21.08.2019

Внедрение WAF. Архитектура

МТС

Ты знаешь, что можешь!

#whoami

Андрей Дугин

Начальник отдела обеспечения информационной безопасности

16 лет в МТС, CCNP Security

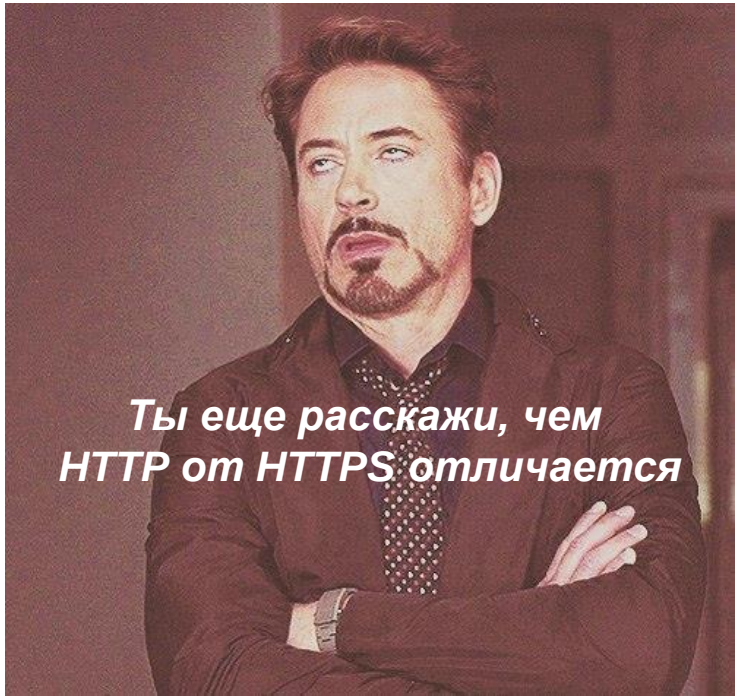
802.1x, SOC, интеграция сетей IP/MPLS

МТС Ты знаешь, что можешь!

Зона покрытия

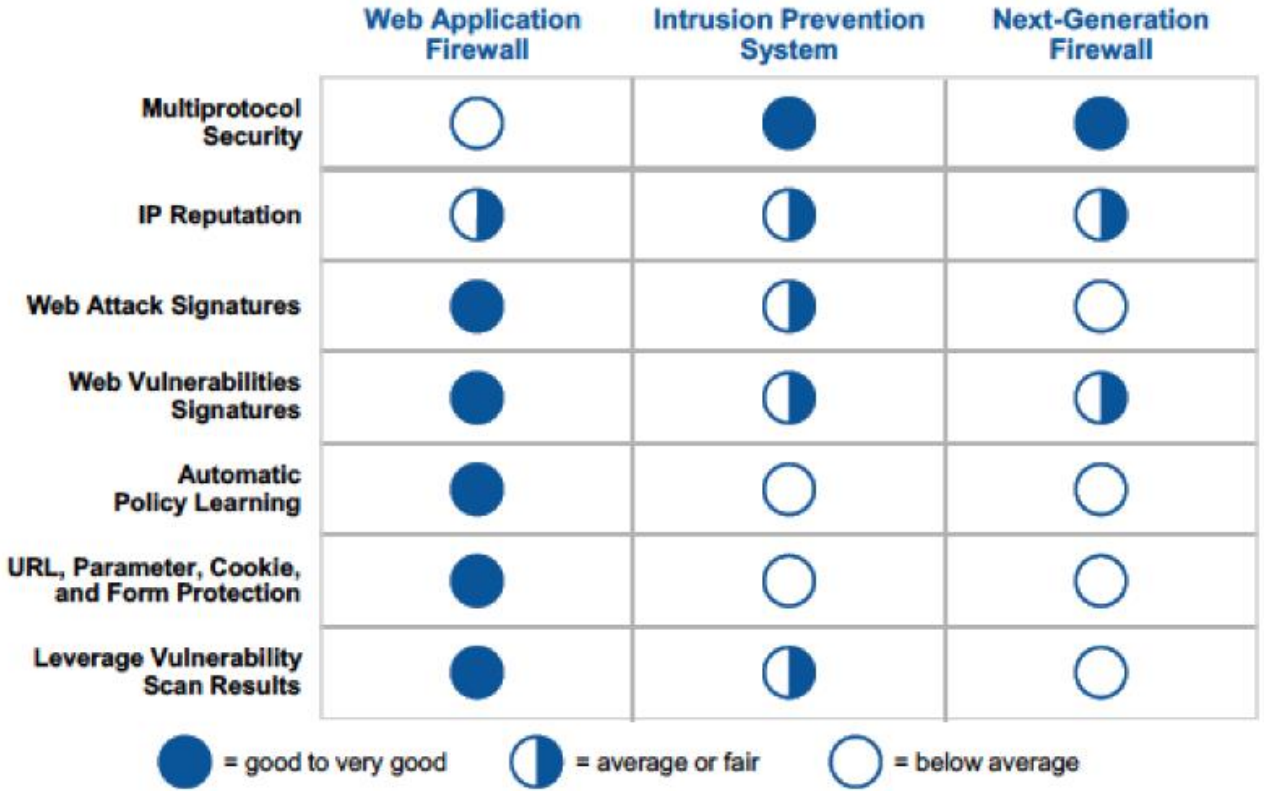
- 11 часовых поясов
- Десятки тысяч сотрудников
- Десятки тысяч ПК/ноутбуков
- Десятки тысяч серверов
- Тысячи единиц активного сетевого оборудования
- >1000 диапазонов внешних IP

Зачем нужен WAF?



- OWASP Top10
- OWASP Risk Rating Methodology
- Virtual patching
- PCI DSS
- Снижение нагрузки на балансировщик и frontend

WAF vs NGFW vs IPS



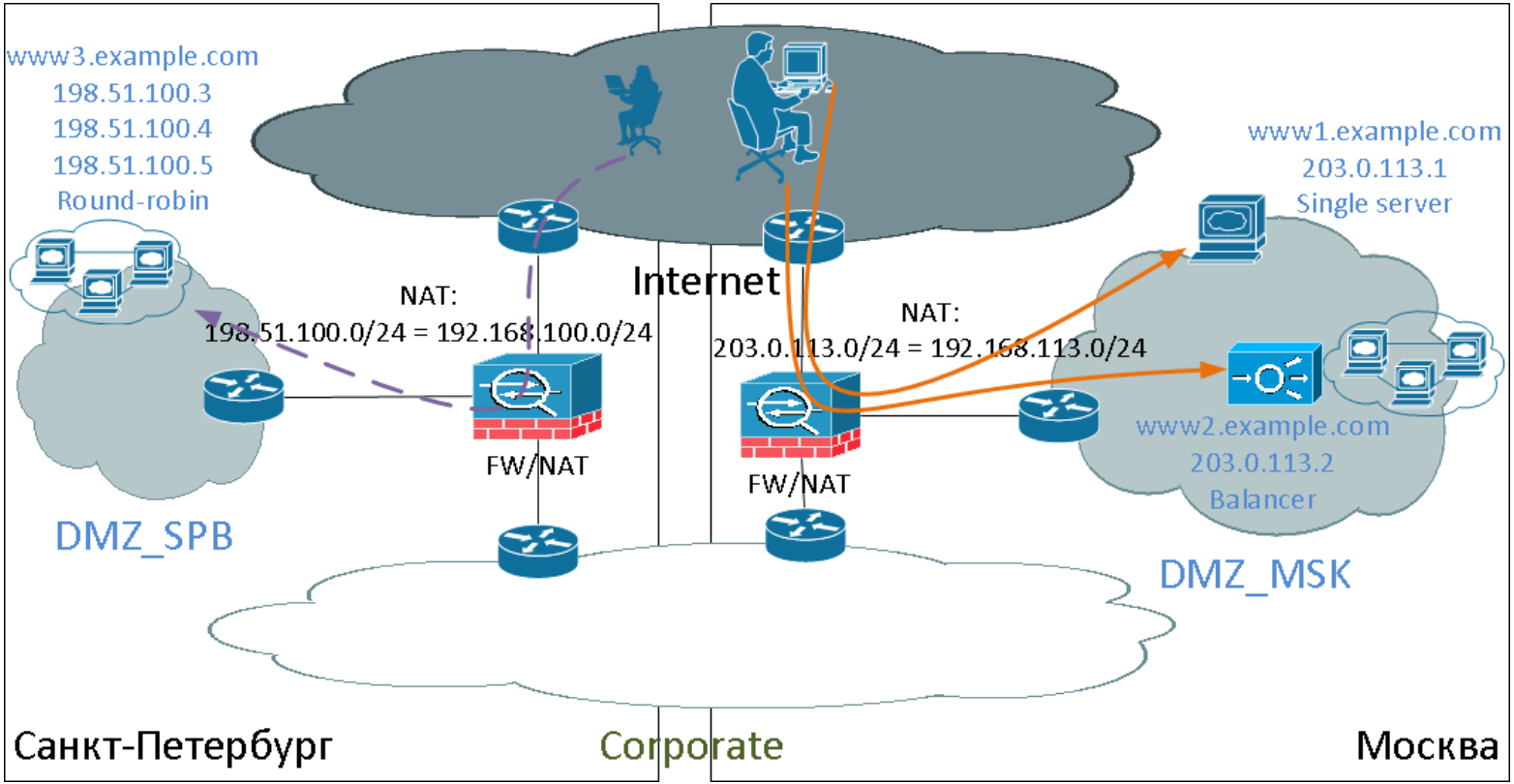
Задача: внедрить WAF

- 3 web-сайта разной архитектуры в 2х городах
- Масштабируемость – до 50 сайтов в 5 городах
- Минимум доработок web-приложений
- Минимум влияния на:
  - Защищаемые web-приложения
  - Остальную инфраструктуру
- Быстро, качественно, недорого

Кому на Руси WAF нужен?

- Интернет-магазин
- Онлайн-бизнес
- Онлайн-платежи
- Личные кабинеты клиентов
- Тем, кто просто не любит, когда сайт взламывают

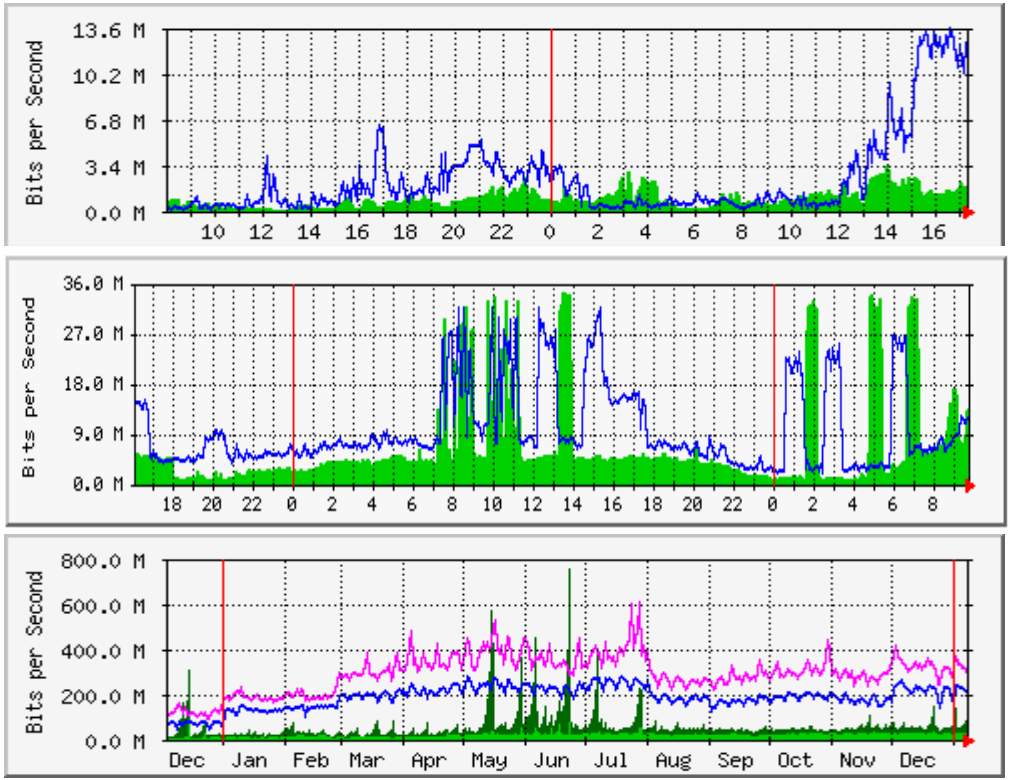
Задача: внедрить WAF. Архитектура



Ценообразующие факторы

- Обрабатываемый трафик:
  - TLS/сек
  - Mbps, Gbps
  - Conns
- Кластеризуемость
- Дополнительные функции

Ценообразующие факторы: Mbps



Ценообразующие факторы: TLS/сек

```
Jul 14 00:01:46 perimeter-fw %ASA-6-302014: Teardown TCP connection
591504883 for outside:192.0.2.208/41862 to dmz:192.168.113.1/443
duration 0:00:34 bytes 43801 TCP FINs

Jul 14 00:01:46 perimeter-fw %ASA-6-302014: Teardown TCP connection
591652278 for outside:192.0.2.63/1172 to dmz:192.168.113.1/443
duration 0:00:21 bytes 72205 TCP FINs

Jul 14 00:01:46 perimeter-fw %ASA-6-302014: Teardown TCP connection
591877877 for outside:192.0.2.242/49748 to dmz:192.168.113.1/443
duration 0:00:32 bytes 94174 TCP FINs
```

Ценообразующие факторы: Conns

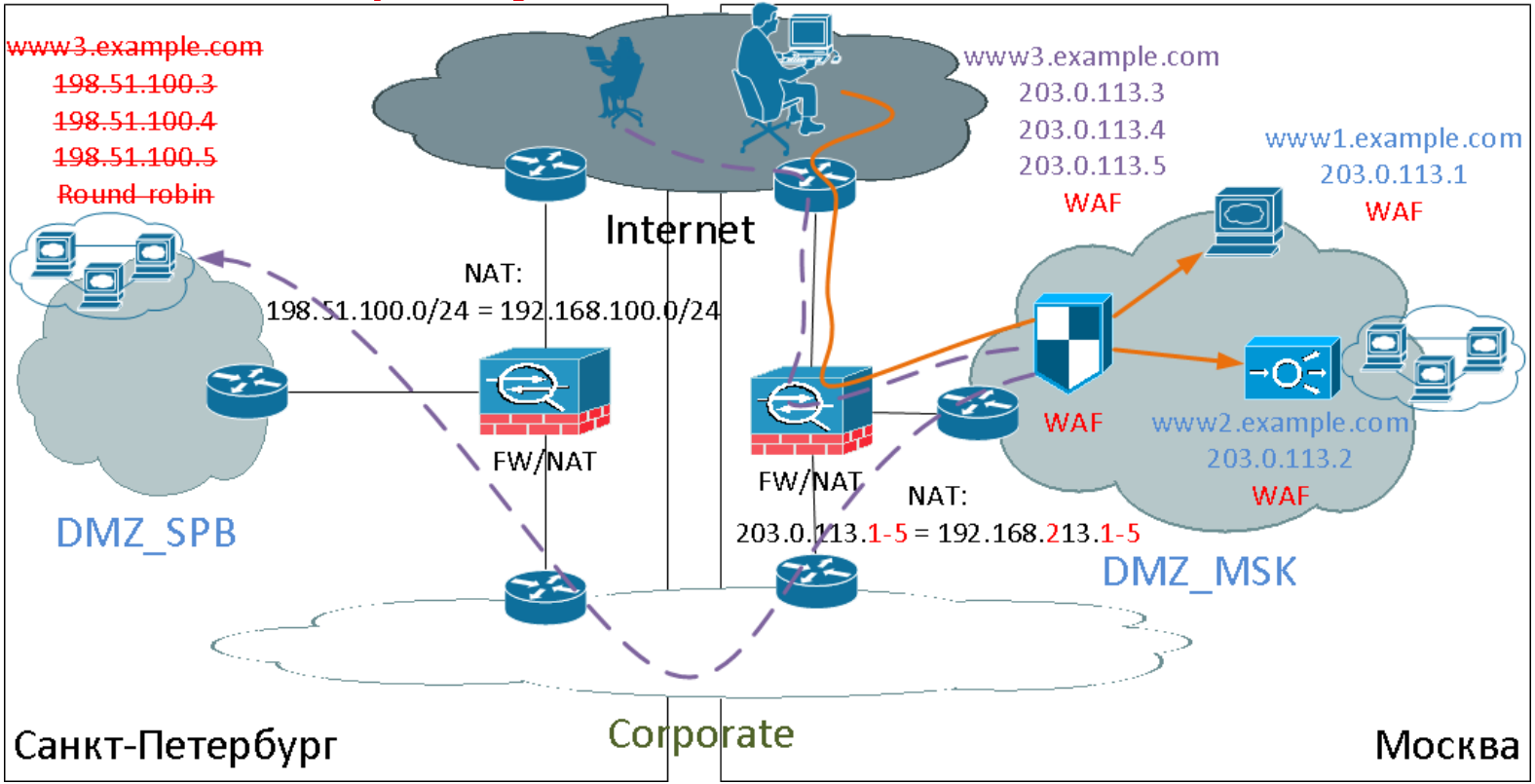
```
if t > d

 then C = T * t

if t < d

 then C = T * d
```

```
C = conns

T = TLS/sec

t = session timeout

d = session duration
```

Варианты архитектуры

- WAF sniffer
- WAF software
- WAF bridge / transparent reverse proxy
- WAF router
- WAF reverse proxy

WAF: reverse proxy



WAF: reverse proxy. Необходимые изменения

- Выделение IP-адресов для WAF
- Доступ из Интернет по HTTP/HTTPS к IP-адресам WAF
- Настройка TLS offload (если используется HTTPS)
- Настройка проксирования и вставки заголовков XFF
- Изменение правил NAT на firewall (если в DMZ на одном firewall)
- Изменение записей DNS (если в разных DMZ на разных firewall)

WAF: reverse proxy. Пример изменений

- Новые адреса для WAF

Серые 192.168.213.0/24

Белые 203.0.113.3-5

- Изменение правил NAT на firewall (в DMZ на одном firewall)

До: 203.0.113.1-5 = 192.168.113.1-5

После: 203.0.113.1-5 = 192.168.213.1-5

- Изменение записей DNS (в разных DMZ на разных firewall)

До:	www3.example.com	После:	www3.example.com
	198.51.100.3		203.0.113.3
	198.51.100.4		203.0.113.4
	198.51.100.5		203.0.113.3

WAF: reverse proxy. Анализ

Преимущества

- Единая точка защиты и контроля web-серверов
- Высокая масштабируемость: IP-маршрутизация + доступ
- Отсутствие влияния на L1/L2/L3-топологию сети
- TLS-offload (снижение нагрузки на сервера)
- Независимость от настроек, сбоев и уязвимостей ОС защищаемых web-ресурсов

Недостатки

- Единая точка отказа (минимизация: кластер, дублирование)
- Изменение настроек в случае аутентификации клиентов по сертификатам
- Подверженность атакам на WAF

Дополнительные аспекты

- Централизованное управление логикой работы (отдельный сервер)
- Резервное копирование конфигураций
- Интеграция с SIEM
- Вставка XFF и парсинг заголовка в логах
- Мониторинг эксплуатационных показателей
- Мониторинг TLS-handshake time
- Мониторинг CRL и времени действия сертификатов