itoro

USŁUGI ANTY-DDOS BEZPIECZEŃSTWO SIECI

Andrisoft Network Security
GOLD PARTNER

WAN GUARD

Oprogramowanie Anty-DDoS firmy Andrisoft.com

- Remotely Triggered Black Hole (RTBH)
- Filtrowanie ruchu za pomocą BGP FlowSpec
- Przekierowanie ruchu do centrum scrubbingu DDoS

Juniper MX

Router brzegowy z warstwą filtrowania DDoS

- Brama filtrująca DDoS
- Ochrona ruchu przychodzącego i wychodzącego
- Ochrona Routing Engine i filtry DDoS

Piotr Okupski
CEO ITORO
itoro.com.pl

O FIRMIE ITORO

WanGuard – oprogramowanie anty-DDoS

- Globalny, dedykowany specjalista ds. integracji WanGuard
- 95%+ wszystkich wdrożeń wykorzystuje port mirror dla najszybszej detekcji
- 100% wdrożeń DPDK (10-400GE) wykorzystuje port mirror

Andrisoft GOLD PARTNER

Przygotowanie i konfiguracja serwerów oraz optymalizacja wydajności systemu Linux

- WanGuard to najlepszy stosunek ceny do możliwości w ochronie przed DDoS wolumetrycznym dla środowisk 10–400 GE na całym świecie
- Szkolenia z systemu WanGuard i transfer wiedzy

Pełne wsparcie przed i po wdrożeniu

- Eksperckie doradztwo w zakresie bezpieczeństwa DDoS oraz rekomendacje hardeningu sieci
- Stałe wsparcie systemu WanGuard — odciążające Twój zespół od dodatkowych obowiązków monitorowania

DOŚWIADCZENI PARTNERZY

ITORO

Integrator bezpieczeństwa sieci

Założona w 2017 — oparta na ponad 25 latach praktycznego doświadczenia w operacjach ISP i sieciowych, w tym ponad 20 lat z platformami Juniper.

Kompleksowa realizacja: projektowanie sieci, konfiguracja routerów i przełączników, wdrożenie oraz stałe wsparcie.

WanGuard to nasz flagowy produkt, wspierany przez rosnące portfolio rozwiązań bezpieczeństwa sieci.

WanGuard

Platforma DDoS od Andrisoft — nasze flagowe narzędzie

W ciągłym rozwoju od 2007 — blisko dwie dekady pracy w środowiskach produkcyjnych.

WanGuard cieszy się zaufaniem globalnych operatorów: Vodafone, Orange, DigitalOcean, Leaseweb, Equinix, Google Fiber.

Pełne pokrycie: BGP FlowSpec, RTBH, detekcja DPDK line-rate, sFlow, IPFIX, NetFlow.

WANGUARD – PLATFORMA OCHRONY PRZED DDOS KLASY OPERATORSKIEJ, Z PRECYZYJNYM FILTROWANIEM RUCHU PRZEZ BGP FLOWSPEC.

Ochrona przed atakami wolumetrycznymi:

Ataki wolumetryczne przekraczają przepustowość uplinku klienta — dlatego ochrona po stronie upstream jest niezbędna.
BGP FlowSpec to preferowana odpowiedź, umożliwiająca granularne filtrowanie ruchu na poziomie ISP lub dostawcy tranzytu.
RTBH stosuje się w ostateczności, gdy wolumen ataku całkowicie wysyca uplink, a sam FlowSpec jest niewystarczający.

Rodzaje ataków DDoS blokowanych przez WanGuard:

Sieciowe i amplifikacyjne

FRAGMENT, SMURF, SNMP
SSDP, MEMCACHED, CHARGEN
SYN-ACK / SYN / ICMP

Aplikacyjne i Protokołowe

SIP, NETBIOS, LDAP/CLDAP
QUIC, INVALID PACKETS
SYN-ACK / SYN / ICMP

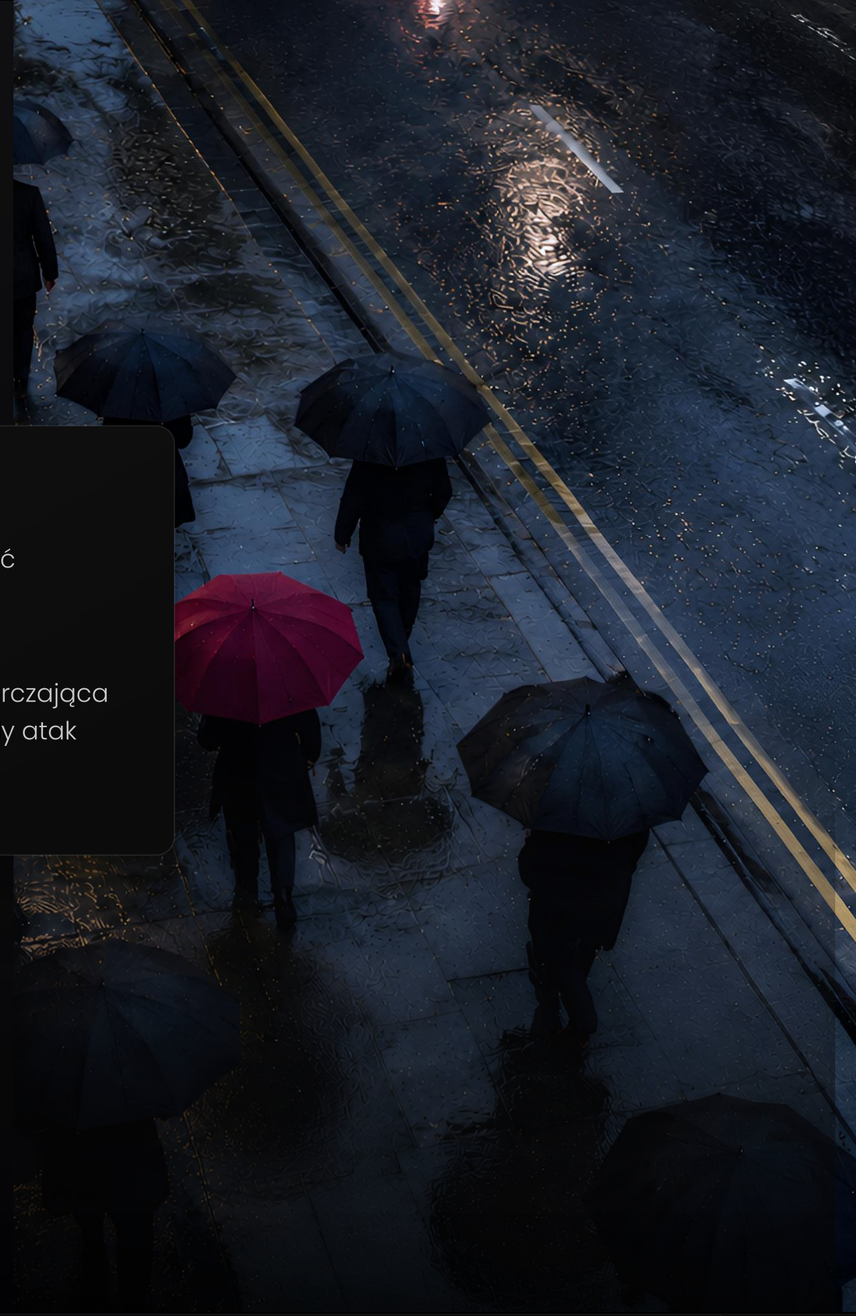
Flood i Wolumetryczne

UDP/TCP Floods
DNS/NTP Flood
TCP:NULL, RST, ACK, SYN-ACK, XMAS
Carpet Bomb — filtrowanie ruchu

Jak WanGuard chroni sieci?

WanGuard automatycznie generuje i wdraża reguły filtrujące BGP FlowSpec w czasie rzeczywistym. Gdy wolumen ataku przekracza możliwości filtrowania, do dostawców upstream wysyłane są rozgłoszenia RTBH — odrzucające złośliwy ruch, zanim dotrze do Twojej sieci.

WANGUARD
- SYSTEM OCHRONY PRZED DDOS



Wolumetryczne ataki DDoS – specjalizacja WanGuard

To ataki polegające na wykorzystaniu wielu botów lub serwerów do wygenerowania ogromnego ruchu i wolumenu pakietów w celu zablokowania usługi lub całej sieci.

Ochrona przed tego typu atakami:

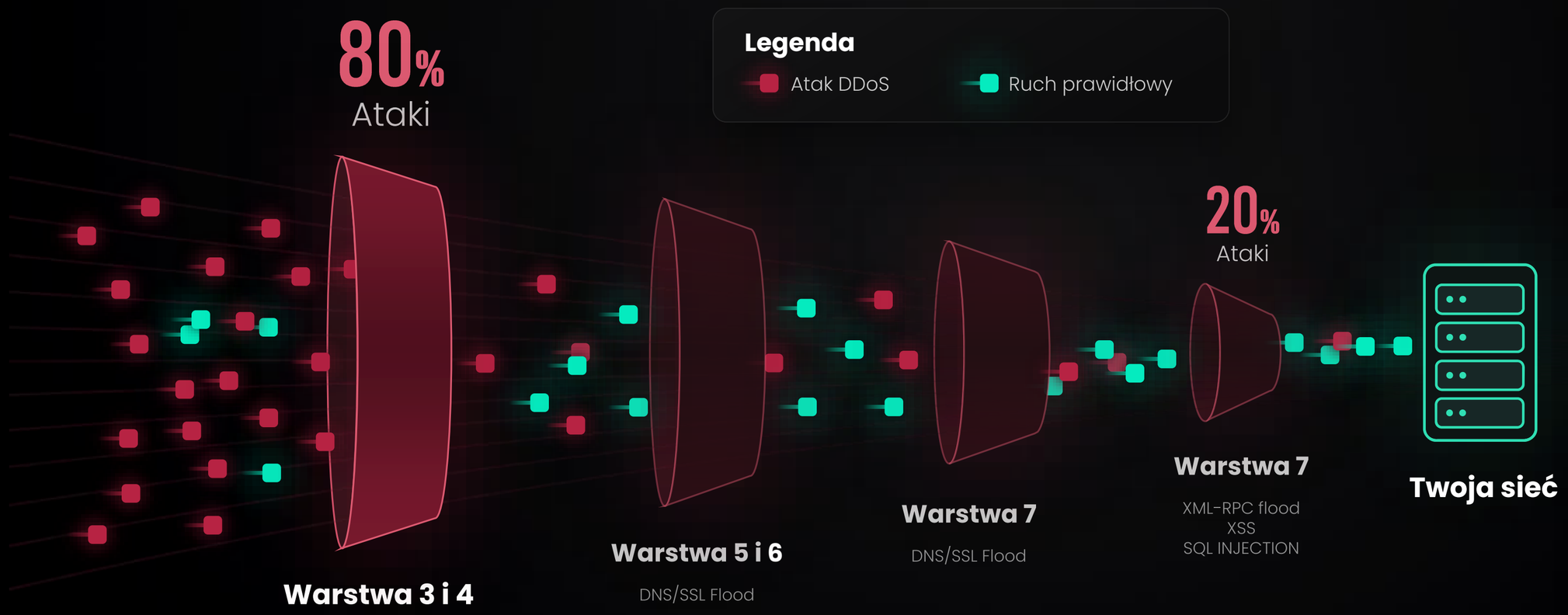
Tylko operator upstream lub dostawca tranzytu może zaabsorbować wolumetryczne ataki na dużą skalę — dysponuje znacznie większą przepustowością niż klient końcowy.

Pierwszą linią obrony jest filtrowanie ruchu (jeśli dostępna jest wystarczająca przepustowość); blackholing RTBH stanowi rozwiązanie awaryjne, gdy atak przekracza dostępną pojemność.

Inne ataki DDoS obsługiwane przez WanGuard:

- SYN-ACK / SYN / ICMP
- FRAGMENT
- SMURF
- SNMP
- SSDP
- MEMCACHED
- QUIC
- INVALID PACKETS
- NETBIOS
- SIP
- LDAP/CLDAP
- CHARGEN
- UDP/ TCP Floods
- TCP: NULL, RST,ACK
- SYN-ACK,TCP-ALL(XMAS)
- DNS/NTP Flood

WANGUARD — OPCJE DETEKCJI



Ataki amplifikacyjne:

- ARMS
- Chargen
- CLDAP
- COAP
- MS SQL RS
- NTP
- NetBIOS
- RIPv1
- SLP
- SNMP
- SSDP
- STUN
- TCP ACK
- TCP RST
- TCP SYN
- TCP SYN/ACK
- UDP port 0 i 80
- WS-DD
- mDNS
- memcached
- rpcbind

WYBIERZ SZYBKOŚĆ DETEKCJI

DWA SPOSOBY WYKRYCIA ATAKU — WYBIERASZ KOMPROMIS

FLOW-BASED

NetFlow / sFlow / IPFIX

35-95SEK

na detekcję i ochronę

- Niższy koszt — mniej pracy przy wdrożeniu, brak strojenia DPDK
- Niezależne od przepustowości — monitoruje wiele routerów jednocześnie
- Wolniejsza detekcja: po 30-65 sek Uplinki mogą być już wysycone
- Nie raportuje pakietów FRAGMENT - DDoS Frag Floods
- Najlepsze do raportowania, Lawful intercept / uniform sFlow, sieci o bardzo dużym ruchu

PORT-MIRROR

ZALECANE

Inspekcja pakietów DPDK

<5SEK

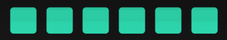
RTBH · filtrowanie ruchu 15–30 sek

- Najszybsza detekcja — reaguje zanim klienci zauważą
- Zatrzymuje carpet-bomb i floody wolumetryczne z prędkością łącza (line rate)
- Reguły BGP FlowSpec — prawidłowy ruch pozostaje nienaruszony
- Skaluje się z ruchem — Sensor obsługuje 2 porty 1–400 GE
- Wybór dla ISP / centrów danych z naciskiem na szybką reakcji ochrony

POZYSKIWANIE RUCHU — WIDOCZNOŚĆ I POKRYCIE

CO FAKTYCZNIE WIDZI KAŻDA METODA

★ Port-Mirror (DPDK)
każdy pakiet



WSZYSTKIE POLA
Możliwości detekcji

PEŁNA KOPIA PAKIETU
Przechwytywanie ruchu

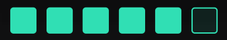
100% PAKIETÓW
Pokrycie pakietów

< 5 S RTBH · FILTR 15–30 S
Opóźnienie detekcji

KAŻDY FRAGMENT
Pofragmentowane pakiety

DOKŁADNE FLAGI (PER PAKIET)
Ataki na flagi TCP (XMAS / NULL / SYN)

IPFIX 315
sekcja ramki (IE 315)



PEŁNE NAGŁÓWKI (PRÓBKA)
Możliwości detekcji

SUROWA RAMKA (1:N)
Przechwytywanie ruchu

REALNE PAKIETY (PRÓBKA)
Pokrycie pakietów

< 5 S — INLINE
Opóźnienie detekcji

WIDOCZNE W SEKCJI RAMKI
Pofragmentowane pakiety

DOKŁADNE FLAGI (PRÓBKA)
Ataki na flagi TCP (XMAS / NULL / SYN)

sFlow
próbkowane pakiety

WSZYSTKIE POLA (PRÓBKA)
Możliwości detekcji

KOPIA PRÓBKOWANA (1:N)
Przechwytywanie ruchu

PRÓBKOWANY UŁAMEK
Pokrycie pakietów

5–30 S (5 S ARISTA)
Opóźnienie detekcji

GDY FRAGMENT W PRÓBCE
Pofragmentowane pakiety

DOKŁADNE (PRÓBKA)
Ataki na flagi TCP (XMAS / NULL / SYN)

IPFIX (v10)
rekordy flow

TYLKO IP/PORTY/PROTO
Możliwości detekcji

REKORDY FLOW
Przechwytywanie ruchu

0% PAKIETÓW (LICZNIKI)
Pokrycie pakietów

35–95 S — ZBYT WOLNO
Opóźnienie detekcji

NIEEKSPORTOWANE
Pofragmentowane pakiety

FLAGI AGREGOWANE
Ataki na flagi TCP (XMAS / NULL / SYN)

NetFlow v5 / v9
rekordy flow

TYLKO IP/PORTY/PROTO
Możliwości detekcji

REKORDY FLOW
Przechwytywanie ruchu

0% PAKIETÓW (LICZNIKI)
Pokrycie pakietów

35–95 S — ZBYT WOLNO
Opóźnienie detekcji

NIERAPORTOWANE
Pofragmentowane pakiety

FLAGI AGREGOWANE
Ataki na flagi TCP (XMAS / NULL / SYN)

Dlaczego to ważne

Port-mirror widzi każde pole każdego pakietu. Agregacja flow (NetFlow / IPFIX) widzi tylko podstawowe pola — źródłowy i docelowy IP, porty i protokół — bez fragmentacji, długości pakietu czy dokładnych flag TCP, które są sygnaturami fragment floods i ataków opartych na flagach. sFlow również widzi te pola, ale tylko na próbkowanym ułamku.

pełne · częściowe / próbkowane · niedostępne

Black-holing RTBH działa ze wszystkimi czterema metodami — różni się tylko szczegółowość detekcji.

WANGUARD — PRZEWAGA W SZYBKOŚCI DETEKCJI NAD INNYMI SYSTEMAMI ANTY-DDOS

Detekcja ruchu oparta na port-mirror z technologią DPDK

<5SEK
Detekcja i ochrona

Black Hole Routing

15-30SEK
Detekcja i ochrona

Filtrowanie ruchu

35-95SEK
Detekcja i ochrona

Inne systemy

(sFlow / NetFlow / IPFIX)

W tym momencie użytkownicy końcowi już utracili dostęp do Internetu.

Po przekroczeniu 65 sekund uplinki są wysycone — ISP i przedsiębiorstwa doświadczają poważnej degradacji łączności i wysokich opóźnień.

Czas eksportu sFlow może różnić się między producentami sprzętu i bywa niższy — np. do 5 sekund.

KLUCZOWE KONCEPCJE OCHRONY PRZED DDOS

Black Hole Routing

Remotely **T**riggered **B**lack **H**ole **R**outing

Blokuje cały ruch do docelowego IP przez rozgłoszenie trasy null (null route) za pomocą BGP

- Odrzuca cały ruch pasujący do atakowanego prefiksu docelowego
- Zapobiega wysycaniu łączy tranzytowych lub brzegowych przez floody wolumetryczne
- Szybkie we wdrożeniu, ale prawidłowy ruch również jest odrzucany

FlowSpec

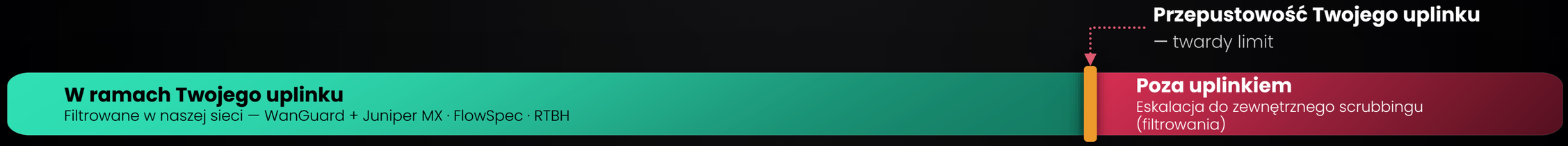
RFC 5575 / 8955 / 8956

Natychmiastowe reguły firewall z użyciem protokołu BGP. Umożliwia różne akcje:

- Odrzucenie / ograniczenie przepustowości ruchu (rate-limit)
- Przekierowanie ruchu
- Ustawianie bitów DSCP (differentiated services) w celu zapewnienia QoS lub innych opcji filtrowania

REALNY ZAKRES OCHRONY · CO MOŻEMY, A CZEGO NIE MOŻEMY ZABLOKOWAĆ

OCHRONA MA SWOJE GRANICE — I JESTEŚMY WOBEC NICH SZCZERZY



Co blokujemy

- Wszystko, na co mogą zadziałać WanGuard + Juniper MX — w ramach przepustowości Twojego uplinku.
- Stałe, bezstanowe filtrowanie MX: anti-spoofing, anti-amplification, rate-limity, CoPP.
- Dynamiczne BGP FlowSpec i RTBH aktywowane w momencie wykrycia ataku.
- Granularne filtrowanie utrzymuje Twojego klienta online — RTBH tylko w ostateczności.

Kiedy eskalujemy

- Ochrona jest ograniczona przepustowością uplinku — nie możemy filtrować więcej, niż przenosi łącze.
- BGP FlowSpec blokuje tylko to, co może wyrazić reguła — niektórych losowych lub adaptacyjnych floodów nie da się przefiltrować i zablokować.
- Gdy ruch przekracza Twój uplink lub nie może zostać przefiltrowany, eskalujemy do zewnętrznego, terabitowego centrum scrubbingu.
- Z góry mówimy, czego nie możemy zablokować — to nasza zasada, a nie drobny druk.

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

Inteligentna detekcja ruchu

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

Automatyczna, dynamiczna ochrona

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 uplinkach + 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, samodzielnie broniącą 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
Ochrona wychodząca — LAN/klient
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

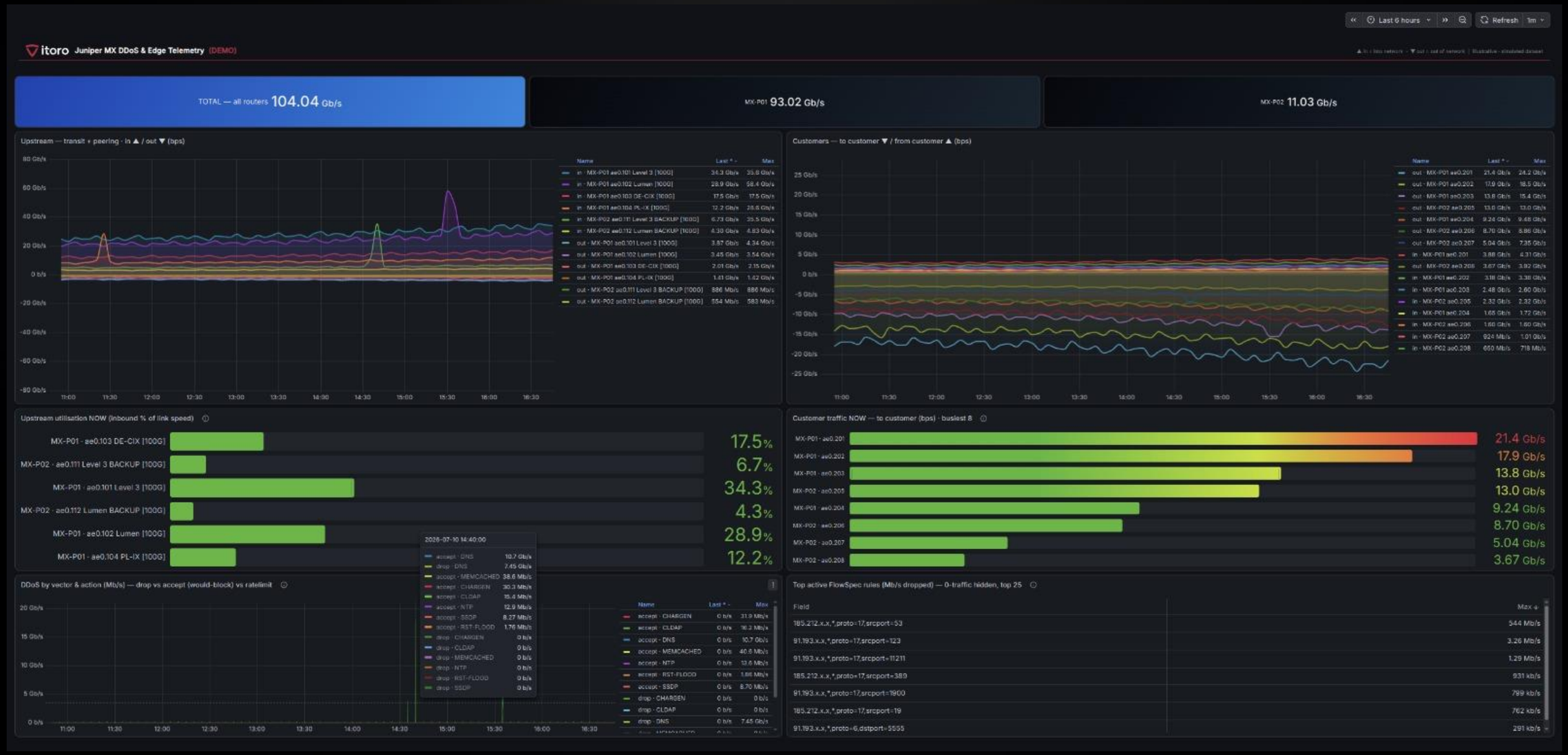
Anti-Spoofing — RPF na wszystkich interfejsach:

- 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



DLACZEGO ITORO

OD PROJEKTU DO PRODUKCJI – JEDEN PARTNER

Prowadzimy Cię przez cały proces i zdalnie realizujemy całe wdrożenie WanGuard za Ciebie.

Analiza

ataki DDoS, wolumen ruchu i szczyty, liczbę lokalizacji (PoP)

Projekt

Architektura i filtry dopasowane do Twojej sieci.

Konfiguracja

Poprawnie skonfigurowane routery, przełączniki i WanGuard.

Wdrożenie

Uruchomienie w jednym oknie serwisowym.

Wsparcie

Stałe strojenie, monitoring i reakcja.

Przed wyborem dostawcy ochrony przed DDoS, zapytaj:

Jaki jest realny zakres ochrony i gdzie są jej granice?

ZAKRES WANGUARD – WDROŻENIE PODSTAWOWEJ OCHRONY - RTBH

INSTALACJA

- Instalacja oprogramowania WanGuard Console i Sensor
- Instalacja sterowników kart sieciowych Intel/Mellanox oraz odpowiednich modułów netmap/PF_RING/DPDK
- Strojenie systemu Debian: CPU Governor, HDD Scheduler, parametry sysctl, GRUB

USTAWIENIA WANGUARD

- Instalacja i konfiguracja serwera BGP GoBGP
- Konfiguracja WanGuard Sensor i optymalizacja CPU dla aktualnego poziomu ruchu
- Dodanie adresów IP rozgłaszanych przez Twój AS i prefiksów tranzytowych, ustawienie progów DDoS

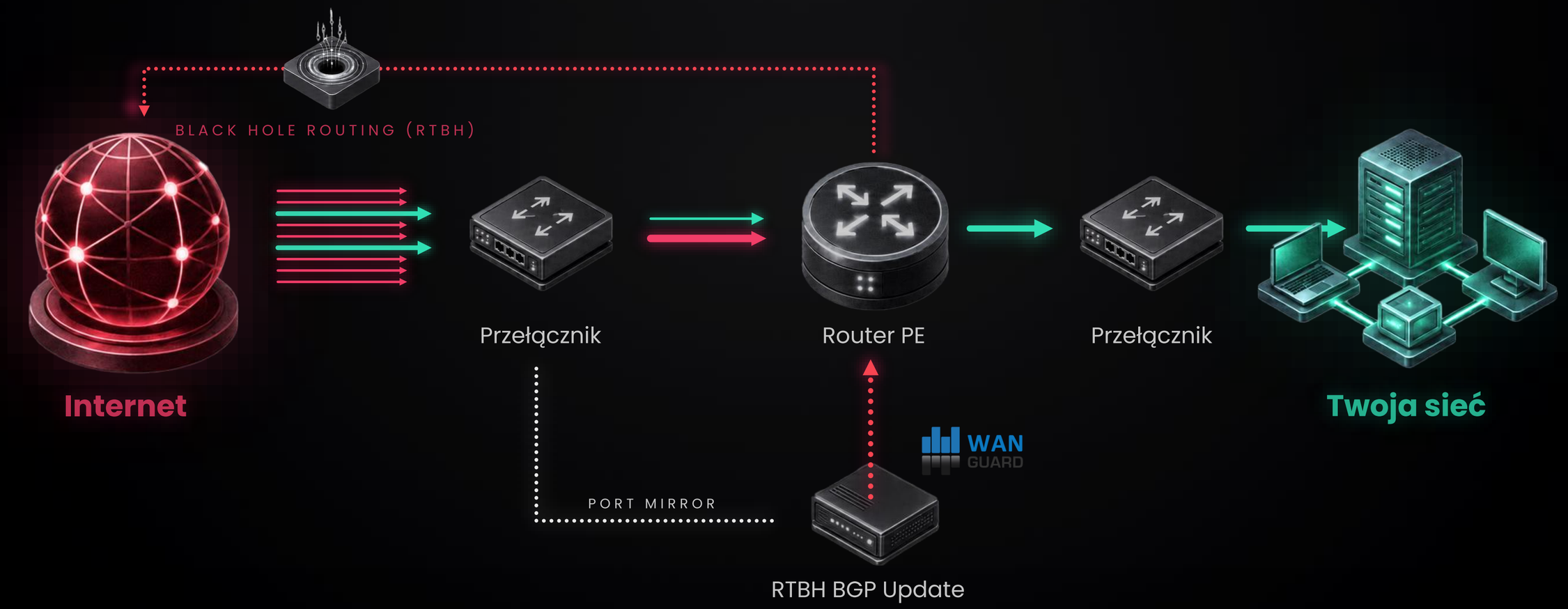
FAZA KOŃCOWA

- Konfiguracja powiadomień e-mail, raportów i alertów z WanGuard
- Ustawienie retencji danych zbieranych przez WanGuard
- Ustawienie progów wstępnych do blokowania ruchu za pomocą RTBH
- Kopia zapasowa konfiguracji WanGuard z kopią na serwerze ITORO (opcja dla wszystkich klientów z pakietami wsparcia ITORO)
- Szkolenie z obsługi systemu i nauka analizy ataków

Uruchomienie produkcyjne.

WANGUARD Z RTBH (BLACK HOLE ROUTING)

Rozgłoszenie BGP z RTBH community jest wysyłane do dostawcy upstream (Tier 1/2), powodując odrzucenie ruchu ataku w ich sieci, zanim trafi do Twojej.



FILTROWANIE RUCHU DDOS

Możliwości filtrowania ruchu:

- Filtrowanie BGP FlowSpec na routerach sprzętowych (Arista /Cisco / Huawei / Juniper / Nokia)
- Filtrowanie z akceleracją DPDK na szybkich kartach sieciowych (Intel / Mellanox)
- Filtrowanie programowe z użyciem Linux iptables / nftables – najlepsze do ataków ukierunkowanych lub o małym wolumenie

ZALETY STOSOWANIA BGP FLOWSPEC

Szybka reakcja na ataki

BGP FlowSpec wdraża reguły filtrowania w całej sieci w kilka sekund, zatrzymując ataki, zanim dotrą do celów.

Integracja

Kompatybilny z routerami obsługującymi BGP od Cisco, Juniper i Arista — integruje się z Twoim obecnym środowiskiem bez dodatkowej złożoności.

Precyzyjne filtrowanie ruchu

Reguły FlowSpec celują w złośliwy ruch według IP, protokołu, portu i cech pakietów — prawidłowy ruch przechodzi bez zakłóceń.

Łatwe w zarządzaniu i wdrożeniu

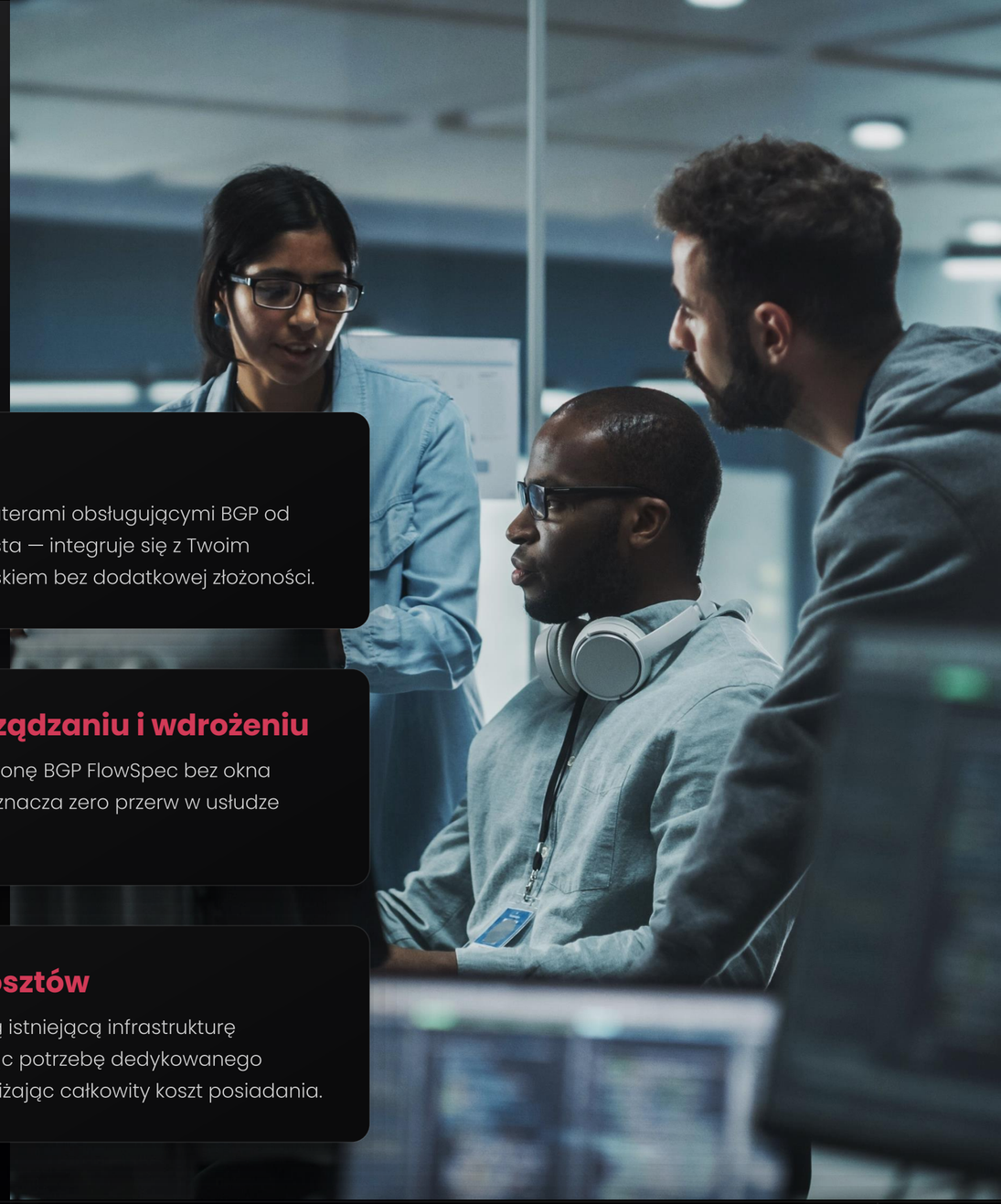
ITORO wdraża ochronę BGP FlowSpec bez okna serwisowego, co oznacza zero przerw w usłudze podczas instalacji.

Skalowalność

BGP FlowSpec działa na istniejącej infrastrukturze BGP, bez dedykowanego sprzętu. Reguły można stosować globalnie lub do wybranych segmentów sieci.

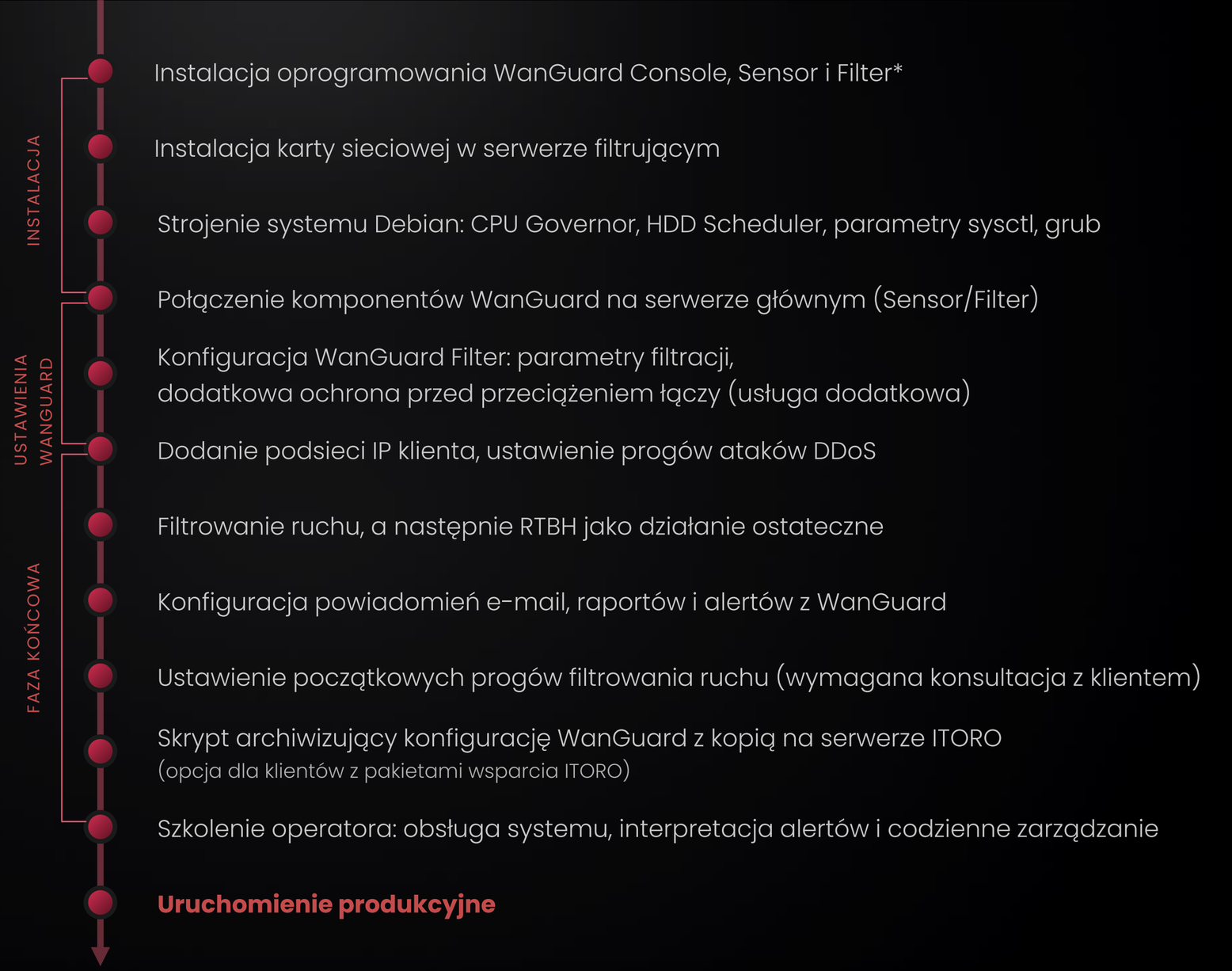
Redukcja kosztów

Wykorzystuje Twoją istniejącą infrastrukturę routerów, eliminując potrzebę dedykowanego sprzętu DDoS i obniżając całkowity koszt posiadania.



ZAKRES WANGUARD – WDROŻENIE ZAAWANSOWANEJ OCHRONY

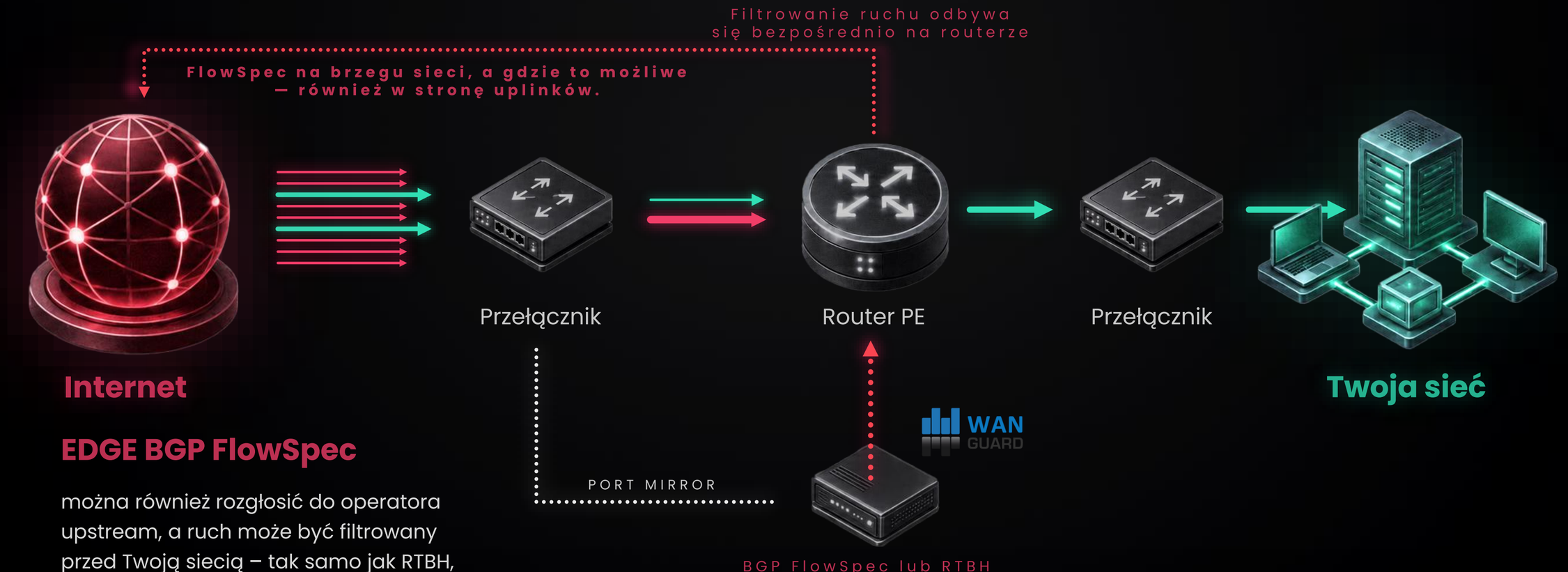
RTBH i BGP FlowSpec — filtrowanie i przekierowanie ruchu



* WanGuard Filter nie może działać samodzielnie; musi współpracować z WanGuard Sensor.

WANGUARD Z BGP FLOWSPEC

Rozgłoszenie BGP z regułami firewall FlowSpec jest wysyłane do Twoich routerów,
powodując, że pasujący ruch jest odrzucany na interfejsach Uplink, bez obciążania Twojej wewnętrznej infrastruktury sieciowej.



EDGE BGP FlowSpec

można również rozgłosić do operatora upstream, a ruch może być filtrowany przed Twoją siecią – tak samo jak RTBH, ale bez jego wady (odcięcia całkowitego).

WANGUARD — ARCHITEKTURA SYSTEMU

Rozwiązanie ochrony przed DDoS WanGuard jest wdrażane na dedykowanych wysokowydajnych serwerach, z których każdy pełni określoną rolę:

Serwer zarządzania i kontroli

- Hostuje scentralizowaną konsolę webową do administracji systemem i monitorowania
- Uruchamia demon GoBGP do dynamicznej propagacji reguł filtrowania do routerów upstream

Szybkie sensory filtrujące

Przyspieszone przetwarzanie DPDK (Data Plane Development Kit) do analizy ruchu o ultra-niskim opóźnieniu, z boku sieci (Off-Ramp). Dynamicznie generują i egzekwują reguły filtrowania BGP FlowSpec wobec złośliwego ruchu.

Specyfikacja wdrożenia

- Interfejsy sieciowe Podwójne porty 10-400 Gbps (Intel/Mellanox NIC) z akceleracją DPDK dla pełnego line-rate przechwytywania ruchu

Metodologia ochrony

Wieloetapowa ochrona:

- Filtrowanie BGP FlowSpec — granularny scrubbing (filtrowanie) ruchu w oparciu o sygnatury ataków w czasie rzeczywistym i adaptacyjne progi
- RTBH (Black Hole Routing) — automatycznie aktywowane w ciągu 5 sekund jako środek ostateczny, by zapobiec pełnemu wysyceniu łącza podczas ekstremalnych ataków wolumetrycznych

Redukcja fałszywych alarmów

- Progi detekcji dostrojone zgodnie z najlepszymi praktykami branżowymi, aby zminimalizować zakłócenia prawidłowego ruchu

WANGUARD — PRZYKŁADOWY ATAK DDOS: UDP PORT 80

Opis ataku:

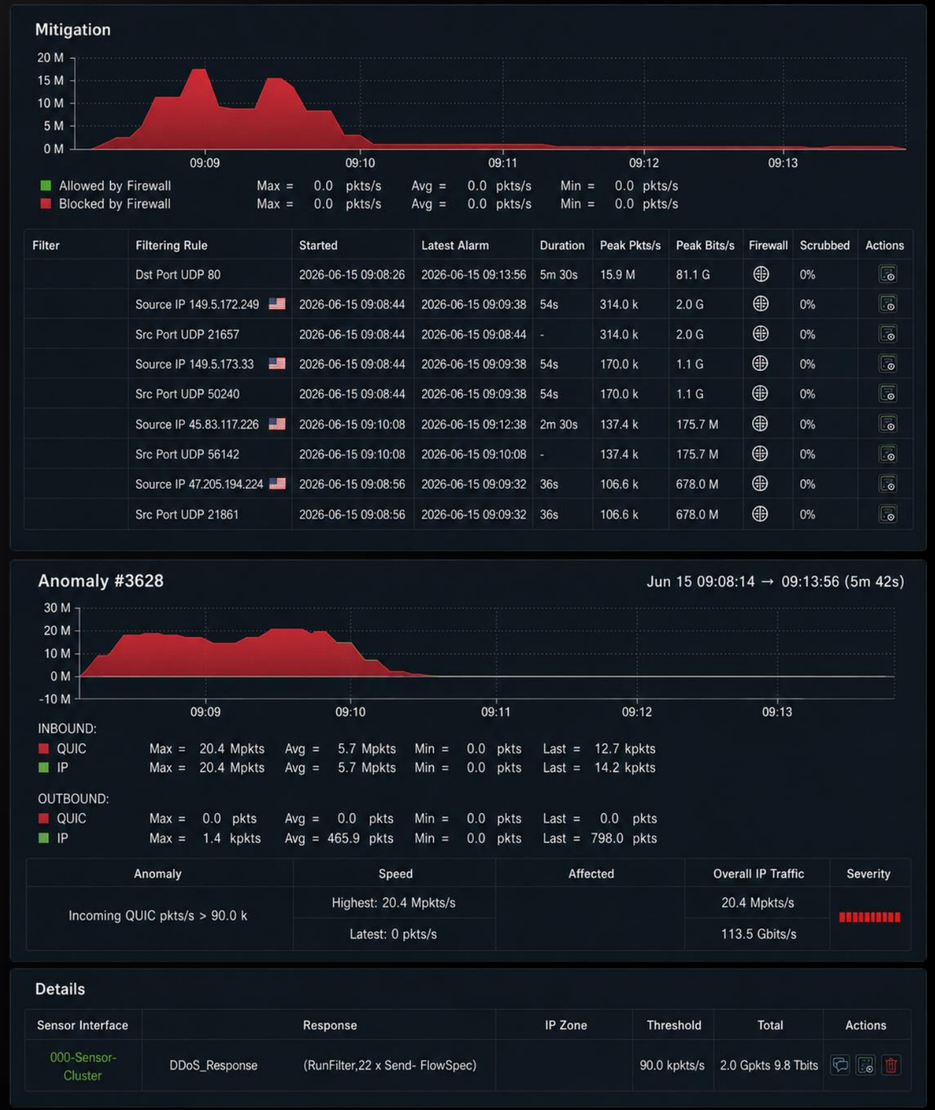
Wolumetryczny atak DDoS wymierzony w UDP port 80, ze szczytem 113 Gbps i nawet 20,4 miliona pakietów/sekundę. Atak został zidentyfikowany jako flood protokołu QUIC.

Odpowiedź systemu WanGuard:

WanGuard automatycznie sklasyfikował atak i wdrożył 22 reguły filtrowania BGP FlowSpec, które zostały rozdystrybuowane przez demon GoBGP do routerów upstream.

Efekt:

Ruch ataku został w całości odfiltrowany (scrubbing) przed dotarciem do sieci klienta. Usługa klienta pozostała stabilna i nieprzerwana przez cały
czas trwania ataku wynoszący 5 minut i 42 sekundy. Żaden prawidłowy ruch nie został zakłócony.



WANGUARD — STUDIUM PRZYPADKU: OPERATOR ISP, ATAK CARPET BOMB (50 GBPS)

Problem

We wrześniu 2024 roku operator ISP zwrócił się do ITORO, mierząc się z codziennymi wolumetrycznymi atakami DDoS przekraczającymi przepustowość jego łącza 10 Gbps — ze szczytami 50–60 Gbps. Jedyną obroną był RTBH, co oznaczało black-holing całych adresów IP i odłączanie klientów od sieci.

Atak

Atak Carpet Bomb DDoS rozkłada ruch ataku na każdy adres IP w docelowej sieci. Pojedynczy prefiks /22 mieści 1 022 adresy IP — przy zaledwie 50 Mbps na IP daje to ponad 51 Gbps przychodzącego ruchu ataku, omijając tradycyjną detekcję opartą na progach.

Rozwiązanie

ITORO wdrożyło WanGuard z BGP FlowSpec we współpracy z ORANGE Polska. Granularne reguły filtrów były wysyłane bezpośrednio do routerów upstream ORANGE, odfiltrowując (scrubbing) złośliwy ruch, zanim dotarł do sieci operatora — całkowicie eliminując potrzebę black hole routing.

Rezultat

W ciągu miesiąca ITORO i operator na bieżąco dostosowywali filtry do ewoluujących wektorów ataku, blokując wzmacniane (amplified) protokoły na poziomie routera. Atakujący ostatecznie porzucił kampanię, gdy stało się jasne, że sieć pozostaje nienaruszona.

No ↓	Prefix	Anomaly	Speed	Duration	IP pkts/s	IP Bits/s	Severity
12824	.68.2	TCP pkts/s > 110.0 k	660.0 k	5s	660.0 k	7.6 G	
12823	.68.1	FRAGMENT pkts/s > 50.0 k	392.7 k	2s	392.8 k	4.6 G	
12822	.68.1	TCP pkts/s > 110.0 k	392.7 k	2s	392.8 k	4.6 G	
12821	.68.37	TCP pkts/s > 110.0 k	341.8 k	<5sec	341.9 k	3.9 G	
12820	.68.37	FRAGMENT pkts/s > 50.0 k	341.9 k	6s	341.9 k	3.9 G	
12819	.68.36	FRAGMENT pkts/s > 50.0 k	554.6 k	6s	554.7 k	6.4 G	
12818	.68.36	TCP pkts/s > 110.0 k	554.5 k	3s	554.7 k	6.4 G	
12817	.68.35	FRAGMENT pkts/s > 50.0 k	428.9 k	3s	429.0 k	5.0 G	
12816	.68.35	TCP pkts/s > 110.0 k	428.8 k	3s	429.0 k	5.0 G	
12815	.68.34	FRAGMENT pkts/s > 50.0 k	516.4 k	8s	516.4 k	6.0 G	
12814	.68.34	TCP pkts/s > 110.0 k	516.3 k	6s	516.4 k	6.0 G	
12813	.68.33	FRAGMENT pkts/s > 50.0 k	504.0 k	6s	504.5 k	5.8 G	
12812	.68.33	TCP pkts/s > 110.0 k	504.4 k	3s	504.5 k	5.8 G	
12811	.68.32	FRAGMENT pkts/s > 50.0 k	501.0 k	2s	501.0 k	5.8 G	
12810	.68.32	TCP pkts/s > 110.0 k	500.9 k	2s	501.0 k	5.8 G	
12809	.68.29	FRAGMENT pkts/s > 50.0 k	52.2 k	<5sec	52.2 k	607.7 M	
12808	.68.30	FRAGMENT pkts/s > 50.0 k	235.6 k	3s	235.7 k	2.7 G	
12807	.68.30	TCP pkts/s > 110.0 k	235.5 k	<5sec	235.7 k	2.7 G	
12806	.68.31	FRAGMENT pkts/s > 50.0 k	375.7 k	3s	375.7 k	4.3 G	
12805	.68.31	TCP pkts/s > 110.0 k	375.6 k	3s	375.7 k	4.3 G	
12804	.68.18	FRAGMENT bits/s > 300.0 M	571.2 M	<5sec	49.5 k	571.3 M	
12803	.68.19	FRAGMENT bits/s > 300.0 M	574.1 M	<5sec	49.8 k	574.2 M	
12802	.68.20	FRAGMENT pkts/s > 50.0 k	51.0 k	<5sec	51.1 k	589.8 M	
12801	.68.21	FRAGMENT pkts/s > 50.0 k	58.4 k	<5sec	58.5 k	675.5 M	
12800	.68.22	FRAGMENT bits/s > 300.0 M	492.7 M	<5sec	42.7 k	493.0 M	
12799	.68.23	FRAGMENT pkts/s > 50.0 k	52.0 k	<5sec	52.1 k	601.5 M	
12798	.68.24	FRAGMENT pkts/s > 50.0 k	51.7 k	<5sec	51.7 k	596.8 M	
12797	.68.25	FRAGMENT pkts/s > 50.0 k	50.4 k	<5sec	50.4 k	582.4 M	
12796	.68.26	FRAGMENT pkts/s > 50.0 k	50.8 k	<5sec	50.8 k	586.6 M	
12795	.68.27	FRAGMENT pkts/s > 50.0 k	57.7 k	<5sec	57.8 k	666.7 M	
12794	.68.28	FRAGMENT pkts/s > 50.0 k	52.3 k	<5sec	52.4 k	604.5 M	
12793	.68.29	FRAGMENT bits/s > 300.0 M	569.2 M	<5sec	49.3 k	569.3 M	
12792	.68.30	FRAGMENT bits/s > 300.0 M	579.8 M	9s	29.3 k	338.0 M	
12791	.68.10	FRAGMENT pkts/s > 50.0 k	88.2 k	<5sec	88.3 k	1.0 G	

WANGUARD — ATAK CARPET BOMB

Wykrycie ataku

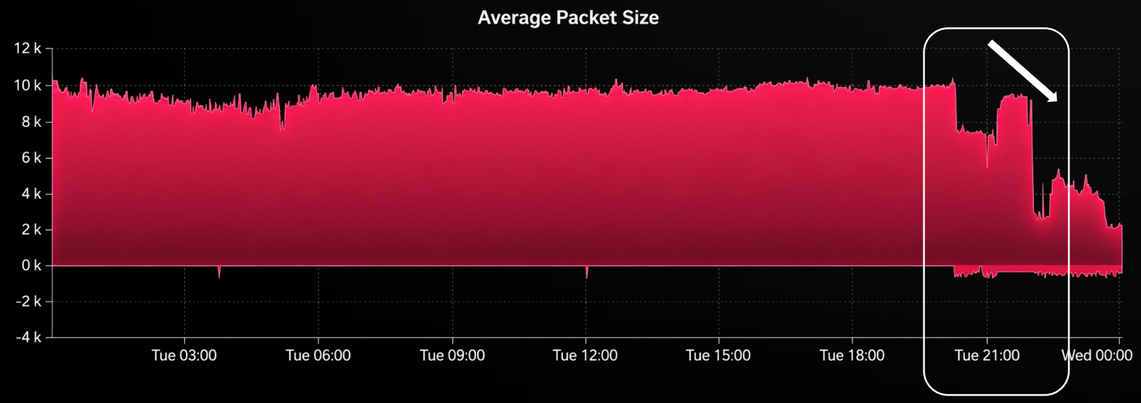
WanGuard wykrył wolumetryczne zdarzenie DDoS wysycające uplink do 7 Gbps, z gwałtownym wzrostem liczby małych pakietów do niemal 1 miliona pakietów/sekundę.

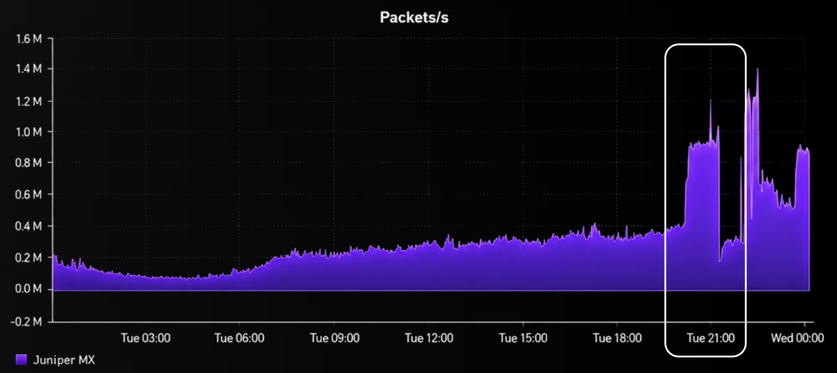
Klasyfikacja ataku: amplifikacja DNS i NTP

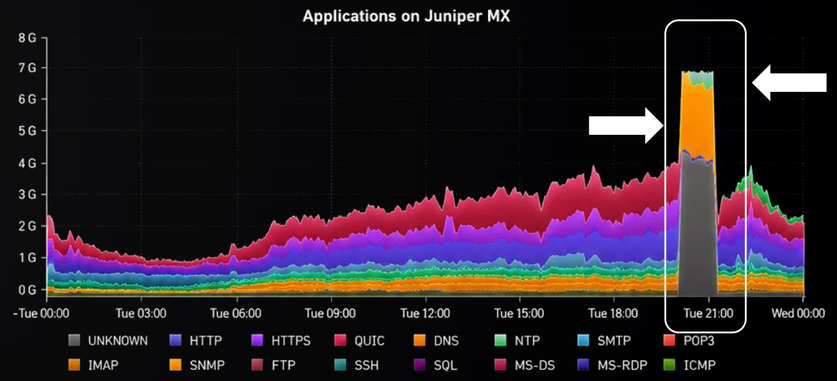
WanGuard zidentyfikował atak jako atak amplifikacyjny DNS i NTP.
Charakter Carpet Bomb został potwierdzony, gdy liczba atakowanych wewnętrznych adresów IP wzrosła z ~200 do ponad 1 800 — co oznacza, że każdy adres IP w prefiksie był atakowany jednocześnie, aby ominąć detekcję progową per-IP.

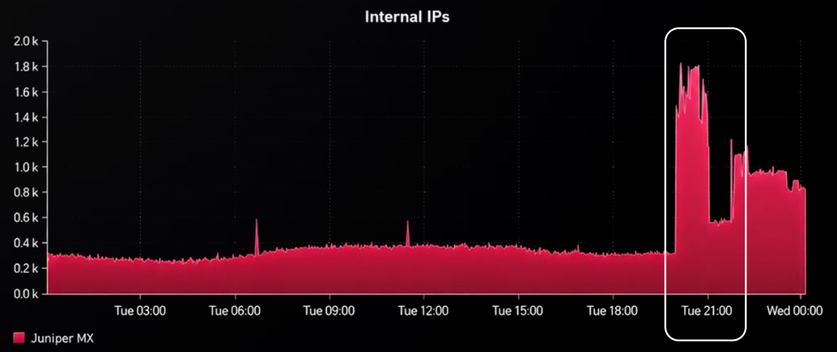
Ochrona

- Atak został odparty przy użyciu kombinacji:
- BGP FlowSpec — granularne reguły filtrów wysłane upstream w celu zablokowania wzmacnianego (amplified) ruchu UDP (port 53/DNS, port 123/NTP)
- RTBH — black hole routing zastosowano tam, gdzie było to potrzebne.









CARPET BOMB PRZYKŁADOWY RAPORT

Anomaly #119704

Jul 03 13:17:07 → 13:39:57 (22m 50s)

INBOUND:

UDP-HTTP	Max	=	28.4	Gbits/s	Avg	=	3.5	Gbits/s	Min	=	0.0 bits/s	Last	=	4.8	Mbits/s
IP	Max	=	28.4	Gbits/s	Avg	=	3.5	Gbits/s	Min	=	0.0 bits/s	Last	=	4.8	Mbits/s

OUTBOUND:

UDP-HTTP	Max	=	0.0	bits/s	Avg	=	0.0	bits/s	Min	=	0.0 bits/s	Last	=	0.0	bits/s
IP	Max	=	0.0	bits/s	Avg	=	0.0	bits/s	Min	=	0.0 bits/s	Last	=	0.0	bits/s

Anomaly	Speed	Affected	Overall IP Traffic	Severity
Incoming UDP-HTTP bits/s > 1.0 M	Highest: 28.4 Gbits/s		2.6 Mpkt/s	
	Latest: 0 bits/s		28.4 Gbits/s	

Details

Sensor Interface	Response	IP Zone	Threshold	Total	Actions
Sensor-2x100GE	DDoS Response (Uruchom Filtr, RTBH, 911 x Wsylij FlowSpec, 79 x Carpet Bomb, Raport DDoS)		1.0 Mbits/s	445.8 Mpkt/s 4.8 Tbits	

Mitigation

DPDK Filter

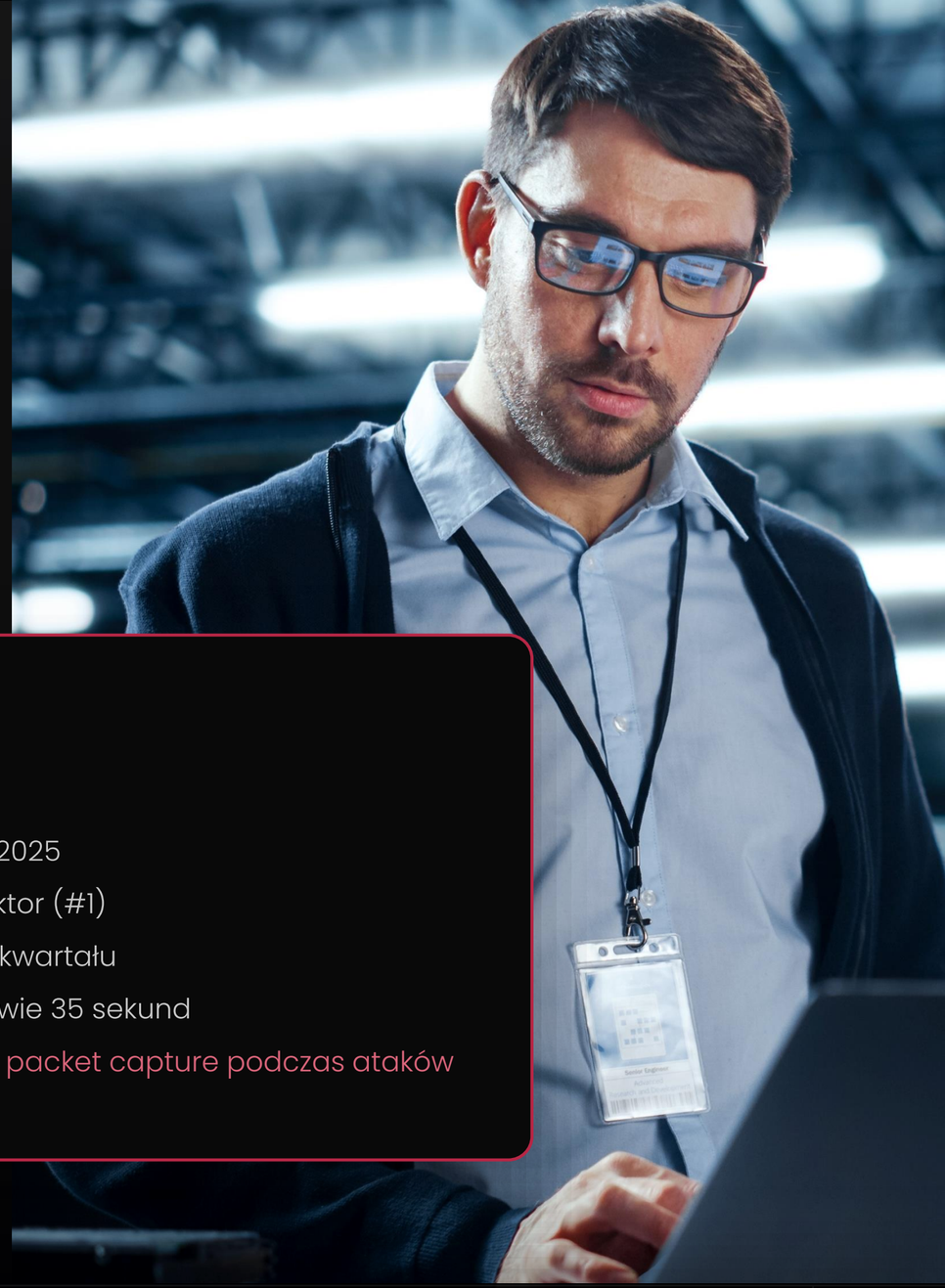
Allowed by Firewall	Max	=	0.0	bits/s	Avg	=	0.0	bits/s	Min	=	0.0 bits/s
Blocked by Firewall	Max	=	0.0	bits/s	Avg	=	0.0	bits/s	Min	=	0.0 bits/s

Filter	Filtering Rule	Started	Latest Alarm	Duration	Peak Pkts/s	Peak Bits/s	Firewall	Scrubbed	Actions
DPDK Filter	Packet Length 1428	2026-07-03 13:17:17	2026-07-03 13:31:33	14m 16s	626.0 k	7.2 G	Ⓕ	-	-
DPDK Filter	TimeToLive 57	2026-07-03 13:17:17	2026-07-03 13:29:47	12m 30s	459.2 k	5.0 G	-	-	-
DPDK Filter	TimeToLive 58	2026-07-03 13:17:17	2026-07-03 13:30:58	13m 41s	428.7 k	4.7 G	-	-	-
DPDK Filter	TimeToLive 56	2026-07-03 13:17:17	2026-07-03 13:28:52	11m 35s	346.2 k	3.8 G	-	-	-
DPDK Filter	Packet Length 1468	2026-07-03 13:17:17	2026-07-03 13:29:47	12m 30s	325.1 k	3.8 G	Ⓕ	-	-
DPDK Filter	TimeToLive 55	2026-07-03 13:19:07	2026-07-03 13:29:27	10m 20s	254.7 k	2.8 G	-	-	-
DPDK Filter	Source IP 82.165.183.200	2026-07-03 13:21:57	2026-07-03 13:22:57	1m	84.8 k	928.9 M	Ⓕ	-	-
DPDK Filter	Src Port UDP 14587	2026-07-03 13:21:57	2026-07-03 13:22:52	55s	73.1 k	800.0 M	Ⓕ	-	-

NOWOŚĆ NA 2026 · REAGOWANIE NA INCYDENTY

AWARYJNE REAGOWANIE NA DDOS

Atak trwa w piątek wieczorem, pojawia się żądanie okupu, progi wymagają dostrojenia?
ITORO reaguje pierwsze. Monitoring na żywo, analiza pakietów oraz strojenie progów / BGP FlowSpec.



ROCZNIE

26000

PLN/rok

Działamy jako Twój zdalny DDoS NOC. Zapytaj o więcej informacji pod adresem sales@itoro.com.pl

Aktualny cennik zawsze na itoro.com.pl

Dlaczego to teraz ważne

- Ataki DDoS wzrosły ponad dwukrotnie, do 47,1 mln w 2025
- Telekomy / ISP to obecnie najczęściej atakowany sektor (#1)
- Zagrożenia Ransom-DDoS wzrosły o 68% kwartał do kwartału
- Największy atak 2025 osiągnął 31,4 Tbps i trwał zaledwie 35 sekund
- Większość ISP nie ma nikogo, kto potrafiłby odczytać packet capture podczas ataków

Źródło: raporty DDoS Cloudflare 2025 · NETSCOUT 2025

WYDAJNOŚĆ SENSORA PORT-MIRROR

CENNIK SENSORÓW Z FILTROWANIEM WEDŁUG PRĘDKOŚCI PORTU

Większa przepustowość oznacza więcej dedykowanych rdzeni CPU. 2×100GE to dzisiejszy standard; 1×400GE to poziom premium dla sieci z dużymi uplinkami i planami rozwoju.

Sensor (2 porty)	Liczba rdzeni CPU	Detekcja	Jednorazowe wdrożenie	Najlepsze dla
2 × 10GE	~12–16	<5s / 15–30s	**13 000 zł**	Małe / brzeg sieci
2 × 40GE	~16-24	<5s / 15–30s	**19 500 zł**	Średni ISP
2 × 100GE ★ standard	~24-32	<5s / 15–30s	**26 000 zł**	Większość ISP obecnie
1 × 400GE premium	~64 (1× CPU)	<5s / 15–30s	**51 900 zł**	Łącza 400G / wzrost
Flow (NetFlow/sFlow)	minimalne	35–95s	**17 300 zł**	Raportowanie / lekkie

Aktualny cennik zawsze na itoro.com.pl

Dodatki:

Sensor 2×100GE
21 600 zł

Konfig. BGP FlowSpec
(Cisco/Juniper)
4 300 zł

Archiwizacja NetFlow
2–40TB
8 700 zł

Licencja WanSight od
1 400 zł

WSPARCIE TECHNICZNE · 2026

WYBIERZ POZIOM WSPARCIA — WIĘKSZOŚĆ ISP WYBIERA GOLD

Awaryjne reagowanie na DDoS, analiza DDoS, strojenie progów na żądanie – rozważ odciążenie swojego NOC/SOC.

SD = tego samego dnia
SBD = tego samego dnia roboczego
NBD = następnego dnia roboczego, 10:00–22:00.

Zadanie wsparcia	Silver NBD · Podstawowy	Gold SBD · ★ Najczęściej wybierany	Gold + Tego samego dnia	Platinum Pełna administracja
Wsparcie e-mail · WanGuard i problemy z Linux · aktualizacje 2×/rok	✓	✓	✓	✓
DDoS rekomendacje progów kopie zapasowe · doradztwo ws. fałszywych alarmów	✓	✓	✓	✓
Aktywne monitorowanie ataków przez ITORO	✗	✓	✓	✓
Dwutygodniowe sesje Zoom: monitoring anomalii i konfiguracji	✗	✓	✓	✓
ITORO wprowadza zmiany w WanGuard za Ciebie	✗	✓	✓	✓
Zdalny monitoring stanu sensora + auto-naprawa (zawsze online)	✗	✓	✓	✓
Pełna administracja / outsourcing (bez potrzeby własnego administratora)	✗	✗	✗	✓
Cena (netto, PLN)	**13 000 zł** /rok	**6 500 zł** /mies.	**7 800 zł** /mies.	**17 300 zł** /mies.

Aktualny cennik zawsze na itoro.com.pl

PODSUMOWANIE

TYPOWE WDROŻENIE

Rekomendowany pakiet	PLN
Wdrożenie Port-Mirror — 2×100GE Sensor i Filter (DPDK)	26 000 zł
30-dniowe strojenie progów + szkolenie operatora	**w cenie**
Wsparcie GOLD — aktywne monitorowanie + auto-heal (rok 1)	6 500 zł /mies.
Licencje WanGuard — Sensor + Filter + DPDK (z rabatem ITORO)	**~10 800 zł / rok**
Suma za pierwszy rok	**114 800 zł**
Kolejne lata	88 800 zł

Czy jesteś pod atakiem DDoS?
Możemy wdrożyć WanGuard w 2 godziny

30
dni ważności oferty

Ceny licencji WanGuard (WAN Sensor + WAN Filter + DPDK) są orientacyjne — zależą od konfiguracji; z rabatem ITORO mogą być niższe.
Aktualny cennik zawsze na itoro.com.pl

NISKIE RYZYKO Z ZAŁOŻENIA

30-dniowa gwarancja strojenia
kalibrujemy, aż fałszywe alarmy zostaną zminimalizowane

Kamień milowy akceptacji
ochrona potwierdzona zgodnie ze specyfikacją przed odbiorem

Twoje serwery i pełna kontrola
brak zewnętrznego centrum scrubbingu, brak uzależnienia od dostawcy (lock-in)

Poparte ponad 20 latami praktyki w sieciach ISP
i tranzytowych

ZGODNOŚĆ · DYREKTYWA UE NIS2 (2022/2555)

ODPORNOŚĆ NA DDOS JEST TERAZ OBOWIĄZKIEM PRAWNYM

NIS2 czyni ochronę przed DDoS i raportowanie incydentów obowiązkowymi dla ISP, telekomów i infrastruktury cyfrowej w całej UE.

Czego wymaga NIS2	Jak ITORO to zapewnia
Środki techniczne do zarządzania ryzykiem cybernetycznym W tym detekcja i ochrona przed DDoS (art. 21)	Ciągłe filtrowanie + monitorowana ochrona zapewniają techniczne środki zarządzania ryzykiem, których oczekuje NIS2.
Raportowanie incydentów Wczesne ostrzeżenie w ciągu 24h, powiadomienie w ciągu 72h, raport końcowy w ciągu 1 miesiąca (art. 23).	Abonament awaryjny (Emergency retainer) zapewnia udokumentowany, ograniczony czasowo proces reagowania na incydenty.
Odpowiedzialność kierownictwa Organy zarządzające odpowiadają za nadzór nad tymi środkami	Telemetria i packet capture — gotowe do raportowania — wspierają Twoje powiadomienia w ciągu 24h / 72h.
Dotyczy podmiotów kluczowych i ważnych: dostawców ISP, IXP, DNS, chmury i telekomunikacji.	Za brak zgodności grożą kary do €10 mln lub 2% globalnego rocznego obrotu — pomagamy Ci zachować zgodność.

Sprawdź gotowość swojej firmy i Twoją odpowiedzialność wobec NIS2 — bezpłatne narzędzie ITORO: itoro.com.pl/narzedzia

itoro

Porozmawiajmy o Twojej sieci.
Rozwiązanie dopasowane do Twoich potrzeb.

sales@itoro.com.pl