PODRĘCZNIK UŻYTKOWNIKA

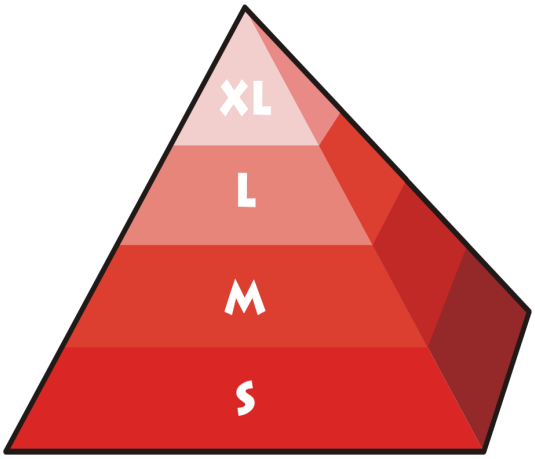
NETASQ wersja 9
ostatnia aktualizacja: 2013-03-14 00:27
opracowanie: DAGMA sp. z o.o.

SPIS TREŚCI

1. Informacje wstępne

Urządzenia NETASQ UTM (Unified Threat Management) integrują w jednej obudowie podstawowe elementy niezbędne do kompletnego zabezpieczenia sieci korporacyjnej. NETASQ UTM to firewall, system wykrywania i blokowania włamań IPS (Intrusion Prevention System), serwer VPN, system antywirusowy, system antyspamowy oraz system filtrowania dostępu do stron internetowych (filtr URL). Ogólnopolskim dystrybutorem rozwiązań NETASQ jest firma DAGMA Sp. z o.o., która świadczy również wsparcie techniczne dla wszystkich klientów, którzy zakupili urządzenia NETASQ w polskim kanale dystrybucyjnym.

Modele urządzeń NETASQ – U, US i NG:



XL: NG5000

L: NG1000

M: Model U: U120 / U250 / U450
M: Model US: U150S / U250S / U500S / U800S

S: Model U: U30 / U70
S: Model US: U30S / U70S

Modele U i NG	U30	U70	U120	U250	U450	NG1000	NG5000
Liczba interfejsów	2	6	6	6	16	8/14	16/22
Przepustowość (FW+IPS)	200Mb/s	600Mb/s	700Mb/s	850Mb/s	1Gb/s	7Gb/s	13.5Gb/s
Przepustowość IPSec (AES)	80Mb/s	120Mb/s	160Mb/s	190Mb/s	225Mb/s	1.5Gb/s	3Gb/s
Liczba połączeń	50 000	100 000	200 000	400 000	600 000	1 000 000	2 500 000
Nowych połączeń/sek	4 000	6 000	6 500	8 500	10 500	75 000	100 000
VLAN 802.1Q	32	32	128	128	128	256	512
Tuneli IPSec VPN	50	100	500	1 000	1 000	5 000	10 000
Tuneli SSL VPN	20	50	256	512	512	1 024	2 048
Tuneli PPTP VPN	48	48	96	96	96	192	192
Dysk twardy na logi	-	-	>=70GB	>=70GB	>=70GB	>=70GB	>=70GB

Modele US	U30S	U70S	U150S	U250S	U500S	U800S
Liczba interfejsów	5 (1+2x2)	8	8	12	12/14	12/14
Przepustowość (FW+IPS)	400Mb/s	800Mb/s	1Gb/s	1,5Gb/s	2Gb/s	3Gb/s
Przepustowość IPSec (AES)	100Mb/s	200Mb/s	250Mb/s	350Mb/s	450Mb/s	550Gb/s
Liczba połączeń	75 000	150 000	250 000	600 000	1 200 000	1 500 000
Nowych połączeń/sek	5 000	8 000	10 000	12 000	16 000	22 000
VLAN 802.1Q	64	64	256	512	512	512
Tuneli IPSec VPN	50	100	500	1 000	1 000	1 000
Tuneli SSL VPN	20	50	75	150	300	500
Tuneli PPTP VPN	48	48	96	96	96	96
Dysk twardy na logi	-	-	>=120GB	>=120GB	>=120GB	>=120GB

Urządzenia od najmniejszego do największego wyposażone są w ten sam moduł Firewall i Intrusion Prevention. Urządzenia różnią się liczbą interfejsów oraz parametrami związanymi z wydajnością (przepustowość, liczba połączeń, liczba obsługiwanych kanałów VPN). Od modelu U120 wyróżnikiem jest także możliwość zapisywania logów bezpośrednio na dysku urządzenia.

Doboru urządzenia dokonuje się na podstawie charakterystyki sieci (liczba stacji roboczych, liczba serwerów itp.). W przypadku jakichkolwiek wątpliwości prosimy o kontakt mailowy na adres pomoc@netasq.pl.

Wsparcie Techniczne

W ramach serwisu użytkownicy rozwiązań NETASQ mają dostęp do wsparcia technicznego w języku polskim. Dział wsparcia technicznego jest dostępny dla Państwa pod numerem telefonu 32 259 11 89, od poniedziałku do piątku w godzinach od 8^{00} do 18^{00}. Prosimy o zgłaszanie problemów technicznych na pierwszym etapie drogą elektroniczną na adres pomoc@netasq.pl lub przy użyciu formularza zgłoszeniowego.

Gwarancja urządzenia

W ramach podstawowej licencji urządzenia NETASQ dostarczone są z podstawowym serwisem gwarancyjnym (**STANDARD EXCHANGE**). Gwarancja ta określa, iż w przypadku awarii urządzenia zostanie ono wymienione (wysyłka) na sprawne w okresie 14 dni roboczych od chwili dostarczenia do producenta. Istnieje możliwość zakupu specjalnego serwisu zapewniającego wymianę urządzenia na następny dzień roboczy (**NEXT BUISNESS DAY EXCHANGE**). Co do szczegółów dotyczących tej licencji prosimy o kontakt na adres : netasq@dagma.pl lub telefonicznie 032 259 11 38.

Podstawowe funkcje NETASQ UTM:

- Stateful Inspection Firewall,
- Instrusion Prevention/Intrusion Detection System (IPS/IDS),
- VPN Server (IPSec VPN, SSL VPN, PPTP VPN),
- uwierzytelnianie i integracja z Microsoft Active Directory Lub LDAP,
- kształtowanie pasma (QoS),
- skaner antywirusowy – ClamAV (http, pop3, smtp, ftp, ssl),
- moduł antyspam,
- klasyfikacja URL – NETASQ URL
- serwer DHCP,
- klient NTP,
- monitorowanie w czasie rzeczywistym,
- logowanie
- NETASQ Event Reporter Light – system raportowania

Wszystkie wymienione wyżej funkcję są dostępne w podstawowej licencji. Funkcje wymagające rozszerzonego serwisu (dodatkowej opcji licencji) to:

- pasywny skaner zagrożeń (SEISMO),
- skaner antywirusowy Kaspersky (http, pop3, smtp, ftp, ssl),
- klasyfikacja URL firmy OPTENET (dostępna dla urządzeń z dyskiem twardym),
- NETASQ Event Analyzer – system raportowania.

Szkolenia techniczne

Firma Dagma Sp. z o.o. jest autoryzowanym centrum szkoleniowym dla rozwiązań NETASQ UTM. Wszystkie informacje na temat szkoleń technicznych znajdują się na stronie: www.acs.dagma.com.pl.

2. Instalacja urządzenia NETASQ UTM

Urządzenia NETASQ UTM dostarczone są w oryginalnym opakowaniu, na którym widoczna jest naklejka z informacją o modelu oraz wersji systemu NS-BSD. Opakowanie zabezpieczone jest przed otwarciem naklejką z logo firmy NETASQ. W przypadku braku naklejki prosimy o kontakt ze sprzedawcą lub firmą DAGMA sp. z o.o.

Po otrzymaniu urządzenia zalecamy przeprowadzenie następujących czynności:

1. weryfikacja zawartości opakowania NETASQ 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 (U30, U30S, U70, U70S) opakowanie powinno zawierać:

- urządzenie NETASQ 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 Serial RS 232,
- płyta CD,
- kabel zasilający,
- zasilacz.

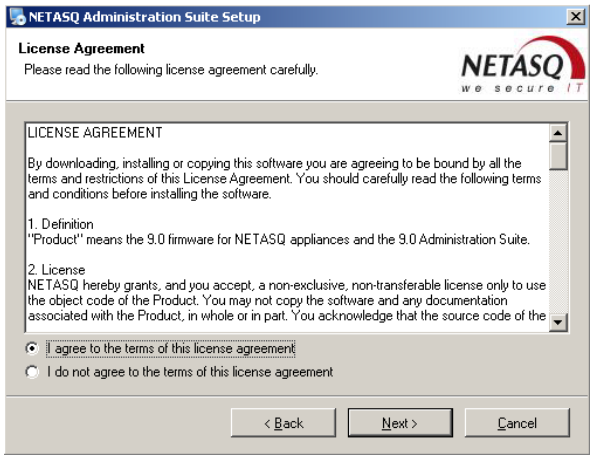
W przypadku wyższych modeli, opakowanie nie zawiera zasilacza (zasilacz jest wbudowany).

Urządzenie NETASQ można skonfigurować przy wykorzystaniu przeglądarki internetowej lub z poziomu wiersza poleceń (CLI). Dodatkowo producent udostępnia w podstawowej licencji pakiet **Administration Suite** w skład, którego wchodzą aplikacja do monitorowania bieżącego stanu urządzenia - **NETASQ Real Time Monitor** i przeglądania logów z urządzenia **NETASQ Event Reporter** (dostępne we wszystkich urządzeniach z dyskiem twardym).

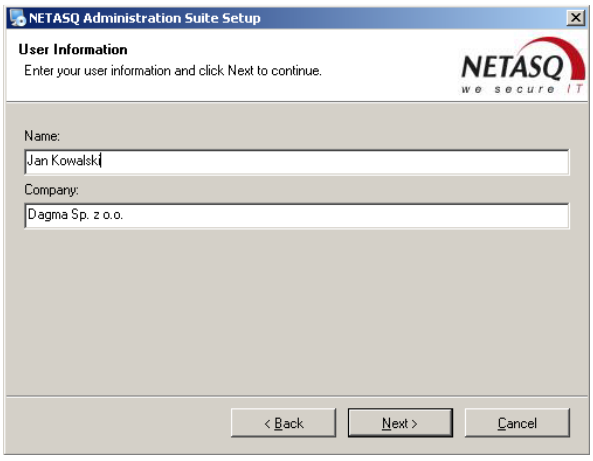
Uwaga

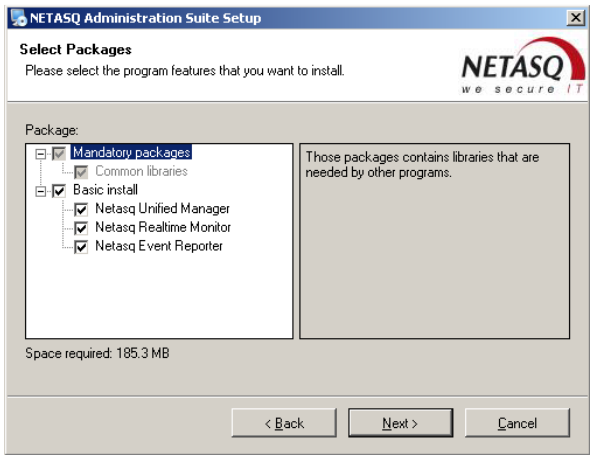
Administration Suite to zbiór aplikacji, które zostaną omówione poniżej. Pełny pakiet oprogramowania **Administration Suite** można pobrać ze strony www.netasq.com w strefie dla klientów (Client Area). Pakiet Administration Suite działa w środowisku systemów operacyjnych Microsoft Windows.

W pierwszym kroku pracy instalatora Administration Suite należy kliknąć *NEXT*, zapoznać się z umową licencyjną i ją zaakceptować:



Następnie należy podać nazwę użytkownika oraz nazwę firmy, dla której zakupiono urządzenie i przejść dalej. W kolejnym kroku pojawi się okno wyboru aplikacji, jakie mają zostać zainstalowane.





NETASQ Unified Manager

W poprzednich wersjach NETASQ NS-BSD aplikacja ta służyła do zarządzania pojedynczym rozwiązaniem NETASQ lub po zmianie trybu jej pracy działała jako system centralnego zarządzania. Od wersji NS-BSD 9 aplikacja ta służy do centralnego zarządzania lub umożliwia podłączenie administracyjne do starszych wersji firmware. W ramach podstawowej licencji Unified manager pozwala na zarządzanie centralne maksymalnie pięcioma urządzeniami. W przypadku potrzeby administracji większą liczbą urządzeń prosimy o kontakt z Działem wsparcia technicznego.

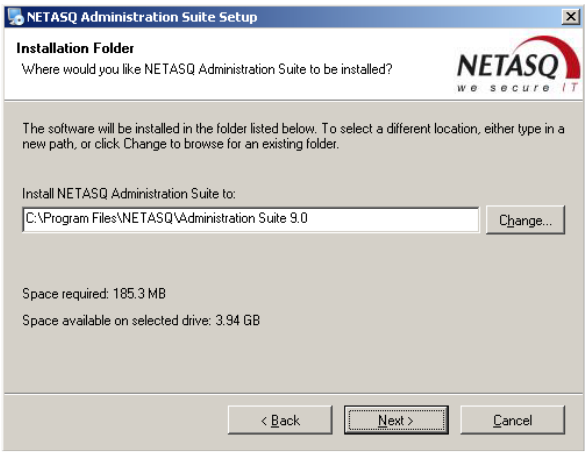
NETASQ Real-Time Monitor

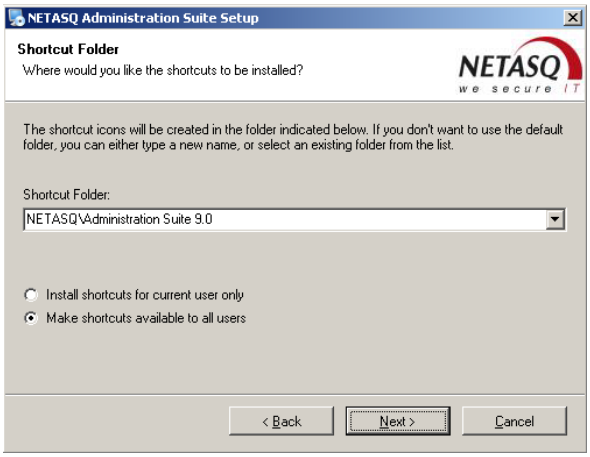
Służy do monitorowania w czasie rzeczywistym pracy urządzenia NETASQ. Aplikacja ta wyświetla stan połączeń dla hostów w sieci, stan kanałów VPN, alarmy IPS itp.

NETASQ Event-Reporter

Służy do przeglądania dzienników (logów). Źródłem danych może być samo urządzenie NETASQ (jeżeli posiada dysk twardy), lub plik logów a serwera syslog.

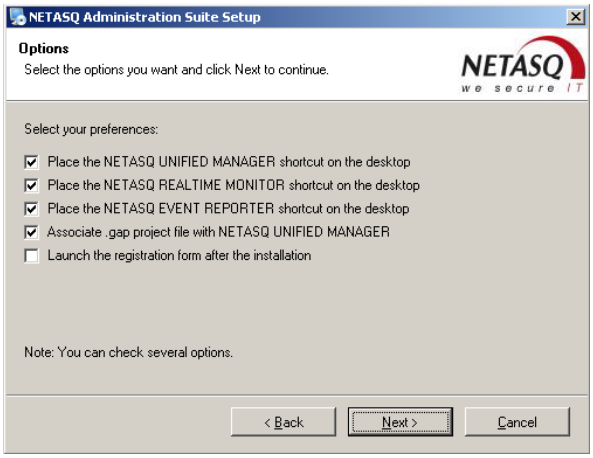
Po wybraniu odpowiedniego typu instalacji należy kliknąć NEXT. Pojawi się okno:

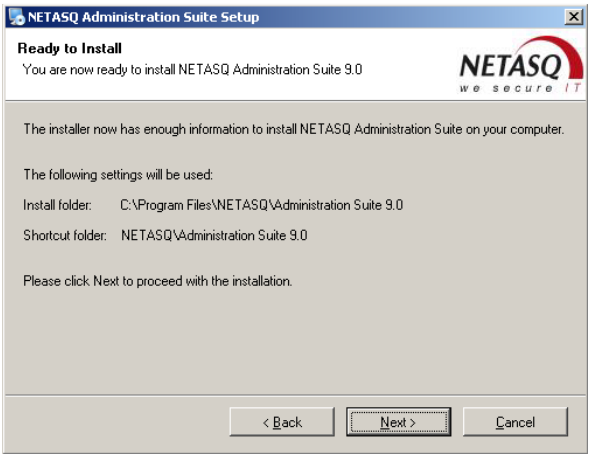


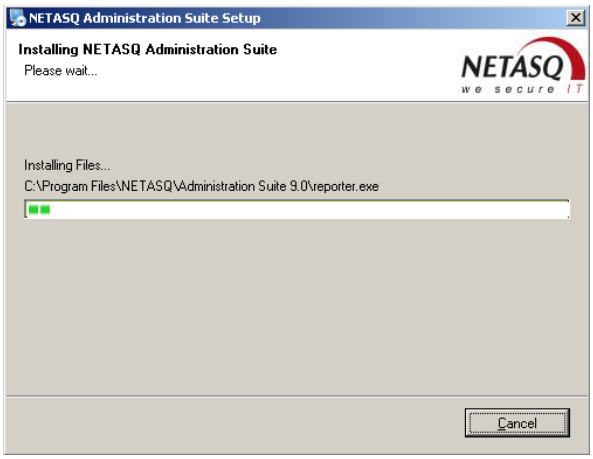


W oknie tym należy określić ścieżkę do katalogu, w którym zainstalowane zostaną pliki NETASQ Administration Suite. Następnie, należy określić nazwę grupy dla aplikacji w menu start.

W kolejnym etapie program zapyta, czy utworzyć skróty do programu na pulpicie. Ostatnia opcja „*Launch the registation form after the installation*" pozwala uruchomić stronę www.netasq.com. Po przejściu na stronę będzie można dokonać rejestracji urządzenia. Jeśli urządzenie zostało wcześniej zarejestrowane to należy odznaczyć tą opcje. Kolejny krok to potwierdzenie parametrów instalacji, po wybraniu przycisku Next rozpocznie się proces instalacji.







Na zakończenie procesu instalacyjnego powinno pojawić się okno potwierdzające poprawne zainstalowanie pakietu Administration Suite. Po wybraniu przycisku Finish nastąpi zakończenie instalacji.

Po zakończeniu instalacji można przystąpić do konfiguracji samego urządzenia.

3. Pierwsze podłączenie do urządzenia

Zaleca się aby pierwszego podłączenia do urządzenia dokonać, gdy:

- Zweryfikowano zawartość opakowania,
- Zarejestrowano urządzenie,
- Zainstalowano Administration Suite,
- Określono sposób podłączenia urządzenia NETASQ do sieci.

Uwaga

Urządzenie należy podłączyć do sieci tylko przy pomocy zasilacza dostarczonego przez producenta. Jeżeli istnieje podejrzenie, iż zasilacz jest uszkodzony lub widoczne są mechaniczne uszkodzenia końcówki zasilacza należy zaniechać podłączenia i zgłosić zaistniałą sytuację na pomoc@netasq.pl

Uwaga

Urządzenia NETASQ należy podłączać do sieci poprzez listwę zabezpieczająca przed przepięciami lub z wykorzystaniem urządzenia UPS.

Uwaga

Wyłączenie NETASQ UTM z sieci musi odbywać się zgodnie z zaleceniami producenta. Służy do tego odpowiednia opcja dostępna z konsoli webGUI lub polecenie *HALT* z linii poleceń. Ponadto urządzenie można wyłączyć za pomocą przycisku na przednim panelu urządzenia.

Podłączenie do urządzenia jest możliwe przy wykorzystaniu:

- Windows Terminal (lub Putty) poprzez port Serial,
- NETASQ Unified Managera,
- klienta SSH,
- przeglądarki www (IE, Firefox);

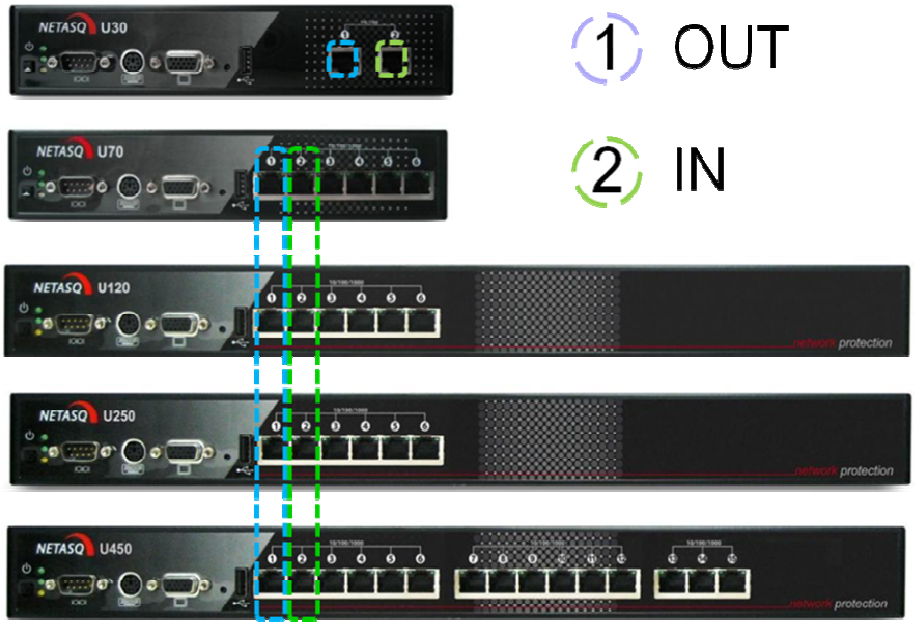
W domyślnej konfiguracji istnieje możliwość dokonania wstępnych ustawień przy użyciu konsoli www. Urządzenie jest dostępne domyślnie pod adresem:
https://10.0.0.254/admin/

Wspierane przeglądarki to:

- Internet Explorer 7, 8 i 9
- Firefox 3.6 lub nowszy

W celu dokonania wstępnej konfiguracji urządzenia należy podłączyć komputer do portu **IN**, którym domyślnie jest interfejs drugi.

SERIA U



Komputer podłączony do tego portu otrzyma adres IP z serwera DHCP. W domyślnej konfiguracji do konsoli można dostać się przy użyciu:

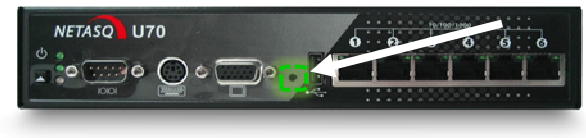
Użytkownik: **admin**
Hasło: **admin**

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 całkowicie uniemożliwi podłączenie do urządzenia poprzez konsolę WebGUI. Należy wtedy uruchomić ponownie urządzenie lub przywrócić do ustawień fabrycznych. Do ponownego uruchomienia urządzenia z poziomu CLI można użyć polecenia „*Reboot*”.

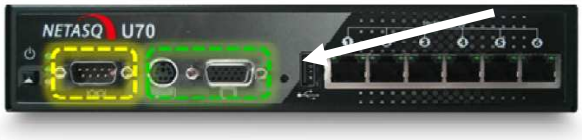
Diody przy interfejsach odpowiednio oznaczają:

zapalona jedna, prawa dioda – 10 Mb/s;
zapalone obie diody – 10/100 Mb/s;
zapalona jedna, lewa dioda – 10/100/1000 Mb/s;
migające diody oznaczają transfer na interfejsie;

Przycisk przywrócenia ustawień fabrycznych:



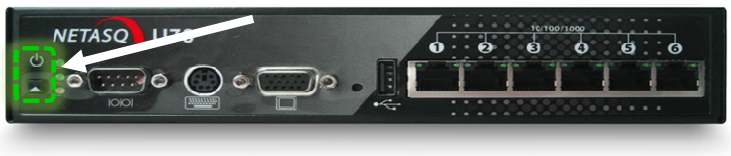
Dostęp do Command Line Interface (CLI):



Zapalone diody z lewej strony urządzenia oznaczają (od góry):

Dioda zielona – urządzenie w trybie online
Dioda zielona – start/zatrzymywanie systemu operacyjnego
Dioda pomarańczowa – sygnalizacja stanu zasilania

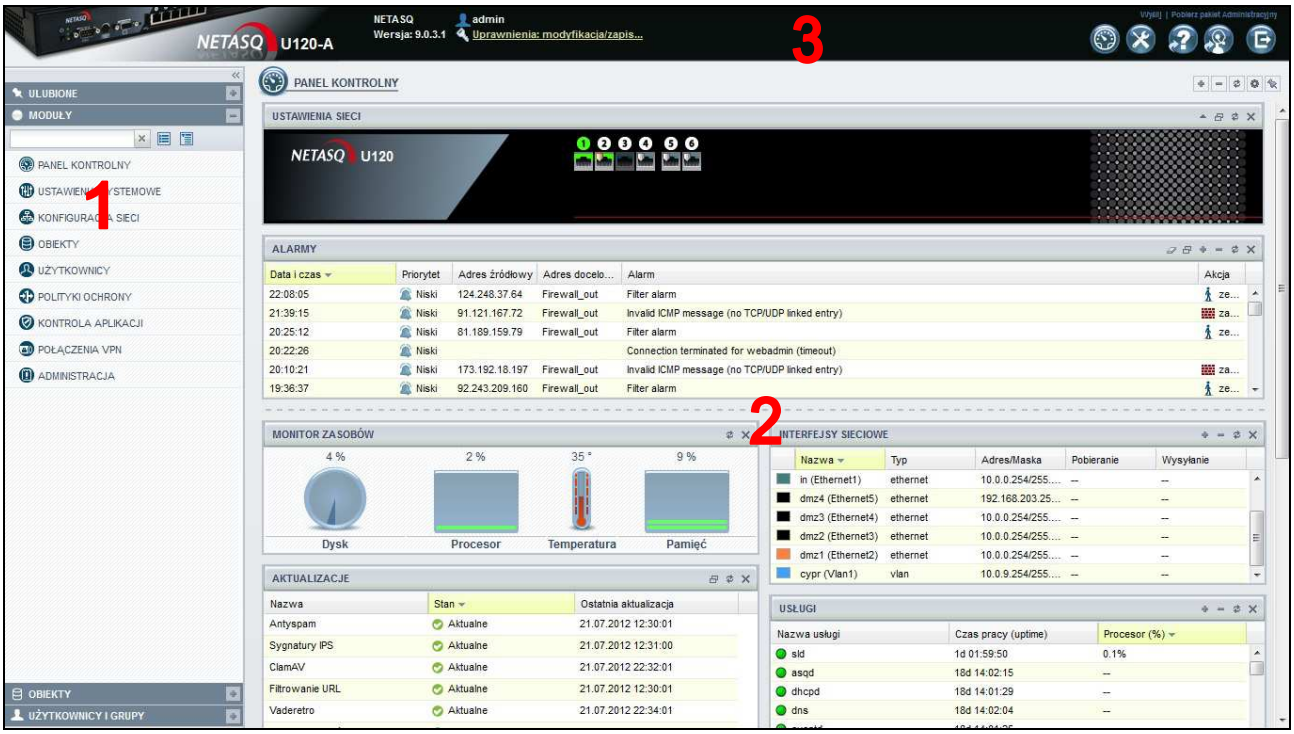
Przycisk wyłącznika, przytrzymany przez około 5 sekund spowoduje zamknięcie systemu. Zamknięcie systemu sygnalizowane jest sygnałem dźwiękowym oraz zgaśnięciem górnej zielonej diody. Proces zamknięcia kończy się zgaśnięciem dolnej zielonej diody.



Konsola NETASQ webGUI

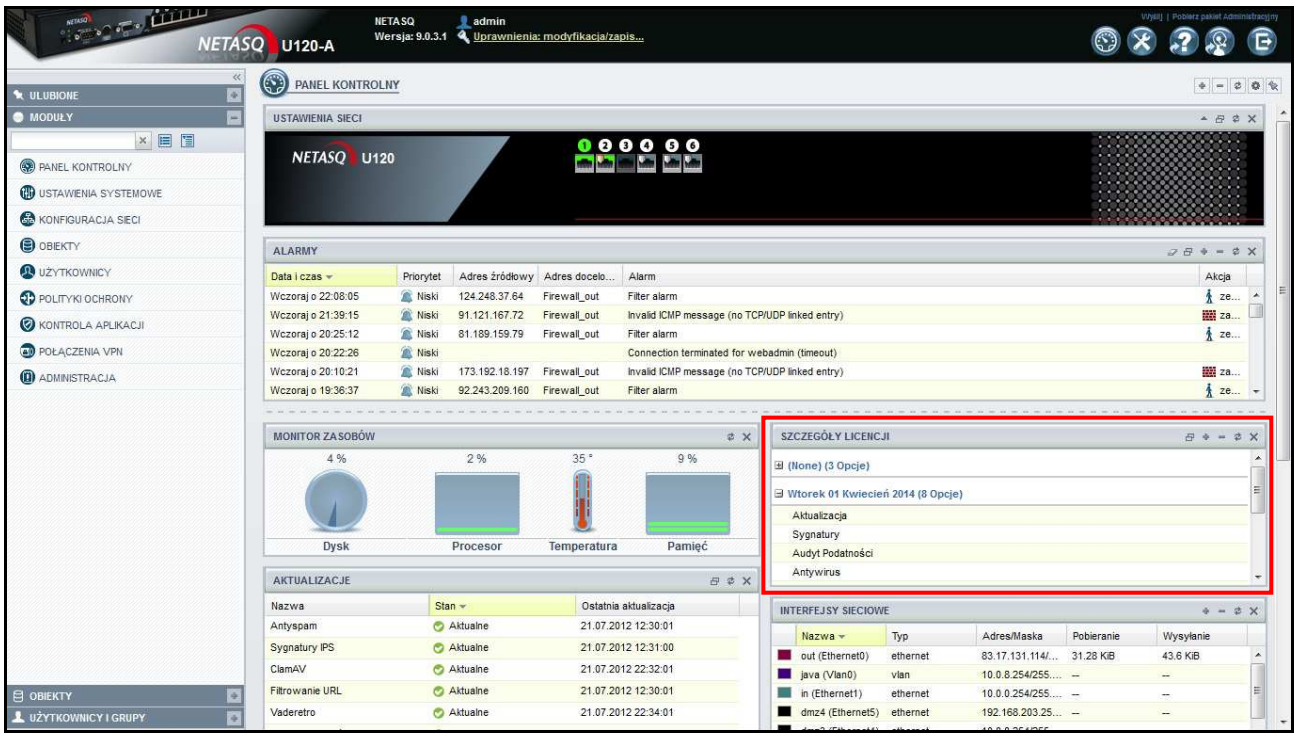
Ekran logowania NETASQ webGUI zaprezentowano poniżej. Wraz z wersją 9.0.0 konsola dostępna jest w trzech językach: Angielskim, Francuskim i Polskim. Autoryzacja polega na podaniu loginu i hasła. Konfiguracja pozwala także na autoryzacje z wykorzystaniem certyfikatu SSL. Wymaga to jednak wcześniejszej konfiguracji serwera PKI na urządzeniu. Po wybraniu pozycji *„OPCJE”* istnieje możliwość zmiany języka lub autoryzacji z uprawnieniami *„tylko do odczytu*”.

Pomyślna autoryzacja na urządzeniu spowoduje uruchomienie do głównego okna konfiguracji. Po lewej stronie ekranu [1] znajduje się główne menu z wszystkimi opcjami konfiguracyjnymi. Okno centralne [2] prezentuje na pierwszej stronie zbiór różnego rodzaju tzw. widżetów, które składają się na PANEL KONTROLNY. Informacje przedstawiane w tych oknach przedstawiają stan poszczególnych modułów (licencje, interfejsy, dzienniki zdarzeń itp.). W górnym panelu [3] znajdują się opcje ustawienia samego WebGUI oraz odnośnik umożliwiający zmianę posiadanych uprawnień do zarządzania urządzeniem.



4. Podstawowa konfiguracja

Po pierwszym zalogowaniu się do urządzenia należy zweryfikować poprawność licencji. Można to zrobić na jednym z widżetów panelu kontrolnego.

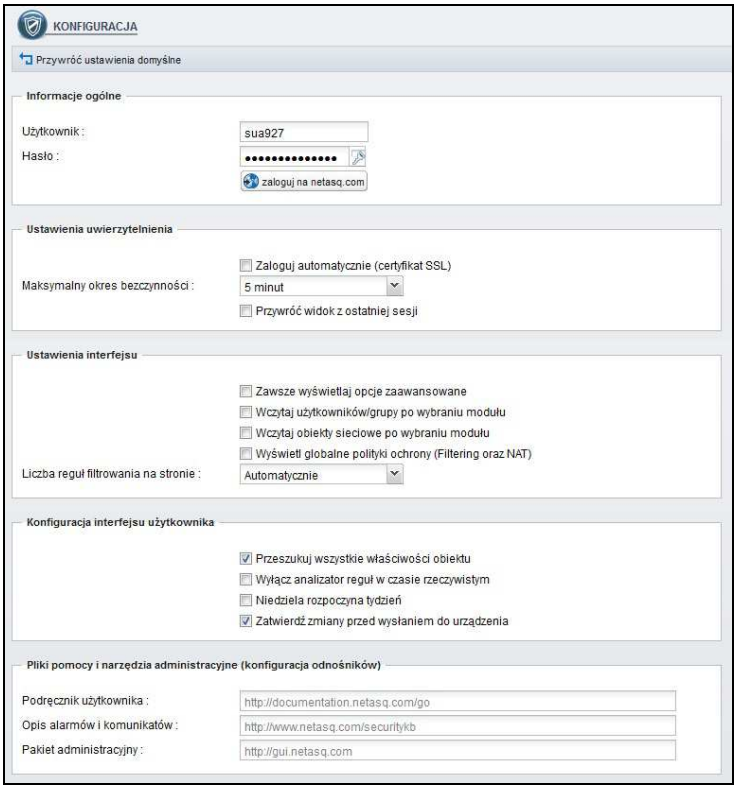


Wstępną konfigurację można podzielić na etapy:

- konfiguracja ustawień WebGUI,
- ogólne ustawienia dotyczące samego urządzenia,
- konfiguracja/zmiana hasła dla użytkownika **admin**,
- ustawienie serwerów DNS na urządzeniu,
- konfiguracja obiektów,
- Konfiguracja usług DHCP - **patrz rozdział 14**,
- Konfiguracja interfejsów urządzenia (trybu pracy) - **patrz rozdział 5**,
- Ustawienie bramy domyślnej na urządzeniu (routing) - **patrz rozdział 6**,
- Konfiguracja zapory (firewall) – **patrz rozdział 7**,
- Konfiguracja translacji adresów (NAT) – **patrz rozdział 8**.

Konfiguracja WebGUI

W pierwszej kolejność należy skonfigurować parametry panelu administracyjnego tzw. WebGUI. W celu konfiguracji WebGUI należy użyć przycisku  , który znajduje się z prawej strony górnego menu. Zmiany w konfiguracji w tej części są aktywowane automatycznie w chwili ustawienia nowej wartości (nie ma potrzeby zatwierdzania zmian).



Informacje ogólne

Należy podać login i hasło do swojej strefy klienta ze strony www.netasq.com. Dane te są dostarczane wraz z urządzeniem po jego zakupie. Uzupełnienie tych danych pozwala na automatyczne pobieranie oraz odnawianie licencji przez urządzenie, a także pozwala na uruchomienia sprawdzenia aktualnego firmware dla urządzenia.

Ustawienia uwierzytelnienia

Sekcja pozwala na ustawienie automatycznego logowania do GUI w wypadku, gdy mamy zaimportowany certyfikat SSL użytkownika o uprawnieniach administracyjnych. *Maksymalny okres bezczynności* pozwala określić czas po którym nastąpi automatyczne wylogowanie z konsoli w wypadku braku aktywności. Zaznaczenie opcji *Przywróć widok z ostatniej sesji* pozwala na zapisanie przez system preferencji użytkownika widoku GUI z ostatniej sesji.

Ustawienia interfejsu

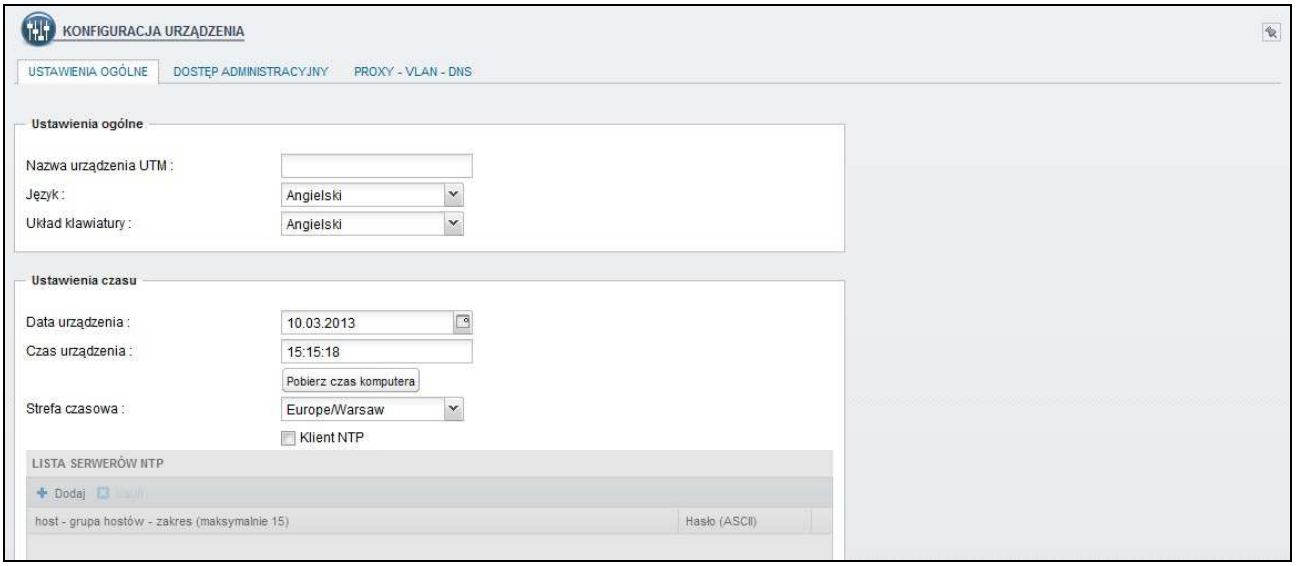
W tej sekcji można ustawić aby opcje *Zaawansowane* były zawsze rozwinięte i widoczne w oknie konfiguracyjnym. Zaznaczenie opcji *Wczytaj użytkowników po wybraniu modułu* oraz *Wczytaj obiekty sieciowe po wybraniu modułu* spowoduje, iż w modułach konfiguracji użytkowników i obiektów sieciowych

elementy te zostaną wyświetlone po przejściu do tych sekcji. Gdy opcja ta jest odznaczona użytkownicy czy obiekty sieciowe są wczytywane po określeniu filtra (np. tylko obiekty typu host).

Ogólne ustawienia, dotyczącego samego urządzenia

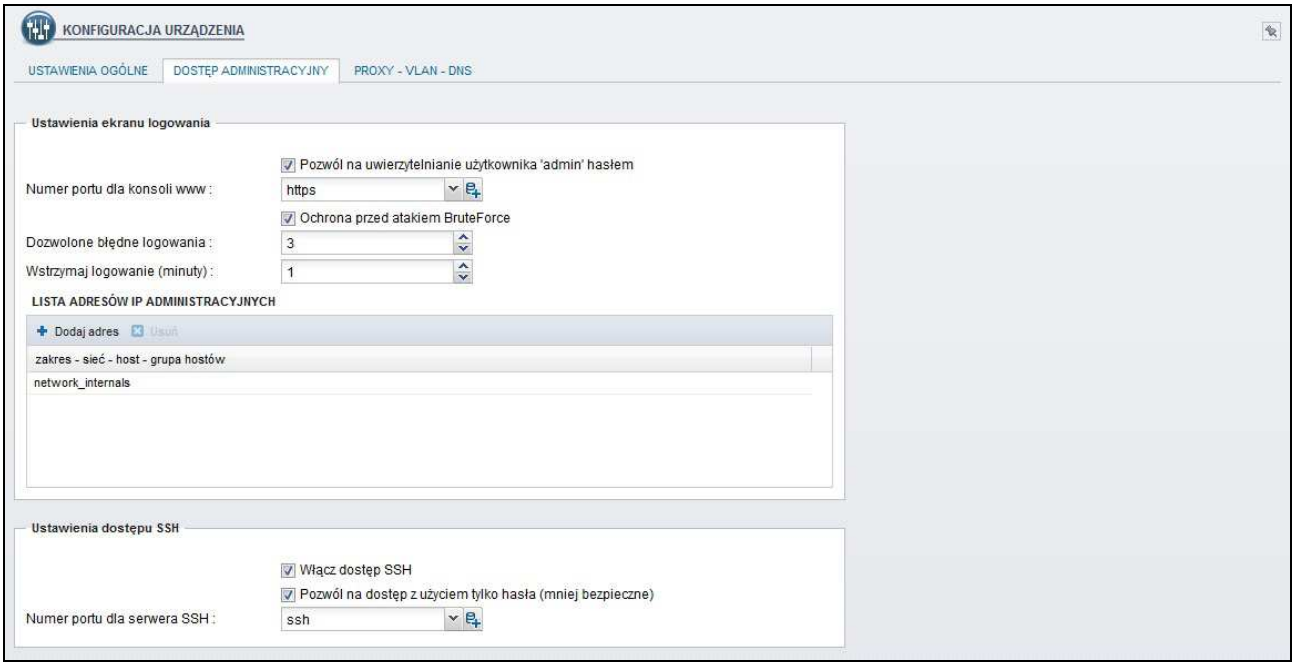
Ustawień ogólnych urządzenia dokonujemy w sekcji **Ustawienia systemowe -> Konfiguracja urządzenia**.

Na pierwszej zakładce można skonfigurować nazwę urządzenia, ustawienia układu klawiatury i języka (kodowanie znaków). Można tutaj również skonfigurować czas urządzenia oraz strefę czasową. Alternatywnie można wskazać serwer NTP (serwer czasu), z którym NETASQ będzie synchronizował czas.

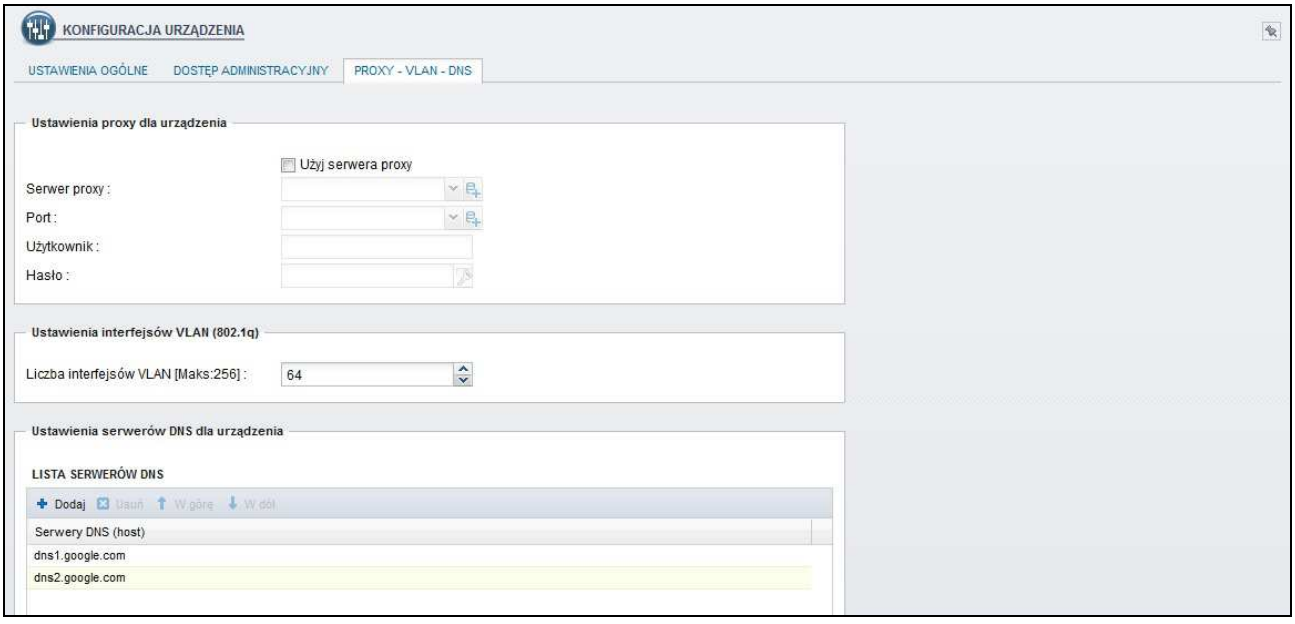


Zakładka **Dostęp administracyjny** pozwala skonfigurować dostęp do urządzenia. Znajdziemy tutaj między innymi możliwość ustawienia porty na którym będzie działał portal administracyjny (domyślnie jest to port https – 443 TCP), adresu lub adresów IP które będą miały możliwość dostępu do WebGUI oraz mechanizmu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

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



Jeśli NETASQ do komunikacji z Internetem musi łączyć się przez zewnętrzny serwer Proxy, to na zakładce **Proxy – VLAN – DNS** można skonfigurować dane dostępowe do tego serwera. Można tutaj wskazać również serwery DNS, z których UTM ma korzystać przy rozwiązywaniu nazw. Skonfigurowanie tej opcji jest niezbędne do poprawnego pobierania aktualizacji przez urządzenia.



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 **Ustawienia systemowe -> Administratorzy** w zakładce **Konto Administratora**.

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

Konfiguracja obiektów

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

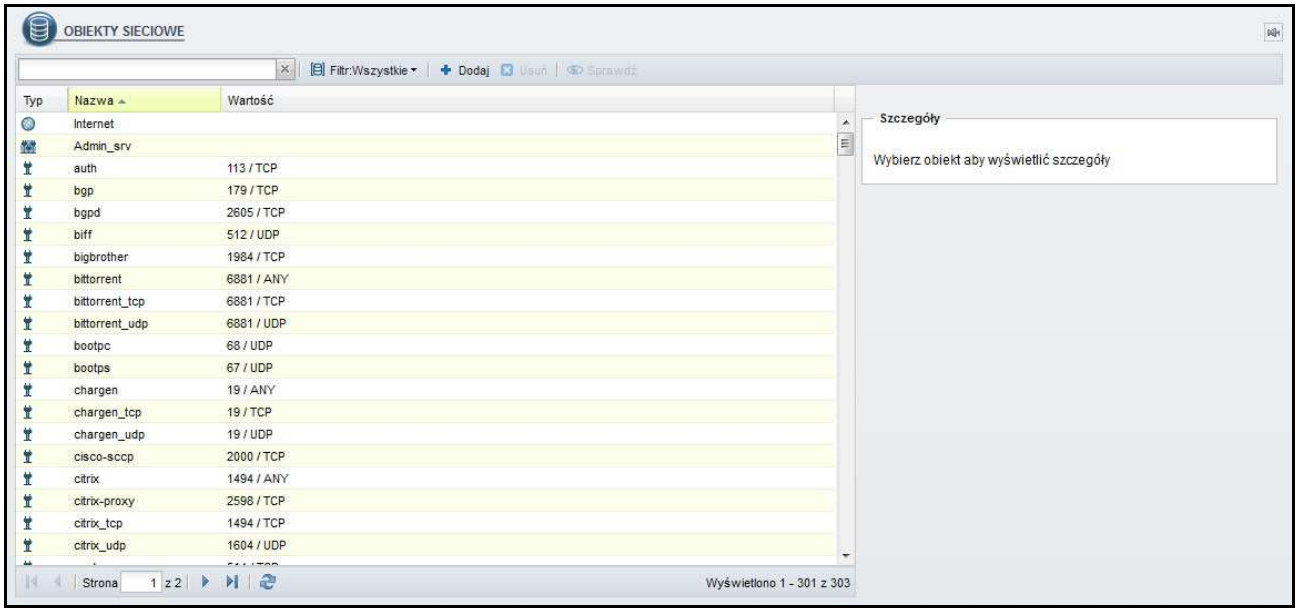
Wyróżnić można kilka typów obiektów:

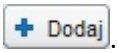
- **Host (Host)**– reprezentuje pojedynczy adres IP ,
- **Zakres (IP address range)** – zakres adresów IP wykorzystywany np. w konfiguracji DHCP czy PPTP,
- **Sieć (Network)** – adres IP i maska. Obiekt reprezentuje wszystkie adresy w sieci,
- **Protokół (IP protocol)** – protokół sieciowy,
- **Port (Port)** – port na którym działa usługa.

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**.

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



Innym sposobem tworzenia obiektów jest rozwinięcie w lewym menu gałęzi obiekty i wybranie ikony 

. 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  , kliknięcie której spowoduje otwarcie okna 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 **Typu obiektu** jako **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 przez edycję obiektu. Pole Adres MAC służy do przypisywania adresu MAC do właściwości obiektu. Opcja ta jest wykorzystywana w przypadku konfiguracji serwera DHCP i ustawienia statycznych rezerwacji adresów IP dla komputerów. Zaznaczenia opcji **Obiekt globalny**

powoduje, że informacje o obiekcie są wymieniane pomiędzy urządzeniami spiętymi modułem **NETASQ Centralized Manager**.

Uwaga

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

Konfiguracja pozostałych typów obiektów będzie analogiczna jak obiektów **Host** z uwzględnieniem charakterystycznych pól dla każdego z typów obiektów.

Uwaga

NETASQ 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. 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

Synchronizację obiektów dynamicznych można przeprowadzić ręcznie używając polecenia:

objectsync

5. Tryb pracy urządzenia

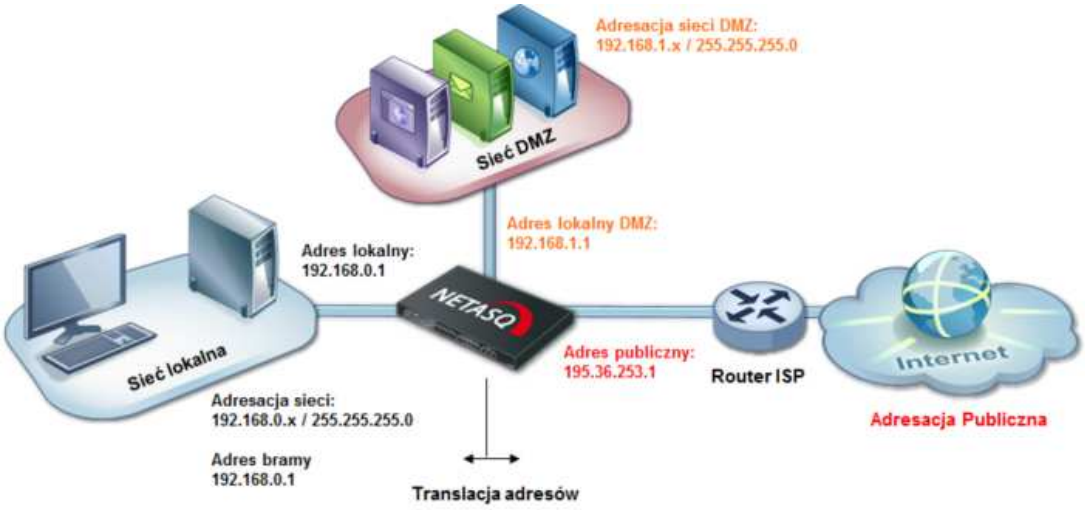
Tryb pracy urządzeń NETASQ zależy od roli, jakie ma spełniać urządzenie w sieci. Tryb pracy określa relację pomiędzy interfejsami. Konfiguracja trybu pracy urządzenia odbywa się w sekcji **Konfiguracja sieci -> Interfejsy**.

Urządzenia NETASQ mogą pracować w trzech trybach:

- BRIDGE (przeźroczysty),
- ADVANCED (zaawansowany, tryb routera),
- HYBRID (mieszany).

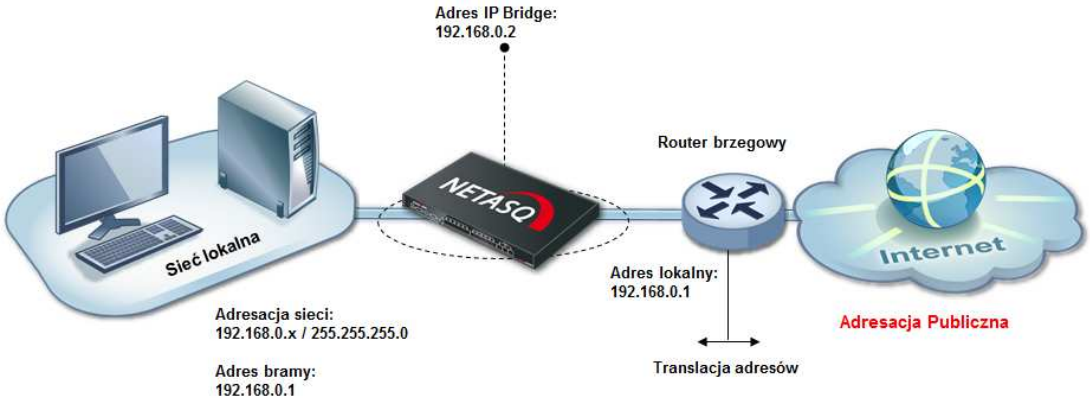
Tryb ADVANCED

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



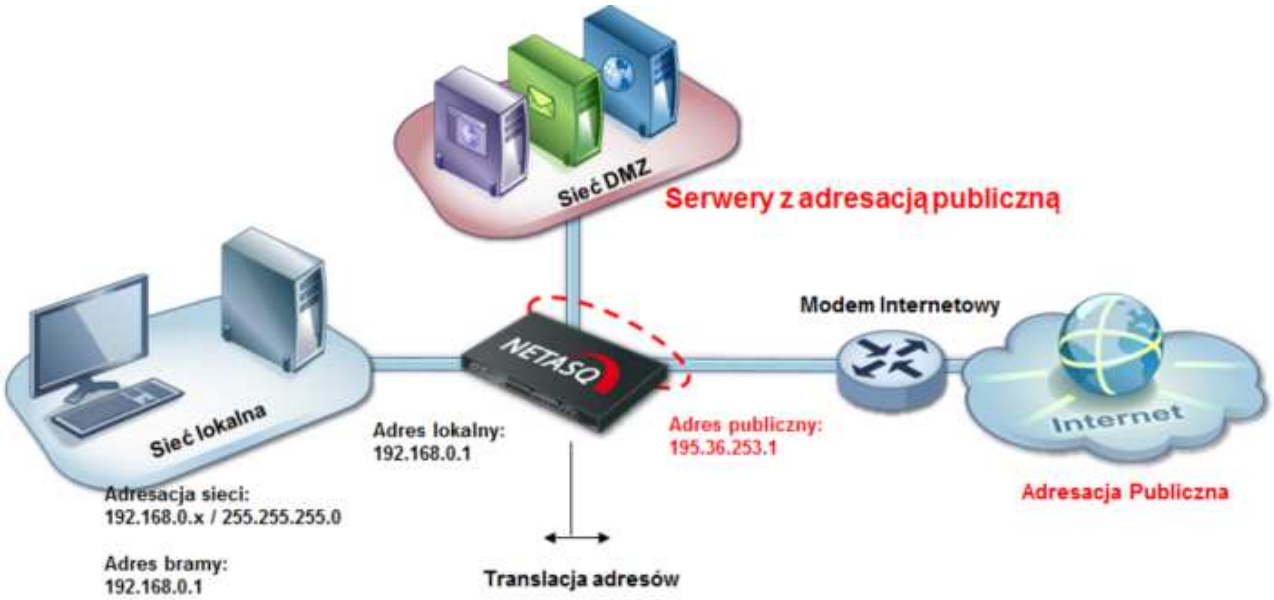
Tryb BRIDGE

Tryb Bridge inaczej jest zwany trybem transparentnym. 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 (translacja NAT).



Tryb HYBRID

Tryb HYBRID jest zwany inaczej trybem mieszanym. Polega on na takim ustawieniu interfejsów NETASQ, że cześć z nich względem siebie jest w trybie BRIDGE, a część w trybie ADVANCED. Jest to jeden z najczęściej używanych trybów.



6. Ustawienia trasowania połączeń (routing)

Trasowanie połączeń, czyli określenie drogi przesyłania pakietów można skonfigurować w NETASQ na kilka sposobów. Kolejność analizy poszczególnych metod trasowania jest następująca:

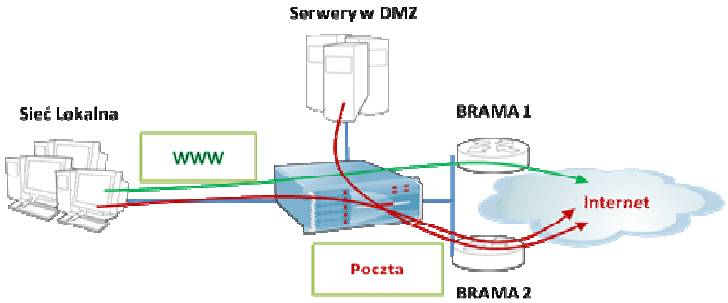
- Routing statyczny,
- Policy Routing,
- Routing by interface,
- Load Balancing,
- Brama domyślna (default gateway).

Routing statyczny

Pozwala na określenie tras statycznych do sieci, które nie są podłączone bezpośrednio do interfejsów urządzenia. Trasy statyczne można skonfigurować w oknie **Konfiguracja sieci -> Routing** na zakładce **Trasy statyczne**.

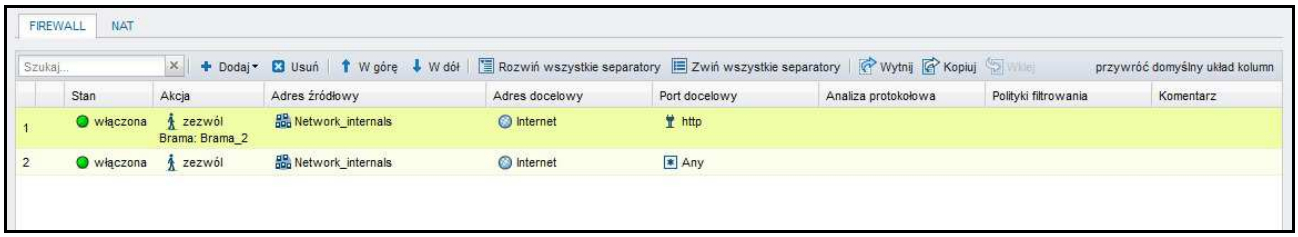
Policy Routing

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 zastosowań:



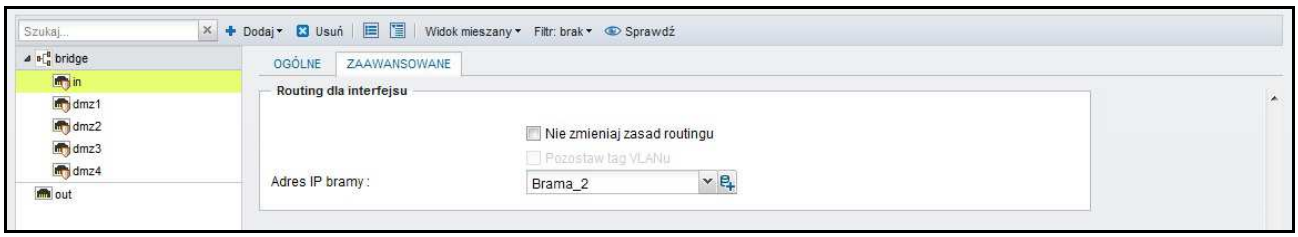
Na ilustracji zaprezentowano sytuacje, w której ruch http kierowany jest przez bramę *BRAMA1*, natomiast ruch związany z pocztą (smtp, pop3) kierowany jest na drugiego usługodawcę *BRAMA2*.

Można skierować ruch na odpowiednie łącze ustawiając w kolumnie **Akcja** opcję **Routing na podstawie reguły (PBR)** poprzez podanie bramy odpowiedniego dostawcy Internetu przy wybranej regule na firewalla.



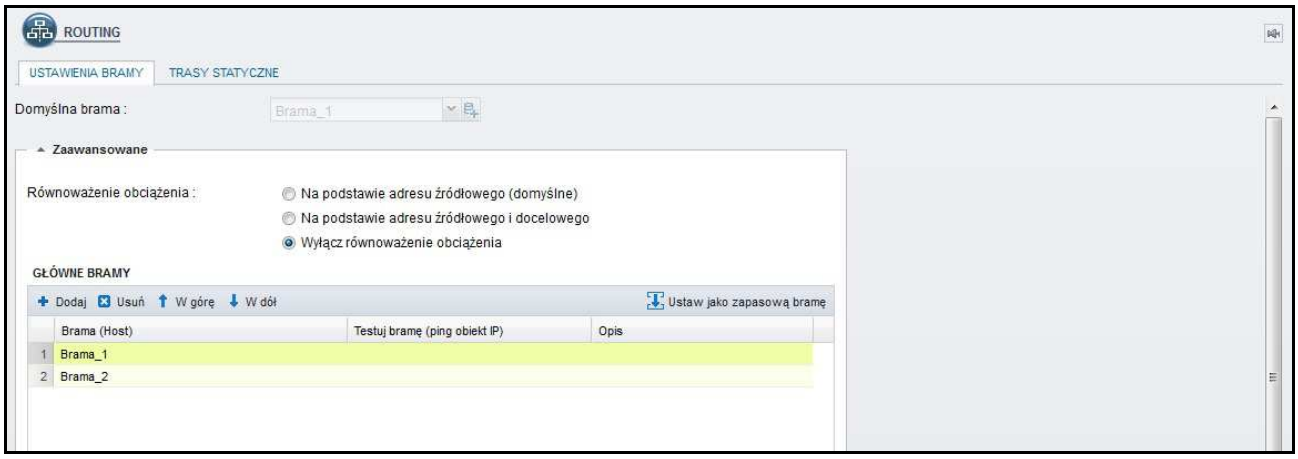
Routing by interface

Ten typ trasowania połączeń pozwala na kierowanie całego ruchu przychodzącego na dany interfejs. Konfiguracja odbywa się w menu **Konfiguracja sieci -> Interfejsy** w zakładce **Zaawansowane** dla danego interfejsu.



Load Balancing by Source/Destination

Równoważenie obciążenia można określić w zależności czy połączenia równoważone są według adresów źródłowych (SOURCE) czy na podstawie adresu źródłowego i docelowego (CONNECTION). Włączenie Load Balancingu polega na wybraniu metody równoważenia i wskazaniu dostępnych ISP w sekcji **BRAMY GŁÓWNE** w zakładce **Konfiguracja sieci -> Routing** . W ramach procesu równoważenia obciążenia wykorzystywany jest algorytm karuzelowy (*round robin*). Kolejne połączenie jest kierowane na kolejną bramę. Jeżeli lista bram się skończy to przydzielanie trasy zaczyna się od początku listy.



Brama domyślna

Domyślna brama (eng. Default gateway) to określenie routera, na który pakiety będą kierowane w przypadku, gdy żadna z powyższych metod nie zostanie wykorzystana. Dodatkowo brama domyślna stanowi bramę dla samego urządzenia NETASQ.

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 –r

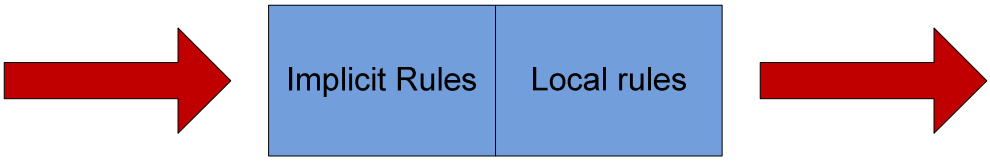
Aby wyświetlić pozostałe metody trasowania należy użyć polecenia:

sfctl –s route

7. Konfiguracja zapory (firewall)

Konfiguracja firewalla w rozwiązaniach NETASQ podzielona jest na dwie części. Pierwszą z nich są reguły domyślne a drugą polityki konfigurowane przez administratora.

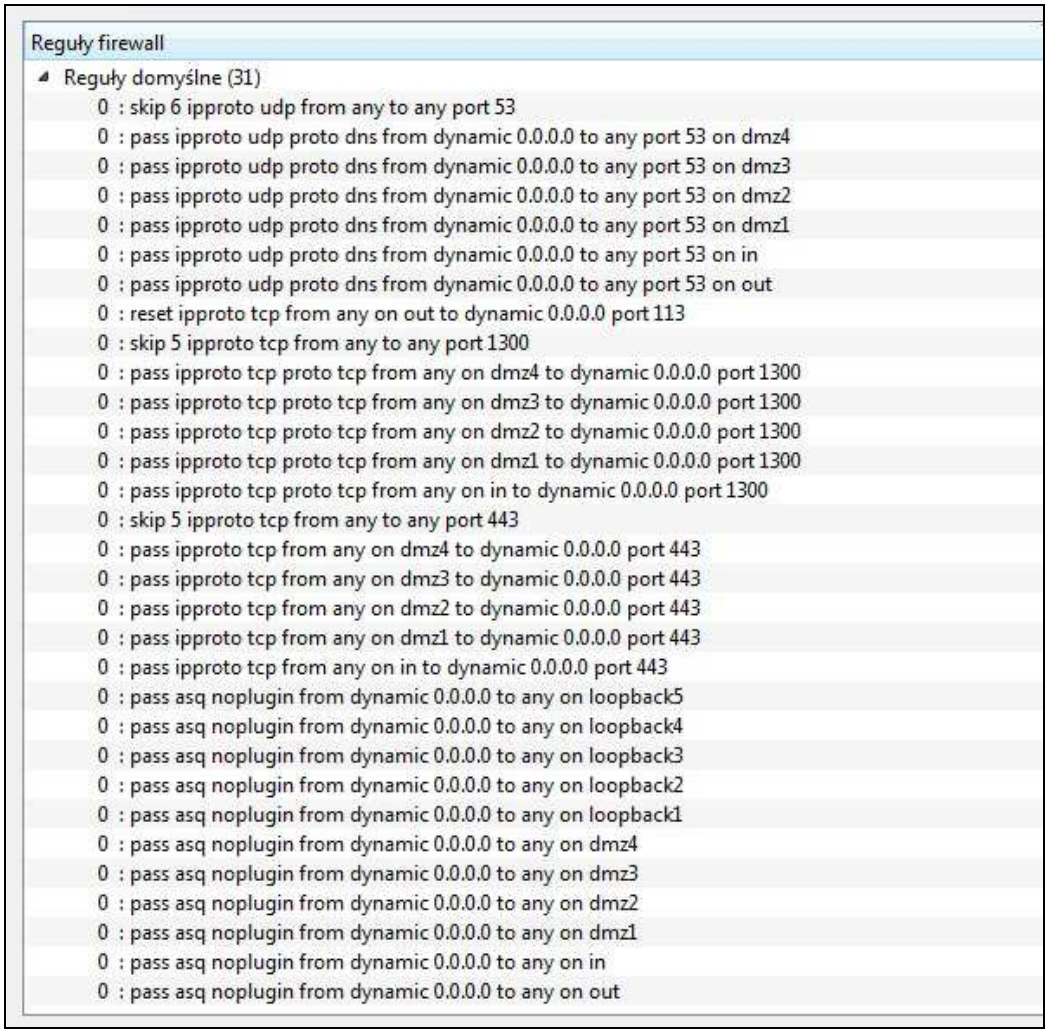
W pierwszej kolejności pakiet sprawdzany jest przez zbiór **Domyślnych reguł firewall** (**Implicit rules**). Jeżeli pakiet nie znajdzie dopasowania do żadnej z reguł domyślnych sprawdzane są dopasowania do reguł polityki stworzonej przez administratora tzw. **Polityki lokalnej**.



Domyślne reguły firewall - Implicit Rules

W sekcji **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 aktywowana jest domyślna polityka Block All, lub kiedy w ramach polityki firewall administrator nie stworzyłby reguł umożliwiających komunikację z urządzeniem co w efekcie aktywowania takiej polityki spowodowałoby utratę łączności z urządzeniem. Poniżej znajduje się okno konfiguracyjne reguł domyślnych:

W przypadku reguł domyślnych nie ma podglądu na ich pełną składnie. Znaczenie poszczególnych reguł można zobaczyć w aplikacji **Real Time Monitor** w zakładce **Reguły firewall**. Poniżej znajduje się lista reguł domyślnych zaprezentowanych w **RTM**.



Uwaga

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

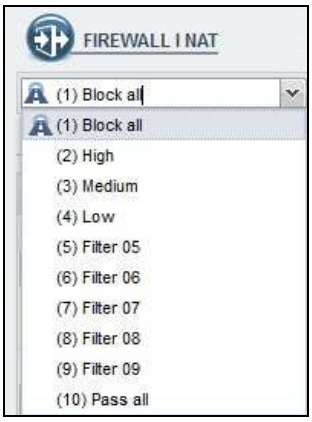
Wskazówka

Do wyświetlenie aktywnych reguł firewall służy polecenie:

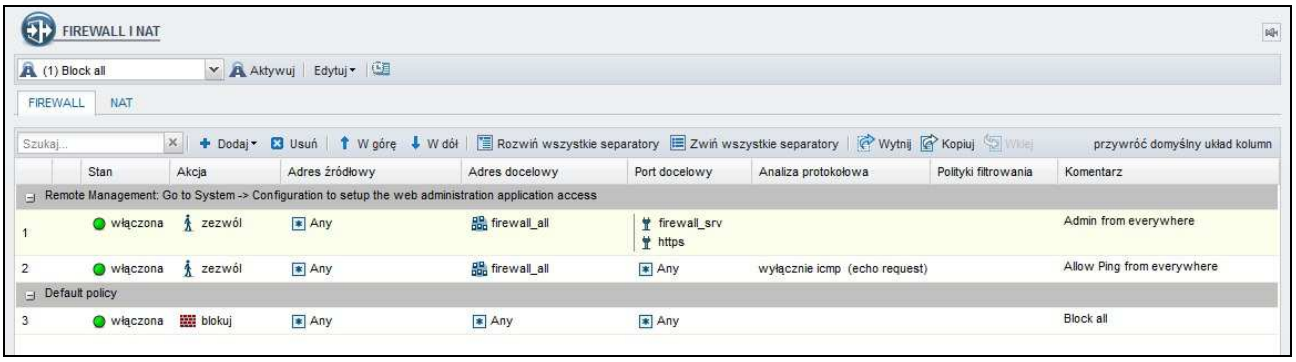
sfctl -s filter

Lokalne polityki ochrony

Konfiguracja zapory NETASQ znajduje się w sekcji **Polityki ochrony -> Firewall i NAT**. Po wybraniu tej opcji ukaże się okno reguł firewalla. NETASQ UTM posiada 10 konfigurowalnych zestawów reguł zwanych slotami. W danej chwili aktywny może być jeden slot i oznaczony jest on symbolem litery „A”.



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

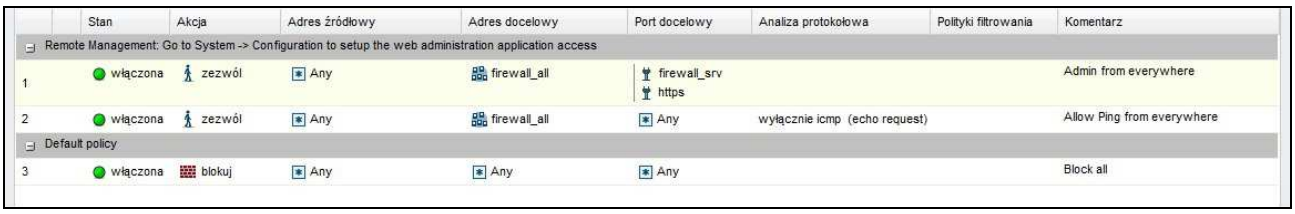


Górna część okna **Firewall i NAT** pozwala na zarządzanie slotami konfiguracyjnymi oraz regułami firewalla.

Dostępne akcje zarządzania regułami firewalla:

Aktywuj	aktywacja wybranego zestawu;
Edytuj	zmiana nazwy slotu, przywrócenie jego ustawień domyślnych oraz przekopiowanie zaznaczonego slotu do innego;
Dodaj	dodanie nowej reguły lub separatora. Z tego miejsca możliwe jest również uruchomienie kreatora reguł specjalnych: SSL Proxy, http Proxy (typu explicit), reguły uwierzytleniania;
Usuń	usuwa zaznaczoną regułę;
W góre/W dół	przesunięcie reguły;
Rozwiń/Zwiń wszystkie separatory	separatorów można użyc do grupowania reguł o podobnych zakresach np. reguły dla LAN, reguły dla DMZ. Jak sama nazwa wskazuje przysicki Rozwiń/Zwiń wszystkie separatory służą do szybkiego zwinięcia/rozwinięcia wszystkich separatorów.
Wytnij/Kopiuj/Wklej	pozwala na szybkie zarządzanie regułami. Reguły można zaznaczać z **Shift** lub **Ctrl** w celu zaznaczenia wielu reguł.

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



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

Kolumnami odpowiedzialnymi za dopasowanie ruchu do reguły są kolumny: **Adres źródłowy**, **Adres docelowy**, **Port docelowy**, **Analiza protokołowa**. Ich konfiguracja obejmuje:

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

Użytkownik - uwierzytelniony użytkownik bazy LDAP
Adres źródłowy - źródło pochodzenia pakietu. Może to być pojedynczy komputer, zakres adresów, sieć, grupa adresów IP.
Interfejs wejściowy – interfejs, do którego podłączony jest komputer inicjujący połączenie. Pozwala na tworzenie reguł zależnych od topologii sieci.

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

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

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

Port docelowy – określa usługę, z której będą skorzystać obiekty określone w Adresie źródłowym łącząc się do obiektu określonego w Adresie docelowym. Inaczej mówiąc jest to port docelowy połączenia.

Opcje dostępne w ramach kolumny **Analiza protokołowa**

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

Jeśli ruch znajdzie dopasowanie w powyższych kolumnach, 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. Do wyboru są:

- **Blokuj** – zablokowanie ruchu i nie wykonywanie dalszej analizy;
- **Zezwól** – przepuszczenie ruchu i wykonywanie dalszej analizy;
- **Loguj** – akcja niebędąca celem ostatecznym, informacja o ruchu zostanie zapisana w logach a pakiet będzie szukał dopasowania w kolejnych regułach firewalla.

Logowanie - informacja o dopasowaniu ruchu do reguły firewalla może zostać zapisana w logach (opcja **zapisz w logach**), lub wywołać **Alarm: priorytet niski** lub **Alarm: priorytet wysoki**, dzięki czemu dopasowanie zostanie zapisane w logach a dodatkowo będzie je można śledzić w Real Time Monitorze.
Harmonogram - Harmonogram jest opcją dopasowania a nie filtrowania ruchu. Dzięki wskazaniu obiektu harmonogramu możemy zdefiniować godziny lub dni, w których reguła jest aktywna i uwzględniana w ramach polityki filtrowania.

Brama - pozwala na trasowanie ruchu w ramach polityk filtrowania.
Kolejka QoS - pozwala na przypisanie ruchu do odpowiedniej kolejki QoS, czyli na priorytetyzowanie ruchu lub sterowanie pasmem.
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**, czyli system wykrywania i blokowania zagrożeń; **IDS**, czyli wykrywanie zagrożeń bez ich blokowania; tryb pracy **Firewall** powoduje, że nie działa moduł ASQ, czyli zagrożenia nie są ani wykrywane, ani tym bardzie blokowane.
Profil ASQ –wybór jednego z 10 profili prac ASQ. Wybór automatyczny 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.
Sekcja **Filtrowanie treści** - konfiguracja poniższych pól konfiguracji związana jest z działaniem modułów proxy:
Antywirus - włączenie/wyłączenie filtrowania ruchu http, ftp, smtp i pop3 za pomocą skanera AV.
Antyspam - włączenie/wyłączenie skanera antyspamowego dla ruchu smtp i pop3.
Filtrowanie URL - wybór jednego z 10 profili filtrowania URL dla ruchu http.
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 po nazwach CA dla ruchu SSL.

Uwaga

Reguły firewalla sprawdzane są w kolejności od pierwszej do ostatniej. Jeśli ruch nie wpadnie w żadną ze zdefiniowanych reguł zostanie on zablokowany przez politykę domyślną.

Analizator reguł

Analizator sprawdza poprawność konfiguracji firewalla, tzn sprawdza, czy stworzone reguły są poprawne pod względem użytych obiektów i metod skanowania ruchu oraz czy nie ma reguł pokrywających się lub sprzecznych. W przypasku wykrycia nieprawidłowośći **Analizator** wyświetli w dolnej części okna konfiguracyjnego alarm informujący o wykrytym problemie oraz symbolem regułę, dla której wykryto nieprawidłowość.Poniżej znajduje się przykładowy komunikat **Analizatora**.

Przykładowe reguły firewalla:

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

Akcja	Adres źródłowy	Adres docelowy	Port docelowy	Analiza protokołowa	Polityki filtrowania
zezwól	Network_LAN	Internet	http https		

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

Akcja	Adres źródłowy	Adres docelowy	Port docelowy	Analiza protokołowa	Polityki filtrowania
zezwól	Internet	Firewall_OUT	firewall_srv https ssh		

Zezwolenie na PING (ICMP) pomiędzy LAN a DMZ

Akcja	Adres źródłowy	Adres docelowy	Port docelowy	Analiza protokołowa	Polityki filtrowania
zezwól	Network_LAN	Network_DMZ	Any	wyłącznie icmp (echo reques	

Wskazówka

W systemie operacyjnym NS-BSD reguły filtrowania przechowywane są odpowiednio w:

/usr/Firewall/ConfigFiles/Filter/XX

Gdzie XX jeśli plikiem oznaczającym numer slotu (zestawu reguł).

W przypadku konfiguracji przy użyciu CLI, można aktywować poszczególny zestaw komendą:

enfilter XX

Gdzie XX to analogicznie numer slotu. Natomiast polecenie:

enfilter off

Wyłączy filtrowanie pakietów. Informacja o slotach, czyli ich nazwa i numer znajduje się w pliku:

/usr/Firewall/ConfigFiles/Filter/slotinfo

8. Konfiguracji translacji adresów (NAT)

Translacja adresów nazywana również maskaradą IP jest mechanizmem tłumaczenia adresów prywatnych sieci lokalnej na adresy publiczne otrzymane od operatora.

Rozróżnia się dwa podstawowe typy translacji:

SNAT (*Source Network Address Translation*) – polega na podmianie IP źródłowego w pakiecie. SNAT jest stosowany jest w przypadku podłączania sieci LAN z adresami prywatnymi do Internetu

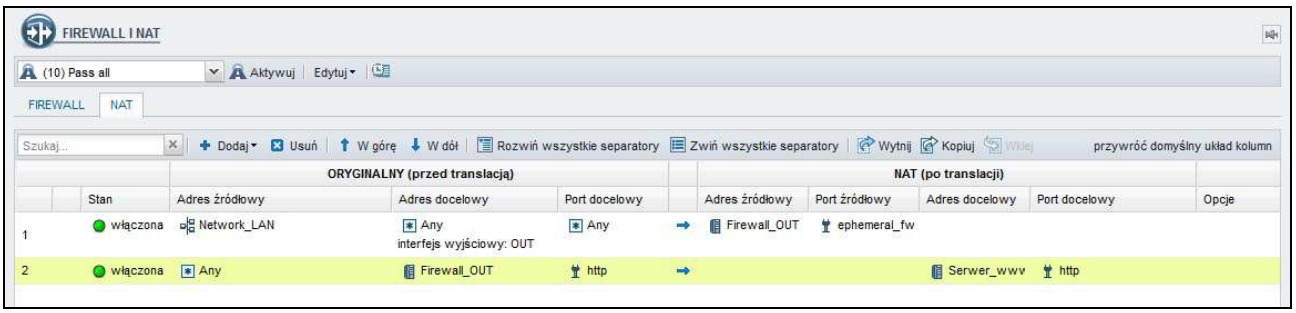
DNAT (*Destination Network Address Translation*) – polega na podmianie IP docelowego w pakiecie. DNAT jest stosowany do udostępniania w Internecie zasobów sieci wewnętrznej, które mają prywatny adres IP.

Można się również spotkać z jednoczesną translacją adresu źródłowego i docelowego tzw. Source and Destination NAT

Mechanizm NAT może służyć nie tylko do tłumaczenia adresów IP (nagłówka 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 translacją DNAT.

Konfiguracja NAT połączona jest z konfiguracją firewalla i znajduje się w sekcji **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.

Konfiguracja NAT w wersji 9 firmware polega na zdefiniowaniu jak powinien wyglądać nagłówek TCP/IP po przejściu pakietu przez urządzenie. Konfiguracja podzielona jest na dwa etapy. W pierwszym definiowane jest dopasowanie ruchu do reguły, jeśli oryginalny nagłówek pakietu znajdzie dopasowanie do reguły firewalla, to wykonywany jest drugi etap polegający na podmianie poszczególnych elementów nagłówka TCP/IP.



Dopasowanie ruchu do reguły NAT – pakiet **Oryginalny (przed translacją)**

Kolumna **Adres źródłowy**:

Użytkownik - uwierzytelniony użytkownik bazy LDAP
Adres źródłowy - źródło pochodzenia pakietu. Może to być pojedynczy komputer, zakres adresów, sieć, grupa adresów IP.
Interfejs wejściowy - wskazanie interfejsu do którego podłączony jest adres IP z którego pochodzi ruch.

Kolumna **Adres docelowy**:

Adres docelowy - adres przeznaczenia pakietu. Może to być pojedynczy komputer, zakres adresów, sieć, grupa adresów IP.
Interfejs wyjściowy – interfejs, którym pakiet opuści urządzenie.

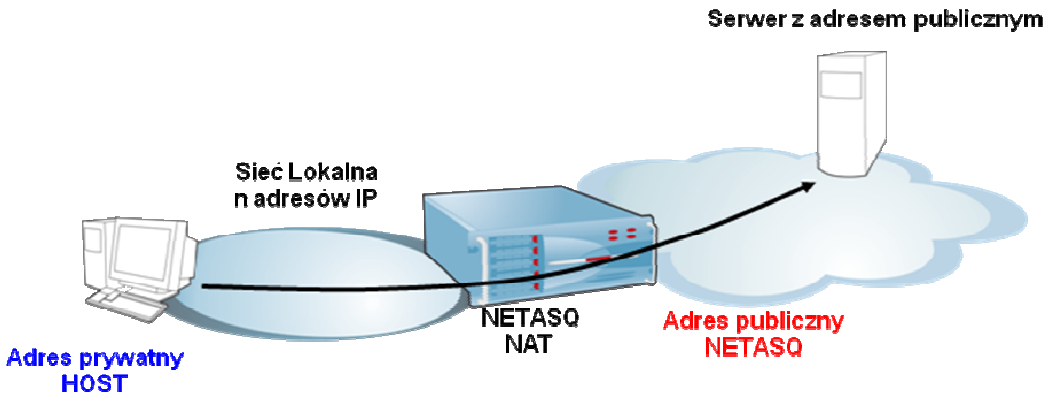
Kolumna **Port docelowy**:

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

Konfiguracja poszczególnych typów translacji

SOURCE NAT – MAP

Rysunek poniżej ilustruje wykorzystanie translacji adresów o nazwie SOURCE NAT. Chodzi o tłumaczenie adresu źródłowego po przejściu przez router z funkcją NAT. Jest to podmiana n-1, czyli ustawienie tłumaczenia n adresów prywatnych na 1 publiczny.



ORYGINALNY (przed translacją)

Adres źródłowy – Sieć LAN (dowolny adres z sieci LAN).
Adres docelowy – Any (dowolny docelowy adres IP), ale ruch musi być trasowany przez interfejs OUT.
Port docelowy – Any.

NAT (po translacji)

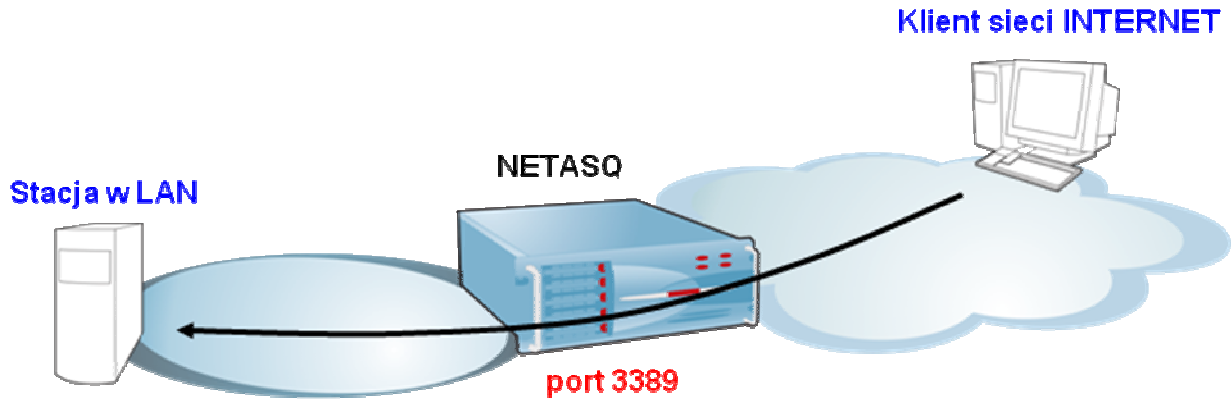
Adres źródłowy – Firewall_OUT, obiekt reprezentujący publiczny adres IP urządzenia. Jeśli ruch ma być natowany na adres publiczny, ale taki, który nie jest przypisany do interfejsu urządzenia konieczne jest wybranie opcji **Publikacja ARP**.
Port źródłowy – ephemeral_fw, pula losowych portów wysokich.
Adres docelowy – Any lub puste pole, oznacza, że adres docelowy zostanie pozostawiony z oryginalnego nagłówka IP.
Port docelowy – Any lub puste pole, oznacza, że port docelowy zostanie pozostawiony z oryginalnego nagłówka TCP/UDP.

Jak czytać translację SNAT?

Każde połączenie pochodzące z sieci LAN, które jest kierowane do Internetu i opuści urządzenie interfejsem OUT zostanie poddane translacji, po której adres źródłowy zostanie zmieniony na adres publiczny urządzenia a port źródłowy zostanie nadpisany nowym portem wysokim natomiast adres docelowy ruchu nie ulegnie zmianie.

DESTINATION NAT – REDIRECT

Translacja Destination NAT jest przydatna w przypadku przekierowania usług z zewnętrznego interfejsu NETASQ do sieci lokalnej na adres prywatny. Można sobie wyobrazić sytuacje np. przekierowania połączenia zdalnego pulpitu (Microsoft-Terminal-Serice).



Klient sieci Internet będzie łączył się na adres publiczny urządzenia NETASQ, a następnie nastąpi przekierowanie na adres lokalny do sieci LAN. Reguła na 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	→			Serwer	microsoft-ts

ORYGINALNY (przed translacją)

Adres źródłowy – Internet (ruch przychodzący z poza sieci wewnętrznych)
Adres docelowy – Firewall_OUT, obiekt reprezentujący publiczny adres IP urządzenia. Jeśli adres docelowy oryginalnego połączenia jest inny niż przypisany do interfejsu urządzenia konieczne jest wybranie opcji **Publikacja ARP**.
Port docelowy – Port, na który nawiązywane jest oryginalne połączenie.

NAT (po translacji)

Adres źródłowy – Any lub puste pole, oznacza, że adres źródłowy zostanie pozostawiony z oryginalnego nagłówka IP.
Port źródłowy – Any lub puste pole, oznacza, że port źródłowy zostanie pozostawiony z oryginalnego nagłówka TCP/UDP.
Adres docelowy – Obiekt reprezentujący prywatny adres IP serwera docelowego.
Port docelowy – Port na którym działa usługa na serwerze docelowym

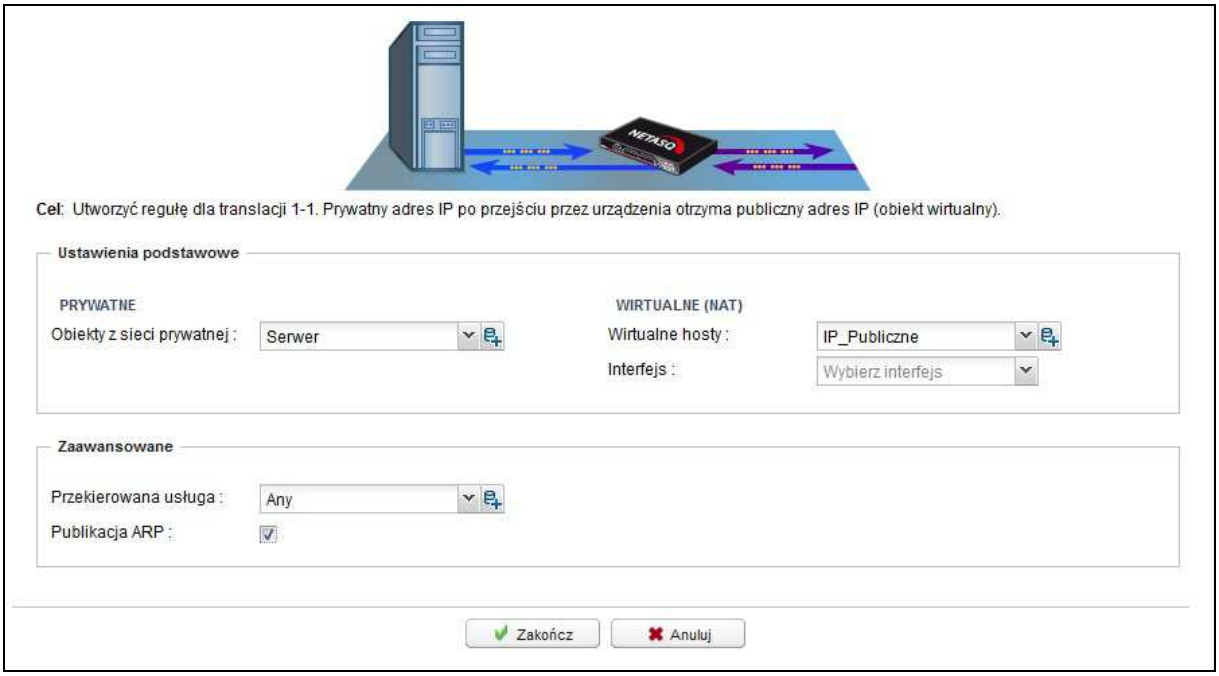
Jak czytać translację DNAT?

Każde połączenie z Internetu, które jest nawiązywane na publiczny adres urządzenia na port microsoft-ts (3389) zostanie poddane translacji NAT w ramach której adres źródłowy i port źródłowy nie zmienią się, natomiast zmianie ulegnie adres docelowy, na prywatny adres IP serwera terminali z zachowaniem portu docelowego.

BI-DIRECTIONAL MAP

Operacja BI-MAP jest translacją typu 1:1, tzn. pozwala na przypisanie adresowi IP z sieci lokalnej wirtualnego adresu publicznego. Translacja BI-Directionam 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. Akcję tą stosuje się najczęściej w przypadku wystawienia kiedy serwer ma być widoczny w Internecie pod tym samym adresem, pod którym odbiera połączenia przychodzące do niego, czyli np. serwer pocztowy.

Konfiguracja translacji BI-MAP odbywa się poprzez **Kreator reguły BIMAP (1:1)**.



Zakończenie pracy kreatora owocuje utworzeniem dwóch reguł, jednej dla ruchu wychodzącego z Serwera do Internetu i drugiej dla ruchu przychodzącego z Internetu na publiczny adres IP NETASQ. Ponieważ publiczne IP nie jest zdefiniowane na interfejsie urządzenia należy włączyć opcję **Publikacja ARP**.

ORYGINALNY (przed translacją)				NAT (po translacji)			
Adres źródłowy	Adres docelowy	Port docelowy		Adres źródłowy	Port źródłowy	Adres docelowy	Port docelowy
Serwer	Any	Any	→	IP_Publiczr			
Any	IP_Publiczne	Any	→			Serwer	

9. System wykrywania i blokowania włamań ASQ (IPS)

System Intrusion Prevention w urządzeniach NETASQ wykorzystuje unikalną, stworzoną w laboratoriach firmy NETASQ 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 sygnatury kontekstowe.

Analiza heurystyczna

W analizie heurystycznej podstawę stanowi statystyka 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 tym standardem może zostać przepuszczony. Kontroli poddawane są nie tylko poszczególne pakiety ale także połączenia i sesje. W ramach technologii ASQ dla poszczególnych typów ruchu sieciowego warstwy aplikacji opracowane zostały specjalne plug-iny (wtyczki programowe) pracujące w trybie kernel-mode. Po wykryciu określonego typu ruchu (np. HTTP, FTP, SMTP, TELNET itp.) automatycznie uruchamiany jest odpowiedni plug-in, który specjalizuje się w ochronie danego protokołu. Tym samym, rodzaj stosowanych zabezpieczeń jest w sposób dynamiczny dostosowywany do rodzaju przepływającego ruchu.

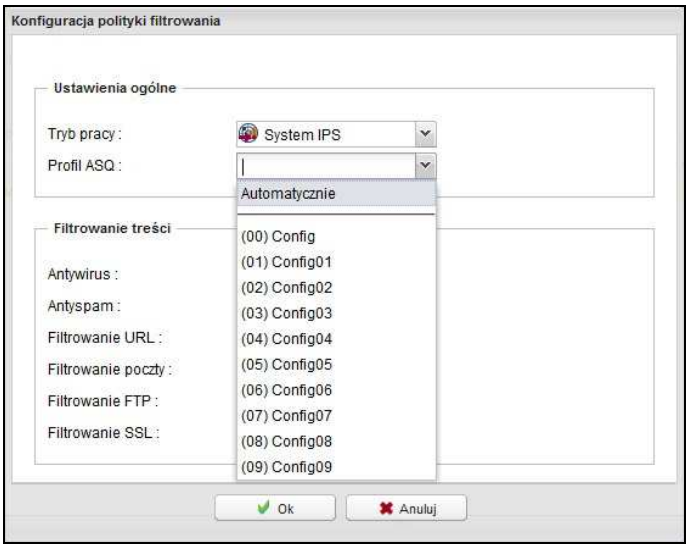
Sygnatury kontekstowe

Ostatni z elementów, to systematycznie aktualizowane sygnatury kontekstowe. Pozwalają 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 jednoczesnym ograniczeniu niemal do zera ilości fałszywych alarmów. Innym istotnym czynnikiem wpływającym na wydajność stosowania części sygnatur jest ich optymalizacja pod kontem skanowania luk występujących w aplikacjach czy protokołach. Jeśli kilka ataków wykorzystuje tę sama lukę tworzona jest tylko jedna sygnatura dla luki 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 natomiast taki, którego pierwszy pakiet transmisji pojawi się na interfejsie Wewnętrznym. Konfigurację profili domyślnych przeprowadza się w sekcji **Kontrola aplikacji -> Ustawienia profili**, gdzie domyślnie ruch przychodzący skanowany jest profilem **(0) Config**, a ruch wychodzący profilem **(1) Config01**.

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 **Automatyczny** na wybrany przez nas profil.



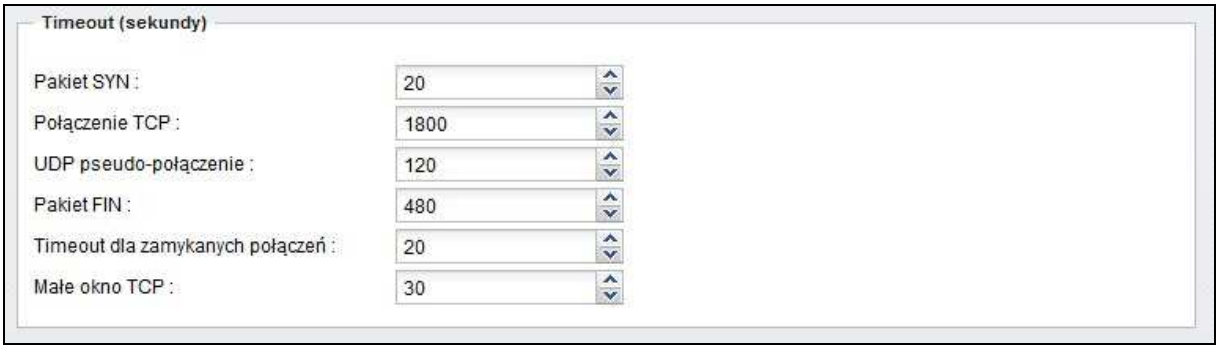
Konfiguracja analizy protokołów

Konfiguracja skanowania protokołów poprzez mechanizm IPS znajduje się w sekcji **Kontrola aplikacji -> Analiza protokołów**. Znajduje się tutaj konfiguracja pluginów dla wszystkich najważniejszych protokołów z warstw od trzeciej (L3) do siódmej (L7) modelu ISO/OSI przy czym każdy z pluginów zawiera pola konfiguracyjne charakterystyczne dla każdego z protokołów.

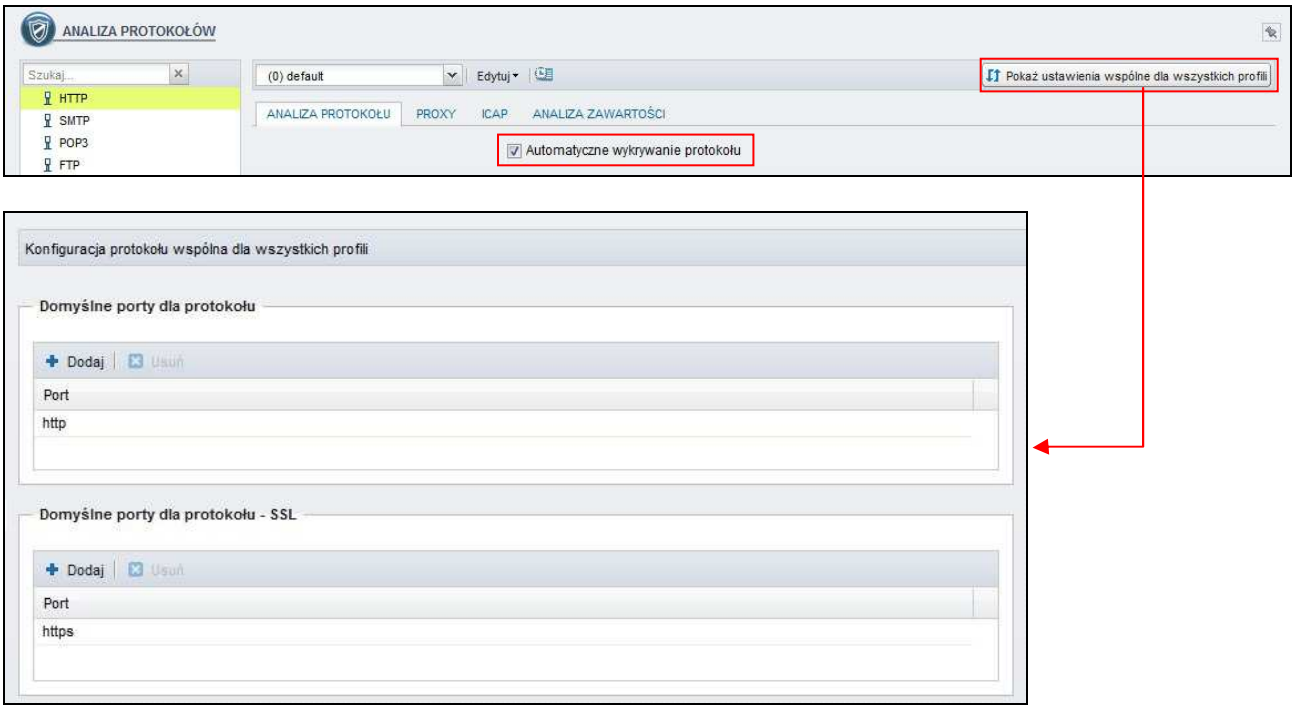
W początkowej fazie transmisji danych używane są pluginy IP oraz TCP/UDP. Odpowiadają one za prawidłowe otwarcie sesji a więc:

Plugin IP – odpowiada za fragmentację pakietów i ich wielkość

Plugin TCP/UDP – odpowiada za otwieranie, trwanie i zamykanie sesji.



Po otwarciu sesji podłączane są pluginy odpowiednie dla każdego z protokołów. O tym jaki plugin będzie użyty decyduje port na którym odbywa się komunikacja. Wybierając opcję **Pokaż ustawieniach wspólnych dla wszystkich profili** w konfiguracji pluginu mamy możliwość zdefiniowania dla komunikacji 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.



Sygnatury kontekstowe

Sygnatury służą do filtrowania ruchu pod kontem wystąpienia cech charakterystycznych dla konkretnej luki 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 **Kontrola aplikacji -> Alarmy**.

Okno Alarmów zawiera następujące elementy:

Kontekst – określa plugin jakim dane połączenie jest obsługiwane, poza kontekstem podawane jest również ID sygnatury, co ułatwia przeszukiwanie sygnatur.
Alarm – nazwa alarmu/sygnatury.
Akcja – Zablokuj/Zezwól ruch sieciowy.
Priorytet – określa poziom ważności alarmu. Alarmy z priorytetem Wysokim lub Niskim pojawiają się w RTM oraz są zapisywane w logach. Alarmy, dla których ustawiona jest akcja Ignoruj nie są wyświetlane, opcja ta jest przydatna jeśli jakiś alarm „zaśmieca” logi.

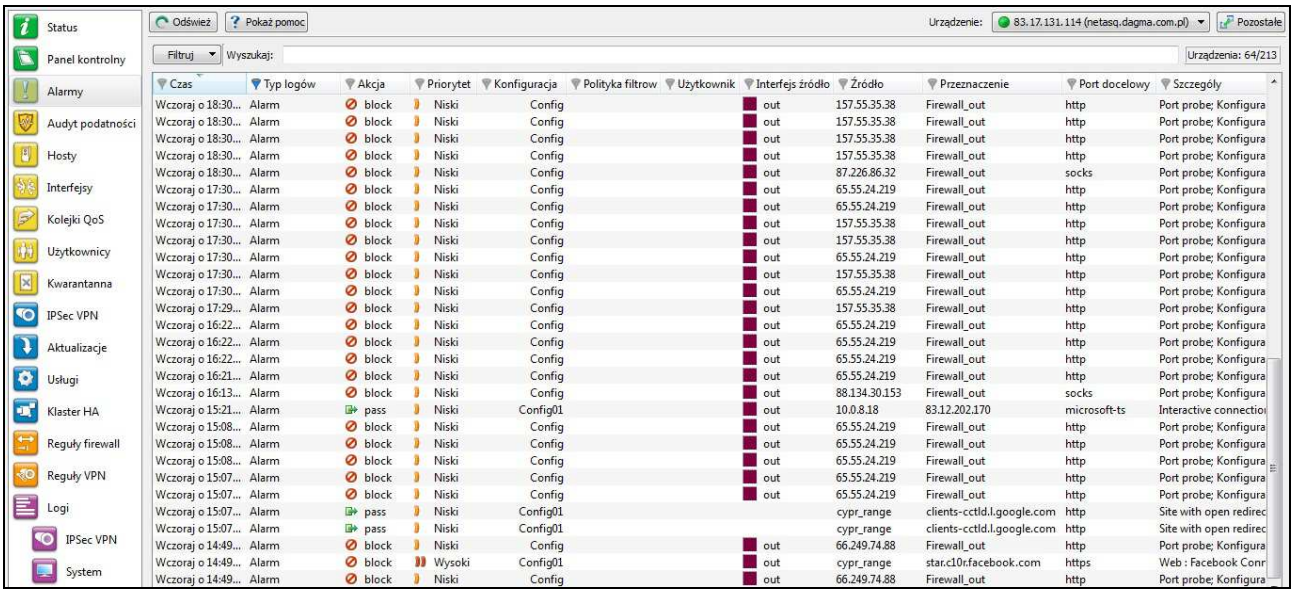
Nowy – w tej kolumnie dla każdej nowej sygnatury pojawia się symbol (wykrzyknika). Ma to na celu wyróżnienie nowych sygnatur, z którymi administrator powinien się zapoznać.
Zaawansowane – pozwala na podjęcie dodatkowych akcji takich jak wysłanie alertu mailowego czy wykonanie zrzutu tcpdump pakietów.

Uwaga

Profile **Analizy protokołów** i **sygnatur** są ze soba ściśle powiązane, tzn. profil 00 Analizy protokołów oraz profil 00 Alarmów tworzą **Profil ASQ 00**, a profil 02 Analizy protokołów oraz profil 02 Alarmów tworzą **Profil ASQ 02**. Profil ASQ jest filtrem IPS implementowanym na poziomie reguł firewalla.

Monitorowanie działania IPS

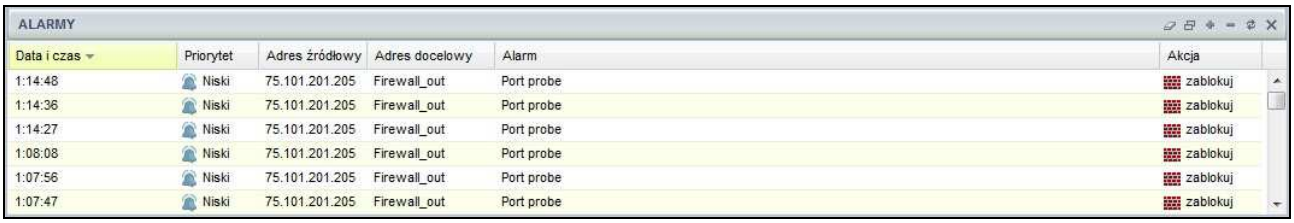
Działanie systemu IPS możemy monitorować z poziomu **Real Time Monitora**. W zakładce Alarmy można znaleźć informacje o filtrowanym ruchu, w przypadku systemu IPS będą to wpisy typu Alarm.



Czas	Typ logów	Akcja	Priorytet	Konfiguracja	Polityka filtrow	Użytkownik	Interfejs źródło	Źródło	Przeznaczenie	Port docelowy	Szczegóły
Wczoraj o 18:30...	Alarm	block	Niski	Config			out	157.55.35.38	Firewall_out	http	Port probe; Konfigura
Wczoraj o 18:30...	Alarm	block	Niski	Config			out	157.55.35.38	Firewall_out	http	Port probe; Konfigura
Wczoraj o 18:30...	Alarm	block	Niski	Config			out	157.55.35.38	Firewall_out	http	Port probe; Konfigura
Wczoraj o 18:30...	Alarm	block	Niski	Config			out	157.55.35.38	Firewall_out	http	Port probe; Konfigura
Wczoraj o 18:30...	Alarm	block	Niski	Config			out	87.226.86.32	Firewall_out	socks	Port probe; Konfigura
Wczoraj o 17:30...	Alarm	block	Niski	Config			out	65.55.24.219	Firewall_out	http	Port probe; Konfigura
Wczoraj o 17:30...	Alarm	block	Niski	Config			out	65.55.24.219	Firewall_out	http	Port probe; Konfigura
Wczoraj o 17:30...	Alarm	block	Niski	Config			out	157.55.35.38	Firewall_out	http	Port probe; Konfigura
Wczoraj o 17:30...	Alarm	block	Niski	Config			out	157.55.35.38	Firewall_out	http	Port probe; Konfigura
Wczoraj o 17:30...	Alarm	block	Niski	Config			out	65.55.24.219	Firewall_out	http	Port probe; Konfigura
Wczoraj o 17:30...	Alarm	block	Niski	Config			out	157.55.35.38	Firewall_out	http	Port probe; Konfigura
Wczoraj o 17:30...	Alarm	block	Niski	Config			out	65.55.24.219	Firewall_out	http	Port probe; Konfigura
Wczoraj o 17:29...	Alarm	block	Niski	Config			out	157.55.35.38	Firewall_out	http	Port probe; Konfigura
Wczoraj o 16:22...	Alarm	block	Niski	Config			out	65.55.24.219	Firewall_out	http	Port probe; Konfigura
Wczoraj o 16:22...	Alarm	block	Niski	Config			out	65.55.24.219	Firewall_out	http	Port probe; Konfigura
Wczoraj o 16:22...	Alarm	block	Niski	Config			out	65.55.24.219	Firewall_out	http	Port probe; Konfigura
Wczoraj o 16:21...	Alarm	block	Niski	Config			out	65.55.24.219	Firewall_out	http	Port probe; Konfigura
Wczoraj o 16:13...	Alarm	block	Niski	Config			out	88.134.30.153	Firewall_out	socks	Port probe; Konfigura
Wczoraj o 15:21...	Alarm	pass	Niski	Config01			out	10.0.8.18	83.12.202.170	microsoft-ts	Interactive connectio
Wczoraj o 15:08...	Alarm	block	Niski	Config			out	65.55.24.219	Firewall_out	http	Port probe; Konfigura
Wczoraj o 15:08...	Alarm	block	Niski	Config			out	65.55.24.219	Firewall_out	http	Port probe; Konfigura
Wczoraj o 15:08...	Alarm	block	Niski	Config			out	65.55.24.219	Firewall_out	http	Port probe; Konfigura
Wczoraj o 15:07...	Alarm	block	Niski	Config			out	65.55.24.219	Firewall_out	http	Port probe; Konfigura
Wczoraj o 15:07...	Alarm	block	Niski	Config			out	65.55.24.219	Firewall_out	http	Port probe; Konfigura
Wczoraj o 15:07...	Alarm	pass	Niski	Config01				cypr_range	clients-cctld.l.google.com	http	Site with open redirec
Wczoraj o 15:07...	Alarm	pass	Niski	Config01				cypr_range	clients-cctld.l.google.com	http	Site with open redirec
Wczoraj o 14:49...	Alarm	block	Niski	Config			out	66.249.74.88	Firewall_out	http	Port probe; Konfigura
Wczoraj o 14:49...	Alarm	block	Wysoki	Config01			out	cypr_range	star.c10r.facebook.com	https	Web : Facebook Conr
Wczoraj o 14:49...	Alarm	block	Niski	Config			out	66.249.74.88	Firewall_out	http	Port probe; Konfigura

Z tego poziomu możliwe jest również wyświetlenie pomocy – opisu danego alarmu.

Innymi miejscem gdzie można sprawdzić działanie IPS jest widget **Alarmy** w **Panelu kontrolnym** dostępnym z poziomu WebGUI. Użycie tego okna jest być może wygodniejsze, ale nie daje tak dokładnego logu jak **Real Time Monitor**.



Uwaga

NETASQ w wersji 9 nie posiada funkcji „bypass". Funkcja ta została zastąpiona poprzez wprowadzenie opcji **Polityki filtrowania -> Firewall (Klasyczny firewall)** w konfiguracji reguł zapory.

10. Konfiguracja Audytu podatności (SEISMO)

Moduł Audytu podatności jest pasywnym skanerwm wnętrza 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 przesyłany poprzez urządzenia w kontekście luk w aplikacjach sieciowych i systemach operacyjnych zainstalowanych na komputerach. Audyt podatności wymaga zakupu dodatkowej licencji.

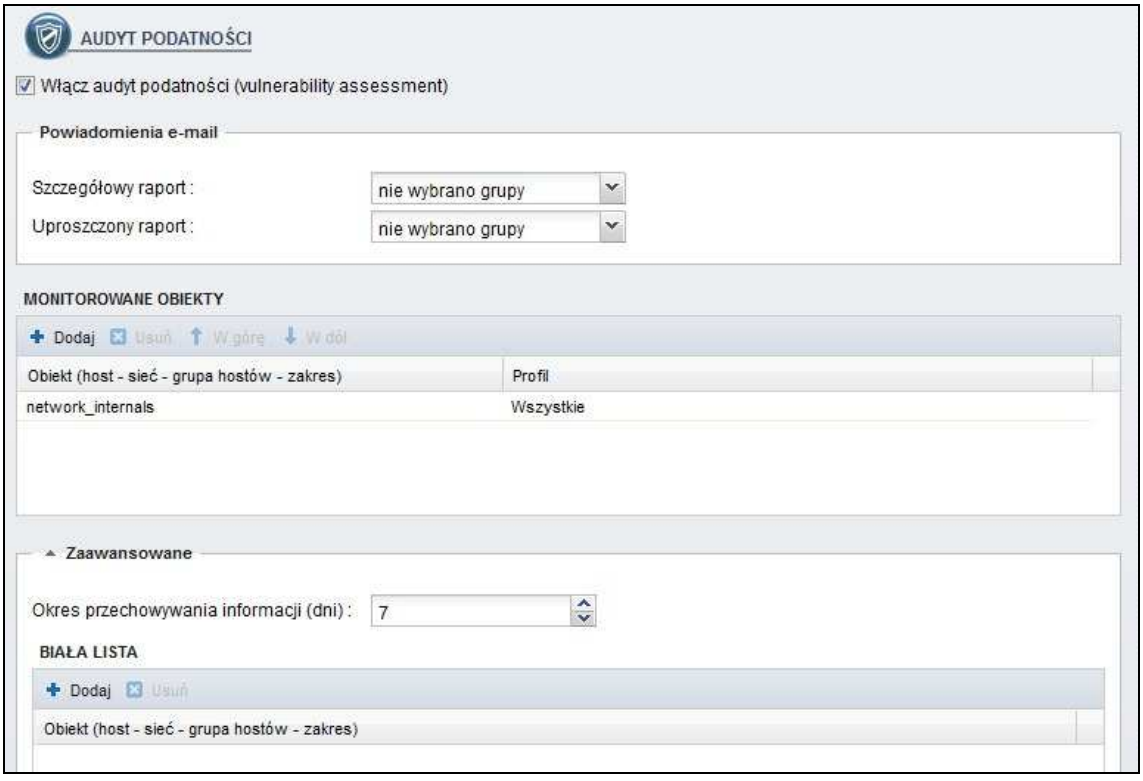
Konfiguracja Audytu podatności odbywa się w zakładce **KONTROLA APLIKACJI -> Audyt podatności**. Jeśli opcja jest wyszarzona oznacza to, iż zainstalowana na urządzeniu licencja nie ma aktywnej funkcji pasywnego skanera sieci.

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

W przypadku konfiguracji audytu podatności istotne jest :

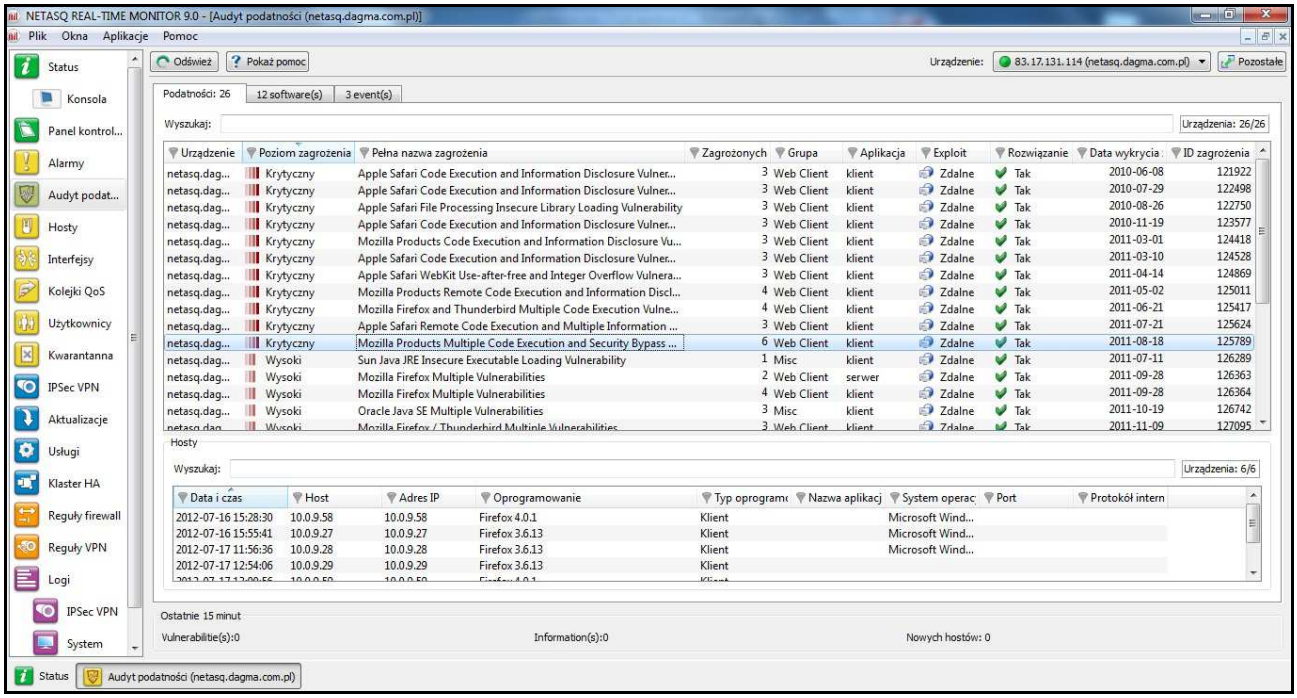
- Określenie komputerów i serwerów, które mają być monitorowane.
- Określenie pod kątem jakiego typu zagrożeń skanowane będą komputery.
- Skonfigurowanie czasu przez jaki informacje o wykrytych zagrożeniach będą przechowywane.
- Zdefiniowanie wykluczeń ze skanowania.

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

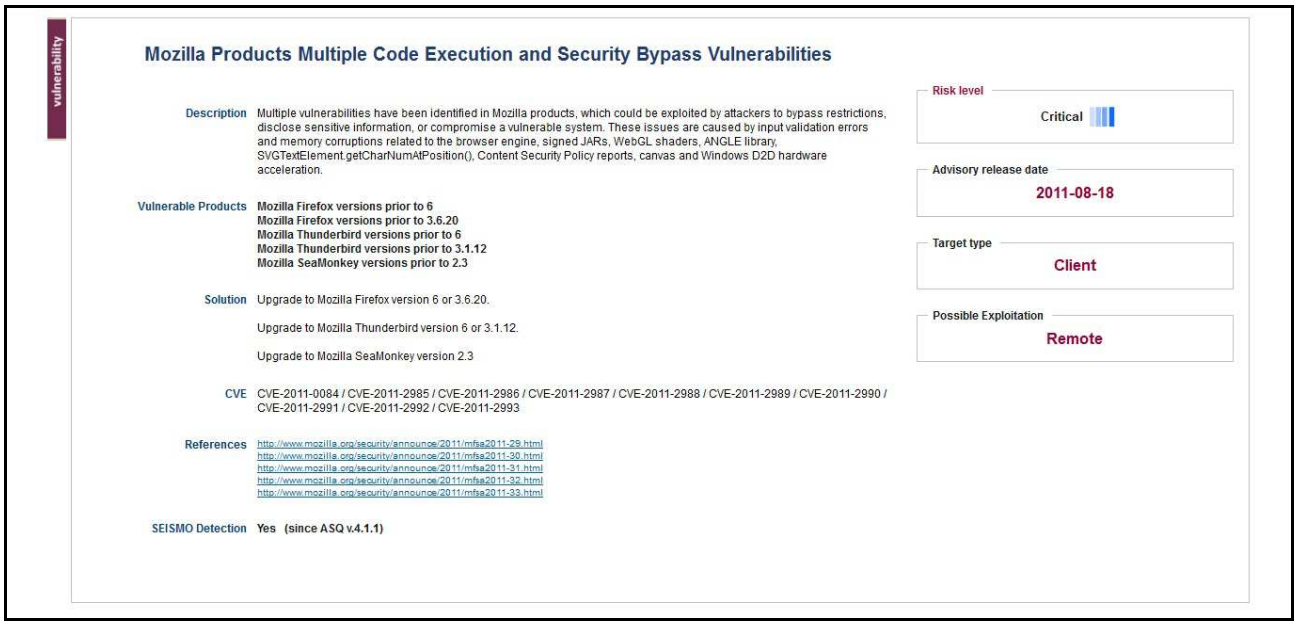


Informacje zebrane przez moduł **Audytu podatności** najłatwiej przeglądać za pomocą **NETASQ Real Time Monitor**.

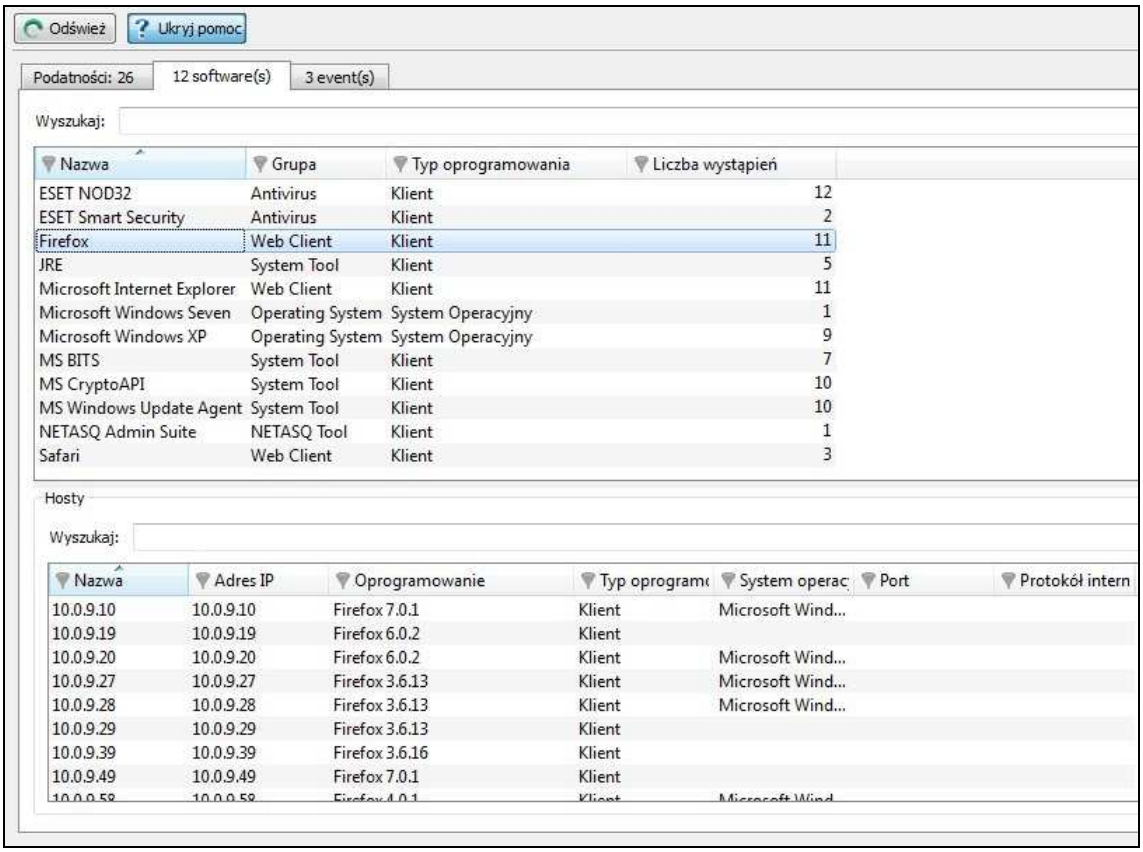
Poniżej przedstawiony jest przykładowy wynik skanowania przeprowadzonego przez SEISMO:



W raporcie znajdziemy między innymi informację o poziomie ważności wykrytego zagrożenia, typie zagrożenia (Klient – Web client itp.) oraz sposobie jego wywołania (Zdalne/Lokalne). Po kliknięciu w wykrytą lukę znajdziemy dodatkowo informacje o komputerach, na których została wykryta podatna aplikacja oraz o tym w jakiej ta aplikacja jest wersji. Aby uzyskać dodatkowe informacje o zagrożeniu można wybrać w górnej części okna opcję **Pokaż pomoc**. W oknie pomocy można znaleźć dokładny opis zagrożenia, linki do stron na których zostało ono opisane oraz wyjaśnienie jakie czynności należy podjąć, aby wyeliminować zagrożenie z sieci.



Audyt podatności jest także doskonałym narzędziem do monitorowania zainstalowanych aplikacji sieciowych i systemów operacyjnych, które łączą się poprzez NETASQ. Od wersji 8 firmware taka informacja jest wyświetlana bezpośrednio w konsoli NETASQ Real Time Monitora :



11. Autoryzacja użytkowników

Rozwiązanie NETASQ UTM pozwala na wykorzystanie trzech typów baz użytkowników:

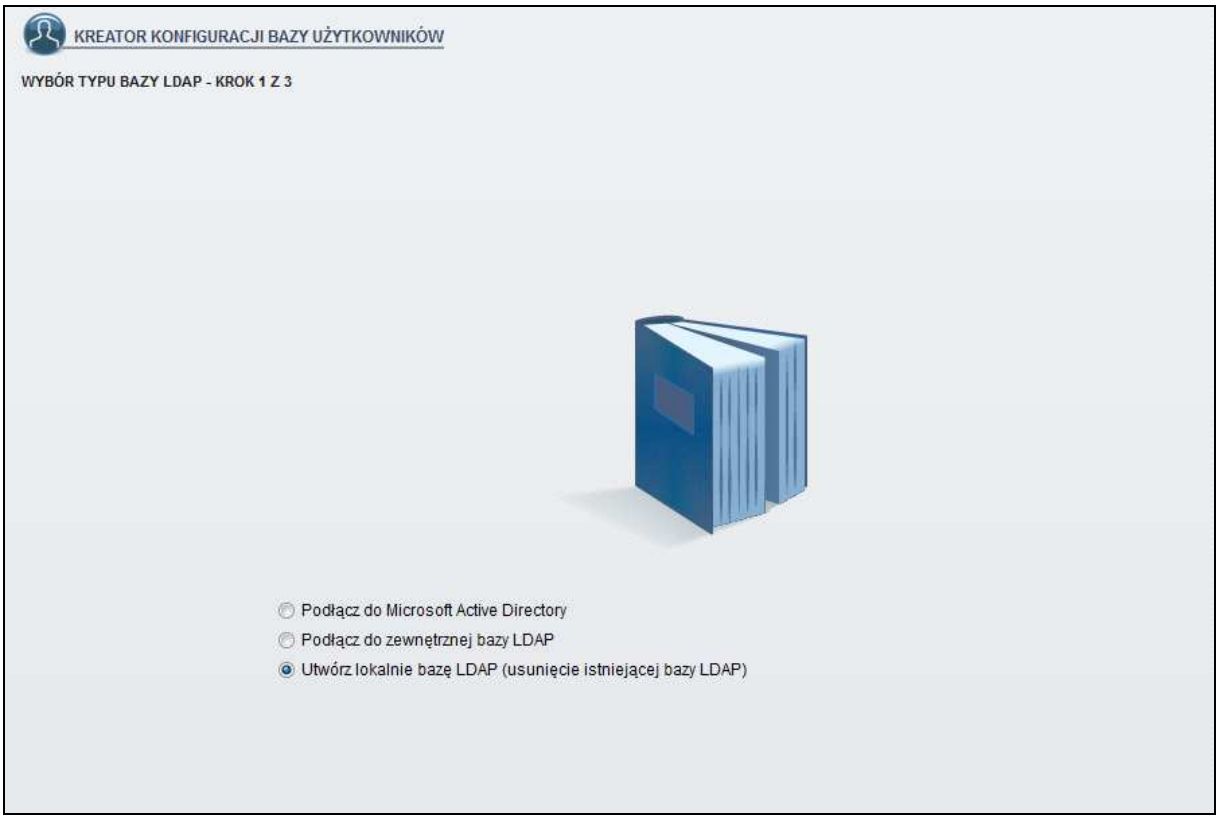
- Zewnętrzna baza zgodna z LDAP – OpenLDAP, Novell eDirectory;
- Microsoft Active Direcotry;
- Wewnętrzna baza LDAP.

Każdą w tych baz można wykorzystać do:

- tworzenia reguł firewalla zgodnie z użytkownikiem zalogowanym na stacji a nie tylko adresu komputera;
- tworzenia tuneli VPN typu Client-to-Site;
- delegowania zadań administracji urządzeniem na użytkowników.

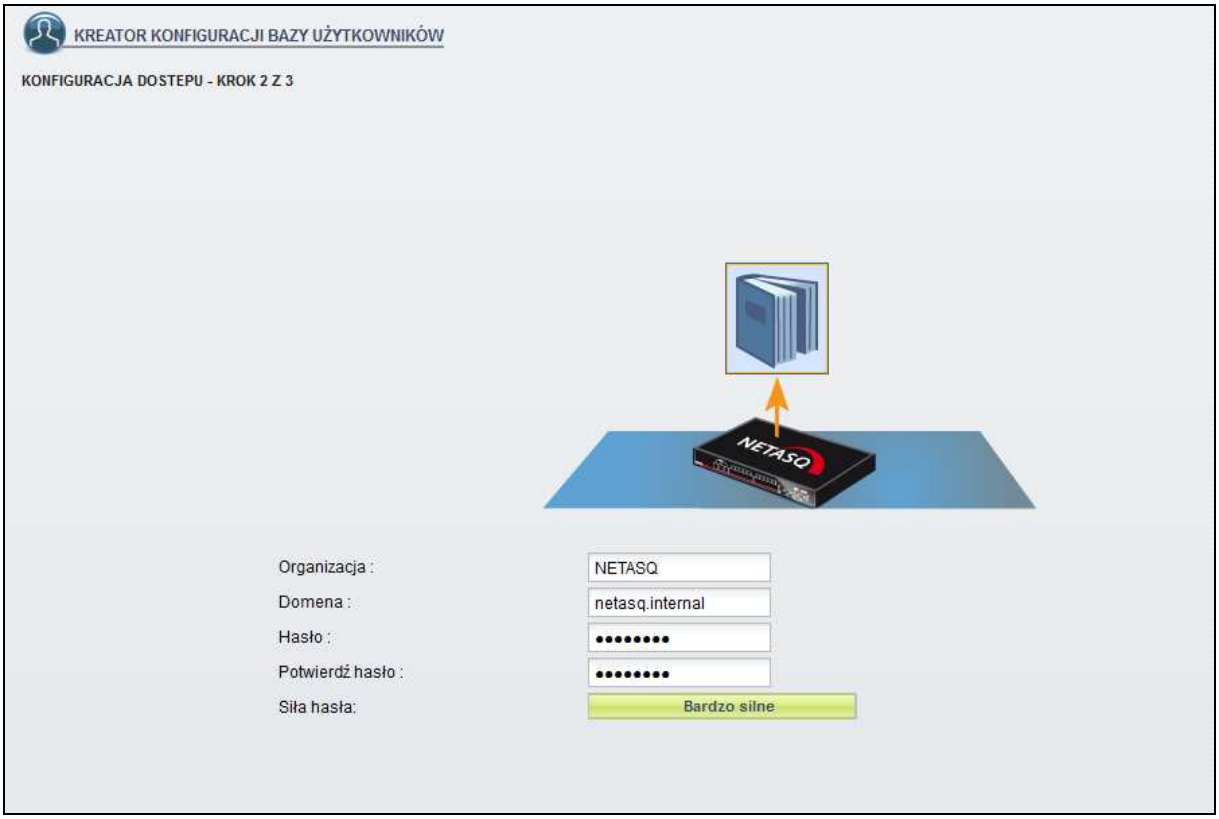
Tworzenie wewnętrznej bazy użytkowników

Aby skonfigurować wewnętrzną bazę użytkowników na urządzeniu NETASQ należy przejść na zakładkę **Użytkownicy -> Konfiguracja bazy LDAP** i wybrać opcję **Utwórz lokalną bazę LDAP**.



W kolejnym oknie konfiguracyjnym należy w polu:

Organizacja: podać nazwę firmy np. NETASQ
Domena: nazwa domeny
Hasło i **Potwierdź hasło**: hasło administratora domeny, może być użyte do integracji zewnętrznej usługi z bazą LDAP.

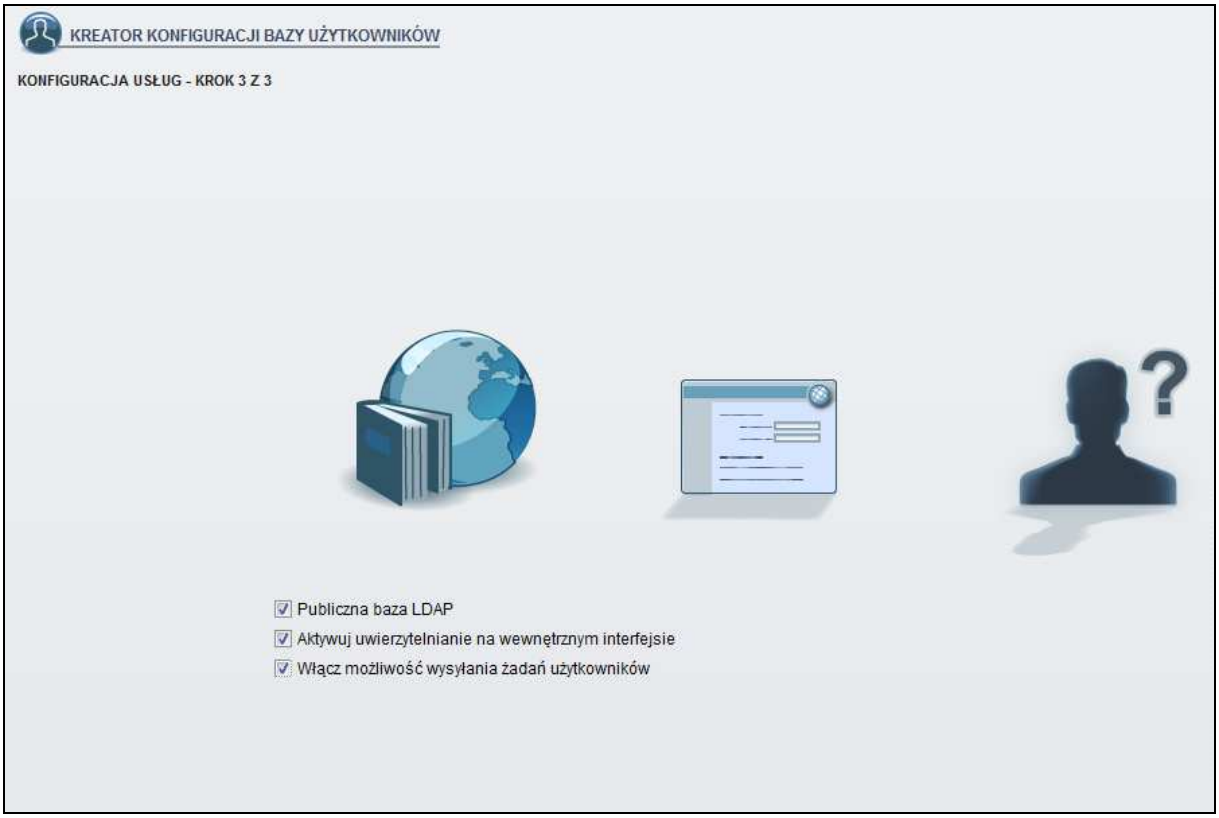


W kolejnym oknie konfiguracji można skonfigurować dodatkowe opcje bazy LDAP:

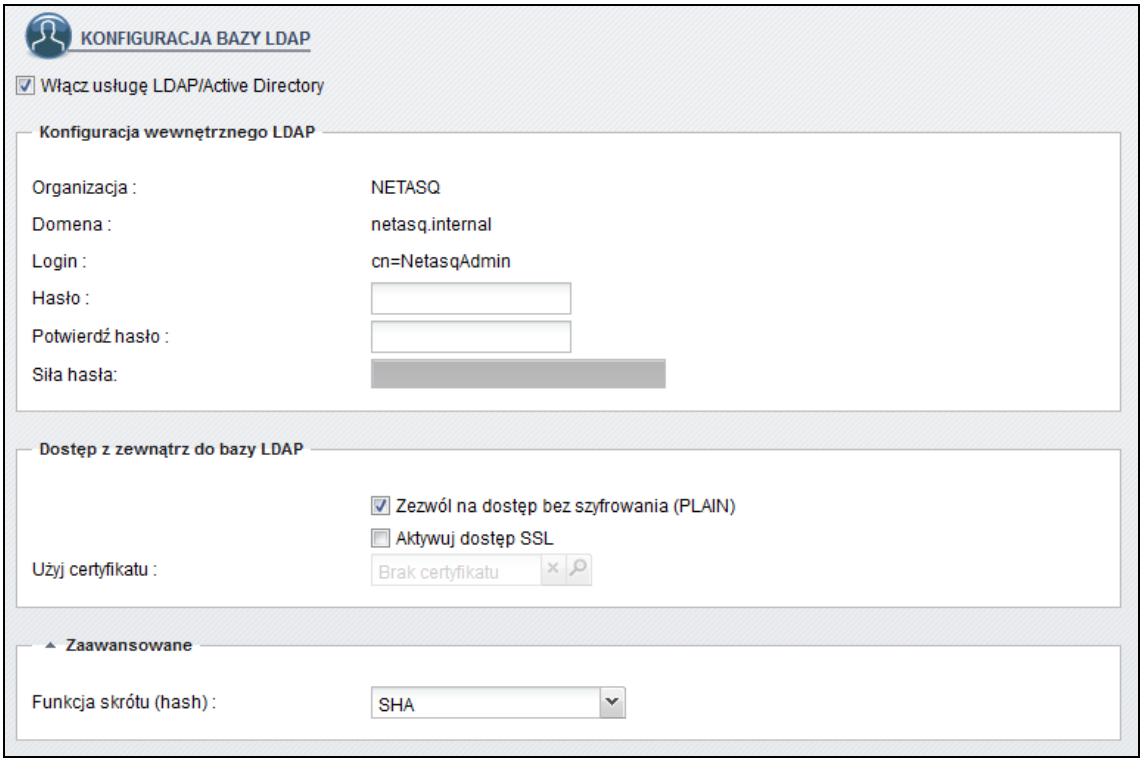
Publiczna baza LDAP – baza użytkowników może być wykorzystywana przez inne usługi sieciowe takie jak np. serwer FTP.

Aktywuj uwierzytelnianie na wewnętrznym interfejsie – na interfejsach wewnętrznych zostanie automatycznie uruchomiony portal autoryzacyjny użytkowników (Captive portal).

Włącz możliwość wysyłania żądań użytkowników – 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.



Wybranie przycisku **Zakończ** zakończy prace i pokaże okno konfiguracyjne bazy LDAP, w którym możemy wybrać między innymi czy komunikacja z bazą LDAP ma odbywać się w formie zaszyfrowanej czy też nie oraz jakim algorytmem szyfrowane są hasła użytkowników w bazie LDAP.



Integracja NETASQ z Microsoft Active Directory

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

W kolejnym oknie konfiguracyjnym należy w polu:

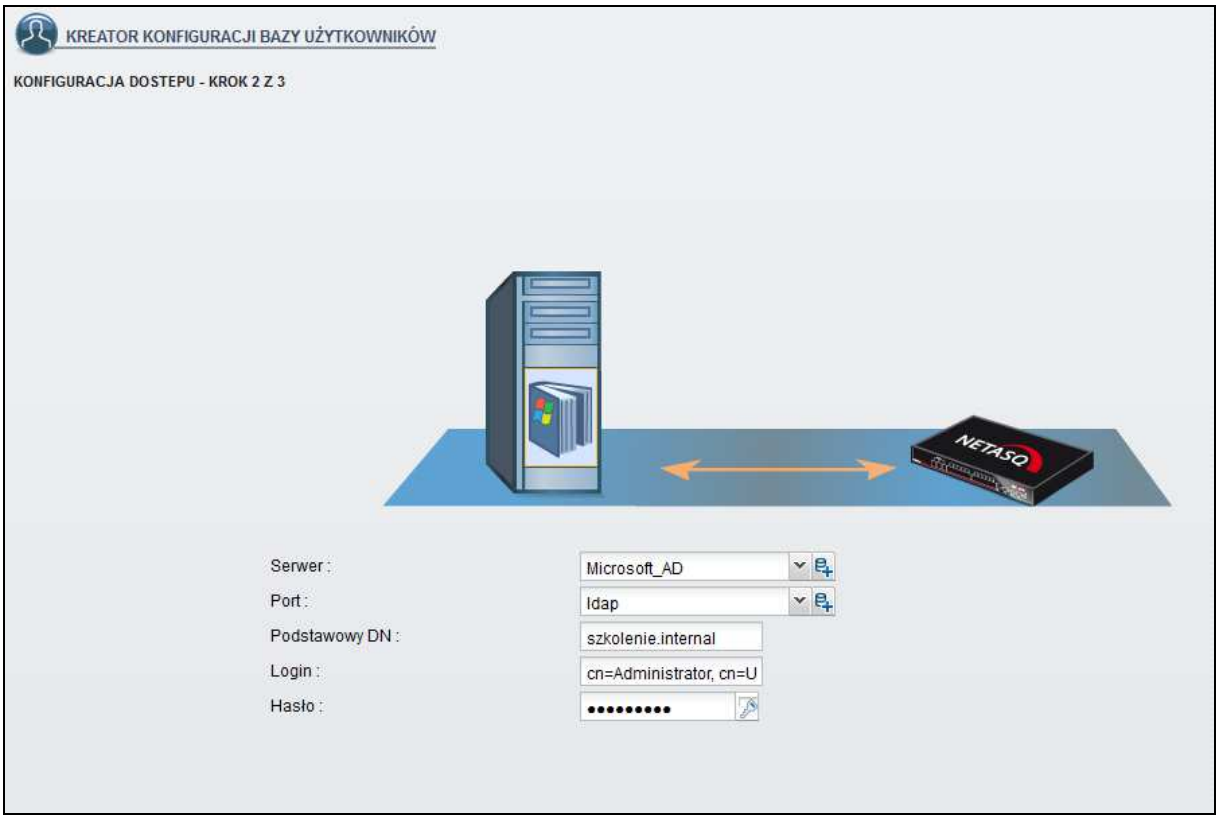
Serwer – wskazać obiekt reprezentujący IP kontrolera domeny

Port – wybrać port używany do komunikacji z LDAP – domyślnie 389

Podstawowy DN – podać pełną nazwę domeny z jaką integrujemy NETASQ, np.: **netasq.internal**

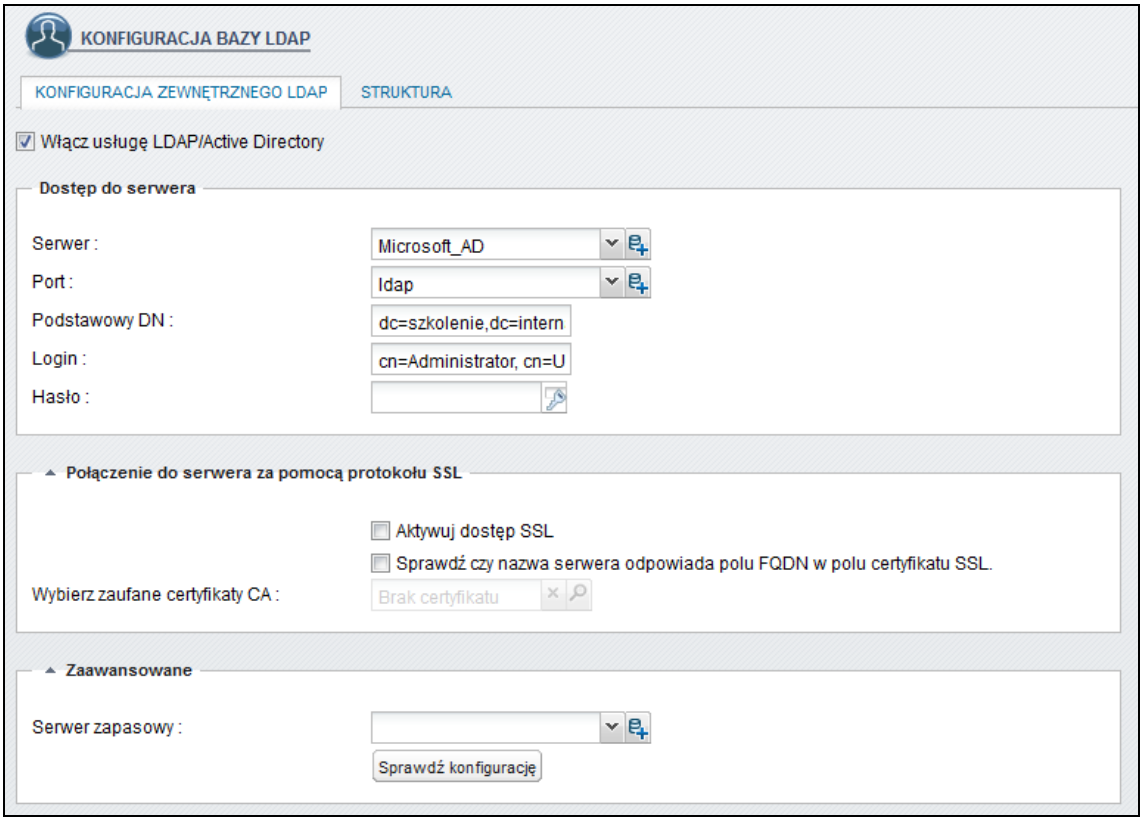
Login – podać login użytkownika używanego do integracji z AD wraz ze wskazaniem kontenera (CN) lub jednostką organizacyjną (OU) AD w którym znajduje się ten użytkownik. Jeśli do integracji używamy wbudowanego konta *Administratora*, który domyślnie znajduje się w kontenerze *Users*, to w polu ***Login*** należy wpisać: *cn=Administrator, cn=Users*.

Hasło – podać hasło domenowe użytkownika wskazanego w polu Login.

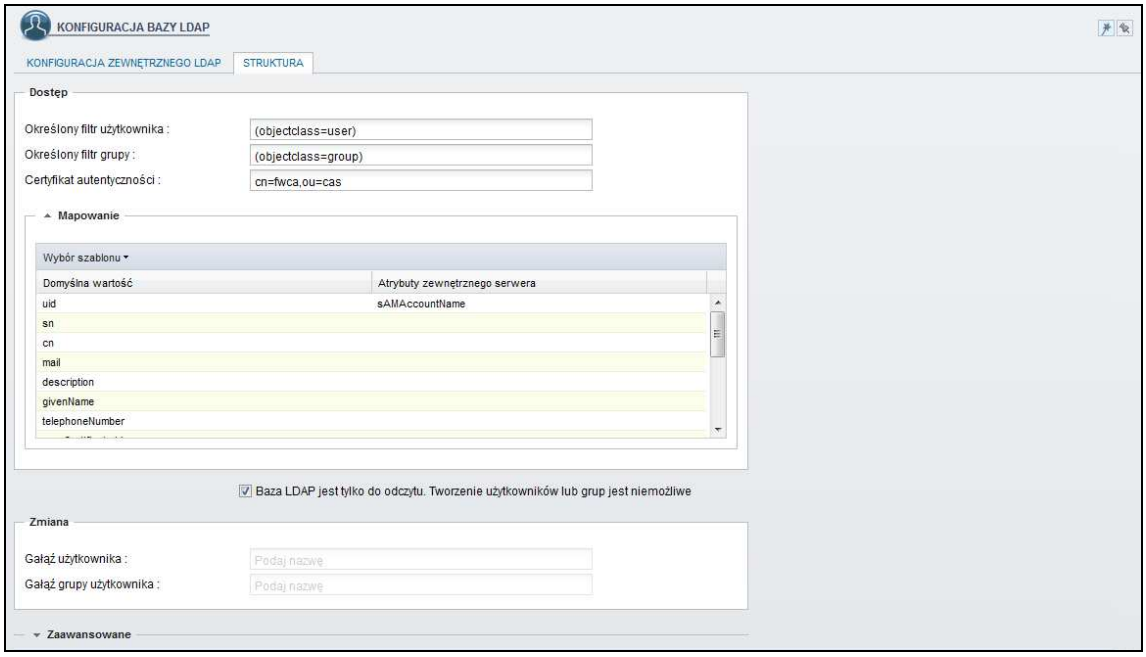


W kolejnym oknie kreatora można włączyć opcję **Aktywuj uwierzytelnianie na wewnętrznym interfejsie**.

Po zakończeniu pracy kreatora powinno pojawić się okno jak poniżej, co jest potwierdzeniem poprawnej integracji.



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

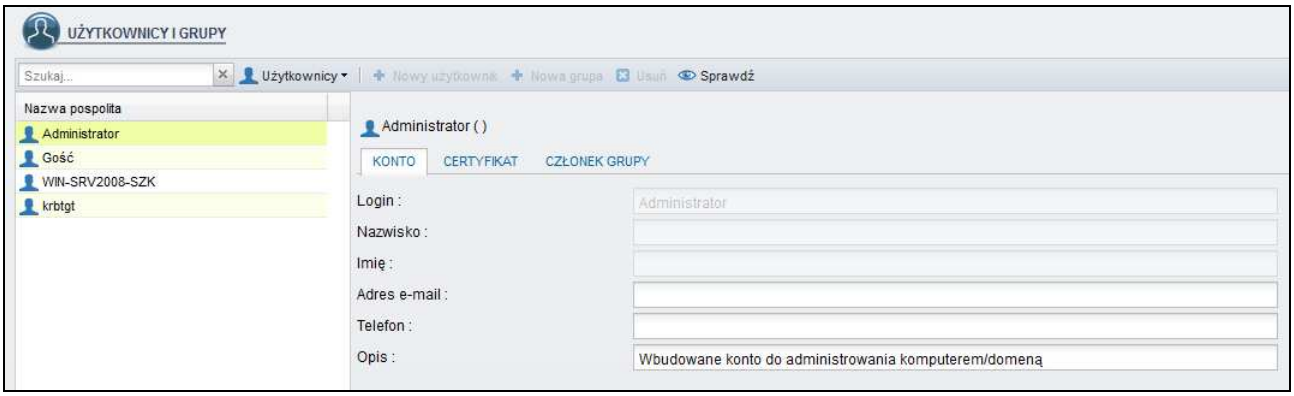


Wskazówka

Jeśli na urządzeniu jest już skonfigurowana baza użytkowników lub włączona jest integracja z bazą zewnętrzną w celu ponownego włączenia **Kreatora konfiguracji bazy użytkowników** należy w prawym górnym rogu okna **Użytkownicy -> Konfiguracja Bazy LDAP** wybrać przycisk .

Zarządzanie użytkownikami

Zarządzanie kontami użytkowników odbywa się w sekcji ***Użytkownicy -> Użytkownicy i grupy***. Po przejściu do tego okna konfiguracyjnego możliwe jest tworzenie, modyfikowanie oraz usuwanie kont użytkowników i grup.



Konto użytkownika pozwala na skonfigurowanie następujących parametrów:

Login – nazwa używana do 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.
Członek grupy – określa przynależność użytkownika go określonych grup bazy LDAP.

Konto grupy pozwala na zdefiniowanie następujących parametrów:

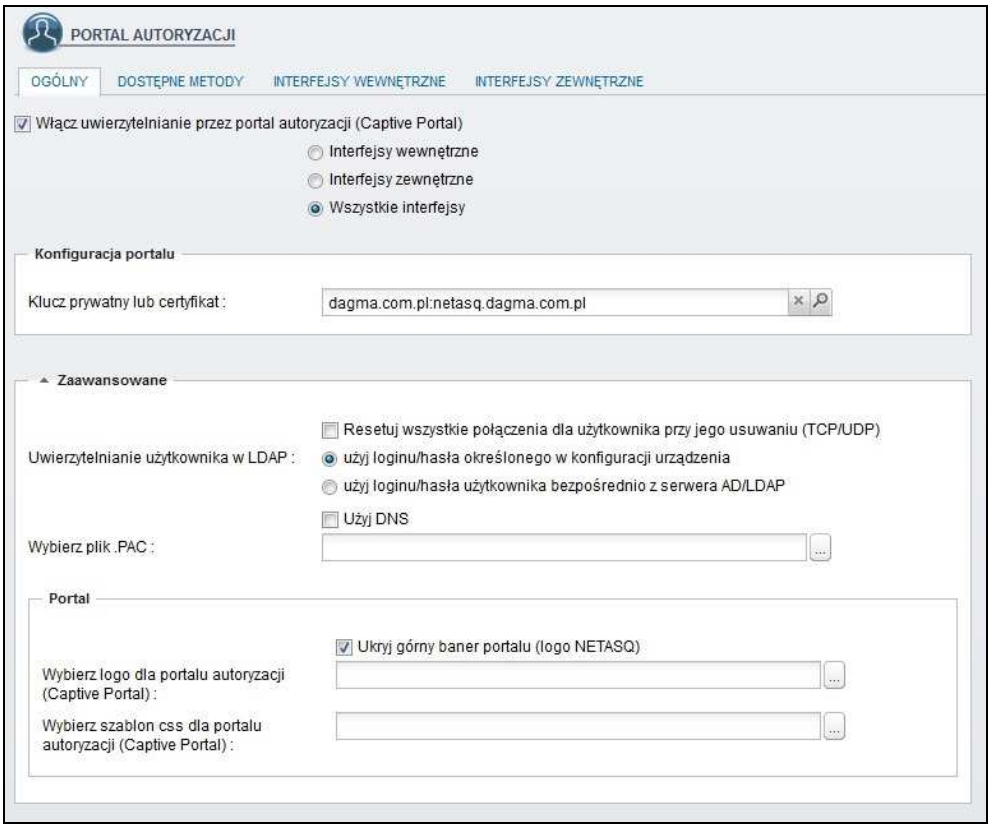
Nazwa grupy – nazwa grupy.
Opis – opis ułatwiający identyfikację grupy.
Członkowie grupy – pole zawierające listę wszystkich członków danej grupy.

Portal autoryzacji użytkowników – Captive portal

Captive portal jest specjalną stroną udostępnianą pod adresem **https://IP_NETASQ/auth/** i wykorzystywaną w celu autoryzacji użytkowników. Mechanizm Captive portal wykorzystywany jest zarówno do autoryzacji użytkowników LAN (tworzenie polityk filtrowania ruchu) jak i WAN (SSL VPN). Konfiguracja Captive portal odbywa się w sekcji **Użytkownicy -> Portal autoryzacji**.

Konfigurację można podzielić na dwa etapy: ogólna konfigurację całego portalu oraz konfigurację logowania zależną od typu interfejsu.

Poniższe okno zawiera ogólną konfigurację portalu i obejmuje następujące funkcje:



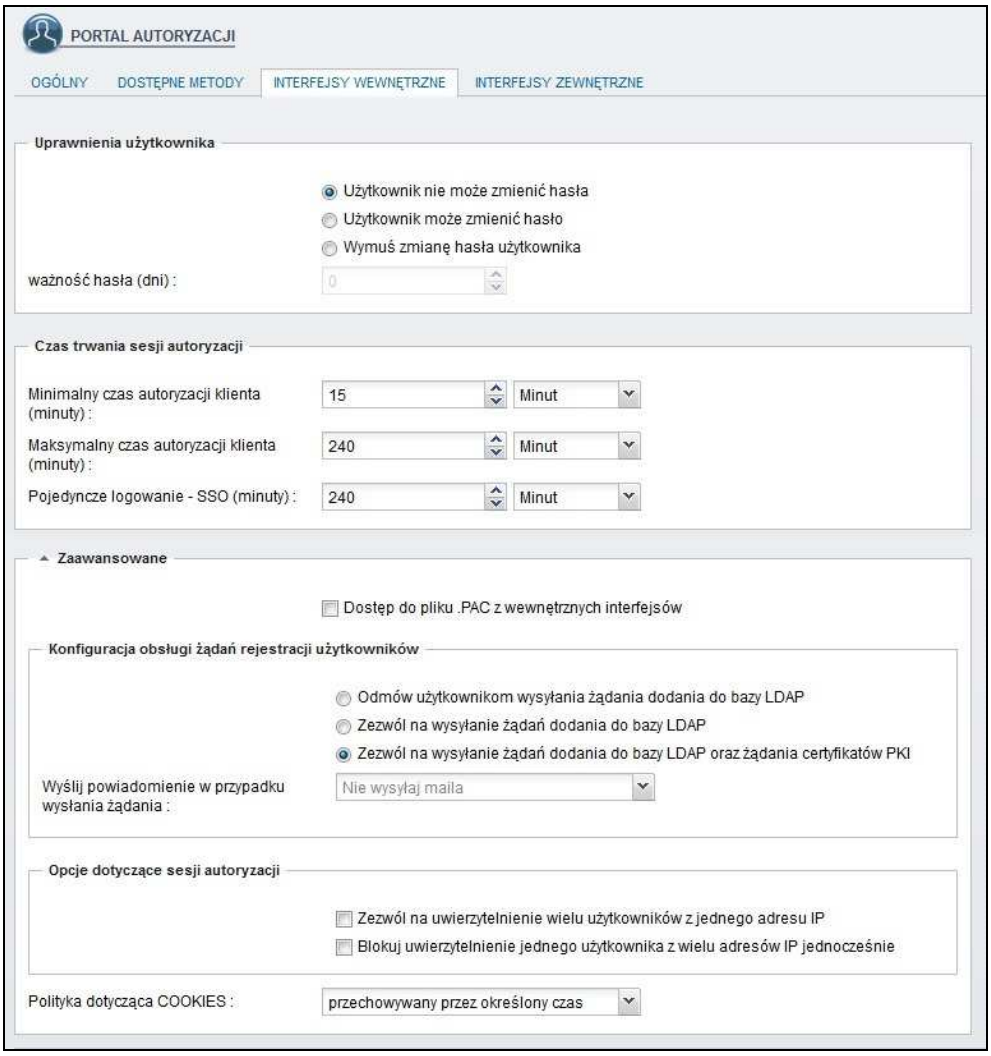
Włącz uwierzytelnianie przez portal autoryzacji (Captive Portal) – określa interfejsy na których usługa będzie dostępna tzn. interfejsy tylko wewnętrzne, interfejsy tylko zewnętrzne lub oba typy interfejsów.

Klucz prywatny lub certyfikat - pozwala na wybór certyfikatu jaki będzie użyty do podpisania portalu autoryzacji. Certyfikat musi być wcześniej wczytany na urządzenie poprzez sekcję **Obiekty -> Certyfikaty – PKI**.

Klucz prywatny lub certyfikat - użyj loginu/hasła określonego w konfiguracji urządzenia – funkcja używana jeśli baza użytkowników jest bazą wewnętrzna urządzenia; **użyj loginu/hasła użytkownika bezpośrednio z serwera AD/LDAP** – funkcja używana gdy urządzenie jest zintegrowane z bazą zewnętrzną.

Portal – sekcja pozwala na wprowadzenie takich zmian w wyglądzie strony jak zmiana logo strony, czy zmiana szablonu css dla strony.

Konfiguracja logowania powiązana z typem interfejsu została przedstawiona poniżej. Zawiera ona następujące opcje:



Uprawnienia użytkownika – uprawnienia użytkownika do zarządzania własnym hasłem.

Czas trwania sesji autoryzacji – 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.

Konfiguracja obsługi żądań rejestracji użytkowników – konfiguracja funkcji, która umożliwia użytkownikom zgłaszania kont do założenia. Użytkownik wypełnia pola właściwości konta swoimi danymi a rola administratora ogranicza się do weryfikacji tych danych i akceptacji utworzenia konta.

Opcje dotyczące sesji autoryzacji - Zezwól na uwierzytelnienie wielu użytkowników z jednego adresu IP – pozwala na logowanie wielu użytkowników z pojedynczego adresu IP, wszyscy zalogowani użytkownicy otrzymują uprawnienia ostatniego zalogowanego użytkownika; **Blokuj uwierzytelnienie jednego użytkownika z wielu adresów IP jednocześnie** – funkcja uniemożliwia zalogowanie jednego użytkownika na wielu komputerach, użycie tej opcji eliminuje „pożyczanie" haseł pomiędzy użytkownikami.

Wskazówka

Portal autoryzacji może działać na innym porcie niż standardowy port https, czyli 443 TCP. Zmiany portu usługi można dokonać w pliku */usr/Firewall/ConfigFiles/auth* edytując w sekcji **[Config]** parametr **HttpsPort=**

Tworzenie reguł firewalla w oparciu o zalogowanego użytkownika

Poniższy screen obrazuje przykładowe reguły zapory stworzone dla zalogowanych użytkowników.

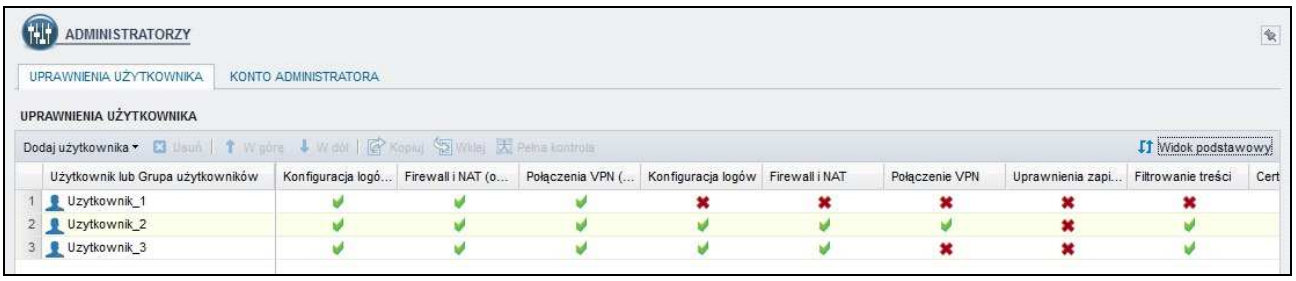
Akcja	Adres źródłowy	Adres docelowy	Port docelowy	Analiza protokołowa	Polityki filtrowania
zezwól	Uzytkownik_1	Internet	web		
zezwól	Uzytkownik_2 @ Komputer	Internet	web		

Reguła pierwsza pozwala na dostęp do usług **web** jedynie dla osoby zalogowanej jako **Uzytkownik_1**.

Reguła druga pozwala na dostęp do **web** dla konta **Uzytkownik_2** ale pod warunkiem, że jest on zalogowany na urządzeniu powiązanym z obiektem Komputer. Uzytkownik_2 zalogowany na innej maszynie nie uzyska tych uprawnień.

Delegowanie zadań administracyjnych na użytkowników bazy LDAP

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



12. 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 VPNy dzielimy na:

Client-to-Site – umożliwiające bezpośrednie połączenie komputera z siecią firmową. Ten typ tunelu wykorzystywany jest przede wszystkim przez użytkowników pracujących mobilnie.

Site-to-Site – gdzie tunel ustanawiany jest pomiędzy dwoma urządzeniami brzegowymi, co pozwala na bezpieczne połączenie sieci chronionych przez te urządzenia.

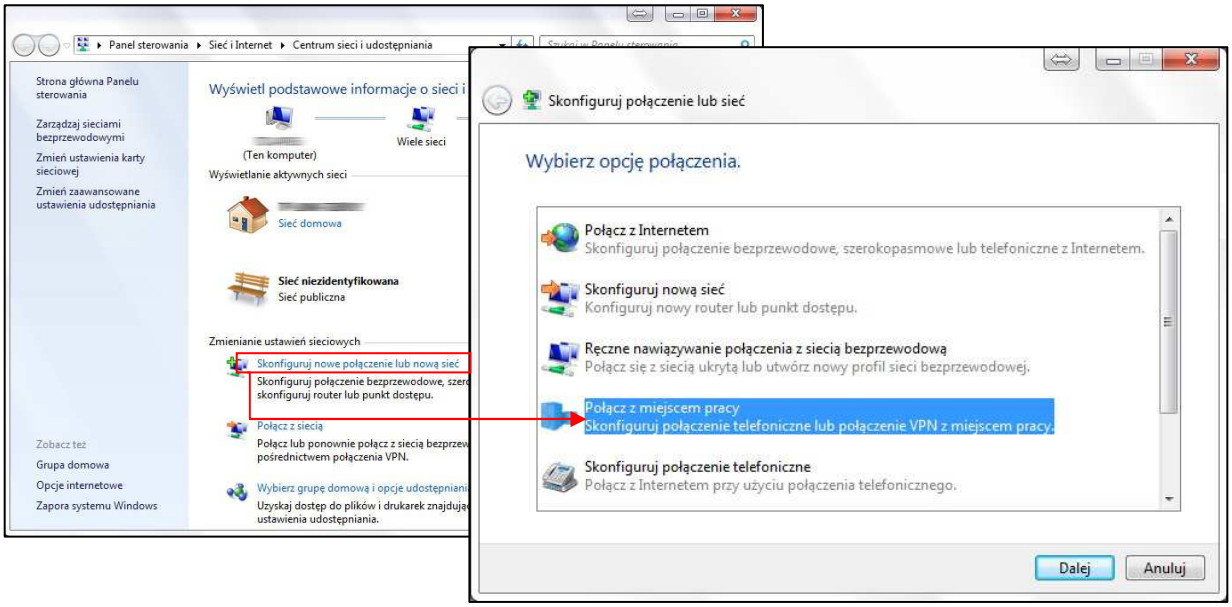
W przypadku urządzeń NETASQ dostępne są trzy możliwości tworzenia kanałów VPN:

- Protokół PPTP VPN
- Protokół SSL VPN
- Protokół IPSec VPN

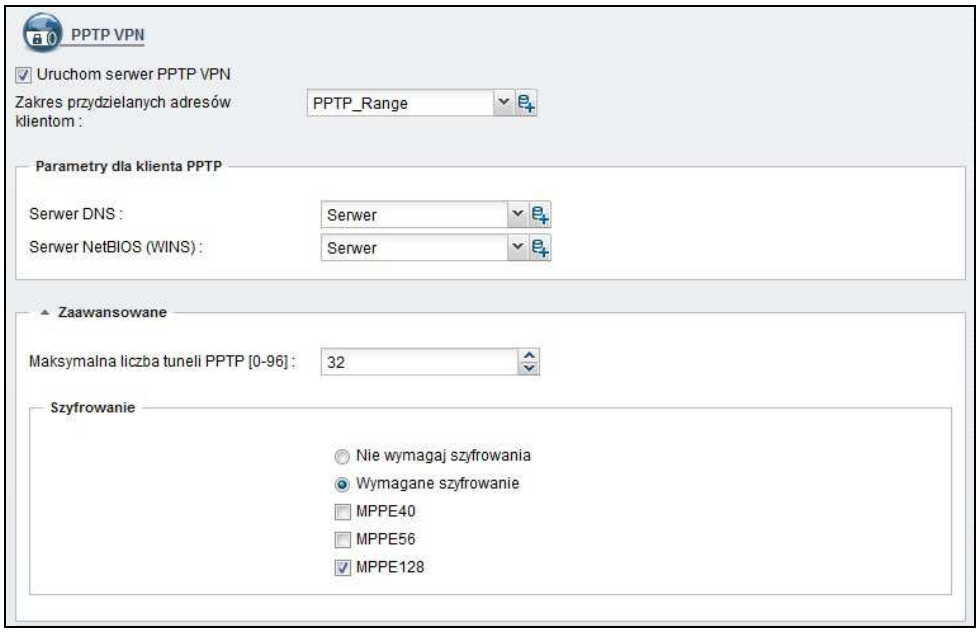
Zastosowanie wybranego protokołu VPN powinno być podyktowane przede wszystkim poziomem zastosowanego bezpieczeństwa oraz kwestiami związanymi z funkcjonalnością protokołu.

PPTP VPN (eng. Point to Point Tunneling Protocol)

PPTP jest protokołem najprostszym w konfiguracji jednak najmniej bezpiecznym. Pozwala on na tworzenie tuneli typu **Client-to-Site** w ramach których możliwy jest pełen dostęp do zasobów firmy. Największą zaletą stosowania tego protokołu jest możliwość wykorzystania klienta wbudowanego w system Microsoft Windows. Po stronie systemu operacyjnego należy **Skonfigurować nowe połączenie lub nową sieć** a następnie uruchomić kreator **Połączenia z miejscem pracy**.



Po stronie NETASQ konfiguracji należy dokonać w sekcji **Połączenia VPN -> PPTP VPN**.



W tym oknie konfiguracyjnym należy skonfigurować opcje:

Uruchom serwer PPTP VPN – włączenie/wyłączenie usługi na urządzeniu.

Zakres przydzielanych adresów klientom - zdefiniowanie zakresu adresów IP jakie będą uzyskiwali klienci łącząc się poprzez PPTP VPN. Ważne jest, aby ten zakres nie pokrywał się z zakresem wykorzystywanym przez inne hosty w LAN.

Serwer DNS –definiowanie serwera DNS dla klientów usługi.

Serwer NetBIOS (WINS) –definiowanie serwera usługi NetBIOS dla klientów VPN.

Maksymalna liczba tuneli PPTP –definiowanie ile tuneli może być uruchomionych jednocześnie. Maksymalna liczba tuneli jest zależna od modelu urządzenia.

Szyfrowanie – pozwala zdefiniować siłę klucza szyfrującego komunikację VPN.

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

SSL VPN

Klientem dla tego rodzaju VPN jest przeglądarka internetowa. Sprawia to, iż zastosowanie tego typu VPN jest bardzo wygodne z punktu widzenia administratora. Jedyny wymóg po stronie klient to zainstalowana przeglądarka internetowa i Java.

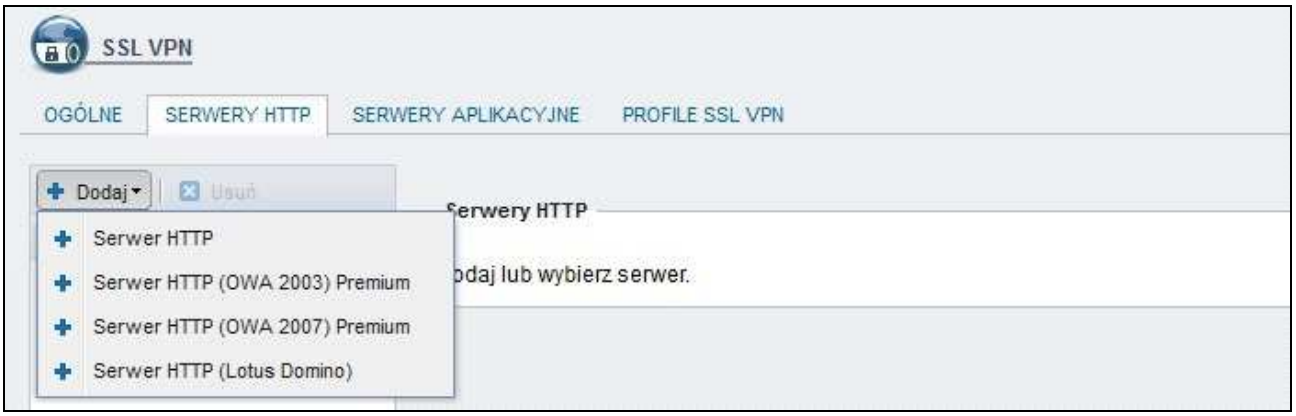
W przypadku SSL VPN każdy z kanałów jest tworzony dla pojedynczej usługi w odniesieniu do konkretnego serwisu. Czyli tunel VPN jest tworzony do konkretnego SERWERA na konkretny PORT. Najczęściej SSL VPN stosowany jest dla tunelowania połączeń zdalnego pulpitu (RDP) lub ukrycia za stroną do autoryzacji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

Konfigurację SSL VPN należy rozpocząć od włączenia serwisu autoryzacyjnego na zewnętrznym interfejsie urządzenia. Konfiguracji tej należy dokonać w sekcji **Użytkownicy -> Portal autoryzacji**.

Aby skonfigurować serwer SSL VPN należy przejść do sekcji **Połączenia VPN -> SSL VPN** gdzie w pierwszej kolejności dokonujemy wyboru 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 IP serwera docelowego,
Port – port usługi http serwera, zazwyczaj jest to port 80TCP,
Adres URL serwera HTTP – pozwala na wskazanie podstrony na którą będzie automatycznie przekierowany ruch,
Nazwa odnośnika na portalu – nazwa pod jaką będzie widoczne połączenie w oknie klienta SSL VPN. Nazwa powinna ułatwiać użytkownikom identyfikację usługi.

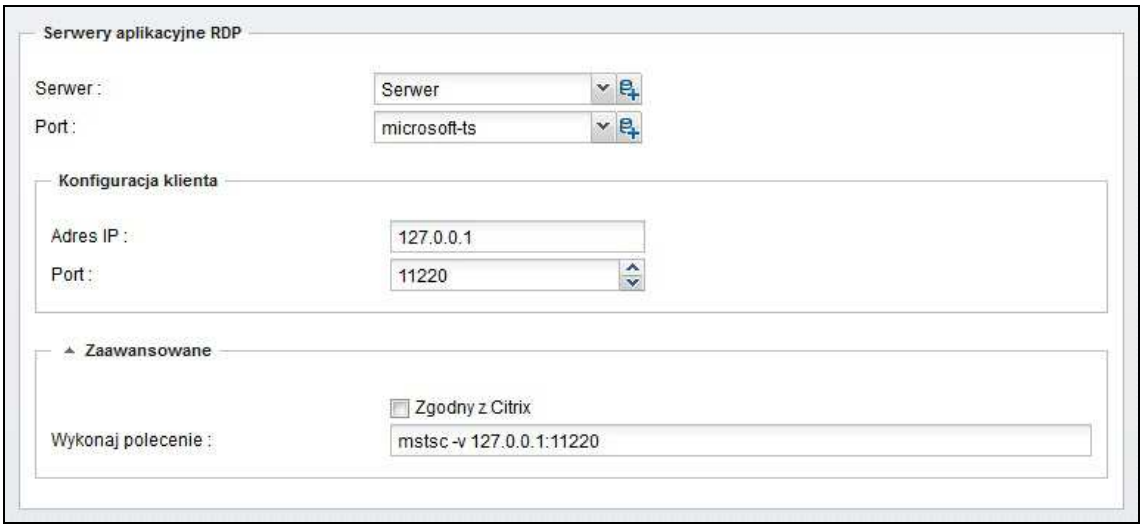
Serwery aplikacyjne

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 (127.0.0.1) i przetunelowanie ich wewnątrz połączenia SSL VPN do serwera docelowego.

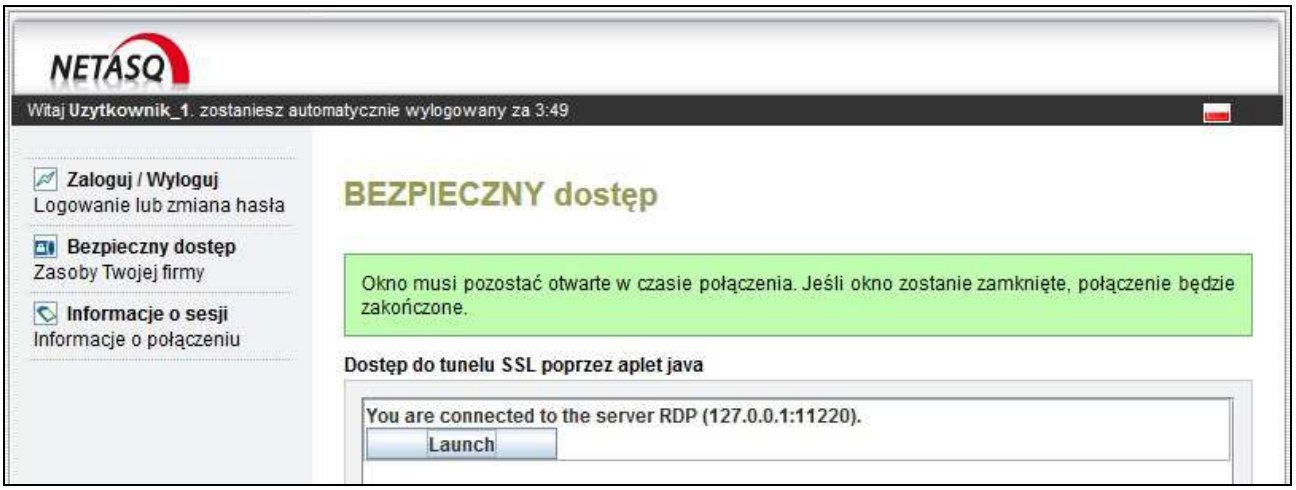
Przykład konfiguracji dostępu do serwerów aplikacyjnych został przedstawiony poniżej i obejmuje:

Serwer - obiekt reprezentujący serwer docelowy,
Port - port usługi serwera, który ma zostać udostępniony,

Adres IP - adres IP, z którego Java będzie przechwytywała połączenia,
Port - port, z którego Java będzie przechwytywała połączenia.

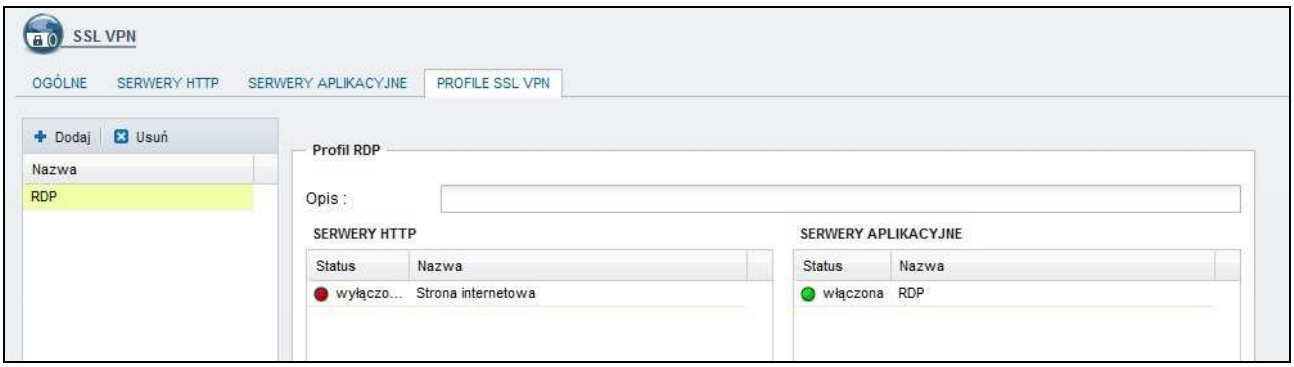


Bardzo przydatnym parametrem jest opcja **Wykonaj polecenie** - pozwala na określenie polecenia, które zostanie wykonane po uruchomieniu apletu Java i wybraniu odpowiedniego przycisku **Launch**. W tym wypadku będzie to polecenie *mstsc –v localhost:11220*, które wywołuje klienta zdalnego pulpitu i uruchamia połączenie do adresu 127.0.0.1 na port 11220. Dzięki temu użytkownik po zalogowaniu się nie musi uruchamiać klienta RDP i wpisywać adresu, wystarczy, że wybierze przycisk Launch co spowoduje automatyczne uruchomienie się klienta (mstsc) wraz z niezbędnymi do polecenia opcjami.



Profile SSL VPN

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



Dowiązania profilu do użytkownika dokonuje się w kolejnym kroku.

Konfiguracja uprawnień użytkowników

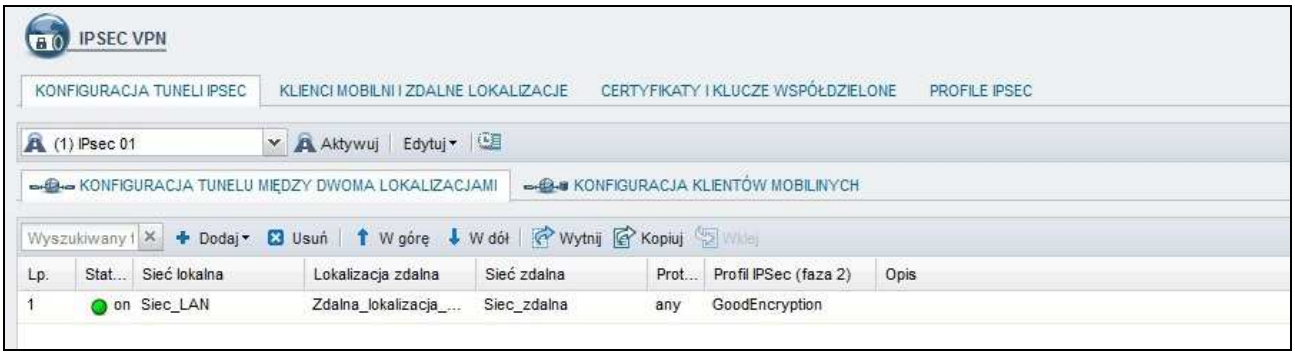
Aby użytkownik mógł się zalogować do SSL VPN konieczne jest skonfigurowanie dla niego odpowiednich praw dostępu. Dokonuje się tego w sekcji **Użytkownicy -> Polityki dostępu**. W zakładce **Domyślne reguły** dostępu można wskazać profil, który ma być dostępny dla każdego zalogowanego użytkownika. Jeśli użytkownik ma mieć inny niż domyślny poziom dostępu taką konfiguracje należy przeprowadzić na zakładce **Reguły dla użytkownika**.

IPSec VPN

Protokół IPSec jest najbezpieczniejszym i najwszechstronniejszym protokołem VPN jaki można skonfigurowac na NETASQ. Pozwala na budowanie tuneli **Client-to-Site** jak i **Site-to-Site** a jego użycie pozwala uzyskać pełen dostęp do zasobów w sieci.

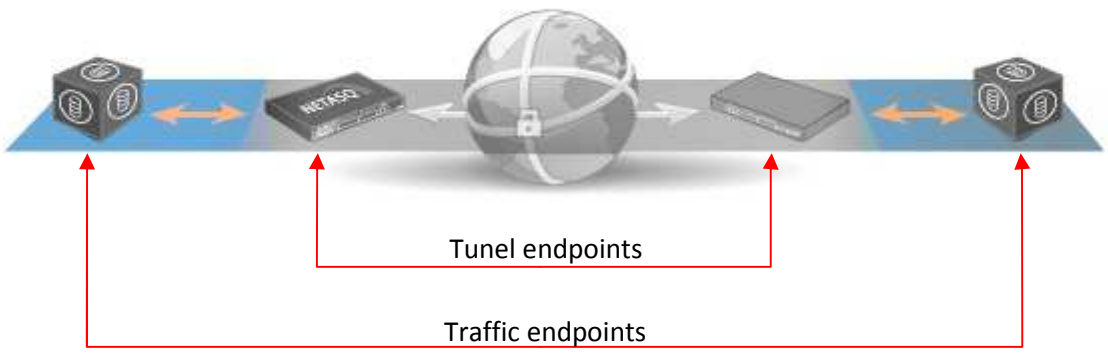
Implementacja IPSec VPN w rozwiązaniach NETASQ jest w pełni zgodna ze standardem IPSec dzięki czemu możliwe jest nawiązywanie połączeń z dowolnymi urządzeniami czy aplikacjami klienckimi, które również wykorzystują zgodną z RFC implementacje tego protokołu.

Konfiguracja IPSec odbywa się w sekcji **Połączenia VPN -> IPSec VPN**. Widok okna konfiguracyjnego przedstawiono poniżej.

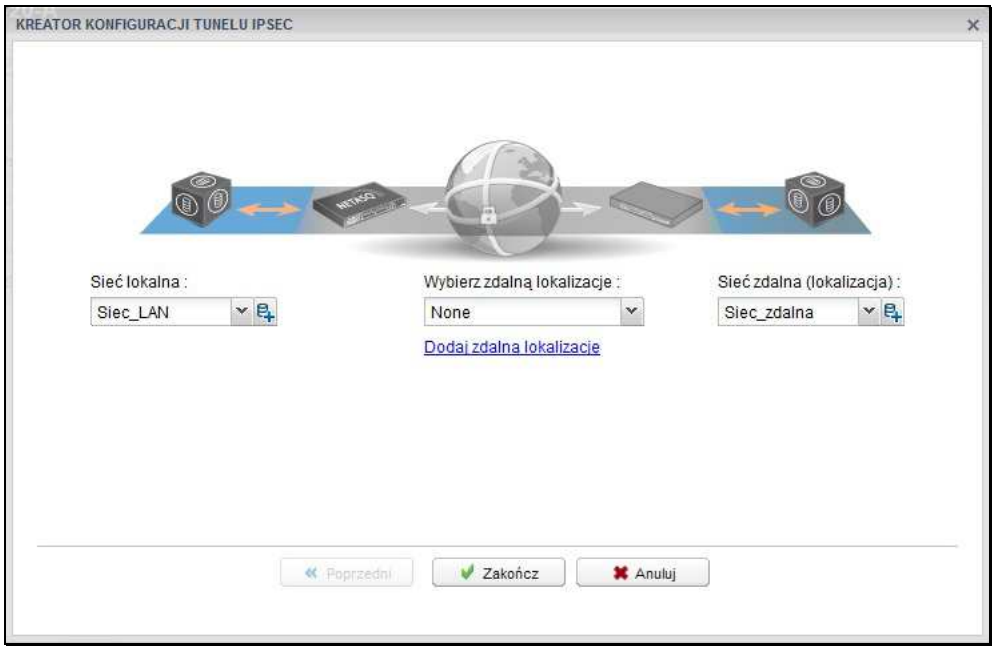


Ponieważ konfiguracja IPSec uważana jest za bardzo skomplikowaną NETASQ przygotował ułatwienia w postaci kreatorów, dzięki którym konfiguracja VPN jest szybka i nieskomplikowana. Po wybraniu opcję **Dodaj** uruchomi się kreator, który pomoże skonfigurować zarówno fazę pierwszą jak i drugą tunelu.

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



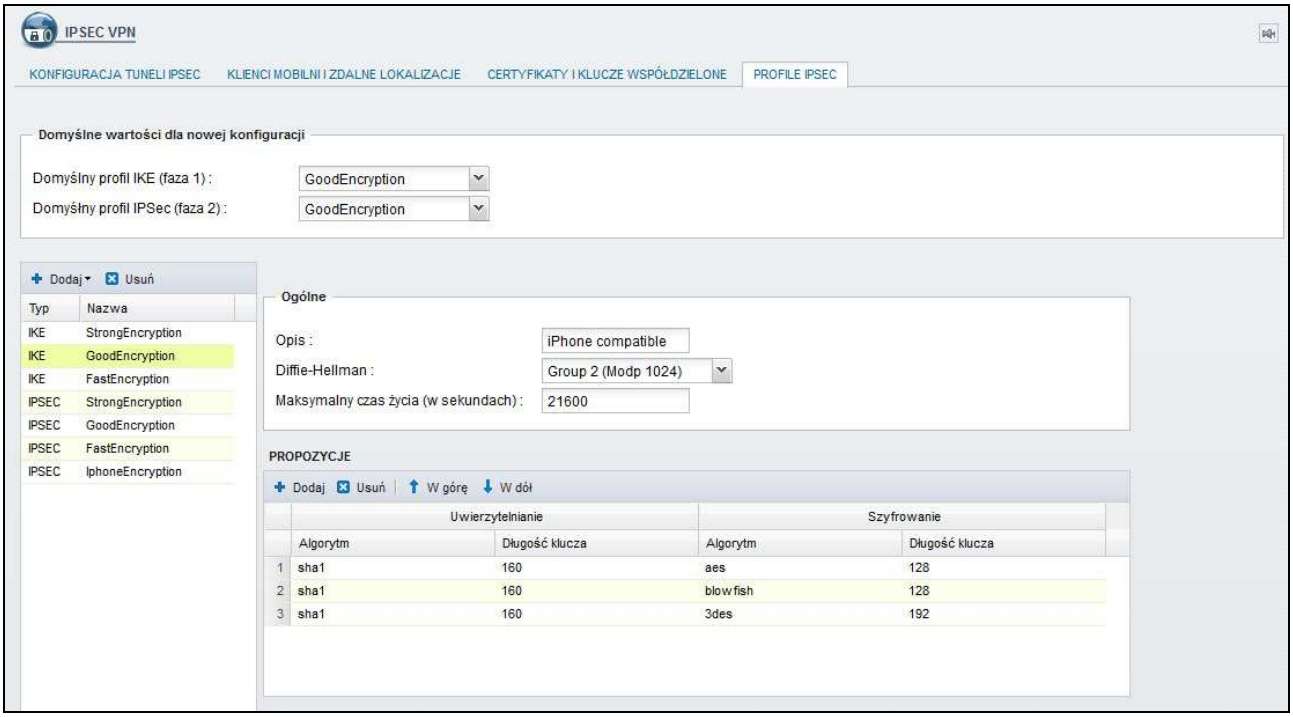
Kreator konfiguracji tunelu IPSec umożliwia konfiguracje Tunel endpoints a więc fazy pierwszej oraz pozwala na wskazanie z jaką zdalną lokalizacją będzie zestawiane połączenie.



Jeśli zdalna lokalizacja nie została jeszcze skonfigurowana wybieramy opcje **Dodaj zdalna lokalizację** co powoduje otwarcie nowego kreatora.

Ten kreator pozwala skonfigurować Tunel endpoints oraz hasło/certyfikat zabezpieczające komunikację. Po zakończeniu pracy obu kreatorów należy jeszcze skonfigurować **Profile Spiec** oraz aktywować slot.

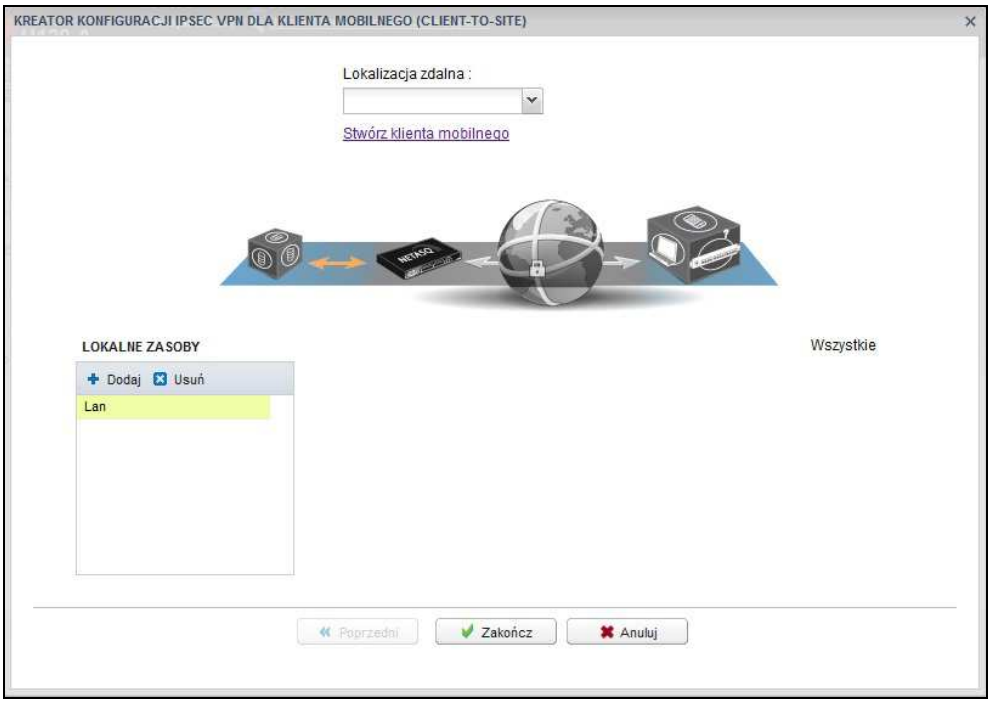
Profile Spiec określają jakie algorytmy i klucze mają być użyte do zabezpieczenie tunelu. Można skorzystać z profili domyślnych lub stworzyć własne zgodne z wymaganiami polityki bezpieczeństwa. Okno konfiguracyjne profili zostało przedstawione na screenie poniżej. Profile **IKE** są profilami fazy pierwszej, natomiast profile **IPSec** są profilami fazy drugiej.



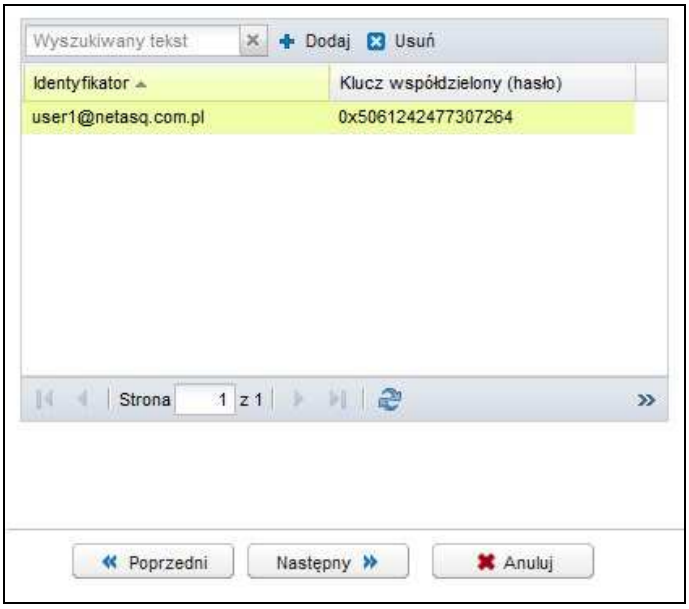
Konfiguracja połączenia Client-to-Site z użyciem NETASQ VPN Client

Konfiguracja po stronie NETASQ

W sekcji **Połączenia VPN -> IPSec VPN** należy przejść do zakładki **Konfiguracja klientów mobilnych** i wybrać **Dodaj -> Nowa polityka**. Tak jak w przypadku konfiguracji Site-to-Site uruchamia się kreator, w którym należy zdefiniować sieci jakie będą dostępne poprzez VPN (Lokalne zasoby) oraz wybrać **Stwórz klienta mobilnego**.



Kreator dodawania nowego klienta pozwoli na zdefiniowanie mechanizmu uwierzytelniania wykorzystywanego przez urządzenie. Najprostszym mechanizmem jest uwierzytelnianie z użyciem identyfikatora i hasła. Na etapie kreatora można stworzyć taką listę uwierzytelniania, można to zrobić również później na zakładce **Certyfikaty i klucze współdzielone**.

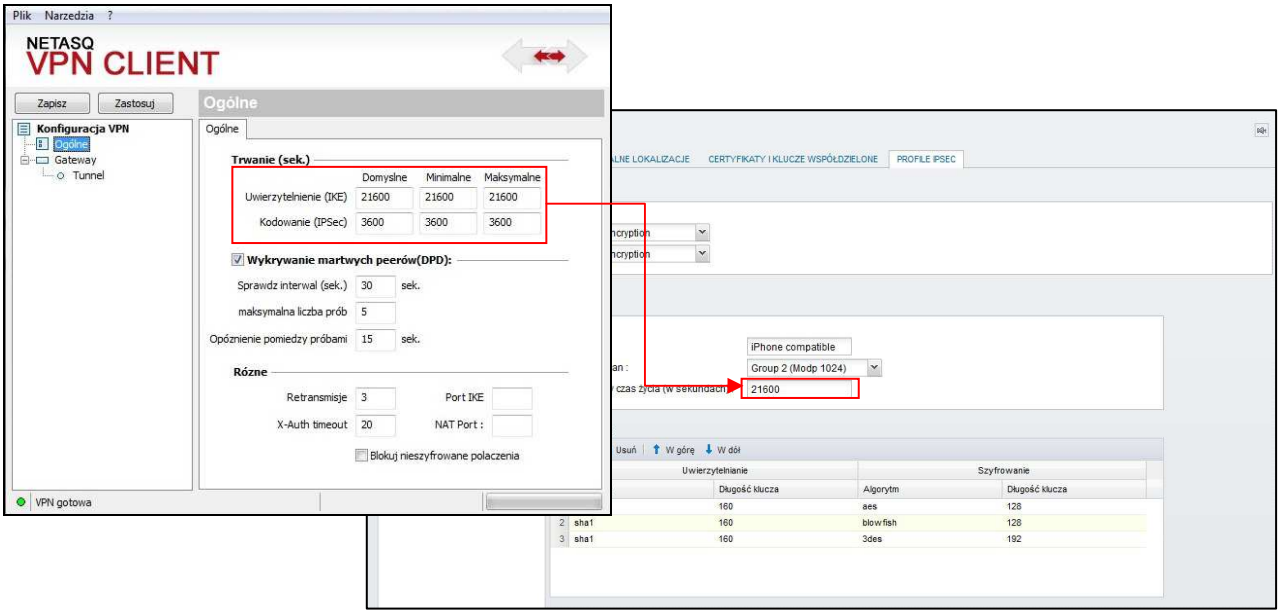


Po stronie urządzenia należy jeszcze dokonać konfiguracji uprawnień użytkowników do tworzenia tuneli oraz reguł firewalla. Uprawnienia dla użytkowników aby mogli tworzyć tunele należy nadać w sekcji **Użytkownicy -> Polityki dostępu**.

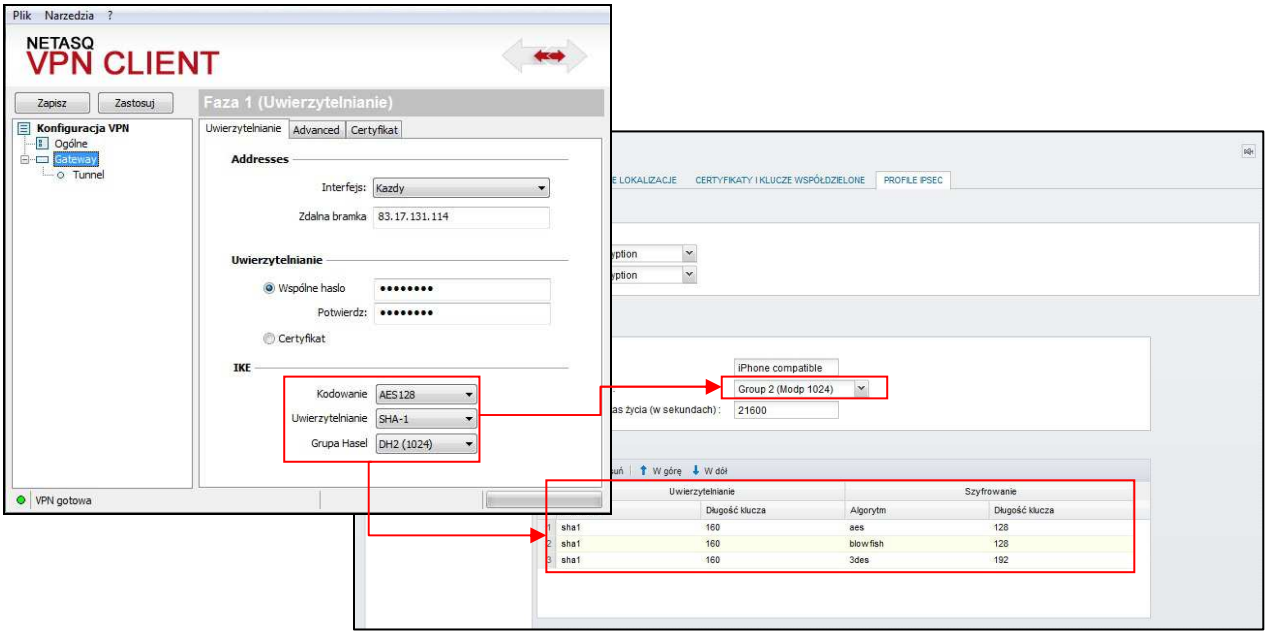
Konfiguracja firewalla powinna zawierać reguły pozwalające na nawiązanie komunikacji na portach 500UDP, 4500UDP oraz na protokole VPN-ESP. Ponadto należy skonfigurować regułę pozwalającą na ruch wewnątrz tunelu.

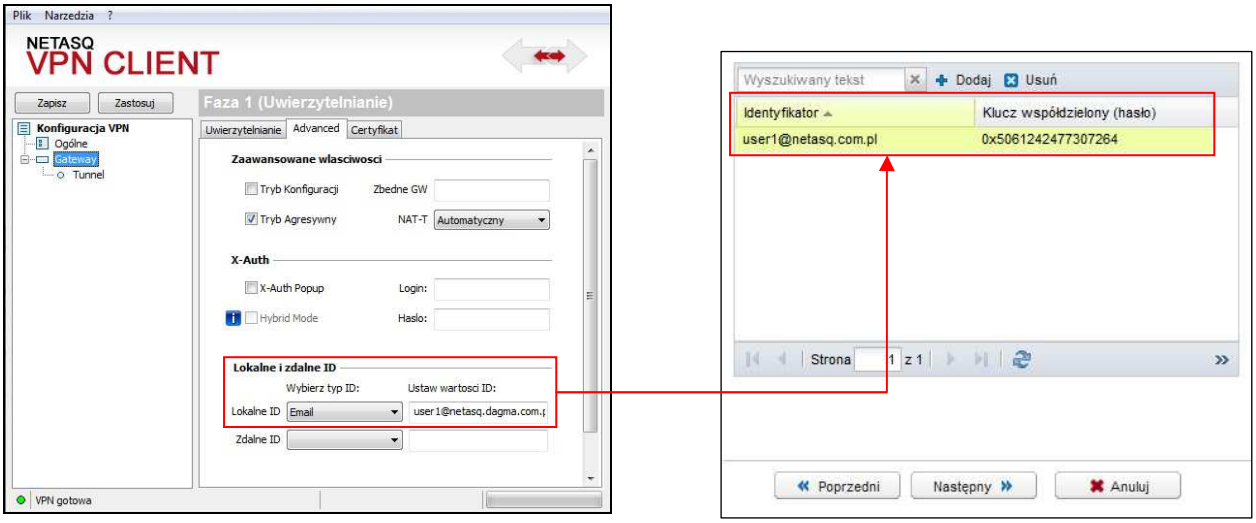
Konfiguracja klienta NETASQ VPN Client

Ustawienia ogólne – należy skonfigurować czas życia tunelu fazy pierwszej i fazy drugiej. Po stronie NETASQ konfiguracji należy dokonać w ustawieniach profili IPSec. Pozostałą konfigurację po stronie klienta należy pozostawić bez zmian.

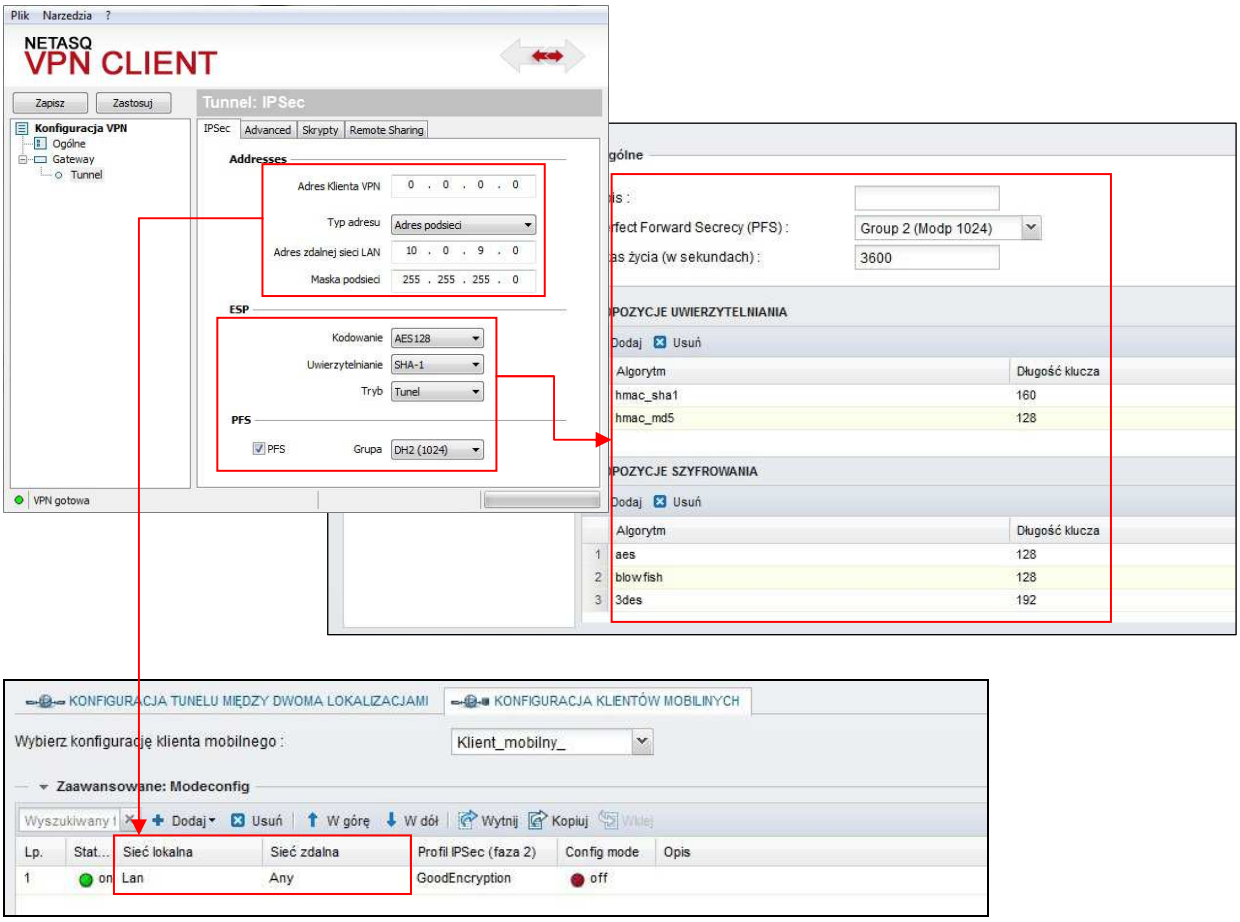


Ustawienia Gateway (faza 1) – na zakładce uwierzytelnianie należy podać publiczny adres IP urządzenia, z którym będzie zestawiany tunel, hasło użytkownika oraz wybrać algorytmy szyfrowania jakie zostaną użyte podczas budowania tunelu. W zakładce należy włączyć opcję **Tryb agresywny**, wybrać wartość **Automatyczny** da opcji **NAT-T** oraz podać identyfikator i nazwę użytkownika używanego do zbudowania tunelu. Jako identyfikator najlepiej wybrać adres e-mail.





Ustawienia Tunel (faza 2) – w zakładce tunel należy określić do jakich sieci będzie się można łączyć w ramach tunelu oraz jakie algorytmy będą wykorzystywane do tego połączenia. Pozostałe opcje należy pozostawić w konfiguracji domyślnej.



Aby zakończyć konfigurację klienta należy wybrać opcję Zapisz. W celu otwarcia tunelu należy kliknąć prawym klawiszem myszy w opcje **Tunel** i wybrać opcję **Otwieranie tunelu** (można również użyć skrótu klawiszowego Ctrl+O). Po otwarciu tunelu powinien pojawić się dymek 

.

Wskazówka

Po otwarciu tunelu w **Real Time Monitorze** w zakładce **IPSec VPN** powinna pojawić się informacja o stanie tunelu i transferze wewnątrz.

W sytuacji kiedy tunel nie może być utworzony w **Real Time Monitorze (RTM)** w zakładce **Logi -> IPSec VPN** powinny pojawić się logi z komunikatem błędu. Zakładka **Logi -> IPSec VPN** jest aktywna tylko w urządzeniach z dyskiem twardym. Jeśli urządzenie nie posiada dysku twardego możliwe jest uzyskanie ostatnich 30 linii logu z poziomu WebGUI. W celu uzyskania logów należy przejść do sekcji **Ustawienia systemowe -> Wiersz poleceń** i wydać polecenie:

monitor log vpn

13. Konfiguracja proxy http, smtp, pop3, ftp, ssl

Każdy z mechanizmów proxy w urządzeniach NETASQ 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 wiedzenia 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.

Funkcjonalność każdego z proxy jest następująca.

http proxy

- klasyfikacja URL (filtrowanie dostępu do wybranych grup stron www),
- skanowanie antywirusowe dla ruchu http,
- określenie maksymalnego rozmiaru pliku pobieranego przez http,
- filtrowanie plików po typie (MIME Type)
- konfiguracja strony informującej o zablokowaniu dostępu do strony www (Block page),

pop3 proxy

- skaner antyspam (wiadomość SPAM jest oznaczana przez dopisek w temacie wiadomości),
- skaner antywirusowy,
- kontrola komend w ramach protokołu pop3.

smtp proxy

- skaner antyspam (wiadomość SPAM jest oznaczana przez dopisek w temacie wiadomości lub może być blokowana),
- skaner antywirusowy,
- filtr SMTP określający reguły filtrowania wiadomości e-mail w odniesieniu do nadawcy lub odbiorcy,
- określenie limitów wielkości poczty i liczby odbiorców.

ftp proxy

- skaner antywirusowy,
- możliwość określenia dozwolonych serwerów FTP,
- kontrola komend w ramach protokołu ftp.

SSL proxy

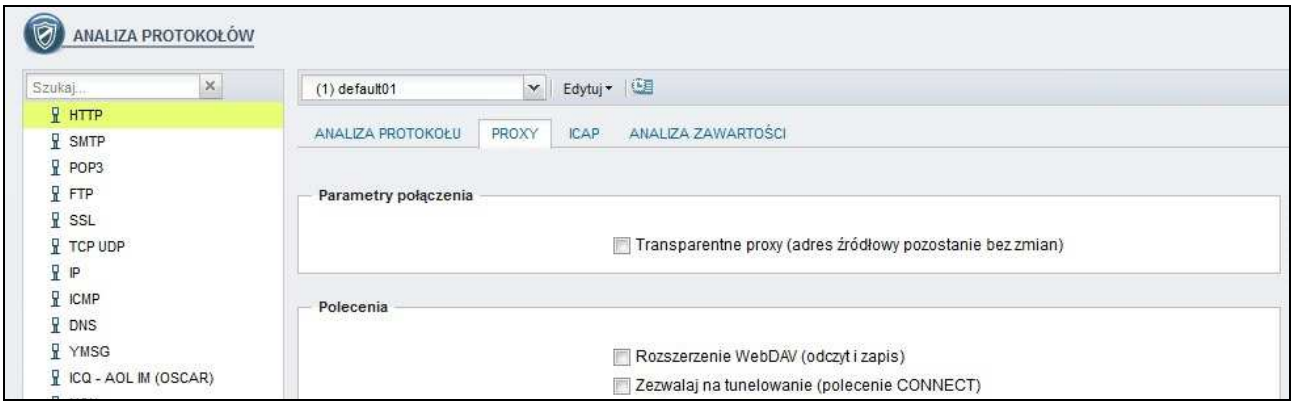
- skanowanie certyfikatów SSL (sprawdzanie poprawności, filtrowanie dostępu na podstawie CN),
- analiza ruchu modułem proxy odpowiednim dla każdego z protokołów nieszyfrowanych.

W firmware 9 nastąpiła bardzo duża zmiana jeśli chodzi o stosowanie mechanizmów proxy. W poprzedniej wersji oprogramowania możliwe było włączenie mechanizmu proxy dla całego interfejsu sieciowego. Oznaczało to, że ruch każdego komputera dla którego był to interfejs wejściowy był skanowany odpowiednimi filtrami. W wersji 9 firmware mechanizmy proxy zostały powiązane z konfiguracją firewalla. Dzięki takiemu podejściu ruch może być skanowany poprzez proxy z dokładnością dla pojedynczej reguły firewalla. Uruchomienie proxy odbywa się poprzez włączenie w regule firewalla w kolumnie **Polityki filtrowania** jednego z modułów **Filtrowania treści**.

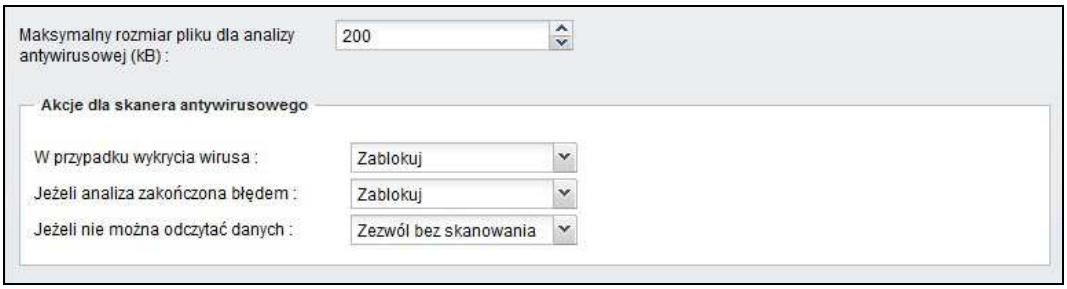
Włączenie skanowania proxy dla reguły firewalla jest jednak ostatnim krokiem konfiguracji. Wcześniej należy skonfigurować ogólne ustawienia proxy oraz skanery i filtry, które będą używane podczas skanowania ruchu.

http proxy

Ogólna konfiguracja proxy http znajduje się w pluginie http a więc w sekcji **Kontrola aplikacji -> Analiza protokołów -> http**. Znajduje się tutaj między innymi konfiguracja trybu pracy modułu proxy czy konfiguracja usługi ICAP.



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



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 producenta – 15 kategorii tematycznych,
- baza producenta z dodatkową klasyfikacją polskich stron – ponad 50 kategorii tematycznych,
- baza Optenet – wymaga dodatkowej licencji, można jej używać tylko na urządzeniach z dyskiem twardym,
- klasyfikacja URL stworzona przez administratora.

Konfiguracja klasyfikacji URL znajduje się w zakładce **Obiekty -> Klasyfikacja URL**. W zakładce **Klasyfikacja producenta** można znaleźć informację o tym jaka baza URL jest wykorzystywana przez urządzenie oraz jakie kategorie tematyczne są dostępne za jej pośrednictwem.

Uwaga

Z poziomu WebGUI nie ma możliwości zmiany klasyfikacji URL na **bazę producenta z dodatkową klasyfikacją polskich stron**. Zmiana tej konfiguracji możliwa jest jedynie z poziomu konsoli wg. poniższej instrukcji:

1. Wyłącz aktualnie używaną klasyfikację URL lub przełącz filtrowanie URL w tryb PASS ALL.
2. Dodaj do bazy obiekt typu host o nazwie: **update.netasq.pl** i adresie IP: **91.201.154.218**. Type obiekty *DYNAMICZNY*.
3. Podłącz się do urządzenie przez SSH (klient PUTTY lub WinSCP).
4. Zmodyfikuj plik konfiguracyjny **autoupdate** wskazując na serwer aktualizacji dla URL FILTERING na *update.netasq.pl*. Możesz to zrobić przy wykorzystaniu edytora *joe*:

>joe /usr/Firewall/ConfigFiles/autoupdate

```
[URLFiltering]
URL=http://update.netasq.pl/1
State=1
Retries=3
Period=1d
Secure=0
RollbackOnFail=0
Start=21:00
Proxy=
ProxyPort=
```

Zapis zmian w edytorze joe: **CTRL + k + x**

5. Następnie wywołaj polecenie:
   autoupdate –f –t URLFiltering
   Po wydaniu polecenie nastąpi automatyczne pobieranie nowej klasyfikacji URL. W kolejnym kroku możesz rozpocząć konfigurację **Filtrowania URL** w oparciu o nowe kategorie.

Klasyfikacja URL stworzona przez administratora

Tworzenie własnych grup polega na określeniu łańcucha znaków, które są porównywane z określonym adresem URL w przeglądarce. 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 blokowani 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.

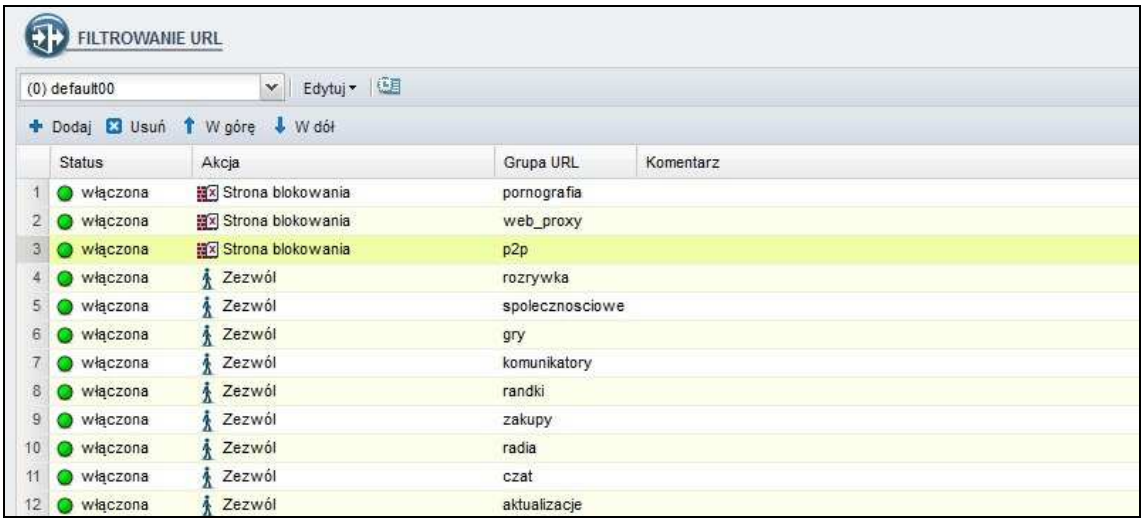
Poniższy zrzut ekranu pokazuje konfiguracje obu przykładów:

Polityka Filtrowania URL

Polityka filtrowania URL określa, jakie kategorie mają być dozwolone a jakie zablokowane w ramach określonego slotu konfiguracji. Slotów **Filtrowania URL** jest 10 co umożliwia stworzenie 10 niezależnych zestawów reguł dostępu do stron www. Konfiguracja polityk znajduje się w sekcji **Polityki filtrowania -> 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
- **Strona blokowania** - dostęp do stron zostanie zablokowany z komunikatem w formie strony www przygotowanym przez administratora.

Poniższy screen 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 w kolejności zdefiniowanej przez administratora a w przypadku znalezienia dopasowania kolejne reguły nie są sprawdzane.

Strona blokowania

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

Wskazówka

Poniżej zaprezentowano przykładowy kod html dla blokowany kategorii URL.

```
  <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
  <html>
  <head>
      <meta http-equiv="CONTENT-TYPE" content="text/html; charset=utf-8">
      <title>Strona blokowana</title>
  </head>
  <body bgcolor=#f3f3f3 link=#0000FF vlink=#000080 alink=#FF0000 text=#000000>
  <table width=800 border=0 align="center" bgcolor=#FFFFFF>
    <tr>
      <td>
        <center><img src="http://www.netasq.com/_img/index-logo.png"></center>
        <br>
        <h2 align="center"><i>Strona zablokowana</i></h2><br>
        <br><br>
        <p align="justify" style="margin: 10px;">Polityka bezpieczenstwa firmy
zabrania odwiedzania witryny <i>$host</i>.<br><br>
        Strona zablokowana przez regule  "<i>$rule</i>".<br><br>
        Adres URL: "<i>http://$host$url</i>"<br>
        <br>
        Skontaktuj sie z administratorem.<br>
        <br>
      </p>
      </td>
    </tr>
  </table>
  </body>
 </html>
```

Wskazówka

Istniej możliwość zgłoszenia niesklasyfikowanego adresu URL. Dokonać tego można przez stronę http://www.netasq.pl/pl/Dodaj_adres_URL.html proponując jednocześnie kategorie do których strona powinna przynależeć. Po zweryfikowaniu poprawności zaproponowanej klasyfikacji strona zostanie dodana do klasyfikacji producenta rozszerzonej o klasyfikację stron polskich.

14. Konfiguracja serwera DHCP

Serwer DHCP służy do przydzielania adresów IP komputerom w sieci LAN. Konfiguracji DHCP można dokonać w zakładce **Konfiguracja sieci -> Serwer DHCP**.

> Uwaga
>
> W domyślnej konfiguracji NETASQ 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.

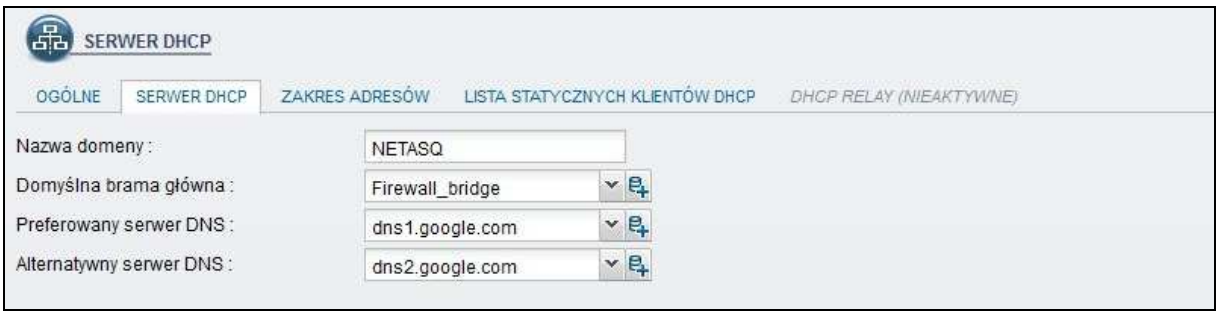
W pierwszej kolejności należy skonfigurować jak NETASQ będzie działał: czy jako serwer DHCP, czy będzie jedynie przekaźnikiem (relay) zapytań DHCP do innego serwera.

Zakładka **SERWER DHCP** służy do konfiguracji podstawowych parametrów przekazywanych przez serwer, takich jak:

Domyślna brama główna – brama do Internetu dla hostów sieci LAN. Obiekt ten powinien być adresem IP NETASQ w podsieci obsługiwanej przez NETASQ

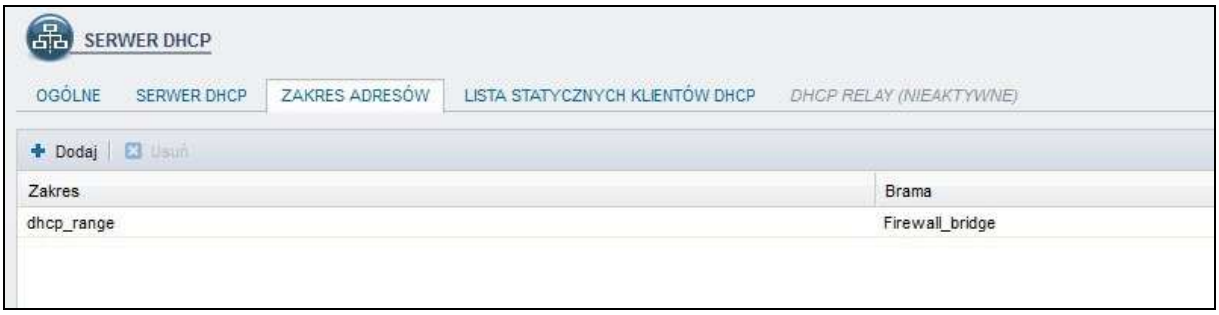
Preferowany, Alternatywny serwer DNS – Podstawowy i zapasowy serwer DNS

Serwery innych usług np. WINS, SMTP, NTP itp.



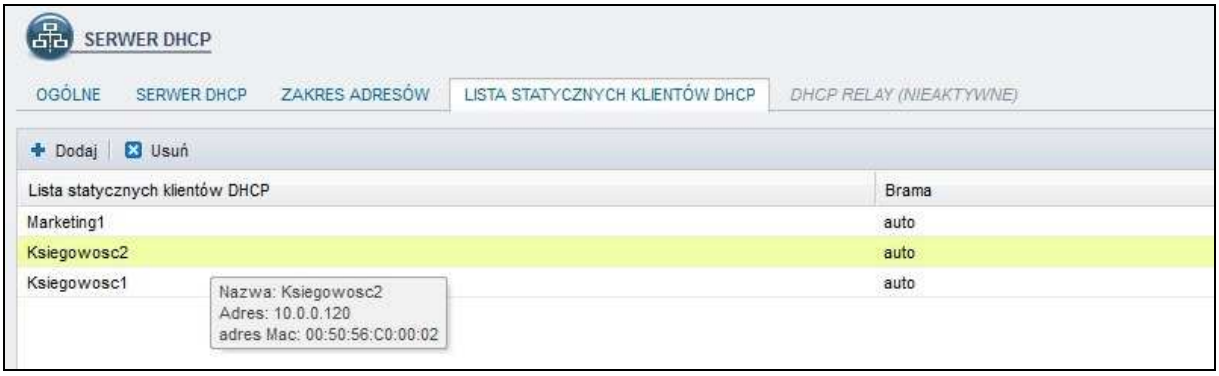
W zakładce Serwer DHCP można skonfigurować również czas dzierżawy adresu IP przez hosty.

W zakładce **ZAKRES ADRESÓW** wskazujemy, z jakiego zakresu serwer DHCP będzie przydzielał adresy. Jeśli NETASQ obsługuje wiele sieci dla każdej z nich należy wybrać inny obiekt w kolumnie **Brama**.



Zakładka **LISTA STATYCZNYCH KLIENTÓW DHCP** pozwala skonfigurować usługę serwera DHCP w taki sposób, aby komputer, o konkretnym adresie MAC mógł dostać zawsze ten same adres IP. Aby to uzyskać muszą być spełnione następujące warunki:

- Komputer musi być reprezentowany przez obiekt typu **Host**.
- Obiekt typu **Host** reprezentujący komputer musi mieć skonfigurowany adres **MAC**.
- Adres IP tego komputera nie może należeć do zakresu adresów rozgłaszanych przez serwer DHCP.



Ostatnia zakładka służy do konfiguracji urządzenia w trybie **DHCP PELAY**, czyli przekazywania zapytań DHCP do wskazanego serwera. W tym trybie NETASQ nasłuchuje zapytań DHCP na wszystkich lub na wskazanych w sekcji **INTERFEJSY DLA DHCP RELAY** interfejsach sieciowych a następnie przekazuje te zapytania do serwera określonego w polu **Serwer DHCP RELAY**.

Wskazówka

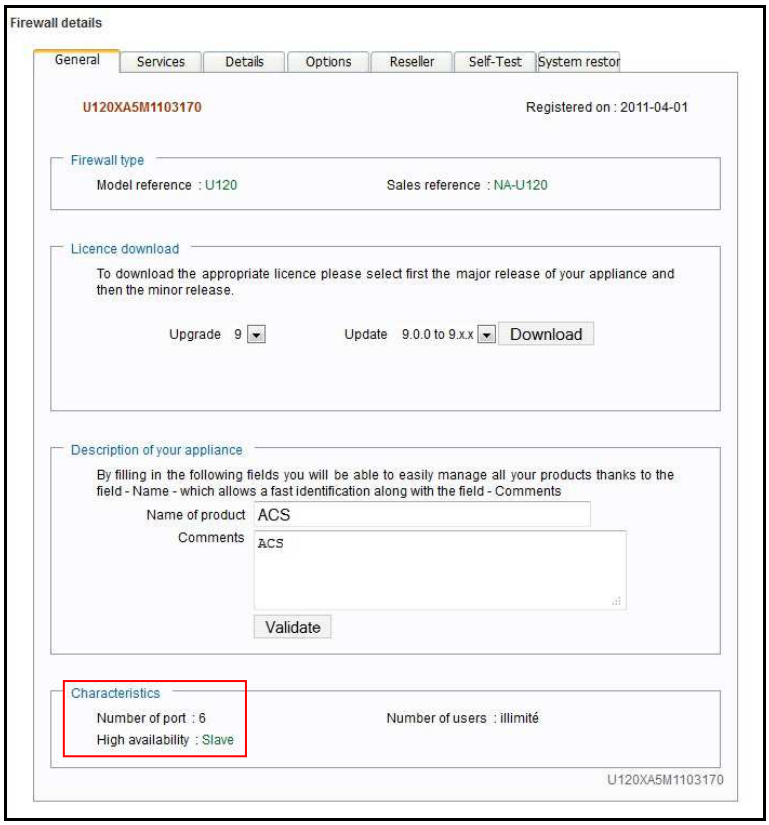
Konfiguracja DHCP znajduje się systemie NS-BSD w pliku */usr/Firewall/ConfigFiles/dhcp*.

Informację o dzierżawie adresów IP przez hosty można uzyskać wywołując polecenie *dhcpinfo*.

15. Klaster High Availability

Klaster HA określa dwa połączone ze sobą urządzenia NETASQ w celu zapewnienia ciągłości pracy sieci w przypadku awarii jednego z urządzeń. Klaster w rozwiązaniach NETASQ klaster 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 mniejszej ilości aktywnych interfejsów sieciowych na pierwszym urządzeniu.

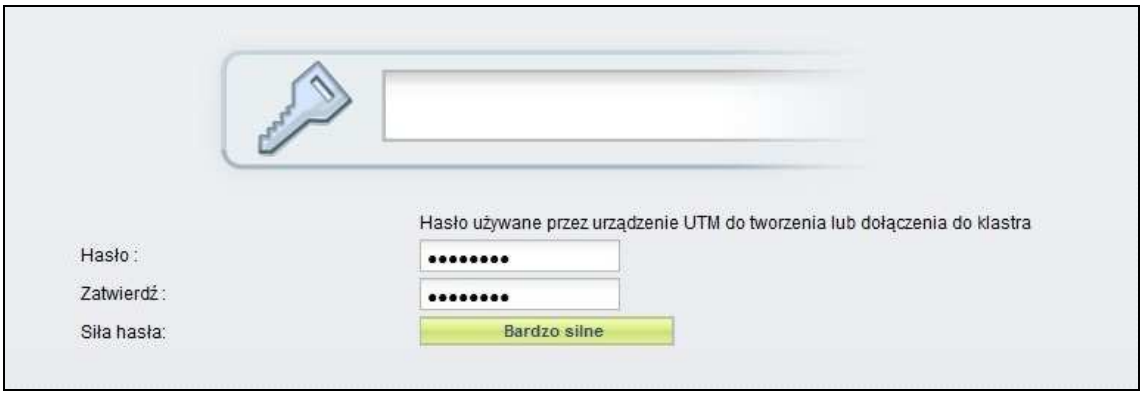
Aby podłączyć dwa urządzenia w klaster Active/Passive wymagane jest wygenerowanie na każde z urządzeń odpowiedniej licencji, tj. licencji typu **Master/Slave**. Można sprawdzić czy urządzenia mają licencje Master lub Slave logując się do *Client Area* na www.netasq.com. Poniżej przykład takiej licencji:



W celu skonfigurowania klastra HA należy na urządzeniu master wejść w zakładkę **USTAWIENIA SYSTEMOWE -> Klaster HA** i wybrać opcję **Utwórz klaster**. W kolejnym kroku należy wybrać interfejs sieciowy, który będzie używany do komunikacji pomiędzy urządzeniami 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.

W kolejnym oknie kreatora należy skonfigurować hasło, które będzie używane do zabezpieczania komunikacji pomiędzy urządzeniami.



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

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 oraz podać hasło do zabezpieczenie komunikacji (to samo, które zostało zdefiniowane na urządzeniu Master).

Zakończenie pracy kreatora spowoduje restart urządzenia Slave.

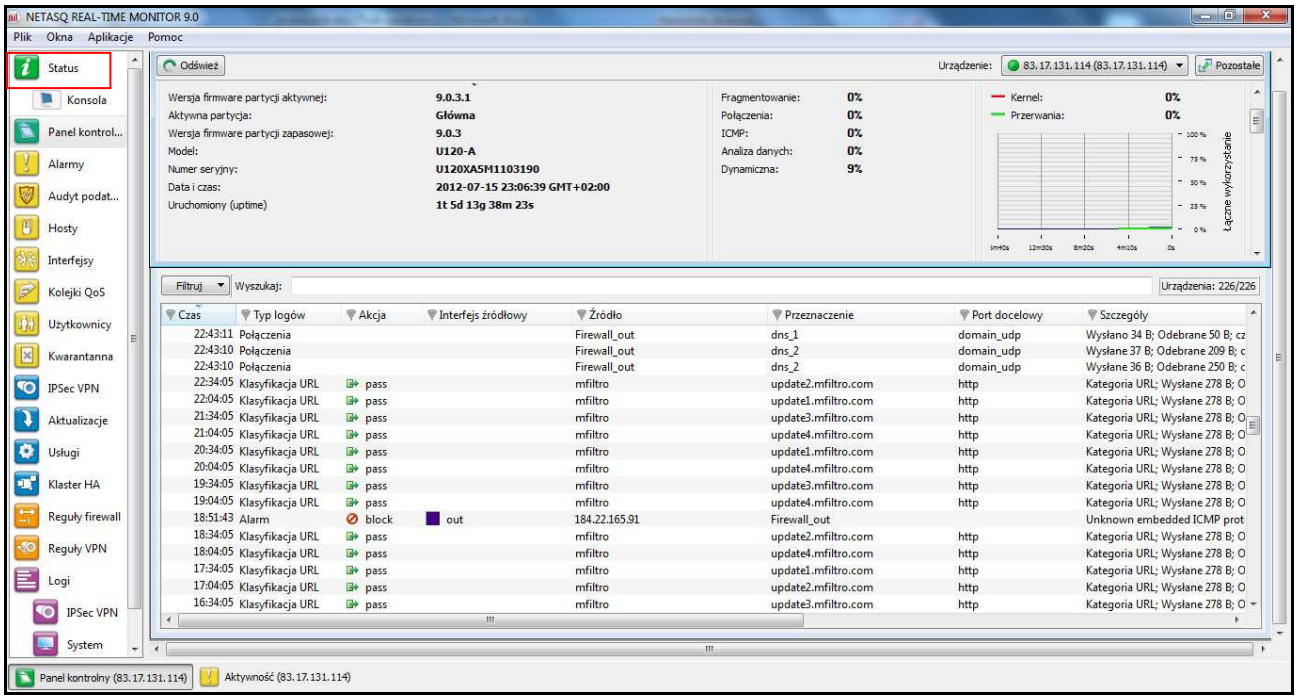
Synchronizacja konfiguracji możliwa jest poprzez użycie przycisku **Synchronizuj urządzenie pasywne z bieżącą konfiguracją** dostępnego z górnego menu interfejsu administracyjnego lub podczas wylogowywania z urządzenia, dlatego niezalecane jest kończenie pracy z interfejsem administracyjnym bez wylogowywania.

Uwaga

Klastra HA nie można wyłączyć z poziomu interfejsu urządzenia. Aby wyłączyć działanie HA należy zrestartować urządzenia do ustawień fabrycznych lub odtworzyć backup konfiguracji, który nie zawiera informacji o konfiguracji HA.

16. NETASQ Real-Time Monitor

Aplikacja NETASQ Real Time Monitor (RTM) służy do monitorowania w czasie rzeczywistym pracy urządzenia oraz do monitorowania stanu sieci. NETASQ RTM udostępnia informacje o hostach podłączonych do sieci, obciążeniu interfejsów sieciowych (w tym łączy internetowych), umożliwia również śledzenie połączeń sieciowych czy połączeń VPN. Poniżej znajduje się przykładowy widok okna Real Time Monitora:



W sekcji **Status** można zdefiniować dostęp do wielu różnych urządzeń i dzięki temu z poziomu jednej konsoli śledzić ich stan. Każde połączenie może odbywać się w T**rybie pełnym** (odczyt zapis) lub w trybie **Tylko odczyt**. Praca w trybie pełnym umożliwia skorzystanie z dodatkowych funkcji takich jak przenoszenie lub usuwanie hosta z kwarantanny, usuwanie aktywnych połączeń VPN, czy zarządzanie urządzeniem za pomocą komend **NSRPC** (zakładka Konsola).

Wskazówka

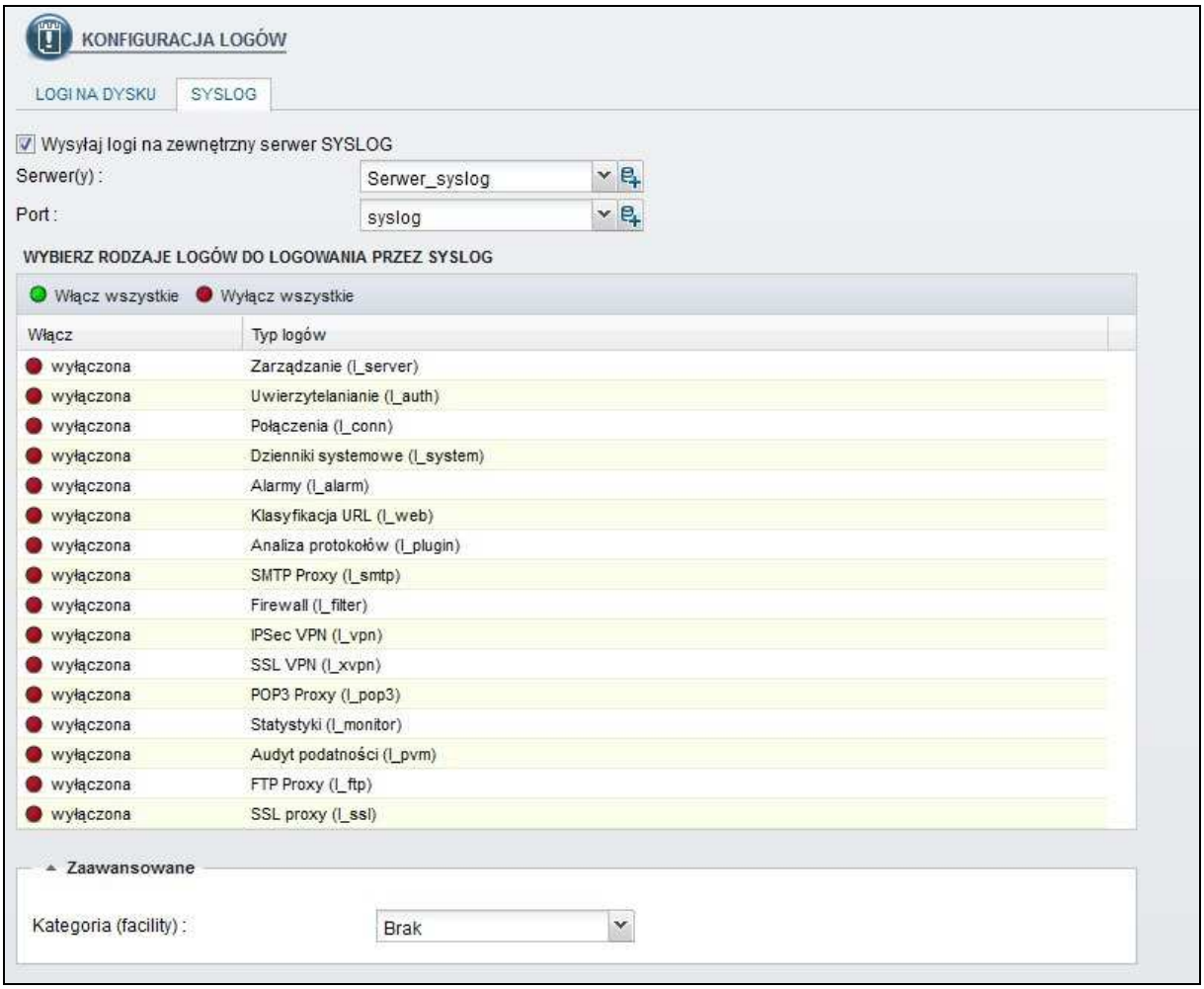
W przypadku blokowania ruchu przez IPS (ASQ) należy w pierwszej kolejności zweryfikować alarmy wyświetlane w sekcji **Alarmy**. Następnie należy odszukać blokujący komunikację alarm w WebGUI w zakładce **KONTROLA APLIKACJI -> Alarmy** i zmienić jego akcje z **Blokuj** na **Zezwól**. Oczywiście należy dokładnie przeanalizować czy ewentualna zmiana nie spowoduje obniżenia poziomu bezpieczeństwa.

17. NETASQ Event Reporter

Aplikacja NETASQ Event Reporter 9 służy do przeglądania logów historycznych z pracy urządzenia:

- Na urządzeniu NETASQ (U120, U150S, U250, U250S, U450,U500S, U800S, U1100, U1500, U6000, NG100, NG5000)
- Na dysku lokalnym stacji roboczej z zainstalowanym syslogiem (wszystkie urządzenia)

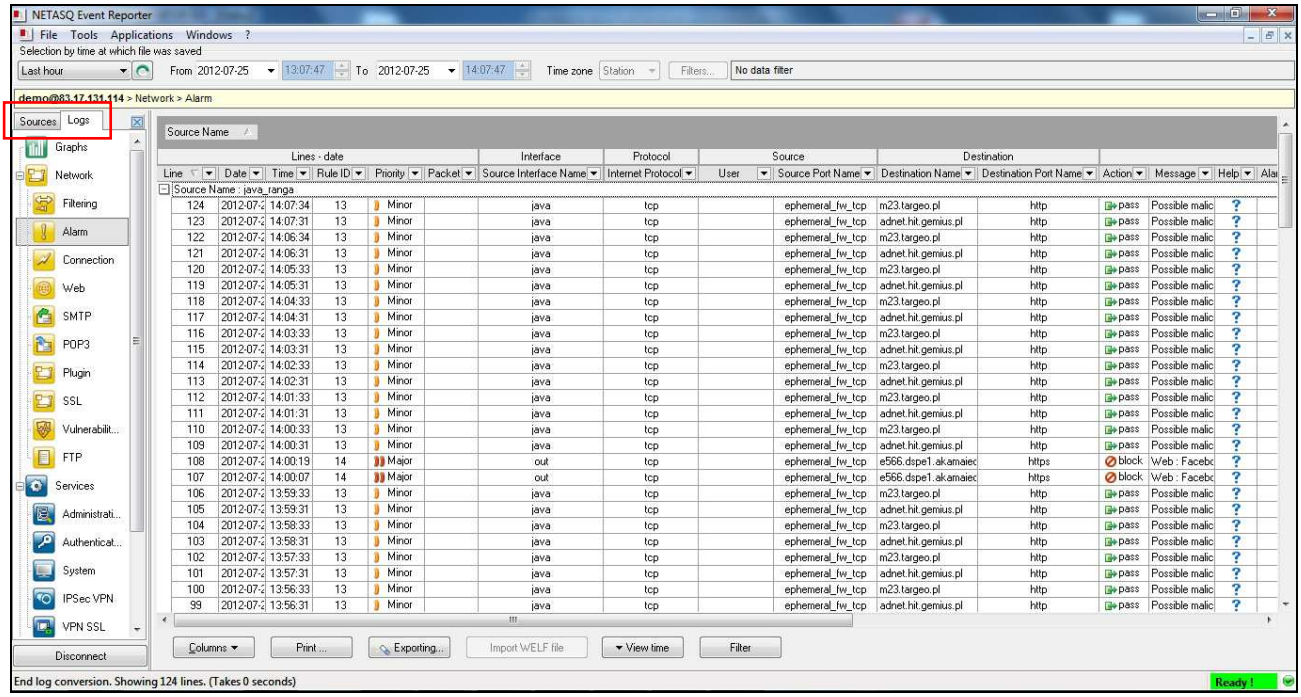
Na urządzeniu przechowywane są tylko i wyłącznie logi w przypadku urządzeń wyposażonych w dysk twardy. Dla pozostałych urządzeń należy ustawić przesyłanie logów na zewnętrzny serwer logów (**Syslog**). Przesyłanie logów na serwer syslog można skonfigurować w WebGUI w sekcji **Administracja -> Konfiguracja logów** w zakładce **Syslog**. Można tutaj ustawić nie tylko na jaki serwer, ale również jakie logi maja być wysyłane.



> **Uwaga**
>
> W przypadku korzystania z serwera syslog należy upewnić się, że wspiera on zbieranie logów w formacie WELF.

Źródło logów można zdefiniować wybierając w lewym menu zakładkę **Źródło (Sources)** i wybierając urządzenie wyposażone w dysk, z którego będą zaczytane logi lub wybierając opcję Syslog, co spowoduje wczytanie logów z serwera logów. Aby wskazać, w którym miejscu serwer Syslog przechowuje logi należy w menu wybrać **Tools -> Options** i przejść na zakładkę **Logs**.

Poniżej przedstawiono okno NETASQ Event Reporter. W lewym Menu można wybrać typ logów jakie będą wyświetlane w głównym oknie aplikacji.



Aby ułatwić przeglądanie logów można skorzystać z opcji agregacji logów. W tym celu należy kliknąć na kolumnę, na podstawie której chcemy agregować logi i przeciągnąć ją na szare pole powyżej kolumn.

18. NETASQ Event Reporter Light

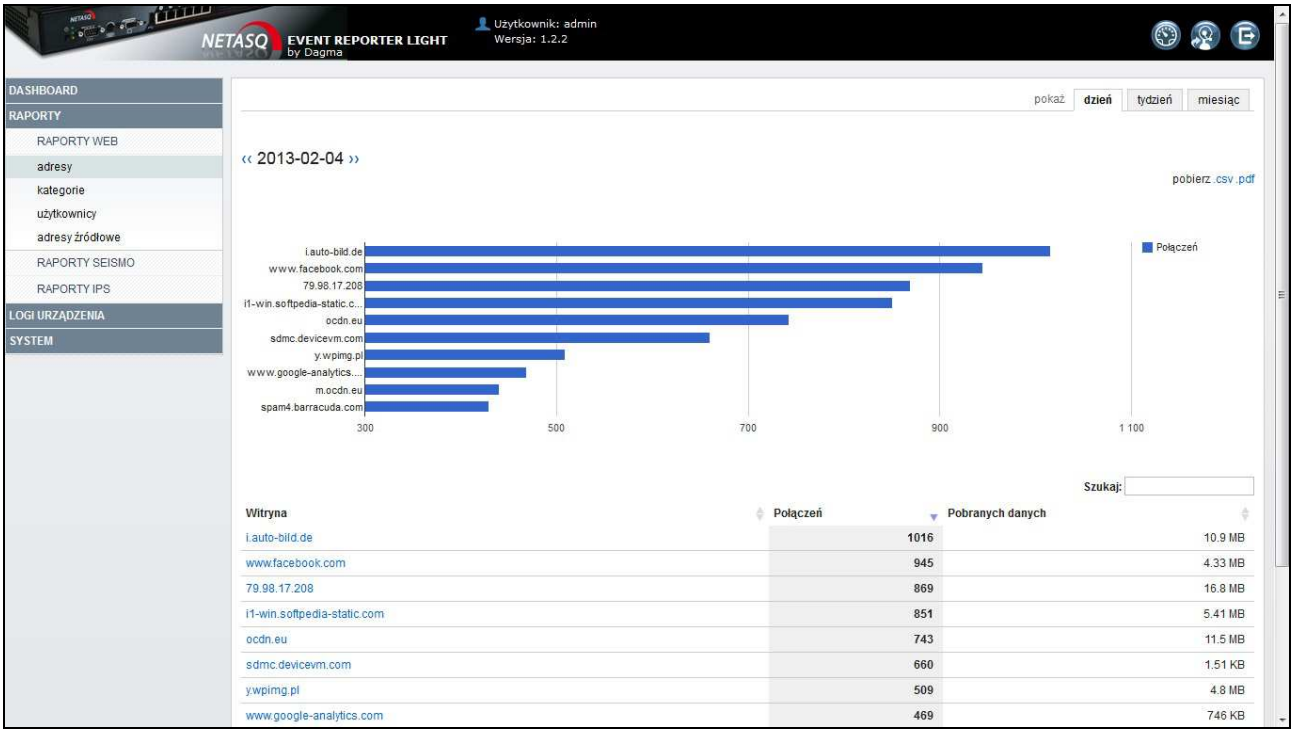
Event Reporter Light to darmowy system raportujący do rozwiązań NETASQ UTM. Administracja **Event Reporterem Light** tak jak samym urządzeniem NETASQ odbywa się poprzez WebGUI . Event Reporter Light oparty jest na darmowym systemie Linux – Xubuntu a więc nie wymaga dodatkowych licencji a jego instalacja odbywa się z obrazu LiveCD na dedykowanym komputerze lub maszynie wirtualnej.

Event Reporter Light (ERL) umożliwia generowanie najbardziej pożądanych przez administratorów raportów z:

- filtra stron www – najczęściej odwiedzane strony, najbardziej aktywni użytkownicy w ujęciu liczby odwiedzin stron oraz ilości pobranych danych;
- systemu IPS – najczęściej generowane alarmy IPS, komputery, których te alarmy dotyczyły;
- audytu podatności – najczęściej wykrywane zagrożenia oraz aplikacje, których one dotyczą;

Wygenerowane raporty mogą obejmować pojedynczy dzień, tydzień lub cały miesiąc i mogą być przeglądane zarówno w postaci stron www jak i raportów wygenerowanych w postaci plików PDF i CSV. Poza raportami graficznymi ERL pozwala również na przeglądanie historycznych logów tekstowych zgromadzonych na urządzeniu.

Poniżej znajduje się przykładowy raport strony najczęściej odwiedzane przez użytkowników sieci.



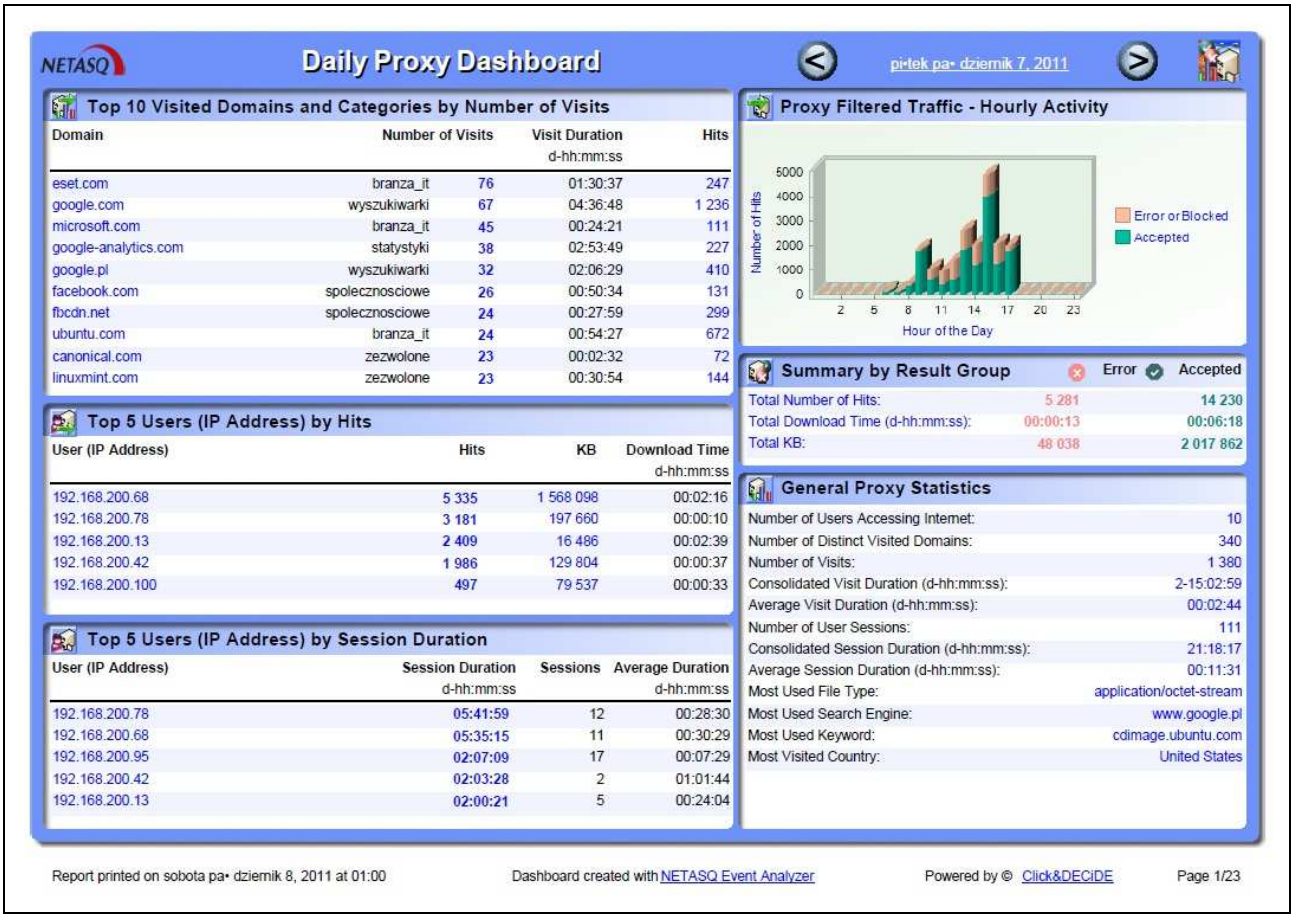
19. NETASQ Event Analyzer

NETASQ Event Analyzer to rozbudowane narzędzie raportujące pozwalające z dużą dokładnością śledzić i analizować aktywność użytkowników i poziom bezpieczeństwa sieci. NETASQ Event Analyzer (NEA) poza podstawowymi raportami takimi jak ilość wizyt na stronie czy ilość pobranych danych pozwala również na generowanie szczegółowych raportów np. z informacjami o średnim czasie przebywania użytkowników na stronie www, czy frazach wyszukiwanych w Internecie. Ponadto NETASQ Event Analyzer pozwala na monitorowanie i ocenę stanu zabezpieczeń firmowej sieci, sprawdzenie rzeczywistego obciążenia łącza, a także umożliwia dokładne przeanalizowanie ewentualnych prób ataku.

Do dyspozycji administratora jest ponad 200 predefiniowanych raportów, które mogą być generowane zgodnie ze zdefiniowanym harmonogramem lub na żądanie. Administrator ma również możliwość przygotowania własnego raportu według zadanych kryteriów.

NETASQ Event Analyzer instalowany jest w środowisku Microsoft Windows a dzięki zastosowaniu wydajnej bazy Microsoft SQL Server NEA sprawdza się świetnie w dużych środowiskach produkcyjnych do których jest dedykowany.

Poniżej znajduje się przykładowy raport wygenerowany za pomocą NEA. Raport zawiera informacje o najczęściej odwiedzanych stronach oraz adresach IP, które adresach IP generujących najwięcej ruchu. Wykres w prawym górnym rogu obrazuje rozkład ilości ruchu w ciągu dnia, dla którego raport powstał.



NETASQ

Daily Proxy Dashboard

piątek pa• dziernik 7, 2011

Top 10 Visited Domains and Categories by Number of Visits

Domain		Number of Visits	Visit Duration d-hh:mm:ss	Hits
eset.com	branza_it	76	01:30:37	247
google.com	wyszukiwarki	67	04:36:48	1 236
microsoft.com	branza_it	45	00:24:21	111
google-analytics.com	statystyki	38	02:53:49	227
google.pl	wyszukiwarki	32	02:06:29	410
facebook.com	spolecznosciowe	26	00:50:34	131
fbcdn.net	spolecznosciowe	24	00:27:59	299
ubuntu.com	branza_it	24	00:54:27	672
canonical.com	zezwolone	23	00:02:32	72
linuxmint.com	zezwolone	23	00:30:54	144

Top 5 Users (IP Address) by Hits

User (IP Address)	Hits	KB	Download Time d-hh:mm:ss
192.168.200.68	5 335	1 568 098	00:02:16
192.168.200.78	3 181	197 660	00:00:10
192.168.200.13	2 409	16 486	00:02:39
192.168.200.42	1 986	129 804	00:00:37
192.168.200.100	497	79 537	00:00:33

Top 5 Users (IP Address) by Session Duration

User (IP Address)	Session Duration d-hh:mm:ss	Sessions	Average Duration d-hh:mm:ss
192.168.200.78	05:41:59	12	00:28:30
192.168.200.68	05:35:15	11	00:30:29
192.168.200.95	02:07:09	17	00:07:29
192.168.200.42	02:03:28	2	01:01:44
192.168.200.13	02:00:21	5	00:24:04

Proxy Filtered Traffic - Hourly Activity

Summary by Result Group

	Error	Accepted
Total Number of Hits:	5 281	14 230
Total Download Time (d-hh:mm:ss):	00:00:13	00:06:18
Total KB:	48 038	2 017 862

General Proxy Statistics

Number of Users Accessing Internet:	10
Number of Distinct Visited Domains:	340
Number of Visits:	1 380
Consolidated Visit Duration (d-hh:mm:ss):	2-15:02:59
Average Visit Duration (d-hh:mm:ss):	00:02:44
Number of User Sessions:	111
Consolidated Session Duration (d-hh:mm:ss):	21:18:17
Average Session Duration (d-hh:mm:ss):	00:11:31
Most Used File Type:	application/octet-stream
Most Used Search Engine:	www.google.pl
Most Used Keyword:	cdimage.ubuntu.com
Most Visited Country:	United States

Report printed on sobota pa• dziernik 8, 2011 at 01:00 Dashboard created with NETASQ Event Analyzer Powered by © Click&DECiDE Page 1/23

Uwaga

Dla NETASQ Event Analyzer dostępna jest osobna dokumentacja, którą można pobrać ze strony www.netasq.pl lub ze strefy klienta (Client Area) na stronie www.netasq.com

20. 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 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 z 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 firmware można pobrać ze strony www.netasq.com po zalogowaniu się do strefy klienta. W strefie klienta poza najnowszymi wersjami firmware można znaleźć między innymi najnowsze wersje pakietu Administration Suite czy dokument Release Note, który opisuje zmiany jakie zostały wprowadzone w najnowszych wersjach oprogramowania.

Jak uruchomić dostęp przez SSH do urządzenia NETASQ?

Dostęp do urządzenia poprzez SSH konfiguruje się w sekcji **Ustawienia systemowe -> Konfiguracja urządzenia** w zakładce **Dostęp administracyjny**. Dostęp może się odbywać z wykorzystaniem hasła (opcja niezalecana) lub z użyciem pary kluczy publiczno-prywatnych, które można pobrać z sekcji **Ustawienia systemowe -> Administratorzy** z zakładki **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 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 w sekcję **Ustawienia systemowe -> System** a następnie w zakładce **Konfiguracja** wybrać przycisk **Pobierz raport**.

Z poziomi CLI raport można wygenerować używając komendy „*sysinfo*”

Jak zmienić hasło użytkownika *admin*

Aby zmienić hasło użytkownika admin należy przejść do sekcji **Ustawienia systemowe -> Administratorzy** na zakładkę **Konto Administratora** a następnie podać dwukrotnie nowe hasło.

Z poziomu CLI hasło można zmienić korzystając z polecenia *chpwd*. Zmiana hasła w ten sposób wiąże się z koniecznością restartu urządzenia.

Uwaga

Hasło użytkownika **admin** można zmienić jedynie będą zalogowanym jako **admin**.

Jak wygląda procedura aktualizacji firmware?

Aby zaktualizować firmware należy przejść do sekcji **Ustawienia systemowe -> System** a następnie na zakładce **Aktualizacja systemu** należy wybrać plik z najnowszą wersją firmware pobrany uprzednio ze **Strefy klienta** na stronie www.netasq.com. Należy upewnić się, że została wybrana opcja **Kopiuj bieżącą partycję na zapasową** przed aktualizacją. 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 serial lub za pomocą monitora i klawiatury, a następnie zrestartować urządzenie.
Przy uruchomieniu się urządzenia pojawi się opcja wyboru, z której partycji ma startować:

NETASQ Firewall BOOT
1) Main
2) Backup
choose:

W tym momencie należy wybrać kilkukrotnie przycisk spacji.
Po uzyskaniu znaku zachęty 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 NETASQ dostępny jest tzw. KNOWLEDGE BASE?

Tak, KNOWLEDGE BASE znajduje się pod adresem https://kb.netasq.com/ i dostępny jest dla każdego zarejestrowanego klienta NETASQ.

Innym sposobem dostępu do KNOWLEDGE BASE jest zalogowanie się do strefy klienta na stronie www.netasq.com i wybranie z górnego menu TECHNICAL SUPPORT -> Knowledge Base.