03.06.2020

Технические аспекты внедрения WAF

МТС

Ты знаешь, что можешь!

#whoami

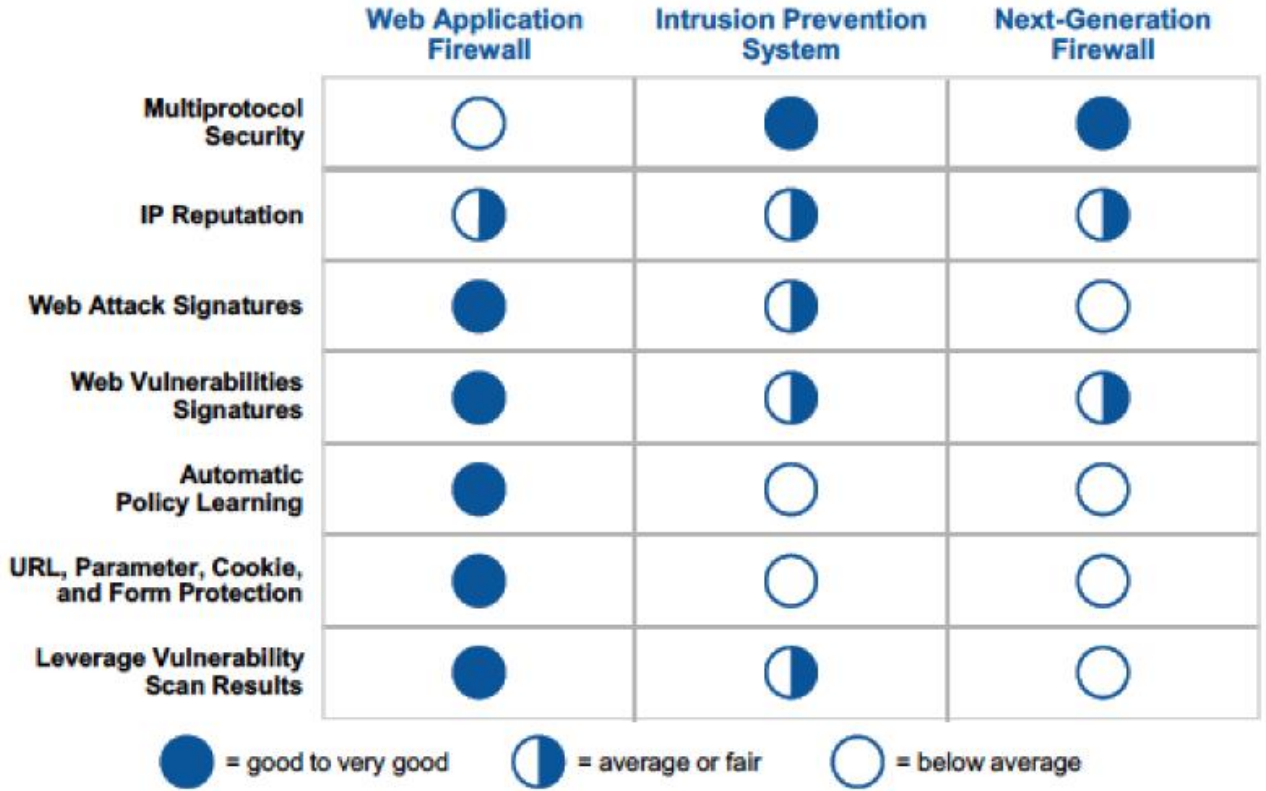
Андрей Дугин

Начальник отдела обеспечения информационной безопасности

http://aodugin.blogspot.com

МТС Ты знаешь, что можешь!

WAF vs NGFW vs IPS



Зачем нужен WAF?

- PCI DSS
- OWASP TOP10

https://www.owasp.org/index.php/Top_10-2017_Top_10

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

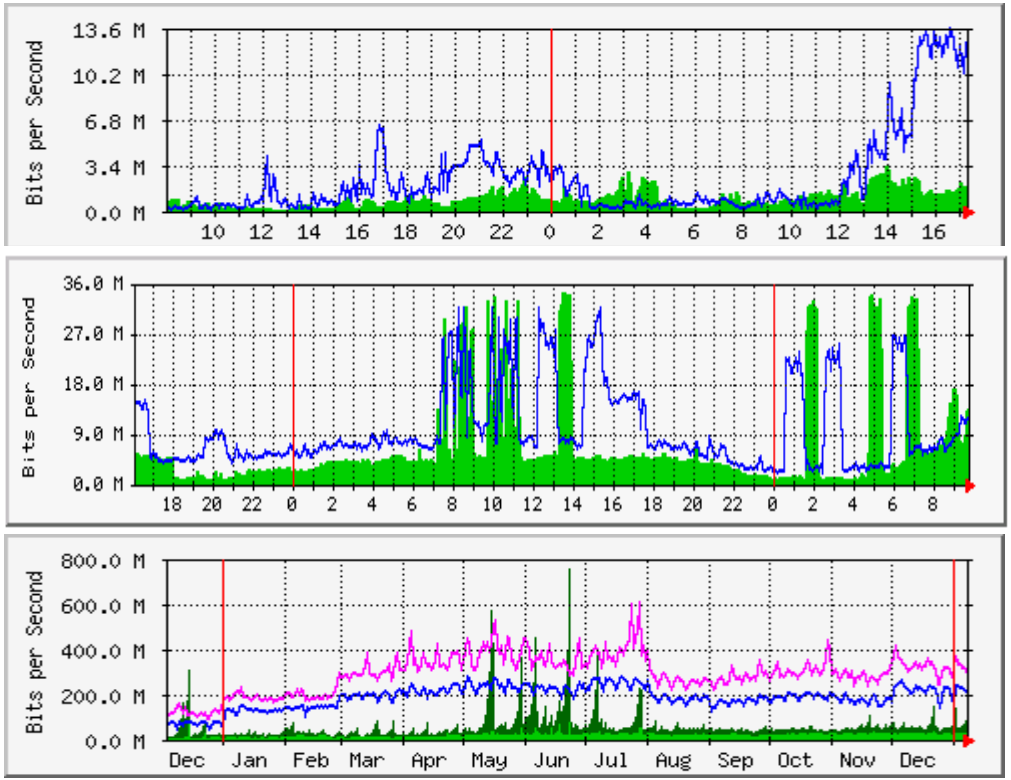
- OWASP Risk Rating Methodology

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Ценообразующие факторы

- Обрабатываемый трафик:
  - TLS/сек
  - Количество параллельных сессий
  - Mbps, Gbps
- Кластеризуемость
- Дополнительные функции

Ценообразующие факторы: Mbps, conns



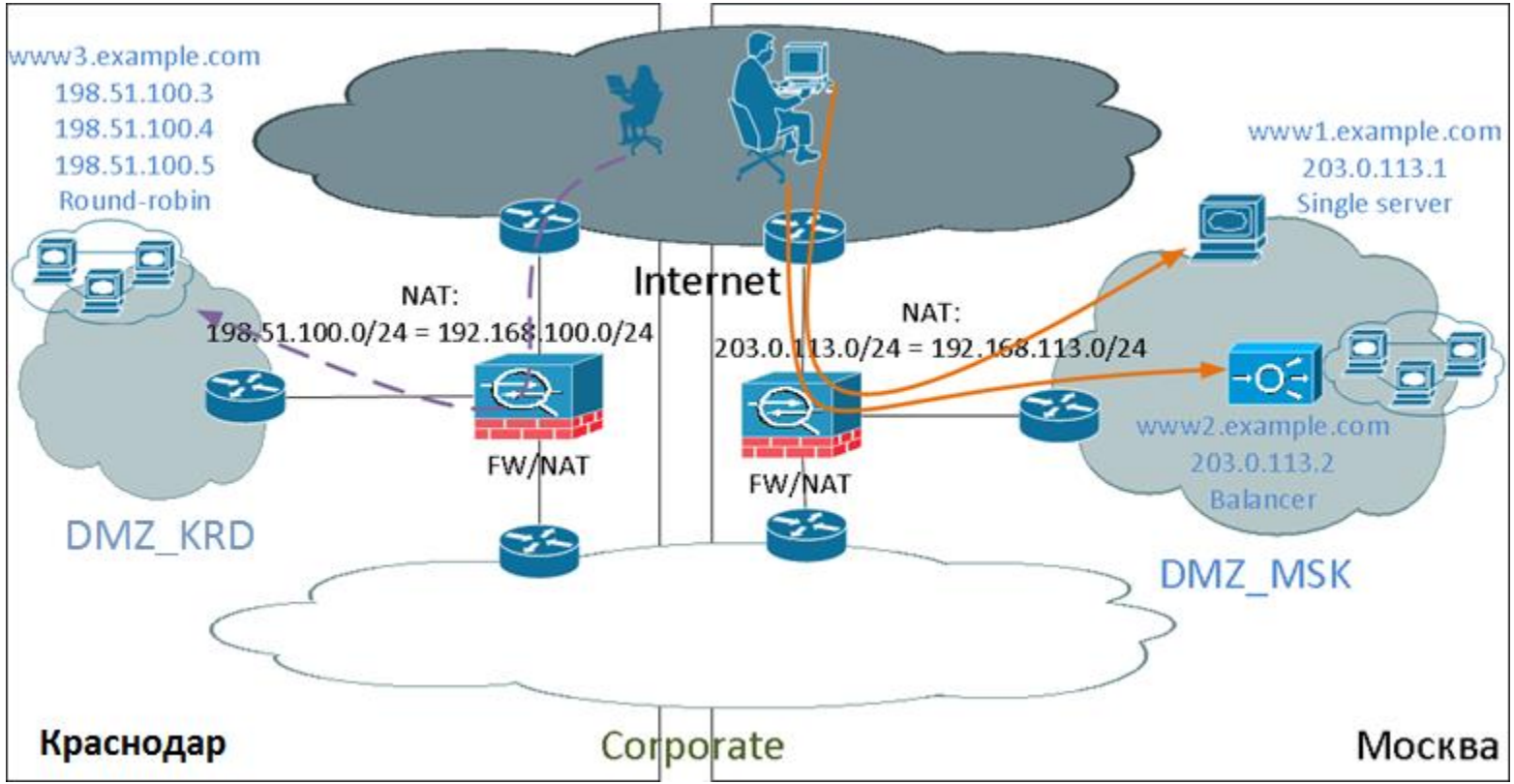
Ценообразующие факторы: TLS/сек

```
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
```

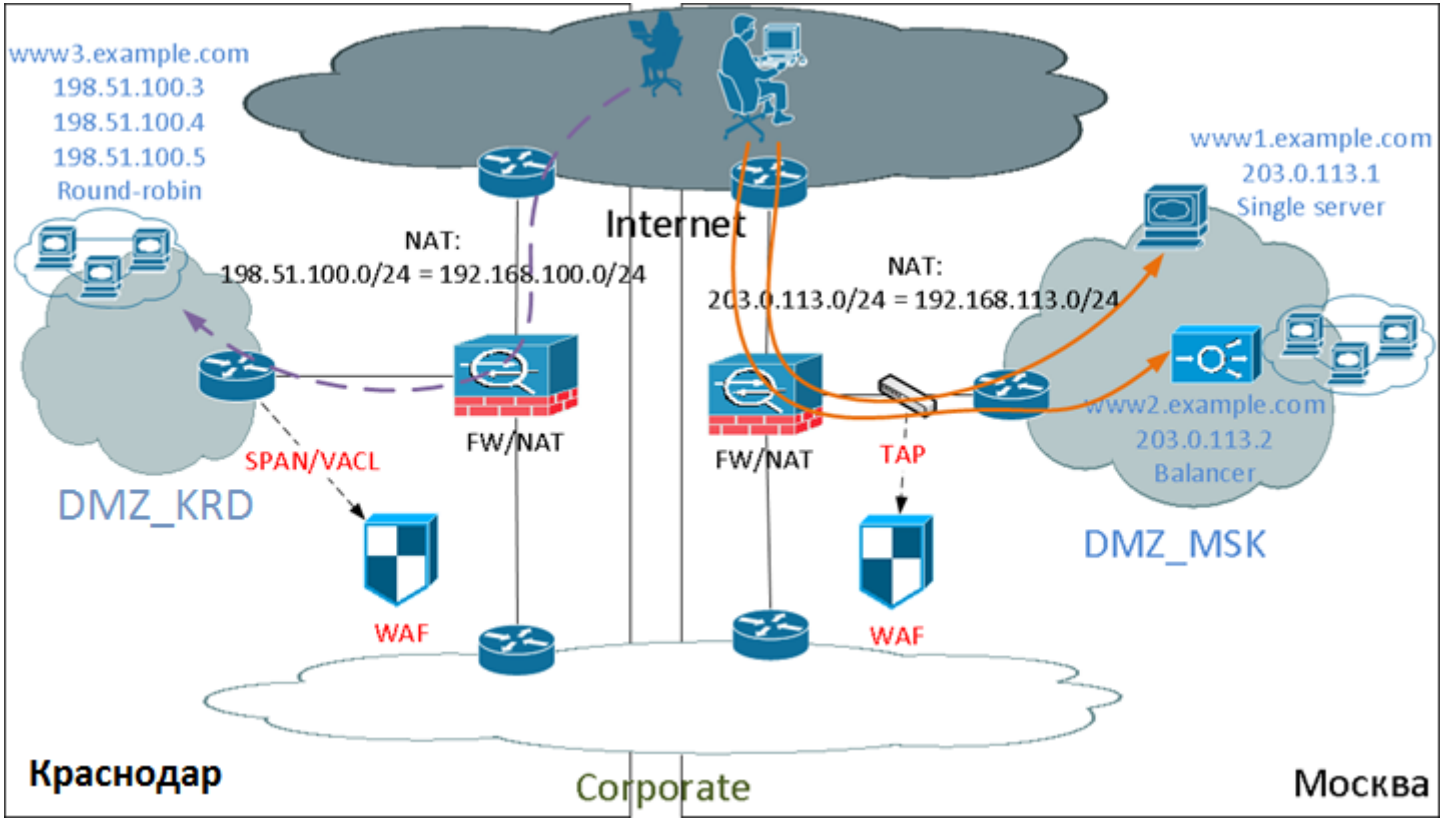
Варианты архитектуры

- Схема без WAF
- WAF sniffer
- WAF reverse proxy
- WAF router
- WAF bridge / transparent reverse proxy

Территориально-распределенная схема



WAF sniffer


www3.example.com
198.51.100.3
198.51.100.4
198.51.100.5
Round-robin
Internet
NAT:
198.51.100.0/24 = 192.168.100.0/24
NAT:
203.0.113.0/24 = 192.168.113.0/24
www1.example.com
203.0.113.1
Single server
FW/NAT
FW/NAT
SPAN/VACL
TAP
www2.example.com
203.0.113.2
Balancer
DMZ_KRD
DMZ_MSK
WAF
WAF
Краснодар
Corporate
Москва

WAF sniffer. Необходимые изменения

- Подача копии web-трафика DMZ на WAF:
  - SPAN/VACL-capture с коммутатора
  - TAP с физических линков

WAF sniffer. Анализ

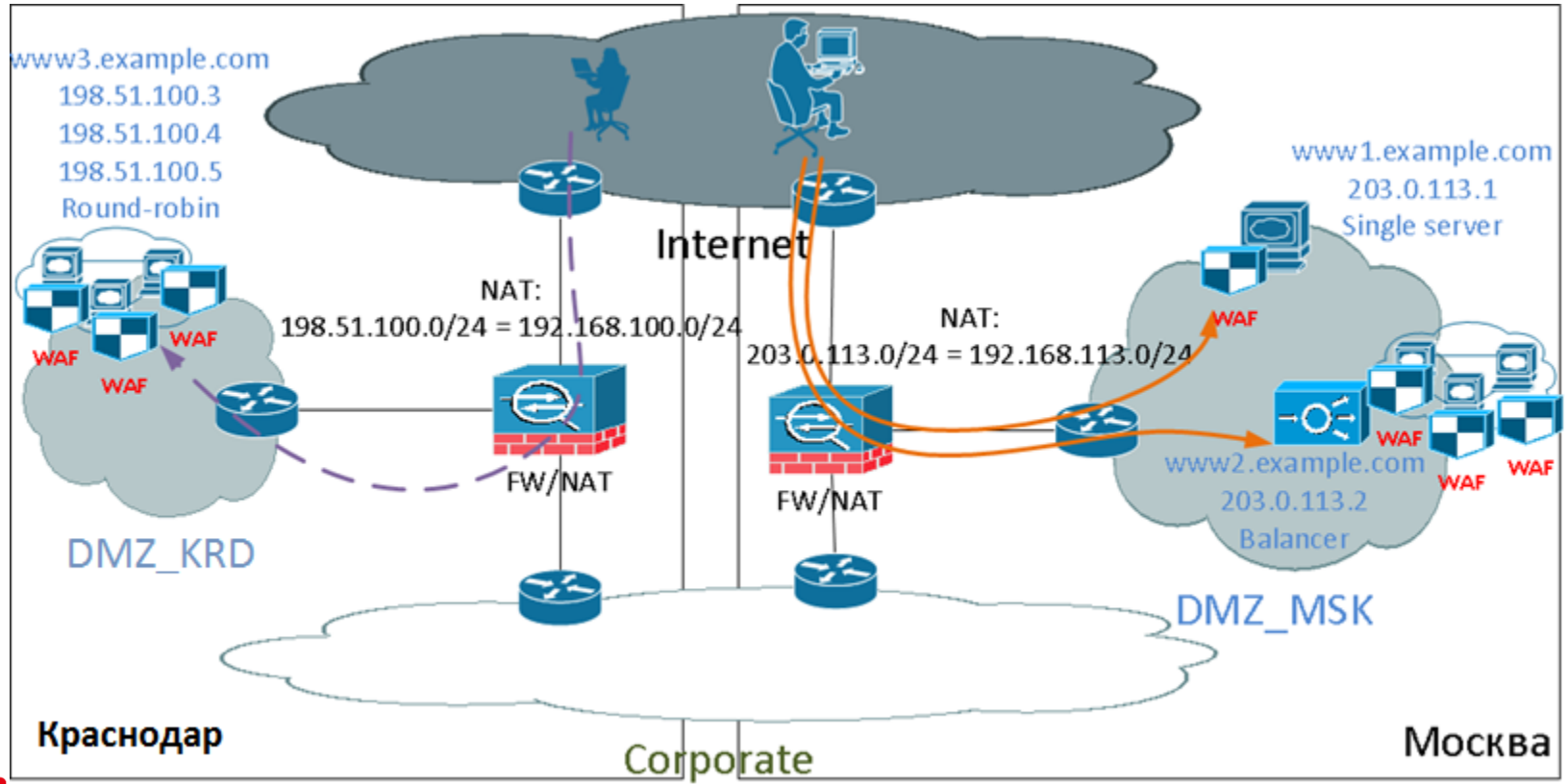
Преимущества

- Отсутствие влияния на трафик

Недостатки

- Отсутствие возможности отражения атак
- Ограничение при анализе TLS
- Масштабируемость: территориальная

WAF: ПО на сервере



WAF ПО на сервере. Необходимые изменения

- Работа с программным модулем WAF:
  - Установка на каждый сервер
  - Настройка

WAF: ПО на сервер. Анализ

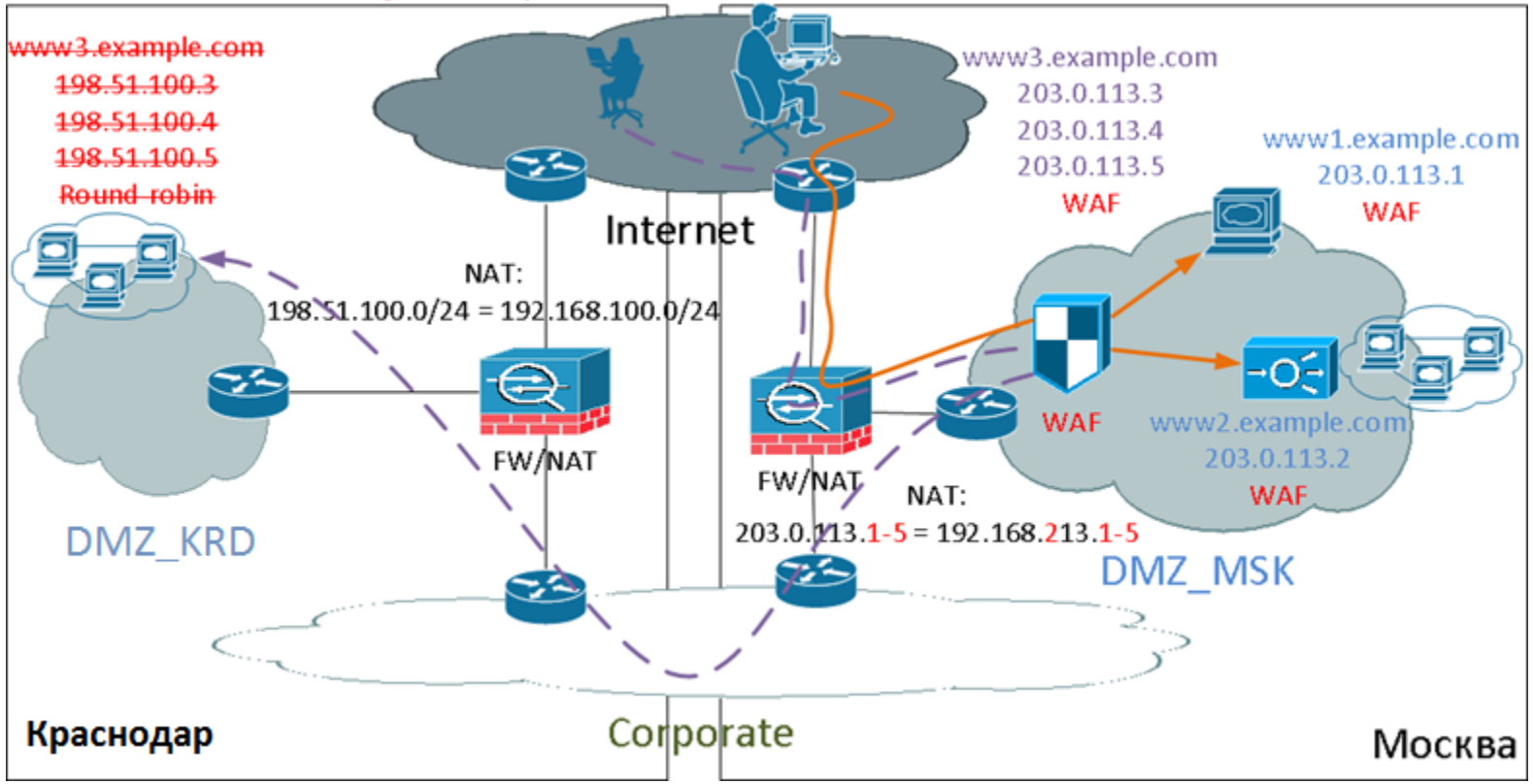
Преимущества

- Неизменность архитектуры
- Независимость от сетевой архитектуры
- Не нужен выделенный сервер для WAF
- Масштабируемость: количество инсталляций

Недостатки

- Использование вычислительных ресурсов web-сервера
- Совместимость с ОС/ПО
- Зависимость от настроек, сбоев и уязвимостей ОС

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. Анализ

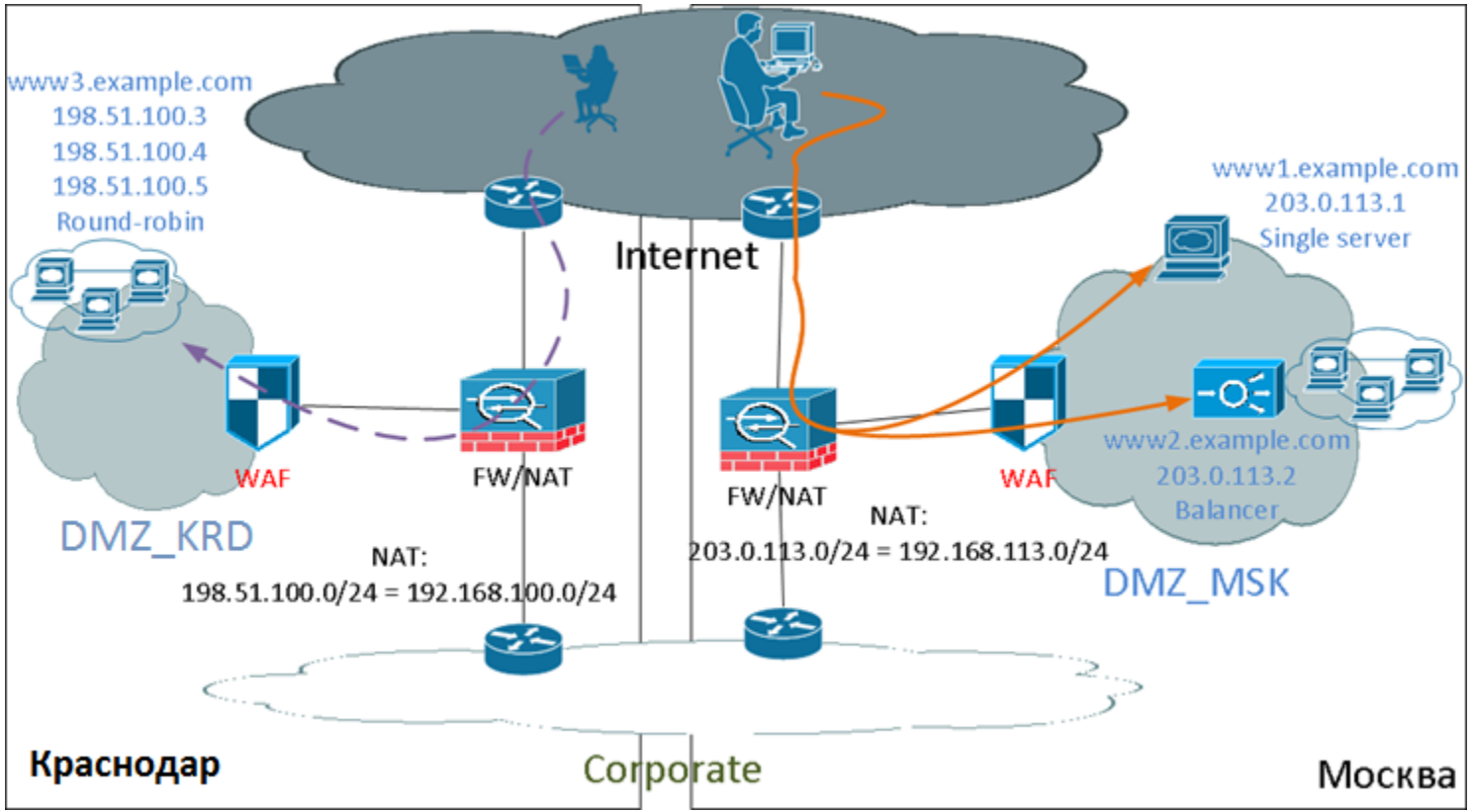
Преимущества

- 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

WAF: router


www3.example.com
198.51.100.3
198.51.100.4
198.51.100.5
Round-robin
Internet
www1.example.com
203.0.113.1
Single server
WAF
FW/NAT
FW/NAT
WAF
www2.example.com
203.0.113.2
Balancer
DMZ_KRD
NAT:
198.51.100.0/24 = 192.168.100.0/24
NAT:
203.0.113.0/24 = 192.168.113.0/24
DMZ_MSK
Краснодар
Corporate
Москва

WAF: router. Необходимые изменения

- Настройка маршрутизации в DMZ через WAF
- Объединение DMZ – при необходимости

WAF: router. Анализ

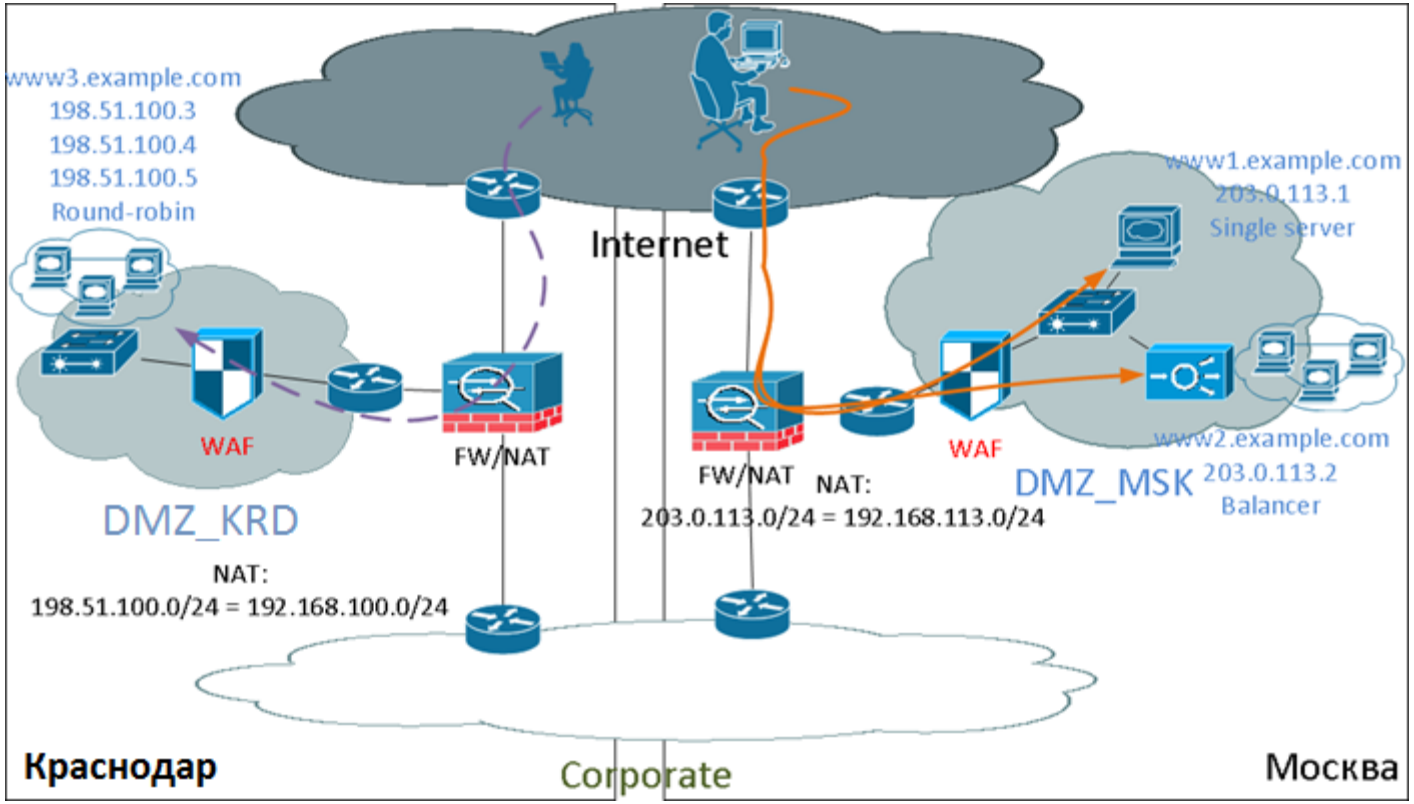
Преимущества

- Единая точка защиты и контроля web-серверов на DMZ
- Масштабируемость: на сервера в пределах L3-сегмента
- Отсутствие необходимости настройки серверов
- Независимость от настроек, сбоев и уязвимостей ОС защищаемых web-ресурсов

Недостатки

- Единая точка отказа всего трафика в DMZ (минимизация: кластер, дублирование)
- Необходимость реорганизации L3-сегмента

WAF: bridge / transparent reverse proxy



WAF: bridge / transparent reverse proxy. Необходимые изменения

- Настройка правил маршрутизации/коммутации трафика в DMZ через линк, на котором установлен WAF
- Объединение DMZ – при необходимости

WAF: bridge. Анализ

Преимущества

- Единая точка защиты и контроля web-серверов на DMZ
- Полная прозрачность
- Масштабируемость: на сервера DMZ за WAF-enabled линком
- Отсутствие необходимости настройки серверов
- Независимость от настроек, сбоев и уязвимостей ОС защищаемых web-ресурсов

Недостатки

- Единая точка отказа всего трафика в DMZ (минимизация: кластер, дублирование, аппаратный bypass)
- Необходимость L1/L2-реорганизации DMZ

WAF: transparent reverse proxy. Анализ

Преимущества

- Единая точка защиты и контроля web-серверов на DMZ
- Полная прозрачность
- Масштабируемость: на сервера DMZ за WAF-enabled линком
- Отсутствие необходимости настройки серверов
- Независимость от настроек, сбоев и уязвимостей ОС защищаемых web-ресурсов
- Возможность TLS offload

Недостатки

- Единая точка отказа всего трафика в DMZ (минимизация: кластер, дублирование, аппаратный bypass)
- Необходимость L1/L2-реорганизации DMZ

WAF: общие задачи при внедрении

- Запас производительности
- Управление сущностями WAF
- Управление политиками
- Управление TLS-сертификатами и ключами
- Мониторинг работоспособности устройств/приложений
- Таймауты: тюнинг и выравнивание
- Интеграция со сканнером безопасности
- Интеграция с SIEM/SOC
- Отчетность