

Визуализация взломов в собственной сети



Денис Батранков
консультант по ИБ, CISSP, CNSE
Palo Alto Networks
russia@paloaltonetworks.com





slideshare-uploading

application function

PowerPoint

file type

slideshare

application

“Confidential and
Proprietary”

content

marketing

group

HTTP

protocol

file-sharing

URL category

rivanov

user

SSL

protocol

canada

destination country

172.16.1.10

source IP

TCP/443

destination port

64.81.2.23

destination IP

344KB

EXE

file type

web-browsing

application

shipment.exe

file name

finance

group

HTTP

protocol

unknown

URL category

ipetrov

user

SSL

protocol

china

destination country

172.16.1.10

source IP

TCP/443

destination port

64.81.2.23

destination IP

Shadow IT – несанкционированные информационные ресурсы и компоненты

Опросили 129 ИТ руководителей привести примеры Shadow IT:

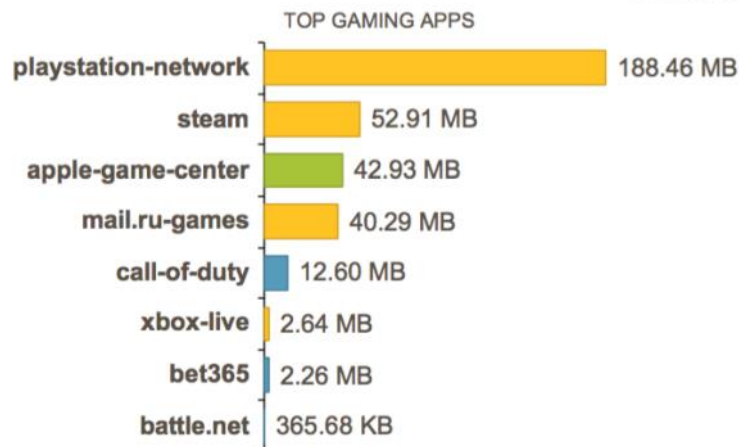
- макросы в Excel 19%
- **программные продукты 17%**
- **облачные приложения 16%**
- ERP 12%
- системы BI 9%
- веб-сайты 8%
- аппаратные устройства 6%
- неучтенный VoIP 5%

Много заказчиков удивляются отчетом по приложениям

Gaming - 342.5MB

14 ■ 21

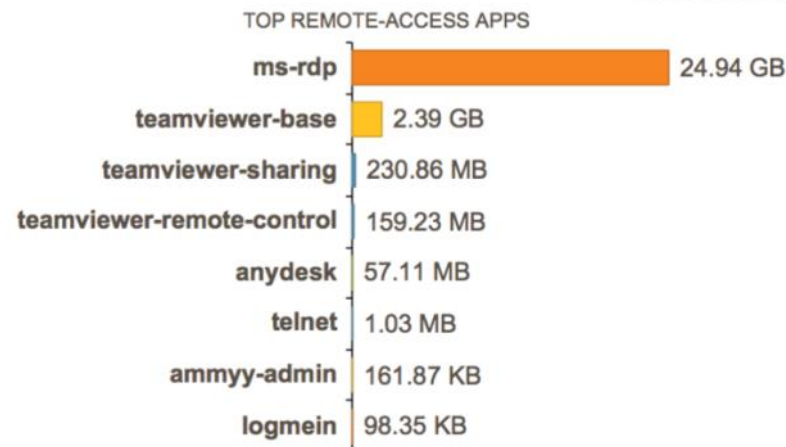
APPLICATION VARIANTS
VS INDUSTRY AVERAGE



Remote-Access - 27.77GB

10 ■ 30

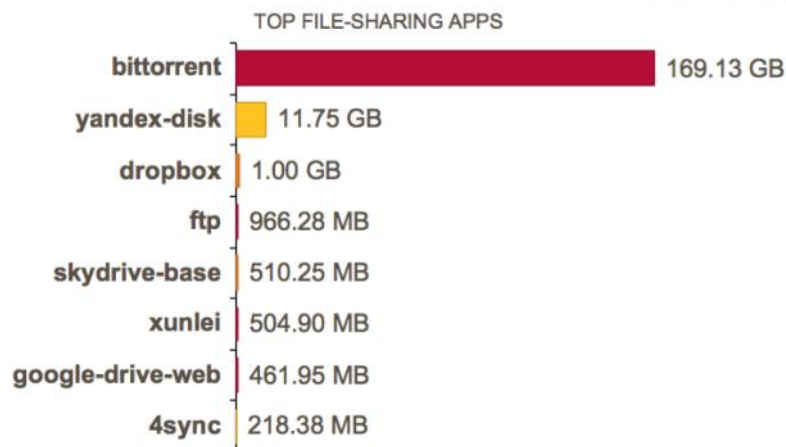
APPLICATION VARIANTS
VS INDUSTRY AVERAGE



File-Sharing - 184.79GB

28 ■ 65

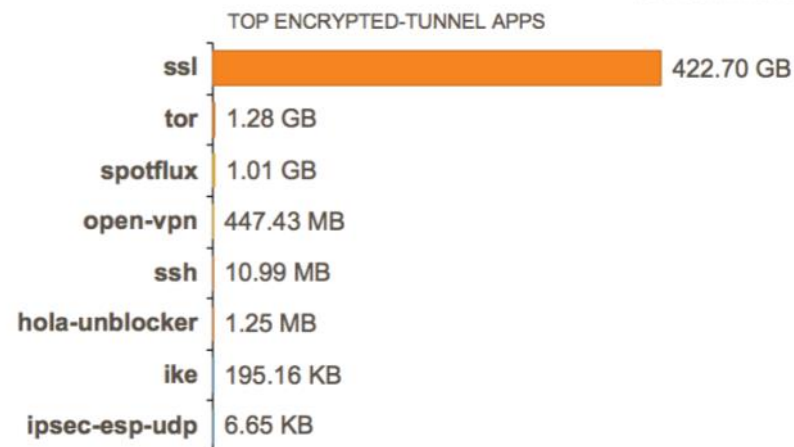
APPLICATION VARIANTS
VS INDUSTRY AVERAGE



Encrypted-Tunnel - 425.44GB

10 ■ 19

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

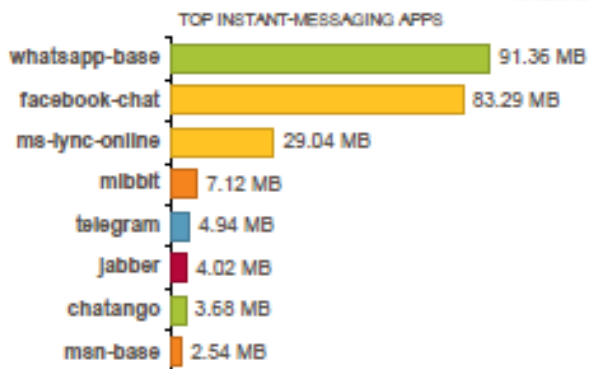


Лучше один раз увидеть

Applications that Introduce Risk (Continued)

Instant-Messaging - 227.04MB

12 10
APPLICATION VARIANTS
VS INDUSTRY AVERAGE



Social-Networking - 1.28GB

14 17
APPLICATION VARIANTS
VS INDUSTRY AVERAGE

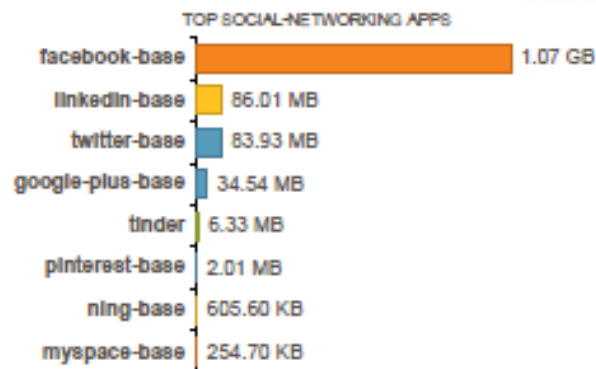
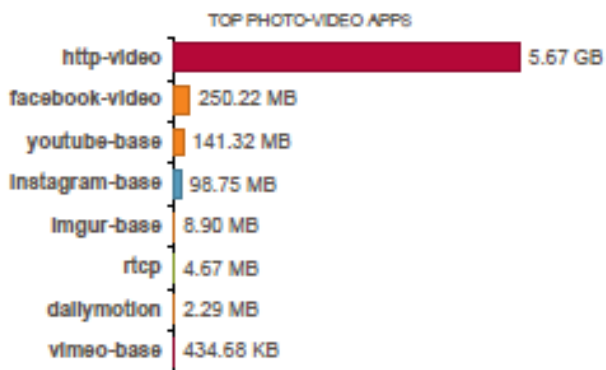


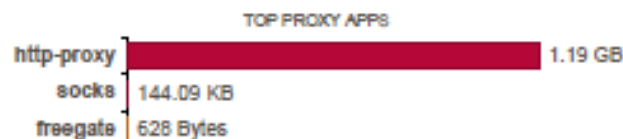
Photo-Video - 6.16GB

13 23
APPLICATION VARIANTS
VS INDUSTRY AVERAGE



Proxy - 1.19GB

3 2
APPLICATION VARIANTS
VS INDUSTRY AVERAGE

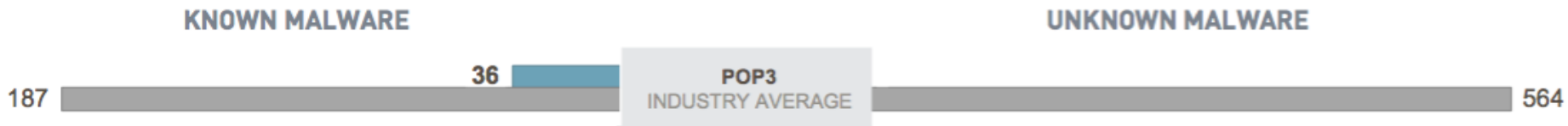
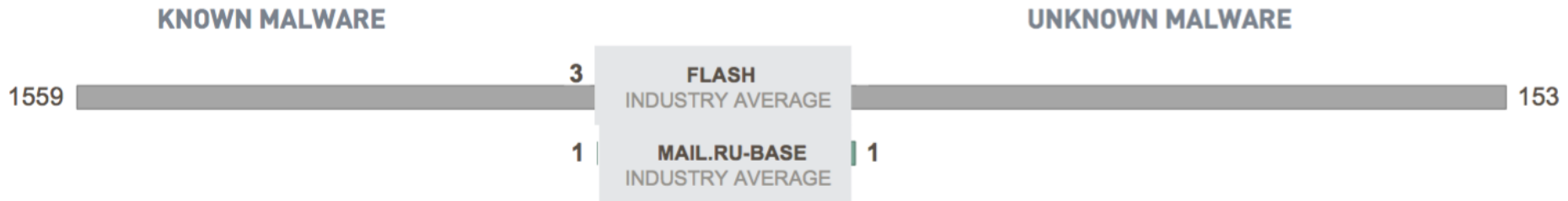
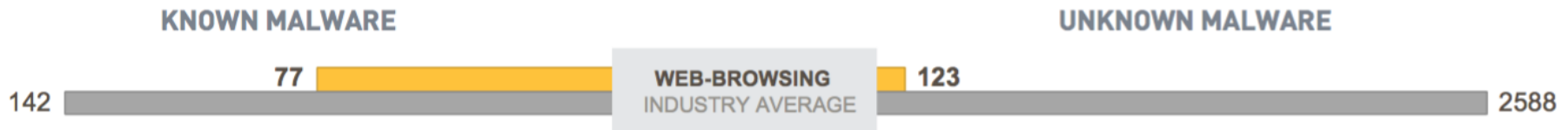


SLR позволяет показать приложения, вирусы, атаки, бот-сети

Security Lifecycle Report (SLR)



Сколько вирусов не знает ваш антивирус?

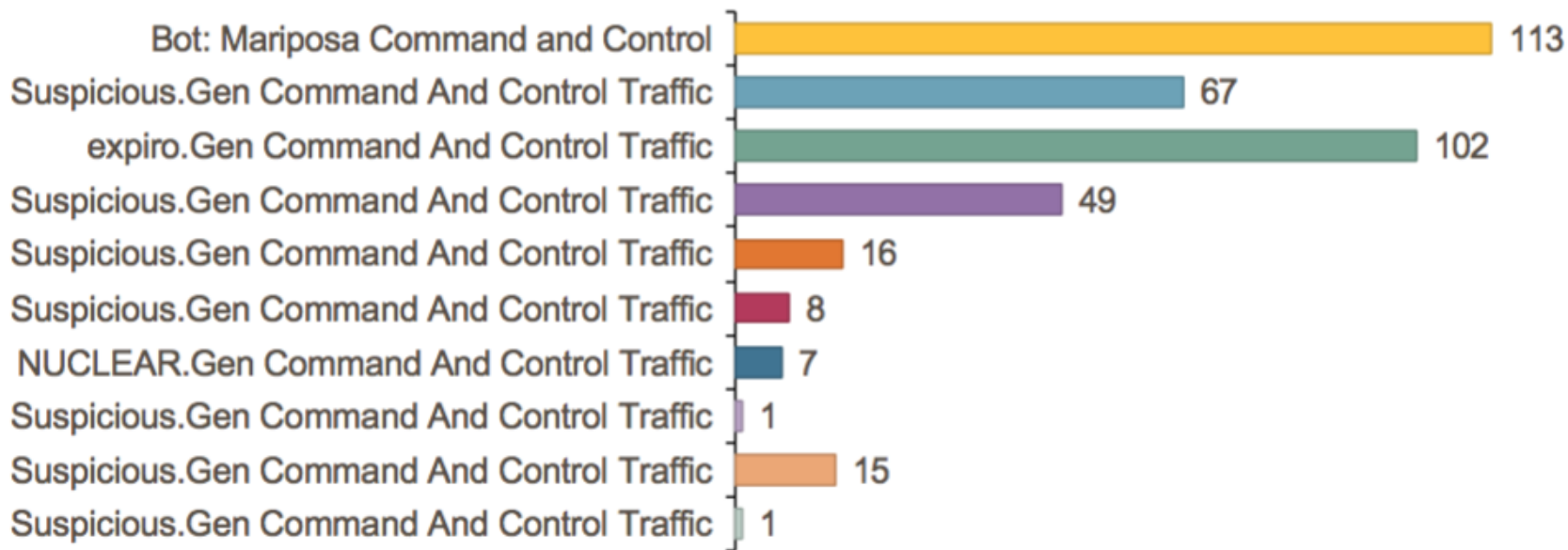


Проверка файлов в песочнице
Wildfire = 5 минут на определение

Сколько компьютеров в бот-сети?

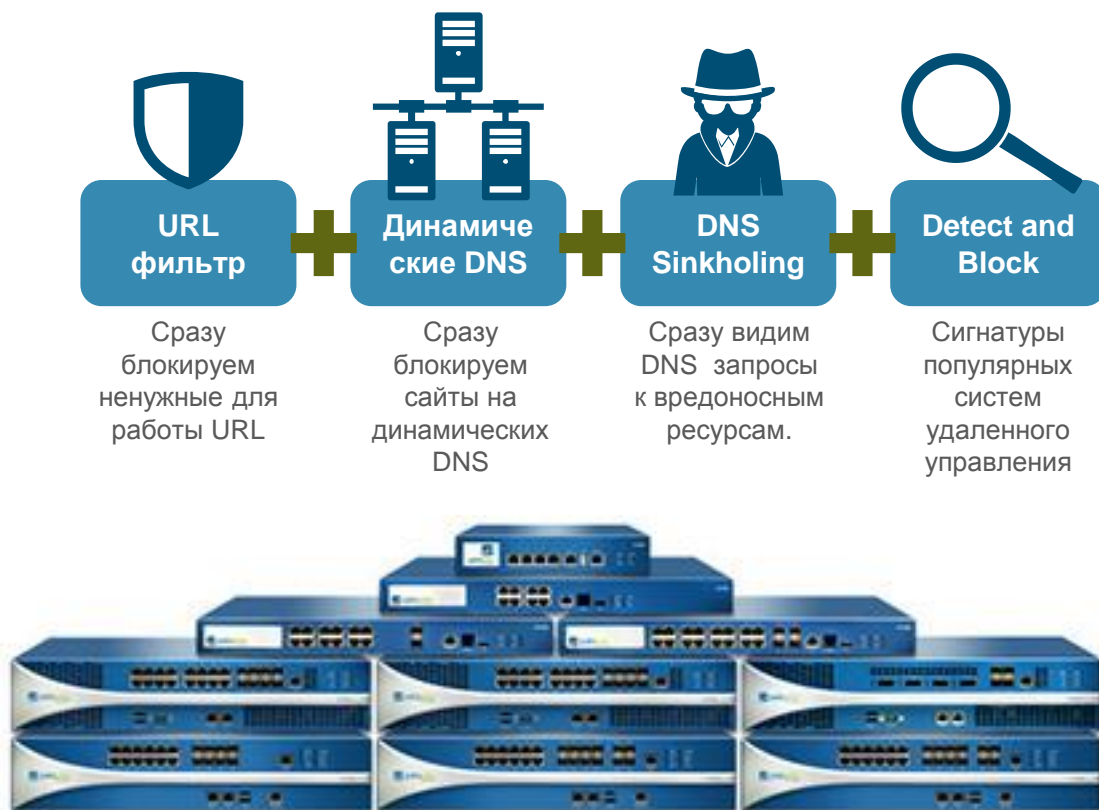
Шпионское ПО, осуществляющее соединение с внешними узлами 2,606

Рисунок ниже демонстрирует взломанные хосты, которые осуществляют попытки соединения с подозрительными внешними серверами.



✓ Threat Intelligence = блокировка центров управления и скачивания malware

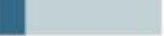
URL категория - malware,
DNS Sinkholing,
Anti-Spyware



Кто из сотрудников пользуется SaaS?



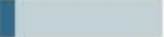
evernote-base: 672.5M

114.1M ↓  558.4M ↑

Risk: 2



windows-azure-base: 667.9M

71.2M ↓  596.8M ↑

Risk: 1



ms-onedrive-base: 499.5M

150.3M ↓  349.2M ↑

Risk: 4



icloud-mail: 489.1M

462.6M ↓  26.5M ↑

Risk: 2



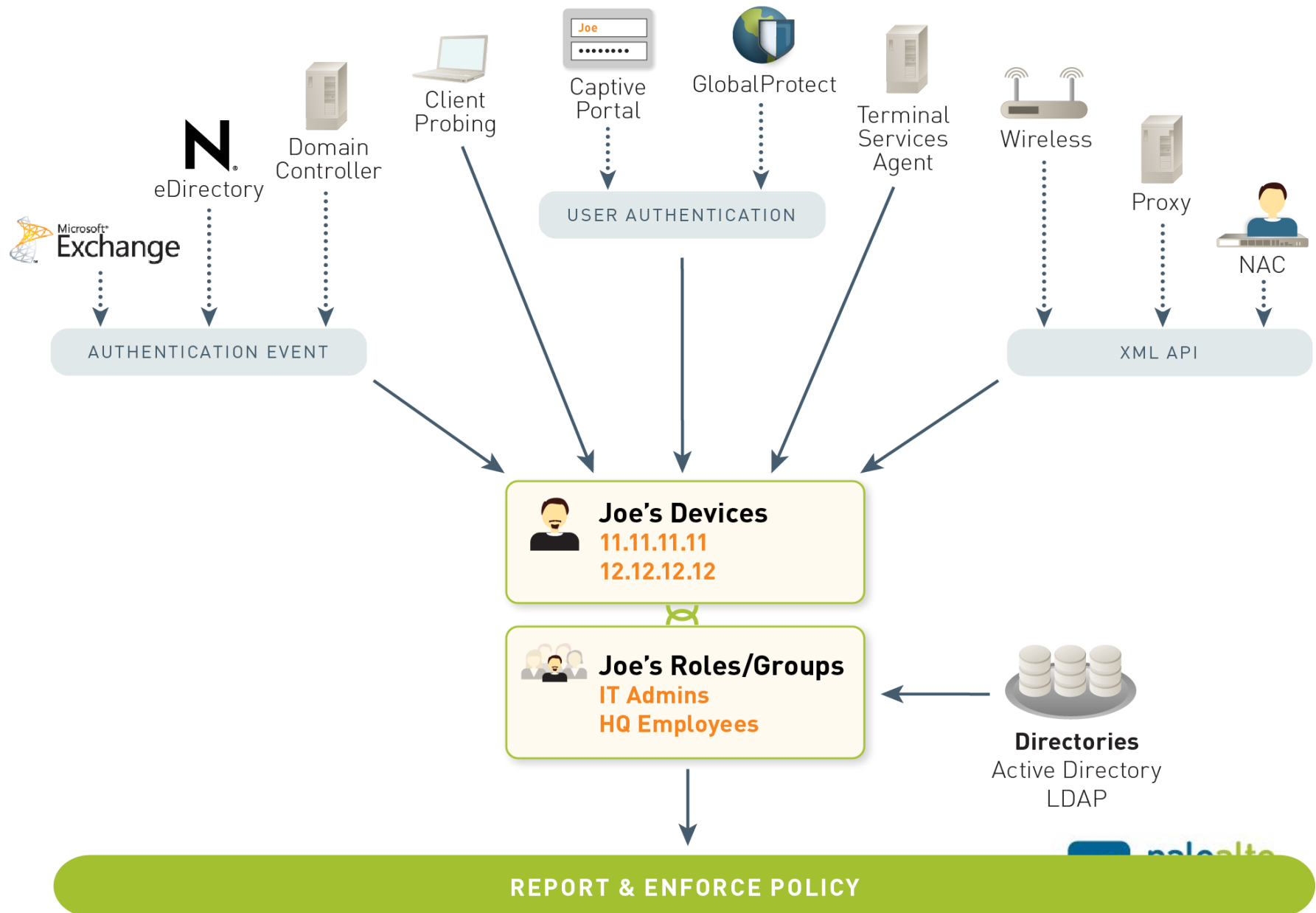
gmail-base: 367.0M

48.3M ↓  318.7M ↑

Risk: 4



User-ID позволяет сопоставить IP и аккаунт



Ваши средства мониторинга видят сеть вот так?

Много
трафика
по порту
80

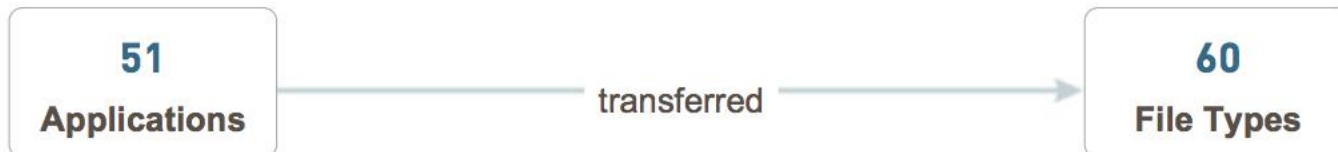
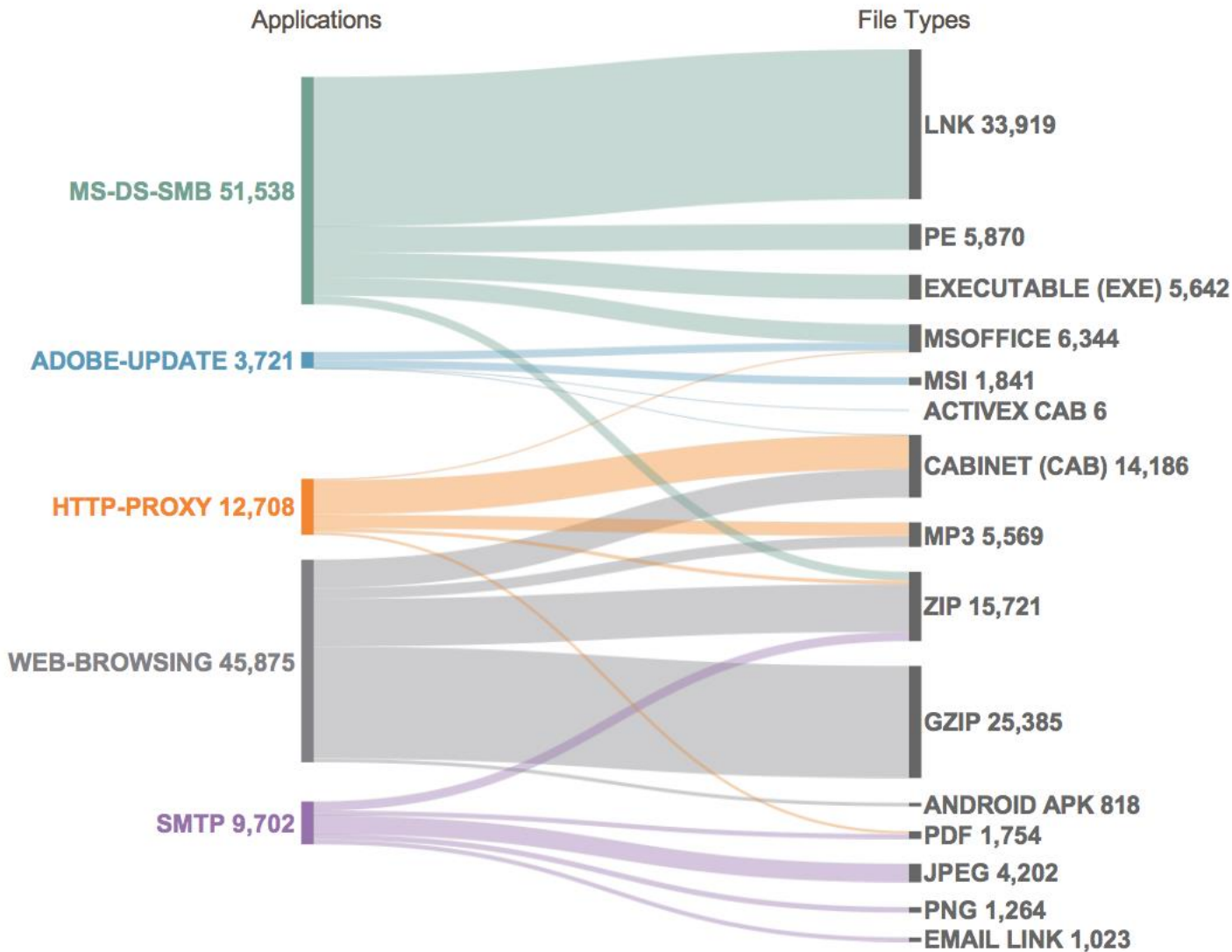
Много
трафика
по порту
21

Много
трафика
по порту
53

Много
трафика
по порту
25

Вы знаете что по сети передают данные 200-400 приложений?





Мода на квесты? У нас есть Ultimate Test Drive

Лабораторная работа с инструктором Palo Alto Networks.

Как самому попробовать? Легко!



- Все уже установлено на виртуальных машинах – осталось запустить

	Ultimate Test Drive - Advanced Endpoint Protection Workshop	5 Machines	9 CPU	210.0 GB Disk	12.0 GB RAM	Add >
	Ultimate Test Drive - Migration Process Workshop	3 Machines	4 CPU	85.0 GB Disk	7.0 GB RAM	Add >
	Ultimate Test Drive - Network Security Management Workshop	6 Machines	12 CPU	228.0 GB Disk	18.5 GB RAM	Add >
	Ultimate Test Drive - Next-Generation Firewall Workshop	5 Machines	6 CPU	125.0 GB Disk	11.5 GB RAM	Add >
	Ultimate Test Drive - Threat Prevention Workshop Welcome to the	5 Machines	6 CPU	141.0 GB Disk	9.5 GB RAM	Add >
	Ultimate Test Drive - Virtualized Datacenter Workshop	7 Machines	26 CPU	535.0 GB Disk	38.1 GB RAM	Add >

TRAPS

Лучше антивируса

Migration Tool

Firewall -> NGFW

Panorama

Управление NGFW

NGFW

URL,AV,IPS,APP, ...

NGFW+TRAPS

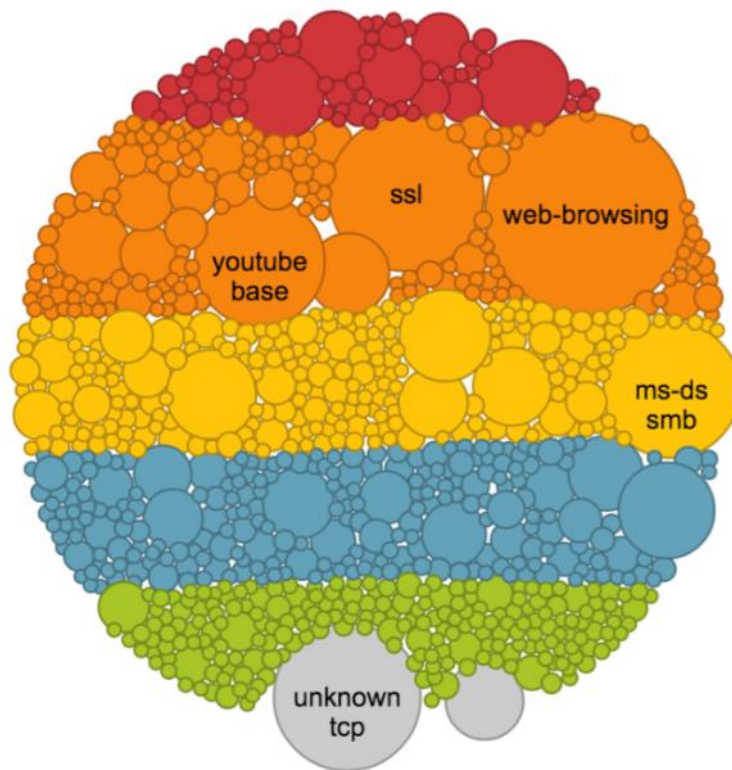
NSX, vCenter, ESXi

Защита виртуализации



Какие задачи решает NGFW для ИТ

- ✓ Switching, Routing, VLAN, Trunks, Policy Based Routing, VPN



- ✓ **Визуализация** ВСЕХ приложений по стандартным и нестандартным портам стека TCP/IP
- ✓ Просмотр и контроль действий пользователей
- ✓ Mobile Device Management и HIP

Какие задачи решает NGFW для ИБ

Новые правила на основе

- ✓ приложений
- ✓ имен/групп AD
- ✓ URL категорий
- ✓ типов файлов

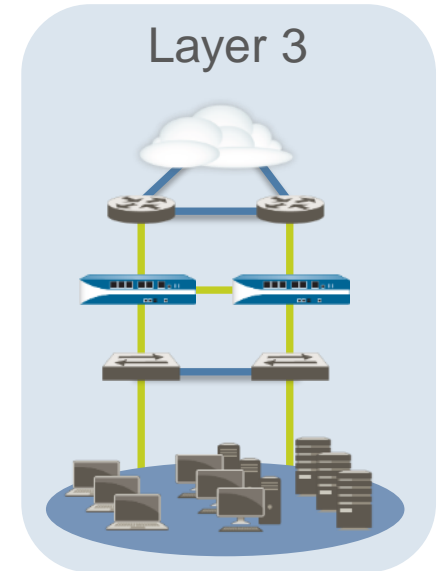
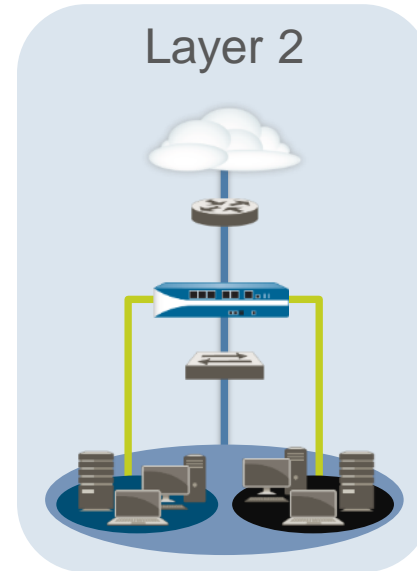
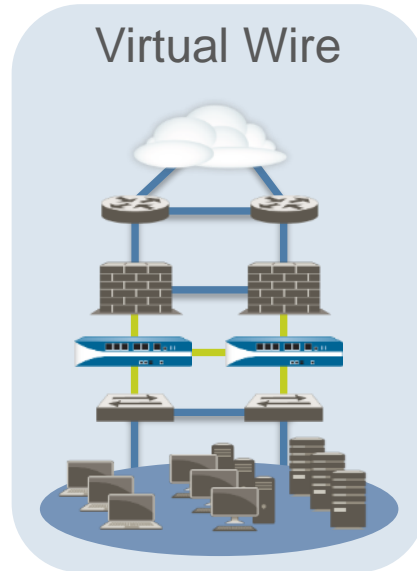
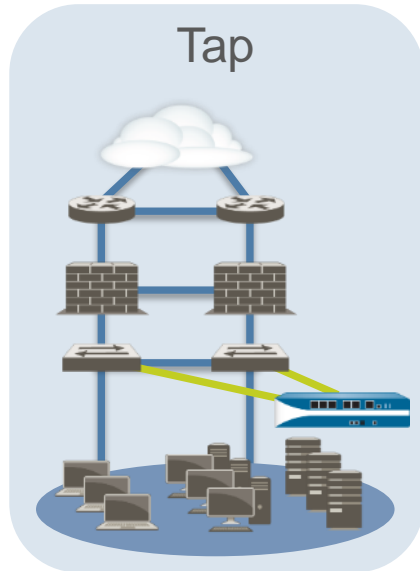
Единая точка контроля

- ✓ VPN
- ✓ Антивирус
- ✓ IPS
- ✓ URL категории
- ✓ Песочница
- ✓ Threat Intelligence
- ✓ DNS Sinkholing
- ✓ Туннелирование/обход firewall

Пример атак хакеров на Positive Hack Days 2017

Threat Name	ID	Threat Type	Threat Catego...	Severity	Count
PHP Remote File Include Vulnerability	33327	vulnerability	code-execution	medium	1.3k
SMB: User Password Brute Force Attempt	40004	vulnerability	brute-force	high	967
HTTP Directory Traversal Vulnerability	30844	vulnerability	info-leak	low	892
HTTP Cross Site Scripting Attempt	32658	vulnerability	code-execution	low	505
Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability	30921	vulnerability	code-execution	high	184
HTTP SQL Injection Attempt	30514	vulnerability	sql-injection	medium	127
Bash Remote Code Execution Vulnerability	36729	vulnerability	code-execution	critical	123
Adobe ColdFusion Multiple Directory Traversal Vulnerabilities	33452	vulnerability	code-execution	high	88
Generic HTTP Cross Site Scripting Attempt	31476	vulnerability	code-execution	high	78
HTTP /etc/passwd access attempt	35107	vulnerability	info-leak	high	76
Apache HTTP Server Reverse Proxy Security Bypass Vulnerability	34485	vulnerability	info-leak	medium	63
HTTP SQL Injection Attempt	36248	vulnerability	sql-injection	low	49
PHP CGI Query String Parameter Handling Information Disclosure and DoS Vulnerability	34804	vulnerability	dos	medium	46
Oracle 9i Application Server Dynamic Monitoring Services Anonymous Access	33756	vulnerability	info-leak	medium	34
FTP Protocol Evasion Application Detection	39826	vulnerability	protocol-anomaly	low	31
Microsoft Windows win.ini access attempt	30851	vulnerability	info-leak	high	28
phpBB viewtopic.php Highlighting Feature Arbitrary PHP Code Execution Vulnerability	30092	vulnerability	code-execution	critical	28
Microsoft IIS Escaped Characters Decoding Command Execution Vulnerability	30444	vulnerability	code-execution	critical	26
HTTP Cross Site Scripting Vulnerability	35864	vulnerability	code-execution	critical	23
HTTP SQL Injection Attempt	35823	vulnerability	sql-injection	medium	22
Joomla Visites Component Remote File Include Vulnerability	34439	vulnerability	info-leak	critical	22
HTTP SQL Injection Attempt	35826	vulnerability	sql-injection	medium	21
HTTP SQL Injection Attempt	37845	vulnerability	sql-injection	low	18
PHPMoAdmin Object Parameter Handling Code Execution Vulnerability	37765	vulnerability	code-execution	high	16
PHPMoAdmin Unauthorized Remote Code Execution Vulnerability	37494	vulnerability	code-execution	critical	16
Oracle 9i HTTP Server OWA_UTIL Stored Procedures Information Disclosure Vulnerability	33779	vulnerability	info-leak	medium	14
HTTP SQL Injection Attempt	36241	vulnerability	sql-injection	medium	14
UNIX Portmapper Remote Information Retrieving Attempt	32796	vulnerability	info-leak	low	12
Microsoft IIS Sample Scripts Arbitrary File Disclosure Vulnerability	30323	vulnerability	info-leak	medium	12
WMNews index.php base_datapath Parameter PHP File Include Vulnerability	22604	vulnerability	code-execution	high	12

Интеграция NGFW в сетевую инфраструктуру



OSPF RIP BGP PBF PIM-SM/SMM IGMP IPv6 NAT VLAN LACP VPN QoS

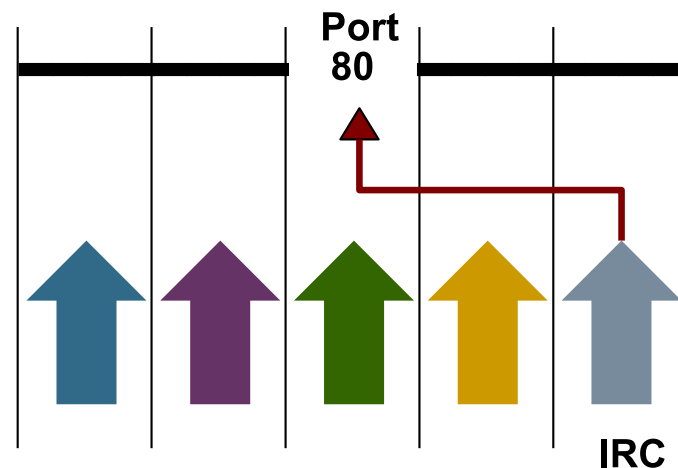
- Порт Tap = SPAN порт – для аудита или составления отчетов
- Порт Virtual Wire = фильтрующий мост, самое легкое внедрение в сеть
- Порт L2 = свитч, поддержка VLAN и VLAN трансляции
- Порт L3 = маршрутизатор, поддержка RIP, OSPF, BGP, Multicast



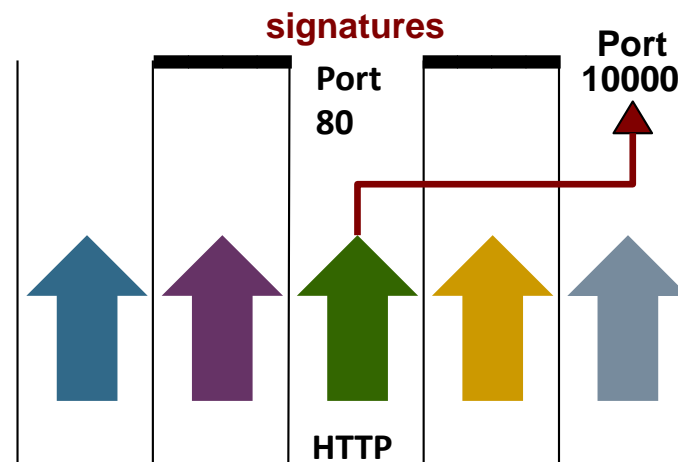
Какие есть способы обхода сетевой защиты?

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



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



Туннелирование поверх DNS

Примеры

- tcp-over-dns
- dns2tcp
- Iodine
- Heyoka
- OzymanDNS
- NSTX

DNS	91 57916	53	Standard query TXT	AAAAAAh5AA.=auth.ec2.mui
DNS	213 53	57916	Standard query response TXT	
DNS	144 57916	53	Standard query TXT	2XKBgAABADFFNkQzMUNGOEE1
DNS	245 53	57916	Standard query response TXT	
DNS	98 57916	53	Standard query TXT	2XI7KiF1AHNzaA.=connect.
DNS	199 53	57916	Standard query response TXT	
DNS	85 57916	53	Standard query TXT	2XIAAAABBA.ec2.muides.co
DNS	240 53	57916	Standard query response TXT	
DNS	85 57916	53	Standard query TXT	2XIAAQACBA.ec2.muides.co
DNS	113 57916	53	Standard query TXT	2XIAAADCFNTSC0yLjAtT3Bl
DNS	85 57916	53	Standard query TXT	2XIAAAEBA.ec2.muides.co
DNS	253 57916	53	Standard query TXT	2XIAAAFCAAAaxQIFPLjhQeS
DNS	85 57916	53	Standard query TXT	2XIAAAAGBA.ec2.muides.co

Authority RRs: 1
Additional RRs: 1
▸ Queries
▼ Answers
▼ AAAAAAh5AA.=auth.ec2.muides.com: type TXT, class IN
Name: AAAAAAh5AA.=auth.ec2.muides.com
Type: TXT (Text strings)
Class: IN (0x0001)
Time to live: 3 seconds
Data length: 34
Text: A2XIAAAh5ADA5VzNLWkdJNONLREwzREc
text:

Использование рекурсивных запросов для передачи инкапсулированных сообщений по TCP в запросах удаленному DNS серверу и ответах клиенту

Две стороны одного протокола SSL

Good?

BlackPOS

Bad?

facebook.

webex
powering real-time meetings on the web

Citadel



ultrasurf



salesforce.com
Success On Demand.™

TDL-4

Aurora



Tor

Rustock



Dropbox



Poison IVY



Ramnit

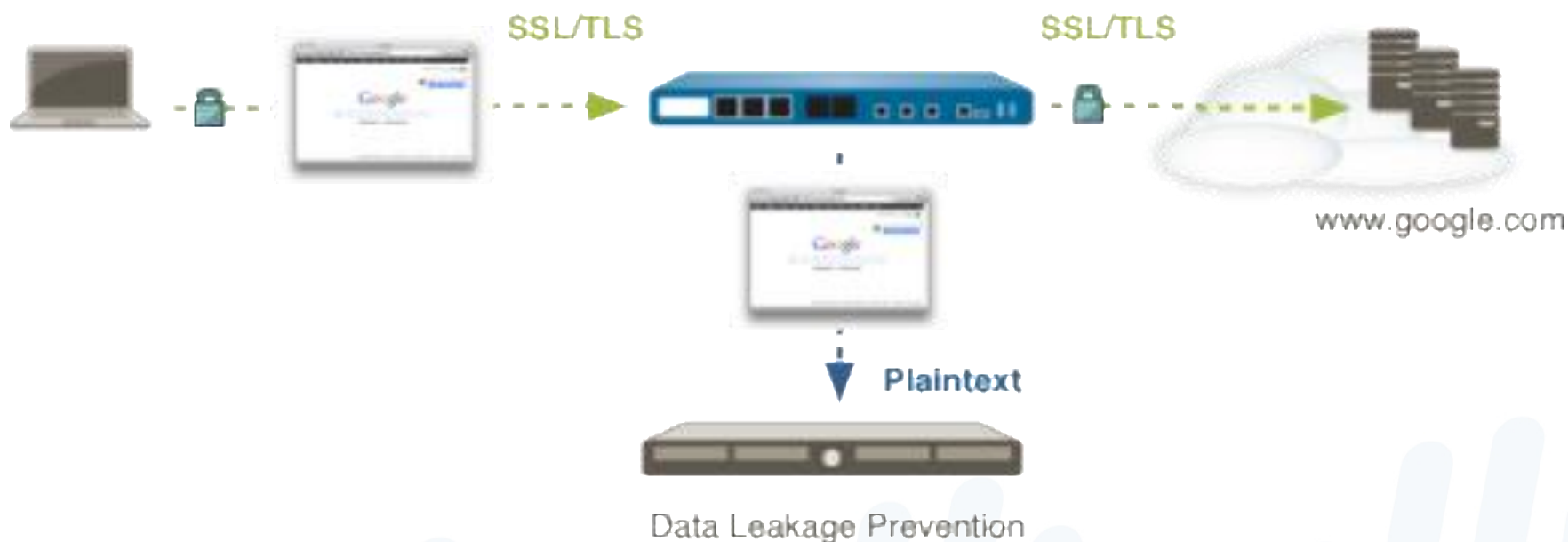


APT1

SSL для защиты данных или чтобы скрыть вредоносную активность?

Схема работы расшифровки SSL/SSH

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



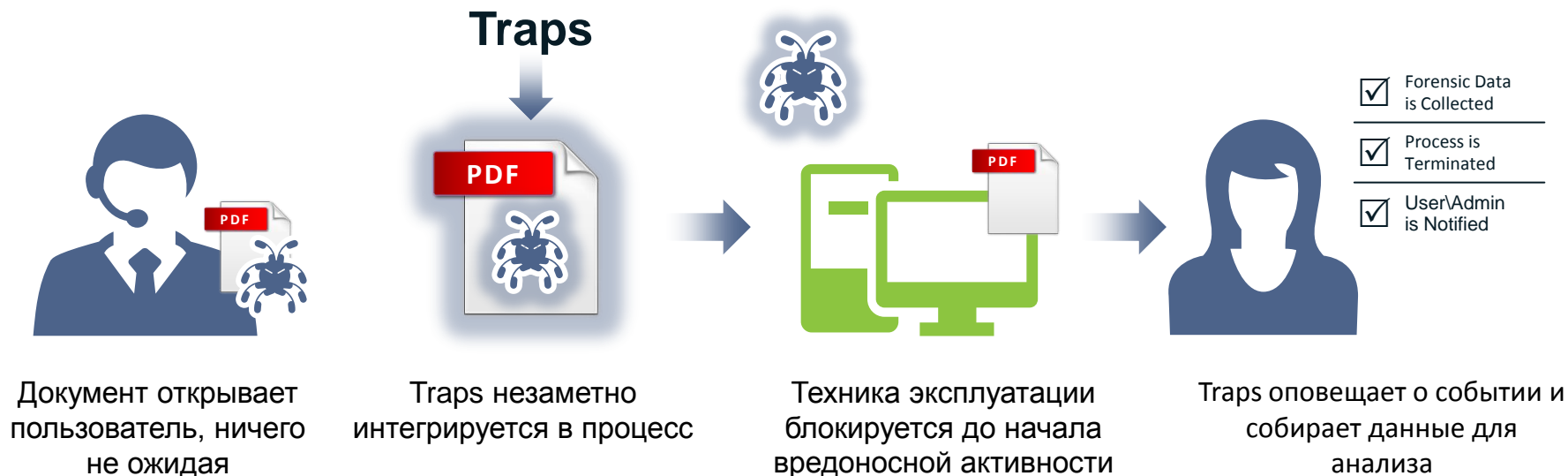
Использовать NGFW удобно для приложений 7 уровня – не нужно помнить стандартные порты приложений

Разрешить MS Lync? Запросто!

1434(UDP), 5060, 5061, 444, 135, 5062, 8057, 8058,
5063, 57501-65535, 80, 443, 8080, 4443, 8060, 8061,
5086, 5087, 5064, 5072, 5070, 5067, 5068, 5081, 5082,
5065, 49152-57500(TCP/UDP), 5073, 5075, 5076, 5066,
5071, 8404, 5080, 448, 445, 881, 5041

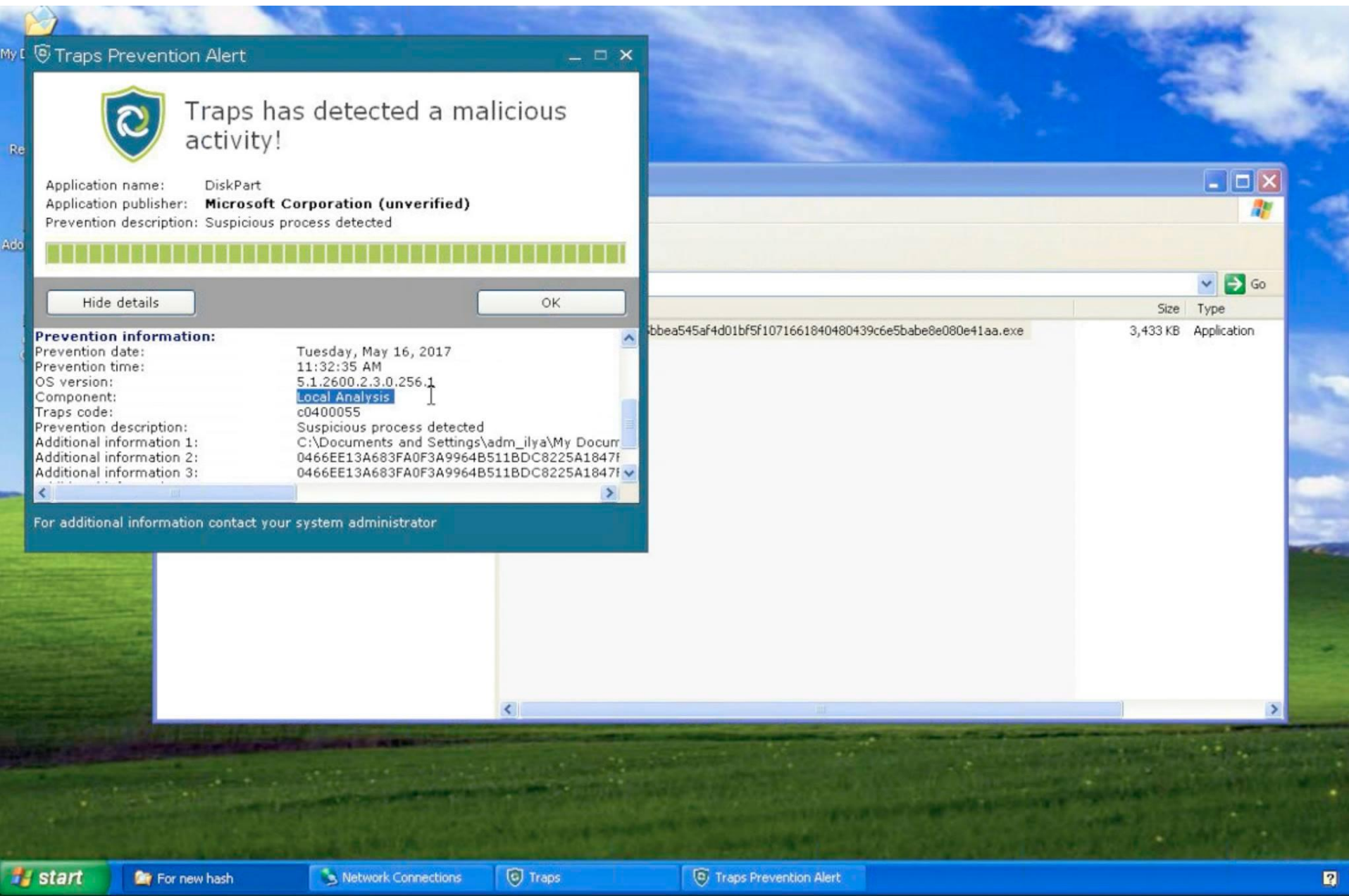
А как разрешить bittorrent?

TRAPS – защита от эксплойтов и песочница Wildfire предотвращает атаки на хостах



**Когда происходит попытка взлома,
то эксплойт вызывает ловушку и останавливается
до того как вредоносная активность начинается**

Блокировка WanaCrypt0r хостовой защитой



Заказчики впечатлены



Customer satisfaction data is collected through post-support call surveys.

Net Promoter Score (likelihood to recommend) = (% Promoters [10 or 9]) – (% Detractors [1-6]). Satisfaction = 1 (low) to 5 (high). An NPS of 50 is considered best-in-class.

Платформа Palo Alto Networks приносит удовольствие



Обеспечиваем заданную производительность при всех включенных сервисах безопасности



Видеозапись демонстрации защиты от криптолокеров

<https://youtu.be/Z2jmzzZniMo>

Email офиса в России: Russia@paloaltonetworks.com



Решаемые задачи: защита Интернет-периметра

- Контроль Интернет-доступа на уровне категорий приложений и пользователей
- Расшифрование входящего/исходящего SSL/SSH трафика, интеграция с DLP
- Анализ и контроль контента
- URL-фильтрация
- Защита от уязвимостей (IPS), Антивирус, защита от botnet
- Защиты от угроз «нулевого дня» и APT (целенаправленных атак)
- Удаленный доступ для мобильных пользователей с аутентификацией и проверкой соответствия корпоративной политике

Решаемые задачи: защита ЦОД и КСПД

- Контроль пользователей и приложений в ЦОД
- Защита от взлома, проникновений угроз и вирусов в ЦОД
- Антивирус, защита от уязвимостей (IPS), защита от botnet
- Защита от угроз «нулевого дня» и целенаправленных атак
- Интеграция с виртуальными серверами (VMware, Hyper-V и др.)
- Защита корпоративных, самописных приложений (пр. проект РЖД)
- Защиты виртуализированных рабочих мест (VDI)
- Интеграция с DLP, SIEM



Решаемые задачи: защита рабочих станций



- Предотвращение известных и неизвестных угроз за счёт применения уникальных методик анализа
- Дополнение новыми функциями безопасности существующего антивируса
- Защита физических (APM), виртуальных сред (VDI) и мобильных ПК
- Полноценная интеграция с компонентами платформы NGFW и Wildfire (песочницы)



Ресурсы для изучения технологий Palo Alto Networks

- <https://applipedia.paloaltonetworks.com/> - список приложений
- <http://researchcenter.paloaltonetworks.com/app-usage-risk-report-visualization-2014/> - пузырьковая диаграмма
- <https://threatvault.paloaltonetworks.com/> - база данных вирусов и атак
- <https://paloaltonetworks.com/resources/datasheets/product-summary-specsheet.html> - спецификация всех продуктов
- www.projectnee.com/HOL/catalogs/catalog/134 - бесплатная лабораторная среда VMware NSX + NGFW
- live.paloaltonetworks.com – портал с ответами на вопросы и материалами
- live.paloaltonetworks.com/t5/Migration-Tool-Articles/Download-the-Migration-Tool/ta-p/56582 – скачать Migration Tool

Пузырьковая диаграмма приложений на Flash

<http://researchcenter.paloaltonetworks.com/app-usage-risk-report-visualization-2014/>

2014 APPLICATION USAGE & THREAT REPORT

ABOUT THE DATA

APPLICATIONS

Applications

Categories

Subcategories

SORT BY:

Technology

Frequency

FILTER BY RISK LEVEL:

5 4 3 2 1 All

FILTER BY REGION:

Global

Americas & Canada

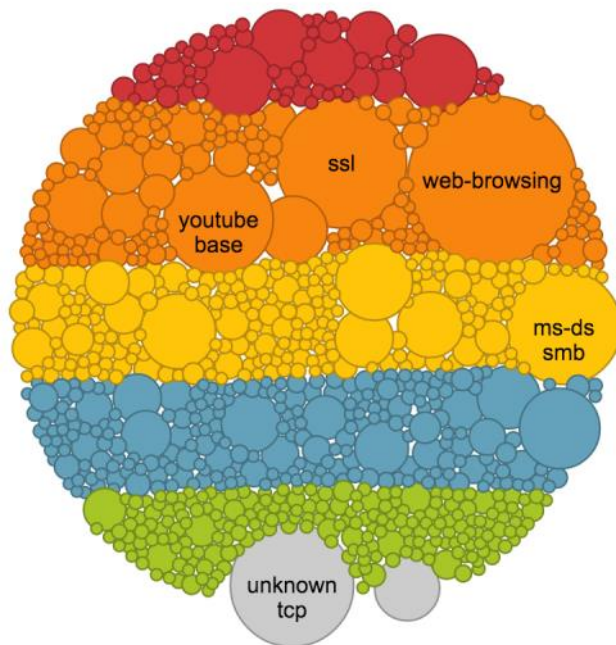
Asia Pacific

Europe

Japan

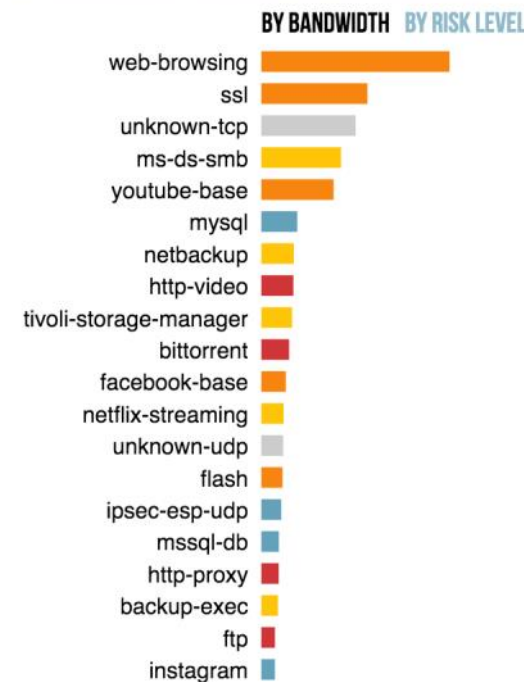
APPLICATION BANDWIDTH

Bubble size is relative to bandwidth consumed. Mouse over bubbles to see application statistics.



TOP 20 APPLICATIONS COMPARED

Applications that consume the most bandwidth.



[Ссылка на диаграмму](#)

База данных вирусов и атак

<https://threatvault.paloaltonetworks.com/>



THREAT VAULT

✓ All Source Types

Anti-spyware Signatures

Antivirus Signatures

DNS Signatures

PAN-DB URL Classifications

Vulnerability Protection Signatures

WildFire Signatures

What are we searching for?

Search

- Domain name, URL, or IP address (i.e. microsoft.com)

UTD - Unified Test Drive – Threat Prevention лучше

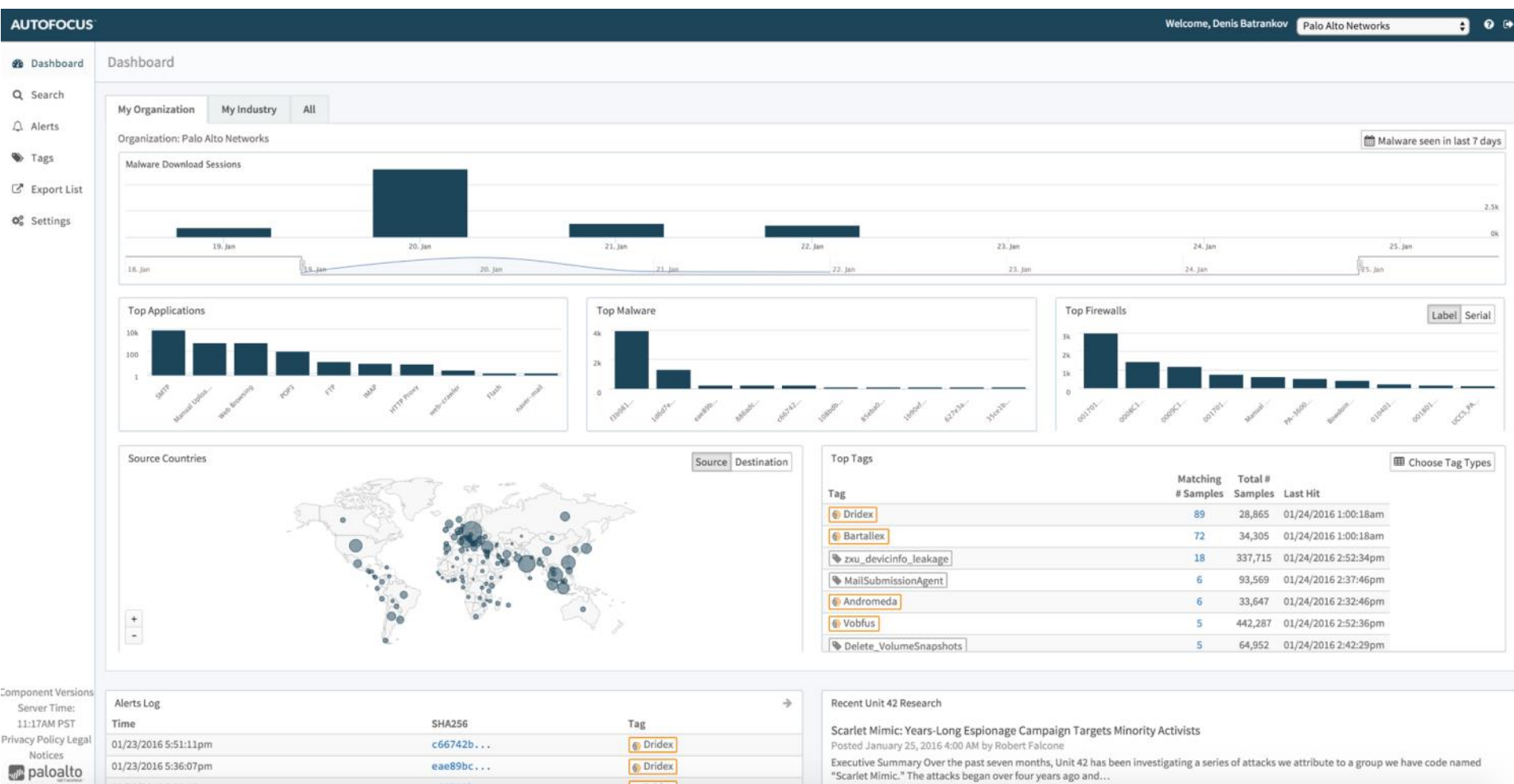
Feature Highlights	UTD-NGFW	UTD-TP	UTD-VDC	UTD-MP	UTD-AEP (New)	AWS-TD as UTD (New)
Application Control	Yes	Yes	Yes	Yes	No	Yes
Modern Malware (WildFire) with VM-Series	Yes	Yes	Yes	No	No	No
Decryption	Yes	Yes	No	No	No	No
URL Filtering	Yes	Yes	No	No	No	No
Control Apps on Non-Standard Port	Yes	Yes	No	No	No	No
Evasive Apps (Block Web Proxy Sites)	Yes	No	No	No	No	No
GlobalProtect	Yes	No	No	No	No	No
In-depth Security Profile (w Threat Traffic)	No	Yes	No	No	No	Yes
DNS Sinkhole	No	Yes	No	No	No	No
Safe Search Enforcement	No	Yes	No	No	No	No
Advanced Endpoint Protection - Traps Introduction	No	Yes	No	No	Yes	No
Advanced Endpoint Protection -Malware and Exploit	No	No	No	No	Yes	No
Review Exploit Chain and Exploit Techniques	No	No	No	No	Yes	No
In-depth ESM Configuration	No	No	No	No	Yes	No
Traps and WildFire Integration	No	No	No	No	Yes	No
Dynamic Object Group	No	No	Yes	No	No	No
Panorama	No	No	Yes	No	No	No
vCenter and NSX Manager	No	No	Yes	No	No	No
NSX traffic steering, security group and policies	No	No	Yes	No	No	No
NSX VXLAN and DFW	No	No	Yes	No	No	No
VM-to-VM traffic control / protection	No	No	Yes	No	No	Yes
Use of VM-1000-HV and VM-100	No	No	Yes	No	No	No
Use of Migration Tool	No	No	No	Yes	No	No
Import 3rd party config file to Migration Tool	No	No	No	Yes	No	No
Migrate port-based policies to application-based policies	No	No	No	Yes	No	No
PAN-OS version	7.0	7.0	6.0	7.0	N.A.	7.0
Current Lab version	3.1	3.2	2.0	1.0	1.0	1.0

Я показываю обычно UTD-TP потому что там NGFW + TRAPS



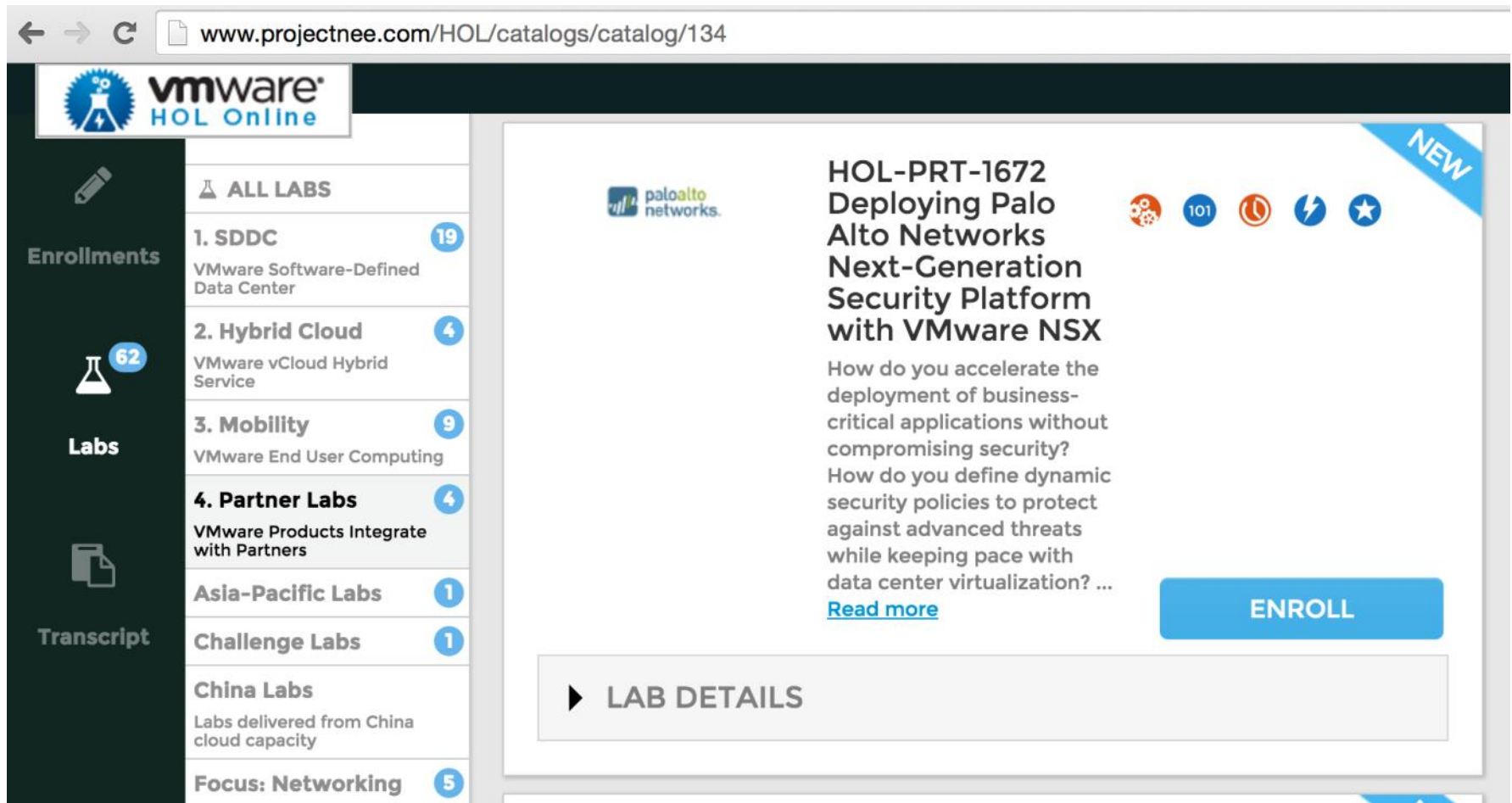
Портал Autofocus

<https://autofocus.paloaltonetworks.com>



NSX Demos + Palo Alto Networks NGFW

<http://www.projectnee.com/HOL/catalogs/catalog/134>



The screenshot shows a web browser window with the URL www.projectnee.com/HOL/catalogs/catalog/134. The page features a dark sidebar on the left with navigation links: "Enrollments", "Labs" (with a "62" badge), and "Transcript". The main content area displays a list of labs under the "ALL LABS" heading. The selected lab, "HOL-PRT-1672 Deploying Palo Alto Networks Next-Generation Security Platform with VMware NSX", is highlighted with a "NEW" badge and an "ENROLL" button. The lab description includes a brief overview and a "Read more" link. Below the description is a "LAB DETAILS" section.

vmware HOL Online

Enrollments

Labs 62

Transcript

ALL LABS

- 1. SDDC** 19
VMware Software-Defined Data Center
- 2. Hybrid Cloud** 4
VMware vCloud Hybrid Service
- 3. Mobility** 9
VMware End User Computing
- 4. Partner Labs** 4
VMware Products Integrate with Partners
- Asia-Pacific Labs** 1
- Challenge Labs** 1
- China Labs**
Labs delivered from China cloud capacity
- Focus: Networking** 5

HOL-PRT-1672
Deploying Palo Alto Networks Next-Generation Security Platform with VMware NSX

How do you accelerate the deployment of business-critical applications without compromising security? How do you define dynamic security policies to protect against advanced threats while keeping pace with data center virtualization? ... [Read more](#)

ENROLL

LAB DETAILS

SPLUNK + Palo Alto Networks

<http://splunkdemo.paloaltonetworks.com/>

splunkdemo.paloaltonetworks.com/en-US/account/login?return_to=%2Fen-US%2F

splunk>enterprise

<input type="text" value="Username"/>	<input type="password" value="Password"/>	<input type="button" value="Sign in"/>
---------------------------------------	---	--

© 2005-2016 Splunk Inc. Splunk 6.2.3 build 264376

LIVE - ответы на все вопросы <https://live.paloaltonetworks.com>

The screenshot shows the Palo Alto Networks LIVE community website. The browser address bar displays <https://live.paloaltonetworks.com/index.jspa>. The page header includes the "LIVEcommunity" logo, "Sign In", and "Get Support" buttons. Below the header, there are "Topics" and "Resources" dropdown menus. A large green banner with a tree pattern displays "Live > Page Not Found". Below the banner, a "Customer Advisory" link is visible. A search bar contains the text "user-id|", and a dropdown menu lists several search results, with "Getting Started: User-ID" highlighted. A red error message states "Please check your URL for typos and try again." The footer includes the Palo Alto Networks logo, a "Connect" section with social media icons, and a list of events.

user-id|

- ☒ User-ID resource list
- ☒ Getting Started: User-ID
- ☒ User-ID best practices
- ☒ Best practices for securing User-ID deployments
- ☒ DotW: User-ID Group Mapping
- ☒ User-ID Nested User Groups
- ☒ How to Configure Agentless User-ID
- ☒ Customer advisory: Security Impact of User-ID Misconfiguration
- ☒ LDAP Profile vs User-ID
- ☒ User-ID Agent Setup Tips

turn off suggestions

Please check your URL for typos and try again.

Connect

Twitter YouTube LinkedIn Facebook

Events

on Fuel at Spark User Summit Boston on December 2015

on Fuel at Spark User Summit Amsterdam 16 December 2015

on Fuel at Spark User Summit Sydney on 9 December 2015

Скачать Migration Tool 3.3.

<https://live.paloaltonetworks.com/t5/Migration-Tool-Articles/MigrationTool-3-3-Info-and-Guide/ta-p/72559>

← → ↻  <https://live.paloaltonetworks.com/t5/Migration-Tool-Articles/Download-the-Migration-Tool/ta-p/56582>

Download the Migration Tool

by panagent on 03-23-2015 11:13 AM - edited on 11-05-2015 04:14 PM by ADMIN syaguma

(28,218 Views)

Labels: Management

Overview

The Palo Alto Networks **Migration Tool** is derived from the successful **Migration Tool** used by the Palo Alto Networks Professional Services Organization and Channel Partners. It's an evolution of the **Migration Tool** into a configuration platform that allows you to, not only **migrate** configurations, but enhance, optimize, add, remove or edit elements, ultimately converting the legacy device rules into a next-generation model by creating App-IDs based on real traffic acquired from devices being installed or already in production. The Palo Alto Networks **Migration Tool** is a valuable asset for network security administrators who need or want to keep their rulebases in a pristine state.

Note: The **Migration Tool** is packaged as a virtual machine image. The download file is a zipped tar archive and the size is approximately 680MB.

Palo Alto Networks Community Members

Community members can download **Migration Tool** 3.1 for VMware ESXi 5.5 (or higher) by clicking the following:

Migration Tool

Download Now

Click here to get the **Migration Tool** for VMplayer and Workstation

Not a Community Member?

If you do not have a Community account, then click the following:

Migration Tool

Download Now

Click to download **Migration Tool** 3.0












Полезные команды CLI

<https://live.paloaltonetworks.com/docs/DOC-4254>

COMMAND	DESCRIPTION	4.1	5.x	6.x
General System Health				
show system info	Shows the system's management IP, serial #, and code version	✓	✓	✓
show jobs processed	Shows when commits, downloads, upgrades are completed.	✓	✓	✓
show system disk-space	Shows percent usage of disk partitions.	✓	✓	✓
show system logdb-quota	Shows the maximum log file sizes.	✓	✓	✓
show system software status	Shows running processes.	✓	✓	✓
Monitor CPUs				
show system resources	Shows processes running in the Management Plane.	✓	✓	✓
show running resource-monitor	Shows the resource utilization in the Dataplane	✓	✓	✓
Dropped Packet Troubleshooting				
ping source <IP_addr_src_int> host <IP_addr_host>	Ping from a specified device source interface to destination IP.	✓	✓	✓
ping host <IP>	Ping from the management interface.	✓	✓	✓
show session all filter source <source-IP> destination <destination-IP>	Shows specific sessions in the sessions table for source and destination IPs.	✓	✓	✓
show session info	Shows usage, pps rates, etc.	✓	✓	✓
show session id <id-number>	Shows session details by entering the session ID number.	✓	✓	✓
Packet Filters and Capture WARNING: Running debug commands on a production device may cause undesirable results.				
debug dataplane packet-diag clear all	Clear/delete settings and files previously created.	✓	✓	✓
debug dataplane packet-diag clear log log				
delete debug-filter file *	Removes all packet capture files.	✓	✓	✓
debug dataplane packet-diag set filter match source x.x.x.x destination y.y.y.y destination-port <port-num>	Sets filter with the source IP, destination IP and port to capture from/to packets.	✓	✓	✓
debug dataplane packet-diag set filter match source y.y.y.y destination x.x.x.x destination-port <port-num>				
debug dataplane packet-diag set filter on	Configures the different stage of capture types to be executed.	✓	✓	✓
debug dataplane packet-diag set capture stage receive file pantac-rx.pcap				
debug dataplane packet-diag set capture stage transmit file pantac-tx.pcap				
debug dataplane packet-diag set capture stage drop file pantac-drop.pcap				
debug dataplane packet-diag set capture stage firewall file pantac-fw.pcap				
debug dataplane packet-diag set capture on				
debug dataplane pack-diag show setting	Verifies packet filters are setup correctly.	✓	✓	✓
show counter global filter delta yes packet-filter yes	While test is running, run the command 2-3 times to verify filtered traffic is being captured.	✓	✓	✓

Фирменный магазин shop.paloaltonetworks.com

<https://shop.paloaltonetworks.com>



Catalogue

In Stock

Stocked

- Executive Gifts
- Tech Items
- Awards & Crystal
- Bags
- Clothing
- Drinkware
- Event Giveaways
- Stationery & Pens
- Travel




On Request

- Executive Gifts
- Tech Items

Welcome to the new Palo Alto Networks store!

To begin ordering, choose a category to your left to start browsing and adding items to your cart. If you have special requests, a **RUSH ORDER / CRITICAL IN-HAND DATE** or if you just need help with something, click 'Contact Us' on the left of the page or email panstore@nadel.com.

Please take careful note of the **Terms and Conditions**, the acceptance of which is a requirement for placing orders on the store.



Basket

-- empty --

[View Basket](#)

Your Account

[Log in](#)

Существующие подписки на NGFW

Threat Prevention - обновления сигнатур антивируса, IPS, анти-spyware

URL Filtering – обновления базы данных категорий URL

Существует две версии баз собственная и сторонняя от BrightCloud.

WildFire – отправка файлов в облако WildFire и получение сигнатур из облака

Decryption Port Mirror (бесплатно) – отправка расшифрованного трафика на зеркальный порт

Virtual Systems – дополнительные виртуальные системы на устройстве.
Модели PA-500, PA-200, VM серия не поддерживают виртуальные системы

Global Protect – поддержка мобильных устройств и large scale VPN

Autofocus – доступ к базе AutoFocus для разбора инцидентов

<https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/getting-started/activate-licenses-and-subscriptions.html>



Компания **PALO ALTO NETWORKS**



- **2005 год** - Санта-Клара (США)
- **Основатель - Нир Зук**
- Специализация - межсетевые экраны нового поколения, защита рабочих станций и облаков
- **3800+ сотрудников** Palo Alto Networks
- **37000 + ЗАКАЗЧИКОВ ПО МИРУ:** банки, финансовые услуги, нефтегазовые компании, производство, телеком, здравоохранение, ритейл, логистические компании и другие

Gartner

Волшебный квадрант

Межсетевые экраны
нового поколения

Лидерство 5 лет
подряд!



Контакт офиса в Москве:

RUSSIA@paloaltonetworks.com

