WANGUARD I JUNIPER MX JAKO KOMPLETNA OCHRONA PRZED ATAKAMI DDOS

ITORO dostarcza to jako gotowy do wdrożenia, w pełni zarządzany pakiet. Oprogramowanie, licencje, konfiguracja i stałe wsparcie.

MX204 – router brzegowy 4x100GE

Koszt: ok. $10,000 – $20,000

WAN GUARD

Koszt: ok. $3000

Ciągłe filtrowanie z prędkością łącza (line-rate)

Juniper MX204 blokuje ruch ataku z prędkością 400 Gbps - 24/7, bez opóźnień, bez ręcznej interwencji

Automatyczna dynamiczna mitygacja

WanGuard monitoruje cały ruch przez port mirror lub sFlow/IPFIX i identyfikuje wzorce ataków w czasie rzeczywistym

Inteligentna detekcja ruchu

WanGuard uruchamia BGP FlowSpec lub RTBH — Juniper natychmiast wykonuje reguły z prędkością łącza (line rate)

JAK TO DZIAŁA — JUNIPER MX + WANGUARD DWA PRODUKTY. JEDNO ROZWIĄZANIE. DOSTARCZANE PRZEZ ITORO.

Juniper MX

Statyczna, zawsze aktywna brama

Działa jako stały silnik scrubbingu z prędkością łącza (line-rate) — filtruje znany ruch ataku, zanim dotrze do Twojej sieci.

- Filtrowanie line-rate 400 Gbps — sprzęt ASIC, zero obciążenia CPU
- Blokuje przychodzące DDoS na łączach uplink + ruch zainfekowanych hostów w LAN
- NTP, DNS, ICMP, amplifikacja UDP/TCP, ruch ze sfałszowanym źródłem (spoofed)
- Zawsze aktywne filtry — wizualizacja w autorskim portalu

WanGuard

Silnik dynamicznej detekcji i reakcji

Wykrywa to, co pomijają filtry statyczne, klasyfikuje atak i automatycznie instruuje Juniper, by zablokował go za pomocą BGP FlowSpec.

- Detekcja ataku poniżej sekundy dzięki silnikowi przyspieszanemu DPDK
- Zbiera ruch przez port mirror lub sFlow/IPFIX
- Wykrywa DNS/NTP floods, Carpet Bomb, anomalie wolumetryczne
- Wysyła reguły BGP FlowSpec do Juniper lub wyzwala RTBH w upstream

ITORO pakietuje oba jako jednorazową inwestycję — będącą Twoją własnością, pod Twoją kontrolą i zarządzaniem.
Razem tworzą kompletną, samobroniącą się sieć — bez potrzeby zewnętrznego centrum scrubbingu.

JUNIPER MX — ZAWSZE AKTYWNA OCHRONA PRZED DDOS

Bezstanowy firewall line-rate — aktywny, zanim jakikolwiek atak dotrze do Twojej sieci

Filtr wejściowy
Ochrona DDoS na wejściu sieci
Blokuje ruch ataków sfałszowanych (spoofed), zniekształconych i amplifikacyjnych

lo0 – Routing Engine CoPP
Control Plane Policing i firewall
Chroni dostęp do BGP, OSPF, SSH, SNMP — router pozostaje online

Filtr wyjściowy
Wychodząca LAN / klient ochrona
Zapobiega wykorzystaniu Twojej sieci jako źródła ataku

Warstwa 1

Tranzytowa ochrona DDoS (interfejsy WAN i LAN)

- Blokuje sfałszowane adresy źródłowe
- Eliminuje zniekształcone pakiety
- Blokuje 17+ kategorii protokołów amplifikacji UDP na wejściu
- Blokuje 15+ kategorii portów źródłowych amplifikacji na wyjściu
- Ogranicza przepustowość (rate-limit) SYN floods, ICMP, DNS, NTP
- ✓ Pełne pokrycie IPv4 i IPv6

Warstwa 2

Ochrona Routing Engine (lo0 CoPP)

- Architektura default-deny
- ✓ Sesje BGP, OSPF, BFD dozwolone tylko od skonfigurowanych peerów
- Dostęp zarządzania (SSH, SNMP, RADIUS, NTP, DNS)
- Cały nierozpoznany ruch jest domyślnie odrzucany

PAKIET FILTRÓW JUNIPER MX — GŁĘBIA I ZŁOŻONOŚĆ

Dostarczany przez ITORO jako gotowa do wdrożenia konfiguracja

SKALA FILTRÓW

Filtry tranzytowe — kategorie twardo blokowane:

- Ograniczane przepustowo (policed, nie odrzucane):
- SYN floods · IP fragments · ICMP · DNS · NTP

Routing Engine CoPP:

- Default-deny — domyślnie nie dozwolony ruch jest odrzucany
- Tysiące potencjalnych wektorów ataku wyeliminowanych samą architekturą

WIDOCZNOŚĆ I ANTI-SPOOFING

Każdy człon filtra ma nazwany licznik:

- Widoczność w czasie rzeczywistym przez Grafana i Juniper Telemetry
- Liczniki mają ustrukturyzowane nazewnictwo — protokół, kierunek, typ ataku
- Monitoring na żywo dostępny również z JunOS CLI w dowolnym momencie

Anti-Spoofing — RPF na wszystkich interfejsach:

- Weryfikuje źródłowe adresy IP przed jakimkolwiek przetwarzaniem filtra
- Tryb feasible-path — obsługuje routing asymetryczny w środowiskach multi-homed
- Dedykowany licznik błędów — naruszenia RPF logowane oddzielnie od liczników DDoS

Kierunek	Zniekształcone	Protokoły amplifikacji
IPv4 / IPv6 Przychodzący	10 / 9 kategorii	17 kategorii protokołów UDP
IPv4 / IPv6 Wychodzący	3 / 3 kategorie	15 kategorii portów źródłowych

Plik	Zawartość	Rozmiar
Filtry tranzytowe DDoS	4 filtry · INPUT/OUTPUT · IPv4 + IPv6 · uRPF · policery	~2 750 linii
Routing Engine CoPP	2 filtry · lo0 · IPv4 + IPv6 · dynamiczne rozwiązywanie peerów	~1 600 linii

TELEMETRIA BRZEGOWA JUNIPER MX