DDOS: УРОКИ ЗАЩИТЫ

RED SECURITY

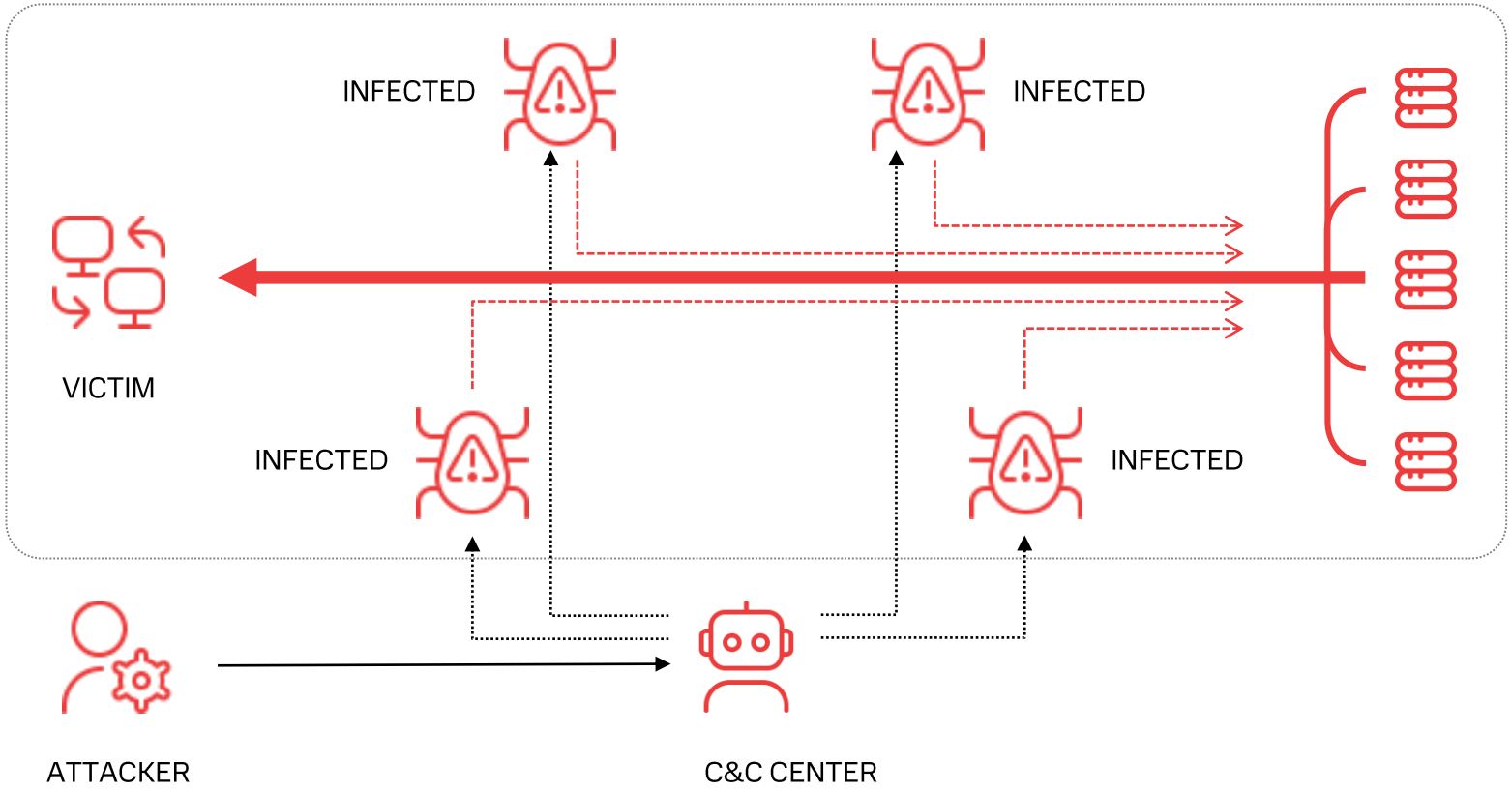
Андрей Дугин

Руководитель центра сервисов кибербезопасности
RED Security

Типовая схема DDoS-атаки и основные вектора

RED SECURITY

- DNS amplification
- NTP amplification
- TCP SYN/ACK flood
- TCP SYN flood*
- HTTP flood*



DDoS может поджидать нас на любом стыке с интернетом

RED SECURITY

Внешние веб-сайты компании	landing, e-commerce, selfcare, webSSO
Инфраструктурные сервисы на периметре	DNS, e-mail smart host, MX, OWA, mobile e-mail
Системы удалённой работы	VPN, VDI, MFA, task trackers
Интеграции с подрядчиками и M2M-взаимодействия через интернет	IP-IP direct, GRE, VPN
СЗИ внешнего периметра	WAF, Antibot, NGFW, VPN
Точки выхода в интернет пользователей и серверов	NAT 1-1, NAT-pool, proxy
Ресурсы компании в облаках Cloud-провайдеров	

Защита от DDoS на сети интернет-провайдера

RED SECURITY

Проходят через центр очистки:

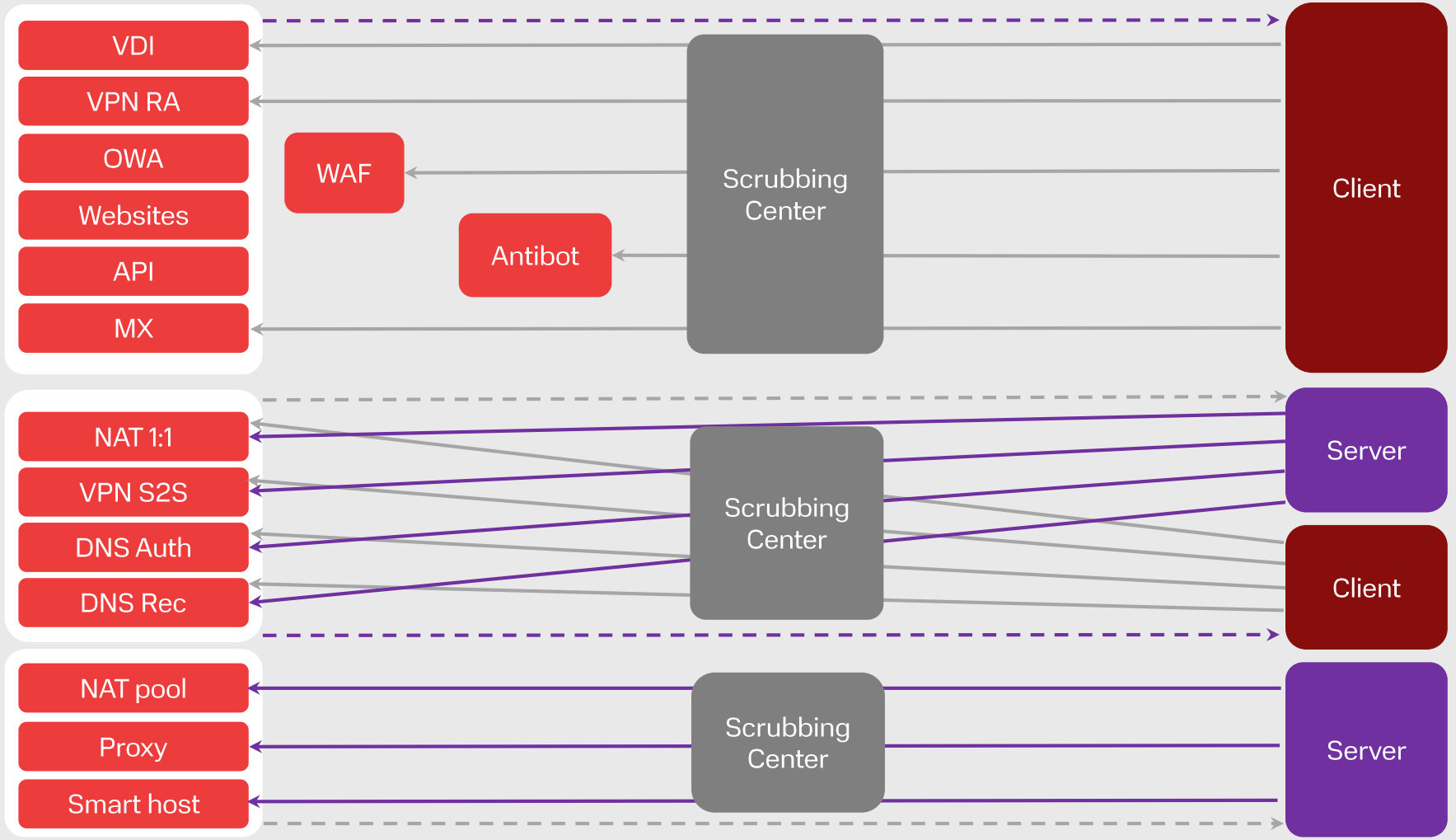
TCP SYN
TCP ACK
UDP request

TCP SYN/ACK
UDP reply

Не проходят через центр очистки:

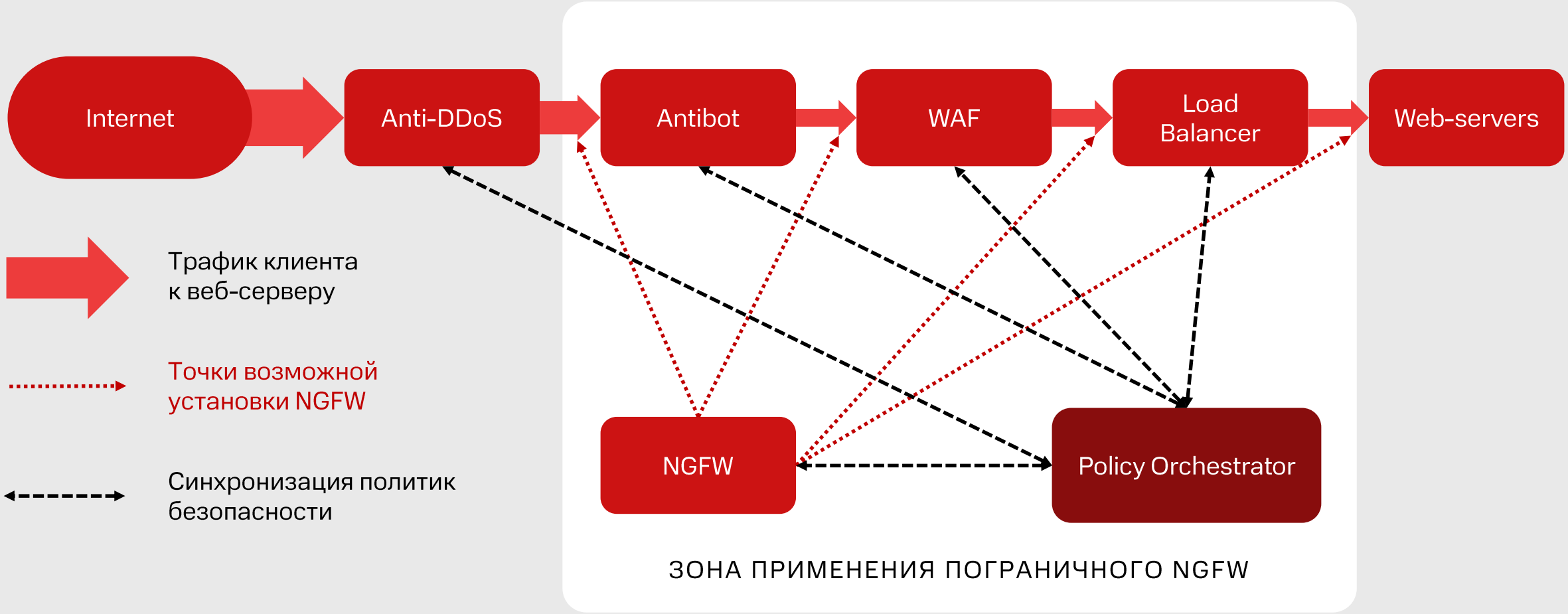
TCP SYN
TCP ACK
UDP request

TCP SYN/ACK
UDP reply



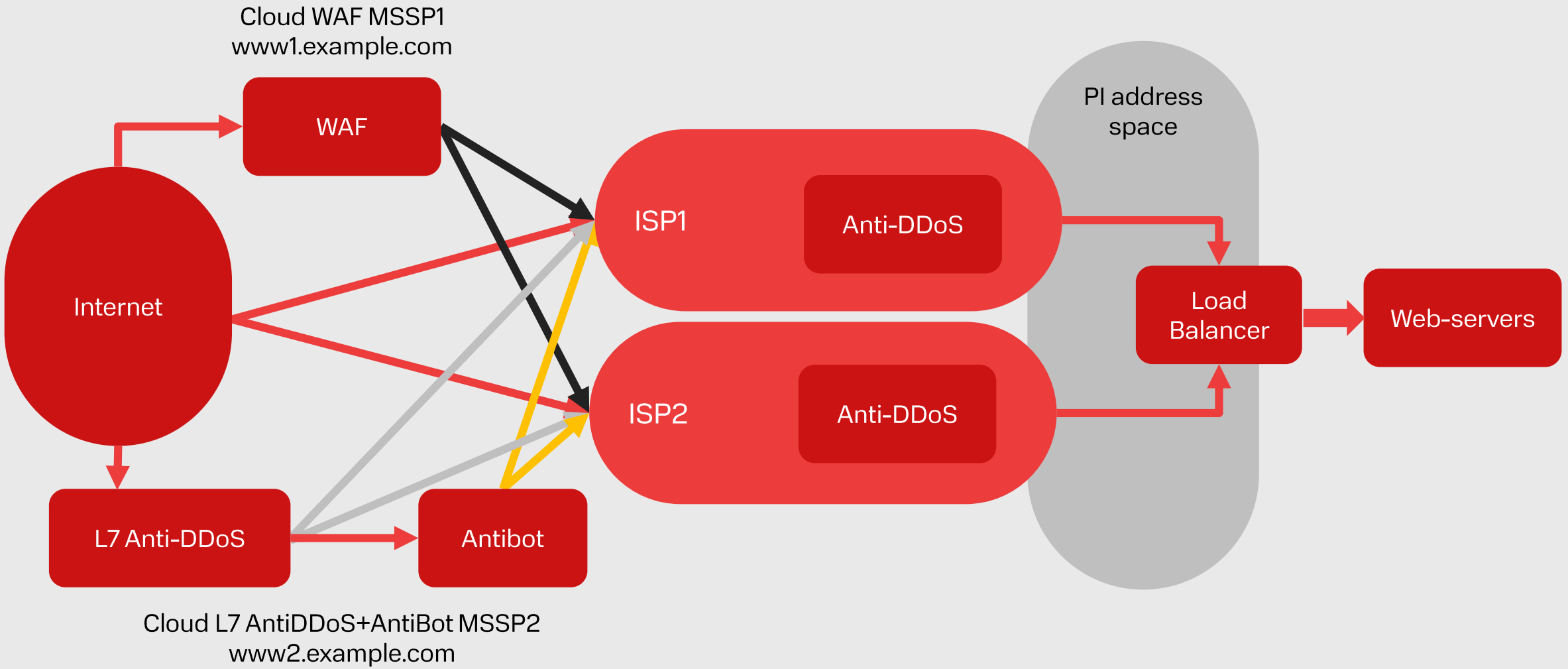
Защита web-ресурсов от DDoS через MSSP

RED SECURITY



Защита web-ресурсов от DDoS через разных MSSP

RED SECURITY



ToDo

RED SECURITY

- Разделить сегменты по направлениям трафика
  - MX и Smart host
  - VPN S2S и VPN RA
  - Серверы в DMZ и точки выхода в интернет (NAT pool, proxy)
  - Авторитативный и рекурсивный DNS
- Организовать инициацию подключения DMZ-серверов в интернет через прокси-сервер
- Синхронизировать правила ACL NGFW и центра очистки
- Использовать разные NGFW на стыке с интернетом и внутренние NGFW
- Разместить локальный центр очистки в своем ЦОД с возможностью cloud signaling с центром очистки ISP
- При подключении к нескольким ISP приобретать сервис Anti-DDoS у каждого, либо быть готовыми оперативно отключать каналы без защиты от DDoS
- При приобретении облачных сервисов WAF либо Antibot, получить подтверждение от MSSP об их защите от DDoS