли вы FTP, IMAP, POP3?

paloalto NETWORKS

# Проверка файлов на NGFW

Межсетевые экраны нового поколения видят файлы (которые приложения передают), дают возможность блокировать передачу файлов по различным критериям, например:

- Запретить передачу данного типа файлов
- Запретить передачу файла, потому что там содержится вирус

Например:
запретить передачу зашифрованного архива RAR в GMAIL

paloalto NETWORKS

# В каких именно приложениях ваше средство защиты видит файлы?

Например:

- HTTP (S)
- SMTP (S)
- POP3 (S)
- IMAP (S)
- FTP (S)
- SMB

paloalto NETWORKS

# В каких именно приложениях работает сигнатурный антивирус?

Например:

- HTTP (S)
- SMTP (S)
- POP3 (S)
- IMAP (S)
- FTP (S)
- SMB

paloalto NETWORKS

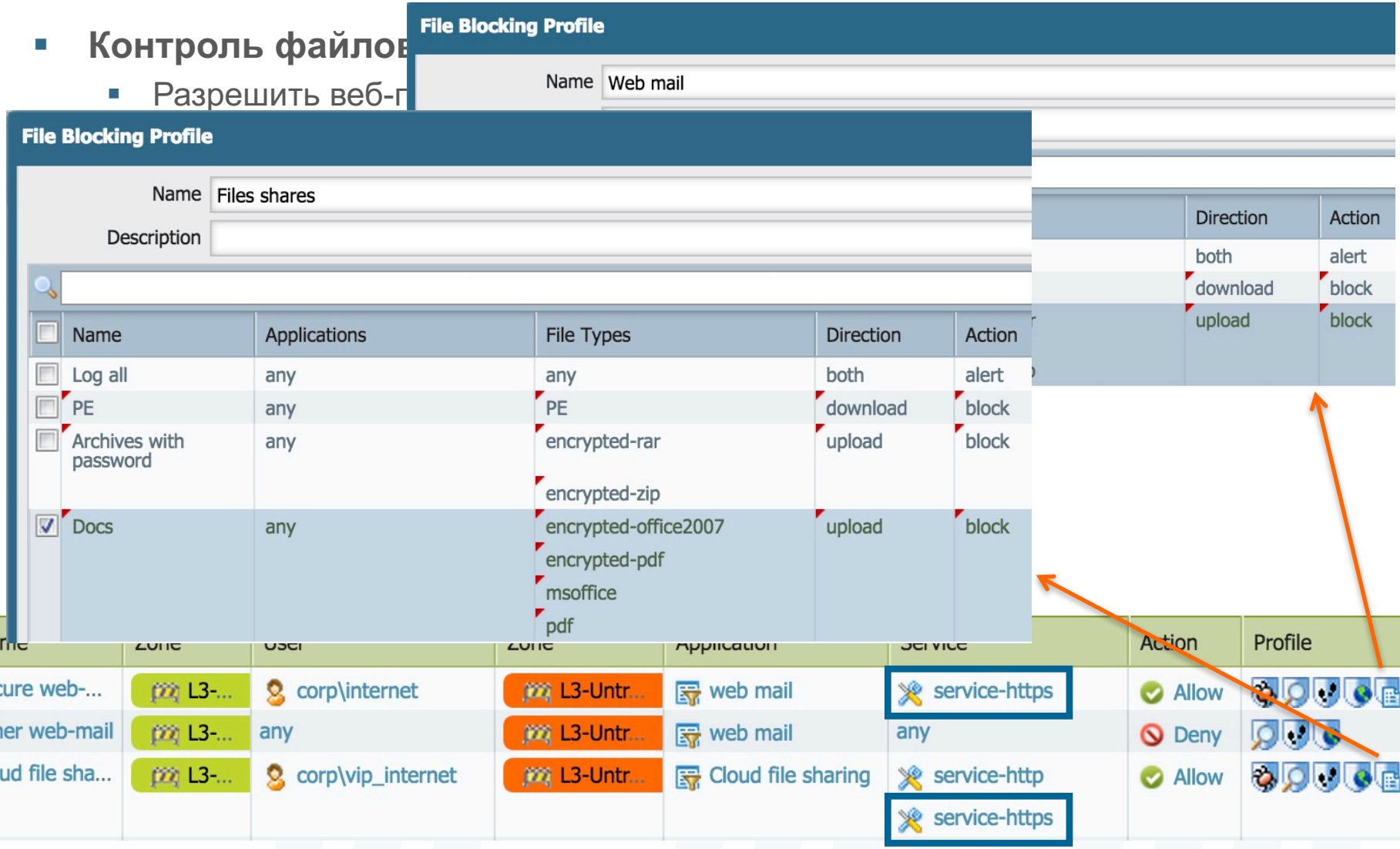
# Как устройство защиты определяет тип файла: по имени или по внутреннему формату?

Например:
Злоумышленник может переименовать exe файл в расширение txt и передать
Злоумышленник может переименовать doc файл в jpg и передать

paloalto NETWORKS

# Пример

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



# Может ли ваш межсетевой экран пройти NGFW тест на сайте http://pdftest.ngfw-test.com/ ?

- Включить блокировку pdf файлов только в приложении Application1. Показать в журнале межсетевого экрана соответствующую запись где есть следующие поля: имя приложения, имя файла (должно быть PowerShell_ISE_v4.pdf) и примененное действие (должно быть заблокировано)
- Включить блокировку вирусов только от приложения Application1. Показать в журнале межсетевого экрана соответствующую запись где есть следующие поля: имя приложения, имя вируса (должно быть Eicar) и действие (должно быть заблокировано)

# Две стороны одного протокола SSL

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

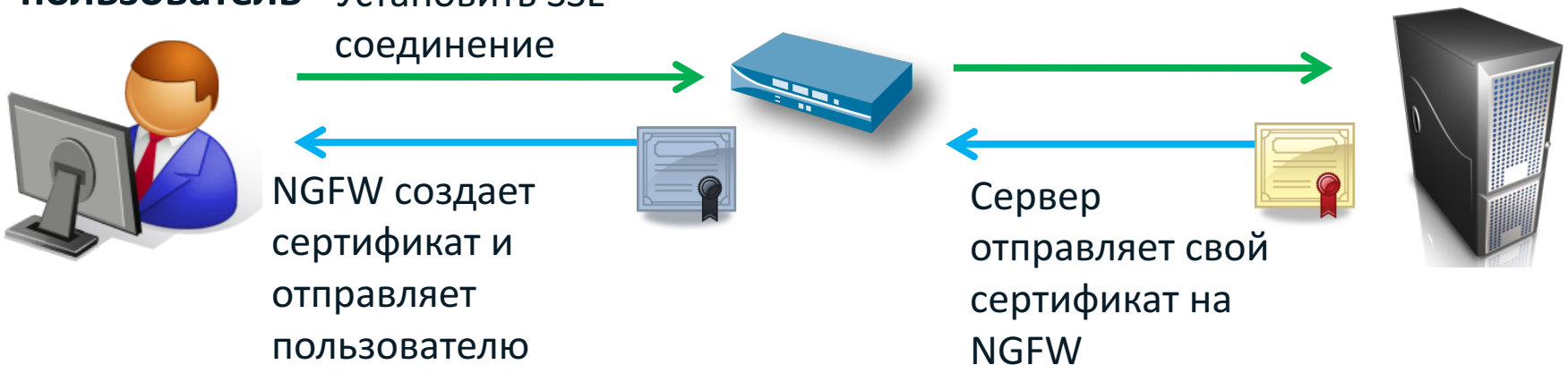
SSL для защиты данных или чтобы скрыть вредоносную активность?

paloalto NETWORKS

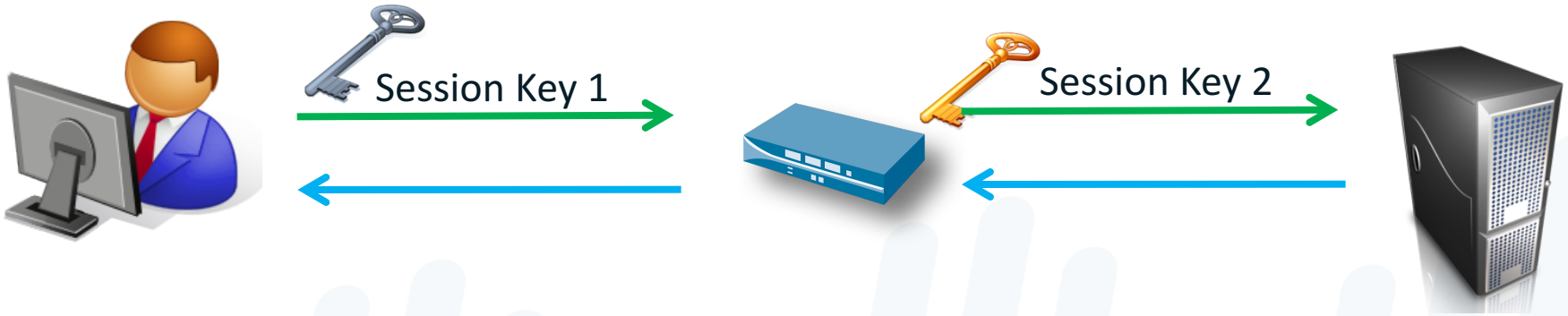
# Исходящий SSL требует перехвата сессии

**Внутренний пользователь**

**Внешний сервер**

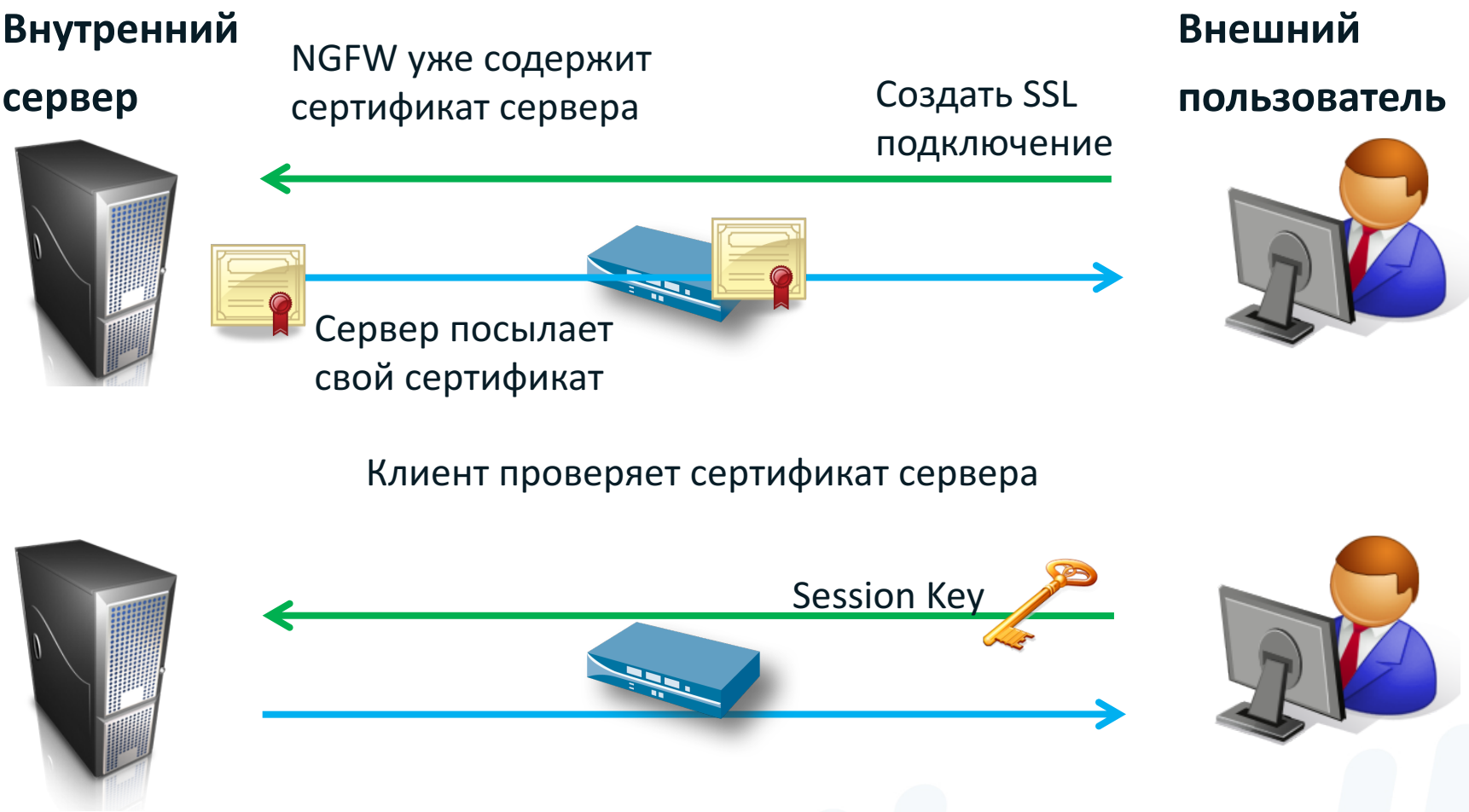



Клиент думает, что проверяет сертификат от сервера, а на самом деле от NGFW




paloalto NETWORKS

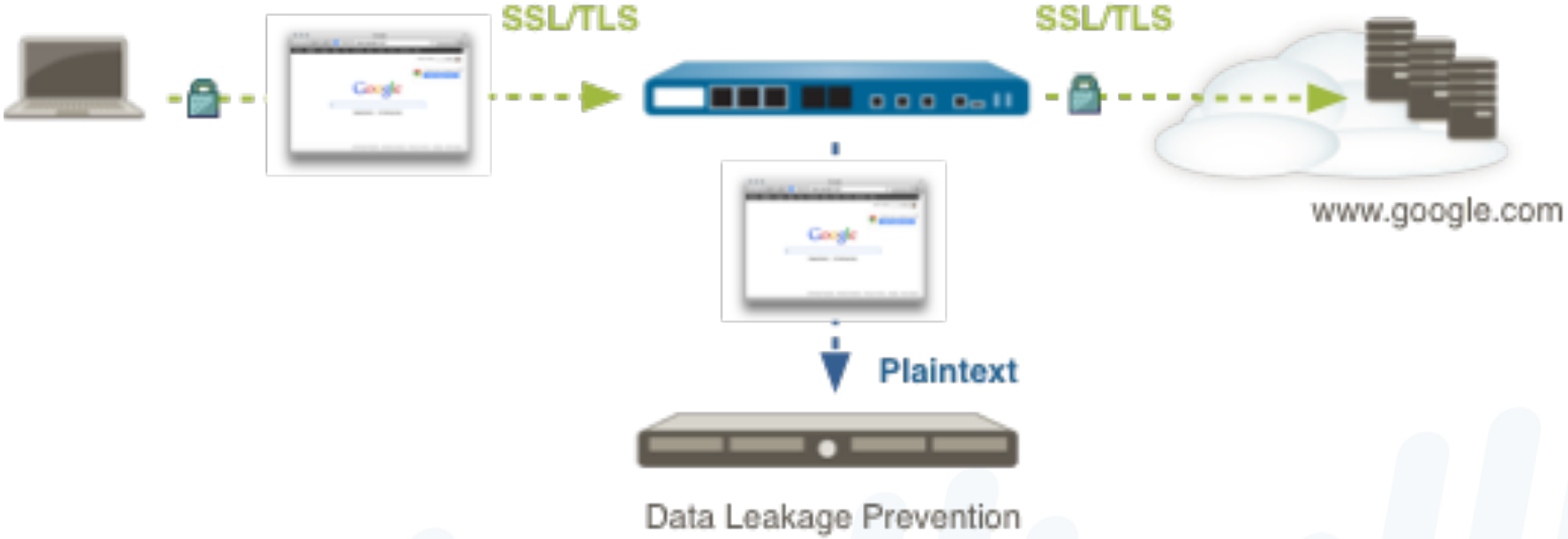
# Входящий SSL не требует перехвата




*Сессия между сервером и пользователем остается неизменной, однако NGFW видит сессионный ключ и расшифровывает трафик*

# Схема работы расшифрования SSL

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



# Вы расшифровываете SSL?

# Насколько сильно падает производительность оборудования при включении расшифрования SSL?

# SSL и URL фильтрация

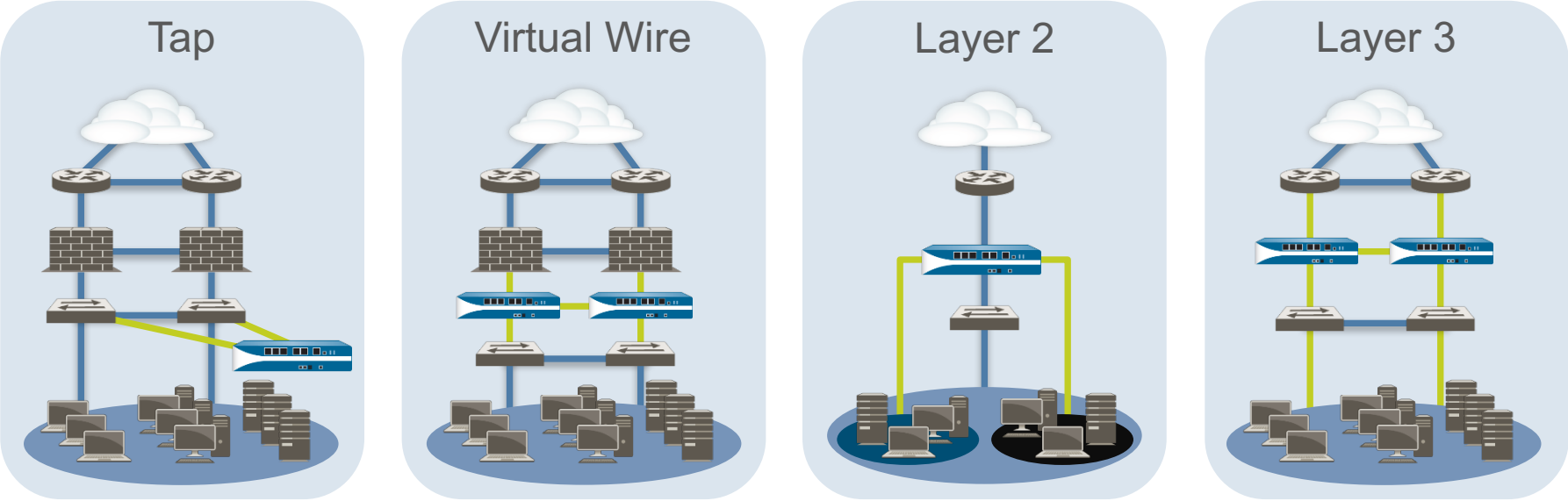
- URL категории без расшифрования
  - IP адрес сервера
  - Common Name and SubjectAlternativeName in a Server Certificate
  - SNI (Server Name Indicator) in TLS Handshake Extension

- URL фильтрация после расшифрования
  - URL база с категориями (60+ Cayegories, millions of URLs)
  - Собственные URL ссылки и категории
    - До 200K собственных URL ссылок в PA-7050

# Как работает URL фильтрация для HTTPS?

# Вы расшифровываете SSH?

# Интеграция 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

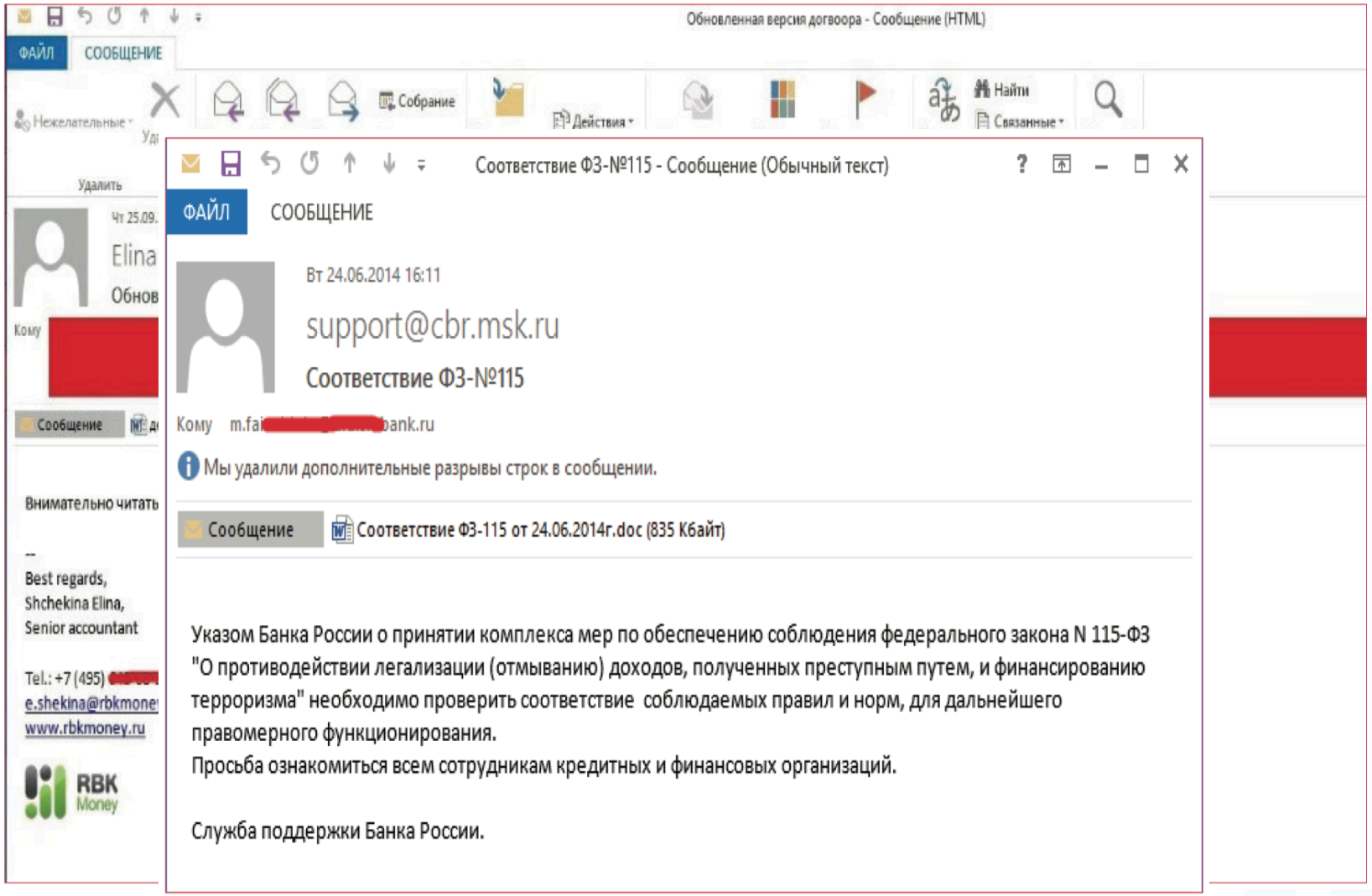
# Какие системы виртуализации защищает решение?

Например: VmWare, Hyper-V, KVM, Citrix

# Построение защиты от современных угроз и целенаправленных атак (APT)

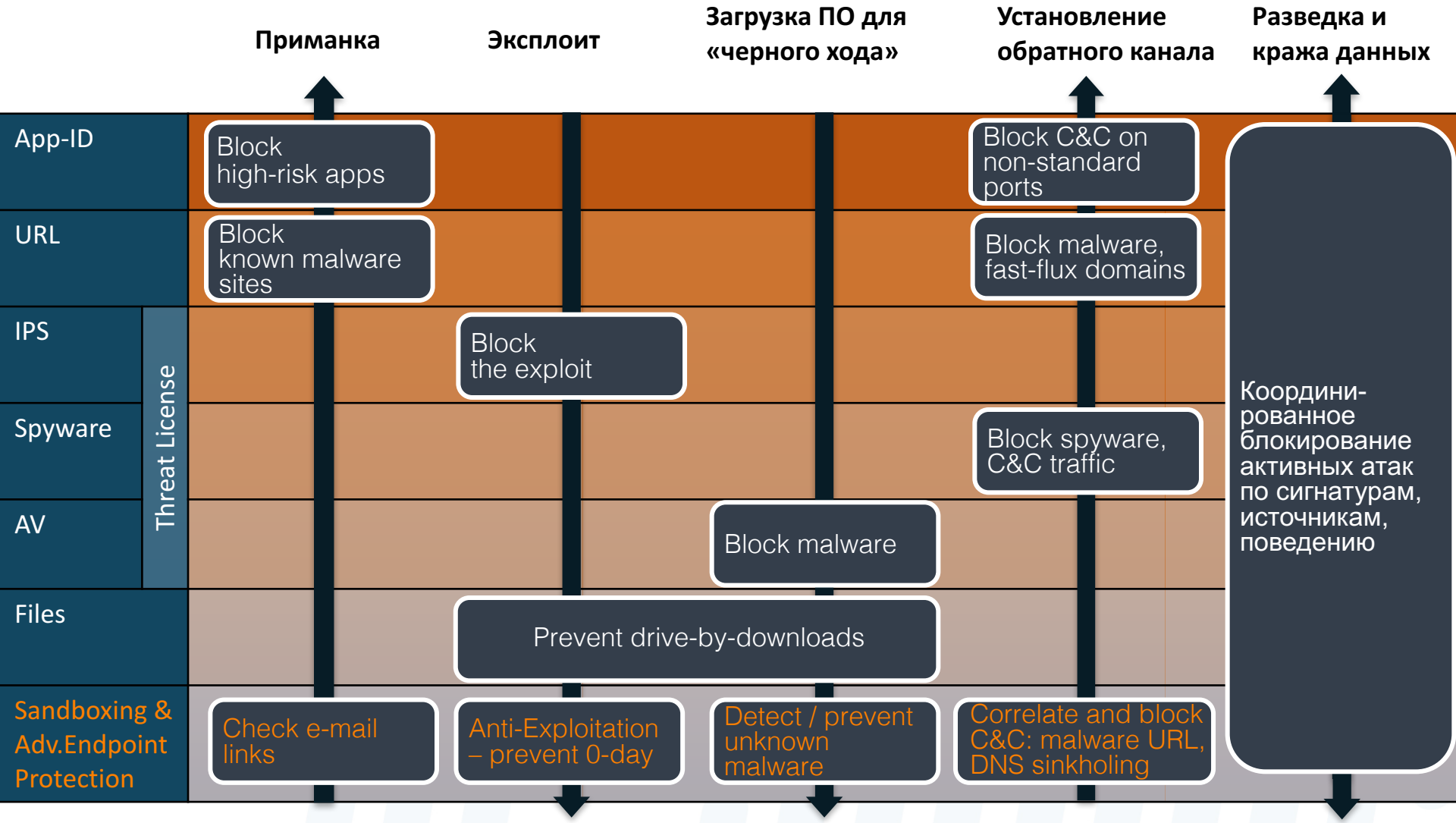
paloalto NETWORKS
the network security company™

# Anunak – письмо с вредоносным вложением




paloalto NETWORKS

# Технологии Palo Alto Networks, применяемые для защиты от современных угроз




Промокод: СказочноеБанное

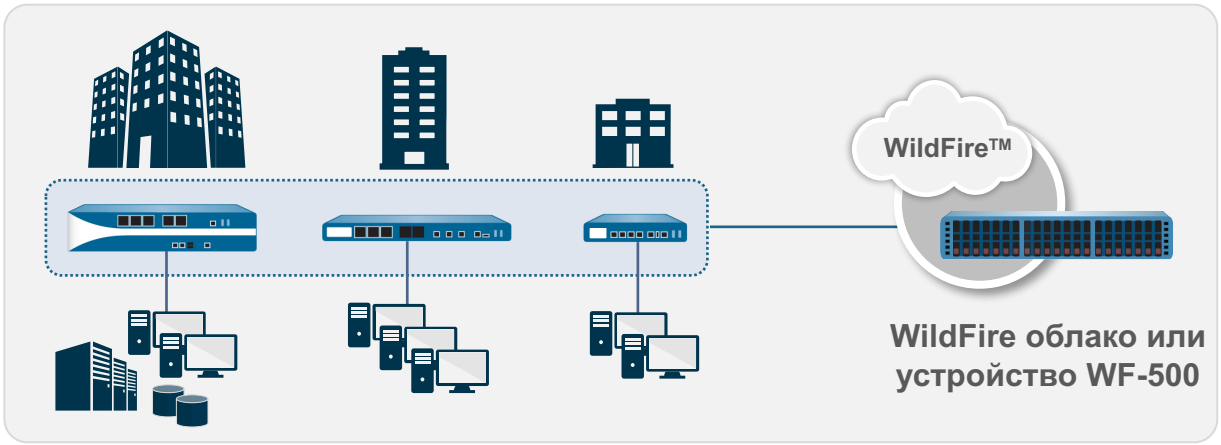
paloalto NETWORKS

# Анализируем поведение: помещаем файл в песочницу

## Wildfire – защита от неизвестных угроз на уровне сети

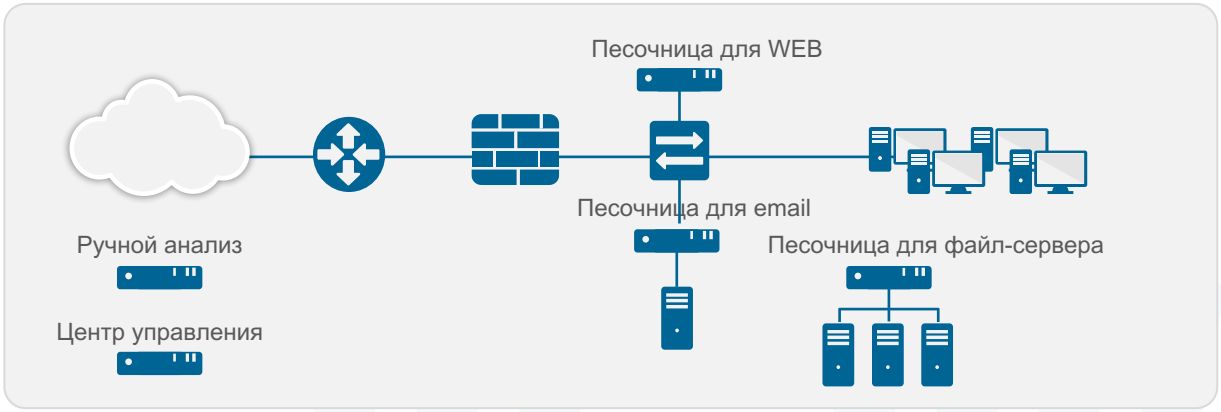
# Разные архитектуры песочниц

## Один межсетевой экран + одна песочница Wildfire.
## При масштабировании новая песочница не нужна




- Легкая интеграция
- Легко расширяется
- Эффективное расходование средств
- Перехват файлов на NGFW и отправка в WildFire
- Отправка файлов в WildFire через XML API

## Много песочниц: на каждое приложение: HTTP, SMTP, POP3, IMAP, FTP, SMB
## При масштабировании нужны снова все эти песочницы




- Сложно управлять
- Сложно масштабировать
- Дорого
- Множество устройств для перехвата файлов из разных приложений

paloalto NETWORKS

# Сколько файлов может обработать песочница в день?

# Скорость создания сигнатуры в песочнице?

# Есть сигнатура в песочнице – чем блокировать теперь трафик с вредоносным кодом?

Будет ли перехватывать файлы песочница по нестандартному порту?

Как работает с нестандартными портами потоковый антивирус?

Как работает с нестандартными портами сетевой IPS?

# Какие типы файлов можно запускать в песочнице?

**Пример:**

**exe, dll, bat, sys, flash, jar, apk, doc, xls, pdf, Mach-O, DMG, PKG**

# В каких приложениях работает песочница?

Например:

- HTTP (S)
- SMTP (S)
- POP3 (S)
- IMAP (S)
- FTP (S)
- SMB

paloalto NETWORKS

# Проверяет ли песочница URL ссылки в почтовых сообщениях песочница?

# Как «песочница» предотвращает отложенное исполнение вредоносных файлов с целью избежать обнаружения?

# Что предлагает производитель делать с файлом, в то время пока файл анализируется и еще нет вердикта?

Пример: сотрудник скачал файл по FTP на свой компьютер. Сигнатурный антивирус говорит, что файл чистый. Песочница еще не вернула результат анализа. Что делать?

paloalto NETWORKS

# Сколько будет стоить техническая поддержка на следующий год?

Есть ли у вендора первый уровень техподдержки на русском языке?

Круглосуточно 24x7 или 8x5?

Как происходит замена оборудования?

Сколько по времени это занимает?

# Средний срок жизни системы?

# Туннелирование в DNS запросах?

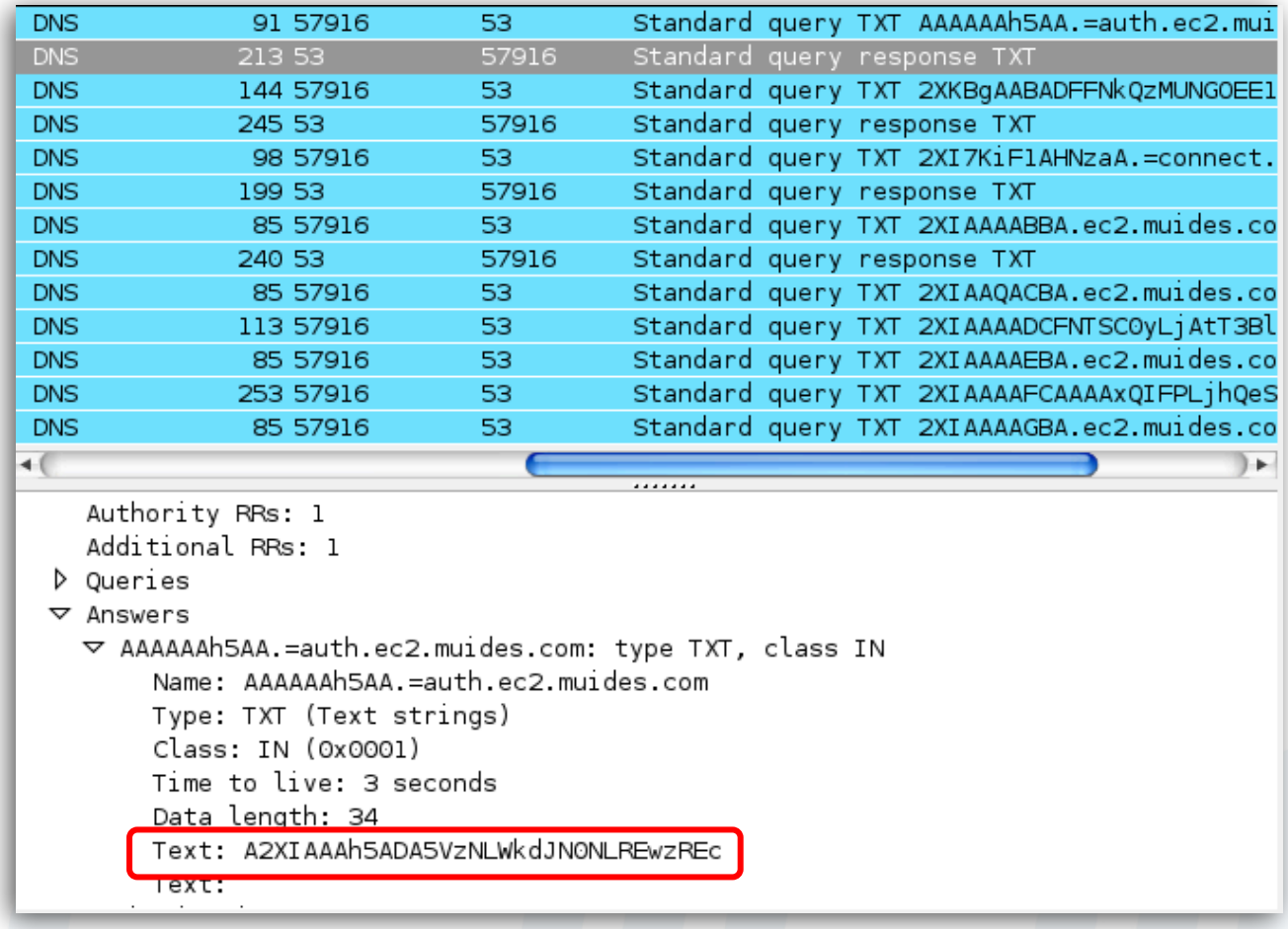
**tcp-over-dns** – мы видим почти в каждой сети этот туннель

Например: Номера кредитных карточек из компании Sony после взлома Sony Playstation Network отправляли внутри DNS запросов

# А видите ли вы туннелирование? Например, внутри трафика 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

# Какие туннели видит продукт?
# И как блокирует?

# Платформа Palo Alto Networks
# Мы работаем для вашей защиты

Обеспечиваем заданную производительность при всех включенных сервисах безопасности

Email офиса в России: Russia@paloaltonetworks.com