STORMSHIELD

NEXT GENERATION FIREWALL

PODRĘCZNIK UŻYTKOWNIKA

Stormshield v4

Ostatnia aktualizacja: 2020-01-19 | Opracowanie: DAGMA sp. z o.o.

SPIS TREŚCI

1. Informacje wstępne

Urządzenia STORMSHIELD UTM (Unified Threat Management) integrują w jednej obudowie podstawowe elementy niezbędne do kompletnego zabezpieczenia sieci korporacyjnej. STORMSHIELD UTM to firewall, system wykrywania i blokowania włamań IPS (Intrusion Prevention System), serwer VPN, system antywirusowy, system antyspamowy, system filtrowania dostępu do stron internetowych (filtr URL) oraz system monitorowania bezpieczeństwa sieci.

Ogólnopolskim dystrybutorem rozwiązań STORMSHIELD jest firma DAGMA Sp. z o.o., która świadczy również wsparcie techniczne dla wszystkich klientów, którzy zakupili urządzenia STORMSHIELD UTM w polskim kanale dystrybucyjnym.

Zestawienie najważniejszych parametrów poszczególnych modeli STORMSHIELD UTM:

	SNi40	SN160	SN160W	SN210	SN210W	SN310
Liczba interfejsów 1 Gb	5 0-2***	1+4(switch)	1+4(switch)	2+6(switch)	2+6(switch)	8
WiFi	-	-	802.11 a/b/g/n 2 x SSID	-	802.11 a/b/g/n 2 x SSID	-
Przepustowość FW+IPS [Gbps]	2,9	1	1	1,6	1,6	2,4
Przepustowość antywirus [Gbps]	-	0,26	0,26	0,4	0,4	0,49
Przepustowość IPsec -AES [Gbps]	1,1	0,2	0,2	0,35	0,35	0,6
Liczba jednoczesnych połączeń	500 000	150 000	150 000	200 000	200 000	300 000
Liczba nowych połączeń/sek	20 000	6 000	6 000	15 000	15 000	18 000
VLAN 802.1Q	64	64	64	64	64	64
Tunele IPsec VPN	500	50	50	50	50	100
Portal SSL VPN	75	20	20	20	20	50
Tunele SSL VPN	100	5	5	20	20	20
Dysk twardy	32GB	Karta SD*	Karta SD*	Karta SD*	Karta SD*	Karta SD*

	SN510	SN710	SN910	SN2100	SN3100	SN6100
Liczba interfejsów 1 Gb	12	8–16** 0–8***	8–16** 2–10***	2–26** 0–24 ***	2–26** 0–24***	8–64** 0–64***
Przepustowość FW+IPS [Gbps]	3,3	8	15	35	55	68
Przepustowość antywirus [Gbps]	0,95	2	2,9	7	10	12,5
Przepustowość IPsec -AES [Gbps]	1	2,4	4	8	10	20,5
Liczba jednoczesnych połączeń	500 000	1 000 000	1 500 000	2 500 000	5 000 000	20 000 000
Liczba nowych połączeń/sek	20 000	40 000	60 000	100 000	130 000	146 500
VLAN 802.1Q	256	256	512	1 024	1 024	1 024
Tunele IPsec VPN	500	1 000	1 000	5 000	5 000	10 000
Portal SSL VPN	75	150	300	1 024	1 024	2048
Tunele SSL VPN	100	150	150	400	500	500
Dysk twardy	≥ 250GB	≥ 250GB	≥ 120GB	≥ 250GB	≥ 250GB	≥ 500GB

* Opcja

** Porty miedziane – 1 Gb / 10 Gb

*** Porty światłowodowe – 1 Gb / 10 Gb / 40 Gb (SN2100, SN3100, SN6100)

Każde urządzenie niezależnie od jego wielkości wyposażone jest w ten sam moduł Firewall oraz Intrusion Prevention System. Urządzenia różnią się liczbą interfejsów oraz parametrami związanymi z wydajnością (przepustowość, liczba połączeń, liczba obsługiwanych kanałów VPN). Urządzenia od SN160 do SN310 mają możliwość podłączenia karty SD, a od modelu SN510 urządzania wyposażone są w dysk twardy.

Doboru urządzenia dokonuje się na podstawie charakterystyki sieci (liczba stacji roboczych, liczba serwerów, liczba nowych / jednoczesnych sesji na sekundę, itp.). W przypadku jakichkolwiek wątpliwości prosimy o kontakt z pomocą techniczną na adres mailowy pomoc@stormshield.pl.

Wsparcie Techniczne

W ramach ważnego serwisu użytkownicy rozwiązań STORMSHIELD mają dostęp do wsparcia technicznego w języku polskim. Dział wsparcia technicznego jest dostępny dla Państwa od poniedziałku do piątku w godzinach od 8^{00} do 18^{00} pod numerem telefonu 32 259 11 89. Problemy techniczne można również zgłaszać drogą elektroniczną na adres pomoc@stormshield.pl lub przy użyciu formularza zgłoszeniowego dostępnego na stronie www.stormshield.pl.

Gwarancja na urządzenia

W ramach podstawowej licencji urządzenia STORMSHIELD UTM dostarczone są z podstawowym serwisem gwarancyjnym (STANDARD EXCHANGE). Gwarancja ta określa, iż w przypadku awarii urządzenia zostanie ono wymienione na sprawne w okresie 14 dni roboczych. Istnieje możliwość zakupu specjalnego serwisu zapewniającego wymianę urządzenia na następny dzień roboczy (NEXT BUSINESS DAY/EXPRESS EXCHANGE – tzw. NBD). Co do szczegółów dotyczących tej licencji oraz jej wyceny prosimy o kontakt na adres mailowy kontakt@stormshield.pl lub telefonicznie 32 259 11 00.

Podstawowe funkcje STORMSHIELD UTM:

- Stateful Inspection Firewall,
- Instrusion Prevention System/Intrusion Detection System (IPS/IDS),
- wsparcie protokołów IPv4 i IPv6,
- VPN Server (IPsec VPN, Full SSL VPN, Portal SSL VPN, PPTP VPN),
- uwierzytelnianie i integracja z Microsoft Active Directory lub LDAP,
- kształtowanie pasma (QoS),
- zarządzanie wieloma łączami do Internetu - równoważenie obciążenia / brama zapasowa,
- skaner antywirusowy – ClamAV (http, pop3, smtp, ftp, ssl),
- moduł antyspam,
- filtrowanie stron WWW (http, https),
- centrum certyfikacji PKI,
- serwer DHCP,
- klient NTP,
- monitorowanie w czasie rzeczywistym,
- logowanie zdarzeń,
- tworzenie raportów TOP10,
- STORMSHIELD Visibility Center – system raportowania.

Wszystkie wymienione wyżej funkcje są dostępne w ramach podstawowej licencji.
Funkcje wymagające zakupu rozszerzonej licencji:

- Audyt Podatności - pasywny skaner zagrożeń (SEISMO),
- zaawansowany skaner antywirusowy (http, pop3, smtp, ftp, ssl),
- rozszerzone filtrowanie stron WWW (http, https) w chmurze STORMSHIELD,
- Stormshield Breach Fighter - sandboxing bazujący na chmurze,
- Obsługa protokołów przemysłowych (BACnet/IP, CIP, EtherNet/IP, IEC-60870-5-104, Modbus, OPC UA, OPC (DA/HDA/AE), PROFINET IO / RT, UMAS, S7 200-300-400)

Szkolenia techniczne

Firma Dagma Sp. z o.o. jest autoryzowanym centrum szkoleniowym dla rozwiązań STORMSHIELD. Wszystkie informacje na temat szkoleń technicznych znajdują się na stronie: https://www.acsdagma.com.

2. Instalacja urządzenia STORMSHIELD UTM

Urządzenia STORMSHIELD UTM dostarczone są w białym kartonie zabezpieczonym taśmą z logo firmy DAGMA. Wewnątrz znajduje się oryginalne opakowanie, na którym widoczna jest naklejka z informacją o modelu i numerze seryjnym urządzenia. Oryginalne opakowanie zabezpieczone jest przed otwarciem przeźroczystą taśmą. W przypadku braku bądź uszkodzenia którejkolwiek z taśm prosimy o kontakt ze sprzedawcą lub firmą DAGMA Sp. z o.o..

Po otrzymaniu urządzenia zalecamy przeprowadzenie następujących czynności:

1. weryfikacja zawartości opakowania STORMSHIELD UTM,
2. analiza sposobu podłączenia urządzenia do sieci firmowej.

Weryfikacja zawartości opakowania.

W zależności od modelu, zawartość opakowania może być różna. Dla modeli bez dysku twardego (SN160(W), SN210(W), SN310) opakowanie powinno zawierać:

- urządzenie STORMSHIELD UTM – etykieta na opakowaniu i etykieta na urządzeniu muszą mieć ten sam numer seryjny. Urządzenie musi posiadać oryginalną nienaruszoną plombę (sticker),
- kabel Ethernet RJ45,
- kabel konsolowy USB A-B lub RS-232 – RJ45 (w zależności od modelu),
- kabel zasilający,
- zasilacz 12V/3.33A (SN160, SN160W, SN210, SN210W, SN310),
- quick start guide.

Urządzenie STORMSHIELD UTM można skonfigurować przy wykorzystaniu przeglądarki internetowej za pomocą interfejsu WebGUI lub z poziomu wiersza poleceń (CLI).

Analiza sposobu podłączenia urządzenia do sieci firmowej.

Urządzenie może pracować w trzech trybach (transparentny, router lub mieszany). Domyślnym trybem pracy jest transparentny. W zależności od potrzeb należy wybrać odpowiedni tryb pracy. Różnice pomiędzy tymi trybami pracy zostały opisane w dalszej części instrukcji (sekcja 5 – Tryb pracy). Zachęcamy do zapoznania się z tą sekcją w celu wyboru właściwego trybu pracy urządzenia.

3. Pierwsze podłączenie do urządzenia

Zaleca się aby pierwszego podłączenia do urządzenia dokonać, gdy:

- zweryfikowano zawartość opakowania,
- wybrano sposób podłączenia urządzenia STORMSHIELD UTM do sieci.

> **Uwaga!**
>
> Urządzenie STORMSHIELD UTM można podłączyć do zasilania jedynie przy pomocy zasilacza dostarczonego przez producenta. Jeżeli istnieje podejrzenie, iż zasilacz jest uszkodzony lub widoczne są mechaniczne uszkodzenia wtyku/gniazda zasilacza należy zaniechać podłączenia i zgłosić zaistniałą sytuację na pomoc@stormshield.pl

> **Uwaga!**
>
> Urządzenie STORMSHIELD UTM należy podłączyć do zasilania poprzez listwę zabezpieczająca przed przepięciami lub z wykorzystaniem urządzenia UPS.

> **Uwaga!**
>
> Wyłączenie urządzenia STORMSHIELD UTM z zasilania musi odbywać się zgodnie z zaleceniami producenta. Służy do tego odpowiednia opcja dostępna z konsoli WebGUI w sekcji *Konfiguracja >Moduły > USTAWIENIA SYSTEMOWE > System > Konfiguracja > System > Zatrzymaj* lub polecenie **`halt`** z linii poleceń.

Podłączenie do urządzenia jest możliwe przy wykorzystaniu:

- przeglądarki WWW (wspierane przeglądarki: Firefox, Chrome, Edge),
- klienta SSH (np. PuTTY),
- portu konsolowego USB lub RS-232 (np. PuTTY),
- klawiatury oraz monitora bezpośrednio podłączonych do urządzenia (wybrane modele).

W domyślnej konfiguracji modyfikację ustawień urządzenia możemy wykonać przy użyciu konsoli WWW (domyślny, zalecany sposób) bądź bezpośrednio korzystając z portu konsolowego (dla użytkowników zaawansowanych). W dalszej konfiguracji można dodatkowo włączyć dostęp SSH.

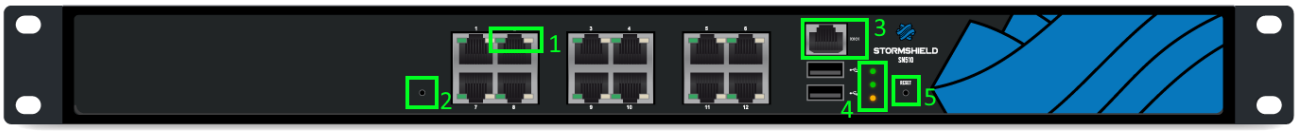
Konsola WebGUI urządzenia dostępna jest domyślnie pod adresem https://10.0.0.254/admin
W celu dokonania wstępnej konfiguracji urządzenia zalecamy podłączyć komputer do portu nr 2, który domyślnie jest skonfigurowany pod nazwą IN.

Na poniższym rysunku zaznaczono ten port kolorem zielonym:

Komputer podłączony do tego portu otrzyma z serwera DHCP adres IP z zakresu 10.0.0.10-10.0.0.100 z maską 255.0.0.0.

> **Uwaga**
> Jeżeli kabel Ethernet nie zostanie podłączony do prawidłowego portu to nie będzie możliwe podłączenie się do urządzenia poprzez przeglądarkę (WebGUI). Przełączanie się pomiędzy interfejsami urządzenia może uruchomić tzw. Antispoofing Mechanism, który zablokuje cały ruch IP z komputera do urządzenia. Należy wtedy ponownie uruchomić urządzenie.
> Do ponownego uruchomienia urządzenia z poziomu CLI można użyć polecenia **`reboot`**.

Widok urządzenia SN510:



1. Diody przy interfejsach:
   - lewa – stan pracy interfejsu – światło ciągłe oznacza połączenie, miganie oznacza transfer danych,
   - prawa – szybkość interfejsu – wyłączona – 10Mbps, kolor zielony – 100 Mbps, kolor żółty 1Gbps.
2. Przycisk przywrócenia konfiguracji do ustawień fabrycznych (brak opisu).
3. Port konsoli urządzenia (RJ45 - RS-232).
4. Diody sygnalizujące stan systemu (od góry):
   - urządzenie w trybie online (urządzenie gotowe do pracy), w przypadku konfiguracji klastra HA migająca dioda oznacza urządzenie pasywne,
   - uruchamianie/zatrzymywanie systemu operacyjnego,
   - sygnalizacja stanu zasilania (dioda pomarańczowa).
5. Przycisk restartu urządzenia (opis: RESET).

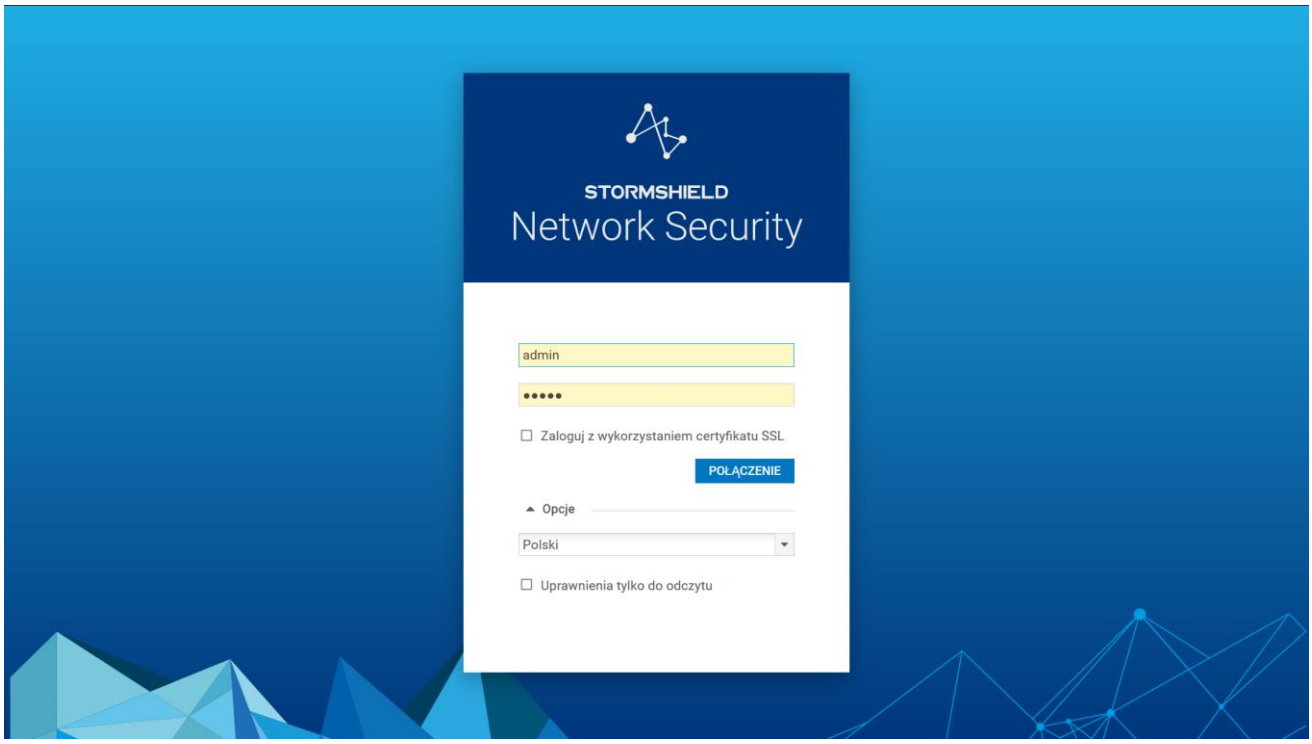
Konsola STORMSHIELD WebGUI

Dostęp do konsoli WebGUI można uzyskać po podaniu loginu i hasła. Konfiguracja pozwala także na autoryzację z wykorzystaniem certyfikatu SSL. Wymaga to jednak wcześniejszej konfiguracji serwera PKI na urządzeniu.

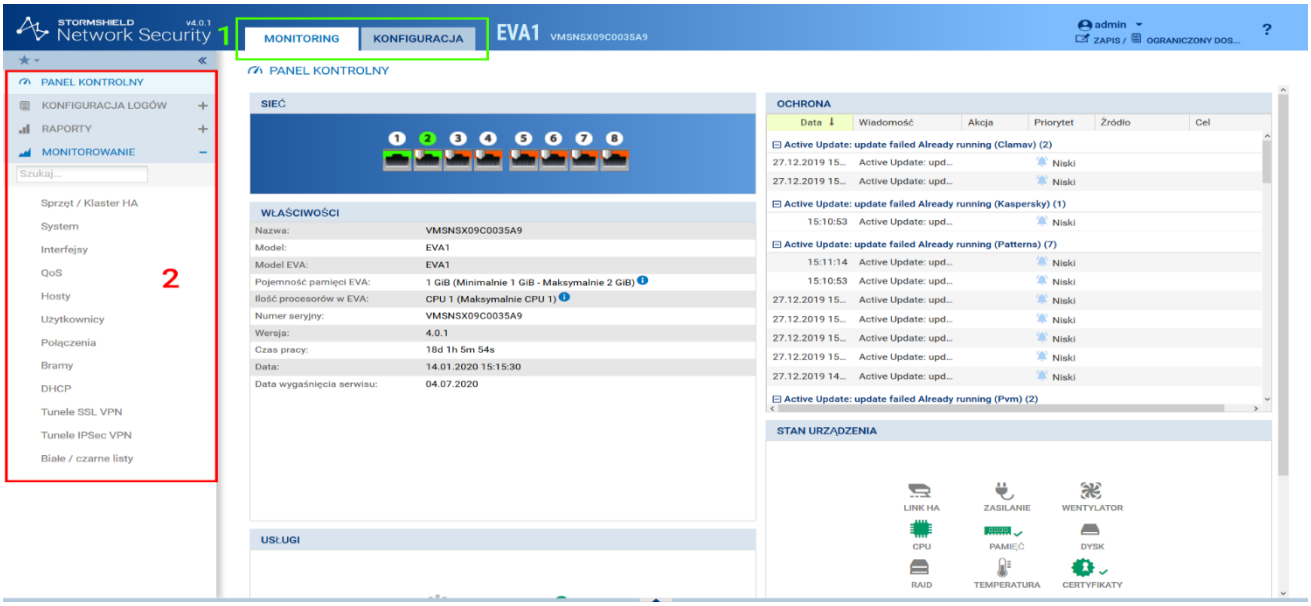
Pozycja *„Opcje”* pozwala zmienić język interfejsu lub zalogować się z uprawnieniami *„tylko do odczytu*”.

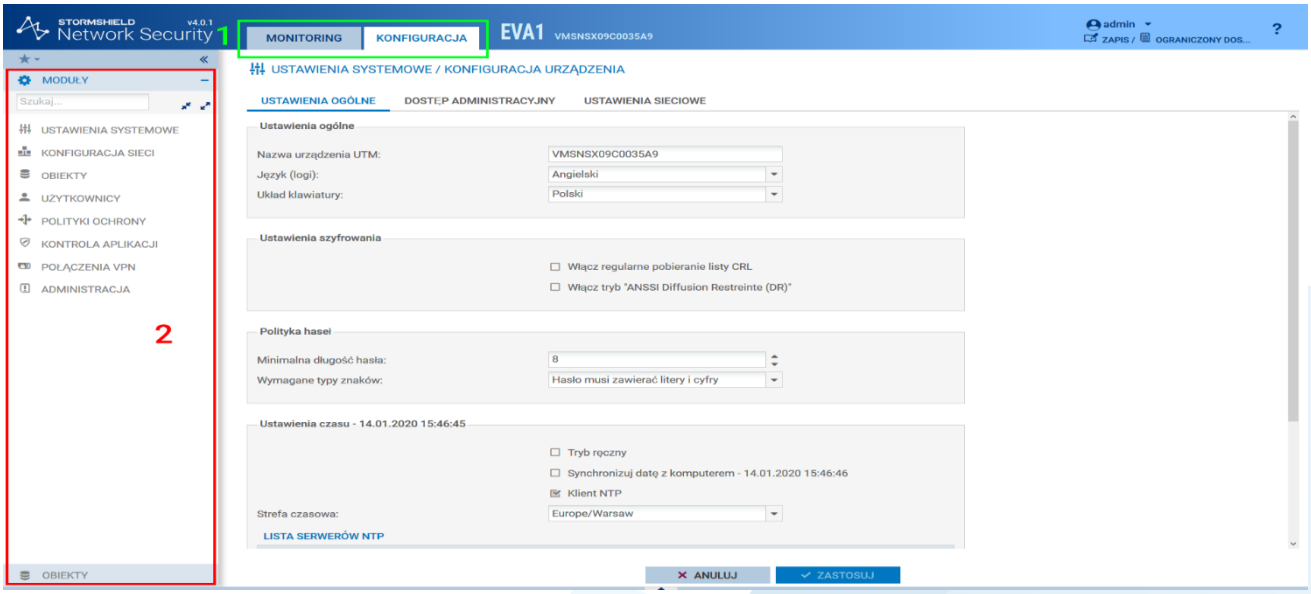
W domyślnej konfiguracji do konsoli można dostać się przy użyciu następujących poświadczeń:

- użytkownik: **admin**
- hasło: **admin**



Pomyślna autoryzacja na urządzeniu spowoduje wyświetlenie interfejsu urządzenia – WebGUI.
W przypadku firmware 4.x różni się on od wcześniejszych wersji i został podzielony na dwie zakładki – Monitoring oraz Konfiguracja [1]. Po lewej stronie ekranu [2] znajduje się menu z opcjami konfiguracji / monitoringu.
W zakładce Monitoring administratorzy mogą monitorować działanie samego urządzenia, jak i ruch przechodzący przez urządzenie oraz przeglądać zarejestrowane logi.
W zakładce Konfiguracja administratorzy mają możliwość konfiguracji urządzenia.
Zaletą takiego podziału interfejsu jest możliwość przełączania się pomiędzy zakładkami, bez utraty stanu obecnej pracy.
Przykładowo, jeżeli administrator konfiguruje regułę firewall i w trakcie tej konfiguracji, jeszcze przed jej zapisem, potrzebuje sprawdzić coś w logach urządzenia, wystarczy, że przełączy się do zakładki Monitoring, gdzie sprawdzi potrzebne dane, a następnie powróci do edycji reguły firewall, która będzie w takim stanie jaką ją pozostawił.



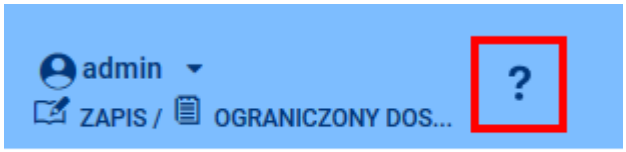


Pomoc kontekstowa

W prawym górnym rogu interfejsu WebGUI, po kliknięciu na znak zapytania otworzy się dokumentacja opisująca poszczególne elementy i funkcje interfejsu WebGUI.

Pomoc działa w sposób kontekstowy tj. po kliknięciu znaku zapytania otwierana jest dokumentacja do aktywnego modułu konfiguracji urządzenia.

Dokumentacja ta dostępna jest jedynie w języku angielskim i francuskim.



STORMSHIELD
TECHNICAL DOCUMENTATION

Management Center

SNS v4 / SMC | Release Notes | Guides | SNS Technical Notes | PDF download

Search

Guides > SNS > User Manual > User Manual > CONFIGURATION

USER MANUAL
- WELCOME
- ACCESS PRIVILEGES
- ACTIVE UPDATE
- LOGS - AUDIT LOGS
- ADMINISTRATORS
- ANTISPAM
- ANTIVIRUS
- APPLICATIONS AND PROTECTIONS
- AUTHENTICATION
- BLOCK MESSAGES
- CERTIFICATES AND PKI
- CLI CONSOLE
- CONFIGURATION
  - "General configuration" tab
  - "Firewall administration" tab
  - "Network settings" tab
- CONFIGURATION OF MONITORING
- DASHBOARD
- DHCP

CONFIGURATION

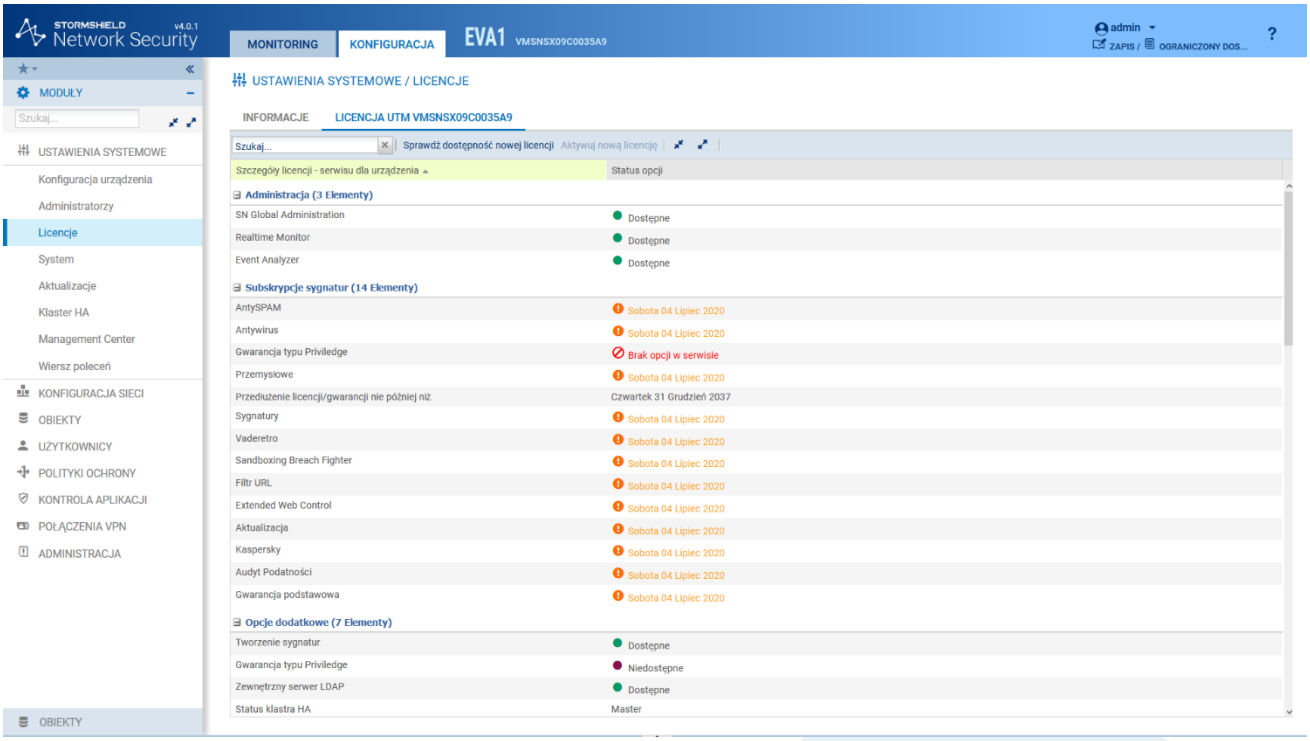
The configuration-administration screen consists of 3 tabs:

- *General configuration*: definition of the firewall's settings (name, language, keyboard), date and time settings and NTP servers.
- *Firewall administration*: configuration of access to the firewall's administration interface (listening port, SSH etc.)
- *Network settings*: Ipv6 activation, configuration of the proxy server and DNS resolution.

"General configuration" tab
"Firewall administration" tab
"Network settings" tab

4. Podstawowa konfiguracja

Po pierwszym zalogowaniu się do urządzenia należy zweryfikować poprawność licencji. Można to zrobić w menu konfiguracji licencji (KONFIGURACJA > USTAWIENIA SYSTEMOWE > Licencje -> LICENCJA UTM …)

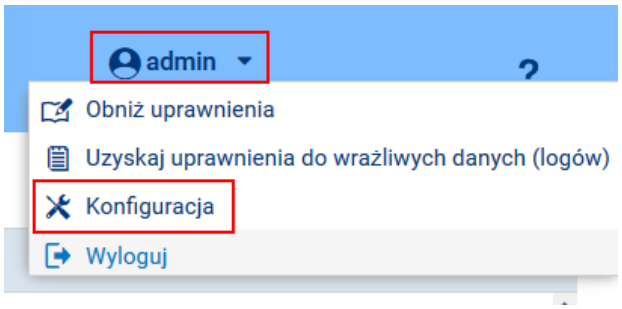


Wstępną konfigurację można podzielić na następujące etapy:

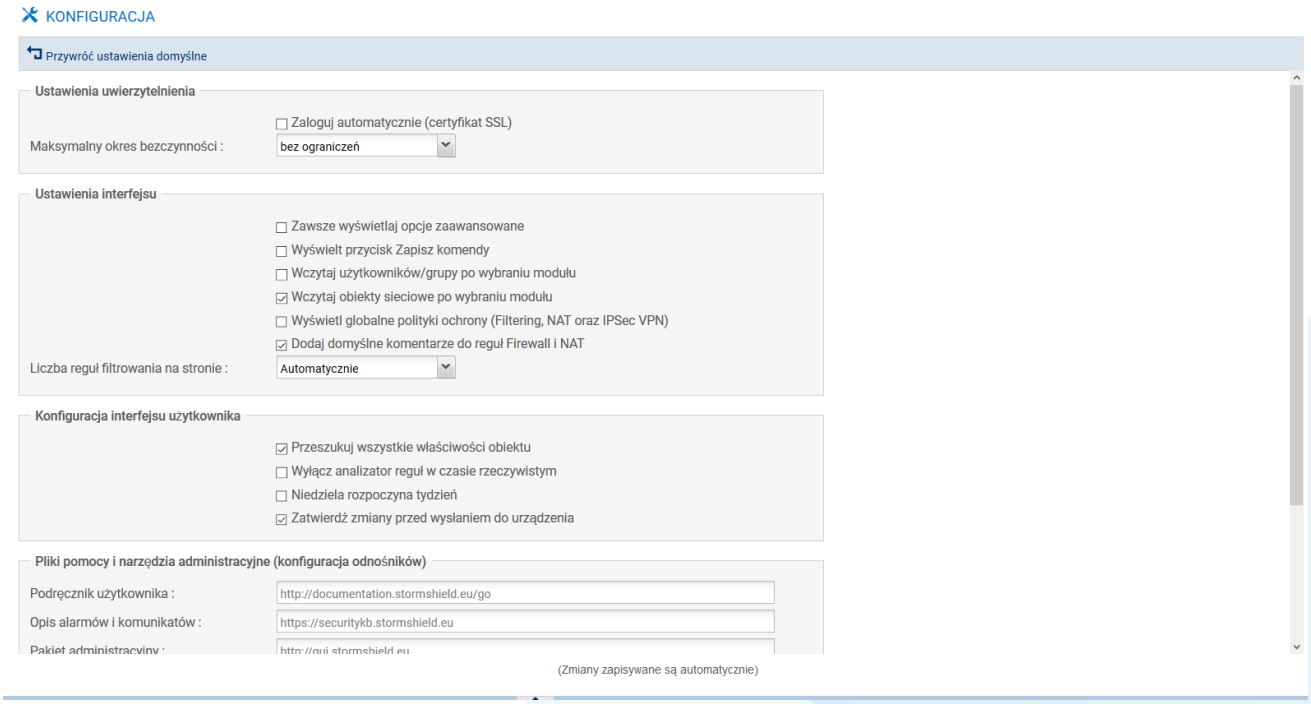
- konfiguracja ustawień WebGUI,
- ogólne ustawienia dotyczące samego urządzenia,
- konfiguracja/zmiana hasła dla użytkownika **admin**,
- konfiguracja obiektów,
- konfiguracja interfejsów urządzenia (trybu pracy),
- konfiguracja usługi DHCP,
- ustawienie bramy domyślnej na urządzeniu (routing),
- konfiguracja zapory (firewall),
- konfiguracja translacji adresów (NAT).

Konfiguracja ustawień WebGUI

W pierwszej kolejność należy skonfigurować parametry panelu administracyjnego WebGUI. W tym celu należy użyć przycisku Konfiguracja, który znajduje się w menu dostępnym po kliknięciu nazwy zalogowanego użytkownika w prawym górnym rogu interfejsu WebGUI.



Zmiany w konfiguracji w tej części są aktywowane automatycznie w chwili ustawienia nowej wartości (nie ma potrzeby zatwierdzania zmian).



Ustawienia uwierzytelnienia

- Zaloguj automatycznie (certyfikat SSL) – uruchamia automatyczne logowanie do WebGUI w przypadku, gdy mamy zaimportowany certyfikat SSL użytkownika o uprawnieniach administracyjnych.
- Maksymalny okres bezczynności – pozwala określić czas (domyślnie 5 min), po którym nastąpi automatyczne wylogowanie z konsoli w wypadku braku aktywności.

Ustawienia interfejsu

W tej sekcji można zdecydować aby opcje Zaawansowane, które domyślnie są zwinięte, były zawsze rozwinięte i widoczne w oknie konfiguracyjnym.

Zaznaczenie opcji *Wczytaj użytkowników/grupy po wybraniu modułu* oraz *Wczytaj obiekty sieciowe po wybraniu modułu* spowoduje, iż w modułach konfiguracji użytkowników i obiektów sieciowych elementy te zostaną wyświetlone po przejściu do tych sekcji. Gdy opcja ta jest odznaczona użytkownicy bądź obiekty sieciowe będą wczytane dopiero po wybraniu odpowiedniego filtra (np. tylko obiekty typu host).
Zaznaczenie opcji *Wyświetl globalne polityki ochrony* spowoduje pojawienie się w konfiguracji Firewall i NAT, IPsec VPN oraz Obiekty sieciowe ustawień globalnych, współdzielonych przez wszystkie urządzenia centralnie zarządzane z wykorzystaniem serwera centralnego zarządzania Stormshield Management Center (SMC).

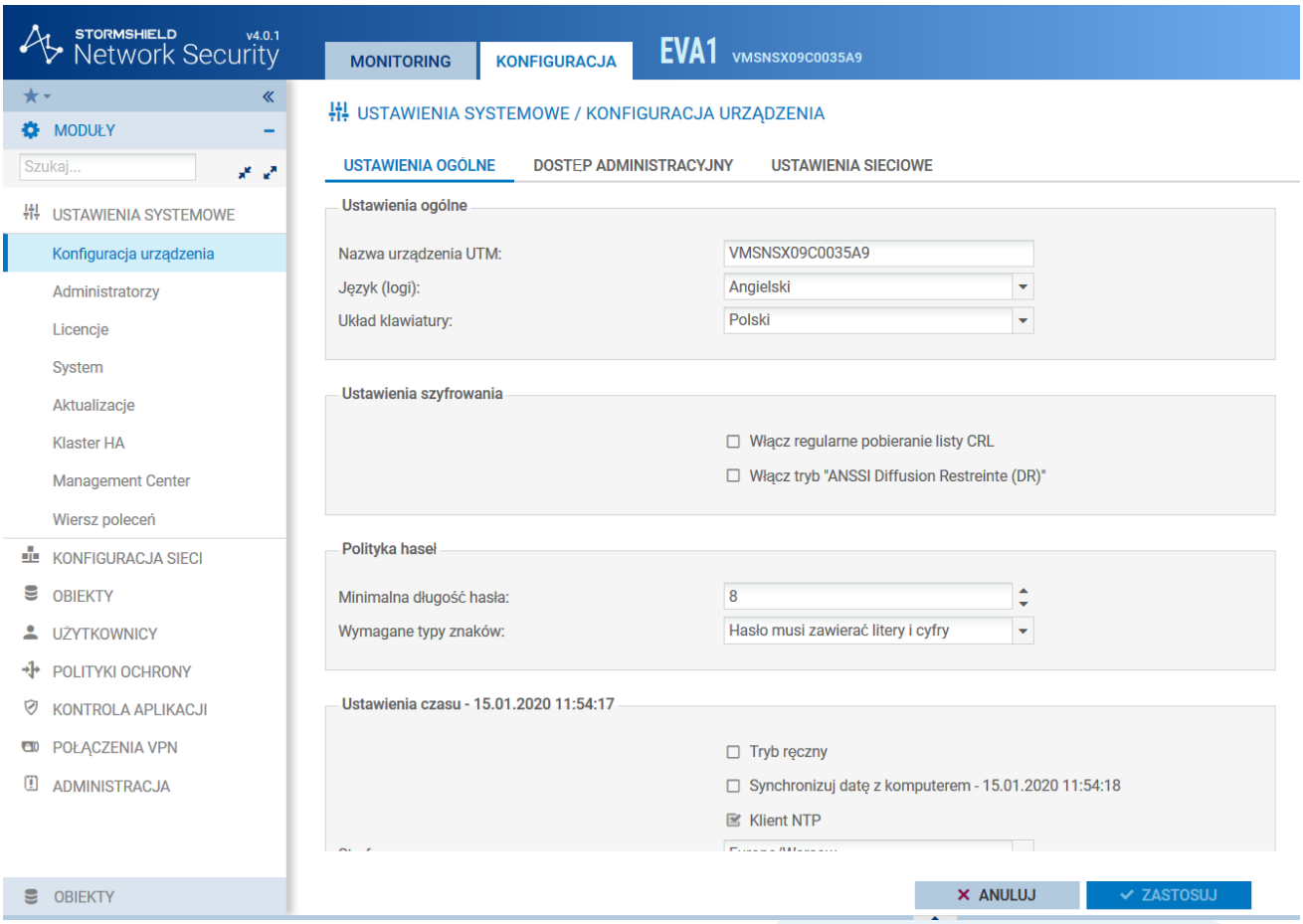
Dostęp do danych wrażliwych

W celu zapewnienia zgodności z rozporządzeniem GDPR (RODO) dane osobowe takie jak nazwa użytkownika, źródłowy adres IP, źródłowy adres MAC, nazwa hosta źródłowego, domyślnie nie są prezentowane w logach i raportach i są zastąpione słowem ***Anonymized***. W celu uzyskania dostępu do tych danych administrator musi kliknąć na opcję ***Uzyskaj dostęp do wrażliwych danych (logów)*** znajdującą się w menu dostępnym po kliknięciu nazwy zalogowanego użytkownika w prawym górnym rogu interfejsu WebGUI.

Ogólne ustawienia dotyczące samego urządzenia

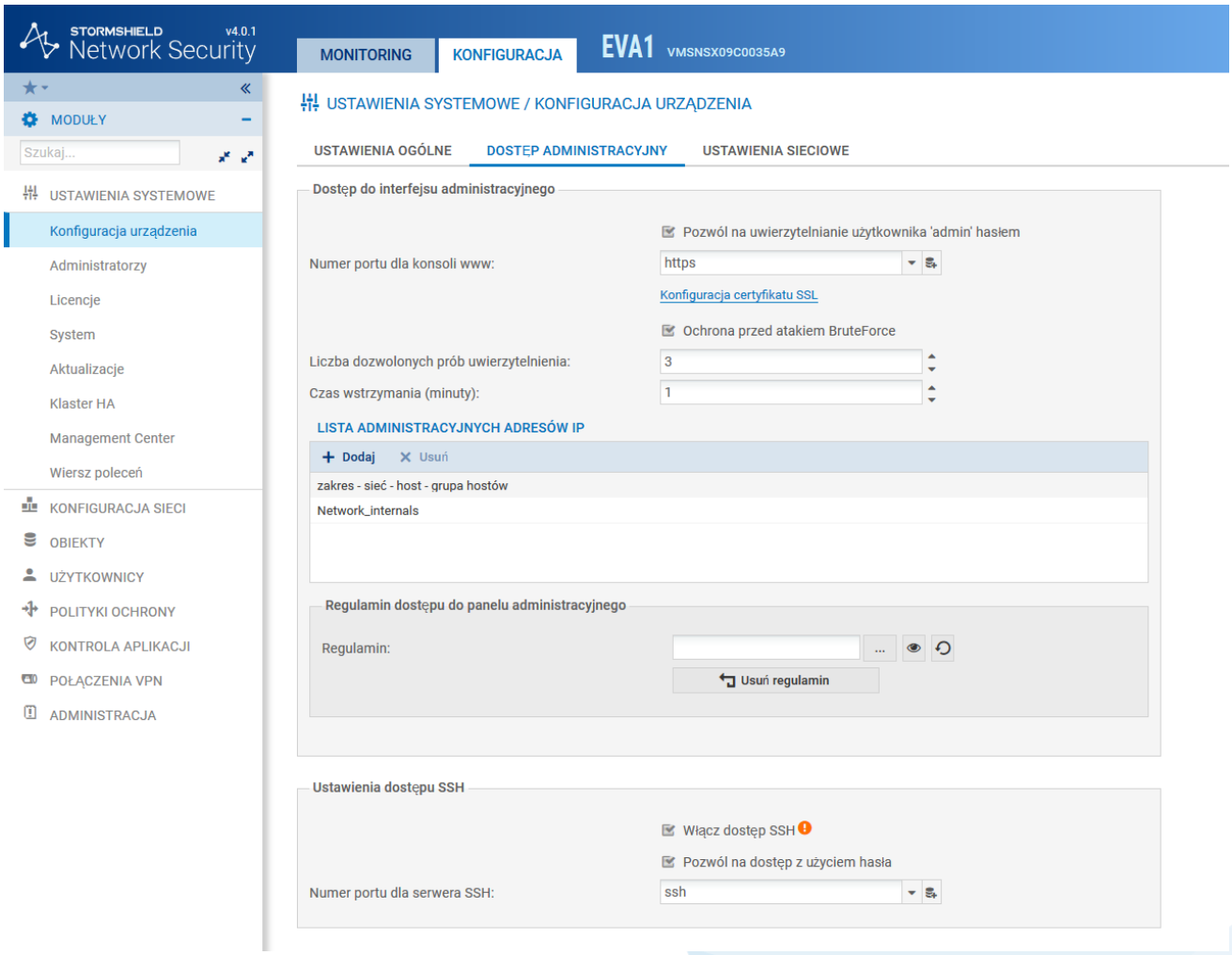
Ogólnych ustawień urządzenia dokonujemy w sekcji KONFIGURACJA > USTAWIENIA SYSTEMOWE > Konfiguracja urządzenia.

W pierwszej zakładce, Ustawienia ogólne, można skonfigurować m.in. nazwę urządzenia, język (kodowanie znaków w logach) i wybrać układ klawiatury. Można tutaj również skonfigurować politykę haseł, czas urządzenia oraz strefę czasową. Alternatywnie można wskazać serwer NTP (serwer czasu), z którym STORMSHIELD UTM będzie synchronizował czas.



Zakładka **Dostęp administracyjny** pozwala skonfigurować dostęp do urządzenia. Znajdziemy tutaj między innymi możliwość ustawienia portu, na którym będzie działał portal administracyjny (domyślnie jest to port https – 443 TCP), adresu/adresów IP które będą miały dostęp do WebGUI oraz mechanizmu zapobiegania atakom typu *Brute Force*.

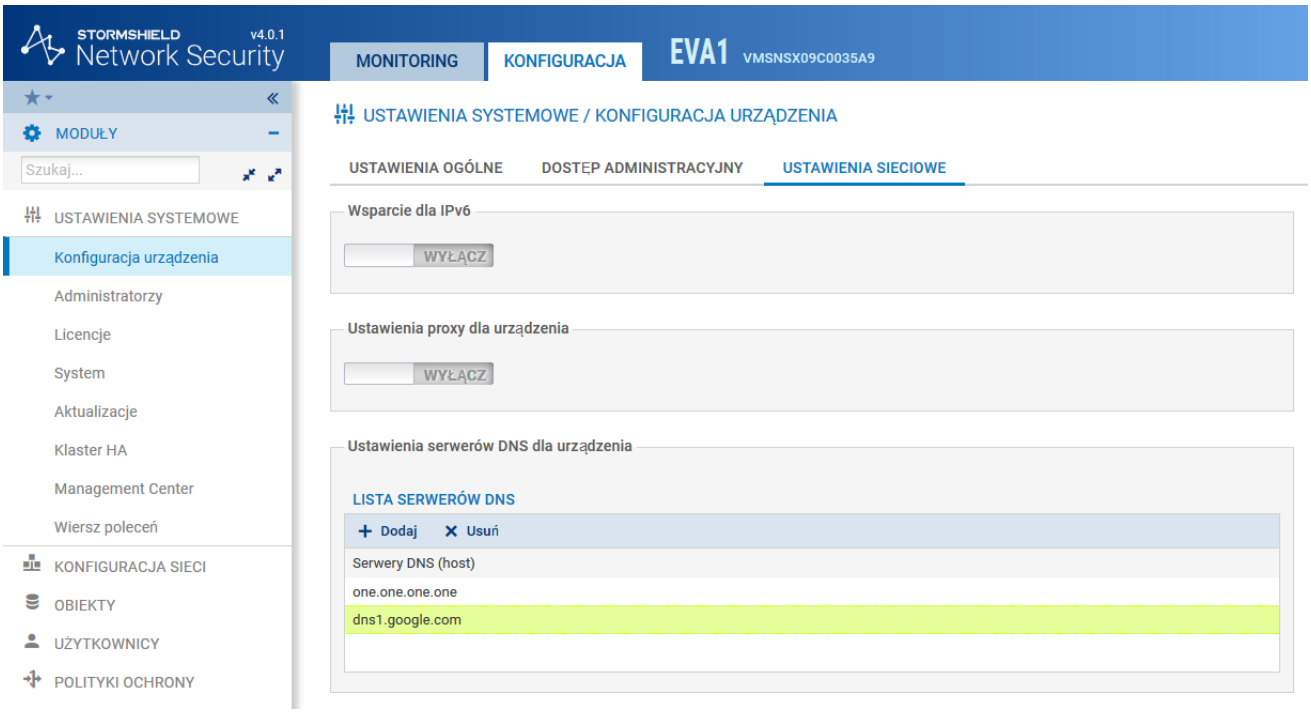
W dolnej części okna można włączyć dostęp do urządzenia poprzez konsolę SSH.



Jeśli STORMSHIELD UTM do komunikacji z Internetem musi łączyć się przez zewnętrzny serwer Proxy, to w zakładce **Ustawienia sieciowe** można skonfigurować dane dostępowe do tego serwera.
Można tutaj również wskazać z jakich serwerów DNS ma korzystać STORMSHIELD UTM przy rozwiązywaniu nazw. Skonfigurowanie tej opcji jest niezbędne do poprawnego pobierania aktualizacji przez urządzenie.

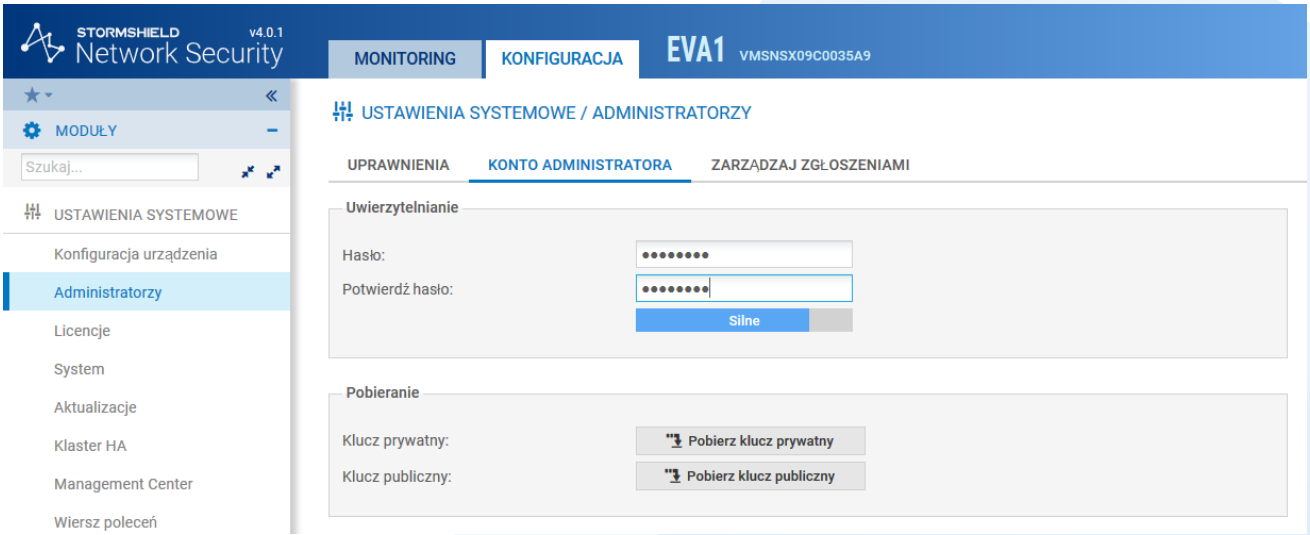
Zakładka ta umożliwia również uruchomienie wsparcia dla protokołu IPv6 tj. filtrowania, analizowania ruchu IPv6 oraz działania usługi dhcpv6.

Uwaga!
Włączenie wsparcia dla IPv6 wymaga restartu urządzenia, ponadto operacji tej nie można cofnąć. Dlatego przed jej uruchomieniem należy koniecznie wykonać backup konfiguracji.



Konfiguracja/zmiana hasła dla użytkownika admin

Pierwsze logowanie do urządzenia odbywa się z użyciem konta ***admin*** i hasłem ***admin***. Hasło admin jest hasłem startowym. Należy je zmienić zaraz po pierwszym logowaniu. Można tego dokonać w sekcji KONFIGURACJA > USTAWIENIA SYSTEMOWE > Administratorzy w zakładce Konto Administratora.



W tej zakładce znajdują się również klucze (prywatny i publiczny), umożliwiające logowanie do urządzenia poprzez SSH bez konieczności podawania hasła.

Uwaga!
Konto **admin** jest jedynym kontem, które ma możliwość logowania się go usługi SSH.

Konfiguracja obiektów

Obiekty to podstawowy element konfiguracji STORMSHIELD UTM. Obiekt symbolizuje element sieci komputerowej.

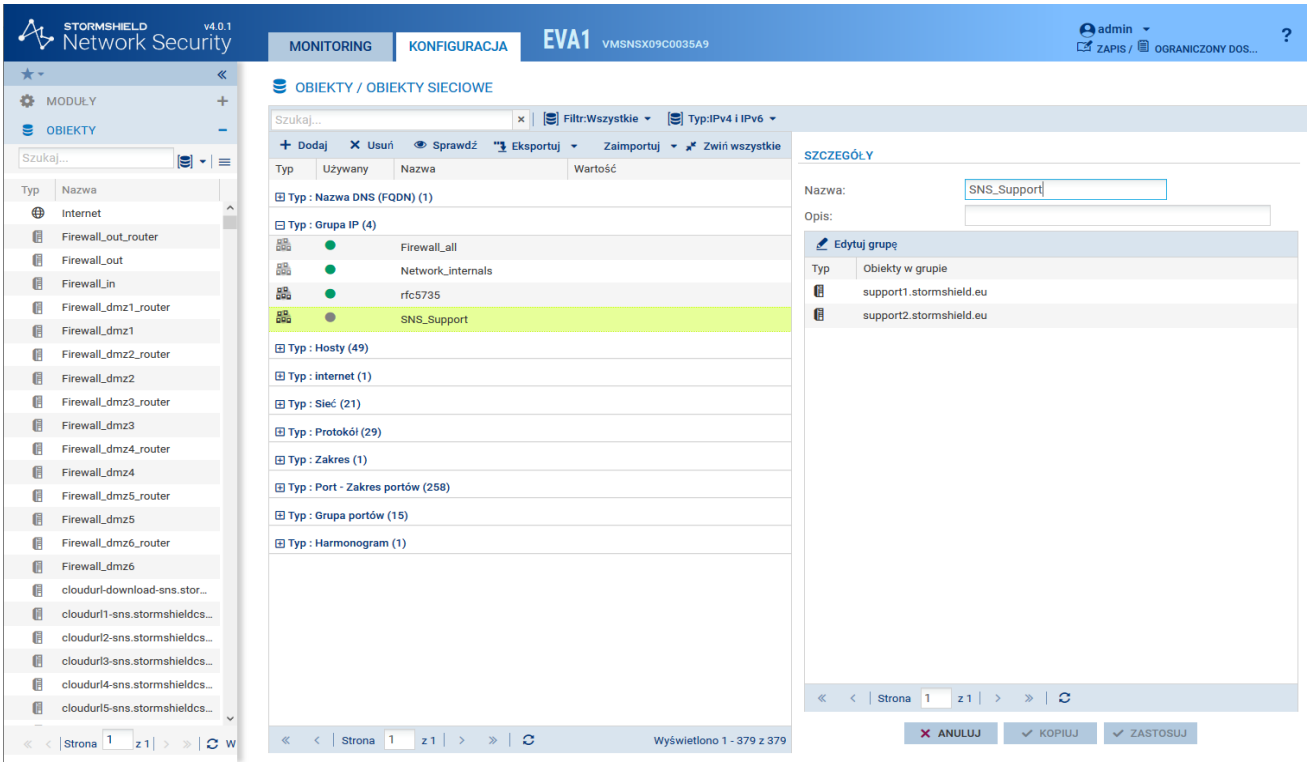
Obiekty można podzielić na następujące typy:

- **Host (Host) –** reprezentuje pojedynczy adres IP,
- **Nazwa DNS (FQDN) (DNS name (FQDN))** – dynamiczny obiekt, który reprezentuje nazwę DNS (FQDN) czyli taką, która może być powiązana z wieloma adresami IP. Obiekty tego typu mogą być użyte jedynie jako adres źródłowy lub docelowy reguł firewall. Nie można ich grupować,
- **Sieć (Network)** – adres IP i maska. Obiekt reprezentuje wszystkie adresy IP we wskazanej sieci,
- **Zakres (IP address range)** – zakres adresów IP wykorzystywany np. w konfiguracji DHCP,
- **Router** – reprezentuje bramy sieciowe dostawców internetowych i relacje w jakich te bramy działają (Load Balancing, Backup Gateways). Obiektu tego typu można użyć zarówno w podstawowej konfiguracji routingu domyślnego jak i w politykach firewall jako routing na podstawie reguł, tzw. Policy Based Routing (PBR),
- **Protokół (IP protocol)** – protokół sieciowy,
- **Port (Port)** – port, na którym nasłuchuje usługa (TCP / UDP/ SCTP),
- **Obiekt harmonogramu (Time object)** – obiekt, który reprezentuje dowolnie zadeklarowany przedział czasu, także w powtarzających się cyklach. Obiekt taki może zostać użyty do aktywacji wybranej reguły firewall wg. wskazanego harmonogramu.

Obiekty odpowiedniego typu można grupować:

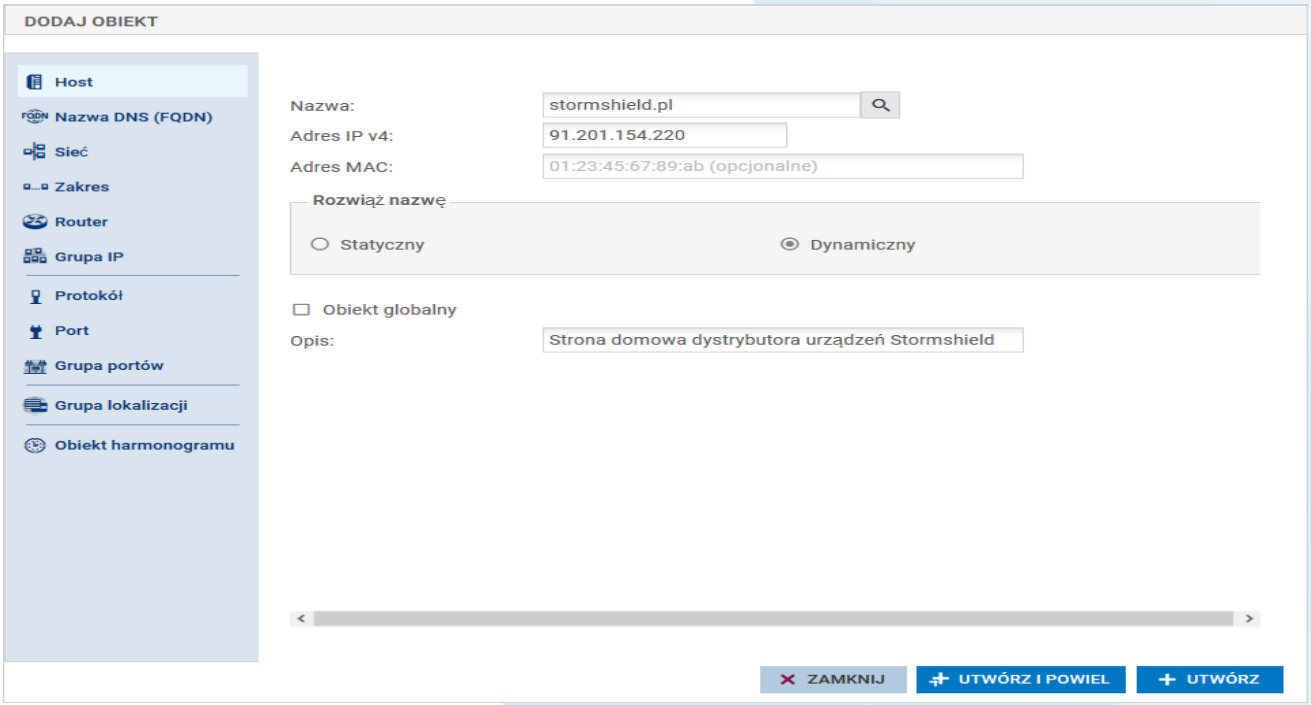
- **Grupa portów (Port group)** – grupa obiektów typu port,
- **Grupa IP (Group)** – grupa obiektów, w skład której mogą wchodzić obiekty typu **Host**, **Zakres**, **Sieć**,
- **Grupa lokalizacji (Region group)** – grupa obiektów lokalizacji IP, w skład której mogą wchodzić kraje lub kontynenty.

Aby utworzyć nowy obiekt należy przejść do sekcji **KONFIGURACJA > OBIEKTY > Obiekty sieciowe** i kliknąć przycisk ***Dodaj***.



Obiekty można również tworzyć będąc w oknie konfiguracyjnym dowolnego z modułów, jeśli opcja którą chcemy skonfigurować wymaga wskazania obiektu, to poza listą już istniejących obiektów, dostępna jest również ikona  14, po kliknięciu której otworzy się okno dodawania obiektu odpowiedniego typu.

Tworzenie obiektu typu Host: Obiekt Host reprezentuje powiązanie nazwy z adresem IP (jest to relacja 1:1).



W polu **Nazwa** należy wpisać nazwę pod jaką obiekt będzie widoczny w konfiguracji urządzenia. Może to być nazwa DNS co pozwoli na automatyczne rozwiązywanie nazwy na **Adres IP** w przypadku zaznaczenia opcji **Dynamiczny**. Opcja ta powoduje, że UTM co 5 minut odpytuje serwery DNS o rozwiązanie nazwy obiektu na adres IP. Wybór opcji **Statyczny** powoduje, że powiązanie **Nazwy** i **Adresu IP** jest trwałe i może być zmienione jedynie poprzez edycję obiektu. Do obiektu można również przypisać adresu MAC. Opcja ta jest wykorzystywana w przypadku konfiguracji serwera DHCP i korzystania ze statycznych rezerwacji adresów IP dla komputerów lub do filtrowania ruchu w regułach firewall na podstawie adresu MAC.

Uwaga!

Skonfigurowanie pola Adres MAC powoduje stworzenie statycznego wpisu w tablicy ARP urządzenia. Jeśli wartość tego pola będzie inna niż rzeczywisty adres MAC komputera o podanym adresie IP komunikacja z nim nie będzie możliwa.

Konfiguracja pozostałych typów obiektów jest analogiczna jak dla obiektu **Host** z uwzględnieniem charakterystycznych pól dla każdego z tych obiektów.

Uwaga!

STORMSHIELD UTM posiada wstępnie skonfigurowaną pulę obiektów i są to głównie obiekty typu Protokół oraz Port.
Część obiektów jest tworzona na etapie konfiguracji urządzenia i są to np. obiekty reprezentujące adres IP oraz sieć skonfigurowane na interfejsie urządzenia. Nazwy takich obiektów rozpoczynają się od frazy **Firewall_** oraz **Network_**, gdzie po znaku "_" umieszczana jest nazwa interfejsu (np. Firewall_in). Obiekty **Firewall_** oraz **Network_** nie mogą być edytowane, ponadto nie można stworzyć ręcznie obiektu, którego nazwa zaczynałaby się od tych fraz.

Wskazówka

Informacje o obiektach typu **Host**, **Zakres**, **Sieć**, **Protokół** oraz **Port** przechowywane są w pliku:
`/usr/Firewall/ConfigFiles/object`

Informacje o obiektach typu **Grupa IP** i **Grupa portów** umieszczone są w pliku:
`/usr/Firewall/ConfigFiles/objectgroup`

Informacje o obiektach typu **Router** umieszczone są w pliku:
`/usr/Firewall/ConfigFiles/router`

Synchronizację obiektów dynamicznych można przeprowadzić ręcznie z poziomu wiersza poleceń (SSH lub konsola) używając polecenia:
`objectsync`

5. Tryb pracy urządzenia

Tryb pracy urządzenia STORMSHIELD UTM zależy od roli jaką ma pełnić w sieci. Tryb pracy określa relację pomiędzy interfejsami. Konfiguracja trybu pracy urządzenia odbywa się w sekcji KONFIGURACJA > KONFIGURACJA SIECI > Interfejsy.

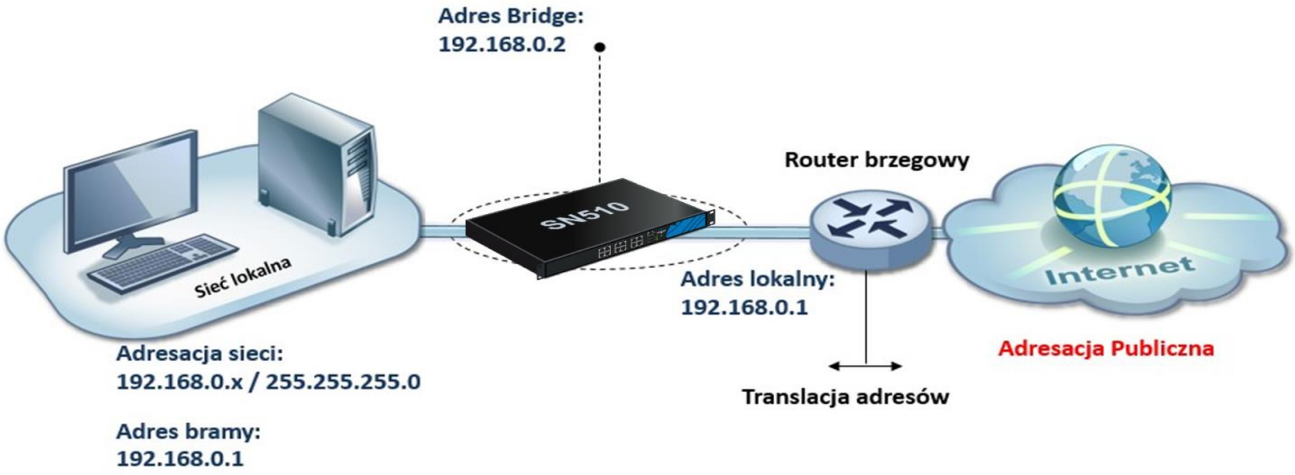
Urządzenia STORMSHIELD UTM mogą pracować w trzech trybach:

- BRIDGE (transparentny/most),
- ADVANCED (zaawansowany, tryb routera),
- HYBRID (mieszany).

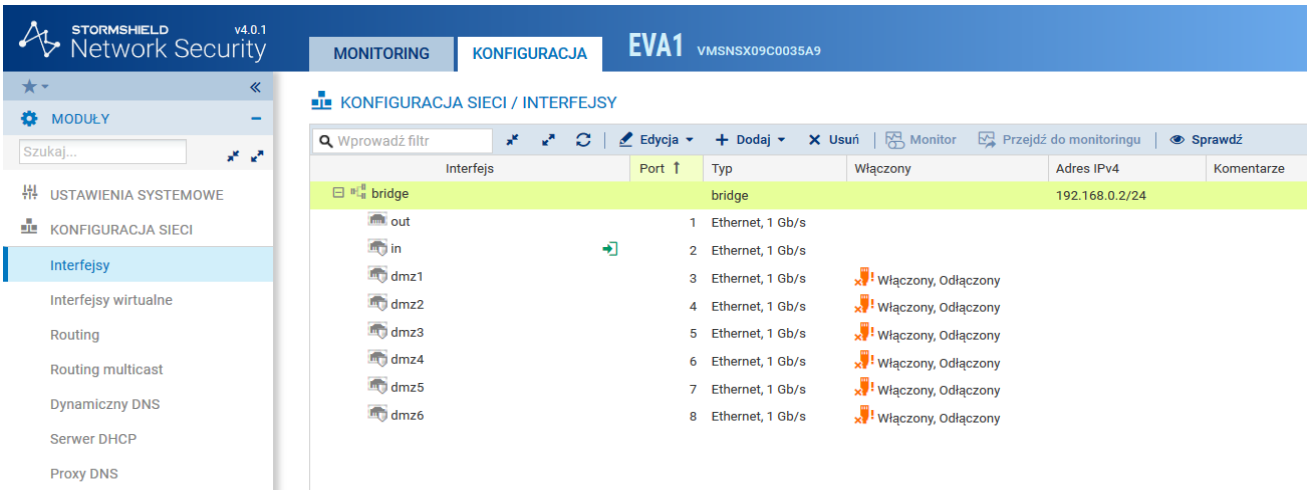
Tryb BRIDGE

Tryb Bridge inaczej jest zwany trybem transparentnym. Jest to tryb, w którym urządzenie jest skonfigurowane domyślnie. W tym trybie wszystkie interfejsy urządzenia należą do tej samej podsieci. Ustawienie adresu IP określone jest na logicznym interfejsie typu BRIDGE, a same interfejsy dziedziczą ten adres. Urządzenie filtruje ruch, który przechodzi pomiędzy interfejsami bez modyfikacji adresów IP (bez translacji NAT).

Schemat topologii:



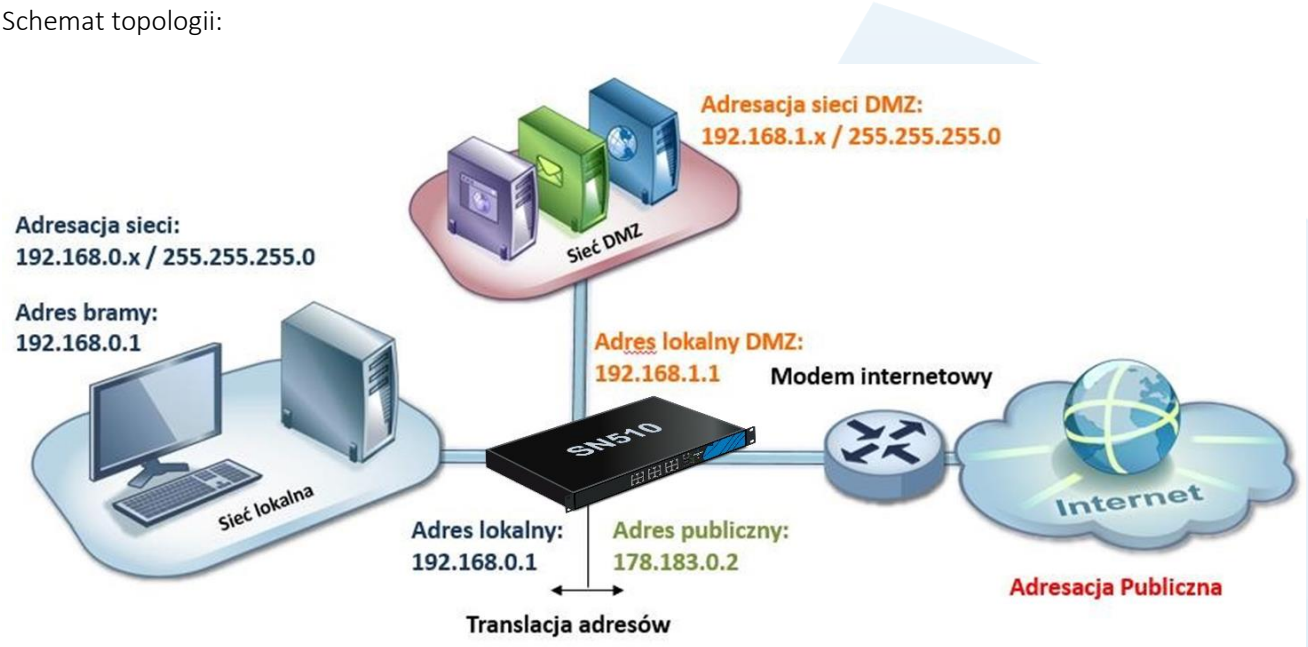
Przykład konfiguracji:



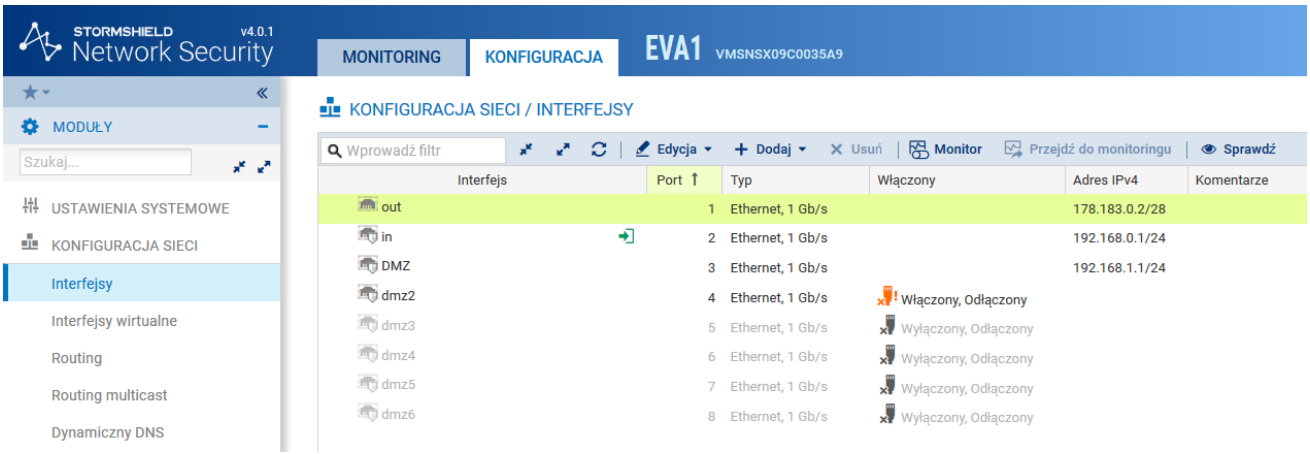
Tryb ADVANCED

Inaczej zwany trybem routera. W tym trybie każdy interfejs ma przypisany adres należący do innej podsieci. Tym samym każdy z interfejsów określa pewną strefę w sieci, stanowi odrębny segment w obrębie firmy. W tym trybie STORMSHIELD UTM pełni rolę routera pomiędzy bezpośrednio podłączonymi do niego sieciami.

Schemat topologii:



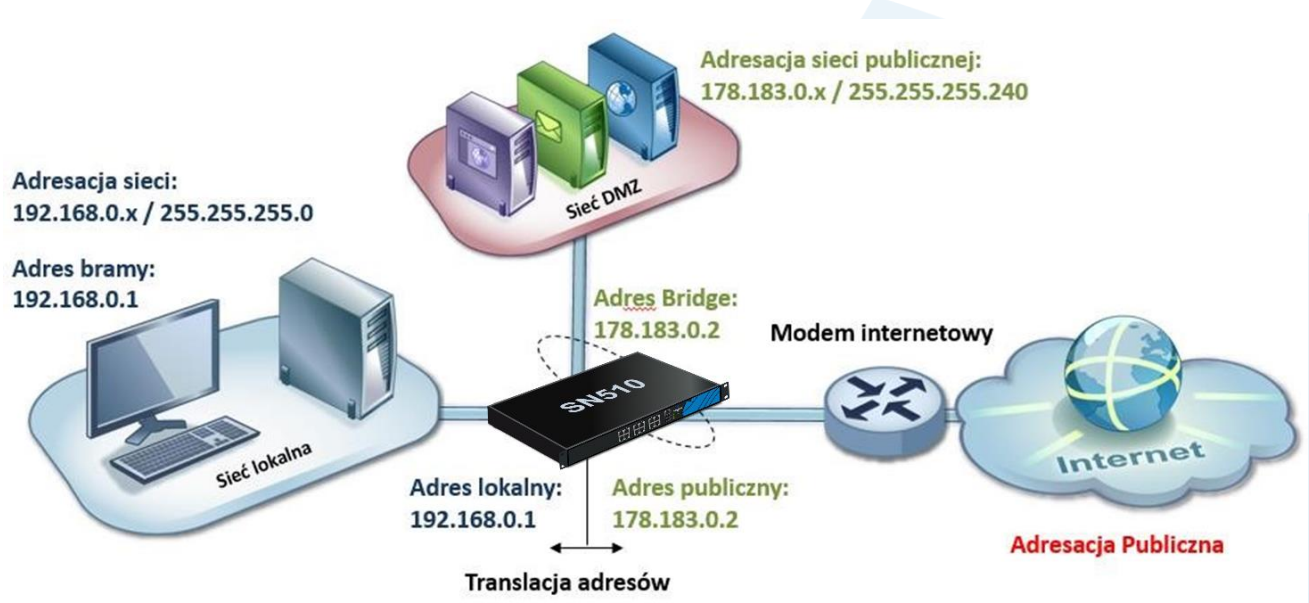
Przykład konfiguracji:



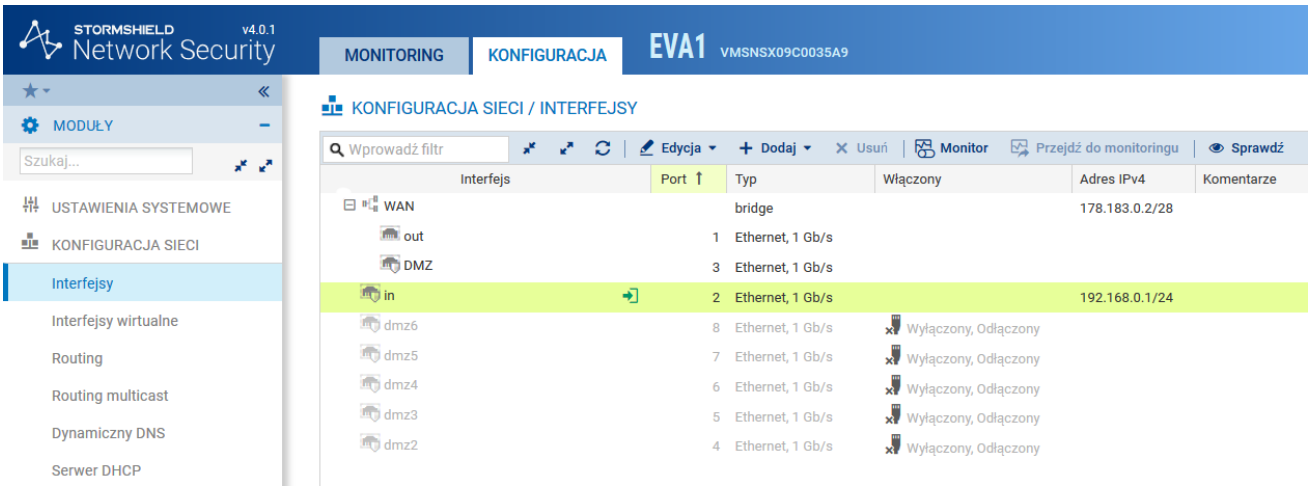
Tryb HYBRID

Tryb HYBRID jest to połączenie dwóch poprzednich trybów, przez co nazywany jest również trybem mieszanym. Polega on na takim ustawieniu interfejsów STORMSHIELD UTM, że cześć z nich względem siebie jest w trybie BRIDGE, a część w trybie ADVANCED. Jest to jeden z najczęściej używanych trybów.

Schemat topologii:



Przykład konfiguracji:


STORMSHIELD
v4.0.1
Network Security
MONITORING
KONFIGURACJA
EVA1
VMSNSX09C0035A9
MODUŁY
Szukaj...
USTAWIENIA SYSTEMOWE
KONFIGURACJA SIECI
Interfejsy
Interfejsy wirtualne
Routing
Routing multicast
Dynamiczny DNS
Serwer DHCP
KONFIGURACJA SIECI / INTERFEJSY
Wprowadź filtr
Edycja
Dodaj
Usuń
Monitor
Przejdź do monitoringu
Sprawdź
Interfejs
Port
Typ
Włączony
Adres IPv4
Komentarze
WAN
bridge
178.183.0.2/28
out
1
Ethernet, 1 Gb/s
DMZ
3
Ethernet, 1 Gb/s
in
2
Ethernet, 1 Gb/s
192.168.0.1/24
dmz6
8
Ethernet, 1 Gb/s
Wyłączony, Odłączony
dmz5
7
Ethernet, 1 Gb/s
Wyłączony, Odłączony
dmz4
6
Ethernet, 1 Gb/s
Wyłączony, Odłączony
dmz3
5
Ethernet, 1 Gb/s
Wyłączony, Odłączony
dmz2
4
Ethernet, 1 Gb/s
Wyłączony, Odłączony

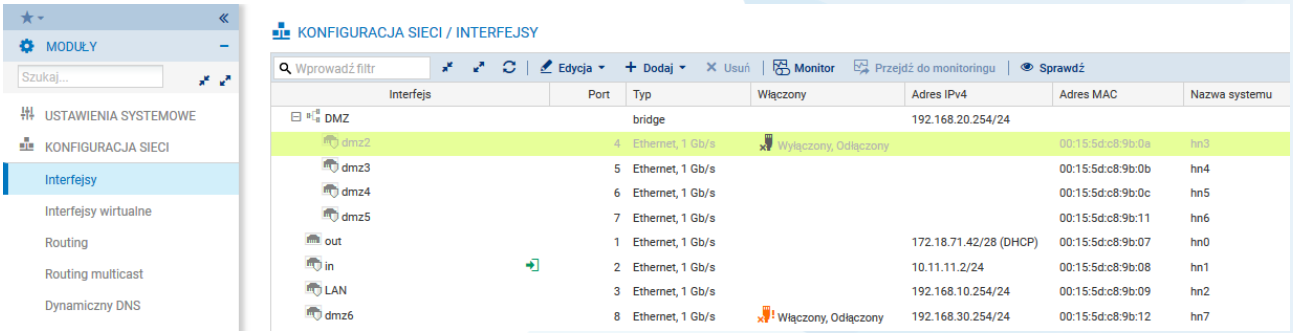
6. Konfiguracja interfejsów sieciowych

Moduł **Interfejsy** umożliwia zarządzanie, dodawanie i usuwanie elementów sieciowych zwanych interfejsami sieciowymi reprezentującymi fizyczne lub wirtualne urządzenia komunikacyjne między różnymi sieciami przechodzącymi przez urządzenie STORMSHIELD UTM.

Na urządzeniu występuje 6 typów interfejsów:

- **Interfejs fizyczny** – fizyczny interfejs zainstalowany na urządzaniu (bezpośrednio lub w postaci modułu rozszerzającego),
- **interfejs bridge** – łączy kilka interfejsów fizycznych lub VLAN w jeden interfejs logiczny (wirtualny). Liczba interfejsów bridge zależy od modelu urządzenia (w domyślnej konfiguracji urządzenia wszystkie fizyczne interfejsy należą do tego samego interfejsu bridge),
- **interfejs VLAN** – segment sieci podłączony do fizycznego interfejsu. Pakiety takiego segmentu oznaczone są tagiem VLAN ID oraz określonym zakresem adresów. Maksymalna liczba interfejsów VLAN zależy od modelu urządzenia,
- **interfejs GRETAP** – interfejs umożliwiający połączenie dwóch zdalnych sieci na poziomie warstwy 2 (L2) modelu ISO/OSI. W tym celu enkapsuluje ramkę Ethernet w pakiecie IP za pośrednictwem protokołu GRE. Dzięki temu hosty z dwóch zdalnych sieci będą mogły komunikować się tak, jakby należały do tej samej sieci LAN.
- **interfejs Modem** – ten typ interfejsu umożliwia obsługę połączeń między UTM a modemem (ADSL, ISDN, PSTN itp.). Możliwe typy połączeń to: PPPoE, PPP, PPTP i 3G,
- **interfejs USB / Ethernet** – są tworzone i używane w połączeniach zdalnych za pośrednictwem modemu bezpośrednio podłączonego do zapory (port USB).

Konfiguracja interfejsów sieciowych znajduje się w menu KONFIGURACJA > KONFIGURACJA SIECI > Interfejsy. W centralnej części znajduje się lista interfejsów zawierająca podsumowanie ich konfiguracji.



Poszczególne kolumny tego widoku oznaczają:

- **Interfejs** –nazwa interfejsu np. out, in, dmz1, ..., mogą tutaj też pojawić się dodatkowe ikony:

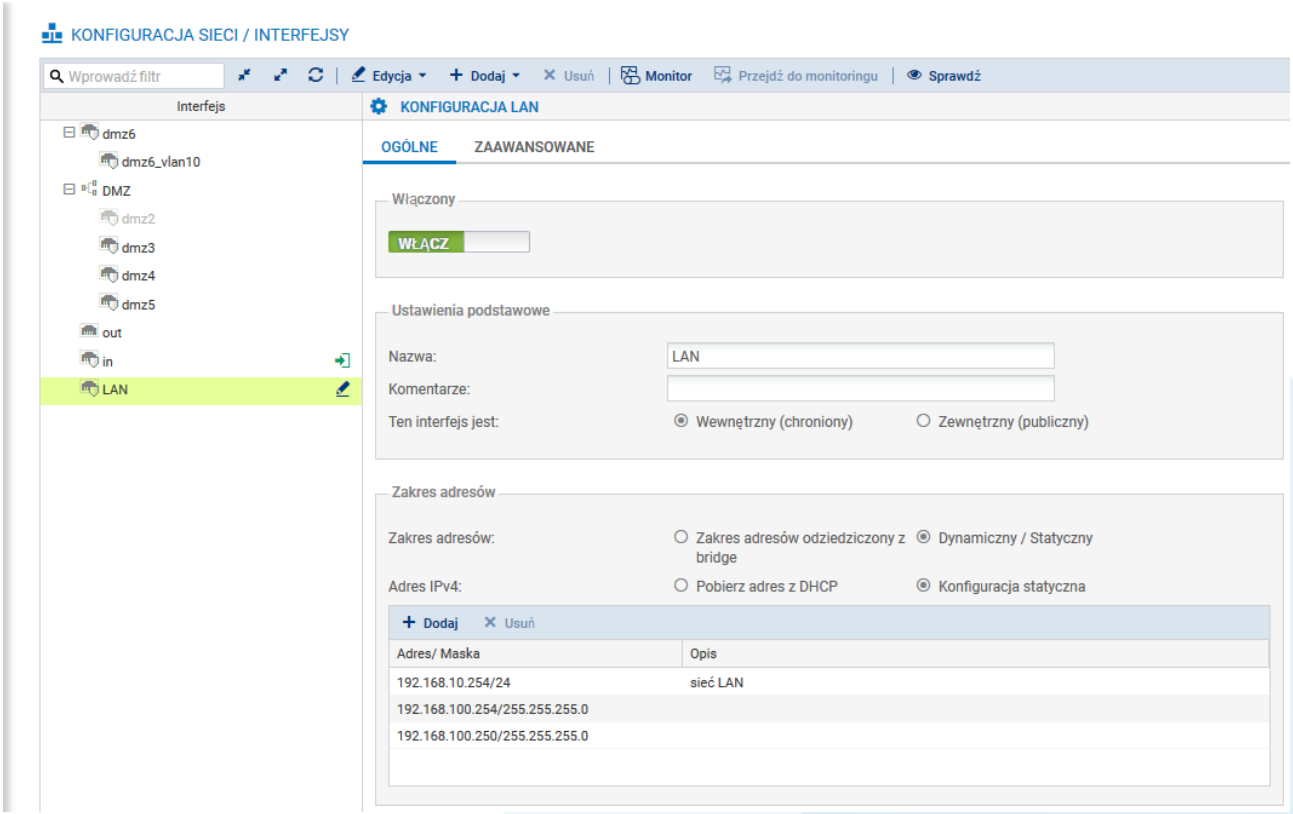
  23 interfejs przez który aktualnie zalogowany jest administrator,

  24 interfejs, który aktualnie jest edytowany,
- **Port** – numer fizycznego interfejsu, dla interfejsów logicznych (VLAN, modem) nr portu nadrzędnego,
- **Typ** – typ interfejsu: bridge, Ethernet, VLAN, PPPoE, ..., prędkość portu, vlan id, ...,
- **Status** – status interfejsu: wyłączony, odłączony. Jeśli interfejs jest podłączony i aktywny kolumna będzie pusta,

- **Adres IPv4** – skonfigurowany adres IPv4 wraz z maską sieciową lub adres pobrany z DHCP jeśli skonfigurowana jest adresacja dynamiczna,
- **Adres IPv6 –** skonfigurowany adres IPv6 wraz z maską sieciową lub adres pobrany z DHCP jeśli skonfigurowana jest adresacja dynamiczna. Ta kolumna pojawia się jedynie po włączeniu na urządzeniu obsługi protokołu IPv6,
- **Adres MAC** – adres MAC interfejsu
- **Nazwa systemowa** – nazwa interfejsu używana przez system operacyjny urządzenia,
- **Komentarz –** pole komentarza.

Przeciągnij i upuść – można używać tej metody do modyfikacji konfiguracji interfejsów np. w celu dodania interfejsu fizycznego do interfejsu typu bridge lub przeniesienia interfejsu typu VLAN do innego interfejsu fizycznego.

Po wejściu w tryb edycji konfiguracji interfejsu (po wybraniu interfejsu dwukrotne kliknięcie lub Edycja w górnym menu) pojawia się ekran konfiguracji interfejsu.



Poszczególne pozycje tego widoku oznaczają:

- **Włącz / Wyłącz** – włączenie lub wyłączenie interfejsu
- **Nazwa** – nazwa interfejsu. Na podstawie tej nazwy automatycznie tworzone są obiekty **Firewall_*nazwa*** i **Network_*nazwa*** zawierające odpowiednio adres IP interfejsu i sieci na nim skonfigurowane.
- **Komentarz** – komentarz
- **Ten interfejs jest** – interfejs może być **Wewnętrzny (chroniony)** lub **Zewnętrzny (publiczny)**.

- **wewnętrzny (chroniony)**: chroniony interfejs akceptuje tylko pakiety pochodzące ze znanego zakresu adresów IP, na przykład bezpośrednio połączona sieć lub sieć zdefiniowana przez trasę statyczną. Dodatkowo ochrona obejmuje rejestrację hostów podłączonych do tego interfejsu (chroniąc w ten sposób przed fałszowaniem adresów IP – tzw. IP address spoofing) i pozwala na generowanie domyślnych reguł firewall podczas aktywacji niektórych usługi urządzenia (na przykład SSH). Chroniony interfejs reprezentowany jest ikoną tarczy 163,
- **zewnętrzny (publiczny)**: oznacza, że interfejs nie korzysta z zabezpieczeń chronionego interfejsu i dlatego może odbierać pakiety pochodzące z dowolnego zakresu adresów (z wyjątkiem adresów przypisanych do interfejsów wewnętrznych). Ten typ interfejsu służy głównie do połączenia z Internetem.

- **Zakres adresów** – dostępne opcje to: Zakres adresów odziedziczony z bridge lub Dynamiczny / Statyczny
  - **Zakres adresów odziedziczony z bridge**: wybierając z listy **Bridge** interfejs typu bridge, interfejs fizyczny zostanie przypisany do interfejsu typy bridge i jednocześnie odziedziczy jego adres IP,
  - **Dynamiczny / Statyczny**: są tu do wyboru dwie opcje: **Pobierz adres z DHCP** – uruchamia klienta usługi DHCP na danym interfejsie oraz **Konfiguracja statyczna**, gdzie można ręcznie podać adres IP interfejsu wraz z maską sieciową. Maskę sieciową można zapisać w notacji pełnej np. 255.255.255.0 lub skróconej np. /24. Interfejs może mieć przypisanych kilka adresów IP należących do tej samej lub do różnych podsieci. Jedynym ograniczeniem jest to, że adresacja na poszczególnych interfejsach musi być unikatowa czyli nie można podać tej samej bądź nakładającej się adresacji sieciowej dla kilku interfejsów (z wyjątkiem interfejsów należących do tego samego interfejsu typu bridge). W przypadku dodania więcej niż jednego adresu IP na interfejsie, automatycznie tworzone są obiekty odpowiednio zawierające kolejne adresy IP **Firewall_*nazwa*_1**, **..._2**, itd. oraz adresację sieci **Network_*nazwa*_1**, **..._2**, itd.

Dla niektórych typów interfejsów pojawiają się dodatkowe opcje:

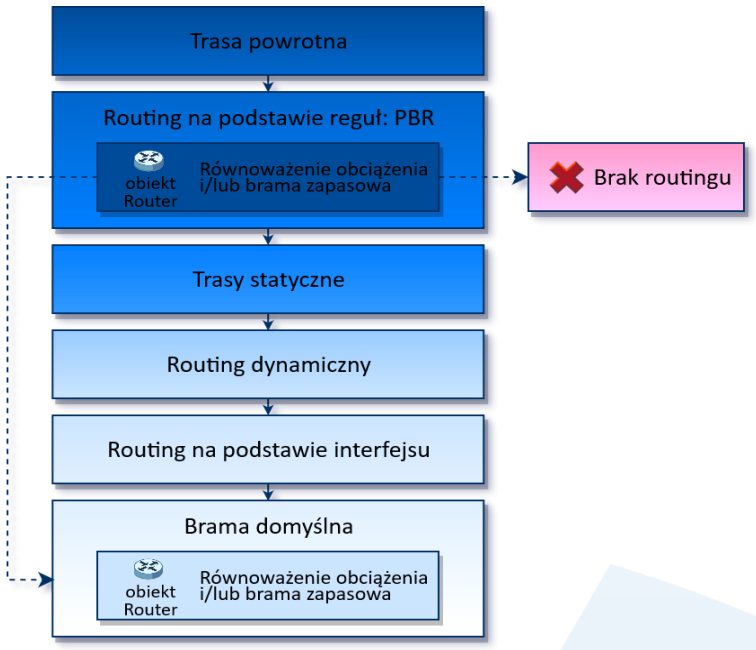
- VLAN:
  - **Interfejs nadrzędny**: interfejs, na którym urządzenie nasłuchuje pakietów oznaczonych tagiem VLAN ID,
  - **ID**: nr VLANu tj. tag VLAN ID,
  - **Priorytet CoS**: wskazana wartość CoS (pole Class of Service) zostanie ustawiona dla wszystkich pakietów wysyłanych przez ten VLAN.
- GRETAP:
  - **Sieć lokalna** – obiekt sieciowy odpowiadający interfejsowi typu bridge, do którego należy sieć lokalna, dla której tworzony jest tunel GRETAP.
  - **Sieć zdalna** – obiekt sieciowy odpowiadający adresowi publicznemu zdalnego urządzenia realizującego połączenie GRETAP.
- Modem:
  - **Interfejs nadrzędny**: interfejs, na którym podłączony jest modem PPPoE,
  - **Adres PPTP**: adres serwera PPTP, do którego nawiązywane będzie połączenie PPTP,
  - **Użytkownik**: nazwa użytkownika wykorzystywana do autentykacji,

- **Hasło**: hasło wykorzystywane do autentykacji,
- **Potwierdź**: potwierdzenie poprawności wpisania hasła.

- Interfejs USB / Ethernet – ten typ interfejsu tworzony jest automatycznie za każdym razem, gdy modem USB HUAWEI 4G obsługujący funkcję HiLink jest podłączony do urządzenia. Jeśli po podpięciu modemu USB do urządzenia port nie został utworzony, należy skonfigurować profil modemu, aby utworzyć interfejs USB / Ethernet powiązany z danym modemem USB. Możliwe jest zdefiniowanie dwóch profili modemu, ale na urządzeniu można dodać tylko jeden interfejs USB / Ethernet.

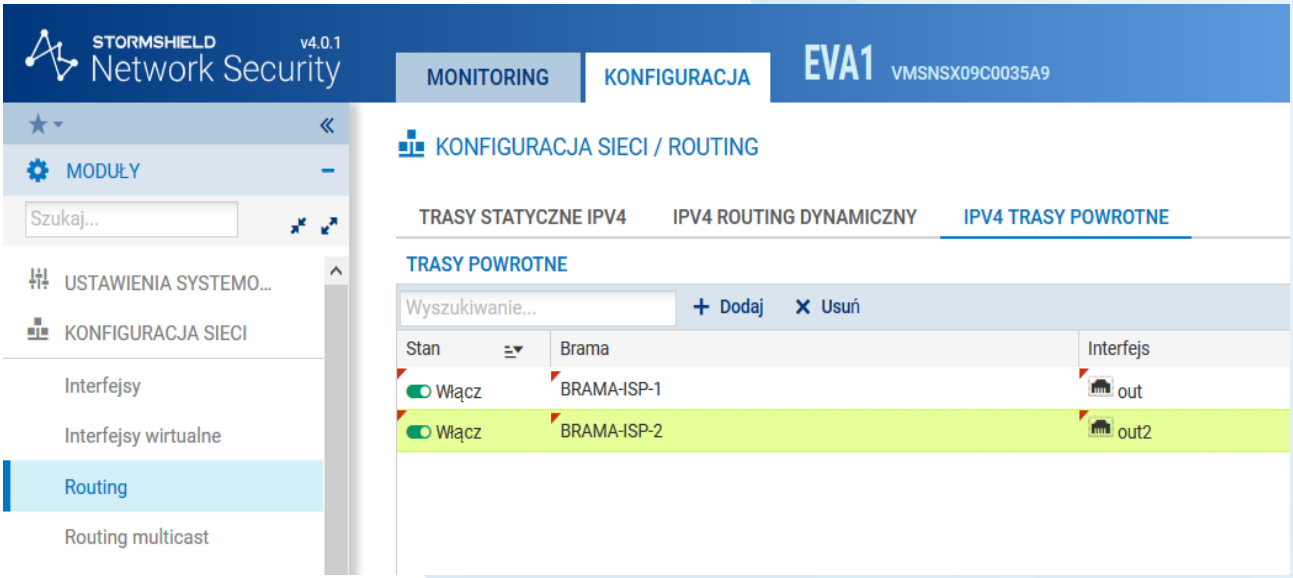
7. Routing (trasowanie połączeń)

Routing, czyli określenie drogi przesyłania pakietów można skonfigurować w STORMSHIELD UTM na kilka sposobów. Trasy mogą być zdefiniowane osobno dla IPv4 jak i IPv6.
Kolejność analizy poszczególnych metod trasowania jest następująca:



Trasa powrotna

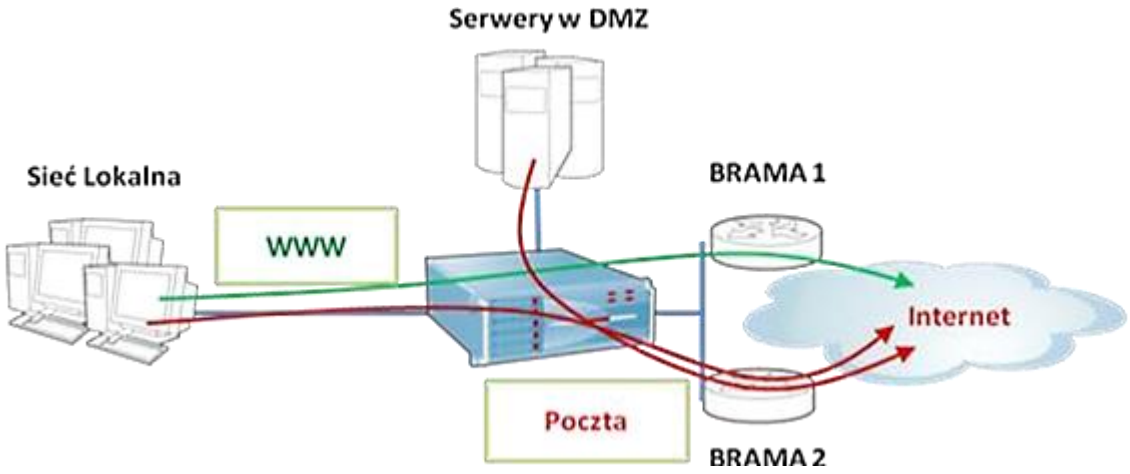
W przypadku posiadania przynajmniej dwóch lub więcej usługodawców Internetu (ISP) należy skonfigurować w STORMSHIELD UTM tak zwane trasy powrotne. Trasy powrotne pozwolą zdefiniować bramę, przez którą będą musiały przejść pakiety zwrotne, tak aby zagwarantowana była spójność połączeń.



Konfiguracja jest bardzo prosta i sprowadza się do wskazania właściwej bramy danego ISP, interfejsu, przez który ta brama jest osiągalna oraz włączenia takiej trasy.

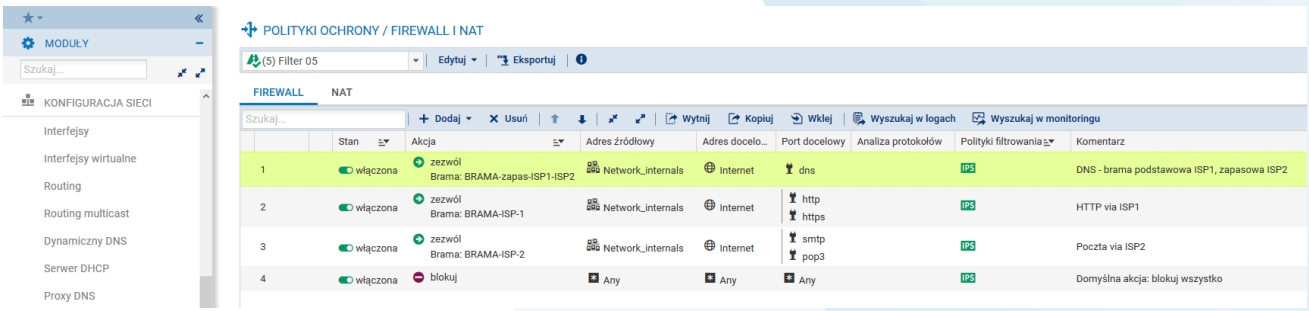
Routing na podstawie reguł – Policy Based Routing (PBR)

Jest to typ trasowania połączeń ze względu na adres źródłowy, adres docelowy pakietu, usługę (serwis, port) lub na podstawie zalogowanego użytkownika. Rysunek poniżej prezentuje jedno z możliwych zastosowań:



Na ilustracji zaprezentowano sytuację, w której ruch WWW kierowany jest przez bramę *BRAMA-ISP-1*, natomiast ruch związany z pocztą (smtp, pop3) kierowany jest przez innego usługodawcę – przez *BRAMA-ISP-2*.

Ruch sieciowy można skierować na wybrane łącze ustawiając odpowiednią opcję w menu **Akcja** edytora reguł firewall (więcej o edytorze w dalszej części dokumentacji). Odpowiada za to pozycja *Brama* w sekcji *Routing na podstawie reguł (PBR)*. Wystarczy tutaj jedynie wskazać obiekt typu Host będący bramą wybranego dostawcy Internetu lub wskazać obiekt typu Router (gdzie skonfigurowanych może być więcej dostawców Internetu na zasadzie Load Balancing lub Backup Gateways).



Równoważenie Obciążenia / Brama Zapasowa - Load Balancing / Backup Gateways

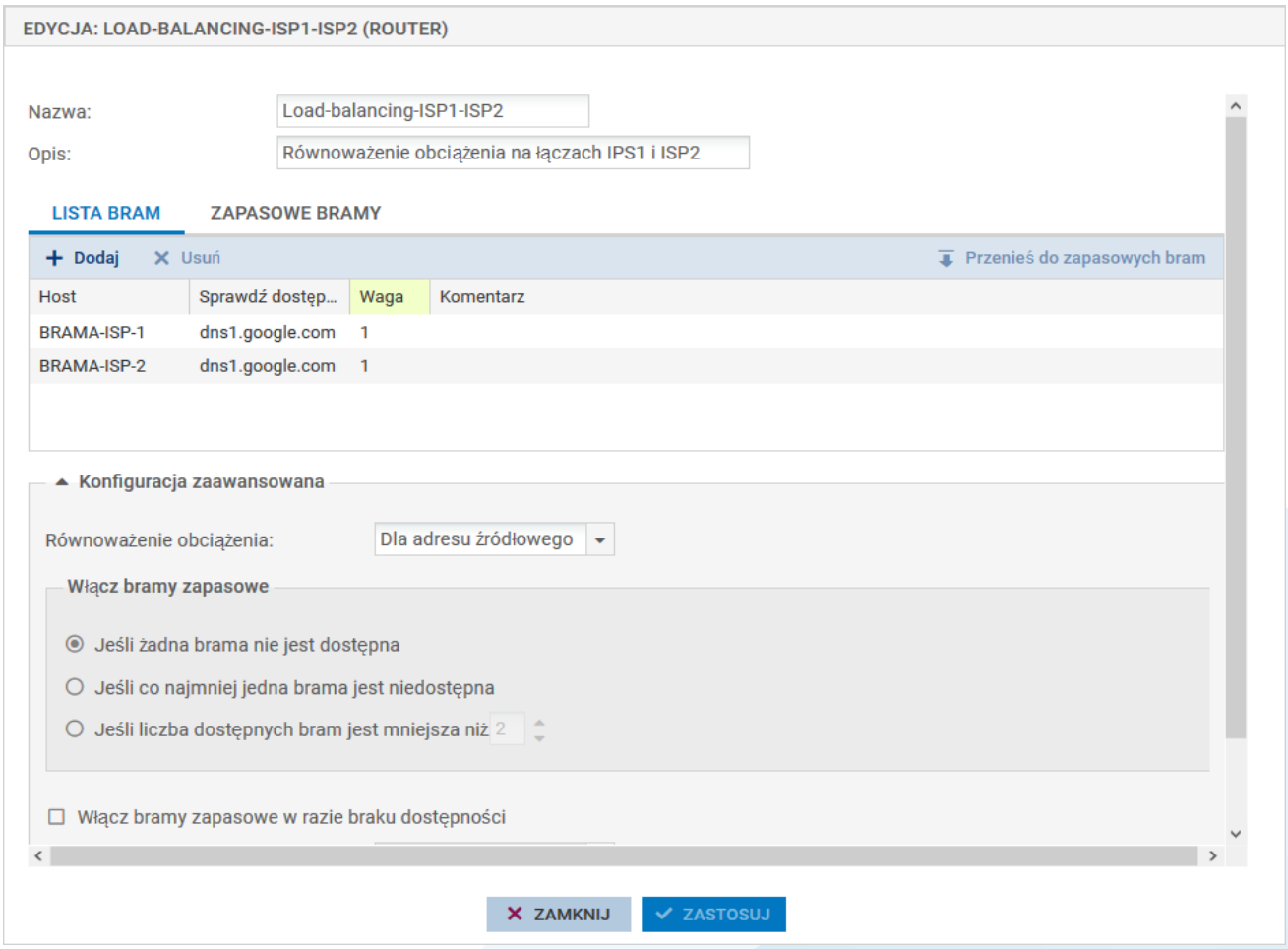
Równoważenie obciążenia może odbywać się na podstawie adresu źródłowego (SOURCE) lub połączenia (CONNECTION). Włączenie Load Balancingu polega na utworzeniu obiektu typu **Router** ze zdefiniowanymi przynajmniej dwiema bramami na liście używanych bram.

Dla każdej bramy można ustawić sposób weryfikowania jej dostępności (tak aby routowany ruch nie był wysyłany na niesprawną bramę). W celu weryfikacji prawidłowości działania poszczególnych bram urządzanie STORMSHIELD UTM wysyła pakiet Ping do hosta/grupy hostów wskazanych w kolumnie sprawdź

dostępność. Domyślnie testowany jest adres samej bramy, jednak w większości wypadków lepszym rozwiązaniem jest testowanie zewnętrznego publicznego adresu IP (takiego, który jest stabilny i dostępny poprzez sieć Internet). Umożliwi to wykrycie awarii nie tylko naszej bramy (zazwyczaj pierwsze w kolejności urządzenie dostawcy Internetu) ale także problemy w dostępie do Internetu naszego ISP.

W przypadku routingu z Równoważeniem Obciążenia dla poszczególnych bram można określić wagę, która definiuje jak duża część ruchu ma być wysyłana na tą konkretną bramę.

Do przełączania bram wykorzystywany jest algorytm round-robin. Oznacza to, że przy tych samych wagach dla każdej z bram ruch będzie do nich kierowany w jednakowym stopniu. Z kolei asymetryczny podział wag np. BRAMA-ISP-1: 3, BRAMA-ISP-2: 1 spowoduje, że do łącza ISP1 będzie trafiało 75% pakietów kierowanych do Internetu, a do łącza ISP2 25%.



Działanie bram zapasowych polega na przełączeniu się z bramy podstawowej na bramę zapasową w przypadku awarii tej pierwszej. W celu skonfigurowania bramy zapasowej należy podczas konfiguracji obiektu typu Router na zakładce ZAPASOWE BRAMY wskazać obiekt typu Host reprezentujący adres IP bramy łącza zapasowego.

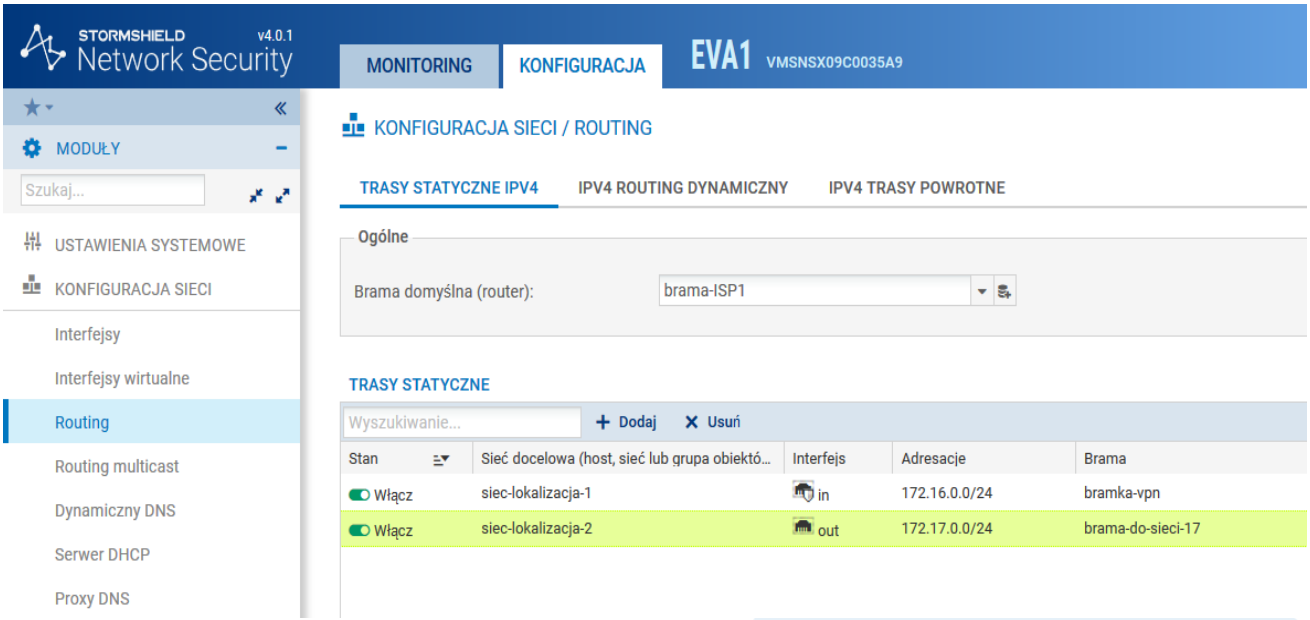
Routing typu Równoważenie Obciążenia i Bramy Zapasowe można wykorzystywać jednocześnie. Oznacza to, że możliwe jest skonfigurowanie np. dwóch łączy ISP1 i ISP2 na zasadzie równoważenia obciążenia i

jednocześnie skonfigurowanie kolejnej, trzeciej bramy np. na łączu bezprzewodowym LTE jako zapasową, na które urządzenie przełączy się w momencie awarii łączy podstawowych.

Obiekt typu Router reprezentujący routing z Równoważeniem Obciążenia i/lub Bram Zapasowych może być użyty na potrzeby routingu na podstawie reguły (PBR) lub routingu domyślnego (brama domyślna).

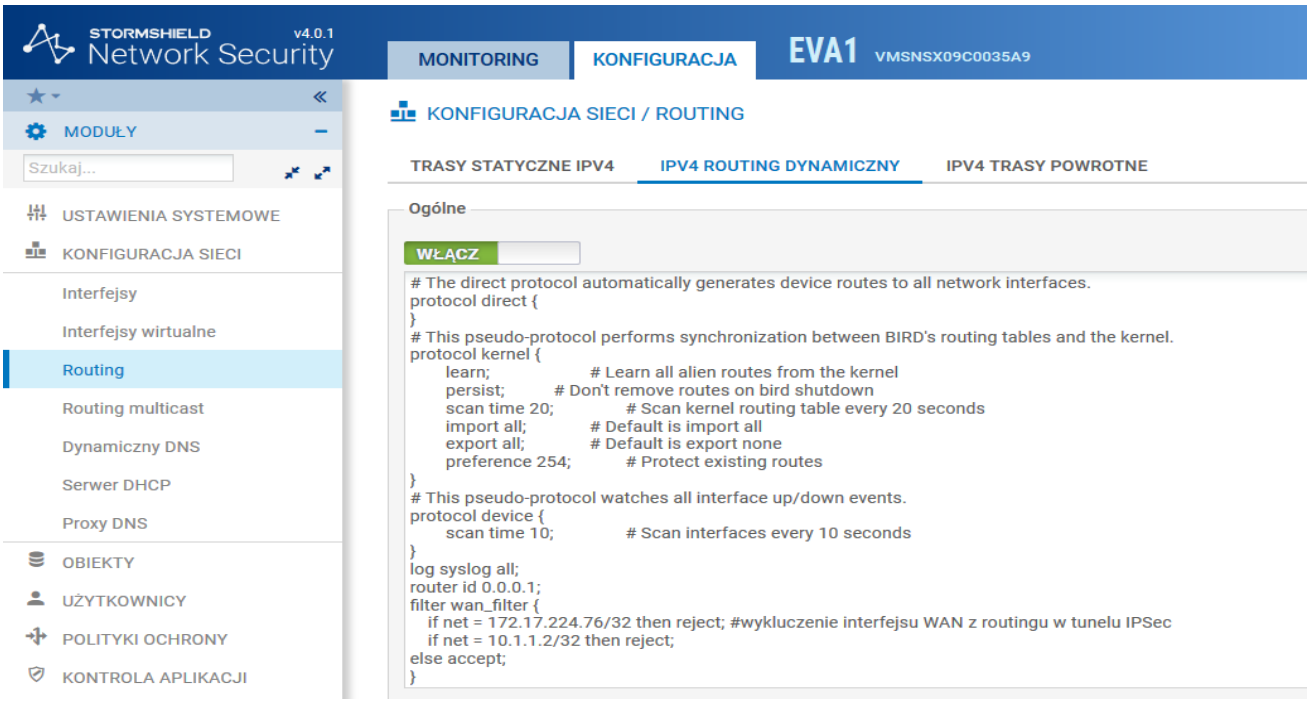
Trasy statyczne

Pozwala na określenie tras statycznych do sieci, które nie są podłączone bezpośrednio do interfejsów urządzenia.



Routing dynamiczny

Pozwala na automatyczną wymianę informacji o trasach routingu oraz aktualizację tablic routingu w środowiskach rozproszonych bądź takich, gdzie trasy routingu mogą się dynamicznie zmieniać.
STORMSHIELD UTM obsługuje 3 protokoły routingu dynamicznego, są to: RIPv2, OSPF, BGP.
Samo routowanie oparte jest o silnik BIRD (http://bird.network.cz/), a jego konfiguracja opiera się na edycji pliku konfiguracji za pośrednictwem WebGUI.



Routing na podstawie interfejsu

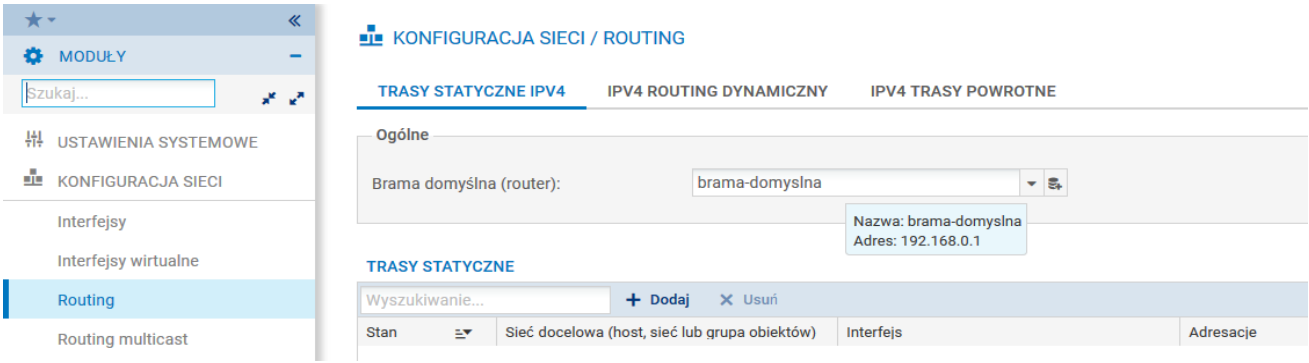
Ten typ trasowania połączeń pozwala na kierowanie całego ruchu przychodzącego na dany interfejs na wskazaną bramę. Ten typ routingu można skonfigurować jedynie z poziomu wiersza poleceń poprzez edycję pliku /usr/Firewall/ConfigFiles/network, przykład poniżej:

```
[ethernet1]
State=1
Name=in
Protected=1
Media=0
Color=408080
Type=1
EEE=0
Address=10.0.0.254
Mask=255.255.255.0
Gateway=BRAMA-ISP-2    # Brama dla całego ruchu przychodzącego tym interfejsem
AddressComment=
```

Brama domyślna

Cały ruch, dla którego nie została znaleziona trasa na podstawie wcześniej omówionych metod routingu będzie skierowany na bramę domyślną (Default Gateway).
Bramę domyślną można skonfigurować w KONFIGURACJA > KONFIGURACJA SIECI > Routing > sekcja Ogólne. W opcji *Brama domyślna (router)* należy wskazać obiekt reprezentujący bramę domyślną i może to być obiekt typu:

- Host – jedno łącze internetowe, bez testowania dostępności bramy, równoważenia obciążenia czy też bram zapasowych,
- Router – więcej niż jedno łącze internetowe z możliwością uruchomienia równoważenia obciążenia i/lub bram zapasowych oraz weryfikacji dostępności poszczególnych bram.



Wskazówka

Konfiguracja bramy domyślnej i tras statycznych znajduje się w pliku:
`/usr/Firewall/ConfigFiles/route`

Aby wyświetlić trasy statyczne oraz trasę domyślną można użyć polecenia:
`netstat -nr`

Aby wyświetlić pozostałe metody trasowania należy użyć polecenia:
`sfctl -s route`

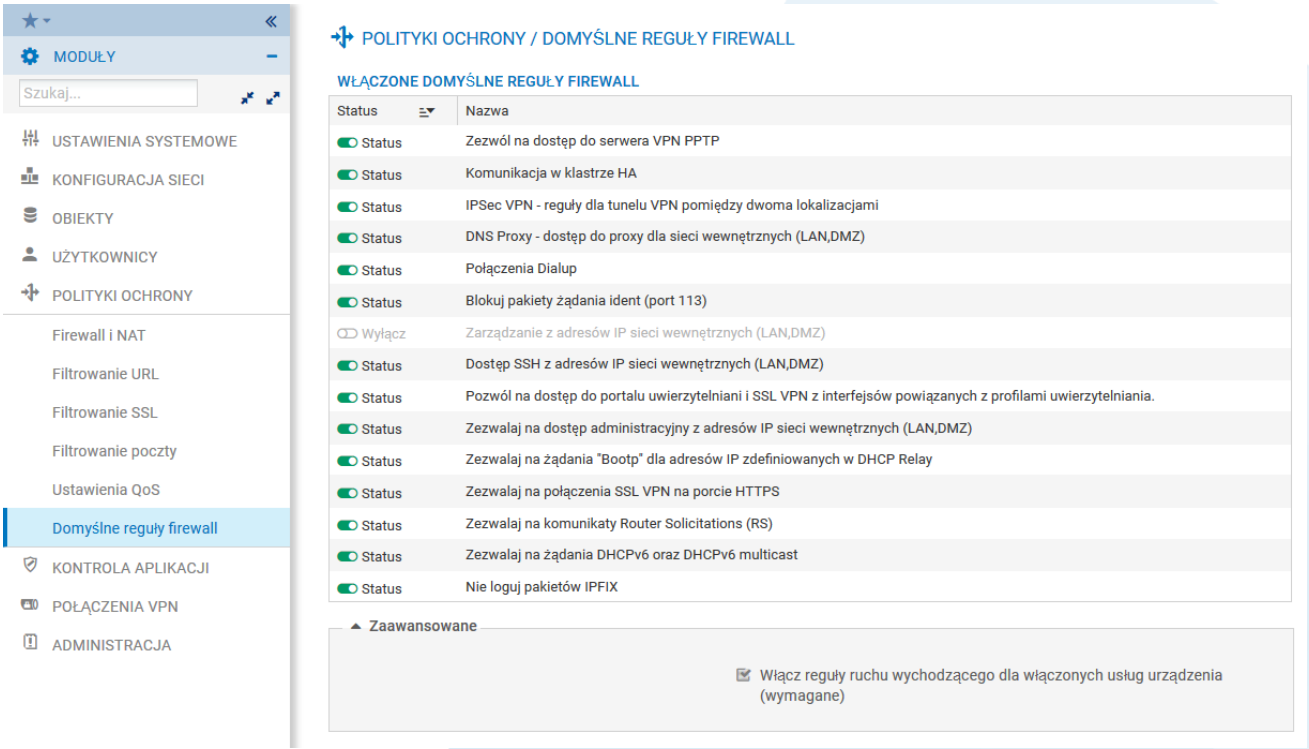
8. Konfiguracja zapory (firewall)

Konfiguracja Firewall w rozwiązaniach STORMSHIELD UTM podzielona jest na dwie części. Pierwszą z nich są reguły domyślne, a drugą polityki konfigurowane przez administratora.

W pierwszej kolejności pakiet sprawdzany jest przez zbiór **Domyślnych reguł firewall** (**Implicit rules**). Jeżeli pakiet nie znajdzie dopasowania do żadnej z reguł domyślnych sprawdzane są dopasowania do reguł polityki stworzonej przez administratora tzw. **Polityki lokalnej**.

Domyślne reguły firewall - Implicit Rules

W sekcji **KONFIGURACJA > POLITYKI OCHRONY > Domyślne reguły firewall** widoczne są reguły domyślne ustawione na zaporze. Reguły te mają na celu zapewnienie komunikacji z urządzeniem nawet w sytuacji, kiedy w ramach lokalnej polityki firewall administrator nie stworzyłby reguł umożliwiających komunikację z urządzeniem czy też omyłkowo stworzył reguły blokujące taką komunikację, co w efekcie aktywowania takiej polityki spowodowałoby utratę łączności z urządzeniem. Poniżej przedstawiono dostępne domyślne reguły firewall. Każdą z nich można włączyć bądź wyłączyć, ale nie można dodać nowych bądź usunąć istniejących:



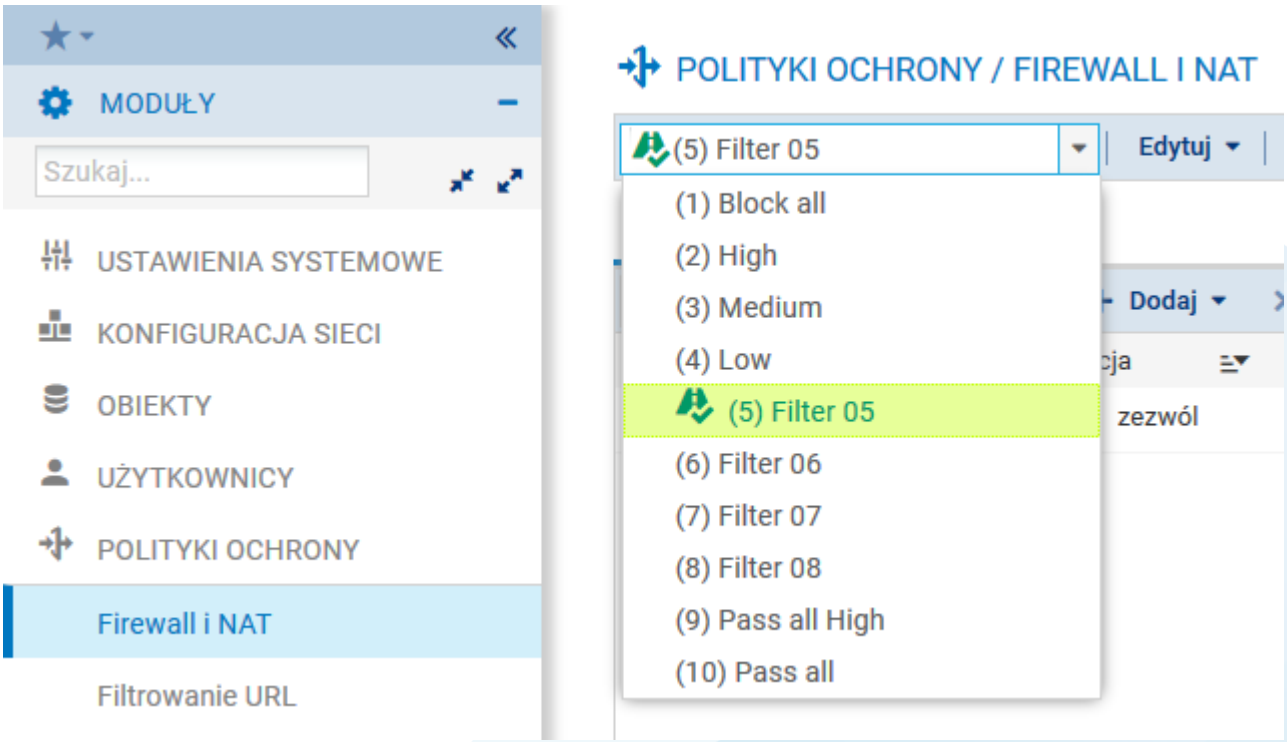
W przypadku reguł domyślnych administrator nie widzi ich pełnej składni, jednak znaczenie poszczególnych reguł można zobaczyć w aplikacji **Real Time Monitor** w zakładce **Reguły firewall**

> **Uwaga**
>
> Wyłączenie reguł domyślnych (implicit rules) bez wcześniejszego utworzenia odpowiednich reguł Polityki lokalnej może skutkować brakiem dostępu do panelu administracyjnego urządzenia. Zmiany reguł domyślnych powinny być dokładnie przemyślane.

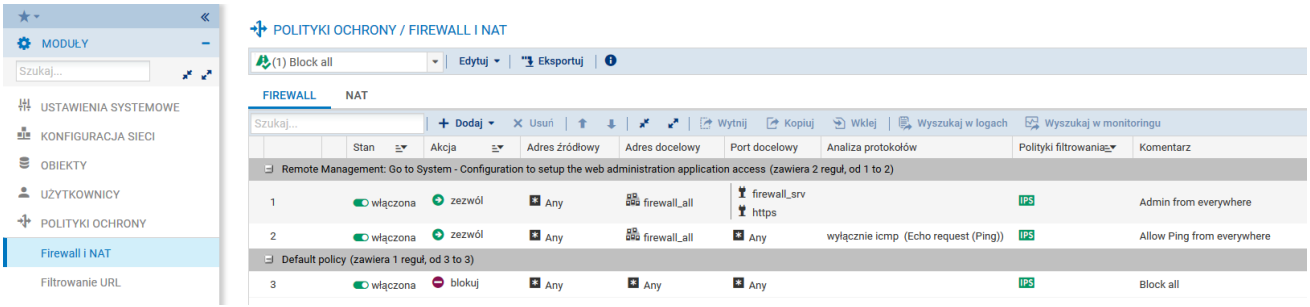
> **Wskazówka**
>
> Do wyświetlenia aktywnych reguł firewall z poziomu SSH służy polecenie:
>
> `sfctl -s filter`

Lokalne polityki ochrony

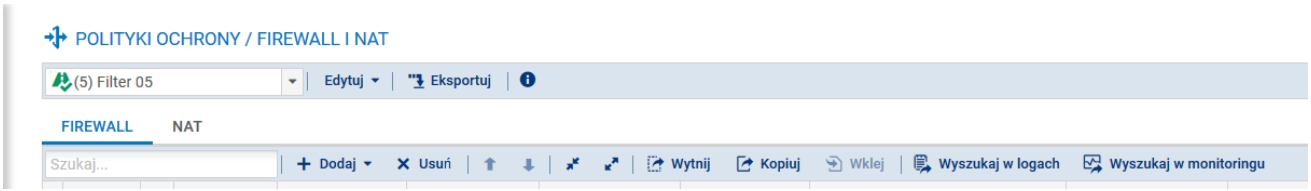
Konfiguracja zapory STORMSHIELD UTM znajduje się w sekcji **KONFIGURACJA > POLITYKI OCHRONY > Firewall i NAT**. Administrator ma do dyspozycji 10 konfigurowalnych zestawów reguł zwanych profilami. W danej chwili aktywny może być tylko jeden profil, który oznaczony jest ikoną 33.



W ramach ustawień profilu określa się politykę filtrowania ruchu sieciowego na poziomie firewall, sposób filtrowania ruchu poprzez system IPS oraz konfiguruje się inne skanery (np. antywirus) i dodatkowe parametry takie jak np. QoS. Poniżej znajduje się okno konfiguracyjne Firewall i NAT, gdzie przedstawiony jest domyślny zestaw reguł, którym jest profil nr 1 o nazwie **Block all**. W ramach tego zestawu możliwe jest podłączenie się do panelu administracyjnego urządzenia (nawet jeśli reguły domyślne są wyłączone) oraz sprawdzenie dostępności urządzenia za pomocą komunikacji *ICMP (PING)*, natomiast każde inne połączenie jest blokowane.



Górna część okna **Firewall i NAT** pozwala na zarządzanie profilami oraz regułami firewall.



Dostępne akcje zarządzania regułami firewall:

Edytuj	Zmiana nazwy profilu, przywrócenie jego ustawień domyślnych oraz przekopiowanie bieżącego profilu do innego.
Eksportuj	Eksport bieżącego profilu do pliku CSV.
Dodaj	Dodanie nowej reguły lub separatora. Z tego miejsca możliwe jest również uruchomienie kreatora reguł specjalnych: SSL Proxy, http Proxy (typu explicit), reguły uwierzytelniania.
Usuń	Usuwa zaznaczoną regułę.
W górę/W dół  37	Przesunięcie zaznaczonej reguły.
Zwiń / Rozwiń (separatory)  38	Separatory można użyć do grupowania reguł o podobnych zakresach np. reguły dla LAN, reguły dla DMZ. Jak sama nazwa wskazuje przyciski Zwiń /Rozwiń wszystkie separatory służą do szybkiego zwinięcia/rozwinięcia wszystkich separatorów.
Wytnij/Kopiuj/Wklej	Pozwala na szybkie zarządzanie regułami. Reguły można zaznaczać z użyciem klawiszy **Shift** lub **Ctrl** w celu zaznaczenia wielu reguł. Można także korzystać ze skrótów klawiszowych **Ctrl+c**, **Ctrl+x**, **Ctrl+v**.
Wyszukaj w logach	Przenosi do sekcji MONITORING > LOGI z aktywnym filtrem wyświetlającym wpisy dziennika tylko zaznaczonej reguły firewall.
Wyszukaj w monitoringu	Przenosi do sekcji MONITORING > MONITOROWANIE > Połączenia z aktywnym filtrem wyświetlającym aktywne połączenia zestawione na podstawie zaznaczonej reguły firewall.

Dolna część okna pozwala na definiowanie poszczególnych reguł firewall. Konfiguracja reguł polega na definiowaniu dopasowania, czyli warunków jakie musi spełnić ruch sieciowy, aby wpaść w regułę oraz akcji – tego co ma się stać z ruchem, który wpadnie w tę regułę.

	Stan	Akcja	Adres źródłowy	Adres docelowy	Port docelowy	Analiza protokołów	Polityki filtrowania	Komentarz
Remote Management: Go to System - Configuration to setup the web administration application access (zawiera 2 reguł, od 1 to 2)								
1	włączona	zezwól	Any	firewall_all	firewall_srv https		IPS	Admin from everywhere
2	włączona	zezwól	Any	firewall_all	Any	wyłącznie icmp (Echo request (Ping))	IPS	Allow Ping from everywhere
Default policy (zawiera 1 reguł, od 3 to 3)								
3	włączona	blokuj	Any	Any	Any		IPS	Block all

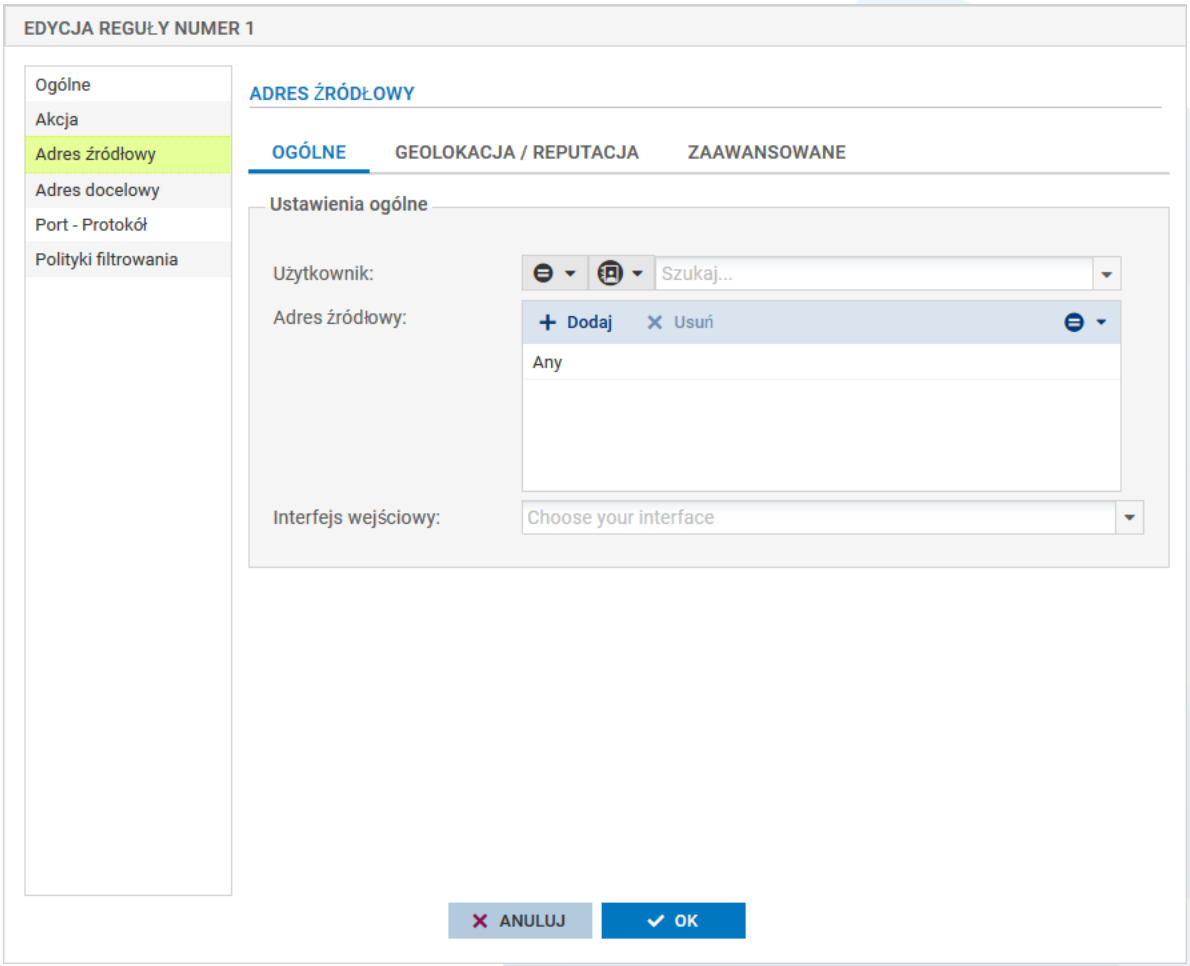
Kolumny odpowiedzialne za dopasowanie ruchu do reguły firewall to: **Adres źródłowy**, **Adres docelowy**, **Port docelowy**, **Analiza protokołów**. Ich konfiguracja obejmuje:

Opcje dostępne w ramach kolumny **Adres źródłowy**:

Użytkownik – uwierzytelniony użytkownik bazy LDAP.

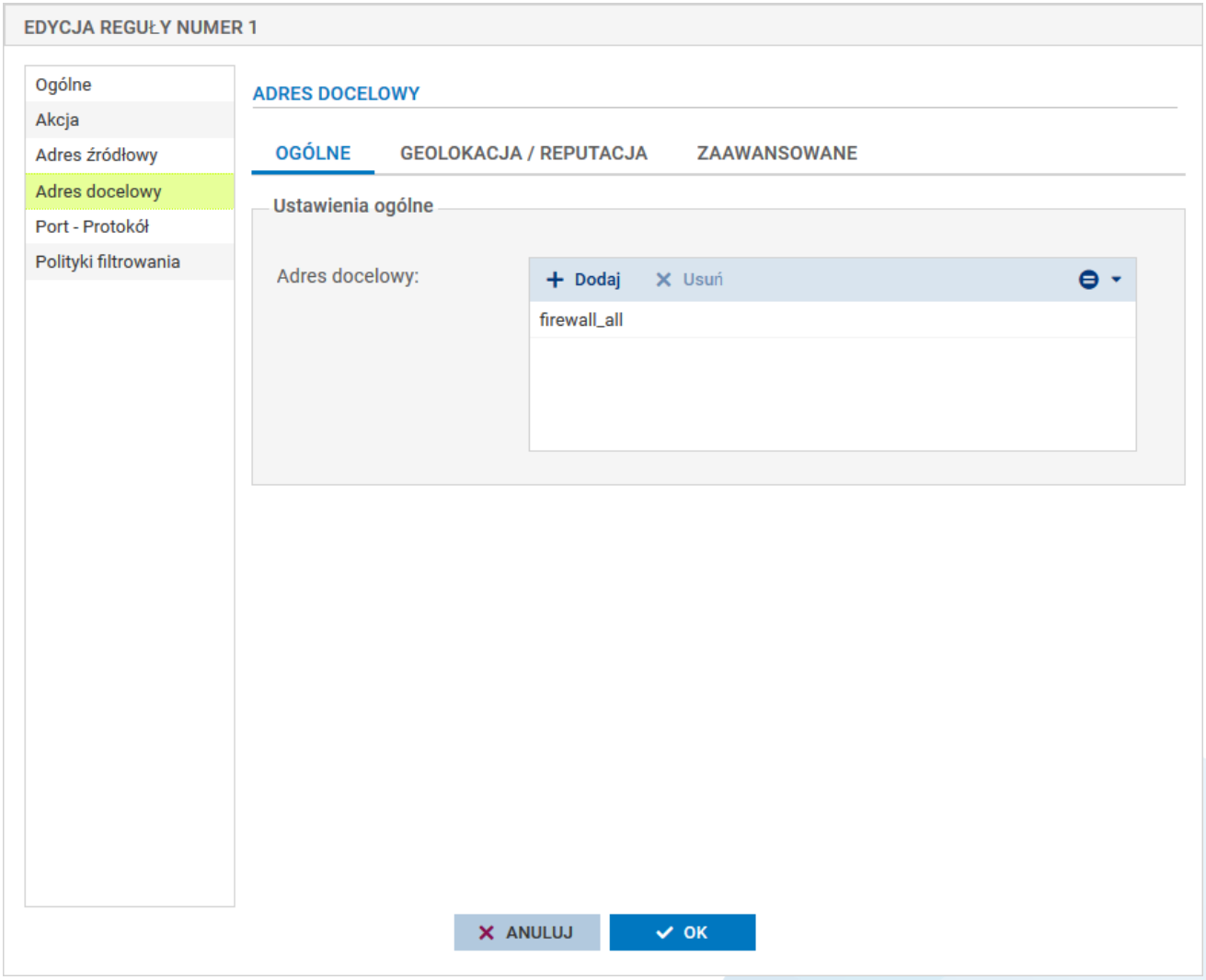
Adres źródłowy – źródłowy adres IP pakietu inicjującego połączenie. Może to być pojedynczy host, zakres adresów, sieć, grupa adresów.

Interfejs wejściowy – interfejs, na którym pojawia się pierwszy pakiet inicjujący połączenie. Pozwala na tworzenie reguł zależnych od topologii sieci.



Opcje dostępne w ramach kolumny **Adres docelowy**:

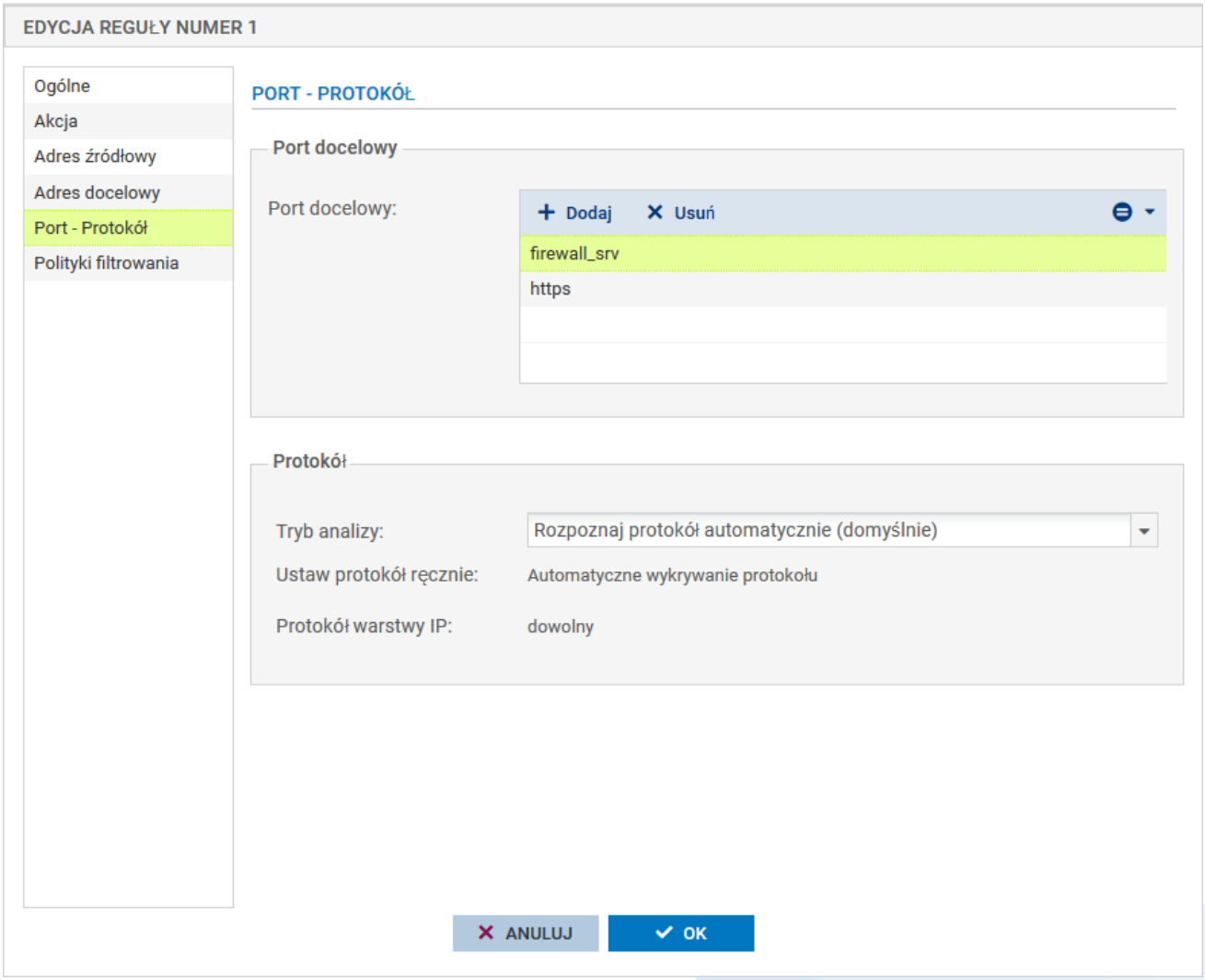
Adres docelowy - adres IP przeznaczenia pakietu. Może to być pojedynczy host, zakres adresów, sieć, grupa adresów.



Opcje dostępne w ramach kolumn **Port docelowy i Analiza protokołów** (edycja z poziomu zakładki Port – Protokół edytora reguł):

Port docelowy – określa usługę, z której będą korzystać obiekty określone w **Adresie źródłowym** łącząc się do obiektu określonego w **Adresie docelowym**. Inaczej mówiąc jest to port docelowy połączenia w ramach protokołu sieciowego (TCP/UDP/SCTP). Może to być pojedynczy port, zakres bądź grupa portów działająca na jednym lub dowolnym z protokołów sieciowych.

Protokół – tryb analizy – określa protokół ruchu wpadającego w regułę. Może to być protokół warstwy IP (ICMP, TCP, UDP, ESP, GRE, itp.) lub protokół warstwy aplikacji (HTTP, DNS, DHCP, itp.)



Jeśli ruch zostanie dopasowany do reguły na podstawie powyższych kolumn, czyli spełni wszystkie określone w nich warunki, to zostaną dla niego wykonane czynności zdefiniowane w kolumnach **Akcja** oraz **Polityki filtrowania**. Ich konfiguracja obejmuje odpowiednio:

Opcje dostępne w ramach kolumny **Akcja**:

Akcja - akcja jaka ma zostać podjęta dla ruchu, który znalazł dopasowanie w regule. Dostępne opcje to:

- **Zezwól** – przepuszczenie ruchu i wykonywanie dalszej analizy (np. skanowanie antywirusowe);
- **Blokuj** – zablokowanie ruchu bez dalszej analizy;
- **Deszyfruj** – uruchomienie modułu SSL proxy w celu deszyfracji ruchu np. HTTPS, POP3S, SMTPS, itp.;
- **Reset** – zablokowanie ruchu i odesłanie pakietu z flagą RST do nadawcy, bez dalszej analizy;

Logowanie – informacja o dopasowaniu ruchu do reguły firewall może zostać zapisana w logach, dostępne opcje to:

- **standardowe (logowanie połączeń)** – zakończone połączenia, które doszły do skutku (czyli te z akcją zezwól) mogą być zapisane w dzienniku (MONITRONG > LOGI > Ruch sieciowy) w zależności od protokołu połączenia i domyślnej konfiguracji logowania danego protokołu,

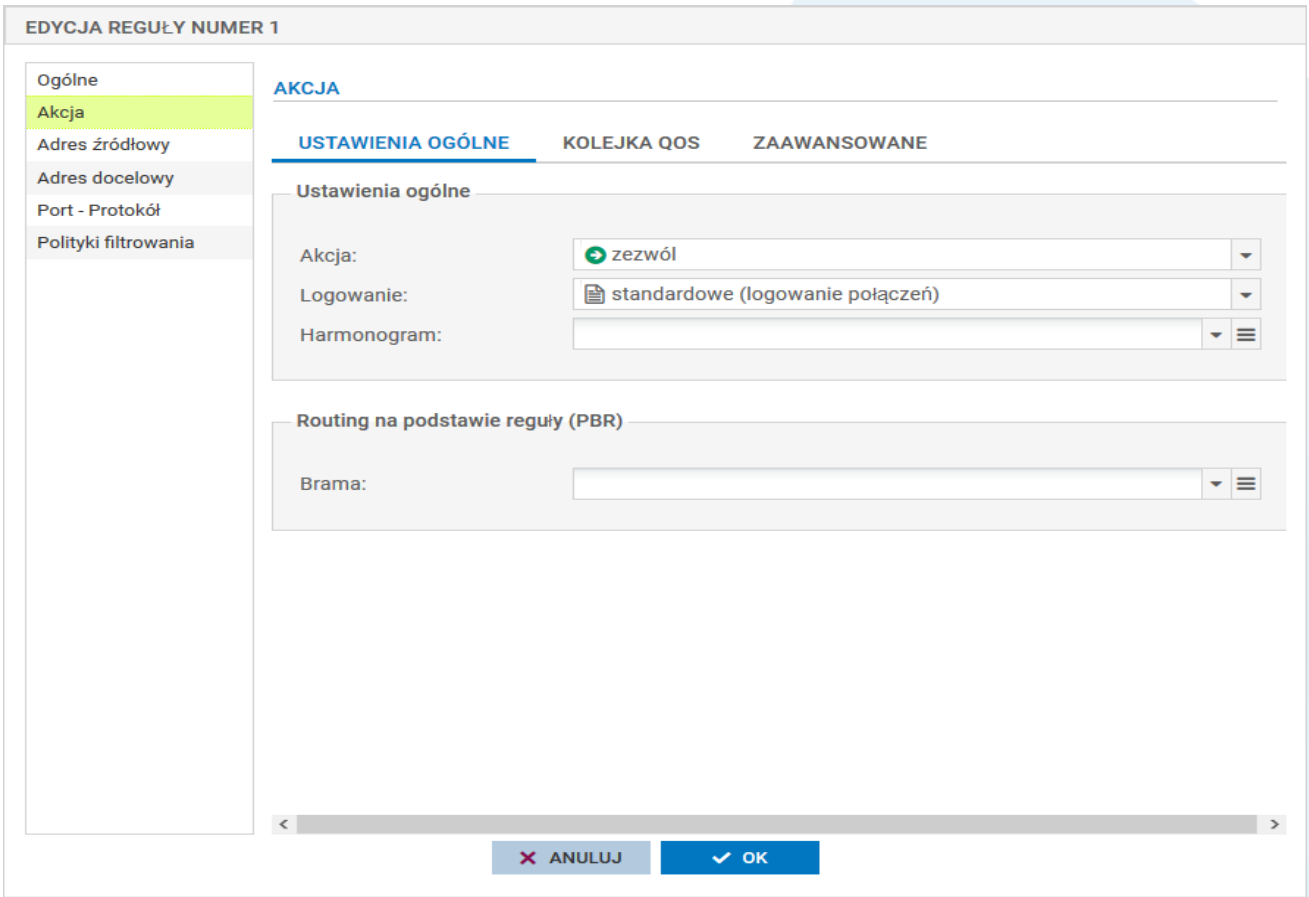
- **szczegółowe (logowanie filtrowania)** – każda próba połączenia odpowiadająca regule firewall będzie zapisana w dzienniku (MONITRONG > LOGI > Ruch sieciowy). Ta opcja nie jest polecana dla reguł typu „Zablokuj wszystko - Deny all" z wyjątkiem debugowania, ponieważ będzie generowała bardzo dużą ilość logów.
- **alarm: priorytet niski** lub **alarm: priorytet wysoki** – w momencie dopasowania reguły do połączenia zostanie wygenerowany alarm o wybranym priorytecie. Taki alarm zostanie zapisany w dzienniku Alarmy oraz może być wysłany przez Syslog (Logs – Syslog – IPFIX) lub powiadomienie email.

Harmonogram – Harmonogram jest opcją dopasowania, a nie filtrowania ruchu. Dzięki wskazaniu obiektu harmonogramu możemy zdefiniować godziny i/lub dni, w których reguła jest aktywna i uwzględniana w ramach polityki filtrowania.

Brama – pozwala na trasowanie ruchu w ramach polityk filtrowania (Routing na podstawie reguły – PBR). W tym miejscu może zostać wskazany obiekt typu Host (pojedyncza brama) lub Router (równoważenie obciążenia/brama zapasowa).

Kolejka QoS – pozwala na przypisanie ruchu do odpowiedniej kolejki QoS, czyli na sterowanie pasmem (kolejki CBQ) lub nadanie określonego priorytetu (kolejki PBQ) połączeniu. Definicja kolejek QoS znajduje się w KONFIGURACJA > POLITYKI OCHRONY > Ustawienia QoS.

Podział względem – pozwala na równe podzielenie przypisanego pasma. Dla opcji **Użytkownik** i **Host** każde ze źródeł ruchu otrzyma taką samą część pasma niezależnie od tego jak wiele sesji generuje. Przy użyciu opcji **Połączenie** podział odbywa się względem połączeń niezależnie od tego ile sesji nawiązuje każde ze źródeł ruchu.



Opcje dostępne w ramach kolumny **Polityki filtrowania**:

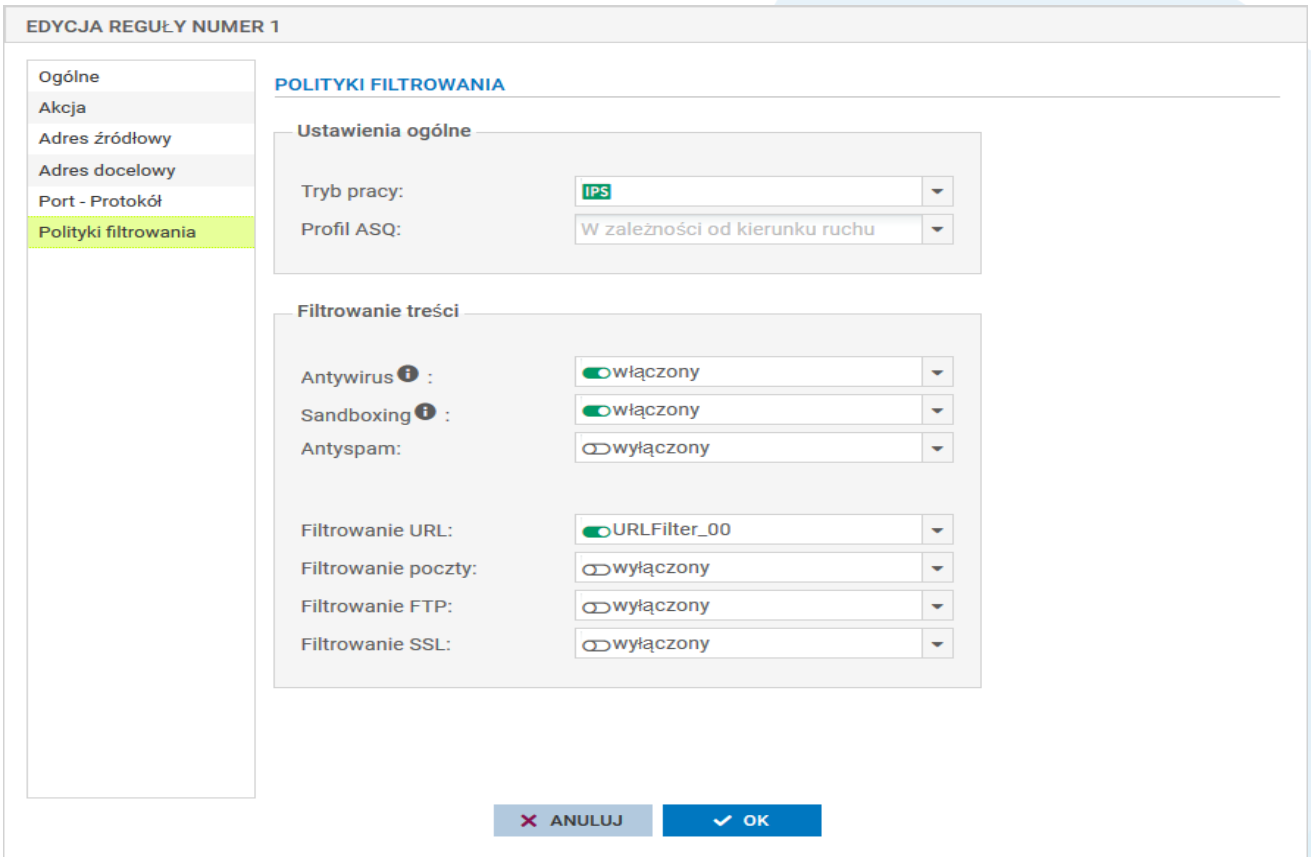
Tryb pracy:

- **IPS** (Intrusion Prevention System) – system wykrywania i blokowania zagrożeń;
- **IDS** (Intrusion Detection System) – wykrywanie zagrożeń bez ich blokowania;
- **Firewall –** powoduje, że nie będzie działał moduł ASQ, czyli zagrożenia nie będą ani wykrywane, ani tym bardzie blokowane (ten tryb pracy nazywany jest też tzw. klasycznym firewallem).

Profil ASQ – wybór jednego z 10 profili prac IPS. Wybór *W zależności od kierunku ruchu* oznacza, że do analizy użyty będzie jeden z profili domyślnych, czyli 00 dla ruchu przychodzącego z zewnątrz i 01 dla ruchu wychodzącego z sieci wewnętrznych (chronionych).

Sekcja **Filtrowanie treści** – konfiguracja poniższych opcji związana jest z działaniem modułów proxy:

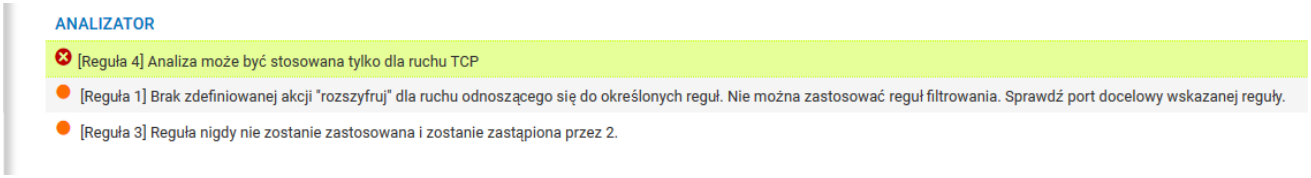
- **Antywirus** – włączenie/wyłączenie filtrowania ruchu http, ftp, smtp i pop3 za pomocą skanera AV.
- **Sandboxing** – włączenie/wyłączenie ochrony typu sandboxing (Breach Fighter). Włączenie tej opcji wymaga użycia silnika antywirusa.
- **Antyspam** – włączenie/wyłączenie skanera antyspamowego dla ruchu smtp i pop3.
- **Filtrowanie URL** – wybór jednego z 10 profili filtrowania URL dla ruchu WWW. Konfiguracja profili filtrowania URL znajduje się w KONFIGURACJA > POLITYKI OCHRONY > Filtrowanie URL.
- **Filtrowanie poczty** – wybór jednego z 10 profili filtrowania nadawców/odbiorców dla ruchu smtp.
- **Filtrowanie FTP** – włączenie/wyłącznie skanera protokołu ftp.
- **Filtrowanie SSL** – wybór jednego z 10 profili filtrowania dla ruchu SSL. Konfiguracja profili filtrowania SSL znajduje się w KONFIGURACJA > POLITYKI OCHRONY > Filtrowanie SSL.



> **Uwaga**
>
> Dopasowanie nowego połączenia do reguły firewall wykonywane jest w kolejności od pierwszej do ostatniej reguły. Jeśli ruch nie „wpadnie" w żadną ze zdefiniowanych reguł zostanie on zablokowany przez politykę domyślną.

Analizator reguł

Analizator reguł sprawdza poprawność konfiguracji firewall, tzn. sprawdza, czy stworzone reguły są poprawne pod względem użytych obiektów i metod skanowania ruchu oraz czy nie ma reguł pokrywających się lub wykluczających się. W przypadku wykrycia nieprawidłowości Analizator wyświetli w dolnej części okna konfiguracyjnego alarm informujący o wykrytym problemie wraz z odpowiednim symbolem: 50 lub 51. Poniżej znajdują się przykładowe komunikaty Analizatora reguł.



Przykładowe reguły Firewall:

Przepuszczenie ruchu WWW (http i https) z sieci LAN do Internetu:

		Stan	Akcja	Adres źródłowy	Adres docelowy	Port docelowy	Analiza protokoł...	Polityki filtrowania
1		włączona	zezwól	Network_LAN	Internet	http https		IPS

Reguła zezwalająca na dostęp administracyjny (SSH, WebGUI) z Internetu do urządzenia:

		Stan	Akcja	Adres źródłowy	Adres docelowy	Port docelowy	Analiza protokoł...	Polityki filtrowania
1		włączona	zezwól	Internet	Firewall_out	ssh https		IPS

Zezwolenie na PING (ICMP) pomiędzy sieciami LAN i DMZ:

		Stan	Akcja	Adres źródłowy	Adres docelowy	Port docelowy	Analiza protokołów	Polityki filtrowania
1		włączona	zezwól	Network_LAN	Network_DMZ	Any	wyłącznie icmp (Echo request (Ping))	IPS

Wskazówka

W systemie operacyjnym urządzenia - NS-BSD reguły filtrowania przechowywane są odpowiednio w:
`/usr/Firewall/ConfigFiles/Filter/XX`

Gdzie XX jeśli plikiem oznaczającym numer profilu (zestaw reguł).
W przypadku konfiguracji przy użyciu CLI, można aktywować poszczególne profile komendą:
`enfilter XX`

Natomiast polecenie:
`enfilter off`
zupełnie wyłączy filtrowanie pakietów (wyłączy firewalla).

Informacja o profilach, czyli ich nazwa i numer znajduje się w pliku:
`/usr/Firewall/ConfigFiles/Filter/slotinfo`

9. Konfiguracja translacji adresów (NAT)

Translacja adresów nazywana również maskaradą IP jest mechanizmem tłumaczenia adresów prywatnych sieci lokalnej na adresy publiczne otrzymane od usługodawcy Internetu (ISP).

Rozróżnia się dwa podstawowe typy translacji adresów:

SNAT (*Source Network Address Translation*) – polega na podmianie źródłowego adresu IP w pakiecie. SNAT stosowany jest w przypadku połączenia z sieci LAN (z adresacją prywatną) do Internetu.

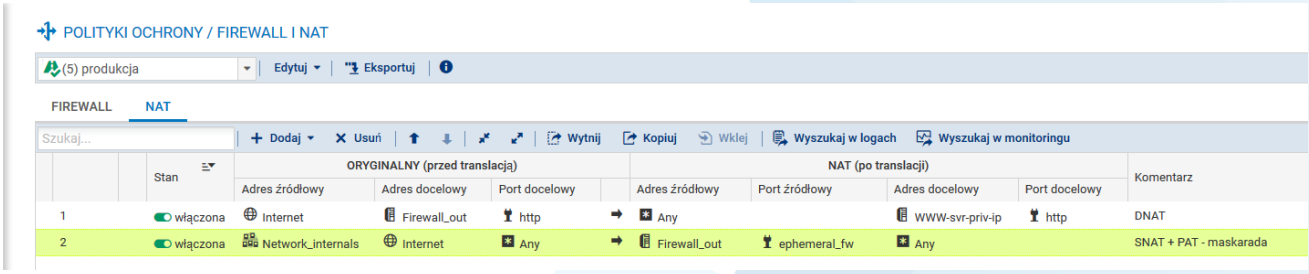
DNAT (*Destination Network Address Translation*) – polega na podmianie docelowego adresu IP w pakiecie. DNAT jest stosowany do udostępnienia w Internecie zasobów sieci wewnętrznej, takich które mają prywatny adres IP.

Oba typy translacji adresów można łączyć, przez co można się również spotkać z jednoczesną translacją adresu źródłowego i docelowego tzw. Source and Destination NAT.

Mechanizm NAT może służyć nie tylko do zmiany adresów IP, ale również do zmiany portów używanych w komunikacji (translacja nagłówka TCP/UDP) jest to tzw. PAT (*Port Address Translation*). PAT jest zazwyczaj połączony z DNAT.

Konfiguracja NAT połączona jest z konfiguracją Firewall i znajduje się w sekcji KONFIGURACJA > POLITYKI OCHRONY > Firewall i NAT. Aktywując Firewall aktywuje się również NAT. Połączenie konfiguracji tych modułów oznacza również, że tak jak w zaporze reguły NAT przetwarzane są zgodnie z ich kolejnością (począwszy od góry).

Konfiguracja NAT polega na zdefiniowaniu jak powinien wyglądać nagłówek TCP/IP po przejściu pakietu przez urządzenie i podzielona jest na dwa etapy. W pierwszym definiowane jest dopasowanie ruchu do reguły – jeśli oryginalny nagłówek pakietu znajdzie dopasowanie do reguły NAT, to wykonywany jest drugi etap polegający na podmianie poszczególnych elementów nagłówka TCP/IP.



Dopasowanie ruchu sieciowego do reguły NAT – pakiet ORYGINALNY (przed translacją)

Kolumna Adres źródłowy:

- Użytkownik – uwierzytelniony użytkownik bazy LDAP
- Adres źródłowy – źródłowy adres IP pakietu inicjującego połączenie. Może to być pojedynczy host, zakres adresów, sieć, grupa adresów.
- Interfejs wejściowy – interfejs, na którym pojawia się pierwszy pakiet inicjujący połączenie.

Kolumna Adres docelowy:

- Adres docelowy – adres IP przeznaczenia pakietu. Może to być pojedynczy host, zakres adresów, sieć, grupa adresów.

- **Interfejs wyjściowy** – interfejs, którym pakiet opuści urządzenie.

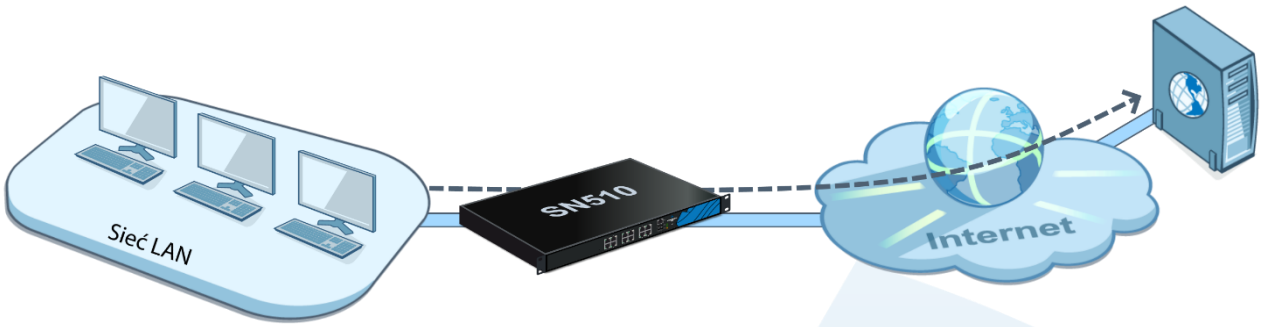
Kolumna **Port docelowy**:

- **Port docelowy** – określa usługę, z której będą korzystać obiekty określone w **Adresie źródłowym** łącząc się do obiektu określonego w **Adresie docelowym**.

Konfiguracja poszczególnych typów translacji

Source NAT (SNAT)

Rysunek poniżej ilustruje wykorzystanie translacji adresów typu **Source NAT**.
Następuje tutaj zmiana adresu źródłowego po przejściu pakietu przez router. Jest to tzw. translacja **n:1**, czyli zmiana wielu adresów prywatnych (**n**) (w poniższym przykładzie jest to cała sieć Network_LAN) na jeden publiczny (**1**) (w przykładzie jest to obiekt Firewall_out).



ORYGINALNY (przed translacją)				NAT (po translacji)			
Adres źródłowy	Adres docelowy	Port docelowy		Adres źródłowy	Port źródłowy	Adres docelowy	Port docelowy
Network_LAN	Internet interfejs wyjściowy: out	Any	➡	Firewall_out	ephemeral_fw	Any	

ORYGINALNY (przed translacją)

- **Adres źródłowy** – Sieć LAN (dowolny adres z sieci LAN).
- **Adres docelowy** – Internet (dowolny docelowy adres IP w Internecie), dodatkowo ruch musi być trasowany przez interfejs OUT.
- **Port docelowy** – Any (dowolny).

NAT (po translacji)

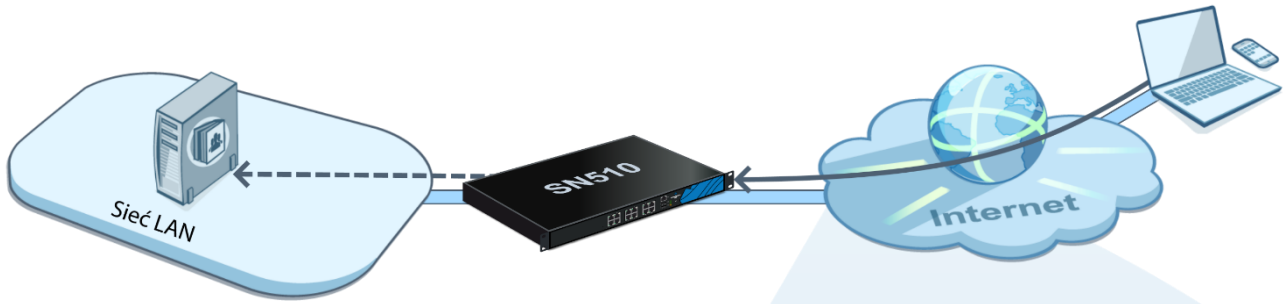
- **Adres źródłowy** – Firewall_out czyli obiekt reprezentujący publiczny adres IP urządzenia STORMSHIELD UTM. Warto tutaj zauważyć, że jeśli ruch ma być zmieniony na publiczny adres IP, który nie jest zdefiniowany na żadnym z interfejsów urządzenia, konieczne będzie zaznaczenie opcji *Publikacja ARP*.
- **Port źródłowy** – ephemeral_fw jest to specjalny obiekt reprezentujący pulę wysokich portów (20 000 – 59 999).
- **Adres docelowy** – Any lub puste pole oznacza, że oryginalny docelowy adres IP pozostanie bez zmian.
- **Port docelowy** – Any lub puste pole oznacza, że oryginalny port docelowy TCP/UDP pozostanie bez zmian.

Jak czytać powyższą translację SNAT?

Każde połączenie pochodzące z sieci LAN, które jest kierowane do Internetu i opuści urządzenie interfejsem OUT zostanie poddane translacji NAT, po której źródłowy adres IP zostanie zmieniony na publiczny adres IP urządzenia reprezentowany przez obiekt Firewall_out, a port źródłowy zostanie nadpisany nowym portem wysokim (z zakresu 20 000 – 59 999). Docelowy adres IP nie ulegnie zmianie. Dzięki temu ruch sieciowy z sieci wewnętrznej może zostać przekazany do sieci Internet, a jeśli docelowy host odpowie, to taka odpowiedź trafi do STORMSHIELD UTM, który będzie wiedział, do którego hosta w sieci wewnętrznej ma taką odpowiedź przekazać.

Destination NAT (DNAT)

Translacja adresów **Destination NAT** inaczej zwana również jako tzw. redirect, jest przydatna w przypadku przekierowania usług z zewnętrznego interfejsu STORMSHIELD UTM do sieci lokalnej na adres prywatny. Przykładem takiego przekierowania może być np. przekierowanie połączenia zdalnego pulpitu Windows (Microsoft Terminal Services).



58

Klient sieci Internet będzie łączył się na adres publiczny urządzenia STORMSHIELD UTM, gdzie nastąpi przekierowanie na prywatny adres IP hosta w sieci LAN.
Taka reguła NAT będzie wyglądać następująco.

ORYGINALNY (przed translacją)				NAT (po translacji)			
Adres źródłowy	Adres docelowy	Port docelowy		Adres źródłowy	Port źródłowy	Adres docelowy	Port docelowy
Internet	Firewall_out	microsoft-ts	➡	Any		TS-svr-priv-ip	microsoft-ts

ORYGINALNY (przed translacją)

- **Adres źródłowy** – Internet (ruch przychodzący z poza sieci wewnętrznych).
- **Adres docelowy** – Firewall_out czyli obiekt reprezentujący publiczny adres IP urządzenia STORMSHIELD UTM. Podobnie jak w przypadku SNAT jeśli ruch jest kierowany na publiczny adres IP, który nie jest zdefiniowany na żadnym z interfejsów urządzenia, konieczne będzie zaznaczenie opcji *Publikacja ARP*.
- **Port docelowy** – Port, na który nawiązywane jest oryginalne połączenie.

NAT (po translacji)

- **Adres źródłowy** – Any lub puste pole oznacza, że oryginalny źródłowy adres IP pozostanie bez zmian.
- **Port źródłowy** – Any lub puste pole oznacza, że oryginalny port źródłowy TCP/UDP pozostanie bez zmian.

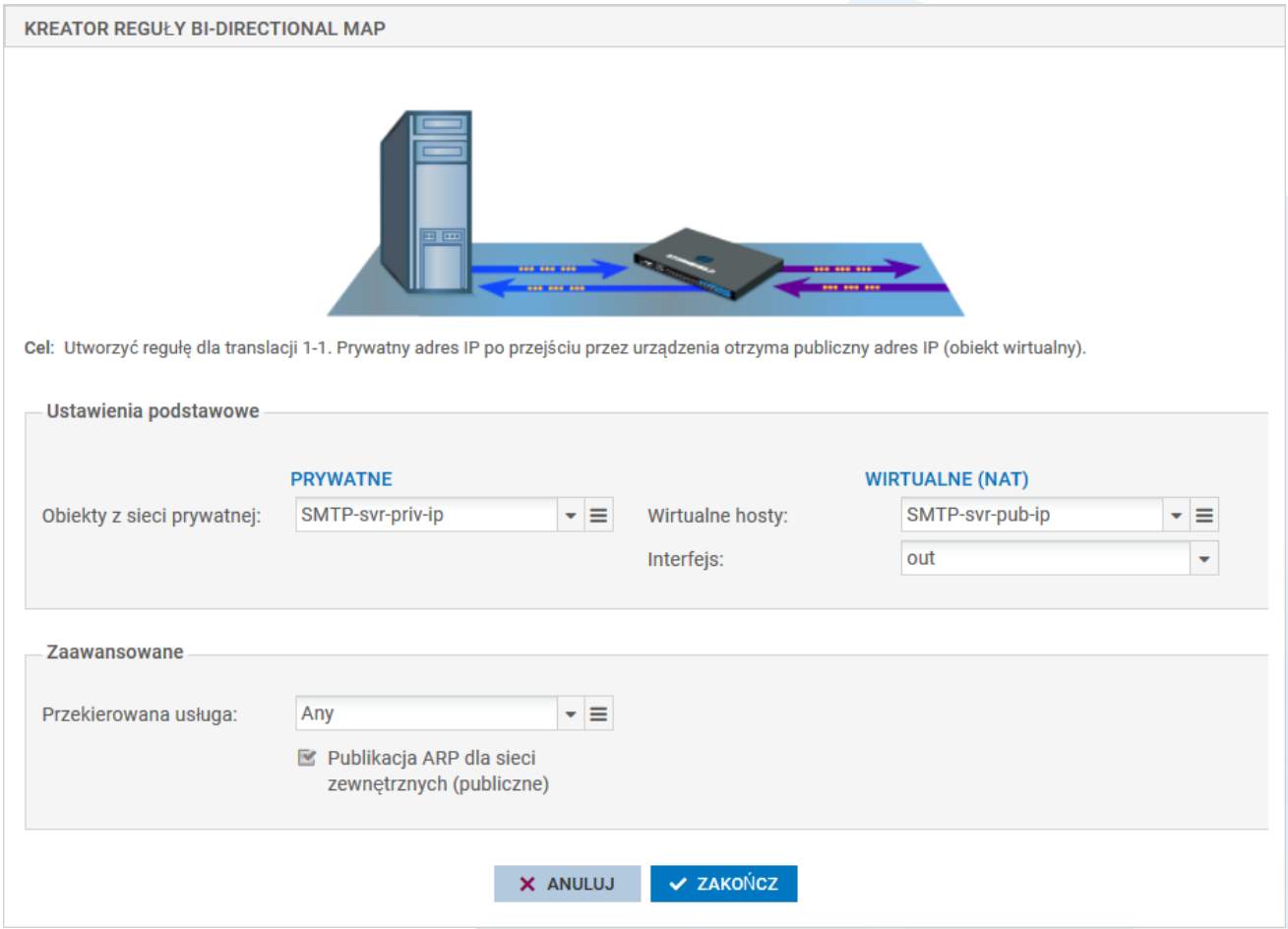
- **Adres docelowy** – Obiekt reprezentujący prywatny adres IP serwera docelowego.
- **Port docelowy** – Port na którym działa usługa na serwerze docelowym.

Jak czytać powyższą translację DNAT?

Każde połączenie z Internetu, które jest nawiązywane na publiczny adres IP urządzenia na port microsoft-ts (3389 TCP) zostanie poddane translacji NAT, w ramach której źródłowy adres IP i port źródłowy nie zmienią się, natomiast docelowy adres IP zostanie zamieniony na prywatny adres IP serwera terminali z zachowaniem portu docelowego. Dzięki temu serwer ww. usługi w sieci lokalnej będzie widział takie połączenie nie z adresem IP STORMSHIELD UTM lecz urządzenia w sieci Internet, od którego pochodzi ten ruch sieciowy.

Bi-Directional map (BI-MAP)

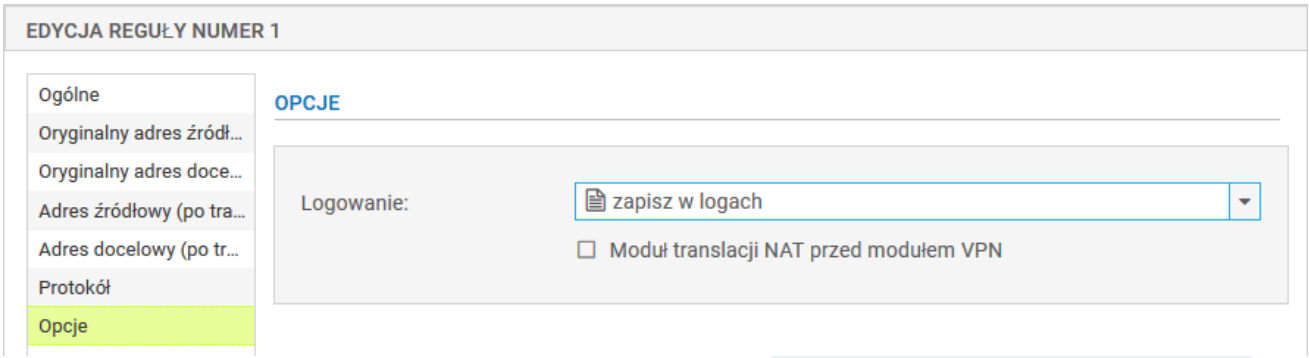
Operacja **Bi-Directional MAP** jest translacją typu **1:1**, tzn. pozwala na przypisanie adresowi IP z sieci lokalnej wirtualnego adresu publicznego. BI-MAP składa się z dwóch reguł, z których jedna jest regułą SNAT, a druga DNAT. Translacja BI-MAP wymaga użycia adresu IP niebędącego adresem urządzenia STORMSHIELD UTM. Taki rodzaj NAT stosuje się najczęściej w przypadku kiedy serwer ma „wychodzić" do Internetu z takim samym publicznym adresem IP, pod którym odbiera połączenia przychodzące do niego, czyli np. serwer pocztowy. Konfiguracja translacji BI-MAP odbywa się poprzez **Kreator reguły BIMAP (1 do 1)**.



Zakończenie pracy kreatora owocuje utworzeniem dwóch reguł – jednej dla ruchu wychodzącego z serwera do Internetu i drugiej dla ruchu przychodzącego z Internetu. Ponieważ publiczne IP nie jest zdefiniowane na interfejsie urządzenia należy zaznaczyć opcję *Publikacja ARP*.

ORYGINALNY (przed translacją)				NAT (po translacji)			
Adres źródłowy	Adres docelowy	Port docelowy		Adres źródłowy	Port źródłowy	Adres docelowy	Port docelowy
SMTP-svr-priv-ip	Any interfejs wyjściowy: out	Any	➡	ARP SMTP-svr-pub-ip			
Any interfejs wejściowy: out	ARP SMTP-svr-pub-ip	Any	➡			SMTP-svr-priv-ip	

Do analizowania i rozwiazywania problemów z translacją NAT można użyć opcji logowania. Każde połączenie odpowiadające regule NAT będzie zapisane w logach. I tak, dla opcji *Logowanie: zapisz w logach* będzie to dziennik Filtering (MONITRONG > LOGI > Ruch sieciowy), natomiast dla opcji *Logowanie: alarm: priorytet niski* lub *alarm: priorytet wysoki* będzie to dziennik Alarmy (MONITRONG > LOGI > Alarmy).



10. System wykrywania i blokowania włamań ASQ (IPS)

System zapobiegania włamaniom (IPS: Intrusion Prevention System) w urządzeniach STORMSHIELD UTM wykorzystuje unikalną, stworzoną w laboratoriach firmy STORMSHIELD technologię wykrywania i blokowania ataków ASQ (Active Security Qualification). Analizie w poszukiwaniu zagrożeń i ataków poddawany jest cały ruch sieciowy od trzeciej (Network Layer) do siódmej (Application Layer) warstwy modelu ISO/OSI. Stosowane są trzy podstawowe metody: analiza heurystyczna, analiza protokołów oraz analiza na podstawie sygnatur kontekstowych.

Analiza heurystyczna

W analizie heurystycznej podstawę stanowi analiza statystyczna oraz analiza zachowań. Na podstawie dotychczasowego ruchu i pewnych założeń dotyczących możliwych zmian określa się czy dany ruch jest uznawany za dopuszczalne odchylenie od normy, czy też powinien już zostać uznany za atak.

Analiza protokołów

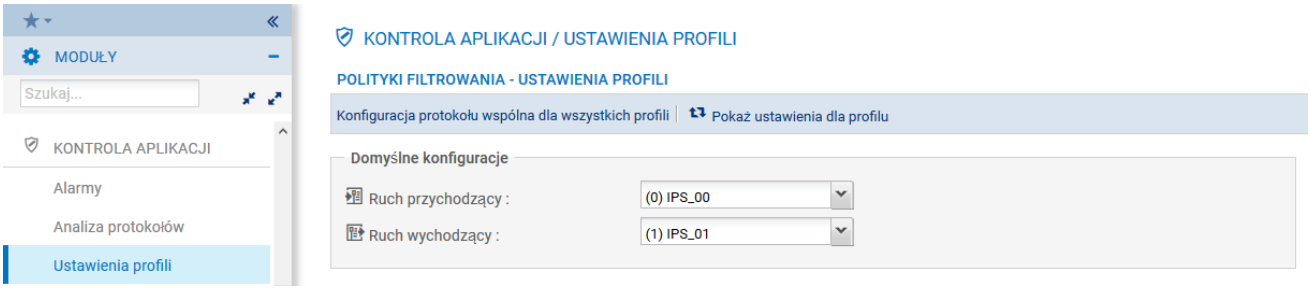
Podczas analizy protokołów kontrolowana jest zgodność ruchu sieciowego przechodzącego przez urządzanie ze standardami RFC. Tylko ruch zgodny z tymi standardami może zostać przepuszczony. Kontroli poddawane są nie tylko poszczególne pakiety, ale także połączenia i sesje. W ramach technologii ASQ dla poszczególnych typów ruchu sieciowego opracowane zostały specjalne pluginy (wtyczki programowe) pracujące w trybie kernel-mode. Po wykryciu określonego typu ruchu (np. HTTP, FTP, SMTP, DNS, …, włączając w to także protokoły przemysłowe m.in. Profinet, Modbus, S7, …) automatycznie uruchamiany jest odpowiedni plugin, który specjalizuje się w ochronie danego protokołu. Tym samym, rodzaj stosowanych zabezpieczeń jest w sposób dynamiczny dostosowywany do rodzaju przepływającego ruchu.

Sygnatury kontekstowe

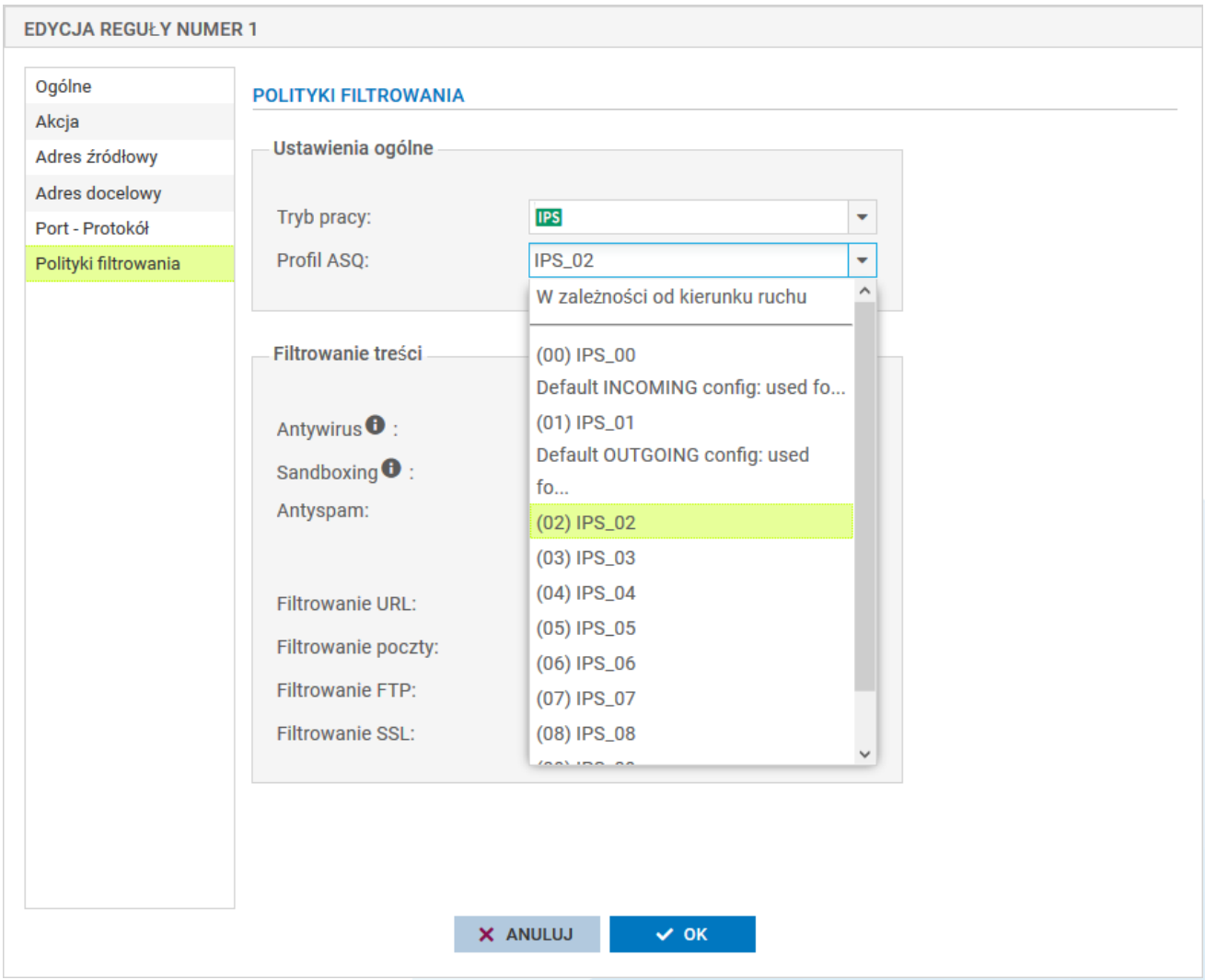
Ostatni z elementów, to systematycznie aktualizowane sygnatury kontekstowe. Pozwalają one na wykrycie znanych już ataków, które zostały sklasyfikowane i dla których zostały opracowane odpowiednie sygnatury. W tym przypadku zasadnicze znaczenie ma kontekst w jakim zostały wykryte pakiety charakterystyczne dla określonego ataku - tzn. rodzaj połączenia, protokół, port. Wystąpienie sygnatury ataku w niewłaściwym dla tego ataku kontekście nie powoduje reakcji systemu IPS. Dzięki temu zastosowanie sygnatur kontekstowych pozwala na znaczne zwiększenie skuteczności wykrywania ataków przy jednocześnie maksymalnym ograniczeniu ilości fałszywych alarmów. Innym istotnym czynnikiem wpływającym na wydajność stosowania sygnatur jest ich optymalizacja pod kątem skanowania podatności występujących w aplikacjach czy protokołach. Jeśli kilka ataków wykorzystuje tą samą podatność tworzona jest tylko jedna sygnatura dla tej podatności, dzięki czemu skraca się czas analizy, a system IPS zabezpiecza sieć również przed tymi atakami, które choć same nie zostały jeszcze opisane to wykorzystują znane dziury i wady protokołów czy aplikacji.

Konfiguracja domyślnych profili IPS

Konfiguracja IPS zawiera 10 w pełni konfigurowalnych profili. Jednak dwa z nich są szczególnie istotne, ponieważ zawierają one konfigurację domyślną dla skanowania ruchu przychodzącego i wychodzącego. Za ruch przychodzący uważa się ten, którego pierwszy pakiet pojawia się na interfejsie oznaczonym jako Zewnętrzny. Ruch wychodzący to taki, którego pierwszy pakiet transmisji pojawia się na interfejsie Wewnętrznym. Konfigurację profili domyślnych przeprowadza się w sekcji KONFIGURACJA > KONTROLA APLIKACJI > Ustawienia profili, gdzie domyślnie ruch przychodzący skanowany jest profilem IPS_00, a ruch wychodzący profilem IPS_01.



Jeśli w ramach filtrowania ruch ma być skanowany innym profilem, to w konfiguracji **Firewall i NAT**, w kolumnie **Polityki filtrowania** należy zmienić opcję **Profil ASQ** z *W zależności od kierunku ruchu*, na wybrany profil.



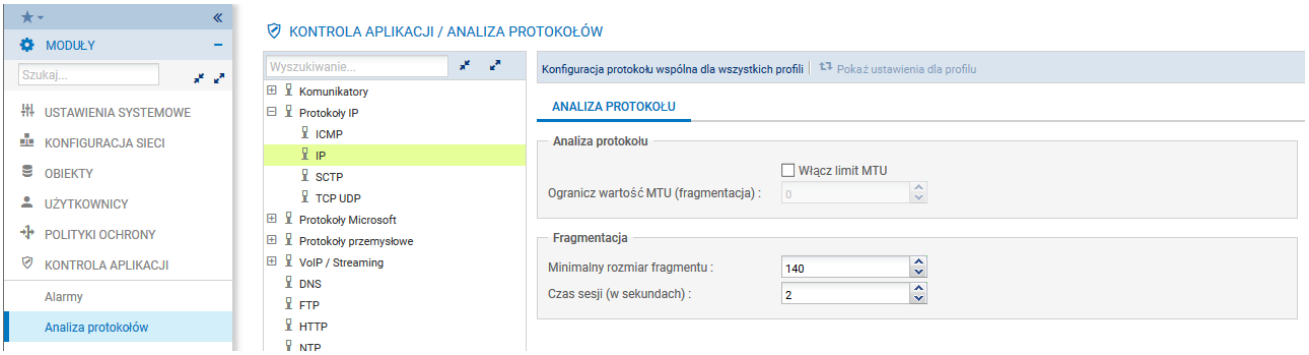
Konfiguracja analizy protokołów

Konfiguracja analizowania protokołów poprzez mechanizm IPS znajduje się w sekcji **KONFIGURACJA > KONTROLA APLIKACJI > Analiza protokołów**. Znajduje się tutaj konfiguracja pluginów dla wszystkich najważniejszych protokołów z warstw od trzeciej (L3) do siódmej (L7) modelu ISO/OSI. Każdy z pluginów zawiera opcje konfiguracyjne dotyczące skanowanych charakterystycznych dla niego parametrów. Dzięki temu efektywność i prędkość skanowania jest maksymalnie zwiększona, ponieważ IPS bada jedynie te

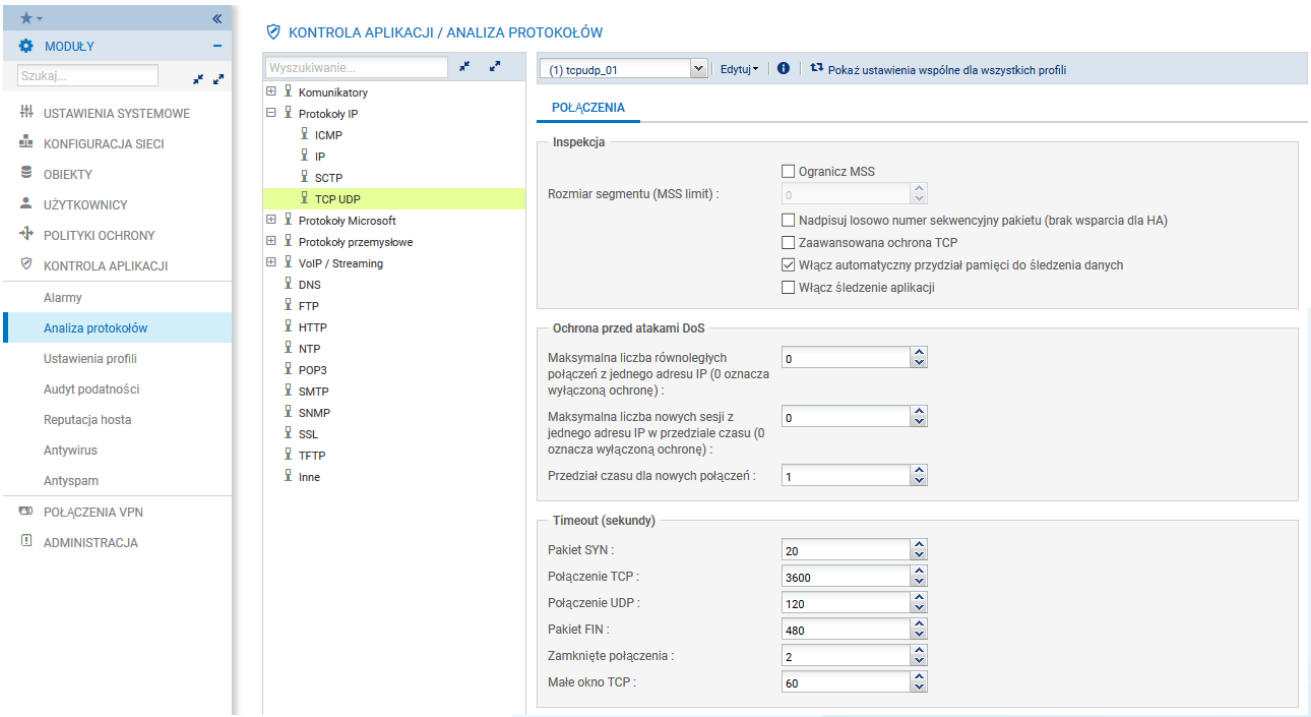
elementy, które mają związek z tym protokołem, natomiast nie analizuje tego co z tym protokołem nie ma żadnego związku.

W początkowej fazie transmisji danych używane są pluginy IP oraz TCP/UDP. Odpowiadają one za prawidłowe otwarcie sesji a więc:

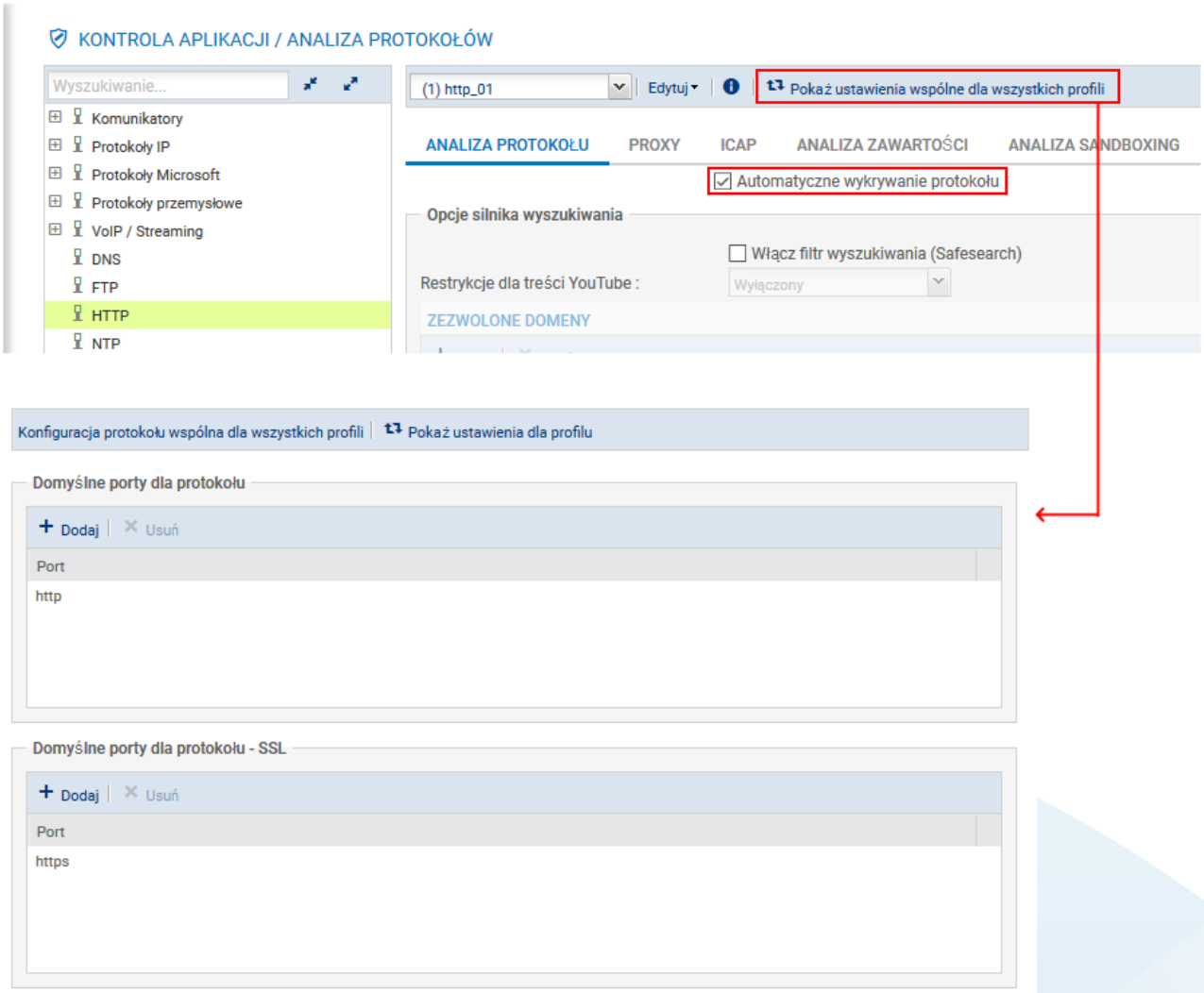
Plugin IP – odpowiada za fragmentację pakietów i ich wielkość.



Plugin TCP/UDP – odpowiada za otwarcie, utrzymanie i zamknięcie sesji.

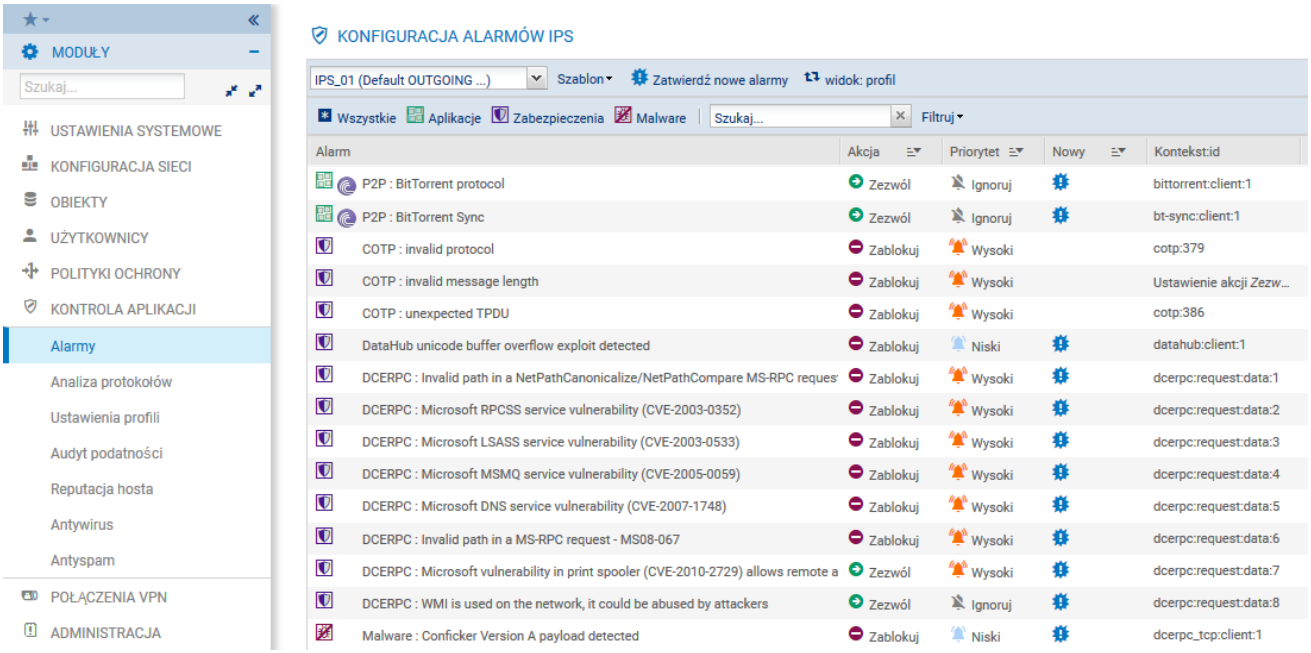


Do każdego nowego połączenia podłączany jest odpowiedni plugin. O tym, który plugin będzie użyty decyduje port, na którym odbywa się komunikacja. Wybierając opcję **Pokaż ustawienia wspólne dla wszystkich profili** w konfiguracji pluginu mamy możliwość zdefiniowania na jakich portach ten plugin będzie używany. Jeśli żaden z pluginów nie obsługuje komunikacji na porcie używanym w czasie połączenia, to ruch będzie skanowany kolejno przez wszystkie pluginy, które mają zaznaczoną opcję **Automatyczne wykrywanie protokołu** w celu ustalenia jakiego typu jest to ruch, i który plugin powinien się nim zająć.



Konfiguracja sygnatur kontekstowych

Jak już wspomniano wyżej, sygnatury służą do filtrowania ruchu pod kątem wystąpienia cech charakterystycznych dla konkretnej podatności lub ataku sieciowego. W przypadku wykrycia schematu działania zgodnego z takim zagrożeniem wywoływany jest odpowiedni alarm oraz wykonywane są zdefiniowane dla niego akcje, które mają na celu np. zablokowanie ruchu. Konfiguracja sygnatur odbywa się w zakładce KONFIGURACJA > KONTROLA APLIKACJI > Alarmy.



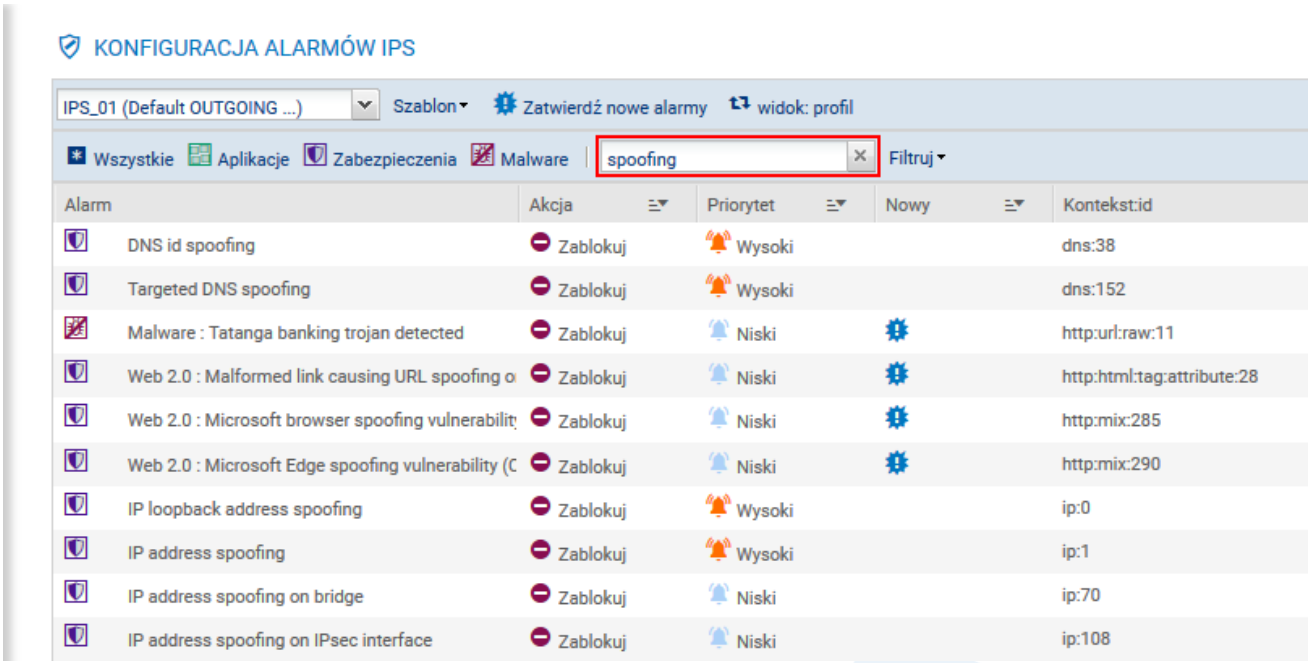
Okno **Alarmy** zawiera następujące elementy:

- **Alarm** – nazwa alarmu/sygnatury.
- **Akcja** – Zablokuj/Zezwól ruch sieciowy.
- **Priorytet** – określa poziom informowania administratora o pojawieniu się danego zagrożenia. Alarmy z priorytetem **Wysokim** lub **Niskim** zapisywane są w logach. Alarmy, dla których ustawiona jest akcja **Ignoruj** nie są wyświetlane (akcja dla tego alarmu nadal jest wykonywana) opcja ta jest przydatna jeśli jakiś alarm „zaśmieca" logi.
- **Nowy** – w tej kolumnie dla każdej nowej sygnatury pojawia się symbol 69. Laboratoria STORMSHIELD na bieżąco pracują nad wykrywaniem nowych ataków, stąd regularnie będą się pojawiać nowe sygnatury. Ten symbol ma na celu wyróżnienie nowych sygnatur, z którymi powinien się zapoznać administrator.
- **Kontekst** – określa plugin jakim dane połączenie jest obsługiwane, poza kontekstem podawane jest również ID sygnatury, co ułatwia przeszukiwanie bazy sygnatur.
- **Zaawansowane** – pozwala na podjęcie dodatkowych akcji, takich jak: wysłanie powiadomienia email, przeniesienie maszyny generującej dany alarm do kwarantanny na określony czas, wykonanie zrzutu pakietu (dump) czy też zastosowanie kolejki QoS dla ruchu generującego dany alarm.

Uwaga

Profile **Analizy protokołów** i **Alarmy** są ze sobą ściśle powiązane, tzn. profil np. **http_00** Analizy protokołów oraz profil **IPS_00** Alarmów tworzą profil **ASQ IPS_00**, a profil **http_02** Analizy protokołów oraz profil **IPS_02** Alarmów tworzą Profil **ASQ IPS_02**. Profil ASQ jest filtrem IPS implementowanym na poziomie reguł firewall.

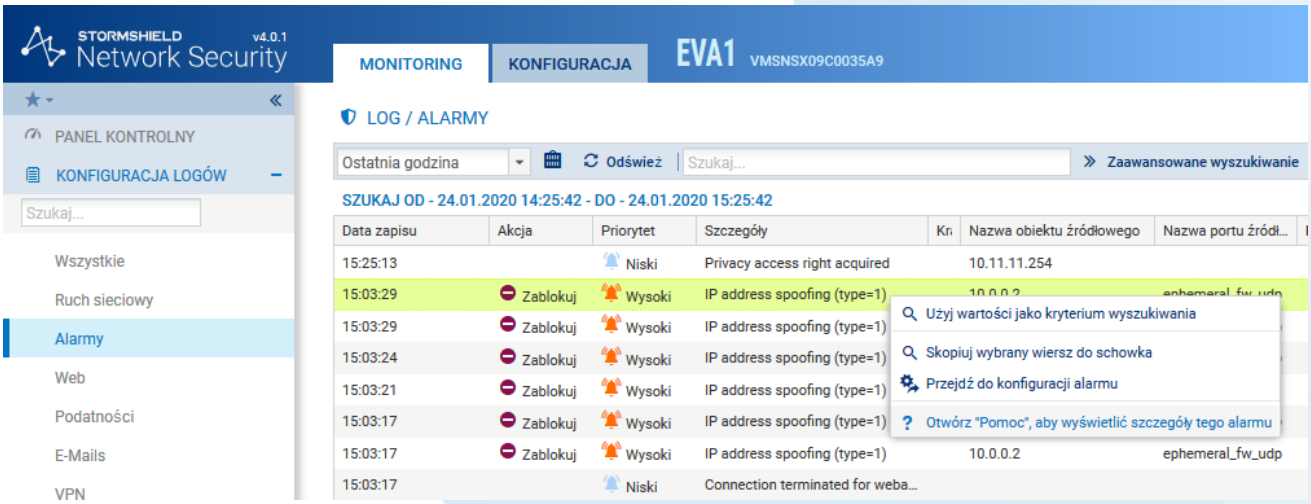
W celu szybszej oraz sprawniejszej konfiguracji sygnatur można skorzystać z filtrowania na podstawie rodzaju sygnatur tj. Aplikacje, Zabezpieczenia, Malware, a także z pola „Szukaj” lub opcji Filtruj zawierającej predefiniowane kategorie aplikacji.



Monitorowanie działania IPS

Działanie systemu IPS możemy kontrolować z poziomu zakładki **MONITORING > Logi > Alarmy**. Znajdują się tutaj wpisy o wystąpieniach wszystkich **Alarmów** o priorytecie Niski lub Wysoki, a także informacje o ruchu zablokowanym przez **Analizę protokołów** (pluginy).

Z tego poziomu możliwe jest również wyświetlenie strony KB (Knowledge Base) zawierającej pełen opis danego alarmu. Pomoc ta jest dostępna z poziomu menu kontekstowego (po kliknięciu na danym wpisie prawym przyciskiem myszy)



11. Konfiguracja Audytu podatności (SEISMO)

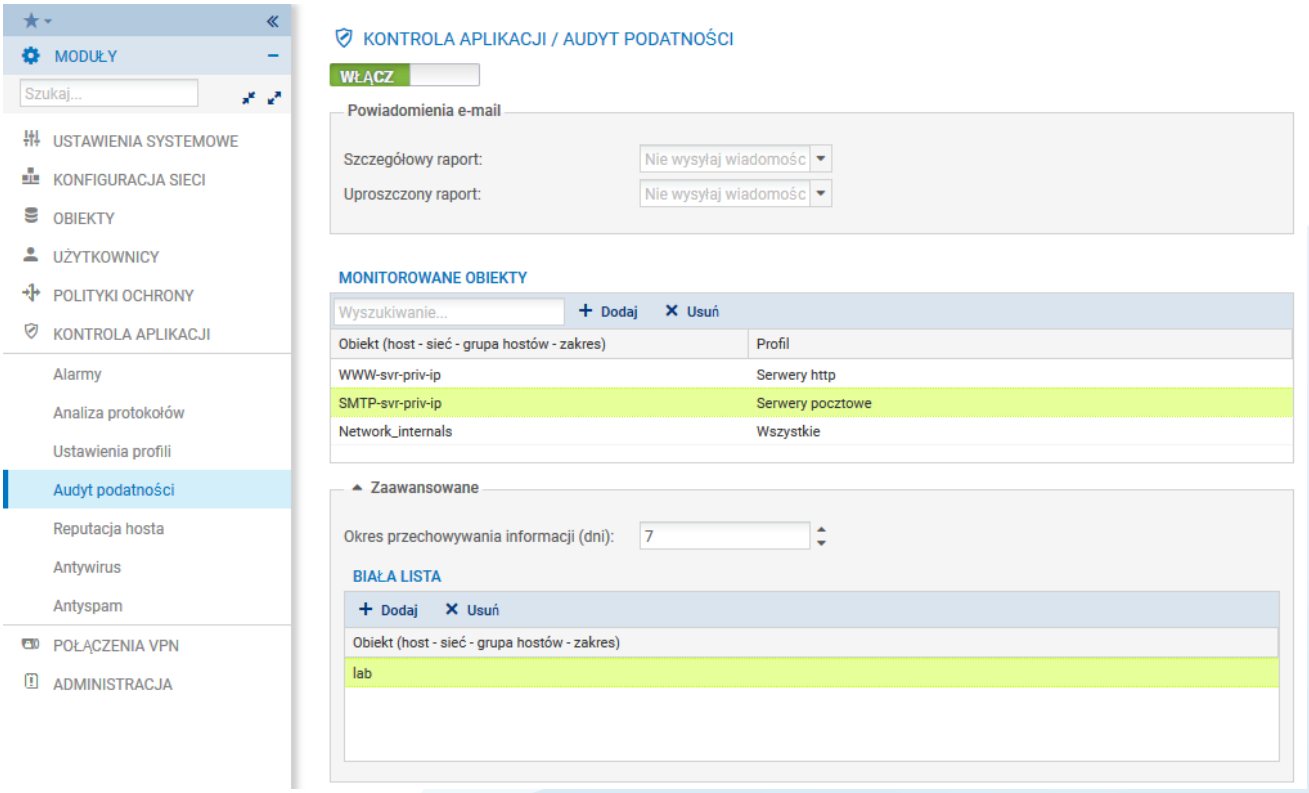
Moduł Audyt podatności jest pasywnym skanerem chronionych sieci. Pasywnym skanerem określamy taki, który nie generuje dodatkowego ruchu w sieci ani nie wymaga instalacji dodatkowego oprogramowania na komputerach w sieci. Skanuje on ruch sieciowy przechodzący poprzez urządzenie STORMSHIELD UTM w kontekście występowania podatności w aplikacjach sieciowych i systemach operacyjnych działających na hostach w tych sieciach.
Audyt podatności wymaga zakupu dodatkowej licencji.

Konfiguracja Audytu podatności odbywa się w zakładce KONFIGURACJA > KONTROLA APLIKACJI > Audyt podatności. Jeśli opcji nie da się włączyć oznacza to, iż zainstalowana na urządzeniu licencja nie zawiera funkcji pasywnego skanera sieci.

Audyt podatności nie blokuje żadnego ruchu, a jedynie wyświetla informacje na temat wykrytych zagrożeń.

W przypadku konfiguracji audytu podatności istotne jest:

- Określenie obiektów, które mają być monitorowane – host, sieć, grupa hostów, zakres.
- Wybranie profilu prowadzonego audytu dla wskazanych obiektów.
- Skonfigurowanie czasu przez jaki informacje o wykrytych zagrożeniach będą przechowywane.
- Zdefiniowanie BIAŁEJ LISTY – wykluczeń ze skanowania.

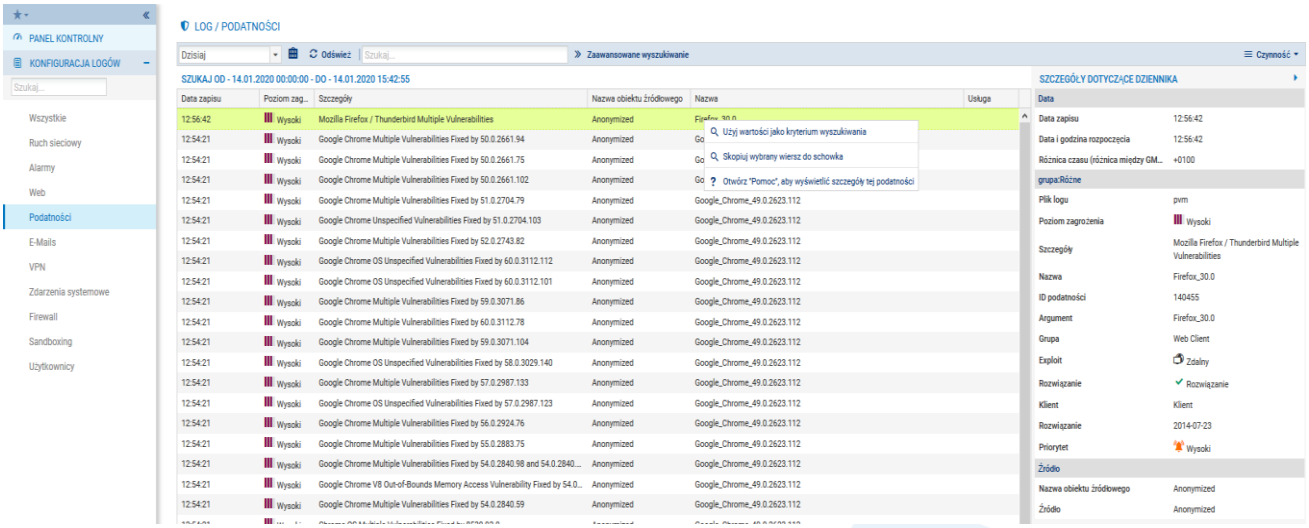


Domyślnie skanowany jest cały ruch generowany przez grupę Network_Internals, czyli wszystkie stacje podłączone do interfejsów określonych jako Wewnętrzne (LAN,DMZ).

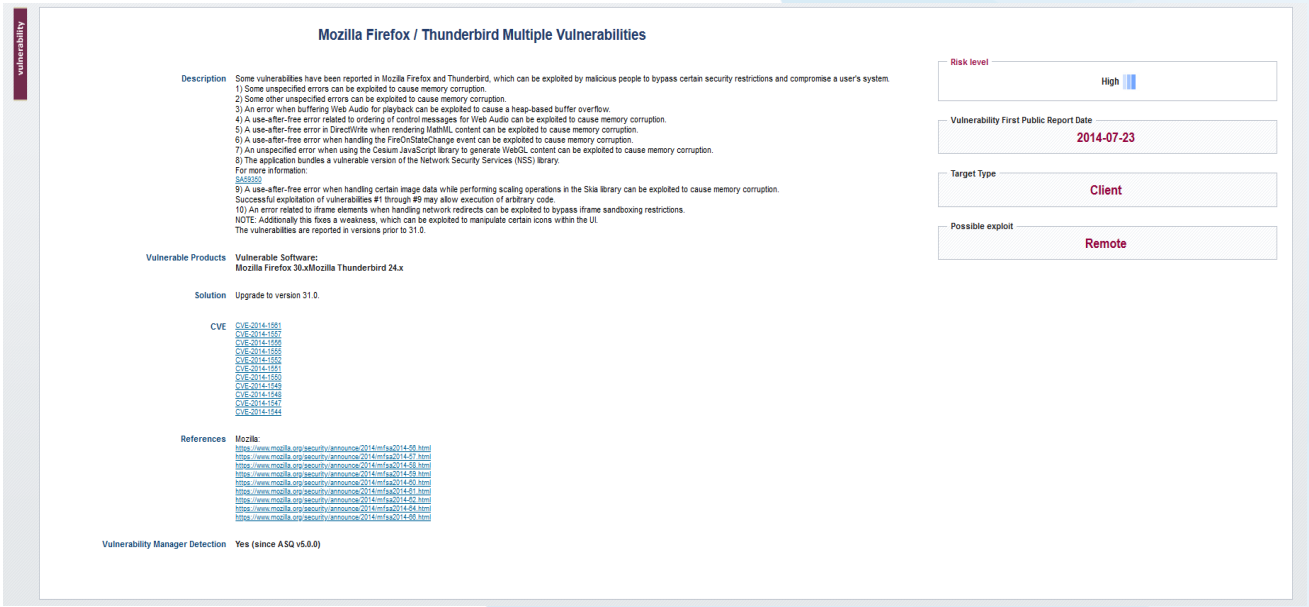
Informacje zebrane przez moduł Audyt podatności można przeglądać w dziennikach logowania MONITORING > LOGI >Podatności lub z poziomu monitorowania hostów MONITORING > MONITOROWANIE > Hosty, po zaznaczeniu interesującego nas hosta dostępna jest zakładka PODATNOŚCI zawierająca

podatności wykryte dla danego hosta. Kolejne zakładki APLIKACJE, USŁUGI, INFORMACJE zawierają dodatkowe informacje generowane przez audyt podatności dotyczące aplikacji oraz systemów działających na hoście. Dzięki temu Audyt podatności jest także doskonałym narzędziem do monitorowania zainstalowanych aplikacji sieciowych i systemów operacyjnych, które działają w sieciach chronionych przez STORMSHIELD UTM.

Poniżej przedstawiony jest przykładowy wynik działania modułu Audyt podatności:



W raporcie znajdziemy między innymi informację o poziomie ważności wykrytego zagrożenia, typie zagrożenia (Web Client itp.), sposobie jego wywołania (Zdalne/Lokalne), informacje o komputerze, na którym została wykryta podatna aplikacja oraz o tym w jakiej wersji jest ta aplikacja. Aby uzyskać dodatkowe informacje o zagrożeniu można z poziomu menu kontekstowego kliknąć **Otwórz „Pomoc", aby wyświetlić szczegóły tej podatności**. Na stronie pomocy można znaleźć dokładny opis zagrożenia oraz linki do stron, na których zostało ono opisane, a także wyjaśnienie jakie czynności należy podjąć, aby wyeliminować to zagrożenie.



12. Autoryzacja użytkowników

W celu określenia obiektu źródłowego, z którego pochodzi ruch sieciowy zazwyczaj stosuje się adres IP takiego hosta. Jednak takie podejście nie informuje o konkretnym użytkowniku lecz o wszystkich użytkownikach danego hosta.
Aby określić konkretnego użytkownika, od którego pochodzi dany ruch sieciowy można skorzystać z mechanizmu autoryzacji użytkowników.

Urządzenie STORMSHIELD UTM pozwala na to poprzez skorzystanie z usług katalogowych. Dostępne są trzy typy takich usług:

- Microsoft Active Directory,
- LDAP,
- LDAP za pośrednictwem PosixAccount.

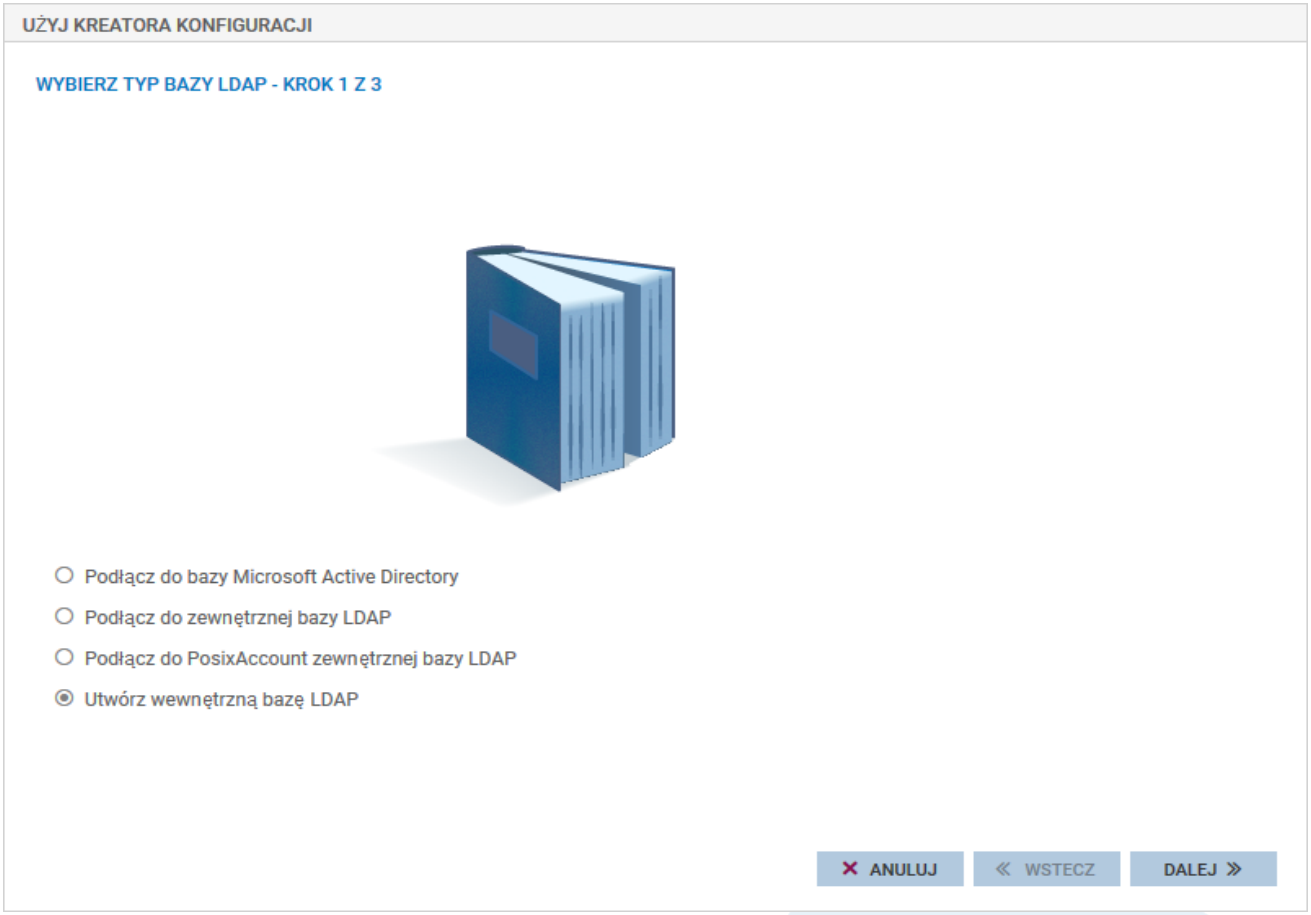
Dodatkowo istnieje możliwość utworzenia jednej wewnętrznej bazy LDAP bezpośrednio w urządzeniu. Należy jednak pamiętać, iż jednocześnie można skonfigurować w urządzeniu maksymalnie pięć takich usług katalogowych: jednej wewnętrznej bazy i czterech zewnętrznych lub pięciu zewnętrznych baz.

Każda z tych baz może być użyta do:

- tworzenia reguł filtrowania/NAT per użytkownik (nie wymaga adresów IP w regułach),
- tworzenia tuneli VPN typu Client-to-Site,
- delegowania zadań administracji urządzeniem na użytkowników.

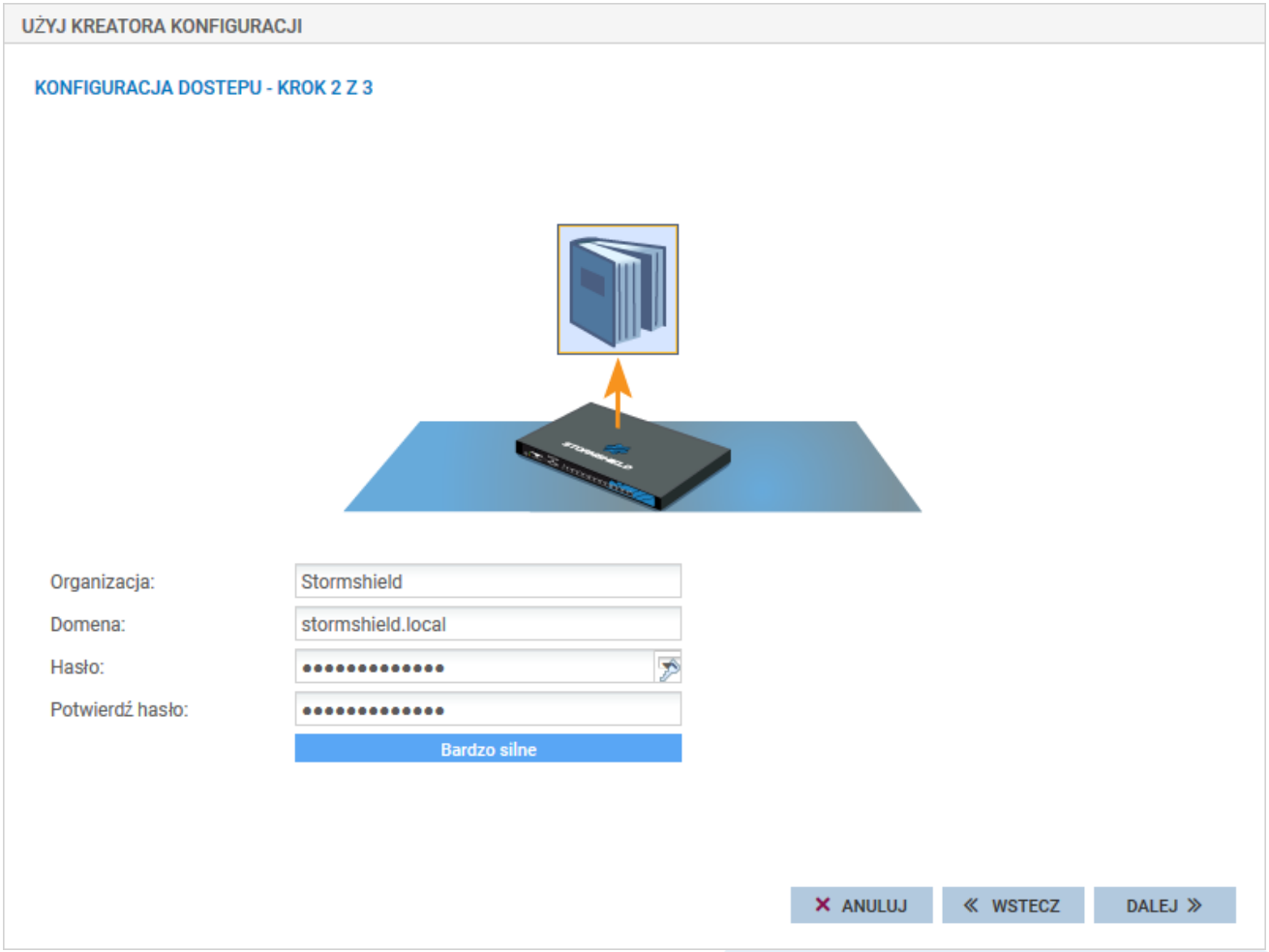
Tworzenie wewnętrznej bazy użytkowników

Aby skonfigurować wewnętrzną bazę użytkowników na urządzeniu STORMSHIELD UTM należy przejść na zakładkę KONFIGURACJA > UŻYTKOWNICY > Konfiguracja bazy LDAP. Jeżeli na urządzeniu nie ma skonfigurowanej żadnej bazy użytkowników uruchomi się KREATOR KONFIGURACJI, jeśli jakakolwiek baza była wcześniej utworzona, należy wybrać opcję Dodaj nowy LDAP. W kreatorze konfiguracji należy wybrać opcję Utwórz wewnętrzną bazę LDAP.



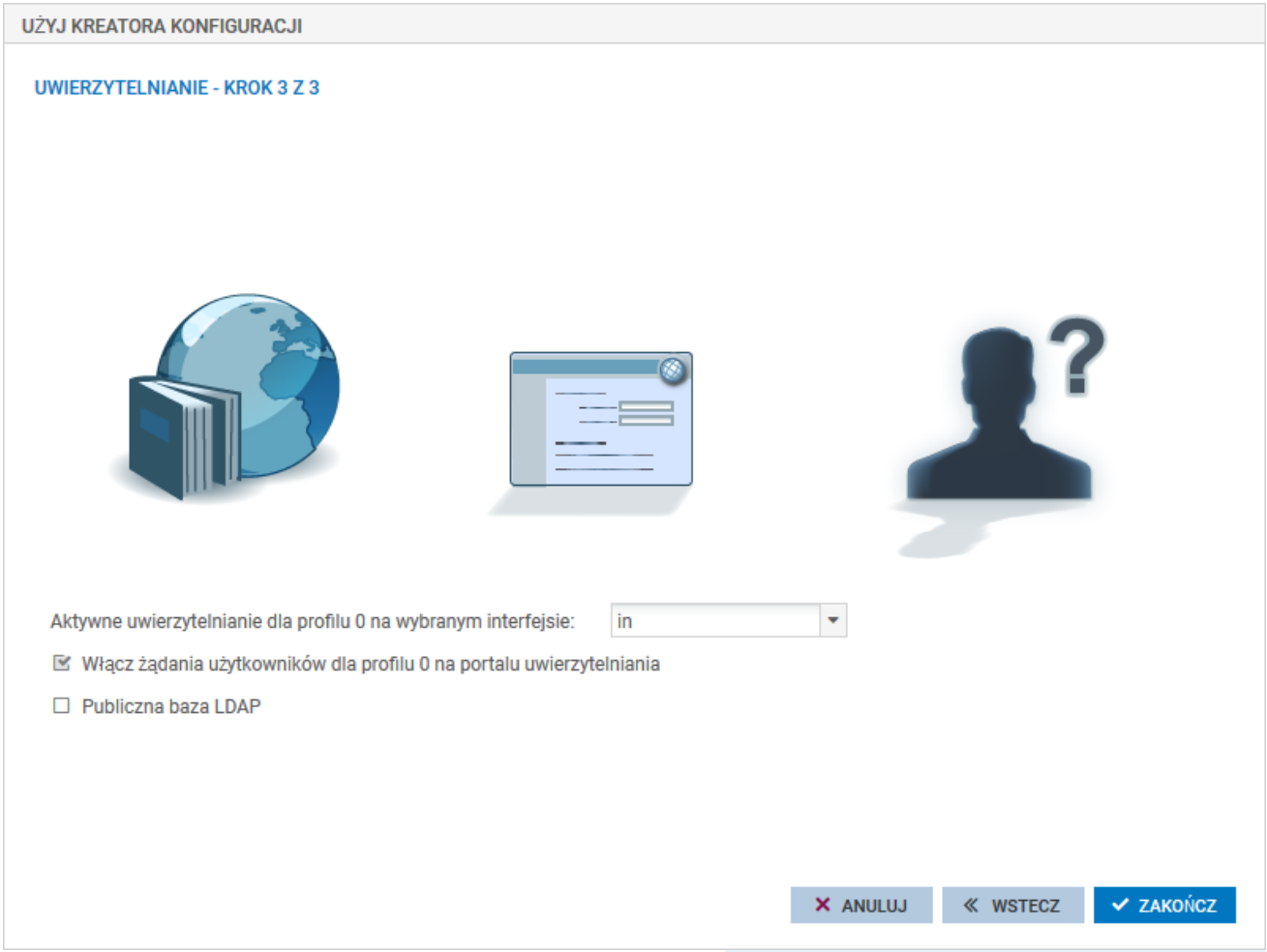
W kolejnym oknie konfiguracyjnym należy wypełnić odpowiednie opcje:

- Organizacja – nazwa firmy np. Stormshield;
- Domena – nazwa domeny;
- Hasło i Potwierdź hasło – hasło administratora domeny (może być użyte do integracji zewnętrznej usługi z lokalną bazą LDAP).

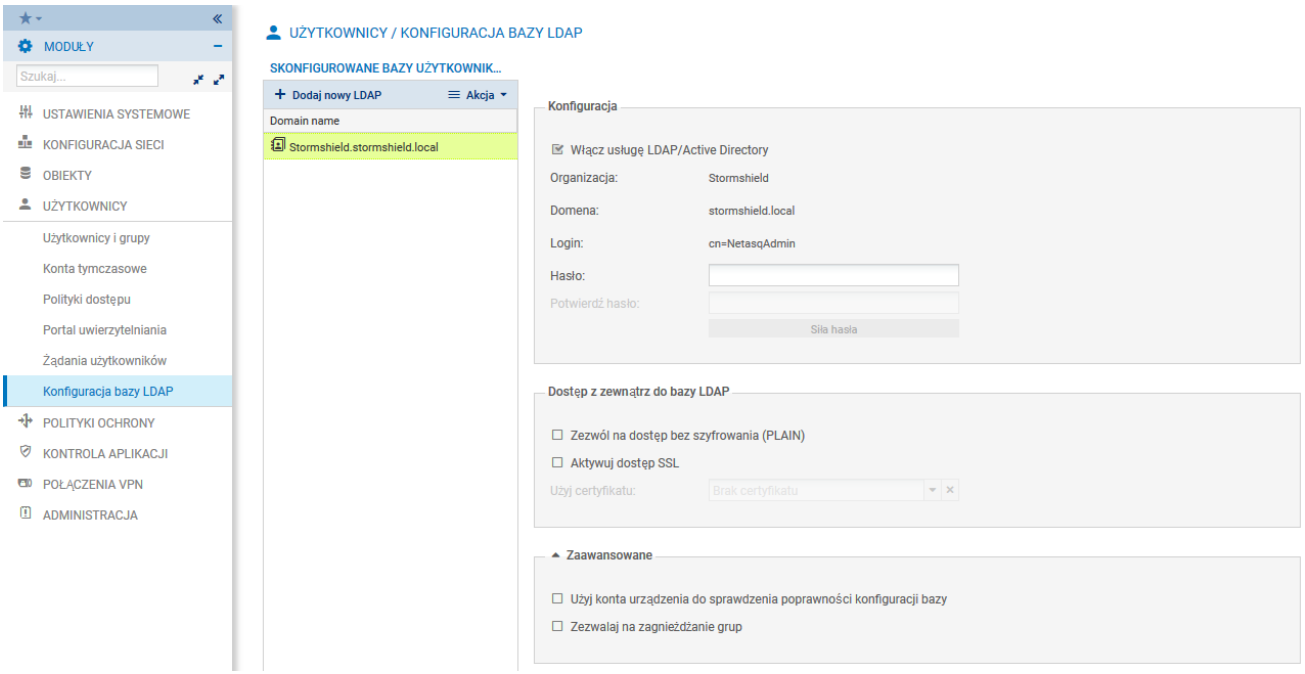


W kolejnym oknie kreatora można skonfigurować dodatkowe opcje bazy LDAP:

- **Aktywne uwierzytelnianie dla profilu 0 na wybranym interfejsie** – na wskazanym interfejsie zostanie automatycznie uruchomiony portal uwierzytelniania (Captive portal), o którym nieco szerzej w dalszej części tej dokumentacji.
  Jeśli profil 0 (internal) jest już przypisany do jakiegokolwiek interfejsu opcja będzie nieaktywna;
- **Włącz żądania użytkowników dla profilu 0 na portalu uwierzytelniania** – włącza usługę rejestracji użytkowników poprzez którą użytkownicy będą mogli zgłaszać prośby o założenie konta w usłudze LDAP, dzięki temu rola administratora może być ograniczona tylko do aktywowania kont zakładanych przez użytkowników;
- **Publiczna baza LDAP** – baza użytkowników może być wykorzystywana przez inne, zewnętrzne usługi sieciowe takie jak np. serwer FTP.



Wybranie przycisku **Zakończ** kończy pracę kreatora i pojawi się okno konfiguracyjne bazy LDAP, w którym możemy wybrać między innymi czy możliwa ma być komunikacja z tą bazą z zewnątrz i czy ma odbywać się w formie zaszyfrowanej czy też nie.

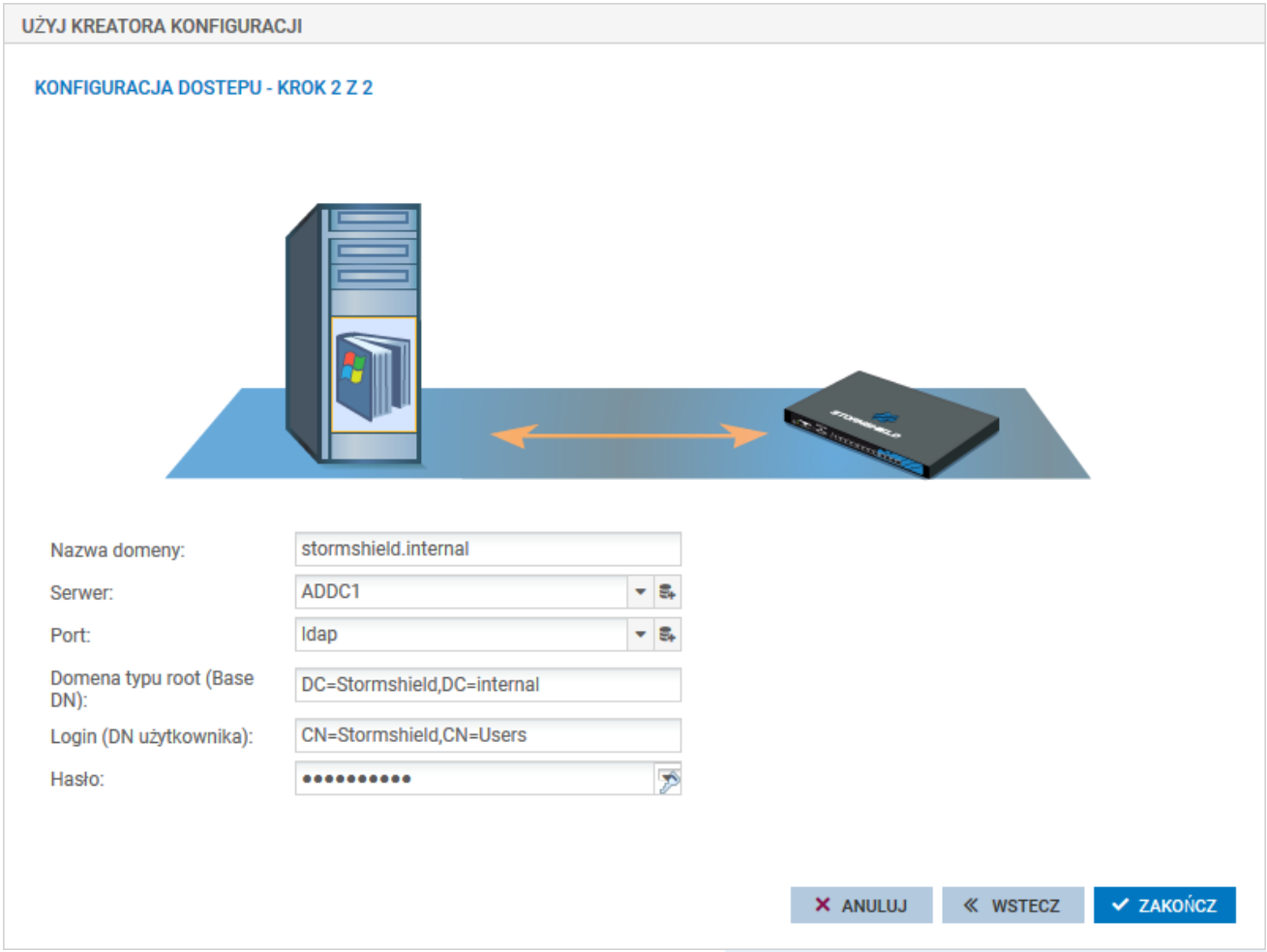


Integracja STORMSHIELD UTM z Microsoft Active Directory

Pierwsze okno kreatora jest takie samo jak w przypadku tworzenia wewnętrznej bazy LDAP. Należy w nim wybrać **Podłącz do Microsoft Active Directory.**

W kolejnym oknie konfiguracyjnym dostępne są następujące pola:

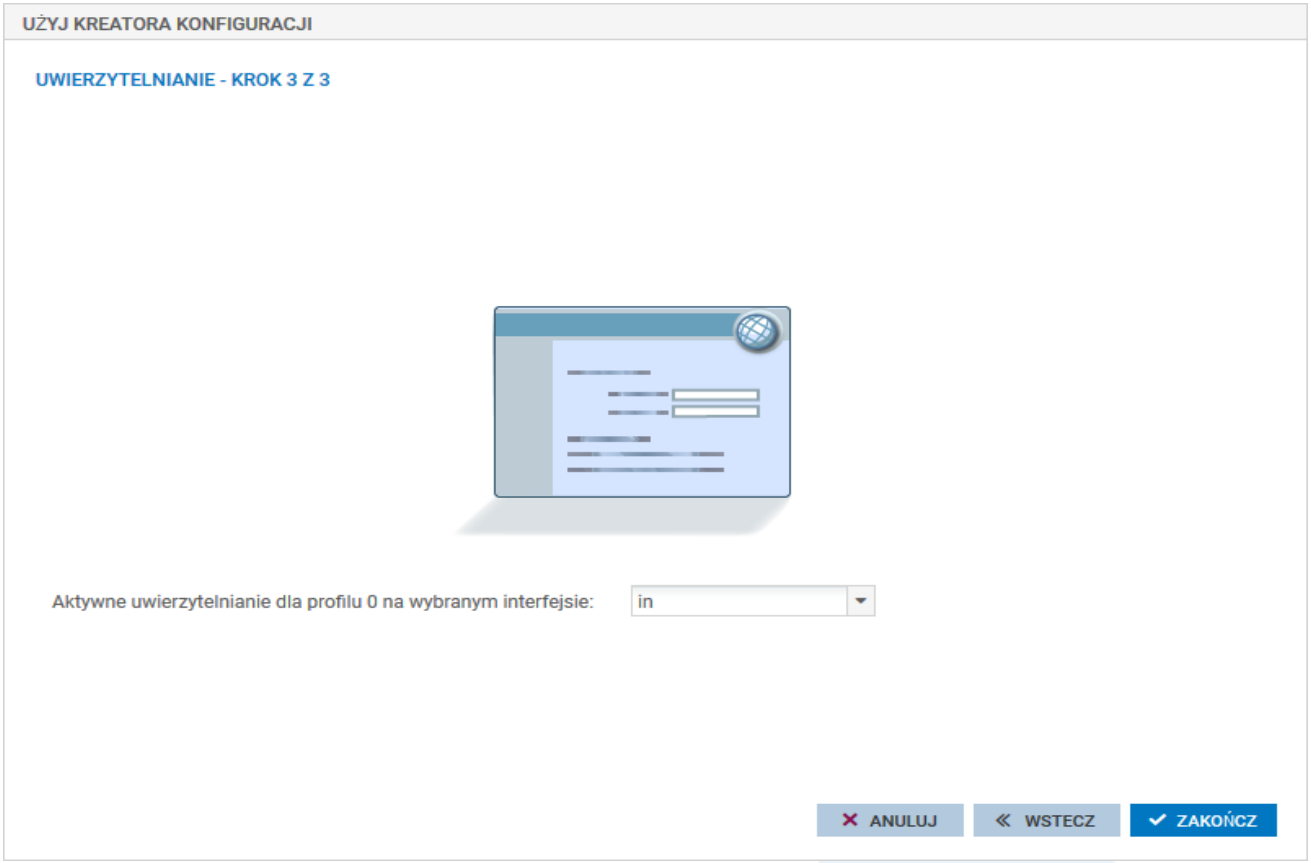
- **Nazwa domeny** – nazwa umożliwiająca identyfikację bazy AD – szczególnie przydatna, gdy na urządzeniu będzie skonfigurowanych kilka baz LDAP. Zalecane jest aby w tym polu była wprowadzona nazwa DNS domeny.
- **Serwer** – obiekt reprezentujący adres IP kontrolera domeny;
- **Port** – port używany do komunikacji z LDAP (domyślnie TCP 389);
- **Domena typu root (Base DN)** – pełna nazwa domeny, np.: dla domeny *stormshield.internal* będzie to *DC=Stormshield,DC=internal*;
- **Login (DN użytkownika)** – login użytkownika używanego do integracji z AD wraz ze wskazaniem kontenera (CN) lub jednostką organizacyjną (OU) AD, w którym znajduje się ten użytkownik. Przykładowo, jeśli do integracji utworzymy dedykowane konto *Stormshield*, które umieścimy w kontenerze *Users*, to w polu ***Login*** należy wpisać: ***CN=Stormshield,CN=Users;***
- **Hasło** – hasło domenowe użytkownika wskazanego w polu **Login**.



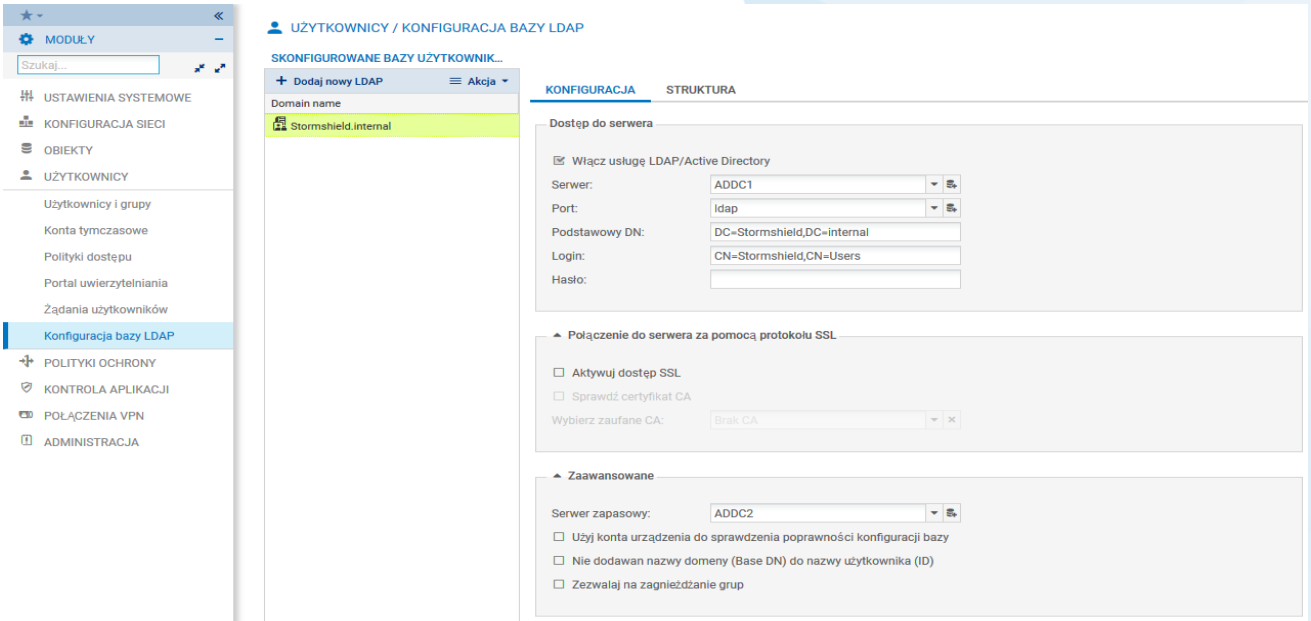
Uwaga

Najczęstsze problemy związane z integracją z domeną AD polegają na wykorzystaniu konta, które nie znajduje się w kontenerze *Users* domeny AD (należy stworzyć użytkownika w kontenerze *Users* i wyłączyć rotację haseł)

W kolejnym oknie kreatora można włączyć opcję *Aktywne uwierzytelnianie dla profilu 0 na wybranym interfejsie*.



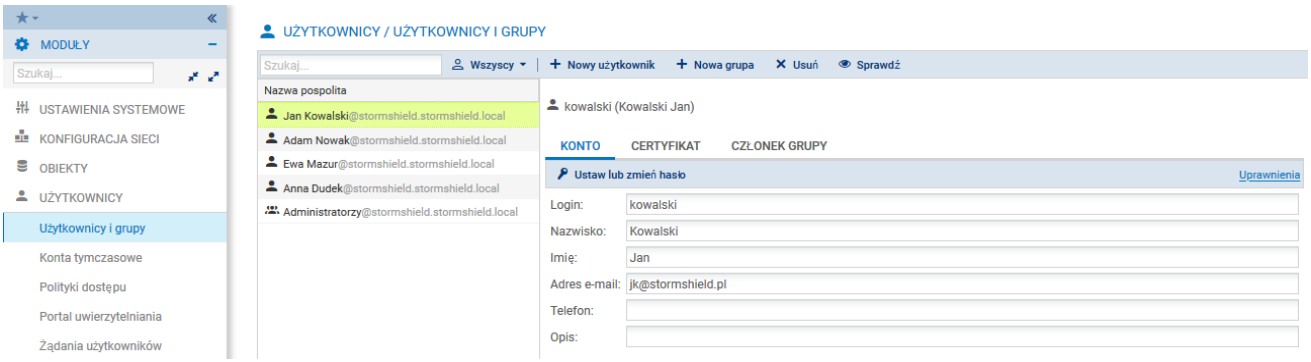
Po zakończeniu pracy kreatora powinno pojawić się poniższe okno, które będzie potwierdzeniem poprawnej integracji.



Okno to pozwala między innymi na wskazanie dodatkowego, zapasowego kontrolera domeny czy też na określenie sposobu łączenia się z bazą Active Directory.

Zarządzanie użytkownikami

Zarządzanie kontami użytkowników odbywa się w sekcji **KONFIGURACJA > UŻYTKOWNICY > Użytkownicy i grupy**. Po przejściu do tego okna konfiguracyjnego możliwe jest tworzenie, modyfikowanie oraz usuwanie kont użytkowników i grup w domyślnej bazie LDAP. Należy pamiętać, że domyślnie lista użytkowników jest pusta. Aby wyświetlić użytkowników należy skorzystać z pola *Szukaj...* bądź też użyć filtr *Wszyscy(Brak)/Użytkownicy/Grupy*.

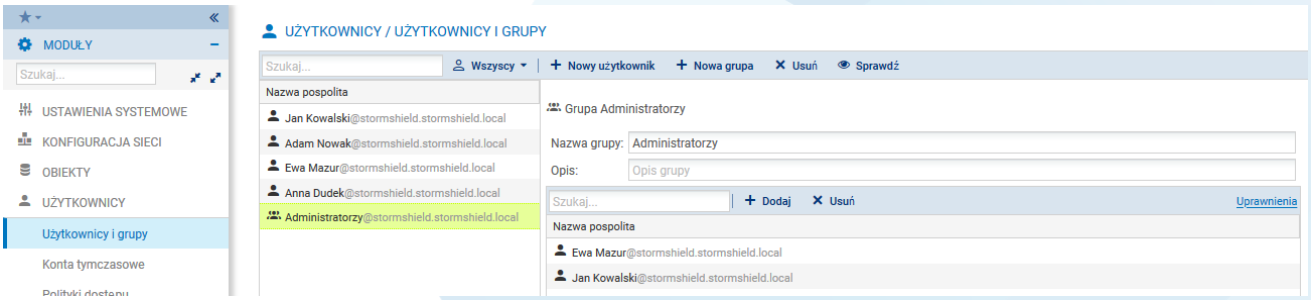


Konto użytkownika pozwala na skonfigurowanie następujących parametrów:

- **Login** – nazwa używana podczas logowania.
- **Nazwisko i Imię** – nazwisko i imię użytkownika.
- **Adres e-mail** – adres e-mail użytkownika. Zawartość tego pola powinna być unikatowa, ponieważ na jego podstawie generowany jest certyfikat użytkownika, ponadto może ono służyć jako identyfikator użytkownika w procesie tworzenia tuneli IPsec VPN.
- **Telefon** – numer telefonu użytkownika.
- **Opis** – opis ułatwiający identyfikację użytkownika w systemie.
- **Certyfikat** – certyfikat użytkownika
- **Członek grupy** – określa przynależność użytkownika do określonych grup bazy LDAP.

Konto grupy pozwala na zdefiniowanie następujących parametrów:

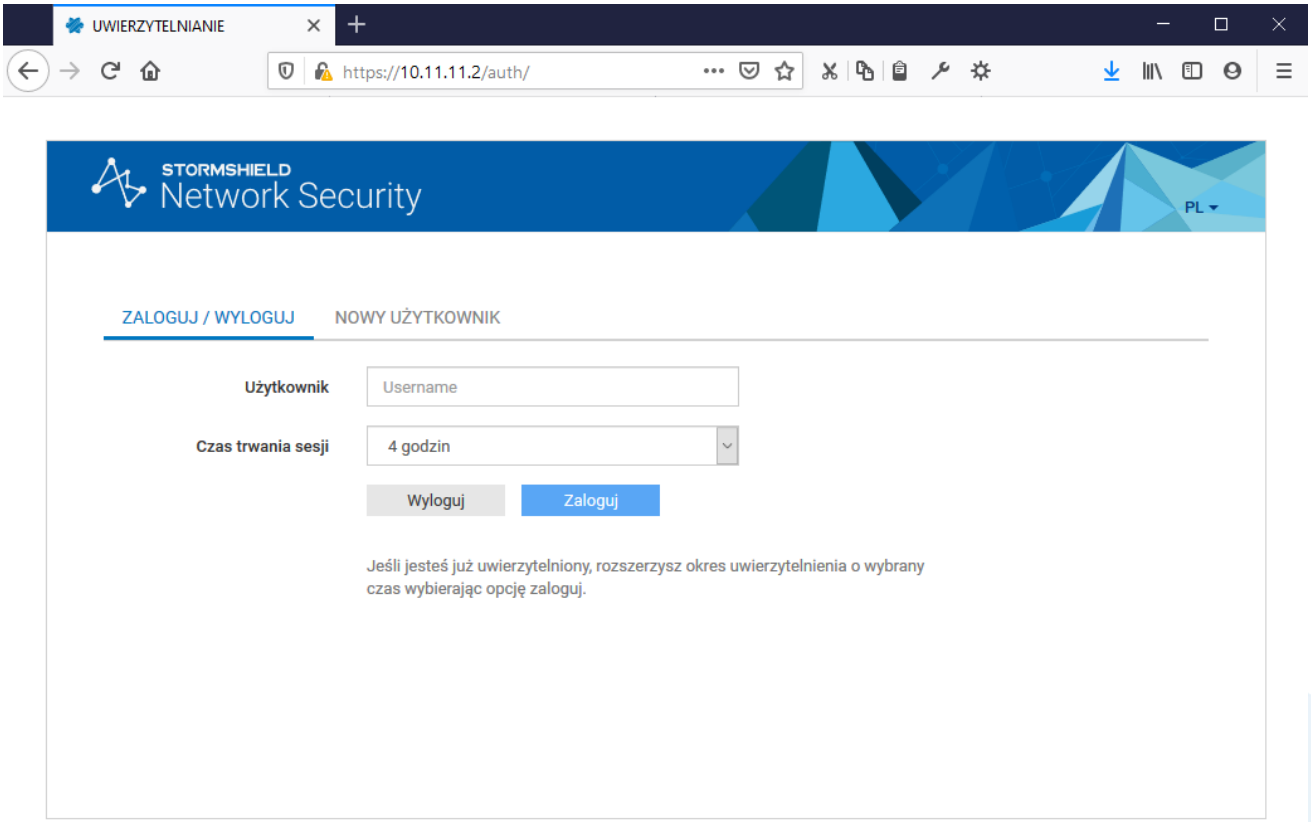
- **Nazwa grupy** – nazwa grupy.
- **Opis** – opis ułatwiający identyfikację grupy.
- **Członkowie grupy** – pole zawierające listę wszystkich członków danej grupy.



Należy zwrócić uwagę na to, że zarządzanie użytkownikami z poziomu STORMSHIELD UTM jest możliwe dla wewnętrznej bazy LDAP. Zarządzenie użytkownikami baz zewnętrznych wykonuje się bezpośrednio w tych bazach.

Portal uwierzytelniania (Captive portal)

Portal uwierzytelniania (Portal autoryzacji) jest specjalną stroną udostępnianą pod adresem **https://IP_STORMSHIELD/auth/** i wykorzystywaną w celu autoryzacji użytkowników.

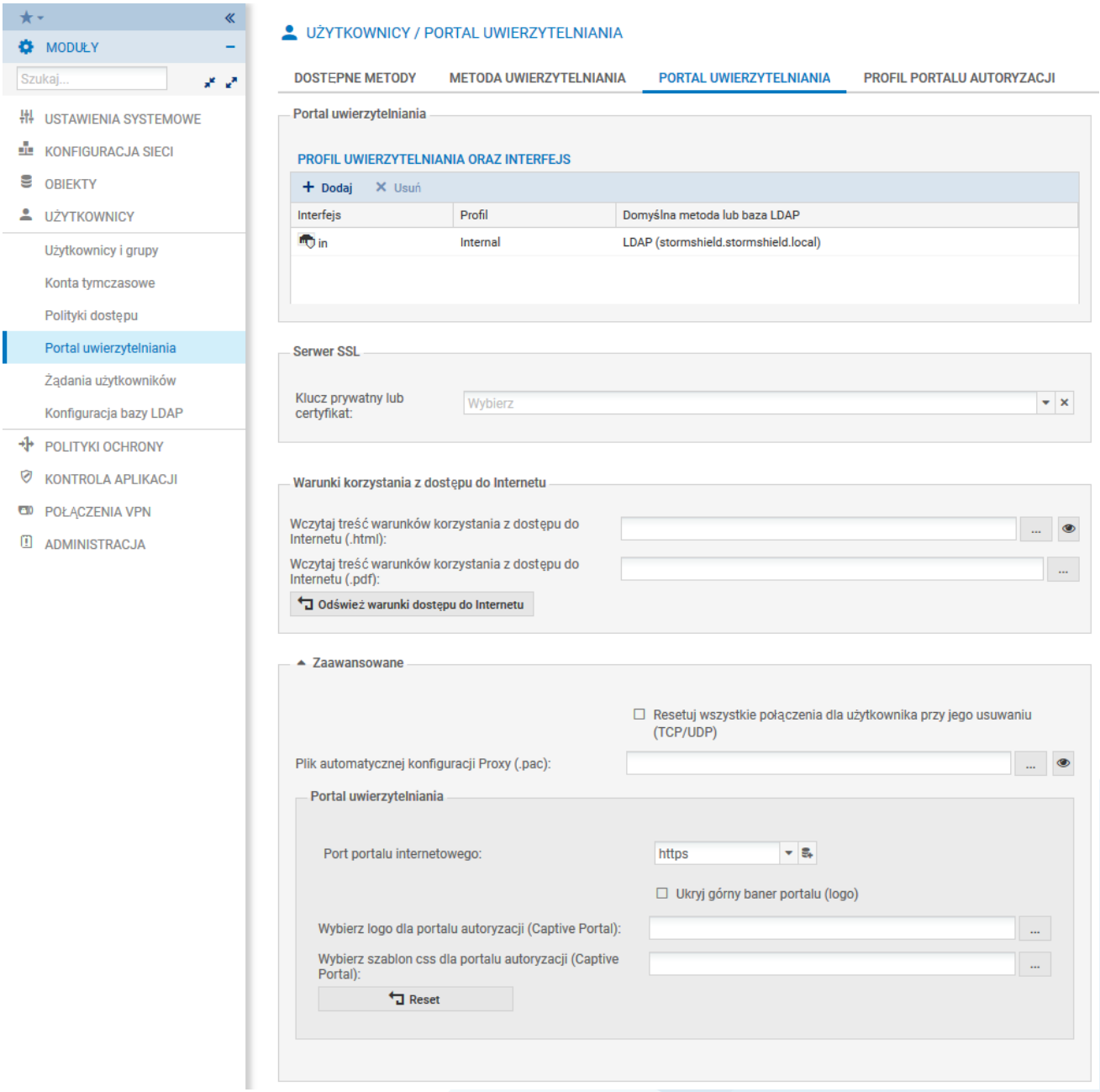


Mechanizm Portalu uwierzytelniania wykorzystywany jest zarówno do autoryzacji użytkowników LAN (np. polityki filtrowania ruchu na podstawie nazwy użytkownika lub grupy) jak i WAN (np. SSL VPN). Konfiguracja Portalu uwierzytelniania odbywa się w sekcji **KONFIGURACJA > UŻYTKOWNICY > Portal uwierzytelniania**.

Konfiguracja portalu podzielona jest na dwa etapy:

- **Portal uwierzytelniania** – ogólna konfiguracja portalu wraz z profilami przypisanymi do poszczególnych interfejsów urządzenia.
- **Profil portalu autoryzacji** – szczegółowa konfiguracja poszczególnych profili portalu.

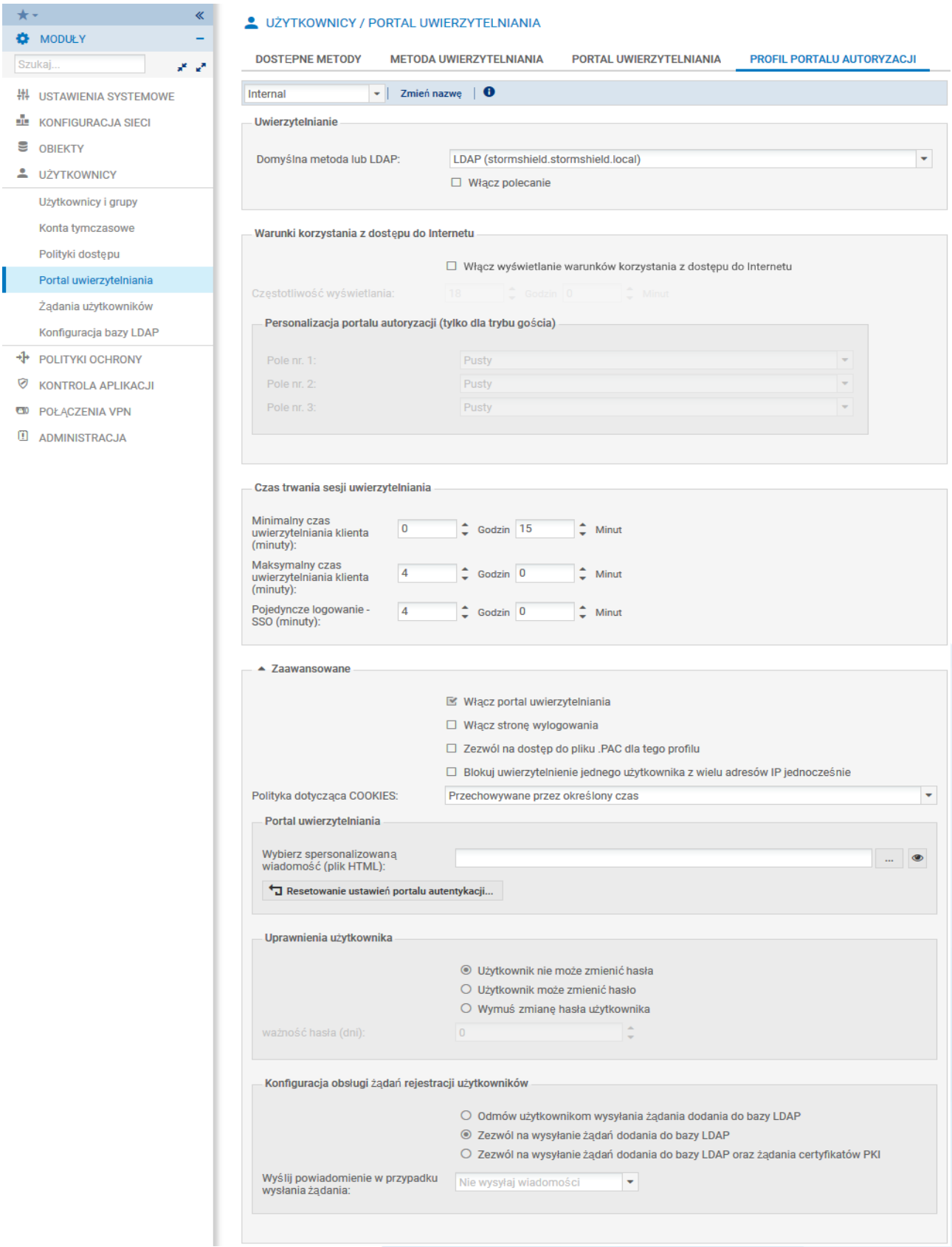
Poniższe okno zawiera ogólną konfigurację portalu i obejmuje następujące funkcje:



- **Profil uwierzytelniania oraz interfejs** – tabela zawierająca powiązania profili Portalu uwierzytelniania z interfejsami urządzenia, znajdują się tu trzy kolumny:
  - **Interfejs** – interfejs urządzenia, do którego ma być przypisany profil,
  - **Profil** – profil portalu uwierzytelniania. Konfiguracja profili znajduje się z zakładce *Profil portalu autoryzacji,*
  - **Domyślna metoda lub baza LDAP** – domyślna metoda lub baza LDAP wskazana w wybranym profilu uwierzytelniania (tylko podgląd);

- **Klucz prywatny lub certyfikat** – pozwala na wybór certyfikatu jaki będzie użyty do podpisania portalu autoryzacji. Certyfikat musi być wcześniej utworzony lub zaimportowany na urządzenie poprzez sekcję **KONFIGURACJA > OBIEKTY > Certyfikaty – PKI**;
- **Wczytaj treść warunków korzystania dostępu do Internetu (.html) / (.pdf)** – możliwość wprowadzenia regulaminu dostępu do Internetu, który będzie wyświetlony użytkownikom na Portalu uwierzytelniania. Użytkownik będzie musiał zatwierdzić regulamin zanim zostanie zautoryzowany;
- **Resetuj wszystkie połączenia dla użytkownika przy jego usuwaniu (TCP/UDP)** – po zaznaczeniu tej opcji w momencie kiedy upłynie czas autentykacji użytkownika wszystkie jego połączenia zostaną przerwane;
- **Plik automatycznej konfiguracji Proxy (.pac)** – pole umożliwia wczytanie pliku zawierającego automatyczną konfigurację proxy (Proxy Auto-Config);
- **Port portalu internetowego** – nr portu na którym działa portal uwierzytelniania, domyślnie 443 (obiekt https);
- **Ukryj górny baner portalu (logo)** – włączenie tej opcji ukrywa (ze względów bezpieczeństwa) logo „Stormshield Network Security" znajdujące się w górnym banerze portalu;
- **Wybierz logo dla portalu autoryzacji** – możliwość personalizacji Portalu uwierzytelniania poprzez wczytanie nagłówka (logo) portalu, obrazek 800x50px;
- **Wybierz szablon CSS dla portalu autoryzacji** – import własnego arkusza styli CSS, który zmodyfikuje oryginalny wygląd Portalu uwierzytelniania;
- **Reset** – przywrócenie oryginalnego wyglądu Portalu uwierzytelniana (reset logo i styli CSS).

Zakładka *PROFIL PORTALU AUTORYZACJI* umożliwia konfigurację poszczególnych profili Portalu uwierzytelniana. Dostępnych jest 10 profili w tym 5 wstępnie skonfigurowanych.

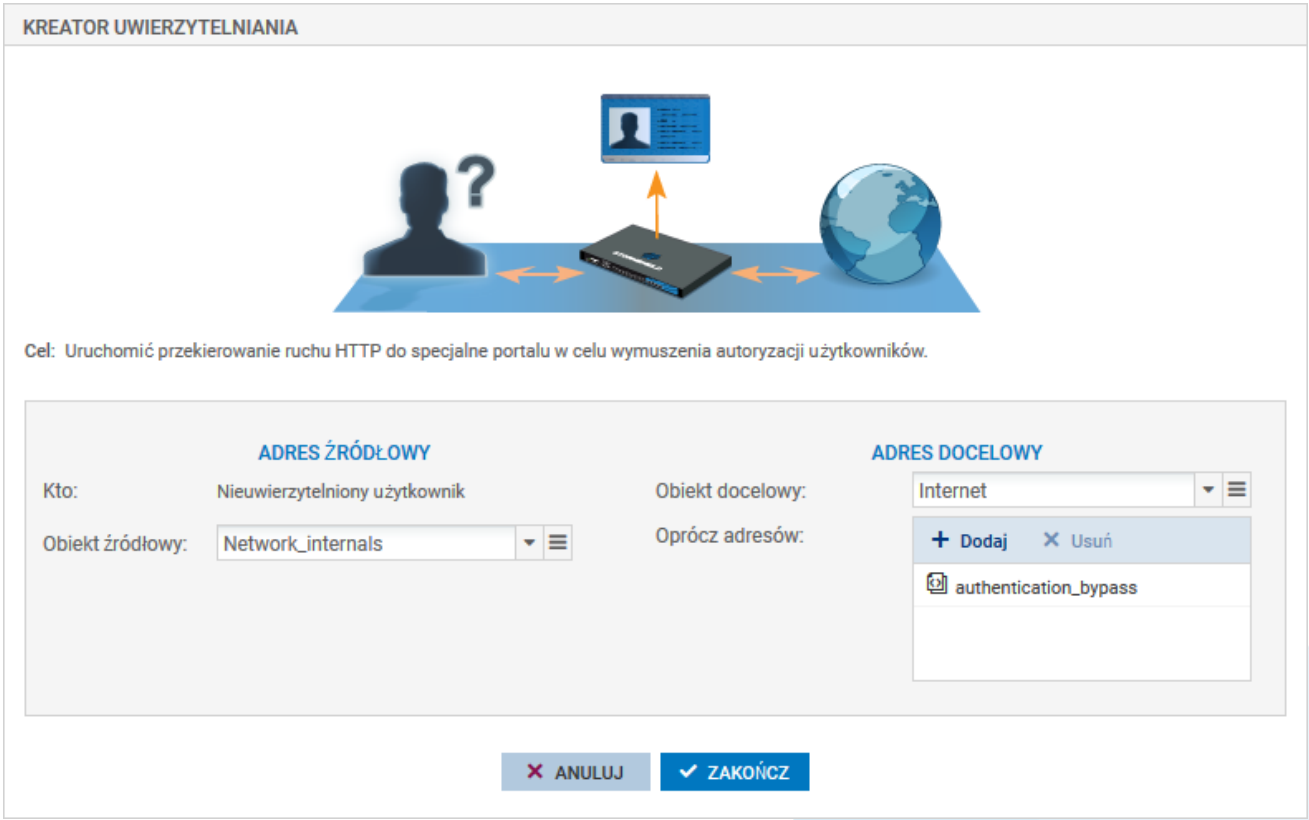


- **Zmień nazwę** – możliwość zmiany nazwy wybranego profilu;
- **Domyślna metoda lub LDAP** – wskazanie domyślnej metody autoryzacji lub bazy LDAP (w przypadku jeśli na urządzeniu jest skonfigurowanych kilka baz LDAP);
- **Włącz polecanie** – możliwość włączenia metody Uwierzytelnianie przez polecającego (Sponsor). Ta opcja jest domyślnie włączona jeśli jako domyślna metoda wskazana jest metoda Sponsor.
- **Włącz wyświetlanie warunków korzystania z dostępu do Internetu** – włączenie wyświetlania regulaminu dostępu do Internetu. Regulamin ten będzie wyświetlony użytkownikowi na Portalu uwierzytelniania podczas autentykacji i będzie musiał zostać zatwierdzony zanim użytkownik zostanie zautoryzowany. Treść regulaminu można wczytać w ogólnej konfiguracji Portalu uwierzytelniania.
- **Częstotliwość wyświetlania** – jak często zautoryzowanym użytkownikom będzie wyświetlany regulamin dostępu do Internetu;
- **Personalizacja portalu autoryzacji** – opcja dotyczy jedynie metody dostępu typu Gość i umożliwia dodanie do trzech pól formularza do strony portalu uwierzytelniania wyświetlającej regulamin dostępu do Internetu. Dostępne typy pól to: Pusty (pole nie będzie wyświetlane), Imię, Nazwisko, Telefon, E-Mail, Informacja, Firma;
- **Czas trwania sesji uwierzytelniania** – maksymalny czas trwania pojedynczej sesji logowania. Na czas trwania sesji konto użytkownika jest „wiązane" z adresem IP, z którego użytkownik się zalogował. Określenie czasu minimalnego i maksymalnego sesji spowoduje, że użytkownik będzie mógł sam wybrać czas trwania sesji;
- **Włącz portal uwierzytelniania** – włącza autentykację z wykorzystaniem danego profilu autoryzacji;
- **Włącz stronę wylogowania** – włączenie tej opcji spowoduje pojawienie się odrębnej strony umożliwiającej zautoryzowanemu użytkownikowi wylogowanie się z portalu;
- **Zezwól na dostęp do pliku .PAC dla tego profilu** – zezwala na dostęp do pliku .pac (Proxy Auto-Config) użytkownikom logującym się na podstawie danego profilu autoryzacji;
- **Blokuj uwierzytelnienie jednego użytkownika z wielu adresów IP jednocześnie** – funkcja uniemożliwia zalogowanie jednego użytkownika na wielu komputerach, użycie tej opcji eliminuje „pożyczanie kont" pomiędzy użytkownikami;
- **Polityka dotycząca COOKIES** – wykorzystanie mechanizmu cookies w procesie uwierzytelniania użytkownika pozwala na wprowadzenie dodatkowego poziomu zabezpieczeń. Po pomyślnym zautoryzowaniu użytkownika Portal uwierzytelniania tworzy w przeglądarce specjalny określony odpowiednim czasem życia plik *connection cookie*. Usunięcie tego pliku bądź jego wygaśnięcie spowoduje unieważnienie autoryzacji użytkownika. Mechanizm ten można jednak wyłączyć;
- **Wybierz spersonalizowaną wiadomość (plik HTML)** – umożliwia dodanie wiadomości zawierającej tekst i obrazy umieszczonej pod tytułem portalu uwierzytelniania. Wiadomość musi być w formacie HTML;
- **Resetowanie ustawień portalu autentykacji** … – usunięcie wiadomości spersonalizowanej;
- **Uprawnienia użytkownika** – uprawnienia użytkownika do zarządzania własnym hasłem;
- **Konfiguracja obsługi żądań rejestracji użytkowników** – konfiguracja funkcji, która umożliwia użytkownikom wysyłanie żądań założenia konta oraz utworzenia/pobrania certyfikatów. Użytkownik

wypełnia pola właściwości konta swoimi danymi, a rola administratora ogranicza się do weryfikacji tych danych i ewentualnej akceptacji utworzenia konta.

Powyższa metoda autoryzacji wymaga aby użytkownik wszedł na stronę portalu i podał swój login oraz hasło. Istnieje jednak metoda wymuszania na przeglądarce otwarcia strony autoryzacji podczas próby wejścia na strony WWW przez niezautoryzowanego użytkownika.

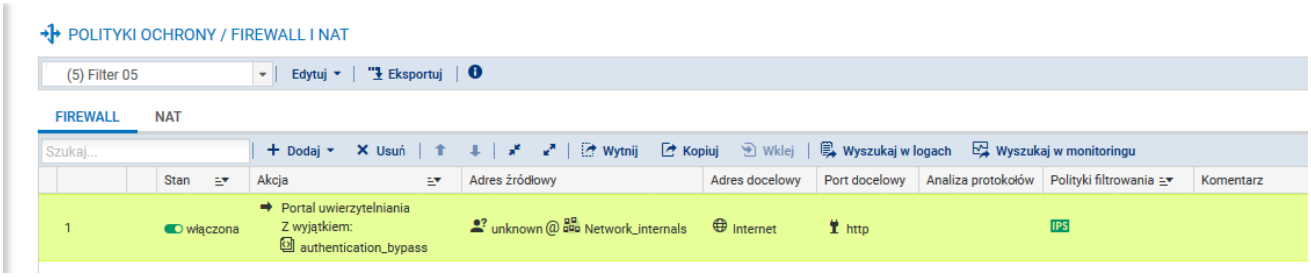
Należy w tym celu uruchomić **Kreator reguły uwierzytelniania** z menu **KONFIGURACJA > POLITYKI OCHRONY > Firewall i NAT > Dodaj,** następnie wypełniamy kreator.



Do zdefiniowania mamy:

- **Obiekt źródłowy –** adres hosta, zakres hostów, całe podsieci, które mają być uwzględniane w trakcie autoryzacji;
- **Obiekt docelowy** – przeznaczenie ruchu sieciowego pochodzącego z obiektu źródłowego (najczęściej Internet);
- **Oprócz adresów** – grupy URL stron, które będą dostępne bez konieczności autoryzacji (np. serwery aktualizacyjne systemów operacyjnych, antywirusowych itp.).

Po zakończeniu kreatora otrzymujemy regułę:



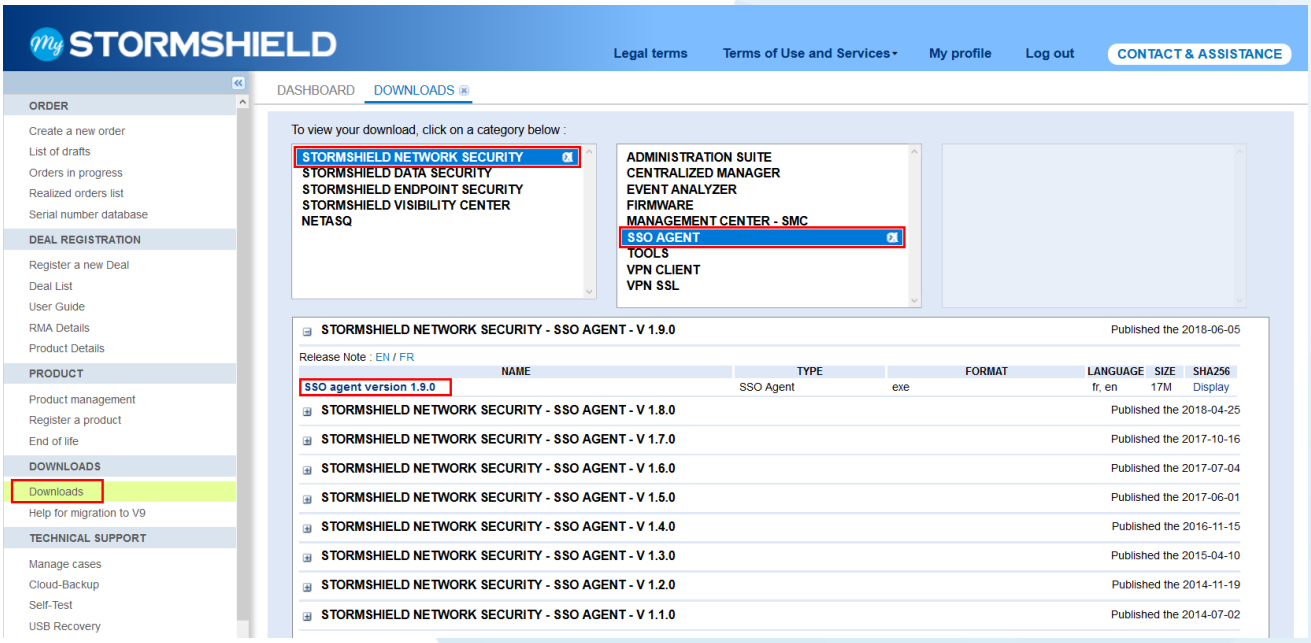
Jak powyżej widać każde połączenie zainicjowane przez nieznanego użytkownika z sieci chronionej, do sieci Internet, które zostanie nawiązane na porcie http STORMSHIELD UTM przekaże do Portalu uwierzytelniania. W przypadku chęci przekierowania ruchu **https** na Portal uwierzytelniania należy odpowiednio zmodyfikować powyższą regułę dodając w porcie docelowym również port https.
Jednak, aby takie przekierowanie działało należy wcześniej zdeszyfrować ruch https, czyli uruchomić moduł SSL Proxy.

Transparentne uwierzytelnianie SSO

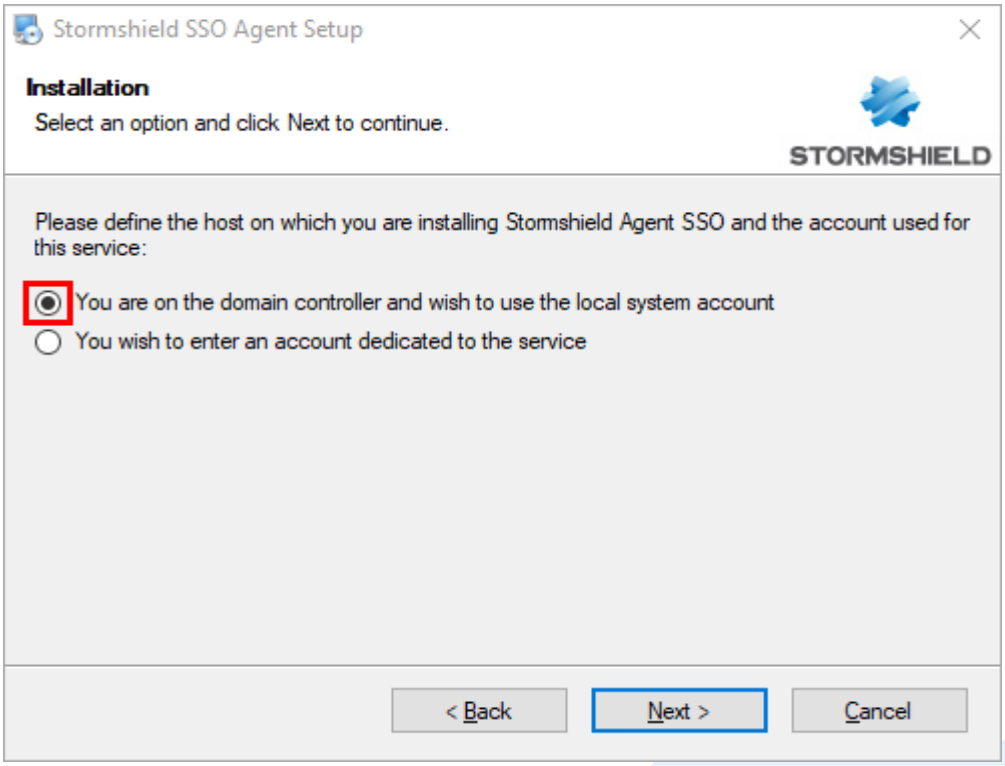
W przypadku korzystania z usługi katalogowej Active Directory istnieje możliwość pominięcia autoryzacji z użyciem Portalu uwierzytelniania na rzecz transparentnego uwierzytelniania SSO (Single Sign-On).

W tym celu należy zainstalować oprogramowanie **Stormshield SSO Agent** na kontrolerze domeny (bądź innym, stale uruchomionym hoście znajdującym się w tej domenie) oraz skonfigurować odpowiednią metodę autoryzacji na urządzeniu STORMSHIELD UTM.

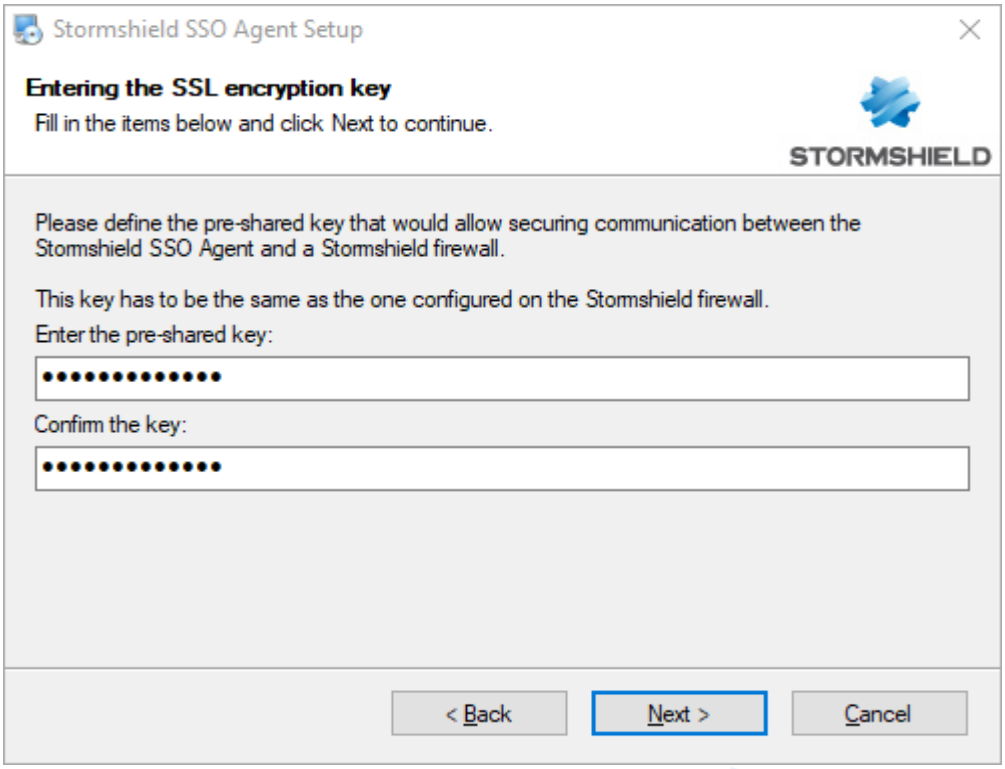
Najnowszą dostępną wersję **Agenta SSO** można pobrać ze strefy klienta (https://mystormshield.eu) w sekcji **Download**:



Podczas instalacji oprogramowania należy wybrać odpowiednią opcję w zależności od tego gdzie je instalujemy. Jeżeli instalacja odbywa się bezpośrednio na kontrolerze domeny to należy wybrać pierwszą opcję:

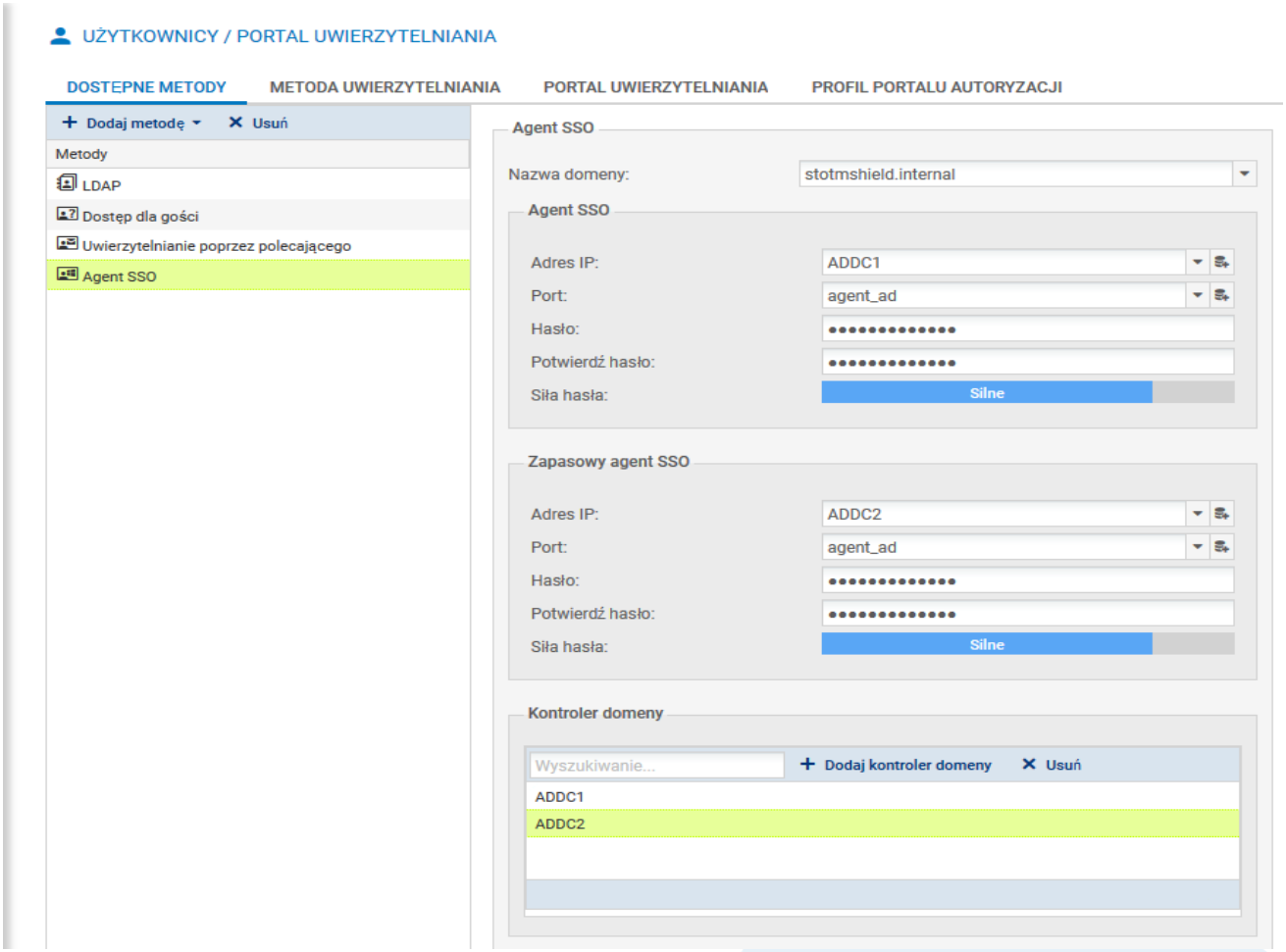


Następnie należy podać hasło współdzielone, które później trzeba będzie podać także po stronie konfiguracji urządzenia STORMSHIELD UTM:

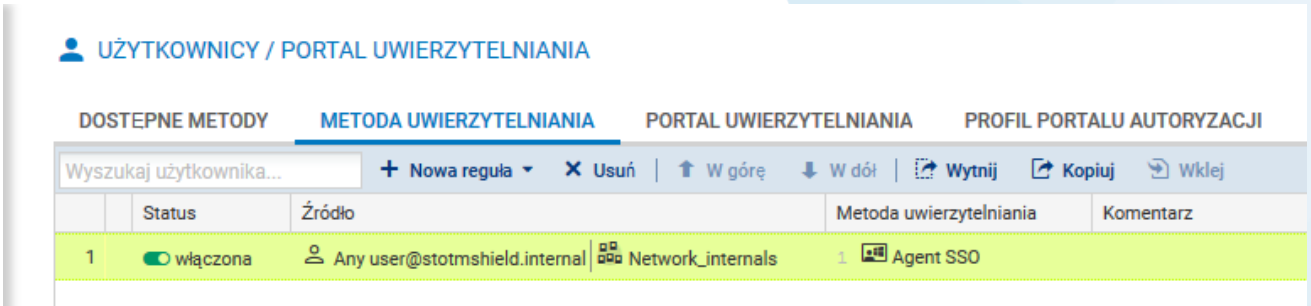


W ostatnim kroku należy zalogować się do urządzenia i przejść do menu KONFIGURACJA > UŻYTKOWNICY > Portal uwierzytelniania, a następnie w zakładce Dostępne metody dodać nową metodę autoryzacji o nazwie Agent SSO.

Po dodaniu nowej metody we właściwościach należy wskazać domenę, której dotyczy połączenie z agentem SSO, adres IP hosta, na którym jest zainstalowany agent SSO (w naszym przypadku są to kontrolery domeny: ADDC1 i ADDC2), następnie podać hasło współdzielone, które zostało zdefiniowane podczas instalacji agenta.



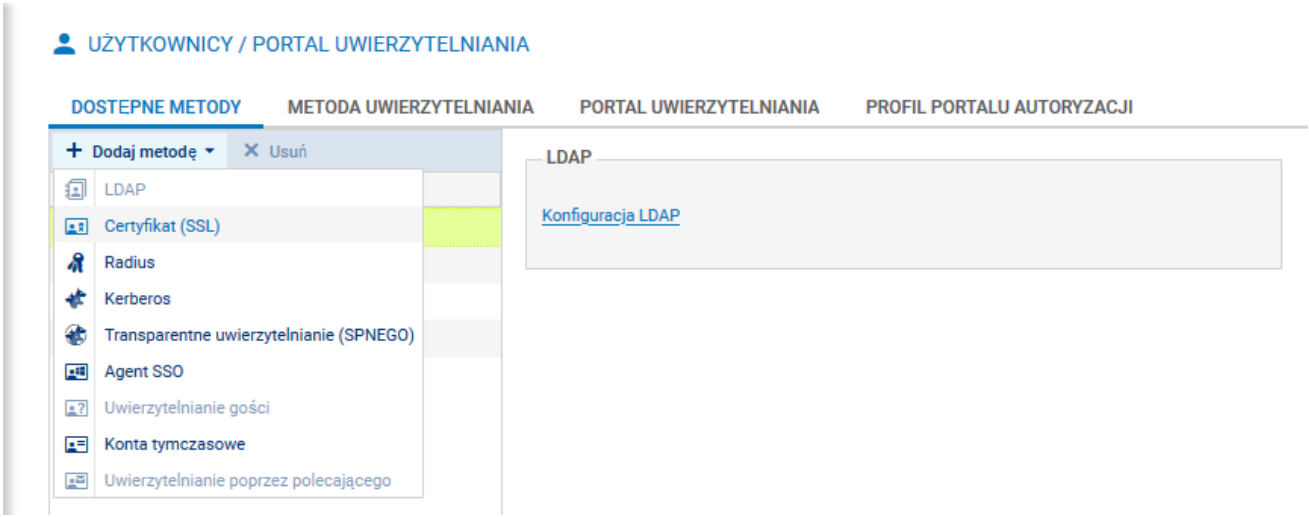
Po skonfigurowaniu metody autoryzacji *Agent SSO* pozostaje aktywować tę metodę w zakładce **Metody Uwierzytelniania**:



Na koniec należy zastosować wprowadzone zmiany i od tego momentu można tworzyć reguły filtrowania z uwzględnieniem zalogowanych użytkowników.

Inne metody autoryzacji

Poza powyższym sposobem autoryzacji użytkowników istnieje również kilka innych metod autoryzacji. Poniżej zostały opisane pozostałe metody autoryzacji w urządzeniu STORMSHIELD UTM:

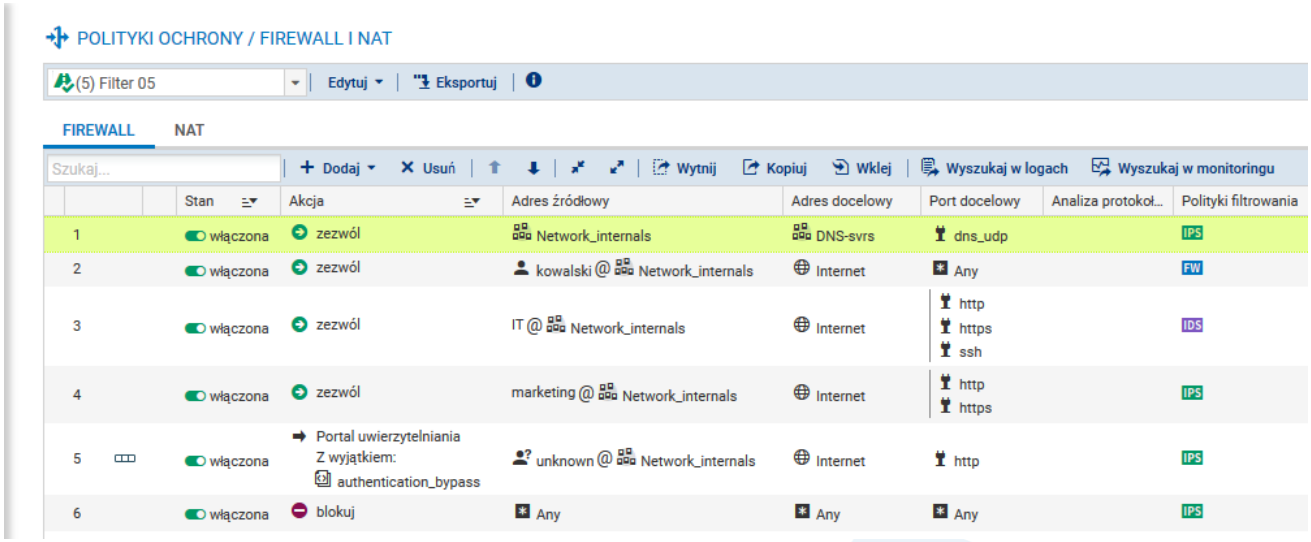


- LDAP – standardowa metoda uwierzytelniania w oparciu o login oraz hasło podane przez użytkownika (metoda domyślna);
- Certyfikat (SSL) – umożliwia automatyczne uwierzytelnienie użytkownika na urządzeniu za pośrednictwem certyfikatu zaimportowanego wcześniej do jego przeglądarki. Sama autoryzacja jest automatyczna i odbywa się „w tle" podczas otwierania dowolnej strony WWW;
- Radius – umożliwia automatyczne uwierzytelnienie użytkownika za pośrednictwem zewnętrznego serwera RADIUS;
- Kerberos – umożliwia uwierzytelnienie użytkownika za pośrednictwem zewnętrznego serwera KERBEROS;
- Transparentne uwierzytelnianie (SPNEGO) – umożliwia transparentne uwierzytelnienie użytkowników w AD za pośrednictwem przeglądarki internetowej. Metoda ta wymaga wysłania zapytania HTTP/GET, a więc autoryzacja nie działa od razu po zalogowaniu się do domeny. Jest to metoda obecnie wyparta przez Agenta SSO;
- Agent SSO – metoda typu Single Sign-On, pozwala na automatyczną autoryzację wymagająca od użytkownika jedynie zalogowania się do domeny Active Directory. Wymaga ona głębszej integracji ze środowiskiem (instalacja specjalnego agenta w domenie), jednak daje największą wygodę oraz prostotę korzystania przez co jest zalecaną metodą autoryzacji;
- Uwierzytelnianie gości – jest to metoda umożliwiająca „uwierzytelnianie" użytkowników bez konieczności podawania poświadczeń. Podczas logowania użytkownikowi wyświetli się regulamin korzystania z dostępu do sieci i jedynie jego zaakceptowanie umożliwi dostęp. Metoda ta jest przydatna w przypadku publicznych sieci Wi-Fi. Warto zwrócić tutaj uwagę na to, że po pomyślnym uwierzytelnieniu logowany jest adres MAC hosta użytego przy połączeniu;
- Konta tymczasowe – ten typ uwierzytelnienia umożliwia zarządzanie kontami o ograniczonym okresie ważności. Konta te mają na celu zapewnienie tymczasowego dostępu np. do Internetu osobom spoza organizacji. Kontami tymczasowymi można zarządzać w KONFIGURACJA > UŻYTKOWNICY > Konta tymczasowe. Konta tymczasowe nie są zapisywane w lokalnej bazie LDAP;
- Uwierzytelnianie przez polecającego – umożliwia identyfikację użytkownika bez konieczności uwierzytelnienia się w Portalu uwierzytelniania. Użytkownik chcąc zostać zautoryzowanym będzie musiał wpisać swoje imię i nazwisko oraz adres e-mail „Sponsora". Sponsor (uprawniony użytkownik

naszej organizacji) otrzyma wówczas wiadomość e-mail zawierającą link potwierdzający taką prośbę. Po zatwierdzeniu żądania strona sponsorowana zostanie automatycznie przekierowana z Portalu dostępowego na żądaną stronę internetową.

Tworzenie reguł filtrowania w oparciu o zalogowanego użytkownika

Poniższy zrzut ekranu obrazuje przykładowe reguły zapory stworzone dla zalogowanych użytkowników.

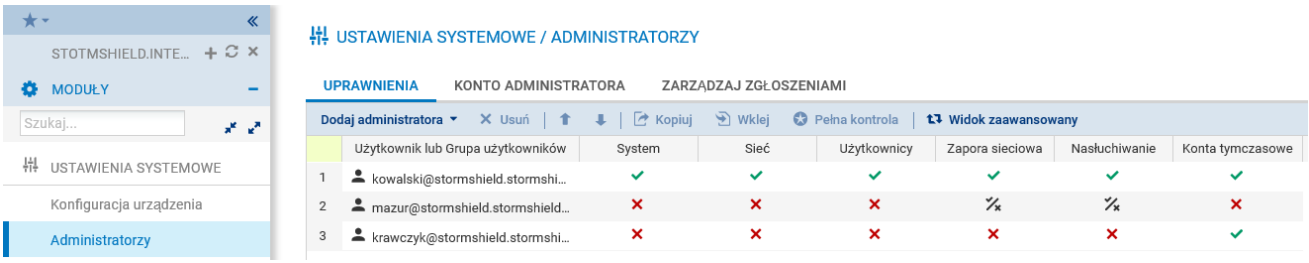


Reguły te odpowiadają kolejno za:

1. Zezwolenie na dostęp dowolnych hostów ze wszystkich sieci chronionych do wskazanych w obiekcie DNS-svrs serwerów dns na porcie 53/UDP.
2. Zezwolenie na dostęp do wszystkich usług w Internecie dla użytkownika kowalski łączącego się z sieci chronionych z wyłączeniem analizy IPS.
3. Zezwolenie użytkownikom należącym do grupy IT łączącym się z sieci chronionych na połączenia realizowane do sieci Internet w ramach portów http, https, ssh z analizą IDS.
4. Zezwolenie użytkownikom należącym do grupy marketing łączącym się z sieci chronionych na połączenia realizowane do sieci Internet w ramach portów http, https.
5. Przekierowanie na Portal uwierzytelniania wszystkich użytkowników nieuwierzytelnionych próbujących wykonać połączenia do sieci Internet na porcie http z sieci chronionych (z wykluczeniem stron zdefiniowanych w obiekcie authentication_bypass).
6. Zablokowanie wszystkich innych połączeń.

Delegowanie zadań administracyjnych użytkownikom bazy LDAP

Konfiguracja delegacji uprawnień odbywa się w sekcji **KONFIGURACJA > USTAWIENIA SYSTEMOWE > Administratorzy**. Konfiguracja pozwala na określenie zakresu dostępu do zarządzania urządzeniem przez poszczególnych użytkowników. Uprawnienia mogą być **pełne** lub **tylko do odczytu** i obejmują wszystkie podstawowe funkcje urządzenia takie jak **Firewall i NAT**, **VPN**, **konfigurację logów**, **IPS**, **filtry treści**, **konfigurację sieci,** itp.



13. Wirtualne sieci prywatne (VPN)

VPN to technologia tworzenia bezpiecznych tuneli komunikacyjnych, w ramach których możliwy jest bezpieczny dostęp do zasobów firmowych. Ze względu na sposób połączenia VPN dzielimy na:

- Site-to-Site – gdzie tunel ustanawiany jest pomiędzy dwoma urządzeniami, co pozwala na bezpieczne połączenie sieci chronionych przez te urządzenia.
- Client-to-Site – umożliwia bezpośrednie połączenie komputera z siecią firmową. Ten typ tunelu wykorzystywany jest przede wszystkim przez użytkowników pracujących mobilnie.
- Client-to-Site (portal) – umożliwia połączenie do usługi wewnątrz sieci firmowej z wykorzystaniem przeglądarki internetowej. Ten typ tunelu wykorzystywany jest przede wszystkim przez użytkowników pracujących mobilnie potrzebujących uzyskać szybki dostęp do konkretnej usługi bez konieczności instalacji/konfiguracji oprogramowania dedykowanego do nawiązywania połączeń VPN.

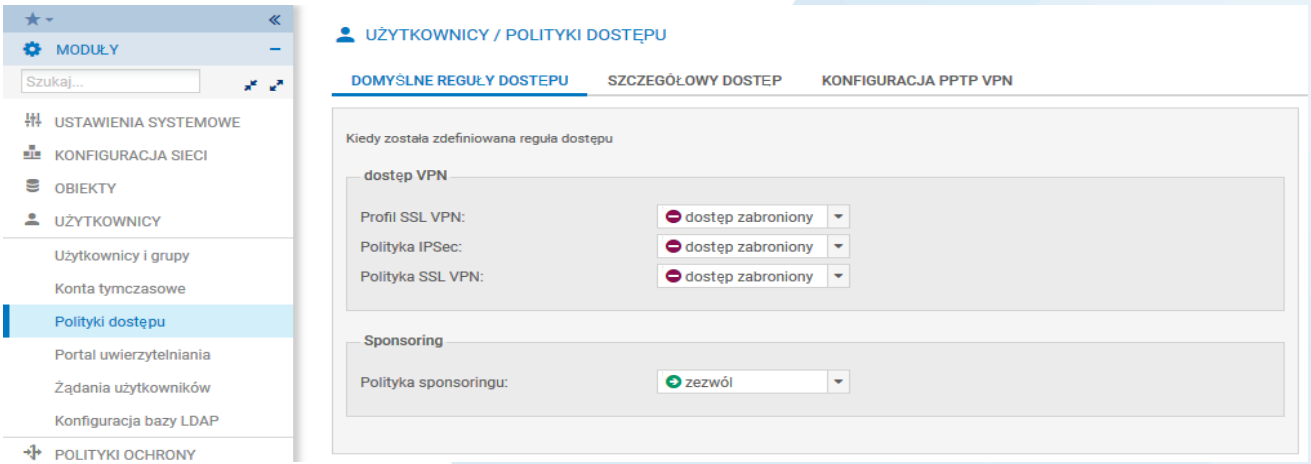
W przypadku urządzeń STORMSHIELD UTM dostępne są cztery możliwości tworzenia kanałów VPN:

- Protokół IPsec VPN – w trybie Client-to-Site oraz Site-to-Site;
- Protokół SSL VPN – w trybie Client-to-Site;
- Portal SSL VPN – w trybie Client-to-Site (portal);
- Protokół PPTP VPN – w trybie Client-to-Site.

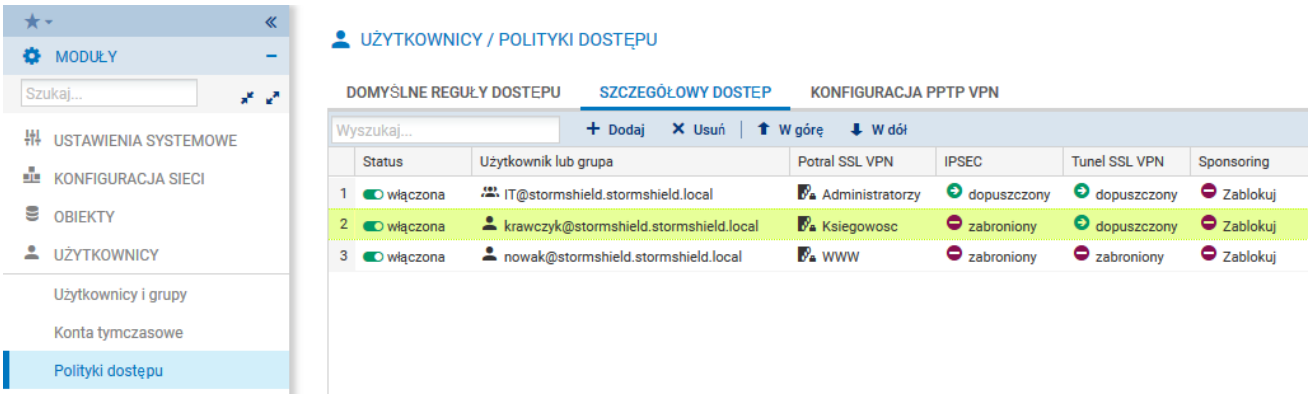
Zastosowanie wybranego protokołu VPN powinno być podyktowane przede wszystkim względami bezpieczeństwa oraz funkcjonalnością wybranego typu połączenia.

Konfiguracja uprawnień użytkowników

W przypadku połączeń Client-to-Site przed przystąpieniem do konfiguracji wybranego typu tunelu najpierw należy skonfigurować uprawnienia użytkowników.
Mając skonfigurowaną już na urządzeniu STORMSHIELD UTM bazę użytkowników (wewnętrzną bądź zewnętrzną) można przystąpić do konfiguracji reguł dostępu. Dokonuje się tego w sekcji KONFIGURACJA > UŻYTKOWNICY > Polityki dostępu. W zakładce Domyślne reguły dostępu można wskazać domyślne ustawienia dla poszczególnych typów połączeń VPN, które będą zastosowane dla wszystkich użytkowników za wyjątkiem tych, dla których określono inne ustawienia na zakładce Szczegółowy dostęp.



Jeśli użytkownik ma mieć inny niż domyślny poziom dostępu taką konfigurację przeprowadza się na zakładce **Szczegółowy dostęp**.



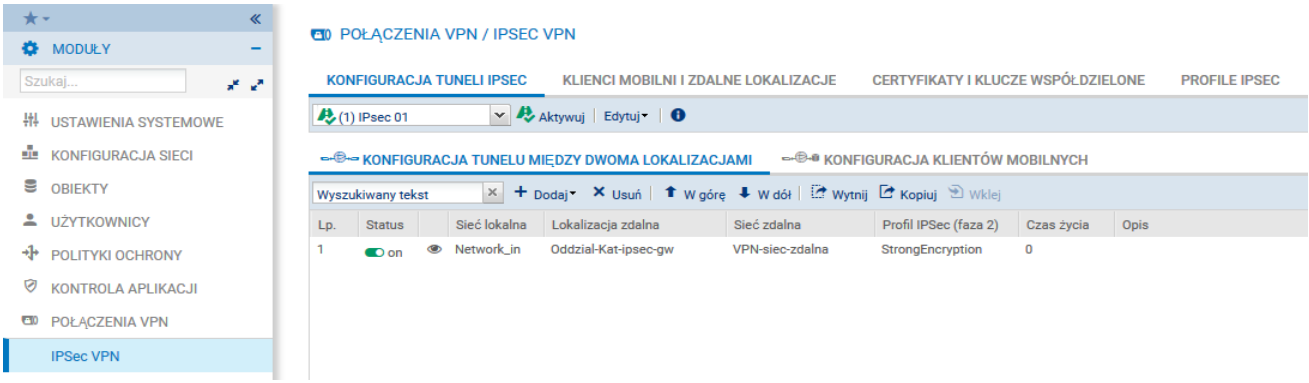
W zależności od wybranego typu tunelu VPN interesują nas następujące opcje:

- **Protokół IPsec VPN** – w *Domyślnych regułach dostępu* **Polityka IPsec**, a w *Szczegółowym dostępie* kolumna **IPSEC**;
- **Protokół SSL VPN** – odpowiednio **Polityka SSL VPN** oraz kolumna **Tunel SSL VPN**;
- **Portal SSL VPN** – tutaj będzie to **Profil SSL VPN** oraz kolumna **Portal SSL VPN**;
- **Protokół PPTP VPN** – ten typ tunelu posiada odrębną konfigurację na zakładce **Konfiguracja PPTP VPN**.

W przypadku Portal SSL VPN na zakładce *Szczegółowy dostęp* można wskazać konkretny profil połączeń SSL VPN w trybie portal tak, aby dany użytkownik po połączeniu miał dostęp tylko do określonych usług. Opis konfiguracji profili Portalu SSL VPN znajduje się w dalszej części dokumentu.

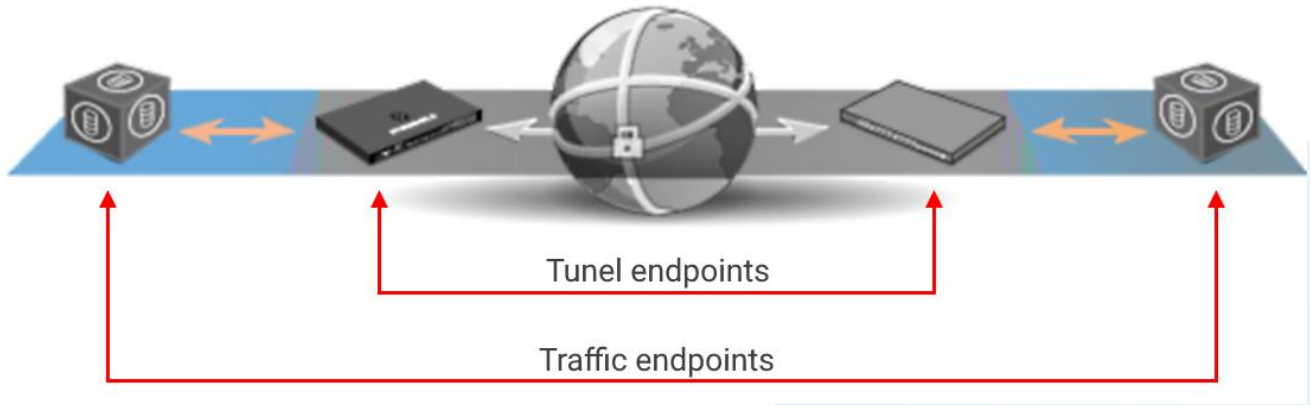
IPsec VPN

Protokół IPsec jest najbezpieczniejszym i najwszechstronniejszym protokołem VPN jaki można skonfigurować na urządzeniu STORMSHIELD UTM. Pozwala na budowanie tuneli **Client-to-Site** jak i **Site-to-Site**, a jego użycie pozwala uzyskać pełen dostęp do zasobów w sieci.
Implementacja IPsec VPN w urządzeniach STORMSHIELD UTM jest w pełni zgodna ze standardem IPsec (zarówno w wersji IKEv1 jak i IKEv2), dzięki czemu możliwe jest zestawienie tunelu VPN z dowolnymi urządzeniami bądź aplikacjami klienckimi, które również wykorzystują zgodną z RFC implementację tego protokołu.
Konfiguracja IPsec odbywa się w sekcji **KONFIGURACJA > POŁĄCZENIA VPN > IPsec VPN**. Widok okna konfiguracyjnego przedstawiono poniżej:



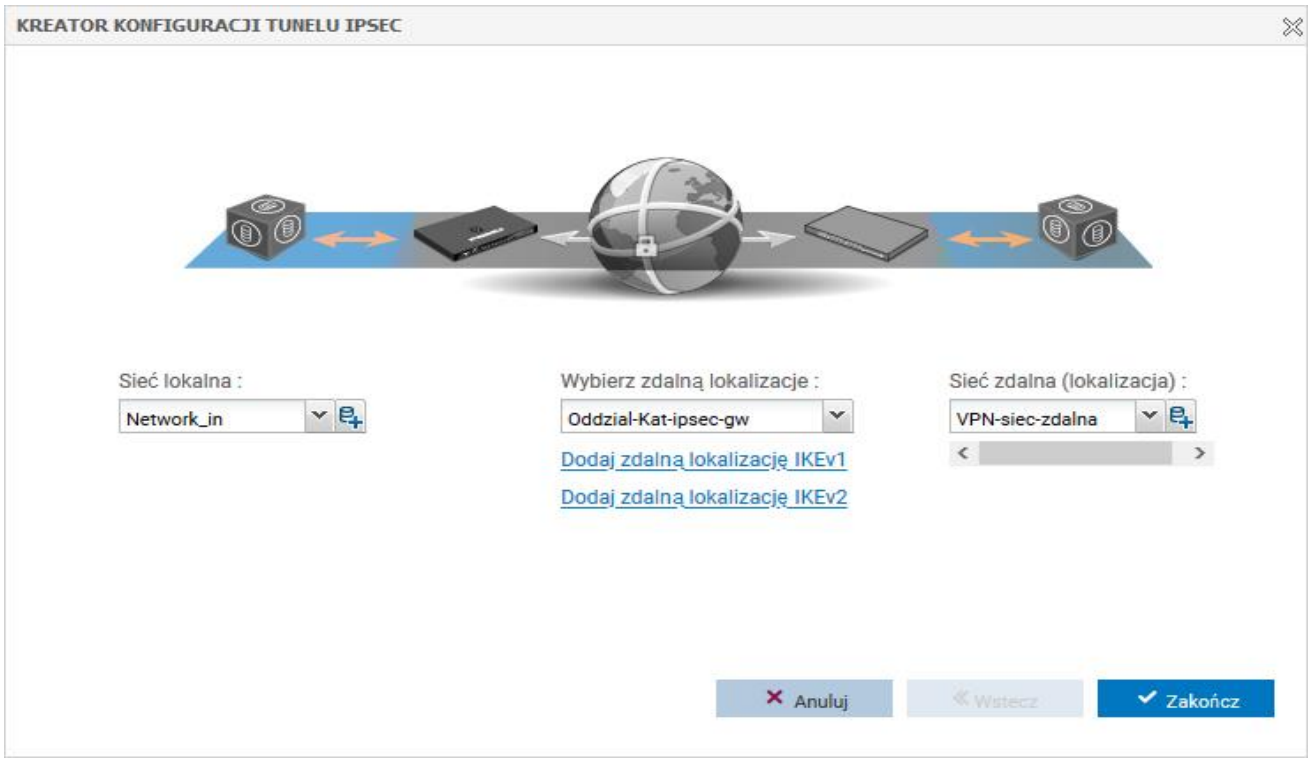
Ponieważ konfiguracja IPsec uważana jest za bardzo skomplikowaną STORMSHIELD przygotował ułatwienia w postaci kreatorów, dzięki którym konfiguracja VPN jest łatwa, szybka i intuicyjna.
Tunele IPsec składają się z dwóch faz. Po wybraniu opcji *Dodaj* i wybraniu interesującej nas opcji, uruchomi się kreator, który pomoże skonfigurować zarówno pierwszą jak i drugą fazę tunelu IPsec.

W obu fazach poza algorytmami szyfrowania definiuje się tzw. **Tunel endpoints** oraz **Traffic endpoints**. **Tunel endpoints** to dwa adresy reprezentujące publiczne adresy IP urządzeń, pomiędzy którymi zestawiany jest tunel. Z kolei **Traffic endpoints** określają sieci wewnętrzne jakie będą brały udział w komunikacji.
Poniższy rysunek przedstawia czym są Tunel endpoints, a czym Traffic endpoints:

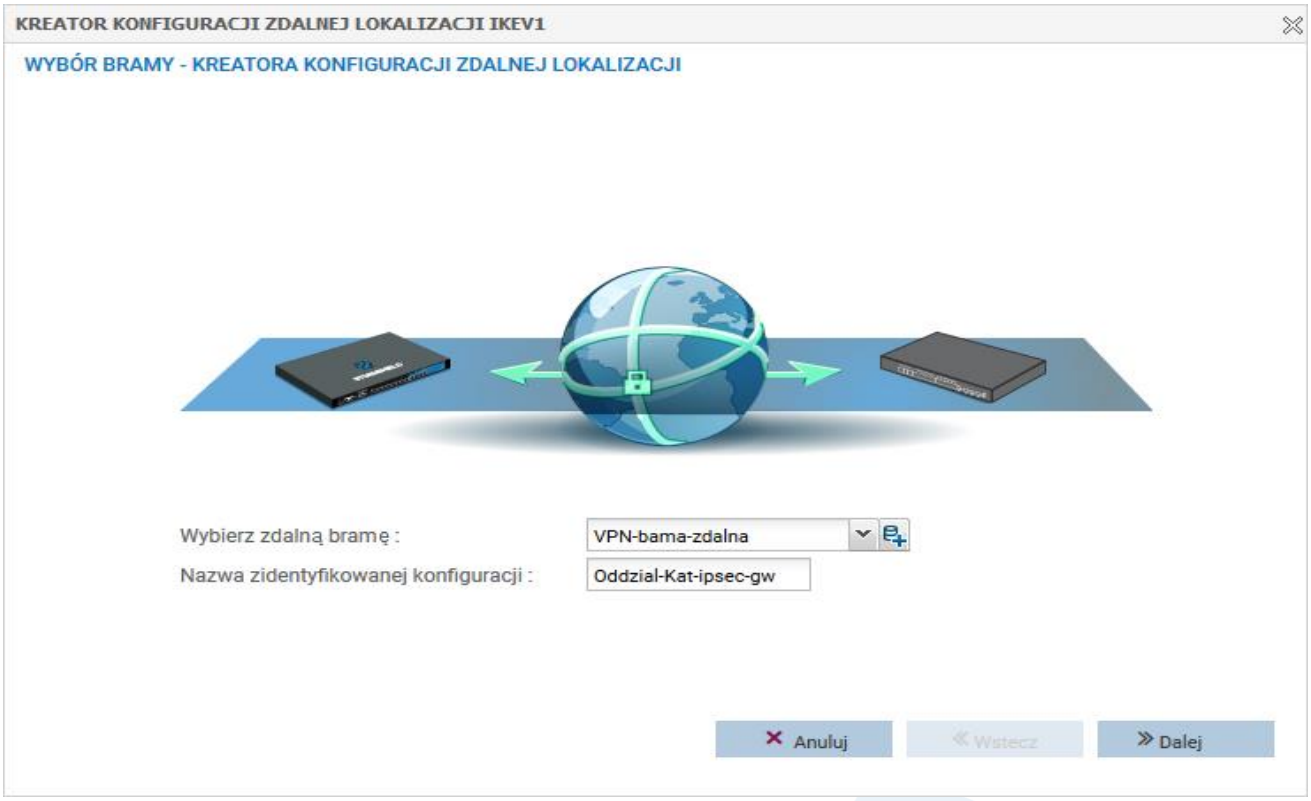


Konfiguracja połączenia typu Site-to-Site

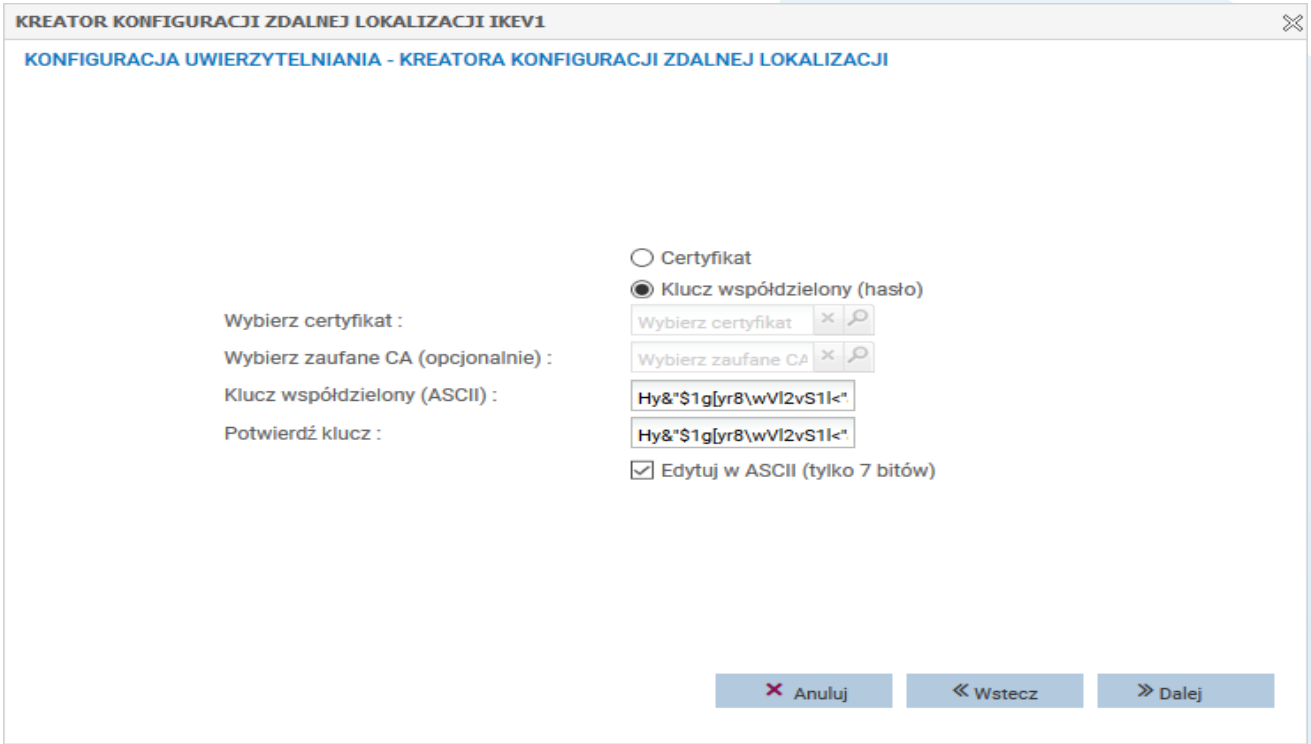
Kreator konfiguracji tunelu IPsec umożliwia stworzenie w szybki i prosty sposób tunelu IPsec. Wystarczy jedynie zdefiniować dwie sieci prywatne biorące udział w komunikacji oraz bramę zdalną, z którą będziemy się komunikować.



Po wskazaniu sieci lokalnej oraz zdalnej (jeśli wcześniej nie została zdefiniowana na urządzeniu STORMSHIELD UTM, można ją dodać z tego poziomu poprzez kliknięcie na ikonie 14) należy wskazać zdalną lokalizację. Jeśli zdalna lokalizacja nie została jeszcze skonfigurowana wybieramy opcję **Dodaj zdalną lokalizację IKEv1** bądź **Dodaj zdalną lokalizację IKEv2** w zależności od użytej wersji protokołu IKE. Spowoduje to otwarcie kreatora zdalnej lokalizacji.

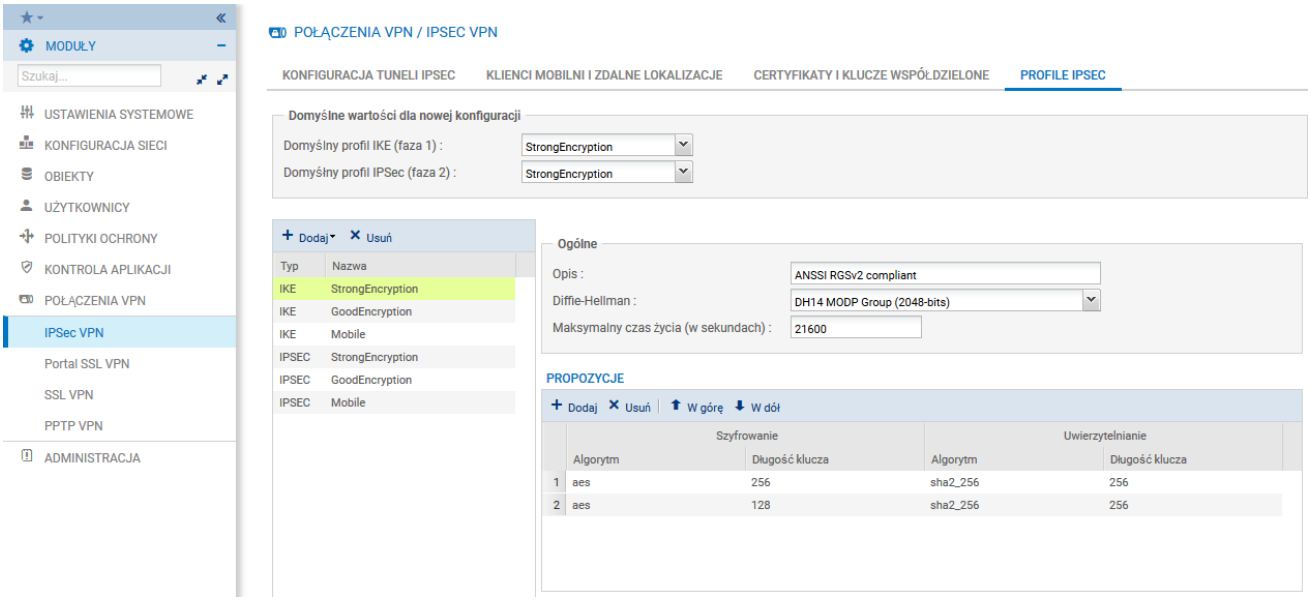


Kreator ten pozwala skonfigurować **Tunel endpoints** oraz hasło/certyfikat zabezpieczające komunikację.



Po zakończeniu pracy obu kreatorów należy jeszcze skonfigurować **Profile IPsec** oraz aktywować profil.

Profile IPsec określają jakie algorytmy i klucze mają być użyte do zabezpieczenia tunelu. Można skorzystać z profili domyślnych lub stworzyć własne, zgodne z wymaganiami polityki bezpieczeństwa. Okno konfiguracyjne profili zostało przedstawione poniżej:



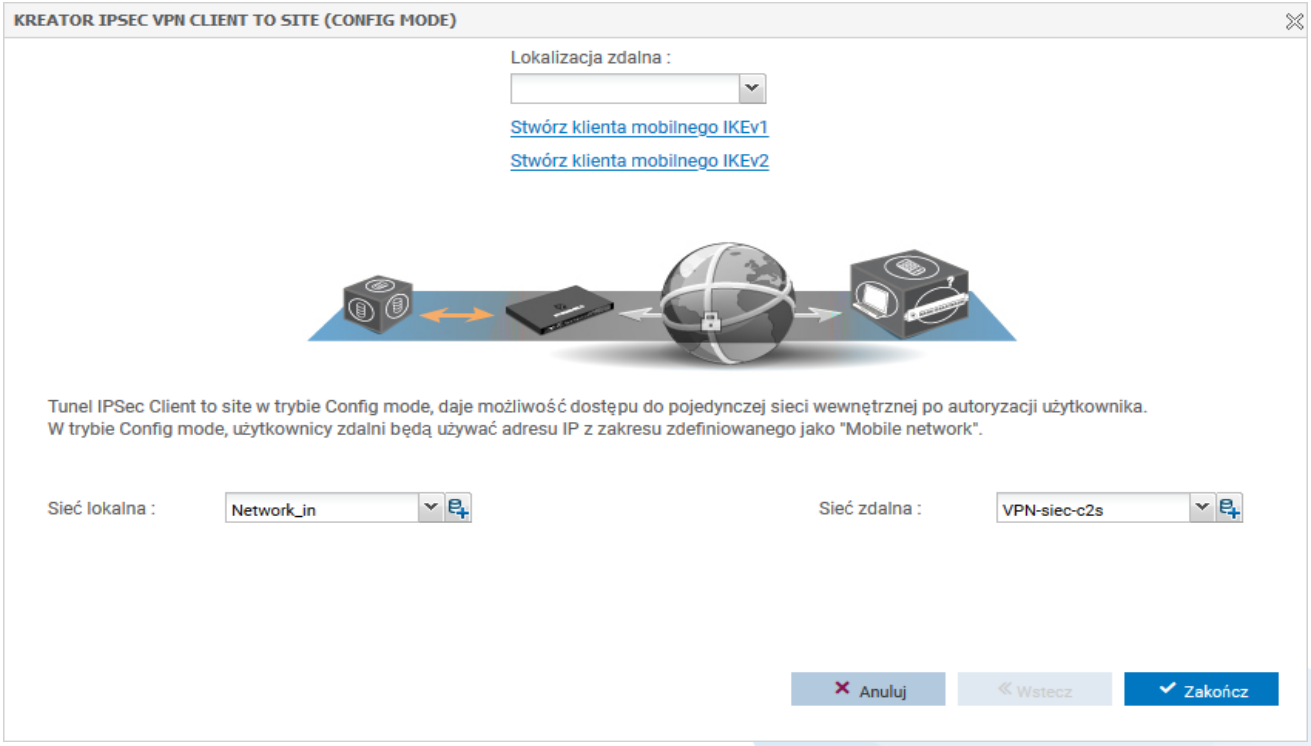
Profile **IKE** są profilami fazy pierwszej, natomiast profile **IPsec** są profilami fazy drugiej.

> **Uwaga**
>
> Najczęstsze problemy z połączeniem IPsec Site-to-Site wynikają z błędnie ustawionych profili IKE i/lub IPsec. Bardzo ważne jest to aby obie strony tunelu miały ustawione takie same algorytmy. Jeżeli jedna ze stron będzie miała inne parametry nie dojdzie do zestawienia tunelu VPN.

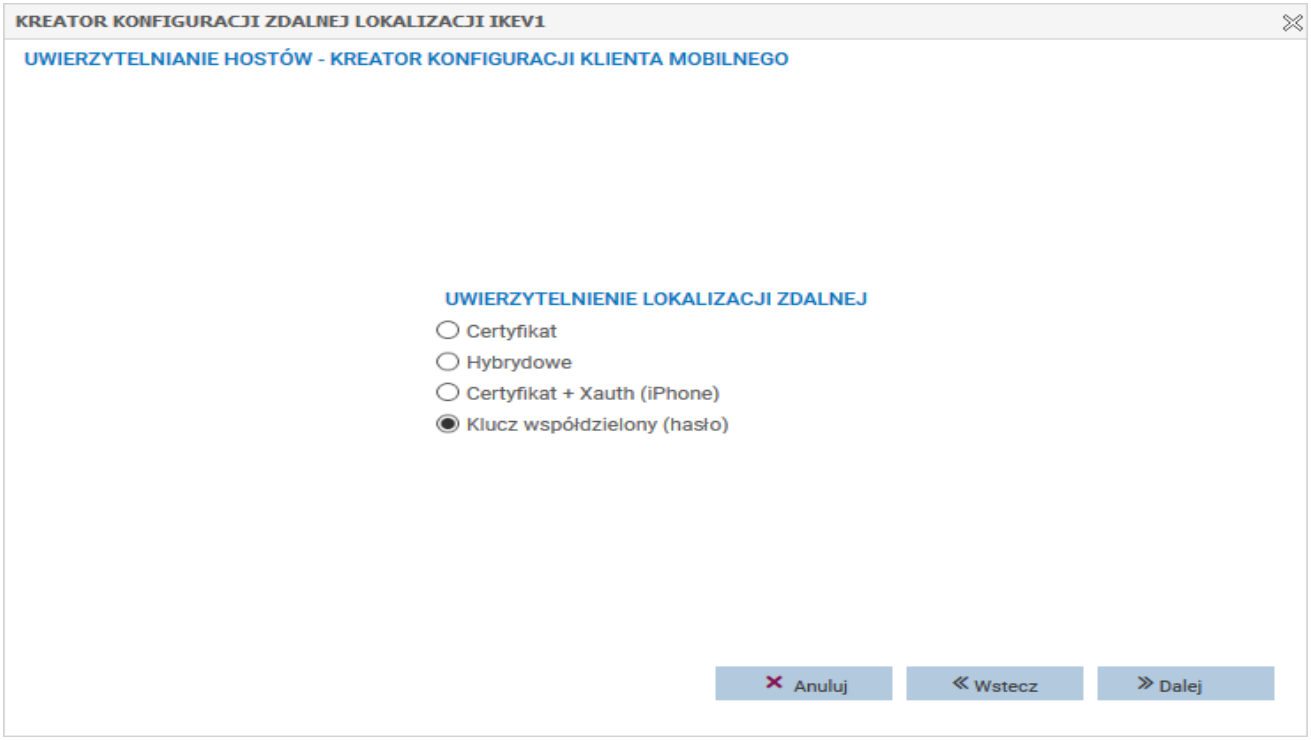
Konfiguracja połączenia Client-to-Site z użyciem STORMSHIELD VPN Client

Konfiguracja po stronie STORMSHIELD

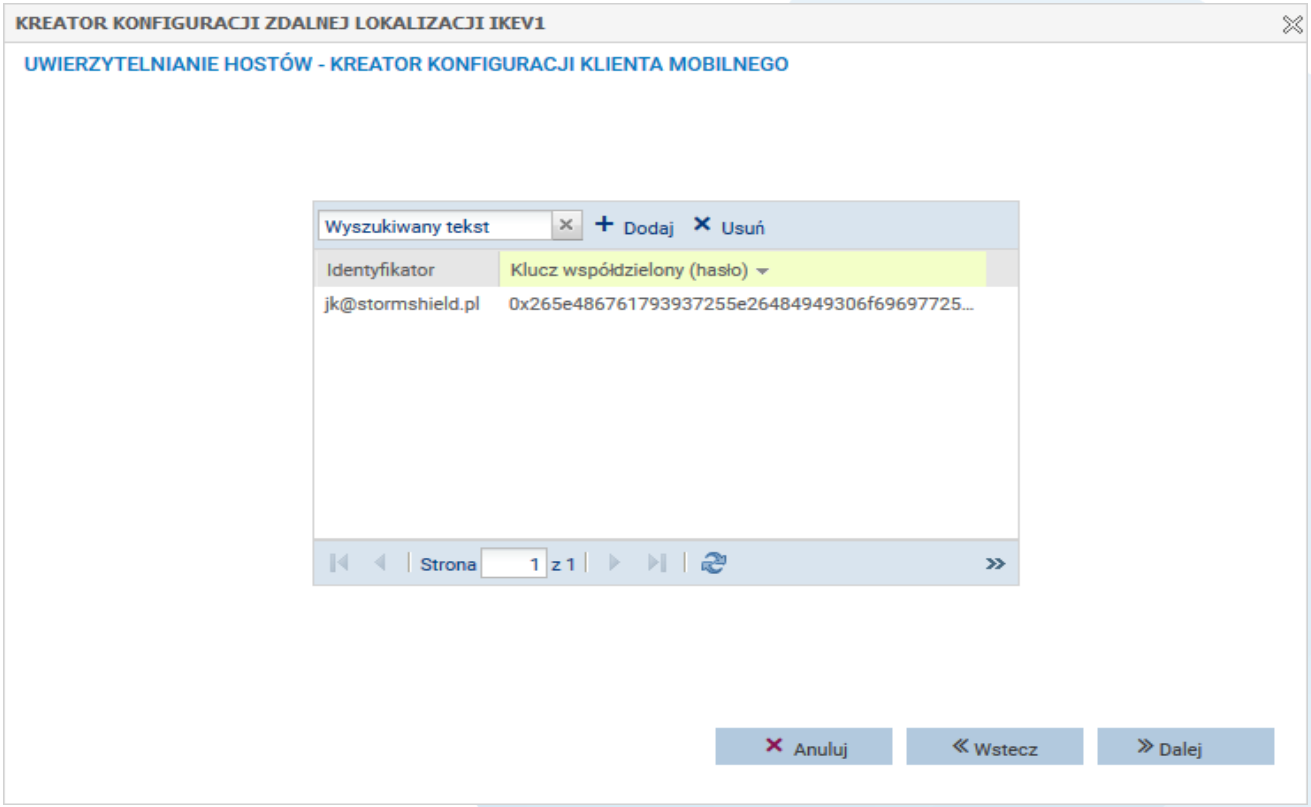
W sekcji **KONFIGURACJA > POŁĄCZENIA VPN > IPsec VPN** należy przejść do zakładki **Konfiguracja Tuneli IPsec > Konfiguracja klientów mobilnych** i wybrać **Dodaj > Nowa polityka Config mode**. Podobnie jak w przypadku konfiguracji Site-to-Site uruchamia się kreator, w którym należy zdefiniować sieci jakie będą dostępne w tunelu: Sieć lokalna, Sieć zdalna (unikalna sieć, w ramach której przydzielane będą adresy klientom VPN) oraz wybrać **Stwórz klienta mobilnego (IKEv1 lub IKEv2)**.



Kreator dodawania nowego klienta pozwoli na zdefiniowanie mechanizmu uwierzytelniania wykorzystywanego przez urządzenie. Najprostszym mechanizmem jest uwierzytelnianie z użyciem identyfikatora i hasła (klucz współdzielony).

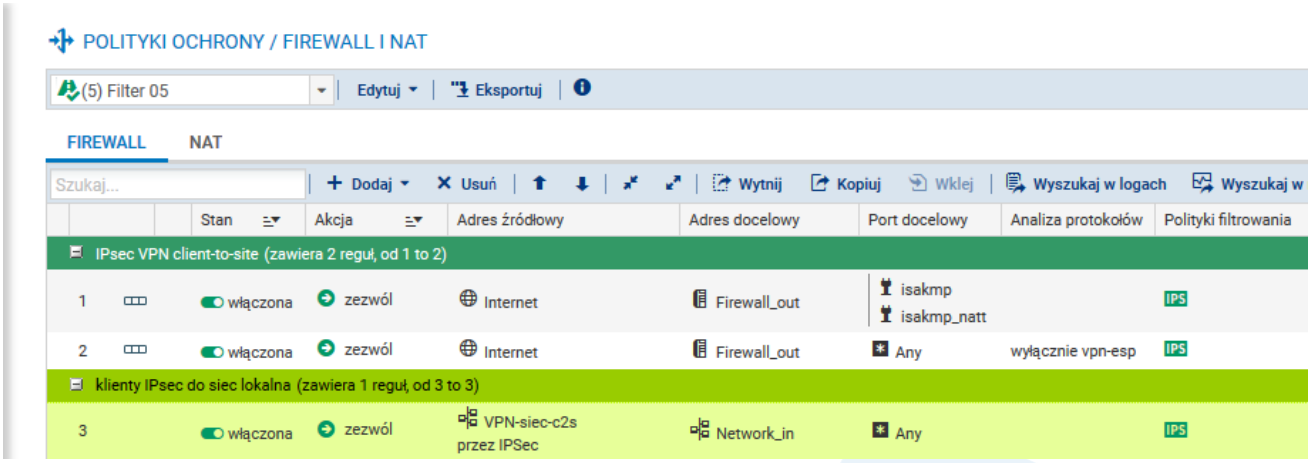


Na etapie kreatora można stworzyć listę uwierzytelniania, ale można to zrobić również później na zakładce **Certyfikaty i klucze współdzielone**.



Jeżeli nie zrobiono tego wcześniej, to należy jeszcze dokonać konfiguracji uprawnień użytkowników (Polityka IPsec / kolumna IPSEC) oraz dodać reguły firewall zezwalające na nawiązywanie połączeń IPsec typu Client-to-Site. Uprawnienia użytkowników do dostępu do usługi VPN nadawane są w sekcji KONFIGURACAJ > UŻYTKOWNICY > Polityki dostępu szczegółowo opisanej wyżej.

Konfiguracja firewall powinna zawierać reguły pozwalające na nawiązanie połączeń na portach 500UDP (isakmp), 4500UDP (isakmp_natt) oraz protokołu VPN-ESP. Ponadto należy skonfigurować regułę pozwalającą na ruch wewnątrz tunelu VPN.
Poniżej przedstawiono jak takie reguły powinny wyglądać:



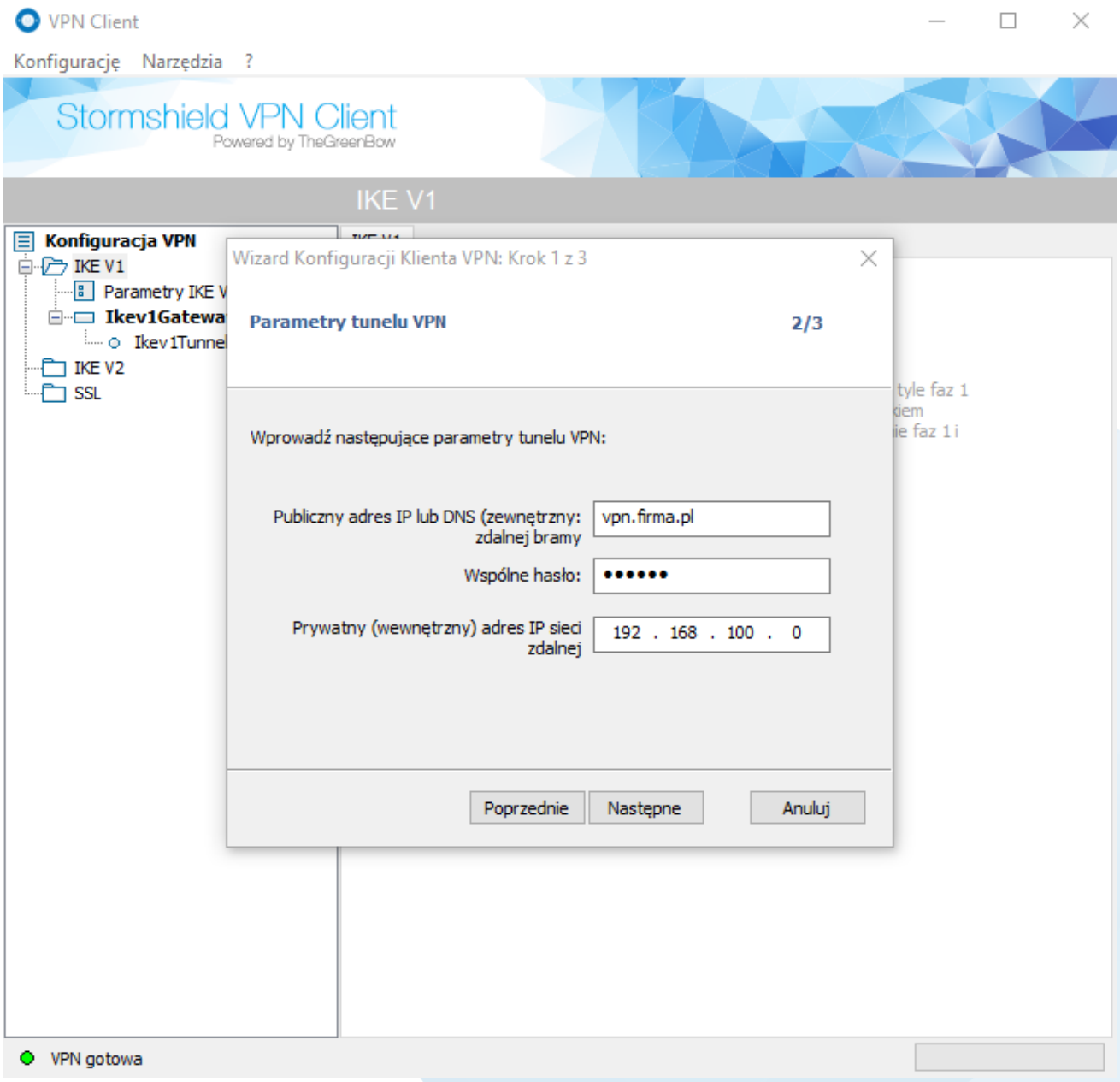
Konfiguracja klienta STORMSHIELD VPN Client

Oprogramowanie Stormshield VPN Client jest dostępne do pobrania ze strefy klienta - https://mystormshield.eu. Do aktywacji oprogramowania wymagana jest dodatkowa licencja.

Po przeprowadzonej instalacji w kliencie VPN uruchamiamy kreator konfiguracji (Plik > Kreator konfiguracji).

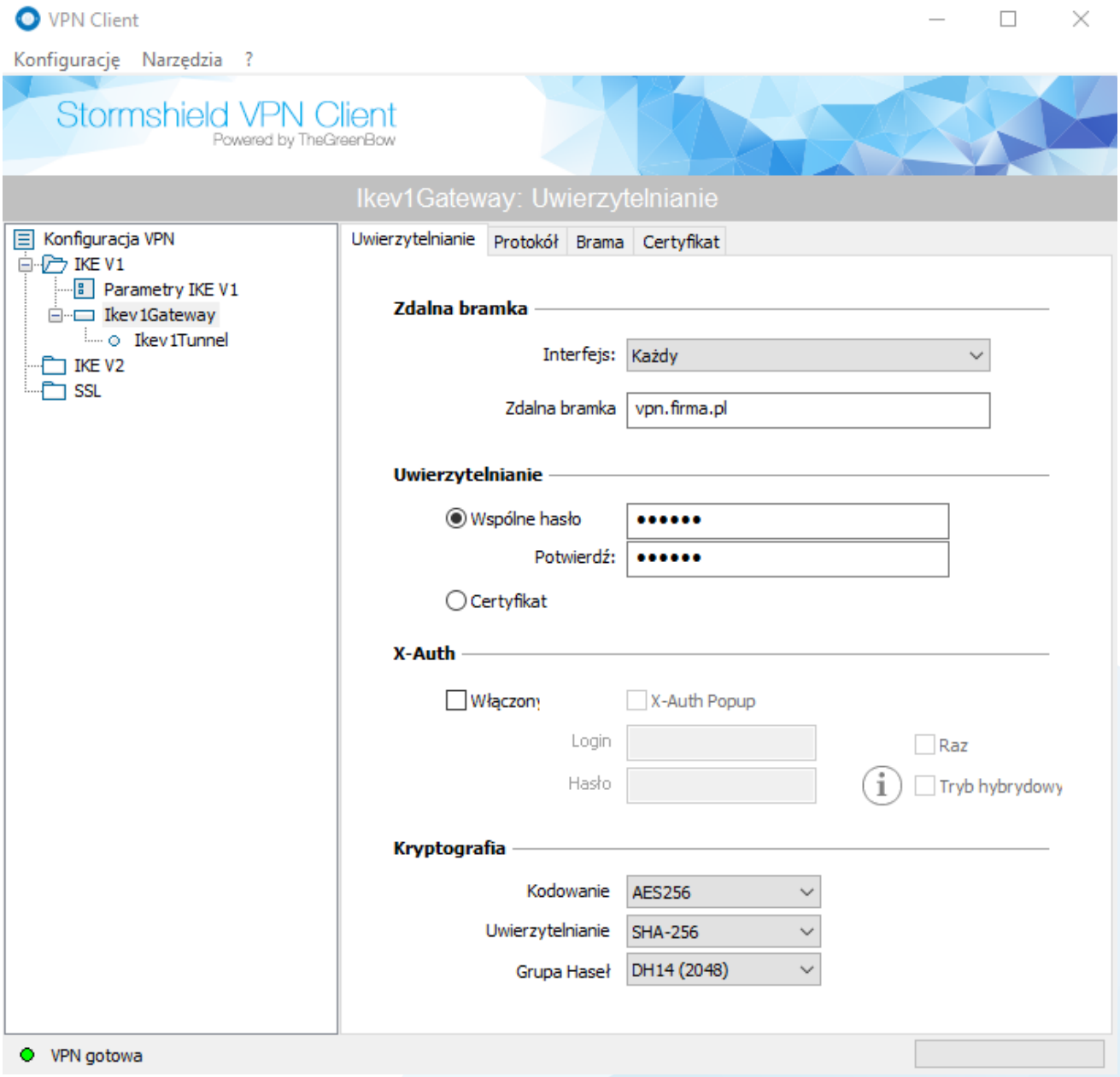
Poniżej przedstawiono konfigurację klienta Stormshield VPN Client na potrzeby połączenia z urządzeniem STORMSHIELD UTM w ramach protokołu IPsec IKEv1.

W kreatorze należy wybrać opcję **Brama IKEv1**, a następnie publiczny adres IP lub FQDN urządzenia STORMSHIELD UTM, hasło współdzielone (nadane dla użytkownika podczas konfiguracji urządzenia) oraz adres sieci wewnętrznej udostępnianej przez urządzenie STORMSHIELD UTM (*Sieć lokalna* w konfiguracji IPsec na urządzeniu):

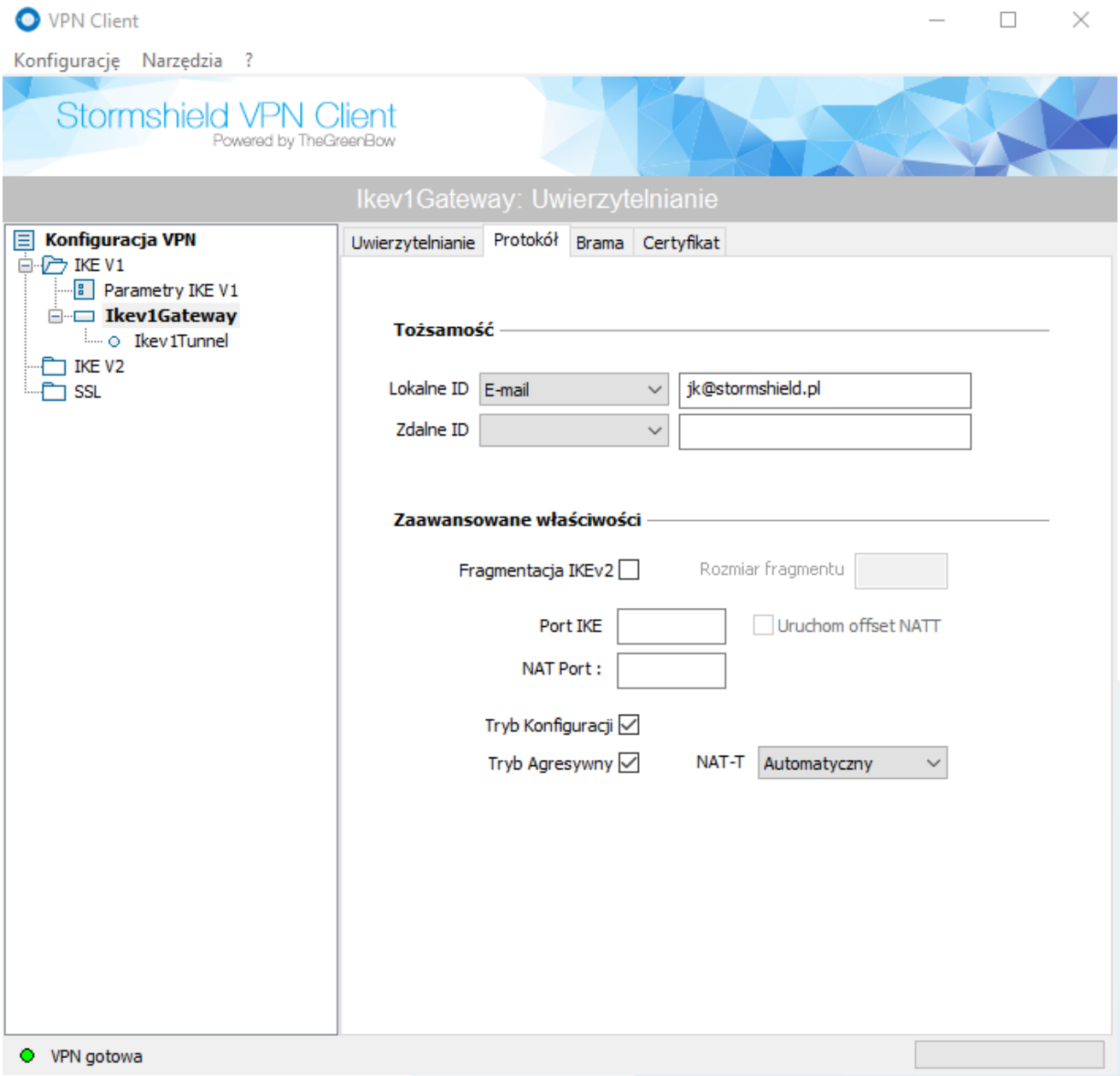


Po zakończeniu Kreatora konfiguracji należy zmodyfikować niektóre z ustawień domyślnych, tak aby były zgodne z konfiguracją profili IKE i IPSEC na urządzeniu oraz podać dane autoryzacyjne:

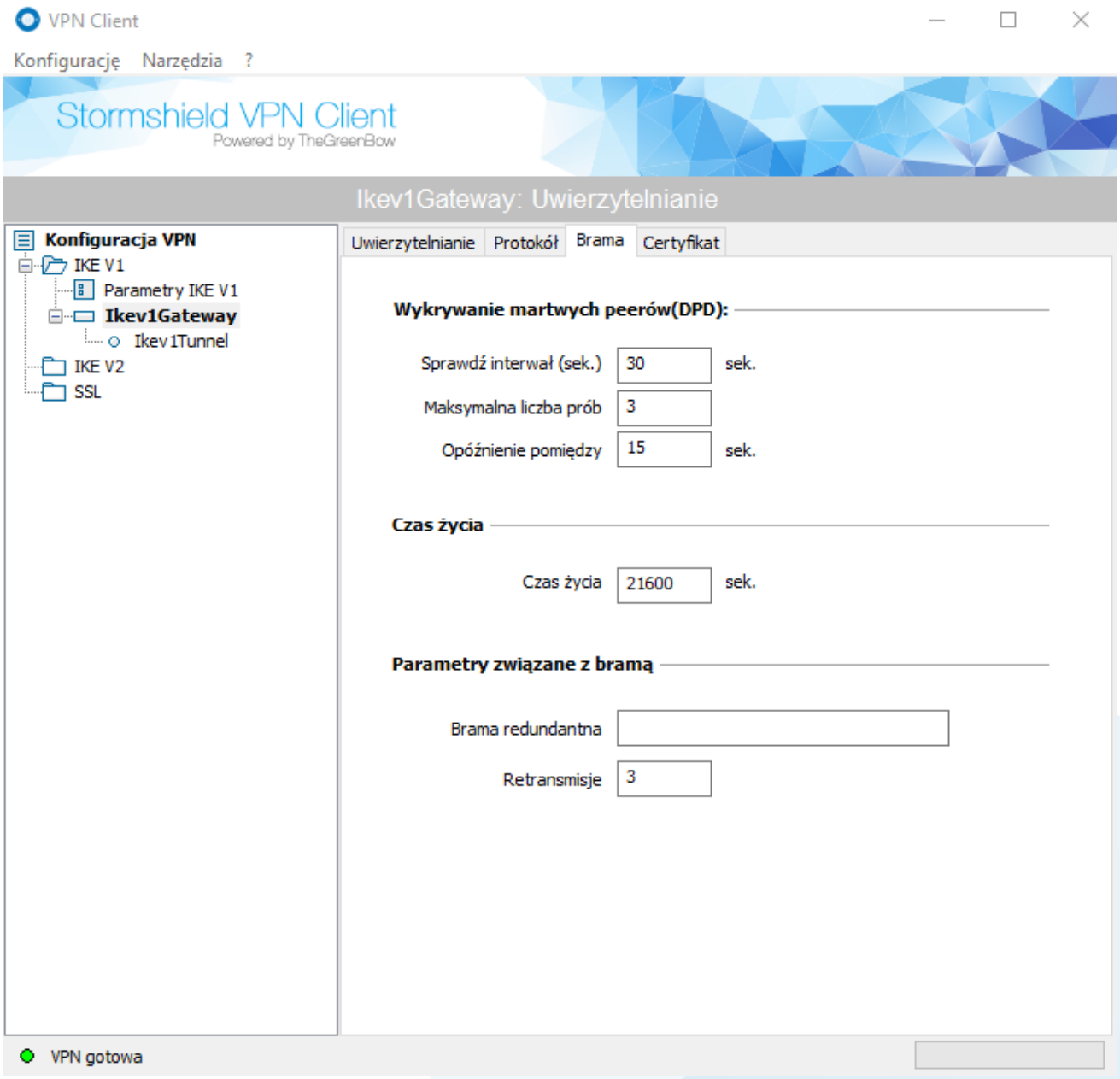
1. W menu **Ikev1Gateway** na zakładce **Uwierzytelnianie** w sekcji **Kryptografia** należy zweryfikować zgodność użytych algorytmów:



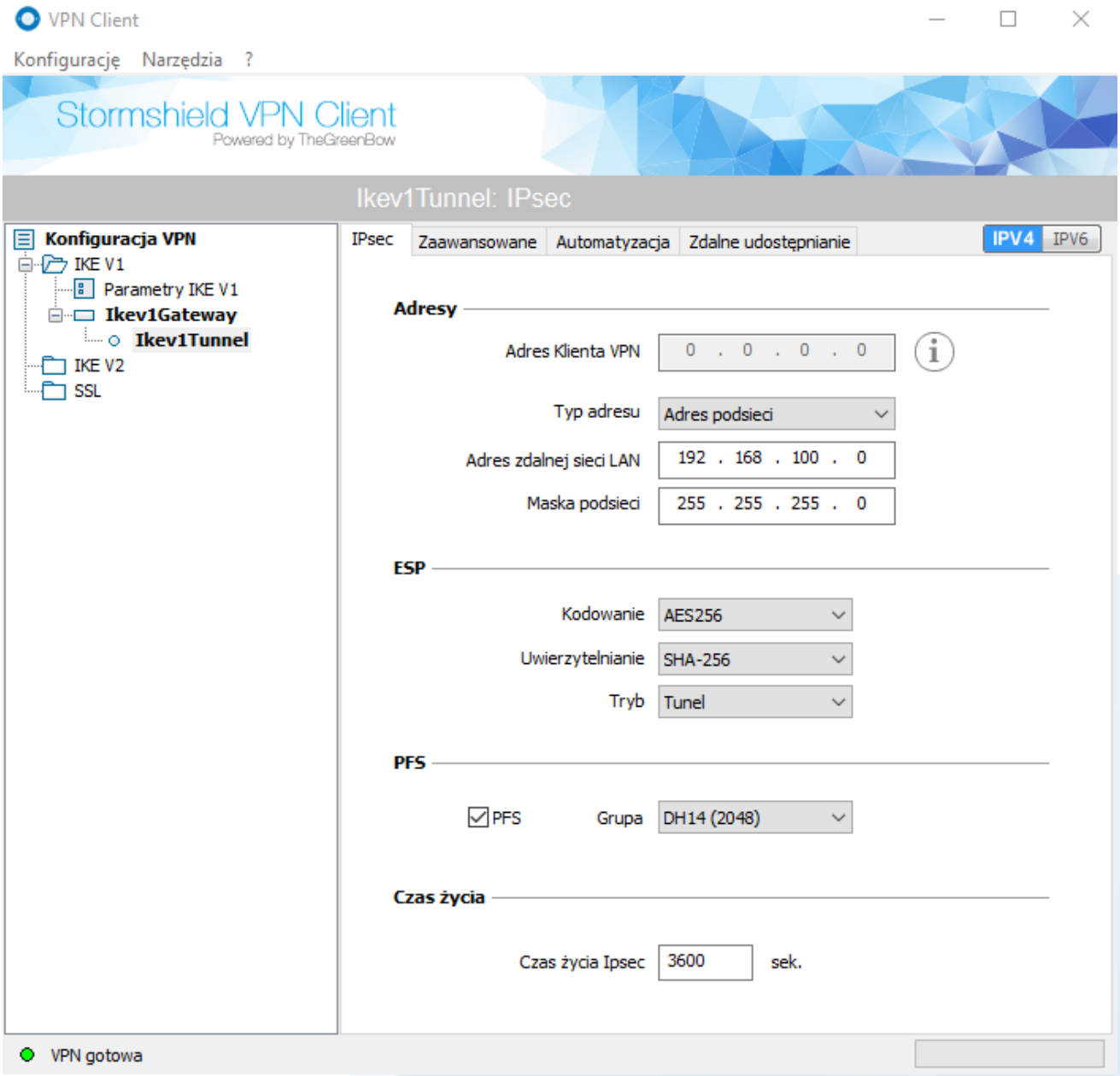
2. Na zakładce **Protokół** w sekcji **Tożsamość** należy wskazać sposób identyfikacji klienta IPsec (jako identyfikator należy wybrać adres e-mail użytkownika zdefiniowanego w usłudze katalogowej LDAP bądź AD), a w sekcji **Zaawansowane właściwości** należy włączyć **Tryb Konfiguracji** i **Tryb Agresywny**



3. Należy też zwrócić uwagę na ustawienie czasu życia fazy 1 (IKE) – zakładka **Brama**, sekcja **Czas życia**. Domyślnym ustawieniem tego parametru na urządzeniu STORMSHIELD UTM jest 21600 (domyślnie użyty profil IKE - StrongEncryption).



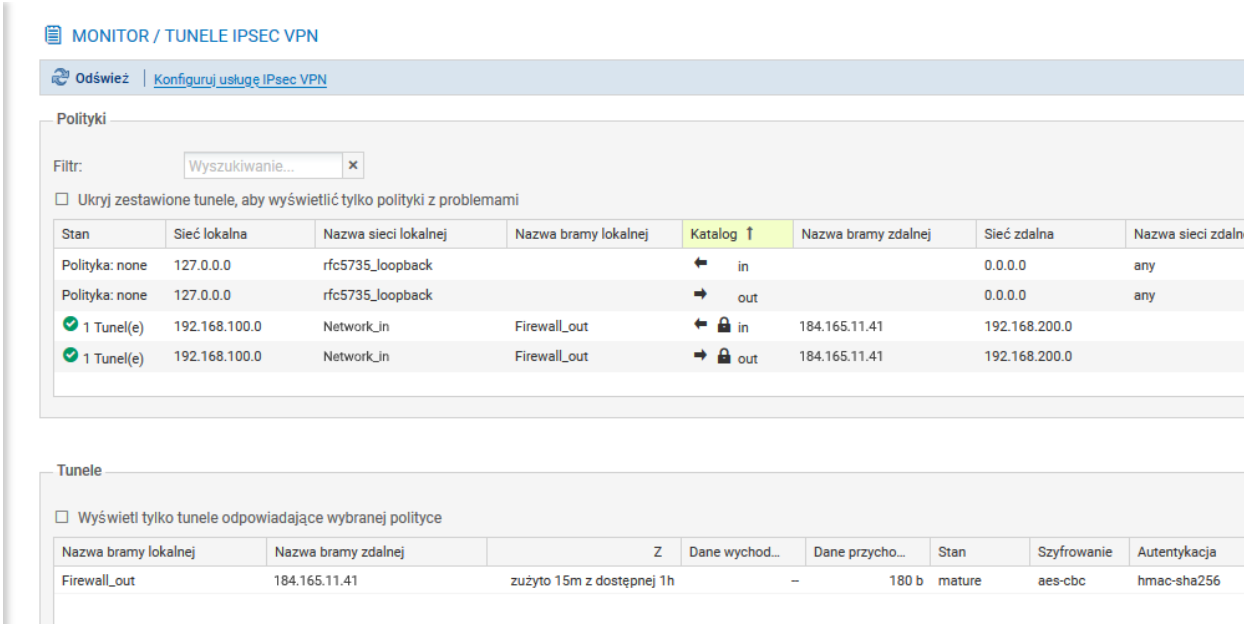
4. Ustawienia dotyczące fazy 2 (IPSEC) znajdują się w menu **Ikev1Tunnel**. Szczególną uwagę należy zwrócić na ustawienia na zakładce **IPsec** i sekcje: **Adresy** – Adres zdalnej sieci LAN (*Sieć lokalna* w ustawieniach urządzenia Stormshield), **ESP** – algorytmy szyfrowania i uwierzytelniania, **PFS** oraz **Czas życia**. Wszystkie powyższe ustawienia muszą być zgodne z ustawieniami drugiej strony tunelu VPN (urządzenie STORMSHIELD UTM). Domyślny profil dla takich połączeń (IPSEC - StrongEncryption) na urządzeniu STORMSHIELD UTM posiada odpowiednio AES256, SHA-256, PFS - DH14 (2048-bits), czas życia – 3600.



Aby zakończyć konfigurację klienta należy wybrać opcję **Plik > Zapisz** i przejść do panelu połączeń (Ctrl + Enter). W celu zestawienia tunelu VPN należy kliknąć przycisk **Otwórz.**
Po zestawieniu tunelu VPN panel powinien wyglądać jak poniżej:

Wskazówka

W menu **MONITORING > MONITOROWANE > Tunele IPsec VPN** można monitorować aktualnie zestawione tunele IPsec VPN



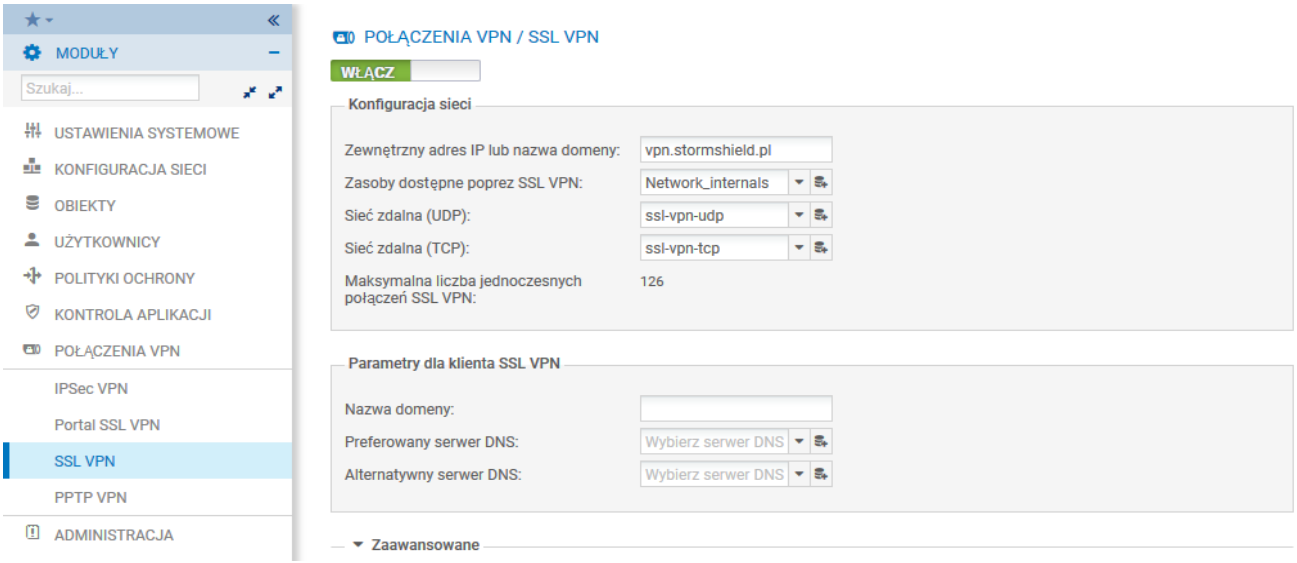
126

Jeśli występują jakiekolwiek problemy z zestawieniem tunelu VPN w pierwszej kolejności należy zweryfikować logi połączeń VPN znajdujące się w MONITORING >LOGI > VPN.

SSL VPN

Full SSL VPN

Tunelowanie SSL VPN pozwala na zestawienie pełnego tunelu **Client-to-Site** pomiędzy klientem mobilnym (stacja robocza, smartfon, itp.), a siecią firmową.
Tunelowanie to jest oparte na serwerze OpenVPN i łączy w sobie prostotę konfiguracji oraz zachowanie wysokiego poziomu bezpieczeństwa z uwagi na zastosowanie algorytmu AES.
W trakcie nawiązywania łączności użytkownik musi podać jedynie adres IP oraz poświadczenia, wszystkie pozostałe parametry związane z szyfrowaniem połączenia są synchronizowane w tle.
Konfiguracja SSL VPN odbywa się w sekcji **KONFIGURACJA > POŁĄCZENIA VPN > SSL VPN**. Widok okna konfiguracyjnego przedstawiono poniżej.

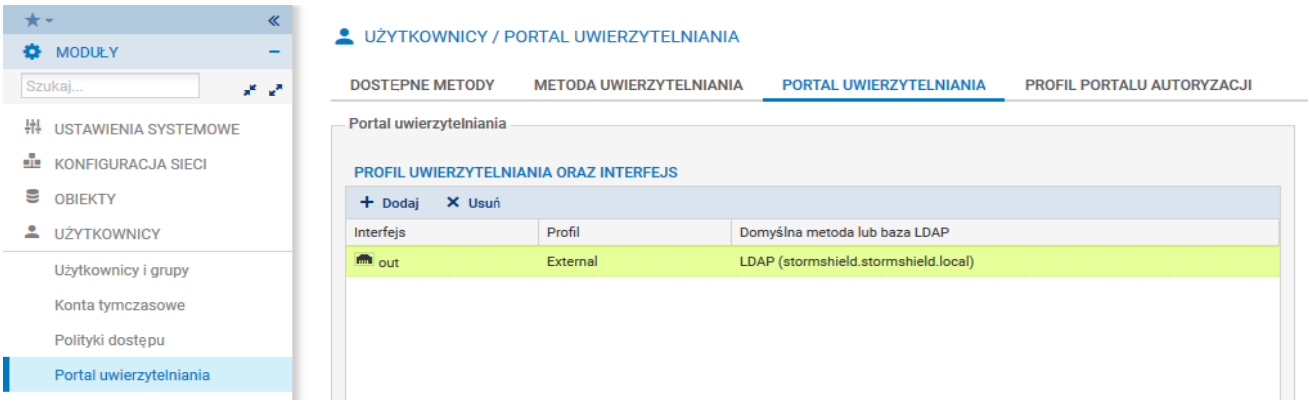


- **Zewnętrzny adres IP lub nazwa domeny –** jednoznacznie identyfikuje publiczny adres IP/domenę, pod którą będzie dostępny serwer SSL VPN (zazwyczaj jest to po prostu adres IP przypisany do interfejsu zewnętrznego STORMSHIELD UTM);
- **Zasoby dostępne poprzez SSL VPN** – wskazuje, które z dostępnych na urządzeniu STORMSHIELD UTM sieci mają być osiągalne dla klientów VPN po zestawieniu tunelu;
- **Sieć zdalna (UDP) –** zakres adresów przydzielany klientom łączącym się za pośrednictwem protokołu UDP (domyślnie port 1194).
- **Sieć zdalna (TCP) –** zakres adresów przydzielany klientom łączącym się za pośrednictwem protokołu TCP (domyślnie port 443).
- **Maksymalna liczba jednoczesnych połączeń SSL VPN** – ilość tuneli, które mogą być jednocześnie uruchomione. Liczba ta zależy od modelu urządzenia, oraz sieci przypisanych klientom zdalnym.
- **Nazwa domeny –** opcjonalna nazwa domeny.
- **Preferowany/Alternatywny serwer DNS –** adres serwera DNS dla klientów mobilnych.

> **Uwaga**
>
> Zarówno **Sieć zdalna (UDP)** jak i **Sieć zdalna (TCP)** nie mogą w żadnej części pokrywać się z wcześniej zdefiniowanymi sieciami na interfejsach urządzenia STORMSHIELD UTM. Sieci te muszą być unikalne.

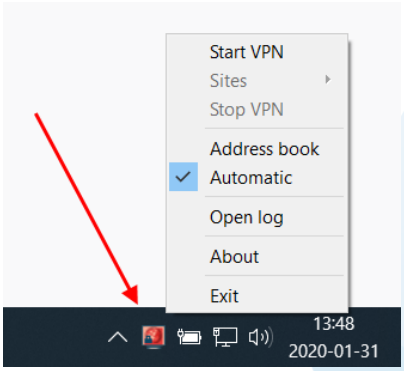
Należy pamiętać aby poza samą konfiguracją SSL VPN udzielić użytkownikom zdefiniowanym na urządzeniu odpowiednich uprawnień dostępowych (KONFIGURACJA > UŻYTKOWNICY > Polityki dostępu).

Domyślny mechanizm działania tuneli SSL VPN na urządzeniach STORMSHIELD UTM wykorzystuje Portal Uwierzytelniania do synchronizacji konfiguracji klienta Stormshield SSL VPN. Konieczne zatem jest włączenie odpowiedniego profilu autoryzacji (zalecanym profilem jest profil External) na zewnętrznym interfejsie urządzenia, na który będą przychodziły połączenia SSL VPN. Poniżej przykład takiej konfiguracji:

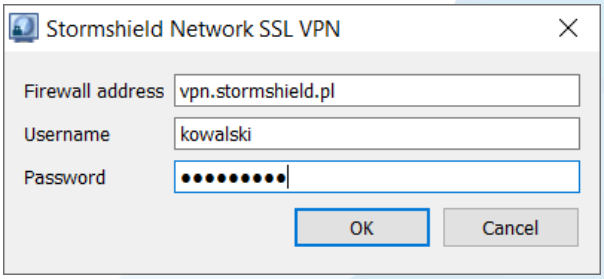


Klient Stormshield SSL VPN

W celu połączenia się poprzez **Tunel SSL VPN** można skorzystać z darmowego klienta VPN SSL Client dostępnego w sekcji **Download** na portalu https://mystormshield.eu.
Po poprawnej instalacji w zasobniku ukaże się ikona klienta. Klikając dwukrotnie lub wchodząc poprzez menu kontekstowe i wybierając *Start VPN* można przejść do konfiguracji klienta.

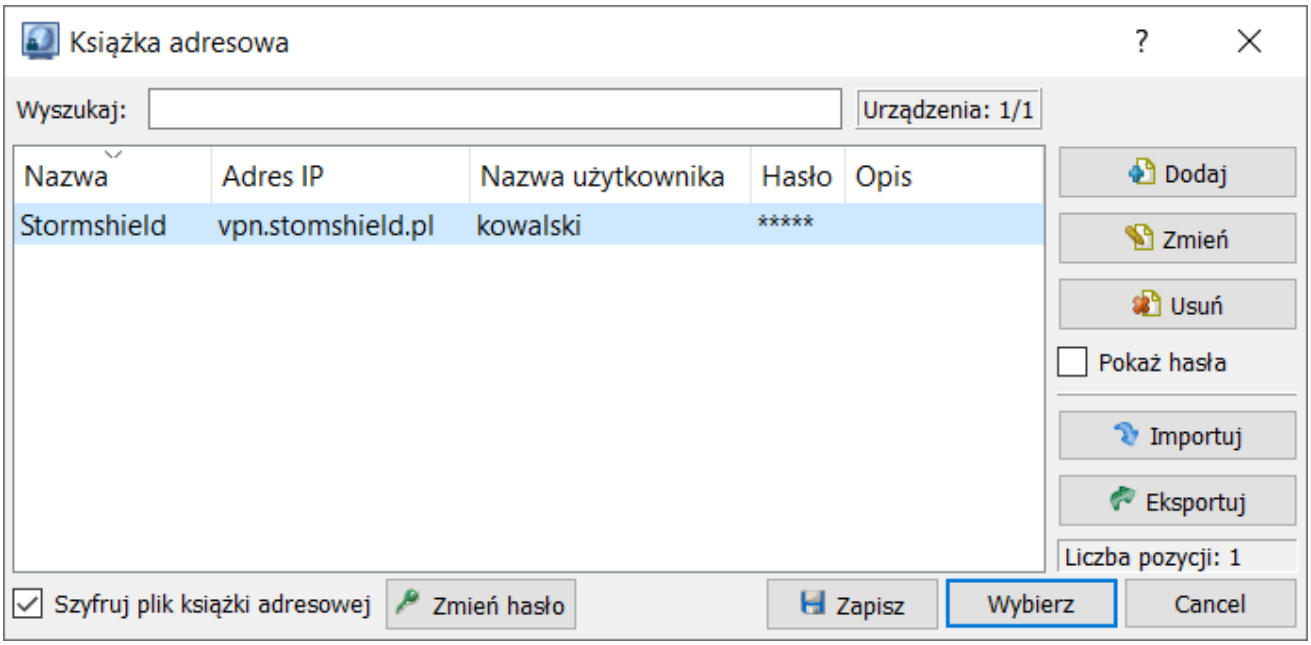


Sama konfiguracja klienta polega na wypełnienia trzech pól:



- **Firewall address –** publiczny adres IP/domena urządzenia, z którym zestawiany jest tunel VPN.
- **Username** – nazwa użytkownika.
- **Password** – hasło wskazanego użytkownika.

W przypadku posiadania większej ilości urządzeń przydatna może okazać się funkcja książki adresowej (Address book).



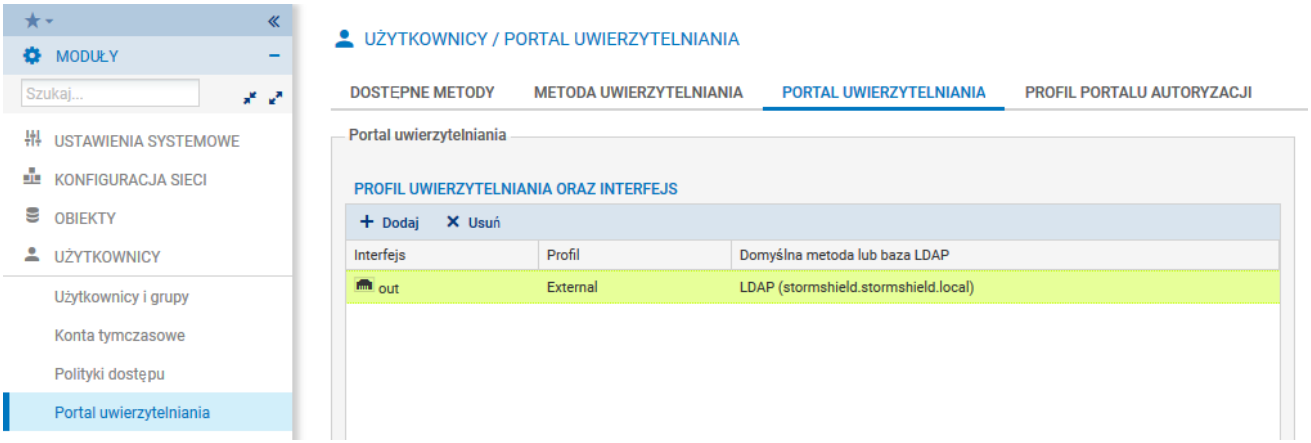
Portal SSL VPN

W odróżnieniu od Full SSL VPN, SSL VPN w trybie Portal nie wymaga instalacji dodatkowego oprogramowania. Klientem dla tego rodzaju połączeń VPN jest przeglądarka internetowa. Jedyny wymóg po stronie klienta to zainstalowana przeglądarka internetowa i oprogramowanie Java (w przypadku korzystania z serwerów aplikacyjnych).

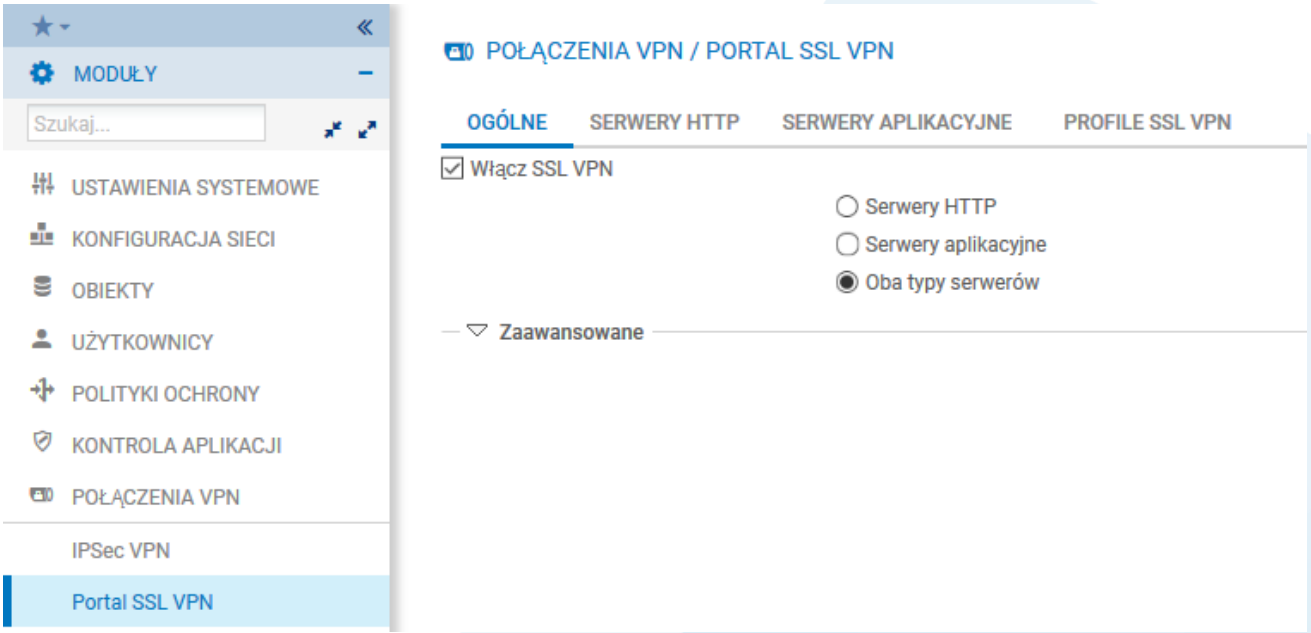
W przypadku Portal SSL VPN każdy z kanałów jest tworzony dla pojedynczej usługi w odniesieniu do konkretnego serwisu. Czyli tunel VPN jest tworzony do konkretnego SERWERA na konkretny PORT. Portal SSL VPN najczęściej stosowany jest do tunelowania połączeń zdalnego pulpitu (RDP) lub połączeń do wewnętrznych serwerów http.

> **Uwaga**
>
> Należy pamiętać, że połączenia są zestawiane na zasadzie Client-to-Site (service) więc dostępny jest tylko jeden port. Jeśli usługa jest wieloportowa nie będzie możliwe jej udostępnienie za pomocą portalu SSL VPN.

Konfigurację SSL VPN należy rozpocząć od włączenia Portalu uwierzytelniania na zewnętrznym interfejsie urządzenia. Konfiguracji tej należy dokonać w sekcji **KONFIGURACJA > UŻYTKOWNICY > Portal uwierzytelniania**.

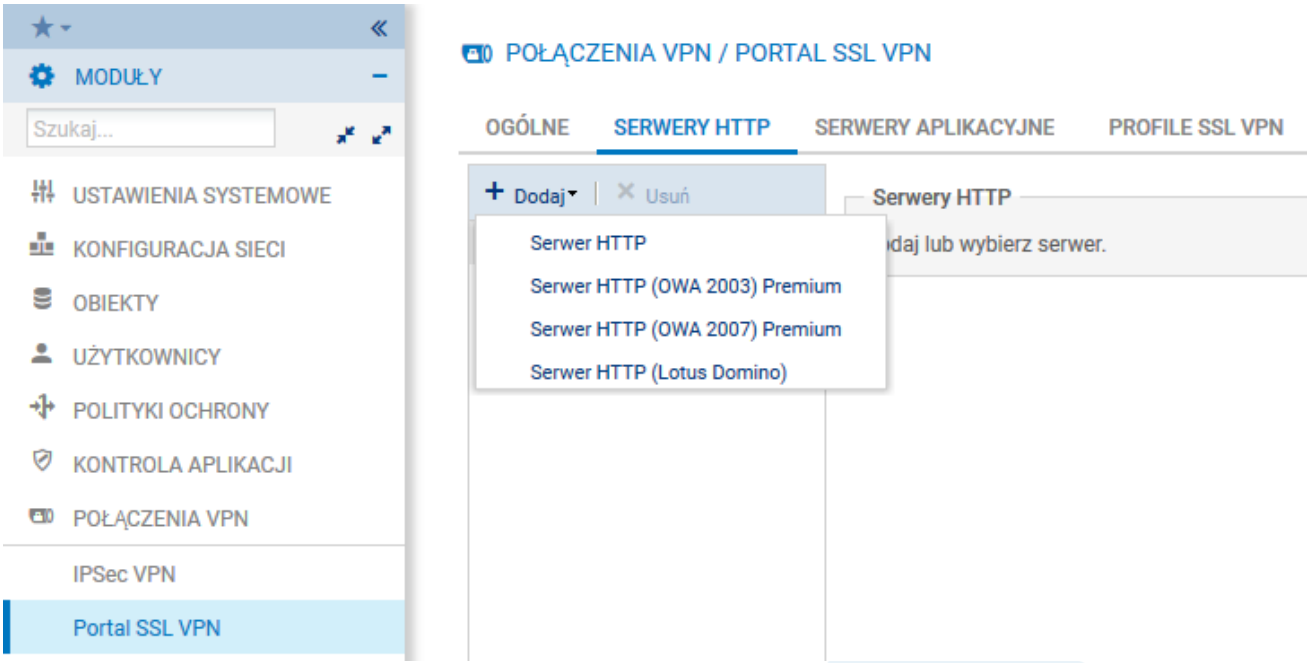


Aby skonfigurować serwer SSL VPN w trybie Portal należy przejść do sekcji **KONFIGURACJA > POŁĄCZENIA VPN > Portal SSL VPN** i zaznaczyć opcję *Włącz SSL VPN*. Następnie należy wybrać jakiego typu usługi chcemy udostępnić za pomocą **SSL VPN**.



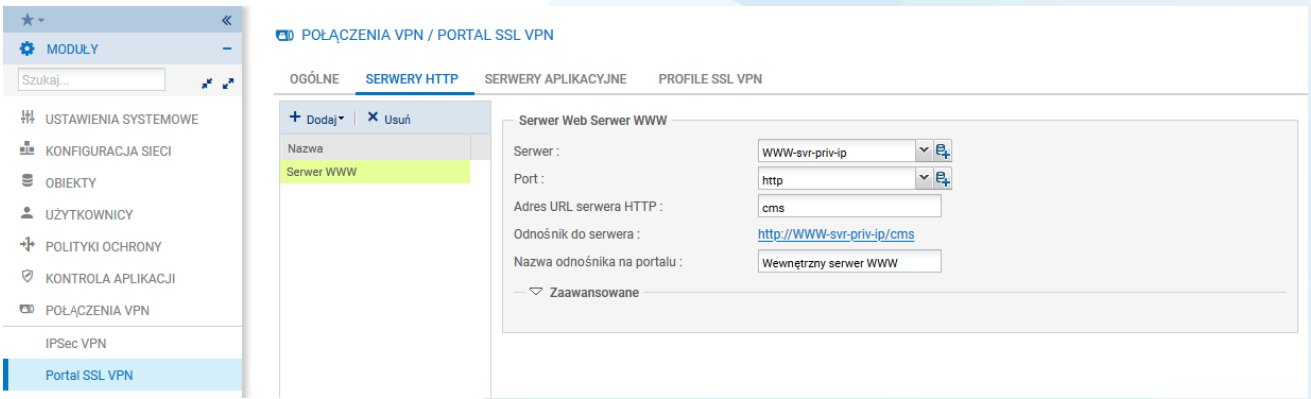
SERWERY HTTP - połączenia do serwerów intranetowych

Na zakładce **SERWERY HTTP** należy użyć przycisku **Dodaj** w celu skonfigurowania nowego zasobu. Do wyboru jest dostęp do zwykłego serwera http lub jeden z predefiniowanych szablonów dostępu do takich usług jak Microsoft OWA czy Lotus Domino.



W oknie konfiguracji dostępu do serwera http można skonfigurować między innymi:

- **Serwer** – obiekt reprezentujący adres IP serwera docelowego;
- **Port** – port usługi http serwera, zazwyczaj jest to port http (80/TCP);
- **Adres URL serwera HTTP** – pozwala na wskazanie podstrony, na którą będzie automatycznie przekierowany ruch;
- **Odnośnik do serwera** – w tym miejscu znajduje się odnośnik, który jest dynamicznie tworzony na podstawie powyższych parametrów;
- **Nazwa odnośnika na portalu** – nazwa pod jaką będzie widoczne połączenie w oknie portalu SSL VPN. Nazwa powinna ułatwiać użytkownikom identyfikację usługi.



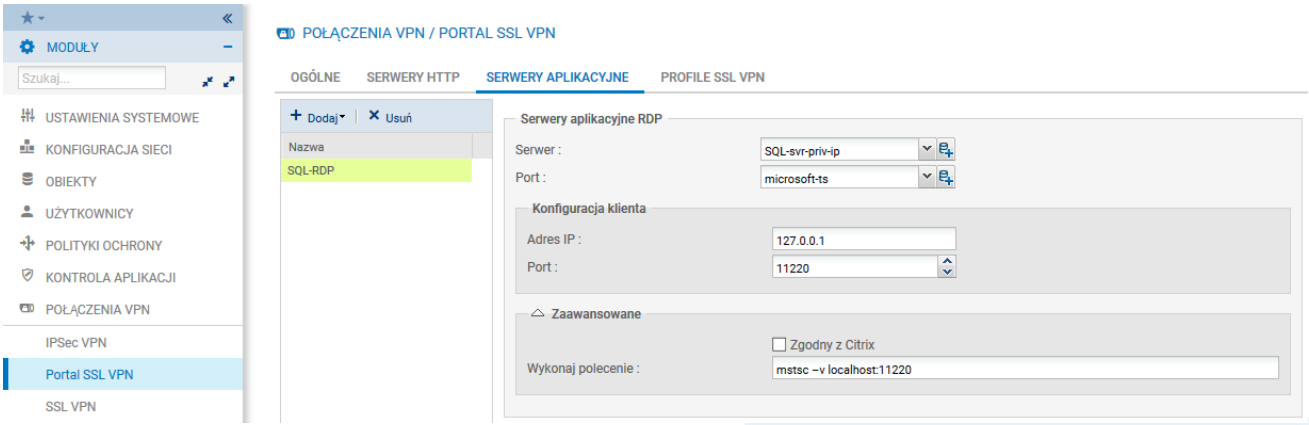
Kolejnym krokiem jest stworzenie odpowiedniego profilu SSL VPN, czynność ta została opisana w kolejnych rozdziałach niniejszej dokumentacji.

SERWERY APLIKACYJNE

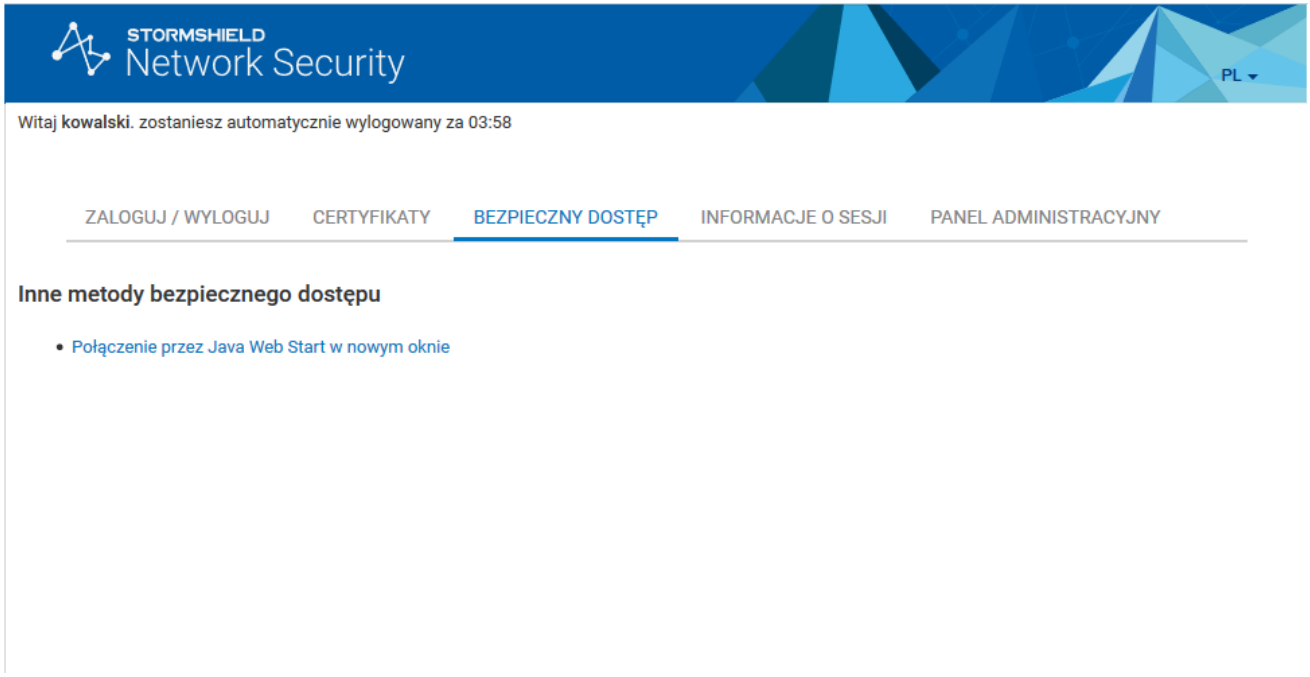
Dostęp do serwerów aplikacyjnych realizowany jest za pomocą aplikacji Java. Działanie tego połączenia opiera się o przechwycenie przez aplet Java połączeń na port loopback komputera klienta (127.0.0.1) i tunelowanie ich wewnątrz połączenia SSL VPN do serwera docelowego.

Przykład konfiguracji dostępu do serwerów aplikacyjnych został przedstawiony poniżej i obejmuje:

- **Serwer** – obiekt reprezentujący adres IP serwera docelowego;
- **Port** – port usługi serwera, która ma zostać udostępniona;
- **Konfiguracja klienta**
  - **Adres IP** – adres IP, z którego Java będzie przechwytywała połączenia;
  - **Port** – port, z którego Java będzie przechwytywała połączenia.

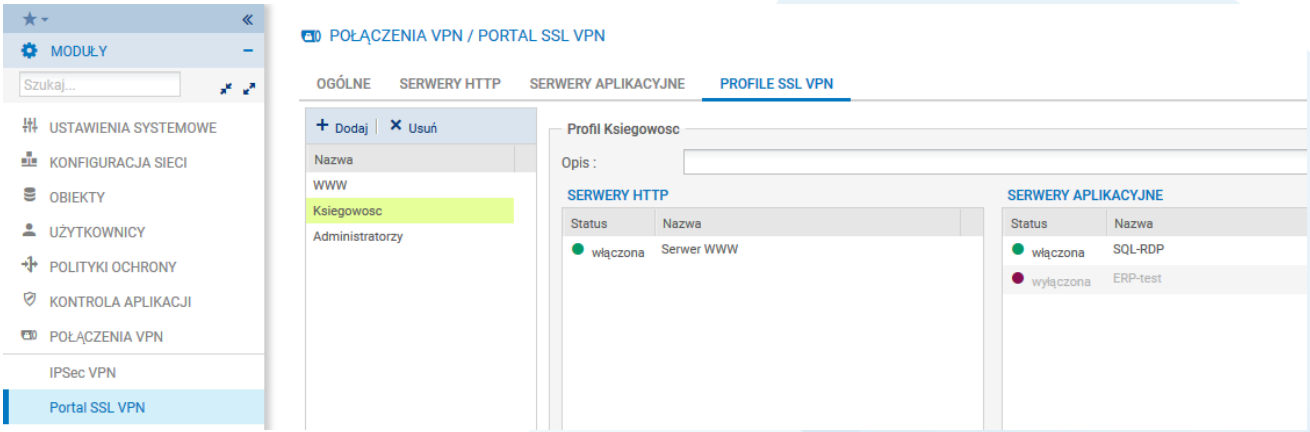


Bardzo przydatnym parametrem jest opcja **Wykonaj polecenie** w ustawieniach zaawansowanych, która pozwala na określenie polecenia, jakie zostanie wykonane po uruchomieniu apletu Java i wybraniu odpowiedniego linku. W tym wypadku będzie to polecenie *mstsc –v localhost:11220*, które wywołuje klienta zdalnego pulpitu (mstsc) i uruchamia połączenie do adresu 127.0.0.1 na port 11220. Dzięki temu użytkownik po zalogowaniu się nie musi uruchamiać klienta RDP i wpisywać adresu ręcznie. Wystarczy, że kliknie link, co spowoduje automatyczne uruchomienie się klienta zdalnego pulpitu wraz z niezbędnymi do połączenia opcjami.



Profile SSL VPN

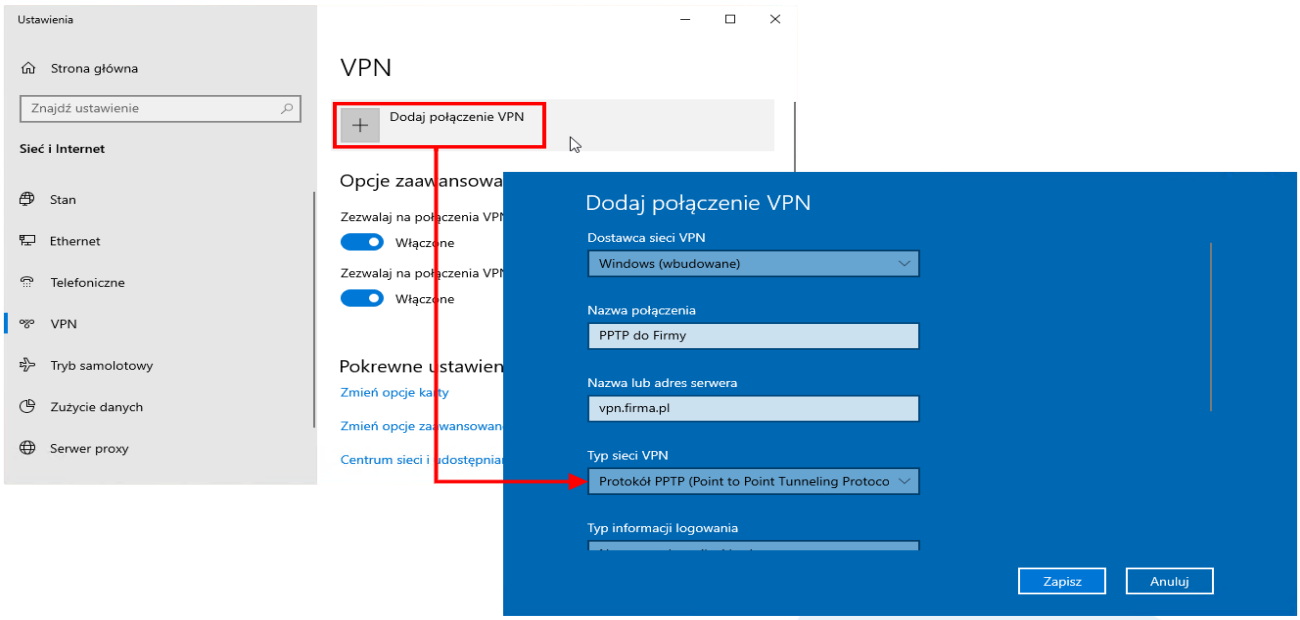
Profile umożliwiają nadanie użytkownikom uprawnień jedynie do wybranych połączeń w ramach całego serwera SSL VPN w trybie Portalu. Zakładka **Profile SSL VPN** służy do konfiguracji, które serwery maja być dostępne w ramach którego profilu.



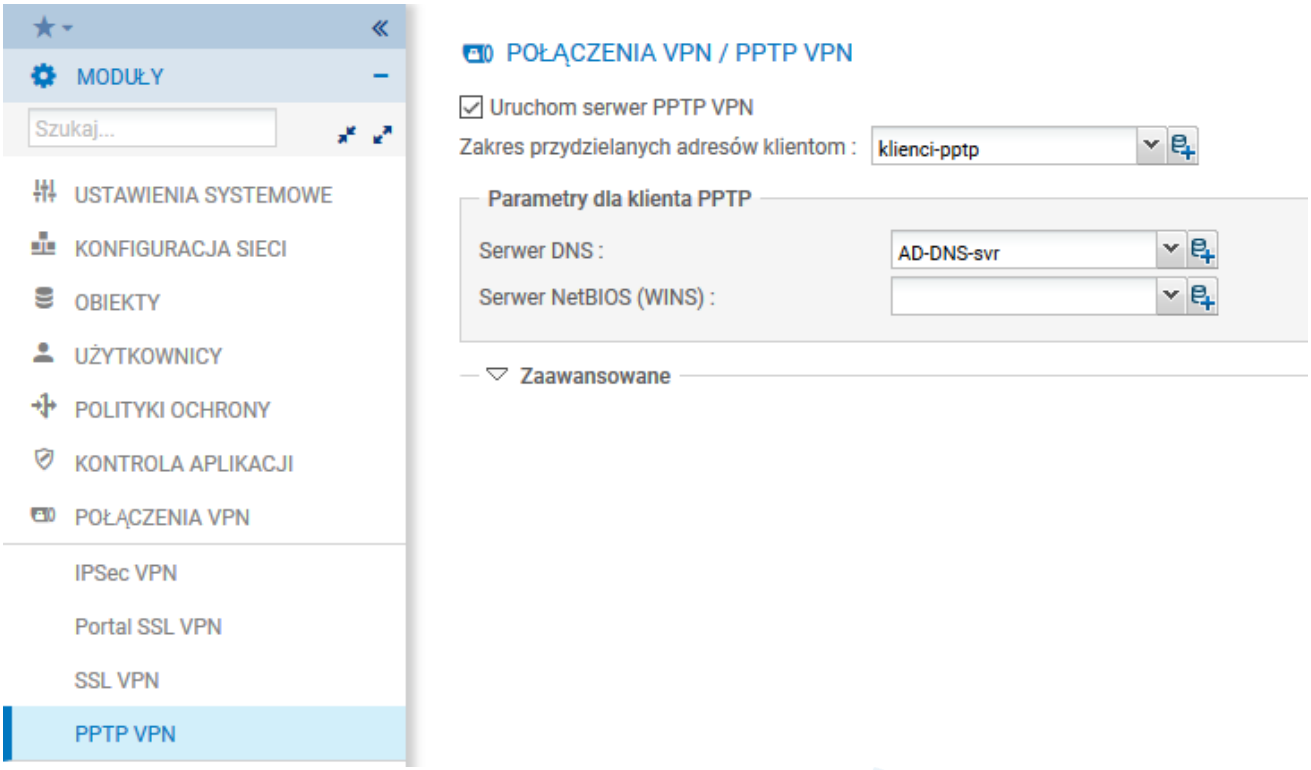
Dowiązania profilu SSL VPN do użytkownika dokonuje się w menu **KONFIGURACJA > UŻYTKOWNICY > Polityki dostępu**.

PPTP VPN (Point to Point Tunneling Protocol)

PPTP jest protokołem najprostszym w konfiguracji jednak najmniej bezpiecznym i odradza się jego użycie z wyjątkiem sytuacji gdzie musimy zestawić tunel VPN z klientem, który nie obsługuje innych typów połączeń VPN. Protokół PPTP pozwala na tworzenie tuneli typu **Client-to-Site** z wykorzystaniem klienta wbudowanego w system Microsoft Windows. Po stronie systemu operacyjnego w ustawieniach **Sieć i Internet > VPN** należy **Dodać połączenie VPN** i podać parametry połączenia PPTP.



Po stronie STORMSHIELD UTM stosownej konfiguracji należy dokonać w sekcji **KONFIGURACJA > POŁĄCZENIA VPN > PPTP VPN**.



W tym miejscu należy skonfigurować następujące opcje:

- **Uruchom serwer PPTP VPN** – włączenie/wyłączenie usługi PPTP na urządzeniu;
- **Zakres przydzielanych adresów klientom** – zakres adresów IP jakie będą uzyskiwali klienci łącząc się poprzez tunel PPTP. Ważne jest, aby ten zakres nie pokrywał się z adresami IP wykorzystywanym przez inne hosty w sieci LAN, jednak (w przeciwieństwie do konfiguracji SSL VPN oraz IPsec VPN) **musi** on zawierać się w tej samej podsieci, do której zestawiany jest tunel VPN (np. gdy używana jest sieć 192.168.1.0/24 to na potrzeby PPTP VPN można użyć zakresu adresów od 192.168.1.240-192.168.1.250);
- **Serwer DNS** – adres serwera DNS dla klientów PPTP VPN;
- **Serwer NetBIOS (WINS)** – adres serwera usługi NetBIOS dla klientów PPTP VPN.

Ostatnim krokiem jest nadanie praw użytkownikom do tworzenia tuneli PPTP VPN. Konfiguracji tej należy dokonać w sekcji **KONFIGURACJA > UŻYTKOWNICY > Polityki dostępu** w zakładce **Konfiguracja PPTP VPN**.

> Uwaga
>
> Z uwagi na luki w protokole PPTP, przy konfiguracji polityk dostępu dla PPTP należy zdefiniować nowe (najlepiej inne) hasło użytkownika.

14. Konfiguracja proxy HTTP, SMTP, POP3, FTP, SSL

Każdy z mechanizmów proxy w urządzeniach STORMSHIELD UTM może działać w sposób transparentny dla użytkownika, tzn. nie wymagać konfiguracji przeglądarki czy innego oprogramowania zależnie od protokołu. Ponadto dla urządzeń działających w trybie bridge możliwe jest przełączenie mechanizmu proxy w tryb transparentny z punktu widzenia sieci, tzn. dla ruchu proxy pozostawiany jest każdorazowo oryginalny nagłówek TCP/IP. W przypadku protokołu HTTP możliwe jest również skonfigurowanie proxy w trybie explicit proxy, tzn. takiego, które jest jawnie skonfigurowane w przeglądarce.
Poniżej przedstawiono funkcjonalność najpopularniejszych z mechanizmów proxy:

HTTP proxy

- klasyfikacja URL (filtrowanie dostępu do wybranych grup stron www),
- konfiguracja strony informującej o zablokowaniu dostępu do strony www (Block page),
- skanowanie antywirusowe dla ruchu http,
- analiza z użyciem mechanizmu Sandboxing (Stormshield Breach Fighter),
- analiza WEB 2.0 – analiza kodu HTML i JavaScript,
- określenie maksymalnego rozmiaru pliku pobieranego przez http,
- filtrowanie plików po typie (MIME Type),
- buforowanie zawartości stron (proxy cache).

POP3 proxy

- skaner antyspam (wiadomość SPAM jest oznaczana przedrostkiem w temacie wiadomości lub może być blokowana),
- skaner antywirusowy,
- analiza z użyciem mechanizmu Sandboxing (Stormshield Breach Fighter),
- kontrola komend w ramach protokołu pop3.

SMTP proxy

- skaner antyspam (wiadomość SPAM jest oznaczana przedrostkiem w temacie wiadomości lub może być blokowana),
- skaner antywirusowy,
- analiza z użyciem mechanizmu Sandboxing (Stormshield Breach Fighter),
- filtr SMTP określający reguły filtrowania wiadomości e-mail w odniesieniu do nadawcy lub odbiorcy,
- kontrola komend w ramach protokołu smtp,
- określenie limitów wielkości poczty i liczby odbiorców.

FTP proxy

- skaner antywirusowy,
- analiza z użyciem mechanizmu Sandboxing (Stormshield Breach Fighter),
- możliwość określenia dozwolonych trybów transmisji FTP,
- możliwość kontroli dostępu na podstawie białej / czarnej listy użytkowników FTP,
- kontrola komend w ramach protokołu FTP.

SSL proxy

- skanowanie certyfikatów SSL (sprawdzanie poprawności, filtrowanie dostępu na podstawie CN),

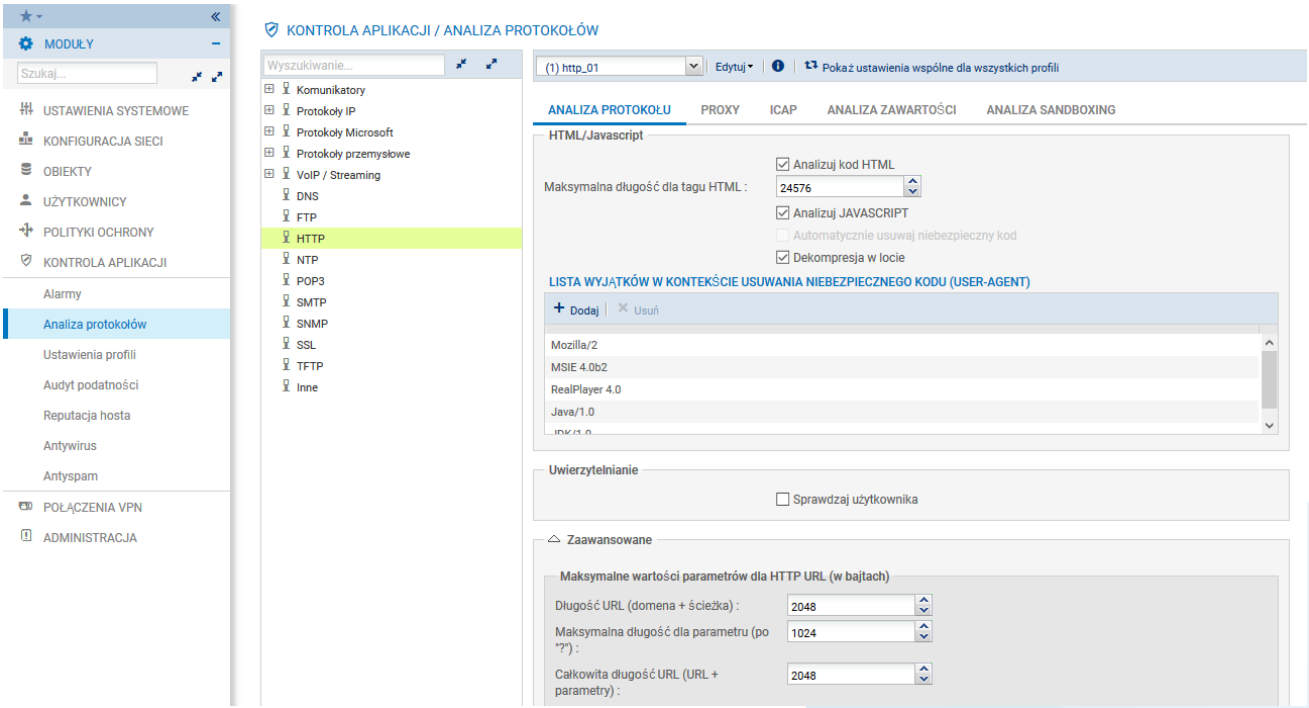
- umożliwienie pozostałym usługom proxy na analizę szyfrowanych wersji protokołów (https, smtps, pop3s).

Uruchomienie proxy odbywa się poprzez włączenie w regule firewall w kolumnie **Polityki filtrowania** jednego z modułów **Filtrowania treści**.

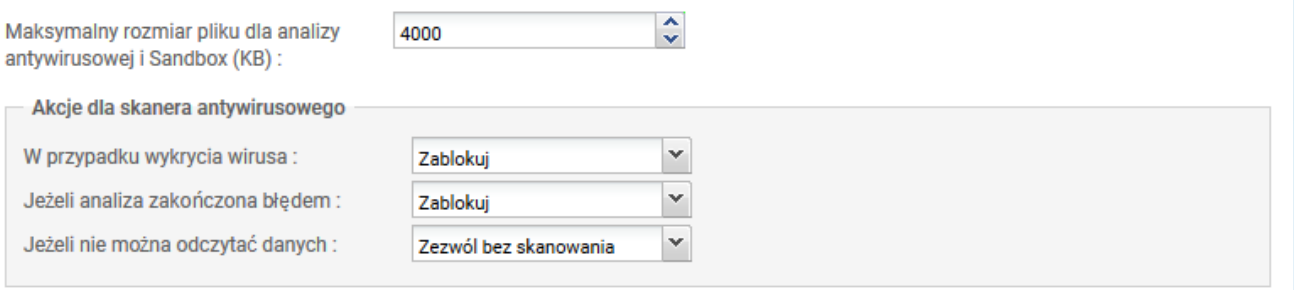
Włączenie skanowania proxy dla reguły firewall jest jednak ostatnim krokiem konfiguracji. Wcześniej należy skonfigurować ogólne ustawienia proxy oraz skanery i filtry, które będą używane podczas skanowania ruchu.

HTTP proxy

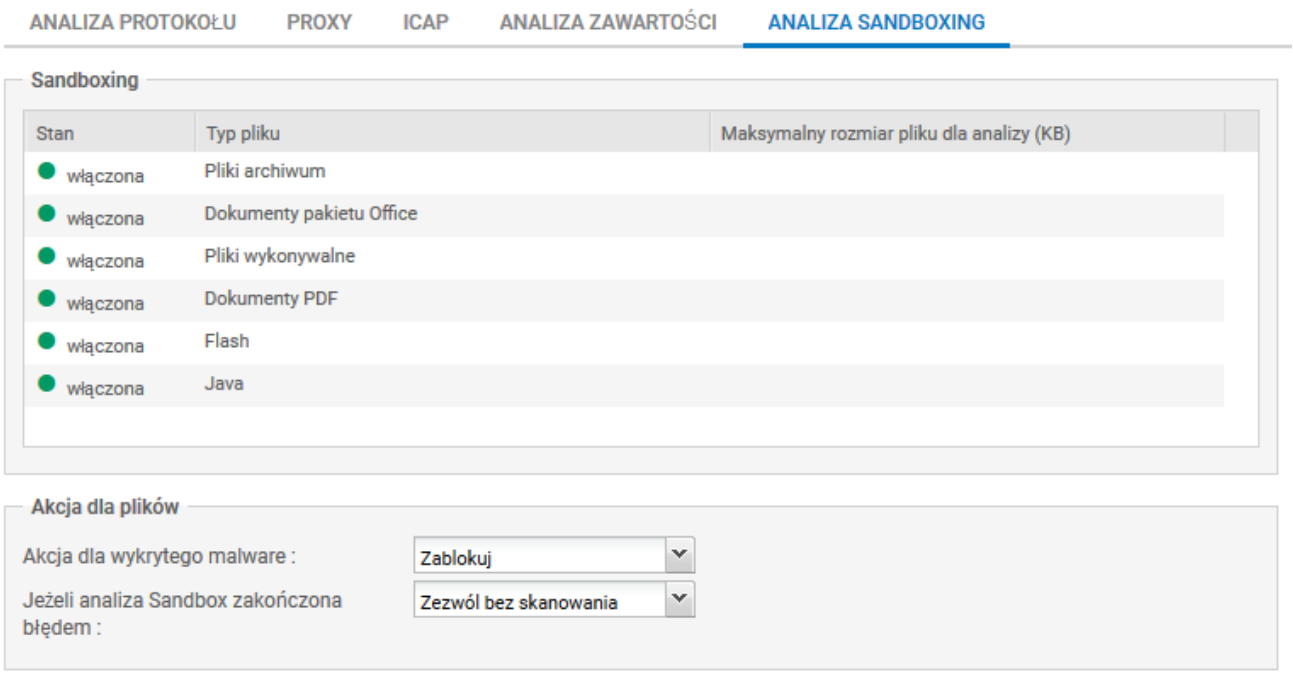
Ogólna konfiguracja proxy http znajduje się w pluginie HTTP a więc w sekcji **KONFIGURACJA > KONTROLA APLIKACJI > Analiza protokołów > HTTP**. Znajduje się tutaj między innymi konfiguracja trybu pracy modułu proxy czy konfiguracja usługi ICAP.



Konfiguracja zakładek **Analiza zawartości** i **Analiza Sandboxing** jest podobna we wszystkich protokołach, dla których można uruchomić proxy i obejmuje konfigurację systemu antywirusowego, tzn. określa **Maksymalny rozmiar pliku dla analizy antywirusowej i Sandbox (kB)** oraz zachowanie systemu AV **w przypadku wykrycia wirusa**, **analizy zakończonej błędem** lub **sytuacji kiedy nie można odczytać danych**.



Z kolei w przypadku Analizy Sandboxing obejmuje możliwość wyłączenia analizy dla wskazanych typów plików oraz definicję podjętej akcji w przypadku **wykrytego malware** lub jeżeli **analiza Sandbox zakończy się błędem.**



W przypadku protokołu http w zakładce **Analiza zawartości** znajdują się funkcje niedostępne w innych protokołach i są to:

- **Częściowe pobieranie plików** – opcja odpowiedzialna za buforowanie danych przed poddaniem ich analizie antywirusowej;
- **Maksymalny rozmiar pliku (kB)** – określenie maksymalnej wielkości pliku jaki będzie można pobrać poprzez protokół http;
- **Filtr pliku ze względu na typ MIME** – pozwala na blokowanie plików określonego typu np. plików audio.

> Uwaga
>
> Jeśli włączona jest analiza AV zalecane jest przełączenie opcji **Częściowe pobieranie plików** na **Zezwól**. W przypadku innej konfiguracji może dojść do problemów z pobieraniem plików np. z aktualizacjami Microsoft czy Adobe.

Konfiguracja filtra URL

Dostęp do stron internetowych można ograniczać wykorzystując wbudowany w urządzenie filtr URL. Do wyboru są następujące filtry URL:

- **baza podstawowa** – 16 kategorii tematycznych,
- **baza podstawowa z polską klasyfikacją stron** – ponad 50 kategorii tematycznych,
- **baza producenta przechowywana w chmurze (Extended Web Control URL**) – ponad 100 mln stron w 65 kategoriach tematycznych,
- klasyfikacja URL stworzona przez administratora.

Konfiguracja klasyfikacji URL znajduje się w zakładce **KONFIGURACJA > OBIEKTY > Klasyfikacja URL**.
W zakładce **Klasyfikacja producenta** można znaleźć informację o tym jaka baza URL jest obecnie wykorzystywana przez urządzenie oraz jakie kategorie tematyczne są dostępne w ramach tej klasyfikacji, a także można z tego poziomu zmienić tą klasyfikację.

> **Wskazówka**
>
> Najprostszym sposobem zmiany klasyfikacji URL na **bazę podstawowa z polską klasyfikacją stron** jest wykonanie kilku poleceń z poziomu konsoli. Zanim jednak polecenia takie będą wykonane należy upewnić się, że w WebGUI *KONFIGURACJA > OBIEKTY > Klasyfikacja URL > Klasyfikacja producenta* ustawiona jest **Podstawowa baza URL**. Po weryfikacji ustawień łączymy się do urządzenia z użyciem protokołu SSH (np. programem PuTTY) i wykonujemy poniższe polecenia:
>
> ```
> setconf ~/ConfigFiles/object Host update.stormshield.pl 91.201.154.218,resolve=dynamic
> setconf ~/ConfigFiles/autoupdate URLFiltering URL http://update.stormshield.pl/1
> setconf ~/ConfigFiles/autoupdate URLFiltering Secure 0
> enobject
> objectsync
> autoupdate -f -t URLFiltering
> ```
>
> Po wydaniu polecenia nastąpi automatyczne pobranie nowej klasyfikacji URL. W kolejnym kroku można rozpocząć konfigurację Filtrowania URL w oparciu o nowe kategorie.

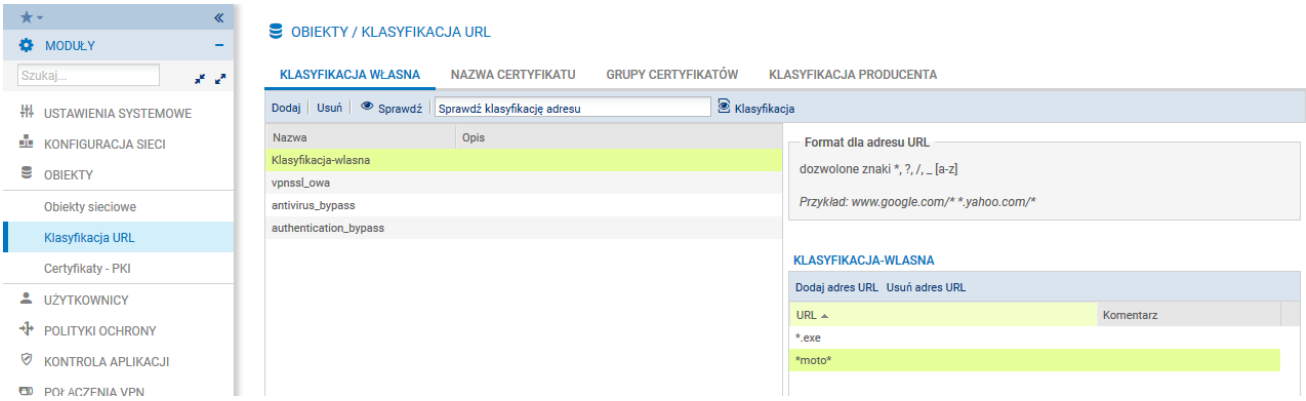
Klasyfikacja URL stworzona przez administratora

Tworzenie własnych grup klasyfikacji polega na określeniu łańcucha znaków, które są porównywane z adresem URL w nagłówku http podczas nawiązania połączenia z serwerem www. Przykładowo aby zablokować wszystkie strony, gdzie w adresie pojawi się łańcuch znaków „moto” należy zdefiniować następujący wpis: **moto**

Tak zdefiniowany wpis *moto* będzie znajdował dopasowanie np. w adresach: *www.motoryzacja.pl*, *www.moto.de*, motory.com.pl, itp.

Innym przykładem zastosowania własnych kategorii URL jest możliwość blokowania plików po ich rozszerzeniach. Jeśli administrator zdefiniuje maskę w formacie **.exe* to pod taki wpis będą znajdowały dopasowanie wszystkie adresy URL kończące się znakami ‘.exe’ a więc adresy będące linkami do plików wykonywalnych exe.

Poniższy zrzut ekranu pokazuje konfiguracje obu przykładów.



Polityka Filtrowania URL

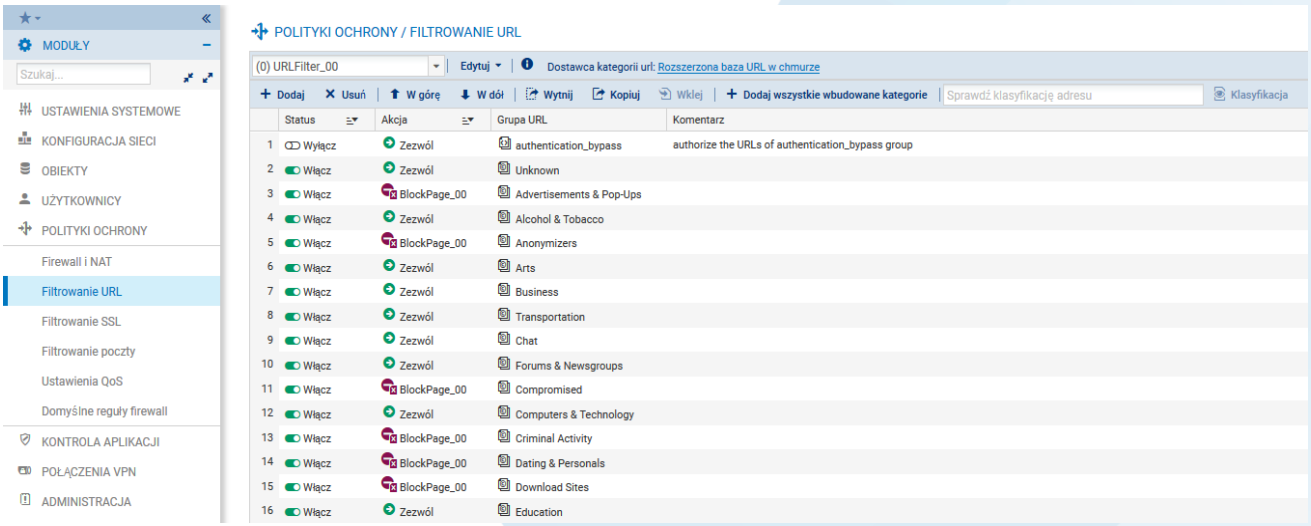
Polityka filtrowania URL określa, jakie kategorie mają być dozwolone a jakie zablokowane w ramach określonego profilu konfiguracji. Profili **Filtrowania URL** jest 10, co umożliwia stworzenie 10 niezależnych zestawów reguł dostępu do stron www. Konfiguracja polityk znajduje się w sekcji **KONFIGURACJA > POLITYKI OCHRONY > Filtrowanie URL**. W ramach polityki możliwe jest zdefiniowanie następujących akcji dla każdej z kategorii:

- **Zezwól** – strony z tej kategorii nie są blokowane;
- **Zablokuj** – dostęp do stron zostanie zablokowany;
- **BlockPage_00** do **BlockPage_03** – dostęp do stron zostanie zablokowany z komunikatem w formie strony www. Do dyspozycji administratora są cztery takie strony, które może dowolnie modyfikować.

Ponadto można skorzystać również z następujących opcji okna konfiguracyjnego:

- **Dodaj wszystkie wbudowane kategorie** – spowoduje wypełnienie listy wszystkimi kategoriami dostępnymi w bazie;
- **Sprawdź klasyfikację adresu** – weryfikuje do jakich kategorii należy wskazana strona WWW.

Poniższy obraz pokazuje przykładową konfigurację polityki filtrowania URL.



Uwaga

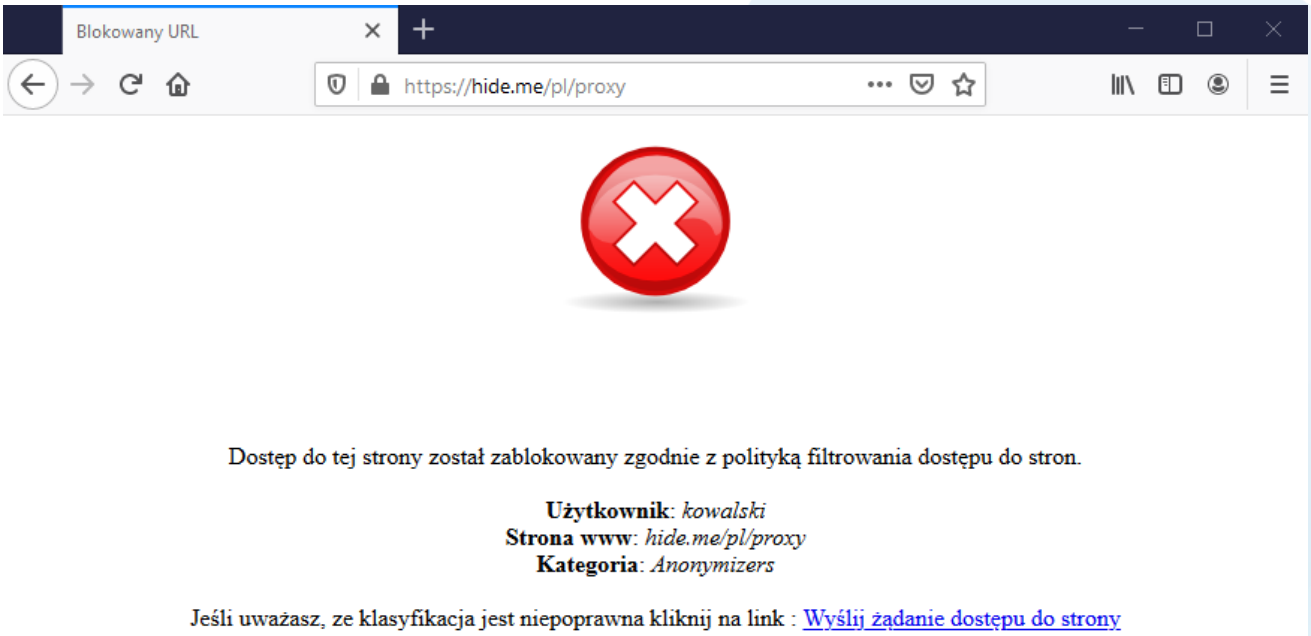
Tak jak w przypadku reguł Firewall i NAT kolejność reguł Filtrowania URL ma znacznie, ponieważ reguły sprawdzane są od pierwszej do ostatniej (kolejność reguł zdefiniowana przez administratora). Jeżeli dana strona należy do więcej niż jednej Grupy URL będzie wykonana akcja zdefiniowana w pierwszej napotkanej regule. Kolejne reguły nie będą przetwarzane.

Wskazówka

Istnieje możliwość zgłoszenia niesklasyfikowanego adresu URL. Dokonać tego można, dla polskiej klasyfikacji URL. Wystarczy wejść na stronę http://www.stormshield.pl/pl/Dodaj_adres_URL.html. Z kolei dla klasyfikacji podstawowej i chmurowej można to zrobić na portalu https://mystormshield.eu/ w sekcji *Technical Support > Report an Netasq / Stormshield URL* lub *Report an Extended Web Control URL* – odpowiednio dla każdej z klasyfikacji. Po podaniu adresu URL należy zaproponować kategorie, do których strona powinna przynależeć. Po zweryfikowaniu poprawności zaproponowanej klasyfikacji strona zostanie dodana do właściwej klasyfikacji.

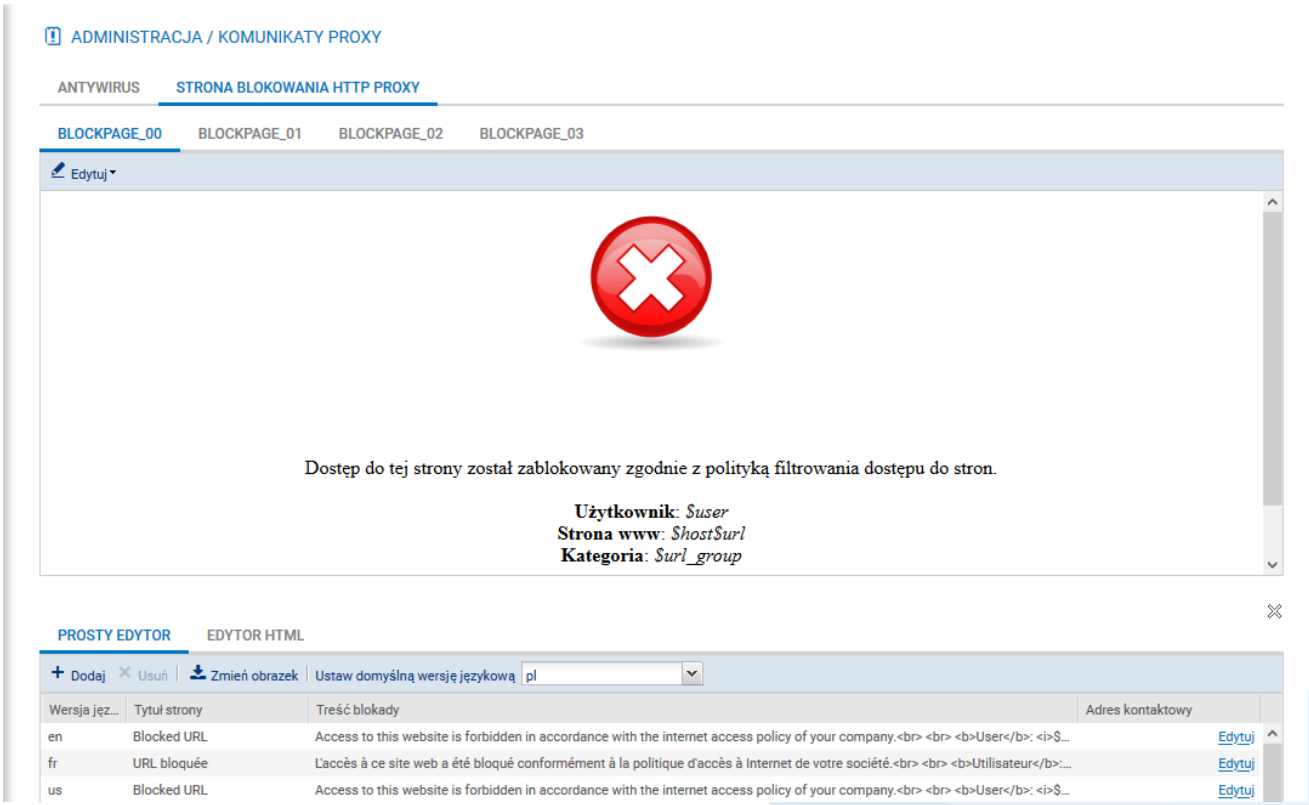
Strona blokowania

Strona blokowania jest stroną zdefiniowana w języku html. Będzie się ona pojawiała użytkownikom próbującym wejść na stronę, do której nie mają dostępu.



Dużą zaletą stosowania strony blokowania jest możliwość zdefiniowania własnego komunikatu, dzięki któremu użytkownik dowie się o powodzie blokady oraz uzyska informację o tym jak zgłosić stronę do odblokowania.

Modyfikację strony blokowania można wykonać w KONFIGURACJA > ADMINISTRACJA > Komunikaty proxy > Strona blokowania http proxy.

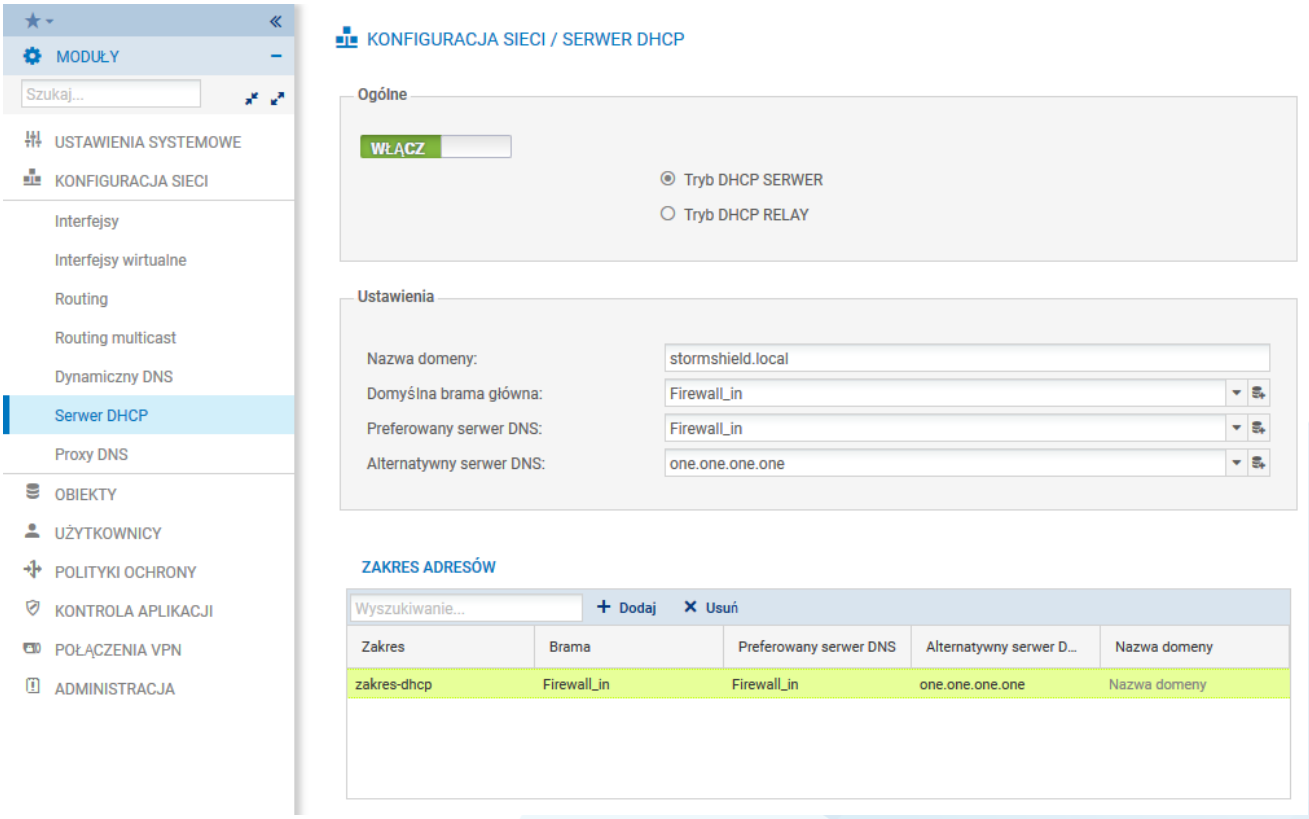


15. Konfiguracja serwera DHCP

Serwer DHCP służy do przydzielania adresów IP komputerom w sieci LAN. Konfiguracji DHCP można dokonać w zakładce KONFIGURACJA > KONFIGURACJA SIECI > Serwer DHCP.

> **Uwaga**
>
> W domyślnej konfiguracji STORMSHIELD UTM usługa serwera DHCP jest włączona. W przypadku posiadania drugiego serwera DHCP (uruchomionego w tej samej sieci) może to spowodować konflikt w sieci i doprowadzić do jej niestabilnego działania.

W pierwszej kolejności należy skonfigurować to jak STORMSHIELD UTM będzie działał – czy jako DHCP SERWER, czy też ma być jedynie przekaźnikiem (DHCP RELAY) dla zapytań DHCP do innego serwera DHCP w sieci.

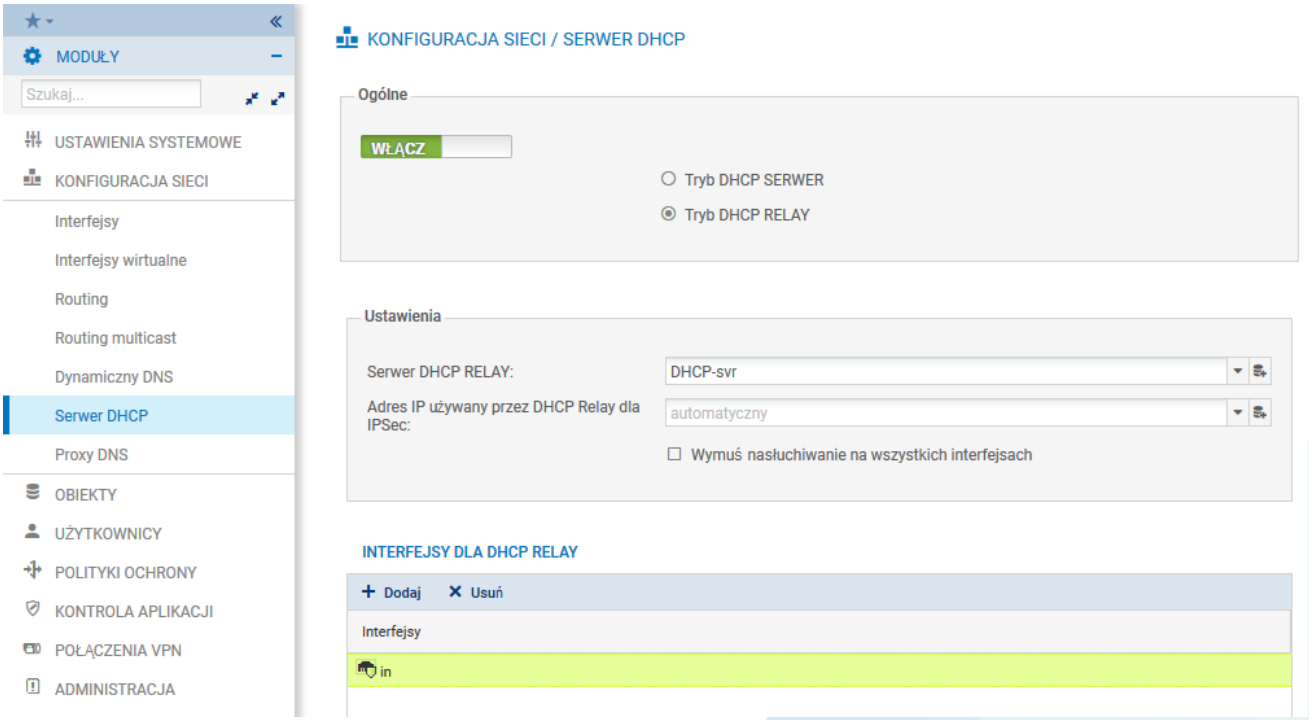


W trybie pracy DHCP SERWER możemy skonfigurować odpowiednie parametry pracy usługi tj.:

- Domyślna brama główna – domyślna brama dostępu do Internetu dla hostów sieci LAN. Obiekt ten powinien być wewnętrznym adresem IP STORMSHIELD UTM;
- Preferowany, Alternatywny serwer DNS – podstawowy i zapasowy serwer DNS;
- ZAKRES ADRESÓW – wskazujemy, z jakiego zakresu serwer DHCP będzie przydzielał dynamiczne adresy IP. Jeśli STORMSHIELD UTM obsługuje wiele podsieci, dla każdej z nich można utworzyć odpowiedni zakres adresów IP, w kolumnie Brama należy wtedy wskazać właściwy dla tej podsieci obiekt reprezentujący adres bramy domyślnej oraz odpowiednie serwery DNS;

- KONFIGURACJA STATYCZNYCH REZERWACJI DHCP – pozwala skonfigurować usługę serwera DHCP w taki sposób, aby komputer, o konkretnym adresie MAC mógł otrzymać zawsze ten sam adres IP. Aby to uzyskać muszą być spełnione następujące warunki:
  - Komputer musi być reprezentowany przez obiekt typu Host zawierający adres IP oraz adres MAC.
  - Adres IP tego komputera nie może należeć do zakresu adresów rozgłaszanych przez serwer DHCP (czyli tych zdefiniowanych w ramach ZAKRESU ADRESÓW).

Tryb DHCP RELAY służy do przekazywania zapytań DHCP do istniejącego w sieci, innego serwera DHCP. Polega to na tym, że STORMSHIELD UTM nasłuchuje zapytań DHCP na wszystkich lub na wskazanych w sekcji INTERFEJSY DLA DHCP RELAY interfejsach sieciowych i jeżeli natrafi na zapytanie o adres IP, to przekazuje je do serwera określonego w polu Serwer DHCP RELAY.



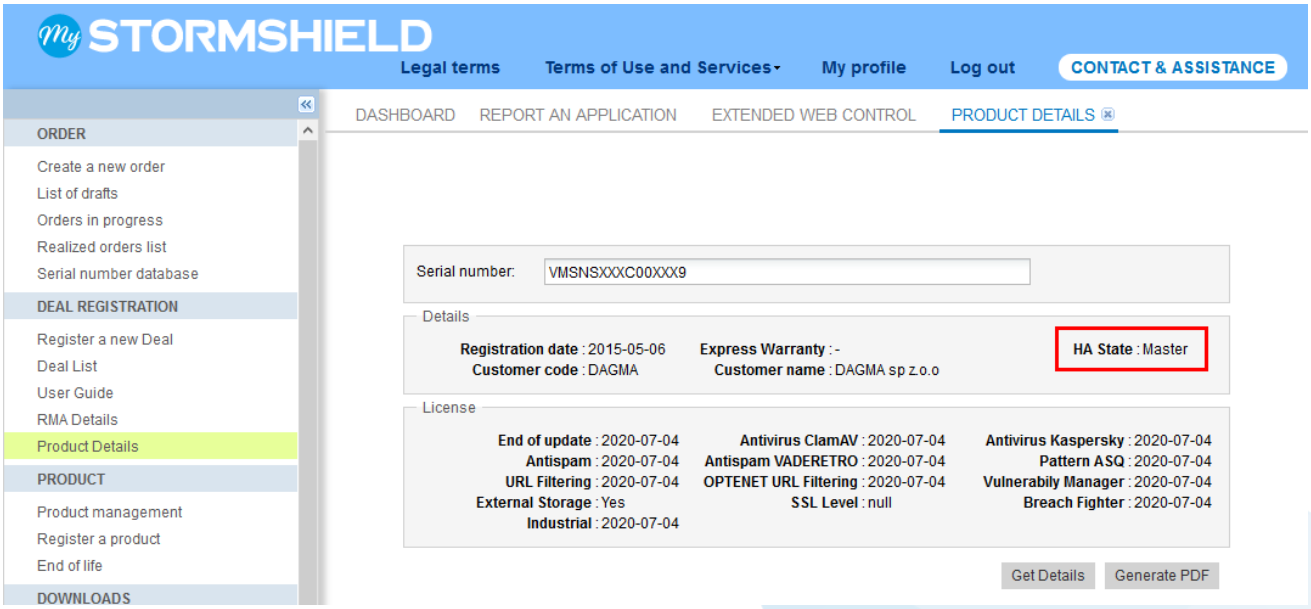
Wskazówka

Informację o aktualnych dzierżawach adresów IP przez hosty można uzyskać w zakładce MONITORING > MONITOROWNIE> DHCP.

16. Klaster wysokiej dostępności (HA)

Klaster HA są to dwa połączone ze sobą urządzenia STORMSHIELD UTM w celu zapewnienia ciągłości pracy sieci w przypadku awarii jednego z tych urządzeń. Klaster w rozwiązaniach STORMSHIELD jest klastrem typu **Active/Passive** co oznacza, że całość ruchu jest filtrowana przez jedno urządzenie (Active) podczas gdy drugie (Passive) jest gotowe do przejęcia ruchu w przypadku wykrycia niedostępności pierwszego lub obniżenia jego sprawności działania (zmniejszonej ilości aktywnych interfejsów sieciowych).

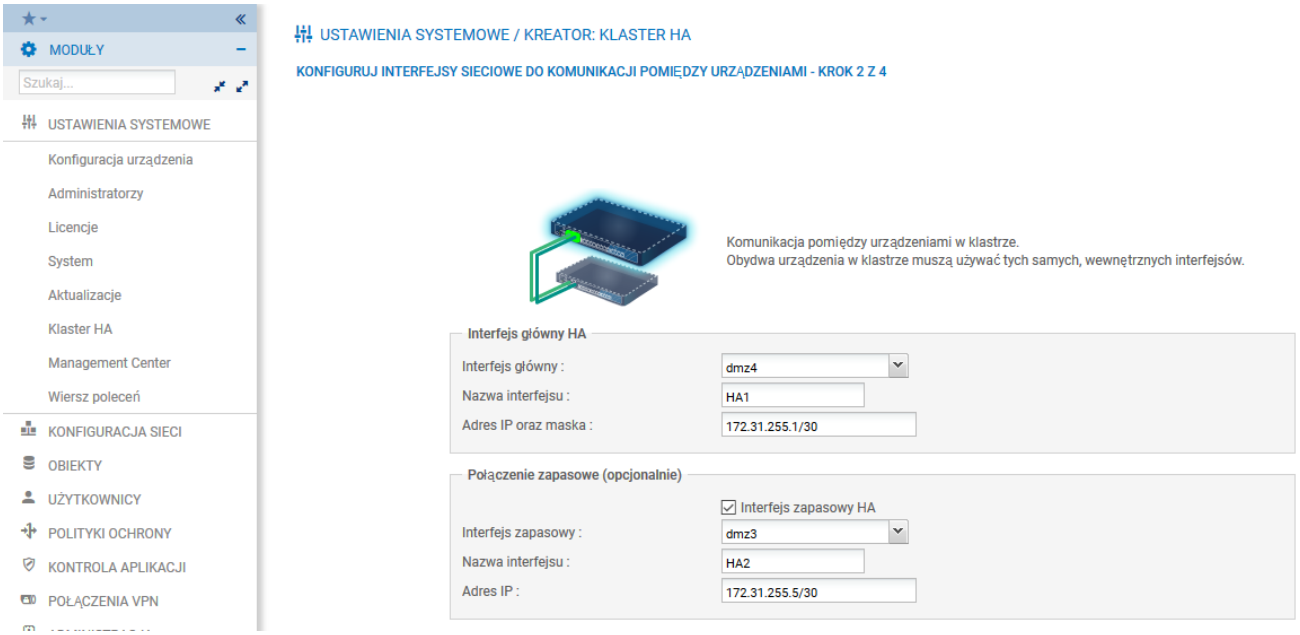
Aby podłączyć dwa urządzenia w klaster wymagane jest wygenerowanie na każdym z nich odpowiedniej licencji, tj. licencji typu **Master/Slave**. Można sprawdzić czy urządzenia mają licencje Master lub Slave logując się do portalu https://mystormshield.eu. Poniżej przykład takiej licencji:



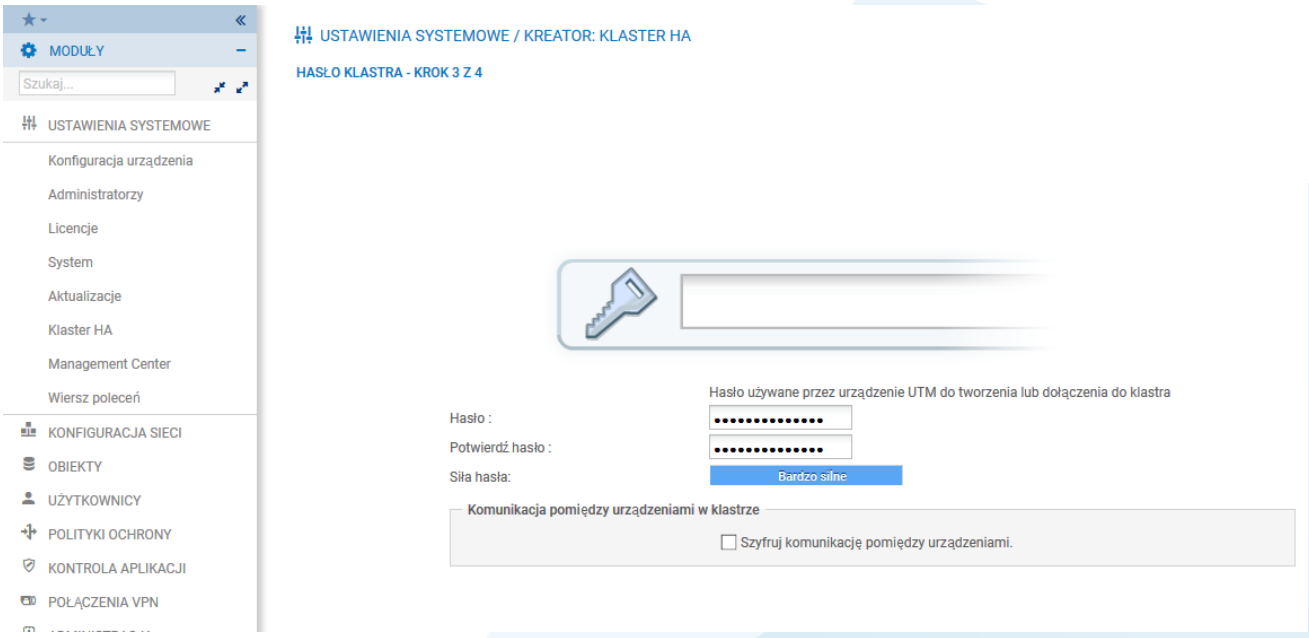
W celu skonfigurowania klastra HA należy na urządzeniu Master wejść na zakładkę **USTAWIENIA SYSTEMOWE > Klaster HA** i wybrać opcję **Utwórz klaster**. W kolejnym kroku należy wybrać interfejs sieciowy, który będzie używany do komunikacji pomiędzy urządzeniami (m.in. tzw. heartbeat) oraz skonfigurować adresację sieciową dla tego interfejsu.

Urządzenia w klastrze HA mogą komunikować się wykorzystując jeden lub dwa interfejsy sieciowe. W celu uniknięcia problemów z połączeniem zalecane jest łączenie urządzeń bezpośrednio bez użycia przełączników czy innych urządzeń sieciowych mogących powodować opóźnienia w komunikacji.

> **Uwaga**
>
> Ponieważ klastra HA nie można wyłączyć z poziomu interfejsu urządzenia i aby wyłączyć działanie HA należy zrestartować urządzenia do ustawień fabrycznych bądź odtworzyć backup konfiguracji, który nie zawiera informacji o konfiguracji HA – zachęcamy do wykonania backupu konfiguracji obu urządzeń przed połączeniem ich w klaster HA.



W kolejnym oknie kreatora należy skonfigurować hasło, które będzie używane do autoryzacji urządzeń i w razie potrzeby włączyć szyfrowanie komunikacji pomiędzy urządzeniami.

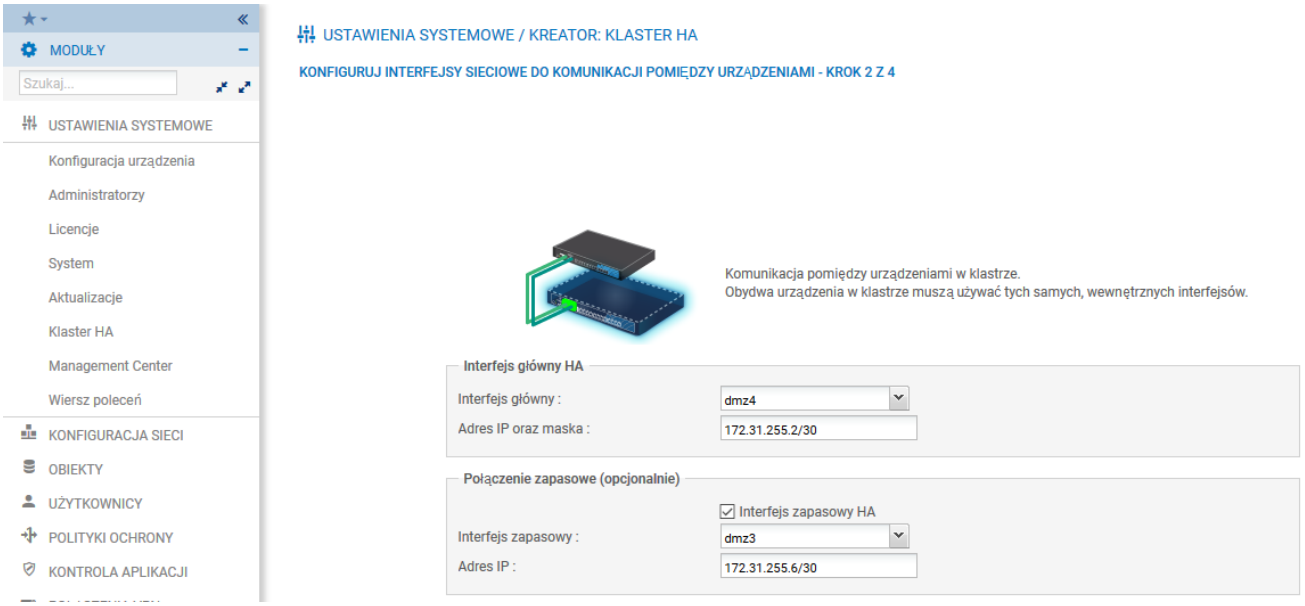


Ostatni krok kreatora kończy się przejściem urządzenia w tryb Master i oczekiwania na urządzenie Slave.

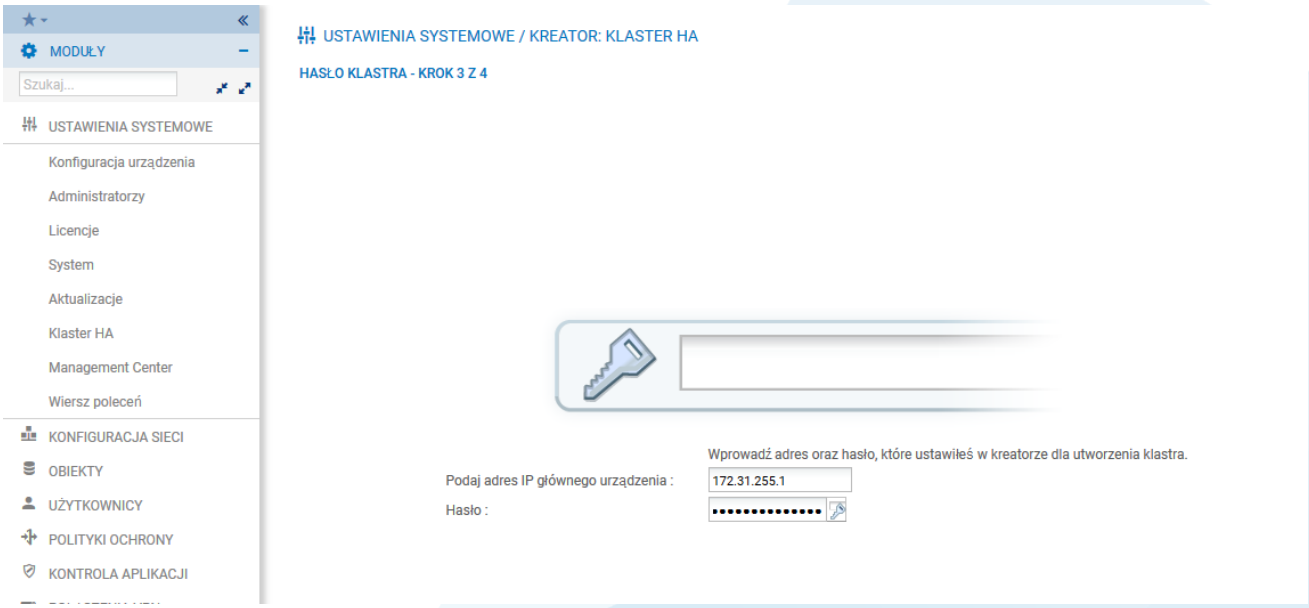
Uwaga

Domyślnie komunikacja pomiędzy urządzeniami w klastrze jest nie szyfrowana. Powodem tego jest fakt, że jest to dedykowane, bezpośrednie połączenie między urządzeniami działającymi w klastrze HA. Włączenie opcji szyfrowania połączenia HA może obniżyć wydajność klastra HA.

Na urządzeniu Slave należy w oknie kreatora konfiguracji HA wybrać opcję **Dołącz do klastra** a następnie skonfigurować interfejs do połączenia urządzeń. W kolejnym oknie kreatora należy wskazać adres IP urządzenia Master,



a następnie podać hasło do zabezpieczenia komunikacji (to samo, które zostało zdefiniowane na urządzeniu Master).

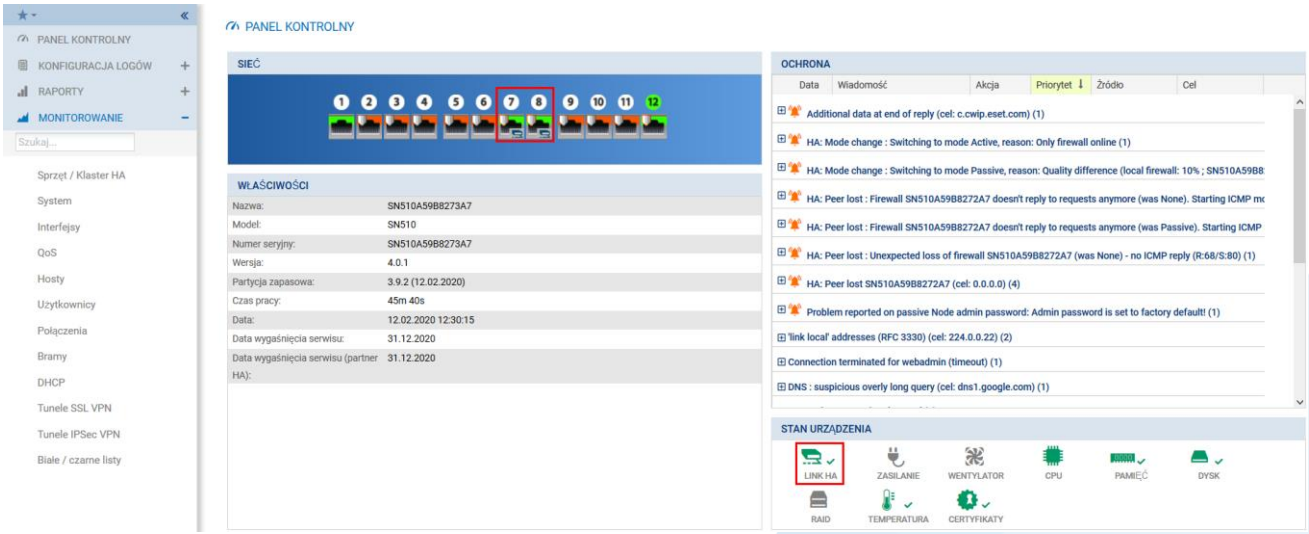


Zakończenie pracy kreatora spowoduje restart urządzenia Slave i dołączenie go do klastra HA.

Synchronizacja konfiguracji możliwa jest poprzez użycie przycisku  146 - **Synchronizuj urządzenie pasywne z bieżącą konfiguracją** dostępnego w górnym menu interfejsu administracyjnego lub podczas wylogowania z urządzenia, dlatego niezalecane jest kończenie pracy z interfejsem administracyjnym bez poprawnego wylogowania z GUI.

> **Uwaga**
>
> Po każdej zmianie w konfiguracji urządzenia Master należy pamiętać o tym aby zsynchronizować klaster HA poprzez kliknięcie na powyższej ikonie synchronizacji.
> Urządzenia nie wykonują tej czynności automatycznie z powodów bezpieczeństwa (gdyby administrator pomylił się w konfiguracji urządzenia Master, co spowodowałoby awarię sieci bądź niedostępność usług i synchronizacja odbywała się automatycznie, to ta pomyłka zostałaby powielona na urządzeniu Slave).

Jeśli klaster działa poprawnie to stosowna informacja wyświetlona będzie w Panelu kontrolnym,



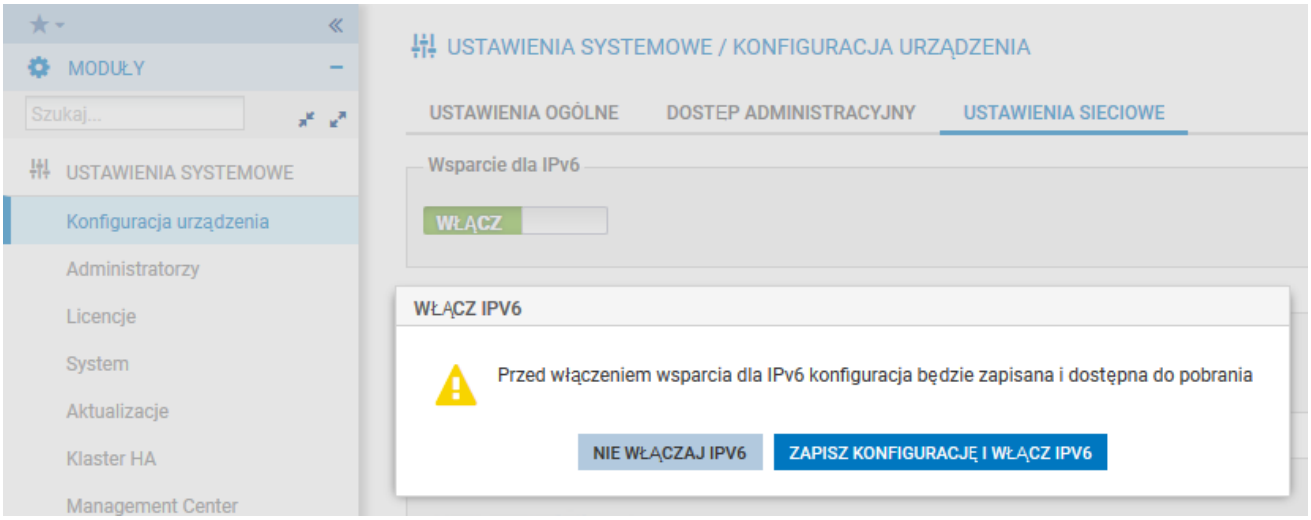
Po kliknięciu ikony **LINK HA** zostanie otwarta strona z podsumowaniem stanu klastra HA.


PANEL KONTROLNY
KONFIGURACJA LOGÓW
RAPORTY
MONITOROWANIE
Szukaj...
Sprzęt / Klaster HA
System
Interfejsy
QoS
Hosty
Użytkownicy
MONITOR / SPRZĘT / KLASTER HA
SPRZET
SZCZEGÓŁY KLASTRA HA
Wskaźnik
Lokalny firewall
Zdalny firewall
Ustawienia
Status
Active
Passive
Wersja
4.0.1
4.0.1
Stan wymuszony
No
No
Indeks jakości
20
Priorytet
Synchronizacja konfiguracji
Zsynchronizowane
Zsynchronizowane
Stan łącza HA
OK
OK
Stan zapasowego łącza HA
OK
OK
Ustawienia zaawansowane

17. Wsparcie dla protokołu IPv6

Wszystkie urządzenia z serii STORMSHIELD UTM wspierają natywnie protokół IPv6, jednak opcja ta jest domyślnie wyłączona.

Aby aktywować tą funkcjonalność należy w menu **KONFIGURACJA > USTAWIENIA SYSTEMOWE > Konfiguracja urządzenia > Ustawienia sieciowe** wcisnąć przycisk **Włącz** w sekcji Wsparcie dla IPv6.



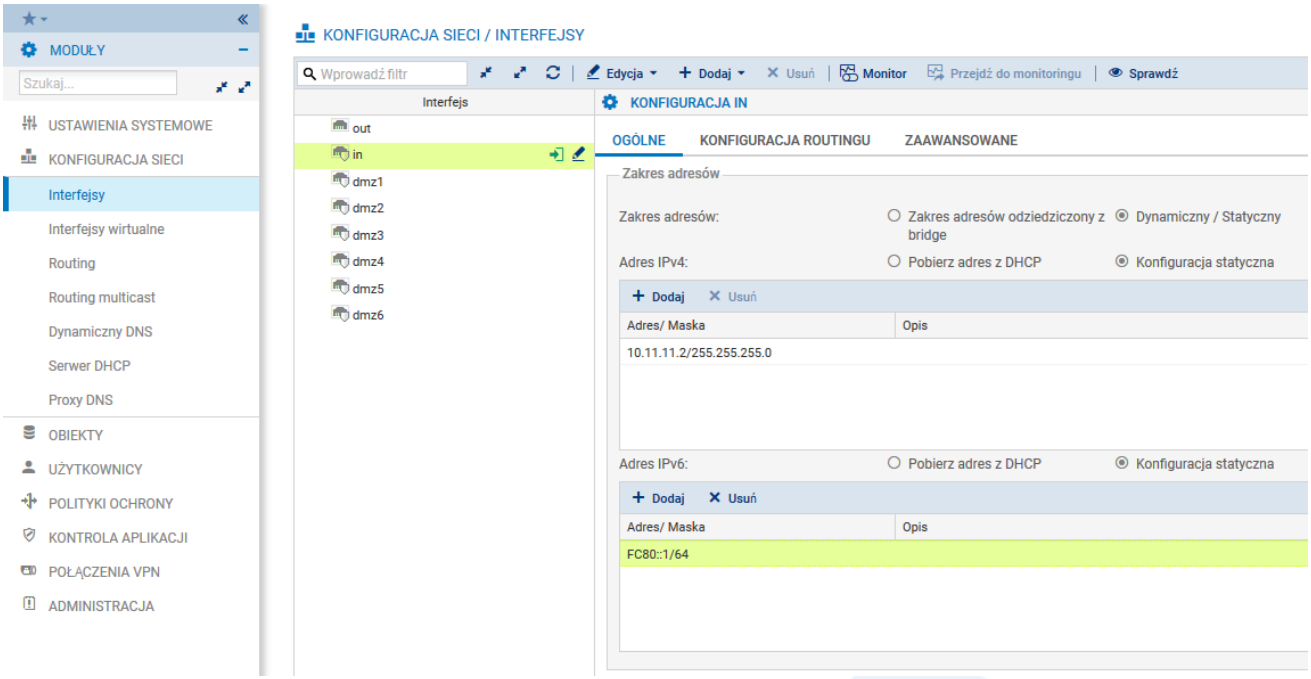
Aktywacja obsługi IPv6 spowoduje automatyczne zapisanie i wyeksportowanie obecnej konfiguracji dla IPv4, po czym nastąpi ponowne uruchomienie urządzenia.

Konfiguracja urządzenia nie ulegnie zmianie, wszystkie wcześniej zdefiniowane moduły będą działały w taki sam sposób jak przed aktywacją, natomiast pojawią się nowe opcje konfiguracyjne m.in.:

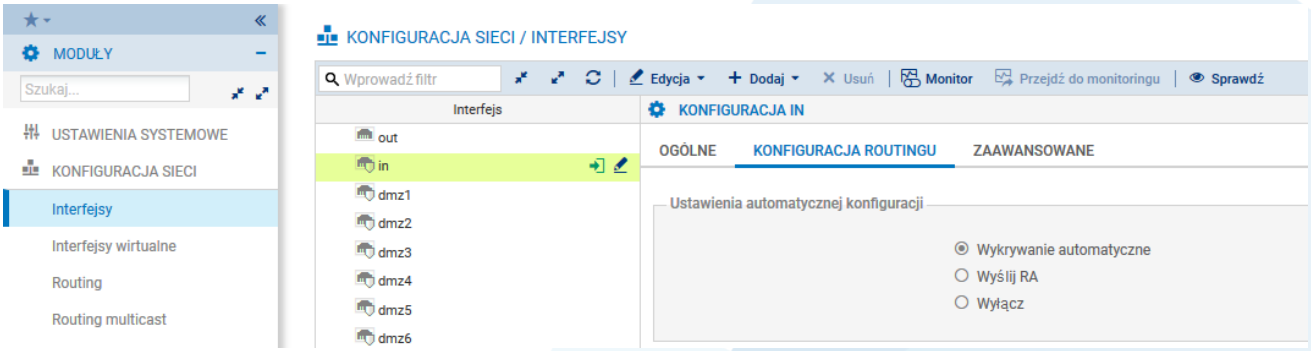
> **Uwaga**
>
> Po włączeniu obsługi protokołu IPv6 nie można jej wyłączyć w inny sposób niż przez przewrócenie ustawień fabrycznych bądź wczytanie backupu konfiguracji urządzenia wykonanego przed włączeniem obsługi protokołu IPv6.

Konfiguracja interfejsów sieciowych IPv6

Po włączeniu obsługi protokołu IPv6 w trybie edycji interfejsu (zakładka **Ogólne**) pojawi się sekcja **Adres IPv6**, gdzie będzie możliwość skonfigurowania adresu IPv6.



Dodatkowo pojawi się nowa zakładka **Konfiguracja routingu,** której opcje są odpowiedzialne za informowanie innych hostów w sieci IPv6 o obecności urządzenia co ułatwia lokalną komunikację.

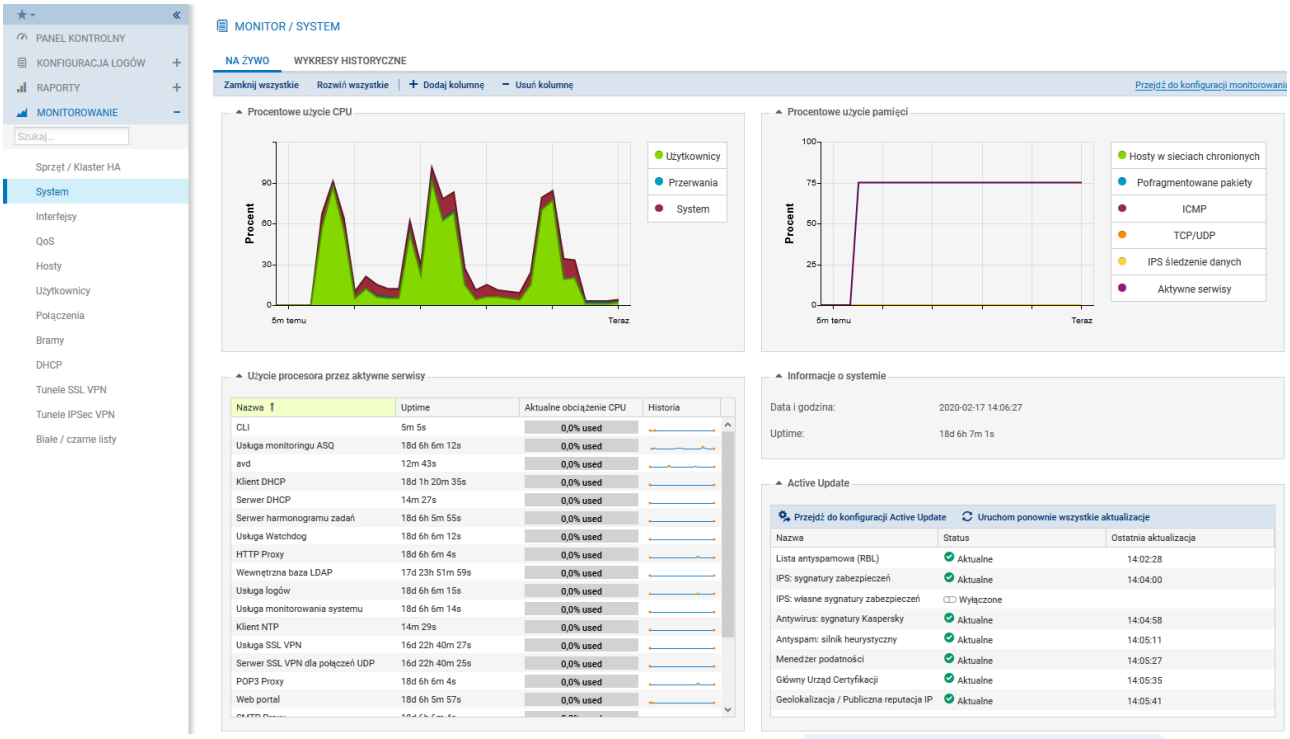


Pozostała konfiguracja związana z IPv6 jest rozsiana po całym urządzeniu m.in. w sekcjach:

- routing,
- serwer DHCP,
- konfiguracja obiektów,
- reguły filtrowania firewall,
- IPsec.

18. MONITOROWANIE

Urządzenie STORMSHIELD UTM umożliwia monitorowanie pracy urządzenia oraz stanu sieci z poziomu WebGUI.



Z poziomu menu **MONITORING > MONITOROWANIE** mamy dostęp do szeregu informacji na temat bieżącej pracy urządzenia takich jak:

- **Sprzęt / Klaster HA** – temperatura urządzenia oraz stan klastra HA;
- **System** – obciążenie procesora i pamięci RAM urządzenia, Uptime urządzenia, Uptime i obciążenie poszczególnych usług, stan aktualizacji poszczególnych modułów urządzenia;
- **Interfejsy** – użyte pasmo oraz ilość połączeń na poszczególnych interfejsach. Włączenie monitoringu na danym interfejsie można wykonać w **KONFIGURACJA > ADMINISTRACJA > Konfiguracja monitoringu > Konfiguracja interfejsu**;
- **QoS** – użyte pasmo poszczególnych kolejek QoS. Włączenie monitoringu kolejki QoS można wykonać w **KONFIGURACJA > ADMINISTRACJA > Konfiguracja monitoringu > Konfiguracja QoS**.
- **Hosty** – aktywne hosty, których połączenia przychodzą do lub przez urządzenie STORMSHIELD UTM, ich reputacja, użyte pasmo, ilość wysłanych/odebranych danych, geolokalizacja, reputacja IP, wszystkie połączenia danego wybranego hosta, podatności, aplikacje i usługi wykryte na hoście, a także dodatkowe informacje o hoście i historia jego reputacji.
  Po kliknięciu prawym przyciskiem myszy na nazwie wybranego hosta pojawi się menu kontekstowe umożliwiające dodatkowe działania takie jak:
  - **Wyszukaj frazę we wszystkich logach** – wyszukuje wpisy dotyczące wybranego hosta w logach;
  - **Sprawdź hosta** – wskazuje pozycje konfiguracji, w których użyty jest wskazany host;
  - **Pokaż szczegóły hosta** – szczegółowe informacje o hoście;

- **Umieść na czarnej liście** (1, 5, 30 minut, 3 godziny) – blokuje komunikację hosta na wskazany czas;
- **Skopiuj wybrany wiersz do schowka;**
- **Dodaj nowy host a następnie dodaj go do grupy** – umożliwia utworzenie obiektu typu host o adresie IP oraz MAC wybranego hosta oraz dodanie go do Grupy IP;

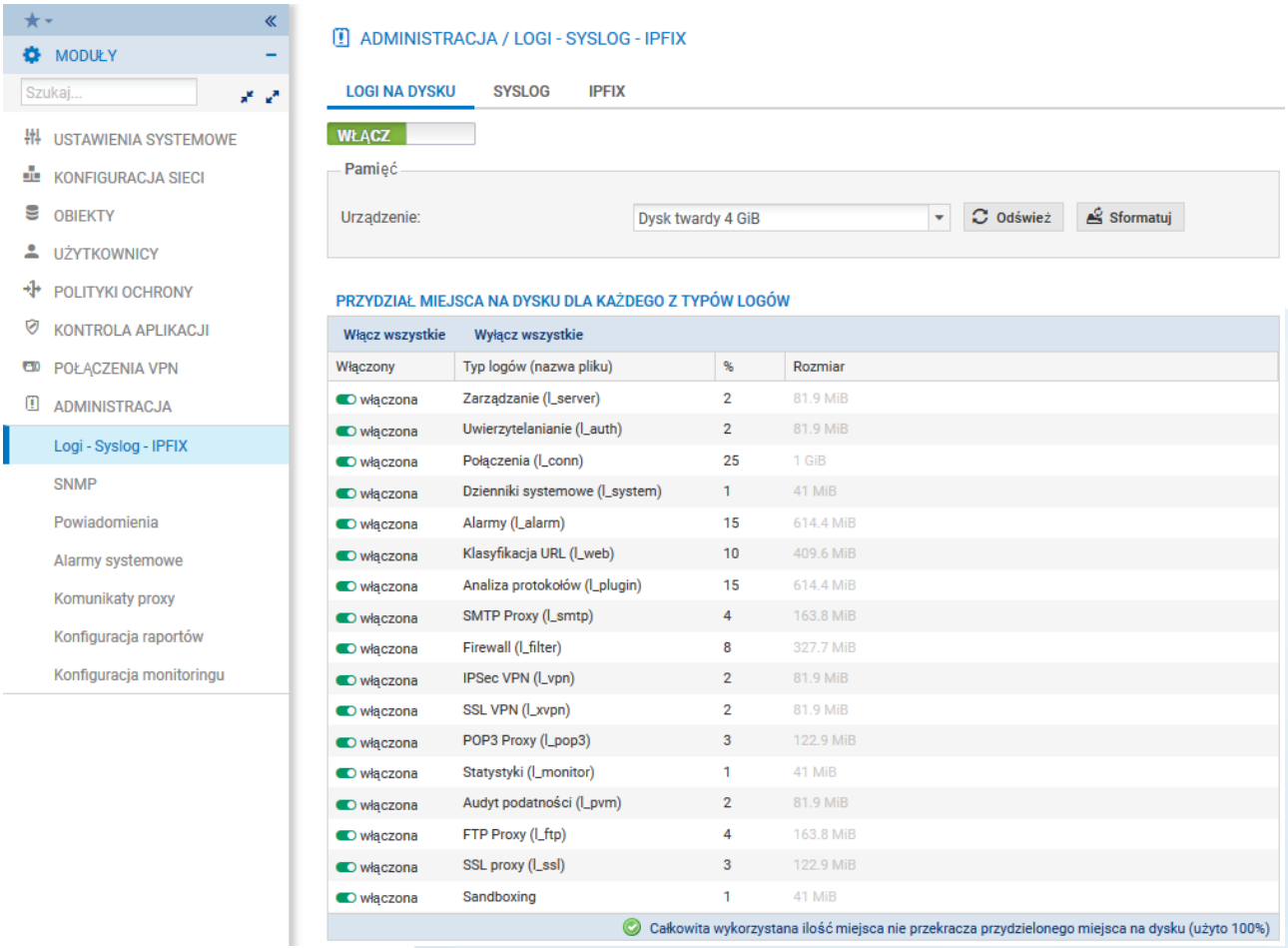
- **Użytkownicy** – informacje o zautentykowanych użytkownikach, adresach IP stacji, na których użytkownik się zautentykował, bazie użytkowników, grupie, dacie wygaśnięcia autentykacji, metodzie uwierzytelnienia, przynależności do grupy administratorów urządzenia Stormshield, uprawnieniach dostępu do usług VPN, wszystkich połączeniach zainicjowanych przez użytkownika oraz podatnościach, aplikacjach usługach i informacjach dotyczących hostów, na których dany użytkownik jest zalogowany.
  Podobnie jak w przypadku hostów także tutaj dostępne jest menu kontekstowe z dodatkowymi opcjami dotyczącymi użytkowników;
- **Połączenia** – informacje o wszystkich trwających połączeniach przechodzących przez urządzenie;
- **Bramy** – monitoring routerów użytych w konfiguracji routingu urządzenia STORMSHIELD UTM takich jak: obiekty typu router, brama domyślna, bramy użyte w routingu na podstawie reguł (PBR) i trasy powrotne;
- **DHCP** – lista hostów, które uzyskały adres IP z lokalnego serwera DHCP;
- **Tunele SSL VPN** – lista hostów, które zestawiły połączenie z urządzeniem STORMSHIELD UTM poprzez tunel SSL VPN;
- **Tunele IPsec VPN** – lista tuneli VPN w aktywnej polityce IPsec VPN. W sekcji **Polityki** widoczny jest stan poszczególnych tuneli (zestawiony lub nie), informacje o sieci i bramie zdalnej oraz lokalnej. W sekcji **Tunele** dostępne są bardziej szczegółowe informacje o zestawionych tunelach m.in. ilość przesłanych danych, czas życia tunelu, oraz użyte algorytmy szyfrowania i autentykacji;
- **Białe / czarne listy** – lista hostów, które trafiły na białe lub czarne listy urządzenia. Jeśli host np. błędnie trafił na czarną listę, można po wskazaniu takiego hosta usunąć go z tej listy klikając przycisk **Usuń element z czarnej listy**.

19. LOGI

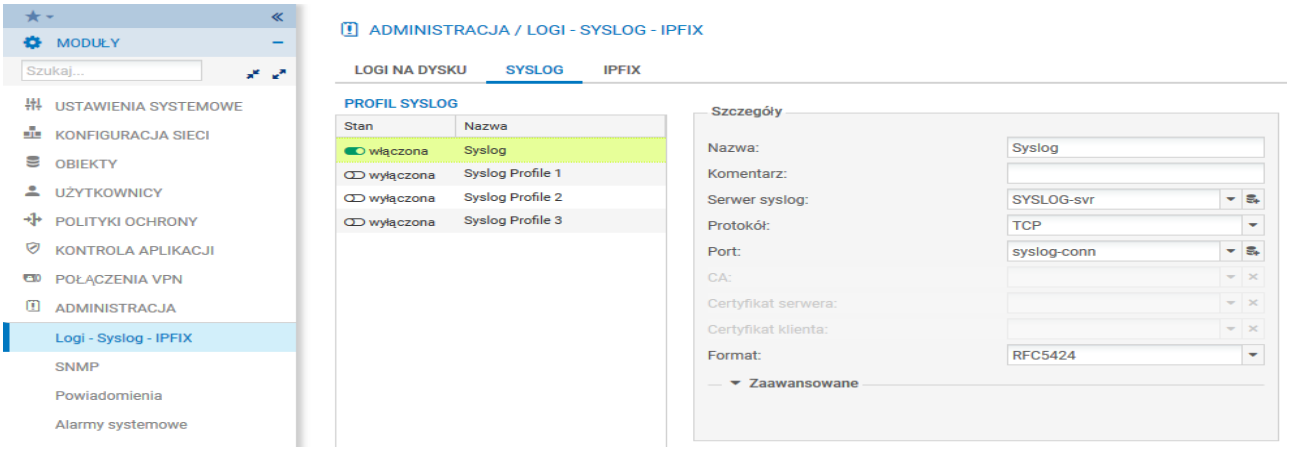
Logowanie zdarzeń

Wszystkie urządzenia STORMSHIELD UTM wyposażone w nośnik danych umożliwiają zapisywanie zdarzeń związanych z ruchem sieciowym oraz z pracą samego urządzenia. Urządzenia posiadające wbudowany dysk twardy tj. SNi40, SN510 oraz wszystkie wyższe modele są w stanie przechowywać logi bezpośrednio w pamięci urządzenia. W przypadku mniejszych modeli tj. SN160(W), SN210(W) i SN310 możliwa jest instalacja karty SD (co najmniej Class 10, UHS Class 1 (U1) lub App Performance 1 (A1) – SDHC lub SDXC) o maksymalnej pojemności 2TB. Producent rekomenduje użycie kart o wysokiej wytrzymałości / przemysłowych lub najlepiej tych, które mają wbudowany układ flash MLC opracowany przez wiodące marki (np. SanDisk, Western Digital, Innodisk, Transcend, itp.).

Domyślnie wszystkie logi są zapisywane, jednak w sekcji **KONFIGURACJA > ADMINISTRACJA > Logi – Syslog – IPFIX > Logi na dysku** można wyłączyć niektóre kategorie bądź zmniejszyć procentową rezerwację miejsca na poszczególne dzienniki na dysku (kolumna %).

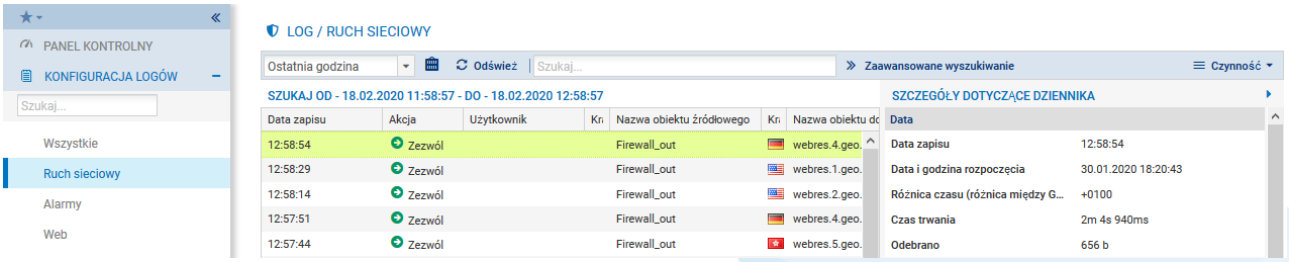


Możliwa jest także konfiguracja do 4 zewnętrznych serwerów syslog (zakładka **Syslog**), na które będą wysyłane logi.



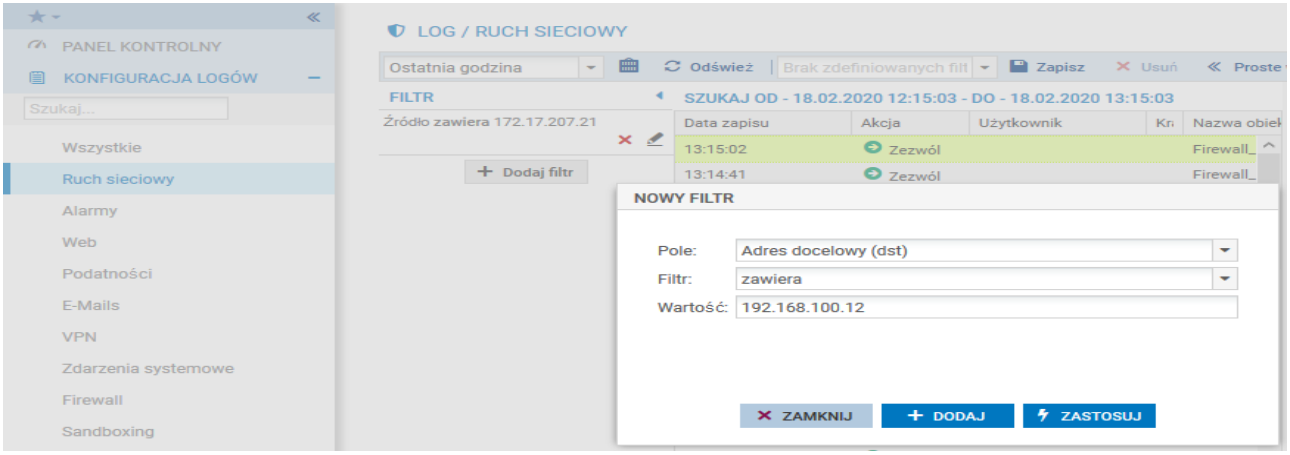
Przeglądanie logów

Logi gromadzone na urządzeniu dostępne są w **MONITORING > LOGI**. To menu dostępne jest jedynie na urządzeniach wyposażonych w nośnik danych. Można tu przeglądać logi gromadzone na urządzeniu grupowane w dziennikach takich jak: Ruch sieciowy, Alarmy, Web, Podatności, E-Mails, VPN, Zdarzenia systemowe, Firewall, Sandboxing, Użytkownicy.

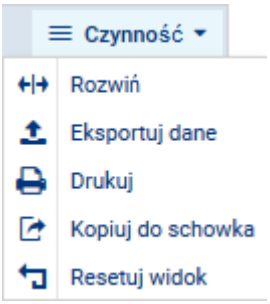


Po przejściu do widoku logów pojawi się tabela zawierająca poszczególne wpisy wybranego dziennika. W górnej części interfejsu można wybrać predefiniowany przedział czasu z jakiego chcemy przeglądać logi lub wskazać własny klikając ikonę **Zmień zakres czasu**.

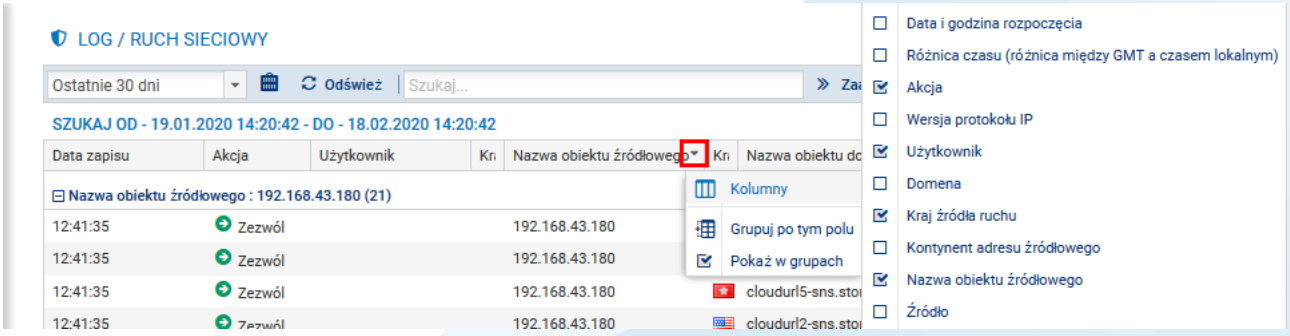
Przycisk **Odśwież** ponownie odczytuje zapisane logi. W polu szukaj można wprowadzić dowolny ciąg znaków wg. którego urządzenie STORMSHIELD UTM ma przefiltrować listę logów – może to być np. nazwa użytkownika, nazwa lub adres obiektu źródłowego bądź docelowego, nazwa lub nr portu, itp. Po wybraniu opcji **Zaawansowane wyszukiwanie** będzie można wskazać szczegółowe kryteria wyszukiwania, a także zapisać utworzony szablonu wyszukiwania lub wskazać wcześniej przygotowany szablon.



Po prawej stronie górnego menu pod przyciskiem **Czynność** można wykonać eksport logów z bieżącego widoku do pliku CSV, wydrukować go lub skopiować do schowka.



W części głównej widoku logów wyświetlane są poszczególne wpisy dziennika. Domyślny widok wyświetla najbardziej niezbędne informacje. Jednak można dostosować rodzaj wyświetlanych informacji po najechaniu wskaźnikiem myszki na nagłówek dowolnej kolumny i kliknięciu na trójkąt pojawiający się w prawej części nagłówka kolumny – dzięki temu będzie można zmodyfikować liczbę wyświetlanych kolumn.



Po kliknięciu wiersza wpisu dziennika po prawej stronie pojawi się okno zawierające pełne informacje zawarte w tym konkretnym wpisie.

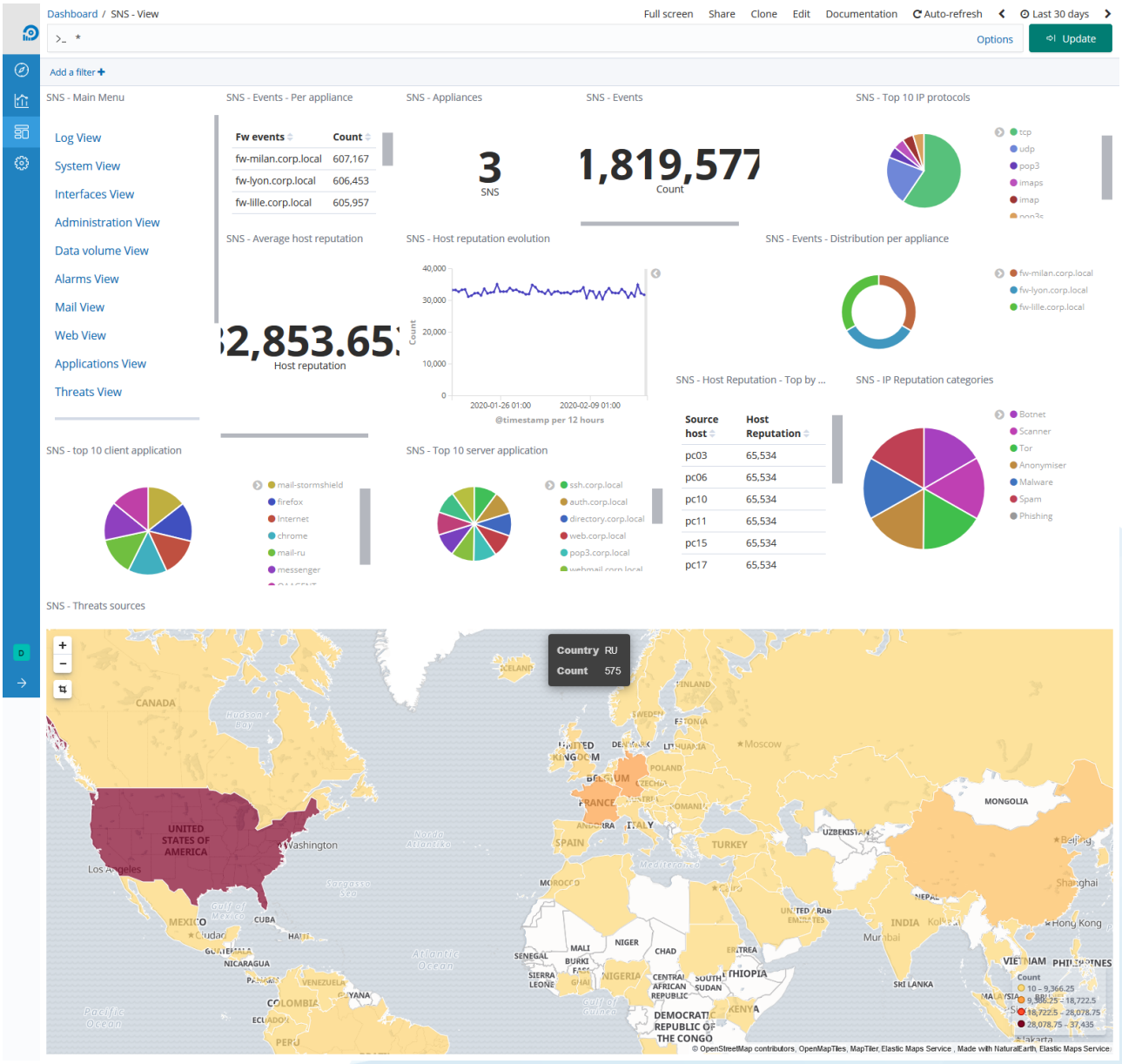
Uwaga

Aby zachować zgodność z europejskim rozporządzeniem RODO (Ogólne rozporządzenie o ochronie danych), dane wrażliwe (nazwa użytkownika, źródłowy adres IP, nazwa źródła, źródłowy adres MAC) nie są wyświetlane w dziennikach i raportach i są zastąpione słowem „Anonimowy".

Aby wyświetlić te wrażliwe dane, administrator musi aktywować „*Pełny dostęp do dzienników (danych wrażliwych)*", klikając opcję **Uzyskaj prawo dostępu do wrażliwych danych (logów)** w menu rozwijanym pod nazwą zalogowanego użytkownika (górny baner interfejsu administracyjnego).

20. STORMSHIELD VISIBILITY CENTER

STORMSHIELD Visibility Center (SVC) to system zbierania, zarządzania logami i raportowania. Narzędzie jest kolejną wersją Virtual Log Appliance. Dzięki tej funkcjonalności możliwe jest zbieranie i przeglądanie logów, a także analizowanie raportów wygenerowanych na ich podstawie. Narzędzie dostępne jest w postaci maszyny wirtualnej i pozwala na równoległe zbieranie logów z wielu urządzeń. STORMSHIELD Visibility Center dostępne jest w postaci maszyny wirtualnej (do pobrania z portalu https://mystormshield.eu) kompatybilnej z platformą VMware oraz Hyper-V.
Narzędzie jest w pełni darmowe.

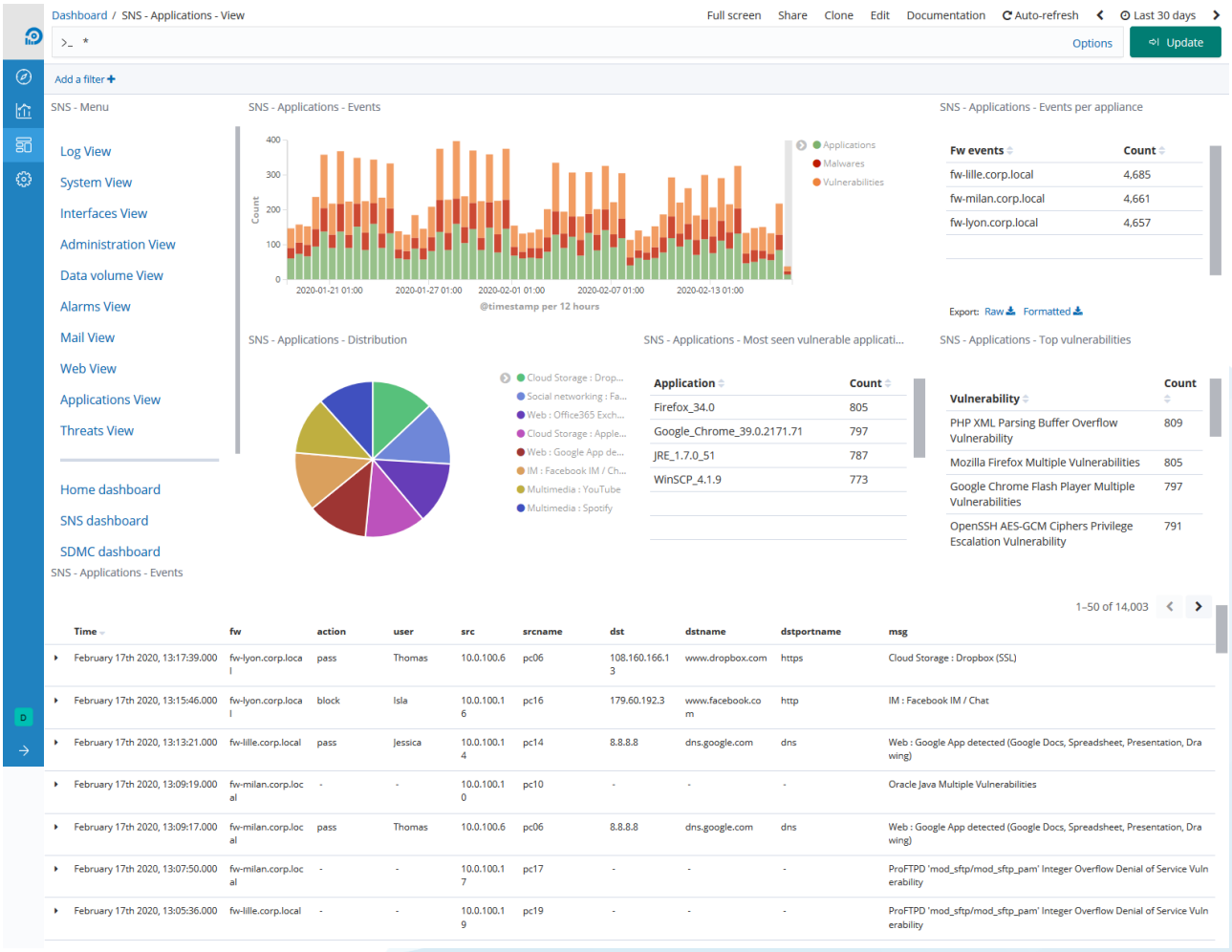


Administrator otrzymuje także możliwość analizy zdarzeń w sieci. Duża ilość informacji przechowywana w bazie danych umożliwia weryfikację wszystkich szczegółów komunikacji, wśród nich:

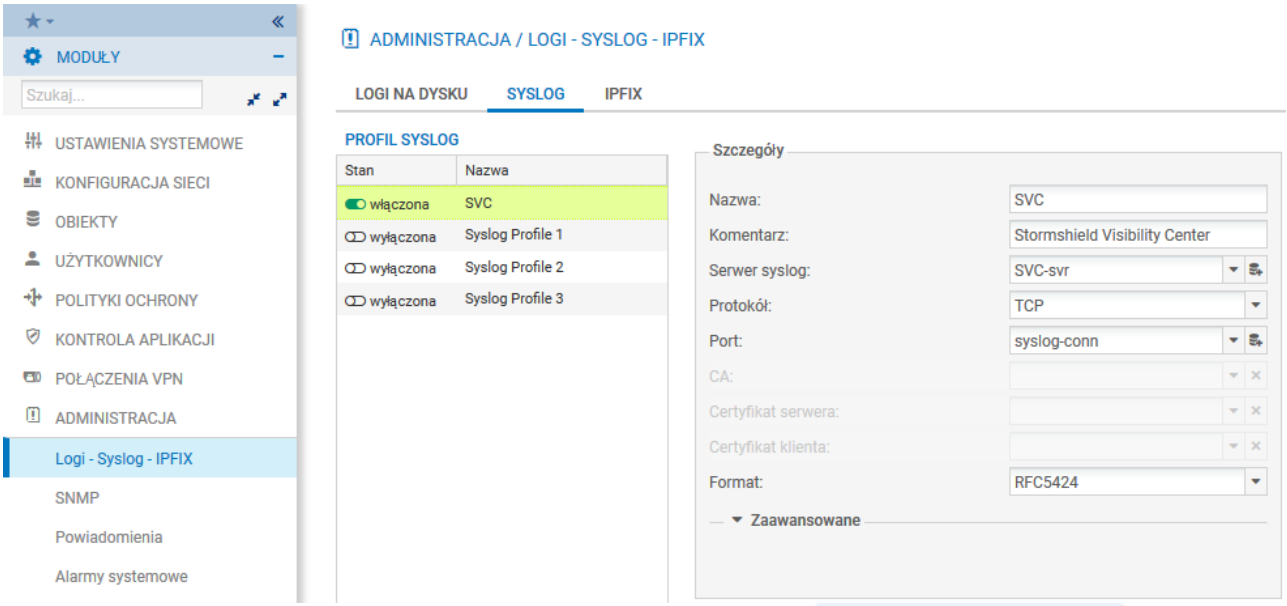
- adres źródłowy,
- adres docelowy,
- użytkownik,
- wykorzystywane porty,
- geograficzne źródła i cele komunikacji,
- a także wiele, wiele innych przydatnych informacji!

Dzięki narzędziu STORMSHIELD Visibility Center można:

- archiwizować logi z wielu urządzeń w jednym miejscu,
- przeglądać graficzne raporty na komputerze, tablecie czy smartfonie,
- szybko znaleźć potrzebne informacje wygodnie filtrując dane.



Po uruchomieniu i podstawowej konfiguracji **SVC** jest gotowe do zbierania logów, które są wysyłane przez urządzenie STORMSHIELD UTM.
Konfiguracja po stronie STORMSHIELD UTM sprowadza się do aktywowania wysyłania logów, podobnie jak w przypadku serwera syslog. Wykonuje się to w sekcji **KONFIGUACJA > ADMINISTRACJA > Logi-Syslog-IPFIX** w zakładce **Syslog**. Wystarczy podać adres IP maszyny wirtualnej SVC, a także protokół, port oraz format wysyłanych danych.



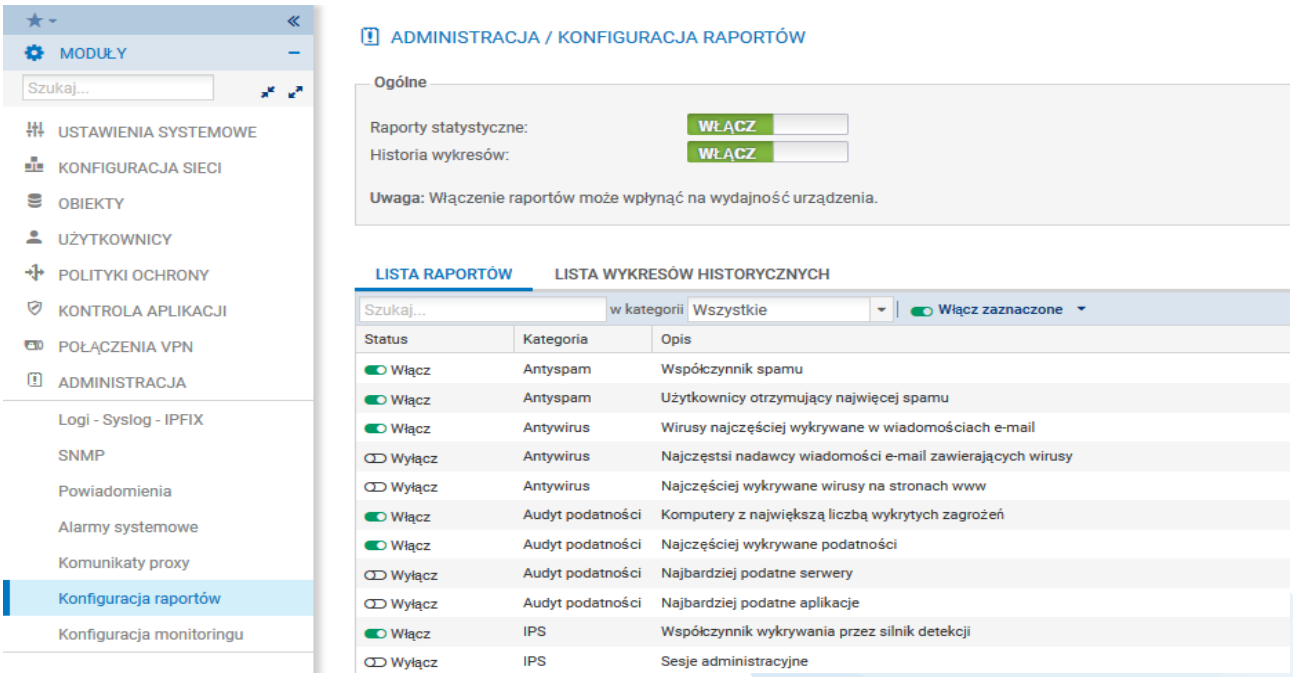
Uwaga!

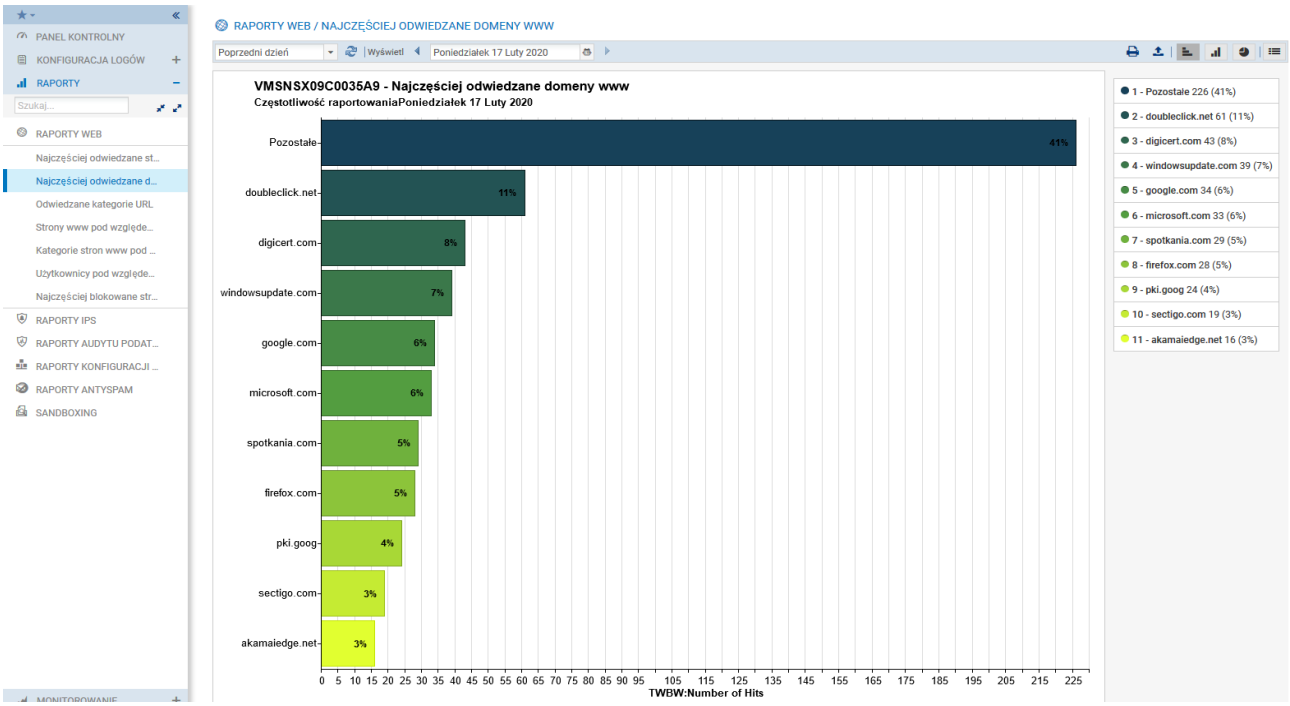
Dla **STORMSHIELD Visibility Center** dostępna jest osobna dokumentacja, którą można pobrać ze strony www.stormshield.pl lub www.mystormshield.eu

21. RAPORTY

Menu raportów będzie dostępne tylko wtedy, gdy w konfiguracji urządzenia zostały włączone raporty statystyczne – KONFIGURACJA > ADMINISTRACJA > Konfiguracja raportów.

Moduł Raporty zawiera raporty „Top 10” w kategoriach: Web, IPS, Antywirus, Antyspam, Audyt podatności, Konfiguracja sieci, Sieć przemysłowa, Sandboxing. Dzięki temu w łatwy sposób można zweryfikować w jaki sposób wykorzystywany jest dostęp do Internetu, jakie ataki zostały zablokowane przez urządzenie STORMSHIELD UTM, a także jakie podatności występują w sieci firmowej. Wiele interaktywnych funkcji pozwala bezpośrednio z poziomu raportów dostroić konfigurację urządzenia.




PANEL KONTROLNY
KONFIGURACJA LOGÓW
RAPORTY
Szukaj...
RAPORTY WEB
Najczęściej odwiedzane st...
Najczęściej odwiedzane d...
Odwiedzane kategorie URL
Strony www pod względe...
Kategorie stron www pod ...
Użytkownicy pod względe...
Najczęściej blokowane str...
RAPORTY IPS
RAPORTY AUDYTU PODAT...
RAPORTY KONFIGURACJI ...
RAPORTY ANTYSPAM
SANDBOXING
RAPORTY WEB / NAJCZĘŚCIEJ ODWIEDZANE DOMENY WWW
Poprzedni dzień
Wyświetl
Poniedziałek 17 Luty 2020
VMSNSX09C0035A9 - Najczęściej odwiedzane domeny www
Częstotliwość raportowaniaPoniedziałek 17 Luty 2020
Pozostałe
doubleclick.net
digicert.com
windowsupdate.com
google.com
microsoft.com
spotkania.com
firefox.com
pki.goog
sectigo.com
akamaiedge.net
41%
11%
8%
7%
6%
6%
5%
5%
4%
3%
3%
0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95 105 115 125 135 145 155 165 175 185 195 205 215 225
TWBW:Number of Hits
1 - Pozostałe 226 (41%)
2 - doubleclick.net 61 (11%)
3 - digicert.com 43 (8%)
4 - windowsupdate.com 39 (7%)
5 - google.com 34 (6%)
6 - microsoft.com 33 (6%)
7 - spotkania.com 29 (5%)
8 - firefox.com 28 (5%)
9 - pki.goog 24 (4%)
10 - sectigo.com 19 (3%)
11 - akamaiedge.net 16 (3%)

22. Najczęściej zadawane pytania (FAQ)

Jak przywrócić urządzenie do ustawień fabrycznych z poziomu CLI (command line)?

Aby przywrócić urządzenie do ustawień fabrycznych należy skorzystać z polecenia *defaultconfig*. Użycie polecenia **`defaultconfig -f -r`** spowoduje przywrócenie ustawień fabrycznych bez wyświetlania komunikatów o błędach i wykona restart urządzenia. Więcej o opcjach polecenia *defautlconfig* można przeczytać wywołując jego pomoc przy użyciu komendy **`defaultconfig -h`**

Gdzie znajdują się pliki konfiguracyjne na dysku urządzenia?

Pliki konfiguracyjne urządzenia znajdują się w folderze **`/usr/Firewall/ConfigFiles`**. Pliki umieszczone są bezpośrednio w tym folderze jak np. **`/usr/Firewall/ConfigFiles/network`** odpowiedzialny za konfigurację interfejsów sieciowych, lub znajdują się w podfolderach tak jak **`/usr/Firewall/ConfigFiles/Filter/10`**, który przechowuje konfigurację 10 slotu konfiguracyjnego Firewall i NAT

Skąd mogę pobrać najnowszą wersję firmware?

Najnowszą wersję można pobrać z sekcji Download po zalogowaniu się na stronie https://mystormshield.eu. Przed pobraniem plików należy wybrać swoją wersja produktu. W strefie Klienta poza najnowszymi wersjami firmware można znaleźć zasobów, między innymi najnowsze wersje klientów VPN, agenta SSO, czy dokumenty Release Note, które opisują zmiany jakie zostały wprowadzone w poszczególnych wersjach oprogramowania (zachęcamy do zapoznania się z tym dokumentem każdorazowo przed aktualizacją firmware urządzenia STORMSHIELD UTM).

Jak uruchomić dostęp przez SSH do urządzenia STORMSHIELD UTM?

Dostęp do urządzenia poprzez SSH konfiguruje się w sekcji KONFIGURACJA > USTAWIENIA SYSTEMOWE > Konfiguracja na zakładce *Dostęp administracyjny*. Dostęp może się odbywać z wykorzystaniem hasła (opcja niezalecana) lub z użyciem pary kluczy publiczno-prywatnych, które można pobrać w sekcji KONFIGURACJA > USTAWIENIA SYSTEMOWE > Administratorzy na zakładce Konto Administratora.

Uwaga! dostęp do urządzenia poprzez SSH jest możliwy jedynie dla głównego konta administratora (konto admin).

Co to jest TECHNICAL REPORT i jak go wygenerować?

Technical Report (Raport techniczny) jest plikiem zawierającym informacje o konfiguracji urządzenia oraz o jego bieżącym stanie. Technical Report jest jednym z podstawowych źródeł informacji używanych przez dział pomocy technicznej do diagnostyki problemów, dlatego powinien być dołączany do każdego zgłoszenia supportowego.

Aby wygenerować Technical Report należy wejść do sekcji KONFIGURACJA > USTAWIENIA SYSTEMOWE > System, a następnie na zakładce Konfiguracja wybrać przycisk Pobierz raport.

Uwaga! Do pobrania raportu technicznego niezbędny jest pełny dostęp do danych wrażliwych

Z poziomi CLI raport można wygenerować używając komendy **`sysinfo`**.

Jak zmienić hasło użytkownika *admin*

Aby zmienić hasło użytkownika admin należy przejść do sekcji **KONFIGURACJA > USTAWIENIA SYSTEMOWE > Administratorzy** na zakładkę Konto Administratora, a następnie dwukrotnie podać nowe hasło.
Z poziomu CLI hasło można zmienić korzystając z polecenia **`fwpasswd`**.

> **Uwaga!**
>
> Hasło użytkownika **admin** można zmienić jedynie będąc zalogowanym jako **admin**.

Jak wygląda procedura aktualizacji firmware?

Aby zaktualizować firmware należy przejść do sekcji **KONFIGURACJA > USTAWIENIA SYSTEMOWE > System**, a następnie na zakładce **Aktualizacja systemu** należy wybrać plik z najnowszą wersją firmware pobrany uprzednio ze strony https://mystormshield.eu. Należy upewnić się, że została wybrana opcja **Kopiuj bieżącą partycję na zapasową** przed aktualizacją (dotyczy jedynie wersji sprzętowych rozwiązania). Kopia znajdująca się na partycji zapasowej pozwoli na szybki powrót do poprzedniej wersji firmware i konfiguracji w przypadku niepowodzenia procesu aktualizacji. Po wybraniu przycisku *Aktualizuj System* rozpocznie się proces aktualizacji, który trwa zazwyczaj kilka minut. Podczas aktualizacji firmware nie należy wyłączać urządzenia.

> Uwaga!
>
> Przed aktualizacją firmware zalecane jest zapoznanie się z dokumentem Release Note opisującym jakie zmiany zostały wprowadzone w nowej wersji oprogramowania.

Zapomniałem hasła dla użytkownika *admin*. Czy istnieje procedura restartu hasła?

Aby zresetować hasło do urządzenia należy podłączyć się do urządzenia przez port konsolowy lub za pomocą monitora i klawiatury (w zależności od modelu urządzenia STORMSHIELD UTM), a następnie zrestartować urządzenie.
Podczas procedury rozruchu pojawi się opcja wyboru, z której partycji ma startować urządzenie:

```
>>FW
1) Main
2) Backup
choose:
```

W tym momencie należy nacisnąć kilkukrotnie przycisk spacji.
Po uzyskaniu znaku zachęty `loader>` wpisujemy: `boot -s` i przyciskamy ENTER.
Po pojawieniu się komunikatu `Enter full pathname of shell or RETURN for /bin/sh:` należy zatwierdzić przyciskiem ENTER.
Następnie wpisujemy: `/usr/Firewall/sbin/chpwd` i wybieramy ENTER, po chwili ukaże się prośba o nadanie nowego hasła. Po weryfikacji poprawności wpisanego hasła nastąpi restart, który kończy procedurę resetu hasła.

Czy dla urządzeń STORMSHIELD UTM dostępny jest tzw. KNOWLEDGE BASE?

Tak, KNOWLEDGE BASE znajduje się pod adresem https://kb.stormshield.eu i dostępny jest dla każdego zarejestrowanego klienta STORMSHIELD.

STORMSHIELD