Ochrona Anty DDoS

Warianty dostępne w OPL RH

Nasze usługi
Twój sukces

orange™

DDoS - co to jest i jak się chronić ?

- **DDoS (Distributed Denial of Service)**
  atak na system komputerowy lub usługę sieciową mający na celu zablokowanie działania usługi poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów (np. zombie).

- **Rodzaje ataków:**
  - na pasmo potrzebne do świadczenia usługi;
  - na wyczerpanie zasobów systemu świadczącego usługę;
  - na konkretną aplikację;
  - na konkretnego użytkownika (IP) w sieci operatora.

- **Standardowa reakcją na anomalię**
  uruchomienie filtrowania gdzie ruch atakowanego hosta zostaje przekierowany do scrubberów w celu mitygacji ataku DDoS. Odfiltrowany ruch jest odsyłany do klienta jego podstawowym łączem.

Zabezpieczenie przed DDoS tranzytu do światowego Internetu, na poziomie łącza ISP

Proste metody zabezpieczania tranzytu:

Black-holing

Blackholing – atak odnosi skutek na atakowany IP ale nie wysyca łącza.
Ograniczenie - możliwość blokowania pojedynczych IP bez możliwości blokowania IP z tranzytowanych ASN.

x10

Zamówienie nadmiarowego pasma tranzytu do Internetu.
W OPL oferujemy otwarty port, rozliczanie usługi 95 percentylem)
1/10 (commitment/burst).

Podział ruchu na VLAN

Ograniczanie zasięgu oddziaływania ataku przez podział ruchu na dedykowane VLAN - rozdzielanie frakcji ruchu na tranzyt, open peering i content CDN.
Usługi dostępne w OPL.

DDoS Protection static – reguły konfigurowane na porcie Operatora

- Stałe wycinanie i policerowanie ruchu do konkretnych portów TCP/UDP powyżej określonego poziomu.
- Mitygacja ataku DDoS warstw 3-4.
- Filtracja ruchu podczas ataku DDoS o bardzo wysokim wolumenie nawet 1,5 Tb/s.

Parametry mitygacji:

- ✓ **chargen**
- ✓ **CLDAP**
- ✓ **DNS**
- ✓ **IP Fragmentation**
- ✓ **L2TP (500-65535)**
- ✓ **mDNS**
- ✓ **memcached**
- ✓ **MS SQL RS**
- ✓ **NetBIOS**
- ✓ **NTP**
- ✓ **RIPv1**
- ✓ **rpcbind**
- ✓ **SNMP**
- ✓ **SSDP**

Akcje firewall:

- ✓ Rate limit o wartości 0,10,50,100,150,200,250,300,350,400,450,500 Mbps
- ✓ dla serwisu IP Fragmentation – limit pasma: 200/400/600/800/1000/1200/1400/1600/1800/2000 Mbps

Przykład:

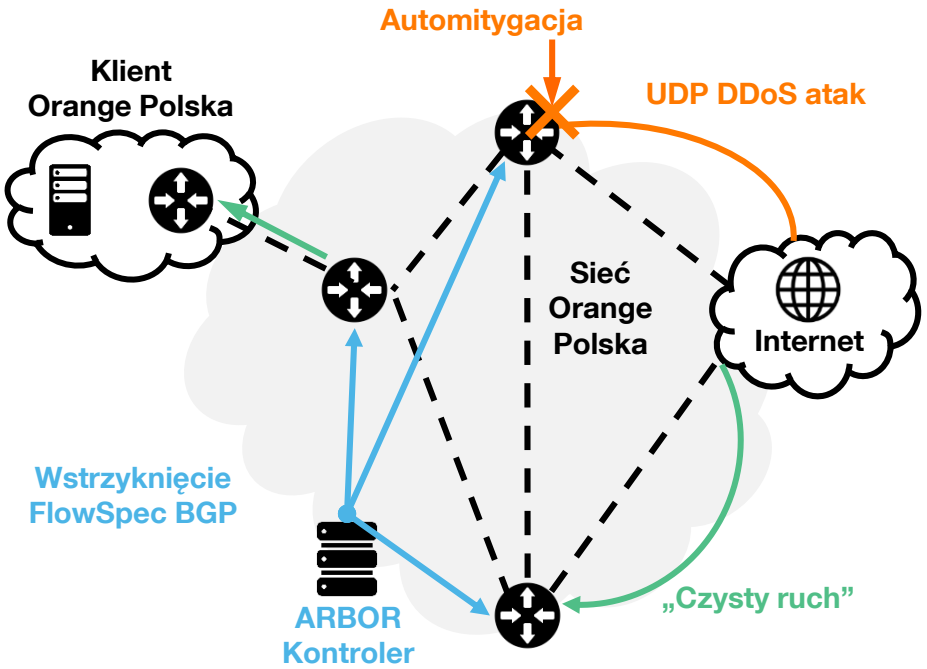
TCP port 0 - 250Mbps
TCP port 53 - 100Mbps
TCP port 123 - 50Mbps
TCP port 389 - 150Mbps
Fragmentowany ruch TCP&UDP - 1Gbps

DDoS Protection Basic – wykrywanie i mitygacja ataku przez ARBOR

- **Automatyczna reakcja systemu tylko podczas ataku, mitygacja popularnych zagrożeń wolumetrycznych i amplifikacyjnych**
- **Automitygacja Flow Spec (FS)**

  usługa automatycznie łagodząca negatywne skutki ataków DDoS
- **Działanie oparte na dwóch elementach:**

BGP FS kontroler – Arbor Sightline odpowiada za wykrycie ataku i wstrzyknięcie „reguły” FlowSpec do routera w sieci OPL	**Routery sieci OPL wykorzystują wbudowany firewall do mitygacji ataku**



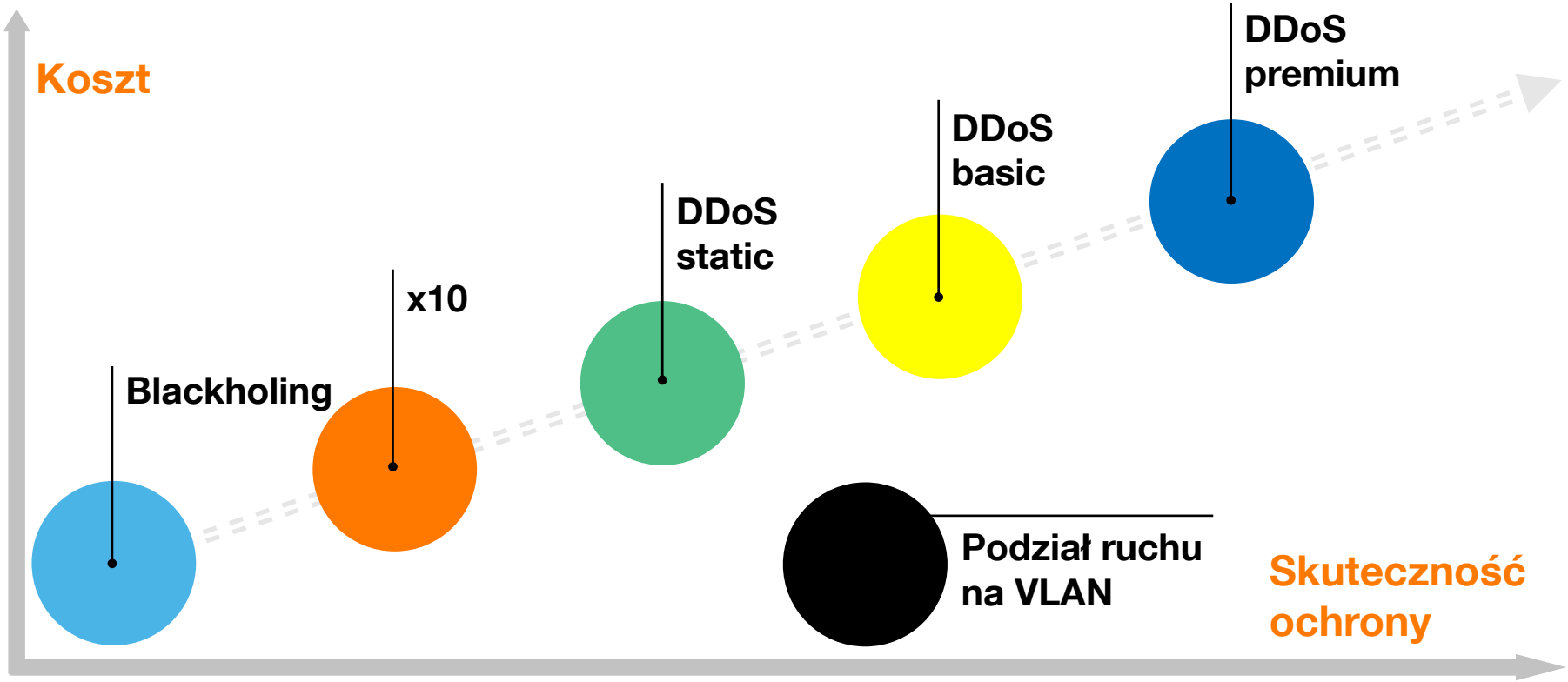
DDoS Protection premium - przejmowanie ruchu i jego czyszczenie

Monitorowanie ruchu sieciowego w sposób ciągły (24/7/365)

- **Analizy wzorca ruchu przychodzącego do Klienta**
- **Powiadomienia o zaobserwowanych anomaliach ruchu i możliwych incydentach bezpieczeństwa**
- **Reakcja na atak DDoS na infrastrukturę Klienta:**
  - filtrowanie ruchu podczas ataku DDoS (do 10 Gbps), filtrowanie ruchu internetowego na styku z zagranicą, blokowanie wybranych adresów IP
  - przejmowanie ruchu na TMS w celu jego odfiltrowania z nietypowych ataków
  - podejmowanie na bieżąco działań w zależności od zmieniającego się wektora ataku
  - aktywowanie ochrony do 15 min. od potwierdzenia ataku przez Klienta
  - dostarczenie do Klienta tylko prawidłowego ruchu sieciowego
  - pisemny raport dla Klienta po ataku DDoS

CERT Orange Polska

Rozwiązania ochrony przed DDoS
skuteczność – koszt



Zapraszamy do kontaktu z Doradcą

www.hurt-orange.pl

Nasze usługi
Twój sukces