

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

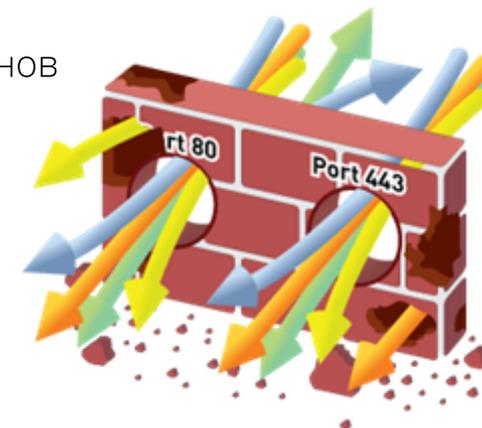
NEXT-GENERATION FIREWALL (NGFW)

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

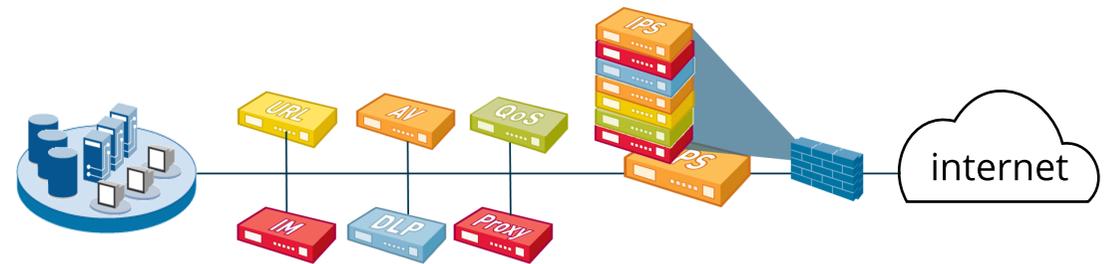
- Политики межсетевых экранов базируются на контроле:
 - Портов
 - IP-адресов
 - Протоколов



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

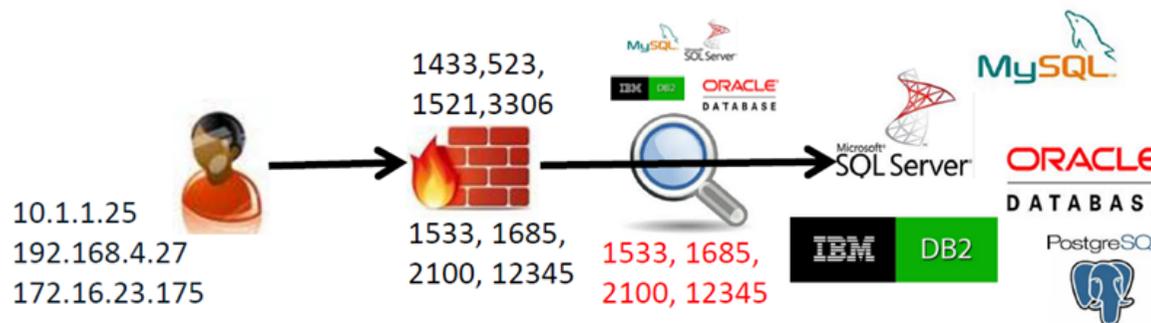


«ПОМОЩНИКИ» МЕЖСЕТЕВОГО ЭКРАНА НЕ ПОМОГАЮТ



- 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

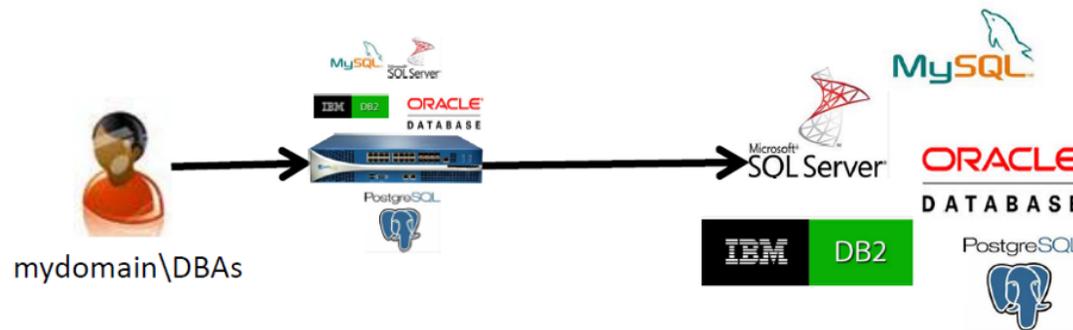
ШАГ 3

- 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)

Name	Tags	Type	Zone	Address	User	HP Profile	Zone	Address	Application	Service	Action	Profile	Options
1 Block_FB	none	universal	any	any	any	any	any	any	facebook	application-d...	Deny	none	
2 ForPetro_apps	VLAN16 Untrust_WAN1	universal	VLAN16	any	dobro\petro	any	Untrust_WAN1	any	browser-ema...	any	Deny	none	
3 ForPetro_url	VLAN16 Untrust_WAN1	universal	VLAN16	any	dobro\petro	any	Untrust_WAN1	any	any	any	Deny	none	
4 SMBD_for_HR	VLAN16 Untrust_WAN1	universal	VLAN16 VLAN17	any	dobro\hr	any	Untrust_WAN1	any	mysql oracle postgres	any	Allow		
5 All access	VLAN17 Untrust_WAN1	universal	VLAN17	any	dobro\admin...	any	Untrust_WAN1	any	any	any	Allow		
6 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	none

НАСТОЯЩИЙ NGFW: БЕЗОПАСНОЕ РАЗРЕШЕНИЕ ПРИЛОЖЕНИЙ

РАСШИФРОВАНИЕ ВХОДЯЩЕГО/ИСХОДЯЩЕГО SSL/SSH

Receive Time	Category	URL	From Zone	To Zone	Source	Destination	Application	Action
02/10 13:53:43	computer-and-internet-info	accounts.google.com/	VLAN16	Untrust_WAN1	172.16.16.30	216.58.209.205	ssl	alert
02/10 13:53:42	web-based-email	mail.google.com/	VLAN16	Untrust_WAN1	172.16.16.30	173.194.116.214	gmail-base	alert
02/10 13:53:39	social-networking	plus.google.com/	VLAN16	Untrust_WAN1	172.16.16.30	173.194.112.229	google-plus-base	alert
02/10 13:53:39	search-engines	clients5.google.com/	VLAN16	Untrust_WAN1	172.16.16.30	173.194.113.41	ssl	alert
02/10 13:53:39	search-engines	clients5.google.com/	VLAN16	Untrust_WAN1	172.16.16.30	173.194.113.41	ssl	alert
02/10 13:53:38	search-engines	www.gstatic.com/	VLAN16	Untrust_WAN1	172.16.16.30	173.194.112.56	ssl	alert
02/10 13:53:38	online-storage-and-backup	docs.google.com/	VLAN16	Untrust_WAN1	172.16.16.30	173.194.112.193	google-docs-base	alert
02/10 13:53:37	content-delivery-networks	doc-0c-54-docs.googleusercontent.com/	VLAN16	Untrust_WAN1	172.16.16.30	173.194.113.44	ssl	alert
02/10 13:53:37	search-engines	www.google.com.ua/	VLAN16	Untrust_WAN1	172.16.16.30	173.194.116.127	ssl	alert
02/10 13:53:37	search-engines	www.google.com/	VLAN16	Untrust_WAN1	172.16.16.30	173.194.113.16	ssl	alert
02/10 13:49:48	content-delivery-networks	doc-0c-54-docs.googleusercontent.com/docs/securec/np1539f2c4ee5v4p4k5op0c3ipmu/4l3jmsa3arvfuhlrvalf56s0...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.112.170	google-docs-base	alert
02/10 13:49:48	online-storage-and-backup	docs.google.com/nonceSigner?nonce=dsrjlpacnamkmd&continue=https://doc-0c-54-docs.googleusercontent.com/docs/se...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.112.194	google-docs-base	alert
02/10 13:49:46	online-storage-and-backup	docs.google.com/nonceSigner?nonce=dsrjlpacnamkmd&continue=https://doc-0c-54-docs.googleusercontent.com/docs/se...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.112.194	google-docs-base	alert
02/10 13:49:46	computer-and-internet-info	accounts.google.com/ServiceLogin?service=writely&passive=1209600&continue=https://docs.google.com/nonceSigner?...	VLAN16	Untrust_WAN1	172.16.16.30	216.58.209.205	web-browsing	alert
02/10 13:49:46	search-engines	www.google.com/accounts/ServiceLogin?service=writely&passive=1209600&continue=https://docs.google.com/nonceSi...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.116.179	web-browsing	alert
02/10 13:49:46	online-storage-and-backup	docs.google.com/nonceSigner?nonce=dsrjlpacnamkmd&continue=https://doc-0c-54-docs.googleusercontent.com/docs/se...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.112.194	google-docs-base	alert
02/10 13:49:45	content-delivery-networks	doc-0c-54-docs.googleusercontent.com/docs/securec/np1539f2c4ee5v4p4k5op0c3ipmu/4l3jmsa3arvfuhlrvalf56s0...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.112.170	google-docs-base	alert
02/10 13:49:45	search-engines	0.client-channel.google.com/client-channel/channel/bind?type=cell&service=appcommonstorage&sessionid=4-z2g...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.66.189	web-browsing	alert
02/10 13:49:17	streaming-media	s.youtube.com/api/stats/watchtime?ms=y&sel=detailpage&pcn=18UkR2pbPoCO3UcR8doic=93ufP93Uonglver=2&ref...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.112.36	web-browsing	alert
02/10 13:49:10	search-engines	0.client-channel.google.com/client-channel/channel/bind?type=cell&service=appcommonstorage&sessionid=4-z2g...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.66.189	web-browsing	alert
02/10 13:49:10	search-engines	0.client-channel.google.com/client-channel/channel/bind?type=cell&service=appcommonstorage&sessionid=4-z2g...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.66.189	web-browsing	alert
02/10 13:49:08	search-engines	0.client-channel.google.com/client-channel/channel/bind?type=cell&service=appcommonstorage&sessionid=4-z2g...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.66.189	web-browsing	alert
02/10 13:49:08	search-engines	0.client-channel.google.com/client-channel/channel/bind?type=cell&service=appcommonstorage&sessionid=4-z2g...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.66.189	web-browsing	alert
02/10 13:49:08	search-engines	0.client-channel.google.com/client-channel/channel/cbp?type=cell&service=appcommonstorage&sessionid=4-z2gC...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.66.189	web-browsing	alert
02/10 13:49:08	search-engines	0.client-channel.google.com/client-channel/channel/cbp?type=cell&service=appcommonstorage&sessionid=4-z2gC...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.66.189	web-browsing	alert
02/10 13:49:03	web-advertisements	googleads.doubleclick.net/pagead/clk/s?js=CAEBut=AFAXiQAAAAAVNnlHubzan4yCjOFBB_allQWGeTc54_botg=1&...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.113.26	web-browsing	alert
02/10 13:48:58	search-engines	0.client-channel.google.com/client-channel/client?dsg="Z";"cello";"y";"appcommonstorage";"B"false]&ctype=cell&se...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.66.189	web-browsing	alert
02/10 13:48:57	search-engines	clients4.google.com/invalidation/lcs/client?service=appcommonstorage&vpc="["ci";"McOrM0jho";"tp";"null";"...	VLAN16	Untrust_WAN1	172.16.16.30	173.194.113.34	web-browsing	alert
02/10 13:48:57	search-engines	www.google.com/tools/feedback/chat_load.js	VLAN16	Untrust_WAN1	172.16.16.30	173.194.116.179	web-browsing	alert
02/10 13:48:56	online-storage-and-backup	drive.google.com/thumbnaill?d=08Sp37n6s-cvTRGQJyYV0LPH8&authuser=0&v=1423389036821&sz=w84-h63	VLAN16	Untrust_WAN1	172.16.16.30	173.194.116.193	google-drive-web	alert



НАСТОЯЩИЙ NGFW: БЕЗОПАСНОЕ РАЗРЕШЕНИЕ ПРИЛОЖЕНИЙ

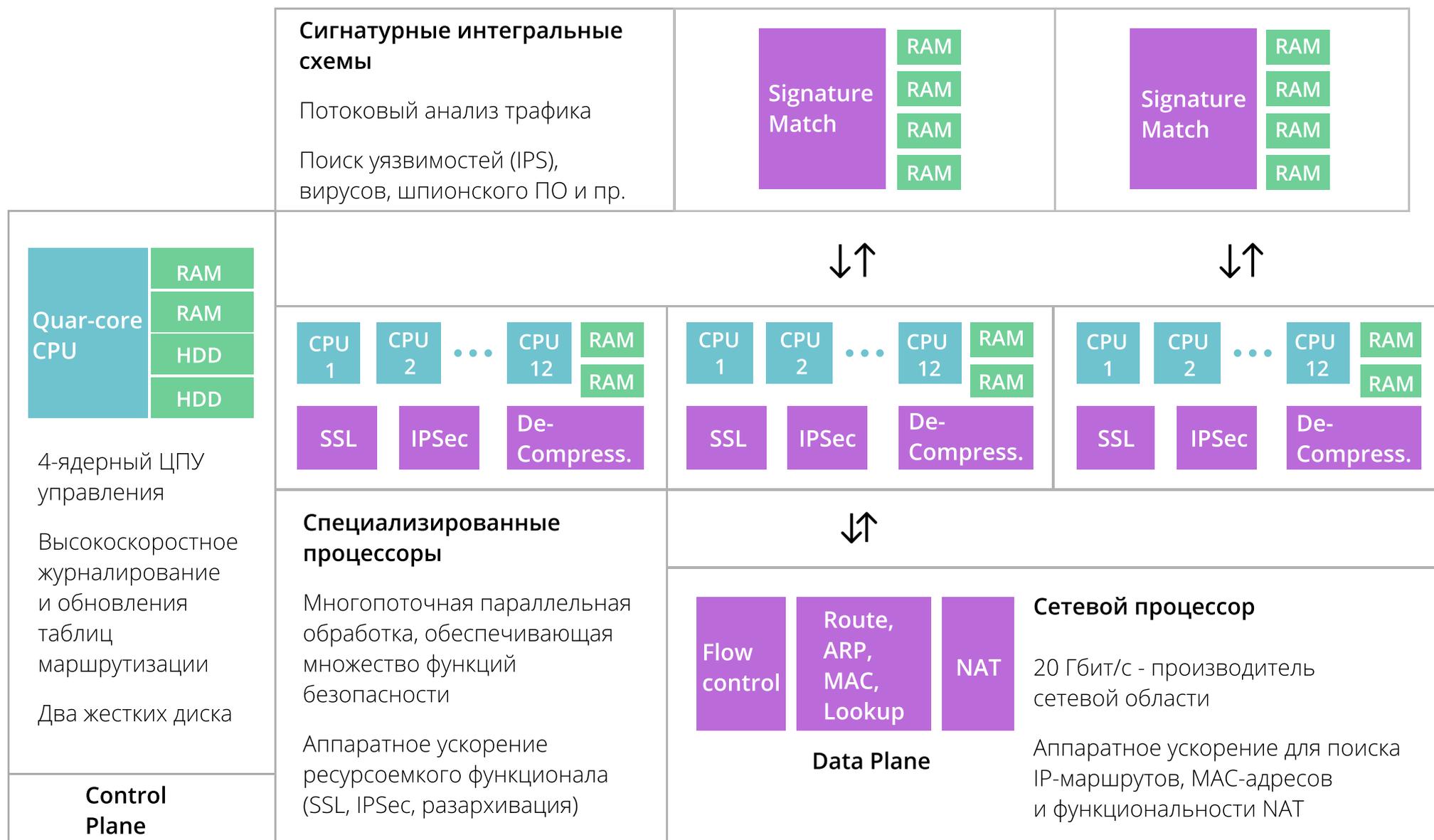
ОБНАРУЖЕНИЕ ИЗВЕСТНЫХ И НЕИЗВЕСТНЫХ УГРОЗ

Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	Severity
03/20 16:24:59	vulnerability	Microsoft Communicator INVITE Flood Denial of Service Vulnerability	Tap-Traffic	Tap-Traffic	192.168.1.123	192.168.2.28	5060	sip	alert	informational
03/20 15:45:31	spyware	DeepPanda.Gen Command And Control Traffic	Tap-Traffic	Tap-Traffic	202.86.190.3	192.168.180.20	1053	unknown-tcp	reset-both	critical
03/20 15:45:31	spyware	DeepPanda.Gen Command And Control Traffic	Tap-Traffic	Tap-Traffic	10.1.4.8	10.16.0.233	31121	web-browsing	reset-both	critical
03/20 15:45:25	vulnerability	Windows Command Reverse Shell Access	Tap-Traffic	Tap-Traffic	10.1.4.8	10.1.96.10	1090	unknown-tcp	alert	critical
03/20 15:45:24	vulnerability	HTTP SQL Injection Attempt	Tap-Traffic	Tap-Traffic	10.16.0.233	10.1.4.8	80	web-browsing	alert	medium
03/20 15:43:55	spyware	DeepPanda.Gen Command And Control Traffic	Tap-Traffic	Tap-Traffic	202.86.190.3	192.168.180.20	1053	unknown-tcp	reset-both	critical
03/20 15:43:55	spyware	DeepPanda.Gen Command And Control Traffic	Tap-Traffic	Tap-Traffic	10.1.4.8	10.16.0.233	31121	web-browsing	reset-both	critical
03/20 15:43:48	vulnerability	Windows Command Reverse Shell Access	Tap-Traffic	Tap-Traffic	10.1.4.8	10.1.96.10	1090	unknown-tcp	alert	critical
03/20 15:43:47	vulnerability	Oracle Java SE Remote Java Runtime Environment Remote Code Execution Vulnerability	Tap-Traffic	Tap-Traffic	192.168.111.201	192.168.111.129	1141	web-browsing	alert	critical
02/19 16:02:49	spyware	DeepPanda.Gen Command And Control Traffic	Tap-Traffic	Tap-Traffic	202.86.190.3	192.168.180.20	1053	unknown-tcp	reset-both	critical
02/19 16:02:49	spyware	DeepPanda.Gen Command And Control Traffic	Tap-Traffic	Tap-Traffic	10.1.4.8	10.16.0.233	31121	web-browsing	reset-both	critical
02/19 16:02:43	vulnerability	Windows Command Reverse Shell Access	Tap-Traffic	Tap-Traffic	10.1.4.8	10.1.96.10	1090	unknown-tcp	alert	critical
02/19 16:02:42	vulnerability	HTTP SQL Injection Attempt	Tap-Traffic	Tap-Traffic	10.16.0.233	10.1.4.8	80	web-browsing	alert	medium

Receive Time	Filename	Source Zone	Destination Zone	Attacker	Attacker Name	Victim	Dest. Port	Application	Rule	Category	Sender Address	Recipient Address	File Type
02/09 19:16:49	masthead_child-vfIR#406_swf	Untrust_...	VLAN17	173.194.113.66		172.16.17.10	49387	flash	allow_all	benign			flash
02/09 00:01:16	soundmanager2_flash9.swf	Untrust_...	VLAN16	111.67.30.225		172.16.16.30	51200	flash	test	benign			flash
02/08 23:55:14	MessageSenderV2.swf	Untrust_...	VLAN16	88.221.132.200		172.16.16.30	51279	flash	test	benign			flash
02/08 23:55:14	imgad	Untrust_...	VLAN16	173.194.112.26		172.16.16.30	51263	flash	test	benign			flash
02/08 23:55:14	imgad	Untrust_...	VLAN16	173.194.112.26		172.16.16.30	51263	flash	test	benign			flash
02/02 18:04:33	mightily.scr	Trust_LAN	Untrust_WAN1	10.10.20.50		74.125.140.116	443	google-docs-uploading	test	malicious			pe
02/02 18:04:14	mightily.scr	Trust_LAN	Untrust_WAN1	10.10.20.50		74.125.140.116	443	google-docs-uploading	test	malicious			pe

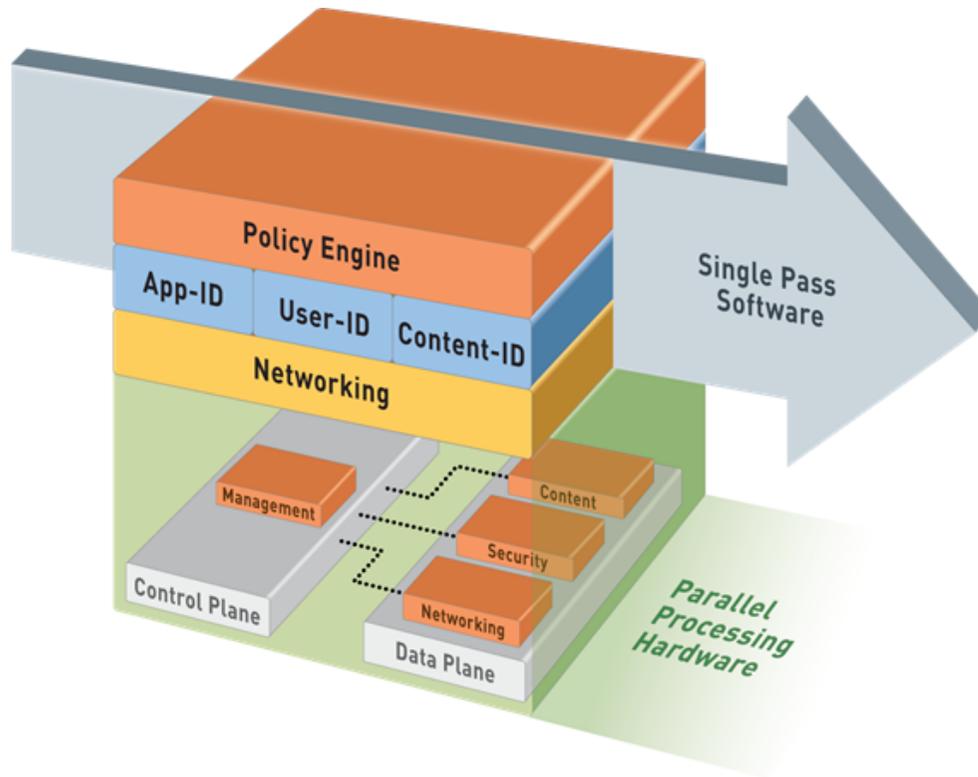
НАСТОЯЩИЙ NGFW: БЕЗОПАСНОЕ РАЗРЕШЕНИЕ ПРИЛОЖЕНИЙ

АРХИТЕКТУРА МЕЖСЕТЕВОГО ЭКРАНА НОВОГО ПОКОЛЕНИЯ PALO ALTO NETWORKS



НАСТОЯЩИЙ NGFW: БЕЗОПАСНОЕ РАЗРЕШЕНИЕ ПРИЛОЖЕНИЙ

АРХИТЕКТУРА ОДНОПРОХОДНОЙ ПАРАЛЛЕЛЬНОЙ ОБРАБОТКИ



Один проход

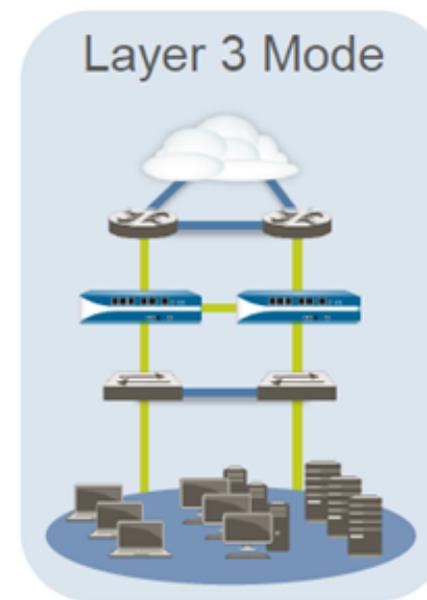
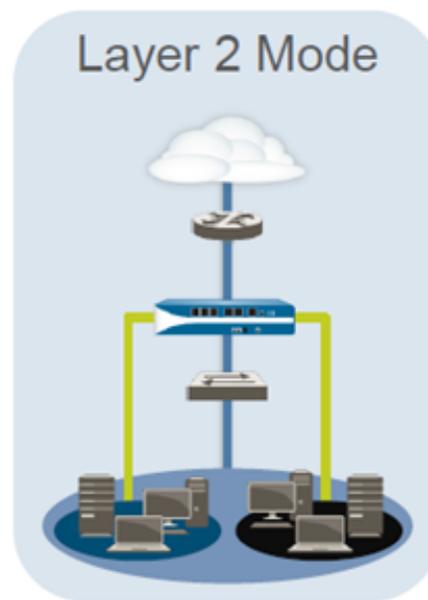
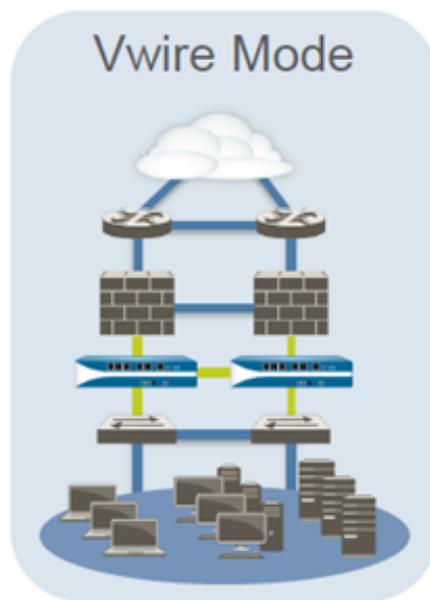
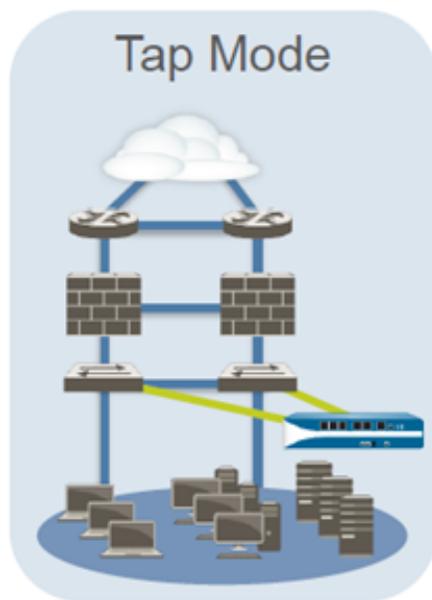
- Каждый пакет сканируется только один раз
- При сканировании одновременно определяется:
 - Приложение
 - Пользователь/группа
 - Контент – угрозы, URL и т.д.

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

Source Address	Source Host Name	Source User	Bytes
1 172.16.17.3	panat17.dobru.net		33.8 K
2 172.16.17.3	panat17.dobru.net	admin/jpna	85.7 M
3 172.16.16.26	efpynat01		4.7 K
4 192.168.201.148	192.168.201.148		3.3 K
5 172.16.17.20	adomnat01		13.1 M
6 192.168.201.244	192.168.201.244		395.9 K
7 192.168.201.4	192.168.201.4		797.4 K
8 192.168.201.2	192.168.201.2		1.4 M
9 192.168.201.8	192.168.201.8		878.0 K
10 192.168.201.8	192.168.201.8		1.4 M
11 192.168.201.8	192.168.201.8		1.2 K
12 192.168.201.8	192.168.201.8		334.0 K
13 192.168.201.8	192.168.201.8		192.1 K
14 192.168.201.8	192.168.201.8		137.2 K
15 192.168.201.8	192.168.201.8		410
16 192.168.201.8	192.168.201.8		253.8 K
17 192.168.201.8	192.168.201.8		291.2 K
18 192.168.201.238	192.168.201.238		52.4 K
19 192.168.201.37	192.168.201.37		294.4 K
20 192.168.201.144	192.168.201.144		374
21 192.168.201.142	192.168.201.142		263.3 K
22 192.168.201.33	192.168.201.33		212
23 192.168.201.2	192.168.201.2		79.3 K
24 172.16.16.30	efpynat01	admin/jpna	41.7 M



Risk	Application Name	Sessions	Bytes	Threats
2	msrp	3.6 K	4.2 M	0
2	msrp	1.5 K	12.8 M	0
3	dns	1.1 K	275.2 K	0
4	insufficient data	350	95.8 K	0
5	msrp	202	173.8 K	0
6	dns	80	193.8 K	0
7	msrp	69	25.1 K	0
8	web-browsing	67	2.3 M	0
9	msrp	25	1.2 M	0
10	msrp	19	66.7 K	0
11	msrp	15	2.3 K	0
12	google-dial-tone	1	1.3 M	0
13	msrp	1	270	0
14	google-advertising	2	353.1 K	0
15	tracroute	2	156	0
16	google-plus-feed	2	74.3 K	0
17	imgp	1	11.4 K	0
18	google-dial-tone	1	65.3 K	0
19	msrp	1	170.1 K	0

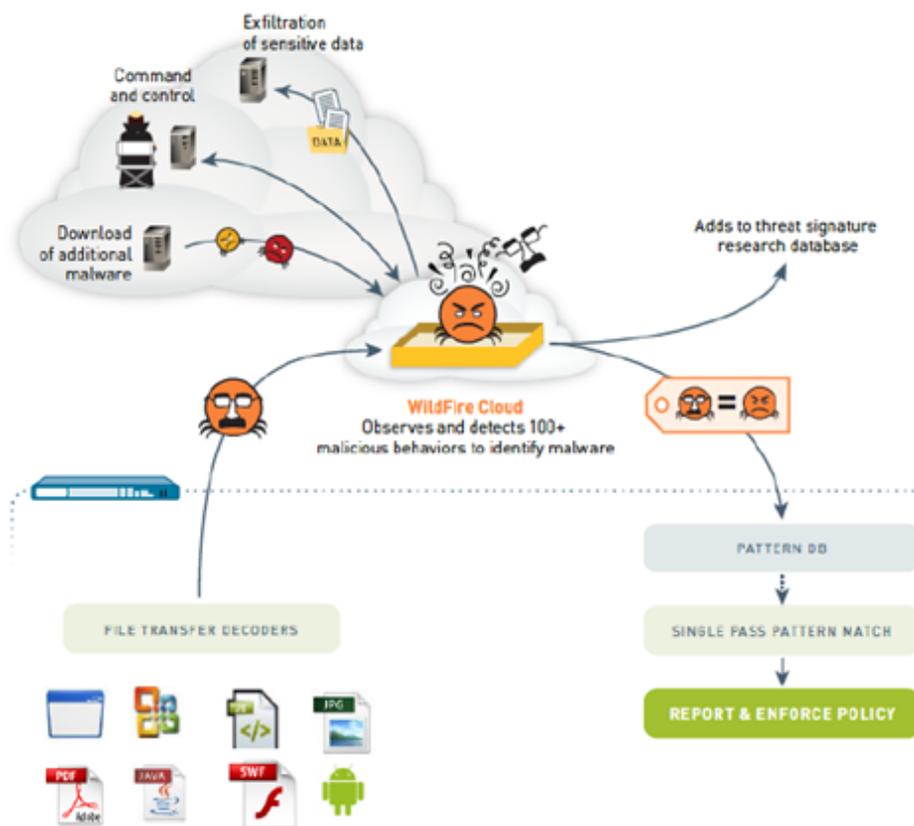
NGFW ПОД УПРАВЛЕНИЕМ PANORAMA

The screenshot displays the Palo Alto Networks Panorama web interface. The top navigation bar includes 'Dashboard', 'ACC', 'Monitor', 'Policies', 'Objects', 'Network', 'Device', and 'Panorama'. The 'Policies' tab is active, showing a list of security policies. The left sidebar contains a tree view of configuration categories: Security (Pre Rules, Post Rules, Default Rules), NAT (Pre Rules, Post Rules), QoS (Pre Rules, Post Rules), and Policy Based Forwarding (Pre Rules, Post Rules). The main content area shows a table of policies with columns for Name, Location, Tags, Type, Zone, Address, User, HIP Profile, Zone, Address, Application, and Service. Below this, a detailed view of the policy list is shown with columns for Name, Tags, Type, Zone, Address, User, HIP Profile, Zone, Address, Application, Service, Action, and Profile.

Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1 Block_FB	none	universal	any	any	any	any	any	any	facebook	application-d...	⊘	none
2 ForPetro_apps	VLAN16 Untrust_WAN1	universal	VLAN16	any	dobro\petro	any	Untrust_WAN1	any	browser-emails	any	⊘	none
3 ForPetro_url	VLAN16 Untrust_WAN1	universal	VLAN16	any	dobro\petro	any	Untrust_WAN1	any	any	any	⊘	none
4 SMBD_for_HR	VLAN16 Untrust_WAN1	universal	VLAN16 VLAN17	any	dobro\hr	any	Untrust_WAN1	any	mysql oracle postgres	any	✓	⊘
5 All access	VLAN17 Untrust_WAN1	universal	VLAN17	any	dobro\administrator	any	Untrust_WAN1	any	any	any	✓	⊘
6 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	✓	none
7 interzone-default	none	interzone	any	any	any	any	any	any	any	any	⊘	none

**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 вредоносных
- Сигнатура и обновление базы AV автоматически создается и загружается на все устройства в течение 15 мин.
- 1 сигнатура покрывает до 1500+ уникальных хэшей SHA
- WF-500 проверяет 4500 уникальных файлов в день: исполняемые, офисные, PDF

ДЕМОНСТРАЦИЯ РАБОТЫ WILDFIRE

Receive Time	Filename	Source Zone	Destination Zone	Attacker	Attacker Name	Victim	Desti... Port	Application	Rule	Category
02/02 15:56:09	winrar-x64-521b2.exe	Untrust_...	Trust_LAN	188.165.200.151		10.10.20.50	51190	web-browsing	test	benign
01/24 14:43:45	...3.docx	Untrust_...	VLAN16	173.194.113.106		172.16.16.30	51157	google-docs-base	All access	benign
01/24 14:43:45	...docx	Untrust_...	VLAN16	173.194.113.106		172.16.16.30	51156	google-docs-base	All access	benign
01/13 15:53:13	DefaultPack.EXE	Untrust_...	Trust_LAN	88.221.132.131		10.10.20.6	49602	web-browsing	fromTrust_LAN	benign
02/02 18:04:33	mightily.scr	Trust_LAN	Untrust_WAN1	10.10.20.50		74.125.140.116	443	google-docs-uploading	test	malicious

WildFire Analysis Summary

File Information

- File Type: PE
- File Signer: [Redacted]
- SHA-256: 637cc5fdbb7a36182083b56cfb4beaf172de0643c275ad3eb030b502240662c
- SHA1: 5de9ca37e413fac24713d9374481ea438c6aff57
- MD5: 68e4fc3e3b227f36d1fdecbbac6b2d3c
- File Size: 29696 bytes
- First Seen Timestamp: 2015-01-30 17:12:53 UTC
- Verdict: **malware**
- Sample File: [Download File](#)

Coverage Status

For endpoint anti-virus coverage information for this sample, visit [VirusTotal](#)

Dynamic Analysis

PCAP	Receive Time	Log	Type	Application	Action	Rule	Bytes	Packets	Severity	Category	URL/File Name
	2015/02/02 18:05:07	TRAFFIC	end	google-docs-uploading	allow	test	86454	91		online-storage-and-backup	
	2015/02/02 18:04:38	THREAT	virus	google-docs-uploading	deny	test			medium	any	pxawkf.exe
	2015/02/02 18:04:38	THREAT	file	google-docs-uploading	forward	test			low	any	mightily.scr

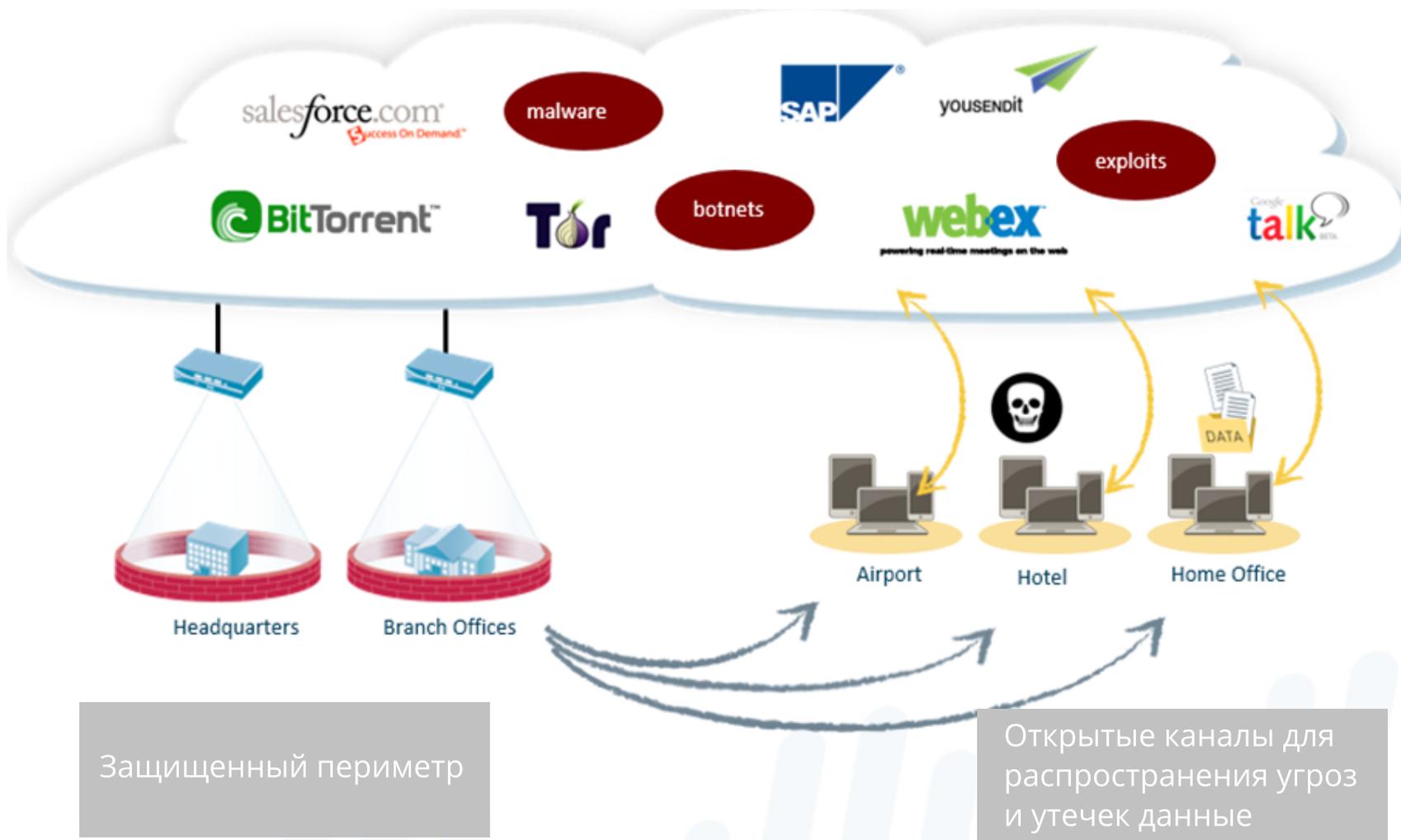
Отчет по работе WildFire

Можно скачать готовый отчет

Доступ на скачивание malware

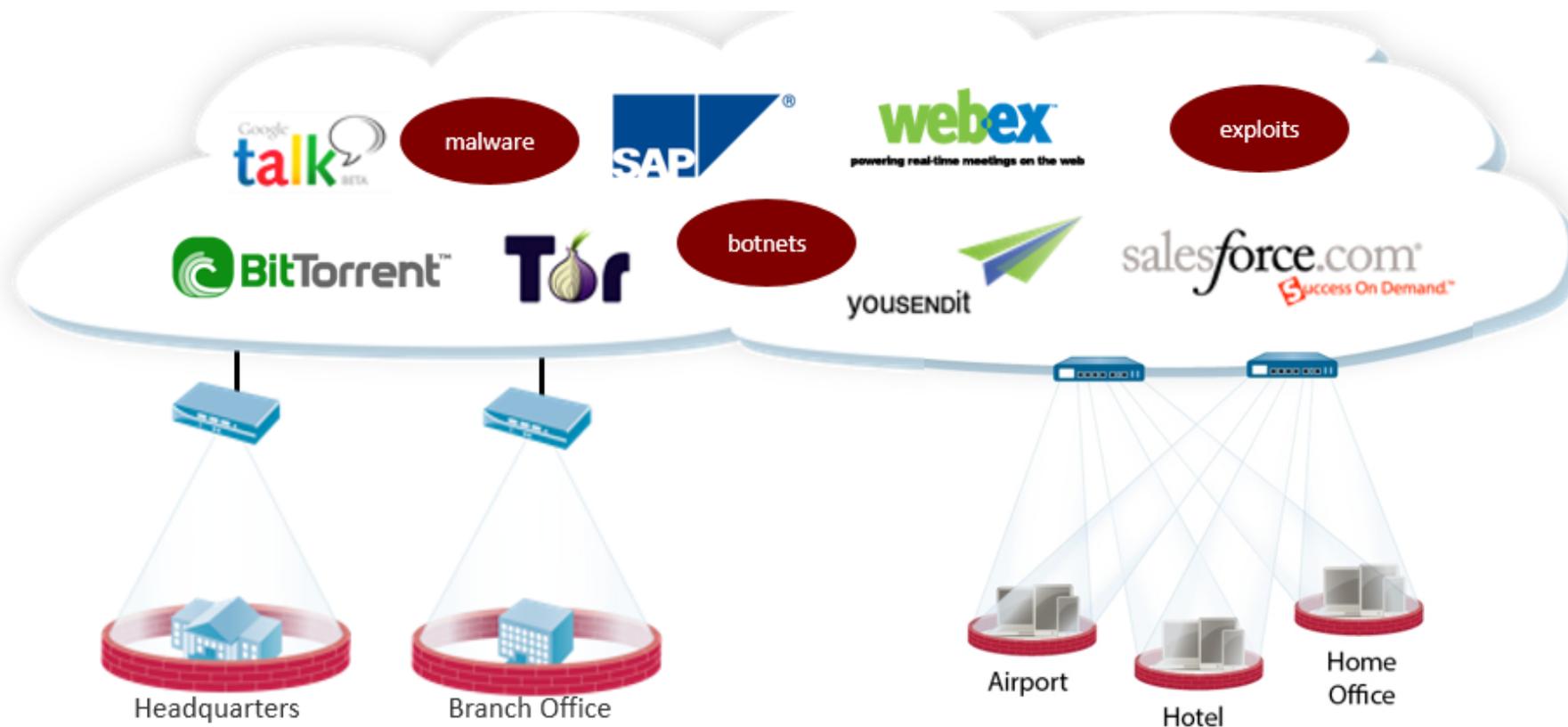
**GLOBAL
PROTECT**

СОВРЕМЕННАЯ КАРТИНА БЕЗОПАСНОСТИ В ЗАВИСИМОСТИ ОТ МЕСТА НАХОЖДЕНИЯ РАБОЧЕЙ СТАНЦИИ



**ЧТО МОЖНО
ИЗМЕНИТЬ ЕСЛИ
ЕСТЬ GLOBAL
PROTECT ?**

ПОЛНАЯ БЕЗОПАСНОСТЬ И КОНТРОЛЬ УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ

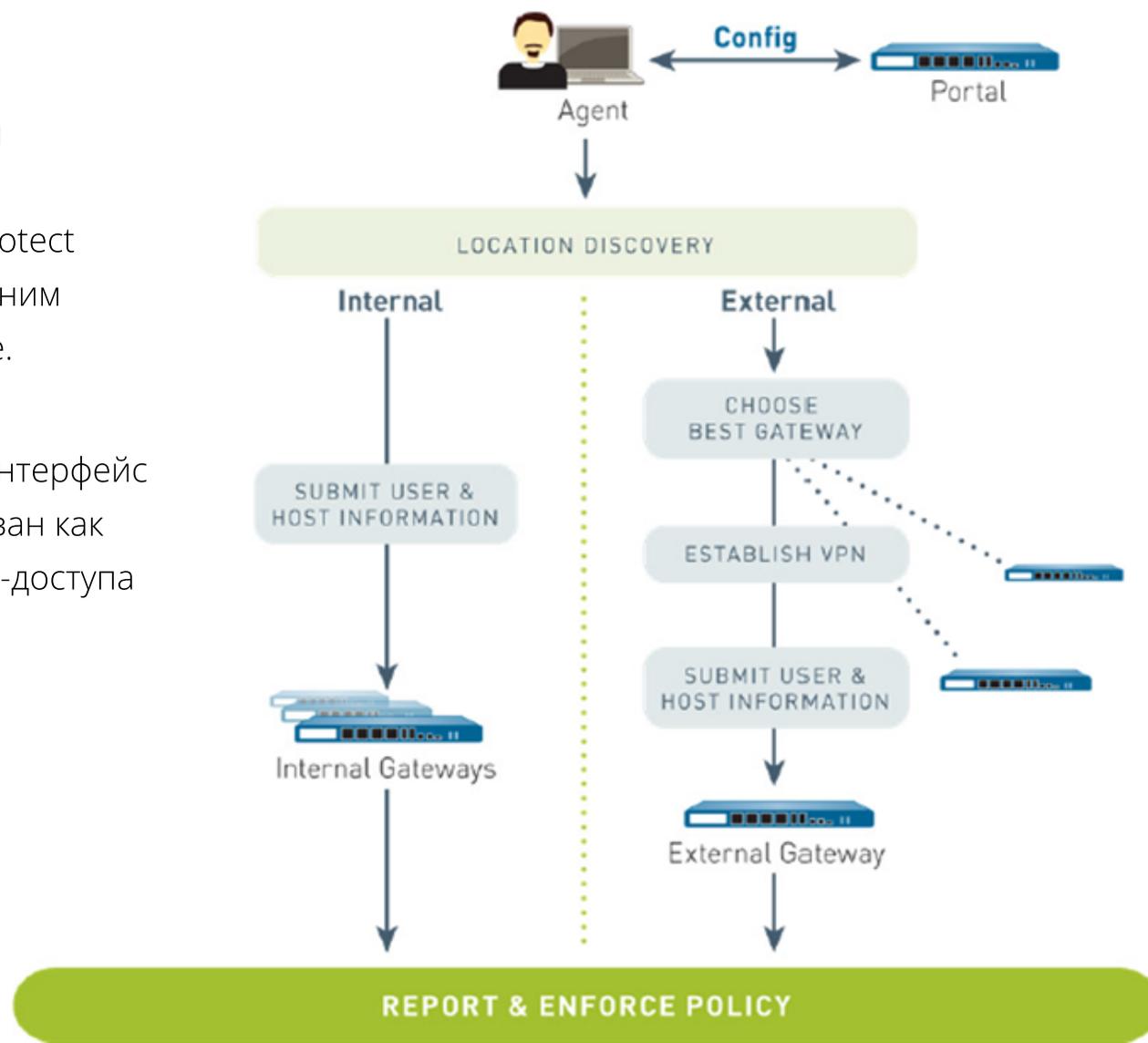


- VPN-соединение к соответствующему настроенному фаерволу который выполняет всю работу по обеспечению безопасности
- Автоматическое защищенное соединение для внутренних и внешних пользователей
- Единая политика контроля, гарантированная прозрачность трафика и встроенная отчетность

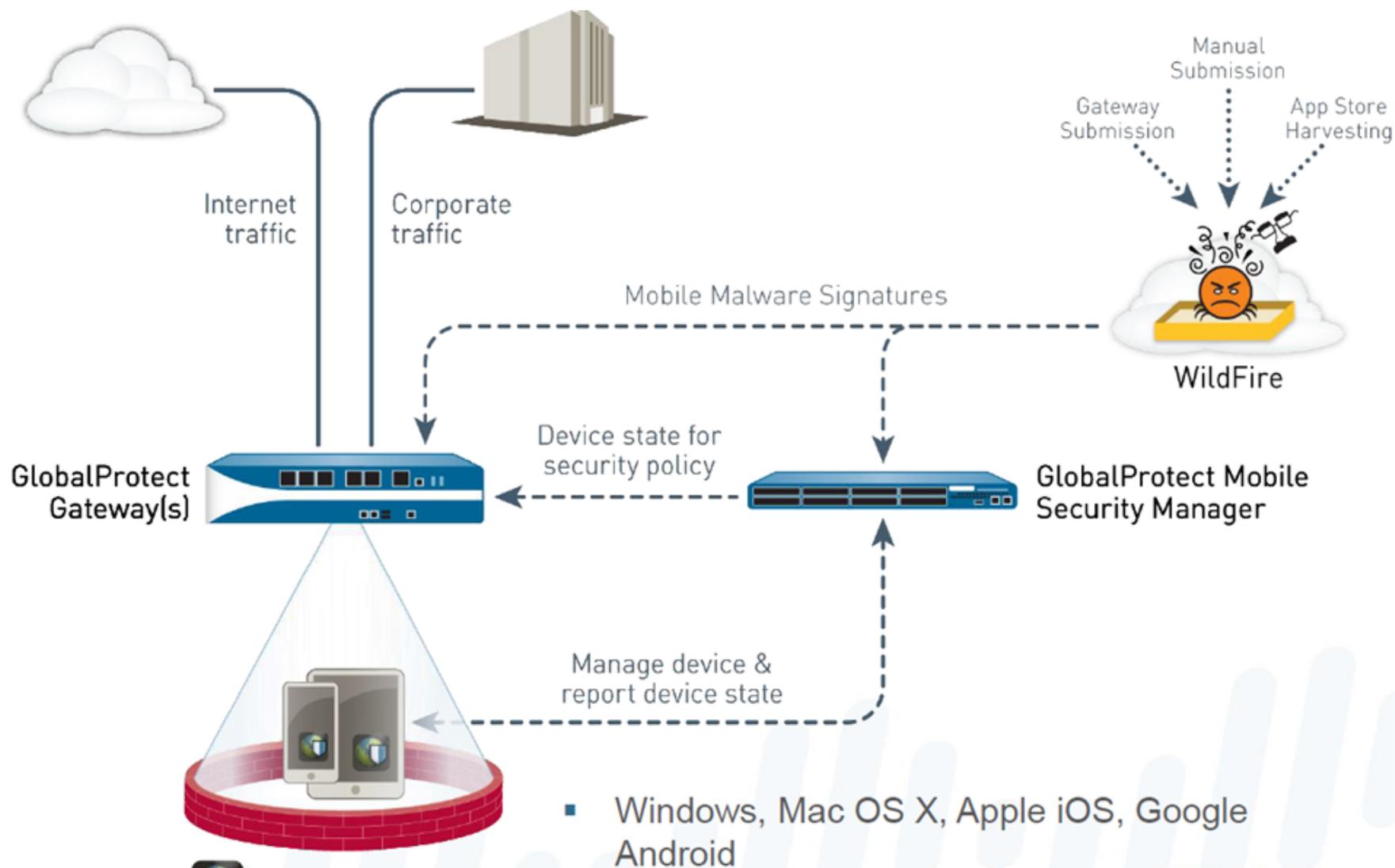
КАК РАБОТАЕТ GLOBAL PROTECT?

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)





the network security company™