Orange Network Security

Portal self-service v7

Spis treści

Interfejs użytkownika

Portal self-service umożliwia analizę danych dziennika zdarzeń sieciowych, dostosowanie raportów, przeglądanie stanu urządzeń sieciowych oraz przeglądanie i konfigurację zasad bezpieczeństwa.

Uwaga!

Zależnie od profilu usługi i opcji widoczny jest dostosowany i niezbędny zestaw przycisków i menu.

Dlatego nie wszystkie są dostępne na kontach administratorów klientów.

Instrukcja opisuje wszystkie opcje przycisków i menu portal ponieważ ma charakter ogólny.

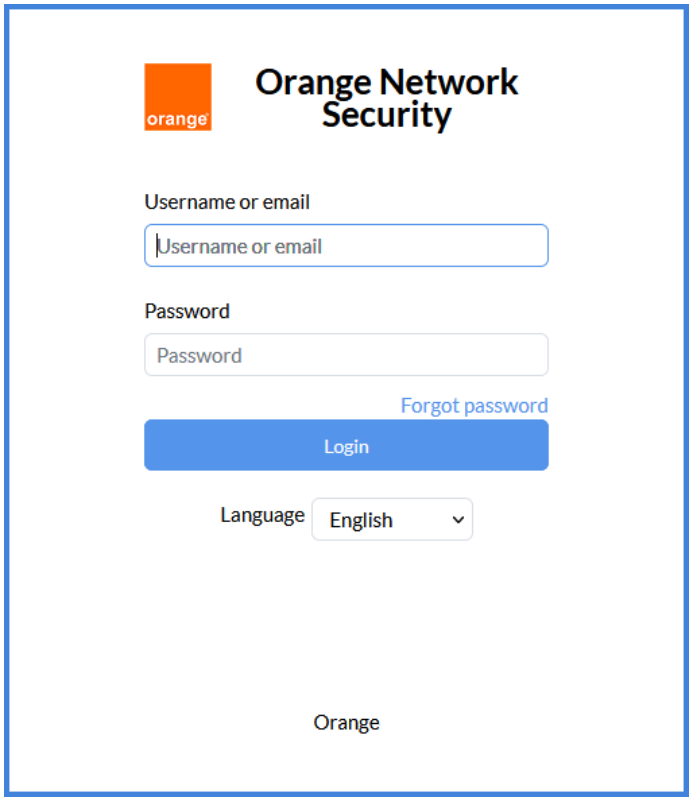
Po pomyślnym zalogowaniu portal wyświetla stronę dashboardu.

Górny baner jest wspólny dla wszystkich stron i zawiera następujące przyciski:

- *Install*: instalacja polityk i konfiguracji usług na podłączonych urządzeniach
- *Help*: wyświetlenie dokumentacji
- *Notifications*: podgląd powiadomień systemowych
- *Change Password*: formularz zmiany hasła
- *Logout*: wylogowanie z systemu Lewy panel zawiera następujące karty, w zależności od uprawnień użytkownika:
- *Insights*: dashboard systemu, monitory, stan urządzeń i dzienniki zdarzeń
- *SD-WAN*: monitorowanie i konfigurowanie SD-WAN
- *Security*: przeglądanie i zarządzanie politykami, obiektami firewalla, wirtualnymi sieciami prywatnymi (VPN), routingiem statycznym i usługami DHCP
- *Switch*: monitorowanie i konfiguracja przełączników sieciowych
- *WiFi*: monitorowanie sieci bezprzewodowych
- *Reports*: wyświetlanie dostępnych raportów
- *Audit*: przeglądanie dziennika aktywności użytkowników systemu
- *Additional Resources*: lista zasobów zewnętrznych skonfigurowanych przez administratora systemu

Strona logowania

Po uruchomieni w przeglądarce internetowej łącza https://ons.orange.pl/ pokaże się strona logowania:



Gdy użytkownik loguje się po raz pierwszy, musi zmienić swoje hasło.

Wsparcie językowe

Portal obsługuje następujące języki:

- angielski
- francuski
- niemiecki
- portugalski
- rumuński
- hiszpański
- włoski

Opcje na liście rozwijanej *Language* na stronie logowania dotyczą tylko strony logowania.

Resetowanie hasła

Aby zresetować hasło:

1. W oknie dialogowym logowania kliknij *Forgot password*.
2. Wprowadź adres e-mail powiązany z kontem użytkownika i kliknij *Send*. System wyśle pod podany adres wiadomość z instrukcją dotyczącą resetowania hasła.

Zmiana hasła

Aby zmienić hasło:

1.1.1.1 W nagłówku portalu kliknij ikonę *Change password* 

1. Wprowadź aktualne hasło i nowe hasło, potwierdź nowe hasło, a następnie kliknij *Save*. Nowe hasło zacznie obowiązywać przy następnej próbie logowania.

Powiadomienia (*Notifications*)

W tym miejscu można przeglądać powiadomienia systemowe.

Dostępne akcje

W oknie *Notifications* dostępne są następujące działania:

Time zone: ustawienie strefy czasowej lokalnej, zgodnej z konfiguracją administratora systemu lub strefę czasową GMT.

Filter: wybór zakresu danych według czasu wystąpienia (*Last 60 Minutes*, *Last 1 Day*, *Last 1 Week* lub *Specify*).

Mark as Read: zaznacz wybrane powiadomienia jako przeczytane.

Delete: usuwanie wybranych powiadomień.

Search: wyszukaj wpisy zawierające wprowadzony tekst.

Show x entries: ogranicz liczbę wpisów wyświetlanych na stronie (20 lub 50).

Instalowanie konfiguracji na urządzeniach

Aby zmiana konfiguracji urządzenia zaczęła obowiązywać, należy wykonać funkcję *Install*.

1. W nagłówku kliknij *Install*.
2. Wybierz urządzenia docelowe.
3. Kliknij *Install*.
4. Wybierz *Yes* , aby potwierdzić instalację.
   Pasek postępu w oknie dialogowym *Install* pokazuje stan instalacji.
5. Po zainstalowaniu pakietu kliknij *Finish*.

Insights

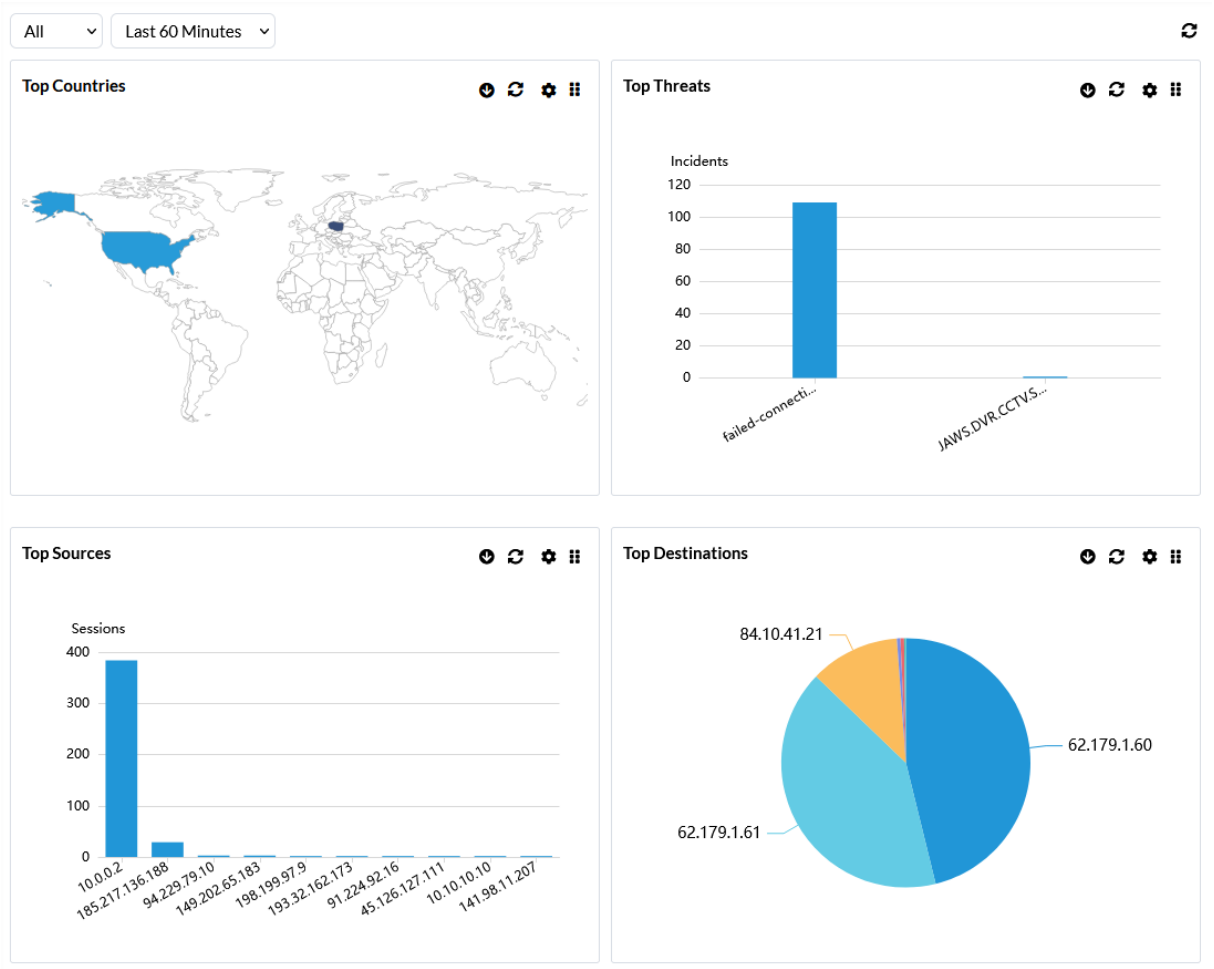
Karta *Insights* zapewnia dostęp do dzienników zdarzeń bezpieczeństwa, widżetów, monitorów i stanu zarządzanych urządzeń.

Dostępne są następujące zakładki:

- Dashboard
- Monitors
- Health
- Logs

Dashboard

Karta *Dashboard* wyświetla różne widoki dzienników zdarzeń bezpieczeństwa i inne informacje.



Karta *Dashboard* jest zorganizowana jako zestaw widżetów.

Dostępne są następujące widżety:

Top Countries (najczęściej odwiedzane kraje)
Top Threats (najważniejsze zagrożenia)
Top Sources (najczęściej spotykane źródła połączeń sieciowych)
Top Destinations (najczęściej występujące cele połączeń sieciowych)
Top Applications (najczęściej używane aplikacje)
Policy Hits (statystyki użytych polityk)
Admin Logins (statystyki logowań administratorów)
System Events (zdarzenia systemowe)
Resource Usage (wykorzystanie zasobów)

Dostępne akcje zakładki Dashboard

W zakładce *Dashboard* dostępne są następujące akcje :

- *Scope:* wybór źródła danych (wszystkie lub tylko wskazane urządzenie)
- *Set Filter:* filtrowanie dane (wg czasu)
- *Refresh*: odświeżanie danych

Po ustawieniu filtra na *Last N…* pojawi się pole N. Należy wprowadzić odpowiednią wartość i kliknąć ikonę *Search*, aby zastosować ten filtr.

Widżety są aktualizowane zgodnie z wyborem dokonanym w filtrze i wartością wprowadzoną w polu wyszukiwania N.

Wcześniej wybrany zakres czasu w jednej z zakładek *Dashboard, Monitors, Logs* lub *SD-WAN > Monitoring* jest automatycznie stosowany do pozostałych.

Dostępne akcje widżetów

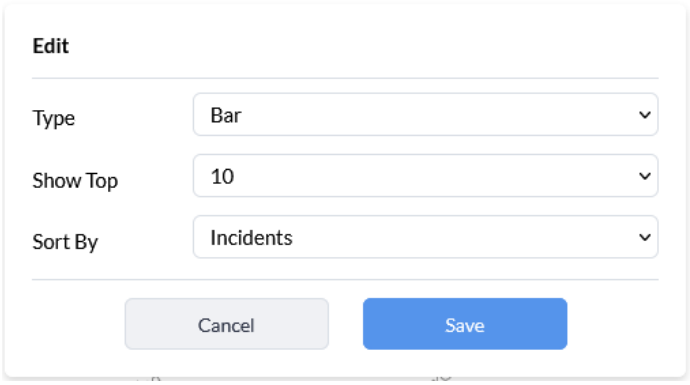
Górny baner każdego widżetu zawiera niektóre lub wszystkie z następujących elementów sterujących:

- *Drill-down*: wyświetlanie danych szczegółowych
- *Refresh*: odświeżanie danych
- *action - Edit*: edytcja widżetu
- *Drag to reorder*: kliknij a następnie przeciągnij i upuść, aby zmienić pozycję widżetu w okienku

Po najechaniu kursorem na widżet, można zobaczyć dodatkowe informacje.

Akcja *Edit*

Wybranie akcji *Edit* powoduje otwarcie okna w widżecie, w którym można wybrać typ wykresu, liczbę pierwszych wyników do prezentacji oraz sposób sortowania danych.



Akcja Drill-down

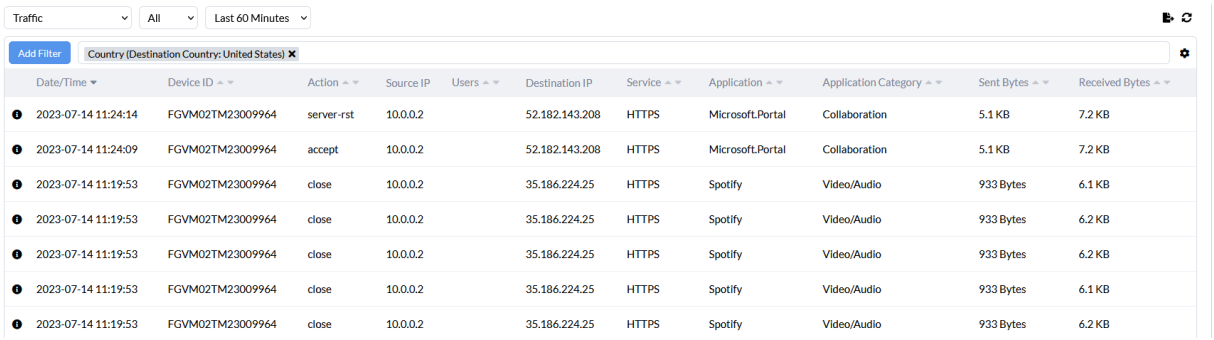
Ikona *Drill-down* wskazuje, że można uzyskać więcej informacji o danych wyświetlanych w widżecie.

Następujące widżety obsługują funkcję przechodzenia do szczegółów:

- Top Countries
- Top Threats
- Top Sources
- Top Destinations
- Top Applications

Każdy z tych widżetów wyświetla wykres lub wykres słupkowy z N najbardziej znaczącymi wynikami, gdzie wyróżnikiem jest region, ruch lub zagrożenie (w zależności od widżetu). Po

wybraniu jednego z wyników zostanie otwarta karta *Logs* z widokiem przefiltrowanym według tego wyniku. Filtr widoku znajduje się nad tabelą.



Date/Time	Device ID	Action	Source IP	Users	Destination IP	Service	Application	Application Category	Sent Bytes	Received Bytes
2023-07-14 11:24:14	FGVM02TM23009964	server-rst	10.0.0.2		52.182.143.208	HTTPS	Microsoft.Portal	Collaboration	5.1 KB	7.2 KB
2023-07-14 11:24:09	FGVM02TM23009964	accept	10.0.0.2		52.182.143.208	HTTPS	Microsoft.Portal	Collaboration	5.1 KB	7.2 KB
2023-07-14 11:19:53	FGVM02TM23009964	close	10.0.0.2		35.186.224.25	HTTPS	Spotify	Video/Audio	933 Bytes	6.1 KB
2023-07-14 11:19:53	FGVM02TM23009964	close	10.0.0.2		35.186.224.25	HTTPS	Spotify	Video/Audio	933 Bytes	6.2 KB
2023-07-14 11:19:53	FGVM02TM23009964	close	10.0.0.2		35.186.224.25	HTTPS	Spotify	Video/Audio	933 Bytes	6.2 KB
2023-07-14 11:19:53	FGVM02TM23009964	close	10.0.0.2		35.186.224.25	HTTPS	Spotify	Video/Audio	933 Bytes	6.1 KB
2023-07-14 11:19:53	FGVM02TM23009964	close	10.0.0.2		35.186.224.25	HTTPS	Spotify	Video/Audio	933 Bytes	6.2 KB

Monitors

Karta *Monitors* wyświetla informacje o zagrożeniach, ruchu oraz aplikacjach i witrynach internetowych. Zawiera również monitor, który wyświetla informacje związane z VPN.

Dostępne są następujące opcje i przyciski:

- *Monitor*: Wybierz pozycję z listy, aby wyświetlić następujące monitory:
    - *Top Threats* (najważniejsze zagrożenia)
    - *Top Sources* (najczęściej spotykane źródła połączeń sieciowych)
    - *Top Destinations* (najczęściej występujące cele połączeń sieciowych)
    - *Policy Hits* (statystyki użytych polityk)
    - *Top Applications* (najczęściej używane aplikacje)
    - *Top Browsing Users* (najaktywniejsi użytkownicy Internetu)
    - *Top Website Domain* Users najczęściej odwiedzane domeny internetowe
    - *VPN* (statystyki połączeń VPN: SSL i Site-to-Site)
- *Scope:* wybór źródła danych (wszystkie lub tylko wskazane urządzenie)
- *Set Filter:* filtrowanie danych (wg czasu)
- *Refresh:* odświeżenie danych
- *Sort*: niektóre kolumny w panelu mają funkcję sortowania, umożliwiającą sortowanie danych w kolejności rosnącej lub malejącej.

Po ustawieniu filtra na *Last N…* pojawi się pole N. Należy wprowadzić odpowiednią wartość i kliknąć ikonę *Search*, aby zastosować ten filtr.

Widżety są aktualizowane zgodnie z wyborem dokonanym w filtrze i wartością wprowadzoną w polu wyszukiwania N.

Wcześniej wybrany zakres czasu w jednej z zakładek *Dashboard, Monitors, Logs* lub *SD-WAN > Monitoring* jest automatycznie stosowany do pozostałych.

W przypadku niektórych raportów lista rozwijana na dole pozwala wybrać liczbę wpisów wyświetlanych na stronie. Ponadto niektóre raporty mają dodatkowy pasek wyszukiwania .

Jeśli są dostępne, można użyć przycisków < i > w prawym dolnym rogu do nawigacji po stronach lub można bezpośrednio wybrać numer strony.

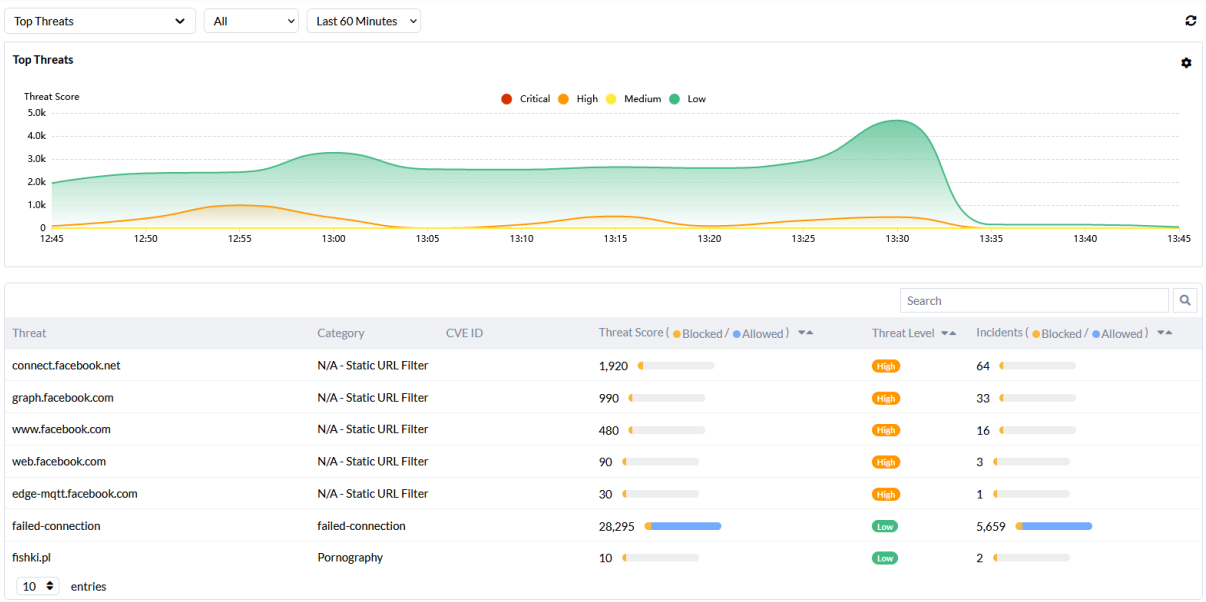
Top Threats

Karta *Top Threats* w obszarze *Insights* > *Monitors* wyświetla informacje o zagrożeniach.

Następujące zdarzenia są uważane za zagrożenia:

- Ryzykowne aplikacje wykryte przez kontrolę aplikacji
- Próby włamań wykryte przez IPS
- Złośliwe strony internetowe wykryte przez web filtering
- Złośliwe oprogramowanie lub botnety wykryte przez program antywirusowy

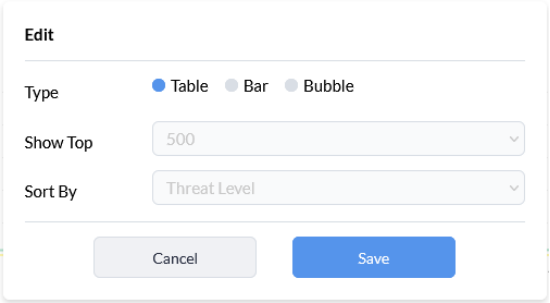
Poniższy rysunek przedstawia kartę *Top Threats*:



Panel wyświetla zagrożenia, kategorie, identyfikatory CVE, ocenę zagrożenia (zablokowane i dozwolone), poziom zagrożenia oraz liczbę incydentów.

Po najechaniu kursorem na wykres, można zobaczyć informacje o zagrożeniach.

Aby edytować wykres najważniejszych zagrożeń należy wybrać pozycję *Settings* (⚙) > *Edit.* Poniższy rysunek przedstawia okienko edycji :

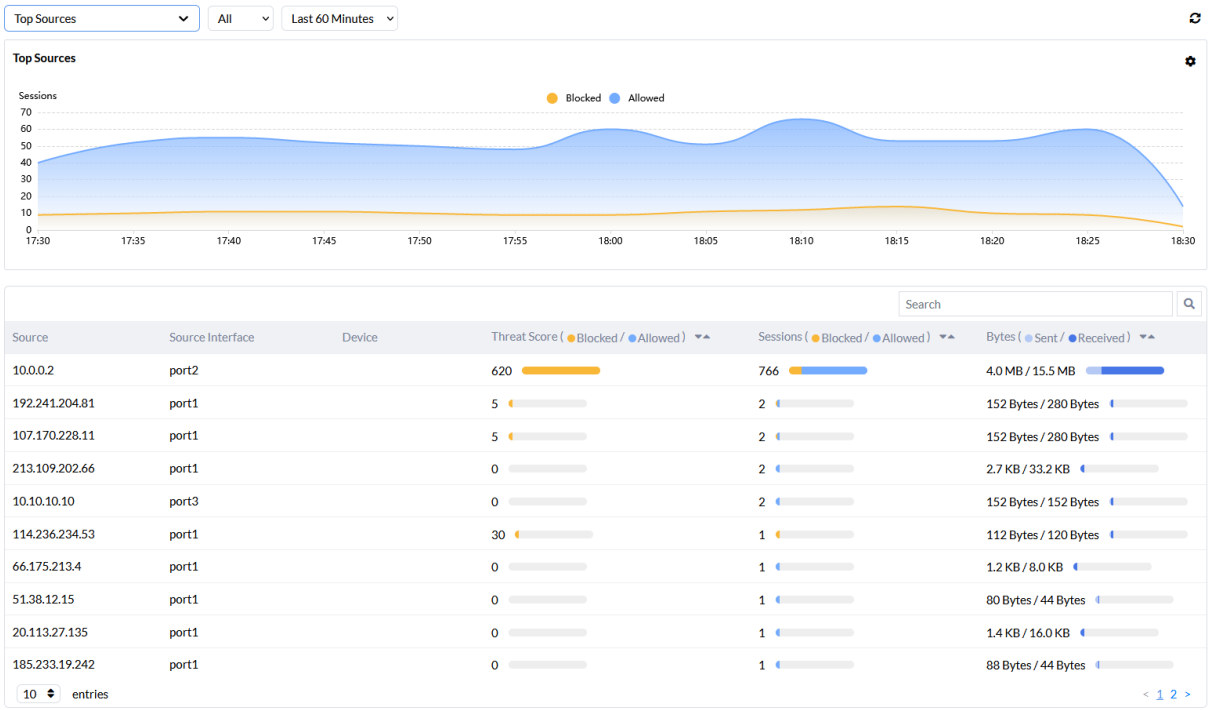


Okienko edycji umożliwia wybór spośród trzech różnych typów wykresów: tabelarycznego, słupkowego lub bąbelkowego. W przypadku wykresów słupkowych i bąbelkowych można wybrać 10, 15 lub 20 największych zagrożeń do wyświetlenia i posortować je według poziomu zagrożenia, oceny zagrożenia lub liczby incydentów.

Top Sources

Karta *Top Sources* w sekcji *Insights* > *Monitors* wyświetla statystyki ruch sieciowego według źródłowego adresu IP, interfejsu źródłowego, urządzenia, wskaźnika poziomu zagrożenia (zablokowane i dozwolone), sesji (zablokowane i dozwolone) oraz przesłanych bajtów (wysłanych i odebranych).

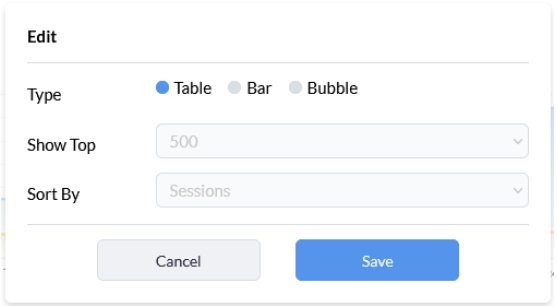
Poniższy rysunek przedstawia kartę *Top Sources* :



Po najechaniu kursorem na wykres można zobaczyć informacje o sesjach.

Aby edytować wykres najpopularniejszych źródeł należy wybrać pozycję *Settings* (⚙) > *Edit*

Poniższy rysunek przedstawia okienko edycji :

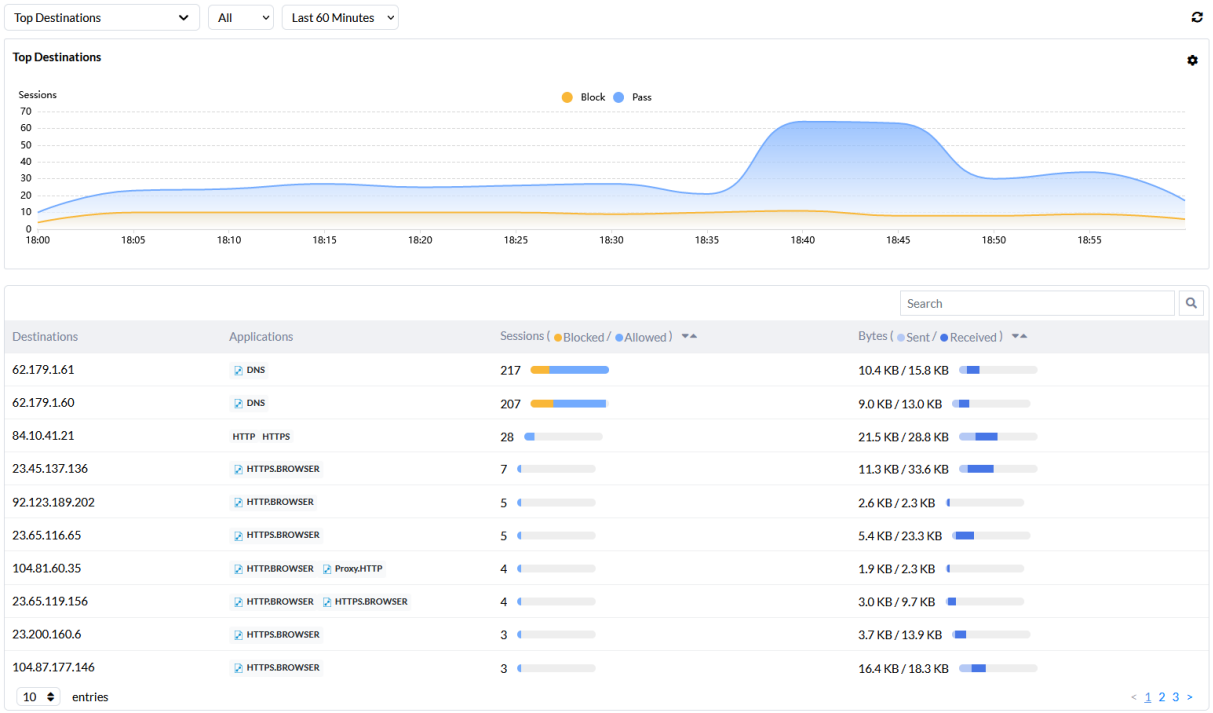


Okienko edycji umożliwia wybór spośród trzech różnych typów wykresów: tabelarycznego, słupkowego lub bąbelkowego. W przypadku wykresów słupkowych i bąbelkowych można wybrać 10, 15 lub 20 najpopularniejszych źródeł do wyświetlenia i posortować je według przepustowości, sesji lub wartości zagrożenia.

Top Destinations

Karta *Top Destinations* w obszarze *Insights* > *Monitors* wyświetla najważniejsze miejsca docelowe z ostatniego ruchu sieciowego według pasma lub liczby sesji.

Poniższy rysunek przedstawia kartę *Top Destinations*:

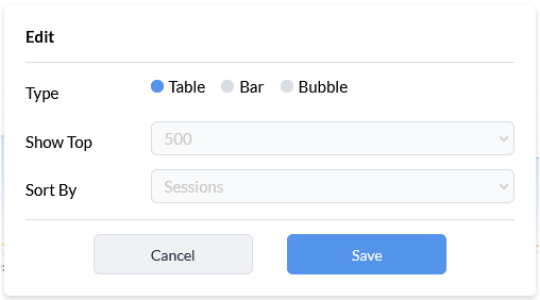


Panel wyświetla docelowy adres IP, nazwę aplikacji, liczbę sesji (zablokowane i dozwolone) oraz wielkość danych (wysłane i odebrane).

Po najechaniu kursorem na wykres można zobaczyć informacje o sesjach.

Aby edytować tabelę *Top Destinations* należy wybrać pozycję *Settings* (⚙) > *Edit.*

Poniższy rysunek przedstawia okienko edycji :

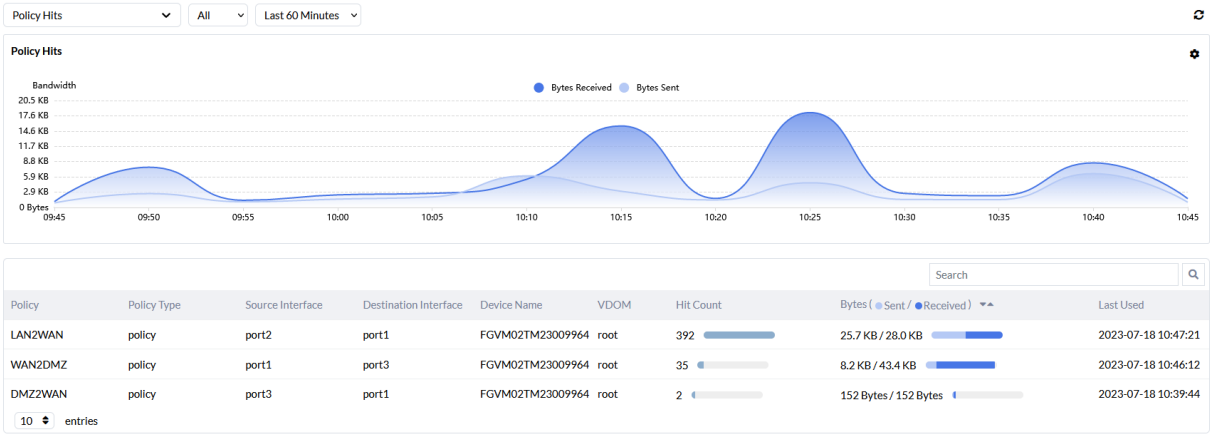


Okienko edycji umożliwia wybór spośród trzech różnych typów wykresów: tabelarycznego, słupkowego lub bąbelkowego. W przypadku wykresów słupkowych i bąbelkowych można wybrać 10, 15 lub 20 najbardziej znaczących adresów docelowych do wyświetlenia i posortować je według przepustowości lub sesji.

Policy Hits

Na karcie *Policy Hits* w obszarze *Insights* > *Monitors* wyświetlane są trafienia polityk z ostatniego ruchu.

Poniższy rysunek przedstawia kartę *Policy Hits*:

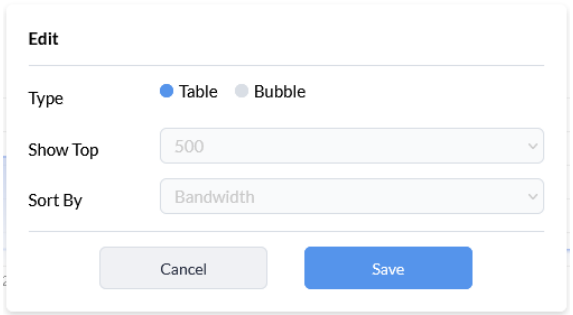


W panelu wyświetlane są następujące informacje:

- Nazwa polityki i jej rodzaj
- Interfejs źródłowy i docelowy
- Nazwa urządzenia
- VDOM
- Liczba trafień
- Bajty (wysłane i odebrane)
- Czas ostatniego trafienia (data i godzina)

Po najechaniu kursorem na wykres można zobaczyć informacje o liczbie przesłanych bajtów we wskazanej jednostce czasowej.

Aby edytować wykres *Policy Hits* należy wybrać pozycję *Settings* (⚙) > *Edit*. Poniższy rysunek przedstawia okienko edycji:

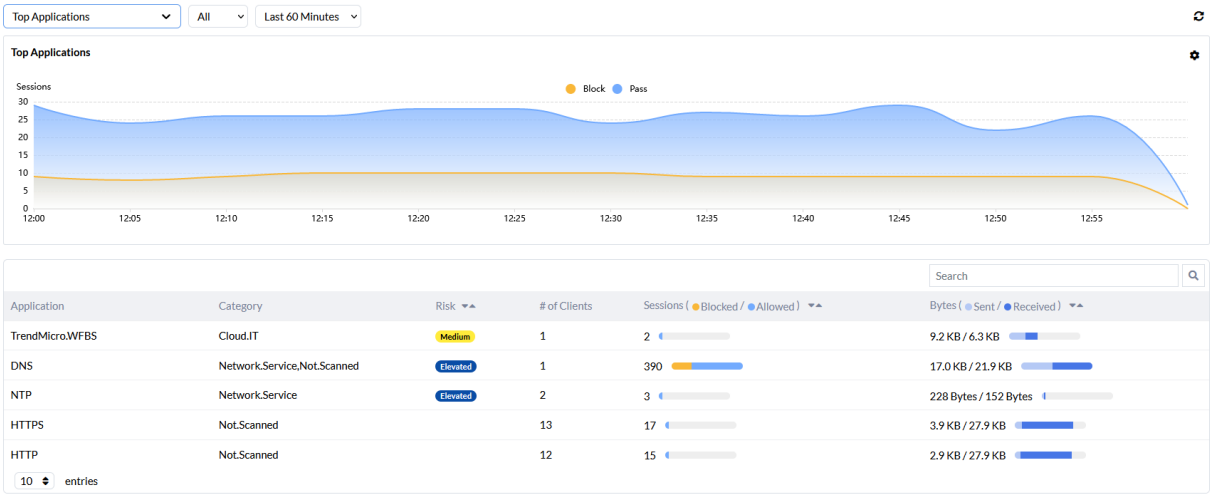


Okienko edycji umożliwia wybór typu wykresu tabelarycznego lub bąbelkowego. W przypadku wykresu bąbelkowego można wybrać 10, 15 lub 20 najczęściej wykorzystywanych polityk do wyświetlenia i posortować je według przepustowości lub liczby wystąpień.

Top Applications

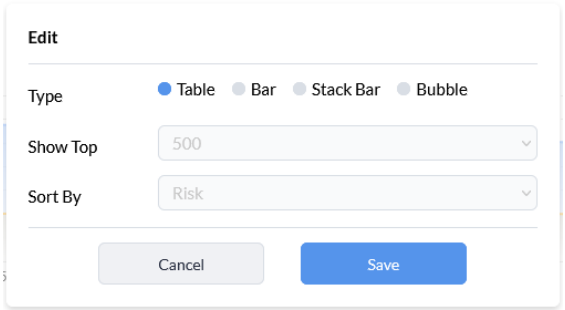
Na karcie *Top Applications* w obszarze *Insights* > *Monitors* są wyświetlane najczęściej wykorzystywane w sieci aplikacje. Wyświetlane są: nazwa aplikacji, kategoria, poziom ryzyka, liczba klientów, liczba sesji (zablokowane i dozwolone) oraz ilość przesłanych danych (wysłane i odebrane).

Poniższy rysunek przedstawia zakładkę *Top Applications*:



Po najechaniu kursorem na wykres można zobaczyć informacje o liczbie sesji we wskazanej jednostce czasowej.

Aby edytować tabelę *Top Application* należy wybrać pozycję *Settings* (⚙) > *Edit.* Poniższy rysunek przedstawia okienko edycji:



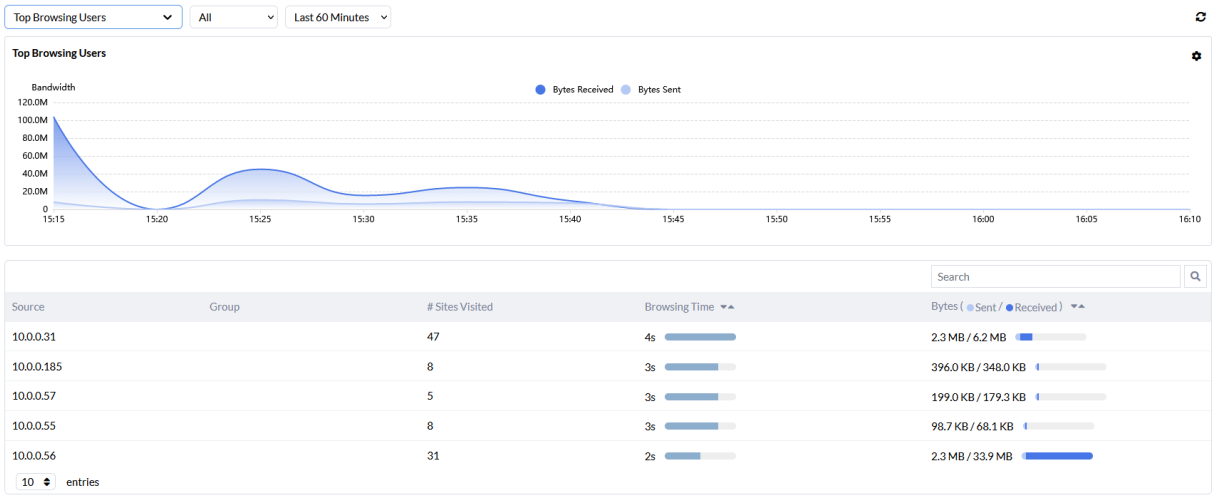
Okienko edycji umożliwia wybór spośród czterech różnych typów wykresów: tabelarycznego, słupkowego, słupkowego składanego lub bąbelkowego. W przypadku wykresów słupkowych i bąbelkowych można wybrać 10, 15 lub 20 najczęściej używanych aplikacji i posortować je według pasma, stopnia ryzyka lub liczby sesji.

Ponadto typ wykresu składanego umożliwia wybranie 5 lub 10 najczęściej używanych aplikacji oraz umożliwia sortowanie wyników według pasma lub liczby sesji.

Top Browsing Users

Na karcie *Top Browsing Users* w obszarze *Insights* > *Monitors* wyświetlane są informacje o użytkownikach najbardziej aktywnych pod względem przeglądania stron internetowych.

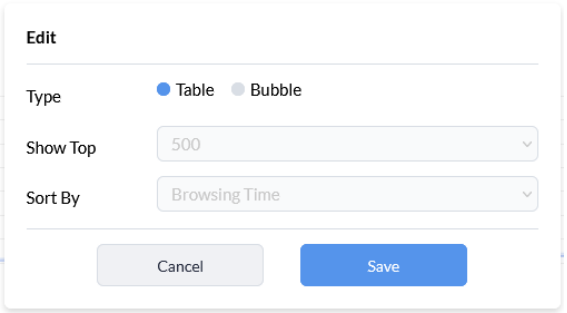
Poniższy rysunek przedstawia kartę *Top Browsing Users*:



Karta *Top Browsing Users* wyświetla źródło (adres lub nazwę), grupę do której przypisane jest źródło, liczbę odwiedzonych witryn, czas przeglądania i ilość przesłanych danych (wysłanych i odebranych).

Po najechaniu kursorem na wykres można zobaczyć informacje o ilości przesłanych danych we wskazanej jednostce czasowej.

Aby edytować tabelę *Top Browsing Users* należy wybrać pozycję *Settings* (⚙) > *Edit.* Poniższy rysunek przedstawia okienko edycji:

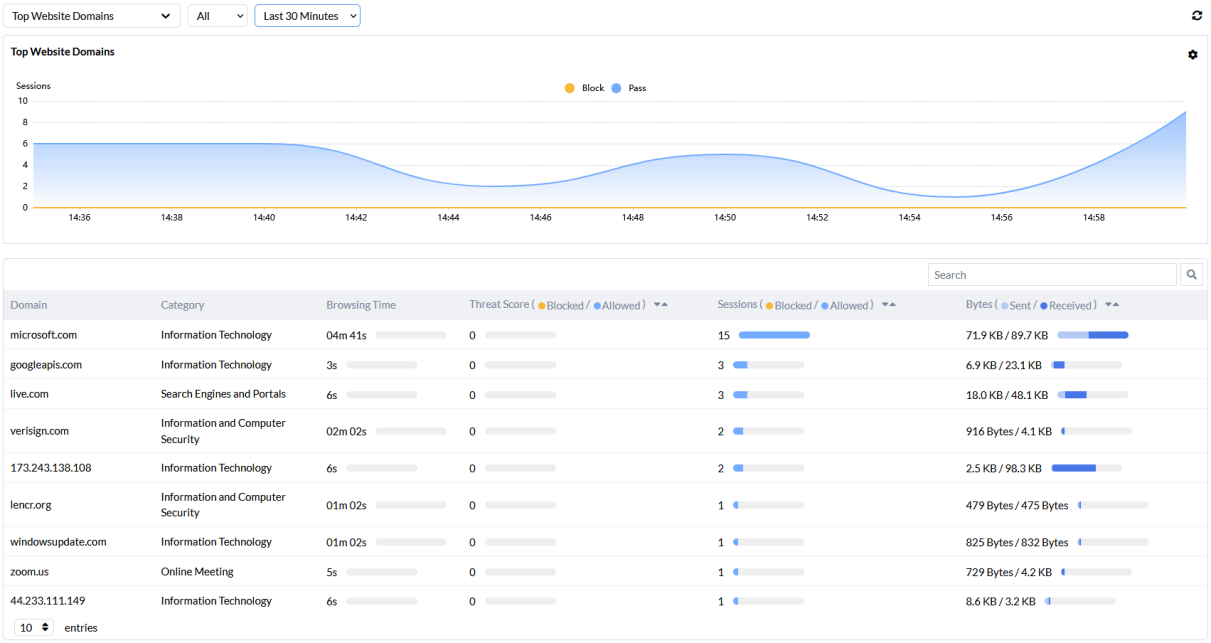


Okienko edycji umożliwia wybór typu wykresu tabelarycznego lub bąbelkowego. W przypadku wykresu bąbelkowego można wybrać 10, 15 lub 20 najbardziej aktywnych użytkowników do wyświetlenia i posortować ich według czasu przeglądania lub ilości przesłanych danych.

Top Website Domains

Na karcie *Top Website Domains* w sekcji *Insights* > *Monitors* są wyświetlane domeny witryn internetowych najczęściej odwiedznych w wybranym przedziale czasu.

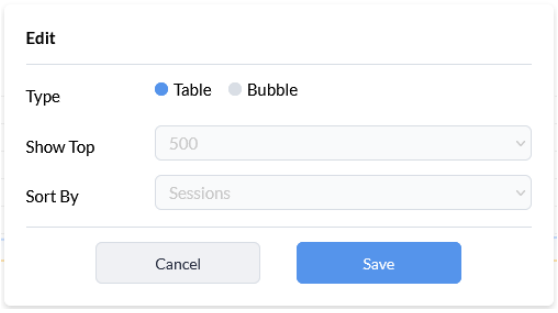
Poniższy rysunek przedstawia zakładkę *Top Website Domains*:



Karta *Top Website Domains* wyświetla nazwę domeny, kategorię, czas przeglądania, ocenę zagrożenia, liczbę sesji i ilość przesłanych danych.

Po najechaniu kursorem na wykres można zobaczyć informacje o liczbie sesji we wskazanej jednostce czasowej.

Aby edytować tabelę *Top Website Domains* należy wybrać pozycję *Settings* (⚙) > *Edit.* Poniższy rysunek przedstawia okienko edycji:



Okienko edycji umożliwia wybór typu wykresu tabelarycznego lub bąbelkowego. W przypadku wykresu bąbelkowego można wybrać 10, 15 lub 20 najczęściej odwiedzanych domen i posortować je liczby przesłanych danych, liczby sesji lub wskaźnika zagrożenia.

VPN

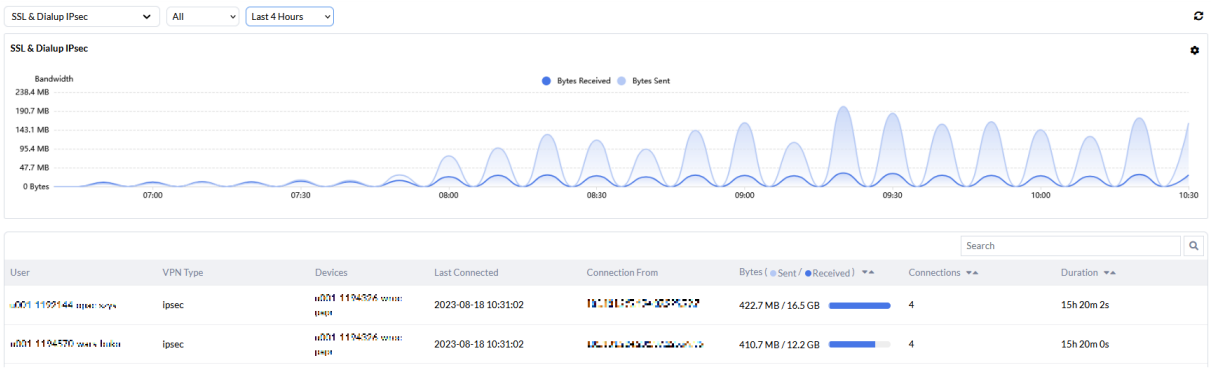
Karty *SSL & Dialup IPsec* i *Site-to-Site IPsec* w menu *Insights* > *Monitors* wyświetlają informacje związane z VPN, umożliwiając użytkownikom monitorowanie połączeń SSL & Dialup IPSec i Site-to-Site IPSec.

Na tej karcie można zobaczyć następujące szczegóły:

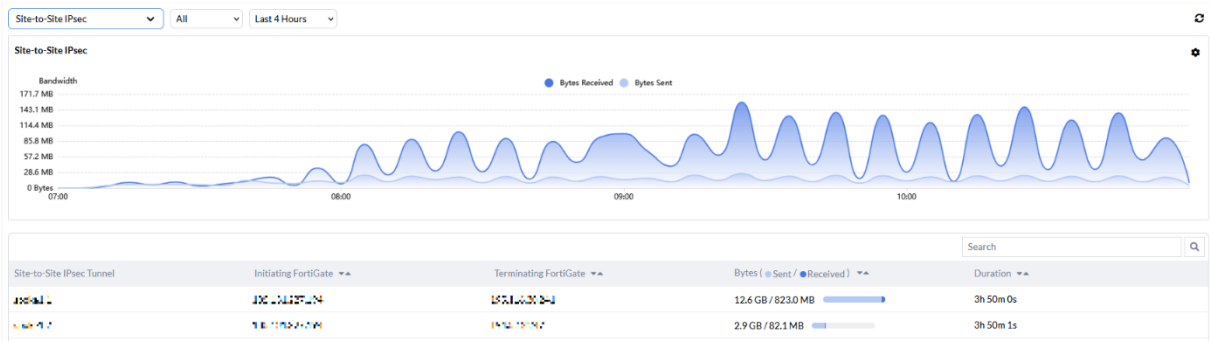
- Użytkownicy VPN
- Czas połączenia
- Lokalizacja połączeń
- Czas trwania połączeń Aby otworzyć widok VPN:

1. Przejdź do Insights > Monitors.
2. Z rozwijanego menu u góry, w sekcji *VPN* wybierz *SSL & Dialup IPsec* lub *Site-to-Site IPsec*. Poniższe rysunki pokazują przykładowe widoki VPN:

SSL & Dialup IPsec



Site to Site IPsec



Po najechaniu kursorem na wykres można zobaczyć informacje o ilości przesłanych danych we wskazanej jednostce czasowej.

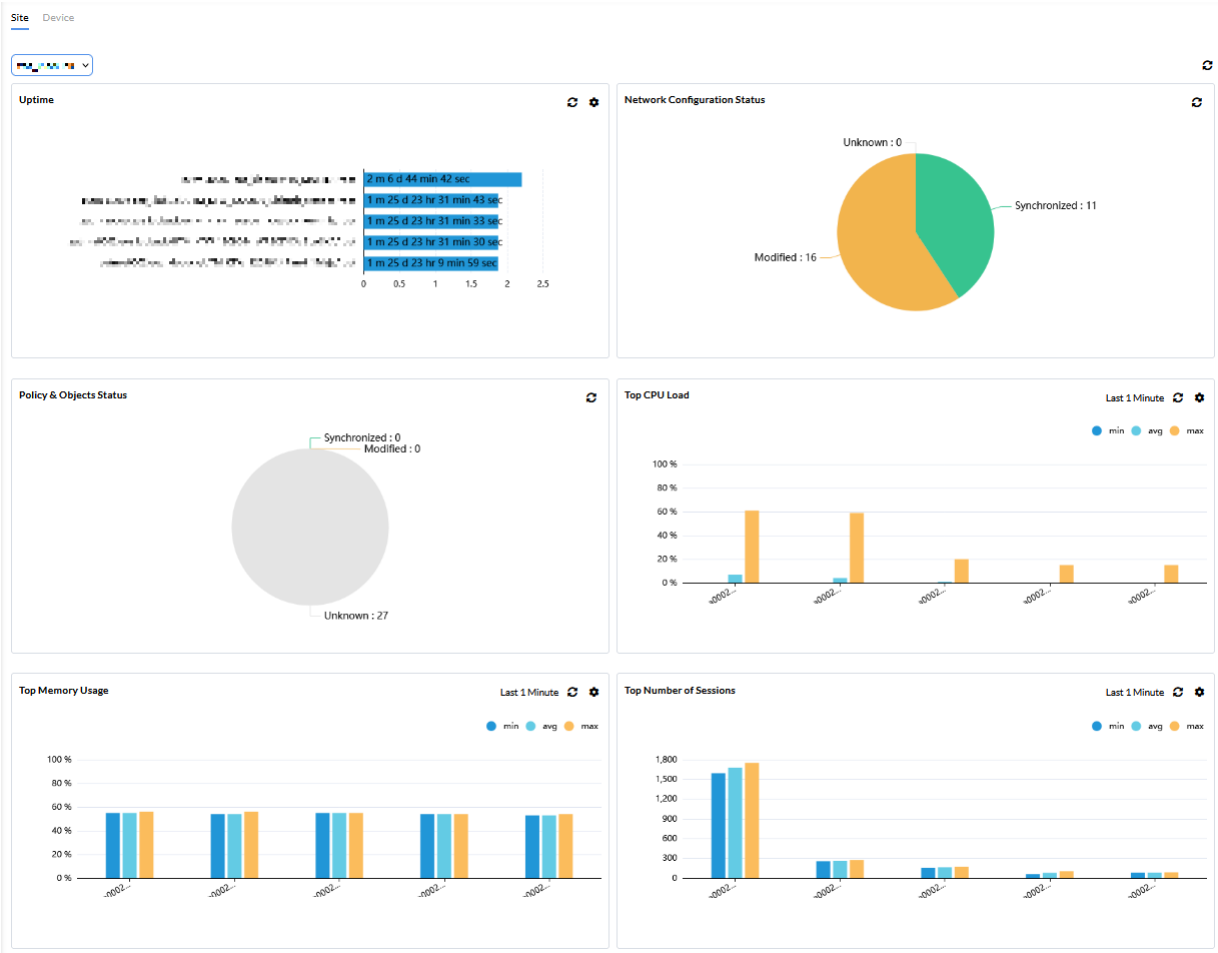
Health

Karta *Health* wyświetla podsumowanie stanu zarządzanych urządzeń, za pomocą tej karty można uzyskać dostęp do informacji o kondycji urządzenia.

Karta zawiera widok monitorowania urządzeń dla wybranej lokalizacji.

Domyślnie wybrany jest widok *Site*.

Karta *Health* wygląda następująco:



Jak pokazano na rysunku, karta *Health* jest zorganizowana jako zestaw widżetów.

Dostępne są następujące widżety:

- *Uptime* - czas pracy
- *Network Configuration Status* - stan konfiguracji sieci
- *Policy & Objects Status* - stan polityk i obiektów
- *Top CPU Load* - największe obciążenie procesora
- *Top Memory Usage* - największe wykorzystanie pamięci
- *Top Number of Sessions* - największa liczba sesji Widok *Device* wyświetla następujące widżety:
- *Bandwith* - wyświetla wykresy przepustowości dla urządzeń nieobsługujących SD-WAN. Możesz wyświetlić przepustowość dla poszczególnych interfejsów wraz z opcjami wyboru danych historycznych, takich jak ostatnie 60 minut, ostatni 1 dzień i ostatnie 7 dni.
- *Session* – wykres liczby jednoczesnych sesji
- *Session Rate* – wykres liczby nowych sesji na sekundę

Akcje karty

Na karcie *Health > Device* dostępne są następujące akcje:

- *View*: wybór rodzaju widoku (*Site* lub *Device*).
- *Scope*: wybór oddziału (*Site*) lub urządzenia (*Device*) w zależności od wybranego widoku.
- *Refresh*: odświeżenie danych.

Akcje widgetów

Górny baner każdego widżetu zawiera niektóre lub wszystkie z następujących elementów sterujących:

- *Interface*: wybór interfejsu.
- *Filter*: filtrowanie danych (wg czasu)
- *Refresh*: odświeżanie danych.
- *action*: edytowanie widżetu.

Należy najechać kursorem na widżety, aby zobaczyć dodatkowe informacje.

Kliknięcie niektórych widżetów otwiera widok tabeli z powiązanymi informacjami.

Logi

Karta *Logs* wyświetla dzienniki zdarzeń bezpieczeństwa. Zawiera filtry i elementy sterujące, które umożliwiają wybieranie i filtrowanie logów.

Można także przejść do szczegółów i wyświetlić powiązany zestaw logów.

Dostępne są następujące opcje i przyciski akcji:

- *Log type:* rodzaje logów:
    - *Traffic* – logi ruchowe
    - Intrusion Prevention – logi usługi IPS
    - *Sandbox* – logi usługi Sandbox
    - *Antivirus* – logi usługi AV
    - *DNS* – logi usługi filtrowania zapytań DNS
    - *Application Control* – logi usługi kontroli aplikacji
    - *Web Filter* – logi usługi filtrowania stron internetowych
    - *Event* – logi zawierające zdarzenia systemowe
- *Scope*: filtrowanie danych dla wybranych lub wszystkich oddziałów.
- *Set Filter*: filtrowanie danych (wg czasu)
- *Export to CSV*: eksportowanie danych do pliku CSV
- *Refresh*: odświeżanie danych
- *Add Filter*: Dodawanie filtra w celu zawężenia wyszukiwania

Można kliknąć dwukrotnie pole w dowolnej tabeli, aby dodać to pole jako filtr. Można łączyć wiele filtrów, aby zawęzić wyszukiwanie.

- *Settings*: otwiera okno dialogowe *Column Settings* . Można wybrać kolumny z listy do wyświetlenia
- *Sort*: sortowanie danych w porządku rosnącym lub malejącym

Lista rozwijana na dole pozwala wybrać liczbę wpisów do wyświetlenia na stronie.

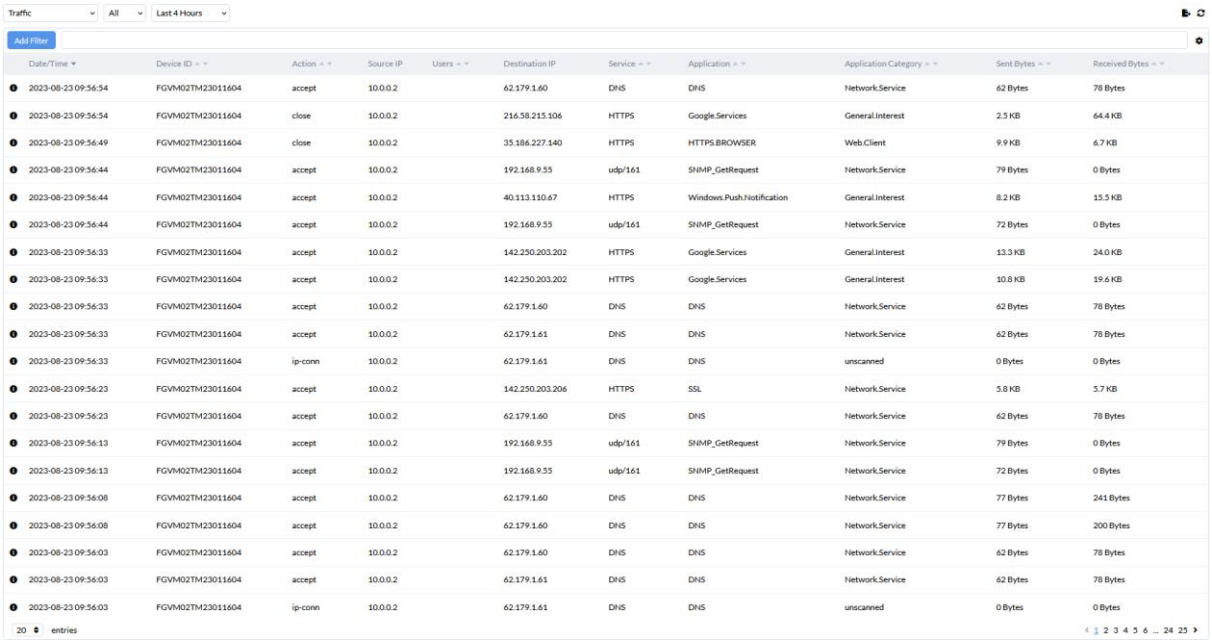
Można użyć przycisków < i > w prawym dolnym rogu do nawigacji po stronie lub można bezpośrednio wybrać numer strony.

Kolejne zakładki udostępniają różne widoki danych.

Traffic

Karta *Traffic* w obszarze *Insights* > *Logs* wyświetla logi dotyczące połączeń sieciowych.

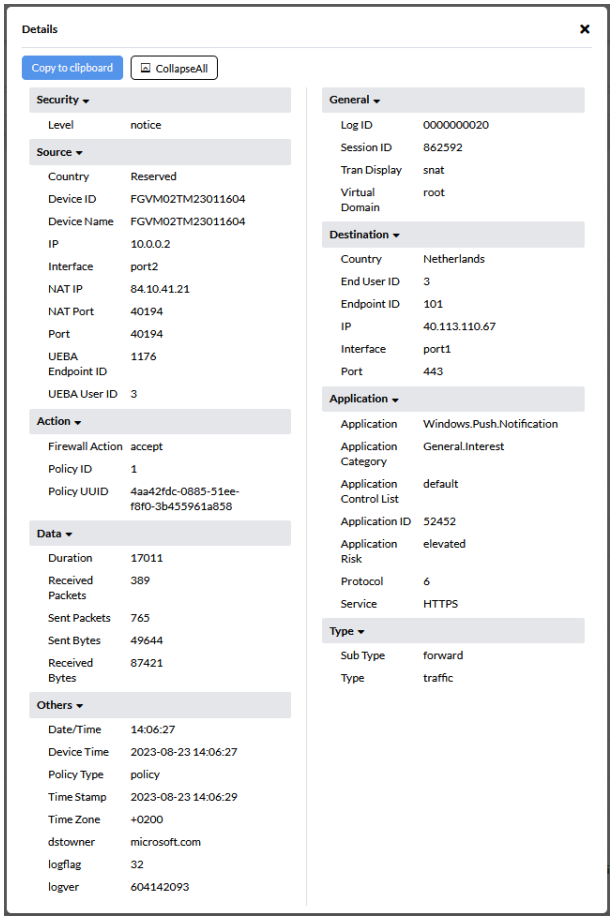
Poniższy rysunek przedstawia przykład zakładki *Traffic*:



Aby zastosować filtr należy kliknąć *Add Filter*. Następnie z rozwijanej listy należy wybrać dostępne kryterium do filtrowania i wprowadzić szczegóły w wyświetlonym polu. Można dodać wiele filtrów, aby zawęzić wyszukiwanie. Alternatywnie można kliknąć dwukrotnie pole, aby dodać jego wartość jako filtr.

Aby zmienić listę wyświetlanych kolumn należy kliknąć ikonę *Column Settings* (⚙) po prawej stronie panelu i zaznaczyć wybrane kolumny.

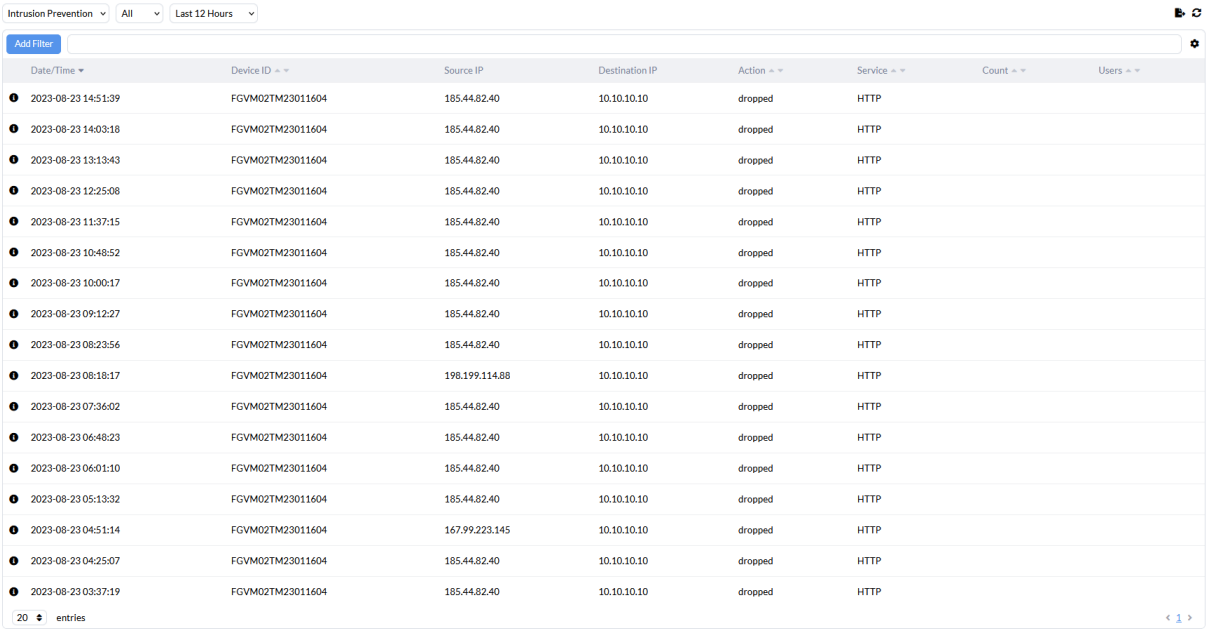
Aby wyświetlić więcej szczegółów dotyczących wybranego zapisu należy kliknąć ikonę *Click to show details* (ℹ).



Intrusion Prevention

Karta *Intrusion Prevention* w obszarze *Insights* > *Logs* wyświetla logi zdarzeń wykrytych przez usługę IPS.

Poniższy rysunek przedstawia przykładową kartę *Intrusion Prevention*:

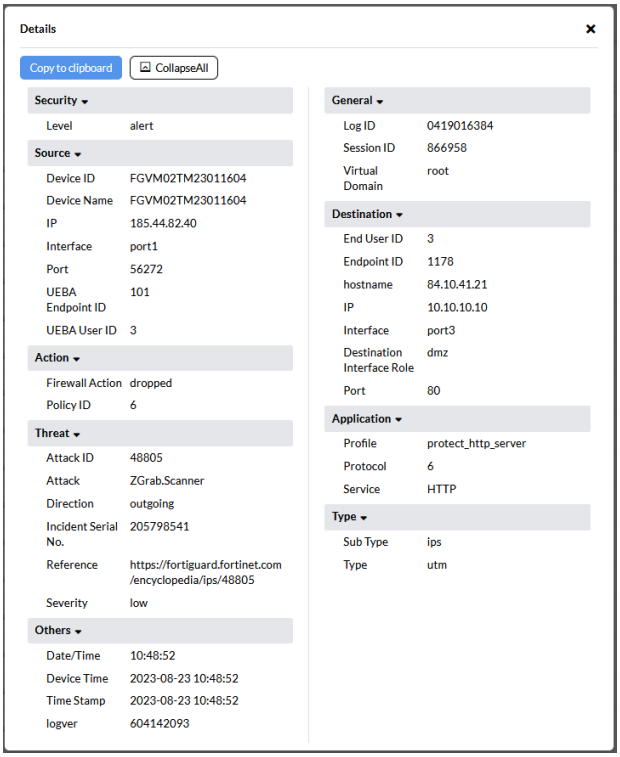


Aby zastosować filtr należy kliknąć *Add Filter*. Następnie z rozwijanej listy należy wybrać dostępne kryterium do filtrowania i wprowadzić szczegóły w wyświetlonym polu. Można

dodać wiele filtrów, aby zawęzić wyszukiwanie. Alternatywnie można kliknąć dwukrotnie pole, aby dodać jego wartość jako filtr.

Aby zmienić listę wyświetlanych kolumn należy kliknąć ikonę *Column Settings* (⚙) po prawej stronie panelu i zaznaczyć wybrane kolumny.

Aby wyświetlić więcej szczegółów dotyczących wybranego zapisu należy kliknąć ikonę *Click to show details* (ℹ).



Sandbox

Karta *Sandbox* w obszarze *Insights* > *Logs* wyświetla logi zdarzeń wykrytych przez usługę Sandbox (usługa opcjonalna).

Aby zastosować filtr należy kliknąć *Add Filter*. Następnie z rozwijanej listy należy wybrać dostępne kryterium do filtrowania i wprowadzić szczegóły w wyświetlonym polu. Można dodać wiele filtrów, aby zawęzić wyszukiwanie. Alternatywnie można kliknąć dwukrotnie pole, aby dodać jego wartość jako filtr.

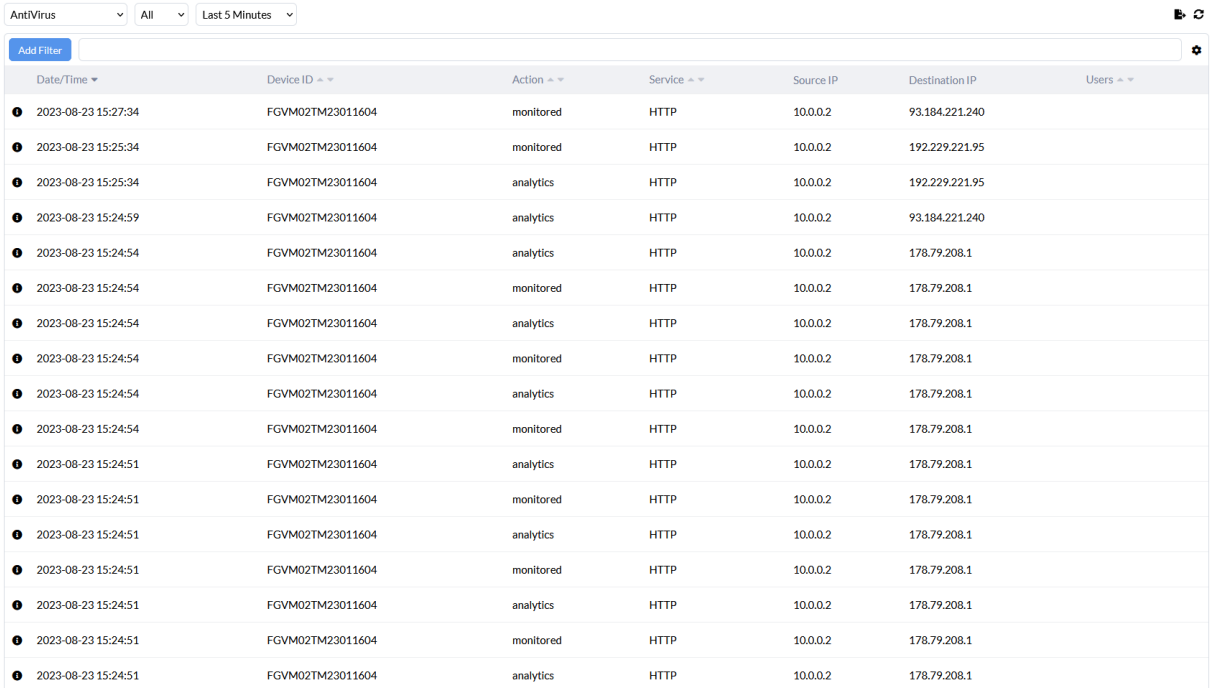
Aby zmienić listę wyświetlanych kolumn należy kliknąć ikonę *Column Settings* (⚙) po prawej stronie panelu i zaznaczyć wybrane kolumny.

Aby wyświetlić więcej szczegółów dotyczących wybranego zapisu należy kliknąć ikonę *Click to show details* (ℹ).

Antivirus

Karta *Antivirus* w obszarze *Insights* > *Logs* wyświetla dzienniki zdarzeń wykrytych przez usługę antywirusową.

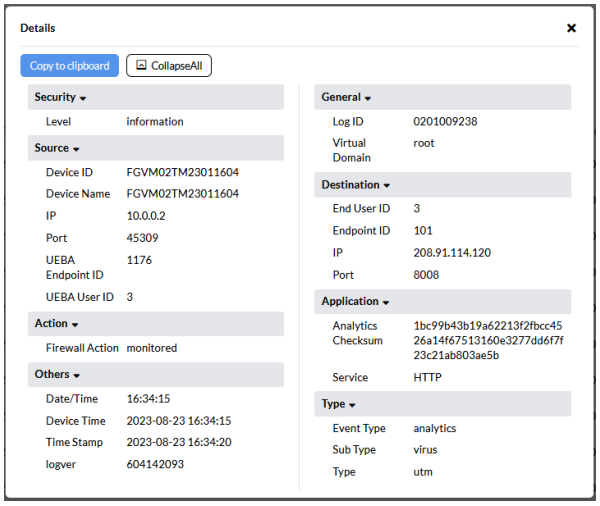
Poniższy rysunek przedstawia przykładową zakładkę *Antivirus*:



Aby zastosować filtr należy kliknąć *Add Filter*. Następnie z rozwijanej listy należy wybrać dostępne kryterium do filtrowania i wprowadzić szczegóły w wyświetlonym polu. Można dodać wiele filtrów, aby zawęzić wyszukiwanie. Alternatywnie można kliknąć dwukrotnie pole, aby dodać jego wartość jako filtr.

Aby zmienić listę wyświetlanych kolumn należy kliknąć ikonę *Column Settings* (⚙) po prawej stronie panelu i zaznaczyć wybrane kolumny.

Aby wyświetlić więcej szczegółów dotyczących wybranego zapisu należy kliknąć ikonę *Click to show details* (ℹ).



DNS

Karta *DNS* w obszarze *Insights* > *Logs* wyświetla dzienniki zdarzeń dla usługi filtracji zapytań DNS.

Aby zastosować filtr należy kliknąć *Add Filter*. Następnie z rozwijanej listy należy wybrać dostępne kryterium do filtrowania i wprowadzić szczegóły w wyświetlonym polu. Można dodać wiele filtrów, aby zawęzić wyszukiwanie. Alternatywnie można kliknąć dwukrotnie pole, aby dodać jego wartość jako filtr.

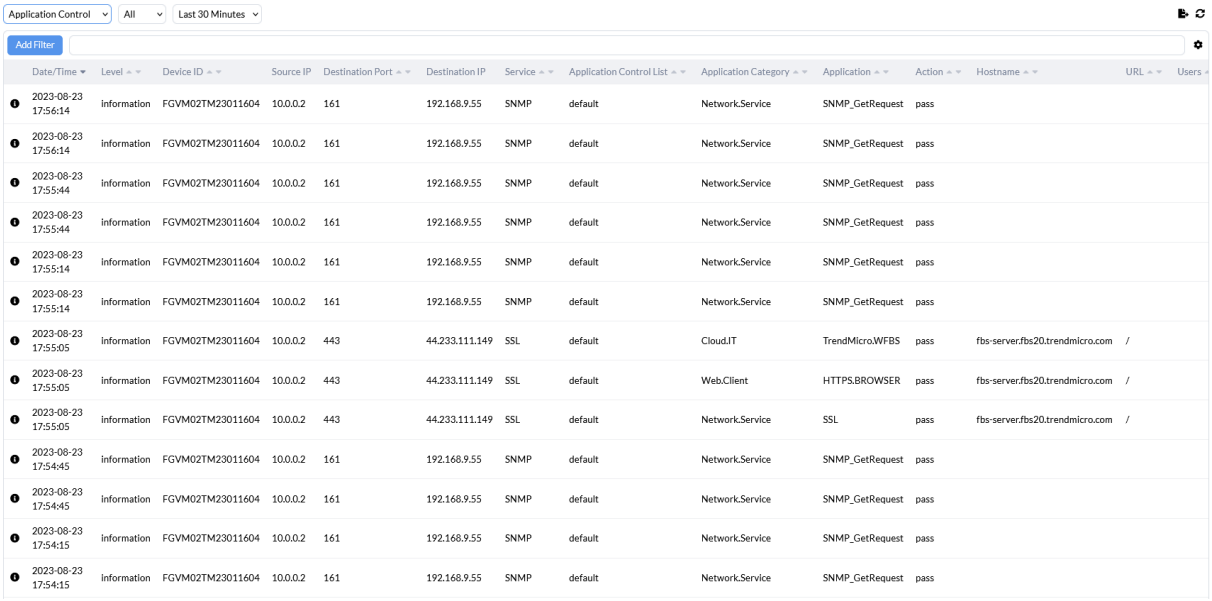
Aby zmienić listę wyświetlanych kolumn należy kliknąć ikonę *Column Settings* (⚙) po prawej stronie panelu i zaznaczyć wybrane kolumny.

Aby wyświetlić więcej szczegółów dotyczących wybranego zapisu należy kliknąć ikonę *Click to show details* (ℹ).

Application Controll

Karta *Application Controll* w obszarze *Insights* > *Logs* wyświetla logi dla usługi kontroli aplikacji.

Poniższy rysunek przedstawia przykładową zakładkę *Application Controll* :



Date/Time	Level	Device ID	Source IP	Destination Port	Destination IP	Service	Application Control List	Application Category	Application	Action	Hostname	URL	Users
2023-08-23 17:56:14	information	FGVM02TM23011604	10.0.0.2	161	192.168.9.55	SNMP	default	Network.Service	SNMP_GetRequest	pass			
2023-08-23 17:56:14	information	FGVM02TM23011604	10.0.0.2	161	192.168.9.55	SNMP	default	Network.Service	SNMP_GetRequest	pass			
2023-08-23 17:55:44	information	FGVM02TM23011604	10.0.0.2	161	192.168.9.55	SNMP	default	Network.Service	SNMP_GetRequest	pass			
2023-08-23 17:55:44	information	FGVM02TM23011604	10.0.0.2	161	192.168.9.55	SNMP	default	Network.Service	SNMP_GetRequest	pass			
2023-08-23 17:55:14	information	FGVM02TM23011604	10.0.0.2	161	192.168.9.55	SNMP	default	Network.Service	SNMP_GetRequest	pass			
2023-08-23 17:55:14	information	FGVM02TM23011604	10.0.0.2	161	192.168.9.55	SNMP	default	Network.Service	SNMP_GetRequest	pass			
2023-08-23 17:55:05	information	FGVM02TM23011604	10.0.0.2	443	44.233.111.149	SSL	default	Cloud.IT	TrendMicro.WFBS	pass	fbs-server.fbs20.trendmicro.com	/	
2023-08-23 17:55:05	information	FGVM02TM23011604	10.0.0.2	443	44.233.111.149	SSL	default	Web.Client	HTTPS.BROWSER	pass	fbs-server.fbs20.trendmicro.com	/	
2023-08-23 17:55:05	information	FGVM02TM23011604	10.0.0.2	443	44.233.111.149	SSL	default	Network.Service	SSL	pass	fbs-server.fbs20.trendmicro.com	/	
2023-08-23 17:54:45	information	FGVM02TM23011604	10.0.0.2	161	192.168.9.55	SNMP	default	Network.Service	SNMP_GetRequest	pass			
2023-08-23 17:54:45	information	FGVM02TM23011604	10.0.0.2	161	192.168.9.55	SNMP	default	Network.Service	SNMP_GetRequest	pass			
2023-08-23 17:54:15	information	FGVM02TM23011604	10.0.0.2	161	192.168.9.55	SNMP	default	Network.Service	SNMP_GetRequest	pass			
2023-08-23 17:54:15	information	FGVM02TM23011604	10.0.0.2	161	192.168.9.55	SNMP	default	Network.Service	SNMP_GetRequest	pass			

Aby zastosować filtr należy kliknąć *Add Filter*. Następnie z rozwijanej listy należy wybrać dostępne kryterium do filtrowania i wprowadzić szczegóły w wyświetlonym polu. Można dodać wiele filtrów, aby zawęzić wyszukiwanie. Alternatywnie można kliknąć dwukrotnie pole, aby dodać jego wartość jako filtr.

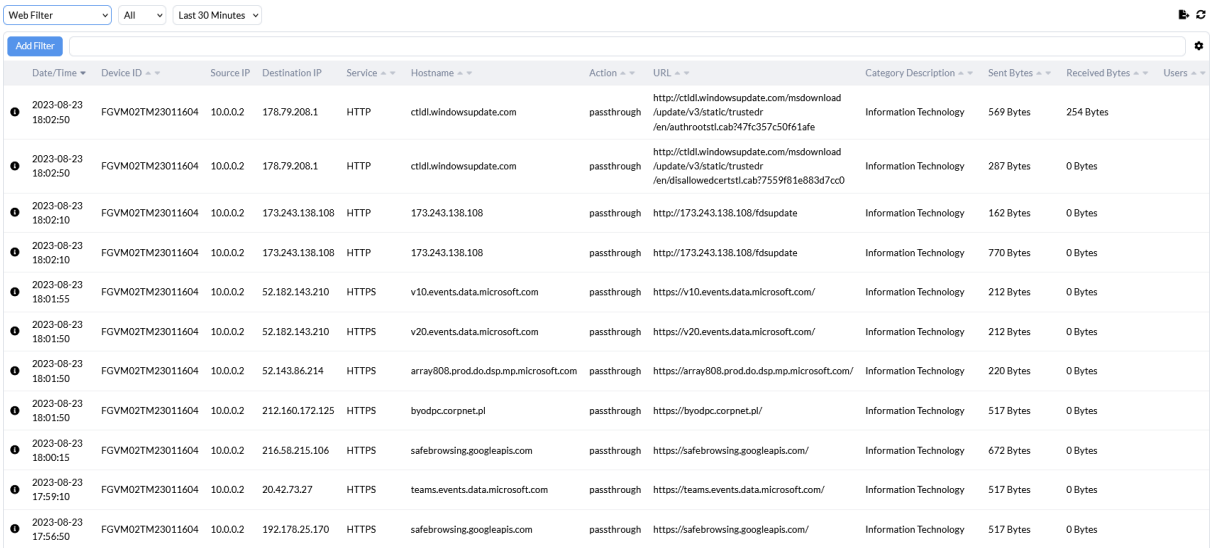
Aby zmienić listę wyświetlanych kolumn należy kliknąć ikonę *Column Settings* (⚙) po prawej stronie panelu i zaznaczyć wybrane kolumny.

Aby wyświetlić więcej szczegółów dotyczących wybranego zapisu należy kliknąć ikonę *Click to show details* (ℹ).

Web Filter

Karta *Web Filter* w obszarze *Insights* > *Logs* wyświetla logi dla usługi filtrowania stron internetowych.

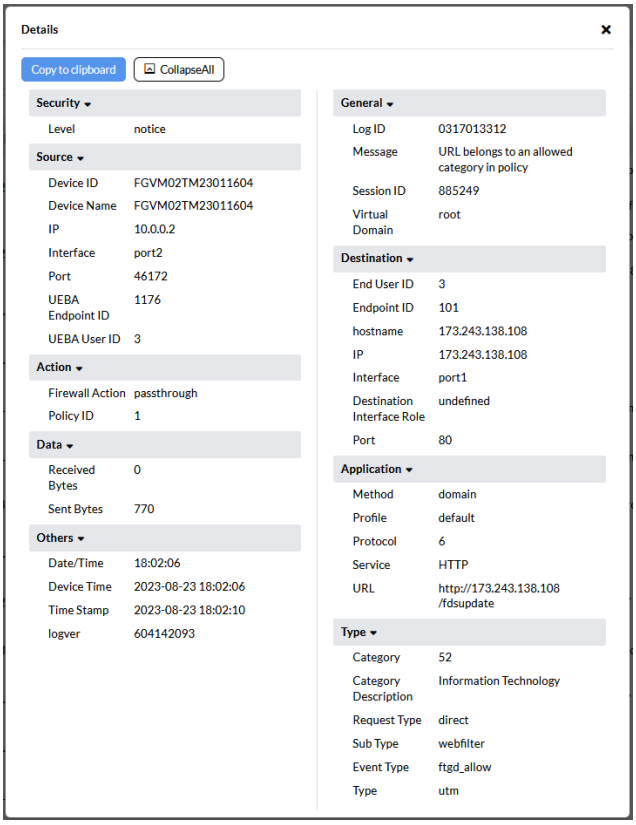
Poniższy rysunek przedstawia przykład karty *Web Filter*:



Aby zastosować filtr należy kliknąć *Add Filter*. Następnie z rozwijanej listy należy wybrać dostępne kryterium do filtrowania i wprowadzić szczegóły w wyświetlonym polu. Można dodać wiele filtrów, aby zawęzić wyszukiwanie. Alternatywnie można kliknąć dwukrotnie pole, aby dodać jego wartość jako filtr.

Aby zmienić listę wyświetlanych kolumn należy kliknąć ikonę *Column Settings* (⚙) po prawej stronie panelu i zaznaczyć wybrane kolumny.

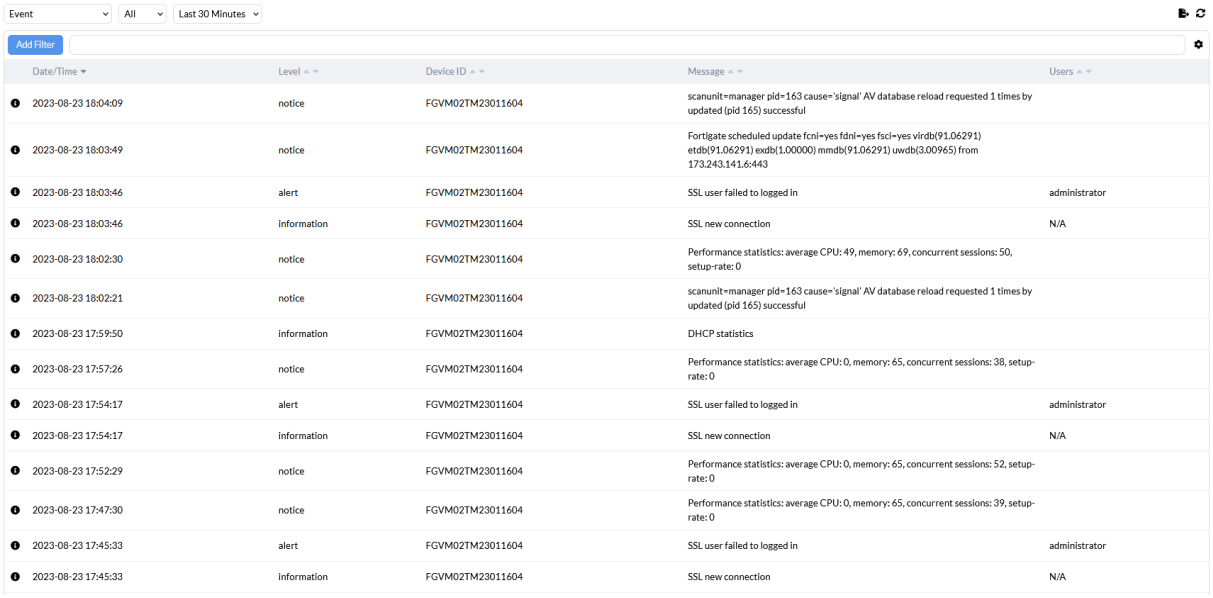
Aby wyświetlić więcej szczegółów dotyczących wybranego zapisu należy kliknąć ikonę *Click to show details* ( ).



Event

Karta *Event* w obszarze *Insights* > *Logs* wyświetla logi dotyczące zdarzeń systemowych.

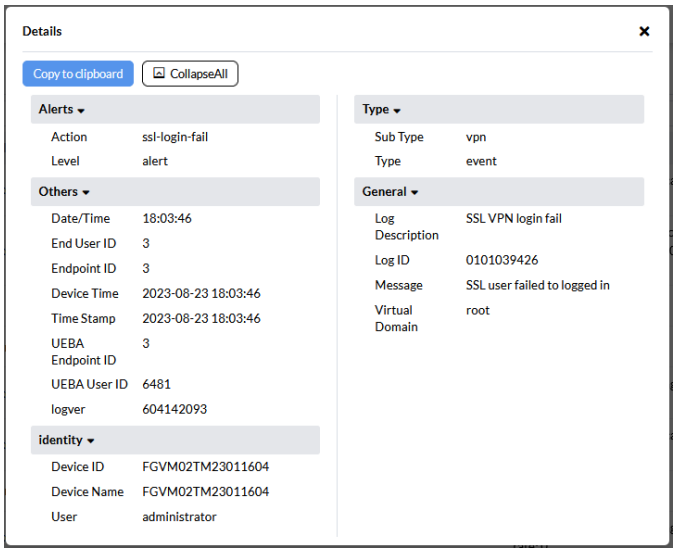
Poniższy rysunek przedstawia przykład zakładki *Event*:



Aby zastosować filtr należy kliknąć *Add Filter*. Następnie z rozwijanej listy należy wybrać dostępne kryterium do filtrowania i wprowadzić szczegóły w wyświetlonym polu. Można dodać wiele filtrów, aby zawęzić wyszukiwanie. Alternatywnie można kliknąć dwukrotnie pole, aby dodać jego wartość jako filtr.

Aby zmienić listę wyświetlanych kolumn należy kliknąć ikonę *Column Settings* (⚙) po prawej stronie panelu i zaznaczyć wybrane kolumny.

Aby wyświetlić więcej szczegółów dotyczących wybranego zapisu należy kliknąć ikonę *Click to show details* (ℹ).



SD-WAN

Zakładka SD-WAN zapewnia dostęp do informacji i konfiguracji SD-WAN.

Dostępne są następujące zakładki:

Monitoring: Sprawdzenie wydajności interfejsów SD-WAN za pomocą zestawu widżetów, w tym monitorowanie urządzeń SD-WAN oparte na logach SD-WAN.

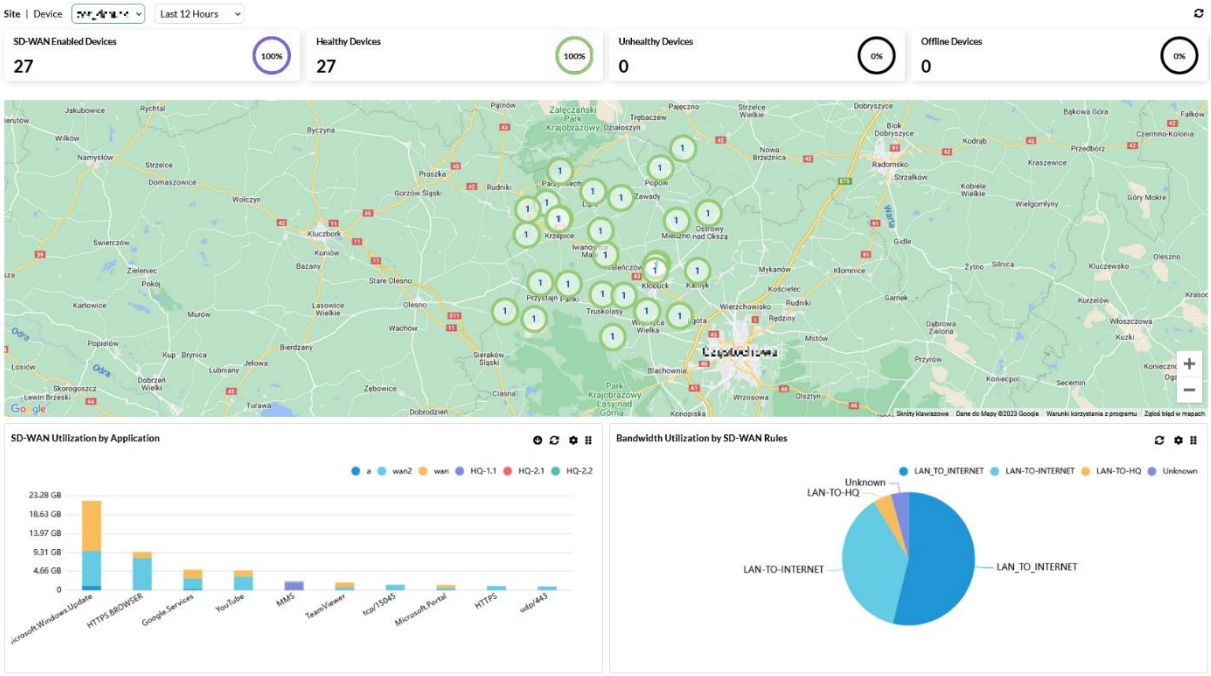
Configuration: przeglądanie i tworzenie szablonów SD-WAN, interfejsów powiązanych i reguł SD WAN.

Monitoring

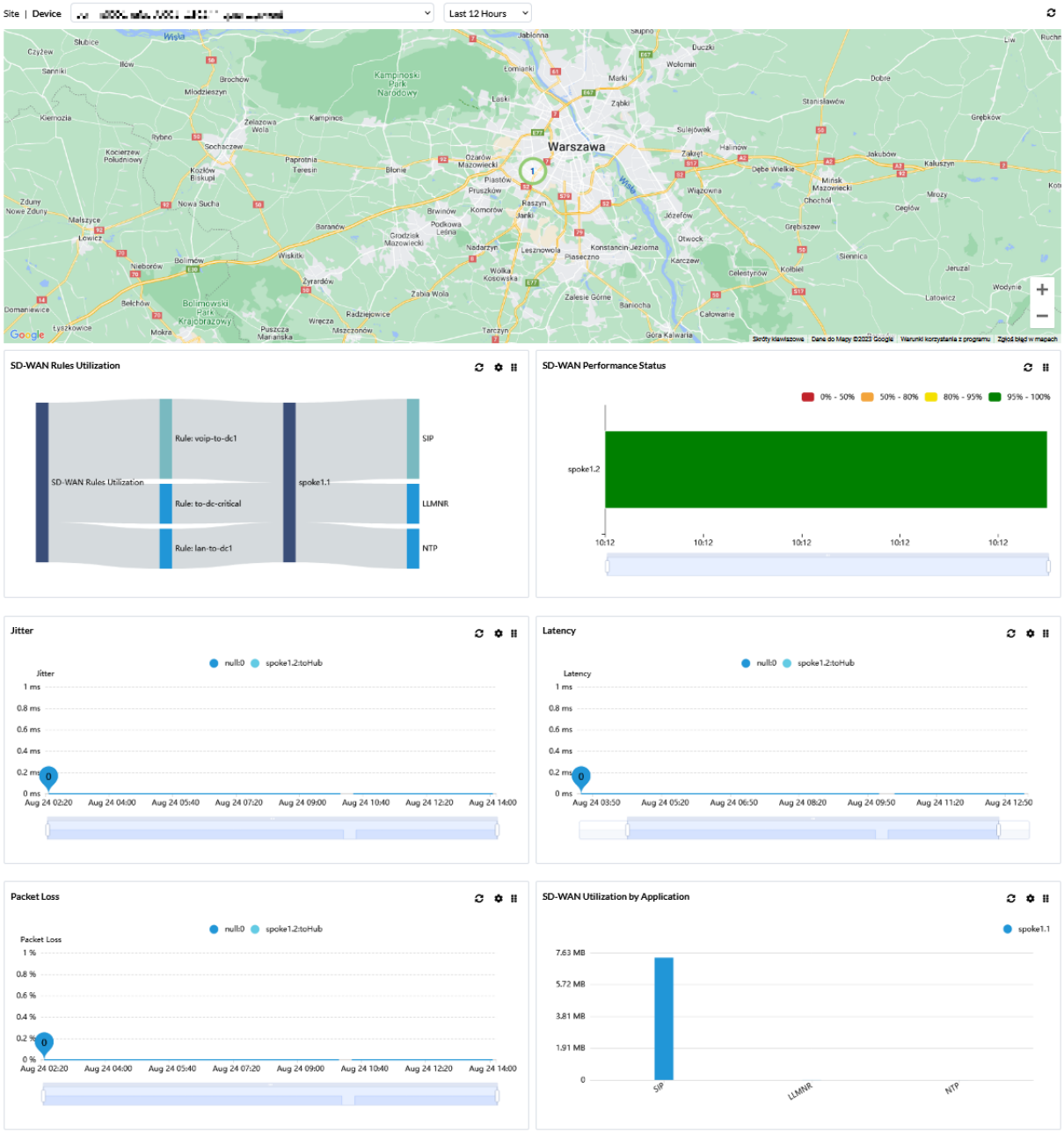
Karta *Monitoring* w menu *SD-WAN* konsoliduje informacje związane z SD-WAN.

Domyślnie wybrany jest widok oddziału (*Site*).

Zakładka *SD-WAN > Monitoring* (widok *Site*) wygląda następująco:



Zakładka *SD-WAN > Monitoring* (widok *Device*) wygląda następująco:



Jak pokazano na rysunkach, zakładka *SD-WAN > Monitoring* jest zorganizowana jako zestaw widżetów.

U góry dostępne są następujące widżety:

- Urządzenia obsługujące SD-WAN (*SD-WAN Enabled Devices*)
- Urządzenia w dobrym stanie (*Healthy Devices*)
- Urządzenia w złym stanie (*Unhealthy Devices*)
- Urządzenia offline (*Offline Devices*)

Dostępne są następujące dodatkowe widżety:

- Wykorzystanie reguł SD-WAN (*SD-WAN Rules Utilization*)
- Stan wydajności SD-WAN (*SD-WAN Performance Status*)
- Stan łącza: wahania, opóźnienia i utrata pakietów (*Link Health*)

- Wykorzystanie SD-WAN dla aplikacji (*SD-WAN Utilization by Application*)
- Wykorzystanie przepustowości dla reguł SD-WAN (*Bandwidth Utilization by SD-WAN Rules*)
- Wykorzystanie łączy SD-WAN (*SD-WAN Link Utilization*)
- Incydenty SD-WAN kategorii High i Critical (*SD-WAN High and Critical Events*)

Akcje karty

Na zakładce *SD-WAN > Monitoring* dostępne są następujące akcje :

- *View*: wybór typu widoku (oddział lub urządzenie)
- *Scope*: wybór zakresu danych wyjściowych (wszystkie lub wybrany oddział)

  Opcja *Scope* jest dostępna tylko dla widoku oddziału

- *Device*: wybór urządzenia

  Opcja *Device* jest dostępna tylko w widoku urządzenia

- *Set Filter*: filtrowanie danych (wg czasu)

SD-WAN Status

Aby otworzyć okno *SD-WAN Status* zawierające informacje dotyczące wydajności urządzenia należy kliknąć wybrane urządzenie umieszczone na mapie w górnej części zakładki *SD-WAN > Monitoring*.

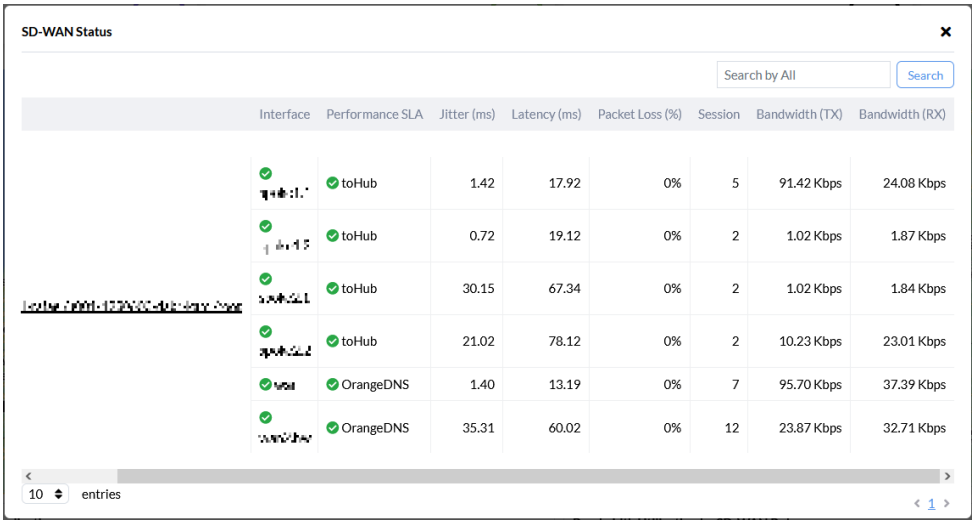
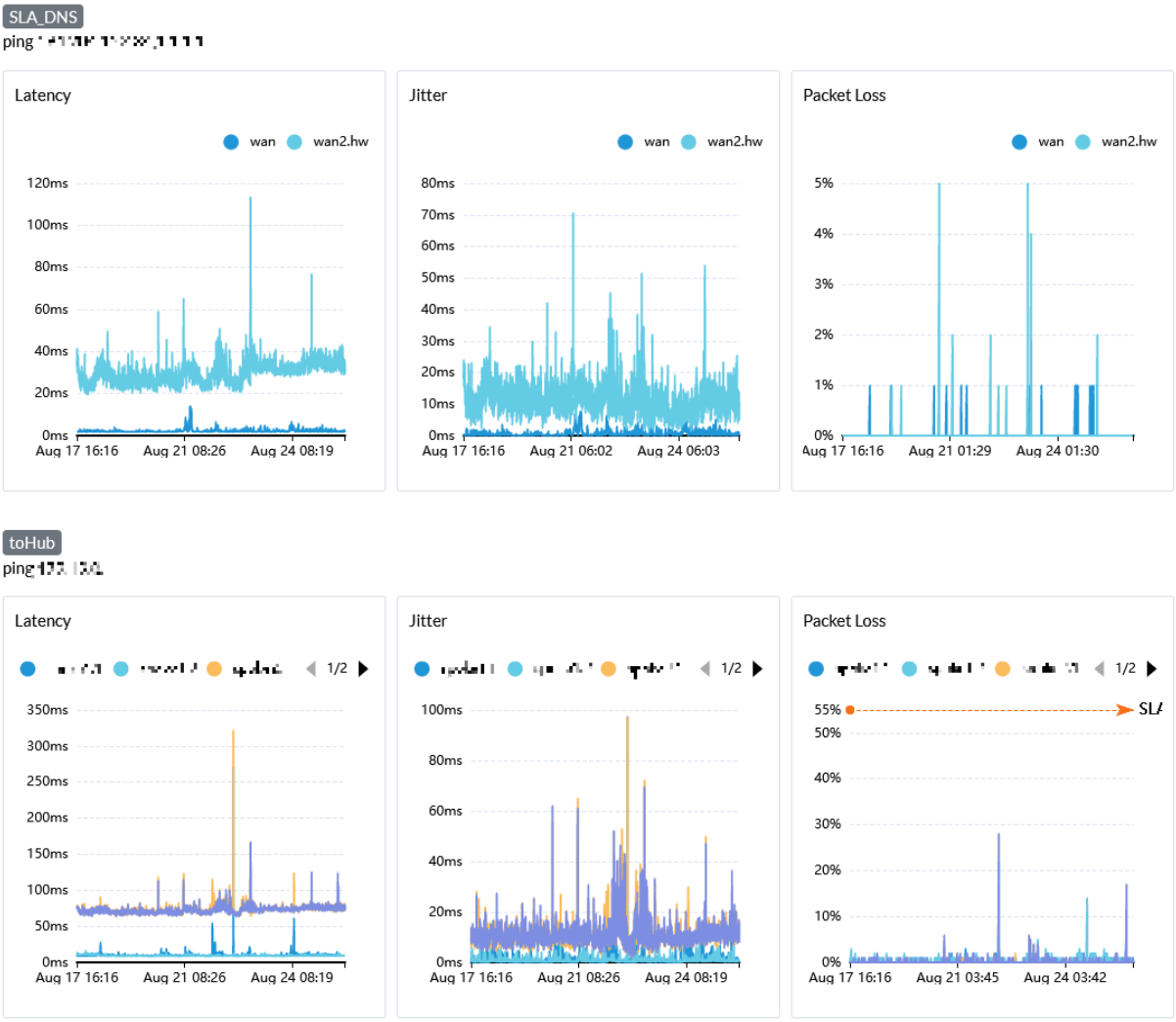


Tabela zawiera dane o jakości połączenia sieciowego z podziałem na interfejsy.

W oknie *SD-WAN Status* po wybraniu urządzenia można zobaczyć szczegółowe wykresy dla podstawowych parametrów określających jakość połączeń sieciowych.


Back / SD-WAN / Monitor /
Last 7 days
Summary
SD-WAN Interfaces
Traffic Overview
16.4 TB
13.6 TB
10.9 TB
8.2 TB
5.5 TB
2.7 TB
0 Bytes
Aug 17 16:18
Aug 19 06:03
Aug 20 19:47
Aug 22 09:34
Aug 23 19:46
Aug 24 11:26
Bandwidth Overview
Total
Sent (bps)
40 Mbps
30 Mbps
20 Mbps
10 Mbps
0 Kbps
Aug 17 16:18
Aug 18 16:47
Aug 19 17:18
Aug 20 17:47
Aug 21 18:15
Aug 22 18:46
Aug 23 17:46
Aug 24 06:06
Aug 24 13:14
Received (bps)
2 Mbps
2 Mbps
1 Mbps
900 Kbps
600 Kbps
300 Kbps
0 Kbps
Aug 17 16:18
Aug 18 16:55
Aug 19 17:34
Aug 20 18:11
Aug 21 18:47
Aug 22 19:26
Aug 23 18:10
Aug 24 06:34
Aug 24 13:30

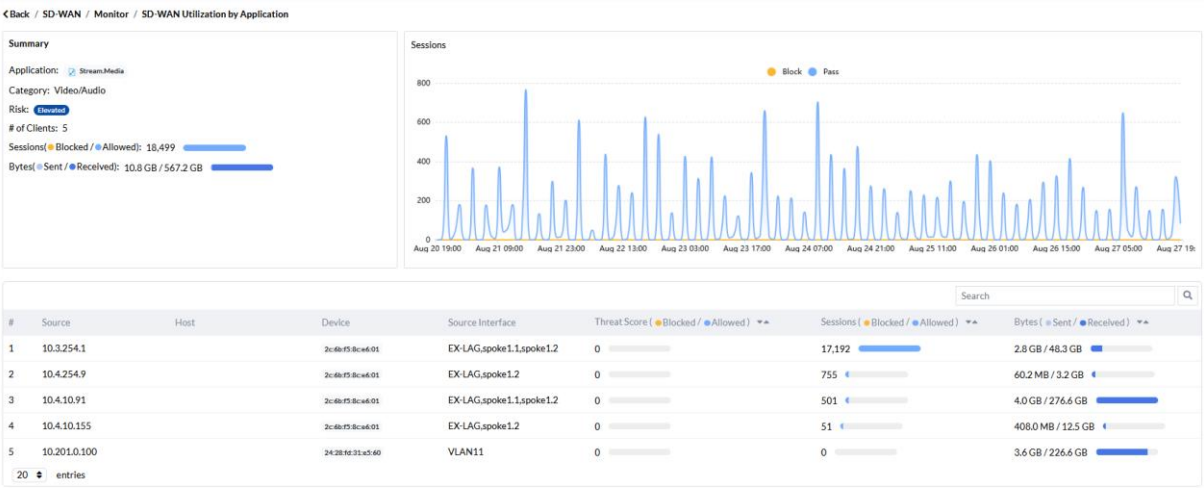


Aby filtrować dane wg czasu można użyć listy rozwijanej *Set Filter* dostępnej u góry pulpitu nawigacyjnego.

SD-WAN Utilization by Application

Widżet *SD-WAN Utilization by Application* wyświetla wielkość ruchu w sieci SD-WAN według aplikacji (np. Facebook, Dropbox itp.).

Aby wyświetlić szczegółową listę użytkowników i urządzeń korzystających z aplikacji, posortowaną według liczby sesji, należy kliknąć wykres dla określonej aplikacji.



Akcje widgetów

Górny baner każdego widżetu zawiera niektóre lub wszystkie z następujących elementów sterujących:

- *Refresh*: odświeżenie danych
- action: Edit
- *Drag to reorder:* należy wybrać a następnie przeciągnij i upuść aby zmienić położenie widżetu w okienku

Aby zobaczyć dodatkowe informacje należy najechać kursorem na widżet.

Akcja *Edit*

Aby otworzyć okno widżetu, w którym można zmienić liczbę wyświetlanych wyników należy kliknąć opcję *Edit* na liście rozwijanej *action*.

Górne Widżety

Widżety u góry (*SD-WAN Enabled Devices*, *Healthy Devices*, *Unhealthy Devices* i *Offline Devices*) po kliknięciu wyświetlają informacje dotyczące wydajności w formie tabeli. Jest to okno stanu SD-WAN , które pojawia się, gdy dostęp do urządzeń jest uzyskiwany z mapy.

Konfiguracja

W celu przeprowadzenia konfiguracji SD-WAN urządzeń należy przejść do zakładki *SD-WAN > Configuration* i z rozwijanego menu wybrać urządzenia z grupy:

- *Central Management*: tworzenie szablonów SD-WAN (*SD-WAN Templates*).
- *Per Device*: tworzenie interfejsów powiązanych (*Interface Members*), wydajnościowych SLA (*Performance* SLA) i reguł SD-WAN (*SD-WAN Rules*).

Aby edytować konfigurację SD-WAN, użytkownik musi mieć zarówno uprawnienia do odczytu i zapisu dla SD-WAN, jak i uprawnienia do odczytu dla interfejsu.

Akcje strony

W zakładce *SD-WAN > Configuration* dostępne są następujące akcje :

- *Devices*: wybór urządzenia w grupie *Central Mangement*, w celu tworzenia szablonów SD-WAN lub w grupie *Per Device*, w celu tworzenia interfejsów powiazanych, wydajnościowych SLA i reguł SD-WAN.
- *SD-WAN Templates/Interface Members/Performance SLA/SD-WAN Rules*: wybór zależy od opcji w polu *Devices.*
- *Add/Create*: tworzenie nowego obiektu zależnie od wyboru w poprzednich polach.
- *Edit*: edycja wybranego obiektu.
- *Delete*: kasowania wybranego obiektu.
- *Assigne to Device*: przypisywanie wybranego szablonu SD-WAN do urządzenia.
- *Move*: przenoszenie wybranej reguły SD-WAN.

- *Search*: wyszukiwanie reguł SD-WAN.
- *Sort*: sortowanie danych w porządku rosnącym lub malejącym.

Lista rozwijana na dole pozwala wybrać liczbę wpisów do wyświetlenia na stronie.

Szablony SD-WAN

Aby zdefiniować SD-WAN dla ADOM należy wybrać *SD-WAN Templates* z listy rozwijanej na karcie *SD-WAN > Configuration*.

Aby dodać szablon SD-WAN:

1. Wybierz *Configuration* w menu *SD-WAN*.
2. Upewnij się, że wybrane jest prawidłowe urządzenie w obszarze *Central Management*.
3. Wybierz *SD-WAN Templates* z listy rozwijanej.
4. Wybierz *Create*.
5. Wprowadź wartości w odpowiednich polach (tabela poniżej).
6. Kliknij *Submit.*

Parametr	***Opis***
Name	Nazwa szablonu.
Description	Opis szablonu.
Status	Wybierz opcję Włącz , aby włączyć status SD-WAN.
Interface Members	Zdefiniuj, które fizyczne interfejsy należą do SD-WAN.
Performance SLA	Zdefiniuj nową umowę dotyczącą poziomu usług (SLA) dotyczącą wydajności.
SD-Wan Rule	Zdefiniuj reguły SD-WAN, aby kontrolować sposób dystrybucji sesji do fizycznych interfejsów w ramach SD-WAN.

Interfejsy należące do szablonu SD-WAN

Interfejsy SD-WAN to porty i interfejsy używane do obsługi ruchu. Aby sieć SD-WAN działała, musi być skonfigurowany co najmniej jeden interfejs. Można skonfigurować do 255 interfejsów powiązanych.

W okienku *Interface Members* w menu *SD-WAN > Configuration > SD-WAN Template* dostępne są następujące akcje:

- *Create*: zdefiniuj nowy interfejs powiązany lub strefę SD-WAN.
- *Edit*: edytuj interfejs powiązany lub strefę SD-WAN.
- *Delete*: usuń interfejs powiązany lub strefę SD-WAN.

Aby określić, które interfejsy fizyczne należą do szablonu SD-WAN:

1. Po kroku 4 w okienku *Interface Members* wybierz *SD-WAN Member* z listy rozwijanej *Create*.

2. W oknie dialogowym *Create New SD-WAN Interface Members* wprowadź wartości w odpowiednich polach (tabela poniżej).
3. Kliknij *Submit.*

Parametr	***Opis***
Sequence Number	Numer kolejny interfejsu powiązanego. Zakres to 0-4294967295.
Interface Member	Wprowadź nazwę interfejsu powiązanego.
SD-WAN Zone	Z listy rozwijanej wybierz strefę SD-WAN.
Gateway IP	Wprowadź adres IPv4 domyślnej bramy dla tego interfejsu.
Cost	Więcej ruchu jest kierowane do interfejsów o wyższych kosztach. Pole *Cost* musi mieć wartość 0 albo więcej.
Status	Włącz lub wyłącz, aby włączyć lub wyłączyć status SD-WAN.
Priority	Przypisz interfejsom priorytet oparty na priorytecie przypisanym do interfejsu.

Aby utworzyć nową strefę SD-WAN:

1. Po kroku 4 w punkcie „Aby dodać szablon SD-WAN” w okienku *Members* wybierz Strefę SD-WAN z listy rozwijanej *Create*.
2. W oknie dialogowym *Create New SD-WAN Zone*:
    a. Wprowadź nazwę strefy SD-WAN.
    b. Dodaj interfejsy powiązane z listy rozwijanej *Interface Members*.
3. Kliknij *Submit*.

Definiowanie SLA

Użyj panelu *Performance SLA* w menu *SD-WAN > Configuration > SD-WAN Template*, aby skonfigurować zarządzanie SLA. W okienku *Performance SLA* dostępne są następujące akcje:

- *Create*: zdefiniuj nową umowę SLA dotyczącą wydajności.
- *Edit*: edytuj istniejącą umowę SLA dotyczącą wydajności.
- *Delete*: usuń istniejącą umowę SLA dotyczącą wydajności.

Aby dodać nową umowę SLA dotyczącą wydajności:

1. Po kroku 4 w punkcie „Aby dodać szablon SD-WAN” w okienku *Performance SLA* wybierz opcję *Create*.
2. W oknie dialogowym *Create New Performance SLA* wprowadź wartości w odpowiednich polach (tabela poniżej).
3. Kliknij *Submit.*

Parametr	Opis
Name	Nazwa SLA wydajnościowego.
IP Version	Z listy rozwijanej wybierz IPv4 lub IPv6.
Probe Mode	Wybierz tryb próbkowania *Active, Passive,* lub *Prefer Passive*.
Protocol	Protokół używany do określenia, czy urządzenie jest aktywne. Wybierz: *HTTP, Ping, TCPECHO, TWAMP* lub *UDP ECHO*.
Health Check Server	Wybierz serwer sprawdzania kondycji.
Participants	*All SD-WAN Members* lub *Specify* (wszystkie lub wybierz)
Enable Probe Packets	Włącz lub wyłącz wysyłanie pakietów próbnych.
SLA Wybierz *Create*, wprowadź wartości w odpowiednich polach i kliknij *Submit*.	
Latency Threshold	Opóźnienie podjęcia decyzji przez SLA w milisekundach. Wartość domyślna to 5; zakres wynosi 0 - 10000000.
Jitter Threshold	Jitter dla SLA do podjęcia decyzji w milisekundach. Wartość domyślna to 5; zakres wynosi 0 - 10000000.
Packet Loss Threshold	Utrata pakietów dla SLA do podjęcia decyzji w procentach. Wartość domyślna to 0; zakres wynosi 0-100.
Link Status	
Interval	Interwał sprawdzania statusu, czyli czas między próbami połączenia z serwerem, w sekundach (1 - 3600, domyślnie = 5).
Failure Before Inactive	Liczba błedów przed uznaniem serwera za utracony (1 - 10, domyślnie = 5).
Restore Link After	Liczba otrzymanych pomyślnych odpowiedzi, zanim serwer zostanie uznany za odzyskany (1–10, domyślnie = 5).
Action When Inactive	
Update Static Route	Włącz lub wyłącz aktualizowanie trasy statycznej.
Update Cascade Interface	Włącz lub wyłącz aktualizację interfejsu kaskadowego.
sla-fail-log-period	Wprowadź w sekundach przedział czasu, w jakim mają być generowane logi błędów SLA.
sla-pass-log-period	Wprowadź w sekundach przedział czasu, w którym mają być generowane logi dla SLA.

Definicja reguł SD-WAN

Aby skonfigurować reguły SD-WAN lub reguły priorytetów, aby kontrolować sposób dystrybucji sesji do fizycznych interfejsów w SD-WAN należy użyć zakładki *SD-WAN Rule* w menu *SD-WAN > Configuration > SD-WAN Template.*

W okienku *SD-WAN Rule* dostępne są następujące akcje:

- *Create*: tworzenie reguły SD-WAN.
- *Edit*: edycja istniejącej reguły SD-WAN.

- *Delete*: usuwanie istniejącej reguły SD-WAN.
- *Move*: przeniesienie reguły SD-WAN.

Dodawanie nowej reguły SD-WAN

1. Po kroku 4 w punkcie „Aby dodać szablon SD-WAN” w okienku *SD-WAN Rule* wybierz opcję *Create*.
2. W oknie dialogowym *Create New SD-WAN Rule* wprowadź wartości w odpowiednich polach (tabela poniżej).
3. Kliknij *Submit.*

Parametr	***Opis***
Name	Nazwa reguły
IP Version	Z listy rozwijanej wybierz IPv4 lub IPv6.
Source	
Source Address	Wybierz adresy źródłowe z listy.
User(s)	Wybierz użytkowników z listy.
User Groups	Wybierz grupy użytkowników z listy.
Destination	Wybierz *Address*, aby użyć adresów lub wybierz *Internet Service* aby użyć usług internetowych jako punktu docelowego.
Address	Dostępne, jeśli *Destination* jest ustawione na *Address*. Wybierz adresy docelowe z listy.
Route Tag	Dostępne, jeśli *Destination* jest ustawione na *Address*. Dostępne, gdy znaczniki tras są zdefiniowane dla mapy tras BGP.
Protocol	Dostępne, jeśli *Destination* jest ustawione na *Address*. Wybierz *TCP, UDP, ANY* lub *Specify*. W przypadku wybrania opcji *Specify* wprowadź numer protokołu, typ usługi i maskę bitową.
Type of Service Bit Mask	Bity oceniane typu usługi. Ta wartość określa, które bity w polu TOS nagłówka IP są znaczące.
Type of Service	Wzorzec bitowy typu usługi.
Internet Service	Dostępne, jeśli *Destination* jest ustawione na *Internet Service*. Wybierz usługi internetowe z listy.
Internet Service Group	Dostępne, jeśli *Destination* jest ustawione na *Internet Service*. Wybierz grupy usług internetowych z listy.
Custom Internet Service	Dostępne, jeśli *Destination* jest ustawione na *Internet Service*. Wybierz niestandardowe usługi internetowe z listy
Custom Internet Service Group	Dostępne, jeśli *Destination* jest ustawione na *Internet Service*. Wybierz niestandardowe grupy usług internetowych z listy.
Application	Dostępne, jeśli *Destination* jest ustawione na *Internet Service*. Wybierz aplikacje z listy.
Application Group	Dostępne, jeśli *Destination* jest ustawione na *Internet Service*. Wybierz grupy aplikacji z listy.

Outgoing Interface	
Strategy	Wybierz opcję *Manual*, *Best Quality*, *Lowes Cost (SLA)* lub *Maximize Bandwidth (SLA)*.
Interface Preference	Ustaw preferowaną kolejność interfejsów, gdy wiele kwalifikujących się łączy ma ten sam koszt.

Per Device Interface Members

Aby dodać nowy interfejs powiązany w opcji *Per Device*:

1. Wybierz *Configuration* w menu *SD-WAN*.
2. Upewnij się, że wybrane jest urządzenie w opcji *Per Device*.
3. Wybierz *Interface Members* z listy rozwijanej.
4. W menu *Create* wybierz *SD-WAN Member* lub *SD-WAN Zone*.
5. Wprowadź wartości w odpowiednich polach wg opisów na poprzednich stronach.
6. Kliknij *Save*.

Per Device Performance SLA

Aby dodać nowe wydajnościowe SLA w opcji *Per Device*:

1. Wybierz *Configuration* w menu *SD-WAN*.
2. Upewnij się, że wybrane jest urządzenie w opcji *Per Device*.
3. Wybierz *Performance SLA* z listy rozwijanej.
4. Wybierz *Create*.
5. Wprowadź wartości w odpowiednich polach wg opisów na poprzednich stronach.
6. Kliknij Save.

Per Device SD-WAN Rule

Aby dodać nową regułę SD-WAN w opcji *Per Device*:

1. Wybierz *Configuration* w menu *SD-WAN*.
2. Upewnij się, że wybrane jest urządzenie w opcji *Per Device*.
3. Wybierz *SD-WAN Rules* z listy rozwijanej.
4. Wybierz *Create*.
5. Wprowadź wartości w odpowiednich polach wg opisów na poprzednich stronach.
6. Kliknij Save.

Security

Karta *Security* zapewnia dostęp do polityk, obiektów firewall, ustawień związanych z siecią oraz tabeli routingu.

Dostępne są następujące zakładki:

- Policy
- Firewall objects
- Network
- Routing

Policy

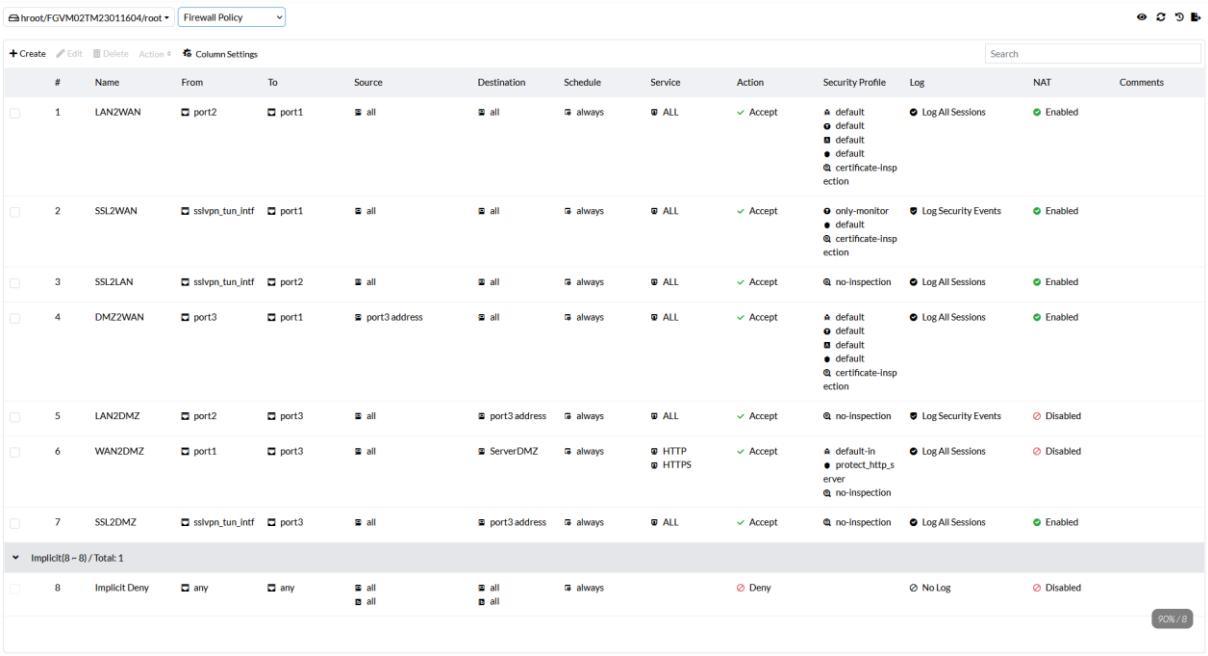
Zakładka *Policy* umożliwia przeglądanie polityk bezpieczeństwa zainstalowanych na urządzeniach i zarządzanie nimi. Zestaw polityk przypisanych do urządzenia jest nazywany pakietem polityk.

Każdy pakiet może być powiązany z jednym lub większą liczbą urządzeń.

W menu *Security* należy wybrać pozycję *Policy* aby wyświetlić polityki dla urządzenia pogrupowane według typu.

U góry strony wyświetlana jest nazwa urządzenia i rodzaj polityki.

Po wybraniu w górnym pasku urządzenia oraz rodzaju polityki w głównym panelu wyświetlone zostaną polityki skojarzone z tym wpisem.



Akcje karty

W zakładce *Policy* dostępne są następujące akcje :

- *Device*: wybór urządzenie do wyświetlenia
- *Policy type*: wybór rodzaju polityki do wyświetlenia dla wybranego urządzenia
- *View*: wyświetlenie ustawień, które mają wpływ na wszystkie polityki w pakiecie

- *Refresh*: odświeżenie informacje o politykach
- *Policy Revisions*: wyświetlenie zapamiętanych wersji polityk
- *Export to CSV:* eksportowanie informacje o pakiecie polityk do pliku CSV
- *Create*: utworzenie nowej polityki
- *Edit*: edycja wybranej polityki
- *Delete*: usunięcie wybranych polityk
- *Action*: włączenie, wyłączenie lub przeniesienie wybranej polityki
- *Column Settings*: ustawienie, jakie kolumny mają być wyświetlane na karcie
- *Search*: wyszukiwanie polityk na podstawie nazwy obiektu, adresu IP lub części adresu IP
  Można także wyszukiwać polityki na podstawie numerów portów w obiektach usług lub obiektach znalezionych w grupach lub grupach zagnieżdżonych.

Zarządzanie politykami

Możliwość zarządzania politykami dotyczy wyłącznie obiektów typu *Firewall Policy.* Wszystkie pozostałe są dostępnie w trybie do odczytu.

Dostępne są następujące dodatkowe operacje na politykach:

- Usuwanie polityki
- Wyłączanie lub włączanie polityki
- Zmiana kolejności polityk
- Instalowanie polityk

Konfigurowanie polityk

Polityki to zestaw instrukcji kontrolujących przepływ ruchu przechodzącego przez firewall. Instrukcje te kontrolują, dokąd zmierza ruch, jak jest przetwarzany, czy jest przetwarzany, a nawet czy może przechodzić przez firewall.

Aby utworzyć lub edytować polityki:

1. Należy przejść do menu *Security > Policy.*
2. Z rozwijanego menu na górze ekranu należy wybrać odpowiednie urządzenie oraz dostępny do edycji rodzaj polityk – *Firewall Policy*.
3. Należy wybrać pozycję *Create* lub wybrać odpowiednią politykę i wybrać pozycję *Edit.*
4. W formularzu należy podać następujące informacje:

Parametr	***Opis***
Name	Nazwa polityki
Incoming Interface	Interfejs wejściowy
Outgoing Interface	Interfejs wyjściowy
Source Internet Service	Włączanie i wyłączanie opcji oraz wybór źródłowej usługi internetowej
IPv4 Source Address	Adresy źródłowe IPv4. Ta opcja jest dostępna tylko wtedy, gdy parametr *Source Internet Service* jest wyłączony.
IPv6 Source Address	Adresy źródłowe IPv6. Ta opcja jest dostępna tylko wtedy, gdy parametr *Source Internet Service* jest wyłączony.

Source User	Użytkownik źródłowy (lista).
Source User Group	Źródłowa grupa użytkowników (lista).
FSSO Groups	Grupa Fortinet Single Sign-On
Destination Internet Service	Włączanie i wyłączanie opcji oraz wybór docelowej usługi internetowej
IPv4 Destination Address	Adresy docelowe IPv4. Ta opcja jest dostępna tylko wtedy, gdy parametr *Destination Internet Service* jest wyłączony.
IPv6 Destination Address	Adresy docelowe IPv6. Ta opcja jest dostępna tylko wtedy, gdy parametr *Destination Internet Service* jest wyłączony.
Service	Usługa lub grupa usług (lista). Ta opcja jest dostępna tylko wtedy, gdy parametr *Destination Internet Service* jest wyłączony.
Schedule	Możliwość wskazania kiedy polityka ma być stosowana.
Action	Określenie czy wskazany ruch ma być zaakceptowany czy odrzucony
Accept Options	
Inspection Mode	Wybór trybu inspekcji ruchu.
Firewall/Network Options	Włączanie i wyłączanie NAT i wybór odpowiednich opcji protokołu.
Security Profiles Options	• Włączanie usług bezpieczeństwa oraz wybór odpowiednich profili • Wybór profilu inspekcji SSL/SSH dla polityki
Traffic Shaping Options	Wybór opcji ograniczania ruchu dla *Shared Shaper, Reverse Shaper i Per IP Shaper.*
Disclaimer Options	
Display Disclaimer	Włączanie komunikatu wymagającego potwierdzenia
Customize Message	Wybór niestandardowego komunikatu. Ta opcja jest dostępna tylko wtedy, gdy włączona jest opcja *Display Disclaimer.*
Logging Options	
Log Violation Traffic	Włączanie logowania ruchu naruszającego regułę.
Capture Packets	Włączanie przechwytywania pakietów.
Generate Logs when Session Starts	Włączanie generowania dodatkowych logów przy uruchamianiu sesji.
Advanced	
WCCP	Włączanie *Web Cache Communication Protocol (WCCP)*
Exempt from Captive Portal	Wykluczenie użycia *Captive Portal* dla tej polityki.
Comments	Opcjonalny komentarz.

5. W celu zapisania zmian należy kliknąć *Save.*

Usuwanie polityk

Aby usunąć politykę, należy zaznaczyć ją na liście i kliknąć *Delete*.

Akcje polityk

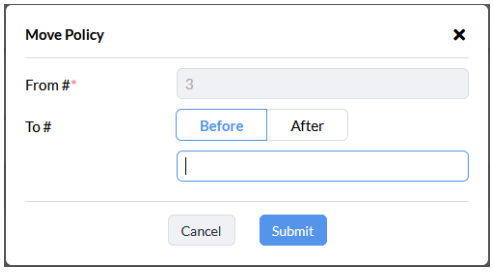
Aby włączyć, wyłączyć lub przenieść politykę należy zaznaczyć ją a następnie fybrać funkcję *Action.*

Wyłączona polityka jest oznaczona na liście znakiem (⊗).

Przenoszenie polityk

Aby zmienić kolejność zasad:

1. Wybierz politykę z listy, a następnie wybierz opcję *Move* z listy rozwijanej *Action* . System otwiera okno dialogowe, pokazujące numer wybranej polisy.



2. Wybierz opcję *Before* lub *After*.
3. Wprowadź numer kolejny polityki docelowej.
4. Kliknij *Submit.*

Wybrana polityka zostanie przeniesiona na nową pozycję przed lub za polityką docelową.

Kolejność polityk jest ważna ze względu na to, że ruch przechodzący przez firewall jest przetwarzany zgodnie z ich kolejnością od góry do dołu.

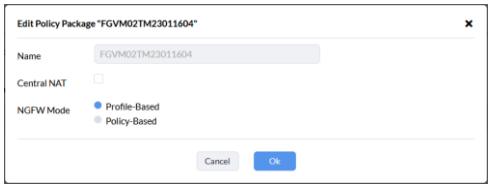
Instalowanie polityk

Aby polityki zaczęły obowiązywać, należy zainstalować aktualizacje polityk na docelowym urządzeniu.

Wyświetlanie ustawień pakietu polityk

Pakiety polityk są wymienione u góry karty *Policy* w menu rozwijanym *Policy Package*.

Aby sprawdzić ustawienia, które mają wpływ na wszystkie polityki w pakiecie, kliknij ikonę *View* ( ) po wybraniu pakietu polityk z listy rozwijanej.



Odświeżanie polityk

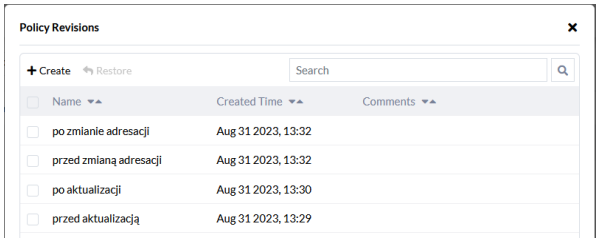
Informacje o politykach są odświeżane co godzinę. Można także odświeżyć dane na żądanie, wybierając przycisk *Refresh* ( ).

Zarządzanie wersjami polityk

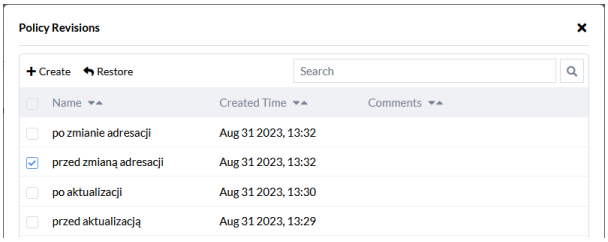
Aby zarządzać wersjami polityk należy z menu wybrać funkcję *Policy Revisions* ( ).

Tworzenie i przywracanie wersji polityk

Aby utworzyć kopię zapasową bieżących polityk i obiektów należy w okienku *Policy Revisions* wybrać funkcję *Create*.



Aby przywrócić polityki należy wybrać wybraną wersję i wybrać funkcję *Restore.*



Konfiguracja kolumn w oknie polityk

Na liście rozwijanej *Column Setting* można zaznaczyć kolumny, które mają być wyświetlane i odznaczyć kolumny, które mają być ukryte.

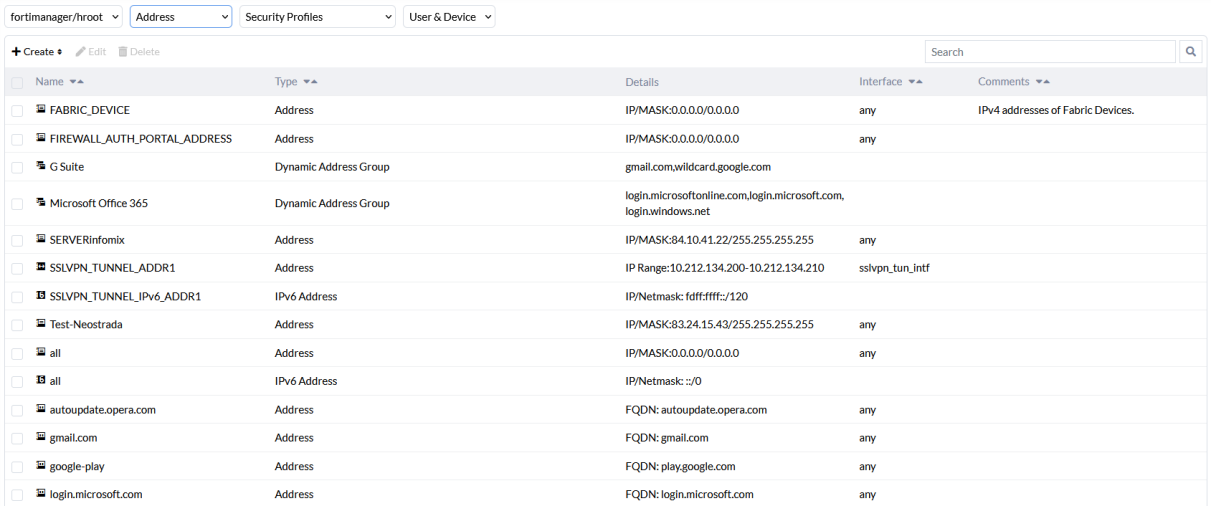
Aby zresetować wyświetlanie kolumn do domyślnych ustawień systemowych należy kliknąć przycisk *Reset* ( ).

Obiekty zapory

W menu *Security > Firewall Objects* można wyświetlić i konfigurować obiekty zapory, które są dostępne do użycia w politykach bezpieczeństwa.

Obiekty zapory obejmują takie elementy jak adresy, harmonogramy, usługi i wirtualne adresy IP, a także profile zabezpieczeń, użytkownicy i grupy użytkowników.

Obiekty mogą być używane w więcej niż jednej polityce.



Dostęp do obiektów zapory można uzyskać za pomocą list rozwijanych u góry tabeli. Należy wybrać urządzenie oraz typ obiektu z listy rozwijanej.

Rodzaje obiektów

Po wybraniu pozycji menu *Security > Firewall Objects* wyświetlane są następujące kategorie obiektów:

- *Firewall Objects*
- *Security Profiles*
- *User & Devices*

Firewall Objects

Obiekty zapory to elementy, które pasują do siebie jak bloki konstrukcyjne. Obiekty zapory można skonfigurować raz, a następnie użyć wielokrotnie.

Obiekty zapory obejmują adresy, harmonogramy, usługi i wirtualne adresy IP.

Address

Adres można określić jako kraj, nazwę FQDN lub podsieć i maskę IP. Adres może odnosić się do wszystkich interfejsów lub można skonfigurować adres jako przypisany do określonego interfejsu.

Można także tworzyć grupy adresów, które definiują grupę powiązanych ze sobą adresów.

Schedule (harmonogram)

Można określić listę dni i przedziałów czasowych z harmonogramami cyklicznymi lub jednorazowymi.

Service (usługa)

Chociaż wiele usług jest już skonfigurowanych, system umożliwia administratorom skonfigurowanie własnych.

Obiekt *Service* określa protokół oraz wszelkie dodatkowe informacje wymagane do identyfikacji usługi (które zależą od protokołu):

- IP: numer protokołu IP
- TCP/UDP/SCTP: adres i zakres portów docelowych
- ICMP: typ i kod

Wirtualny adres IP

Obiekty *Virtual IP* mapują zewnętrzne adresy IP na adresy wewnętrzne. Usługa ONS obsługuje następujące typy obiektów Virtual IP:

- *Virtual IP*: używa statycznego NAT do mapowania zakresu adresów zewnętrznych na zakres adresów wewnętrznych
- *Virtual IP Group*: Grupa jednego lub więcej wirtualnych adresów IP ułatwiająca administrację

Security Profiles

Funkcje zabezpieczeń chroniące sieć przed zagrożeniami są wspólnie nazywane profilami zabezpieczeń. ONS obsługuje następujące profile zabezpieczeń:

- *Antivirus Profile* (profil antywirusowy – wykrywanie i identyfikacja wirusów)
- *Intrusion Prevention Profile* (profil zapobiegania włamaniom – ochrona przed atakami hakerskimi i próbami wykorzystania luk w zabezpieczeniach)
- *Local Category* (kategorie lokalne uzupełniające globalna kategorie usługi Web Filtering)
- *Web Rating Overrides* (przypisanie URLi do kategorii usługi Web Filtering nadpisujące definicje globalne)
- *Web Filter Profile* (możliwość ochrony lub ograniczenia aktywności użytkowników w sieci)
- *Application Control* (możliwość wykrywania ruchu w sieci i kontrolowania komunikacji aplikacji)
- *File Filter Profile* (profil filtra plików)
- *Video Filter* (umożliwia filtrowanie filmów z YouTube według kategorii lub kanału)
- *SSL/SSH Inspection* (umożliwia szczegółową kontrolę zaszyfrowanego ruchu)

User & Device

Zasady bezpieczeństwa mogą zezwalać na dostęp tylko określonym użytkownikom i grupom użytkowników.

User

Użytkownik to konto użytkownika składające się z nazwy użytkownika, hasła i w niektórych przypadkach innych informacji, skonfigurowane w zaporze sieciowej lub na zewnętrznym

serwerze uwierzytelniającym. Użytkownicy mogą uzyskiwać dostęp do zasobów wymagających uwierzytelnienia tylko wtedy, gdy są członkami dozwolonej grupy użytkowników.

Można tworzyć użytkowników lokalnych (konta przechowywane w urządzeniu zapory)

User Group

Grupa użytkowników to lista tożsamości użytkowników. Po ustawieniu typu grupy i dodaniu członków nie można zmienić typu grupy bez usunięcia jej członków. Po zmianie typu, członkowie grupy zostaną automatycznie usunięci.

Akcje strony

Na zakładce *Firewall Objects* dostępne są następujące akcje :

- *ADOM*: wybór ADOMu w celu wyświetlenia powiązanych obiektów zapory
- *Type*: wybór typu obiektu zapory
- *Security Profiles*: wybór profilu zabezpieczeń
- *Create*: utworzenie obiekt zapory lub profilu zabezpieczeń
- *Edit*: edycja wybranego obiektu zapory lub profilu zabezpieczeń
- *Delete*: usunięcie wybranego obiektu zapory lub profilu bezpieczeństwa
- *Search*: wyszukanie obiektu zapory lub profilu zabezpieczeń
- *Sort*: sortowanie danych w porządku rosnącym lub malejącym
- *Show x entries*: ograniczenie liczby wpisów wyświetlanych na stronie (20 lub 50)

Network

Zakładka w menu *Security > Network* pozwala na:

- Konfigurację IPSec faza 1 i faza 2.
- Definiowanie routing statycznego.
- Konfigurowanie usługi DHCP.
- Zarządzanie certyfikatami SSL.

Akcje strony

W zakładce *Security > Network* dostępne są następujące akcje :

- *Create*: konfiguracja routingu statycznego i serwerów DHCP.
- *Edit*: zmiana istniejącej konfiguracji routingu statycznego i serwerów DHCP.
- *Delete*: usuwanie konfiguracji routingu statycznego i serwerów DHCP.
- *Search*: wyszukiwanie wpisów sieciowych w tabeli.

- *Sort*: sortowanie danych w porządku rosnącym lub malejącym
- *Show x Entries*: ograniczenie liczby wpisów do wyświetlenia (20 lub 50)

Routing

Lista rozwijana *Route* na karcie *Security* > *Network* wyświetla listę routingu statycznego.

Konfigurowanie routingu statycznego

Dodanie nowego wpisu w routingu statycznym

1. Wybierz *Static Route* z listy rozwijanej Route.
2. Wybierz *Create*, aby utworzyć nowy wpis.
3. Wprowadź wartości w odpowiednich polach (tabela poniżej).
4. Wybierz *Save*.

Aktualizowanie wpisu w routingu statycznym

1. Wybierz *Static Route* z listy rozwijanej Route.
2. Wybierz jeden z wpisów, a następnie wybierz opcję *Edit*.
3. Zaktualizuj wartości, które uległy zmianie.
4. Wybierz *Save*.

Usuwanie wpisu w routingu statycznym

1. Wybierz *Static Route* z listy rozwijanej Route.
2. Wybierz jeden z wpisów a następnie wybierz *Delete*.

Pola definiujące routing statyczny

Parametr	***Opis***
Destination	Parametr wymagany. Wybierz *Subnet* lub *Named Addrss* jako typ miejsca docelowego. • *Subnet*: wprowadź docelowy adres IP i maskę sieci. • *Named Address*: wybierz z listy rozwijanej.
Gateway	Parametr wymagany. Wprowadź adres IPv4 dla następnego przeskoku. Uwaga: Ta opcja nie jest dostępna, gdy włączony jest interfejs SD-WAN.
SDWAN Interface	Włącz interfejs SD-WAN.
SDWAN Zones	Z listy rozwijanej wybierz strefę SD-WAN. Uwaga: Ta opcja jest dostępna, gdy włączony jest interfejs SD-WAN .
Interface	Parametr wymagany. Z listy rozwijanej wybierz interfejs sieciowy, który łączy się z bramą. Uwaga: Ta opcja nie jest dostępna, gdy włączony jest interfejs SD-WAN.

Distance	Parametr wymagany. Wprowadź odległość. Wartość domyślna to 10. Wartość maksymalna to 255.
Priority	Parametr wymagany. Wprowadź priorytet. Wartość domyślna to 0. Wartość maksymalna to 4294967295. Uwaga: Ta opcja nie jest dostępna, gdy włączony jest interfejs SD-WAN .
Comments	Parametr opcjonalny. Wprowadź opis trasy statycznej. Wartość to ciąg znaków o maksymalnej długości 255 znaków.
Status	Włącz lub wyłącz trasę statyczną.

System

Lista rozwijana *System* na karcie Security > *Network* zapewnia dostęp zarządzania serwerami DHCP.

DHCP serwer

Ta funkcja umożliwia dodawanie, aktualizowanie i usuwanie serwerów DHCP.

Dodanie serwera DHCP

1. Wybierz *DHCP Server* z listy rozwijanej *System*.
2. Wybierz opcję *Create* aby utworzyć nowy serwer DHCP.
3. Wprowadź wartości w odpowiednich polach (tabela poniżej).
4. Wybierz *Save*.

Aktualizowanie serwera DHCP

1. Wybierz *DHCP Server* z listy rozwijanej *System*.
2. Wybierz serwer DHCP, a następnie wybierz opcję *Edit*.
3. Zaktualizuj wartości, które chcesz zmienić.
4. Wybierz *Save*.

Usuwanie serwera DHCP

1. Wybierz *DHCP Server* z listy rozwijanej *System*.
2. Wybierz serwer DHCP, a następnie wybierz *Delete*.
3. Potwierdź aby usunąć wybrany serwer DHCP.

Parametry opisujące serwer DHCP

Okna dialogowe *Create DHCP Server* i *Edit DHCP Server* zawierają następujące pola:

Parametr	***Opis***
Interface	Z listy rozwijanej wybierz interfejs.
DHCP Status	Włącz/wyłącz DHCP.
IP Range	Zakres adresów IP DHCP. Zakres adresów IP każdego serwera DHCP musi być zgodny z zakresem adresów sieciowych.

Netmask	Maska sieci przypisana przez serwer DHCP.
Default Gateway	Wybierz opcję *Same as Interface IP* (domyślnie) lub *Specify*. Po wybraniu opcji *Specify* wprowadź adres IP bramy domyślnej przypisany przez serwer DHCP.
DNS server	Opcje przypisywania serwerów DNS do klientów DHCP: • *Same as System DNS* — klientom są przypisywane skonfigurowane w urządzeniu serwery DNS. • *Same as Interface IP* — adres IP interfejsu, z którego pochodzi serwer DHCP staje się adresem IP serwera DNS klienta. • *Specify* — Określ maksymalnie cztery serwery DNS w konfiguracji serwera DHCP (domyślny).
DNS server1	Serwer DNS1. Uwaga: Ta opcja jest dostępna tylko wtedy, gdy jako serwer DNS wybrano opcję *Specify*.
DNS server2	Serwer DNS2. Uwaga: Ta opcja jest dostępna tylko wtedy, gdy jako serwer DNS wybrano opcję *Specify*.
DNS server3	Serwer DNS3. Uwaga: Ta opcja jest dostępna tylko wtedy, gdy jako serwer DNS wybrano opcję *Specify*.
DNS server4	Serwer DNS4. Uwaga: Ta opcja jest dostępna tylko wtedy, gdy jako serwer DNS wybrano opcję *Specify*.
Lease time	Ustaw czas, po którym przypisany adres IP wygaśnie, w sekundach. Wartość domyślna to 604800.

Konfigurowanie zakresu adresów IP

1. W polu *IP Range* wybierz + aby dodać nowy zakres adresów IP.
2. W polu *IP Range* wprowadź zakres adresów IP.

Routing

Opcja *Routing* wyświetla widok tylko do odczytu tabel routingu urządzeń, zarówno statycznego jak i dynamicznego.

Listę można filtrować według parametrów *Site* (lokalizacja) i *Device* (urządzenie) oraz według wersji protokołu IP.

Raporty

Zakładka *Reports* wyświetla listę dostępnych raportów.

Akcje strony

Ta zakładka zawiera następujące akcje:

- *Set Filter*: filtrowanie danych wg czasu.
- *Run Reports:* kliknij, a następnie określ raporty do uruchomienia.
- *Search*: wyszukiwanie według nazwy raportu.
- *Show x entries*: ograniczenie liczby wyświetlanych raportów (20 lub 50)

Po kliknięciu jednej z ikon w kolumnie *Format* można pobrać raport w jednym z formatów: XML, CSV lub PDF.

Akcja *Run Reports*

Okno *Report to be Executed* zawiera następujące opcje:

Parametr	***Opis***
Report Duration	Czas trwania danych uwzględnionych w raporcie*: Today, Yesterday, Last 7 Days, or Last 14 Days*
Reports	Wybierz raporty do uruchomienia.
Device	Wybierz urządzenia, dla których chcesz uruchamiać raporty.

Audit

Zakładka Audyt wyświetla dziennik aktywności użytkownika systemu.

Akcje strony

- *Time zone*: wybór strefy czasowej *Local Time Zone* lub *GMT Time Zone.*
- *Filter*: ograniczenie zakresu wyświetlanych dzienników wg czasu.
- *Export to CSV*: eksport dzienników jako plik z wartościami rozdzielanymi przecinkami (CSV).
- *Search*: wyszukiwanie według poziomu, nazwy użytkownika, typu zdarzenia, adresu IP klienta lub trași.
- *Show x entries*: ograniczenie liczby wpisów do wyświetlenia.
- *Sort*: sortowanie listy rosnąco lub malejąco według dat.