Фабрика безопасности Fortinet

Алексей Андрияшин

01.06.2017

Кибербезопасность трансформируется в цифровую безопасность

- Эволюционирующий ландшафт безопасности
  - » Продвинутые угрозы
  - » Обнаружение и реагирование
  - » Шпионское ПО/Вымогатели
- Управление/соответствие
  - » Управление рисками
  - » Регулирование индустрии
  - » Сертификация
- Развитие инфраструктуры
  - » Данные в облаках
  - » IoT/OT
  - » Рост скоростей

Современные тренды – Internet 2 в ближайшее время

Возросшее количество атак

65K инцидентов в отчёте только Verizon DBIR

SDN/NFV

Software-defined everything. SD WAN

Virtualization

80% приложений виртуализированы

SaaS

По статистике около 10 приложений компании размещены в облаке

Mobile

Не внедрён контроль устройств (BYOD)

SSL Traffic Growth

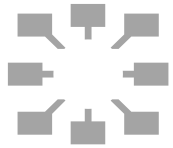
40% всего трафика зашифровано SSL

Social

Рост использования полосы пропускания

IoT

35B устройств подключено к сети



100G

Bandwidth

Wi-Fi достиг скоростей LAN. 100G сети уже построены. Рост бизнес трафика на 20% ежегодно.

Analytics

Big Data

5G

Wireless

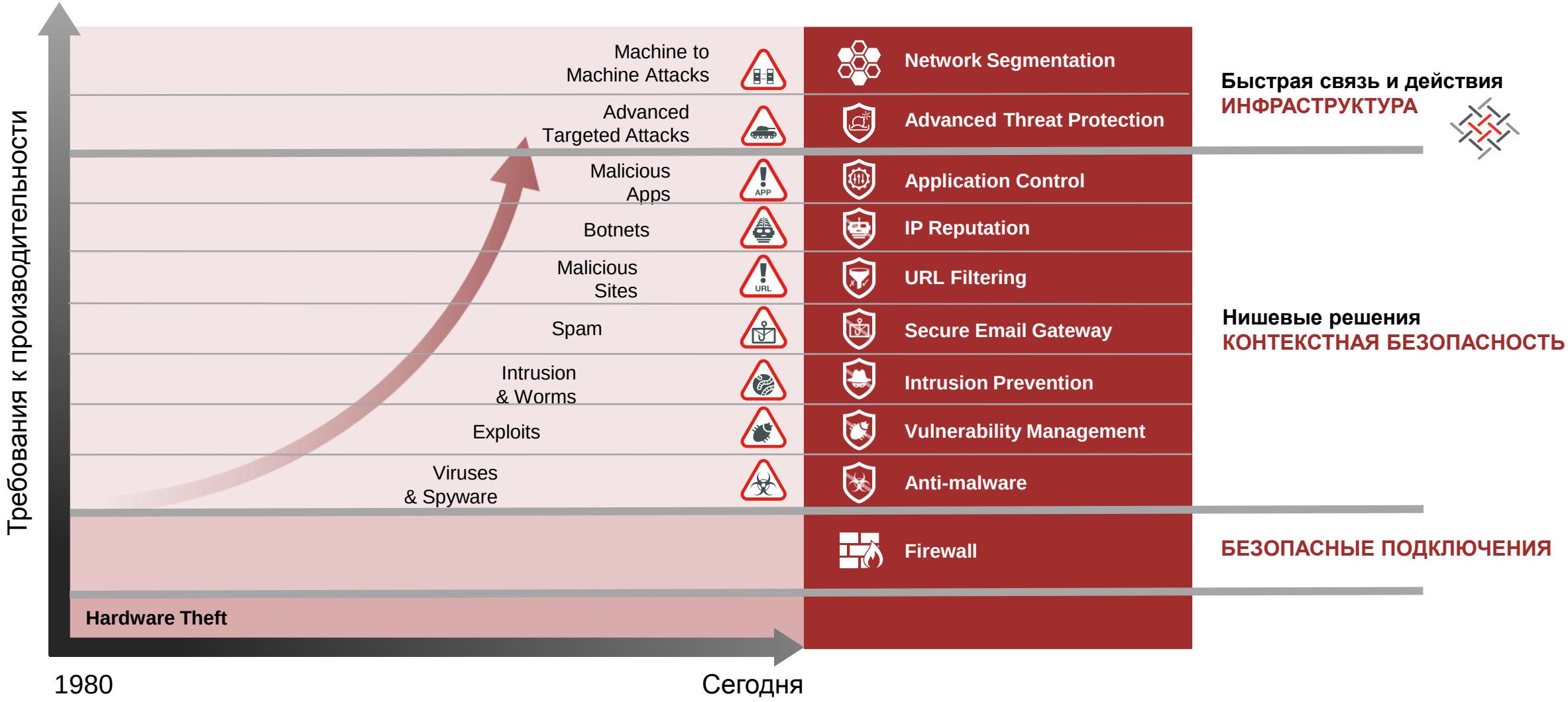
Internet 2

100 Gbps и

UHDTV

БУДУЩЕЕ

Предотвращение **Продвинутых угроз** требует быстрой реакции элементов защиты



Потребности в анализе SSL растут

SSL данных на данный момент

Более **40%**

Веб-браузинга в HTTPS (SSL)

Источник:
Google Web Performance Labs

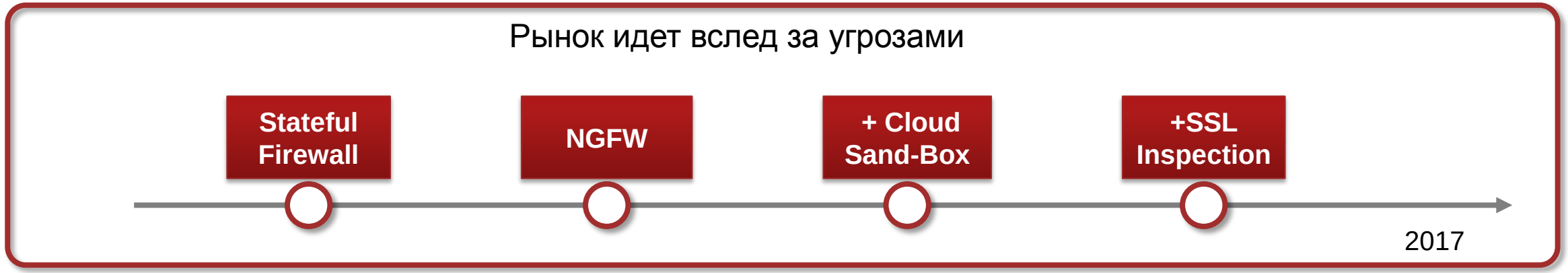
Шифрованных вредоносных кодов

Более **50%**

Количество атак с использованием шифрования прогнозируется в 2017*

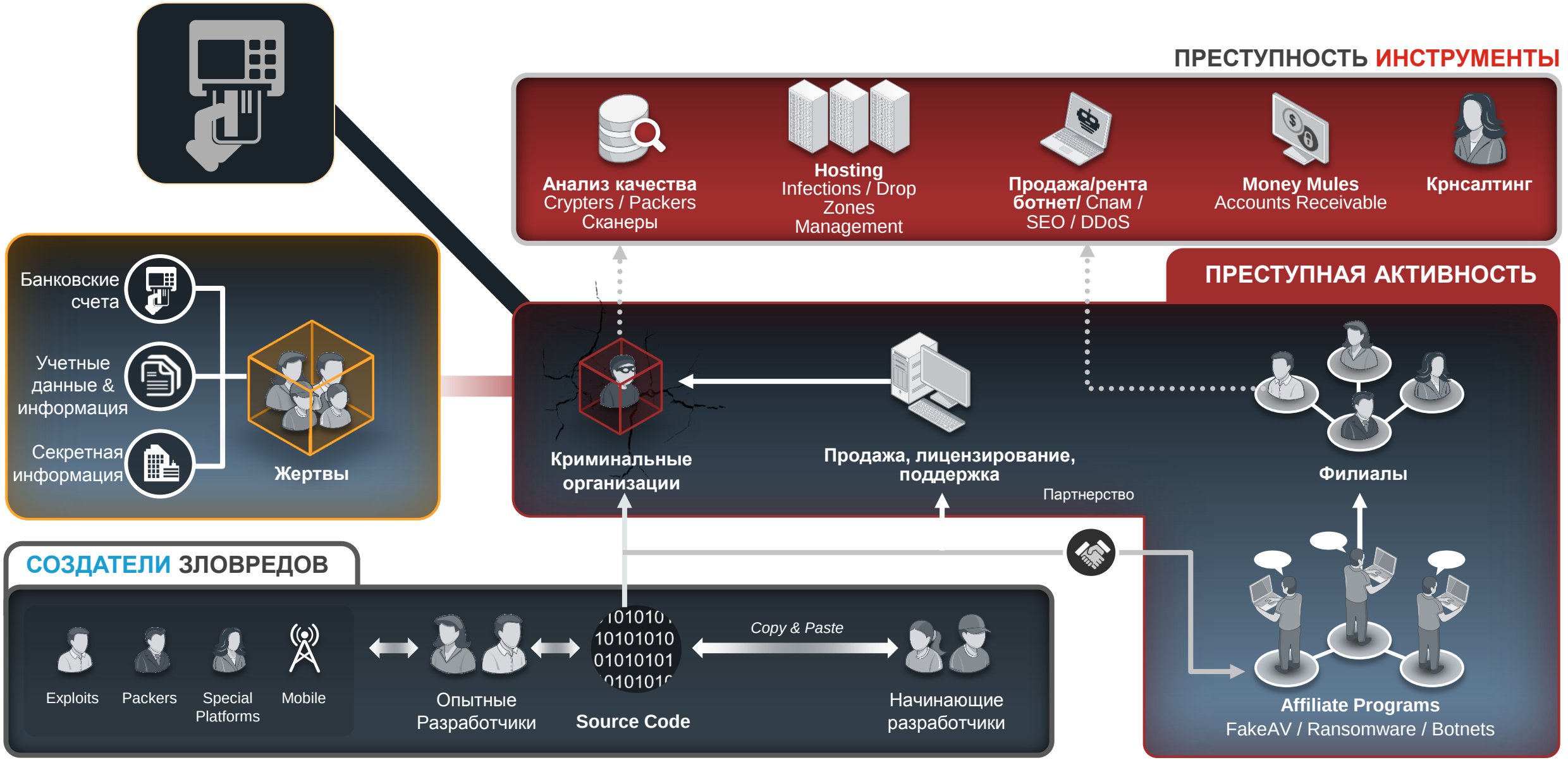
Источник:
Gartner

Изменение требований к защите сетей



50%	Количество пользователей NGFW возрастет с 50% до 90% к 2019
85%	К 2019 году 85% новых внедрений песочниц будут интегрированы с NGFW
$12B	Прогноз IDC по рынку сетевой безопасности на 2017 год, рост 9%

Организованная киберпреступность

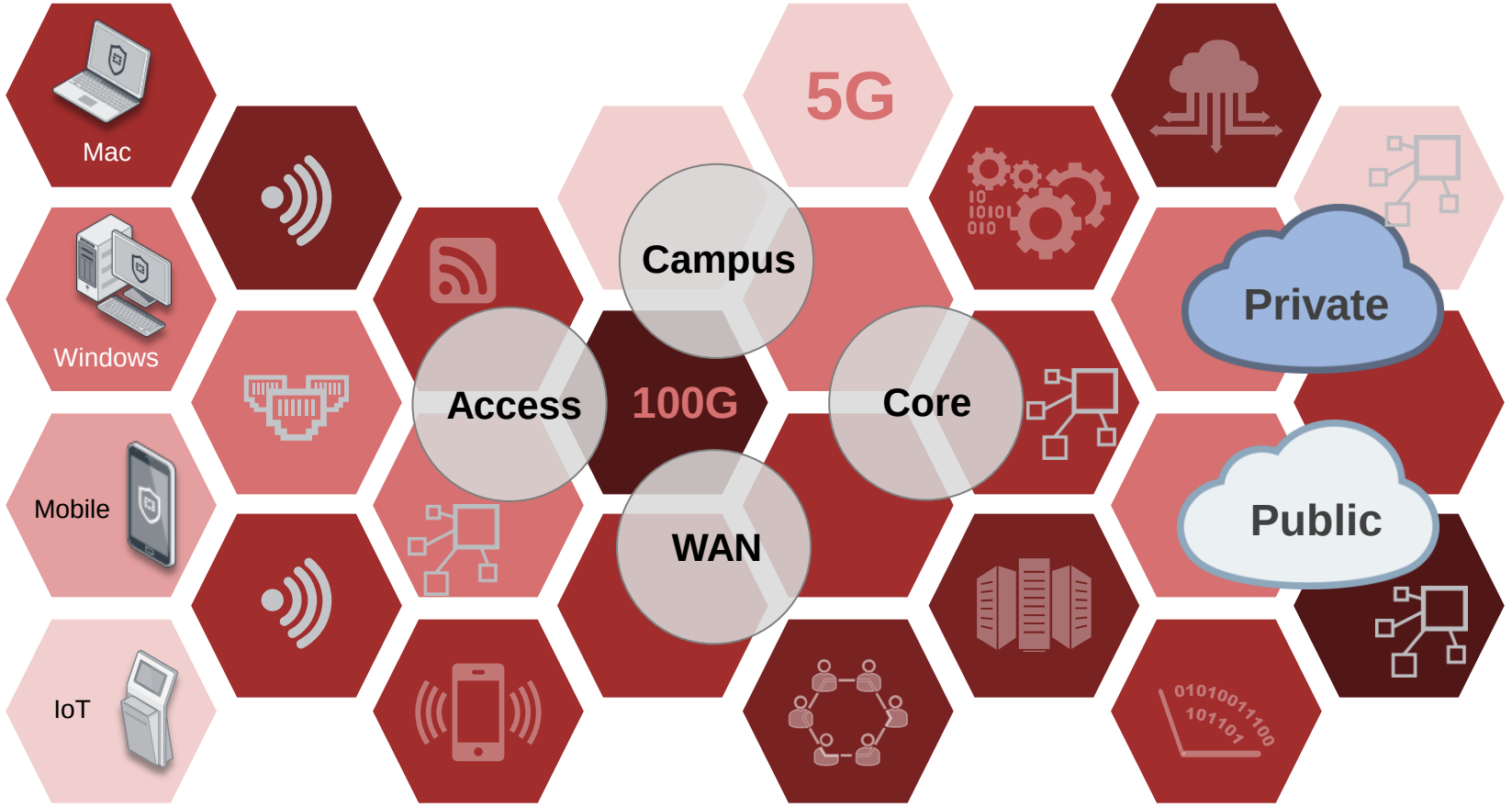


Возможностей для кибер атак стало больше

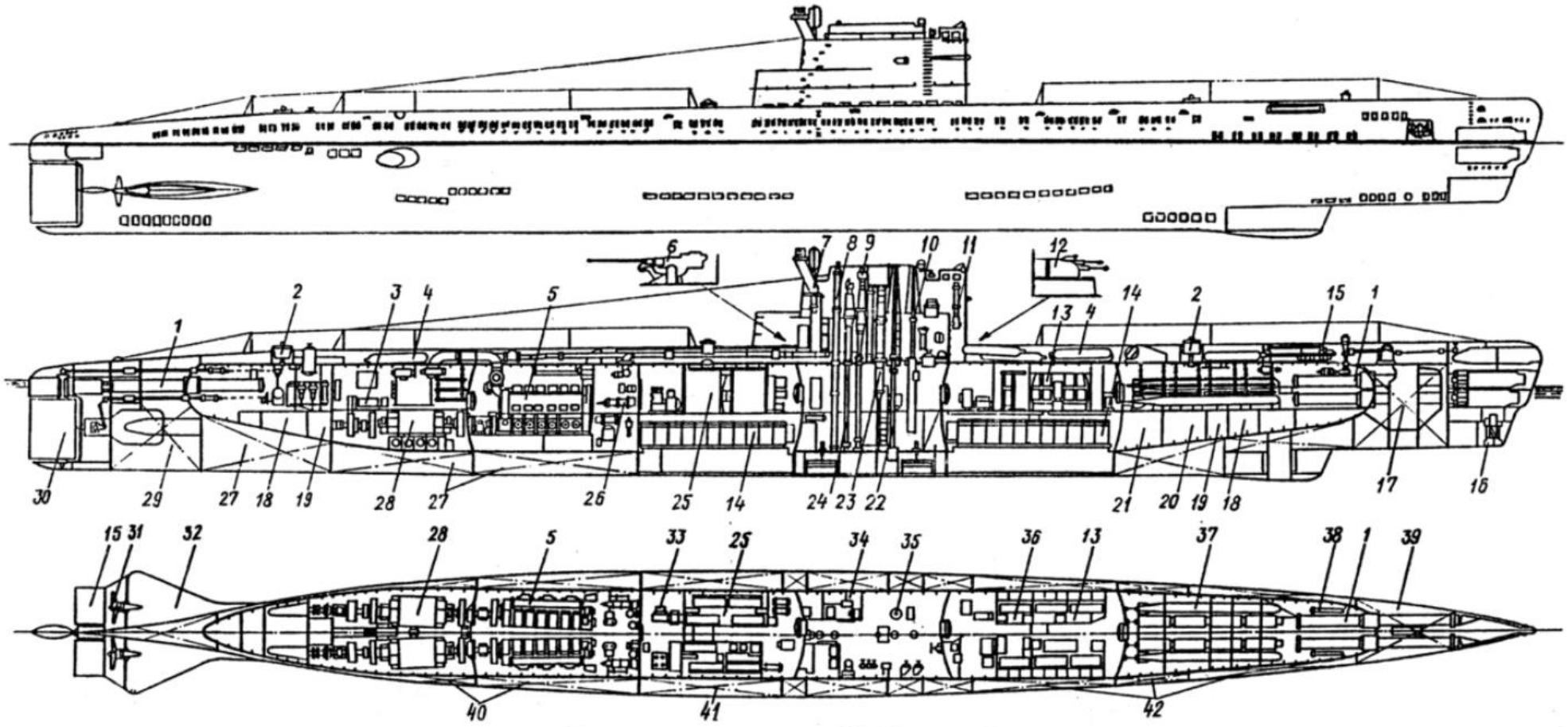
Современная безопасность не имеет границ

- Сети
- Приложения
- Данные
- Люди

Современные сети не имеют границ – архитектура сетевой сегментации от IoT до Облаков

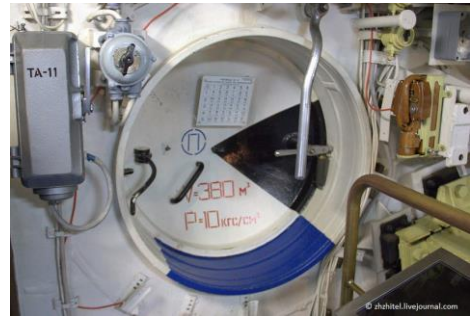


Слушать в отсеках!



Подводная лодка проекта 613. Продольный разрез, план:

1 — торпедный аппарат; *2* — аварийный телефонный буй; *3* — электродвигатель экономического хода; *4* — баллон сжатого воздуха; *5* — дизельный двигатель 37Д; *6* — артиллерийская установка СМ-24-ЗИФ; *7* — газоотвод двигателя 37Д; *8* — антенна «ВАН»; *9* — антенна «Накат»; *10* — перископ атаки; *11* — магнитный компас ГОН-23М; *12* — артиллерийская установка 2М-8; *13* — 4-местная каюта офицеров; *14* — аккумуляторная батарея; *15* — горизонтальный руль; *16* — гидролокационная станция «Тамир-5Л»; *17* — цепной ящик; *18* — дифферентная цистерна; *19* — цистерна пресной воды; *20* — торпедозаместительная цистерна; *21* — топливная цистерна внутри прочного корпуса; *22* — зенитный перископ; *23* — неподвижная воздушная шахта РДП; *24* — антенна «Флаг»; *25* — жилое помещение старшин; *26* — дизель-компрессор ДК-2; *27* — топливная цистерна вне прочного корпуса; *28* — гребной электродвигатель ПГ-101; *29, 39, 40, 41, 42* — цистерны главного балласта; *30* — вертикальный руль; *31* — гребной винт; *32* — стабилизатор; *33* — электрокомпрессор воздуха высокого давления; *34* — рубка радиолокации; *35* — основной компас;

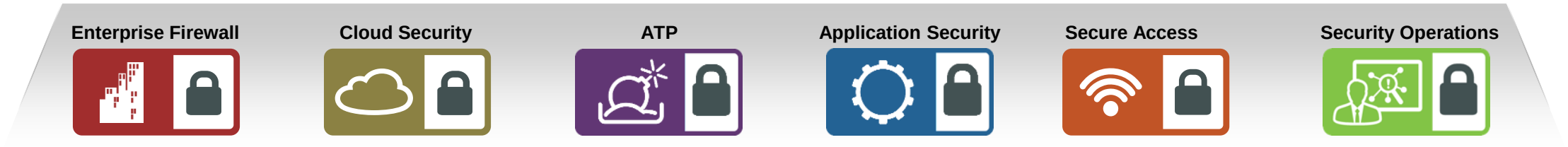


Новые вызовы безопасности

Миссия Fortinet - предоставить самую инновационную, самую эффективную сетевую фабрику безопасности для обеспечения и упрощения ИТ-инфраструктуры

Отсутствие сетевых границ **Медленный – уязвимый!** **Сложность - это враг безопасности**

Операторы Энтерпрайз SMB



FORTINET SECURITY FABRIC

ШИРОТА
МОЩНОСТЬ
ИНТЕЛЛЕКТ

FORTINET SECURITY FABRIC

Широта – Фабрика предоставляет полную визуализацию, покрытие и гибкость по всему динамическому спектру атак

Видимость

Широкий охват

- Облачная безопасность
- Безопасность приложений
- Сетевая защита
- Защищенный доступ
- Клиент/IoT защита

Гибкость/Открытость

FORTINET SECURITY FABRIC

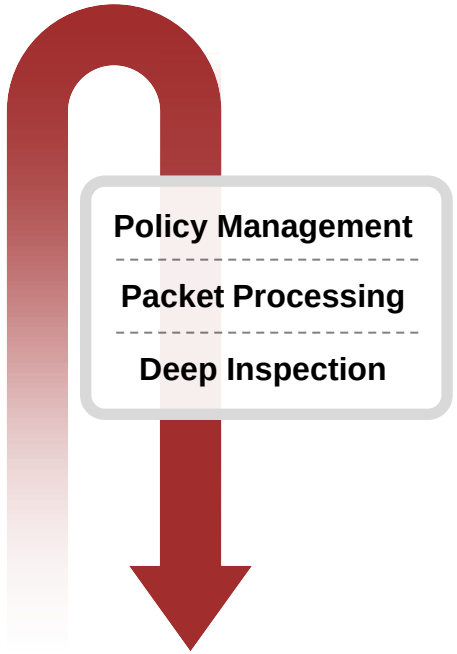
Широта – Фабрика предоставляет широкие возможности по интеграции с технологическими партнерами

FORTINET Fabric Ready

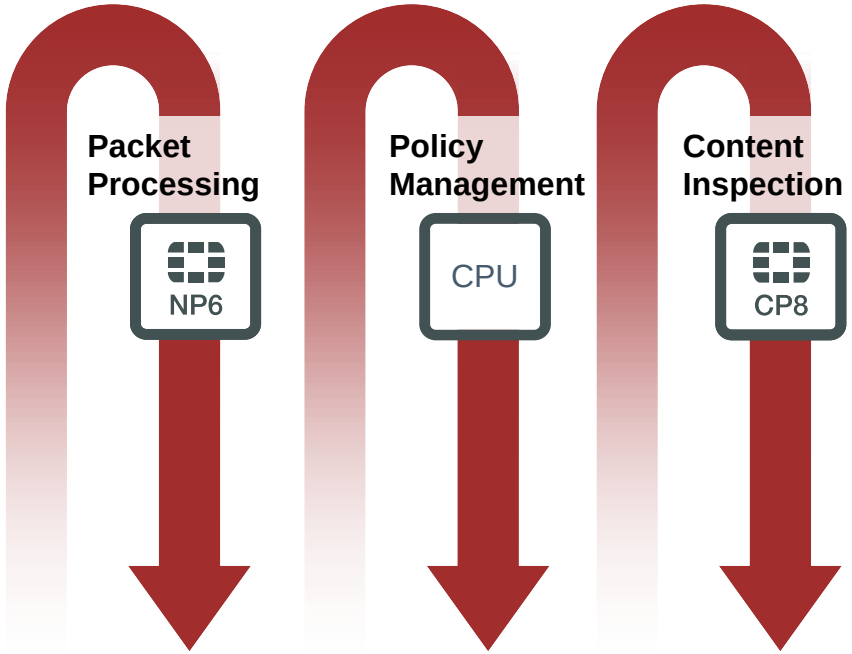
Безопасность для современных Сетей

Медленный значит взломанный – новый виток “гонки вооружений”

CPU Only
Обычный вендор



Parallel Path Processing (PPP)
Fortinet



Использование Fortinet ASIC

Больше производительность

Меньше задержка

Энергоэффективность

Меньше места в стойках

Продуктовая линейка Fortigate

Начальный уровень

Model	FW
FGT 30E*	950 Mbps
FGT 50E	2.5 Gbps
FGT 60E	3 Gbps
FGT 80D	1.3 Gbps
FGT 90E	4 Gbps

Средний уровень

Модель	FW
FGT 100D	2.5 Gbps
FGT 200D	4 Gbps
FGT 300D	8 Gbps
FGT 400D	16 Gbps
FGT 500D	16 Gbps
FGT 600D (10G)	36 Gbps
FGT 800D	36 Gbps
FGT 900D	52 Gbps

Верхний уровень

Модель	FW
FGT 1000D	52 Gbps
FGT 1200D	72 Gbps
FGT 1500D	80 Gbps
FGT 2000E	90 Gbps
FGT 2500E	150 Gbps
FGT 3000D	80 Gbps
FGT 3700D (40G)	160 Gbps
FGT 3800D (100/40G)	320 Gbps
FGT 3960/ 3980E (100/10G)	640 Gbps 1 Tbps

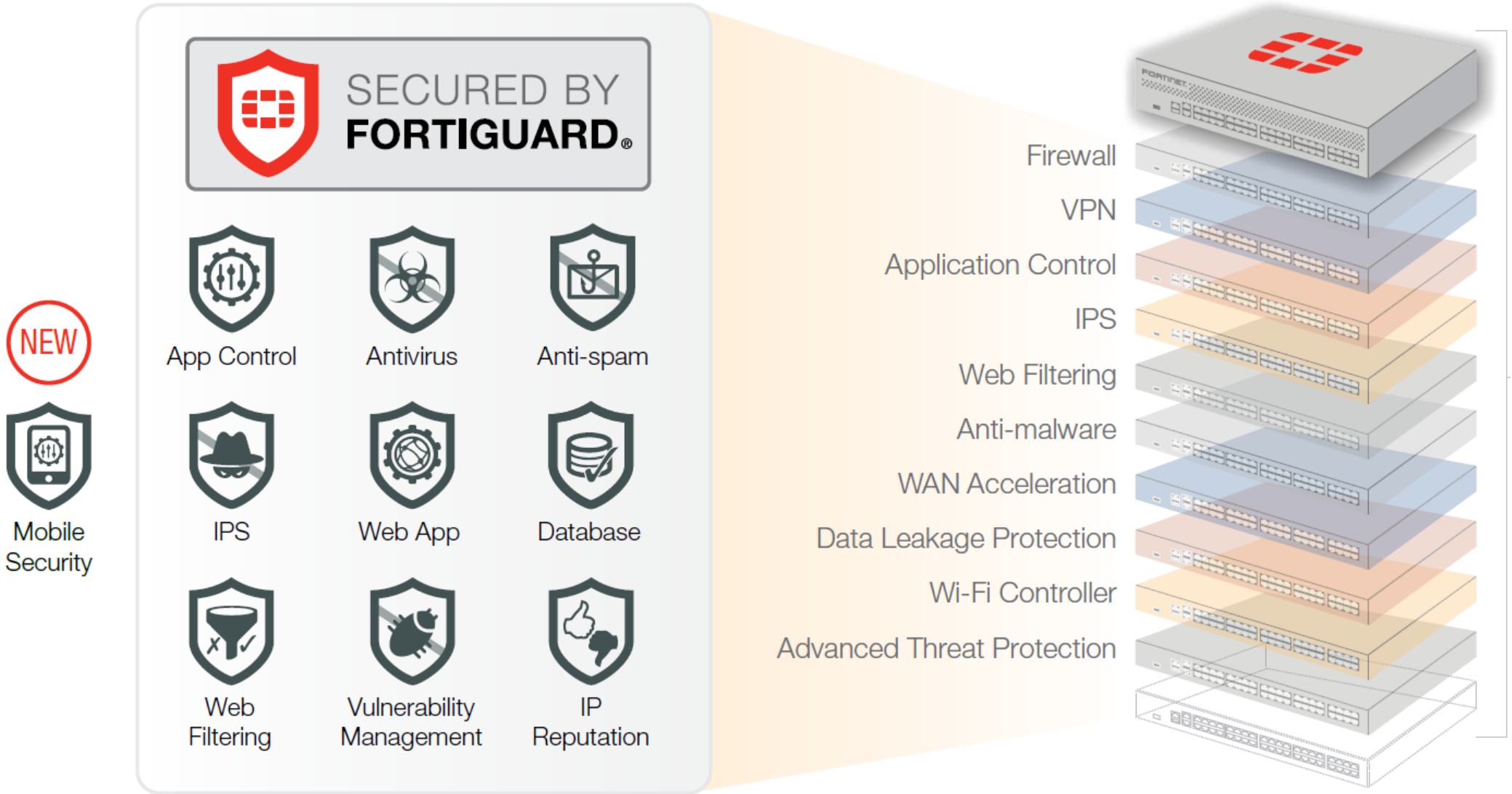
Операторский класс

Модель	FW
FGT 5144C	1 Tbps
FGT 5903	40G
FGT 5913	100G

Корпоративные шасси

Модель	FW
FGT 7040E (100/40/10G)	315 Gbps
FGT 7060 (100/40/10G)	2X 7040E

Сервисы безопасности и технологии



FortiGate – комплекс сетевой безопасности

НАЧАЛЬНЫЙ УРОВЕНЬ
30-90 СЕРИЯ

- **Распределенные**
- **Начального уровня**
  - » SOC Based
  - » FW Throughput ~ 4 Gbits/s
  - » NGFW Throughput ~ 400 Mbits/s
  - » Ports 1Ge

СРЕДНИЙ УРОВЕНЬ
100-900 СЕРИЯ

- **NGFW**
- **Филиалы**
  - » NP + CP Based
  - » FW Throughput ~ 50 Gbits/s
  - » NGFW Throughput ~ 5 Gbits/s
  - » Ports 1Ge 10Ge

ТОПОВЫЙ УРОВЕНЬ
1000-3000 СЕРИЯ

- **ЦОД**
- **NGFW**
  - » Multiple NP + CP Based
  - » FW Throughput ~ 300 Gbits/s
  - » NGFW Throughput ~ 30 Gbits/s
  - » Ports 10Ge, 40Ge & 100Ge

ОПЕРАТОРСКИЙ КЛАСС
5000/7000 СЕРИЯ

- **Операторы**
- **ЦОД**
  - » Blade NP + CP Based
  - » FW Throughput ~ 1 Tbps
  - » NGFW Throughput ~ 100 Gbits/s
  - » Ports 10, 40 & 100G

Новинка

Пример: Новая серия 200E в сравнении с 200D

Цена, DDP Москва: 8091$

1. **16x GE RJ45 Ports**
2. **4x GE SFP**
3. **Резервирование блоков питания**

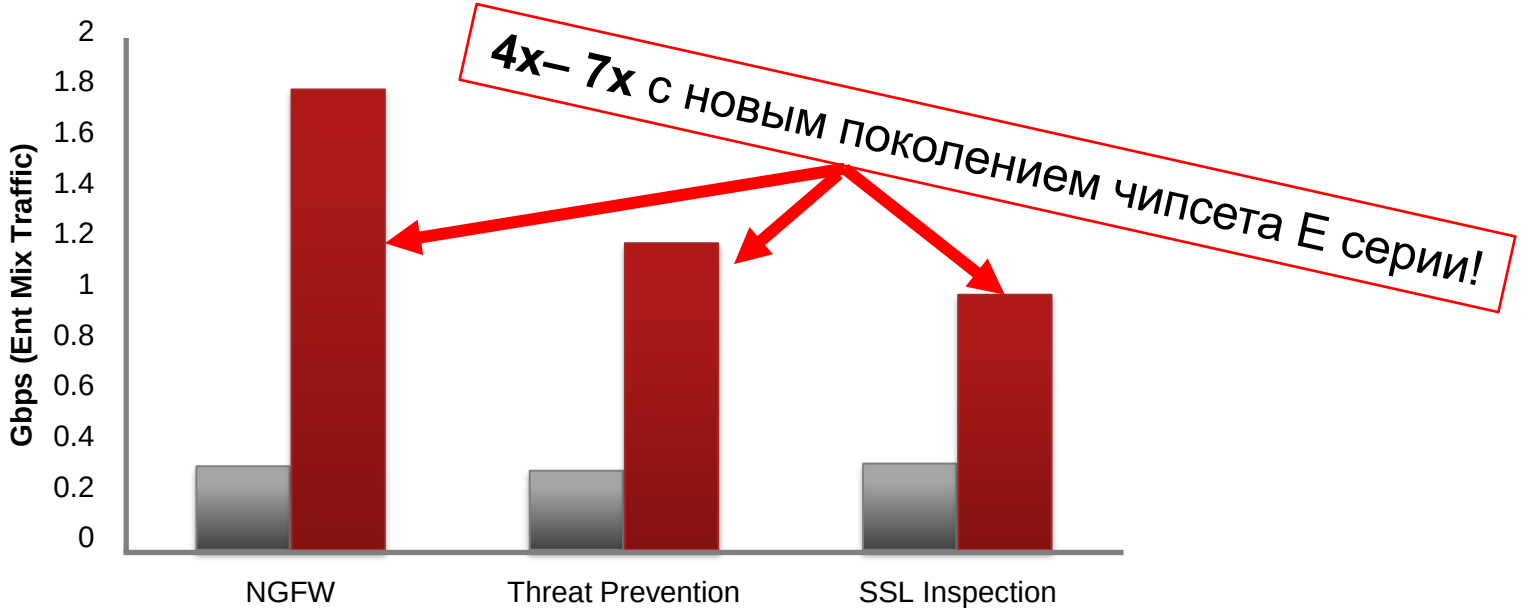
Максимальный уровень защиты

20 Gbps
FW Throughput

6 Gbps
IPS Throughput

1.8 Gbps
NGFW Throughput

Сравнение производительности FortiGate 200D и 200E



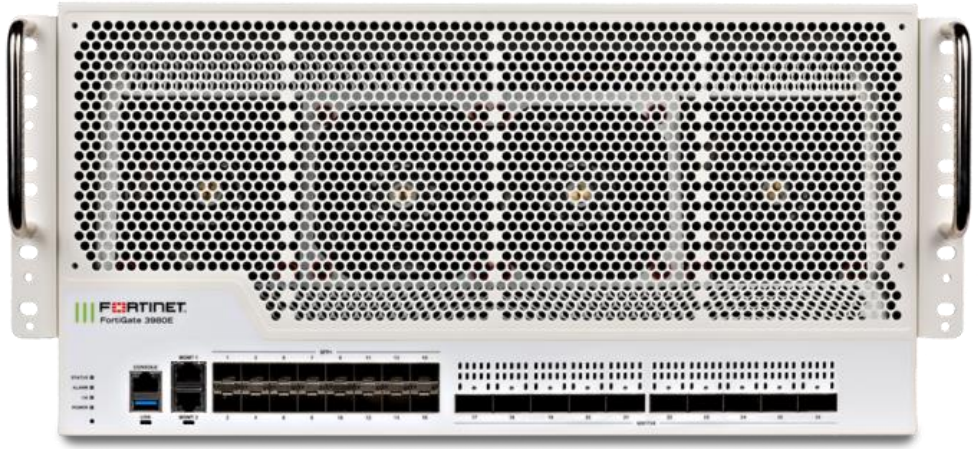
FG-200E-BDL (IPS, AV, URL, Botnet, Antispam)	$8 091

Новинка

Пример: Межсетевые экраны серии FortiGate 3980E

1 Tbps производительность в режиме Firewall

10 портов 100Gbps на борту



Specification	
Firewall Throughput	**1.12 Tbps**
IPSec VPN Throughput	**470 Gbps**
LAN	10 x 100G zQSFP+ 16 x 1/10G SFP/SFP+
FortiASIC	28 x NP6 4 x CP9
Storage	2 x 400GB, internal storage
Management	2 x GE RJ45 1 x RJ45 Console

Q1/17

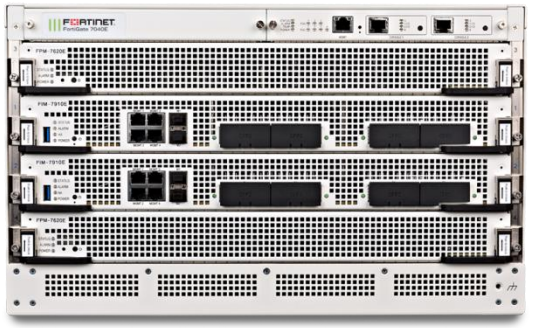
Для самых требовательных задач

Пример: Межсетевые экраны серии 7000

Новинка

Для инспекции приложений на скоростях в 100Gbps!

FG-7040E

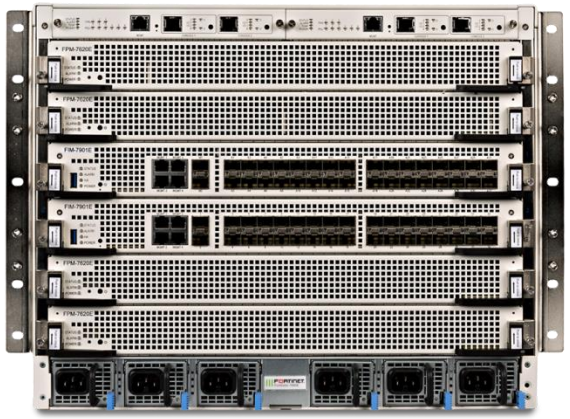


Specification	
Form Factor	6RU, 4-slot
I/O Interface	2x FIM-79XXE (selection)
Processor	2x FPM-7620E
Storage	NIL
Management	2 x RJ45 Console
Power	3 + 1 hot swappable redundant PSU

Уже доступно

315 Gbps/ 80 Gbps Application Control Throughput

FG-7060E



Specification	
Form Factor	8 RU, 6-slot
I/O Interface	Up to 2x FIM-79XXE (selection)
Processor	Up to 4x FPM-7620E
Storage	NIL
Management	2 x RJ45 Console
Power	5 + 1 hot swappable redundant PSU

Появляется в течении Q1 2017

2x Производительность 7040E

FORTINET SECURITY FABRIC

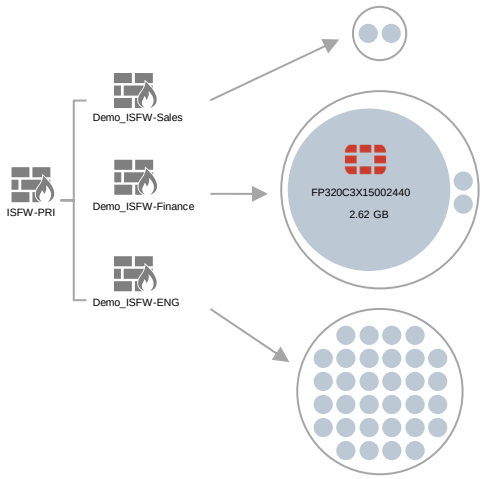
Интеллект Быстрая и скоординированная реакция на угрозы

Глобально и локально

Известные угрозы
FortiGuard

Неизвестные угрозы
FortiSandbox

Аудит и рекомендации

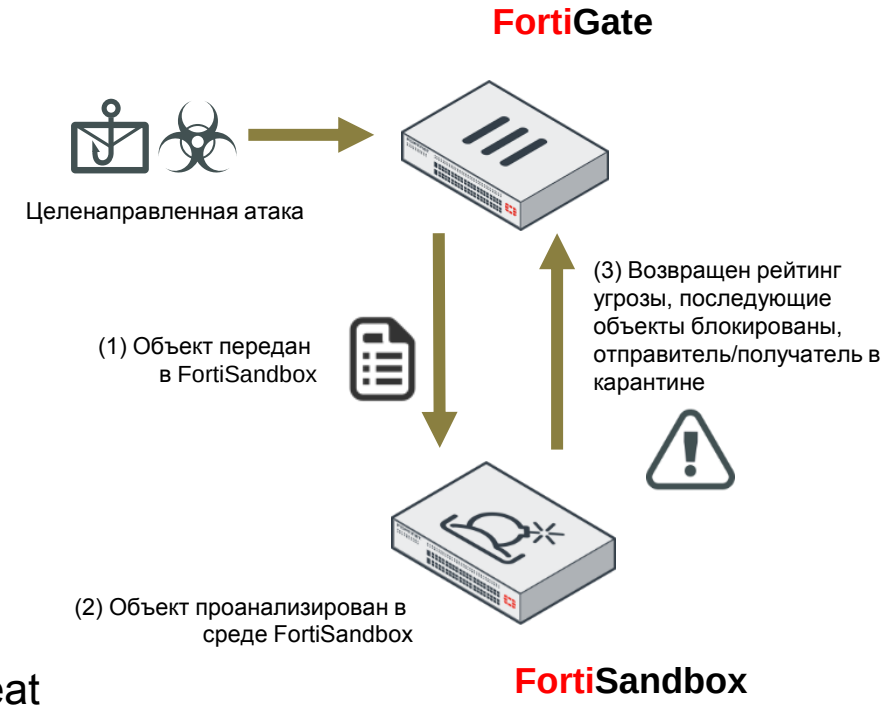


Координация

FortiSandbox эффективно дополняет существующие методы

Интеграция FortiGate и FortiSandbox

- Со стороны FortiGate
  - Инспекция входящего/исходящего трафика
  - Передача подозрительных/всех объектов в FortiSandbox
  - Получение результатов и локальных обновлений
  - Действия в один клик (карантин)
  - Блокировка распространения атаки
- Со стороны FortiSandbox
  - Сниффер извлекает объекты для анализа и индикаторы активности C&C
  - Прием объектов от FortiGate
  - Анализ всех объектов и сетевой активности
  - Определение и рейтинга объектов
  - Динамическая генерация и распространение "threat intelligence"



SECURED BY FORTIGUARD

Сервис NGFW
- Сигнатуры приложений
- Правила IPS

Сервис Веб-фильтрации
- Рейтинги риска
- Категорирование

Антивирусная защита
- Сигнатурная база
- Эвристика, эмуляция

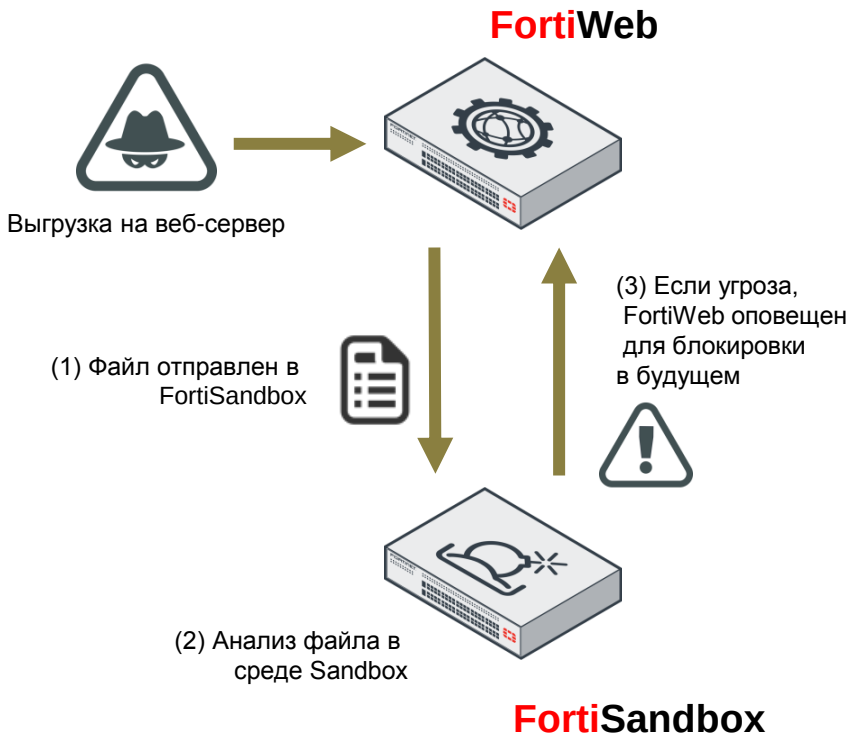
Облачный сервис FortiSandbox
- Песочница
- Выявление C&C

Сервис мобильного вредоносного ПО
- Сигнатурная база

Интеграция FortiWeb и FortiSandbox

- **Со стороны FortiWeb**
  - » Предотвращение эксплуатации уязвимостей
  - » Блокировка выгрузки известного вредоносного ПО (антивирус)
  - » Отправка подозрительных/всех выгрузок на анализ в песочницу
  - » Прием результатов и предотвращение вредоносного ПО или файлов с высоким риском

- **Со стороны FortiSandbox**
  - » Сниффер извлекает объекты для анализа и индикаторы активности C&C
  - » Прием объектов от FortiWeb для анализа
  - » Определение и рейтинга объектов
  - » Поддержание базы результатов FortiSandbox



SECURED BY FORTIGUARD®

Сервис Web App Security
- Сигнатуры прикладного уровня
- Признаки ботов
- База подозрительных URL
- Обновления сканера

Сервис IP репутации
- DDoS, Фишинг, Бот-сети, Спам, Анонимные прокси и зараженные отправители

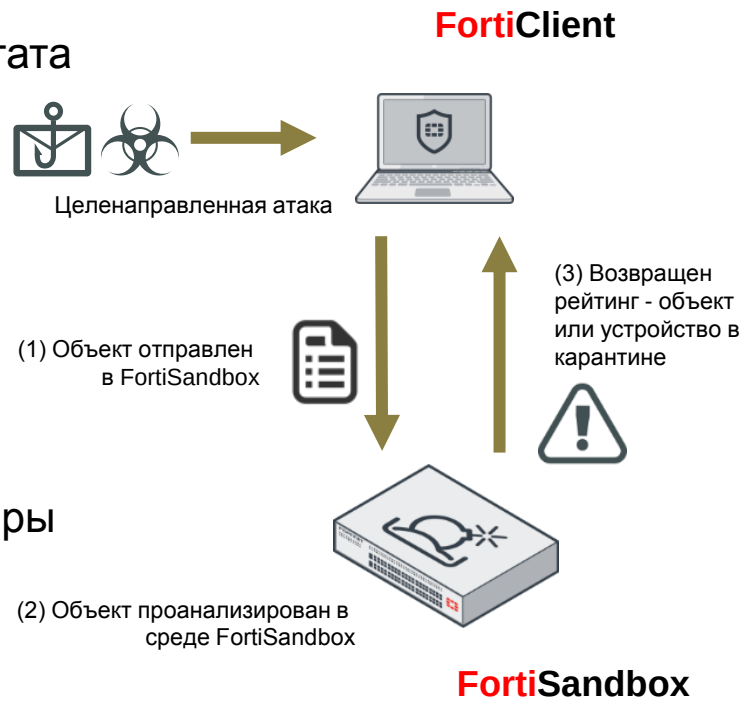
Антивирусная защита
- Сканирование выгружаемых файлов
- Регулярная и расширенная антивирусные базы

Предотвращение злонамеренных Email:

- FortiMail для инспекции email
  - » Блокирование известных угроз
  - » Удержание сообщений до определения рейтинга Sandbox
  - » Упрощенное развертывание - 1 sandbox поддерживает несколько Fortimail
- FortiSandbox для анализа объектов
  - » Выявляет неизвестные угрозы
  - » Предоставляет "threat intelligence" для подавления
  - » Итоговые результаты опционально предоставляются в FortiGuard

Интеграция FortiClient и FortiSandbox

- Со стороны FortiClient
  - Отправка объектов на анализ
  - Опционально - задержка запуска объектов до результата анализа
  - Автоматический карантин вредоносных объектов
  - Прием "threat intelligence" от локального FortiSandbox
  - Блокировка объектов, признанных вредоносными - FortiGuard
- Со стороны FortiSandbox
  - Сниффер извлекает объекты для анализа и индикаторы активности C&C
  - Прием объектов от FortiClient
  - Анализ всех объектов и сетевой активности
  - Назначение и предоставление рейтинга
  - Поддержание базы результатов FortiSandbox



SECURED BY FORTIGUARD

Антивирусная защита
- Сигнатурная база
- Эвристика, эмуляция

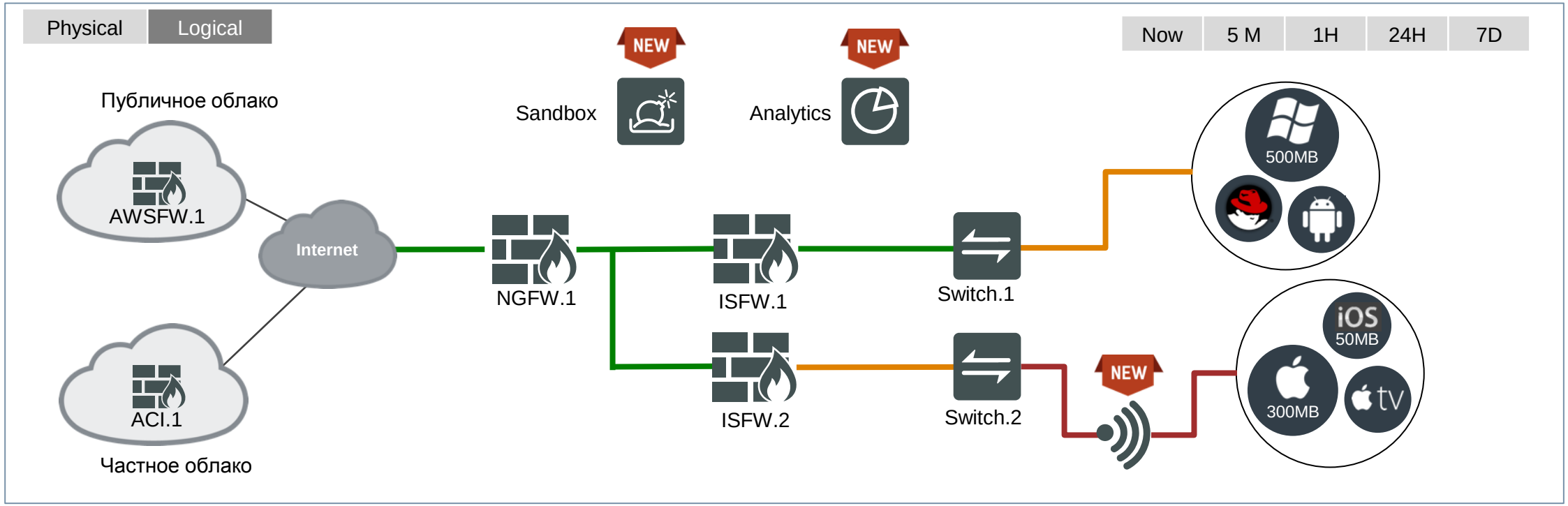
Сервис Веб-фильтрации
- Рейтинги риска
- Категорирование

Сервис контроля приложений
- Сигнатуры приложений
- Контроль по категориям

Сервис анализа уязвимостей
- База уязвимостей
- Правила повышения защищенности

Как это всё работает совместно

Визуализация сети и передачи данных



Контроль за устройствами в сети

Направления передачи данных

Удобное управление устройствами

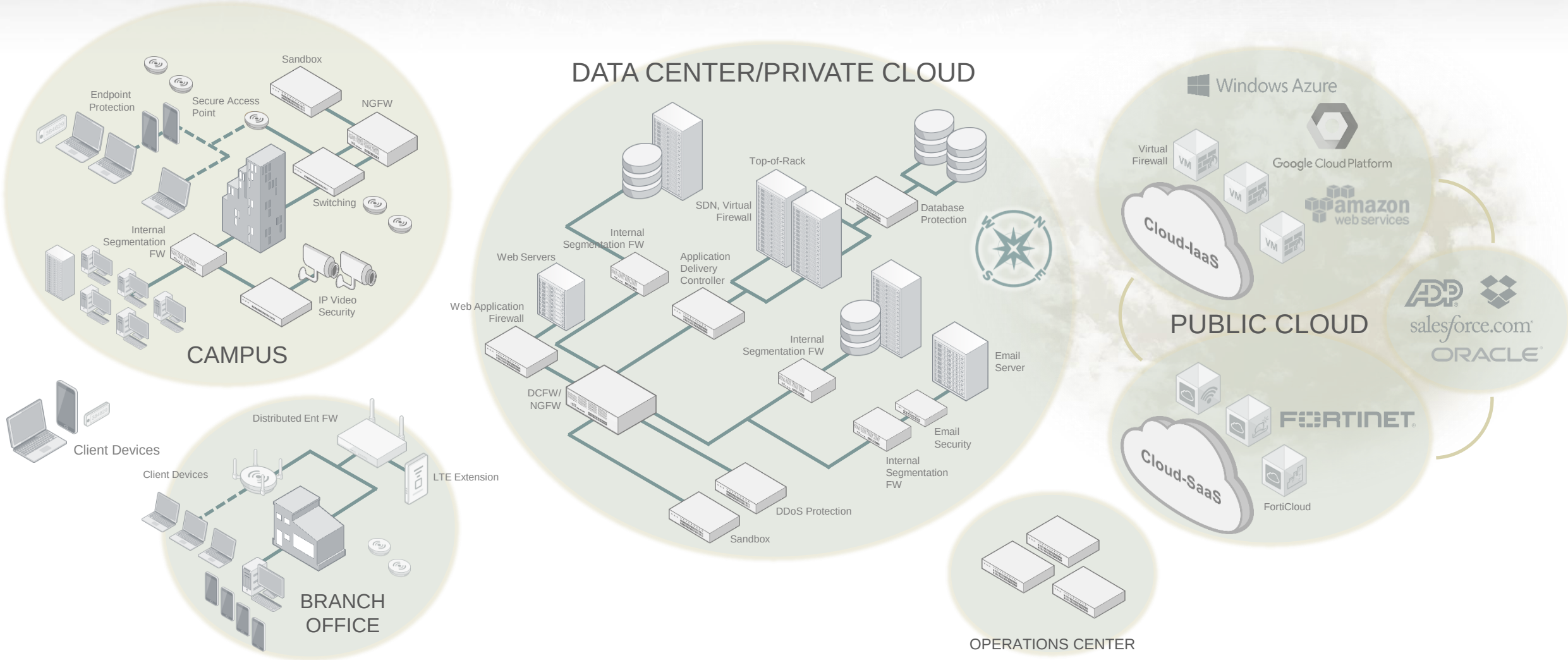
Карантин устройств

ФАБРИКА БЕЗОПАСНОСТИ

Fabric Security Fabric - это концепция, которая обеспечивает безопасность без компромиссов: широко, мощно, интеллектуально

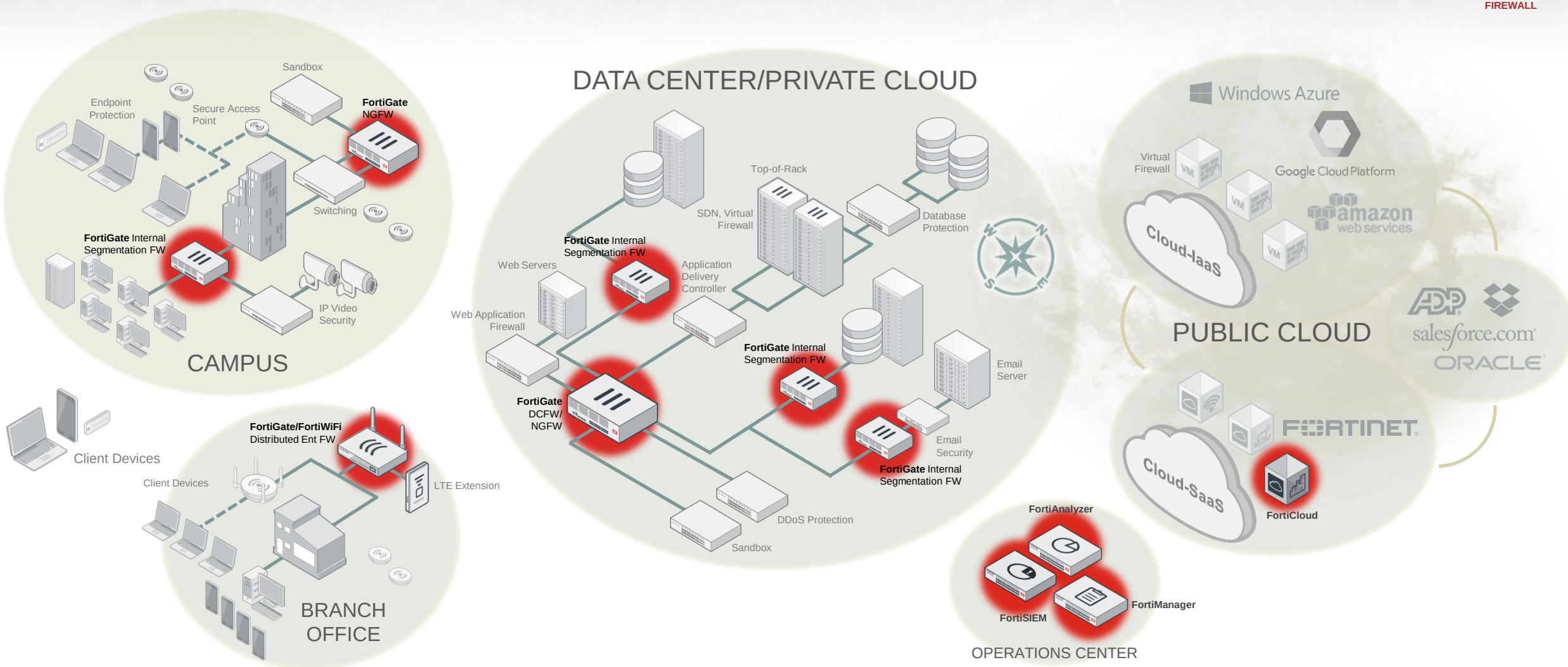
ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ ФАБРИКИ БЕЗОПАСНОСТИ

ФАБРИКА БЕЗОПАСНОСТИ FORTINET



ФАБРИКА БЕЗОПАСНОСТИ FORTINET

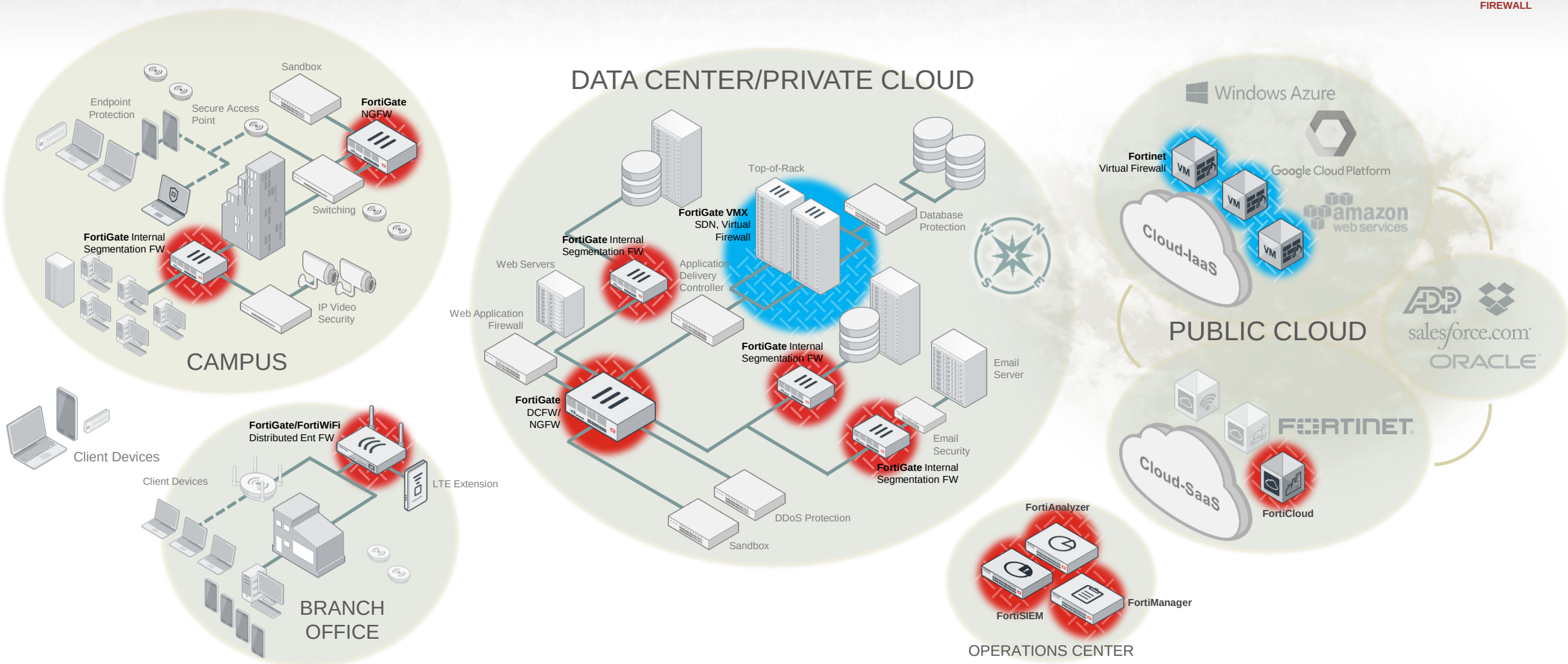
ENTERPRISE FIREWALL



ФАБРИКА БЕЗОПАСНОСТИ FORTINET

CLOUD SECURITY

ENTERPRISE FIREWALL

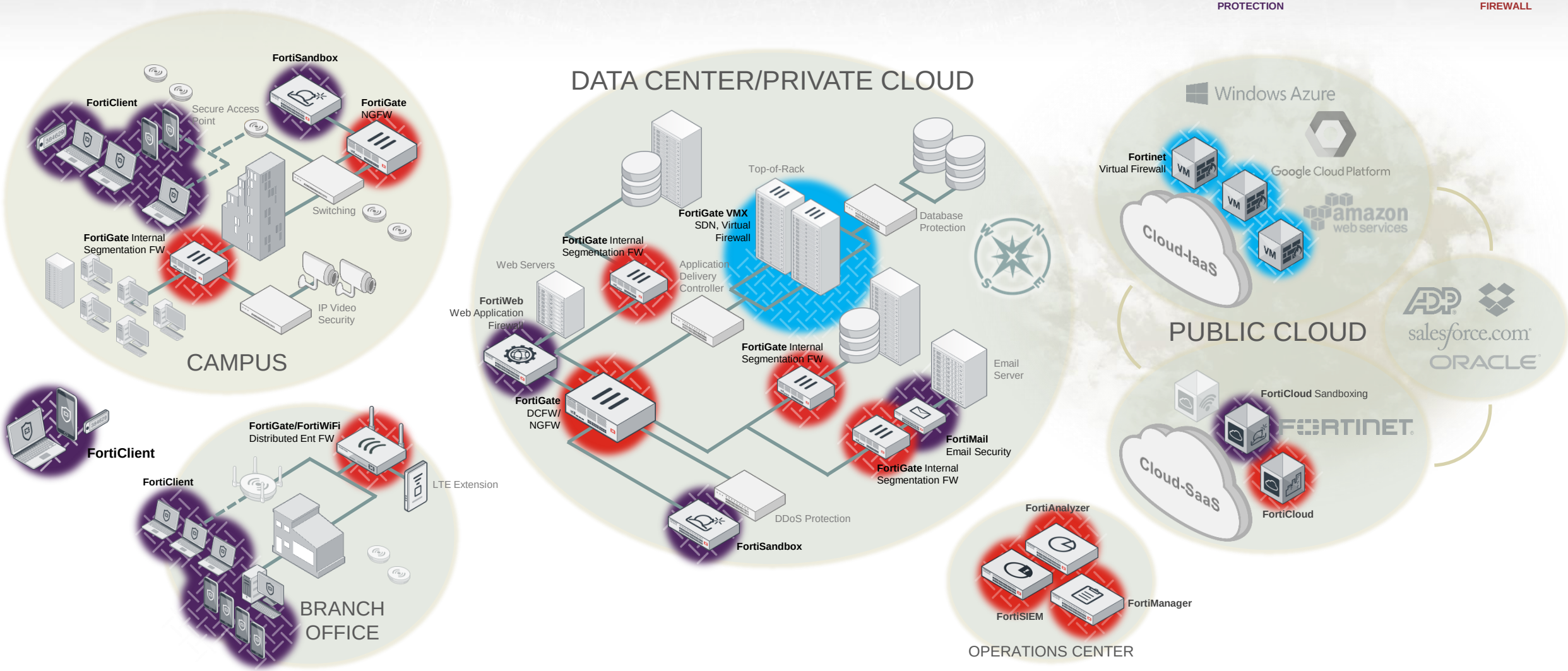


ФАБРИКА БЕЗОПАСНОСТИ FORTINET

ADVANCED THREAT PROTECTION

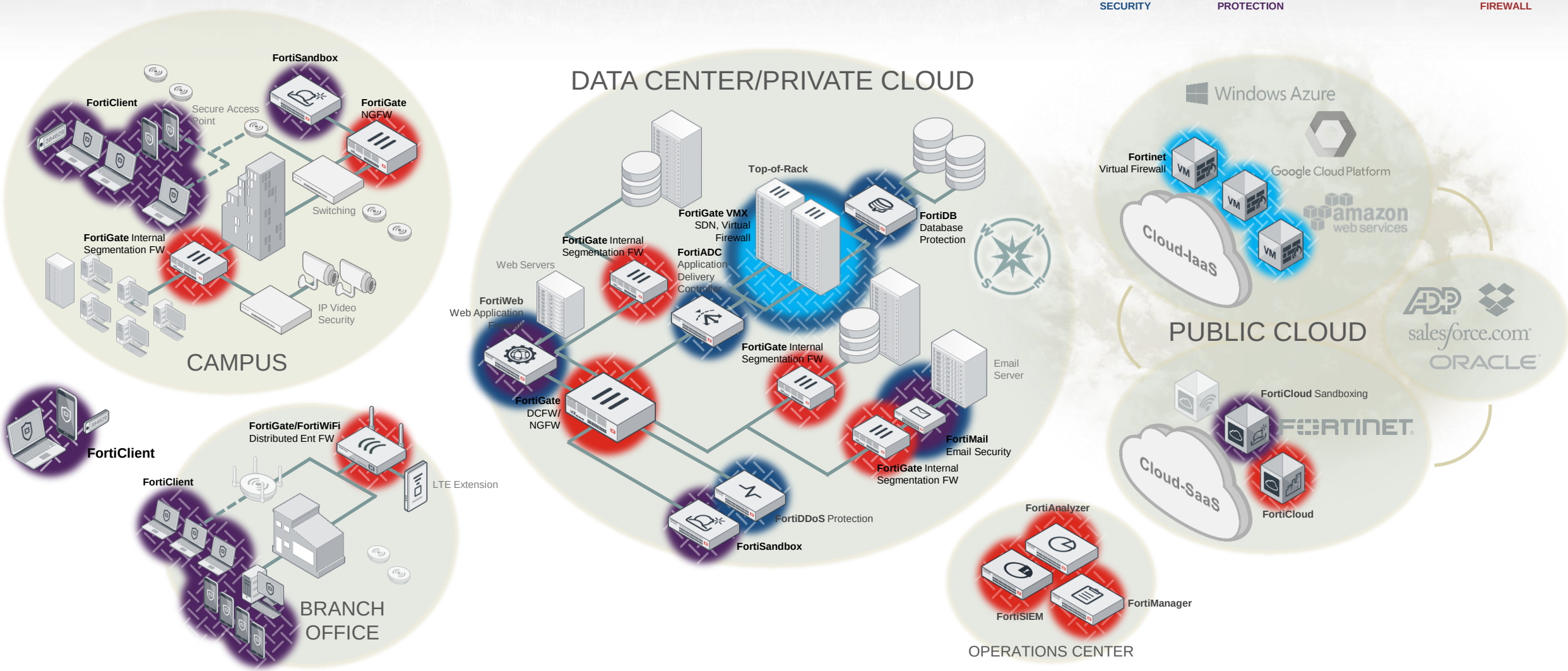
CLOUD SECURITY

ENTERPRISE FIREWALL



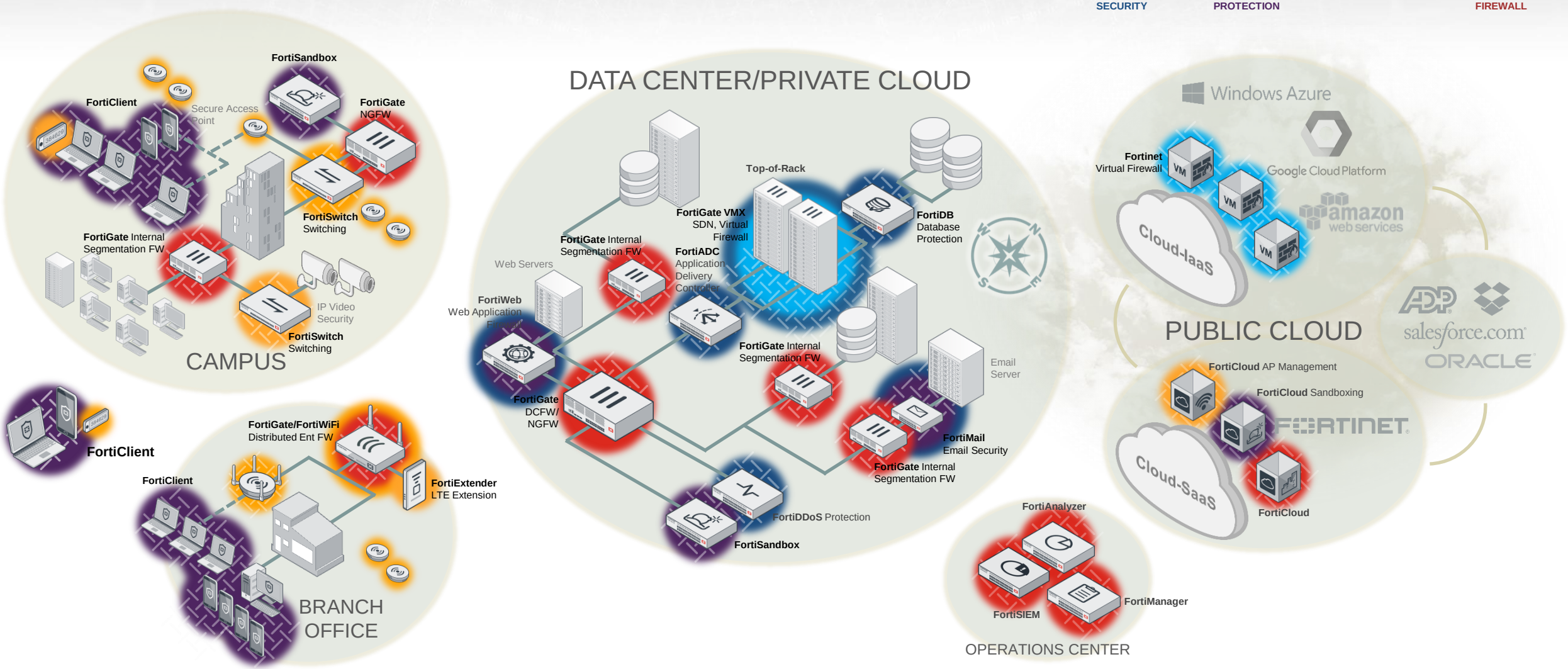
ФАБРИКА БЕЗОПАСНОСТИ FORTINET

APPLICATION SECURITY | ADVANCED THREAT PROTECTION | CLOUD SECURITY | ENTERPRISE FIREWALL

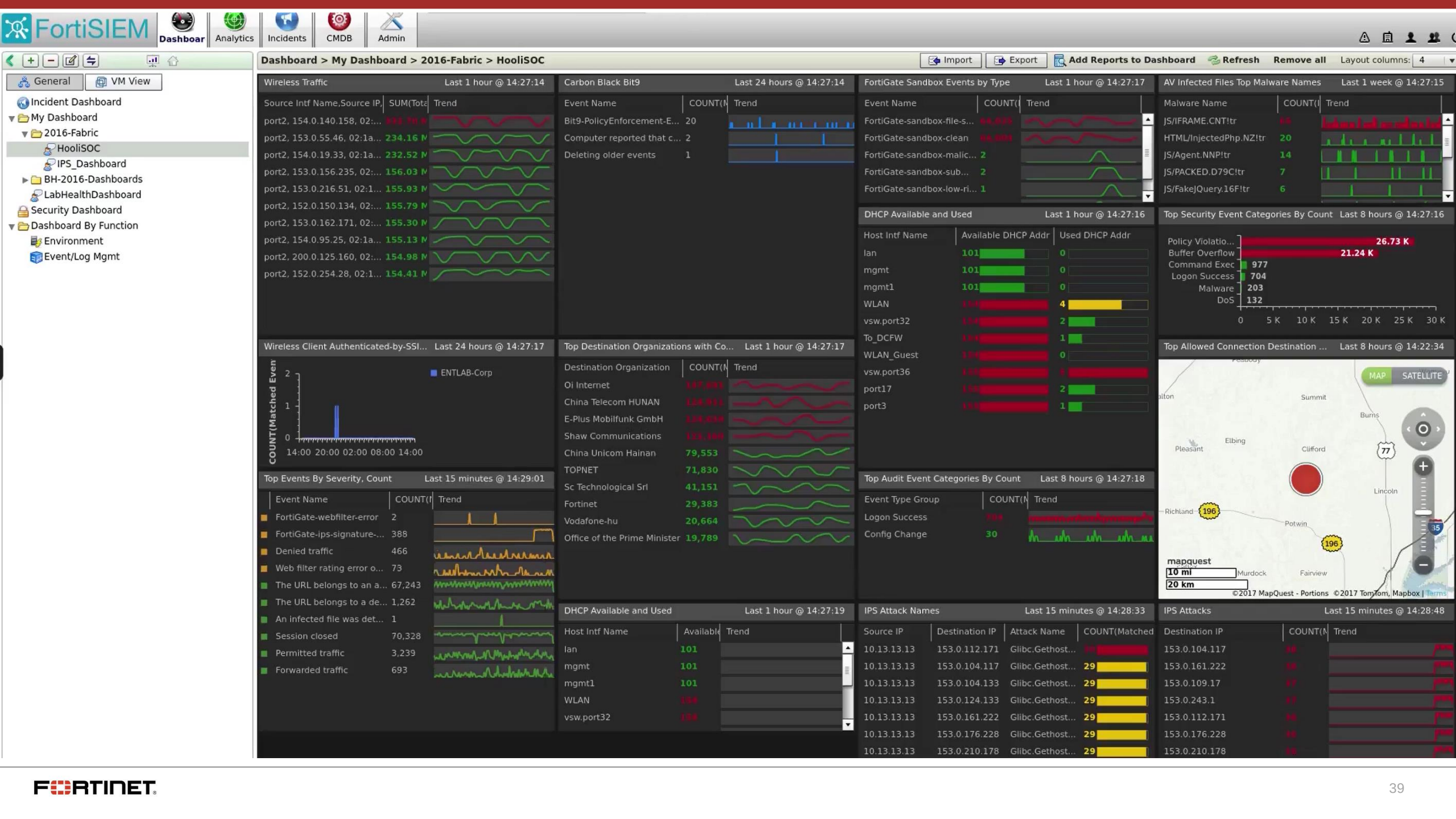


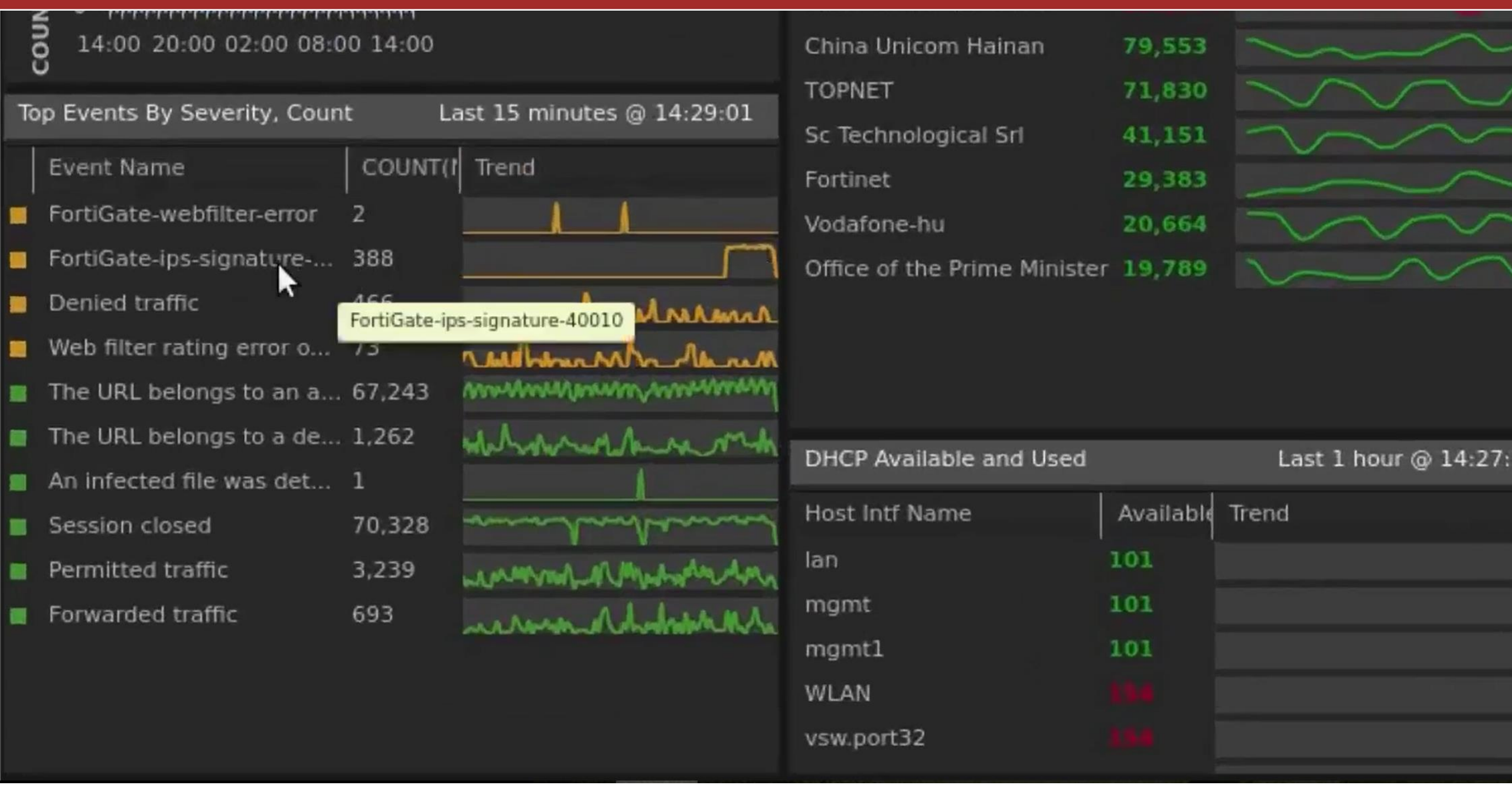
ФАБРИКА БЕЗОПАСНОСТИ FORTINET

SECURE ACCESS | APPLICATION SECURITY | ADVANCED THREAT PROTECTION | CLOUD SECURITY | ENTERPRISE FIREWALL

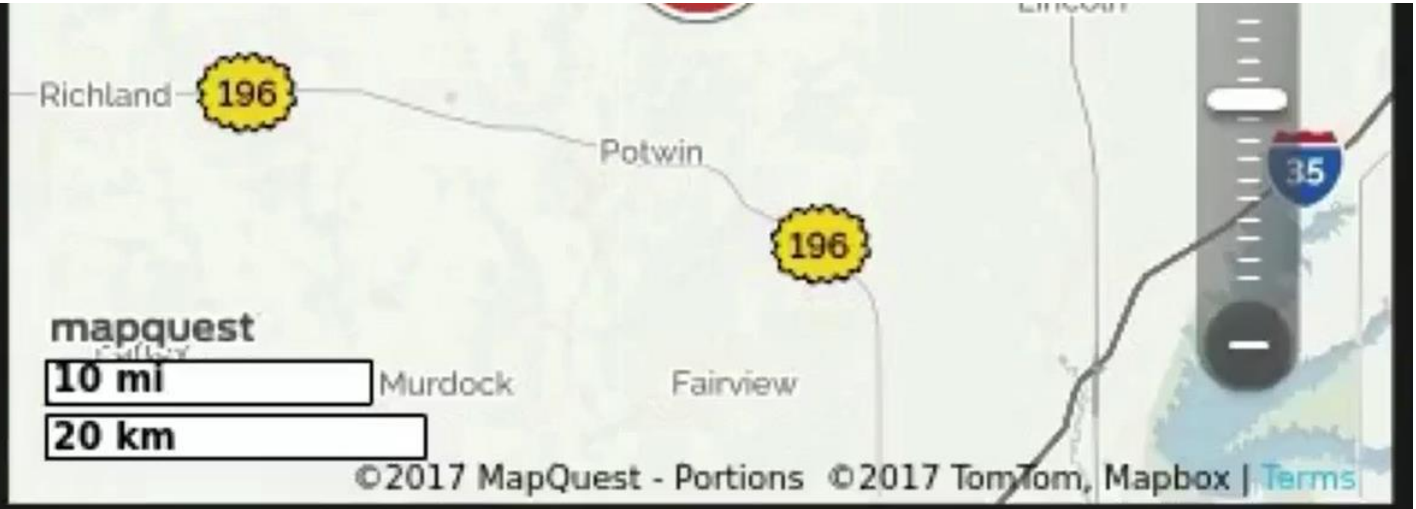


ПРИМЕР РАБОТЫ с ФАБРИКОЙ БЕЗОПАСНОСТИ


FortiSIEM
Dashboar
Analytics
Incidents
CMDB
Admin
Dashboard > My Dashboard > 2016-Fabric > HooliSOC
Import
Export
Add Reports to Dashboard
Refresh
Remove all
Layout columns: 4
General
VM View
Incident Dashboard
My Dashboard
2016-Fabric
HooliSOC
IPS_Dashboard
BH-2016-Dashboards
LabHealthDashboard
Security Dashboard
Dashboard By Function
Environment
Event/Log Mgmt
Wireless Traffic
Last 1 hour @ 14:27:14
Source Intf Name,Source IP,
SUM(Tota
Trend
port2, 154.0.140.158, 02:...
port2, 153.0.55.46, 02:1a... 234.16 M
port2, 154.0.19.33, 02:1a... 232.52 M
port2, 153.0.156.235, 02:... 156.03 M
port2, 153.0.216.51, 02:1... 155.93 M
port2, 152.0.150.134, 02:... 155.79 M
port2, 153.0.162.171, 02:... 155.30 M
port2, 154.0.95.25, 02:1a... 155.13 M
port2, 200.0.125.160, 02:... 154.98 M
port2, 152.0.254.28, 02:1... 154.41 M
Carbon Black Bit9
Last 24 hours @ 14:27:14
Event Name
COUNT(
Trend
Bit9-PolicyEnforcement-E... 20
Computer reported that c... 2
Deleting older events 1
FortiGate Sandbox Events by Type
Last 1 hour @ 14:27:17
Event Name
COUNT(
Trend
FortiGate-sandbox-file-s...
FortiGate-sandbox-clean
FortiGate-sandbox-malic... 2
FortiGate-sandbox-sub... 2
FortiGate-sandbox-low-ri... 1
AV Infected Files Top Malware Names
Last 1 week @ 14:27:15
Malware Name
COUNT(
Trend
JS/IFRAME.CNT!tr 44
HTML/InjectedPhp.NZ!tr 20
JS/Agent.NNP!tr 14
JS/PACKED.D79C!tr 7
JS/FakeJQuery.16F!tr 6
DHCP Available and Used
Last 1 hour @ 14:27:16
Host Intf Name
Available DHCP Addr
Used DHCP Addr
lan 101 0
mgmt 101 0
mgmt1 101 0
WLAN 4
vsw.port32 2
To_DCFW 1
WLAN_Guest 0
vsw.port36
port17 2
port3 1
Top Security Event Categories By Count
Last 8 hours @ 14:27:16
Policy Violatio... 26.73 K
Buffer Overflow 21.24 K
Command Exec 977
Logon Success 704
Malware 203
DoS 132
0
5 K
10 K
15 K
20 K
25 K
30 K
Wireless Client Authenticated-by-SSI...
Last 24 hours @ 14:27:17
COUNT(Matched Even
ENTLAB-Corp
2
1
0
14:00 20:00 02:00 08:00 14:00
Top Destination Organizations with Co...
Last 1 hour @ 14:27:17
Destination Organization
COUNT(
Trend
Oi Internet
China Telecom HUNAN
E-Plus Mobilfunk GmbH
Shaw Communications
China Unicom Hainan 79,553
TOPNET 71,830
Sc Technological Srl 41,151
Fortinet 29,383
Vodafone-hu 20,664
Office of the Prime Minister 19,789
Top Allowed Connection Destination ...
Last 8 hours @ 14:22:34
MAP
SATELLITE
Summit
Burns
Elbing
Pleasant
Clifford
77
Lincoln
Richland
196
Potwin
mapquest
10 mi
20 km
Murdock
Fairview
©2017 MapQuest - Portions ©2017 TomTom, Mapbox | Terms
Top Events By Severity, Count
Last 15 minutes @ 14:29:01
Event Name
COUNT(
Trend
FortiGate-webfilter-error 2
FortiGate-ips-signature-... 388
Denied traffic 466
Web filter rating error o... 73
The URL belongs to an a... 67,243
The URL belongs to a de... 1,262
An infected file was det... 1
Session closed 70,328
Permitted traffic 3,239
Forwarded traffic 693
Top Audit Event Categories By Count
Last 8 hours @ 14:27:18
Event Type Group
COUNT(
Trend
Logon Success
Config Change 30
DHCP Available and Used
Last 1 hour @ 14:27:19
Host Intf Name
Available
Trend
lan 101
mgmt 101
mgmt1 101
WLAN
vsw.port32
IPS Attack Names
Last 15 minutes @ 14:28:33
Source IP
Destination IP
Attack Name
COUNT(Matched
10.13.13.13 153.0.112.171 Glibc.Gethost...
10.13.13.13 153.0.104.117 Glibc.Gethost... 29
10.13.13.13 153.0.104.133 Glibc.Gethost... 29
10.13.13.13 153.0.124.133 Glibc.Gethost... 29
10.13.13.13 153.0.161.222 Glibc.Gethost... 29
10.13.13.13 153.0.176.228 Glibc.Gethost... 29
10.13.13.13 153.0.210.178 Glibc.Gethost... 29
IPS Attacks
Last 15 minutes @ 14:28:48
Destination IP
COUNT(
Trend
153.0.104.117
153.0.161.222
153.0.109.17
153.0.243.1
153.0.112.171
153.0.176.228
153.0.210.178


14:00 20:00 02:00 08:00 14:00
Top Events By Severity, Count
Last 15 minutes @ 14:29:01
Event Name
COUNT(
Trend
FortiGate-webfilter-error 2
FortiGate-ips-signature-... 388
Denied traffic
FortiGate-ips-signature-40010
Web filter rating error o... 73
The URL belongs to an a... 67,243
The URL belongs to a de... 1,262
An infected file was det... 1
Session closed 70,328
Permitted traffic 3,239
Forwarded traffic 693
China Unicom Hainan 79,553
TOPNET 71,830
Sc Technological Srl 41,151
Fortinet 29,383
Vodafone-hu 20,664
Office of the Prime Minister 19,789
DHCP Available and Used
Last 1 hour @ 14:27:
Host Intf Name
Available
Trend
lan 101
mgmt 101
mgmt1 101
WLAN
vsw.port32

Group	COUNT(N	Trend
ess	704	
nge	30	



Names — Last 15 minutes @ 14:28:33

	Destination IP	Attack Name	COUNT(Matched
3	153.0.112.171	Glibc.Gethost...	30
3	153.0.104.117	Glibc.Gethost...	29
3	153.0.104.133	Glibc.Gethost...	29
3	153.0.124.133	Glibc.Gethost...	29
3	153.0.161.222	Glibc.Gethost...	29
3	153.0.176.228	Glibc.Gethost...	29
3	153.0.210.178	Glibc.Gethost...	29

IPS Attacks — Last 15 minutes @ 14:28:48

Destination IP	COUNT(N	Trend
153.0.104.117	38	
153.0.161.222	38	
153.0.109.17	37	
153.0.243.1	37	
153.0.112.171	36	
153.0.176.228	36	
153.0.210.178	36	

Analytics > Real-time Search

Filter Criteria: Simple Structured Create Rule

Event Type CONTAIN FortiGate-ips-signature

Display Columns:

Source IP,Destination IP,Attack Name,Event Typ...

Search Historical Search

Pause Fast Forward Stop Clear Filter Quick Info Locations

34 events in the last 13s Updated records:5

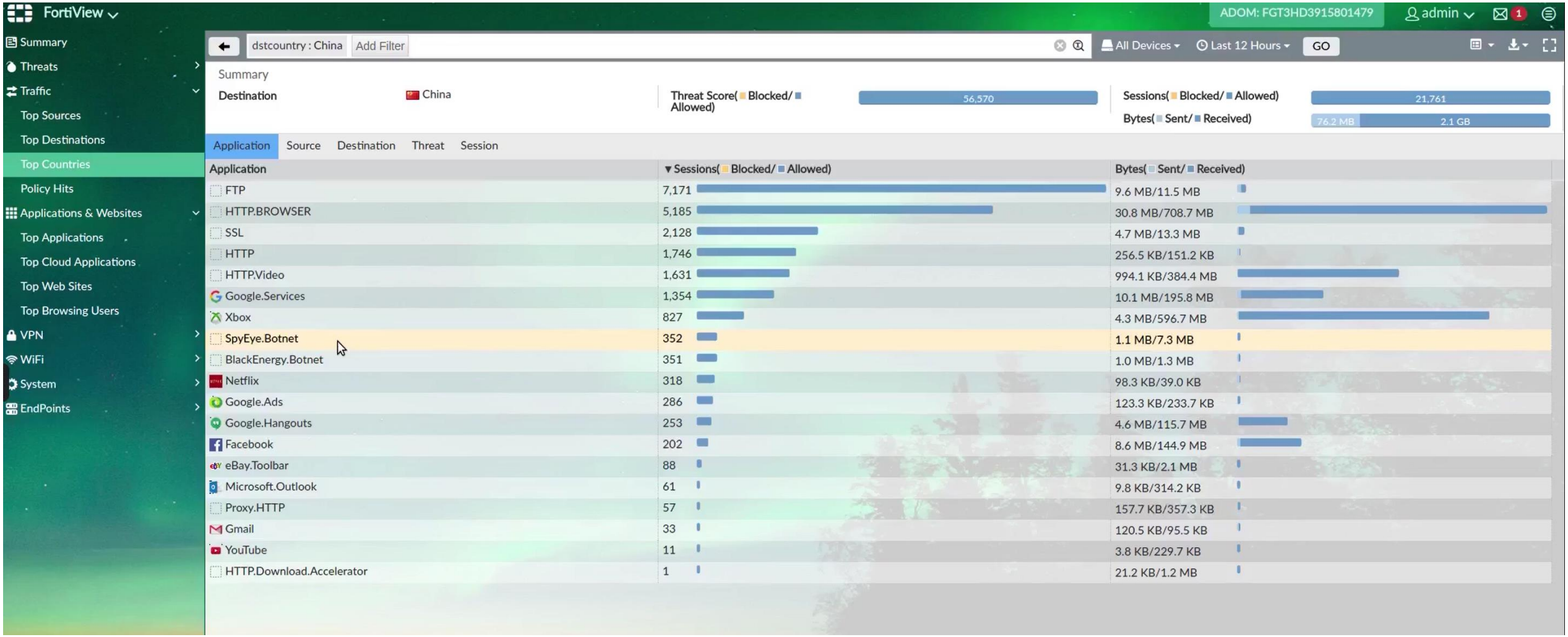
Source IP	Destination IP	Attack Name	Event Type	Application Name
10.13.13.13	153.0.176.228	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.243.1	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.210.178	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.124.133	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.104.133	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.104.117	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.161.222	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.109.17	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.174.181	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.112.171	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.176.228	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.243.1	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.210.178	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.124.133	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.104.133	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.104.117	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.109.17	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.174.181	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.161.222	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.174.181	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.124.133	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.104.117	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.210.178	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.161.222	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.112.171	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.210.178	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.104.133	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	
10.13.13.13	153.0.243.1	Glibc.Gethostbyname.Buffer.Overflow	FortiGate-ips-signature-40010	

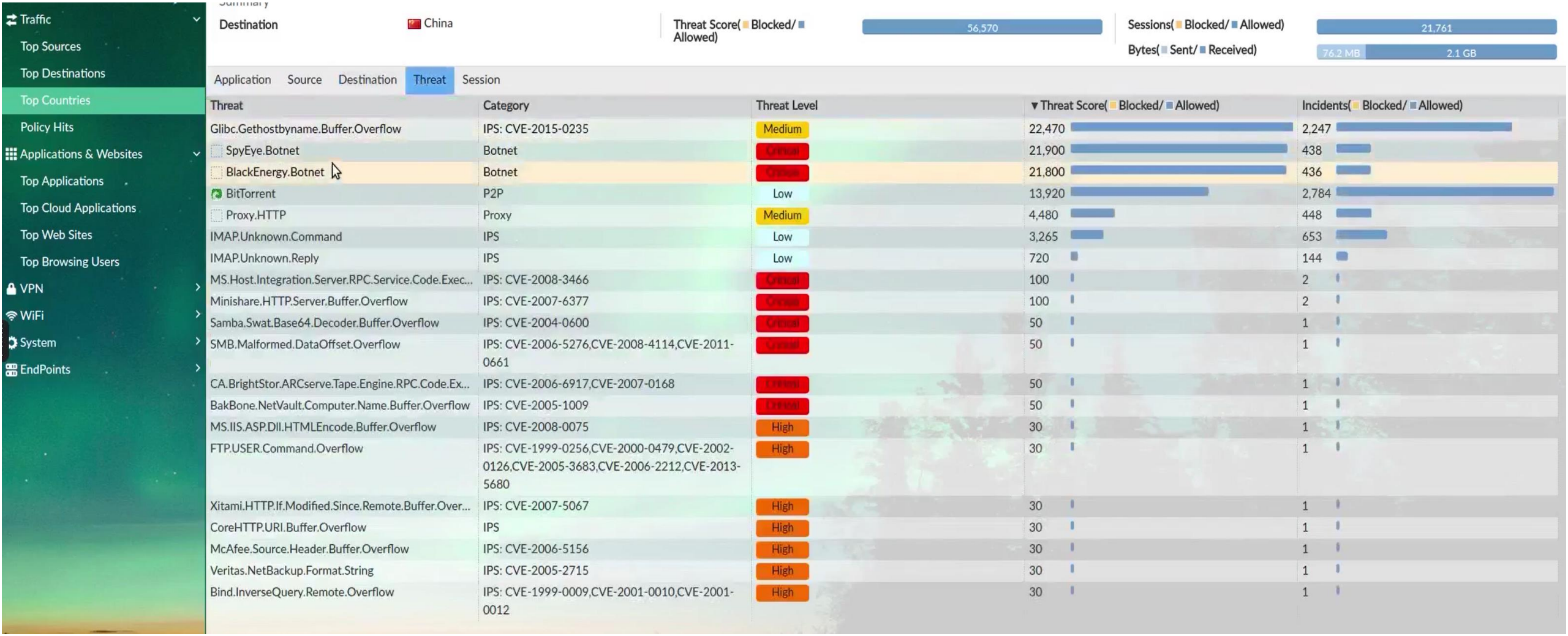
Threat	SpyEye.Botnet	Category	Botnet
Threat Score(Blocked/ Allowed)	17,800	Incidents(Blocked/ Allowed)	356
Threat Level	Critical		

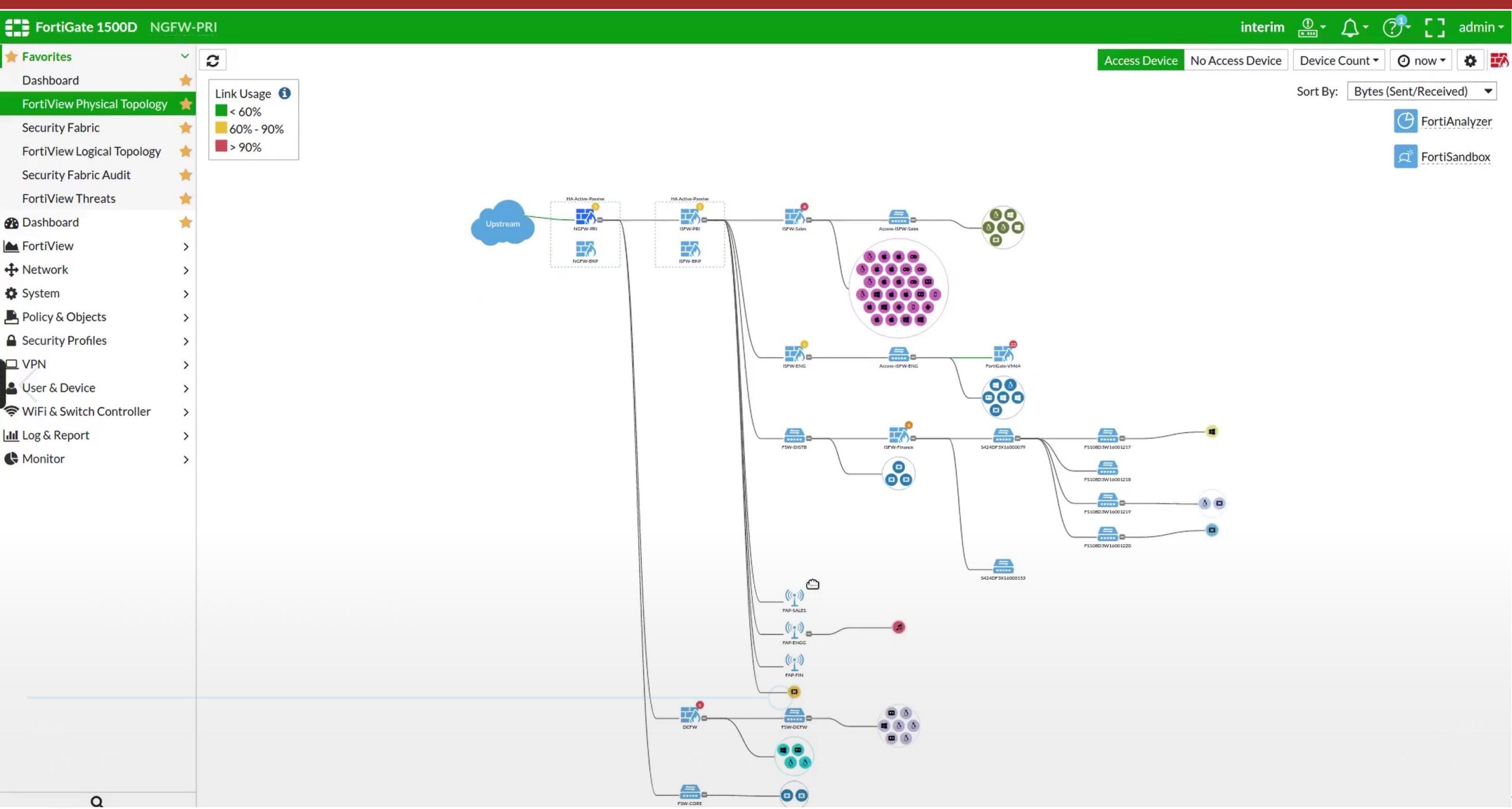
Source | Destination | Country | Session

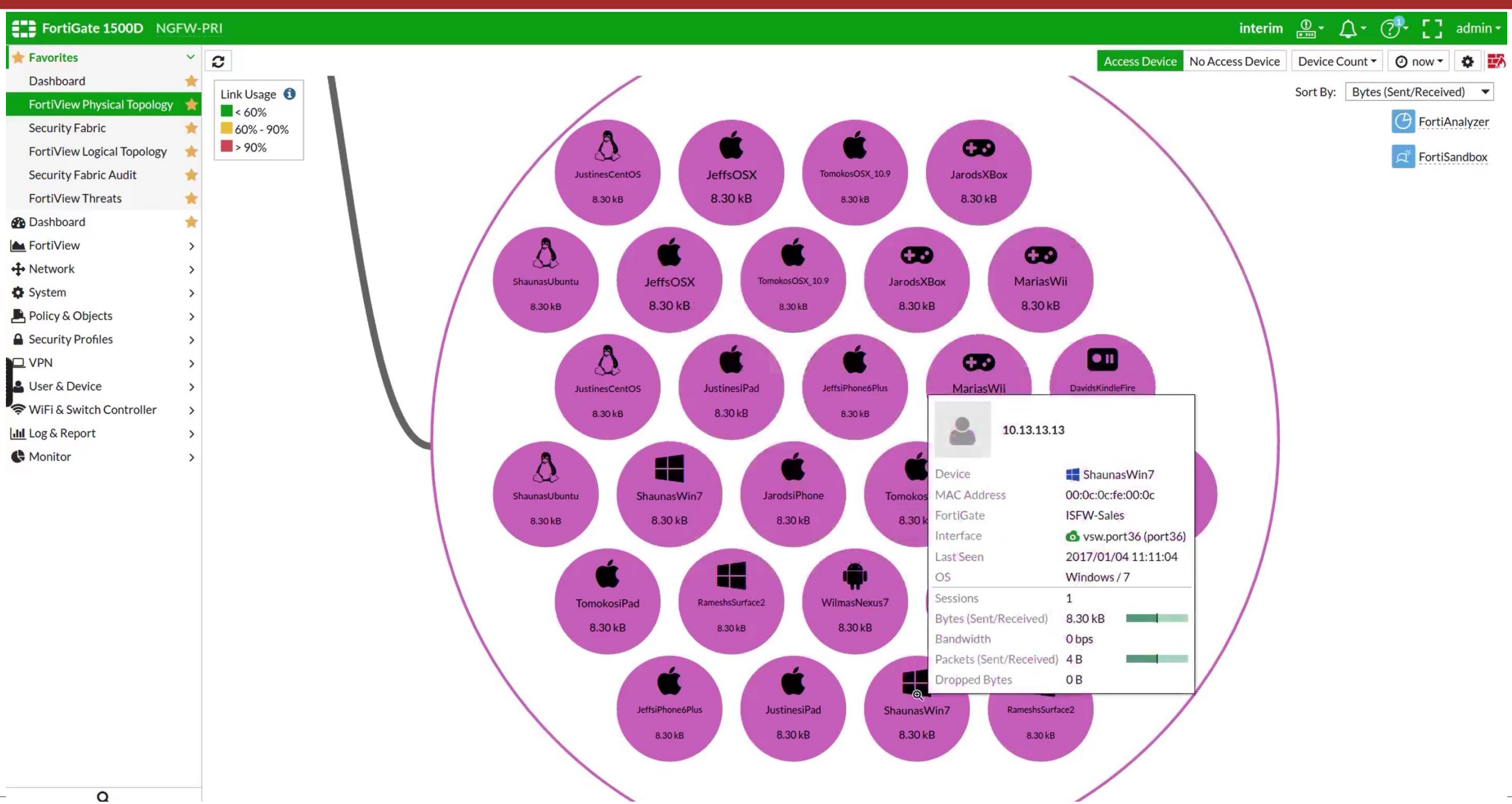
▲ Date/Time	Source/Device	Destination	Service	Sent/Received	User	Application	Security Action
01-03 14:32	10.13.13.13	153.0.162.122	HTTP	3.4 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.102.24	HTTP	3.2 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.31.59	HTTP	3.2 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.11.51	HTTP	3.2 KB/21.2 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.139.121	HTTP	3.2 KB/21.2 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.25.92	HTTP	3.2 KB/21.2 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.145.213	HTTP	3.0 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.36.118	HTTP	3.0 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.45.174	HTTP	3.5 KB/21.2 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.170.219	HTTP	2.9 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.162.122	HTTP	3.8 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.102.24	HTTP	3.2 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.31.59	HTTP	3.2 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.11.51	HTTP	3.1 KB/21.2 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.139.121	HTTP	3.2 KB/21.2 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.25.92	HTTP	3.2 KB/21.2 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.145.213	HTTP	3.0 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.36.118	HTTP	3.0 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.45.174	HTTP	3.5 KB/21.2 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.170.219	HTTP	2.9 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.162.122	HTTP	3.8 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.102.24	HTTP	3.2 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.31.59	HTTP	3.2 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.11.51	HTTP	3.2 KB/21.2 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.139.121	HTTP	3.2 KB/21.2 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.25.92	HTTP	3.2 KB/21.2 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.145.213	HTTP	3.0 KB/21.1 KB		SpyEye.Botnet	
01-03 14:31	10.13.13.13	153.0.36.118	HTTP	3.0 KB/21.1 KB		SpyEye.Botnet	
01-03 14:30	10.13.13.13	153.0.45.174	HTTP	3.5 KB/21.2 KB		SpyEye.Botnet	
01-03 14:30	10.13.13.13	153.0.170.219	HTTP	2.9 KB/21.1 KB		SpyEye.Botnet	
01-03 14:30	10.13.13.13	153.0.162.122	HTTP	3.4 KB/21.1 KB		SpyEye.Botnet	

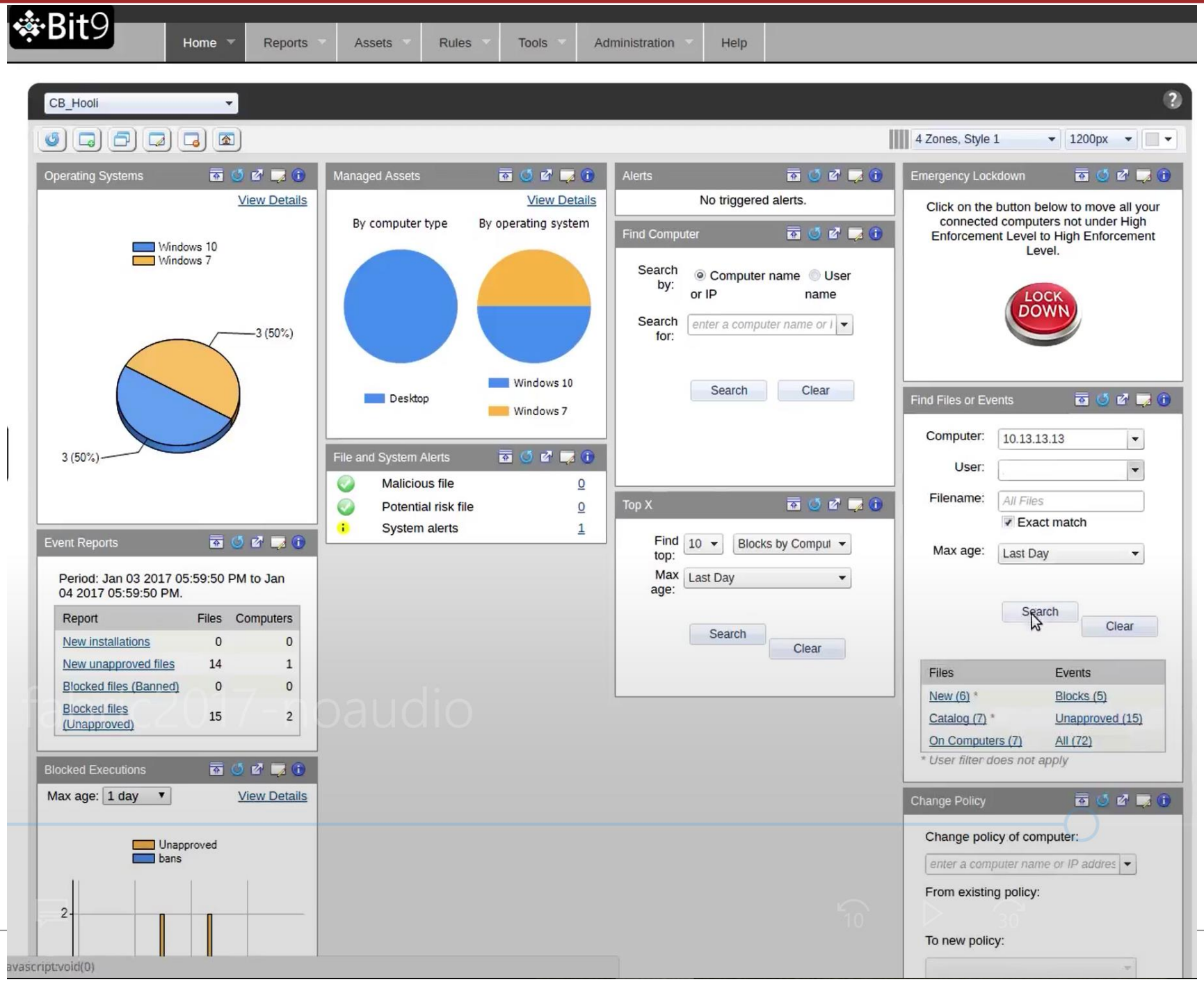

FortiView
ADOM: FGT3HD3915801479
admin
Summary
Threats
Traffic
Applications & Websites
Top Applications
Top Cloud Applications
Top Web Sites
Top Browsing Users
VPN
WiFi
System
EndPoints
Add Filter
All Devices
Last 12 Hours
GO
Application | Category | Risk | Sessions(Blocked/ Allowed) | Bytes(Sent/ Received)
Proxy.HTTP | Proxy | Critical | 1,401 | 113.0 MB/422.4 MB
BlackEnergy.Botnet | Botnet | Critical | 276 | 818.9 KB/1019.5 KB
SpyEye.Botnet | Botnet | Critical | 283 | 902.0 KB/5.8 MB
RDP | Remote.Access | High | 3 | 12.1 KB/8.6 KB
BitTorrent | P2P | High | 16 | 9.3 KB/32.4 KB
POP3 | Email | Medium | 8 | 4.4 KB/11.6 KB
SMTP | Email | Medium | 4 | 5.8 KB/3.0 KB
SSL | Network.Service | Medium | 14,430 | 36.1 MB/97.9 MB
Facebook | Social.Media | Medium | 2,499 | 99.6 MB/1.7 GB
IMAP | Email | Medium | 1 | 3.1 KB/6.7 KB
Gmail | Email | Medium | 505 | 1.5 MB/1.3 MB
Microsoft.Outlook | Email | Medium | 576 | 124.8 KB/3.3 MB
HTTP.BROWSER | Web.Client | Medium | 17,715 | 99.0 MB/2.1 GB
Netflix | Video/Audio | Elevated | 1,084 | 364.1 KB/137.3 KB
RTMP | Video/Audio | Elevated | 8 | 3.6 KB/7.8 KB
SSH | Network.Service | Elevated | 9 | 87.4 KB/171.7 KB
Skype | Collaboration | Elevated | 7 | 1.6 KB/4.1 KB
Citrix.ICA | General.Interest | Elevated | 13 | 339.2 KB/1.3 MB
FTP | Network.Service | Elevated | 29,675 | 39.7 MB/47.3 MB
Google.Accounts | General.Interest | Elevated | 223 | 360.5 KB/3.5 MB
Google.Ads | General.Interest | Elevated | 413 | 185.4 KB/337.9 KB
Google.Hangouts | Collaboration | Elevated | 2,170 | 88.5 MB/1.0 GB
Google.Plus | Social.Media | Elevated | 282 | 11.2 MB/292.7 MB
Google.Services | General.Interest | Elevated | 3,052 | 24.4 MB/457.6 MB
HTTP.Download.Accelerator | General.Interest | Elevated | 1 | 21.2 KB/1.2 MB
HTTP.Video | Video/Audio | Elevated | 7,103 | 4.2 MB/1.6 GB
IRC | Collaboration | Elevated | 22 | 553.7 KB/1.3 MB
LinkedIn | Social.Media | Elevated | 278 | 12.3 MB/18.0 MB
Microsoft.Portal | Collaboration | Elevated | 609 | 8.8 MB/12.2 MB
BGP | Network.Service | Elevated | 2 | 956.0 B/1.0 KB
Windows.File.Sharing | Network.Service | Elevated | 4 | 4.0 KB/3.8 KB
Xbox | Game | Elevated | 3,519 | 20.4 MB/2.7 GB
0:03:57


FortiView
ADOM: FGT3HD3915801479
admin
1
Summary
Threats
Traffic
Top Sources
Top Destinations
Top Countries
Policy Hits
Applications & Websites
Top Applications
Top Cloud Applications
Top Web Sites
Top Browsing Users
VPN
WiFi
System
EndPoints
dstcountry : China
Add Filter
All Devices
Last 12 Hours
GO
Summary
Destination
China
Threat Score(Blocked/ Allowed)
56,570
Sessions(Blocked/ Allowed)
21,761
Bytes(Sent/ Received)
76.2 MB
2.1 GB
Application
Source
Destination
Threat
Session
Application
▼Sessions(Blocked/ Allowed)
Bytes(Sent/ Received)
FTP 7,171 9.6 MB/11.5 MB
HTTP.BROWSER 5,185 30.8 MB/708.7 MB
SSL 2,128 4.7 MB/13.3 MB
HTTP 1,746 256.5 KB/151.2 KB
HTTP.Video 1,631 994.1 KB/384.4 MB
Google.Services 1,354 10.1 MB/195.8 MB
Xbox 827 4.3 MB/596.7 MB
SpyEye.Botnet 352 1.1 MB/7.3 MB
BlackEnergy.Botnet 351 1.0 MB/1.3 MB
Netflix 318 98.3 KB/39.0 KB
Google.Ads 286 123.3 KB/233.7 KB
Google.Hangouts 253 4.6 MB/115.7 MB
Facebook 202 8.6 MB/144.9 MB
eBay.Toolbar 88 31.3 KB/2.1 MB
Microsoft.Outlook 61 9.8 KB/314.2 KB
Proxy.HTTP 57 157.7 KB/357.3 KB
Gmail 33 120.5 KB/95.5 KB
YouTube 11 3.8 KB/229.7 KB
HTTP.Download.Accelerator 1 21.2 KB/1.2 MB


Traffic
Top Sources
Top Destinations
Top Countries
Policy Hits
Applications & Websites
Top Applications
Top Cloud Applications
Top Web Sites
Top Browsing Users
VPN
WiFi
System
EndPoints
Destination
China
Threat Score(Blocked/ Allowed)
56,570
Sessions(Blocked/ Allowed)
21,761
Bytes(Sent/ Received)
76.2 MB
2.1 GB
Application
Source
Destination
Threat
Session
Threat
Category
Threat Level
▼Threat Score(Blocked/ Allowed)
Incidents(Blocked/ Allowed)
Glibc.Gethostbyname.Buffer.Overflow
IPS: CVE-2015-0235
Medium
22,470
2,247
SpyEye.Botnet
Botnet
Critical
21,900
438
BlackEnergy.Botnet
Botnet
Critical
21,800
436
BitTorrent
P2P
Low
13,920
2,784
Proxy.HTTP
Proxy
Medium
4,480
448
IMAP.Unknown.Command
IPS
Low
3,265
653
IMAP.Unknown.Reply
IPS
Low
720
144
MS.Host.Integration.Server.RPC.Service.Code.Exec...
IPS: CVE-2008-3466
Critical
100
2
Minishare.HTTP.Server.Buffer.Overflow
IPS: CVE-2007-6377
Critical
100
2
Samba.Swat.Base64.Decoder.Buffer.Overflow
IPS: CVE-2004-0600
Critical
50
1
SMB.Malformed.DataOffset.Overflow
IPS: CVE-2006-5276,CVE-2008-4114,CVE-2011-0661
Critical
50
1
CA.BrightStor.ARCserve.Tape.Engine.RPC.Code.Ex...
IPS: CVE-2006-6917,CVE-2007-0168
Critical
50
1
BakBone.NetVault.Computer.Name.Buffer.Overflow
IPS: CVE-2005-1009
Critical
50
1
MS.IIS.ASP.Dll.HTMLEncode.Buffer.Overflow
IPS: CVE-2008-0075
High
30
1
FTP.USER.Command.Overflow
IPS: CVE-1999-0256,CVE-2000-0479,CVE-2002-0126,CVE-2005-3683,CVE-2006-2212,CVE-2013-5680
High
30
1
Xitami.HTTP.If.Modified.Since.Remote.Buffer.Over...
IPS: CVE-2007-5067
High
30
1
CoreHTTP.URI.Buffer.Overflow
IPS
High
30
1
McAfee.Source.Header.Buffer.Overflow
IPS: CVE-2006-5156
High
30
1
Veritas.NetBackup.Format.String
IPS: CVE-2005-2715
High
30
1
Bind.InverseQuery.Remote.Overflow
IPS: CVE-1999-0009,CVE-2001-0010,CVE-2001-0012
High
30
1


FortiGate 1500D
NGFW-PRI
interim
admin
Favorites
Dashboard
FortiView Physical Topology
Security Fabric
FortiView Logical Topology
Security Fabric Audit
FortiView Threats
Dashboard
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
WiFi & Switch Controller
Log & Report
Monitor
Link Usage
< 60%
60% - 90%
> 90%
Access Device
No Access Device
Device Count
now
Sort By:
Bytes (Sent/Received)
FortiAnalyzer
FortiSandbox
Upstream
NGFW-PRI
NGFW-BKP
ISFW-PRI
ISFW-BKP
ISFW-Sales
Access-ISFW-Sales
ISFW-ENG
Access-ISFW-ENG
FortiGate-VM64
FSW-DISTB
ISFW-Finance
S424DF3X16000079
FS108D3W16001217
FS108D3W16001218
FS108D3W16001219
FS108D3W16001220
S424DF3X16000153
FAP-SALES
FAP-ENGG
FAP-FIN
DCFW
FSW-DCFW
FSW-CORE


FortiGate 1500D NGFW-PRI
interim
admin
Favorites
Dashboard
FortiView Physical Topology
Security Fabric
FortiView Logical Topology
Security Fabric Audit
FortiView Threats
Dashboard
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
WiFi & Switch Controller
Log & Report
Monitor
Access Device
No Access Device
Device Count
now
Sort By:
Bytes (Sent/Received)
FortiAnalyzer
FortiSandbox
Link Usage
< 60%
60% - 90%
> 90%
JustinesCentOS 8.30 kB
JeffsOSX 8.30 kB
TomokosOSX_10.9 8.30 kB
JarodsXBox 8.30 kB
ShaunasUbuntu 8.30 kB
JeffsOSX 8.30 kB
TomokosOSX_10.9 8.30 kB
JarodsXBox 8.30 kB
MariasWii 8.30 kB
JustinesCentOS 8.30 kB
JustinesiPad 8.30 kB
JeffsiPhone6Plus 8.30 kB
MariasWii
DavidsKindleFire
ShaunasUbuntu 8.30 kB
ShaunasWin7 8.30 kB
JarodsiPhone 8.30 kB
TomokosiPad 8.30 kB
RameshsSurface2 8.30 kB
WilmasNexus7 8.30 kB
JeffsiPhone6Plus 8.30 kB
JustinesiPad 8.30 kB
ShaunasWin7 8.30 kB
RameshsSurface2 8.30 kB
10.13.13.13
Device ShaunasWin7
MAC Address 00:0c:0c:fe:00:0c
FortiGate ISFW-Sales
Interface vsw.port36 (port36)
Last Seen 2017/01/04 11:11:04
OS Windows / 7
Sessions 1
Bytes (Sent/Received) 8.30 kB
Bandwidth 0 bps
Packets (Sent/Received) 4 B
Dropped Bytes 0 B


Bit9
Home
Reports
Assets
Rules
Tools
Administration
Help
CB_Hooli
4 Zones, Style 1
1200px
Operating Systems
View Details
Windows 10
Windows 7
3 (50%)
3 (50%)
Managed Assets
View Details
By computer type
By operating system
Desktop
Windows 10
Windows 7
Alerts
No triggered alerts.
Emergency Lockdown
Click on the button below to move all your connected computers not under High Enforcement Level to High Enforcement Level.
LOCK DOWN
Find Computer
Search by:
Computer name
User name
or IP
Search for:
enter a computer name or I
Search
Clear
File and System Alerts
Malicious file 0
Potential risk file 0
System alerts 1
Top X
Find top:
10
Blocks by Compul
Max age:
Last Day
Search
Clear
Find Files or Events
Computer:
10.13.13.13
User:
Filename:
All Files
Exact match
Max age:
Last Day
Search
Clear
Files
Events
New (6) *
Blocks (5)
Catalog (7) *
Unapproved (15)
On Computers (7)
All (72)
* User filter does not apply
Event Reports
Period: Jan 03 2017 05:59:50 PM to Jan 04 2017 05:59:50 PM.
Report
Files
Computers
New installations 0 0
New unapproved files 14 1
Blocked files (Banned) 0 0
Blocked files (Unapproved) 15 2
Blocked Executions
Max age: 1 day
View Details
Unapproved
bans
2
Change Policy
Change policy of computer:
enter a computer name or IP addres
From existing policy:
To new policy:
javascript:void(0)

Server Management	File analysis requested	Hooli\WIN7-SHAUNA	User 'System' requested analysis of file 'googleupdatesetup.exe' [3C79F...420F0] with 'FortiSandbox'.	10.13.13.13
Server Management	File analysis requested	Hooli\WIN7-SHAUNA	User 'System' requested analysis of file 'fsa_downloader.exe' [5C53B...932D6] with 'FortiSandbox'.	10.13.13.13
Server Management	File analysis requested	Hooli\WIN7-SHAUNA	User 'System' requested analysis of file 'totally_legit.exe' [C0E14...3B96E] with 'FortiSandbox'.	10.13.13.13
Server Management	File analysis requested	Hooli\WIN7-SHAUNA	User 'System' requested analysis of file 'pepflashplayer.dll' [7CFE1...1968A] with 'FortiSandbox'.	10.13.13.13
Server Management	File analysis requested	Hooli\WIN7-SHAUNA	User 'System' requested analysis of file 'fsa_downloader.exe' [5C53B...932D6] with 'FortiSandbox'.	10.13.13.13
Discovery	Certificate checked	Hooli\WIN7-SHAUNA	Agent detected that certificate 'Symantec SHA256 TimeStamping CA Symantec Trust Network Symantec Corporation US' is valid.	10.13.13.13
Discovery	Certificate checked	Hooli\WIN7-SHAUNA	Agent detected that certificate 'VeriSign Universal Root Certification Authority "(c) 2008 VeriSign, Inc. - For authorized use only" VeriSign Trust Network "VeriSign, Inc." US' is valid.	10.13.13.13
Server Management	File analysis completed	Hooli\WIN7-SHAUNA	File 'totally_legit.exe' [C0E14...3B96E] was successfully analyzed with 'FortiSandbox'. Zero Day Malware (SpyEye) found.	10.13.13.13
Discovery	New unapproved file to computer	Hooli\WIN7-SHAUNA	Computer Hooli\WIN7-SHAUNA discovered new file 'c:\users\shauna\appdata\local\google\chrome\user data\pepperflash\24.0.0.186\pepflashplayer.dll' [7CFE1...1968A]. DiscoveredBy[Kernel:Rename] FileCreated[1/3/2017 8:38:26 PM] Discovered[1/3/2017 8:38:26 PM (Hash: 1/3/2017 8:38:26 PM)]	10.13.13.13
Discovery	New file on network	Hooli\WIN7-SHAUNA	Server discovered new file 'c:\users\shauna\appdata\local\google\chrome\user data\pepperflash\24.0.0.186\pepflashplayer.dll' [7CFE1...1968A].	10.13.13.13
Policy Enforcement	Execution prompt allowed (unapproved file)	Hooli\WIN7-SHAUNA	File 'c:\users\shauna\downloads\totally_legit.exe' [C0E14...3B96E] was approved because of user response.	10.13.13.13
Discovery	First execution on network	Hooli\WIN7-SHAUNA	File 'c:\users\shauna\downloads\totally_legit.exe' [C0E14...3B96E] was executed for the first time.	10.13.13.13
Discovery	Certificate checked	Hooli\WIN7-SHAUNA	Agent detected that certificate 'Symantec SHA256 TimeStamping Signer - G1 Symantec Trust Network Symantec Corporation US' is valid.	10.13.13.13
Server Management	File analysis requested	Hooli\WIN7-SHAUNA	Analysis of file 'totally_legit.exe' [C0E14...3B96E] with 'FortiSandbox' was requested by event rule 'FortiSandbox-Fabric'.	10.13.13.13
Discovery	New unapproved file to computer	Hooli\WIN7-SHAUNA	Computer Hooli\WIN7-SHAUNA discovered new file 'c:\users\shauna\downloads\totally_legit.exe' [C0E14...3B96E]. DiscoveredBy[Kernel:Rename] FileCreated[1/3/2017 8:37:16 PM] Discovered[1/3/2017 8:38:00 PM (Hash: 1/3/2017 8:37:16 PM)]	10.13.13.13

High Risk Botnet (SpyEye)

Mark as clean (false positive)

Received	Jan 04 2017 14:38:00
Started	Jan 04 2017 14:38:30
Status	Done
Rated By	VM Engine
Submit Type	Adapter
Digital Signature	No
Scan Bypass Configuration	N/A
Virus Total	

More Details

File Type	exe
Downloaded From	totally_legit.exe
File Size	40842696 (bytes)
MD5	69377ea4959c5bf135de270cbfe4dfab
SHA1	6d1b174df3fd820e584377ef5ece0aeb68d52754
SHA256	2c9b00edcfdb69858f177c4de75dd6e0386365a4a2aeea9654f88d5f78edcabc
ID	3153681576566354530
Submitted By	CarbonBlack
Submitted Filename	totally_legit.exe
Filename	totally_legit.exe
Start Time	Jan 04 2017 14:38:00
Finish Time	Jan 04 2017 14:38:30
Scan Time	30 seconds
Scan Unit	FSA3KD3R16000092
Device	ADPBIT1483560804
Detection OS	WIN7X64VM
Infected OS	WIN7X64VM
Adapter IP	192.168.113.110 -> 192.168.113.110
Platform	Microsoft Windows 7 x64 Professional Service Pack 1 (6.1.7601)

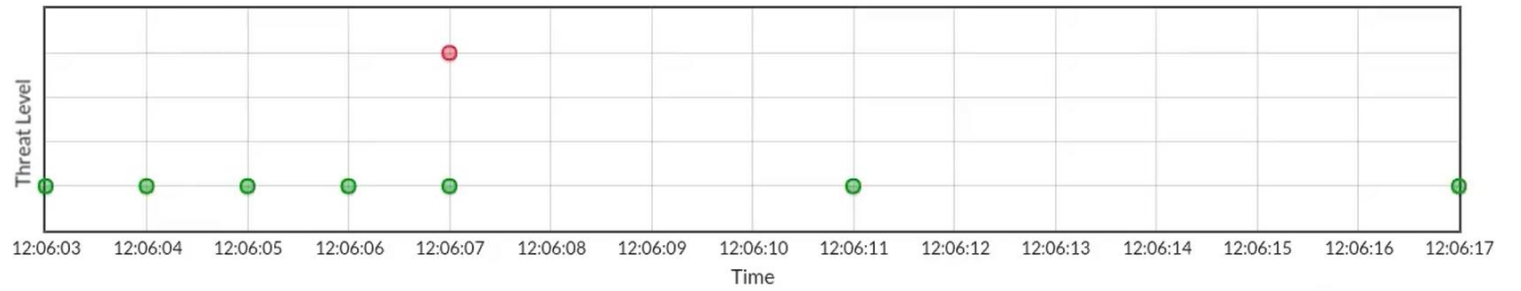
Behavior Summary

Analysis Details

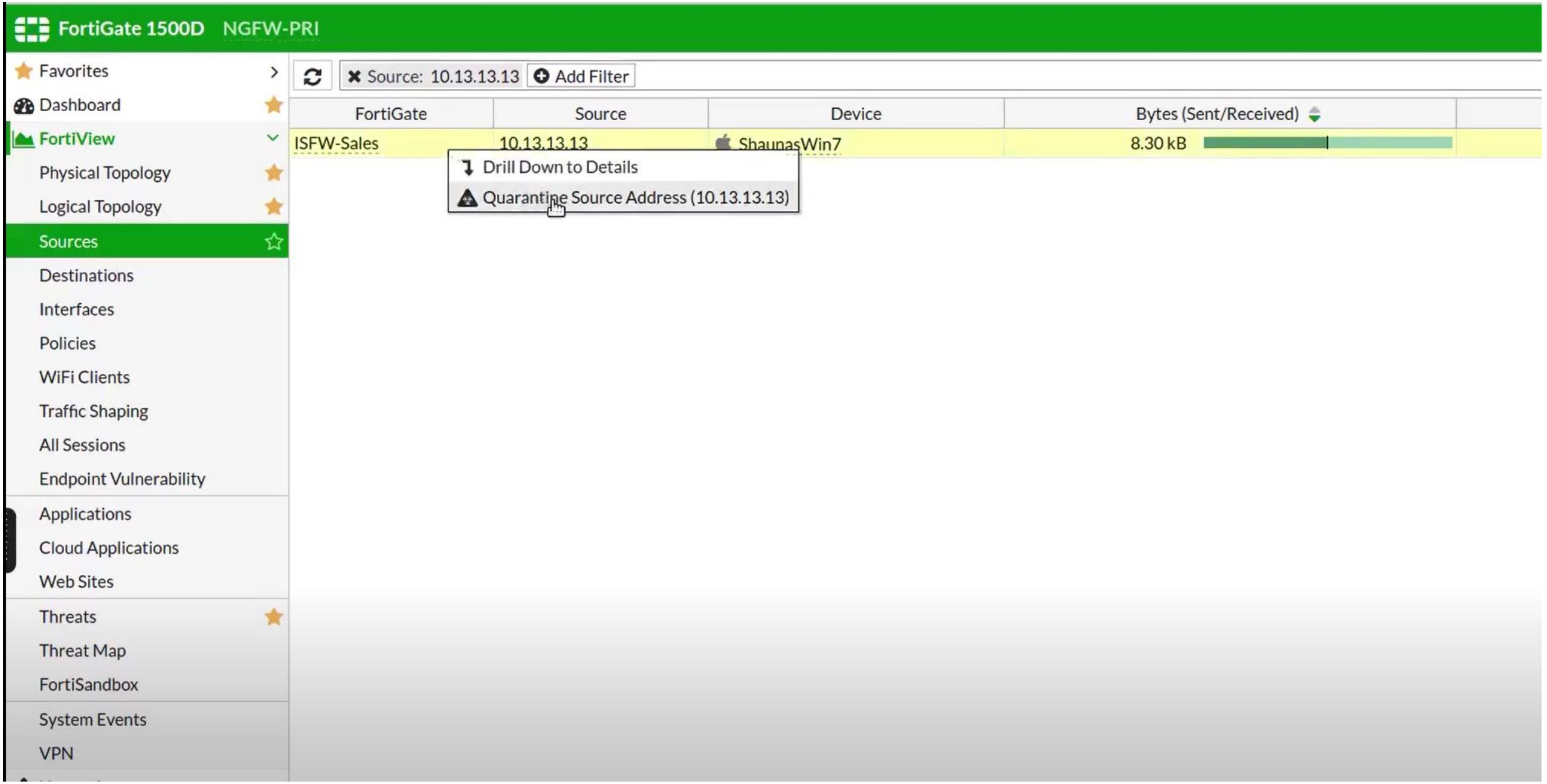
WIN7X64VM

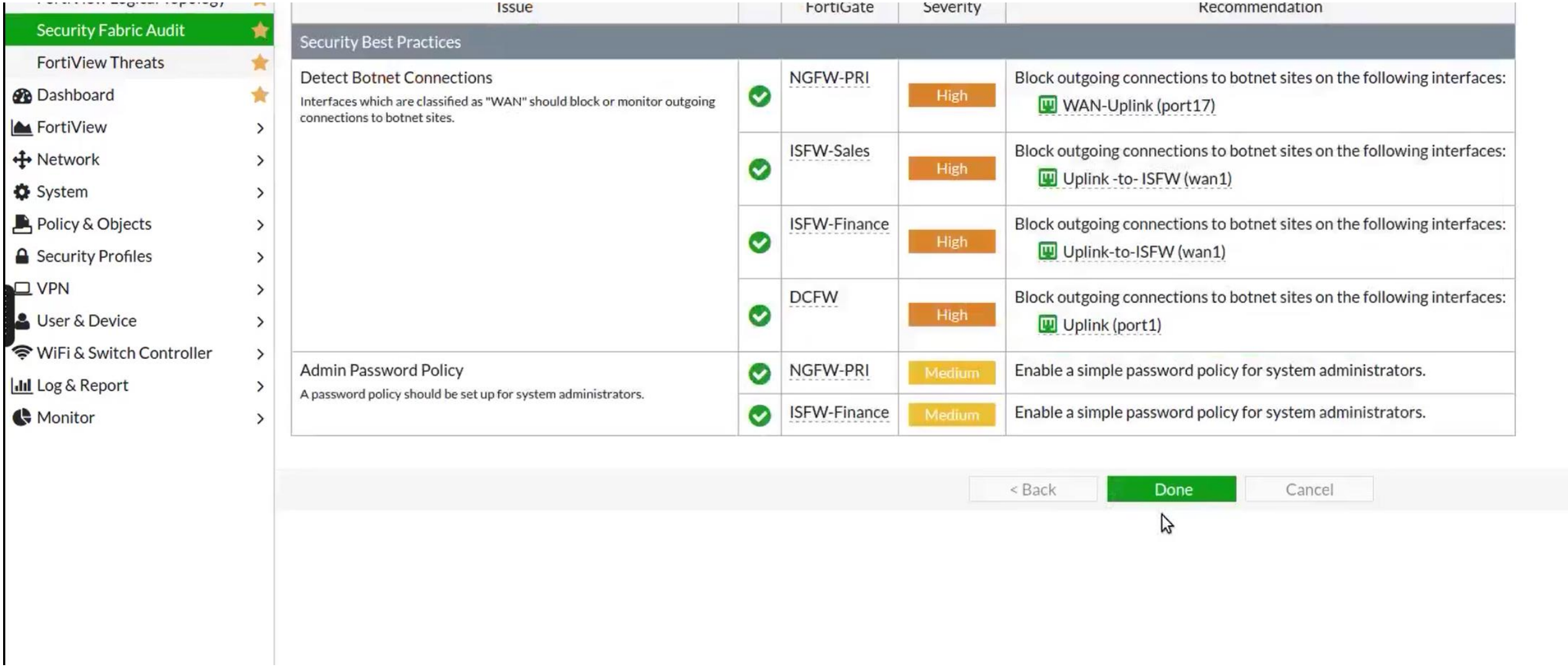
Captured Packets | Original File | Tracer Package | Tracer Log

Behavior Chronology Chart



- Suspicious Behaviors (1)
  - Virus detected
- Static Analysis (1)
- Files Created (2)
- Launched Processes (1)
- Network Behaviors (8)
- Behaviors In Sequence (143)


FortiGate 1500D
NGFW-PRI
Favorites
Dashboard
FortiView
Physical Topology
Logical Topology
Sources
Destinations
Interfaces
Policies
WiFi Clients
Traffic Shaping
All Sessions
Endpoint Vulnerability
Applications
Cloud Applications
Web Sites
Threats
Threat Map
FortiSandbox
System Events
VPN
Source: 10.13.13.13
Add Filter
FortiGate
Source
Device
Bytes (Sent/Received)
ISFW-Sales
10.13.13.13
ShaunasWin7
8.30 kB
Drill Down to Details
Quarantine Source Address (10.13.13.13)


Security Fabric Audit
FortiView Threats
Dashboard
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
WiFi & Switch Controller
Log & Report
Monitor
Issue
FortiGate
Severity
Recommendation
Security Best Practices
Detect Botnet Connections
Interfaces which are classified as "WAN" should block or monitor outgoing connections to botnet sites.
NGFW-PRI
High
Block outgoing connections to botnet sites on the following interfaces:
WAN-Uplink (port17)
ISFW-Sales
High
Block outgoing connections to botnet sites on the following interfaces:
Uplink -to- ISFW (wan1)
ISFW-Finance
High
Block outgoing connections to botnet sites on the following interfaces:
Uplink-to-ISFW (wan1)
DCFW
High
Block outgoing connections to botnet sites on the following interfaces:
Uplink (port1)
Admin Password Policy
A password policy should be set up for system administrators.
NGFW-PRI
Medium
Enable a simple password policy for system administrators.
ISFW-Finance
Medium
Enable a simple password policy for system administrators.
< Back
Done
Cancel

Wireless Traffic — Last 1 hour @ 14:54:52

Source Intf Name,Source IP,	SUM(Tota	Trend
port2, 154.0.140.158, 02:...	238.73 M	
port2, 153.0.55.46, 02:1a...	234.14 M	
port2, 154.0.19.33, 02:1a...	232.24 M	
port2, 154.0.95.25, 02:1a...	156.33 M	
port2, 153.0.162.171, 02:...	156.28 M	
port2, 153.0.216.51, 02:1...	155.69 M	
port2, 152.0.254.28, 02:1...	155.15 M	
port2, 153.0.156.235, 02:...	154.81 M	
port2, 152.0.150.134, 02:...	154.60 M	
port2, 151.0.87.157, 02:1...	154.39 M	

Carbon Black Bit9 — Last 24 hours @ 14:54:52

Event Name	COUNT(N	Trend
Bit9-PolicyEnforcement-E...	20	
Computer reported that c...	2	
Deleting older events	1	

FortiGate Sandbox Events by Type — Last 1 hour @ 14:54:53

Event Name	COUNT(	Trend
FortiGate-sandbox-file-s...	66,098	
FortiGate-sandbox-clean	66,093	
FortiGate-sandbox-malic...	2	
FortiGate-sandbox-sub...	2	
FortiGate-sandbox-low-ri...	1	

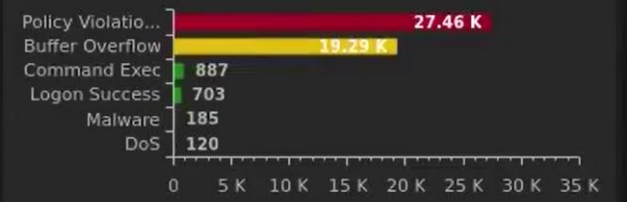
AV Infected Files Top Malware Names — Last 1 week @ 14:54:53

Malware Name	COUNT(I	Trend
JS/IFRAME.CNT!tr	63	
HTML/InjectedPhp.NZ!tr	20	
JS/Agent.NNP!tr	14	
JS/PACKED.D79C!tr	7	
JS/FakeJQuery.16F!tr	6	

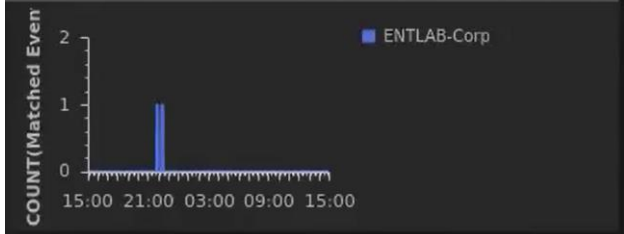
DHCP Available and Used — Last 1 hour @ 14:54:54

Host Intf Name	Available DHCP Addr	Used DHCP Addr
lan	101	0
mgmt	101	0
mgmt1	101	0
WLAN	154	4
vsw.port32	154	2
To_DCFW	154	1
WLAN_Guest	154	0
vsw.port36	153	1
port17	153	2
port3	153	1

Top Security Event Categories By Count — Last 8 hours @ 14:54:54



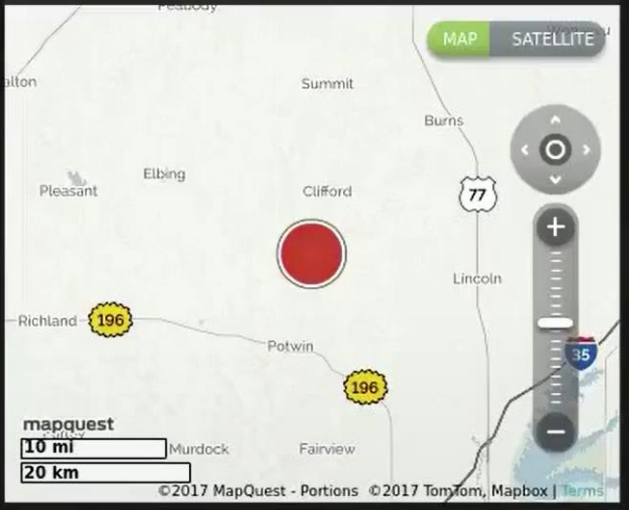
Wireless Client Authenticated-by-SSI... — Last 24 hours @ 14:54:54



Top Destination Organizations with Co... — Last 1 hour @ 14:54:55

Destination Organization	COUNT(N	Trend
Oi Internet	147,629	
China Telecom HUNAN	124,390	
E-Plus Mobilfunk GmbH	124,364	
Shaw Communications	120,970	
China Unicom Hainan	114,057	
TOPNET	71,425	
Sc Technological Srl	41,082	
Fortinet	30,087	
Vodafone-hu	20,598	
Office of the Prime Minister	19,764	

Top Allowed Connection Destination ... — Last 8 hours @ 14:54:55



Top Events By Severity, Count — Last 15 minutes @ 14:58:13

Event Name	COUNT(	Trend
FortiGate-webfilter-error	1	
FortiGate-ips-signature-...	1,879	
Denied traffic	505	
Web filter rating error o...	62	
The URL belongs to an a...	73,452	
The URL belongs to a de...	1,220	
Exemptlisted web traffic...	4	
An infected file was det...	1	
Session closed	74,845	
Permitted traffic	3,503	

Top Audit Event Categories By Count — Last 8 hours @ 14:54:56

Event Type Group	COUNT(N	Trend
Logon Success	703	
Config Change	30	

DHCP Available and Used — Last 1 hour @ 14:54:56

Host Intf Name	Available	Trend
lan	101	
mgmt	101	
mgmt1	101	
WLAN	154	
vsw.port32	154	

IPS Attack Names — Last 15 minutes @ 14:58:07

Source IP	Destination IP	Attack Name	COUNT(Matched
10.13.13.13	153.0.104.133	Glibc.Gethost...	188
10.13.13.13	153.0.112.171	Glibc.Gethost...	188
10.13.13.13	153.0.109.17	Glibc.Gethost...	188
10.13.13.13	153.0.161.222	Glibc.Gethost...	188
10.13.13.13	153.0.176.228	Glibc.Gethost...	188
10.13.13.13	153.0.210.178	Glibc.Gethost...	188
10.13.13.13	153.0.243.1	Glibc.Gethost...	188

IPS Attacks — Last 15 minutes @ 14:58:06

Destination IP	COUNT(N	Trend
153.0.104.133	188	
153.0.112.171	188	
153.0.109.17	188	
153.0.161.222	188	
153.0.176.228	188	
153.0.210.178	188	
153.0.243.1	188	

russia@fortinet.com


FORTINET