

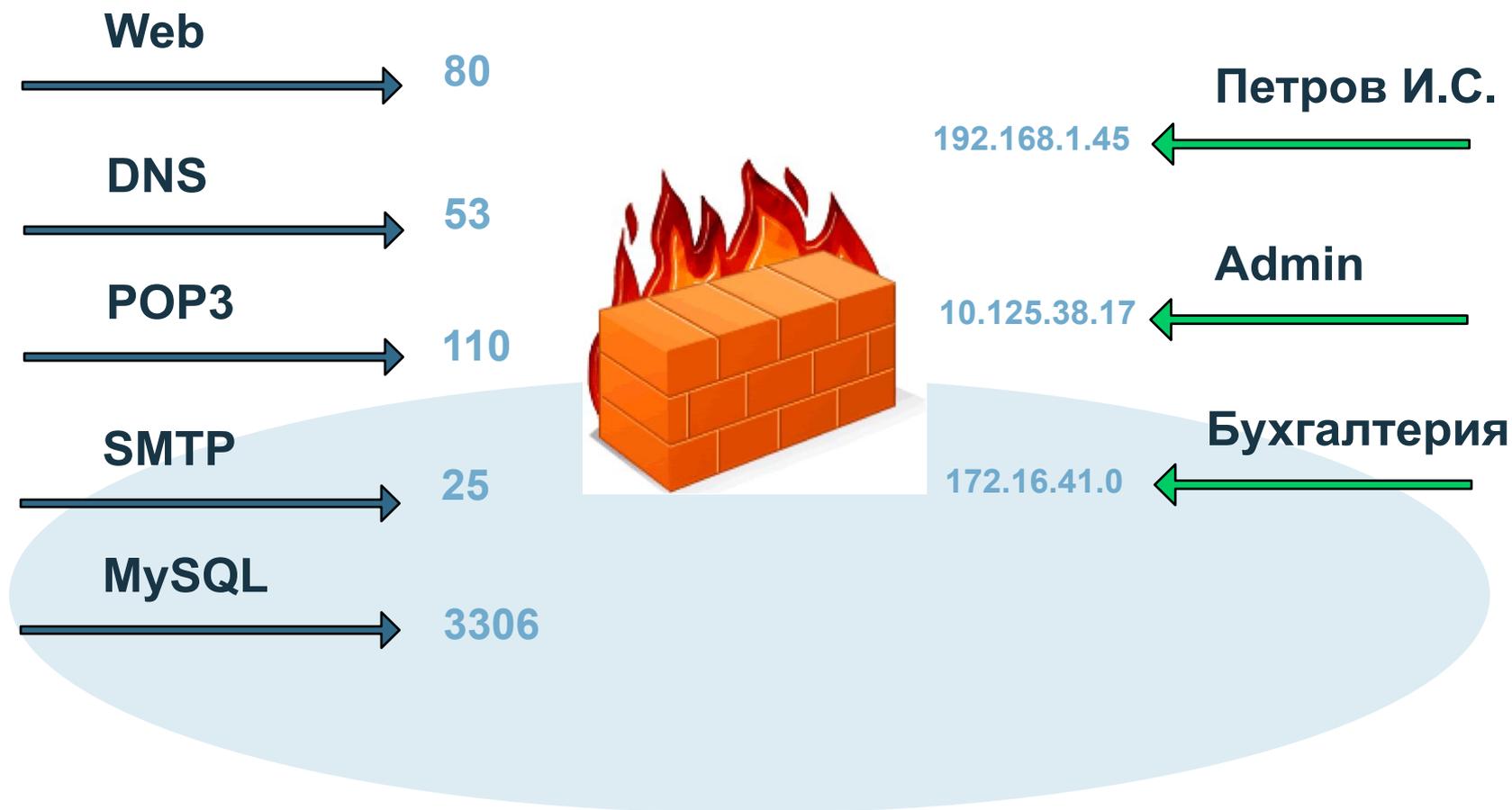
Palo Alto Networks



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

twitter

meebo

SAP



YouTube

BitTorrent™

webex™



1С
ФИРМА «1С»

@mail.ru
национальная почтовая служба

G M
by Google

skype™

icq

youSENDit

salesforce.com
Business On Demand™

LinkedIn

Microsoft Office
SharePoint

XING

Adobe Connect

В КОНТАКТЕ



Google Docs

ORACLE®

TSP 80: бизнес приложения



ТСР 80: другие приложения

twitter

meebo

SAP



YouTube

BitTorrent

webex



1С
ФИРМА «1С»

@mail.ru
национальная почтовая служба

G M
by Google

skype



icq

youSENDit

salesforce.com

Microsoft Office
SharePoint

XING

LinkedIn

Adobe Connect

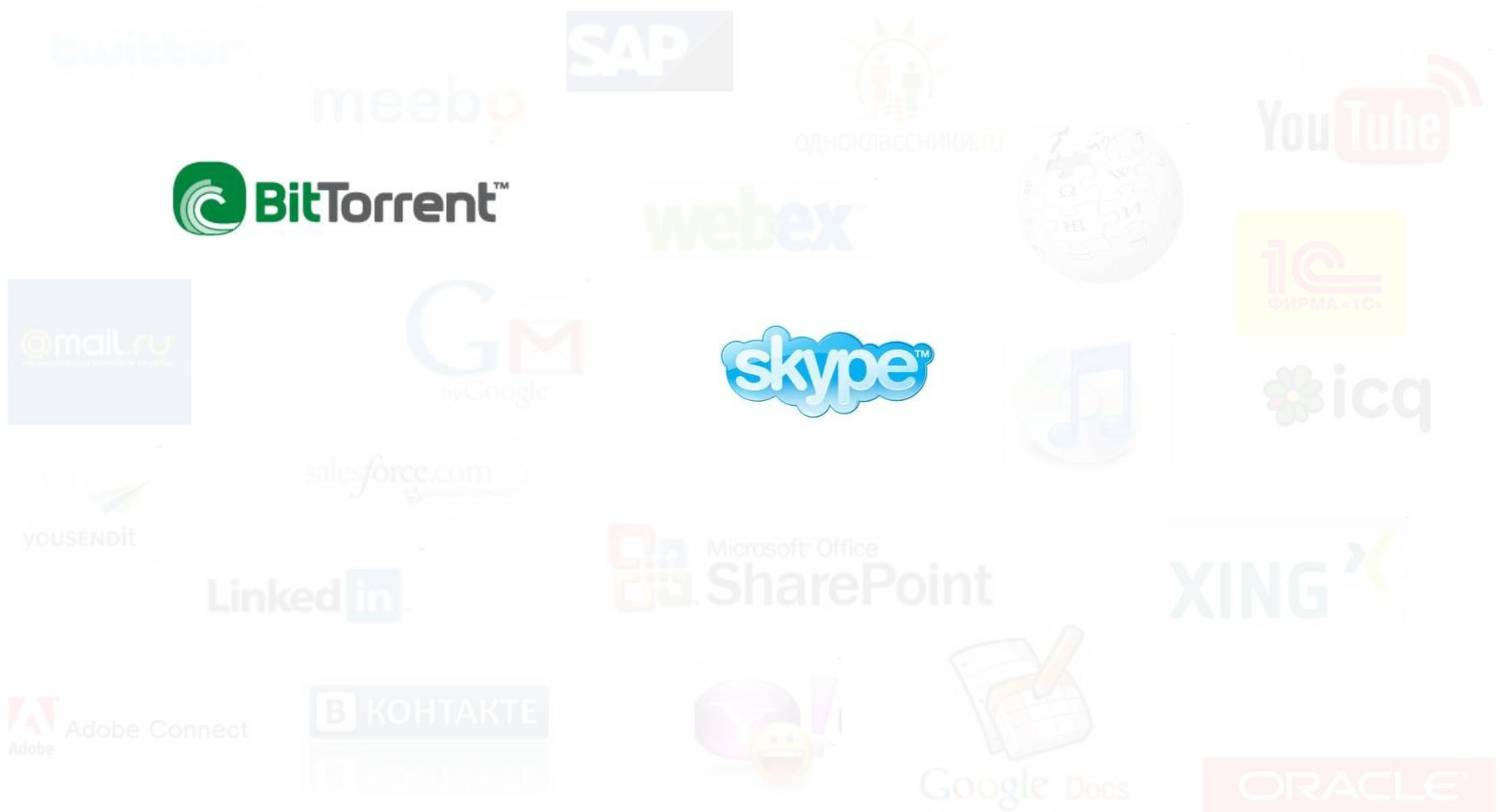
В КОНТАКТЕ



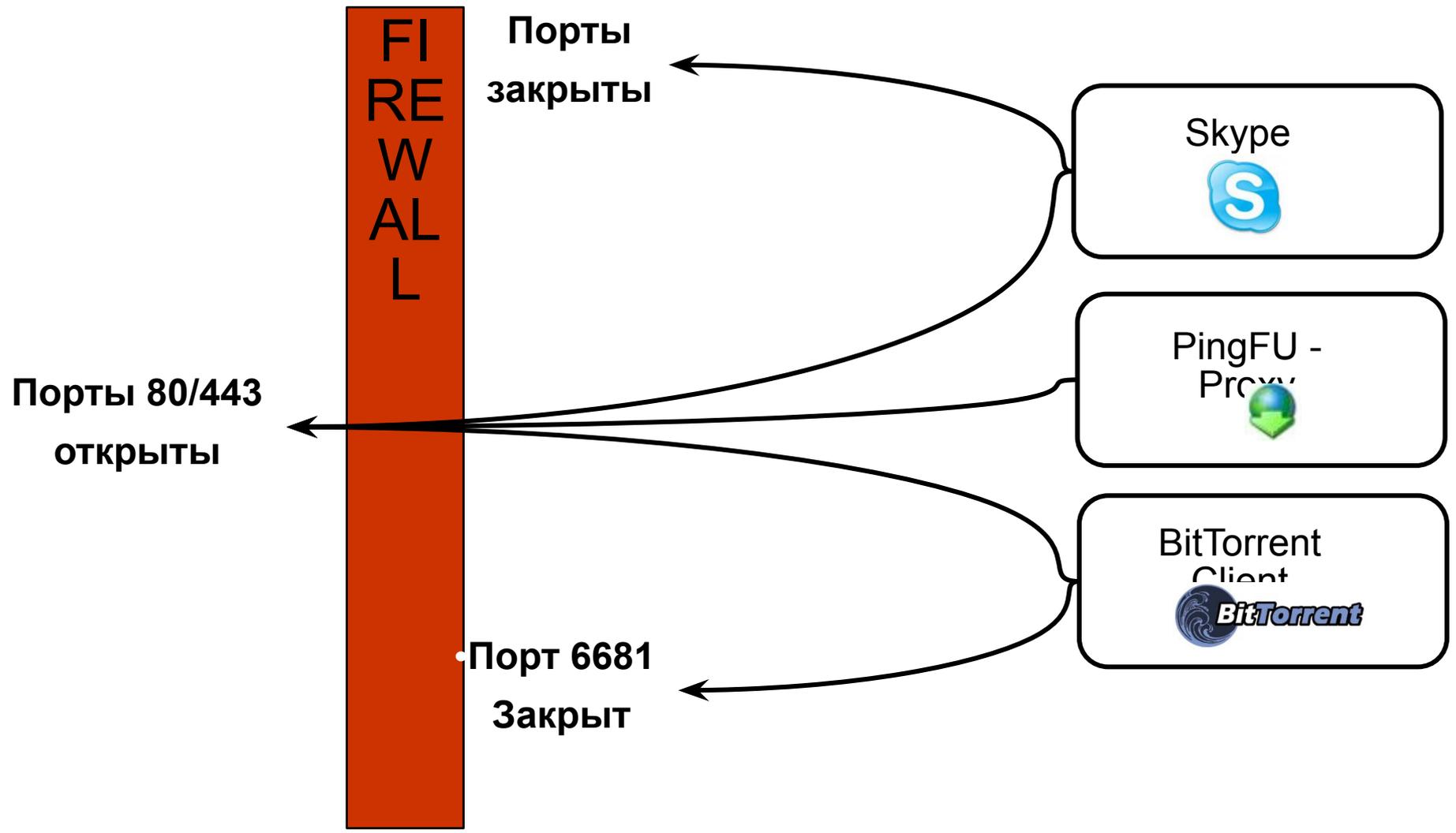
Google Docs

ORACLE

Тактика обхода систем безопасности



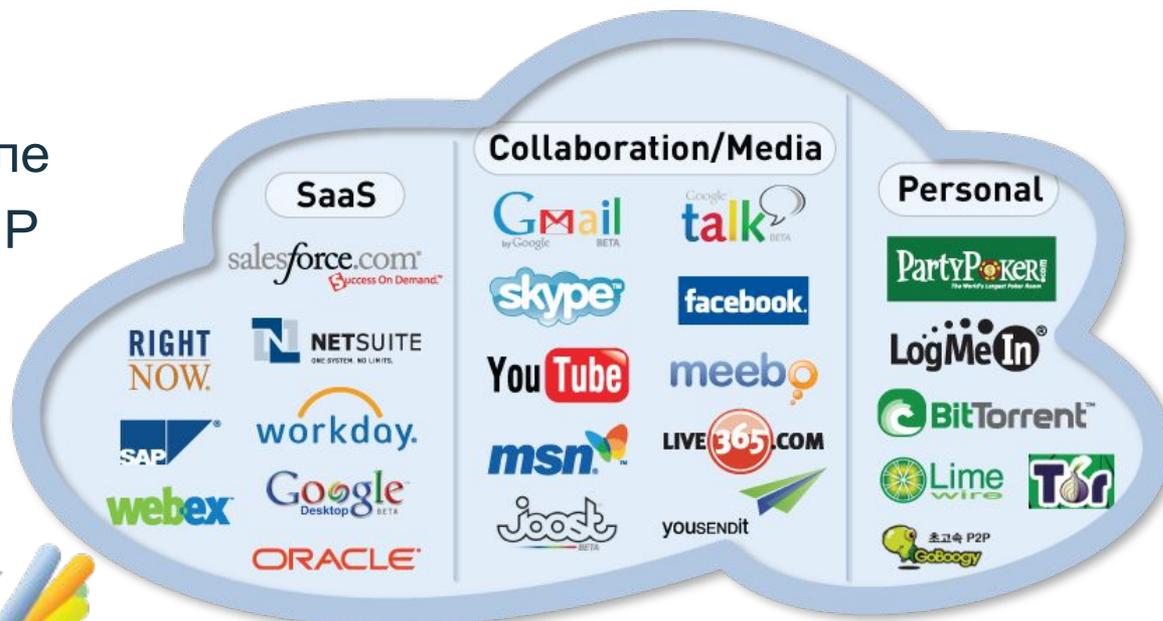
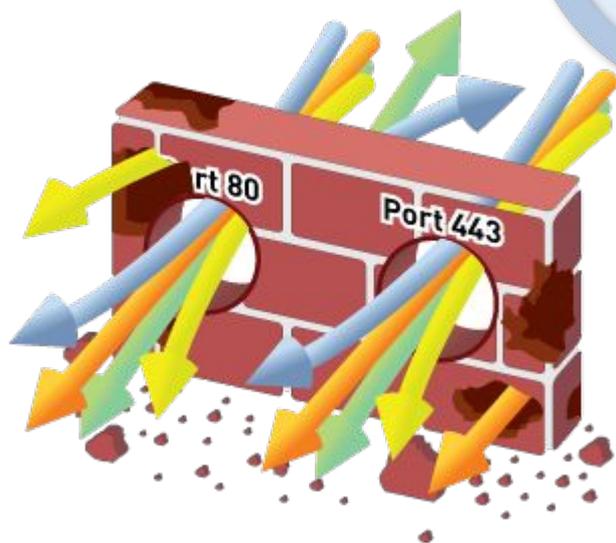
Тактика обхода систем безопасности. Пример



Вывод:

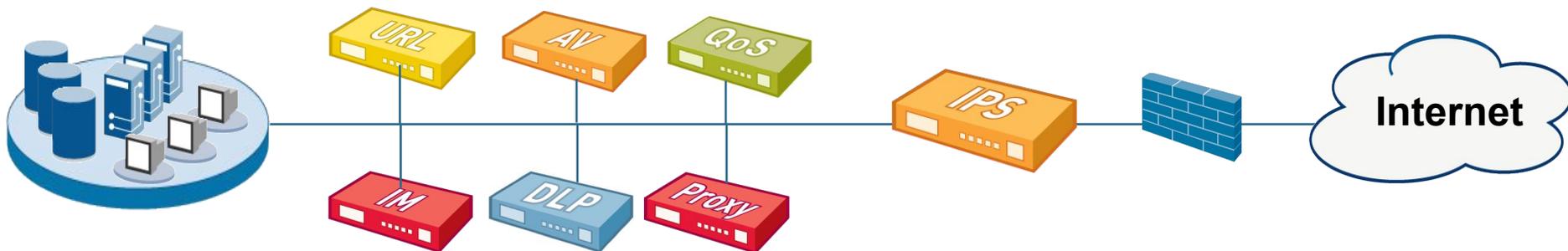
Приложения изменились, а фаерволы - нет

Политики фаерволов базируются на контроле портов, протоколов и IP адресов...



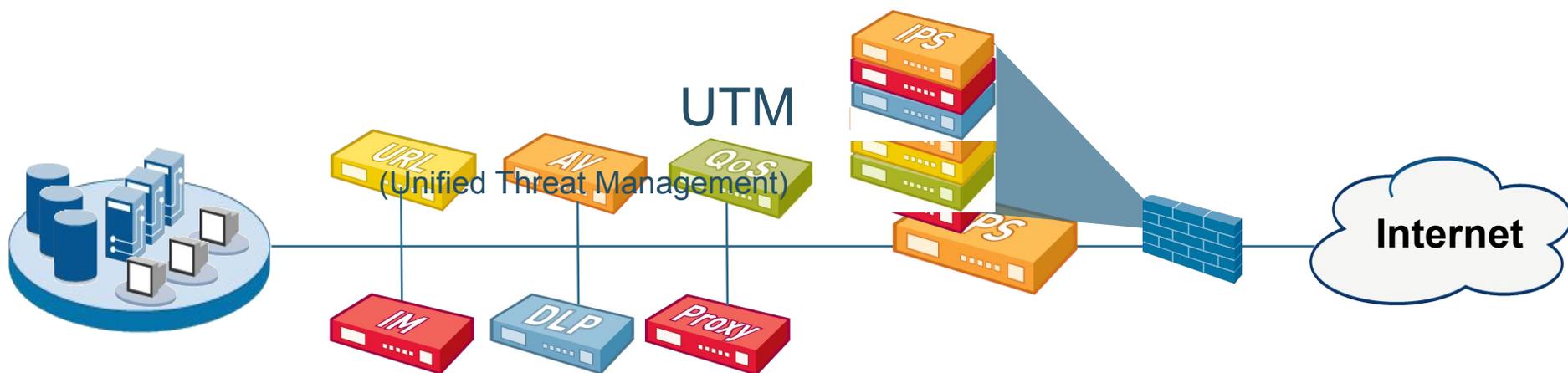
... а должны контролировать приложения, пользователей и передаваемые данные

«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

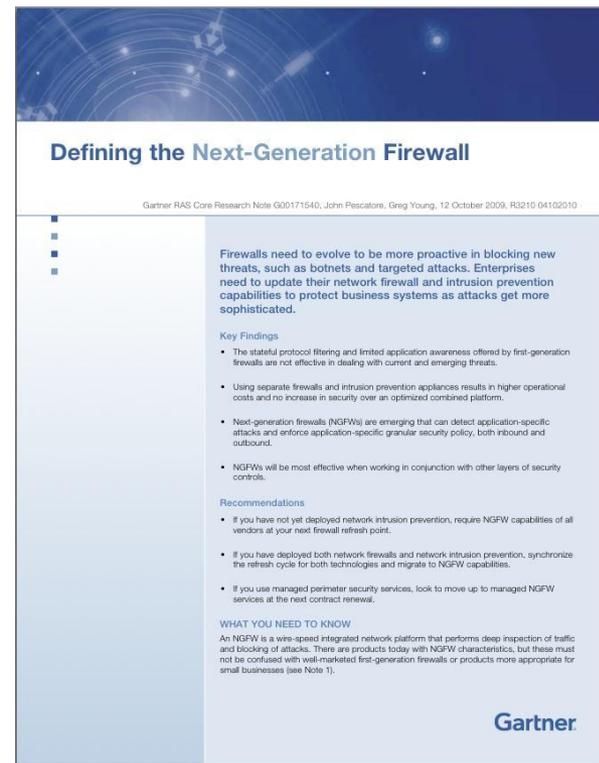
Интеграция со службами каталогов (Active Directory и т.д.)

✓ 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

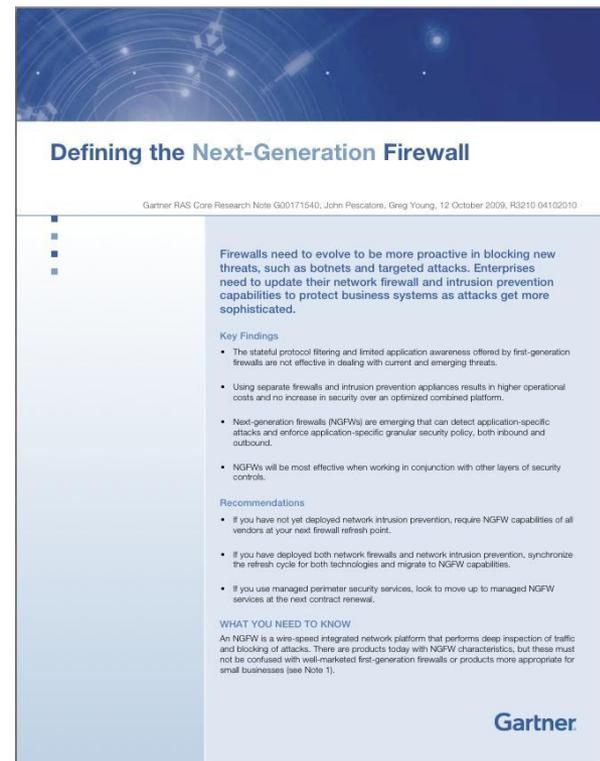
An NGFW is a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks. There are products today with NGFW characteristics, but these must not be confused with well-marketed first-generation firewalls or products more appropriate for small businesses (see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

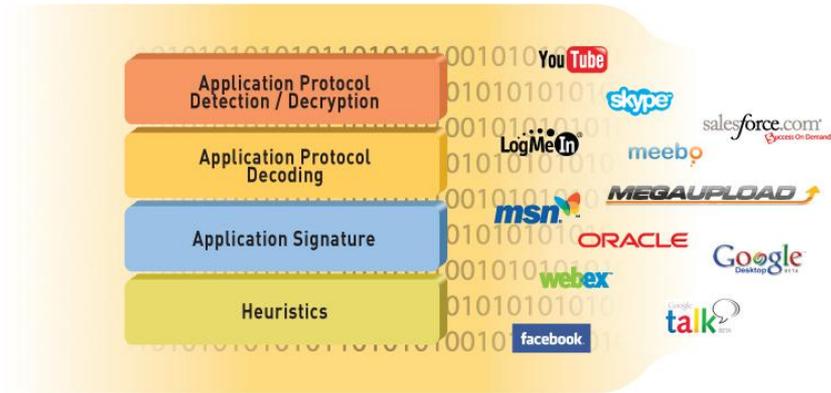
1. Определение приложений вне зависимости от порта и шифрования SSL
2. Определение пользователей вне зависимости от IP адреса
3. Применение политик к приложениям и функционалу этих приложений
4. Интегрированная защита от сетевых атак
5. Производительность до 10 Гбит/с



Уникальные технологии изменили фаервол

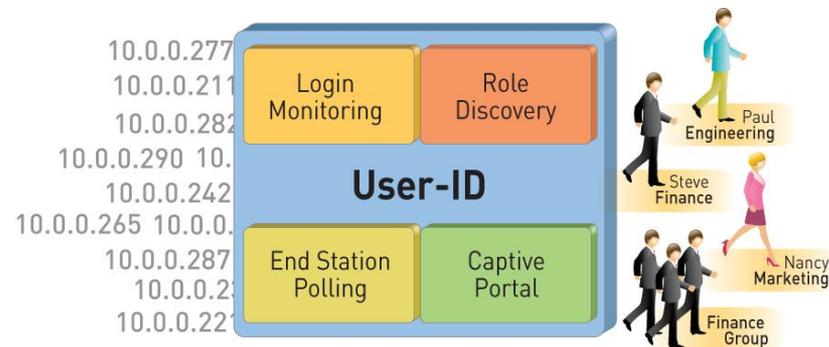
App-ID

Идентификация приложений



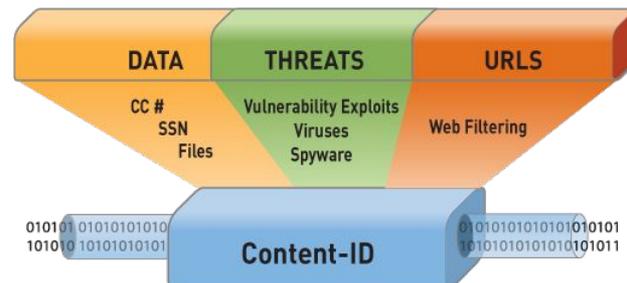
User-ID

Идентификация пользователей

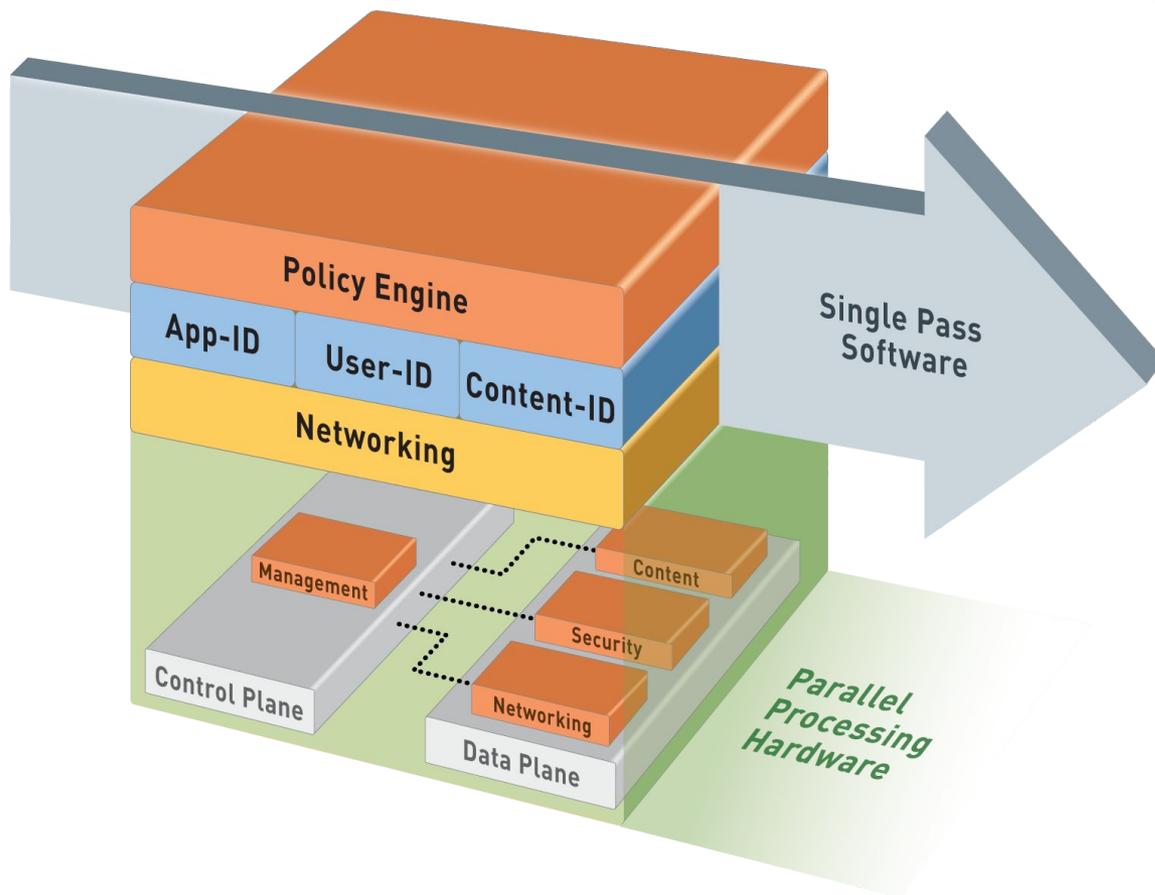


Content-ID

Контроль данных



«Однопроходная» архитектура



Один проход

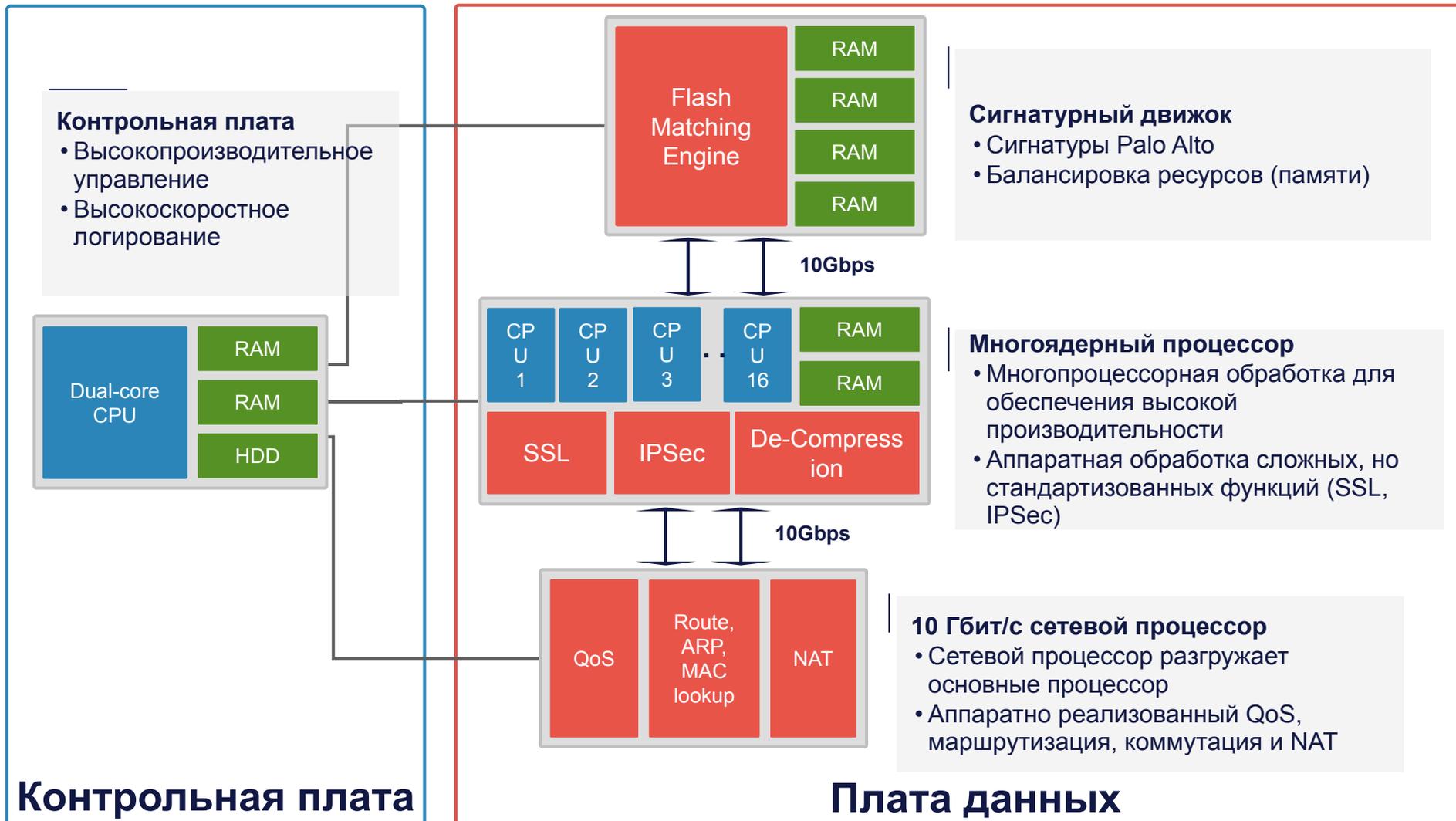
- Одна операция на пакет
 - Классификация трафика (App-ID)
 - Определение пользователей/групп
 - Сканирование данных – угрозы, URLы, конфиденциальные данные
- Единая политика
 - Политика применяется к приложению, IP адресу, пользователю и т.д.

Параллельная обработка

- Специализированное аппаратное обеспечение
- Разделение контрольной платы от платы данных

Производительность до 10 Гбит/с,
маленькая задержка

Специализированная архитектура (PA-4000)



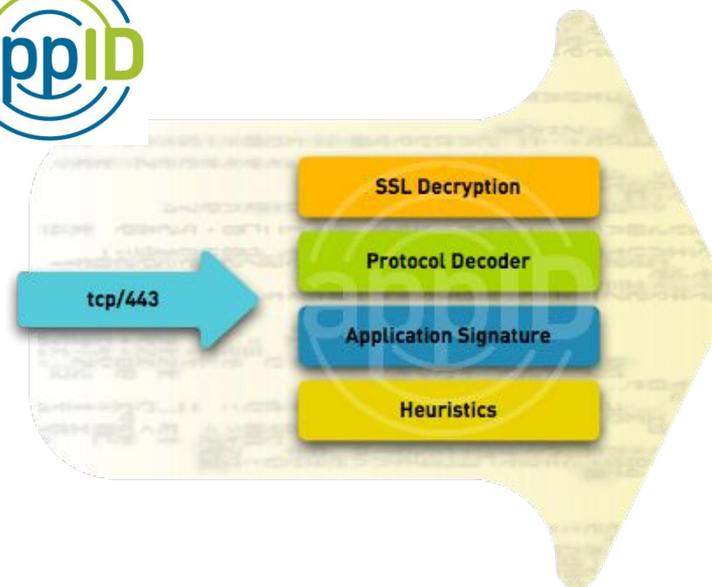
Распознавание приложений (1000+):

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

stateful inspection

tcp/443

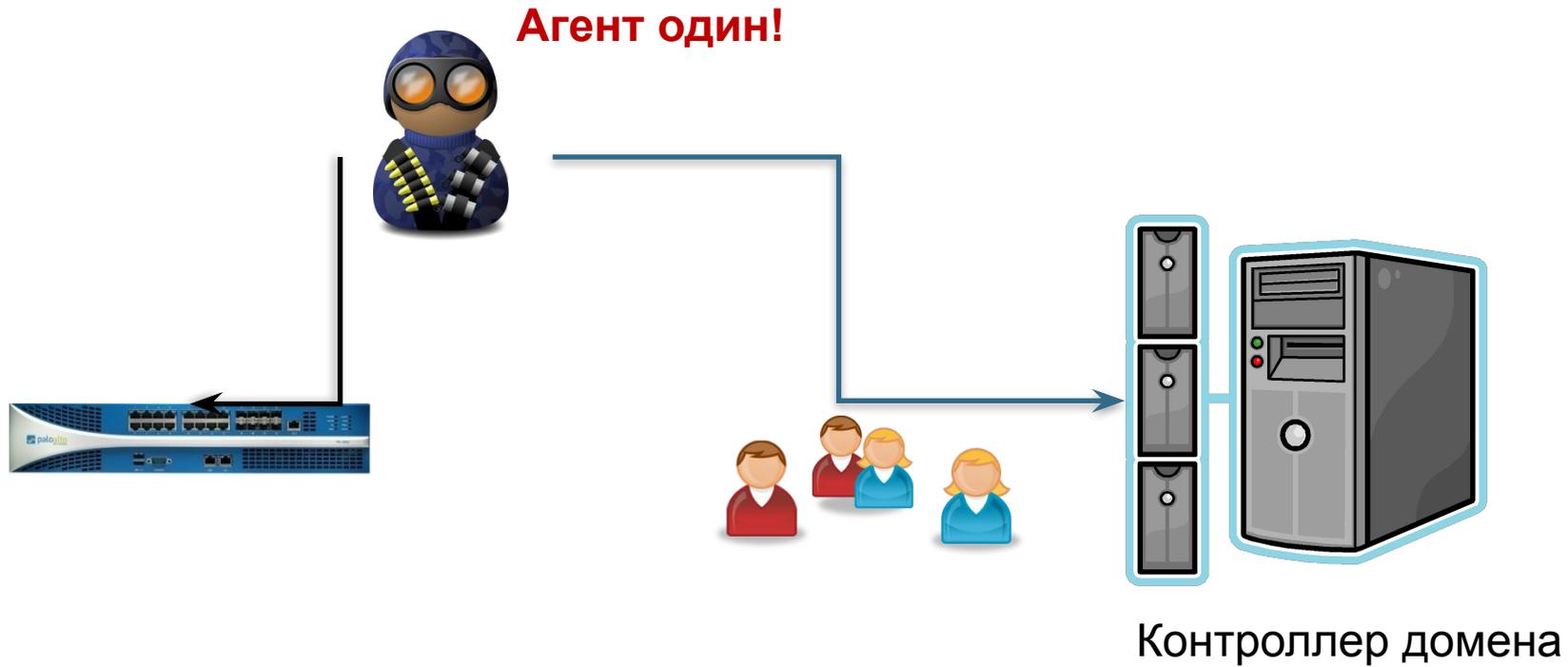
tcp/
443



meebo

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

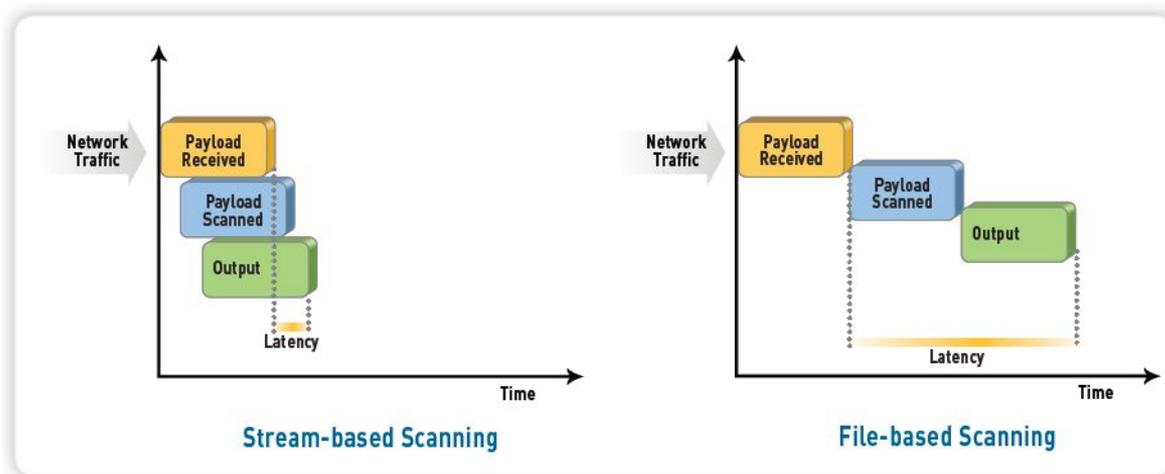
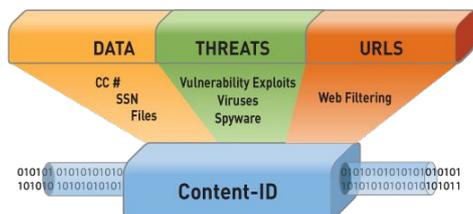
	Source User	Application	Action
1	hzielinski	web-browsing	allow
2	hzielinski	gnutella	allow
3	hzielinski	facebook	allow
4	hzielinski	yahoo-mail	allow
5	hzielinski	limelight	allow

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



- Потокное (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 (20М, 76 категорий, 1000 URL/сек)
 - Динамическая база (с кэшированием)



Интерфейс

The screenshot shows the Palo Alto Networks Application Command Center (ACC) interface. At the top, there are navigation tabs: Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. Below these are controls for Time Frame (Last Hour), Sort By (Sessions), Top N (5), and a Set Filter button. A risk level indicator shows a score of 4.0. The main content area is divided into several sections:

- Application:** A table listing top applications by risk and sessions.

Risk	Application	Sessions	Bytes	Threats
1	web-browsing	131,896	2,541,836,174	371
2	dns	70,250	41,210,568	0
3	ssl	52,483	896,077,997	0
4	skype	31,841	32	0
5	azureus	30,232	63	0
- URL Filtering:** A table showing categories and session counts.

Category	Sessions
personal-sites-and-blogs	23,936
web-advertisements	22,840
educational-institutions	13,692
internet-portals	13,161
business-and-economy	6,681
- Threat Prevention:** A table listing threats with severity, ID, and type.

Severity	Threat	ID	Type
MEDIUM	MSSQL Login failed for user sa	38010	vulnerability
LOW	NetBIOS nbstat query	31707	vulnerability
LOW	180Search_Assistant Tracked Event URL	11206	spyware
INFORMATIONAL	HTTP OPTIONS Method	30520	vulnerability
LOW	Microsoft RPC ISystemActivator bind	30846	vulnerability
- Data Filtering:** A table with columns for Name, ID, Type, and Count.

Фильтр на Skype

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

This section provides detailed information for the selected application (skype) and source user (oharris).

Application Info:

- Name:** skype
- Description:** Skype is software that allows users to make telephone calls over the Internet. Calls to other users of the service and to free-of-charge numbers are free, while calls to other landlines and mobile phones can be made for a fee. Additional features include instant messaging, file transfer and video conferencing. It was created by entrepreneurs Niklas Zennström, Janus Friis, and a team of software developers based in Tallinn, Estonia. The Skype Group has its headquarters in Luxembourg, with offices in London, Tallinn, Tartu, Stockholm, Prague, and San Jose. Skype has experienced rapid growth in popular usage since the launch of its services. It was acquired by eBay in September 2005 for \$2.6 billion.
- Standard Ports:** tcp/dynamic, udp/dynamic
- Capable of File Transfer:** yes
- Used by Malware:** yes
- Excessive Bandwidth Use:** yes
- Evasive:** yes
- Tunnels Other Applications:** no
- Additional Information:** Wikipedia Google Yahoo!

Source User: oharris

Top Sources:

Source address	Source Host Name	Source User	Bytes
10.154.173.189	labs189.net173.bigedu.local	oharris	48,407,556

Top Destinations:

Destination address	Destination Host Name	Destination User	Bytes
69.227.146.101	ppp-69-227-146-101.dsl.srio01.pacbell.net		43,835,506
207.161.50.205	brndnb0239w-ds01-50-205.dynama.ms.net		1,207,543
69.167.86.13	69.167.86.13		1,172,268

Фильтр для Skype и пользователя O. Harris

This table shows the top applications after filtering for the user 'oharris'.

Application	Sessions	Bytes
1 web-browsing	6,142	73,161,316
2 gnutella	1,046	1,187,576
3 facebook	883	24,229,786
4 yahoo-mail	300	4,552,200
5 limelight	228	1,330,026
6 ssl	206	1,582,127
7 flash	191	13,918,590
8 hotmail	176	1,419,816
9 photobucket	120	9,779,180
10 unknown-udp	80	2,189,138

Убрать Skype и посмотреть все приложению O. Harris

Система отчетов

Application and Threat Summary

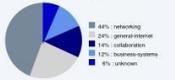
Apr 09, 2008

Application Usage

Risk Trend



Category Breakdown



Top 5 Applications

Application	Sessions	Bytes
web-browsing	77,859	3,061,989,586
msrpc	46,121	5,220,877,220
longp	38,103	5,362,784
dns	31,188	11,993,882
skype-probe	28,248	13,059,461

Threat Types

Top 5 Spyware

Spyware	Count
MiniBug retrieve weather information	377

Top 5 Vulnerabilities

Vulnerability	Count
AKONan Remote Code Execution Vulnerability	7,336
DnsDC Daemon Command Execution	5,125
Shellshock Shellshock Command Execution	3,558
HTTP OPTIONS Method	2,482
HTTP SQL Injection Attempt	2,372

Top 5 Viruses

Virus	Count
No matching data found!	

User Behavior

Top 5 Users

User	Sessions	Bytes
paloaltonetwork	743,869	53,737,432,686
paloaltonetwo	557,999	1,855,589,371
paloaltonetfing	520,748	2,109,052,450
paloaltonetfour	156,793	4,220,867,356
paloaltonetfive	131,483	6,900,749,979

Top 5 URL Categories

Category	Count
unknown	93,844
infrastructure	23,828
news	14,870
computing-and-internet	14,756
advertisements-and-poppups	13,643

Top 5 Destination Countries

Destination	Count
Reserved (10.0.0.0 - 10.255.255.255)	3,267,489
United States	1,148,207
Unknown	73,266
France	70,470
China	64,917

paloaltonetwork/binahara

Highest Risk User

Top 5 URL Categories

Category	Count
business	13,790
unknown	10,393
computing-and-internet	3,807
infrastructure	2,784
news	1,985

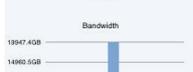
Top 5 Applications

Application	Sessions	Bytes
skype-probe	957,516	485,701,118
unknown-udp	81,352	20,242,917
ssl	166,063	1,157,247,715
skype	133,752	65,618,460
msrpc	817,743	218,670,488,833

Top 5 Threats

Threat	Count
MiniBug retrieve weather information	6,890
SCAN-Host Sweep	15,956
port ftp [IP: 192.168.1.100] (not defined)	216

Trends



- 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

Top 5 Gainers (last 60 minutes vs yesterday)



Top 5 Losers (last 60 minutes vs yesterday)



Top 5 Bandwidth Consuming Source (last 60 mins)



Top 5 Bandwidth Consuming Apps (last 24 hours)



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 файрволов на одном устройстве

• Простое, гибкое управление

- CLI, Web, Panorama, SNMP, Syslog



PA-4060



PA-4050



PA-4020



PA-2050

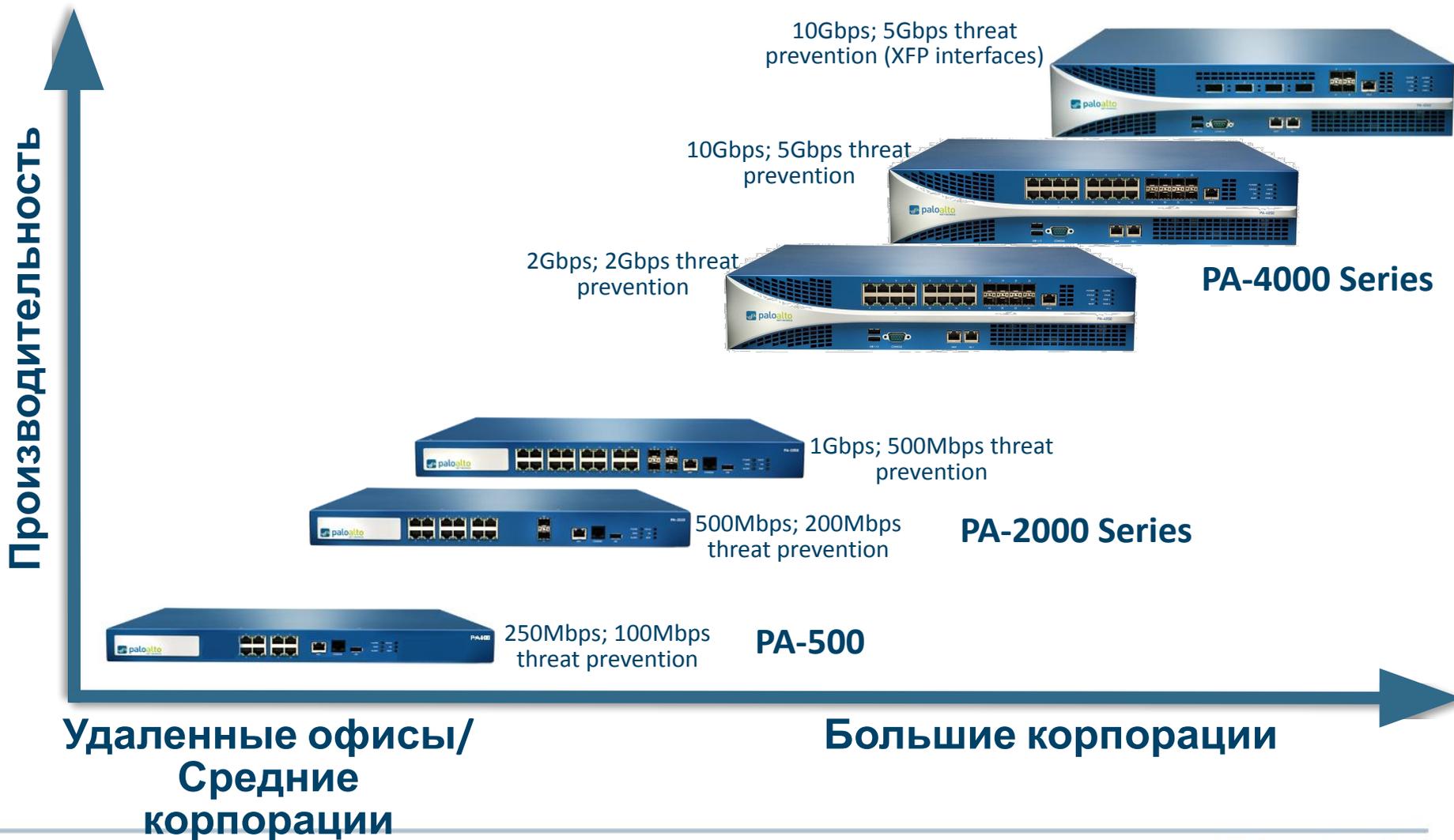


PA-2020



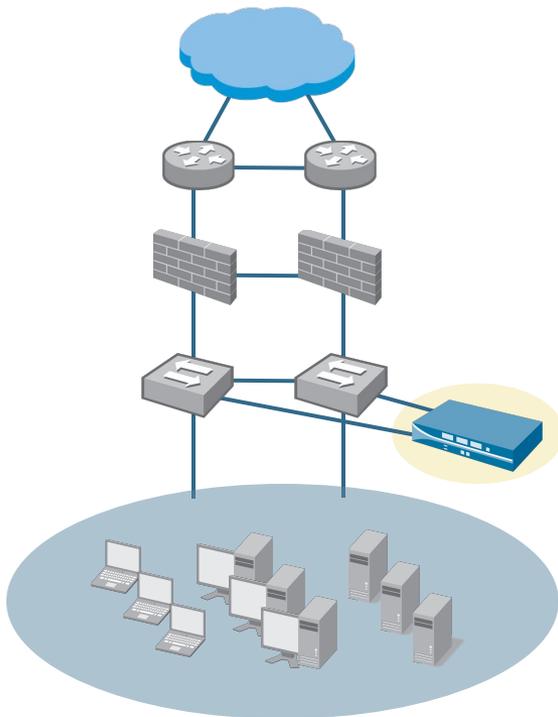
PA-500

Семейство платформ



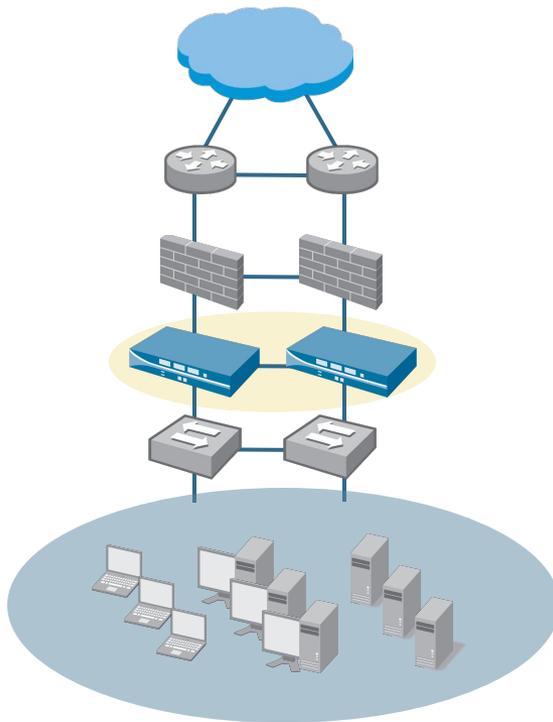
Способы установки в сеть

Мониторинг



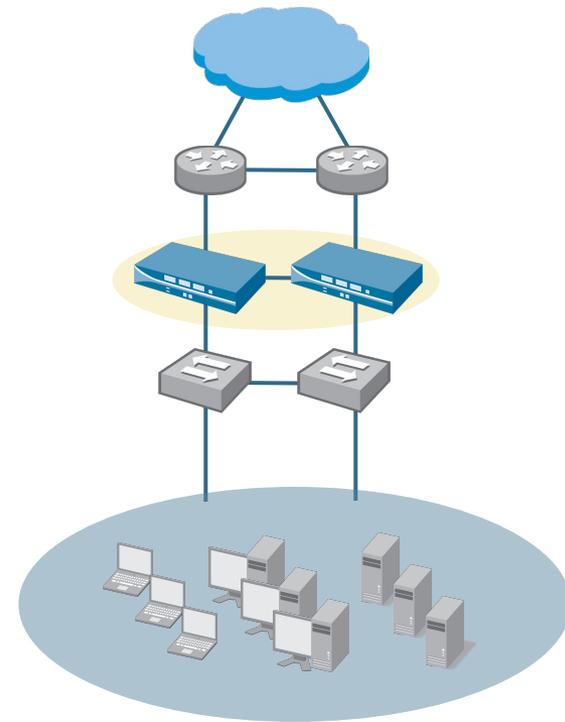
- Мониторинг без вмешательства в работу сети

Прозрачный In-Line



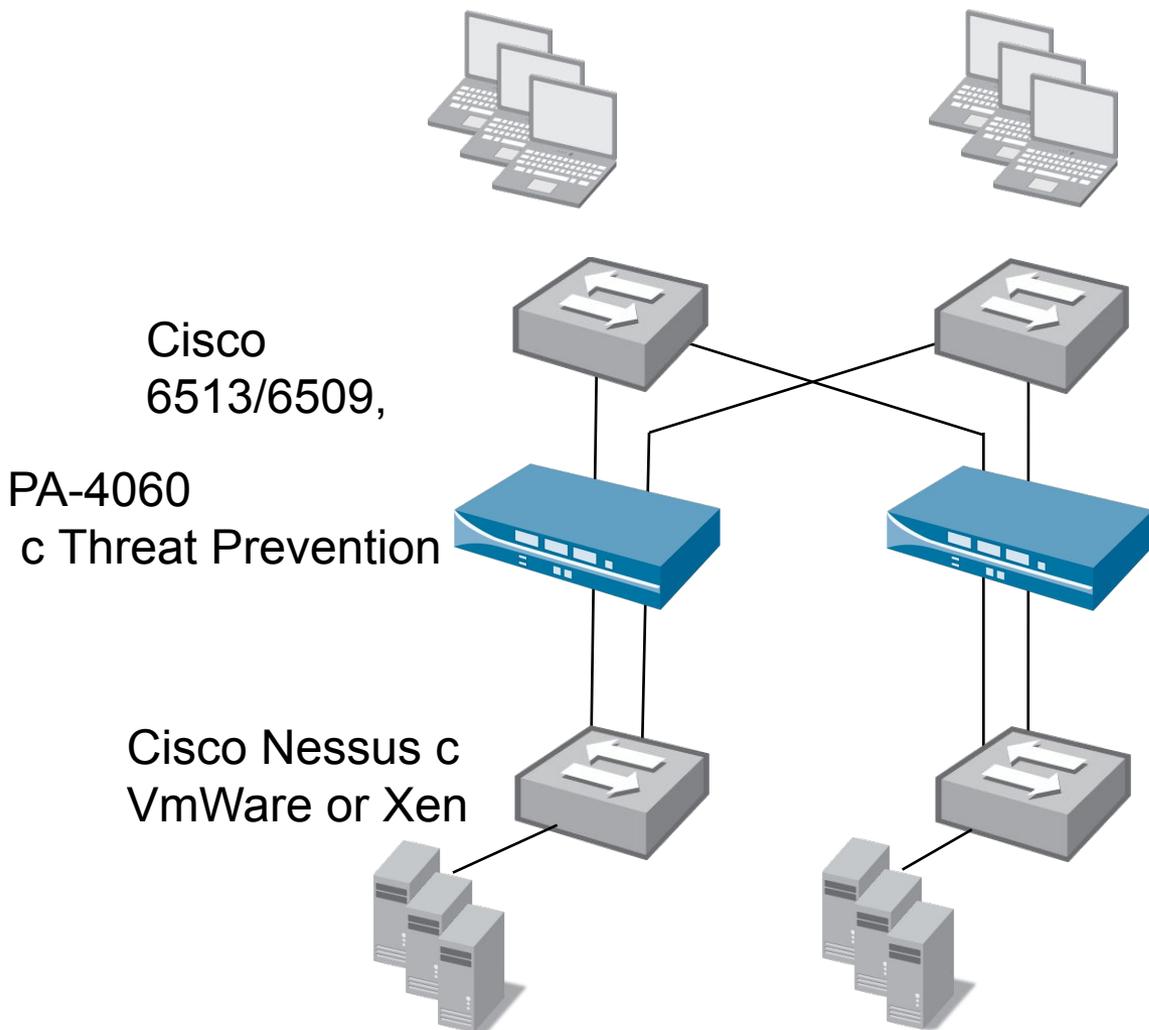
- Функции защиты от угроз
- IPS + AV + URL фильтрации

Firewall



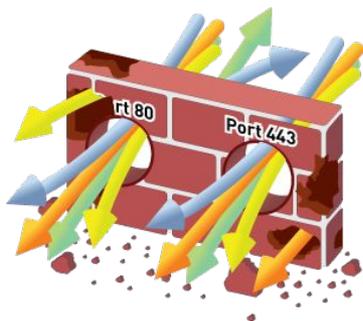
- Вместо Firewall
- Firewall + IPS + AV + URL фильтрация

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



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' 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>

