MSSP

Безопасность как сервис

Алексей Андрияшин,
aandriyashin@fortinet.com
+79859996477

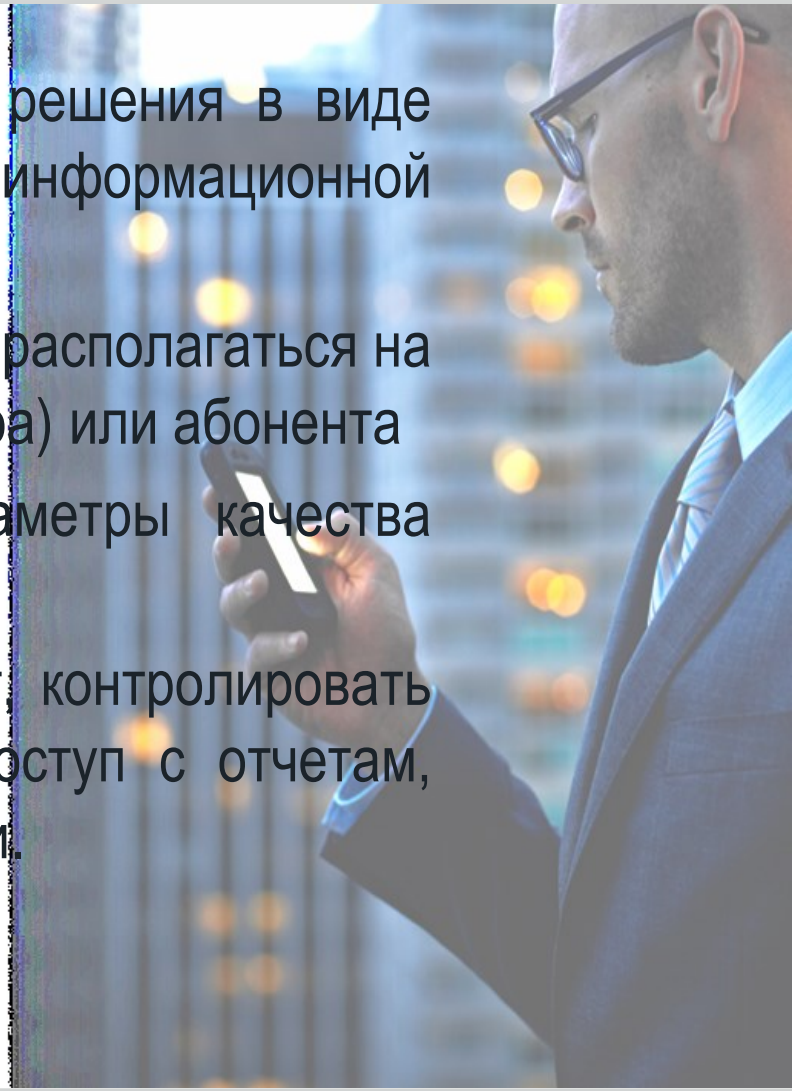
February 24, 2014

Некоторые мнения, озвученные на форуме

- …документов по безопасности в банке больше чем всех остальных, включая операционную деятельность…
- …банкам зачастую дешевле выплачивать деньги клиентам, чем проводить расследование…
- …ИБ - самое проверяемое подразделение банка. И ФСБ, и ФСТЭК, и ЦБ, и PCI DSS…
- …за последние 2 месяца было 3 целенаправленные атаки на крупные банки!
- …чтобы проверить все филиалы "по всем правилам ФСТЭК и ЦБ" банку < somewherebank> требуется 2 года…

Определение MSS

- **Managed Security Services** – готовые решения в виде набора услуг по обеспечению информационной безопасности
- Решение частично или полностью может располагаться на площадке **сервис провайдера** (оператора) или абонента
- **Оператор** гарантирует заданные параметры качества (SLA),
- **Клиент** может управлять набором услуг, контролировать соблюдение SLA, иметь постоянный доступ с отчетам, статистике, диагностической информации.



Рост рынка MSSP

- **Рынок MSSP достигнет $15Млрд к 2016**
  - Мировой рынок MSS $9 Млрд в 2013 (Frost)
  - Отечественные операторы готовятся предоставлять сервисы по безопасности
- **Популярность на рынке SMB**
  - SMB MSS может занять примерно 50% рынка
  - Модель услуг широко востребована на рынке
- **Ожидание высокой конкуренции среди операторов связи**
  - Привлечение новых клиентов и повышение их лояльности
  - Увеличение прибыли за счет новых дифференцированных услуг

Прогноз по вертикальным рынкам

	2007	2008	2009	2010	2011	2012	2013	2014	2015
Financial	347,3	384,9	452,1	524,4	610,4	680,5	795,7	937,4	1 089,4
Government	148,4	171,7	206,7	246,2	291,0	347,7	402,9	473,2	539,5
Healthcare	121,8	135,9	166,7	200,6	243,3	292,6	352,5	425,3	501,5
Technology	97,0	113,1	139,5	165,7	202,3	243,8	302,2	365,4	418,5
Utilities	76,1	87,0	90,4	92,7	102,0	114,5	123,4	142,7	162,6
Others*	160,8	194,6	236,6	290,4	341,0	440,9	541,4	651,0	746,9
Growth Rate		14,2	18,8	17,6	17,7	18,4	18,7	18,9	15,4

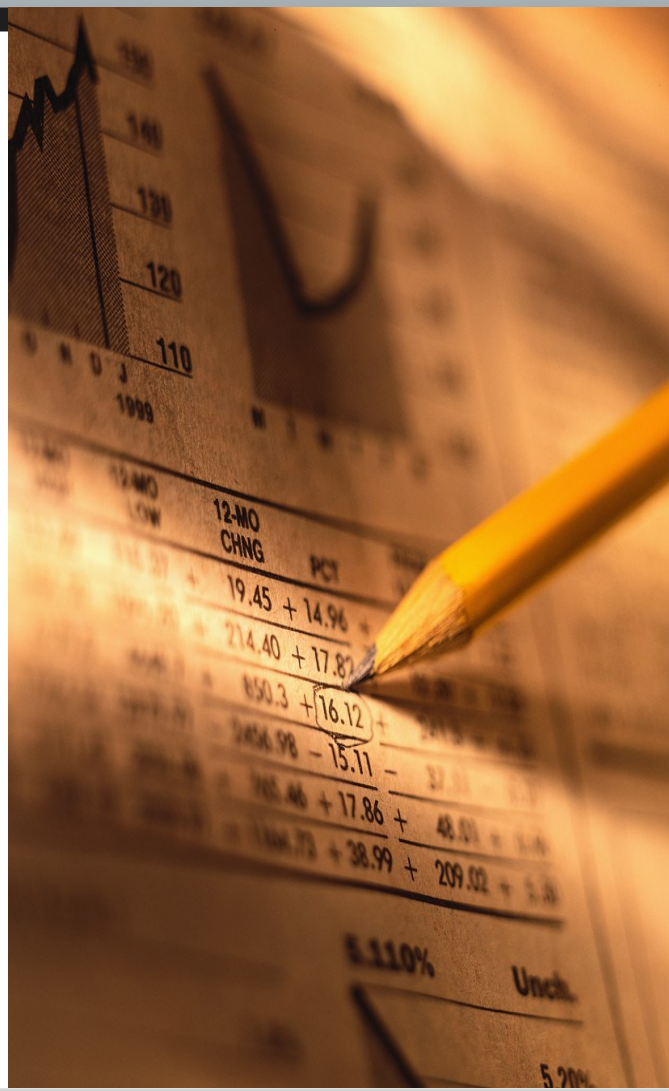
*Другие включают в себя: розничная торговля, производство, СМИ, транспорт, СМИ

Примечание: Все цифры округлены. Источник: Frost & Sullivan

FORTINET

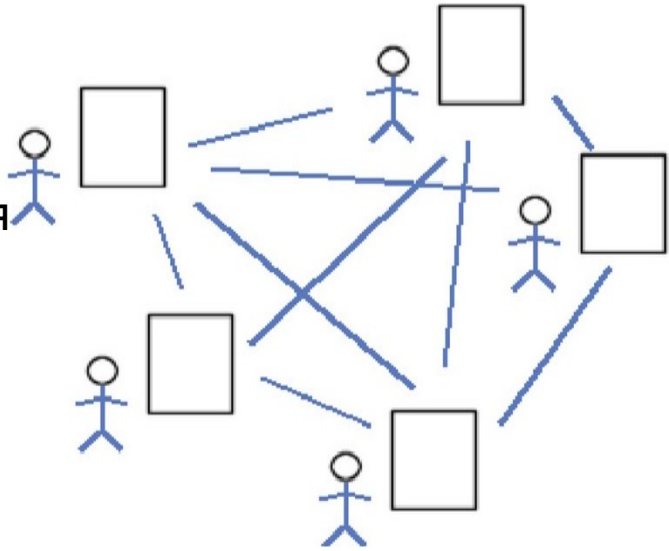
Предпосылки для роста рынка MSS

- **Снижение затрат**
  - OPEX – снижение затрат на 60-70%
  - CAPEX – снижение затрат на 30-40%
  - Высокий уровень ROI
- **MSS**
  - Защита в реальном времени и техническая экспертиза 24x7
  - Управление изменениями и отчетность
- **Управление**
  - Управление сервисами
  - Поддержка заданного уровня качества обслуживания

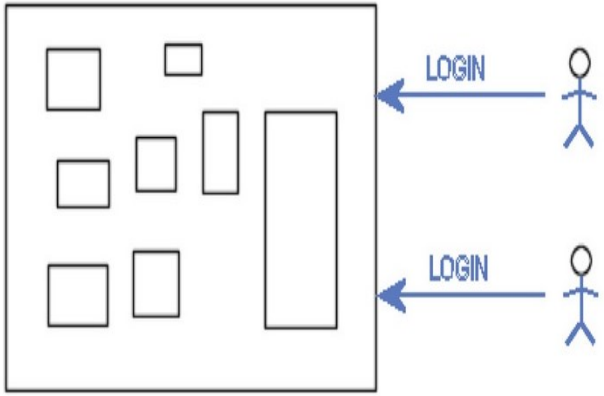


Модели предоставления MSS

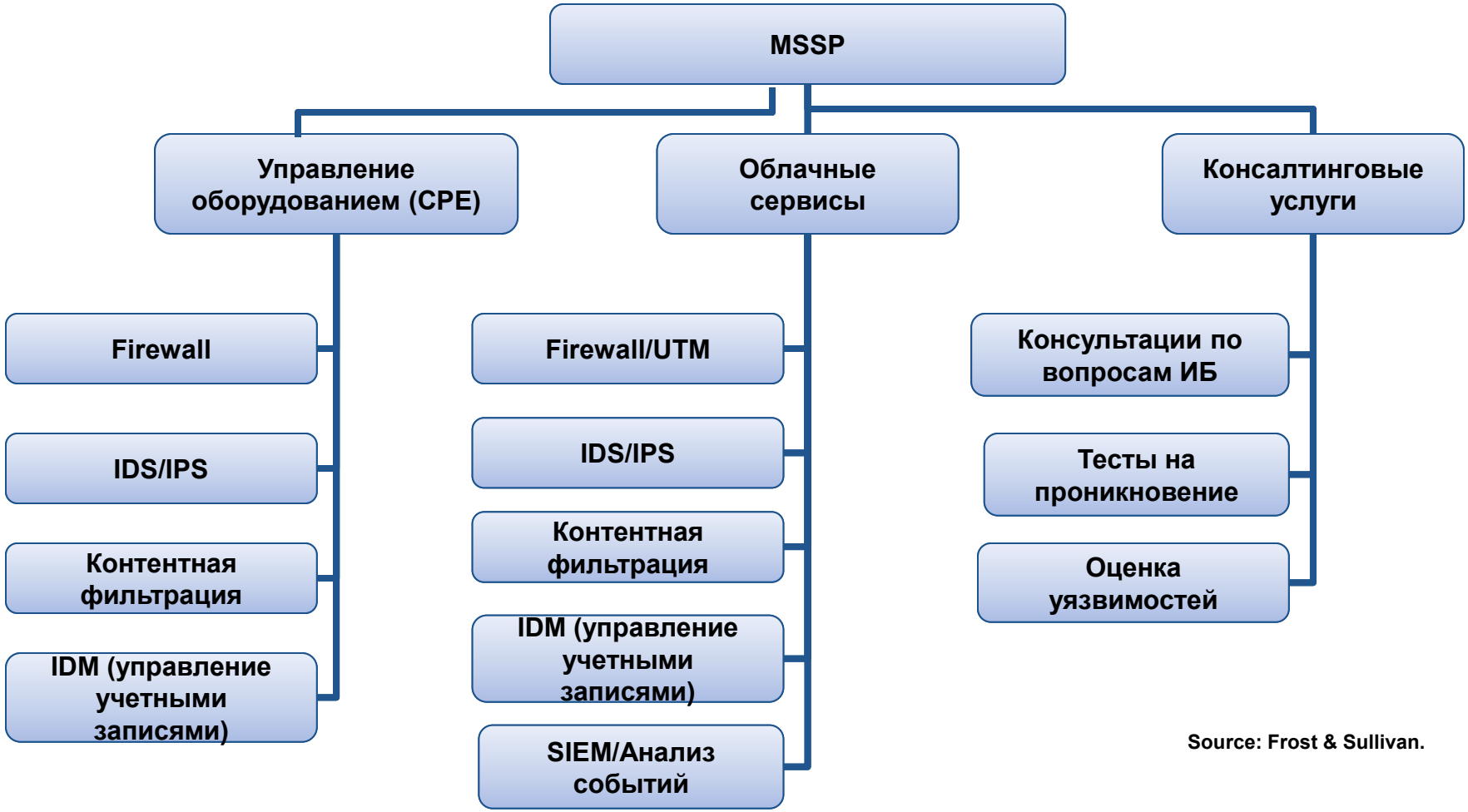
- **CPE-модель**
  - Оборудование преимущественно располагается у клиента
  - Наиболее популярная модель предоставления услуг
  - Идеально подходит для розничной торговли и распределенных филиальных сетей



- **Облачная модель**
  - Security-as-a-Service, централизация на уровне поставщика услуги
  - Низкие эксплуатационные расходы
  - Наиболее перспективная модель

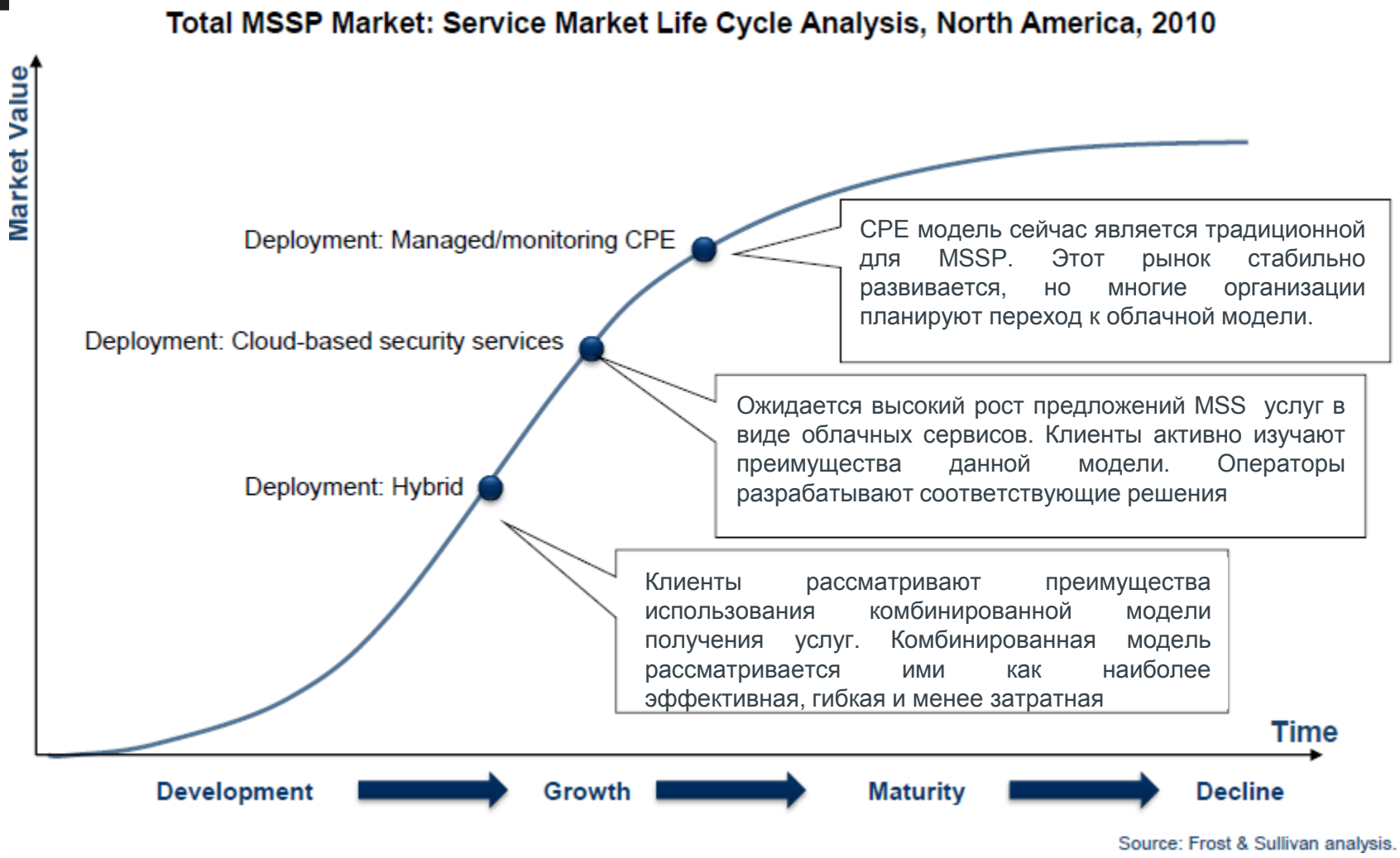


Варианты предоставления сервисов по модели MSS



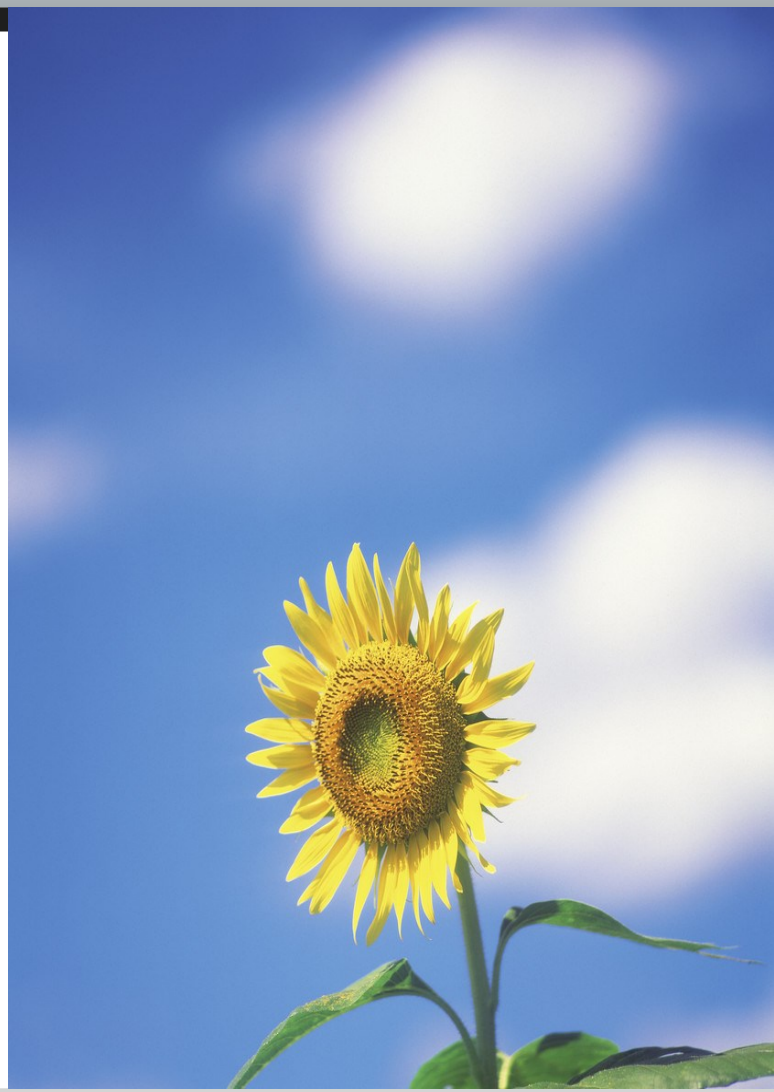
Source: Frost & Sullivan.

Развитие рынка MSSP



Cloud-based Security-as-a-Service

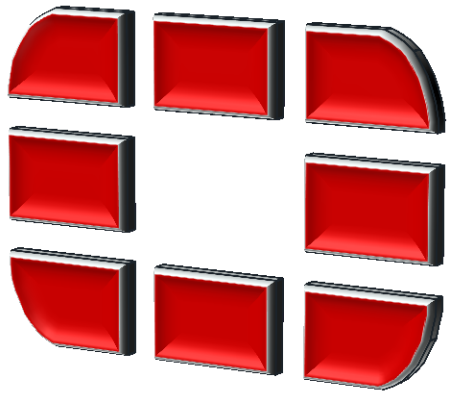
- **Преимущества для клиента**
  - “Clean Pipe” – Вредоносный трафик блокируется до «последней мили». Повышается производительность сети
  - “Single Pane of Glass” – Централизация ресурсов (сервис, управление, отчетность)
  - Тарификация по объему трафика или виду услуг
- **Преимущества для MSSP**
  - Сокращение времени начала предоставления услуг
  - Меньшие затраты на развертывание в сравнении с CPE моделью
  - Легкость предоставления новых сервисов

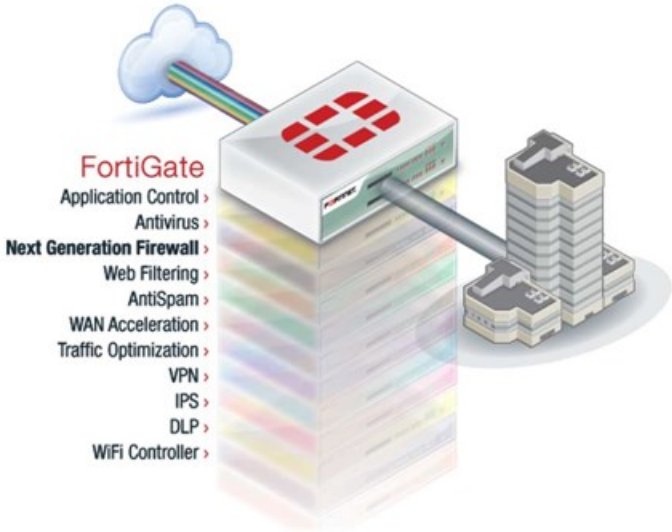


FORTINET

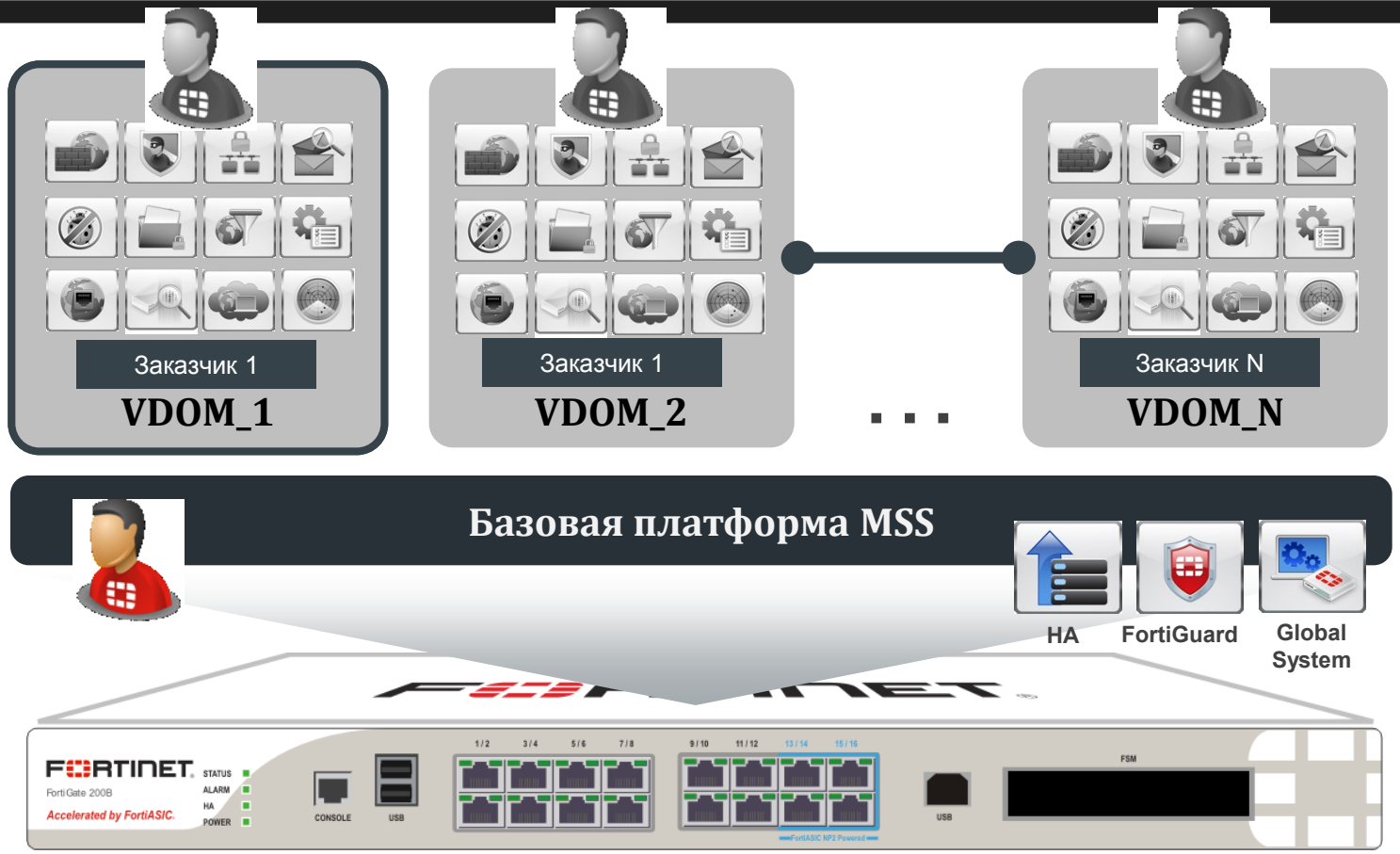
Перечень сервисов безопасности

- Межсетевое экранирование
- Антивирусная/Антибот защита
- Защита почтового трафика
- Блокирование DDoS атак
- Контроль приложений
- Веб фильтрация
- Обнаружение и предотвращение угроз





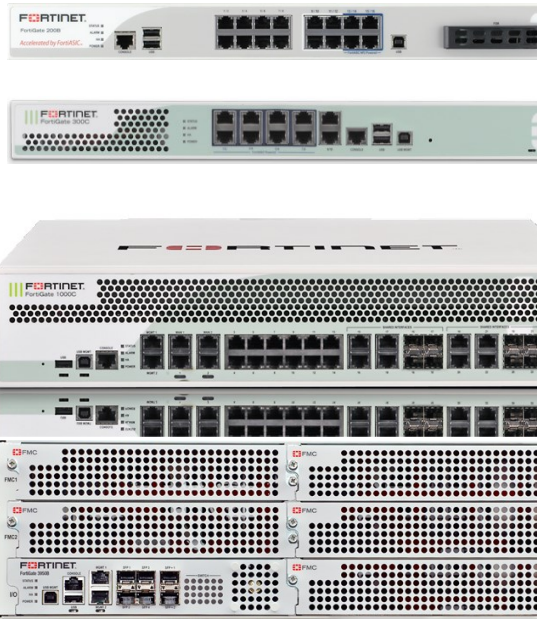
Принцип независимого предоставления сервисов в многопользовательской модели (multi tenant)



VDOM – виртуальный домен безопасности (контекст)

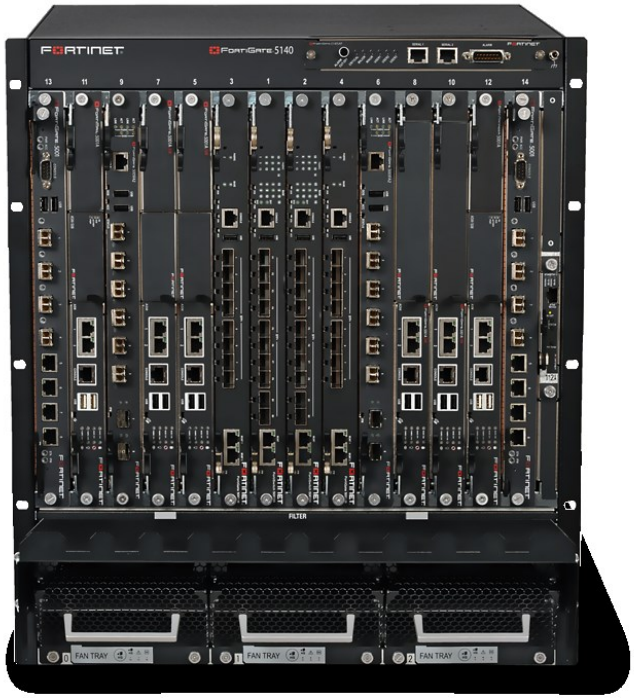
В рамках каждого контекста предоставляется независимый набор сервисов

MSS решения Fortinet



Различные платформы

- Все сетевые сервисы
- Все сервисы безопасности
- Независимые контексты безопасности / VM
- Простая схема лицензирования

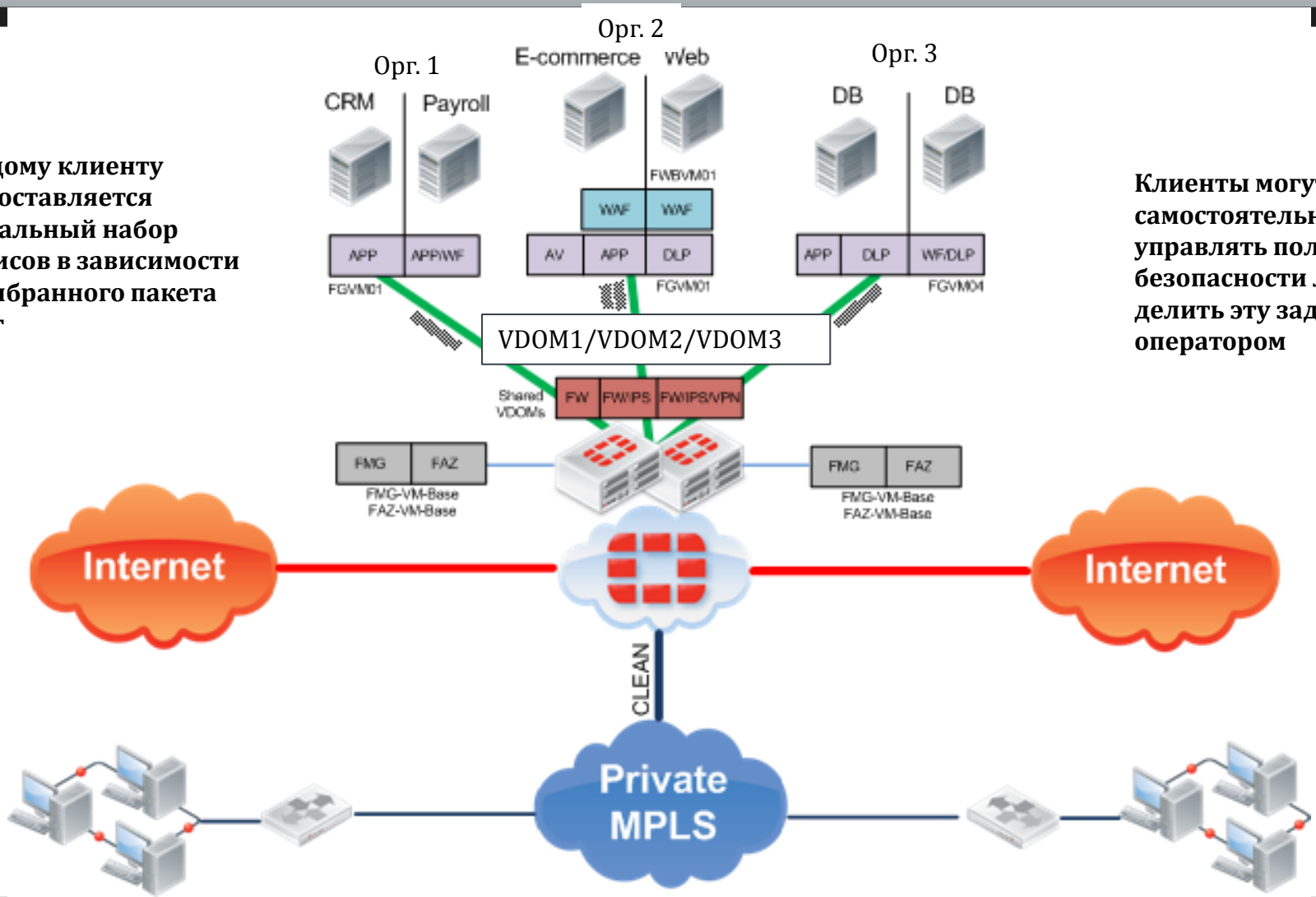


2011 Виртуализация сервисов безопасности Стратегия и компания года

Архитектура SaaS Cloud

Предоставление сервисов безопасности клиентам (облачная модель)

Каждому клиенту предоставляется уникальный набор сервисов в зависимости от выбранного пакета услуг



Клиенты могут самостоятельно управлять политикой безопасности либо делить эту задачу с оператором

FORTINET

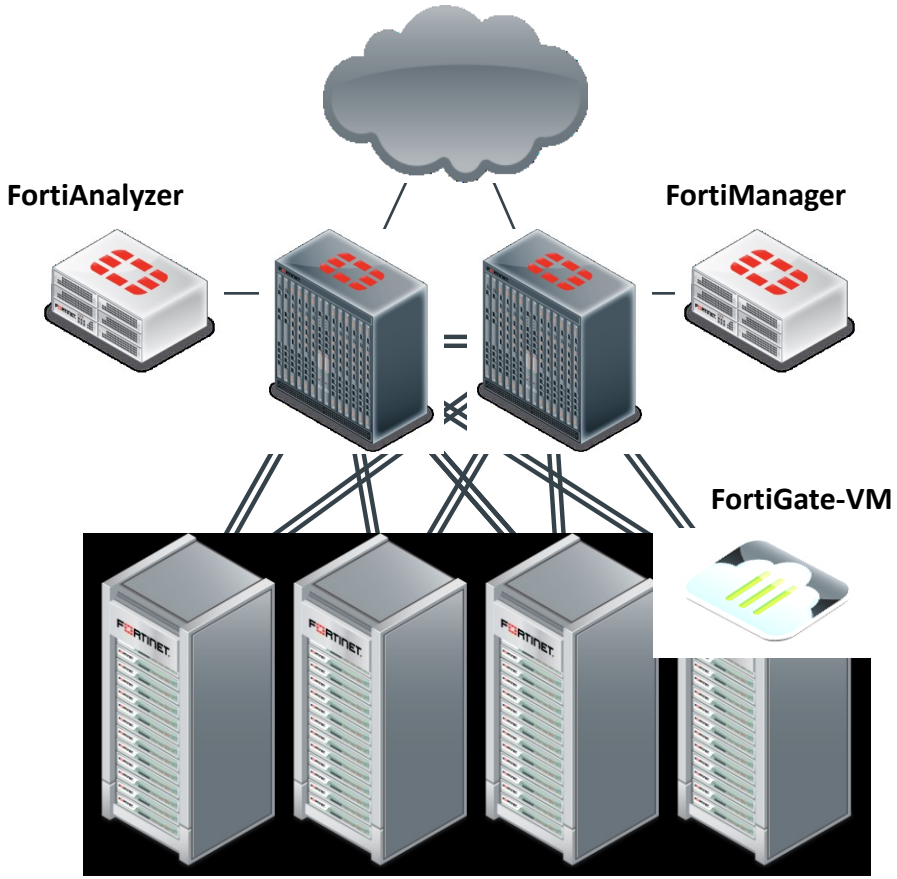
Виртуальные домены/контексты

- **Ключевые преимущества для MSSPs:**
  - Каждый VDOM выступает в роли отдельного FW
  - Каждый VDOM работает независимо от других
  - Поддержка всего функционала UTM
  - Гибкая система тарификации
  - API/Web GUI для интеграции с порталом обслуживания (SSP)

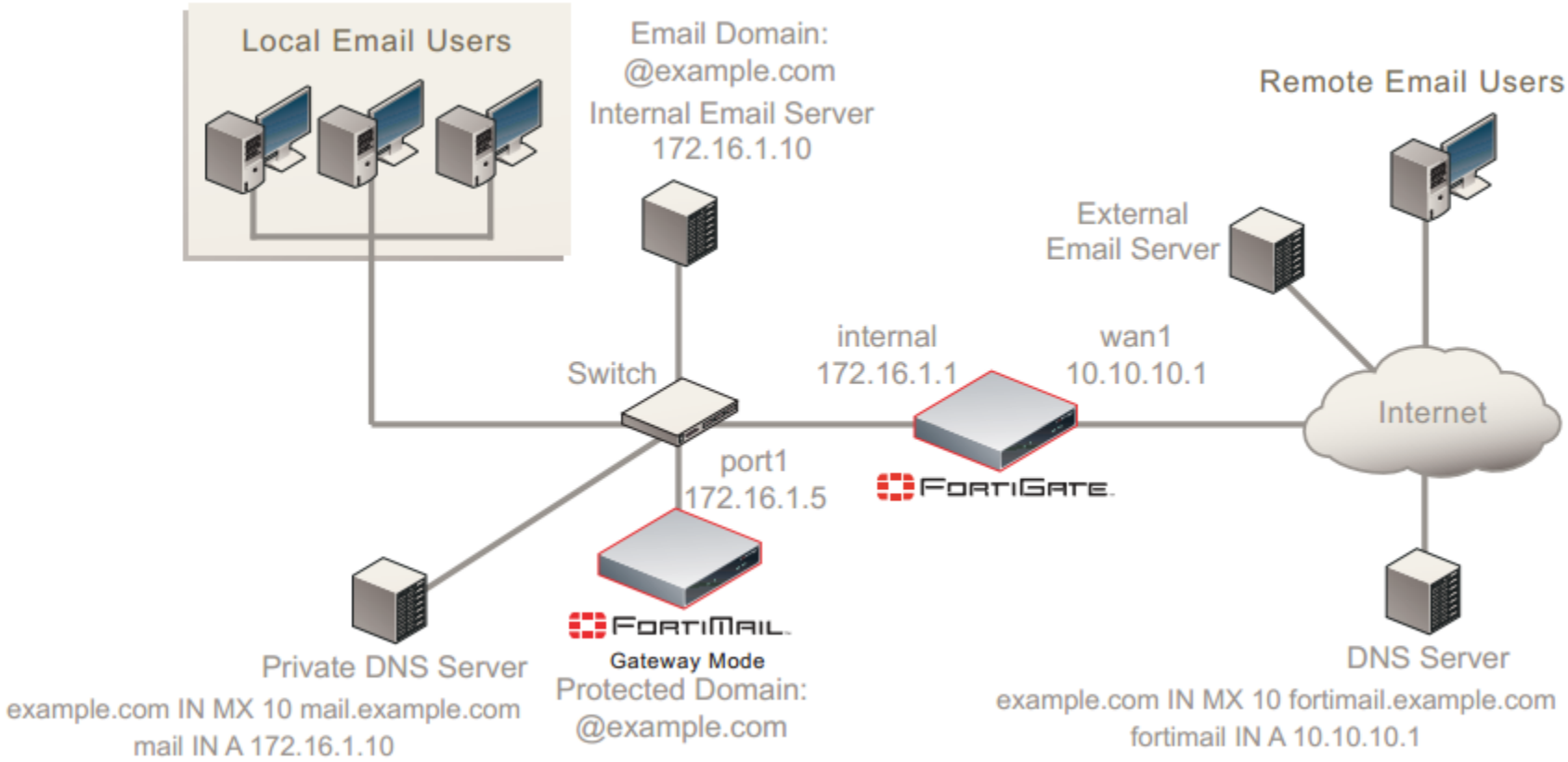
- **Ключевые преимущества для клиентов:**
  - Поддержка всего функционала UTM
  - Самостоятельное управление политиками
  - Возможно расширение в процессе эксплуатации
  - Поддержка как Cloud так и CPE моделей

Комбинация виртуальных и физических решений

- Физические устройства с аппаратным ускорением для защиты опорных сетей
- Виртуализированные решения для клиентских сервисов
- ESXi / Xen серверы в качестве платформы
- Многопользовательская среда
- Поддержка множества VDOM на одном виртуальном FW

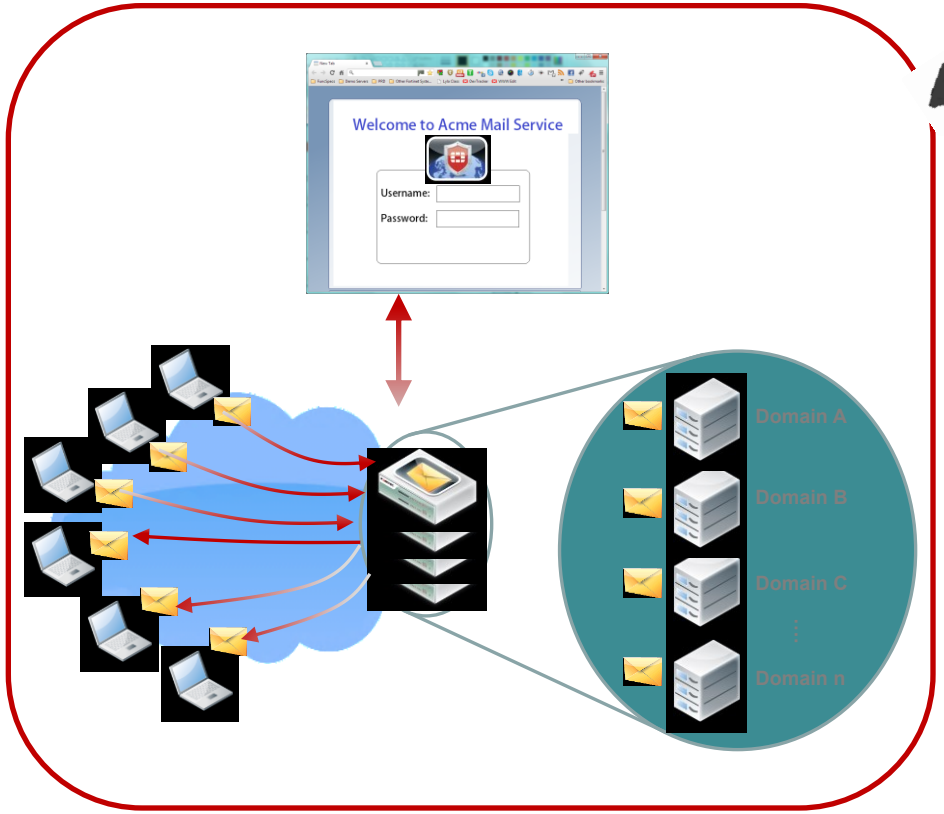


MSSP Защита почтового трафика (пример)



FORTINET

MSSP решение по защите почты



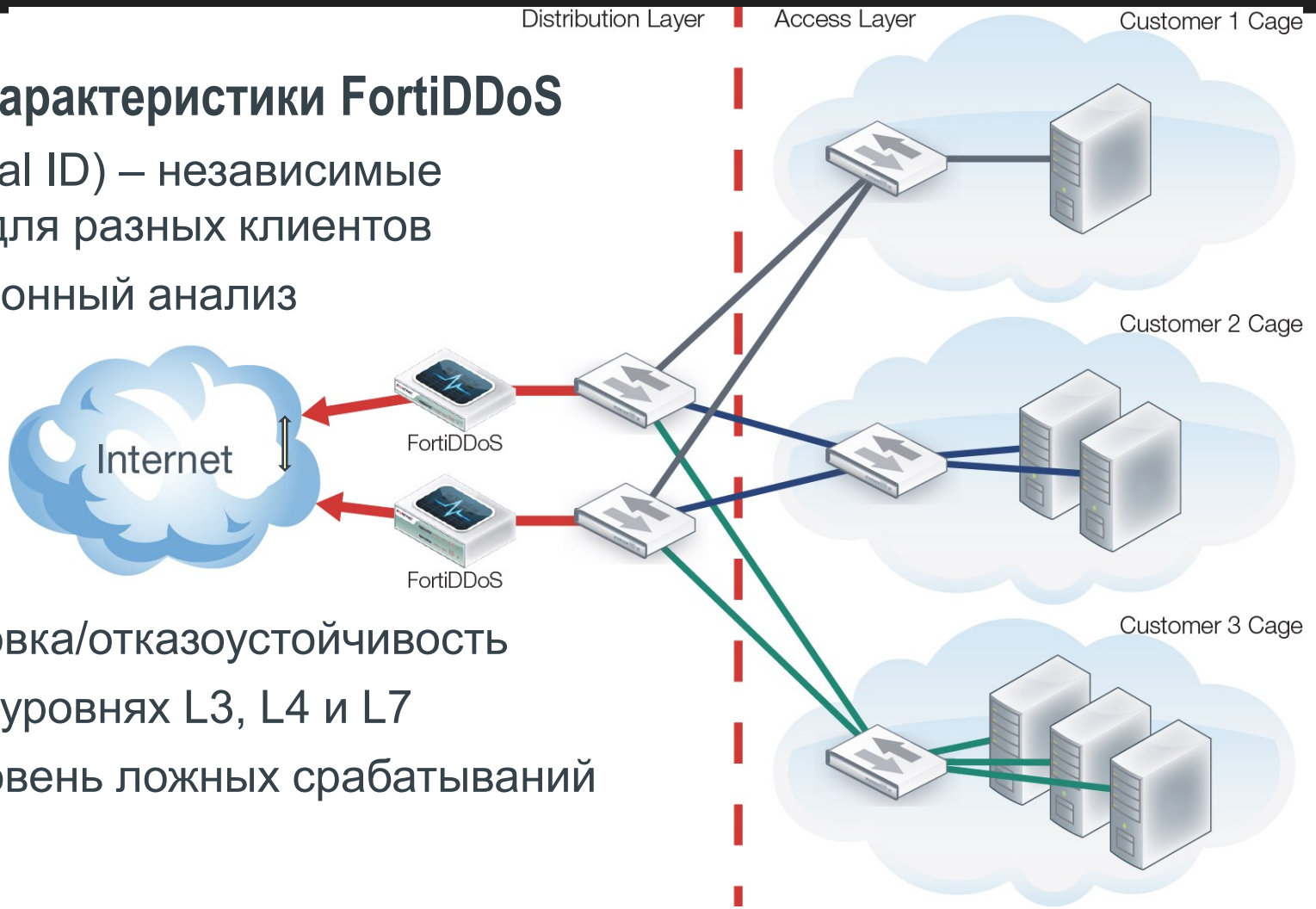
Mail Security Service Provider in a box!

MSSP сервис

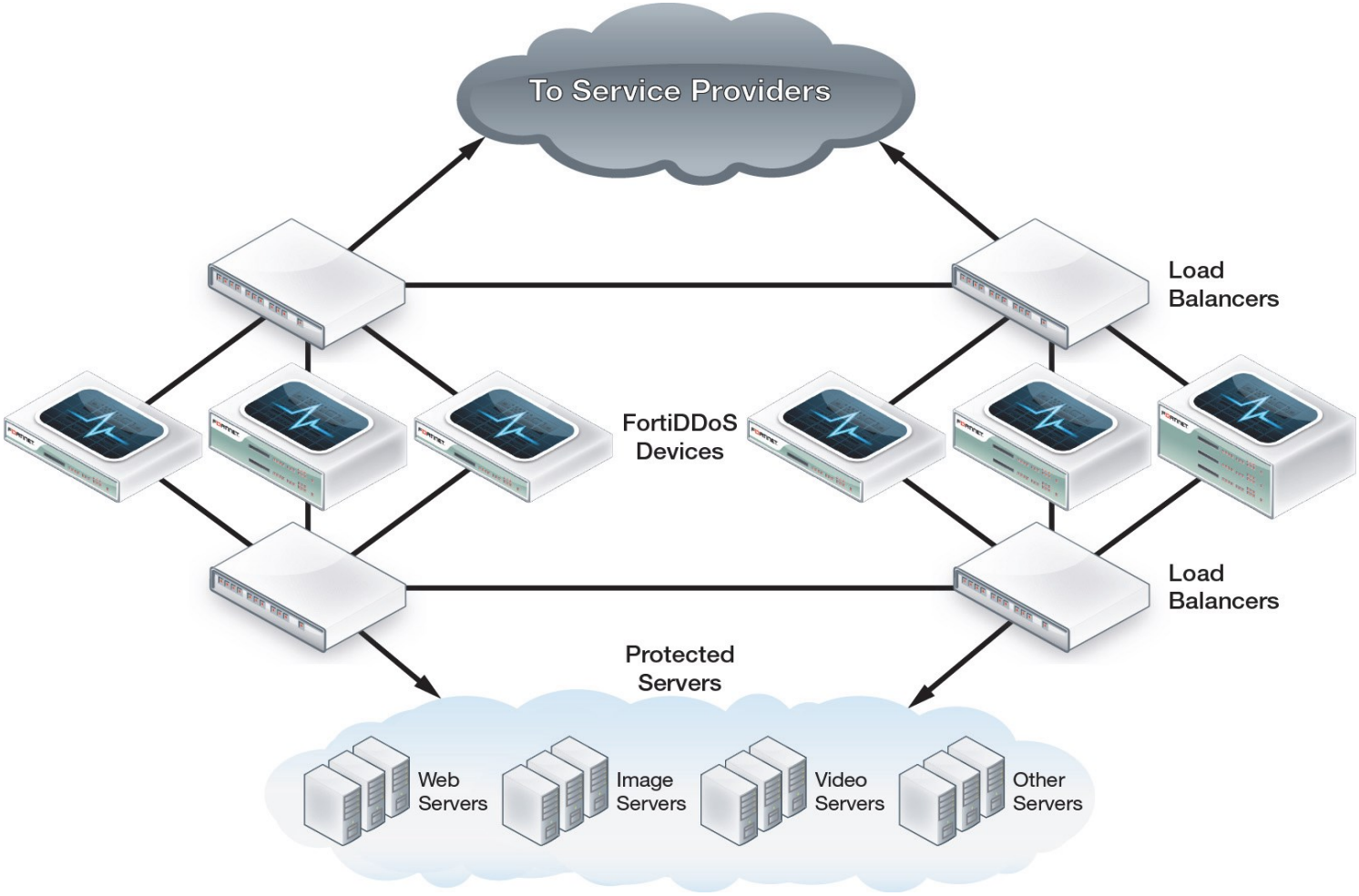
- Очистка почтового трафика
- Многодоменные политики
- Применение на уровне провайдера
- Делегирование прав управления политикой клиентам
- Портал самообслуживания

MSSP Защита от DDoS

- **Основные характеристики FortiDDoS**
  - VIDs (Virtual ID) – независимые политики для разных клиентов
  - корреляционный анализ
  - балансировка/отказоустойчивость
  - работа на уровнях L3, L4 и L7
  - низкий уровень ложных срабатываний



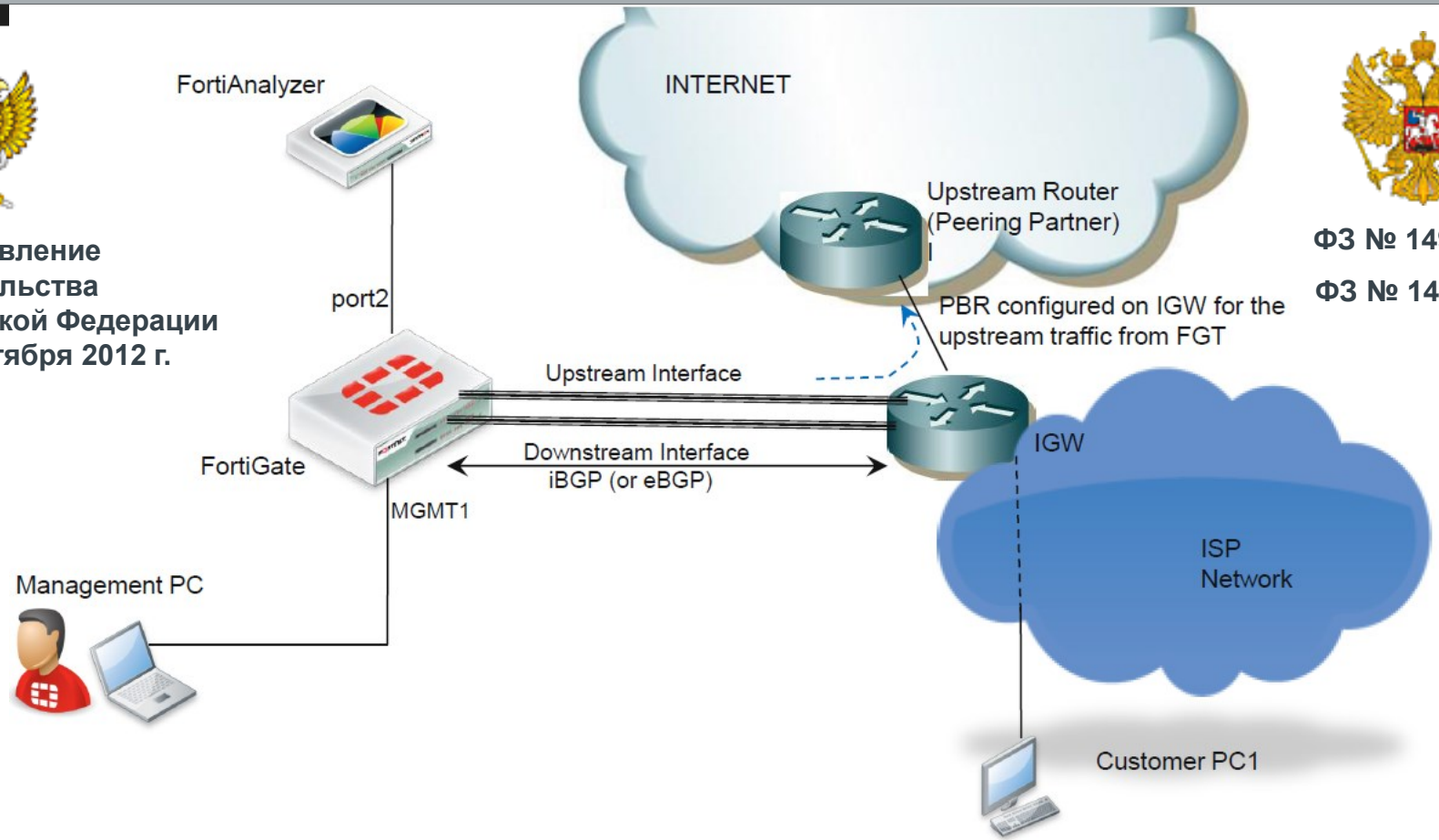
MSSP Защита от DDoS (масштабирование и отказоустойчивость)



WEB фильтрация

(идентификация сайтов содержащих информацию, распространение которой запрещено в РФ)

Постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101



ФЗ № 149-ФЗ

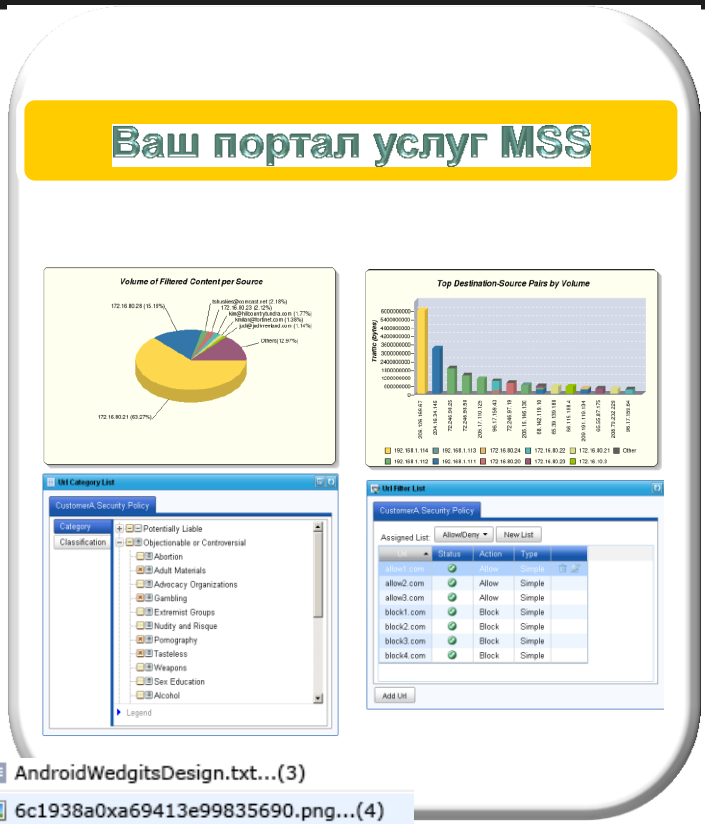
ФЗ № 149-ФЗ

Блокирование доступа к ресурсам в соответствии с **Единым реестром запрещённых сайтов**

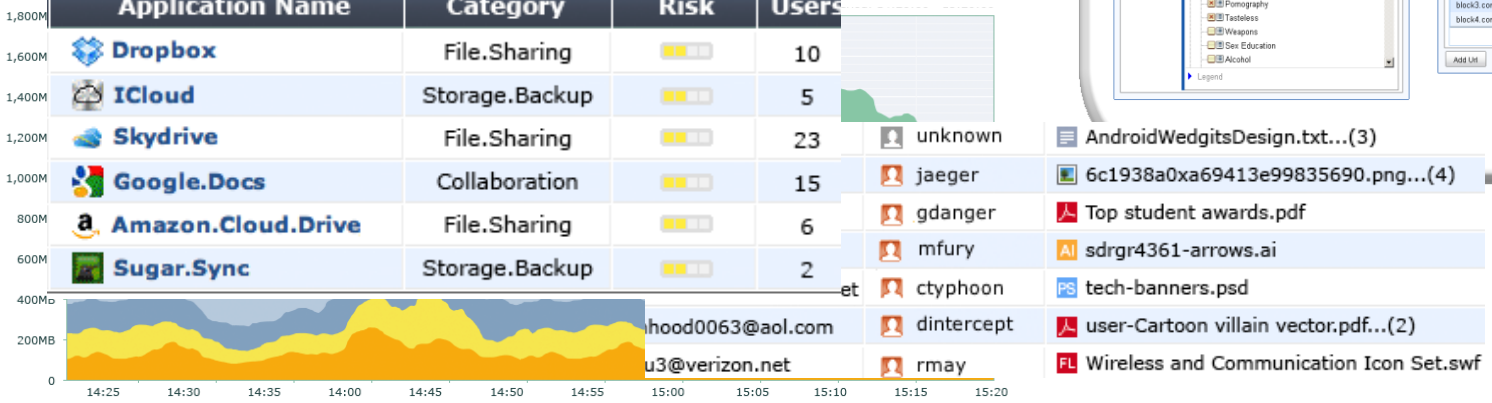
Автоматизация управления услугами

Управление сервисами

- Кабинеты пользователей
- Предоставление отчетов
- Управление услугами/подписками
- Оповещение об инцидентах
- Корреляция событий
- Обновление сервисов



Application Name	Category	Risk	Users
Dropbox	File.Sharing		10
ICloud	Storage.Backup		5
Skydrive	File.Sharing		23
Google.Docs	Collaboration		15
Amazon.Cloud.Drive	File.Sharing		6
Sugar.Sync	Storage.Backup		2

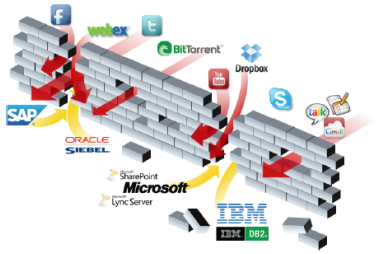


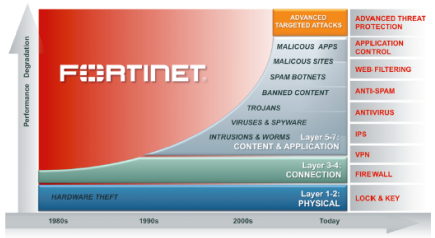
Детализированная отчетность

Application Control and Assessing Risks

Application Visibility is Critical

Application control provides granular policy enforcement of application traffic, even with the multitude of traffic using HTTP, which traditional firewalls and security gateways cannot distinguish. It includes the ability to identify more applications than any other vendor in the market, and to selectively block application behavior to minimize the risk of data loss or network compromise.





Complete Content Protection

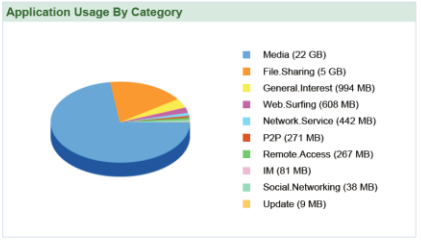
Assessing network risks requires complete content protection, which is more than simply identifying applications and allowing or denying traffic. It is application control coupled with identity-based policy enforcement of all content. It enables organizations to utilize all the security and networking technologies included in the FortiGate platforms, such as access control, traffic shaping, IPS, DLP, and antivirus/antispyware. Complete content protection continuously protects networks against malicious content hidden within applications and data, even from trusted applications from trusted sources.

Backed by FortiGuard

Fortinet has been giving its customers the ability to deploy application-based security since FortiOS 3.0, enabling them to detect and manage applications independent of port or protocol. FortiGuard is the culmination of years worth of security research. New applications and potential threats are identified daily to keep your network up to speed.

Application Usage By Category

As part of the traffic classification process, the FortiGate identifies and categorizes the applications crossing the network into different categories based on the number of sessions and bandwidth. This data complements the granular application threat data and provides a more complete summary of the types of applications in use on the network.

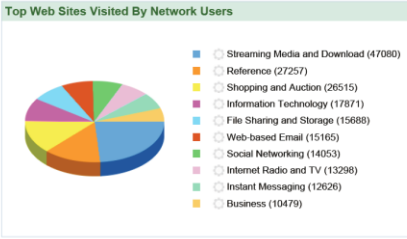


Top 30 Application Category

Application Category	Bandwidth
Media	21.56 GB
File.Sharing	5.36 GB
General.Interest	995.50 MB
Web.Surfing	608.01 MB
Network.Service	442.16 MB
P2P	272.25 MB
Remote.Access	266.86 MB
IM	80.70 MB
Social.Networking	37.67 MB

Top Web Categories Visited By Network Users

User browsing habits can not only be indicative of inefficient use of corporate resources, but can also indicate an inefficient optimization of web filtering policies. It can also give some insight into the general web browsing habits of corporate users and assist in defining corporate compliance guidelines. This chart details web categories by the number of times URLs within those categories were requested and by the number of bandwidth used.



Top Web Sites Visited By Network Users

Category Description	Sessions	Bandwidth
Streaming Media and Download	47076	18.41 GB
Reference	27255	77.72 MB
Shopping and Auction	26514	8.88 MB
Information Technology	17870	35.90 MB
File Sharing and Storage	15685	5.36 GB
Web-based Email	15163	5.08 MB
Social Networking	14052	25.65 MB
Internet Radio and TV	13298	31.50 MB
Instant Messaging	12625	165.96 MB

Основные риски при применении облачных технологий

(из выступления Лютикова Виталия Сергеевича, ФСТЭК Росии)

Основные риски для поставщиков облачных услуг

- Неопределенность в распределении ответственности
- Несогласованность политик безопасности
- Непрерывная модернизация
- Конфликт юрисдикций разных стран
- Общедоступность инфраструктуры
- Недобросовестность поставщиков услуг
- Злоупотребления со стороны потребителей

Основные риски для потребителей облачных услуг

- Неопределенность ответственности
- Потеря управления, доверия
- Привязка к провайдеру облачных услуг
- Недостатки управления информацией/облачными ресурсами
- Потеря и утечка данных

Рекомендации операторам по предоставлению сервисов безопасности

cloud security alliance®

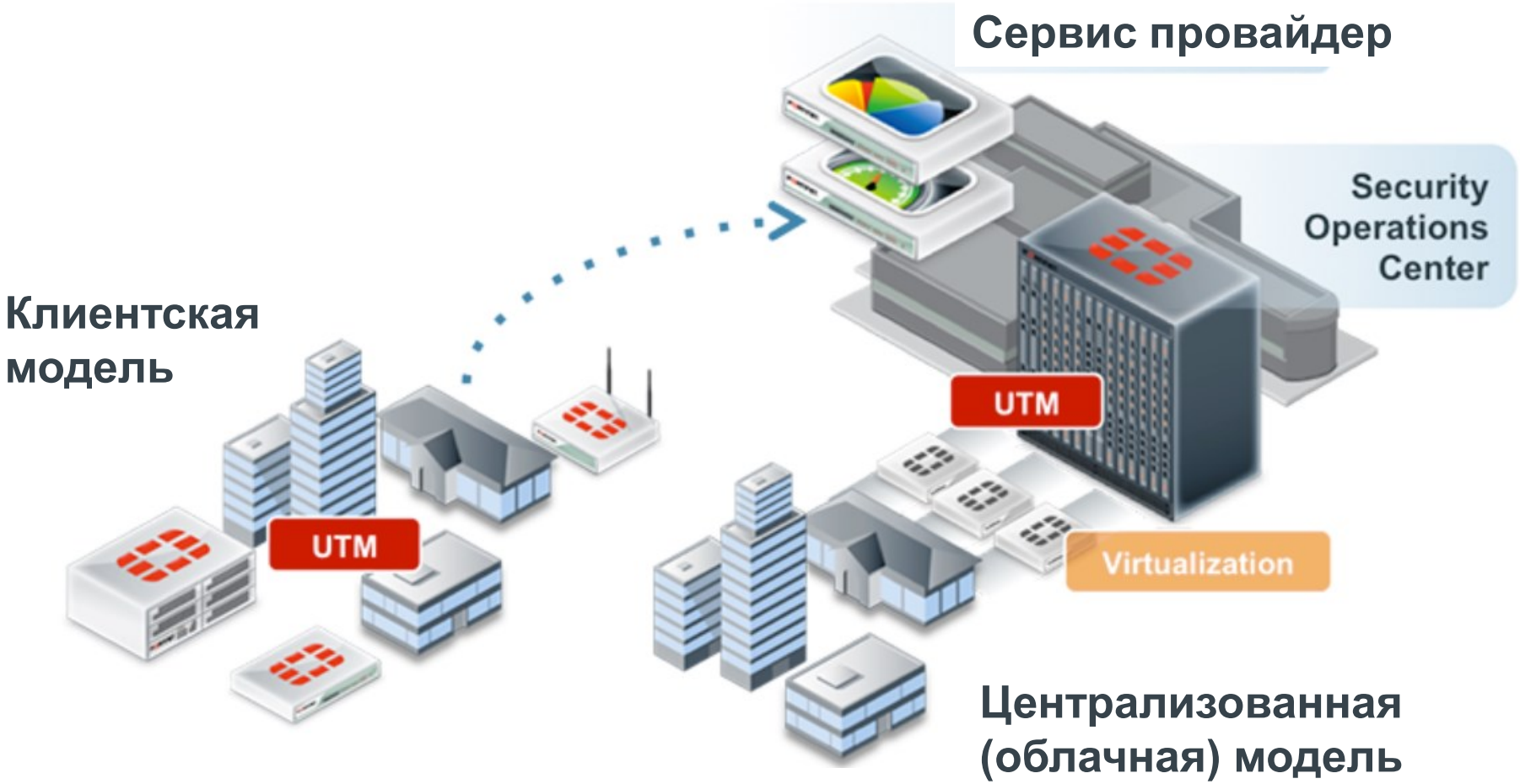
- Identity and Access Management
- Data Loss Prevention
- Web Security
- Email Security
- Security Assessments
- Intrusion Management
- Encryption
- BCDR
- Security Information and Event Management
- Network Security

cloud security alliance℠ Russian Chapter

https://cloudsecurityalliance.org/about/

http://www.risspa.ru/csa

Модели предоставления сервисов ИБ



СПАСИБО!

Алексей Андрияшин,
aandriyashin@fortinet.com
+79859996477

FORTINET®