FOSA

SYSTEM DETEKCJI I FILTRACJI ATAKÓW DDoS

Sprint

FOSA

Filtrująco-Ochronny System AntiDDoS

FOSA jest autorskim projektem Sprint S.A. stworzonym na bazie własnych doświadczeń w dziedzinie aktywnej ochrony i zabezpieczeń przed atakami DDoS. Siłą FOSY jest optymalne dostrojenie technologii Andrisoft WanGuard w połączeniu z niezawodną platformą sprzętową.

Geneza projektu

W dzisiejszych czasach ataki DDoS (Distributed Denial of Service) są jednym z największych zagrożeń dla bezpieczeństwa serwerów pracujących w sieci Internet. Z każdym rokiem stają się liczniejsze, silniejsze i w skutkach coraz bardziej dotkliwe. Ochrona przed atakami DDOS to już nie przesadzone wymaganie a codzienna konieczność.

Sprint S.A. posiada własne data center i ulokowane w nim setki serwerów. Od roku 2013 intensywność ataków DDoS wzrosła tak mocno, że byliśmy zmuszeni do szybkiego wdrożenia ochrony antiDDoSowej. Na rynku jest wiele sprzętowych rozwiązań dedykowanych do ochrony przed atakami DDoS. Ich wspólną cechą jest bardzo wysoki koszt wdrożenia i rocznego utrzymania. Jest to inwestycja, na którą może pozwolić sobie jedynie duży operator.

Skuteczność i skalowalność dla każdego

Potrzeba zmotywowała nas do stworzenia rozwiązania, które oferowałoby funkcjonalność uznanych marek i jednocześnie koszt inwestycji byłby uzasadniony od strony ekonomicznej. W efekcie tych prac powstała FOSA – Filtrująco-Ochronny System AntiDDoS.

Sprawdzone standardy, skuteczniejsze działanie

FOSA to rozwiązanie oparte na istniejącym oprogramowaniu WanGuard i fizycznym serwerze zbudowanym na sprawdzonej platformie Supermicro. Powyższe rozwiązanie zostało wdrożone w Sprint Data Center. Przez rok rozwiązanie było testowane, parametryzowane i dostrajane, tak by finalnie osiągnąć maksymalną wydajność sprzętową FOSY. Dzisiaj FOSA skutecznie chroni blisko 1000 serwerów.

FOSA – zakres usługi

- Analiza bieżącej konfiguracji węzła dostępowego Klienta
- Projekt implementacji rozwiązania FOSA
- Dostawa urządzeń systemu FOSA i licencji oprogramowania WanGuard
- Wdrożenie rozwiązania FOSA
  - instalacja
  - konfiguracja platformy i parametryzacja oprogramowania
  - testy rozwiązania
- Wsparcie techniczne w zakresie ochrony przed atakami DDoS

Przetestuj FOSĘ we własnej sieci. Bezpłatnie i bez ryzyka.

Wdrożenie testowe* obejmuje implementację FOSY wraz z asystą techniczną inżyniera systemowego Sprint S.A. Asysta przewiduje instalację urządzenia FOSA w Państwa środowisku sieciowym oraz konfigurację jego ustawień.

KONTAKT: +48 89 522 12 20 (pn.-pt. 8.00 - 16.00) fosa@sprintdatacenter.pl

*) Wdrożenie testowe jest przedmiotem odrębnej umowy zawartej pomiędzy stroną użytkującą urządzenie FOSA a Sprint S.A.

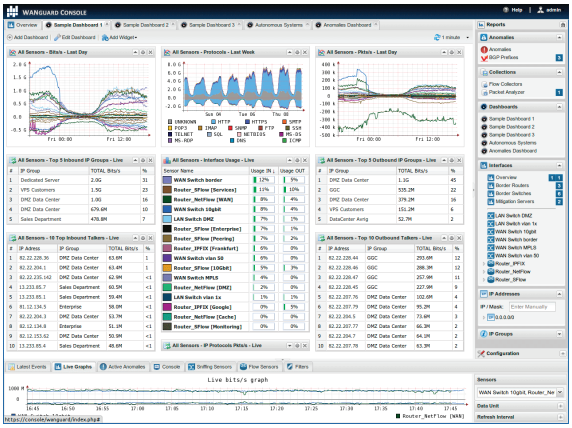
FOSA

Ataki DDoS to jedno z najbardziej uciążliwych zagrożeń w ruchu sieciowym

Nieprzewidziane wzorce ruchu w sieciach wpływają na niezadowolenie użytkowników, zmuszają do planowania zakupów pasma ponad miarę i zatykają kosztowne łącza tranzytowe. Dostarczanie wydajnych i niezawodnych usług sieciowych jest kluczowym elementem sukcesu dla dzisiejszych firm.

Wraz ze wzrostem kosztów niesionych przez problemy i przerwy w wydajnej pracy sieci, natychmiastowa identyfikacja zagrożeń wydajnosci i maksymalne ograniczenie ich negatywnych skutków staje się niezbędne w celu zapewnienia wymaganego poziomu usług i ich dostępności (SLA). Zagrożenia te obejmują rozproszone ataki odmowy usługi (DDoS), takie jak zalew pakietów SYN ze sfałszowanych adresów IP (SYN flood), wzmocnienie NTP, zalew UDP (UDP flood), dystrybucję robaków sieciowych, ataki z botnetów, błędne użycie usług sieciowych i mieszanie czułego na opóźnienia ruchu kluczowego z ruchem masowym.

FOSA jako narzędzie do nadzoru, nawet skomplikowanych, wielowarstwowych sieci zarówno przełączanych jak i routowanych, ze swoim unikatowym zestawem cech jest stworzony specjalnie do sprostania zadaniu dokładnej identyfikacji tych zagrożeń i ich eliminacji.



Panel zarządzania parametrami sieci i monitoringiem zagrożeń

KLUCZOWE FUNKCJE I KORZYŚCI

- **PEŁNA WIDOCZNOŚĆ SIECI** - Wspiera najnowsze metody monitoringu ruchu IP w sieciach: bezpośrednią analizę pakietów z prędkością 10 Gb/s; NetFlow v5, v7 i v9; sFlow, IPFIX, NetStream, jFlow, cflowd.
- **WYKRYWANIE DDOS** - Wydajny mechanizm detekcji anomalii szybko wykrywa ataki wolumetryczne profilując bieżące zachowanie użytkowników i porównując ponad 120 parametrów z progami definiowanymi przez administratora.
- **FILTROWANIE DDOS** - Chroni sieci i usługi przez wykrywanie i czyszczenie złośliwego ruchu na umieszczonych w sieci szeregowo lub równolegle serwerach filtrujących, lub też przez zastosowanie blackholingu BGP.
- **ROZBUDOWANE MECHANIZMY REAKCJI** - Automatyzacja reakcji na zagrożenia z użyciem predefiniowanych lub niestandardowych akcji: powiadomienia e-mail, rozgłoszenia prefiksów przez BGP, komunikaty SNMP trap, modyfikacja ACL, wykonanie dowolnych skryptów z dostępem do ponad 70 parametrów przez łatwe w użyciu API itd.
- **SZCZEGÓŁOWA ANALIZA INCYDENTÓW** - Pakiety lub informacje o sesjach (flow) z każdego ataku są zachowywane dla późniejszej analizy bezpieczeństwa. Szczegółowe raporty z ataków mogą zostać rozesłane e-mailem do Ciebie, dotkniętego atakiem klienta lub operatora sieciowego atakującego użytkownika.
- **ZAAWANSOWANA KONSOLA WWW** - Scentralizowane zarządzanie i raportowanie poprzez spójny, czytelny, interaktywny, konfigurowalny portal HTML5. Możliwość definiowania własnych zestawów wskaźników, ról użytkowników, zdalnego uwierzytelnienia itp.
- **SNIFFER PAKIETÓW** - Zawiera rozproszony sniffer pakietów, który może zapisywać zrzuty pakietów z różnych części sieci. Szczegóły ruchu można obejrzeć w zbliżonym do Wiresharka, wygodnym interfejsie WWW.
- **ZBIERANIE NETFLOW** - Udostępnia w pełni wyposażony zbieracz informacji o ruchu w sieci. Obsługuje protokoły NetFlow, sFlow, IPFIX. Informacje archiwizowane są w skompresowanej formie w celu długotrwałego przechowywania i mogą być w łatwy sposób przeglądane, przeszukiwane, filtrowane, sortowane i eksportowane.
- **ZŁOŻONE ANALIZY** - Tworzy najbardziej złożone analizy z danych agregowanych dla serwerów, interfejsów, aplikacji, portów, protokołów, firm, działów, krajów, systemów autonomicznych i innych.
- **RAPORTOWANIE NA ŻYWO** - Wykresy pasma są animowane, a ich maksymalna rozdzielczość sięga czasów nawet tak krótkich, jak 5 sekund.
- **RAPORTY HISTORYCZNE** - Raporty ruchu mogą obejmować okres od ostatnich 5 sekund aż do ostatnich 10 lat dzięki możliwości wyboru dowolnego zakresu czasu w tym okresie. Histogram pasma zawiera wartości 95 percentyla, dla rozliczeń zużycia.
- **RAPORTY REGULARNE** - Każdy raport może zostać wygenerowany automatycznie i rozesłany zainteresowanym stronom w możliwych do skonfigurowania odstępach czasu.
- **SZYBKOŚĆ I SKALOWALNOŚĆ** - Oprogramowanie Wan Guard zostało stworzone tak, aby pracować na standardowym sprzęcie, a jego komponenty mogą zostać rozproszone na klastry serwerów.
- **NAJNIŻSZY KOSZT** - Najtańszy dostępny system przeciwdziałania atakom DDoS do zainstalowania we własnej serwerowni.

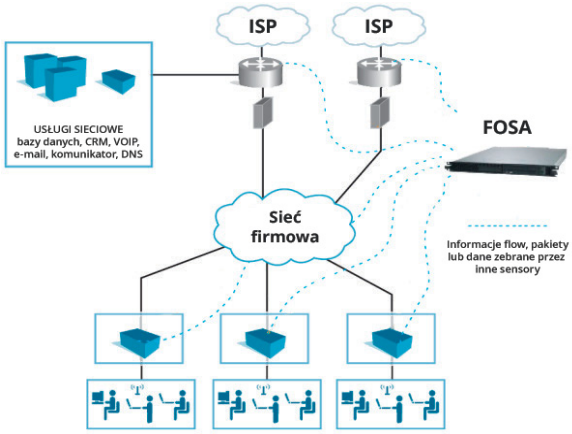
FOSA Sensor

Inteligentny mechanizm wykrywania zagrożeń

Sensor poprzez analizę pakietów lub informacji typu flow (NetFlow itp.) zapewnia nadzór ruchu IP, wykrywanie ataków odmowy usługi (DoS i DDoS) oraz innych ataków wolumetrycznych, zbieranie dogłębnych analiz ruchu oraz danych rozliczeniowych.

Zbierane informacje pozwalają na tworzenie złożonych raportów ruchu, wykresów i statystyk; natychmiastowe określenie bezpośredniej przyczyny incydentów sieciowych; zrozumienie wzorców w wydajności usług i świadome planowanie rozbudowy infrastruktury.

Sercem sensora jest wysoce skalowalny mechanizm korelacji ruchu sieciowego zdolny do nieprzerwanej analizy setek tysięcy adresów IP. Złożone algorytmy statystyczne integrują dane o ruchu aby zbudować szczegółowy i dokładny obraz bieżącego jak i historycznego przepływu pakietów w sieci.



KLUCZOWE FUNKCJE I KORZYŚCI

- Sensor zawiera w pełni skalowalny mechanizm analizy ruchu IP zdolny do monitorowania w czasie rzeczywistym dziesiątek tysięcy adresów IPv4 i IPv6 i bloków tych adresów.
- Zarządzanie i raportowanie z centralnej konsoli WWW ze spójnym, holistycznym widokiem
- Wykrywa wszystkie anomalie w paśmie ruchu
  - Rozproszone ataki odmowy usługi (DDoS), nieznane wolumetryczne ataki DoS
  - Ataki wzmocnione NTP, typowe zalewy UDP i ICMP (UDP i ICMP flood), ataki SMURF
  - Zalewy pakietów SYN, TCP/UDP na port 0, LOIC, ataki P2P itp.
  - Skanowanie i robaki wysyłające pakiety do niepoprawnych lub niezaalokowanych adresów, omijające ruch do krytycznych usług
- Elastyczne możliwości reakcji na zagrożenia:
  - Aktywacja filtra WanGuard w celu ograniczenia skutków ataku DDoS
  - Aktywacja blackholingu BGP, zmiana routingu do atakowanego celu
  - Powiadomienie operatorów NOC e-mailem według szablonów edytowanych przez użytkownika
  - Wysłanie dostosowanych komunikatów Syslog do zdalnych serwerów logowania lub systemów SIEM
  - Zachowanie zrzutu pakietów w celu późniejszej analizy lub zachowania dowodu
  - Rozszerzanie wbudowanych możliwości własnymi skryptami korzystającymi z łatwego w użyciu API
- Udostępnia rozliczenia ruchu sieciowego i wykresy poszczególnych adresów IP / sieci / grup adresów dla następujących rodzajów ruchu: sumaryczny, TCP, TCP+SYN, UDP, ICMP, inny, błędny, sesje, sesje+syn, HTTP, HTTPS, SSL, poczta, DNS, SIP, NTP, RDP, SNMP, SSH, IPSec, Facebook, Youtube, Netflix, Hulu i innych w przyszłości.
- Tworzy statystyki i wykresy najbardziej aktywnych obiektów, zewnętrznych IP, grup adresów, systemów autonomicznych, krajów, portów TCP i UDP, protokołów IP itd.
- Maksymalna rozdzielczość wykresów przepustowości jest konfigurowalna w zakresie od 5 sekund do 10 minut.
- Użytkownicy mogą zapisać dane konkretnych sesji (flow) lub zrzuty pakietów w celach późniejszej analizy bezpieczeństwa lub pomocy w rozwiązywaniu problemów z siecią. Dane sesji mogą być łatwo przeszukiwane, filtrowane, sortowane i eksportowane. Zrzuty pakietów mogą zostać pobrane lub być oglądane bezpośrednio w konsoli WanGuard, w interfejsie zbliżonym do znanego programu Wireshark.
- Wspiera pracę w trybie klastrowym, zbierane dane agregowane są z wielu sensorów sniffujących lub zbierających dane w trybie flow. Obciążenie poszczególnych instancji może być rozkładane na poszczególne rdzenie CPU lub serwery.
- Na serwerach w sieci może zostać uruchomiona dowolna liczba instancji sensora.
- Można użyć PF_RING/DNA dla zrzutów pakietów na interfejsach 10 Gb/s bez problemów z wydajnością i strat.

PARAMETRY TECHNICZNE

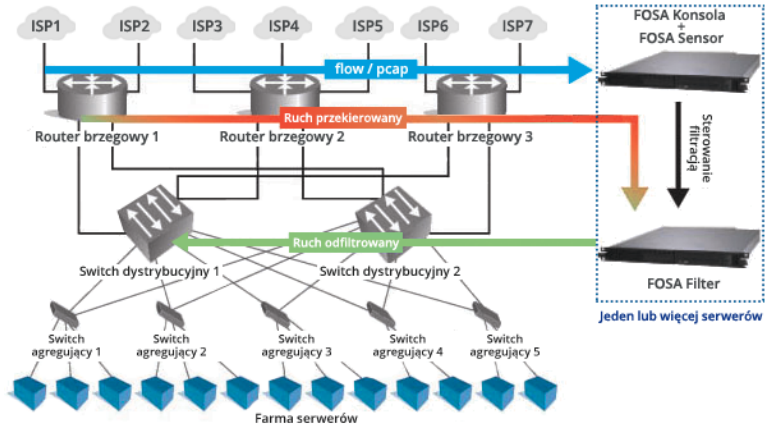
	Sensor sniffujący	Analiza NetFlow
Metoda analizy ruchu	Instalacja szeregowa Port monitorujący Urządzenie TAP	NetFlow® v5 v7 v9 sFlow® v4 v5 IPFIX
Czas detekcji DDoS	< 5 sekund	< czas eksportu NetFlow + 5 sekund
Pojemność pojedynczej instancji sensora	1x interfejs 10 Gb/s Ethernet	1x eksporter NetFlow obejmujący liczne interfejsy 10Gb/s Ethernet
Platforma sprzętowa	FOSA 1G / FOSA 10G	FOSA 1G

FOSA Filter

Dynamiczna filtracja i skuteczna neutralizacja szkodliwych pakietów

FOSA Filter wykrywa wzorce ruchu i generuje reguły filtracji, które czyszczą ruch z anomalii w sposób minimalizujący ich negatywny wpływ na usługi świadczone użytkownikom.

SCENARIUSZE UŻYCIA



- **Serwer umieszczony równolegle** - Na obrazku przedstawiono Filtr, który wysyła aktualizację tablicy routingu przez BGP do routera brzegowego obsługującego ruch przychodzący. Router ustawia następny hop dla podejrzanego ruchu na adres filtra. Następnie filtr blokuje złośliwy ruch a oczyszczony kierowany jest z powrotem do sieci. Ta technika pozwala kierować do filtra jedynie ruch kierowany do atakowanych celów, bez ryzyka wpływu działania filtra na resztę sieci.
- **Serwer umieszczony szeregowo, skonfigurowany jako router** - Filtr pracuje na serwerze umieszczonym szeregowo w ścieżce danych. Serwer skonfigurowany jest jako router.
- **Serwer umieszczony szeregowo, skonfigurowany jako most** - Filtr pracuje na serwerze umieszczonym szeregowo w ścieżce danych. Serwer skonfigurowany jest jako most sieciowy warstwy drugiej OSI.
- **Serwer podłączony do urządzenia typu TAP lub portu monitorującego** - Filtr pracuje na serwerze, który otrzymuje kopię ruchu sieciowego z urządzenia TAP lub portu monitorującego przełącznika. Bezpośrednie czyszczenie nie jest możliwe, ale filtr nadal może generować reguły filtrujące, które ułatwiają zrozumienie mechanizmów obserwowanego ataku lub mogą zostać zastosowane w innych używanych w sieci urządzeniach bezpieczeństwa, jak firewalle czy IPS-y.

KLUCZOWE FUNKCJE I KORZYŚCI

- Chroni przed znanymi, nieznanymi i rozwijającymi się atakami DoS, DDoS i innymi atakami wolumetrycznymi przez dynamiczne, automatyczne budowanie reguł i filtrowanie ruchu na ich podstawie. Reguły zawierają dowolne połączenia źródłowych i docelowych adresów IP (IPv4 i IPv6), źródłowych i docelowych portów TCP, źródłowych i docelowych portów UDP, protokołów IP, błędnych pakietów IP, rodzajów pakietów ICMP, TTL, długości pakietów i innych.
- Rozpoznaje i blokuje złośliwy ruch w czasie poniżej 5 sek.
- Nie blokuje poprawnego ruchu klientów.
- Nie wymaga uczenia standardowego ruchu ani manualnej interwencji użytkownika.
- Elastyczne możliwości reakcji na zagrożenia i łatwe w użyciu API dla oskryptowania reakcji na wzorce ataków:
  - Powiadomienie operatorów NOC e-mailem według szablonów edytowanych przez użytkownika
  - Wysłanie dostosowanych komunikatów Syslog do zdalnych serwerów logowania lub systemów SIEM
  - Zachowanie zrzutu pakietów w celu późniejszej analizy lub zachowania dowodu
  - Rozszerzanie wbudowanych możliwości własnymi skryptami: konfiguracja ACL lub wykonanie komendy PIX "shun" na routerach lub firewallach, filtracja atakujących IP przez zastosowanie komend "route blackhole" na serwerach linuksowych, wysłanie komunikatów trap SNMP do stacji monitorujących itp.
- Obsługuje wiele mechanizmów filtracji pakietów:
  - Filtrowanie programowe przy użyciu mechanizmu NetFilter zawartego w jądrze systemu Linux
  - Filtrowanie sprzętowe na gigabitowych i 10-gigabitowych kartach z chipsetem Intel 82599 (Intel X520, Intel X540, HP 560 i inne) lub lepszym
  - Dedykowane firewalle i IPS-y sprzętowe przy użyciu skryptów integrujących
- Serwer filtra może zostać uruchomiony szeregowo lub filtrować złośliwy ruch przy użyciu przekierowania BGP na serwer włączony w sieć równolegle.
- Odfiltrowany ruch może zostać włączony ponownie do sieci przy użyciu routingu statycznego lub tunelowania GRE.
- Możliwość użytkowania na łatwo dostępnym, powszechnym sprzęcie serwerowym.

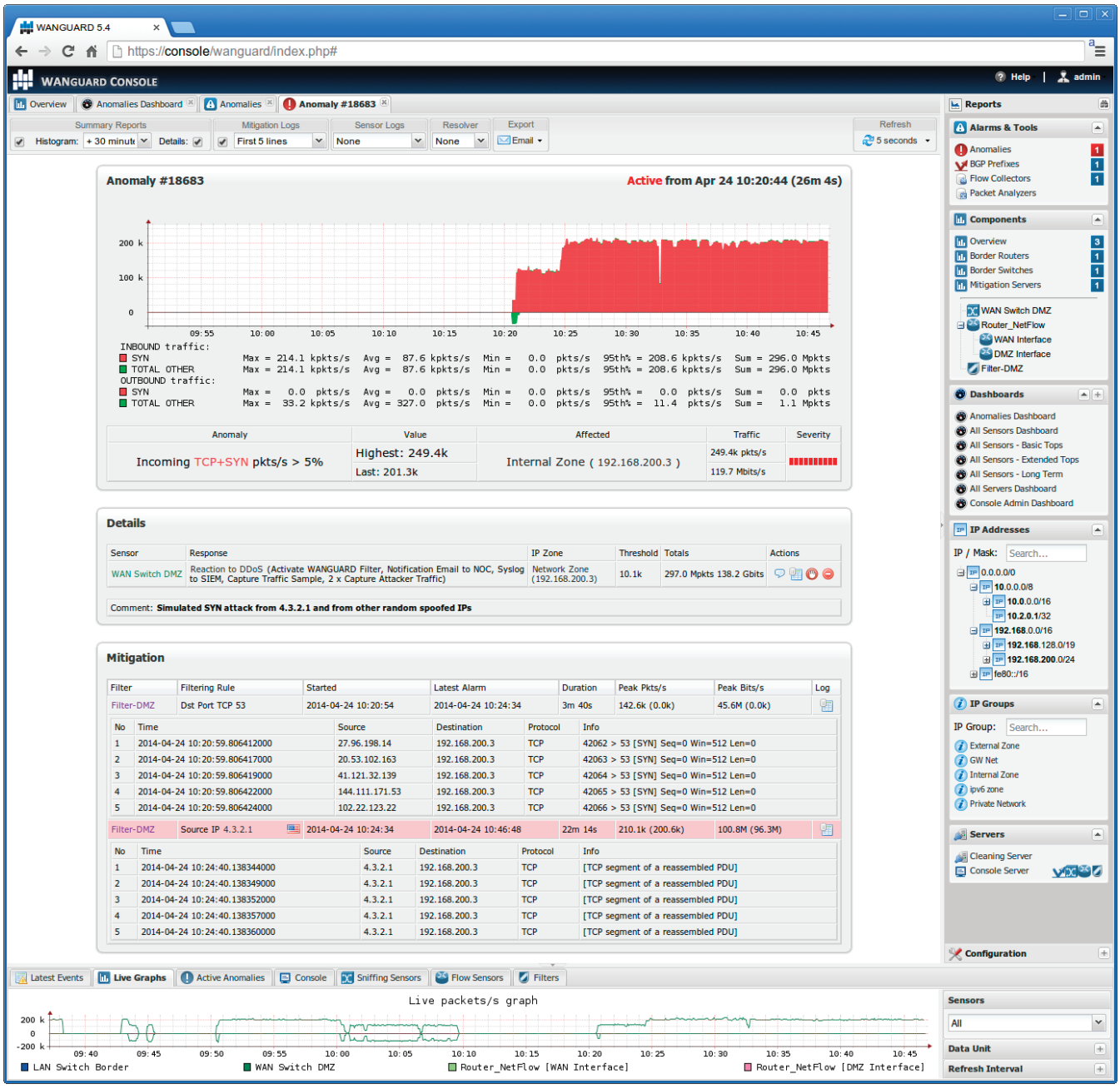
PARAMETRY TECHNICZNE

	FOSA 1G • Filtracja 1 Gb/s	FOSA 10G • Filtracja 10 Gb/s
Architektura wdrożenia	Instalacja szeregowa lub równoległa	Instalacja szeregowa lub równoległa
Interfejsy sieciowe	2x 1Gb/s RJ45	2x 1Gb/s RJ45, 2x 10Gb/s SFP+
Obudowa	1U	1U
Wymiary WxGxS [mm]	43x437x650	43x437x650
Zasilanie	2x 500W	2x 500W

FOSA Konsola

Wielopoziomowy monitoring i zarządzanie bezpieczeństwem sieci

Administrowanie FOSĄ odbywa się poprzez rozbudowaną konsolę administracyjną.Dzięki niej, administrator aplikacji może monitorować wszystkie parametry pracy sieci lokalnej oraz natychmiast reagować w przypadku wykrycia wszelkich nieprawidłowości i zagrożeń.



KONTAKT

Sprint S.A. • SprintDataCenter
ul. Jagiellończyka 26, 10-062 Olsztyn
tel. +48 89 522 12 20 (pn.-pt. 8.00 - 16.00)
fosa@sprintdatacenter.pl

www.sprint.pl
www.sprintdatacenter.pl