



# Orange Network Security

Portal self-service



## Spis treści

Portal konfiguracji usługi Orange Network Security (ONS) .....	4
Strona startowa.....	5
Resetowanie hasła .....	6
Zmiana hasła.....	7
Dashboard .....	8
Akcje.....	9
Działania wewnątrz widżetów .....	9
Policy .....	10
Ustawienia kolumn w zakładce <i>Policy</i> .....	10
Odświeżanie danych dotyczących polityki.....	10
Kopia zapasowa polityk bezpieczeństwa.....	10
Przeglądanie ustawień pakietu polityk.....	10
Tworzenie i przywracanie kopii polityk.....	11
Konfigurowanie polityk .....	11
Dodanie nowej polityki .....	12
Aktualizacja polityki.....	12
Usuwanie polityki .....	12
Włączanie lub wyłączanie polityki.....	12
Pola definicji polityki.....	12
Przesuwanie polityki.....	13
Instalacja polityk .....	14
Przegląd polityk .....	14
Obiekty.....	16
Rodzaje obiektów .....	16
Firewall Objects.....	16
Security Profiles .....	17
User & Device.....	19
Konfigurowanie obiektów .....	21
Dodawanie nowego obiektu.....	21
Aktualizacja obiektu .....	21



Usuwanie obiektu.....	21
View .....	22
Widok aplikacji.....	22
Widok Ataku .....	23
Sandbox .....	24
Raporty .....	25
Akcje.....	25
Audit.....	26
Akcje.....	26



## Portal konfiguracji usługi Orange Network Security (ONS)

Portal konfiguracji usługi ONS pozwala na analizowanie logów zdarzeń bezpieczeństwa, przeglądanie raportów, przeglądanie i zmianę konfiguracji polityk bezpieczeństwa oraz obiektów firewall'a i profili zabezpieczeń.

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

- *Help* - dodatkowe okno pomocy, które kontekstowo wyświetla strony pomocy
- *Alerts* - okno, w którym wyświetlane są nieprzeczytane alerty
- *Change Password* - wyświetla okno dialogowe do zmiany hasła
- *Logout* - wylogowanie z portalu

W lewym panelu znajdują się następujące opcje:

- *Dashboard* - podgląd konfigurowalnych widżetów, które wyświetlają statystyki dotyczące ruchu sieciowego
- *Policy* - przeglądanie i modyfikacja polityk bezpieczeństwa
- *Objects* - przeglądanie i modyfikacja obiektów firewall'a i profili zabezpieczeń
- *View* - przeglądanie logów związanych z działaniem usługi ONS
- *Reports* - podgląd dostępnych raportów
- *Audit* - dziennik aktywności użytkowników systemu



## Strona startowa

Aby zalogować się do systemu, należy w przeglądarce internetowej wpisać adres:

<https://ons.orange.pl/fpc/login>

Poniższy rysunek przedstawia domyślną stronę startową:

Orange Network Security

Bezpieczeństwo

Login

Username or email

Password

Login

[Forgot password](#)

Portal self-service

System obsługuje następujące języki: angielski, francuski, niemiecki, portugalski, rumuński, hiszpański i włoski.



## Resetowanie hasła

Aby zresetować hasło lub uruchomić portal po raz pierwszy należy na stronie logowania wybrać łącze *Forgot password*

Reset your password ✕

Please enter your email address and we will send you a temporary password

\* Email:

W oknie dialogowym należy wprowadzić adres e-mail powiązany z kontem użytkownika. System zresetuje i wyśle hasło tymczasowe w emailu.



## Zmiana hasła

Wybranie ikony *Change password* oraz logowanie za pomocą hasła tymczasowego powoduje wyświetlenie okna dialogowego pokazanego na poniższym rysunku:

**Change Password** ⓘ

Old Password

New Password

Confirm New Password

Należy wprowadzić dotychczasowe hasło, dwukrotnie nowe hasło i zatwierdzić zmianę przyciskiem *Save*. Nowe hasło będzie obowiązywać przy następnej próbie logowania.

# Dashboard

Dashboard wyświetla różne widoki dziennika zdarzeń bezpieczeństwa oraz statystyki ruchowe usługi ONS.

Wygląd Dashboard'u przedstawiono poniżej:



Jak widać na rysunkach, dashboard jest zorganizowany jako zestaw widżetów.

Dostępne są następujące widżety:



- Top Countries – statystyka ruchu wg kraju docelowego
- Top Threats – statystyka wg wykrytych zagrożeń
- Top Sources – statystyka ruchu wg adresu IP źródła
- Top Destinations – statystyka ruchu wg adresu IP docelowego
- Top Applications – statystyka wg rozpoznanych aplikacji
- Policy Hits – statystyka ruchu dla zdefiniowanych polityk
- Admin Logins – statystyka logowań do systemu
- System Events – statystyka komunikatów systemowych

## Akcje

Na stronie *Dashboard* dostępne są następujące czynności:

- *Add Widget(s)* – dodanie widżetu do dashboardu
- Wybór zakresu danych (w przypadku gdy usługa ONS obsługuje więcej niż jedną wirtualną domenę)
- Wybór zakresu czasowego (ostatnie 5, 30, 60 minut, ostatnie 4, 12 godzin, ostatni 1 dzień, ostatnie 7 dni lub zakres dat)
- Odświeżanie danych

## Działania wewnątrz widżetów

Górny baner na każdym widżecie zawiera niektóre lub wszystkie z poniższych elementów sterujących:

- *Drill down* - symbol strzałki widoczny wewnątrz widżetu oznacza możliwość przejścia do szczegółowych danych w sekcji *View* po kliknięciu w wybrany element (tylko dla wybranych widżetów)
- *Refresh* - odświeżanie danych
- *Edit* - edycja widżetu, zmiana sposobu prezentacji danych (typ wykresu, liczba prezentowanych elementów, sposób sortowania danych)
- *Delete* - usunięcie widżetu z Dashboardu

## Policy

Wybranie pozycji *Policy* w lewym menu pozwala przejść do okna prezentującego pakiety polityk bezpieczeństwa zaimplementowane w usłudze ONS.

Każdy pakiet może być powiązany z jedną lub kilkoma wirtualnymi domenami (liczba dostępnych domen zależy od wykupionej opcji usługi)

Seq.#	ID	Name	Source Interface	Destination Interface	Source	Destination	Schedule	Service	Action	Log	NAT	Web Filter	Application Control	AntiVirus
1	4	Android	lan	root-trans0	all	all	* always	ALL	Accept	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	proxy-porn-and-risk-block	default	proxy-default
2	1	LAN	lan	root-trans0	all	all	* always	ALL	Accept	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	proxy-porn-and-risk-block	default	proxy-default
3	3	SSLVPN2WAN	sslvpn_tun_intf	root-trans0	SSLVPN_TUNNEL_ADDR1_689_3	all	* always	ALL	Accept	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	proxy-porn-and-risk-block	default	proxy-default

Okno w górnej części zawiera listę rozwijaną oraz hierarchiczny widok polityk. Po wybraniu wpisu w widoku hierarchicznym, panel główny wyświetla dane polityki związanej z tym wpisem.

### Ustawienia kolumn w zakładce *Policy*

W powyższym oknie można wybrać, które kolumny będą widoczne. Można to zrobić w następujący sposób:

1. Wcisnąć przycisk *Column Settings*, aby wyświetlić formularz konfiguracyjny.
2. Zaznaczyć kolumny, które powinny być wyświetlane i usunąć zaznaczenie kolumn, które powinny być ukryte.
3. Nacisnąć przycisk *Apply*.

### Odświeżanie danych dotyczących polityki

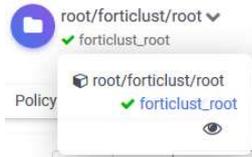
Informacje o politykach są odświeżane co godzinę. Można również odświeżać dane na żądanie wybierając przycisk *Refresh*.

### Kopia zapasowa polityk bezpieczeństwa

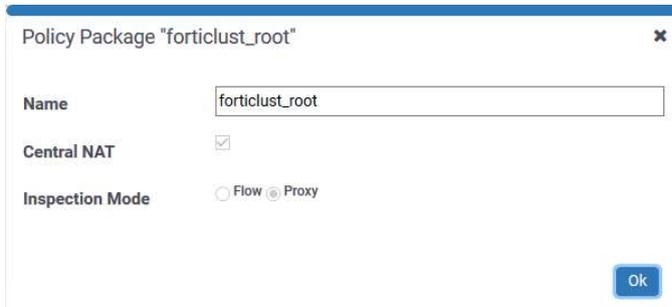
Przycisk *Revision Backup* pozwala na zarządzanie kopią polityk wybranego pakietu. System może zapisać tylko jedną kopię polityk dla każdego pakietu. Nowa kopia zastępuje istniejącą kopię (jeśli istnieje).

### Przeglądanie ustawień pakietu polityk

Pakiety polityk są wymienione w górnej części okienka *Policy*.



Aby sprawdzić ustawienia, które mają wpływ na wszystkie polityki w pakiecie, należy kliknąć ikonę oka obok pakietu polityk.



## Tworzenie i przywracanie kopii polityk

Aby otworzyć okno zarządzania kopiami polityk należy wybrać przycisk  *Revision Backup*.

Kopię zapasową aktualnych polityk i definicji obiektów tworzymy przy użyciu przycisku *Create*. Jeśli kopia już istnieje, w oknie Revision Backup można zobaczyć jej opis:



Aby przywrócić kopię zapasową, należy kliknąć prawym przyciskiem myszy i wybrać polecenie *Restore*.



## Konfigurowanie polityk

W usłudze ONS można w zakresie zależnym od wykupionej opcji usługi konfigurować polityki bezpieczeństwa definiujące sposób ochrony ruchu sieciowego.



## Dodanie nowej polityki

1. Kliknij prawym przyciskiem myszy w oknie zawierającym listę polityk i wybierz polecenie *Create New*.
2. Wprowadź wartości w odpowiednich polach i wybierz *Save*.

## Aktualizacja polityki

1. Kliknij prawym przyciskiem myszy na politykę na liście i wybierz *Edit*.
2. Zmodyfikuj odpowiednie pola i wybierz *Save*.

## Usuwanie polityki

Kliknij prawym przyciskiem myszy na politykę na liście i wybierz *Delete*.

## Włączanie lub wyłączenie polityki

Kliknij prawym przyciskiem myszy na politykę na liście i wybierz polecenie *Enable* lub *Disable*. Polityka w stanie wyłączonym jest zaznaczona czerwonym kółkiem na liście w kolumnie *Seq.#*.

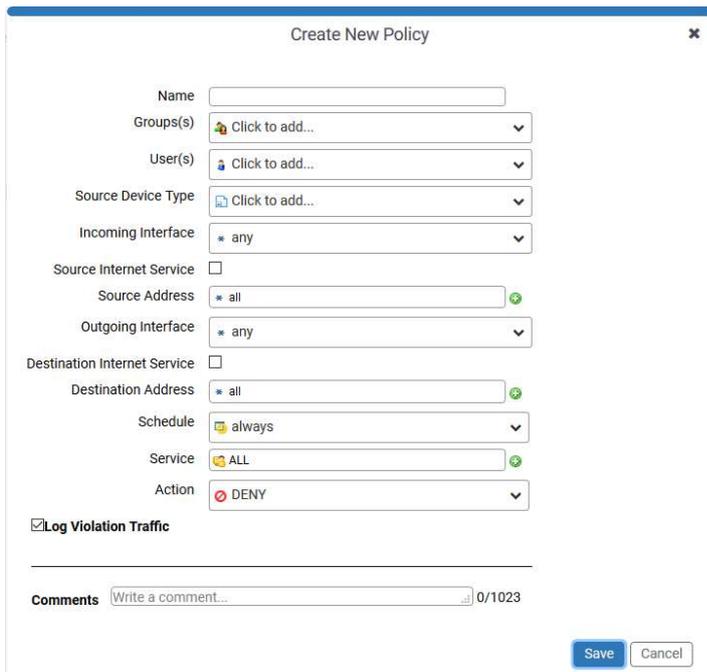
## Pola definicji polityki

Formularze *Create New Policy* i *Edit Policy* zawierają następujące pola:

Pole	Wytyczne dotyczące ustawień
<i>Name</i>	Nazwa polityki
<i>Groups</i>	Lista grup użytkowników, które będą kontrolowane przez tę politykę
<i>Users</i>	Lista użytkowników, którzy będą kontrolowani przez tę politykę
<i>Source Device Type</i>	Rodzaje urządzeń, które będą kontrolowane przez tę politykę
<i>Incoming Interface</i>	Interfejs sieciowy, z którego inicjowany ruch będzie kontrolowany
<i>Source Address</i>	Lista źródłowych adresów sieciowych, z których ruch będzie kontrolowany
<i>Outgoing Interface</i>	Wyjściowy interfejs sieciowy, którego ruch będzie kontrolowany
<i>Destination Address</i>	Lista docelowych adresów sieciowych, dla których ruch będzie kontrolowany
<i>Schedule</i>	Określenie czasu, w którym polityka będzie aktywna
<i>Service</i>	Lista usług sieciowych, które będą poddane kontroli
<i>Action</i>	Akceptacja lub odmowa.
Jeśli działanie jest ustawione na Odmowa	
<i>Log Violation Traffic</i>	Zaznaczenie tego pola spowoduje generowanie logów dla każdego odrzuconego połączenia
Jeśli akcja jest ustawiona na Accept	
<i>NAT</i>	Włączenie translacji adresów sieciowych

<i>Use Destination Interface Address</i>	Do translacji zostanie użyty adres interfejsu wyjściowego
<i>Dynamic IP Pool</i>	Do translacji zostanie użyta pula adresów wybrana z listy
<i>Logging Options</i>	Opcje logowania
<i>No log</i>	W ramach polityki nie będą generowane logi
<i>Log Security Events</i>	Logi będą generowane tylko dla zdarzeń bezpieczeństwa
<i>Log All Sessions</i>	Logi będą generowane dla wszystkich sesji
<i>Security Profiles</i>	Pozwala na włączenie usług bezpieczeństwa i wybranie dla każdej usługi jednego z wcześniej przygotowanych profili
<i>Traffic Shaping</i>	Kształtowanie ruchu dla kierunku do Internetu
<i>Reverse Direction Traffic Shaping</i>	Kształtowanie ruchu dla kierunku z Internetu
<i>Per-IP Traffic Shaping</i>	Opcja niedostępna
<i>Comments</i>	Opcjonalny komentarz do polityki.

Poniższy rysunek przedstawia okno dialogowe *Create New Policy*



## Przesuwanie polityki

Ruch sieciowy w usłudze ONS jest analizowany na podstawie polityk zgodnie z ich kolejnością zdefiniowaną w oknie *Policy*. Dlatego ważne jest prawidłowe ich posortowanie.

Aby zmienić kolejność polityk:

1. Należy kliknąć prawym przyciskiem myszy na politykę i wybrać polecenie *Move*. System otworzy okno dialogowe, w którym wyświetli identyfikator wybranej polityki.



2. Następnie należy wybrać opcję *Before* lub *After* i podać identyfikator polityki względem której dokonane zostanie przesunięcie.

UWAGA! Należy wprowadzić identyfikator (ID) a nie numer porządkowy (Seq. #).

Move Policy

Policy ID : 4  
Option : Before After  
\*Target :

Save Cancel

## Instalacja polityk

Po dodaniu lub modyfikacji polityk należy wybrać przycisk  *Installation*, aby zaimplementować wprowadzone zmiany w usłudze ONS.

Zostanie otwarte okno dialogowe *Policy Package*.

Policy Package

Please select the installation target:

<input checked="" type="checkbox"/>	Installation Target	Policy Package Status
<input checked="" type="checkbox"/>	forticlust[root]	installed

Install Cancel

Domyślnie w oknie dialogowym *Policy Package* wybrane jest urządzenie, na liście którego znajduje się dany pakiet polityk.

1. Wybierz jedno lub więcej urządzeń z listy.
2. Kliknij przycisk *Install*.
3. Pasek postępu w oknie dialogowym *Policy Package* pokazuje stan instalacji.
4. Po zainstalowaniu pakietu polityk kliknij przycisk *Finish*.

## Przegląd polityk

Kliknij przycisk *Policy*, następnie z listy rozwijanej wybierz polecenie *Review*, aby zobaczyć wszystkie skonfigurowane polityki i obiekty zapory sieciowej.



Dashboard

SD-WAN-622/DC5/root  
DC5\_root

Review

Max Rules Per Page: 10 [Print](#)

### Policy

ID	Source Interface	Destination Interface	Source	Destination	Action	Status	NAT	Service	Schedule	Authentication	Log	Security Profiles	Comments
1	OL_INET_0_OL_MPLS_0	port10	* all	* all	accept	enable	enable	ALL	* always		Log Security Events	no-inspection	
6	OL_INET_0_OL_MPLS_0	port1	* all	* all	accept	enable	enable	ALL	* always		Log Security Events	no-inspection	
3	port2_port3	port10	* all	* all	accept	enable	enable	ALL	* always		Log Security Events	no-inspection default	
4	OL_INET_0_OL_MPLS_0	OL_INET_0_OL_MPLS_0	* all	* all	accept	enable	disable	ALL	* always		Log Security Events	no-inspection	

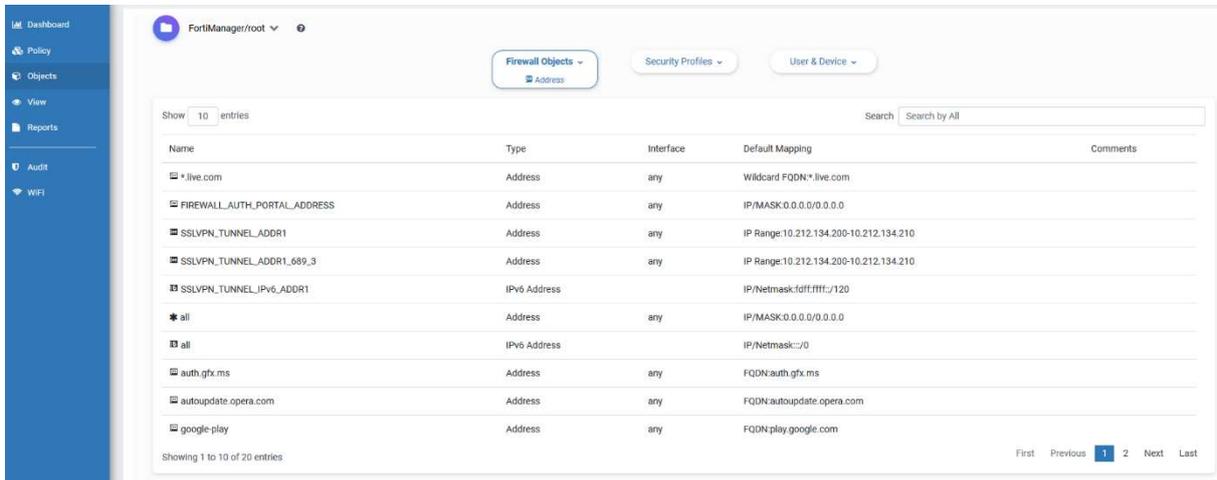
### Address

Name	Type	Interface	Default Mapping	Comments
FABRIC_DEVICE	Address	any	IPMASK:0.0.0.0/0.0.0.0	IPv4 addresses of Fabric Devices.
FGT4_internal	Address	any	IPMASK:10.100.4.0/255.255.255.0	
FGT5_internal	Address	any	IPMASK:10.100.5.0/255.255.255.0	
FIREWALL_AUTH_PORTAL_ADDRESS	Address	any	IPMASK:0.0.0.0/0.0.0.0	
G Suite	Address Group		gmail.com, wildcard.google.com	
HUB1_internal	Address	any	IPMASK:10.201.1.0/255.255.255.0	

Aby wysłać informacje do drukarki lub utworzyć plik PDF należy wybrać opcję *Print*.

## Obiekty

Strona *Objects* udostępnia widok obiektów, które są zdefiniowane w usłudze ONS. Obiekty mogą zawierać elementy takie jak adresy, usługi, definicje ochrony przed włamaniami, sygnatury antywirusowe i profile filtrujące strony internetowe. Można używać obiektu w więcej niż jednej polityce, aby uniknąć powtarzania danych w wielu miejscach.



Name	Type	Interface	Default Mapping	Comments
*live.com	Address	any	Wildcard FQDN:*live.com	
FIREWALL_AUTH_PORTAL_ADDRESS	Address	any	IP/MASK:0.0.0.0/0.0.0.0	
SSLVPN_TUNNEL_ADDR1	Address	any	IP Range:10.212.134.200-10.212.134.210	
SSLVPN_TUNNEL_ADDR1_689_3	Address	any	IP Range:10.212.134.200-10.212.134.210	
SSLVPN_TUNNEL_IPv6_ADDR1	IPv6 Address		IP/Netmask:ffff:ffff::/120	
*all	Address	any	IP/MASK:0.0.0.0/0.0.0.0	
all	IPv6 Address		IP/Netmask::/0	
auth.gfx.ms	Address	any	FQDN:auth.gfx.ms	
autoupdate.opera.com	Address	any	FQDN:autoupdate.opera.com	
google-play	Address	any	FQDN:play.google.com	

Strona zawiera lewy panel i rozwijane menu u góry, które umożliwiają dostęp do obiektów. Po wybraniu pozycji w menu rozwijanym, w panelu głównym wyświetlane są dane związane z obiektami wybranego typu.

## Rodzaje obiektów

Na stronie wyświetlane są następujące kategorie obiektów:

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

Obiekty te zostały opisane w kolejnych rozdziałach.

## Firewall Objects

Obiekty typu firewall obejmują *Address* (adresy), *Schedule* (harmonogram), *Services* (usługi) i *Virtual IP* (wirtualny adres IP).

### Address

Obiekty *Address* mogą określać kraj, FQDN lub podsieć IP i maskę adresów IP. *Address* może odnosić się do wszystkich interfejsów, lub można do obiektu przypisać konkretny interfejs.

Można również utworzyć *Address Group*, która definiuje grupę powiązanych adresów.



## Schedule

Można określić zestaw dni i zakresów czasowych z harmonogramami powtarzalnymi lub jednorazowymi. Obiekt *Schedule* można przypisać później do polityki w celu wskazania w jakich przedziałach czasowych będzie obowiązywać wybrana polityka.

## Service

Chociaż wiele usług jest już skonfigurowanych, system pozwala administratorom na samodzielną ich konfigurację.

Obiekt *Service* określa protokół i wszelkie dodatkowe informacje wymagane do identyfikacji usługi (zależnie od protokołu):

- Dla IP - numer protokołu IP
- Dla TCP/UDP/SCTP – źródłowy i docelowy zakres portów

Można również utworzyć *Service Group*, która definiuje grupę powiązanych usług podstawowych.

## Virtual IP

Wirtualne obiekty IP mapują zewnętrzne adresy IP na adresy wewnętrzne. Opcja jest dostępna tylko w przypadku gdy usługa ONS pracuje z włączoną translacją adresów (NAT).

Usługa ONS obsługuje następujące typy obiektów Virtual IP:

- *IPv4 Pool* - definiuje adres IP lub zakres adresów IP, które mają być używane jako adres źródłowy (inny niż adres IP interfejsu)
- *Virtual IP* - wykorzystuje statyczny NAT do mapowania szeregu adresów zewnętrznych na wewnętrzny zakres adresów
- *VIP Group* - definiuje grupę jednego lub więcej wirtualnych adresów IP, dla ułatwienia administracji.

## Security Profiles

W zależności od wykupionego pakietu usługi ONS dostępne mogą być następujące profile bezpieczeństwa:

- Antivirus Profile
- Application Sensor
- IPS Sensor
- Web Filter Profile
- Local Category
- Rating Overrides
- DNS Filter Profile

### Local Category i Rating Overrides

W usłudze ONS można utworzyć kategorię lokalną dla *Web Filter Profile*, a następnie użyć funkcji *Rating Overrides* do przypisania wybranych adresów URL do nowej kategorii.

Pozwala to na nadpisanie kategoryzacji dostarczonej przez dostawcę usługi. W ten sposób można odblokować lub zablokować dostęp do konkretnych serwisów www z pominięciem standardowej kategoryzacji.

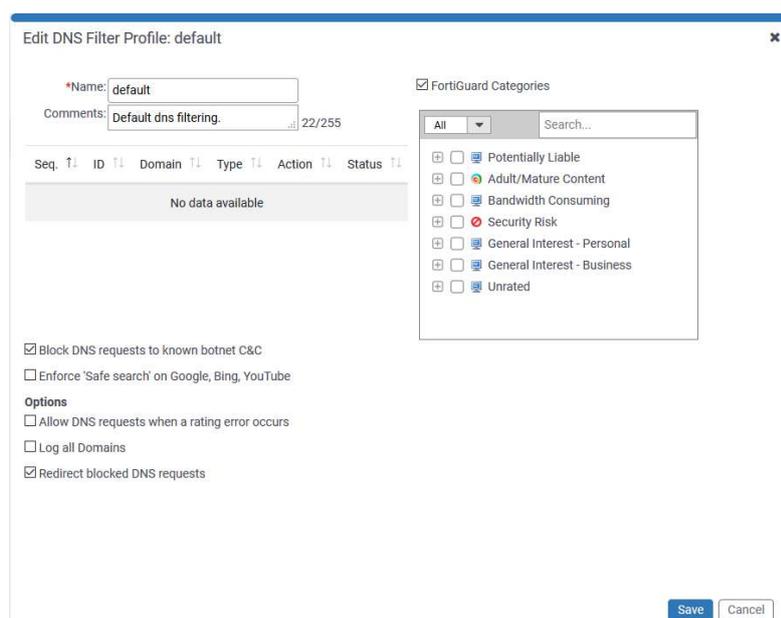
## DNS Filter Profile

Filtrowanie stron internetowych DNS można skonfigurować tak, aby umożliwiać, blokować lub monitorować dostęp do treści internetowych zgodnie ze standardowymi kategoriami zaimplementowanymi w usłudze ONS. Zapytania DNS wracają z adresem IP i oceną domeny, która obejmuje kategorie przypisane stronie internetowej. Następnie otrzymane odpowiedzi są filtrowane wg przypisanej kategorii oraz definicji profilu przygotowanej przez administratora. W ten sposób można się zabezpieczyć przed niepożądanymi połączeniami bez implementowania mechanizmu rozszywania ruchu HTTPS.

Dostawca usługi prowadzi również bazę danych zawierającą listę znanych adresów należących do sieci botnetów i Command and Control (C&C). Jest to baza danych dynamicznie aktualizowana i przechowywana na serwerach dostawcy. Wszystkie zapytania DNS dotyczące botnetów i C&C mogą zostać zablokowane. Mechanizm DNS Filter używa odwróconego dopasowania prefiksu, więc wszystkie połączenia do subdomen będą również zablokowane. Aby włączyć tę funkcję, należy włączyć opcję *Block DNS requests to known botnet C&C* w oknie edycji profilu filtra DNS.

W ramach profilu filtra DNS można również utworzyć statyczną listę filtrów URL obsługiwanych niezależnie od standardowej kategoryzacji. Zapytanie DNS dla domeny, która jest zgodna z domeną na statycznej liście filtrów URL może być zablokowane, monitorowane lub dozwolone. W przypadku zablokowania użytkownik nie może sprawdzić adresu oraz połączyć się ze stroną. Jeśli jest dozwolone, dostęp do strony jest dozwolony, nawet jeśli do jej zablokowania użyto innej metody.

Poniższy rysunek przedstawia okno edycyjne profilu filtra DNS:



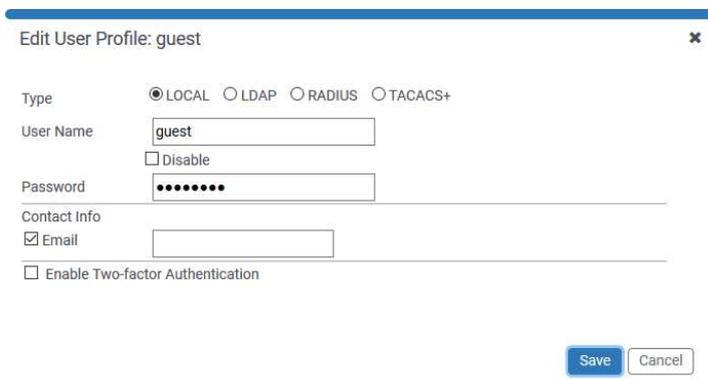
## User & Device

Zasady bezpieczeństwa mogą dopuszczać dostęp tylko do określonych użytkowników i grup użytkowników (typy obiektów w zakładce *User & Device*). Konfiguracja zasad dostępu wymaga kontaktu z dostawcą usługi ONS.

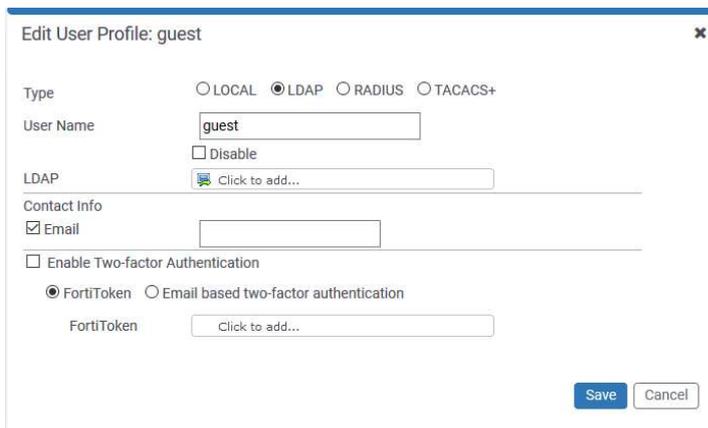
### User Definition

W usłudze ONS można tworzyć użytkowników lokalnych (konta zapisane w usłudze ONS) lub zdalnych (konta zapisane na zdalnym serwerze uwierzytelniania). Usługa ONS obsługuje serwery LDAP, RADIUS i TACACS+.

Na poniższym rysunku przedstawiono okno dialogowe Edit User dla użytkownika lokalnego:



Dla zdalnego użytkownika należy określić zdalny serwer, jak pokazano na poniższym rysunku:



### Dwuskładnikowe uwierzytelnianie (Two-Factor Authentication)

Metody dwuskładnikowego uwierzytelniania, w tym FortiToken, zapewniają dodatkowe bezpieczeństwo. Można włączyć dwuskładnikową metodę uwierzytelniania za pomocą FortiAuthenticator.

Aby użyć dwuskładnikowego uwierzytelniania:

1. Przejdź do menu *Objects*.
2. W menu rozwijanym *User & Device* wybrać opcję *User definition*.

3. Należy kliknąć prawym przyciskiem myszy pod nagłówkiem i wybrać *Create New* lub kliknąć prawym przyciskiem myszy na istniejącą definicję użytkownika i wybrać *Edit*.
4. Należy wybrać opcję *Enable Two-factor Authentication*.
5. Jeśli używany będzie system FortiToken do dwuskładnikowego uwierzytelniania, należy wybrać opcję *FortiToken*.

FortiToken to zewnętrzny generator haseł jednorazowych. Jest to fizyczne urządzenie, które po naciśnięciu przycisku wyświetla sześciocyfrowy kod uwierzytelniający. Kod ten jest wprowadzany razem z nazwą użytkownika i hasłem jako dwuskładnikowe uwierzytelnienie. Wyświetlany kod zmienia się co 60 sekund. Istnieje również aplikacja na telefon komórkowy, FortiToken Mobile, która spełnia te same funkcje. Informacje o FortiToken są szyfrowane w każdym momencie przesyłania. Gdy system otrzyma kod, który odpowiada numerowi seryjnemu danego FortiTokena, jest on dostarczany i przechowywany w postaci zaszyfrowanej. FortiToken może być przypisany tylko do jednego konta.

6. Jeśli używany będzie mechanizm oparty o wiadomość e-mail, należy wybrać opcję *Email based two-factor authentication*.

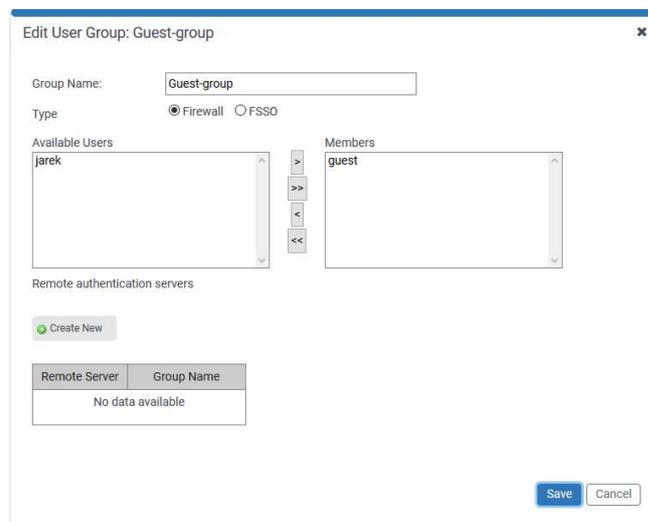
Podczas autoryzacji w oparciu o pocztę elektroniczną system wysyła losowo wygenerowany sześciocyfrowy kod numeryczny na podany adres e-mail. Należy wprowadzić ten kod, gdy pojawi się monit o zalogowanie. Ten kod jest ważny przez 60 sekund.

5. Wybierz opcję *Save*.

## User Group

User Group to lista tożsamości użytkowników. Aby dodać lub edytować grupę użytkowników, należy kliknąć prawym przyciskiem myszy pod wierszem nagłówka i wybrać opcję *Create New* lub *Edit*. Następnie należy wybrać członków grupy z listy dostępnych użytkowników.

Po ustawieniu typu grupy i dodaniu członków, nie można zmienić typu grupy bez usunięcia jej członków.



Dialog box titled "Edit User Group: Guest-group".

Group Name:

Type:  Firewall  FSSO

Available Users:

Members:

Remote authentication servers

Remote Server	Group Name
No data available	



## Konfigurowanie obiektów

Dostawca usługi, w zależności od wykupionego pakietu udziela dostępu do niektórych lub wszystkich obiektów polityki użytkownika. Jeśli tak, można dodawać/edytować/usuwać obiekty wyświetlane na stronie.

### Dodawanie nowego obiektu

1. Należy kliknąć prawym przyciskiem myszy na dowolny obiekt na liście i wybrać polecenie *Create New*.
2. Po modyfikacji odpowiednich pól i należy wybrać polecenie *Save*.

### Aktualizacja obiektu

1. Należy kliknąć prawym przyciskiem myszy na obiekt na liście i wybrać polecenie *Edit*.
2. Po modyfikacji odpowiednich pól i należy wybrać polecenie *Save*.

### Usuwanie obiektu

1. Należy kliknąć prawym przyciskiem myszy na obiekt na liście i wybrać *Delete*.

Jeżeli nowy lub zaktualizowany obiekt jest używany w dowolnej polityce, należy uruchomić funkcję *Installation* w zakładce *Policy*, aby ponownie zainstalować pakiety polityk w usłudze ONS.



## View

W zakładce *View* wyświetlane są informacje dziennika zdarzeń bezpieczeństwa. Zawiera ona filtry i elementy sterujące, które pozwalają na grupowanie logów na różne sposoby, a także przeglądanie szczegóły związane z odpowiednim zestawem logów.

Na górze strony dostępne są następujące przyciski akcji:

- *Application/Attack/Sandbox* - przeglądanie dziennika zdarzeń pogrupowanych według aplikacji, rodzaju ataku, plików analizowanych w Sandbox'ie.
- *Scope* - podgląd dla wszystkich urządzeń lub dla wybranego (jeśli usługa obsługuje więcej niż jedno urządzenie)
- *Set Filter* - filtrowanie danych wg czasu (ostatnie 5 minut, ostatnie 30 minut, ostatnie 60 minut, ostatnie 4 godziny, ostatnie 12 godzin, ostatni 1 dzień, ostatnie 7 dni, lub dla wybranego zakresu dat)
- *Refresh* - odświeżanie danych
- *Sort* - kolumna posiada funkcję sortowania, która pozwala na sortowanie danych w kolejności rosnącej lub malejącej.

Nagłówek tabeli zawiera rozwijane menu wyboru liczby pozycji do wyświetlenia.

Po wybraniu opcji *Application*, *Attack*, *Sandbox* lub *VPN* można wybrać sposób sortowania dzienników zdarzeń.

Poniższe zakładki zawierają różne widoki danych:

- *Application* - uporządkowana według aplikacji. Zobacz sekcję *Widok aplikacji*
- *Attack* - uporządkowany według ataków. Więcej informacji na ten temat znajduje się w części *Widok ataku*.
- *Sandbox* - uporządkowana według analiz wykonanych przez Sandbox. Zobacz sekcję *Sandbox*.
- *Source* - dane ułożone według urządzenia źródłowego.
- *Destination* – dane ułożone według urządzenia docelowego (adres IP, protokół, port).

### Widok aplikacji

Zakładka *Application* w menu *View* wyświetla dzienniki zdarzeń pogrupowane według aplikacji.

Na poniższym rysunku przedstawiono przykładową zakładkę *Application*.



Application Name	Application ID	Category	Sent Bytes	Received Bytes	Sent Packets	Received Packets	Users	Service
Adobe Web (United States)	30061	General Interest	24116	24421	219	222	djang	ADOBE-WEB
Amazon AWS (United States)	27210	Cloud IT	1752	6236	12	10		AMAZON-AWS
Anydesk-Anydesk (France)		Unknown	320	92	6	2	iborkovkha	ANYDESKANYDESK
Anydesk-Anydesk (Germany)		Unknown	1100	892	21	17		ANYDESKANYDESK
Anydesk-Anydesk (Germany)		Unknown	320	112	6	2	hjqiao	ANYDESKANYDESK
Chrome Remote Desktop (United States)	29610	Remote Access	60	52	1	1		HTTPS
Chrome Remote Desktop (United States)	29610	Remote Access	92	92	2			GOOGLE-GMAIL
Chrome Remote Desktop (United States)	29610	Remote Access	303	52	3			HTTPS
Chrome Remote Desktop (United States)	29610	Remote Access	303	52	3			HTTPS
DHCP6		Unscanned	0	0	0	0		DHCP6

## Widok Ataku

Zakładka *Attack* w menu *View* wyświetla dzienniki zdarzeń pogrupowane według nazwy ataku.

Poniższy rysunek przedstawia przykładową zakładkę *Attack*:

Attack Name	Count	Level	Device ID	Attack ID	Policy ID	Service
DNS Amplification Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification Detection		alert	FGT37D4615801346	32784	19	DNS

Po wybraniu jednego z wpisów w tabeli system wyświetla dane dla pierwszego poziomu filtrowania.

Dla każdego z pozostałych filtrów, poziome menu po lewej stronie zawiera przyciski do wykonania następnego poziomu filtrowania (zobacz poniższy rysunek):

Source	Source Port	Source Interface
172.17.65.199	1025	64FortguardDev
172.17.65.199	1053	64FortguardDev
172.17.65.199	1174	64FortguardDev
172.17.65.199	1212	64FortguardDev
172.17.65.199	1374	64FortguardDev
172.17.65.199	1375	64FortguardDev
172.17.65.199	1376	64FortguardDev
172.17.65.199	1378	64FortguardDev
172.17.65.199	1378	64FortguardDev
172.17.65.199	1379	64FortguardDev

Zastosowane filtry są wyświetlane poziomo na ekranie (patrz poprzedni rysunek). Aby usunąć wybrany filtr należy przycisnąć znacznik x znajdujący się obok.

## Sandbox

Zakładka *Sandbox* w menu *View* wyświetla dzienniki zdarzeń związanych z analizami wykonanymi w urządzeniu Sandbox.

Na poniższym rysunku przedstawiono przykładową zakładkę *Sandbox*.

Device ID	Malware Name	Level	Client Device	Risk
No matching records found				

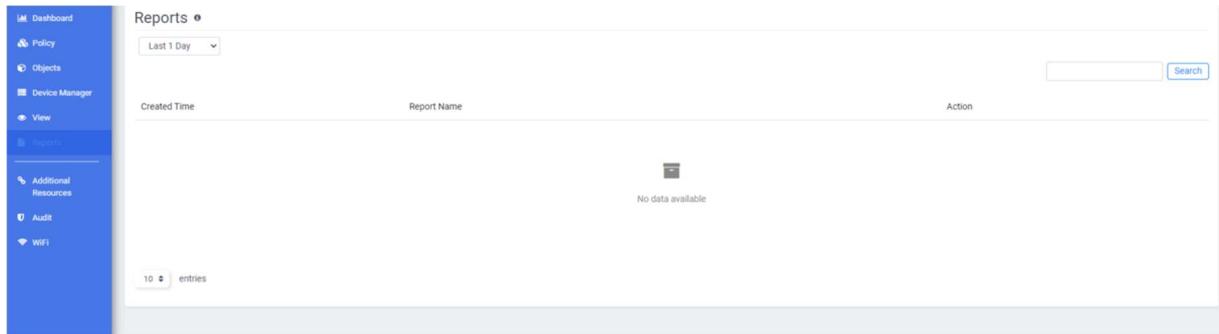
W tym widoku można użyć zakładki *Source* lub *Destination* do filtrowania widoku.

Po wybraniu jednego z wpisów w tabeli, widok danych z Sandboxa działa jak widok *Attacks*. System wyświetla pierwszy poziom filtrowania. Dla każdego z pozostałych filtrów, poziome menu po lewej stronie zawiera przyciski do zastosowania następnego poziomu filtrowania.

Zastosowane filtry są wyświetlane poziomo na ekranie. Aby usunąć wybrany filtr należy przycisnąć znacznik x znajdujący się obok.

## Raporty

Na stronie *Reports* wyświetlana jest lista dostępnych raportów.



## Akcje

Na tej stronie dostępne są następujące akcje:

- *Set Filter* - filtrowanie raportów wg czasu (dzisiaj, ostatni 1 dzień, ostatni 1 tydzień, ostatni 1 miesiąc, lub wybrany zakres dat).
- *Search* - wyszukiwanie tekstowe według nazwy raportu

Po najechaniu kursorem myszki na wybrany raport w kolumnie Akcja pojawia się następująca ikona:

- *Download* - pobieranie wybranego raportu w postaci pliku PDF



## Audit

Zakładka *Audit* wyświetla dziennik aktywności użytkownika w interfejsie administracyjnym:

Audit Log List

Last 60 Minutes Export to CSV Search

Date(GMT)	Level	User Name	Event Type	Client IP Address	Message	Action
2020-06-25 16:01:01	Info	techdoc@fortinet.com	Update device-level SD-WAN	192.168.1.1	Update device-level SD-WAN for adom CorpLogs	Details
2020-06-25 15:57:50	Info	techdoc@fortinet.com	Update device-level SD-WAN	192.168.1.1	Update device-level SD-WAN for adom CorpLogs	Details
2020-06-25 15:57:23	Info	techdoc@fortinet.com	Update device-level SD-WAN	192.168.1.1	Update device-level SD-WAN for adom CorpLogs	Details
2020-06-25 15:57:21	Info	techdoc@fortinet.com	Update device-level SD-WAN	192.168.1.1	Update device-level SD-WAN for adom CorpLogs	Details

10 entries

## Akcje

- *Audit Log List* - ustawianie zakresu czasu wyświetlanych logów (ostatnie 60 minut, ostatni 1 dzień, ostatni 1 tydzień, lub zakres dat)
- *Search* - wyszukiwanie danych według poziomu, nazwy użytkownika, typu zdarzenia, adresu IP użytkownika lub treści.
- *Export to CSV* - eksportowanie listy logów audytowych w postaci pliku CSV.
- *Sort* - pozwala na sortowanie listy logów w kolejności rosnącej lub malejącej według daty zdarzenia.