ESKA we develop & integrate

ПЛАТФОРМА СЕТЕВОЙ БЕЗОПАСНОСТИ PALO ALTO NETWORKS

ПЛАТФОРМА КИБЕР-БЕЗОПАСНОСТИ НОВОГО ПОКОЛЕНИЯ

Natively integrated	Extensible	Automated

NG ФАЙЕРВОЛ

- App-ID, User-ID, Threats
- Расшифрование SSL/SSH
- Инспекция на L7 всего трафика по всем портам
- Безопасное разрешение приложений
- Отсылает подозрительные неизвестные файлы в облако, passive DNS
- Блокирует угрозы на уровне сети

NG ЗАЩИТА КОНЕЧНЫХ ТОЧЕК TRAPS (ADVANCED ENDPOINT PROTECTION

- Инспекция всех процессов Windows
- Предотвращение известных и неизвестных угроз
- «Легковесный» клиент и облачный сервис

GLOBALPROTECT

- IPsec/SSL VPN, Mobile Security, BYOD

ОБЛАКО БЕЗОПАСНОСТИ

- Десятки тысяч заказчиков
- Сбор подозрительных файлов и DNS-запросов с МЭ и сетевых хостов
- Поведенческий анализ и корреляция угроз, создание сигнатур (IPS, AV, DNS) и обновление репутационной базы URL
- Распространение обновлений на МЭ и клиентское ПО

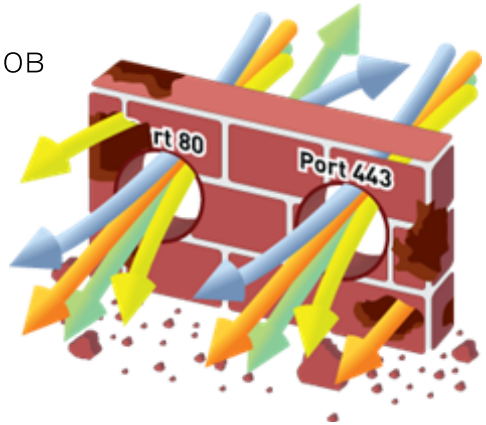
NEXT-GENERATION FIREWALL (NGFW)

СЕТЕВЫЕ ПРИЛОЖЕНИЯ ИЗМЕНИЛИСЬ…

- 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)

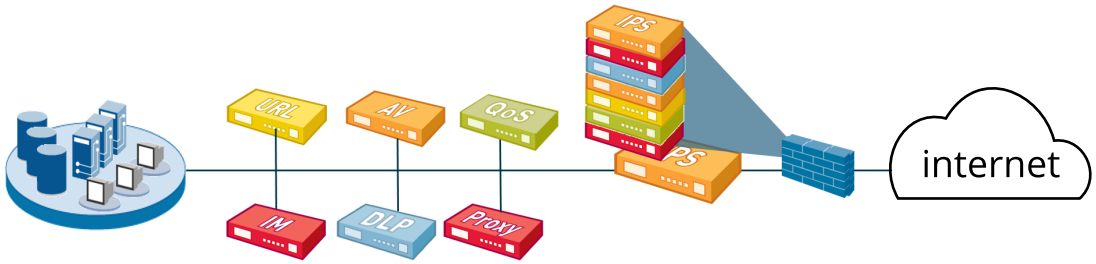
…А ТРАДИЦИОННЫЕ МЕЖСЕТЕВЫЕ ЭКРАНЫ – НЕТ

- Политики межсетевых экранов базируются на контроле:
  - Портов
  - IP-адресов
  - Протоколов



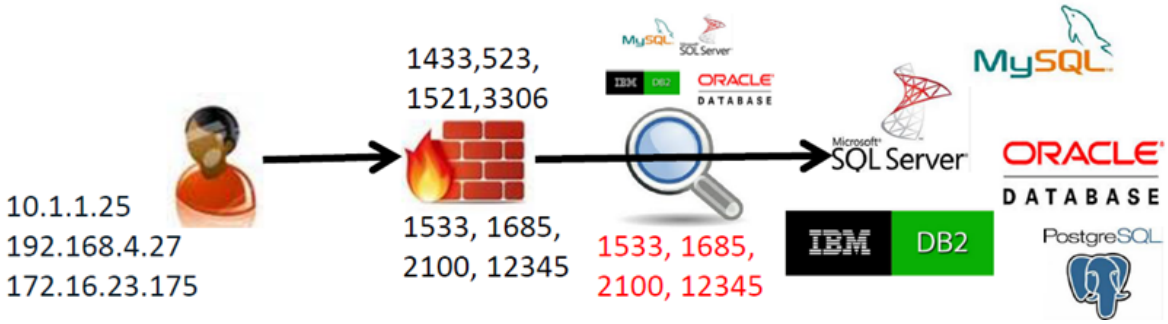
- НО…приложения изменились
- Порты ≠ Приложения
- IP-адреса ≠ Пользователи
- Пакеты ≠ Контент

«ПОМОЩНИКИ» МЕЖСЕТЕВОГО ЭКРАНА НЕ ПОМОГАЮТ



- Сложная топология и нет «прозрачной» интеграции
- «Помощники» межсетевого экрана не имеют полного представления о трафике – нет корреляции
- Дорогое в обслуживании решение
- Использование отдельных функциональных модулей в одном устройстве (UTM) делает его медленным

ПРИМЕР РАЗРЕШЕНИЯ ДОСТУПА АДМИНИСТРАТОРАМ СУБД (МЭ+IPS)



ЛЮБОЙ НОВЫЙ ЭКЗЕМПЛЯР БД ИЛИ ИЗМЕНЕНИЕ В СУЩЕСТВУЮЩЕМ ПОТРЕБУЕТ ПРАВКИ НАСТРОЕК МЭ И IPS.

ШАГ 1

- Определить машины пользователей по IP с резервированием DHCP или поместить в отдельный VLAN (NAC, 802.1x)

ШАГ 2

- Узнать и «открыть» на МЭ все необходимые порты: провести опрос админов, поискать в Интернете стандартные порты, применить политику, проверить «drops», вручную зайти на серверы и проверить открытые порты, исправить политику

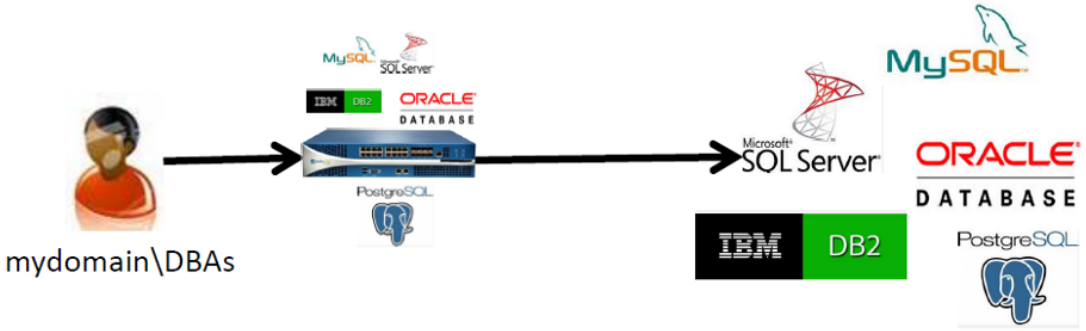
ШАГ 3

- Включить IPS, вручную настроить сигнатуры для нестандартных портов (дублирование настроек)

ШАГ 4

- Надеяться, что ничего не изменится

ПРИМЕР РАЗРЕШЕНИЯ ДОСТУПА АДМИНИСТРАТОРАМ СУБД (NGFW)



STATEFUL INSPECTION FIREWALL + IPS + URL + USERS + APPS ≠ NGFW

ШАГ 1

- Создать единое правило для группы domain\DBAs, разрешающее доступ ко всем СУБД, используя статическую или динамическую группу приложений, с профилем IPS по умолчанию (default/strict). Любые методы аутентификации. Остальные приложения (в том числе неизвестные) блокируются автоматически.

ШАГ 2

- Не требуется! В случае изменения приложения или состава группы администраторов политики будут применяться благодаря App-ID, User-ID, Content-ID

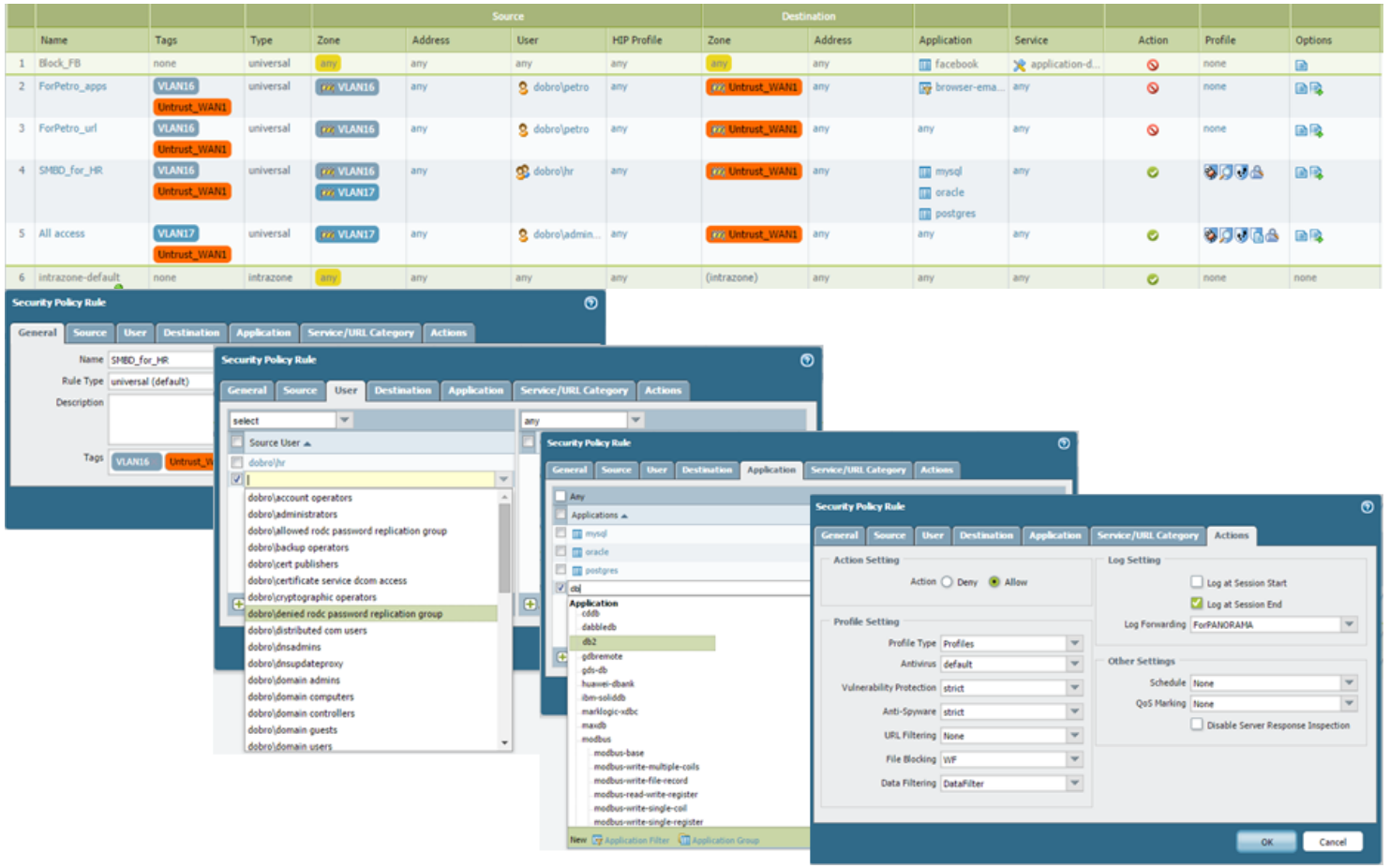
НАСТОЯЩИЙ NGFW: БЕЗОПАСНОЕ РАЗРЕШЕНИЕ ПРИЛОЖЕНИЙ

- Единая политика безопасности
- Идентификация, контроль и безопасное разрешение приложений (App-ID) для каждого пользователя /группы (User-ID)
- Расшифрование входящего/исходящего SSL/SSH
- Обнаружение известных и неизвестных угроз в режиме реального времени (Content-ID)
- Высокая пропускная способность, низкие задержки
- Простота и большое количество вариантов внедрения

НАСТОЯЩИЙ NGFW: БЕЗОПАСНОЕ РАЗРЕШЕНИЕ ПРИЛОЖЕНИЙ

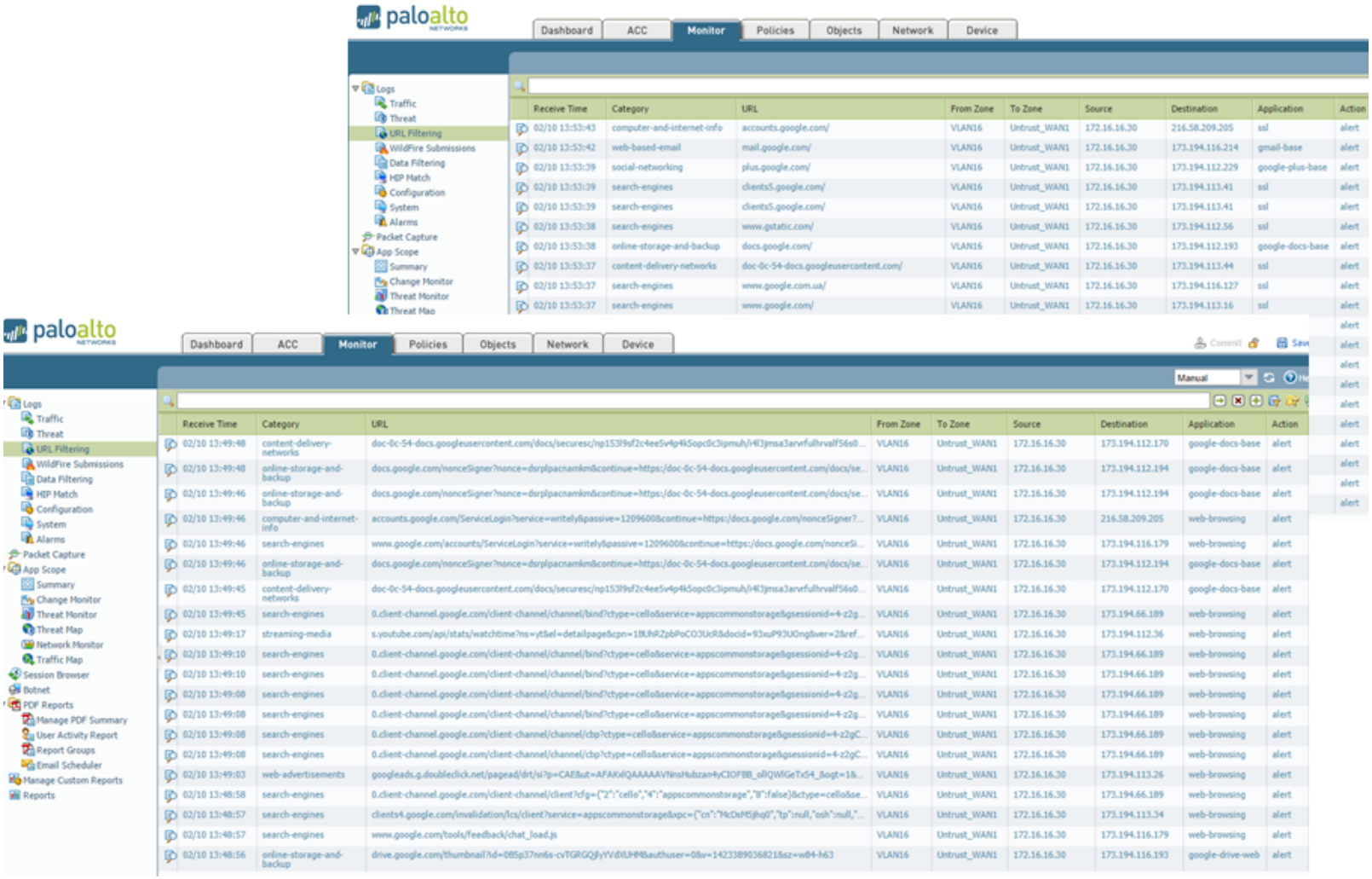
ЕДИНАЯ ПОЛИТИКА БЕЗОПАСНОСТИ

ИДЕНТИФИКАЦИЯ, КОНТРОЛЬ И БЕЗОПАСНОЕ РАЗРЕШЕНИЕ ПРИЛОЖЕНИЙ (APP-ID) ДЛЯ КАЖДОГО ПОЛЬЗОВАТЕЛЯ /ГРУППЫ (USER-ID)



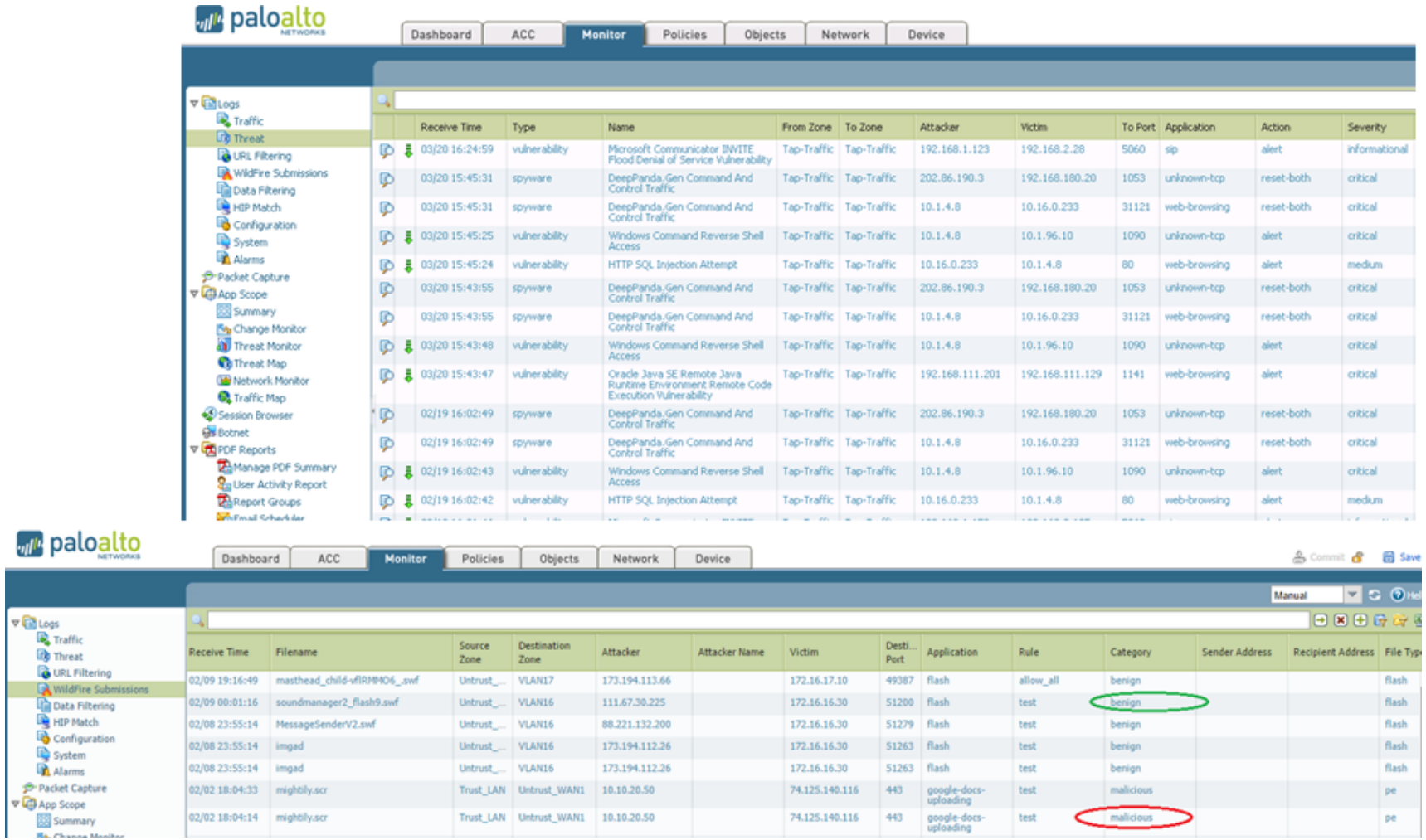
НАСТОЯЩИЙ NGFW: БЕЗОПАСНОЕ РАЗРЕШЕНИЕ ПРИЛОЖЕНИЙ

РАСШИФРОВАНИЕ ВХОДЯЩЕГО/ИСХОДЯЩЕГО SSL/SSH



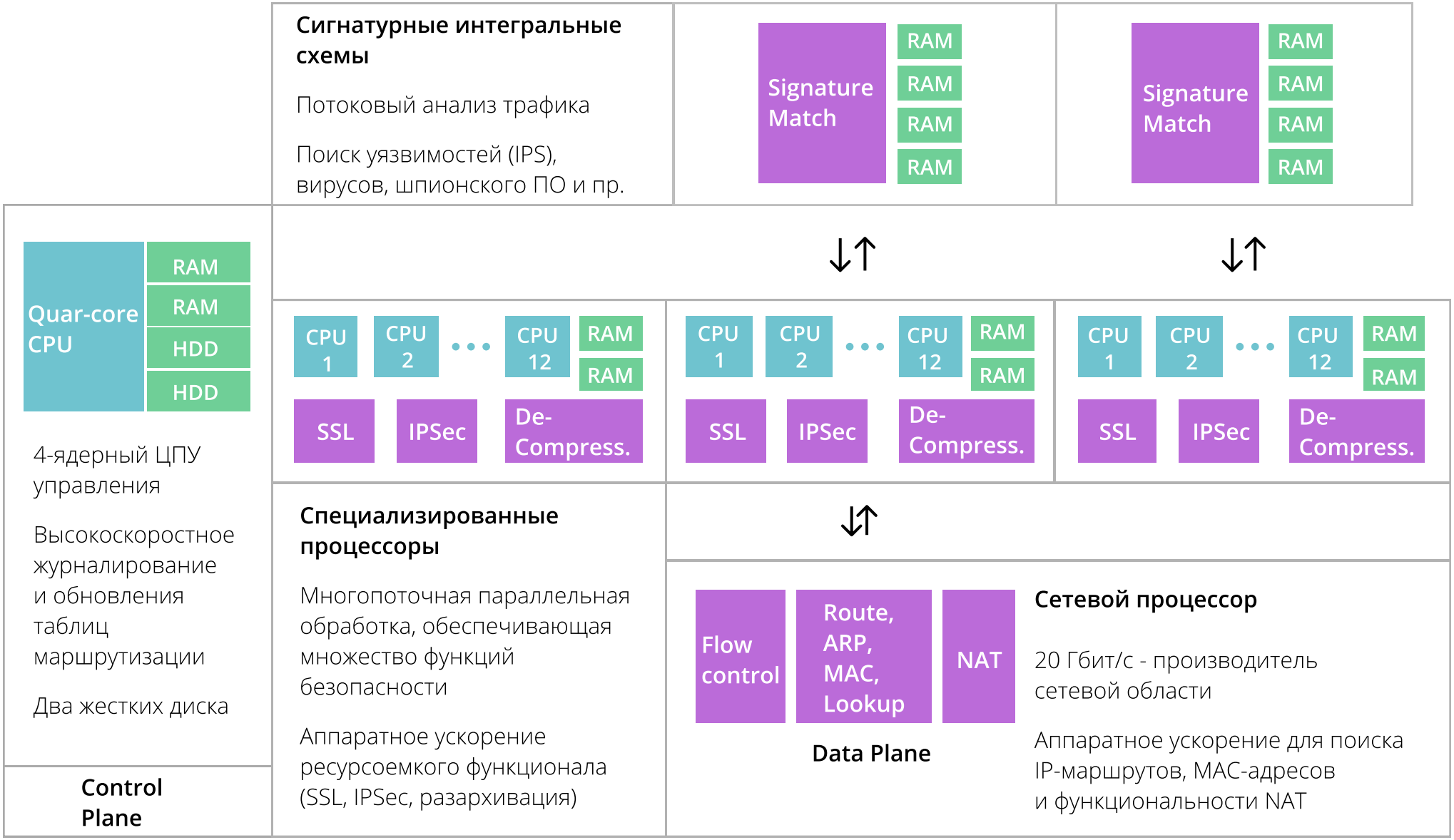
НАСТОЯЩИЙ NGFW: БЕЗОПАСНОЕ РАЗРЕШЕНИЕ ПРИЛОЖЕНИЙ

ОБНАРУЖЕНИЕ ИЗВЕСТНЫХ И НЕИЗВЕСТНЫХ УГРОЗ



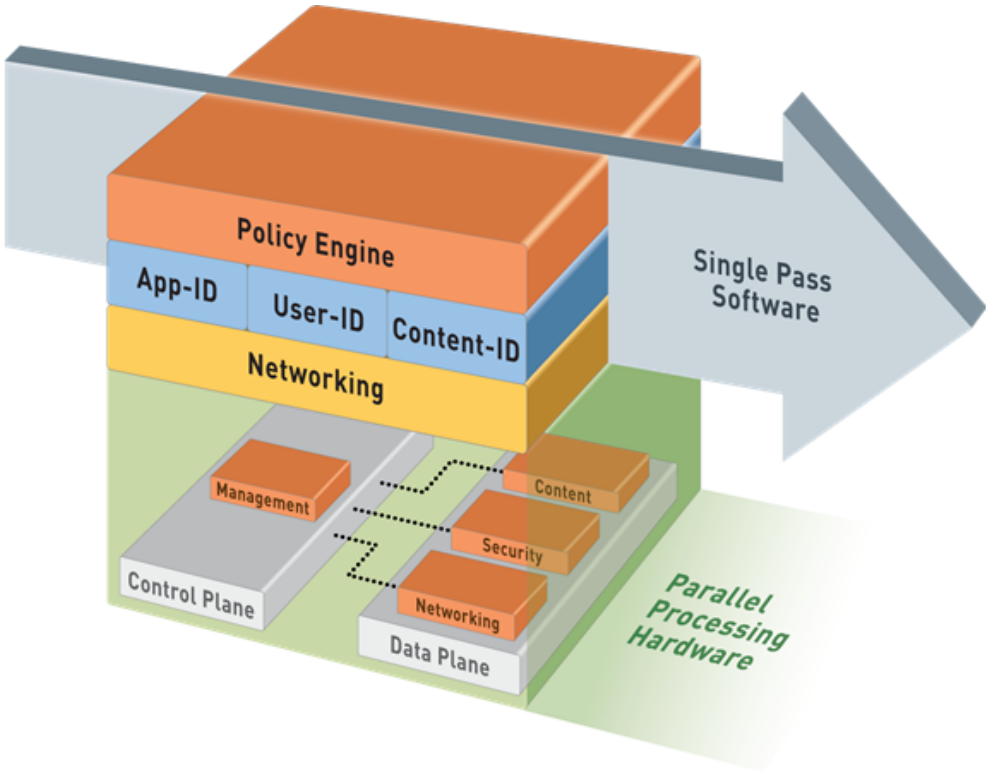
НАСТОЯЩИЙ NGFW: БЕЗОПАСНОЕ РАЗРЕШЕНИЕ ПРИЛОЖЕНИЙ

АРХИТЕКТУРА МЕЖСЕТЕВОГО ЭКРАНА НОВОГО ПОКОЛЕНИЯ PALO ALTO NETWORKS



НАСТОЯЩИЙ NGFW: БЕЗОПАСНОЕ РАЗРЕШЕНИЕ ПРИЛОЖЕНИЙ

АРХИТЕКТУРА ОДНОПРОХОДНОЙ ПАРАЛЛЕЛЬНОЙ ОБРАБОТКИ



Один проход

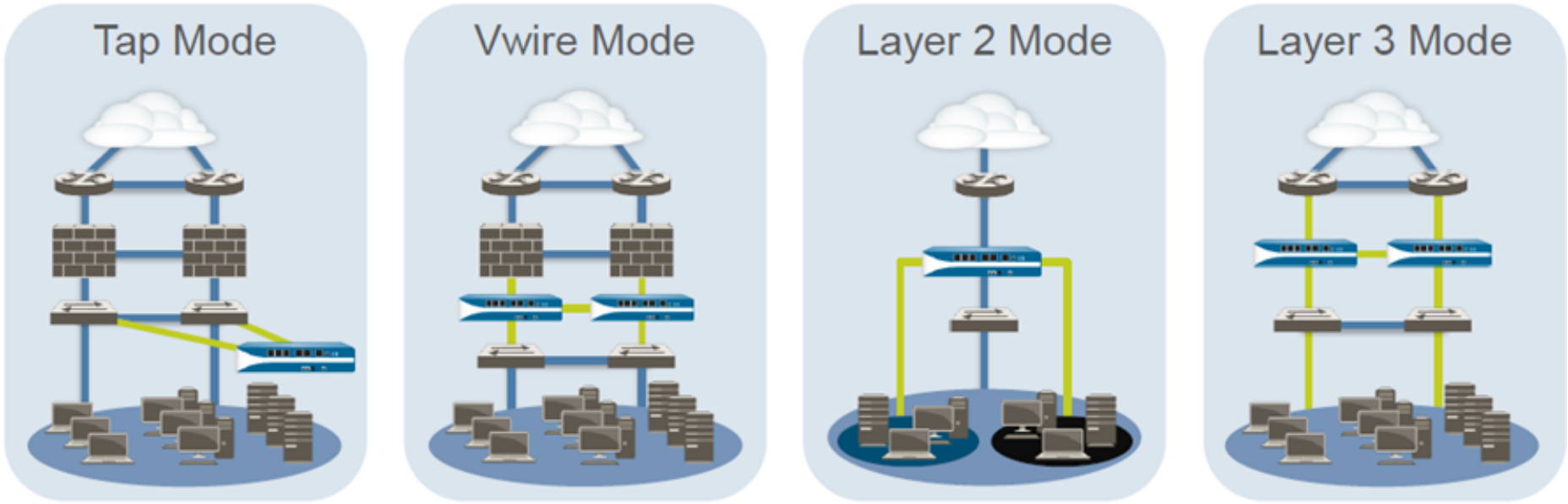
- Каждый пакет сканируется только один раз
- При сканировании одновременно определяется:
  - Приложение
  - Пользователь/группа
  - Контент – угрозы, URL и т.д.

Параллельная обработка

- Специализированное аппаратное обеспечение для каждой задачи
- Разделение Data plane и Control plane

НАСТОЯЩИЙ NGFW: БЕЗОПАСНОЕ РАЗРЕШЕНИЕ ПРИЛОЖЕНИЙ

ИНТЕГРАЦИЯ С СУЩЕСТВУЮЩЕЙ ИНФРАСТРУКТУРОЙ

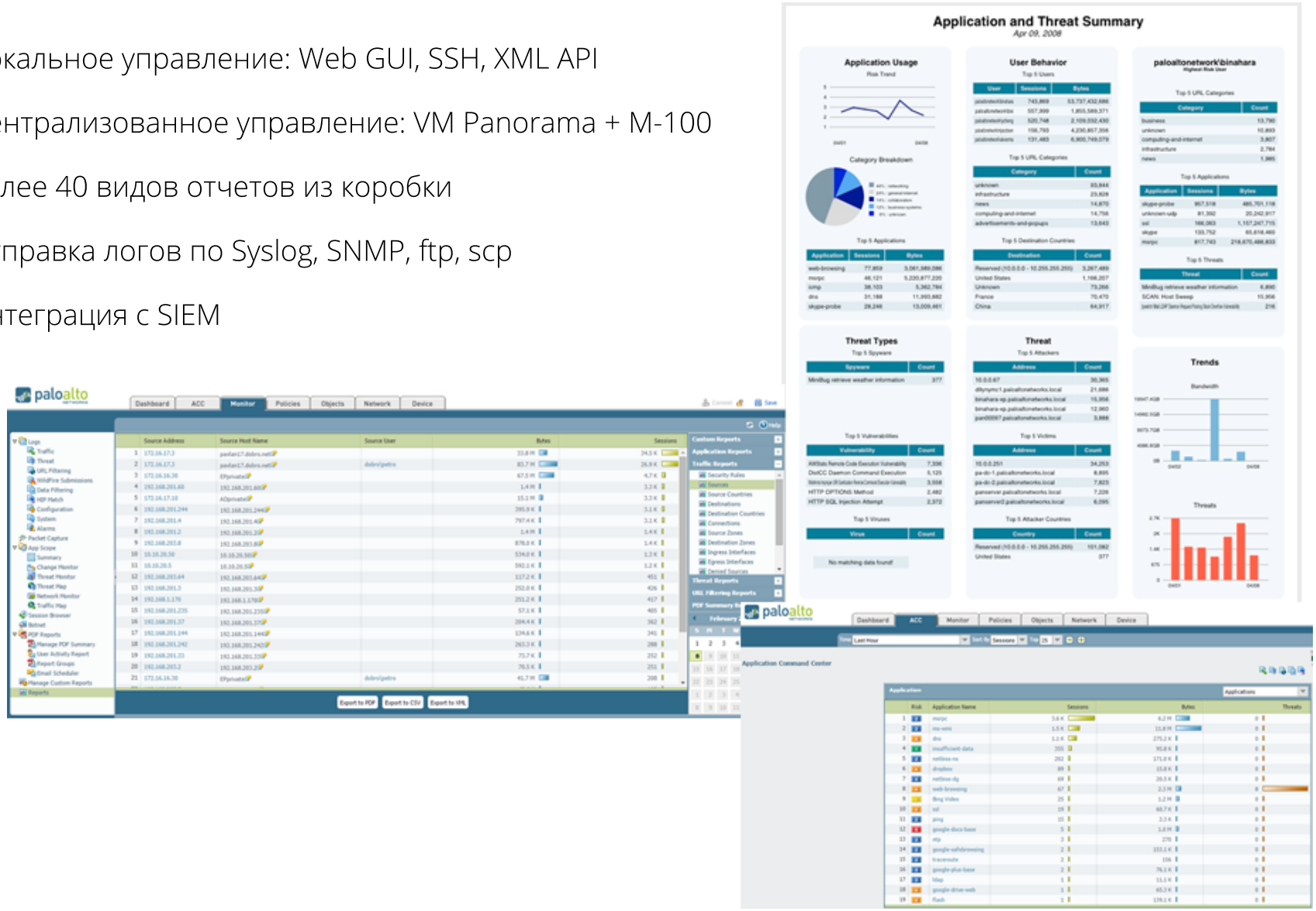


- Анализ SPAN для аудита приложений и обнаружения угроз
- Прозрачное подключение без изменения настроек сети и адресации (L1)
- Обеспечение защиты и коммутации сегментов сети на L2-уровне
- Обеспечение защиты и маршрутизации на L3-уровне

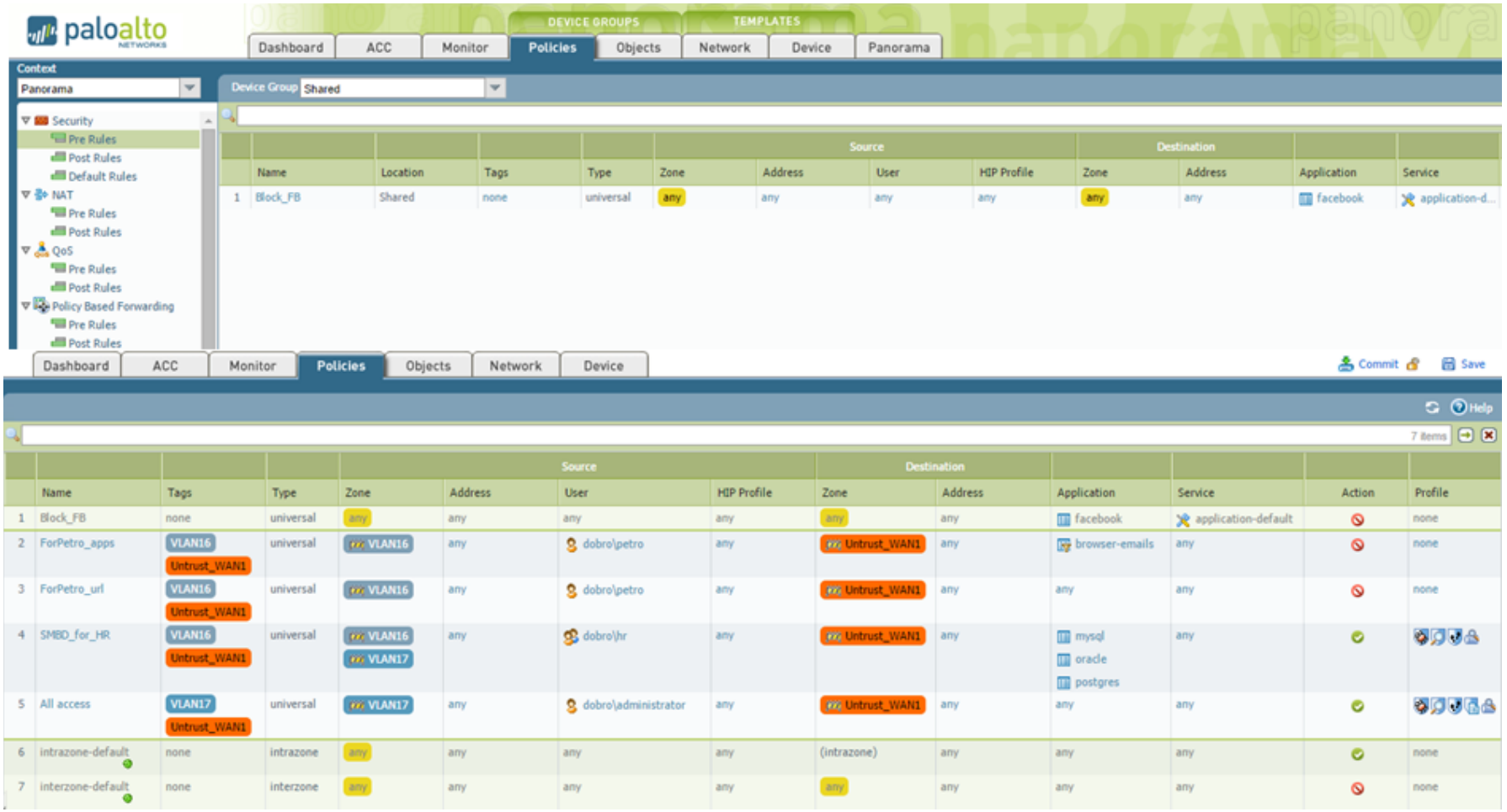
УПРАВЛЕНИЕ И ОТЧЕТНОСТЬ NGFW

СРЕДСТВА УПРАВЛЕНИЯ, ОТЧЕТНОСТИ И ИНТЕГРАЦИИ

- Локальное управление: Web GUI, SSH, XML API
- Централизованное управление: VM Panorama + M-100
- Более 40 видов отчетов из коробки
- Отправка логов по Syslog, SNMP, ftp, scp
- Интеграция с SIEM



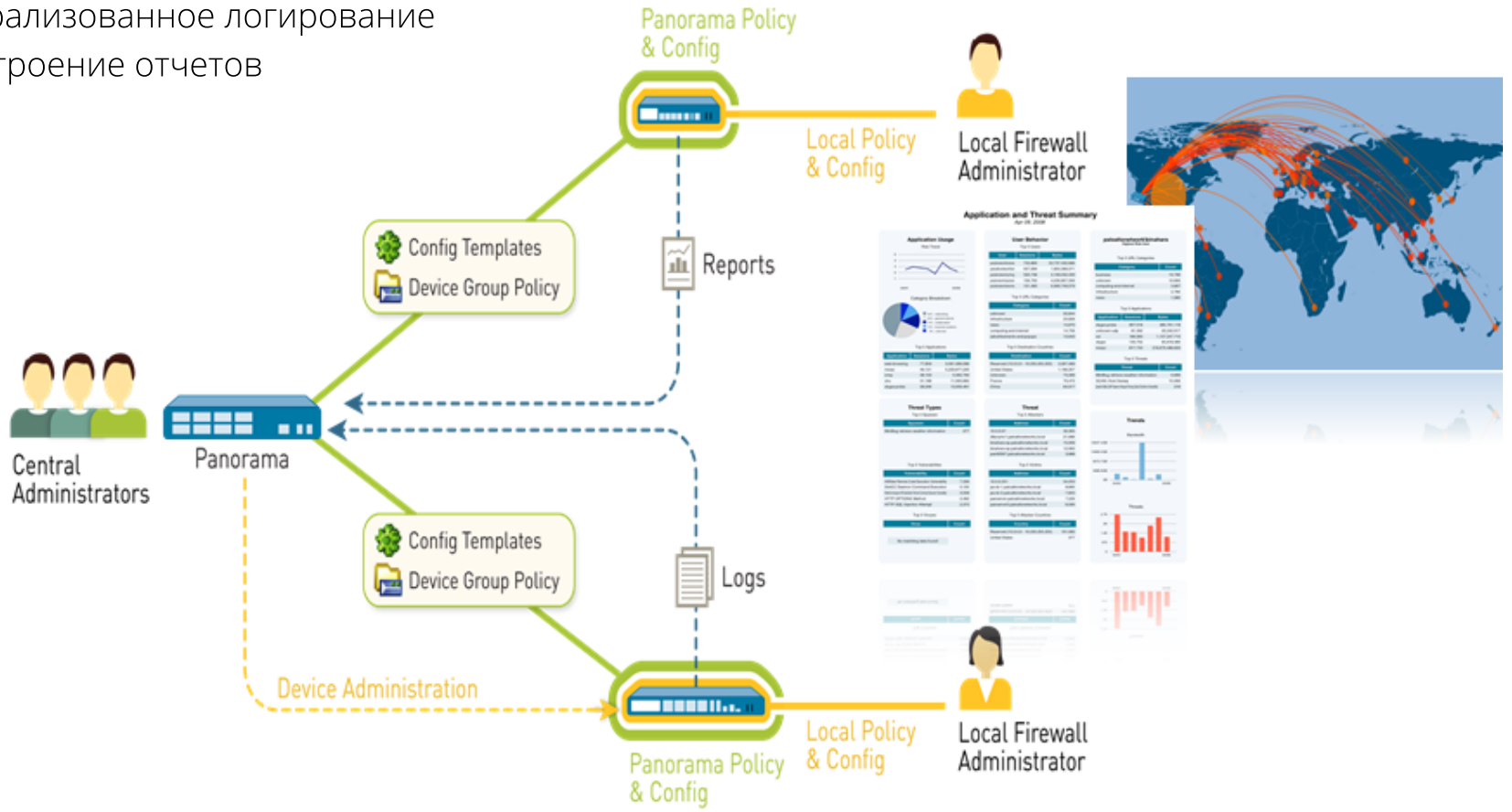
NGFW ПОД УПРАВЛЕНИЕМ PANORAMA



ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ С ИСПОЛЬЗОВАНИЕМ ПО PANORAMA

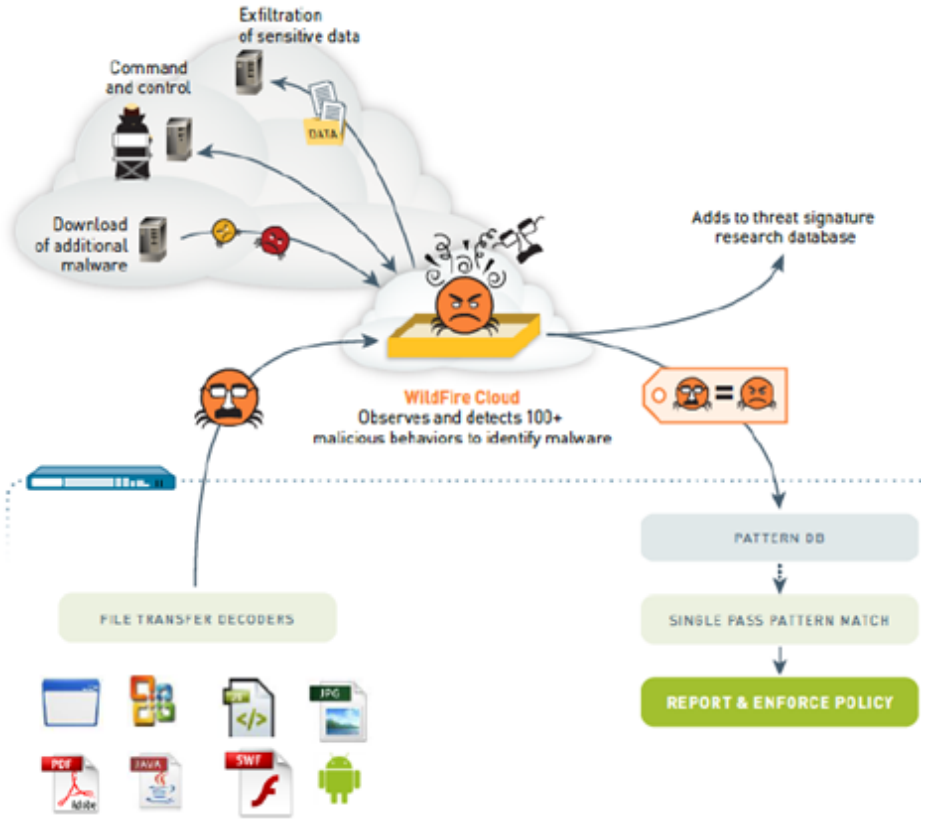
(ПРОДОЛЖЕНИЕ)

- Централизованное логирование и построение отчетов



ОБЛАКО БЕЗОПАСНОСТИ (WILDFIRE)

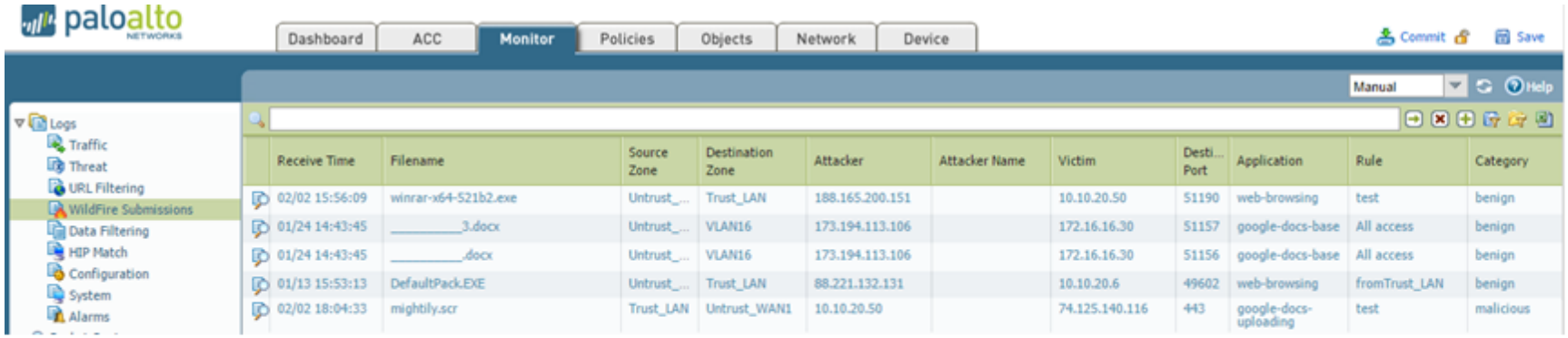
КАК РАБОТАЕТ СЕРВИС WILDFIRE



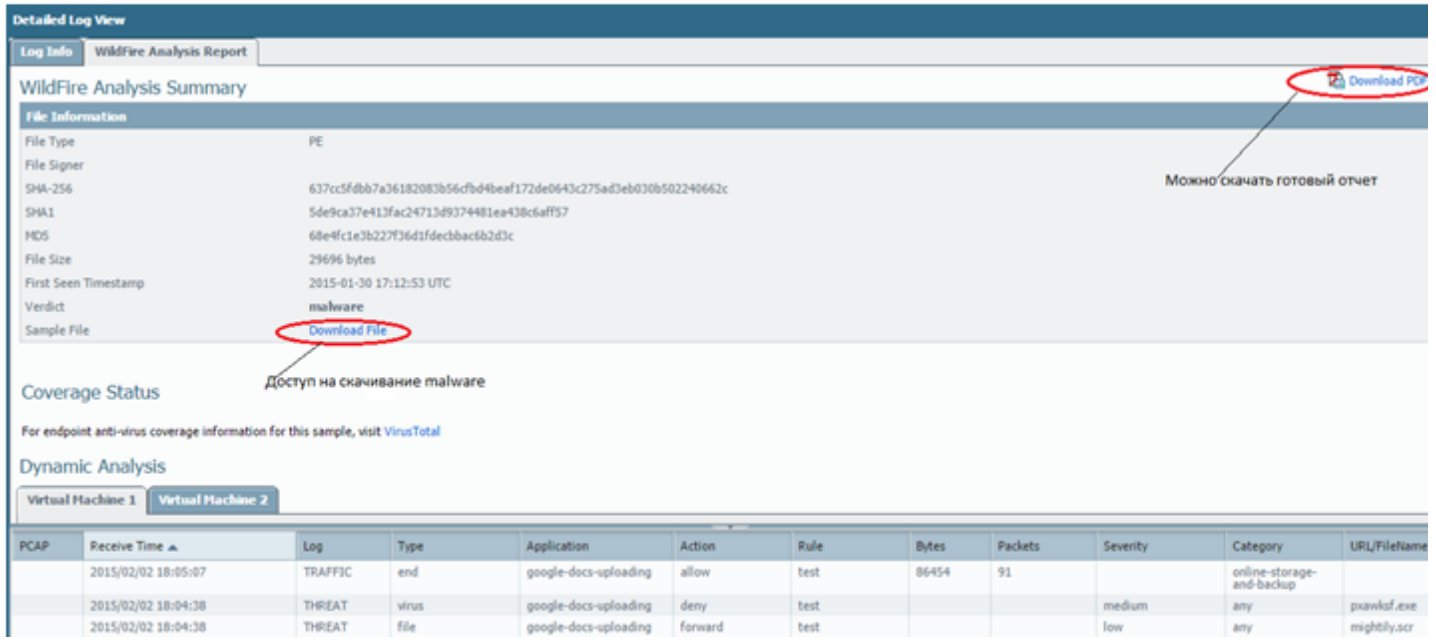
- 80% новых вирусов неизвестны ни одному AV согласно VirusTotal
- 50% остаются неизвестными спустя неделю!

- «Песочница» в публичном/частном облаке (WF-500)
- Анализируется 130+ типов поведения Защита от обнаружения «песочницы» (собственный гипервизор и образы VM, honeypots, эмуляция активности пользователя)
- Безопасный доступ в Интернет из «песочницы» (плюс Tor)
- 40% новых экземпляров – это вариации одних и тех же вредоносов
- Сигнатура и обновление базы AV автоматически создается и загружается на все устройства течении 15 мин.
- 1 сигнатура покрывает до 1500+ уникальных хэшей SHA
- WF-500 проверяет 4500 уникальных файлов в день: исполняемые, офисные, PDF

ДЕМОНСТРАЦИЯ РАБОТЫ WILDFIRE

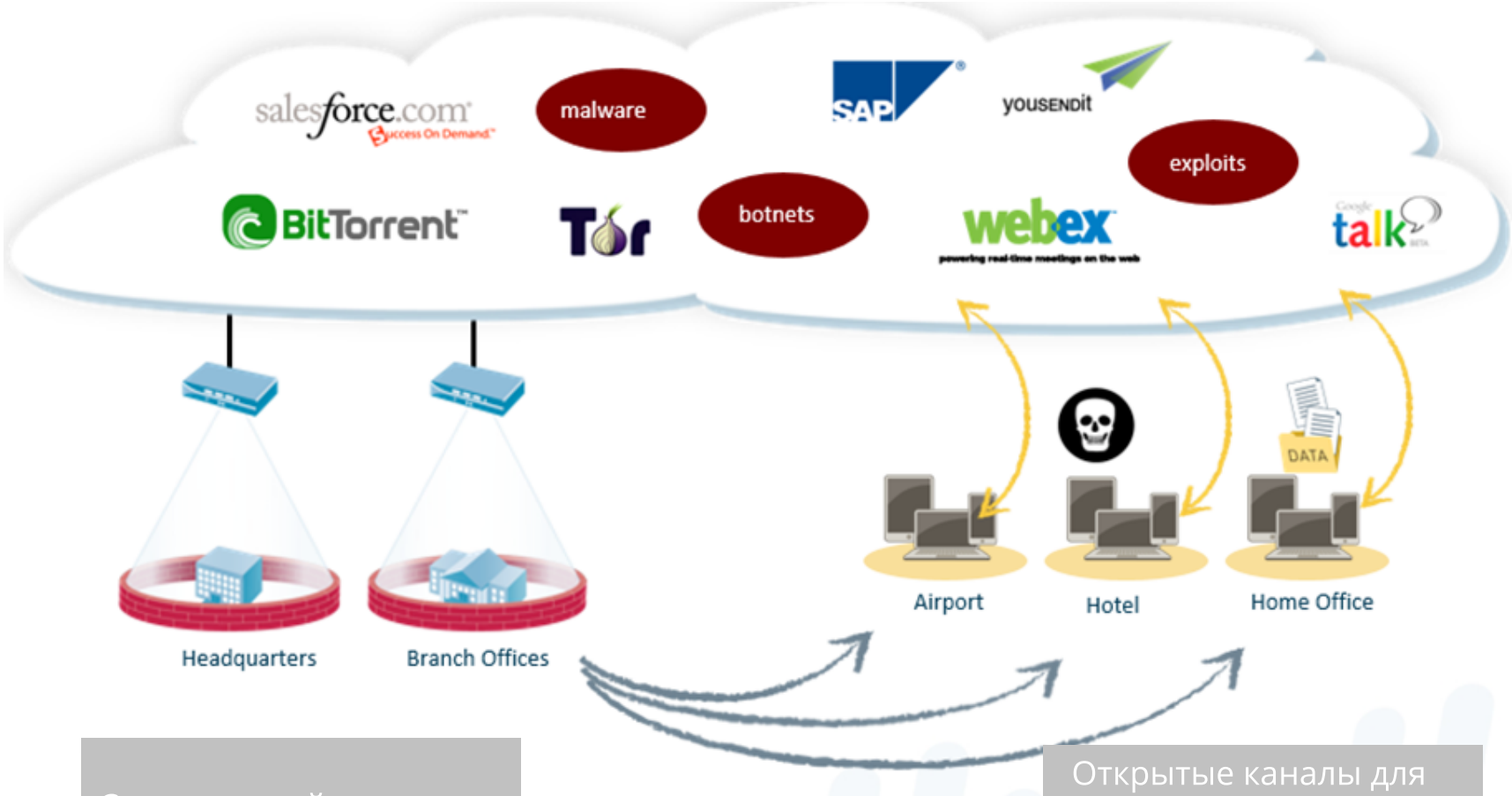


Отчет
по работе
WildFire



GLOBAL PROTECT

СОВРЕМЕННАЯ КАРТИНА БЕЗОПАСНОСТИ В ЗАВИСИМОСТИ ОТ МЕСТА НАХОЖДЕНИЯ РАБОЧЕЙ СТАНЦИИ

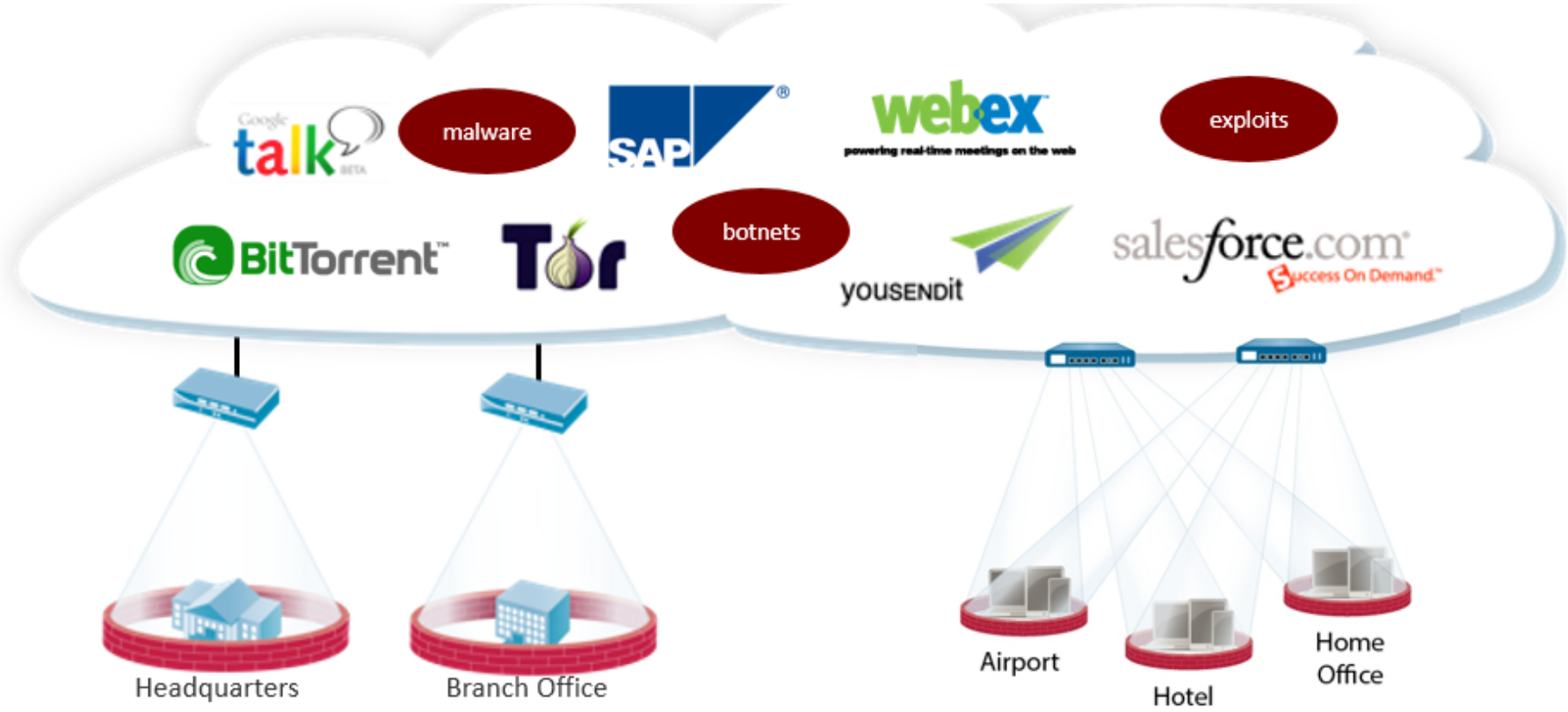


Защищенный периметр

Открытые каналы для распространения угроз и утечек данные

ЧТО МОЖНО ИЗМЕНИТЬ ЕСЛИ ЕСТЬ GLOBAL PROTECT ?

ПОЛНАЯ БЕЗОПАСНОСТЬ И КОНТРОЛЬ УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ

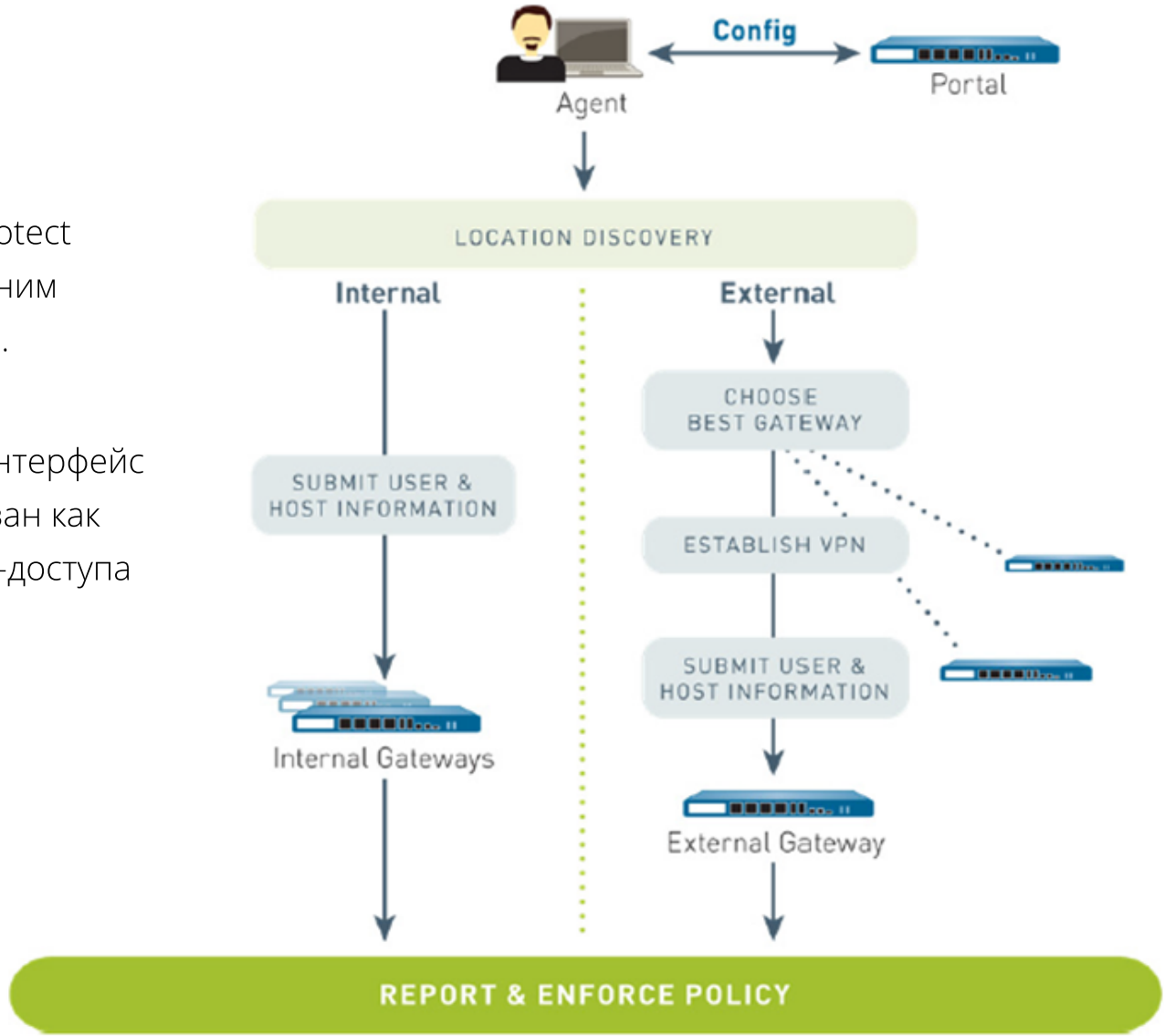


- VPN–соединение к соответственно настроенному файрволу который выполняет всю работу по обеспечении безопасности
- Автоматическое защищенное соединение для внутренних и внешних пользователей
- Единая политика контроля, гарантированная прозрачность трафика и встроенная отчетность

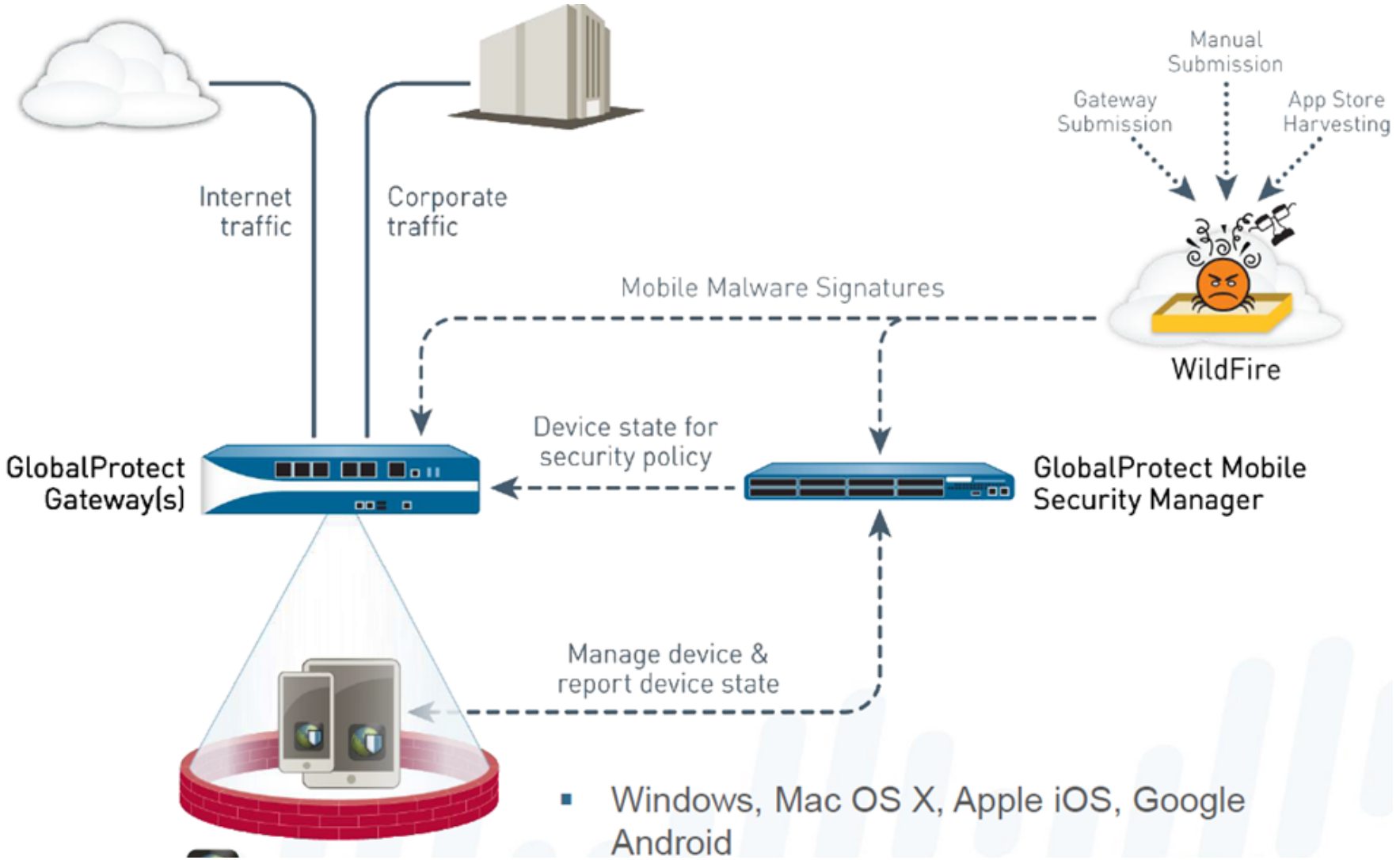
КАК РАБОТАЕТ GLOBAL PROTECT?

Internal Gateway – внутренний интерфейс Palo Alto NGFW, сконфигурирован как Global Protect Gateway для доступа к внутренним ресурсам, подлежащим защите.

External Gateway – внешний интерфейс Palo Alto NGFW, сконфигурирован как Global Protect Gateway для VPN-доступа удаленных пользователей



КАК РАБОТАЕТ GLOBAL PROTECT? (ПРОДОЛЖЕНИЕ)




paloalto
NETWORKS
the network security company™