23.09.2016

Внедрение WAF: взгляд архитектора

МТС

Ты знаешь, что можешь!

Андрей Дугин

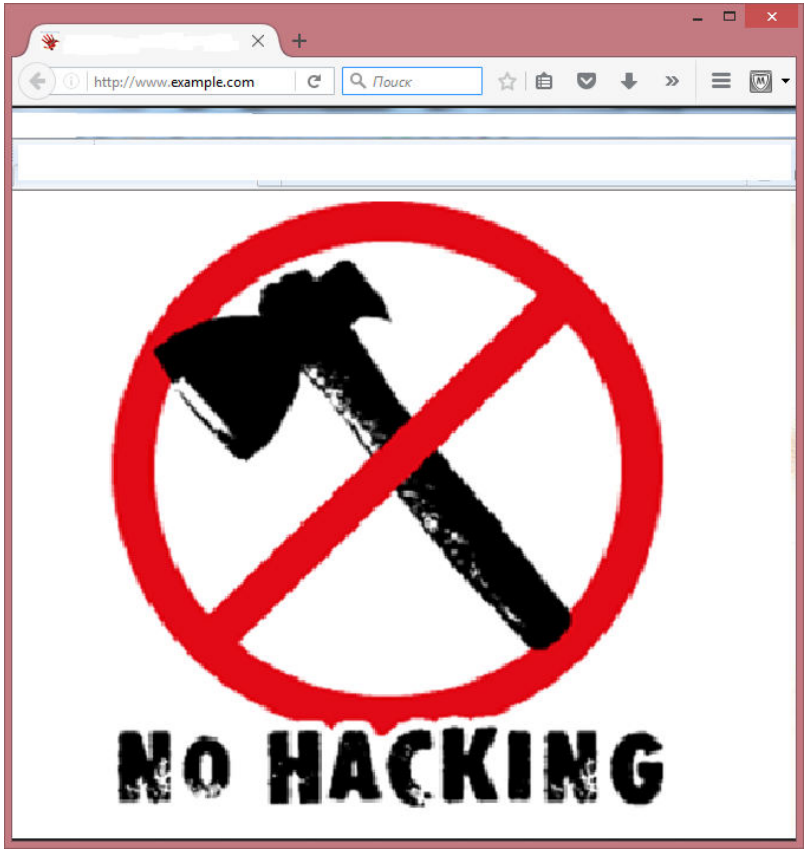
Инженер по защите информации

Департамент информационной безопасности и специальных проектов

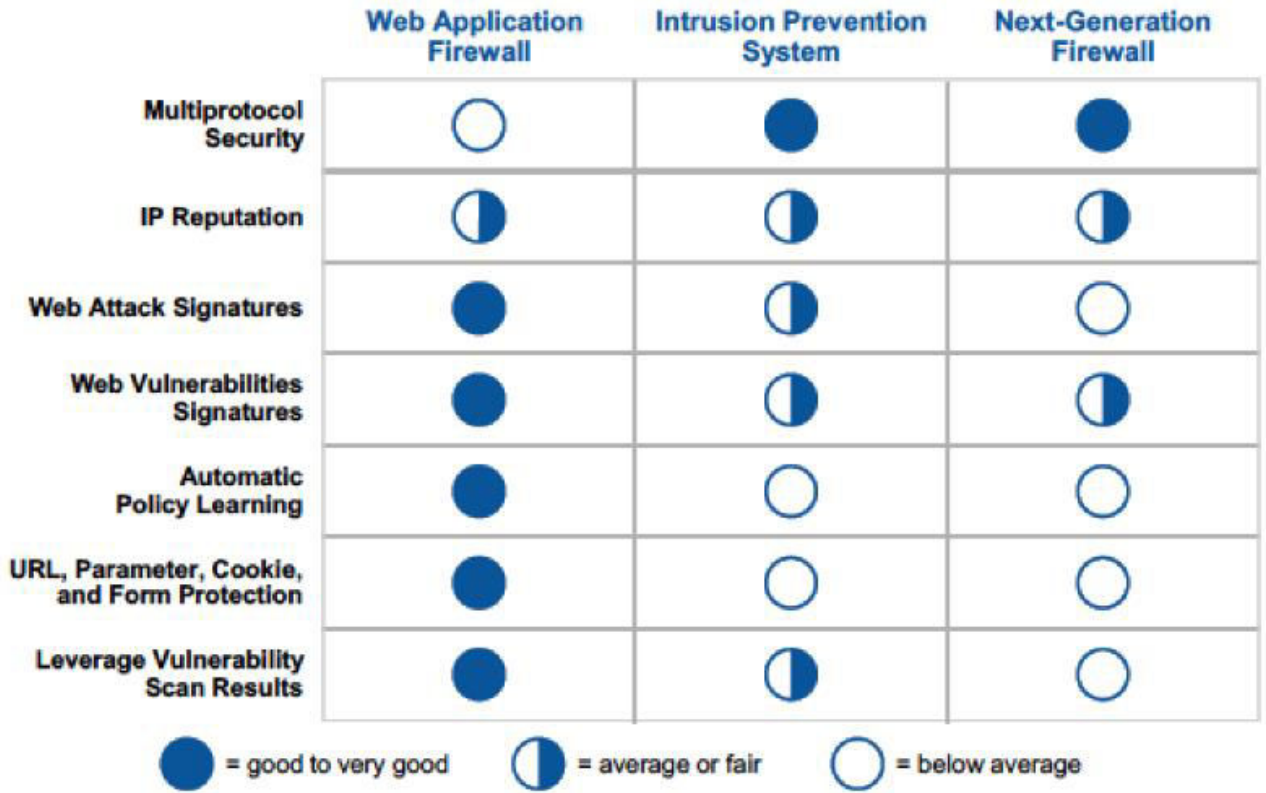
МТС Ты знаешь, что можешь!

Что такое WAF?

- Программный либо программно-аппаратный модуль, предназначенный для защиты сайтов от атак, направленных на web-приложения.



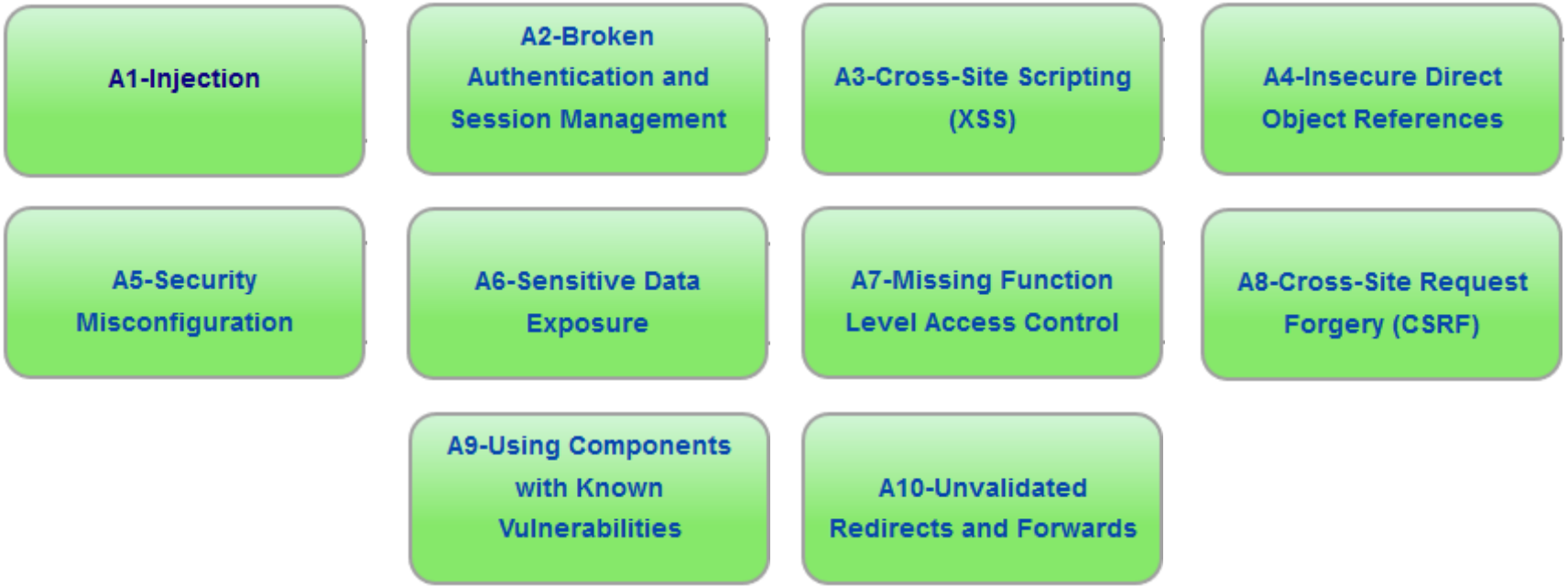
WAF vs NGFW vs IPS



Зачем нужен WAF? PCI DSS 3.2

- 6.6 For **public-facing web applications**, ensure that either one of the following methods is in place as follows:
- ...
- Examine the system configuration settings and interview responsible personnel to verify that **an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place** as follows:
  - Is situated in front of public-facing web applications to detect and prevent web-based attacks.
  - Is actively running and up to date as applicable.
  - Is generating audit logs.
  - Is configured to either block web-based attacks, or generate an alert that is immediately investigated.

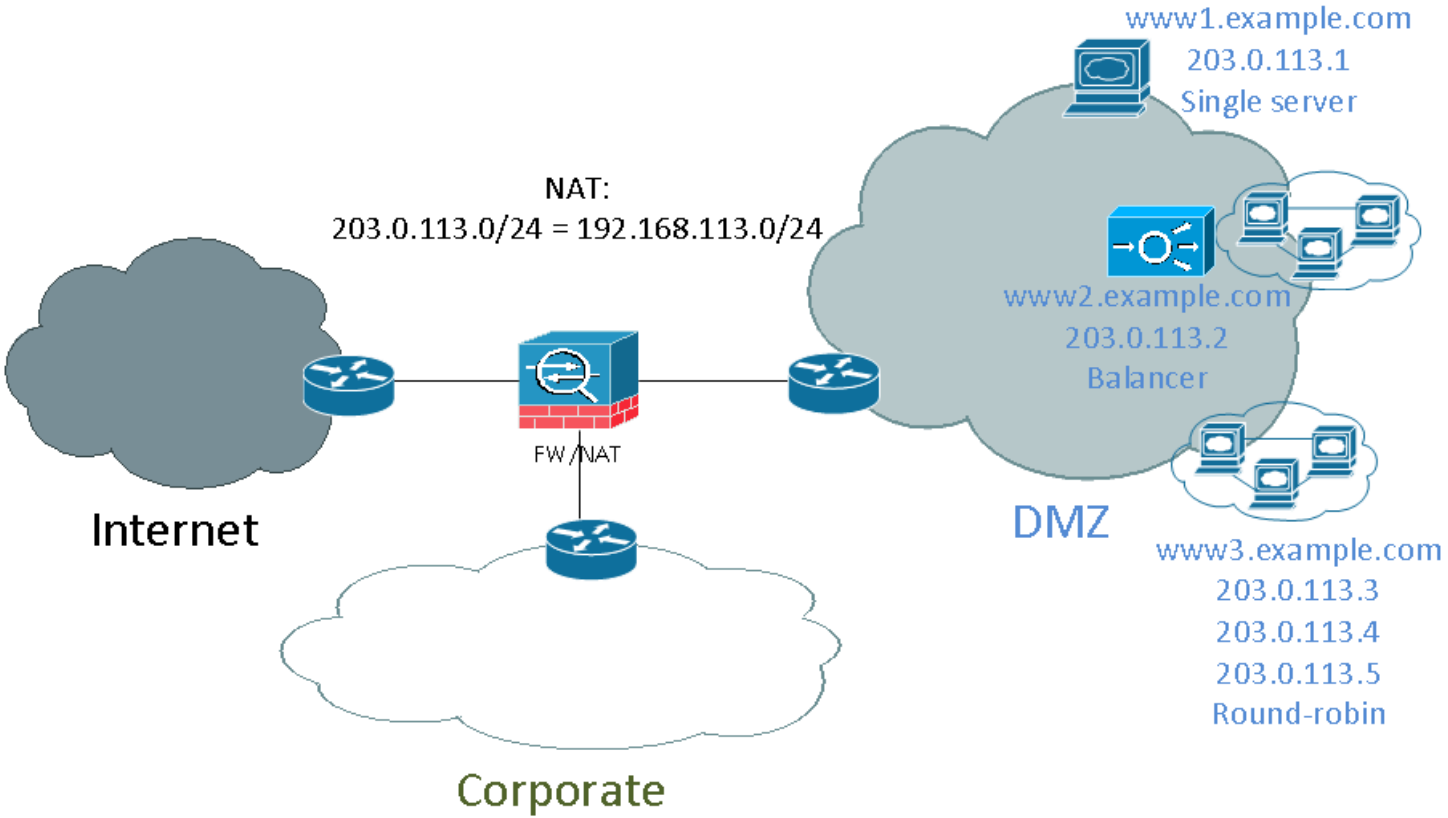
Зачем нужен WAF? OWASP Top 10



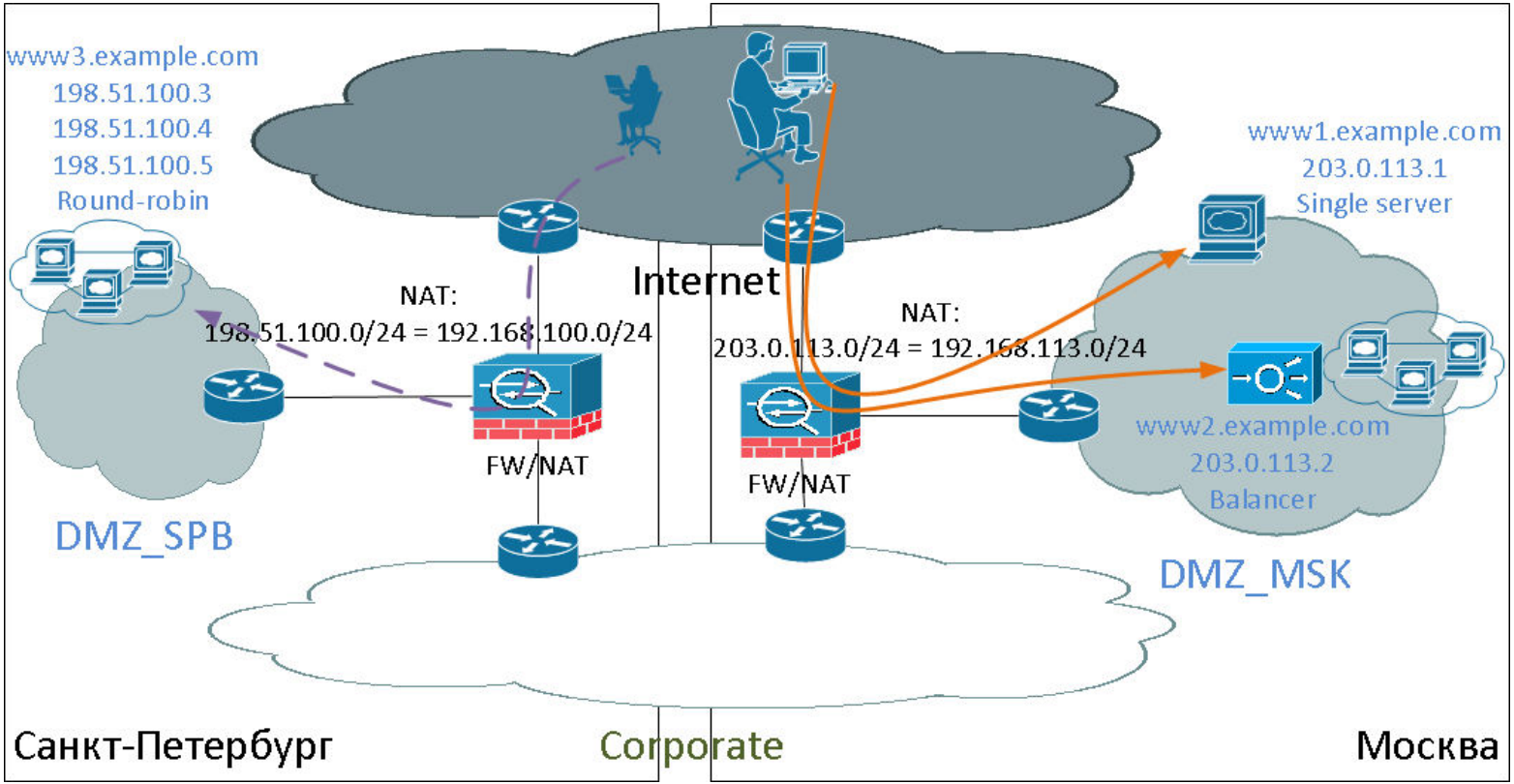
Варианты архитектуры

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

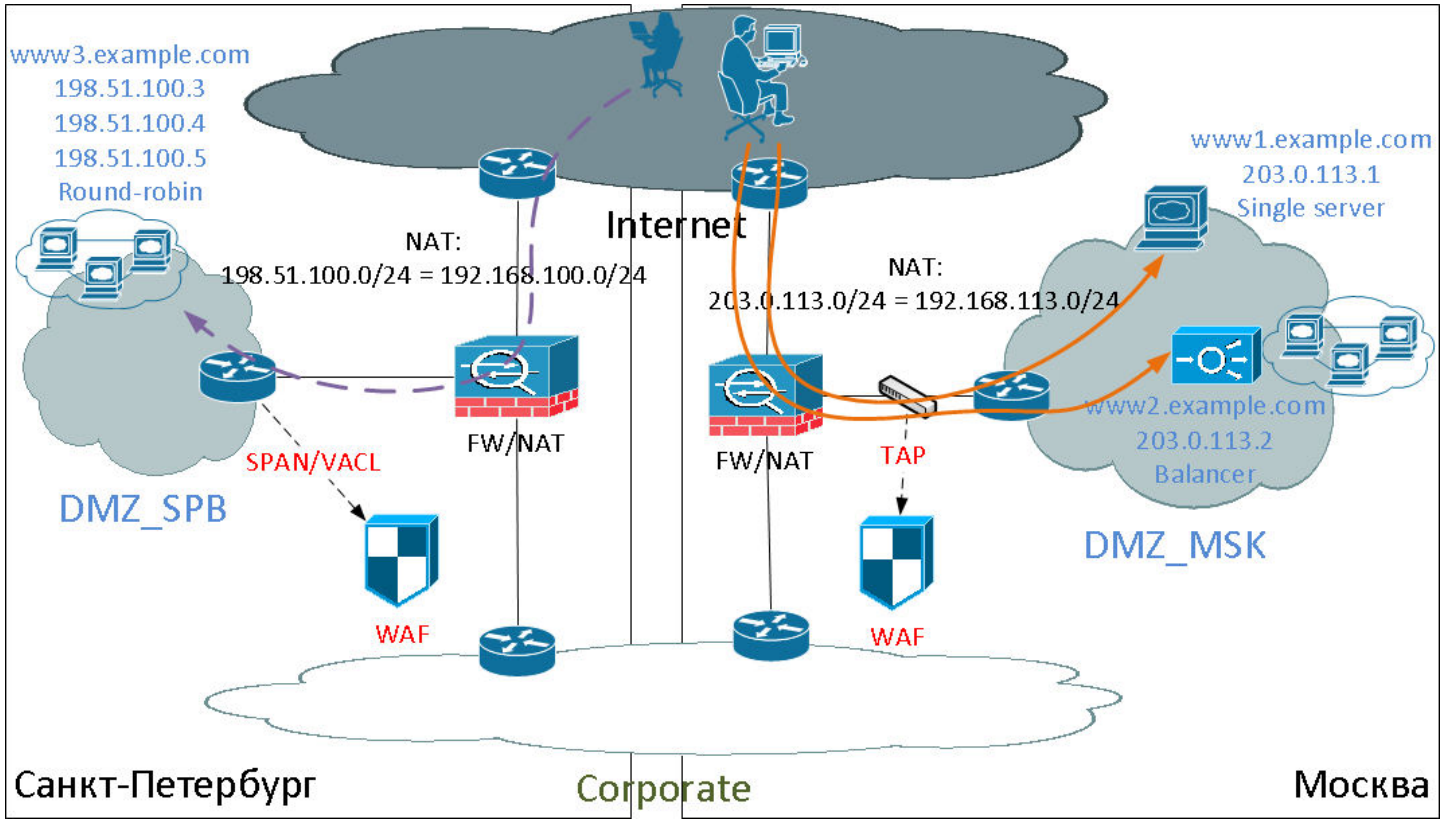
Упрощенная схема



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_SPB
DMZ_MSK
WAF
WAF
Санкт-Петербург
Corporate
Москва

WAF sniffer. Необходимые изменения

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

WAF sniffer. Анализ

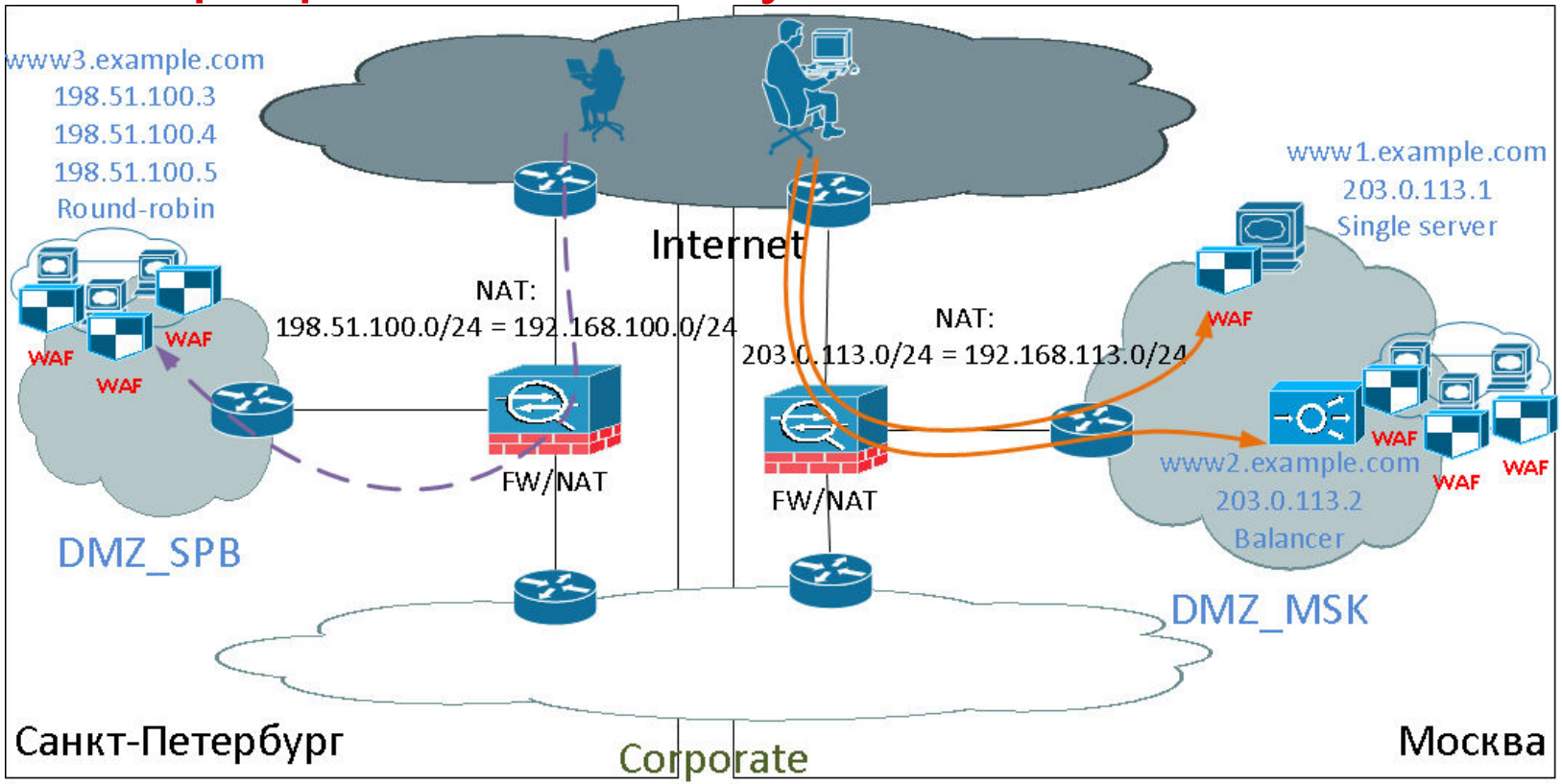
Преимущества

- Отсутствие влияния на трафик

Недостатки

- Отсутствие возможности отражения атак
- Масштабируемость: территориальная

WAF: программный модуль



WAF: программный модуль. Необходимые изменения

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

WAF: ПО на сервер. Анализ

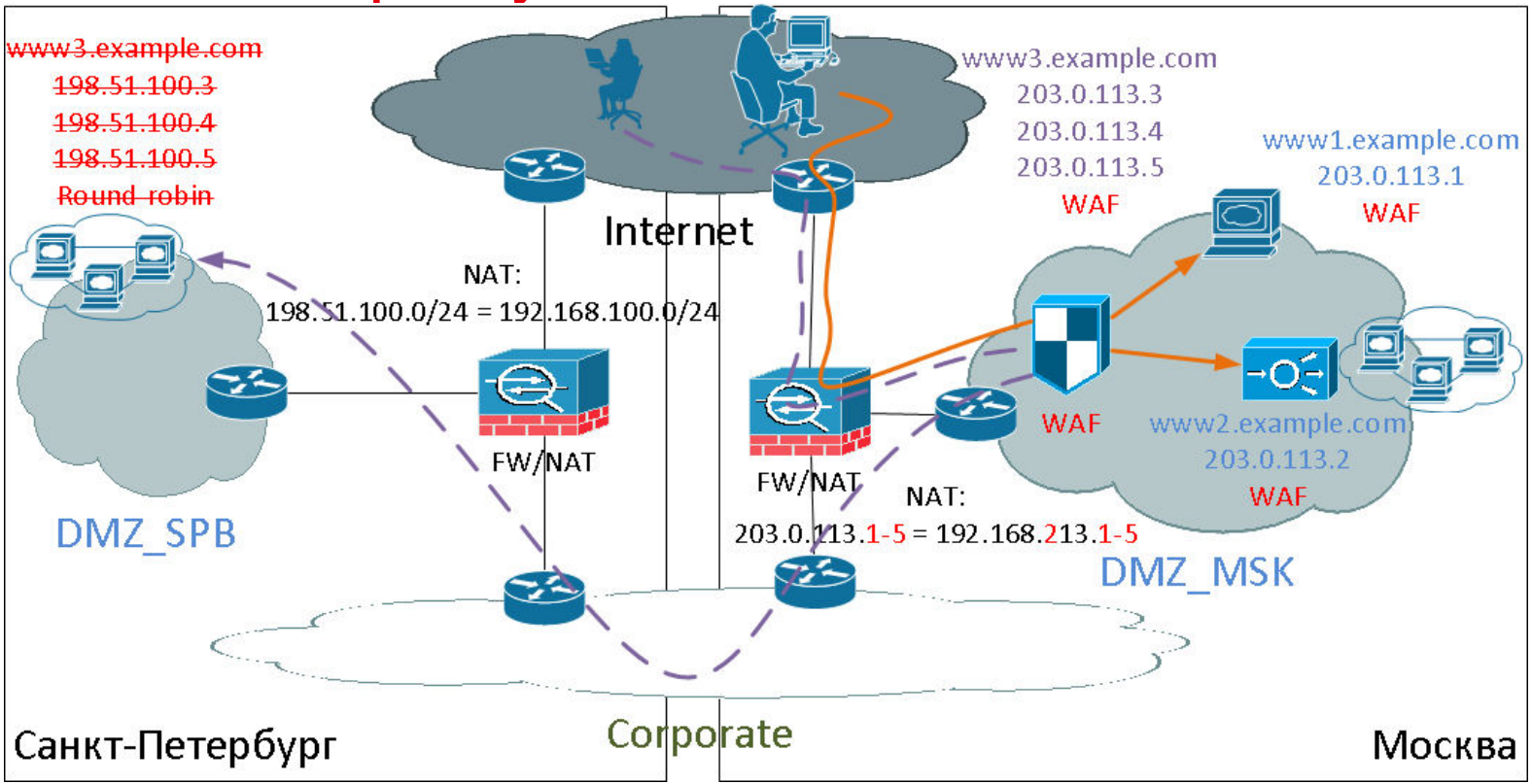
Преимущества

- 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 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

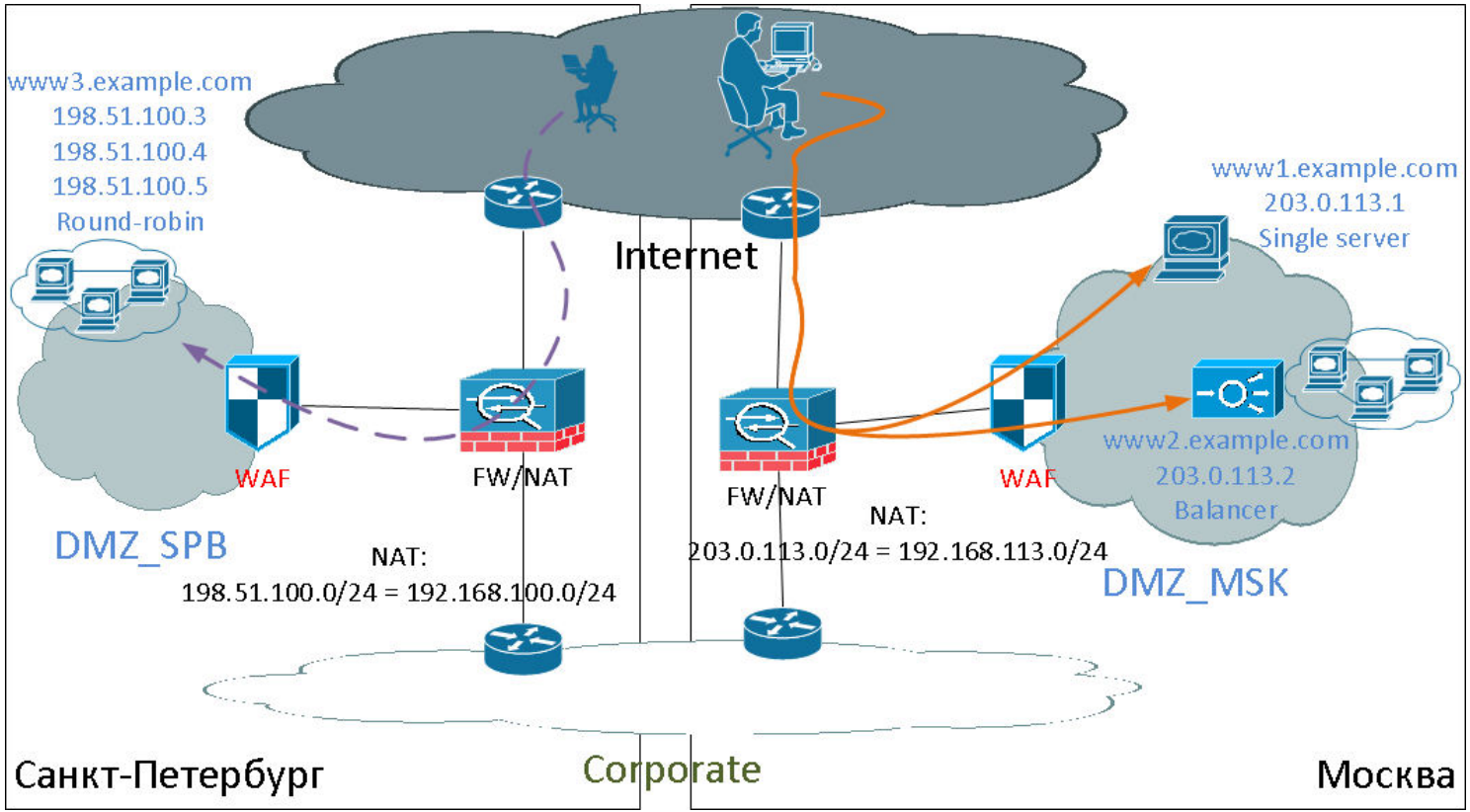
Преимущества

- 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

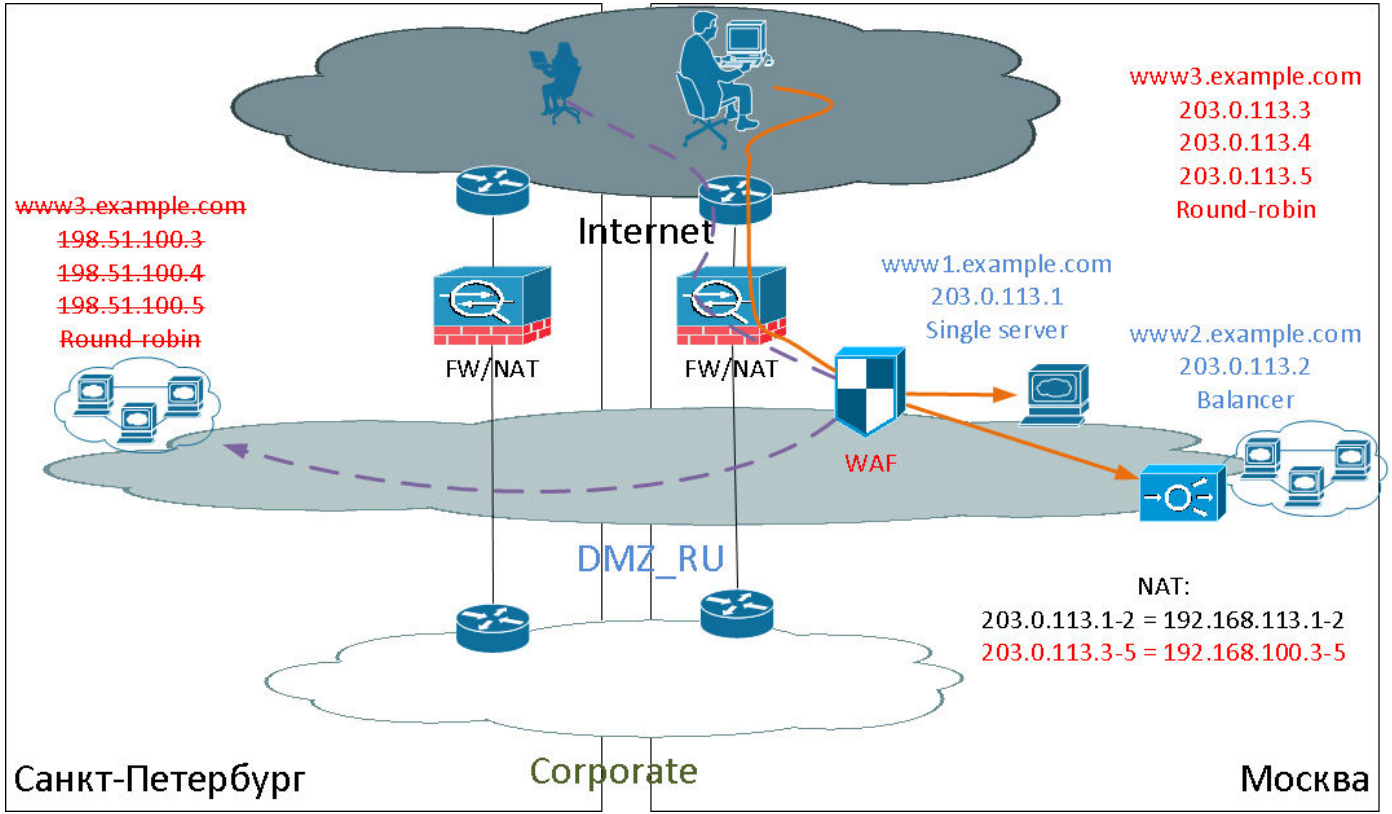
Недостатки

- Единая точка отказа (минимизация: кластер, дублирование)
- Подверженность атакам на WAF

WAF: router. 2 DMZ



WAF: router. 1 DMZ



WAF: router. Необходимые изменения

- Настройка маршрутизации в DMZ через WAF
- Объединение DMZ – при необходимости
- Изменение маршрутизации/NAT/DNS – при объединении DMZ

WAF: router. Анализ

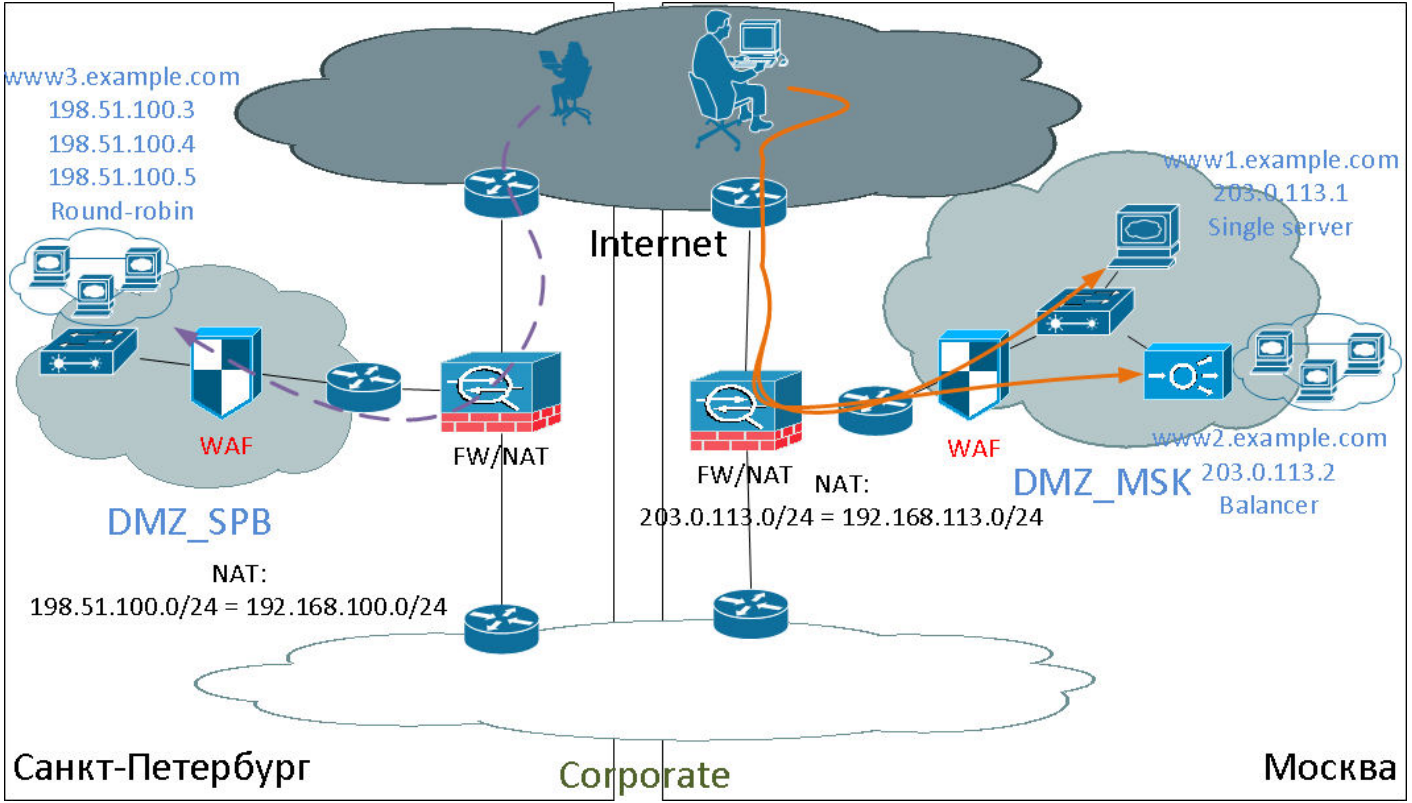
Преимущества

- 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

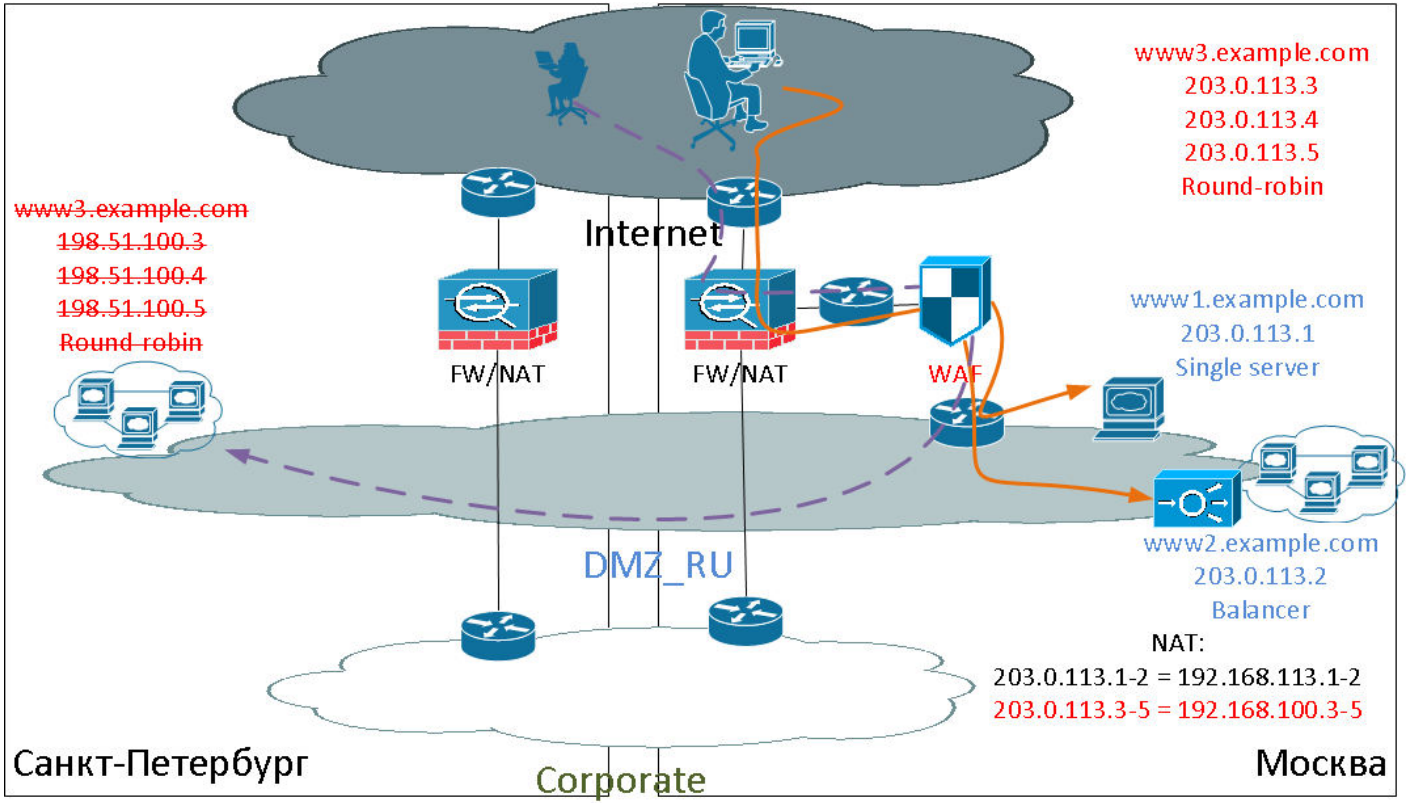
Недостатки

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

WAF: bridge / transparent reverse proxy. 2 DMZ



WAF: bridge / transparent reverse proxy. 1 DMZ



WAF: bridge / transparent reverse proxy. Необходимые изменения

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

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)
- Необходимость L1/L2-реорганизации DMZ

WAF: общие задачи

- 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