

External Network Perimeter Profiling. The Simple Way to Protect from DDoS

RED
SECURITY

Andrey Dugin
Managed Cybersecurity Services CTO
RED Security

RED Security is Russian MSSP. Portfolio

RED SECURITY

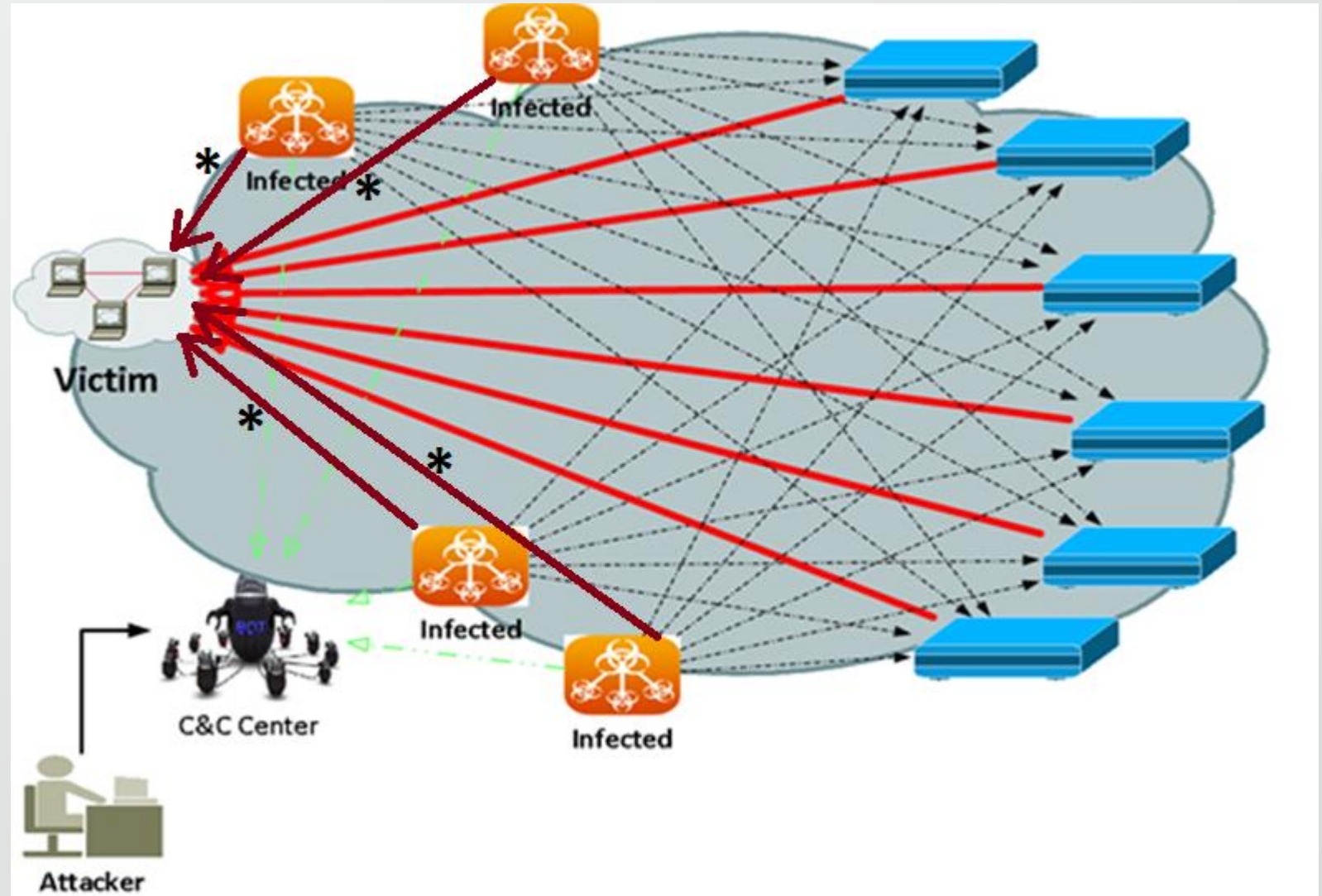


- Managed Cybersecurity Services:
 - Security Operations Center (SOC)
 - AntiDDoS (ISP-based)
 - AntiBot
 - Managed Web Application Firewall (WAF)
 - Managed Virtual Private Network (VPN)
 - Multi-Factor Authentication (MFA)
 - Security Awareness (SA)
- Integration services
- Consulting & Audit

- Head of Managed Cybersecurity Services @RED Security
- 20+ years of experience in the field of network security, network architecture, and cybersecurity
- Worked in 5 countries
- 15+ years of in-house experience
- 8 years of MSSP experience
- Started and managed 7 cybersecurity services from scratch
 - Security Operations Center (SOC)
 - AntiDDoS
 - AntiBot
 - Managed Web Application Firewall (WAF)
 - Managed Virtual Private Network (VPN)
 - Multi-Factor Authentication (MFA)
 - Security Awareness (SA)

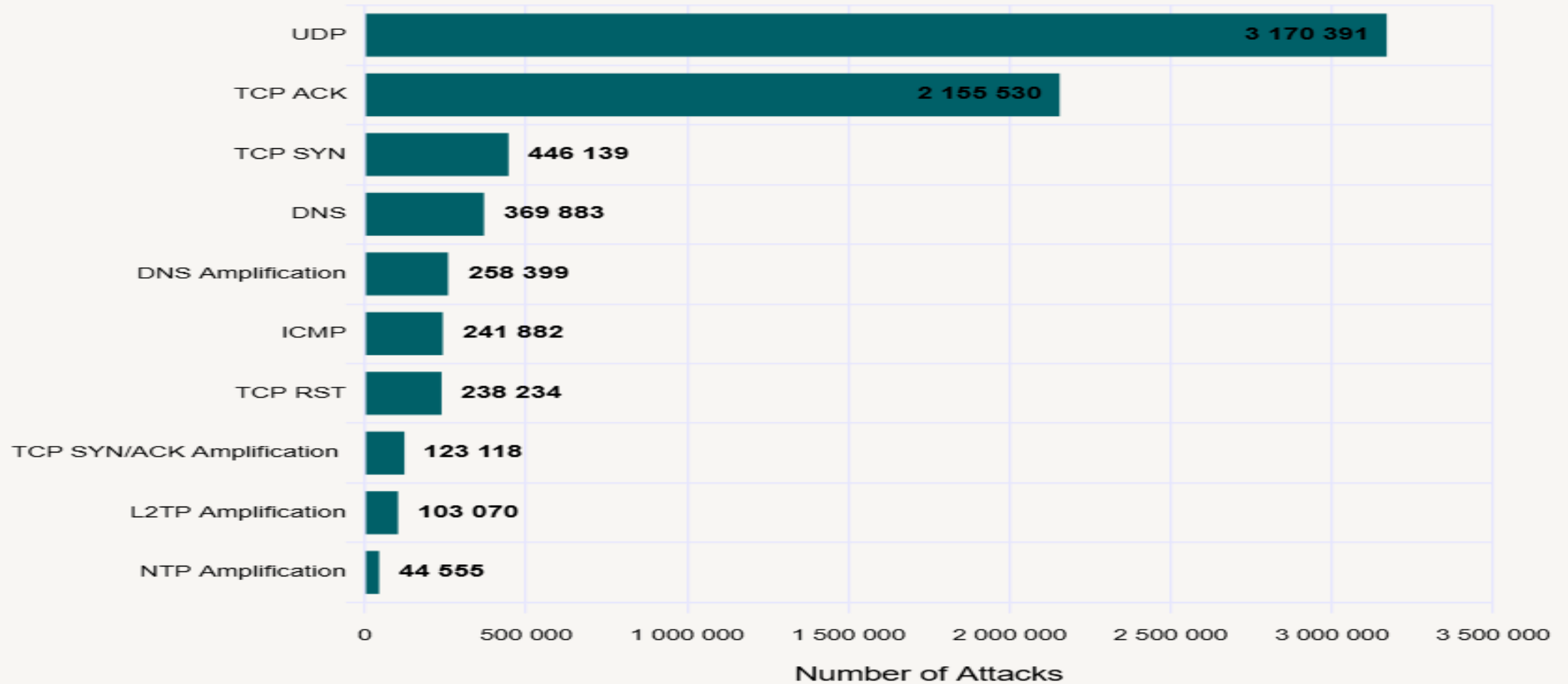
Typical DDoS-attack for majority vectors

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



NETSCOUT DDoS Threat Intelligence Report - Global

Top 10 Global DDoS Attack Vectors



NETSCOUT DDoS Threat Intelligence Report – Viet Nam

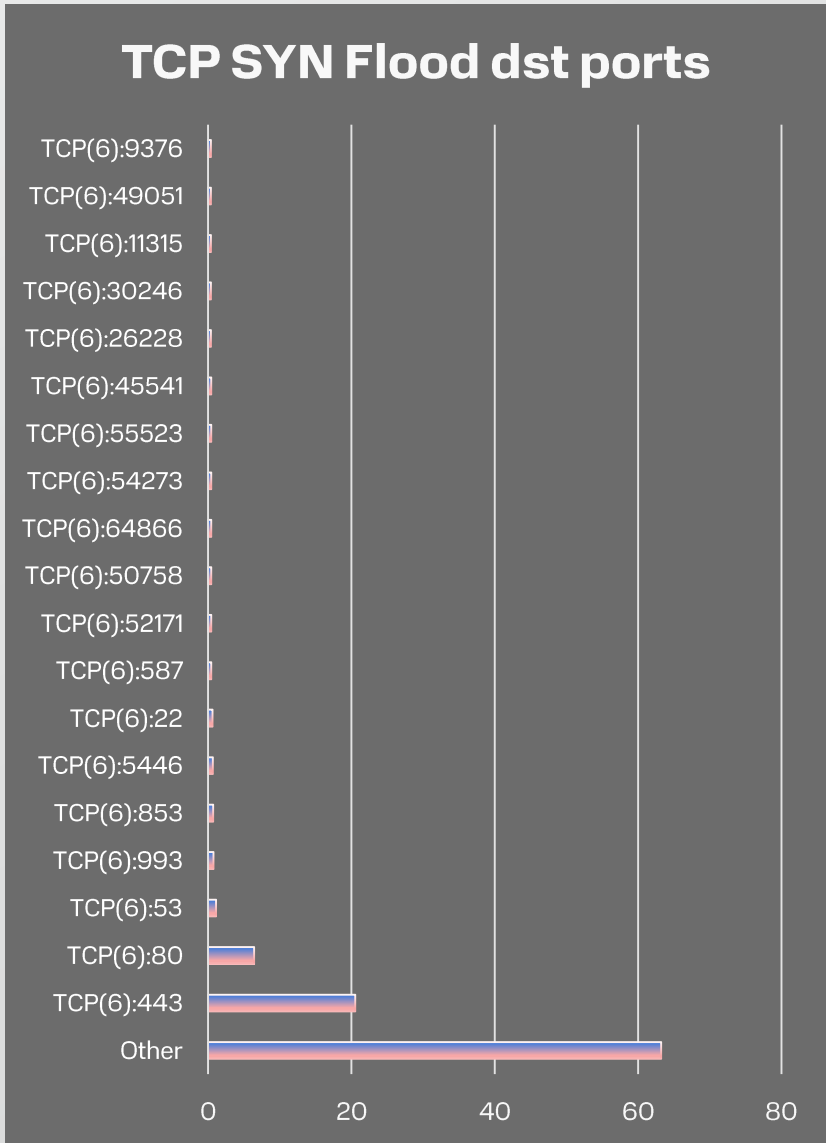
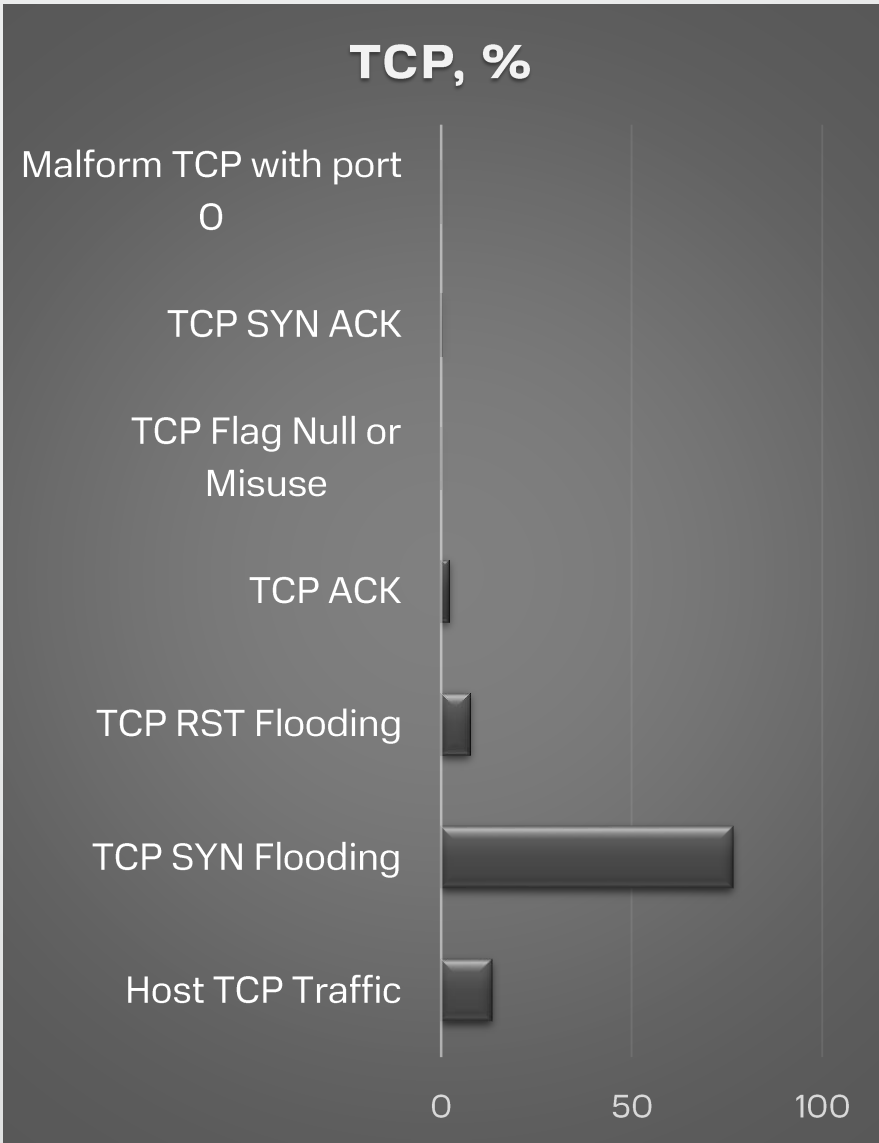
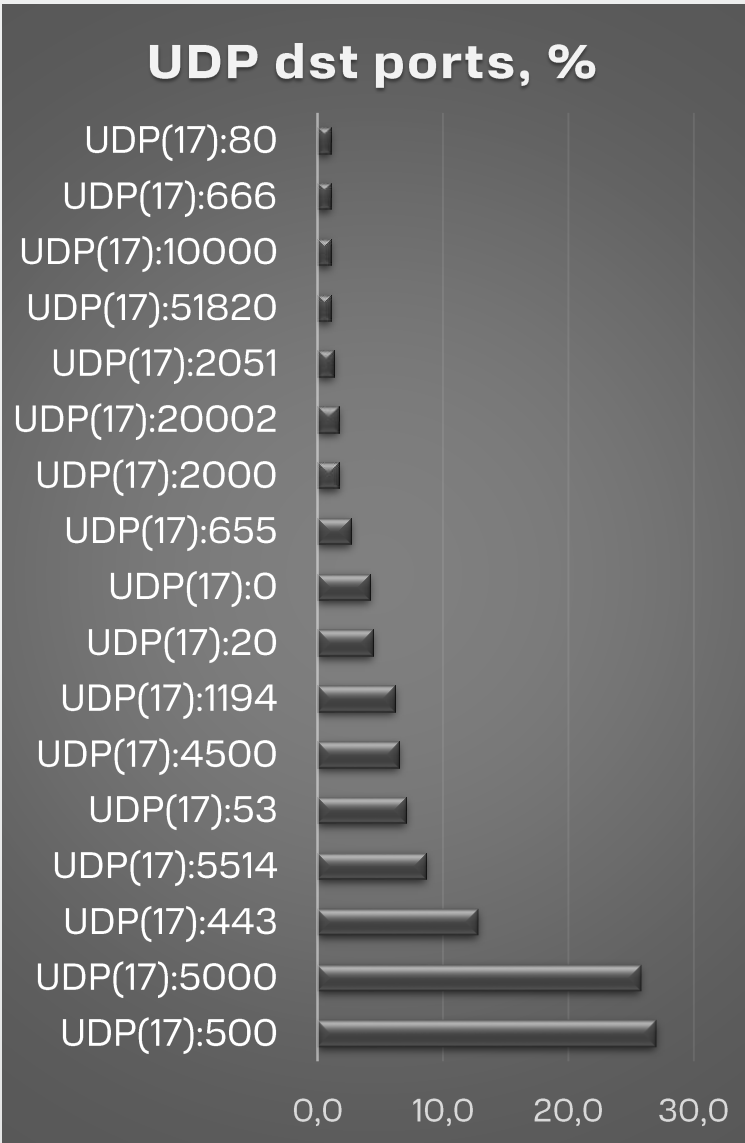
Attack Vectors Used

- | | | |
|----------------------------|--------------------------|---------------------------|
| 1. CLDAP Amplification | 9. NetBIOS Amplification | Amplification |
| 2. COAP Amplification | 10. RIPv1 Amplification | 17. UDP |
| 3. DNS | 11. SNMP Amplification | 18. WS-DD Amplification |
| 4. DNS Amplification | 12. SSDP Amplification | 19. chargen Amplification |
| 5. ICMP | 13. TCP ACK | 20. mDNS Amplification |
| 6. L2TP Amplification | 14. TCP RST | 21. memcached |
| 7. MS SQL RS Amplification | 15. TCP SYN | Amplification |
| 8. NTP Amplification | 16. TCP SYN/ACK | 22. rpcbind Amplification |

TOP ATTACK VECTORS



RED Security Attack Vectors Stats (Russia)

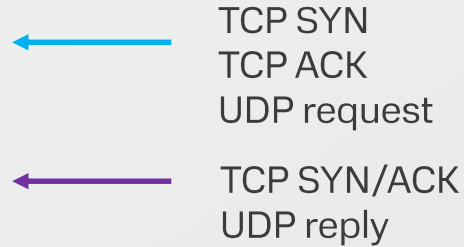


DDoS protection at ISP level: how does it work

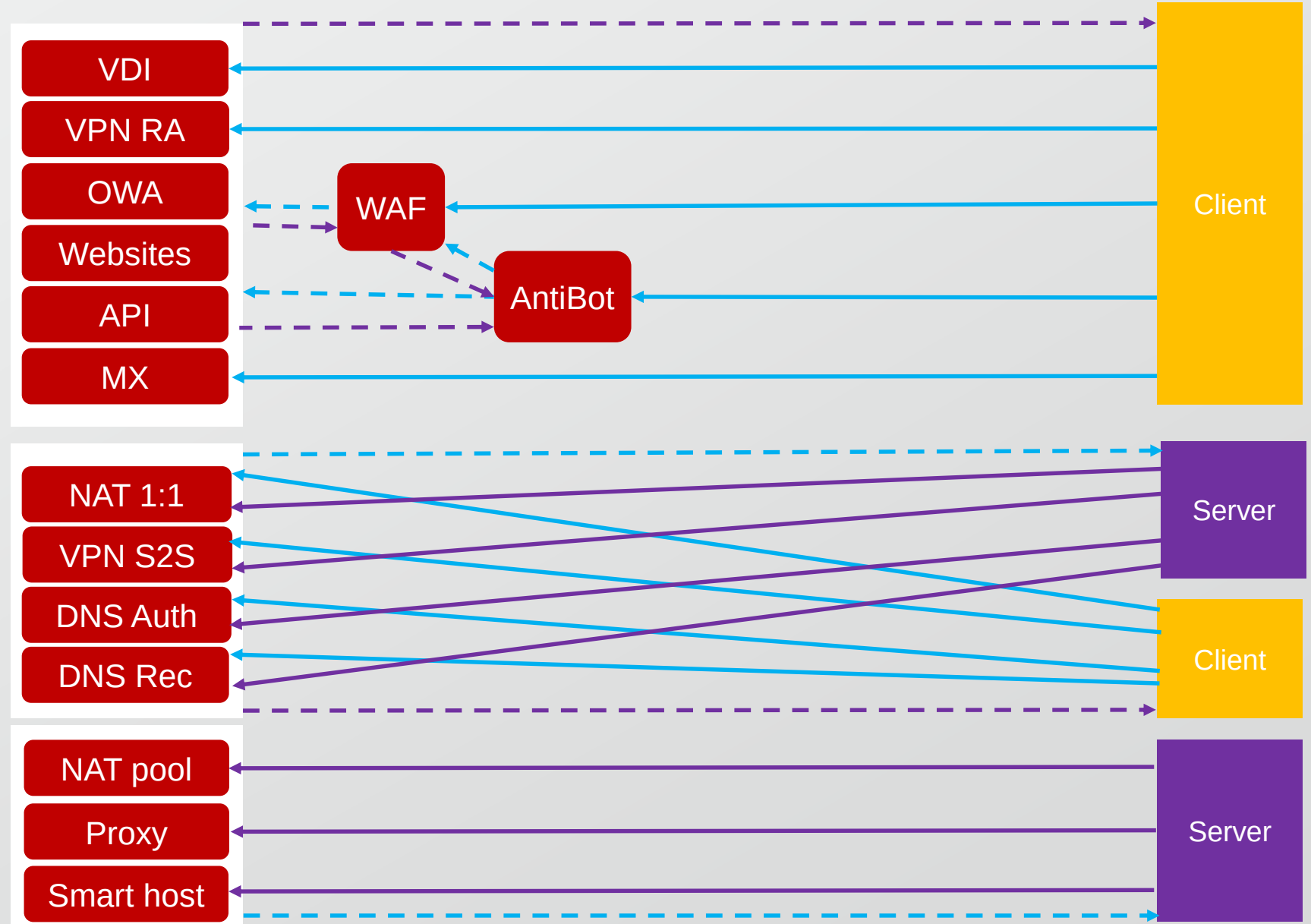
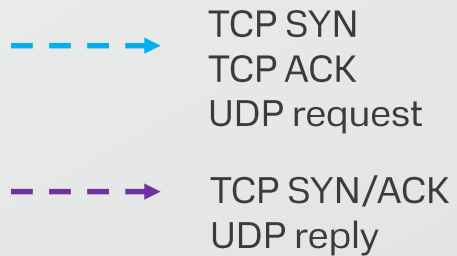
RED SECURITY

Asymmetric traffic!

Processed by scrubbing center



NOT processed by scrubbing center

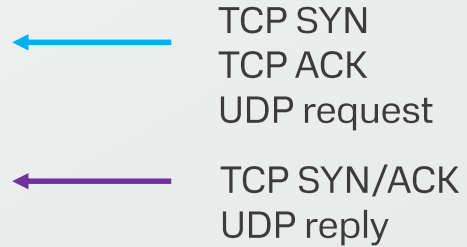


DDoS protection at ISP level: how does it work

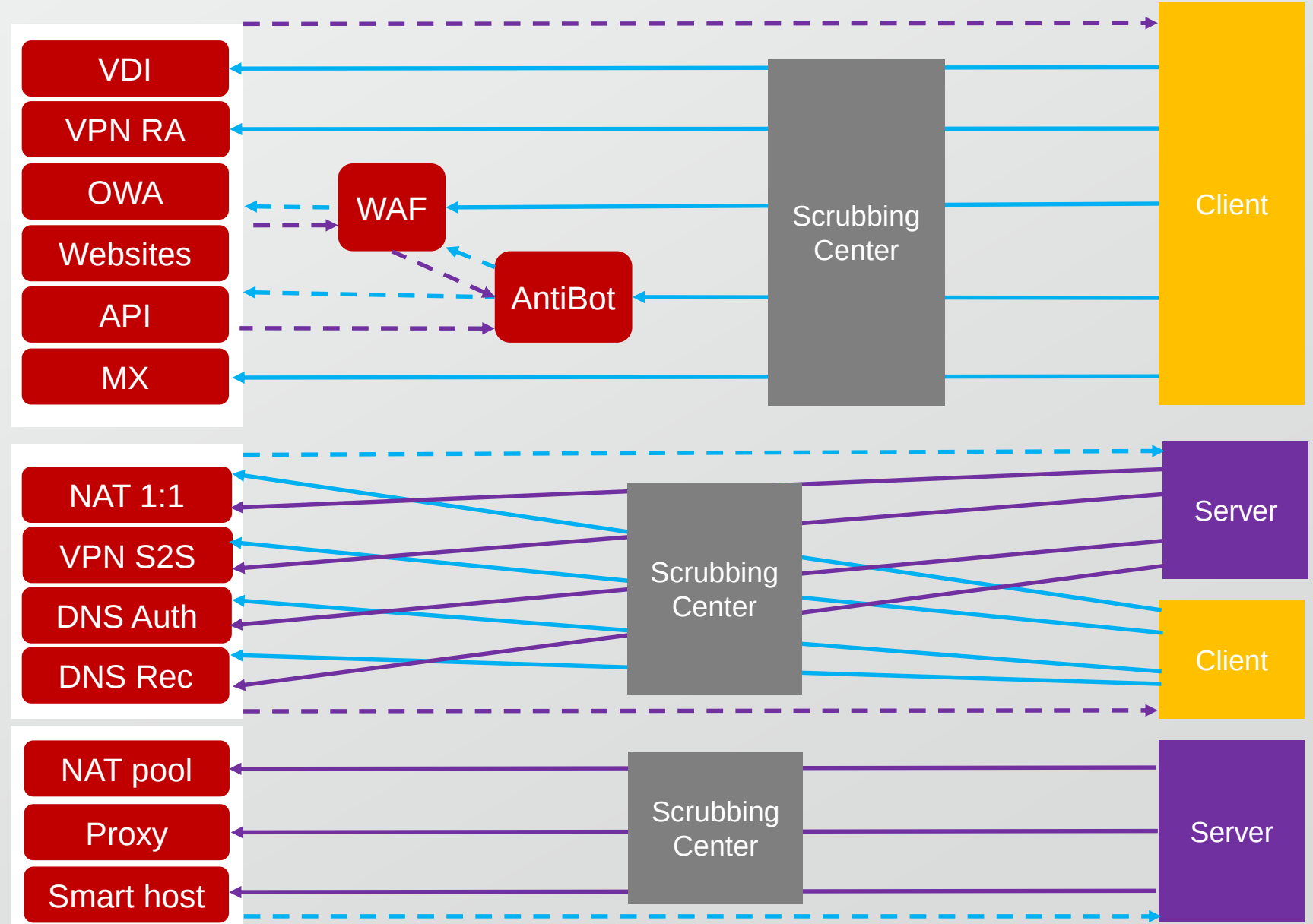
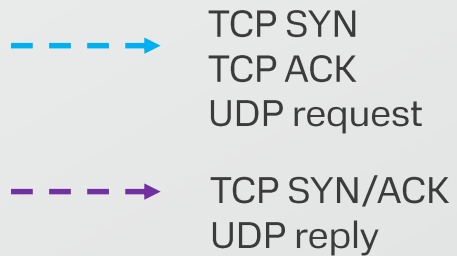
RED SECURITY

Asymmetric traffic!

Processed by scrubbing center

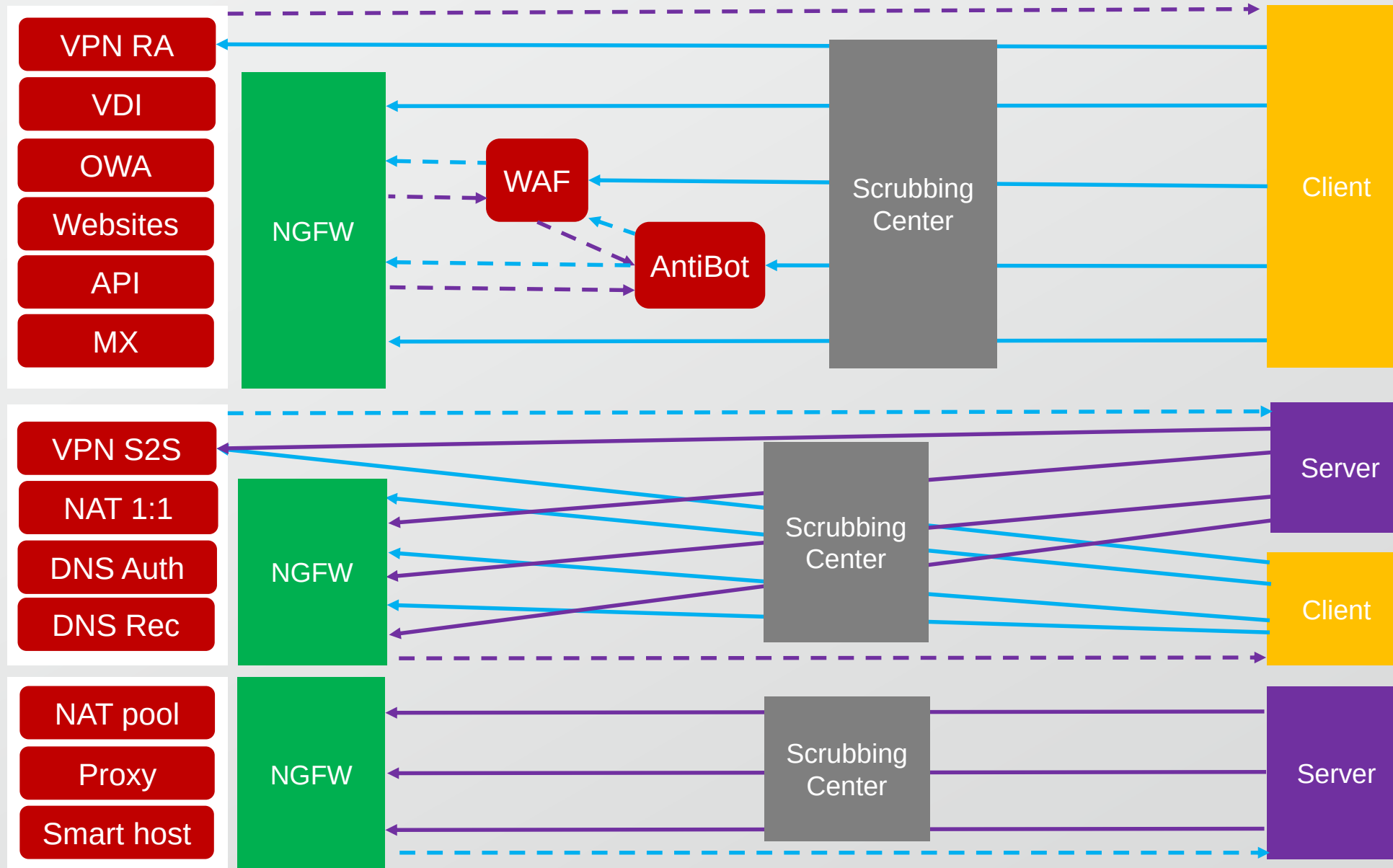


NOT processed by scrubbing center



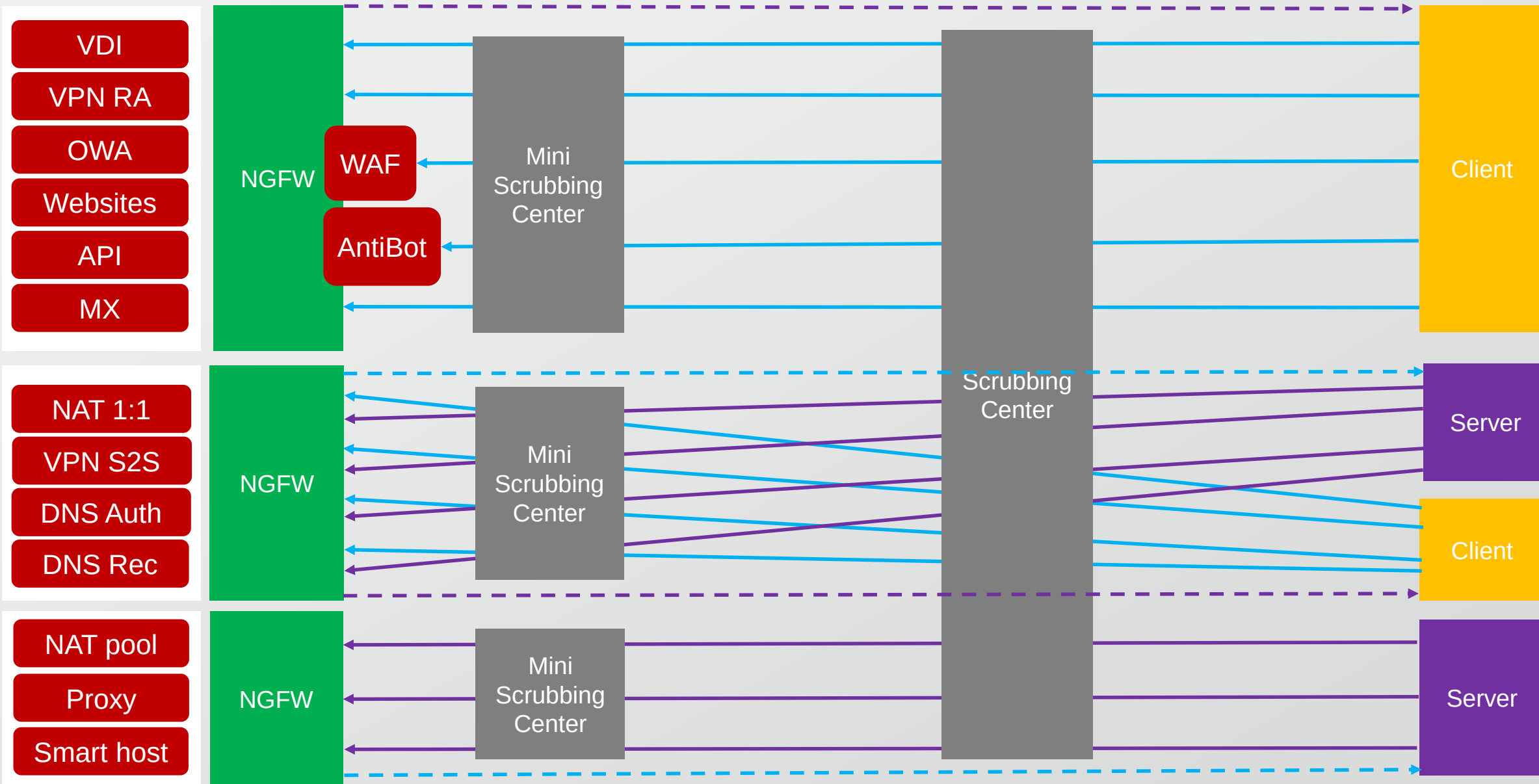
NGFW as a single point of failure during DDoS

RED SECURITY

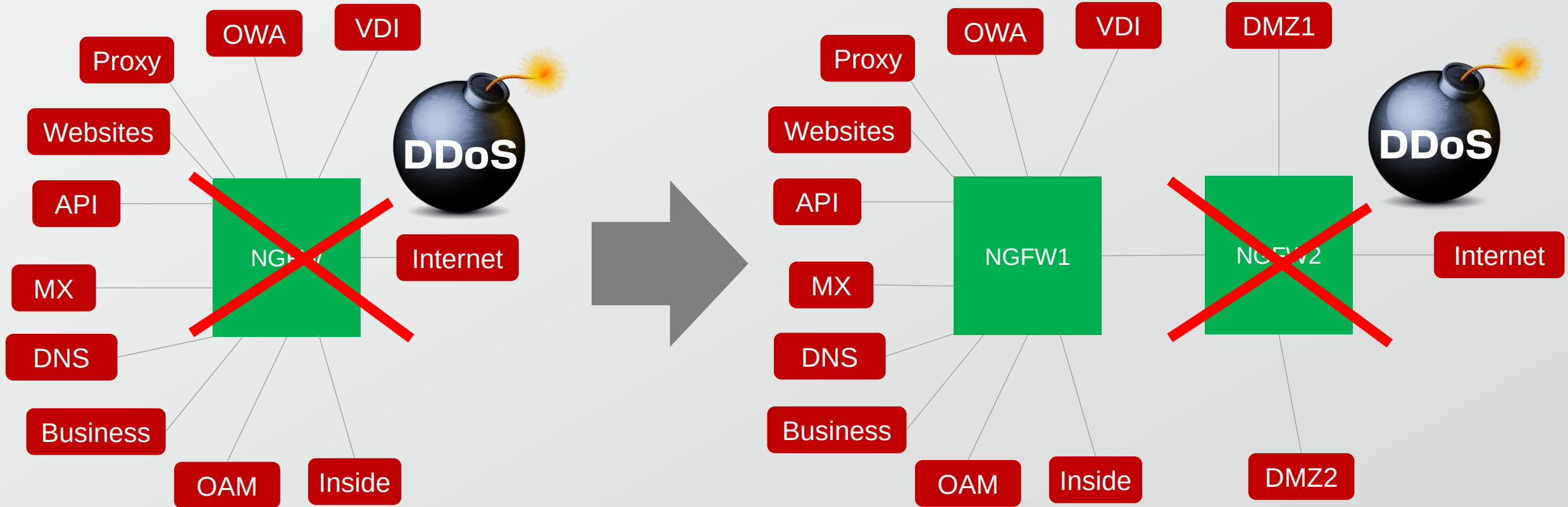


Protect NGFW from DDoS

RED SECURITY



Minimize failure risk for NGFW by network architecture

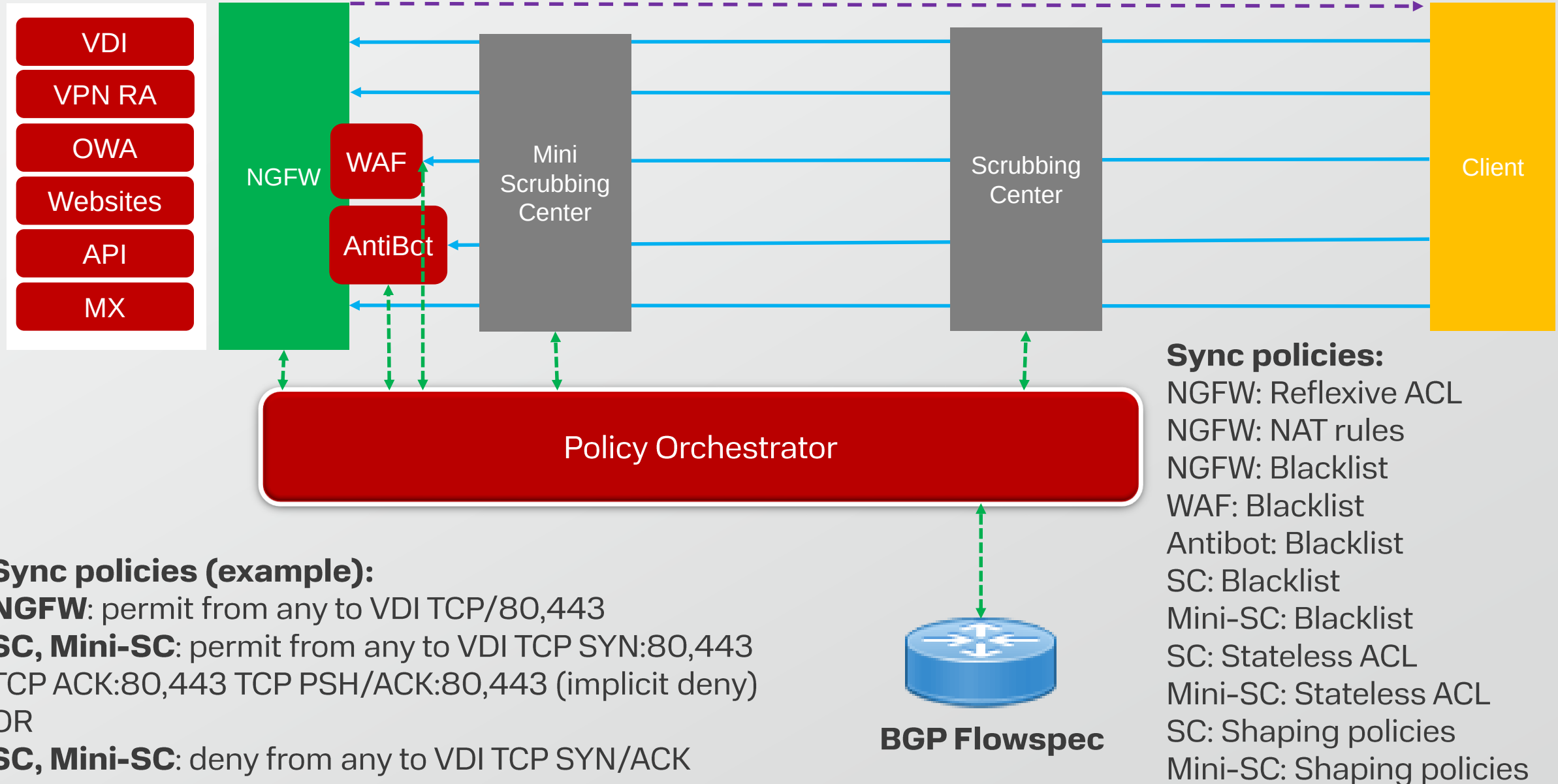


Network segments can't interact if **NGFW** falls in case of DDoS

Even if **NGFW2** dies internal segments interact OK

100% SYN/ACK Flood Elimination

RED SECURITY



100% SYN Flood Elimination

Sync policies (example):

NGFW: permit from Proxy to any TCP/80,443

SC, Mini-SC: permit from any to Proxy TCP SYN/ACK src port 80,443 (implicit deny)

OR

SC, Mini-SC: deny from any to Proxy TCP SYN

Sync policies:

NGFW: Reflexive ACL

NGFW: NAT rules

NGFW: Blacklist

SC: Blacklist

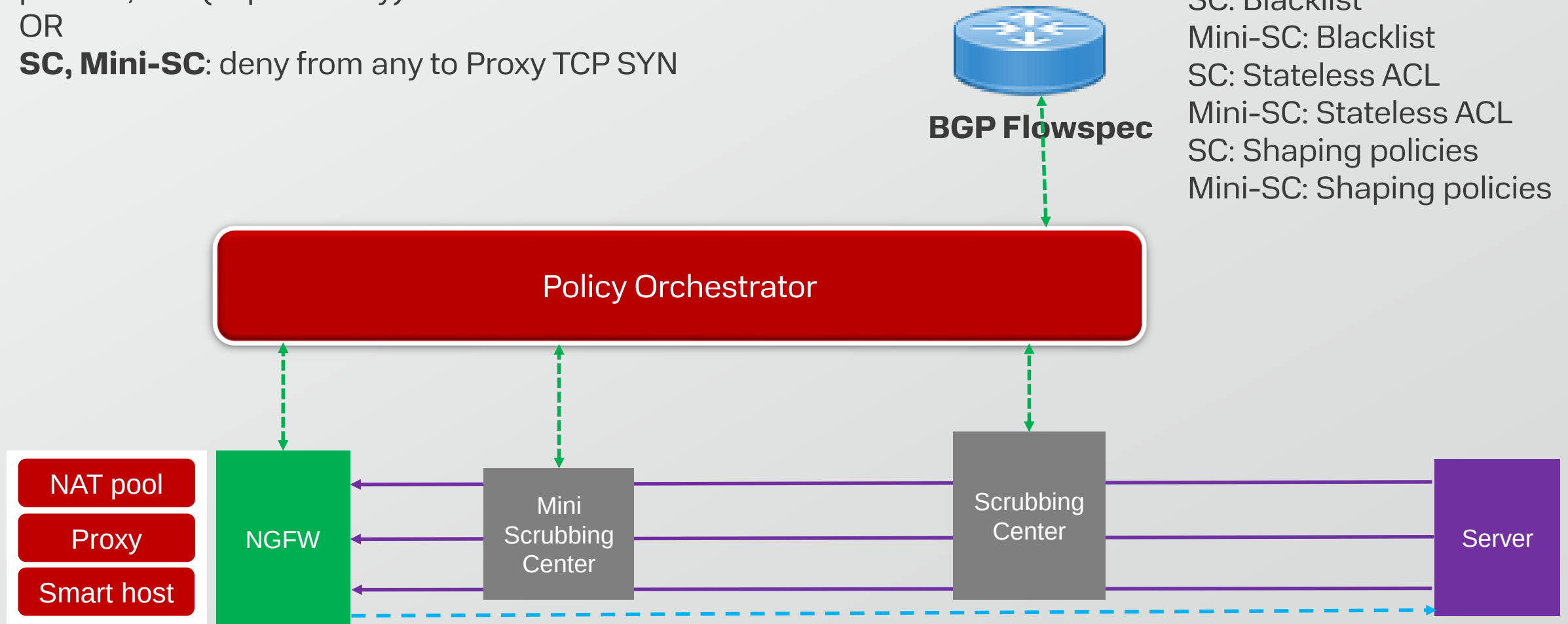
Mini-SC: Blacklist

SC: Stateless ACL

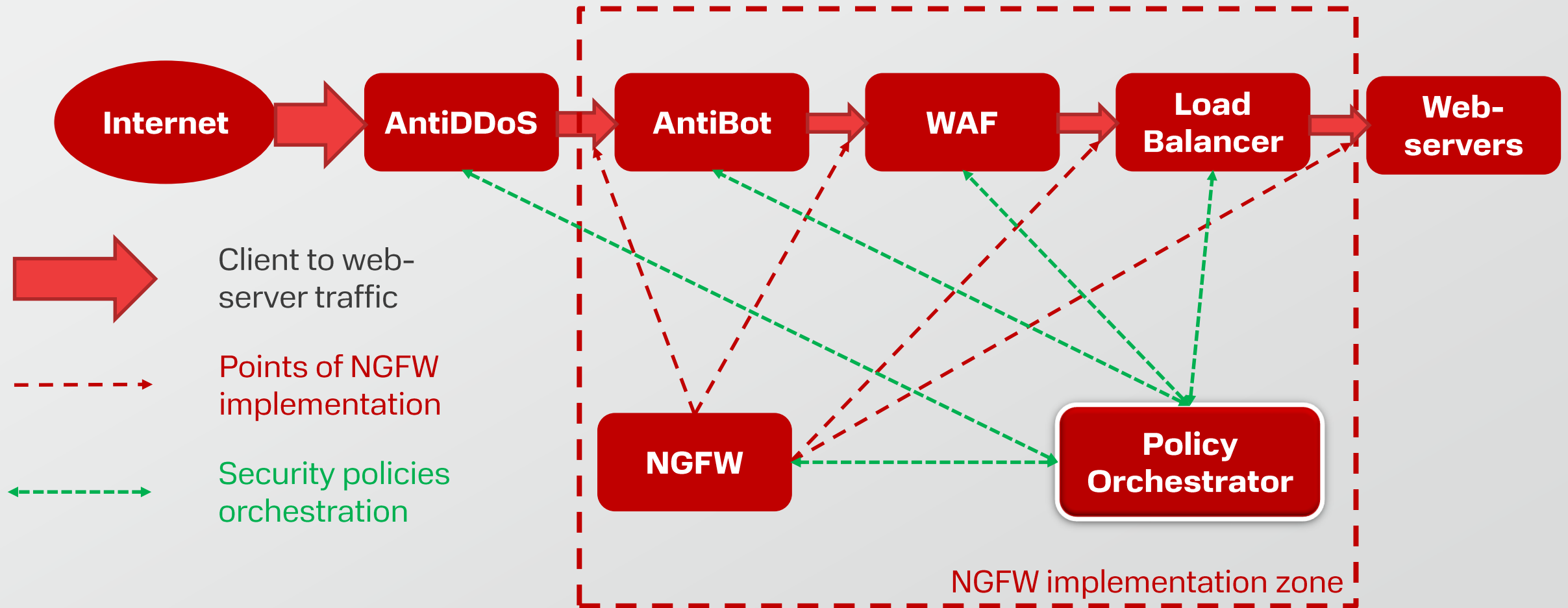
Mini-SC: Stateless ACL

SC: Shaping policies

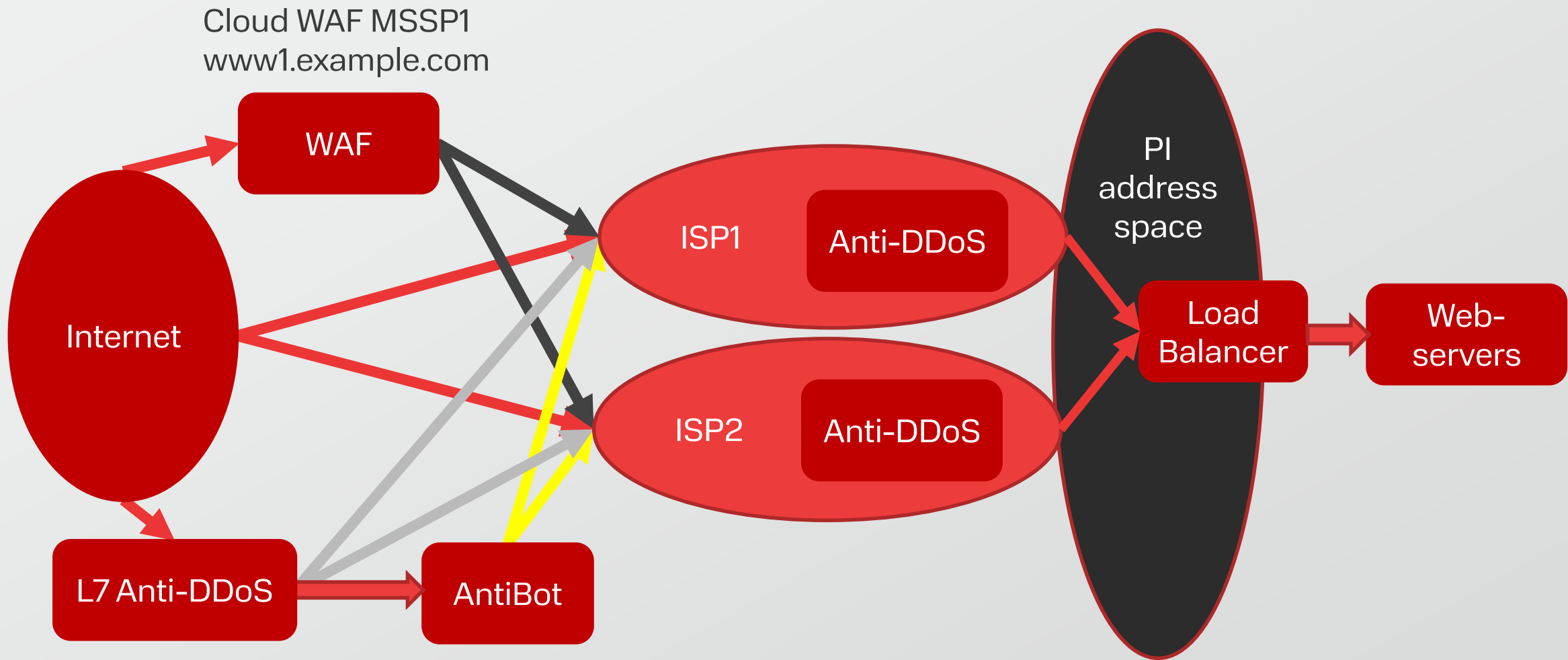
Mini-SC: Shaping policies



Protect web-sites from DDoS by cloud MSSP



Protect web-sites from DDoS by 2 different cloud MSSP



Cloud L7 AntiDDoS+AntiBot MSSP2
www2.example.com

- Separate external network segments by traffic direction
 - Email: MX and Smart host
 - VPN-servers: VPN S2S и VPN RA
 - DMZ-servers and corporate/provider exit nodes to the Internet (NAT pool, proxy)
 - DNS: authoritative and recursive
- DMZ-servers (NAT 1:1) must initiate connection to the Internet via proxy (e.g. for updates)
- Synchronize ACL on NGFW and scrubbing center
- Use different NGFW instances/nodes for internal segmentation and Internet-facing ones
- Use local scrubbing center in your datacenter and integrate it with ISP SC by cloud signaling
- If you use several ISPs buy Anti-DDoS service with each provider or be ready to switch traffic during attack to the protected one
- WAF/Antibot cloud services must be protected with Anti-DDoS