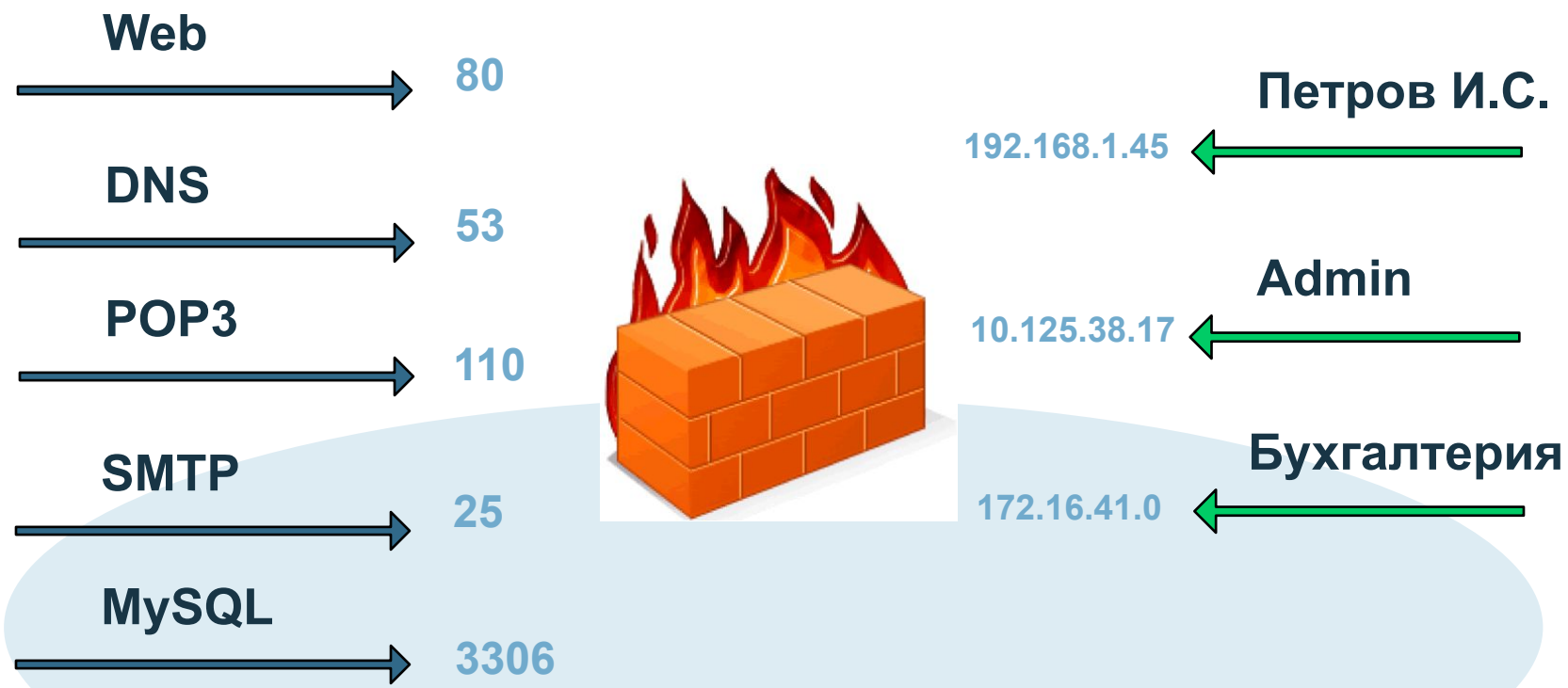
Palo Alto Networks

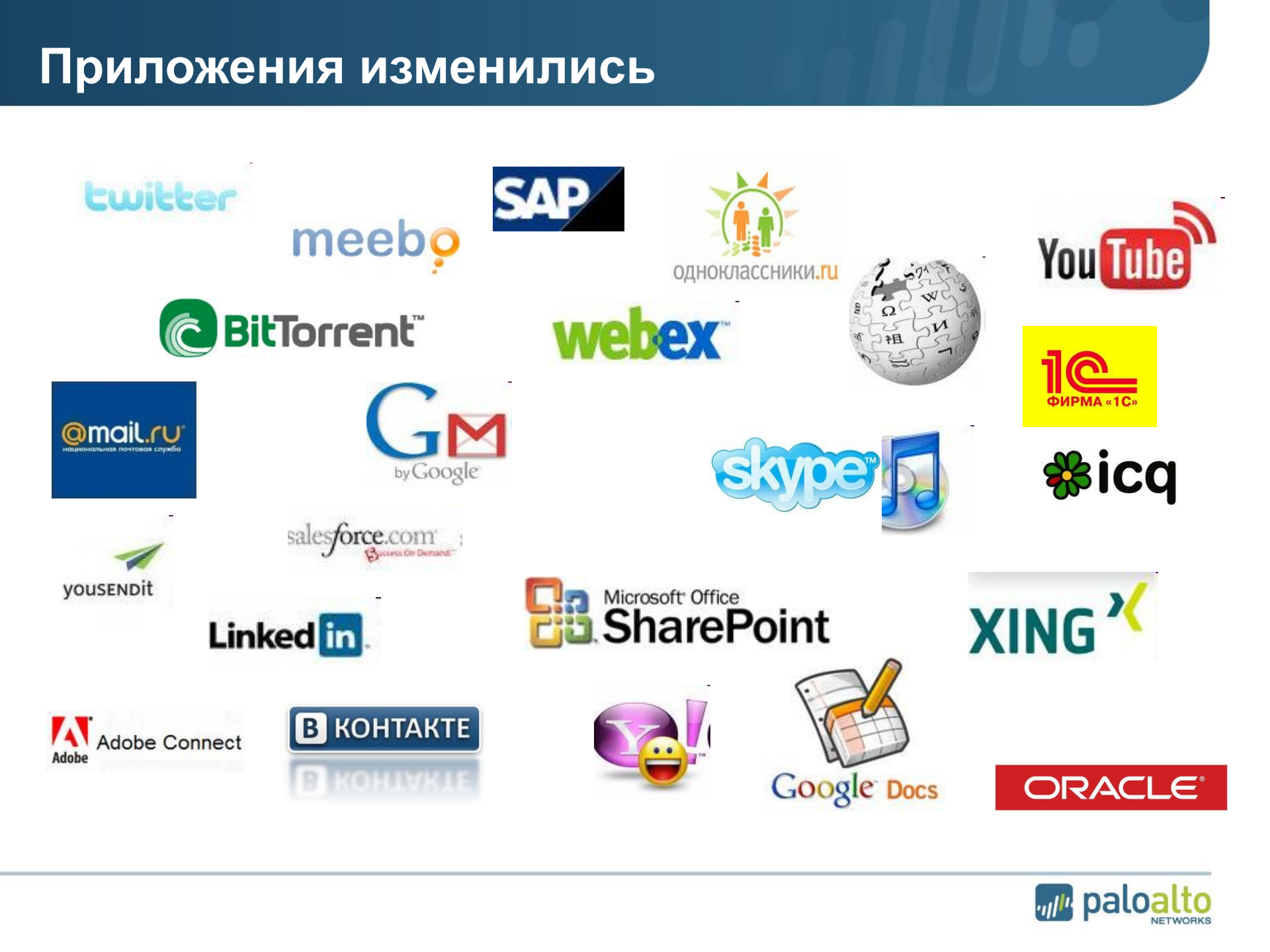
Межсетевые экраны нового поколения

- ✔ Тенденции развития современных сетевых приложений
- ✔ Современные требования к межсетевым экранам
- ✔ Межсетевые экраны нового поколения
- ✔ Уникальные технологии Palo Alto
- ✔ Межсетевые экраны Palo Alto

Межсетевые экраны



Приложения изменились

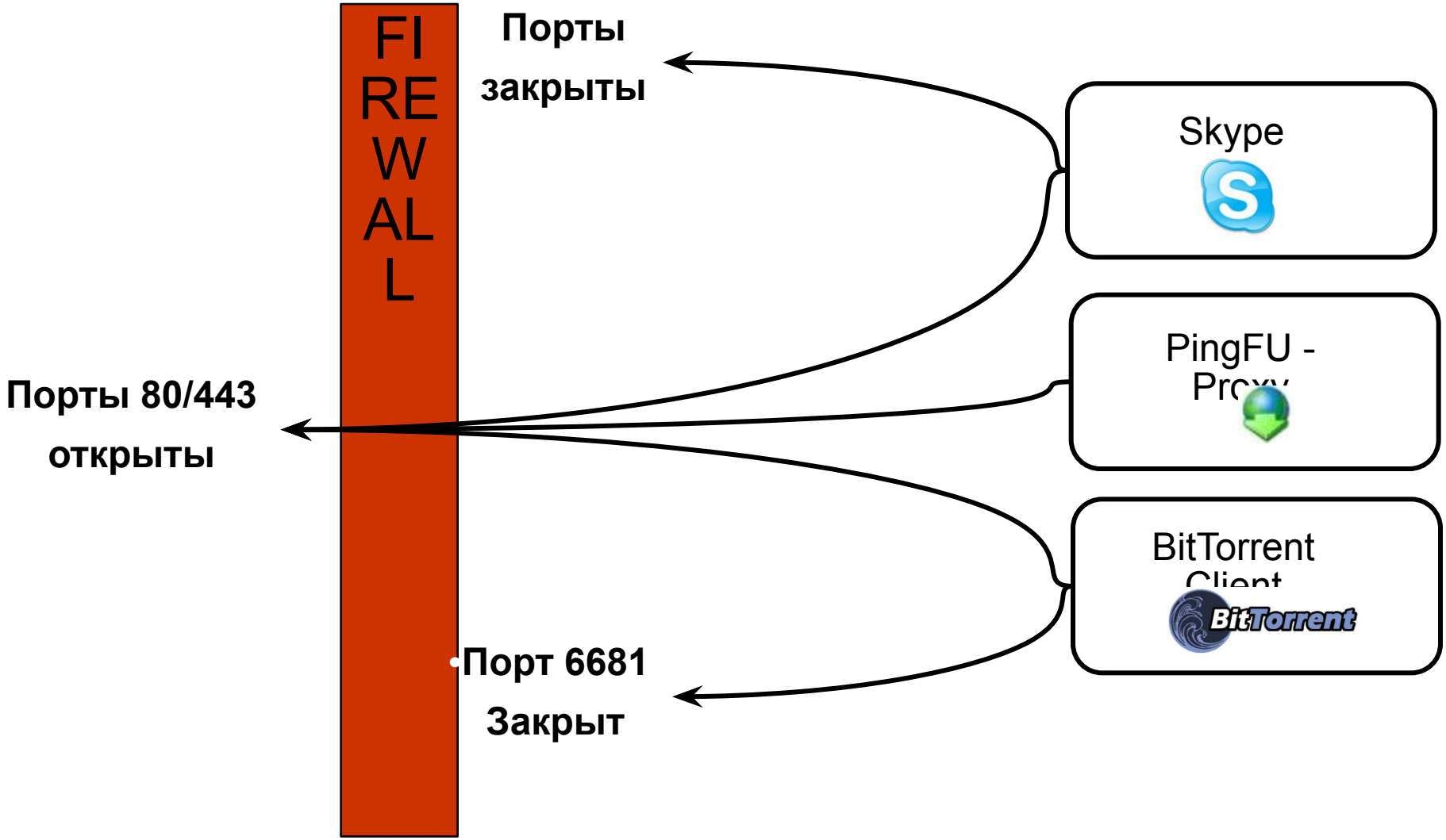


TCP 80: бизнес приложения

TCP 80: другие приложения

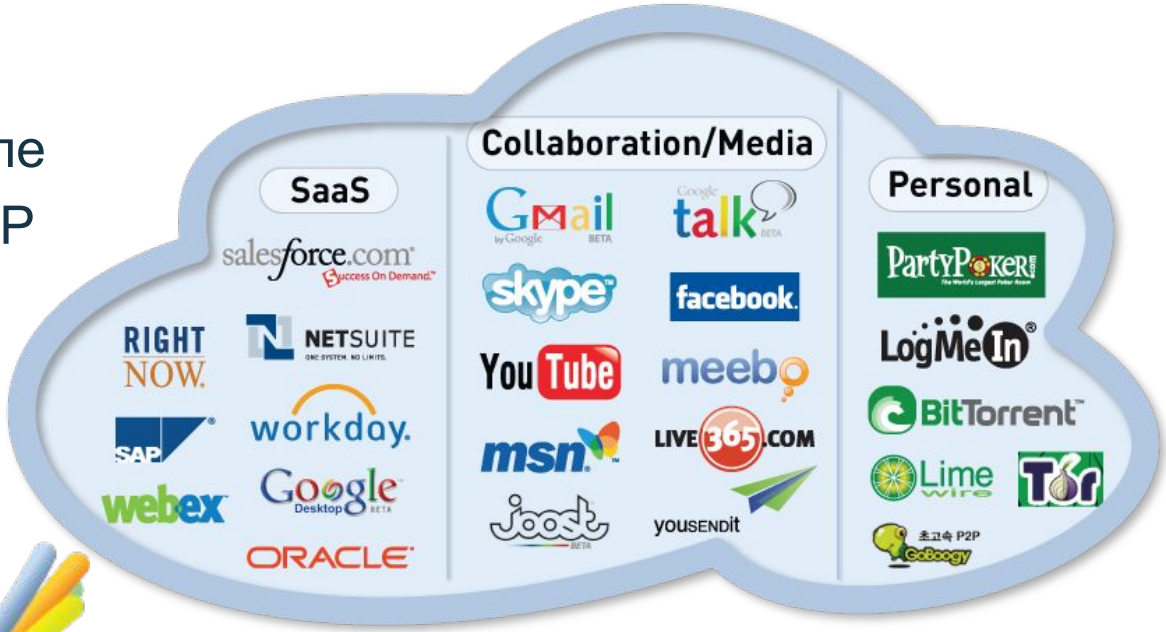
Тактика обхода систем безопасности

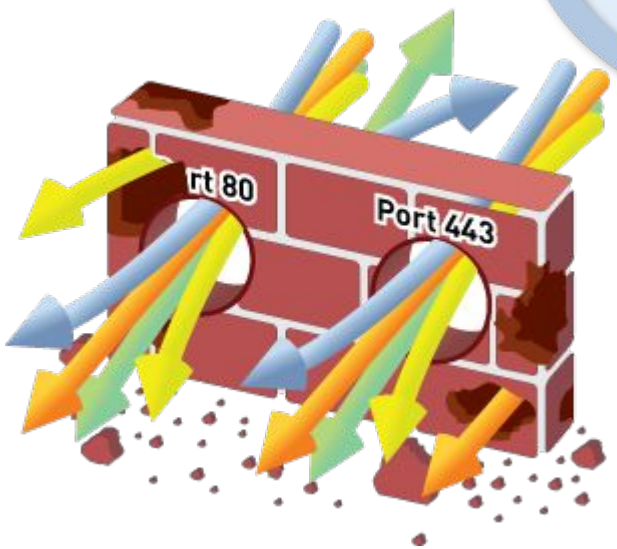
Тактика обхода систем безопасности. Пример



Вывод:
Приложения изменились, а файерволы - нет

Политики файерволов базируются на контроле портов, протоколов и IP адресов…

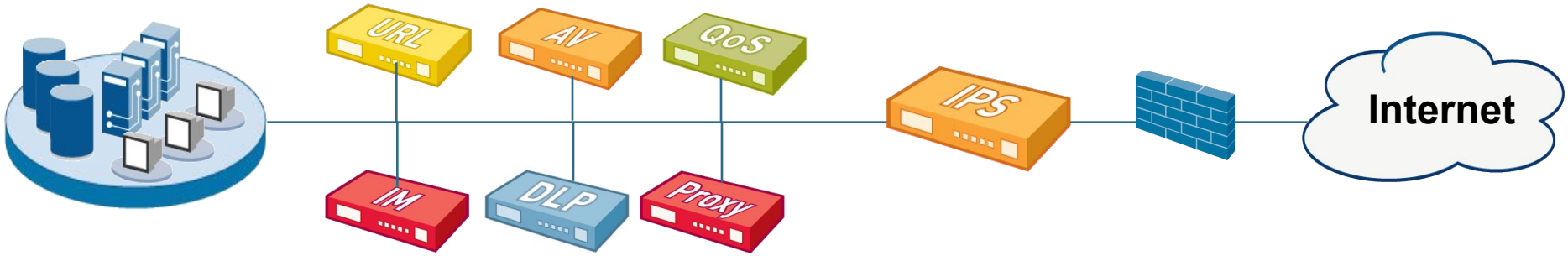




… а должны контролировать приложения, пользователей и передаваемые данные

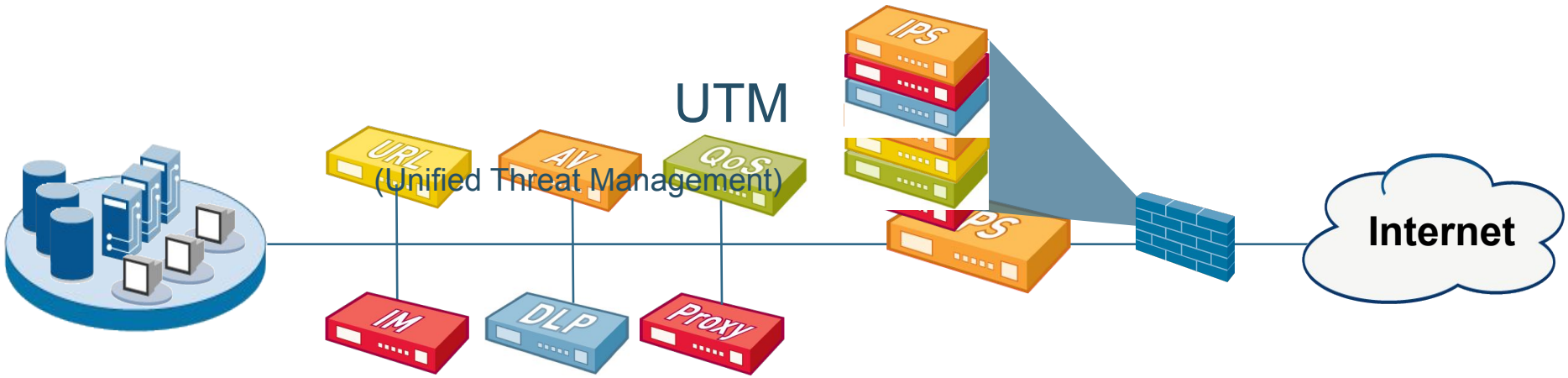
Файервол должен восстановить контроль над сетью

«Помощники» файервола не помогают!



- Увеличивается сложность и стоимость
- Производительность ухудшается
- Сеть так и не становится прозрачной и контролируемой

«Помощники» файервола не помогают!



- Увеличивается сложность и стоимость
- Производительность ухудшается
- Сеть так и не становится прозрачной и контролируемой

Что должен уметь файервол нового поколения?

Gartner: Требования к файерволу нового поколения

- ✔ **Контроль на уровне приложений**

  Должна быть возможность запретить приложение (вне зависимости от порта)

- ✔ **Полностью интегрированные**

  Дополнительные функции не должны влиять на производительность

- ✔ **Функции для определения пользователей**

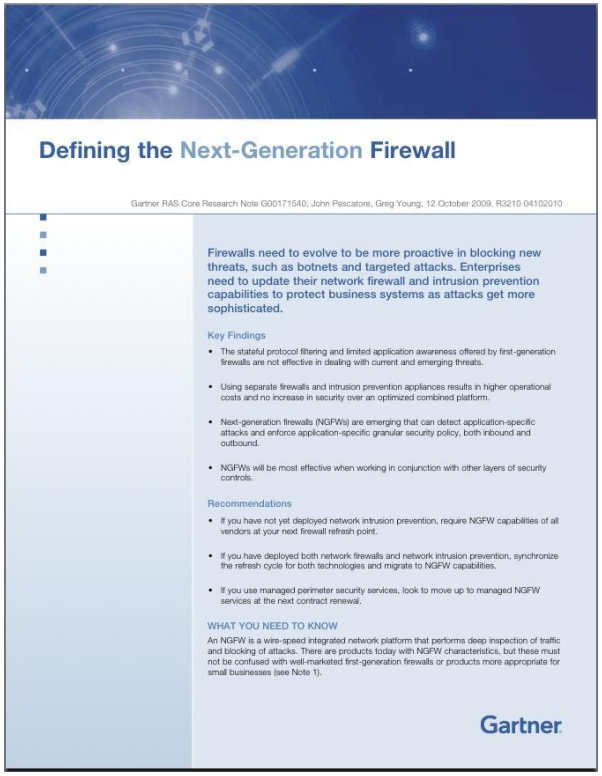
  Интеграция со службами каталогов (Active Directory и т.д.)

- ✔ **Функции обычных файерволов**

  Фильтрация пакетов, NAT, динамическая маршрутизация и т.д..

- ✔ **Должен легко устанавливаться в сеть**

  Легкая прозрачная установка в работающую сеть



Defining the Next-Generation Firewall

Gartner RAS Core Research Note G00171540, John Pescatore, Greg Young, 12 October 2009, R3210 04102010

Firewalls need to evolve to be more proactive in blocking new threats, such as botnets and targeted attacks. Enterprises need to update their network firewall and intrusion prevention capabilities to protect business systems as attacks get more sophisticated.

Key Findings

- The stateful protocol filtering and limited application awareness offered by first-generation firewalls are not effective in dealing with current and emerging threats.
- Using separate firewalls and intrusion prevention appliances results in higher operational costs and no increase in security over an optimized combined platform.
- Next-generation firewalls (NGFWs) are emerging that can detect application-specific attacks and enforce application-specific granular security policy, both inbound and outbound.
- NGFWs will be most effective when working in conjunction with other layers of security controls.

Recommendations

- If you have not yet deployed network intrusion prevention, require NGFW capabilities of all vendors at your next firewall refresh point.
- If you have deployed both network firewalls and network intrusion prevention, synchronize the refresh cycle for both technologies and migrate to NGFW capabilities.
- If you use managed perimeter security services, look to move up to managed NGFW services at the next contract renewal.

WHAT YOU NEED TO KNOW

An NGFW is a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks. There are products today with NGFW characteristics, but these must not be confused with well-marketed first-generation firewalls or products more appropriate for small businesses (see Note 1).

Gartner

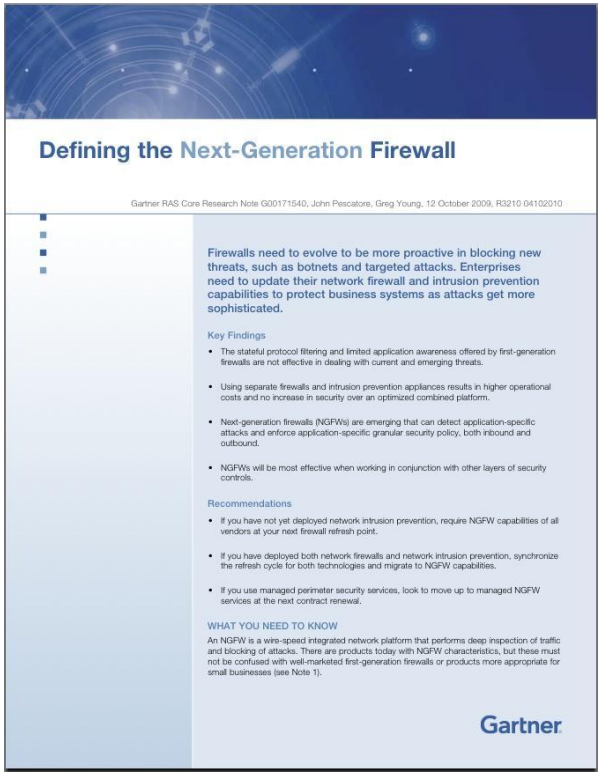
Что должен уметь файервол нового поколения?

Gartner: Не являются файерволами нового поколения:

- ✔ **Устройства UTM (Unified Threat Management)**

  это НЕ файерволы нового поколения

  - ✔ **DLP (Data Leak Prevention) это НЕ файерволы нового поколения**
  - ✔ **Web шлюзы это НЕ файерволы нового поколения**
  - ✔ **E-mail шлюзы это НЕ файерволы нового поколения**



Defining the Next-Generation Firewall

Gartner RAS Core Research Note G00171540, John Pescatore, Greg Young, 12 October 2009, R3210 04102010

Firewalls need to evolve to be more proactive in blocking new threats, such as botnets and targeted attacks. Enterprises need to update their network firewall and intrusion prevention capabilities to protect business systems as attacks get more sophisticated.

Key Findings

- The stateful protocol filtering and limited application awareness offered by first-generation firewalls are not effective in dealing with current and emerging threats.
- Using separate firewalls and intrusion prevention appliances results in higher operational costs and no increase in security over an optimized combined platform.
- Next-generation firewalls (NGFWs) are emerging that can detect application-specific attacks and enforce application-specific granular security policy, both inbound and outbound.
- NGFWs will be most effective when working in conjunction with other layers of security controls.

Recommendations

- If you have not yet deployed network intrusion prevention, require NGFW capabilities of all vendors at your next firewall refresh point.
- If you have deployed both network firewalls and network intrusion prevention, synchronize the refresh cycle for both technologies and migrate to NGFW capabilities.
- If you use managed perimeter security services, look to move up to managed NGFW services at the next contract renewal.

WHAT YOU NEED TO KNOW

An NGFW is a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks. There are products today with NGFW characteristics, but these must not be confused with well-marketed first-generation firewalls or products more appropriate for small businesses (see Note 1).

Gartner

Файервол нового поколения

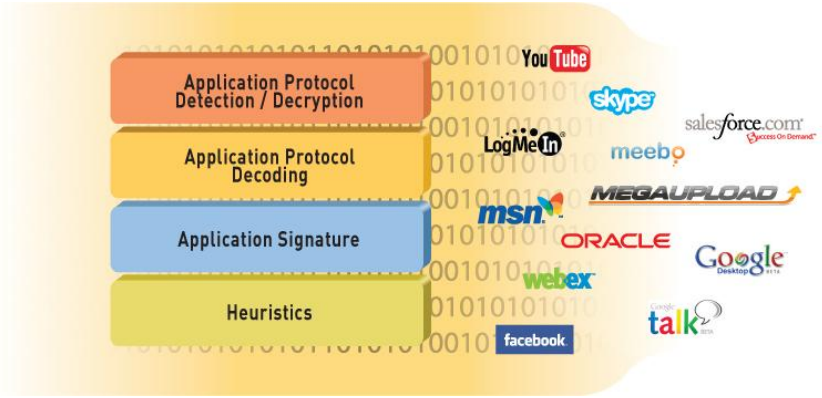
Функции:

1. Определение приложений вне зависимости от порта и шифрования SSL
2. Определение пользователей вне зависимости от IP адреса
3. Применение политик к приложениям и функционалу этих приложений
4. Интегрированная защита от сетевых атак
5. Производительность до 10 Гбит/с

Уникальные технологии изменили файервол

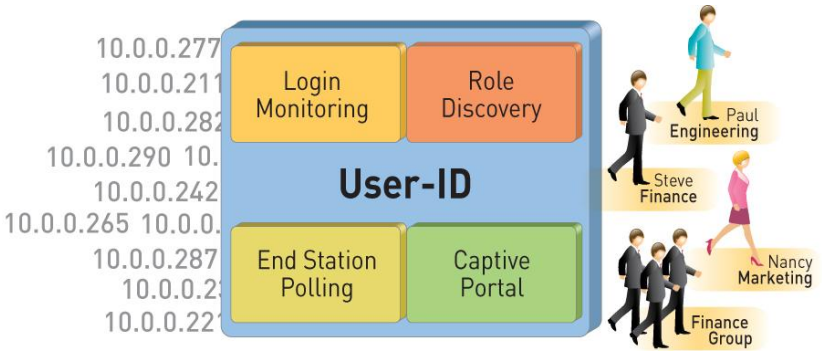
App-ID

Идентификация приложений



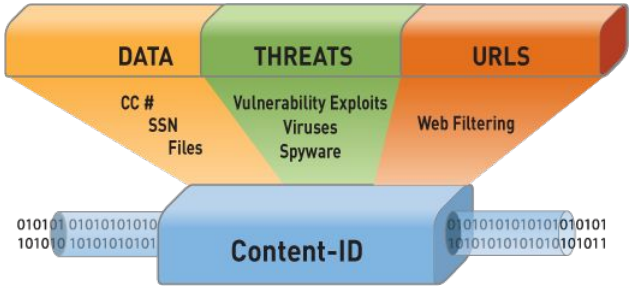
User-ID

Идентификация пользователей

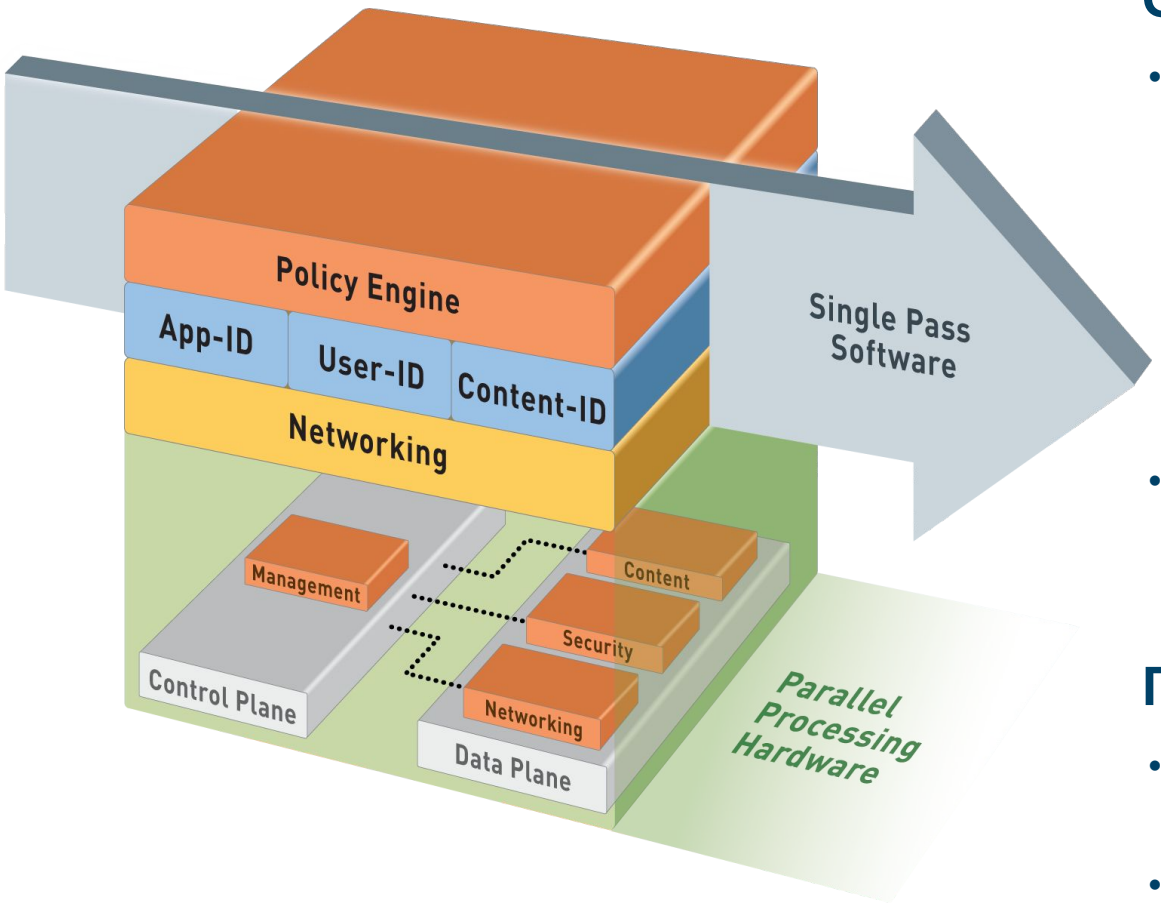


Content-ID

Контроль данных



«Однопроходная» архитектура



Один проход

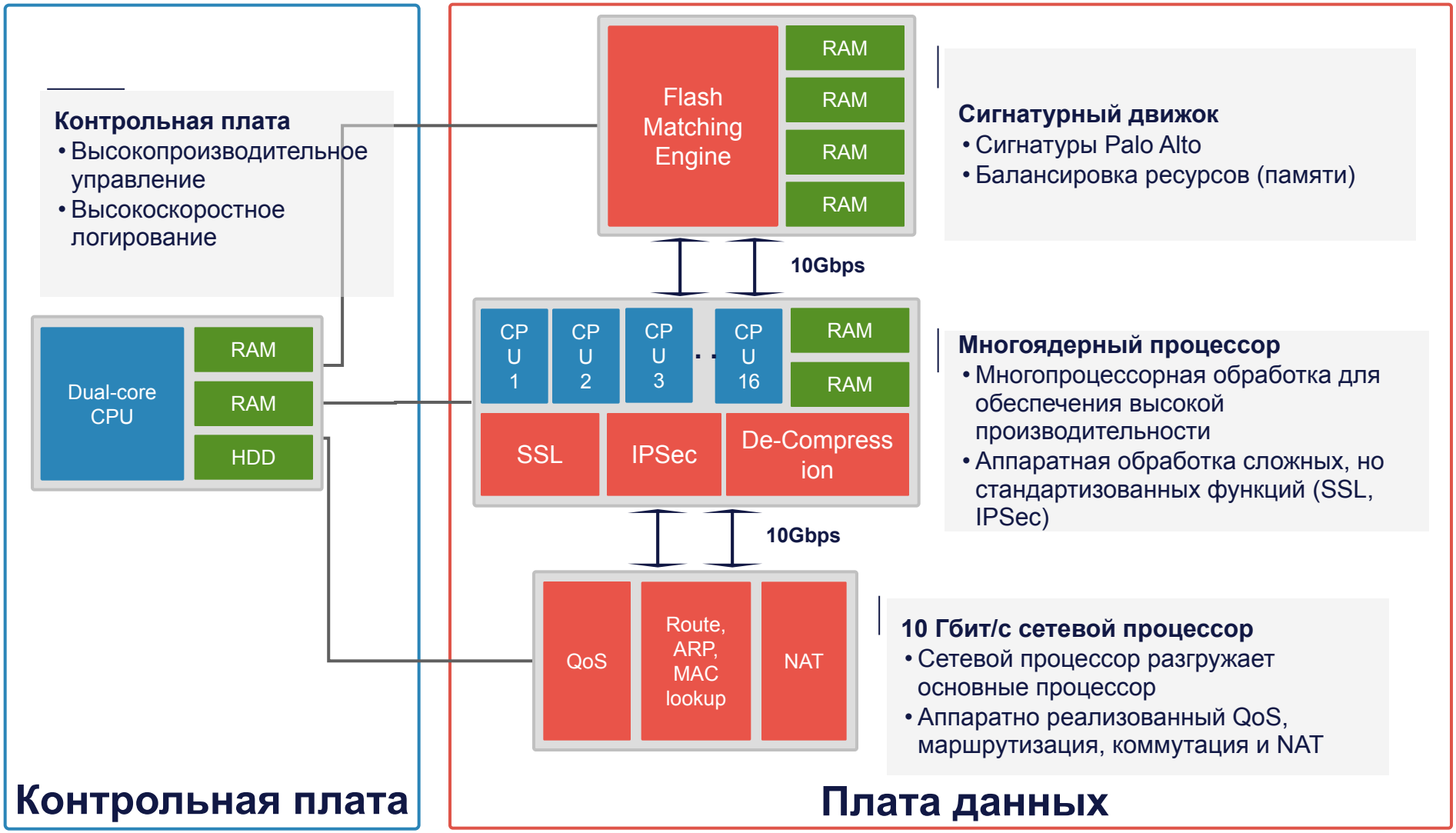
- Одна операция на пакет
  - Классификация трафика (App-ID)
  - Определение пользователей/групп
  - Сканирование данных – угрозы, URLы, конфиденциальные данные
- Единая политика
  - Политика применяется к приложению, IP адресу, пользователю и т.д.

Параллельная обработка

- Специализированное аппаратное обеспечение
- Разделение контрольной платы от платы данных

Производительность до 10 Гбит/с, маленькая задержка

Специализированная архитектура (PA-4000)



Контрольная плата
- Высокопроизводительное управление
- Высокоскоростное логирование

Сигнатурный движок
- Сигнатуры Palo Alto
- Балансировка ресурсов (памяти)

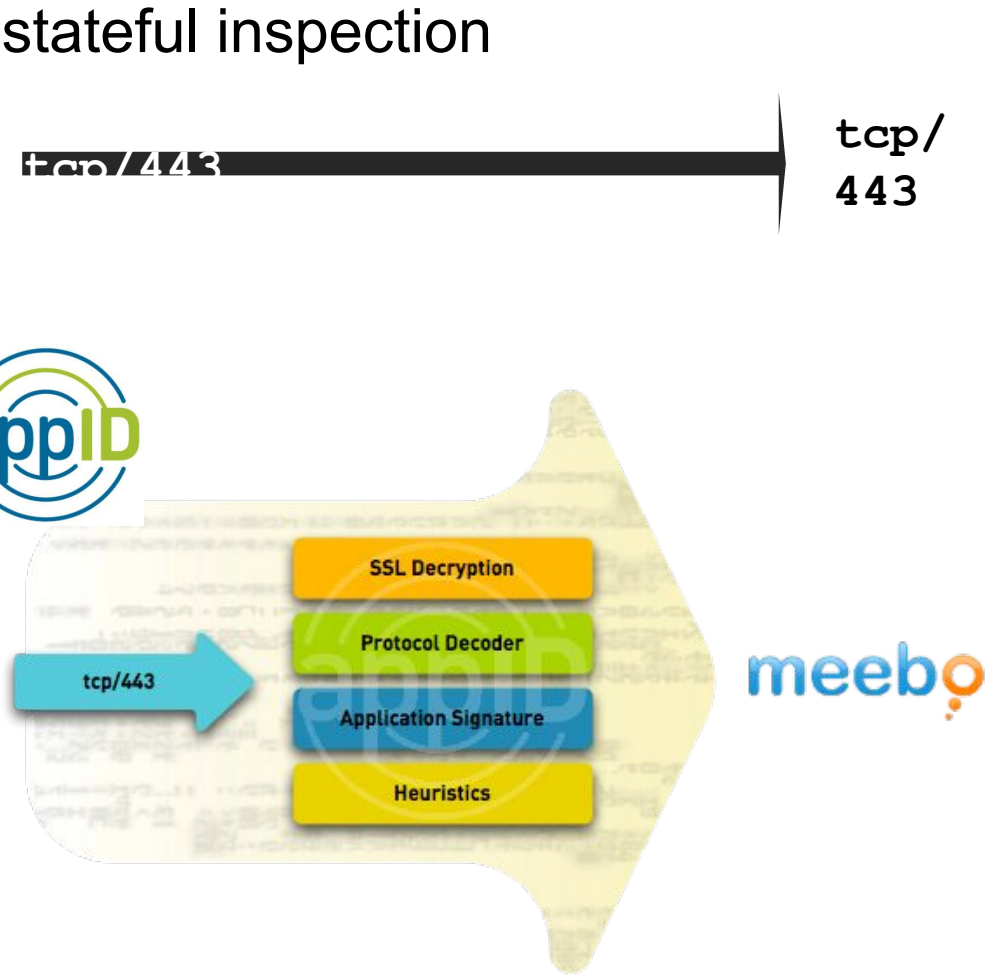
Многоядерный процессор
- Многопроцессорная обработка для обеспечения высокой производительности
- Аппаратная обработка сложных, но стандартизованных функций (SSL, IPSec)

10 Гбит/с сетевой процессор
- Сетевой процессор разгружает основные процессор
- Аппаратно реализованный QoS, маршрутизация, коммутация и NAT

App-ID

Распознавание приложений (1000+):

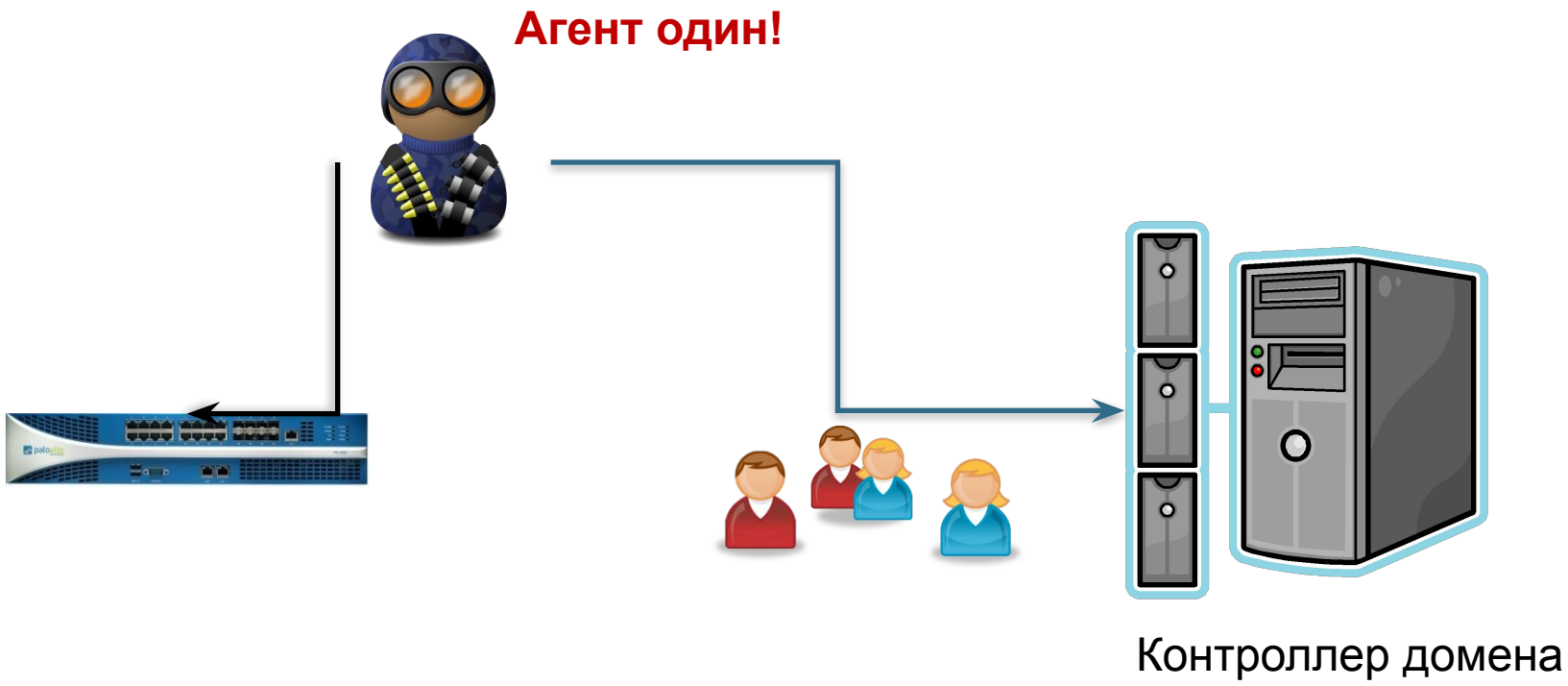
- Дешифрация (SSL)
- Распознавание/ декодирование протоколов 7 уровня
- Сигнатурный анализ
- Эвристический анализ (коммуникации)



paloalto NETWORKS

User–ID: Active Directory

- Агент подключается к контроллеру домена
- Считываются данные о пользователях и группах AD
- Строится таблица соответствия Пользователь - IP



Использование App-ID и User-ID

В логах

- Сортировка по приложениям/ пользователям
- Фильтрация по приложениям/ пользователям

From User	To User	From Port	To Port	Protocol	Application
tlewis		49764	53	udp	dns
	mellison	1150	137	udp	netbios-ns
tlewis		49763	53	udp	dns
	rrosa	1150	137	udp	netbios-ns
	nburt	4140	3184	udp	emule
bbrown7		4981	80	tcp	limelight
tlewis		49785	53	udp	dns

В политиках

- Применение к приложениям
- Применение к пользователям и группам

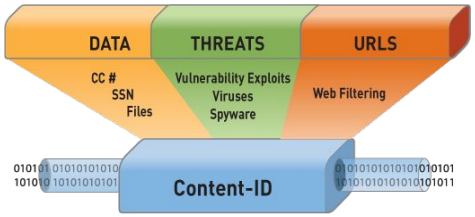
hzielinski App Usage 2008/12/23 08:24:21

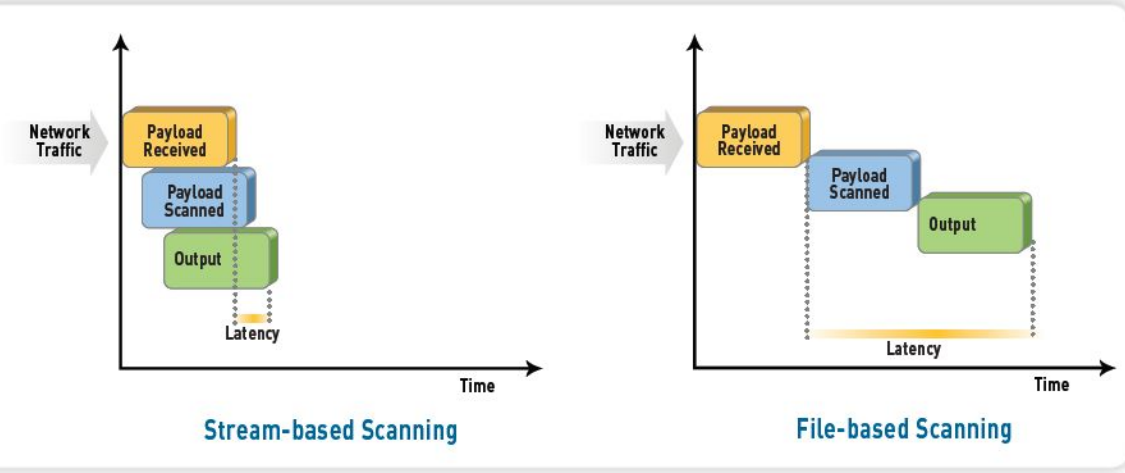
	Source User	Application	Action
1	hzielinski	web-browsing	allow
2	hzielinski	gnutella	allow
3	hzielinski	facebook	allow
4	hzielinski	yahoo-mail	allow
5	hzielinski	limelight	allow

8	Allow IT Remote Access	trust	untrust	any	pancademo.local\administrators	any	Remote Access
9	CFO Warcraft	trust	untrust	any	pancademo.local\jstoller	any	worldofwarcraft

Content-ID

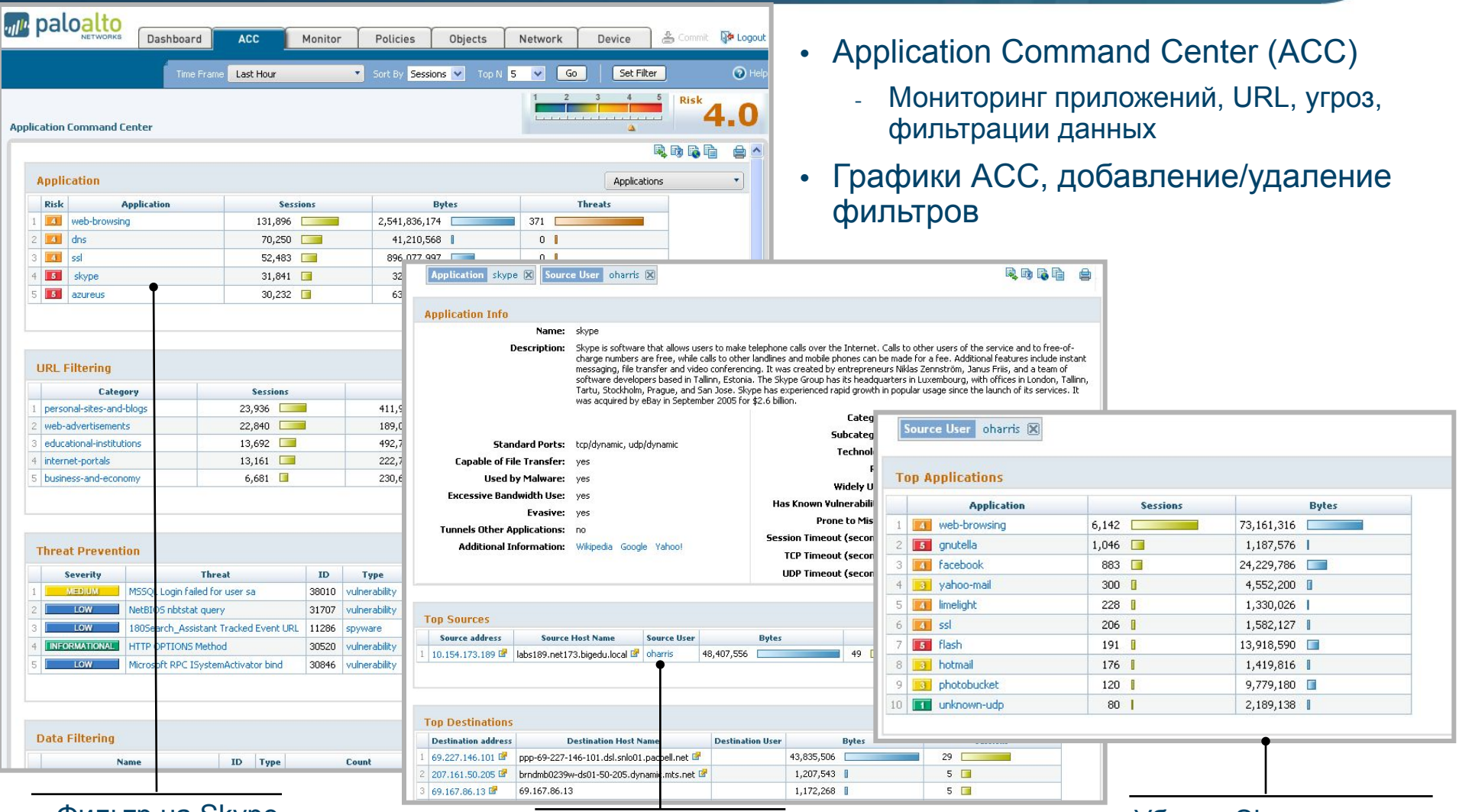
- Потоковое (не файловое!) сканирование на широкий спектр угроз
  - Сигнатурный движок сканирует на вирусы, бот-неты, шпионское ПО и т.д.
  - Интегрированная защита от уязвимостей (IPS)
- Защищает от утечек конфиденциальной информации
  - Блокирование передачи файлов определенного типа (в различных приложениях)
  - Блокирование по маске (например, номера кредитных карт, по грифу «Конфиденциально»)
- Фильтрация по URL
  - Локальная база URL (20M, 76 категорий, 1000 URL/сек)
  - Динамическая база (с кэшированием)





Интерфейс

- Application Command Center (ACC)
  - Мониторинг приложений, URL, угроз, фильтрации данных
- Графики ACC, добавление/удаление фильтров



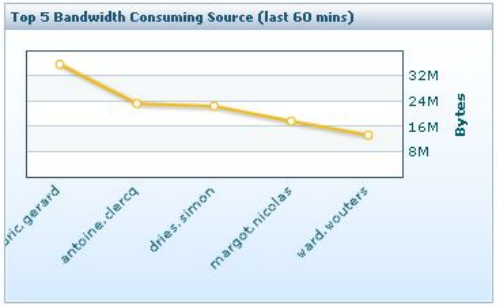
Фильтр на Skype

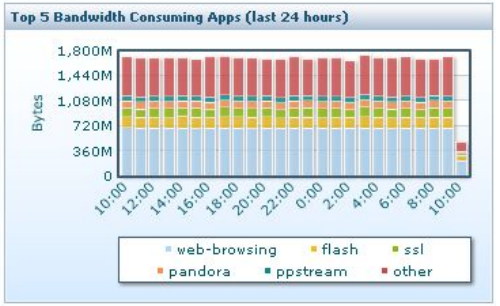
Фильтр для Skype и пользователя O. Harris

Убрать Skype и посмотреть все приложению O. Harris

Система отчетов

- Построение отчетов по пользователям, приложениям (по конкретному или top)
- Отчет по URL, посещенным пользователем (все или top)
- Отслеживание изменений трафика в сети
- Карта распределения трафика
- Отчет по сетевым атакам
- Настраиваемые (custom) отчеты
- Сводный отчет AVR
- Оформление в PDF
- Настройка рассылки по времени





PAN-OS (Palo Alto Networks Operating System)

Функции ОС:

- Сетевые функции
  - Динамическая маршрутизация (OSPF, RIPv2, BGP)
  - Удаленные доступ SSL VPN
  - Подключение к SPAN
  - Прозрачный in-line режим (“Layer 1”)
  - Режим L2/L3
- Зоновый подход
  - Все интерфейсы могут быть помещены в зоны безопасности
- Резервирование
  - Активный / пассивный
  - Синхронизация конфигураций
- QoS шейпинг
  - Приоритезация
  - Применение политик к конкретным приложениям, пользователям, зонам и т.д.
- Виртуальные системы
  - Несколько виртуальных файерволов на одном устройстве
- Простое, гибкое управление
  - CLI, Web, Panorama, SNMP, Syslog


PA-4060


PA-4050


PA-4020


PA-2050


PA-2020


PA-500

Семейство платформ

Производительность

10Gbps; 5Gbps threat prevention (XFP interfaces)

10Gbps; 5Gbps threat prevention

2Gbps; 2Gbps threat prevention

PA-4000 Series

1Gbps; 500Mbps threat prevention

500Mbps; 200Mbps threat prevention

PA-2000 Series

250Mbps; 100Mbps threat prevention

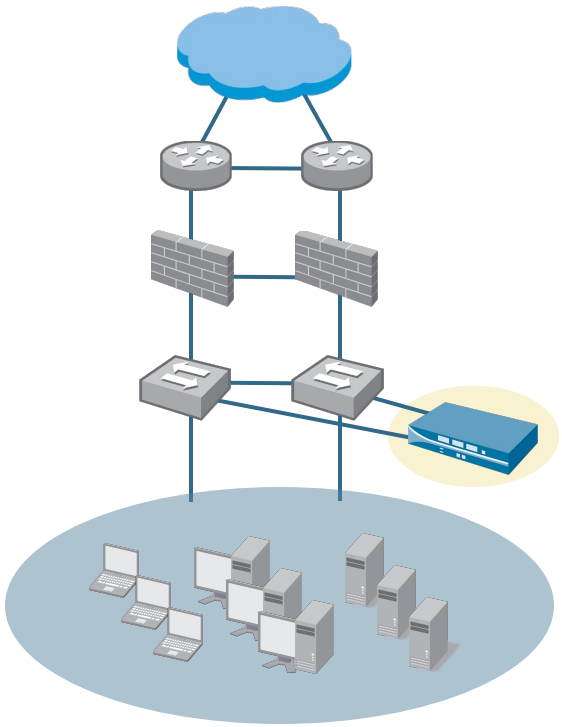
PA-500

Удаленные офисы/ Средние корпорации

Большие корпорации

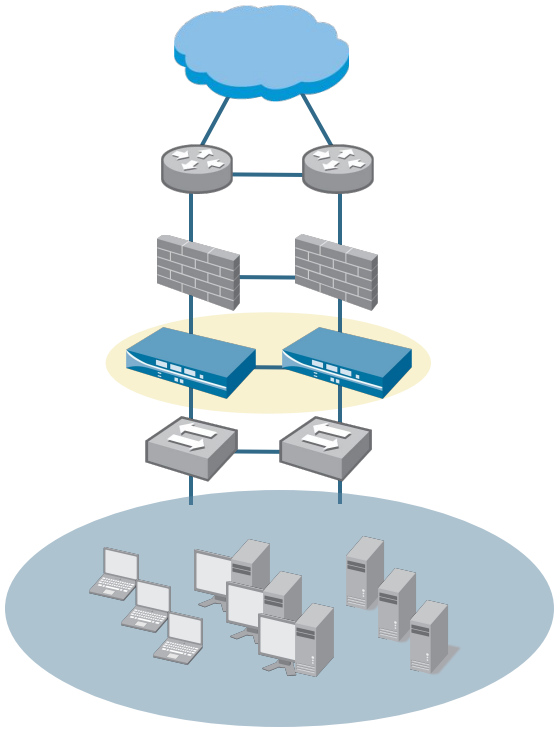
Способы установки в сеть

Мониторинг



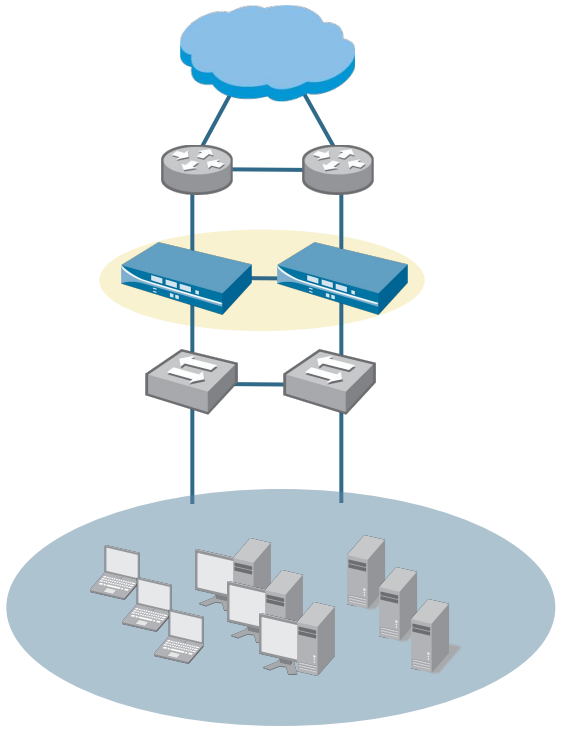
- Мониторинг без вмешательства в работу сети

Прозрачный In-Line



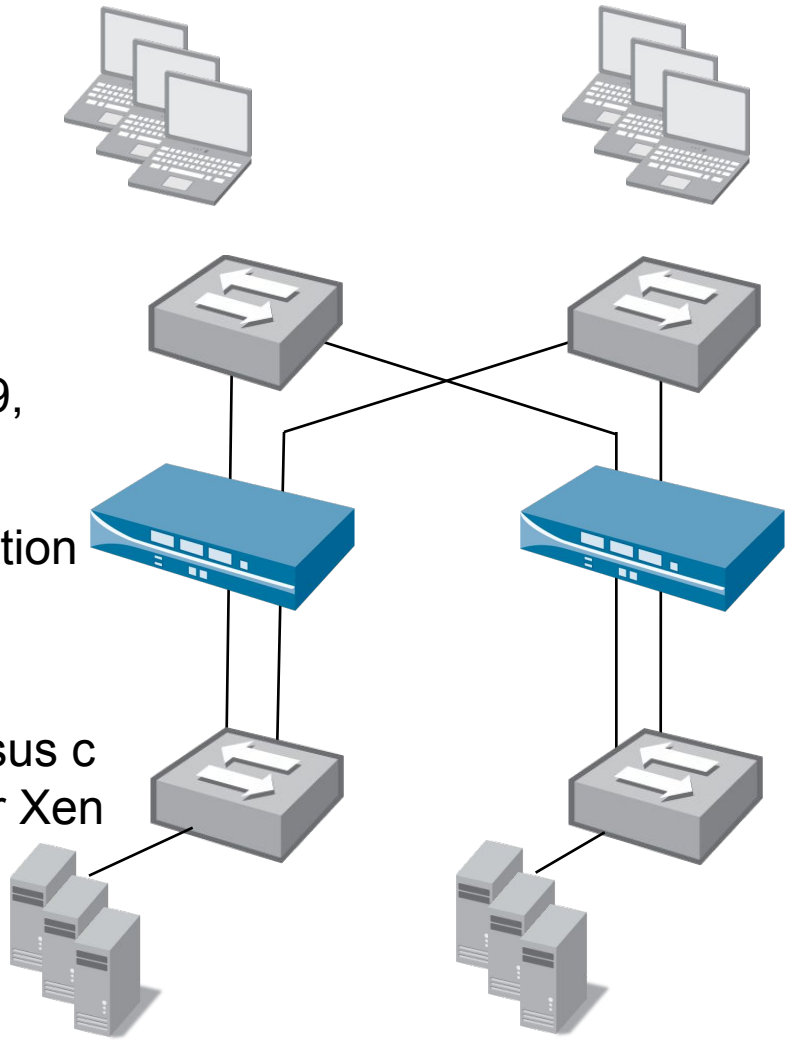
- Функции защиты от угроз
- IPS + AV + URL фильтрации

Firewall



- Вместо Firewall
- Firewall + IPS + AV + URL фильтрация

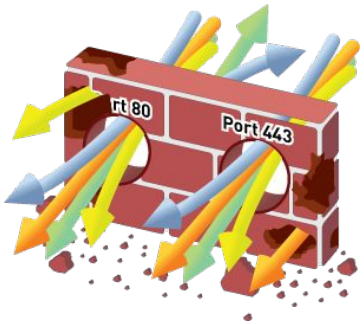
Palo Alto в data-центре



Palo Alto:

- Интерфейсы 10G
- Производительность до 10 Гбит/с
- Сканирование на все угрозы до 5 Гбит/с
- Одновременное сканирование на 3 млн. сигнатур
- Защита от bot-net
- Написание собственных приложений
- Отказоустойчивость
- Движок DLP
- Централизованное управление

Итог



Применение политик к приложениям, а не к портам

Применение политик к пользователям, а не к IP адресам

Контроль передаваемых данных

- Защита от вирусов, уязвимостей, шпионского ПО, bot-net
- Контроль передаваемых файлов по типам
- Контроль передаваемых данных по маске

Тестирование

Тестирование независимой лабораторией:

NSS Labs

NSS Labs' Rating: Recommend

Product	Effectiveness	Throughput
Palo Alto Networks PA-4020	93.4%	2,259 Mbps

Демонстрационное тестирование на вашей площадке:

- PA-2050
- Полный функционал
- 1-2 недели
- Итоговый отчет AVR

Спасибо

Дополнительная информация на
http://www.paloaltonetworks.com

paloalto NETWORKS