NETASQ

NETASQ

PODRĘCZNIK UŻYTKOWNIKA

Kontakt:

Dagma sp. z o.o., www.netasq.pl

032 259 11 38 netasq@dagma.pl

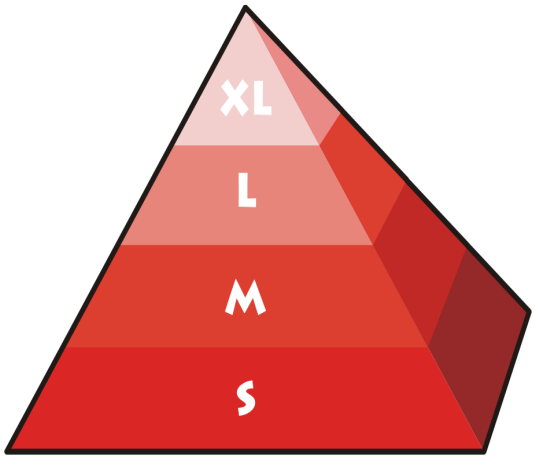
SPIS TREŚCI

1. Wprowadzenie

Gratulujemy zakupu NETASQ UTM!

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 - seria U:



Seria XL: U6000

Seria L: U1100 / U1200

Seria M: U120 / U250 / U450

Seria S: U30 / U70

	U30	U70	U120	U250	U450	1100	U1500	U6000
Interfejsy	2	6	6	6	15	8	10	6-24
Liczba połączeń	50000	100000	200000	400000	600000	800000	1200000	2500000
Przepustowość	200	600	700	850	1000	2800	3800	5000
Nowe połączenia/sek	4000	6000	6500	8500	10500	20000	25000	40000
SSL VPN	-	50	256	512	512	1024	1024	2048
IPSec VPN	50	100	500	1000	1000	4000	6000	10000
PPTP	48	48	96	96	96	192	192	192
Dysk Twardy	-	-	70GB	70GB	70GB	70GB	70GB	70GB

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 urządzenie dokonuje się na podstawie charakterystyki sieci (liczba stacji roboczych, liczba serwerów etc.). W przypadku jakichkolwiek wątpliwości prosimy o kontakt na adres pomoc@dagma.pl.

Podstawowe funkcje NETASQ UTM:

- Stateful Inspection Firewall,
- Instrusion Prevention/Intrusion Detection System (IPS/IDS),
- Pasywny skaner zagrożeń (SEISMO),
- VPN Serwer (IPSec VPN, SSL VPN, PPTP VPN),
- Uwierzytelnianie i integracja Microsoft Active Directory Lub LDAP,
- Kształtowanie pasma (QoS),
- Skaner antywirusowy – ClamAV lub Kaspersky (http, pop3, smtp, ftp),
- Moduł antyspam,
- Klasyfikacja URL – NETASQ URL lub Optenet URL (od modelu U120),
- Serwer DHCP,
- Klient NTP,
- Monitorowanie w czasie rzeczywistym,
- Logowanie i raportowanie.

Wszystkie funkcję są w podstawowej licencji. Funkcje wymagające rozszerzonego serwisu to:

- Pasywny skaner zagrożeń (SEISMO),
- Antywirus firmy Kaspersky,
- Klasyfikacja URL firmy OPTENET.

2. Przed podłączeniem urządzenia

Urządzenia NETASQ UTM dostarczone są w oryginalnym opakowaniu. Na opakowaniu widoczna jest naklejka z informacją o modelu oraz wersji firmware. Opakowanie zabezpieczone jest przed otwarciem inną 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. Rejestracja urządzenia (pobranie licencji)[1],
3. 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, U70, F25, F50, F60) 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 (tylko modele klasy S).

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

[1] Nie dotyczy jeśli wraz z urządzeniem dostarczono informacje rejestracyjne.

Rejestracja urządzenia (pobieranie licencji).

Uwaga

Jeżeli do urządzenia dołączono informację rejestracyjną tj. nazwę użytkownika i hasło do strefy dla klientów na www.netasq.com to można pominąć sekcję na temat rejestracji. Oznacza to, iż urządzenie zostało już zarejestrowane i licencja jest wczytana na urządzenie.

Każde urządzenie NETASQ należy zarejestrować. Po rejestracji możliwe jest pobranie licencji na korzystanie z poszczególnych usług, a także na automatyczne pobieranie aktualizacji dla systemu antywirus, antyspam, IPS etc. Dodatkowo, rejestracja jest wymagana do uzyskania wsparcia technicznego ze strony DAGMA sp. z o.o.. Aby dokonać rejestracji potrzebne jest przygotowanie danych, które znajdują się na spodzie urządzenia. Rysunek poniżej przedstawia etykietę na spodzie urządzenia:

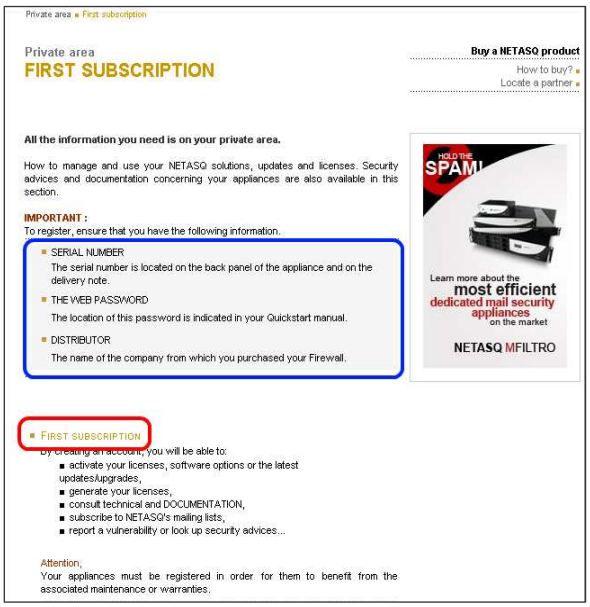
Rejestracji dokonać należy na stronie www.netasq.com. Dokładny adres strony do rejestracji to: http://www.netasq.com/en/secure/client-register.php

Na stronie www.netasq.com należy wybrać **CLIENTS–PARTNERS** następnie pozycję *„Register your first NETASQ product”:*

Do rejestracji potrzebne są:

- Numer seryjny urządzenia (*serial number*),
- Web (*web password*) – patrz etykieta na spodzie urządzenia,
- Dystrybutor – określa sprzedawcę urządzenia,
- Dane kontaktowe. Podczas rejestracji ważne by uzupełnić poprawnie wszystkie dane kontaktowe (pełna nazwa firmy, adres, telefon, fax oraz e-mail).

W przypadku pierwszej rejestracji należy wybrać „*First Subscription*".



W kolejnym etapie można:

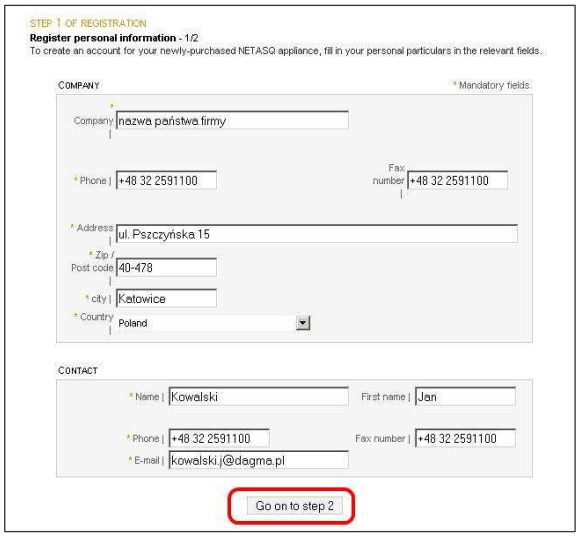
- zalogować się do **PRIVATE AREA** (jeśli zakupiono kolejne rozwiązanie NETASQ),
- ponownie potwierdzić pierwszą rejestrację „*Register your first NETASQ product*".

Wskazówka

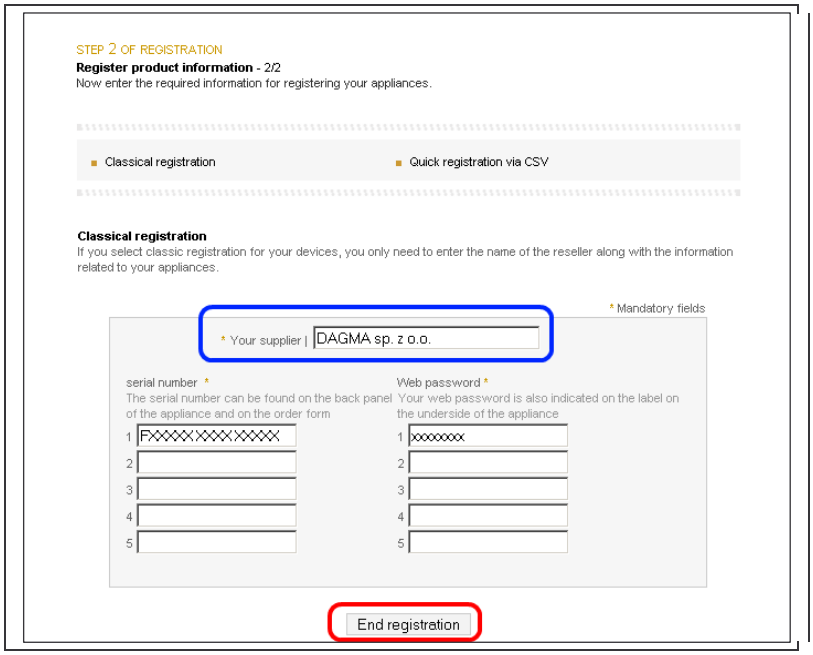
Pomyślne zakończenie rejestracji gwarantuje otrzymanie nazwy użytkownika (*login*) i hasła (*password*). Uprawniają one do korzystania z **PRIVATE AREA** na www.netasq.com. Serwis ten oferuje:

- pobieranie aktualizacji firmware,
- pobieranie licencji do urządzenia,
- dostęp do bazy wiedzy (*knowledge base*),
- dostęp do plików dokumentacji (wersja angielska).

Kolejny krok to wypełnienie informacji na temat Państwa firmy. Pola oznaczone * są wymagane do przeprowadzenia pomyślnej rejestracji. Dane wprowadzone na tym etapie będzie można później modyfikować. Po wypełnieniu formularza należy wybrać „*Go on to step 2*". Pola oznaczone gwiazdką są obowiązkowe. Dane zawarte na tej stronie będzie można później zmienić.



Dalej należy wprowadzić numer seryjny rejestrowanego urządzenia i hasło (*web password*), które znajdują się na spodzie urządzenia.



Pole „*Your supplier*" należy uzupełnić nazwą firmy sprzedawcy urządzenia lub wpisać DAGMA sp. z o.o.. Jednorazowo można określić do pięciu urządzeń które są rejestrowane. Jeżeli urządzeń jest więcej niż pięć należy wybrać opcję „*Quick registration via CSV*" i podać listę rejestrowanych urządzeń w pliku.

Po wprowadzeniu wszystkich danych należy kliknąć „*End registration*". Na ekranie ukaże się potwierdzenie dokonania rejestracji. Zostaną także wyświetlone nazwa użytkownika (*login*) i hasło (*password*) do **CLIENT AREA** na www.netasq.com. Dane te zostaną także wysłane na adres e-mail podany przy rejestracji. Zakończenie procesu rejestracji wyzwala proces generowania licencji.

Uwaga

Automatyczne generowanie licencji, po zakończeniu rejestracji, może trwać ok. jednej godziny.

Uwaga

W przypadku jakichkolwiek wątpliwości lub problemów podczas procesu rejestracji prosimy o kontakt. Dane kontaktowe znajdują się na stronie www.netasq.pl. Można także wysłać wiadomość pod adres pomoc@dagma.pl, wpisując w temacie „*problem z rejestracją NETASQ UTM*".

Analiza sposobu podłączenia urządzenia do sieci firmowej.

Przed przystąpieniem do instalacji urządzenia NETASQ zalecamy analizę sposobu, w jaki sposób urządzenie zostanie podłączone w istniejącą infrastrukturę. Przygotowanie tzw. topologii sieci wraz z analizą dotyczącą ustawień funkcji na urządzeniu NETASQ znacznie przyśpiesza proces wdrożenia. Dobrą praktyką jest określenie używanej adresacji, a także przygotowania polityki bezpieczeństwa w odniesieniu do infrastruktury sieciowej.

Topologia sieci z określeniem adresacji jest również wymagana przy zgłoszeniu zapytań do działu wsparcia technicznego firmy DAGMA sp. z o.o..

3. Instalacja oprogramowania Administration Suite

Administration Suite jest to pakiet oprogramowania firmy NETASQ służący do zarządzania, monitorowania oraz zarządzania logami z urządzenia NETASQ UTM. Oprogramowanie należy zainstalować na stacji roboczej administratora. Dodatkowo można zainstalować na serwerze, który będzie pełnił rolę maszyny agregującej pliki dzienników.

Uwaga

Administration Suite to zbiór aplikacji i wszystkie one zostaną omówione poniżej. Co ważne, wszystkie te aplikacje są zaszyte w jeden plik instalacyjny. Nie ma więc potrzeby pobierać dodatkowych aplikacji. Oprogramowanie narzędziowe, instalowane osobno, to: Windows Terminal, Putty, WinSCP, WireShark. Dokument ten nie omawia procedury ich instalacji i sposobu wykorzystania.

Gdy urządzenie jest w domyślnej konfiguracji istnieje możliwość dokonania wstępnych ustawień przy użyciu konsoli www poprzez tzw. Kreator konfiguracji (domyślnie pod adresem https://10.0.0.254). W każdym innym przypadku do konfiguracji wykorzystuje się pakiet Administration Suite.

Poniżej przedstawiono kolejne kroki instalacji oprogramowania w wersji 7 i 8. Pełny pakiet oprogramowania Administration Suite można pobrać ze strony www.netasq.com w strefie dla klientów lub wykorzystując poniższe odnośniki:

Wersja 7: www.dagma.pl/new/netasq/software/as_7.exe

Wersja 8: www.dagma.pl/new/netasq/software/as_8.exe

Wymaganie systemowe dla oprogramowania Administration Suite.

Procesor: minimum 2GHz

Pamięć RAM: 512 MB (Windows XP) dla stacji roboczej, 2 GB dla instalacji na serwerze.

Przestrzeń dyskowa: ~ 300MB

System operacyjny (32-bit): Instalacja na stacji klienckiej: Microsoft Windows Server 2003 SP2, Microsoft Windows XP Service Pack 2 lub wyższy, Microsoft Windows Vista. Instalacja oprogramowania serwerowego (Collector, Autoreporter, PostgreSQL):Microsoft Windows Server 2003 SP2, Microsoft Windows XP Service Pack 2 lub wyższy

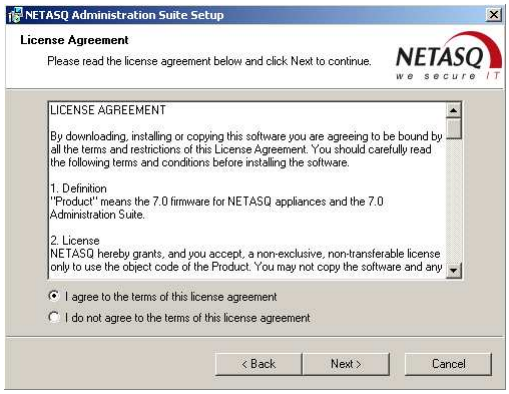
Uwaga

Urządzenia NETASQ dostarczone jest ze startową wersją firmware. Należy pamiętać, że aby podłączyć się do urządzenia z firmware w wersji np. 7.0.5.1 należy posiadać zainstalowane oprogramowanie Administration Suite w wersji 7.x Na płycie CD dostarczonej wraz z urządzeniem znajduje się zawsze odpowiadająca wersja Administration Suite wraz z dokumentacją.

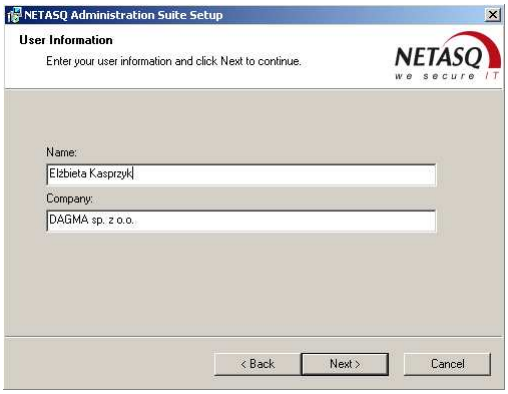
Uwaga

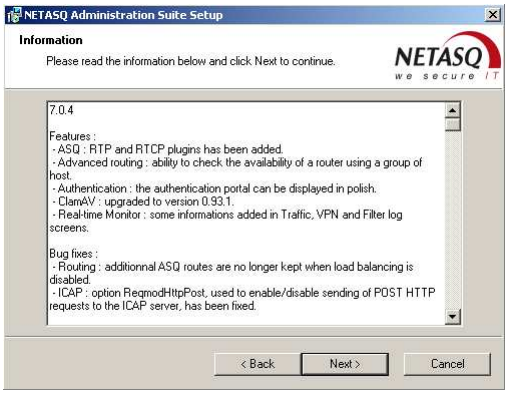
Na końcu tego dokumentu, w rozdziale: „*Najczęściej zadawane pytania (FAQ)*", znajdziecie Państwo informację na temat aktualizacji firmware. Aby dokonać aktualizacji firmware trzeba przynajmniej raz podłączyć się do urządzenia w celu nadania hasła dla administratora.

Po uruchomieniu instalatora Administration Suite należy kliknąć *NEXT*, zapoznać się z umową licencyjną i ją zaakceptować:



Następnie podać należy nazwę użytkownika oraz nazwę firmy, dla której zakupiono urządzenie i przejść dalej klikając na przycisk *NEXT*. W kolejnym kroku pojawi się okno informuje o nowościach w aktualnie instalowanym pakiecie, jak i odpowiadającej jej najnowszej wersji firmware. W przypadku aktualizacji oprogramowania zalecane jest zapoznanie się z tym dokumentem (dostępny również na www.netasq.com jako tzw. *Release info*).





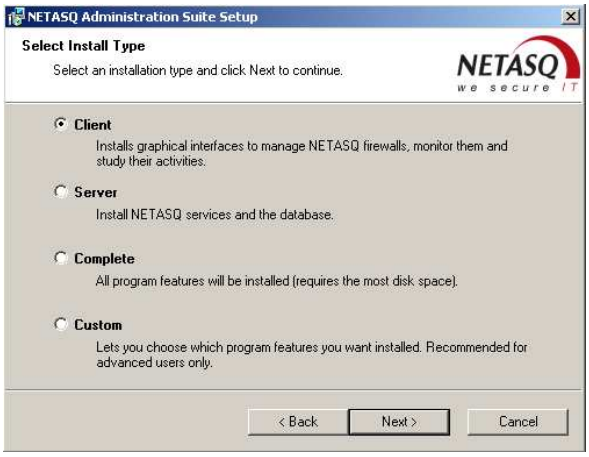
Po wybraniu przycisku NEXT pojawi się okno wyboru typu instalacji. Dostępne są cztery tryby:

Client – instalacja podstawowa (Unified Manager, Real-Time Monitor, Event-Reporter, NETASQ Updater).

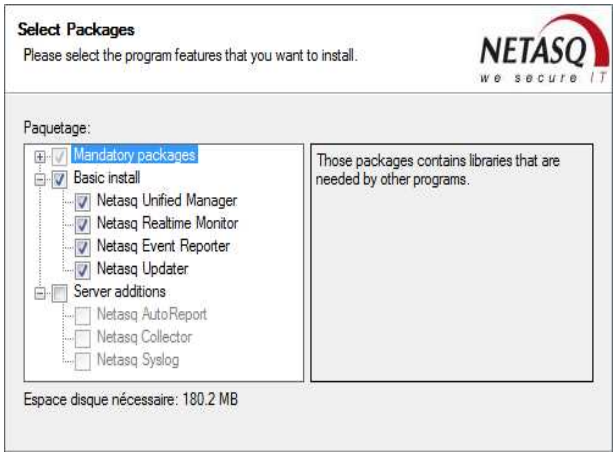
Server – instalacja serwerowa (PostgreSQL, NETASQ Collector, NETASQ Autoreporter, NETASQ Syslog).

Complete – instalacja pełna.

Custom – instalacja użytkownika.



wersja 7



wersja 8

Do zarządzania NETASQ zalecana jest instalacja podstawowa. Krótki opis wszystkich aplikacji znajduje się poniżej:

NETASQ Unified Manager (w wersji 6.x zwany Firewall Manager)

Pozwala na konfigurację urządzeń NETASQ. Unified Manager domyślnie pracuje w trybie „Firewall Mode". Tryb ten pozwala na konfigurację jednego urządzenia. Drugim dostępnym trybem pracy jest tryb „*Global Administration mode*" pozwalający na administrację jednym lub kilkoma urządzeniami. Domyślna licencja pozwala na administrację maksymalnie do 5 urządzeniami. NETASQ Unified Manager wchodzi w skład instalacji typu *Client*.

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 etc. W przypadku urządzeń wyposażonych w dysk twardy umożliwia także podgląd logów. NETASQ Real-Time Monitor wchodzi w skład instalacji typu *Client*.

NETASQ Event-Reporter

Służy do przeglądania dzienników (logów). Źródłem danych może być samo urządzenie NETASQ (jeżeli posiada dysk twardy), baza danych PostgreSQL lub dzienniki zapisane w plikach tekstowych na komputerze (pobrane przez NETASQ Syslog). NETASQ Events-Reporter wchodzi w skład instalacji typu *Client*.

NETASQ Collector

Jest odpowiedzialny za import plików dzienników do bazy danych PostgreSQL.

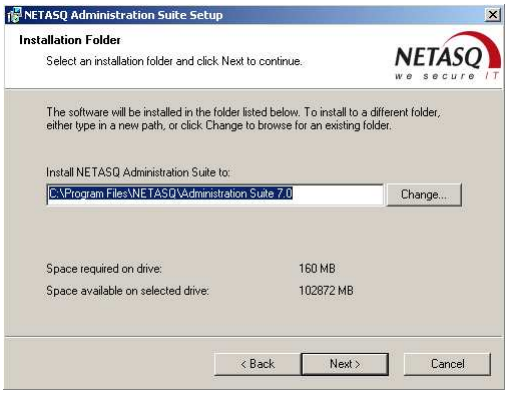
NETASQ Autoreporter

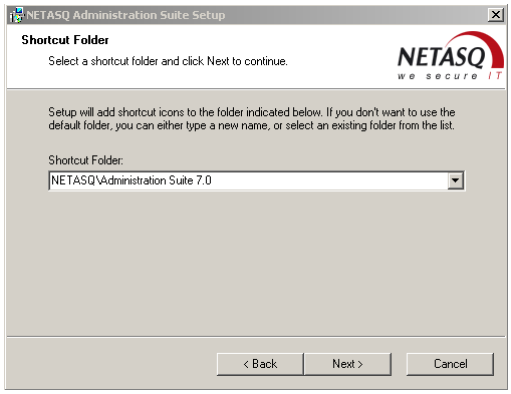
Odpowiada za tworzenie raportów. Raporty generowane są na podstawie danych składowanych w bazie PostgreSQL. Instalacja NETASQ Autoreportera automatycznie wymusza instalacje serwera PostgreSQL.

NETASQ Updater

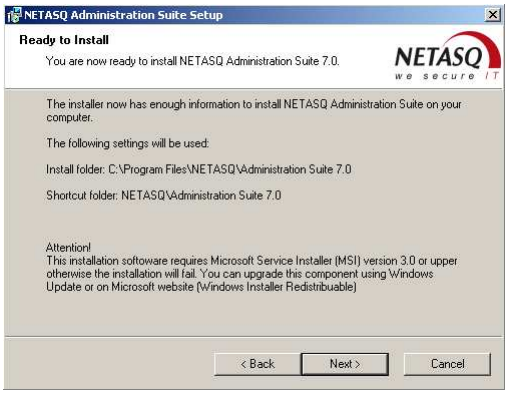
Służy do pobierania aktualizacji plików pomocy urządzeń NETASQ. NETASQ Updater. Wchodzi w skład instalacji typu *Client*.

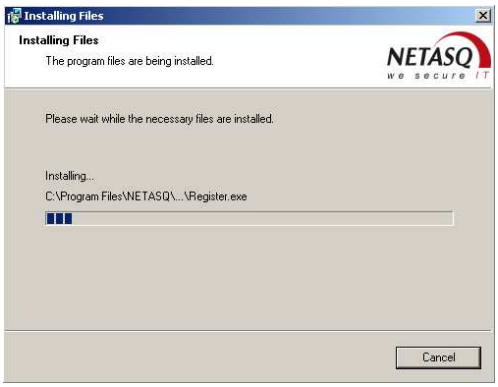
Po wybraniu odpowiedniego typu instalacji należy kliknąć NEXT. Pojawi się okno:

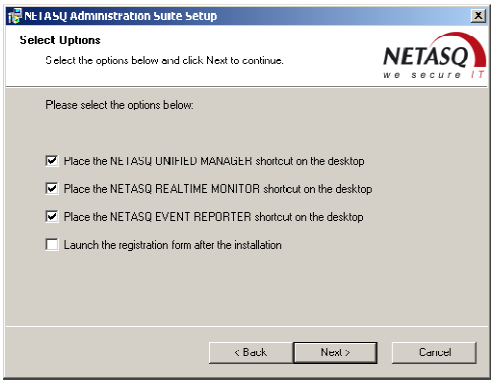




W oknie tym należy określić ścieżkę do katalogu, w którym zainstalowane zostaną pliki NETASQ Administration Suite. Następnie, należy określić nazwę grupy dla aplikacji w menu start. Kolejny krok to potwierdzenie parametrów instalacji.







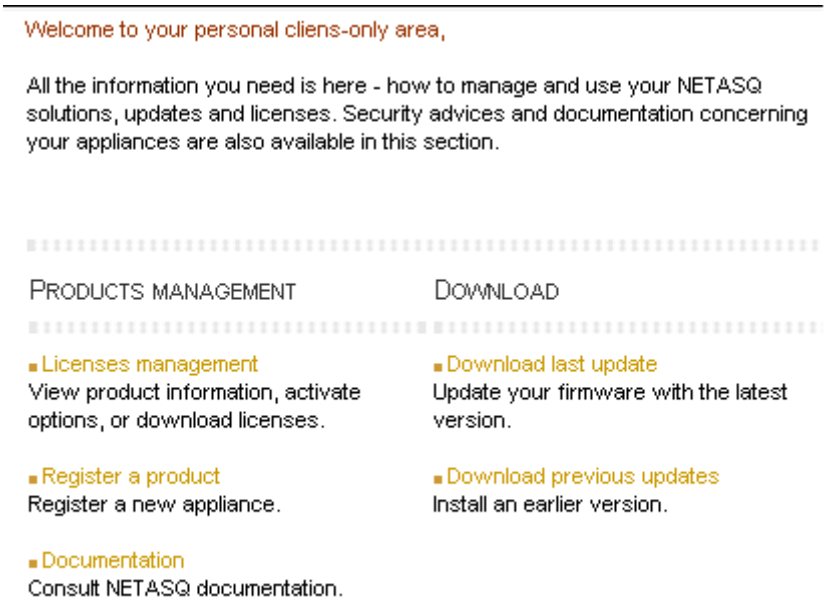
W ostatnim etapie instalacji program pyta, czy utworzyć skróty do programu na pulpicie. Ostatnia opcja „*Launch the registation form after the installation*" pozwala na koniec instalacji uruchomić stronę www.netasq.com. Po przejściu na stronę można będzie dokonać rejestracji urządzenia. Jeśli urządzenie zostało wcześniej zarejestrowane to należy odznaczyć tą opcje. Po wybraniu przycisku NEXT nastąpi zakończenie instalacji.

4. 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.

Przed włączeniem urządzenia należy pobrać licencje do urządzenia NETASQ. W tym celu należy przejść do strony: http://www.netasq.com/en/secure/client-register.php. Do logowania wykorzystać nazwę użytkownika i hasło otrzymaną podczas rejestracji. Dzięki autoryzacji uzyskujecie Państwo dostęp do tzw. *CLIENT AREA*. Po pomyślnym zalogowaniu się pojawi się ekran:



Licenses management

W tym miejscu można pobrać licencje dla zarejestrowanych urządzeń NETASQ.

Register a product

Umożliwia rejestracje kolejnego urządzenia NETASQ.

Documentation

Pozwala na pobranie dokumentacji w języku angielskim.

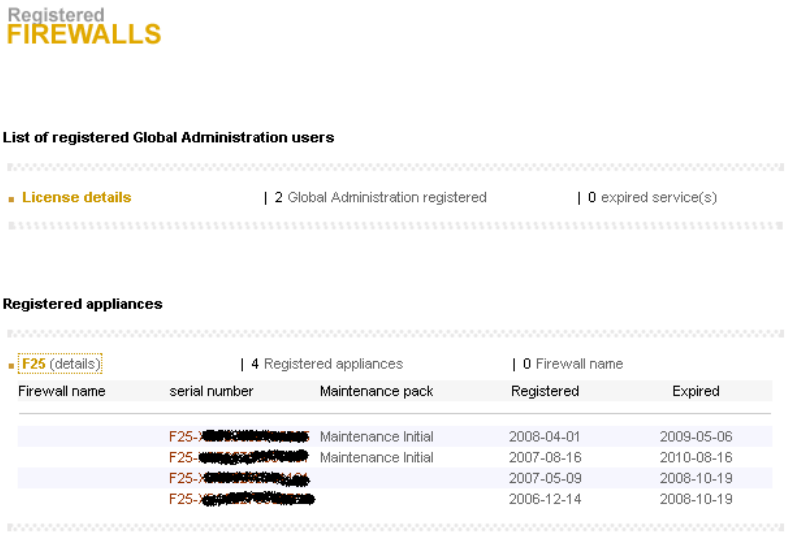
Download last update

Na tej stronie można pobrać najnowsze wersje firmware dla zarejestrowanych urządzeń.

Download previous updates

Pozwala na pobranie archiwalnych wersji firmware.

Zgodnie z powyższym należy pobrać licencję. Po wybraniu opcji *„Licenses management”*, pojawi się strona:

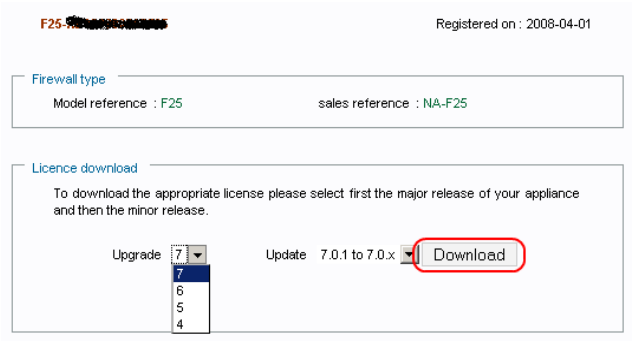


Na liście urządzeń będą widoczne wszystkie zarejestrowane urządzenia. Po wybraniu odpowiedniego numeru seryjnego nastąpi przejście do witryny, na której można pobrać plik licencyjny.

Wskazówka

Jeżeli na stronie nie widać żadnego numeru seryjnego urządzenia oznacza to, że proces automatycznego generowania licencji nie został jeszcze zakończony. Proszę spróbować ponownie za 60 minut lub napisać na adres e-mail: pomoc@dagma.pl.

Dla wskazanego urządzenia pojawia się możliwość pobrania licencji. W pierwszym etapie należy pobrać wersję licencji zgodną z wersją firmware zainstalowaną na urządzeniu.



Plik z licencją (*.license) należy zapisać na komputerze, z którego zostanie dokonane pierwsze podłączenie do urządzenia oraz na którym zainstalowano Administration Suite. Następnie można przystąpić do kolejnego kroku, pierwszego podłączenia się do urządzenia.

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@dagma.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 Unified Manager lub polecenie *HALT* z linii poleceń. Dla serii F, od modelu F200 dostępny jest przycisk, który służy do bezpiecznego wyłączenia urządzenia. Należy przycisnąć go raz (dioda zacznie mrugać), a następnie przycisnąć drugi raz w celu potwierdzenia wyłączenia. W przypadku serii U przycisk wyłączenia znajduje się 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);

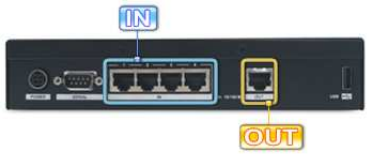
Urządzenie w ustawieniach domyślnych pozwala jednak na zastosowanie tylko dwóch metod:

- Przy wykorzystaniu Unified Managera;
- Przy wykorzystaniu przeglądarki www (IE, Firefox) – https://10.0.0.254 lub https://numer_seryjny.

Zalecana metoda to podłączenie przez NETASQ Unified Managera. Dostęp przez przeglądarkę www jest przeznaczony tylko do podstawowej konfiguracji i aktywny jest tylko do momentu ustalenia hasła dla administratora (użytkownik **admin**).

Urządzenie NETASQ należy podłączyć kablem Ethernet dostarczonym od producenta do komputera z zainstalowanym Administration Suite w celu dokonania wstępnej konfiguracji. Urządzenie w domyślnej konfiguracji dostępne jest pod adresem IP NETASQ (*10.0.0.254*). Tak więc, komputer musi mieć skonfigurowany adres IP z sieci 10.0.0.0/8 (np. *10.0.0.7/255.0.0.0*). Kabel należy podłączyć do portu **IN** urządzenia i karty sieciowej komputera. Poniższe rysunki wskazują port **IN** w konkretnych modelach.

SERIA F



F25

PORT IN – PORT 1

F50

PORT IN – PORT 1

F60

PORT IN – PORT 1

F200

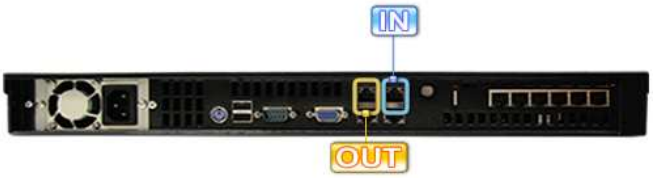
PORT IN – PORT 2

F500

PORT IN – PORT 2

F800

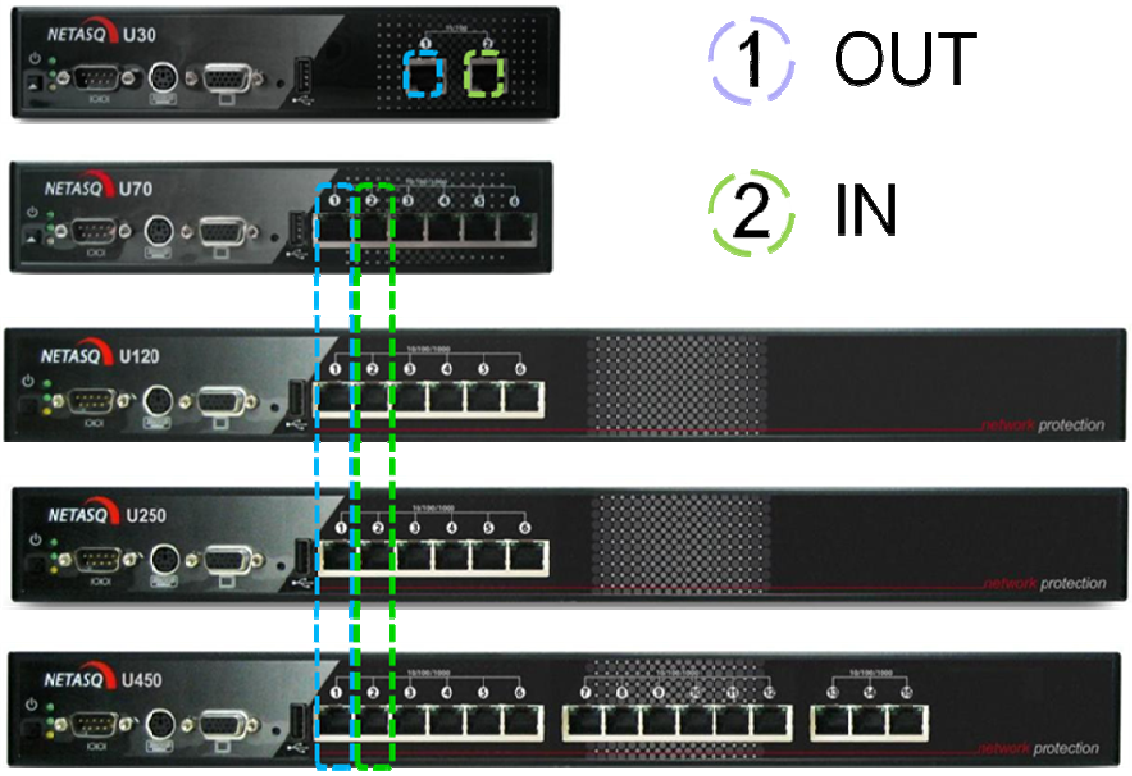
PORT IN – PORT 2



F1200

PORT IN – PORT 2

SERIA U



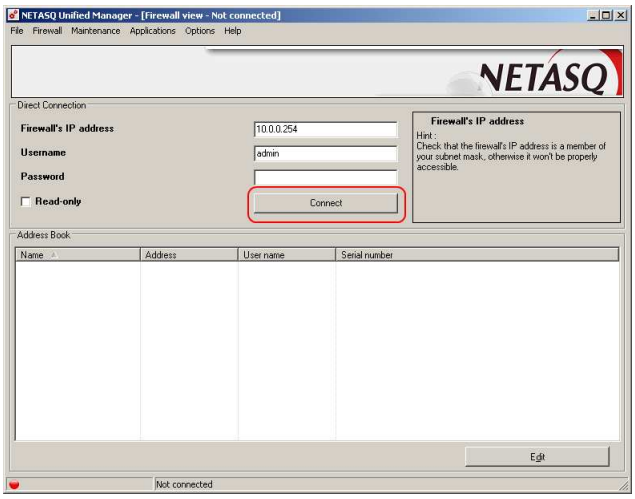
Uwaga

Jeżeli kabel Ethernet nie zostanie podłączony do prawidłowego portu to nie będzie możliwe podłączenie przez Unified Managera. Przełączanie się pomiędzy interfejsami urządzenia może uruchomić tzw. Antispoofing Mechanism, który uniemożliwi całkowicie podłączenie konsoli. Należy wtedy uruchomić ponownie urządzenie lub przywrócić do ustawień fabrycznych. Do ponownego uruchomienia urządzenia z poziomu CLI (połączenie przez port serial) można użyć polecenia „*Reboot*".

Uwaga

Poniżej opisano podłączenie przez dedykowaną aplikację. W przypadku, gdy urządzenie jest w ustawieniach fabrycznych to możliwe jest dokonanie wstępnej konfiguracji przy użyciu kreatora. Jest on dostępny pod adresem https://10.0.0.254.

Po uruchomieniu Unified Managera pojawi się ekran:



W konfiguracji domyślnej NETASQ ma adres IP: 10.0.0.254 (*Firewall's IP address*). Użytkownik (*Username*) to **admin**. Pole hasło (*Password*) jest puste. Po kliknięciu przycisku **CONNECT** nastąpi połączenie do urządzenia. Z racji, iż urządzenie jest w trybie domyślnych ustawień (*default settings*) hasło dla użytkownika **admin** nie jest ustawione. Przy pierwszym podłączeniu ukaże się komunikat mówiący o nadaniu hasła.

Uwaga

Kilka uwag dotyczących hasła dla użytkownika **admin**:

- Hasło musi składać się co najmniej z 8 znaków.
- Hasło powinno zawierać duże i małe litery oraz przynajmniej jeden znak specjalny.
- Przejęcie tego hasła przez osoby trzecie może powodować poważne zagrożenie dla bezpieczeństwa danych w chronionej sieci.

Jeżeli hasło zostanie dwukrotnie poprawnie wprowadzone, zostanie wyświetlony komunikat o inicjalizacji hasła oraz wykonywaniu potrzebnych procedur. W zależności od modelu, może to potrwać do kilku minut.

Następnie pojawi się informacja o numerze seryjnym urządzenia, do którego się podłączamy. Należy zweryfikować poprawność numeru seryjnego w wyświetlonym oknie z tym, który jest na urządzeniu. Jeśli zgadza się wystarczy potwierdzić.

Uwaga

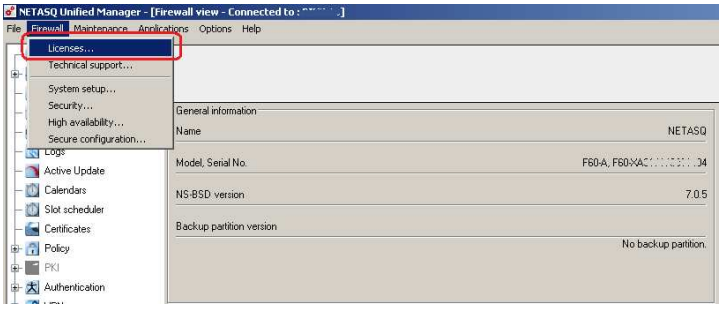
Jeżeli pojawi się komunikat błędu o treści:

Oznacza to że okres decyzji o potwierdzeniu numeru seryjnego urządzenia będzie trwał za długo (*timeout*). Należy wtedy ponownie podłączyć się do urządzenia z domyślnymi wartościami. Komunikat może też się pojawiać, gdy ktoś wcześniej nadał hasło dla użytkownika **admin**.

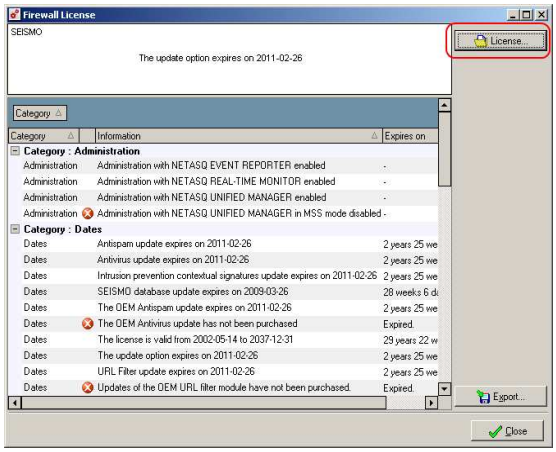
Wskazówka

W celu ułatwienia zarządzania można, w aplikacji NETASQ Unified Manager, uzupełnić tzw. Książkę adresową (*Address book*). W książce adresowej znajdować się będą wszystkie informacje potrzebne do autoryzacji na wybranym firewallu (login, hasło, adres IP, opis). Numer seryjny urządzenia zostanie uzupełniony automatycznie podczas pierwszego podłączenia. Należy pamiętać by plik książki adresowej przechowywać jedynie w formie zaszyfrowanej. Konfiguracja książki adresowej jest dostępna w górnym menu NETASQ Unified Managera: **FILE->ADDRESS BOOK...**

Pomyślne podłączenie do konsoli ukazuje główny ekran NETASQ Unified Managera. W pierwszym etapie należy wgrać licencję pobraną ze strony netasq.com. W górnym menu konsoli należy wybrać (**Firewall-> Licenses...**):



Po wybraniu wskazanej pozycji otworzy się okno dotyczące szczegółów licencji. W prawym górnym rogu ekranu widoczny będzie przycisk pozwalający na wskazanie pliku licencji.



Jeśli licencja zostanie prawidłowo wczytana nastąpi restart urządzenia. Po restarcie należy zweryfikować poprawność dat ważności.

Uwaga

W przypadku niezgodności danych z zamawianym przez Państwa serwisem prosimy o wysłanie maila na adres pomoc@dagma.pl z tematem: „Nieprawidłowa licencja" oraz z załączeniem pliku *Technical Support*. Po przegenerowaniu licencji należy pobrać ze strony nową licencję i ponownie zaimportować do urządzenia.

Uwaga

W domyślnej konfiguracji urządzenia NETASQ:

- mają włączony serwer DHCP,
- są w trybie BLOCK ALL – blokują wszystkie połączenia (z wyjątkiem np. połączenia administracyjnego tcp,1300).

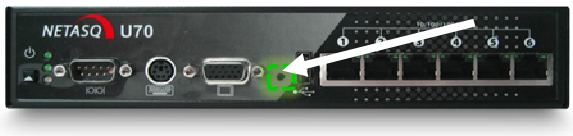
Uwaga

Restart do ustawień fabrycznych nie usuwa aktualizowanego firmware oraz nie usuwa wgranej licencji. Przywracana jest jedynie domyślna konfiguracja.

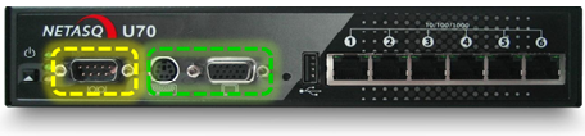
W przypadku urządzeń U30, U70, U120, U250, U450 wprowadzono zupełnie nową obudowę urządzeń. Poniżej zaprezentowano odpowiednie oznaczenia.

Diody przy interfejsach odpowiednio oznaczają:
zapalona jedna, lewa dioda – 10 Mbps;
zapalone obie diody – 10/100 Mbps;
zapalona jedna, prawa dioda – 10/100/1000 Mbps;
migające diody oznaczają transfer na interfejsie;

Przycisk przywrócenia ustawień fabrycznych:



Dostęp do Command Line Interface (CLI):



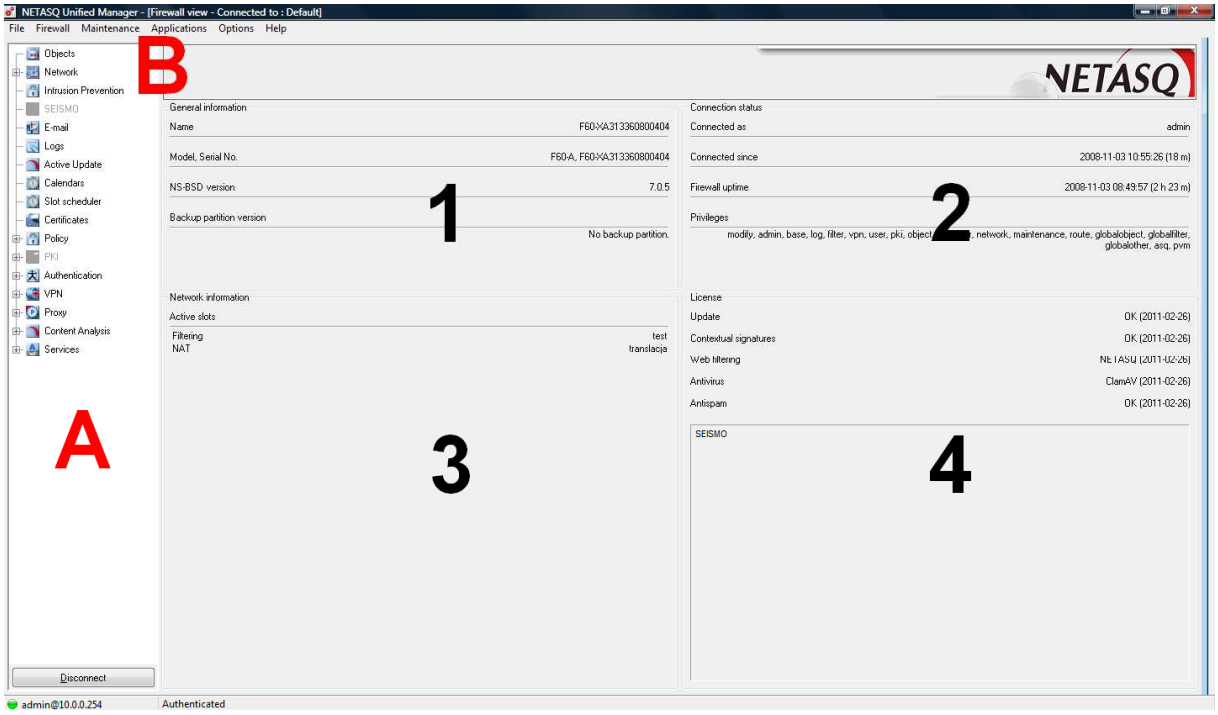
Sygnalizacja diodowa z lewej strony urządzeń oznacza odpowiednio od góry:

Dioda STANU (online)
Dioda STATUSU (status)
Dioda ZASILANIA (power)

Przycisk wyłącznika (rysunek poniżej), zadziała po przytrzymaniu go przez okres 4 sekund, do momentu gdy dioda STANU zgaśnie:

Konsola NETASQ Unified Manager

Po uruchomieniu aplikacji do zarządzania NETASQ Unified Manager, pojawi się główne okno. Można określić cztery części informacyjne określone na rysunku poniżej jako 1,2,3,4. Części A i B stanowią dwa menu: lewe i górne. Odpowiednio opisane pod rysunkiem.



PANEL 1 – GENERAL INFORMATION

W panelu tym znajdują się informację na temat :

- Nazwy firwalla (*Name*),
- Numeru seryjnego i modelu urządzenia (*MODEL, Serial No.),*
- Wersji firmware (*NS-BSD version*),
- Wersji zapasowej partycji systemowej (*Backup partition version*). Dotyczy serii U i dla serii F od modelu F200.

PANEL 2 – CONNECTION STATUS

Panel ten opisuje informacje dotyczące bieżącego połączenia do konsoli:

- Nazwa użytkownika, który jest podłączony w obecnej sesji (*Connected as*),
- Czas trwania połączenia z urządzeniem (*Connected since*),
- Czas, który upłynął od uruchomienia urządzenia (*Firewall uptime*),
- Uprawnienia zalogowanego, bieżącego użytkownika (*Privileges*).

PANEL 3 – NETWORK INFORMATION

W panelu tym znajdują się informację na temat ustawień sieci, a dokładniej wyświetlane są aktywne polityki (sloty) dla konkretnych funkcji:

- Nazwa aktywnej polityki filtrowania pakietów(*Filtering*),
- Nazwa aktywnej polityki dla translacji adresów (*NAT*),
- Nazwa aktywnej polityki dla filtrowania URL (*URL Filtering*),
- Nazwa aktywnej polityki dla IPSec VPN.

Dodatkowo dla aktywnego trybu klastra HA widoczna jest informacja o statusie synchronizacji urządzeń w trybie ACTIVE/PASSIVE (jeśli skonfigurowany został tryb HA).

Brak informacji o poszczególnych aktywnych slotach oznacza, iż dana funkcja nie została włączona. Domyślnie aktywny jest jedynie zbiór ustawień dla firewalla (*Filtering*) o nazwie BLOCK ALL.

PANEL 4 – LICENSE

W tym panelu wyświetlana jest informacja dotycząca ważności licencji dla poszczególnych serwisów urządzenia NETASQ.

MENU A – KONFIGURACJI FUNKCJI URZĄDZENIA

W MENU A, zwanym w dalszej części – MENU LEWYM, znajdują się wszystkie opcje dotyczące konfiguracji funkcji urządzenia NETASQ (Firewall, IPS, VPN, Antywirus, Antyspam, DHCP etc.).

MENU B – KONFIGURACJI USTAWIEŃ URZĄDZENIA

W MENU B, zwanym w dalszej części – MENU GÓRNYM, znajdują się wszystkie opcje dotyczące bezpośrednio urządzenia NETASQ, np.:

- Nazwa urządzenia,
- Określenie strefy czasowej urządzenia,
- Konfiguracja dostępu przez SSH do urządzenia,
- Zmiana hasła dla użytkownika **ADMIN**,
- Wykonanie kopii zapasowej konfiguracji,
- Aktualizacja firmware.

5. Tryb pracy urządzenia

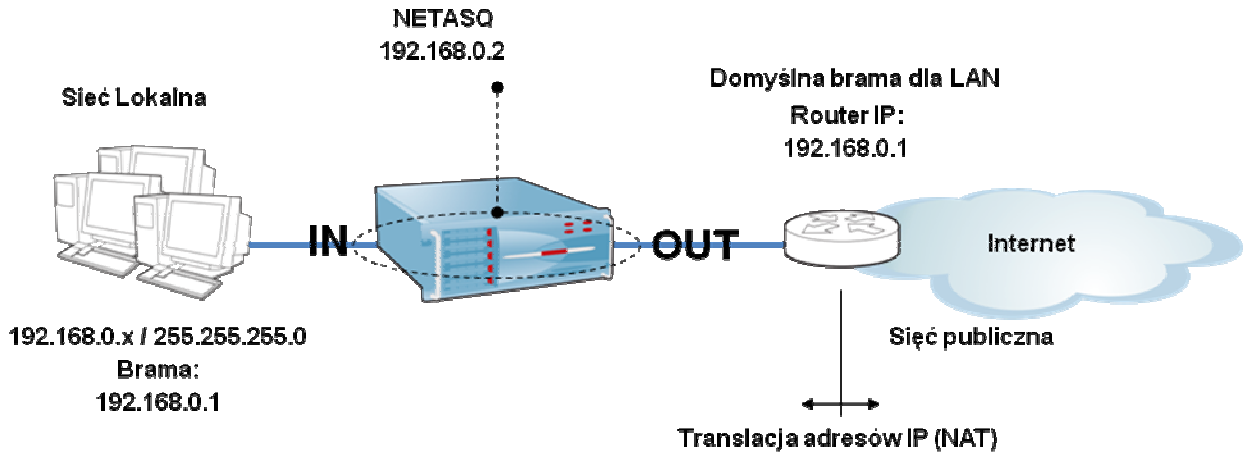
Tryb pracy urządzeń NETASQ zależy od roli, jakie ma spełniać urządzenie w sieci. Tryb pracy określa relację pomiędzy interfejsami. Konfiguracja trybu pracy urządzenia odbywa się w sekcji **NETWORK->INTERFACES.**

Urządzenia NETASQ mogą pracować w trzech trybach:

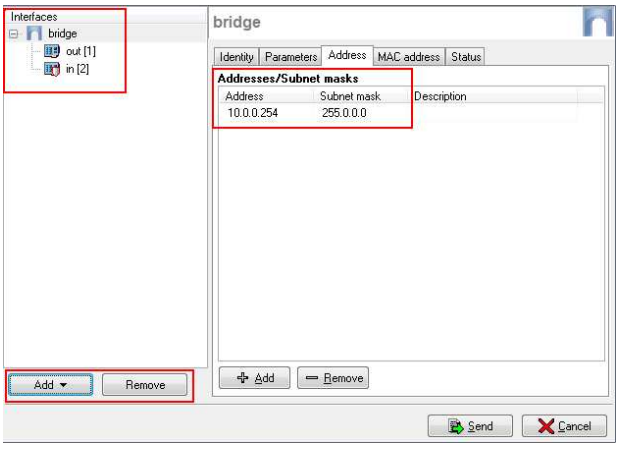
- BRIDGE (przeźroczysty),
- ADVANCED (zaawansowany, tryb routera),
- HYBRID (mieszany).

Tryb BRIDGE (transparent)

Urządzenie z ustawieniami domyślnymi określa, iż na każdym z interfejsów urządzenia NETASQ skonfigurowana jest ta sama sieć. Rysunek poniżej przedstawia przykład takiej topologii:



W przykładzie używane są tylko dwa interfejsy IN i OUT. W praktyce interfejsów może być więcej (włączając w to oczywiście interfejsy wirtualne VLAN (IEEE 802.1Q)). W przypadku konfiguracji NETASQ interfejsy będą skonfigurowane w następujący sposób:



Przycisk **ADD** pozwala na dodanie np. interfejsów VLAN lub dodanie kolejnego BRIDGE (oczywiście aby było to możliwe urządzenie musi posiadać co najmniej cztery interfejsy). Przycisk **REMOVE** pozwala na usunięcie **BRIDGEa** lub interfejsu **VLAN**. Po zaznaczeniu interfejsu **BRIDGE** możliwa jest zmiana adresu IP urządzenia w zakładce **ADDRESS.** Z punktu widzenia topologii sieci urządzenie transparentnie filtruje przechodzące pakiety bez modyfikacji adresów IP.

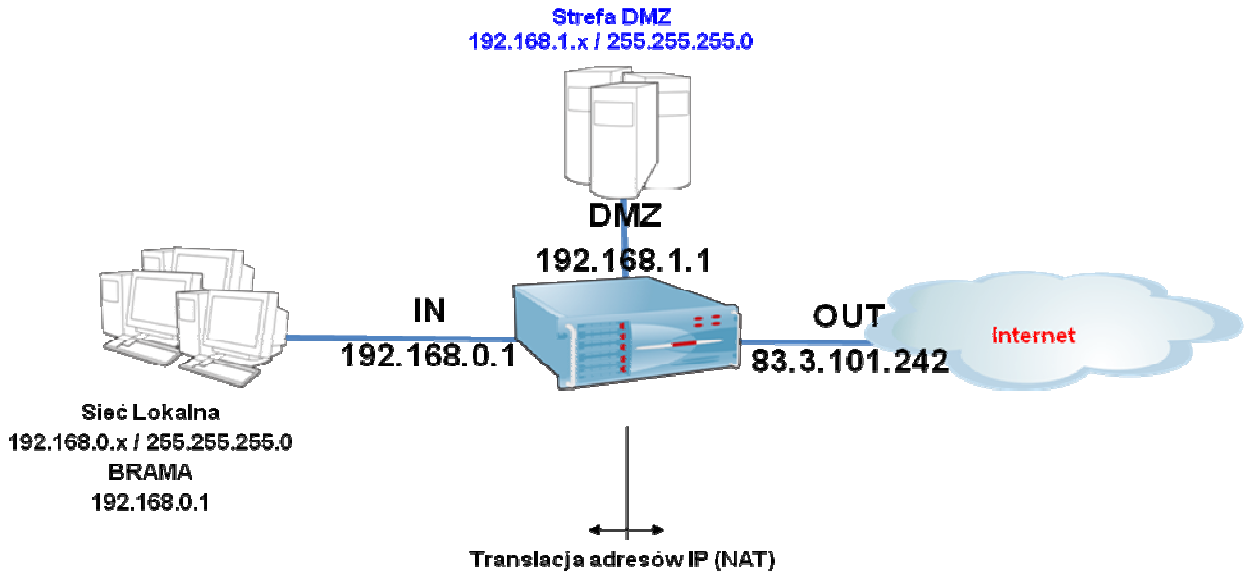
Wskazówka

Z poziomu CLI można wykorzystać polecenie *ifinfo* lub *ifinfo show_ports*. Dzięki jego zastosowaniu możemy podejrzeć konfiguracje interfejsów na urządzeniu. W drugim przypadku można także zweryfikować stan interfejsu (state up/down).

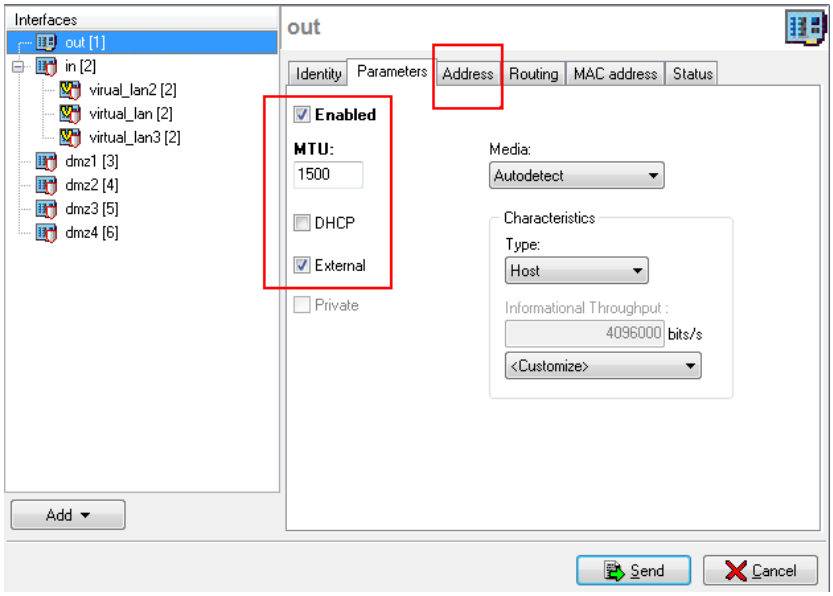
```
F25-XD765760601001>ifinfo show_ports
port       name NS-BSD   state  address
  1        out   fxp0      up  83.3.101.242/29
  2         in   fxp1      up  10.0.0.254/24, 192.168.200.254/24, 192.168.100.254/24

F25-XD765760601001>ifinfo
interface list:
ipsec (enc0)
in (protected,fxp1)
      10.0.0.254/255.255.255.0
      192.168.200.254/255.255.255.0
      192.168.100.254/255.255.255.0
out (fxp0)
      83.3.101.242/255.255.255.248
```

Tryb ADVANCED

Tryb ten jest najczęściej stosowany. NETASQ umiejscowiony jest w sieci jako główny router, tzw. Bramka na styku sieci firmowej i wyjścia do zewnętrznej sieci. NETASQ pełni funkcję urządzenia filtrującego ruch na styku sieci (np. LAN, DMZ, INTERNET). Do każdego z interfejsów przyłączona jest sieć, stanowiąca odrębny segment sieci. Pozwala to na pełne monitorowanie ruchu pomiędzy sieciami. NETASQ w tym trybie wykorzystywany jest do translacji adresów IP, tłumaczenie adresów komputerów lokalnych na adres publiczny, a także przekierowanie (*redirect*) przychodzących połączeń na adres publiczny do serwerów w DMZ.



Okno konfiguracji może wyglądać następująco:



Warto zwrócić uwagę, iż po usunięciu domyślnego **BRIDGE**a wszystkie interfejsy będą wyszarzane. Należy wtedy w sekcji **PARAMETERS** ustawić odpowiednie flagi:

ENABLED – włączenie/wyłączenie interfejsu.

EXTERNAL – należy zaznaczyć, jeśli jest to interfejs wyjściowy (ikona interfejsu bez tarczy). Odznaczenie opcji oznacza, iż jest to segment chroniony (*protected interface*).

DHCP – zaznaczamy, jeśli interfejs pobierze adres dynamicznie.

PRIVATE – po zaznaczeniu opcji stacje, serwery należące do podsieci interfejsu nie będą dostępne dla stacji należących do sieci zewnętrznych (*external interface*).

W przypadku, gdy flaga **DHCP** jest odznaczona, na zakładce **ADDRESS** należy określić adres IP interfejsu wraz z maską podsieci, w jakiej będzie używany.

Po wykonaniu zmian wybrać należy przycisk **SEND**. W przypadku zmian adresów domyślnych nastąpi rozłączenie konsoli. Należy wtedy ponownie się połączyć w ramach nowej adresacji.

Tryb HYBRID

Tryb ten zwany jest inaczej trybem mieszany. Część interfejsów pracuje w trybie BRIDGE a część znajduje się poza nim.

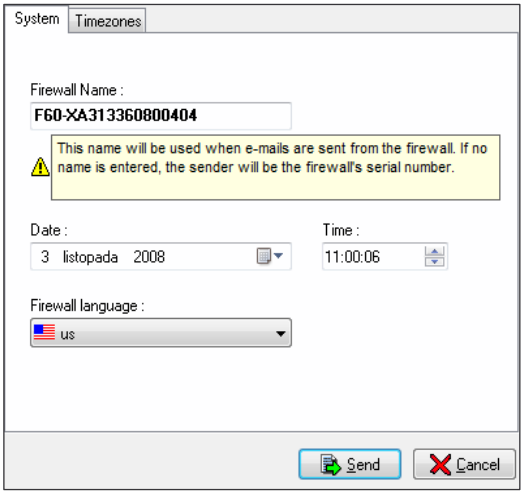
6. Podstawowa konfiguracja

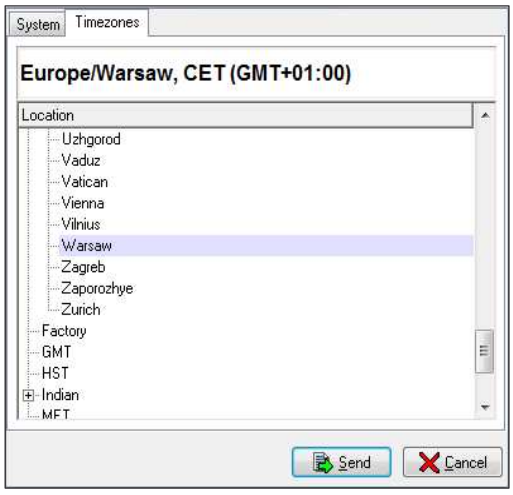
Przed dokonaniem podstawowej konfiguracji należy upewnić się, że licencja została poprawnie wgrana oraz okres ważności licencji jest zgodny z zamówieniem. Wstępną konfigurację można podzielić na etapy:

- Ustalenie nazwy urządzenia oraz określenie strefy czasowej,
- Konfiguracja hasła dla użytkownika **admin**,
- Konfiguracja obiektów,
- Ustawienie bramy domyślnej na urządzeniu (routing),
- Ustawienie serwerów DNS dla urządzenia,
- Konfiguracja usług DHCP, NTP,
- Konfiguracja zapory (firewall) – **patrz rozdział 8.**
- Konfiguracja translacji adresów (NAT) – **patrz rozdział 9.**

Strefa czasowa, nazwa urządzenia.

Ustawienia obu parametrów znajdują się w sekcji **Firewall->System Setup** w górnym menu NETASQ Unified Managera.



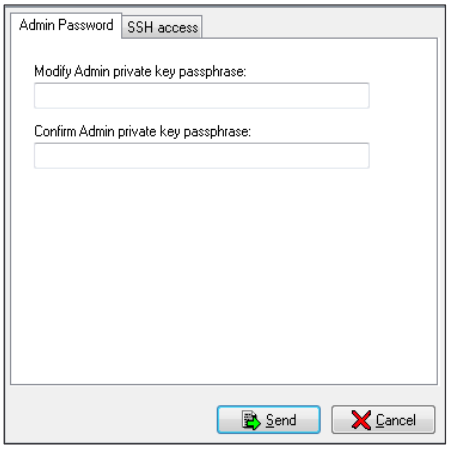


Po zmianie tych ustawień na prawidłowe należy wybrać przycisk **SEND** aby wysłać ustawienia na urządzenie. Zmiany wymagają ponownego uruchomienia urządzenia (jest to sygnalizowane odpowiednim komunikatem).

Konfiguracja hasła dla użytkownika admin

Podczas pierwszego podłączenia do urządzenia (lub w trakcie pracy kreatora www) ustalono hasło dla użytkownika **ADMIN.** Hasło to można zmienić wybierając opcje z w górnym menu NETASQ Unified Managera **Firewall->Security**.

Poniżej zaprezentowano okno programu, w którym można dokonać zmiany hasła:



Po dwukrotnym wprowadzeniu hasła należy zatwierdzić zmianę przyciskiem **SEND.**

Konfiguracja obiektów

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

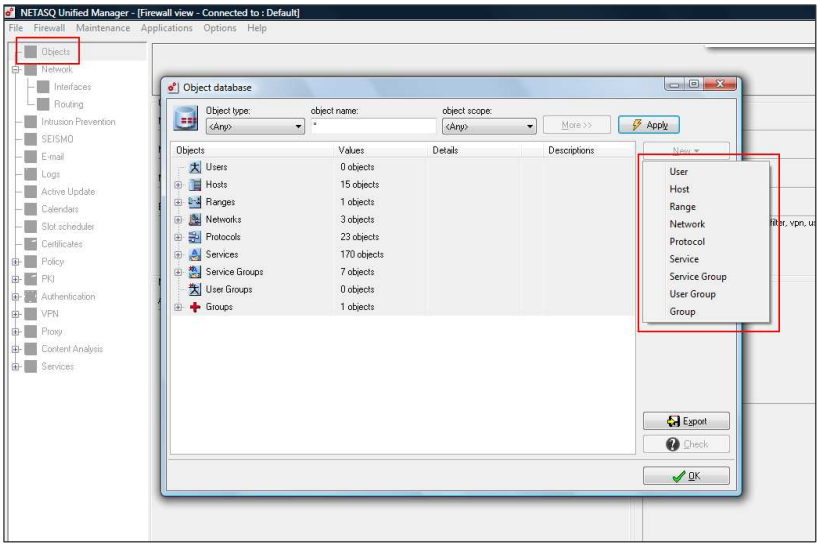
Wyróżnić można kilka typów obiektów:

- USER,
- HOST,
- RANGE,
- NETWORK,
- PROTOCOL,
- SERVICE.

Obiekty odpowiedniego typu można grupować:

- **SERVICE GROUP** – grupa obiektów typu **SERVICE,**
- **USER GROUP** – grupa obiektów typu **USER,**
- **GROUP** – grupa obiektów, w skład której mogą wchodzić obiekty typu **HOST**, **RANGE**, **NETWORK**.

Aby utworzyć obiekt należy kliknąć na **OBJECT** w lewym menu Unified Managera:



W oknie **OBJECTS** po prawej stronie jest przycisk **NEW** umożliwiający tworzenie przedstawicieli konkretnego typu obiektów. I tak:

OBIEKT TYPU USER

Reprezentuje użytkownika. Aby móc tworzyć obiekty tego typu wymagane jest posiadanie bazy użytkowników. Baza użytkowników może być:

- Skonfigurowana na urządzeniu NETASQ (**internal LDAP**),
- Na zewnętrznym serwerze LDAP (**external LDAP**),
- Synchronizowana z Microsoft Active Directory.

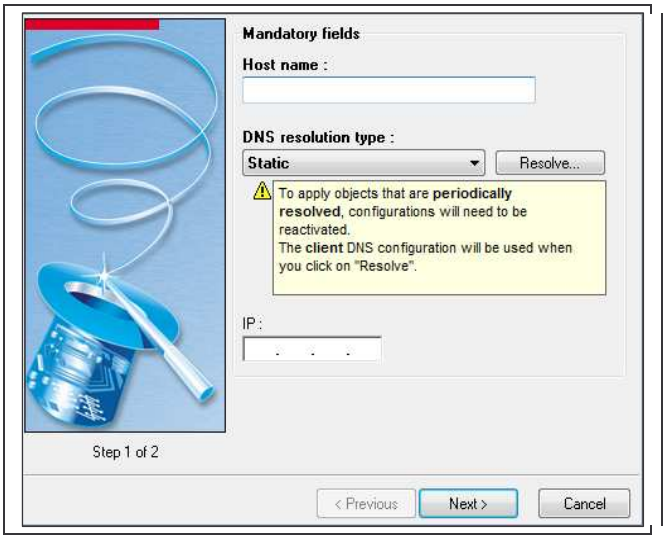
Konfiguracja bazy LDAP znajduje się w lewym menu w sekcji **AUTHENTICATION->LDAP DATABASE.** Dostępny jest specjalny kreator, który krok po kroku prowadzi przez konfigurację tej usługi.

OBIEKT TYPU HOST

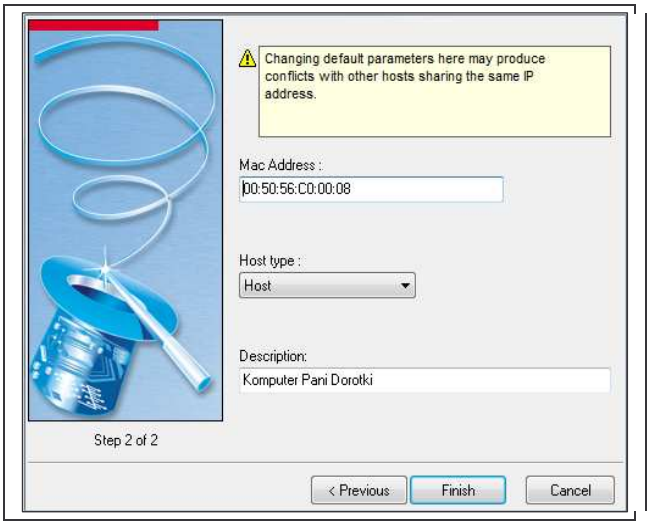
Obiekt ten reprezentuje powiązanie nazwy z adresem IP. Czyli relacja 1-1. Na początek zaleca się dodanie dwóch obiektów tego typu:

1. Domyślna brama;
2. Serwer DNS.

W docelowej konfiguracji, do obiektów najlepiej dodać wszystkie obiekty symbolizujące pojedynczy adres IP. Z pewnych względów wygodniej jest zastosować obiekt typu **RANGE** lub **NETWORK.**
W przypadku tworzenia obiektu typu host uruchomiony jest kreator, który składa się z dwóch okien. Okno pierwsze wygląda następująco:



Gdyby dla przykładu należało stworzyć obiekt reprezentujący bramę w polu **HOST NAME** można wpisać *„BRAMA”*. **DNS RESOLUTION TYPE** należy pozostawić na opcji **STATIC.** W sekcji **IP** należy wpisać adres IP reprezentujący w sieci bramę (np. adres bramy otrzymanej od dostawcy usług internetowych - ISP). Po wypełnieniu danych klikamy przycisk **NEXT.** W drugim etapie wszystkie pola są opcjonalne.



Opcjonalny parametr **MAC ADDRESS** pozwala na określenie adresu MAC. Może to być przydatne w przypadku używaniu na NETASQ usługi DHCP (dynamiczne przydzielanie adresów IP). W takim przypadku komputer z kartą sieciową o danym adresie MAC dostanie dynamicznie określony na poprzedniej zakładce adres IP. **HOST TYPE** jest właściwością obiektu wykorzystywaną do wyszukiwania elementów w głównym oknie obiektów. **DESCRIPTION** stanowi opis elementu.

OBIEKT TYPU RANGE

Obiekt typu **RANGE** stanowi zakres adresów IP od konkretnego adresu IP do konkretnego adres IP. Tego typu obiektu wymaga się przy konfiguracji serwera DHCP, w ramach konfigurowanego zakresu komputery w sieci lokalnej otrzymują dynamicznie adres IP.

OBIEKT TYPU NETWORK

Obiekt ten symbolizuje sieć. Przy konfiguracji podaje się adres sieci z odpowiednią maską.

OBIEKT TYPU PROTOCOL

Obiekt ten symbolizuje powiązanie nazwy z numerem protokołu IP.

OBIEKT TYPU SERVICE

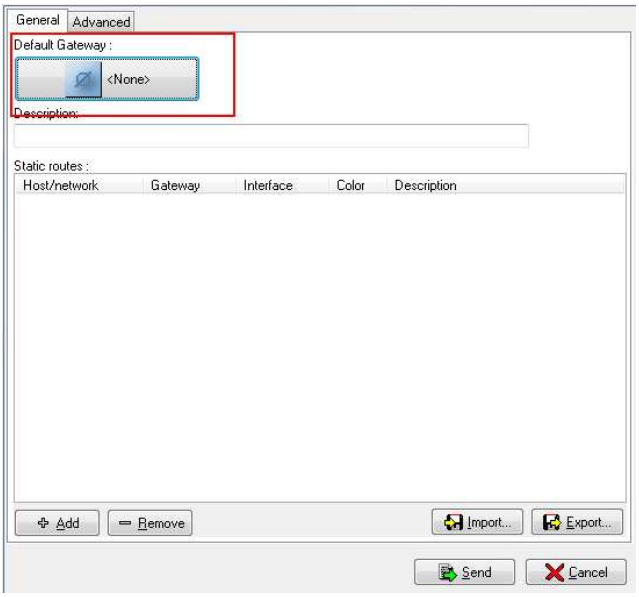
Obiekt symbolizuje powiązanie nazwy własnej z numerem portu tcp lub udp. Większość znanych usług (eng. service) jest domyślnie dodana. W trakcie pracy kreatora dodawania obiektu tego typu, można także dodać zakres portów.

Uwaga

Przy każdym z obiektów, niezależnie od typu, może istnieć jedna z dwóch ikon (patrz rysunek poniżej). Ikona ze znakiem zakazu oznacza, iż nie można jej usunąć i że obiekt został automatycznie stworzony na bazie konfiguracji innych elementów. Przykładem mogę być obiekty typu **NETWORK** i **HOST**, których nazwa zaczyna się od *„Firewall_”.* Symbolizują one adresy i sieci dołączone do interfejsów NETASQ. Tworzone są automatycznie po konfiguracji adresów IP na interfejsach.

Ustawienie DOMYŚLNEJ BRAMY (Default Gateway)

Domyślna brama jest podstawowym elementem konfiguracji routera. Aby ustawić domyślną bramę należy najpierw upewnić się, iż odpowiedni obiekt (typu **HOST**) został dodany do zbioru obiektów. Następnie w sekcji **NETWORK->ROUTING**, zakładka **GENERAL** określamy domyślną bramę przez wybranie pola zaznaczonego na rysunku poniżej:

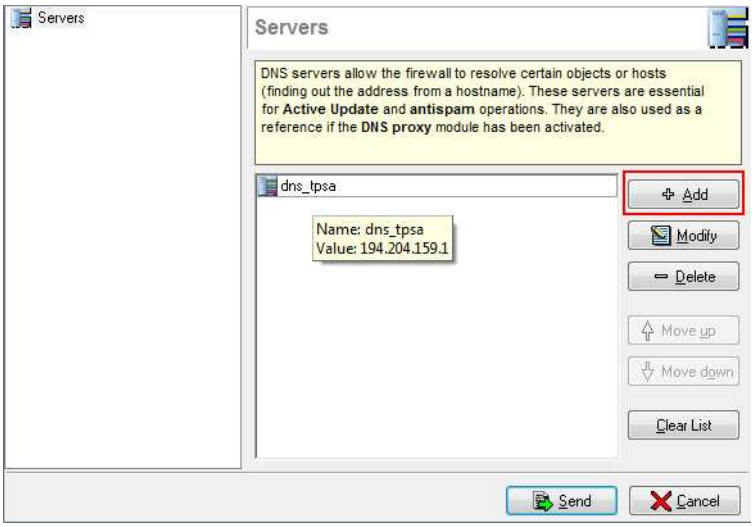


W sekcji **NETWORK->ROUTING** można także ustawić trasy statyczne (routing statyczny). W zakładce **GENERAL** w sekcji **STATIC ROUTES** można dodać wpis określający dostępność danej sieci przez wybrany router (*gateway*), przez konkretny interfejs.

W zakładce **ADVANCED** można ustawić, w przypadku posiadania dwóch dostawców Internetu, trasę GŁOWNĄ (**main gateway**) i trasę ZAPASOWĄ (**backup gateway**). Dodatkowo w przypadku ustawienia obu ISP jako **MAIN GATEWAY** można ustawić tzw. **LOAD BALANCING**, czyli równoważenie obciążenia łącza.

Ustawienie serwerów DNS

Serwery DNS ustawiamy w sekcji **SERVICES->DNS**. Podobnie jak w przypadku domyślnej bramy wcześniej należy posiadać obiekt symbolizujący DNS.



Serwery ustawione w tym miejscu stanowią wskazania na DNS dla samego urządzenia NETASQ.

Wskazówka

Obiekty można modyfikować z poziomu CLI edytując plik:

/usr/Firewall/ConfigFiles/objects

Plik można edytować z wykorzystaniem edytora **Joe** polecenie:

F60-XA313360800404>joe /usr/Firewall/ConfigFiles/objects

Po edycji pliku do zapisania zmian służy polecenia: **CTRL + K + X**

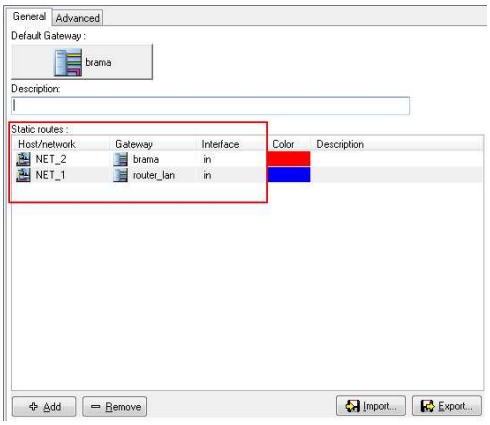
7. Ustawienia trasowania połączeń (routing)

Trasowanie połączeń, czyli określenie zasad dotyczących kierowania tras dla połączeń można skonfigurować na NETASQ na kilka sposobów. Kolejność analizy poszczególnych typów jest następująca:

- Routing statyczny,
- Policy Routing[2],
- Routing by interface,
- Load Balancing by source,
- Load Balancing by destination,
- Brama domyślna (default gateway).

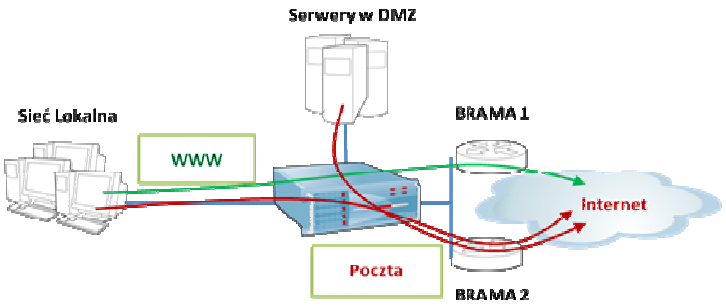
Routing statyczny

Pozwala na określenie tras statycznych do sieci, które nie są podłączone bezpośrednio do interfejsów urządzenia. Trasy statyczne można określić w NETASQ Unified Managerze przez lewym MENU **NETWORK -> ROUTING** sekcja *Static Routes.*



Policy Routing

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



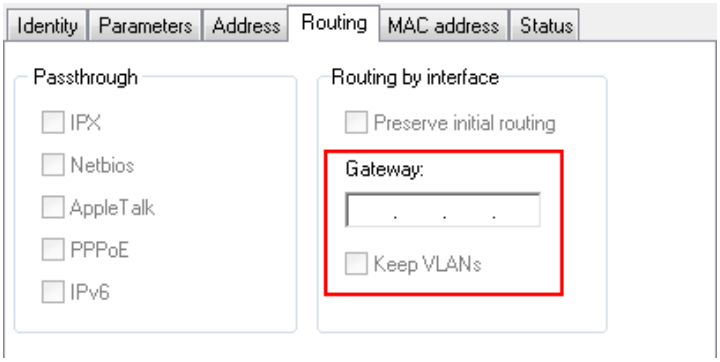
Na ilustracji zaprezentowano sytuacje w której ruch http kierowany jest przez bramę ISP 1, natomiast ruch związany z pocztą (smtp, pop3) kierowany jest na drugiego usługodawcę ISP.

[2] dostępny od wersji 8 firmware

Skierować ruch na odpowiednie łącze można ustawiając w kolumnie **Routing** bramę danego ISP przy odpowiedniej regule na firewallu.

Routing by interface

Ten typ trasowania połączeń pozwala na kierowanie całego ruchu przychodzącego na dany interfejs. Konfiguracja odbywa się w opcjach konkretnego interfejsu w NETASQ Unified Managerze w sekcji **NETWORK->INTERFACES**:



Load Balancing by Source/Destination

Równoważenie obciążenia łączy można określić w zależności czy równoważone są według adresów docelowych (DESTINATION) lub źródłowych (SOURCE). W NETASQ Unified Managerze wybieramy jedynie bramy kolejnych ISP jako **MAIN GATEWAY**. 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

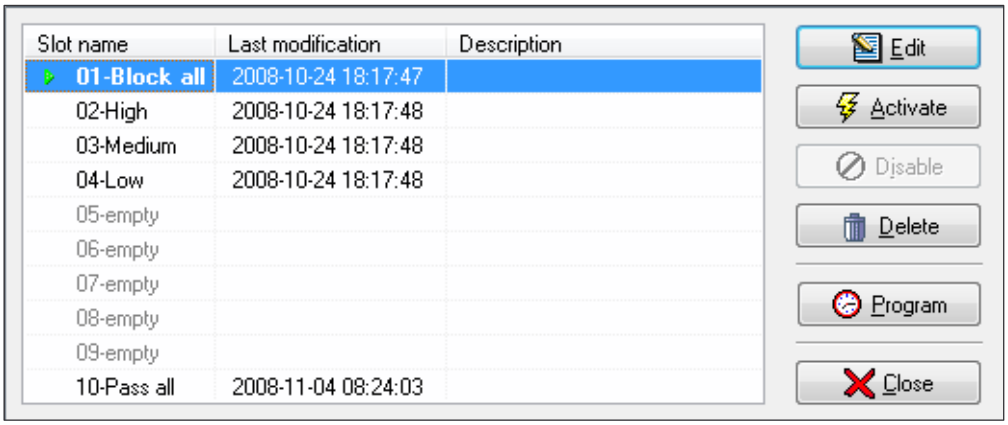
Domyślna brama (eng. Default gateway) to określenie routera na który pakiety będą kierowane w przypadku, gdy żadna z powyższych metod nie zostanie wykorzystana. Dodatkowo brama domyślna stanowi bramę dla samego urządzenia NETASQ.

Wskazówka

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

8. Konfiguracja zapory (firewall)

Konfiguracja zapory na NETASQ znajduje się w sekcji **POLICY->FILTERING** w NETASQ Unified Manager. Po wybraniu tej opcji ukaże się okno tzw. **SLOT**ów. Slot to zestaw reguł. W danej chwili aktywny może być jeden slot i oznaczony jest on zieloną strzałką. Do dyspozycji administratora jest 10 slotów. Domyślnie włączony jest slot nr. 01 o nazwie **BLOCK ALL**. Rysunek poniżej prezentuje główne okno zestawu reguł z aktywnym domyślnym slotem.



W ramach ustawień filteringu określa się sposób działania zapory, przypisać można dla połączeń odpowiedni profil ustawień IPS oraz kształtowania pasma. Dlatego też, dzięki funkcji kalendarza (*Program*) można definiować w jaki dzień tygodnia i o jakiej godzinie zostanie uruchomiony odpowiedni slot. Po zaznaczeniu danego zestawu można wybrać jedna z poniższych akcji:

EDIT – pozwala na edycję zestawu, czyli docelowe tworzenie reguł.

ACTIVATE – aktywacja zaznaczonego zestawu.

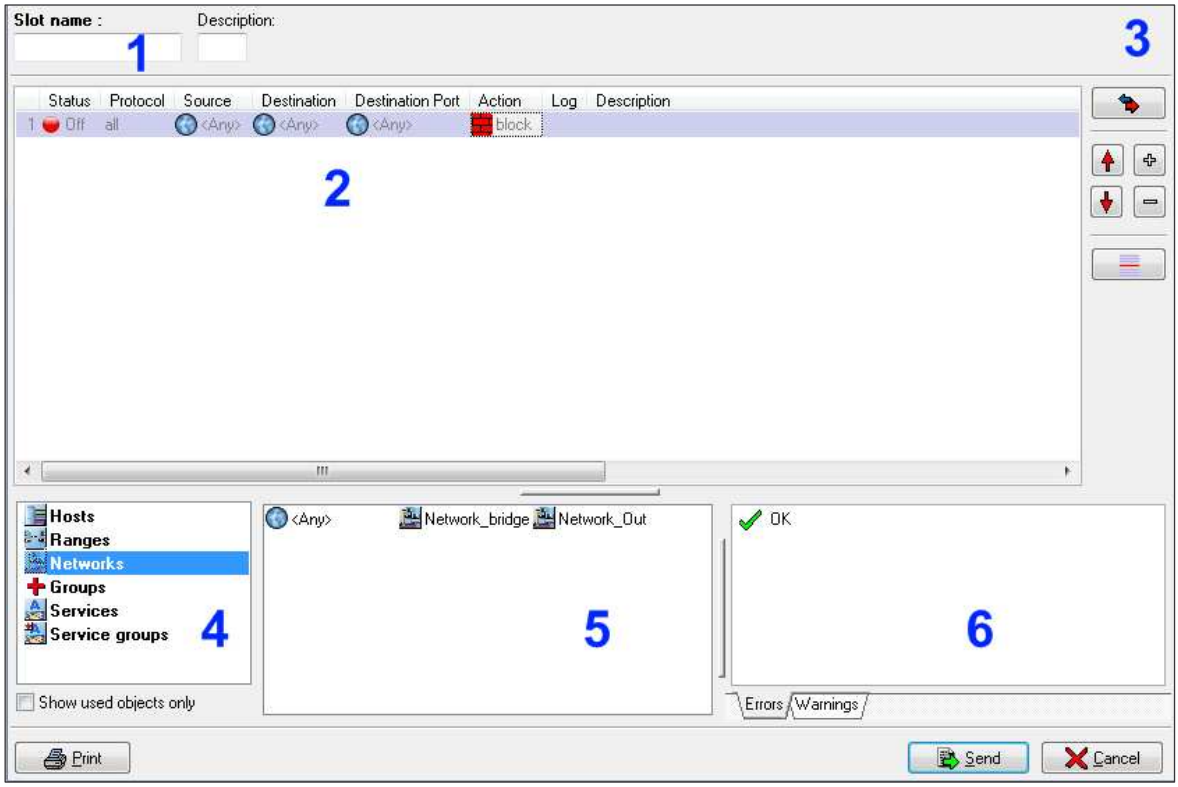
DISABLE – powoduje dezaktywację zaznaczonego zestawu. W praktyce oznacza to blokowanie wszystkich połączeń (z wykluczeniem Policy -> Implicit Rules).

DELETE – usuwa zaznaczony slot.

PROGRAM – pozwala na ustawienie kalendarza (tygodniowego) automatycznej aktywacji zestawu reguł (slot).

CLOSE - zamyka okno.

Po wybraniu edycji wybranego Slotu (lub stworzeniu nowego) pojawi się okno:



SEKCJA 1

W polu **SLOT NAME** określamy nazwę zestawu – pole jest wymagane.

SEKCJA 2

To lista reguła na firewallu. Domyślnie występuje jedna reguła. Poszczególne kolumny:

STATUS – On/Off (zielone/czerwone) pozwala na określenie czy w ramach aktywnego zestawu dana reguła będzie włączona czy wyłączona.

PROTOCOL – określa protokół, dla którego jest dana reguła (all – wszystkie).

SOURCE – to źródło pakietu. Może to być pojedynczy komputer (**HOST**), zakres adresów (**RANGE**), sieć (**NETWORK**), grupa adresów IP (**GROUP**) lub użytkownik (**USER**).

DESTINATION – to docelowy komputer, sieć, zakres lub grupa adresów.

DESTINATION PORT – to usługa (service), z którego będą chciały skorzystać obiekty określone w **SOURCE** łącząc się do obiektu określonego w **DESTINATION**. Inaczej mówiąc jest to port docelowy połączenia.

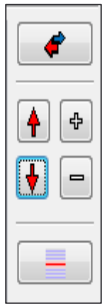
ACTION – akcja, jaka zostanie wykonana (PASS/BLOCK) po dopasowaniu danego pakietu.

LOG – (LOG/MINOR/MAJOR) – czy wystąpienia konkretnego pakietu, określonego przez powyższe parametry i akcję ma być logowane (LOG), czy ma być traktowane jako alarm (poziom MINOR lub MAJOR).

DESCRIPTION – opis reguły.

SEKCJA 3

W sekcji tej znajdują się przyciski pozwalające na:



Dwie strzałki skierowane w przeciwne strony pozwalają na wyświetlenie zaawansowanych ustawień (dodatkowe kolumny). Chodzi tu o ustawienie IPS (ASQ) dla danych połączeń lub np. kształtowanie pasma (QoS).

Przyciski PLUS/MINUS pozwalają na dodawanie lub usuwanie reguł.

Strzałki GÓRA/DOŁ pozwalają na odpowiednie przesunięcie reguły.

Ostatni przycisk pozwala na dodanie tzw. separatora. Może on służyć do oddzielenia reguł, co poprawia czytelność.

Poniżej przykład listy reguł rozdzielonych separatorami:

SEKCJA 4 i 5

W sekcji 4 można zaznaczyć typ obiektów, a następnie zobaczyć ich reprezentantów w sekcji 5. Dzięki temu można przeciągnąć odpowiedni obiekt do konkretnej kolumny reguły na firewallu. Wyjątek stanowi typ obiektów **USER**. Jeśli chcemy wybrać w regule obiekt tego typu należy dwukrotnie kliknąć na wybraną kolumnę (np. SOURCE) i wybrać odpowiedniego użytkownika z listy.

SEKCJA 6

W oknie tym wyświetlany jest komunikat w przypadku nie spójności logicznej reguł. Status **OK**, oznacza że reguły w zestawie zostały prawidłowo skonfigurowane i nie wykluczają się.

Zakończenie konfiguracji reguł na firewallu odbywa się przez kliknięcie na przycisk **SEND** (wysyła reguły na urządzenie), a następnie aktywowanie zestawu (SLOTu) tak by pojawiła się zielona strzałka.

Wskazówka

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

/usr/Firewall/ConfigFiles/Filter/XX

Gdzie XX to numer slotu (zestawu).

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

*F60-X0000000000>**enfilter XX***

Gdzie analogicznie XX to numer slotu (zestawu). Natomiast polecenie:

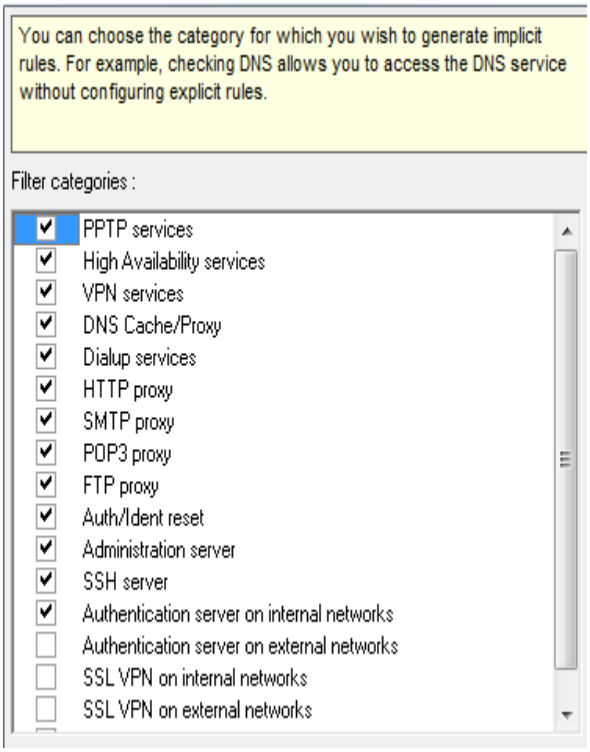
*F60-X0000000000>**enfilter off***

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

/usr/Firewall/ConfigFiles/Filter/slotinfo

Reguły Domyślne - Implicit Rules

W sekcji **POLICY -> IMPLICIT RULES** widoczne są reguły domyślne ustawione na zaporze. To wyjaśnia, dlaczego w przypadku aktywnego domyślnego zestawu **BLOCK ALL** można zalogować się do konsoli Administration Suite. Poniżej przedstawiono widok na reguły domyślne z NETASQ Unified Manager jak i NETASQ Real-Time Monitor (omówionego w dalszej części). W tym przypadku aktywowany był zestaw o nazwie **Pass All**.



Wskazówka

Wyświetlenie aktywnych reguł filteringu (firewall, IPS) z CLI to:

F60-XA313360800404>**sfctl -s filter**

Wyświetlenie aktywnych reguł NAT z CLI to:

F60-XA313360800404>**ipnat –l**

9. Konfiguracji translacji adresów (NAT)

Translacja używana jest do tłumaczenia adresów prywatnych na publiczne lub w odwrotną stronę, jeśli ruch przychodzący na adres publiczny trzeba przetłumaczyć na adres prywatny serwera w DMZ. Można wyróżnić dwa podstawowe typy translacji:

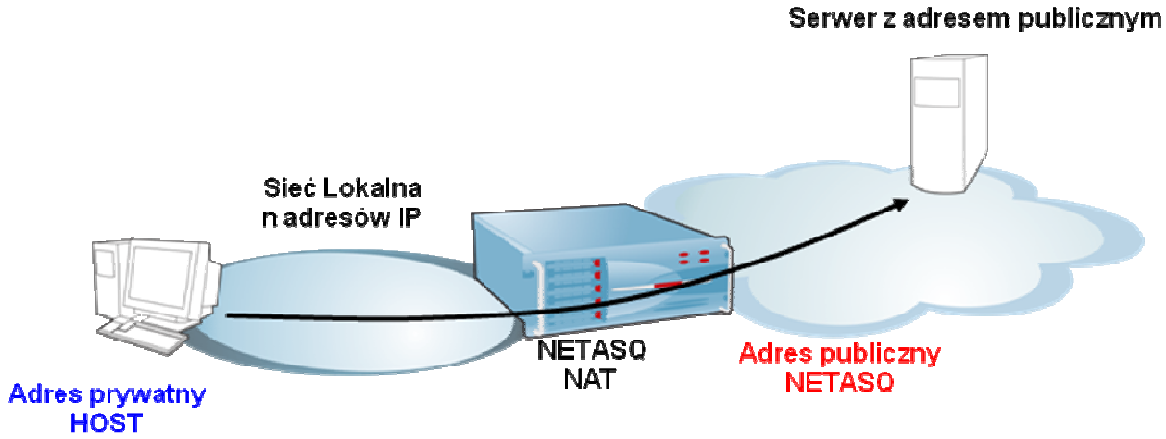
- SOURCE NAT **(map)**
- DESTINATION NAT **(redirect)**

Istnieje jeszcze kilka innych typów translacji dostępnych w konfiguracji NETASQ. Dokładny opis znajduje się w bazie wiedzy na stronie www.netasq.com w strefie dla klientów (Client AREA):

http://en.knowledgebase.netasq.com/index.php/NAT

SOURCE NAT – MAP ACTION

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.



Konfiguracji NAT można dokonać w NETASQ Unified Manager w **POLICY->NAT.** Analogicznie jak w przypadku firewalla mamy dostępne zestawy reguł (*slots*). Reguła dla MAP może wyglądać następująco:

Ustawienie dla akcji **MAP**:

STATUS – reguła włączona/wyłączona (ON/OFF);

ACTION – określa typ translacji, w tym wypadku **MAP**;

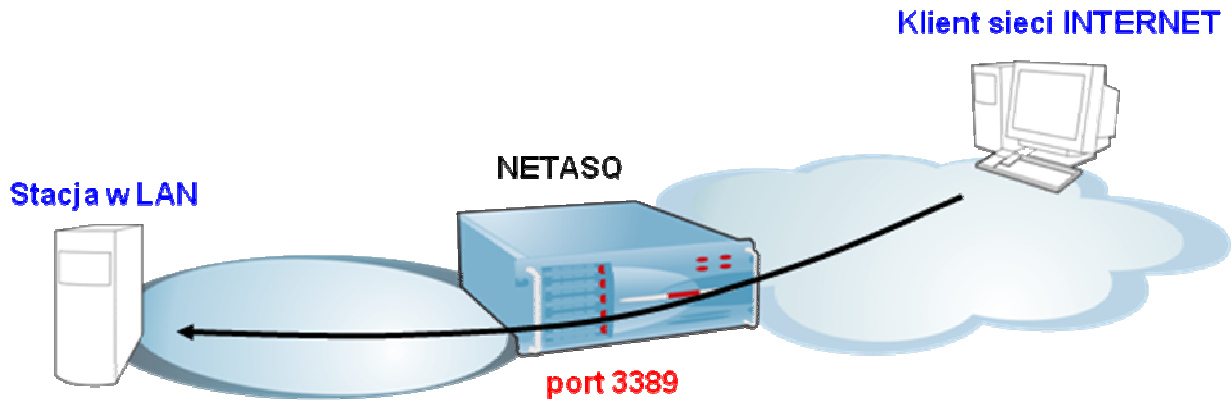
ORGINAL SOURCE – adres źródłowy poddawany translacji (MAP=SOURCE NAT);

DESTINATION – określa docelowe adres lub adresy IP, dla których odbywać się będzie translacja adresów IP. W przypadku ogólnym należy wybrać **ANY** co oznacza dowolny adres IP.
DESTINATION PORT – określa docelowy port (usługę), dla której będzie odbywać się translacja adresów.
TRANSLATED – określa adres który zostanie podmieniony w miejsce **ORIGINAL SOURCE**.

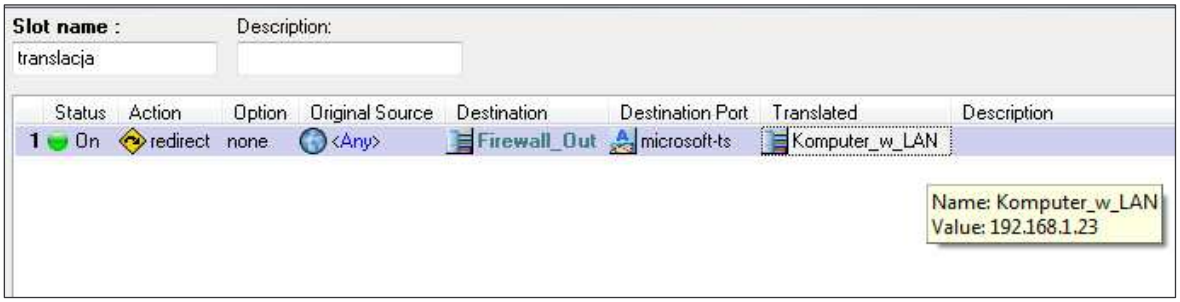
Podsumowując, akcja MAP tłumaczy obiekt **ORGINAL SOURCE** na obiekt **TRANSLATED**. W podanym przykładzie sieć reprezentowana obiektem *NETWORK_BRIDGE (10.0.0.0/24)* przy połączeniach wychodzących będzie tłumaczona na jeden adres IP reprezentowany przez obiekt *FIREWALL_OUT* (publiczny adres IP skonfigurowany na zewnętrznym interfejsie urządzenia o nazwie OUT).

DESTINATION NAT – REDIRECT ACTION

Translacja 1 do 1 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.



Ustawienie dla akcji **REDIRECT**:

STATUS – reguła włączona/wyłączona (ON/OFF);

ACTION – określa typ translacji, w tym wypadku **REDIRECT**;

ORGINAL SOURCE – to dowolna stacja, dowolny adres IP klienta, sieć INTERNET, czyli obiekt o nazwie **ANY**;

DESTINATION – określa adres IP, na który przychodzi połączenie. W tym przypadku będzie to publiczny adres NETASQ skonfigurowany na zewnętrznym interfejsie.

DESTINATION PORT – określa na jaki port przychodzi połączenie, które ma być przetłumaczone (przekierowane). Dla podanego przykładu będzie to port 3389 reprezentowany przez obiekt *microsoft-ts*;

TRANSLATED – w tej kolumnie należy określić obiekt reprezentujący docelowy komputer, dla którego odbywa się translacja. Jak nazwa wskazuje REDIRECT = DESTINATION NAT. Czyli obiekt w kolumnie **DESTINATION** jest przekierowany na obiekt w kolumnie **TRANSLATED.**

W obu przypadkach po zapisaniu reguł należy aktywować slot.

Wskazówka

W systemie operacyjnym NS-BSD reguły translacji przechowywane są odpowiednio w:
/usr/Firewall/ConfigFiles/NAT/XX
Gdzie XX to numer slotu (zestawu).
W przypadku konfiguracji przy użyciu CLI, można aktywować poszczególny zestaw komendą:
F60-X0000000000>**ennat XX**
Gdzie analogicznie XX to numer slotu (zestawu). Natomiast polecenie:
F60-X0000000000>**ennat 00**
wyłączy aktywny slot Nat. Informacja o slotach, czyli ich nazwa i numer znajduje się w pliku:
/usr/Firewall/ConfigFiles/NAT/slotinfo

Wskazówka

Błędna konfiguracja NAT może spowodować zablokowanie dostępu do urządzenia. W tym przypadku zaleca się dokonywanie zmian na nowym zestawie, pozostawiając stary zestaw bez zmian.
Dobrym zwyczajem jest wykorzystanie kalendarza do testowania nowych ustawień. Można to zrobić w ten sposób, że testowany SLOT załączy się jedynie na 5 minut, a następnie na powrót aktywuje się stary, sprawdzony SLOT. Podczas 5 minut, w czasie których działa zaktualizowany zestaw będzie można przetestować jego prawidłowe działanie.

10. 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 OSI. Stosowane są trzy podstawowe metody: analiza protokołów, analiza heurystyczna oraz sygnatury kontekstowe.

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.

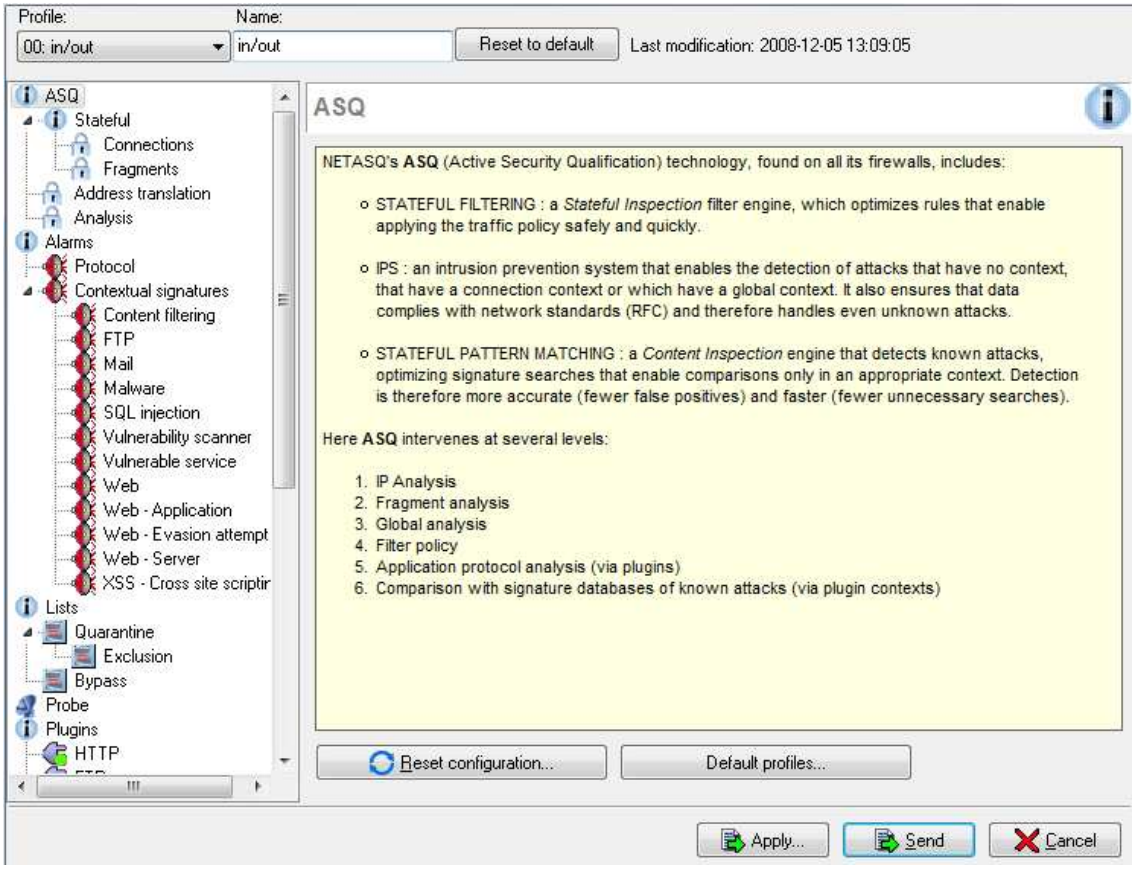
Analiza heurystyczna

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.

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.

Konfiguracja ASQ odbywa się przy pomocy NETASQ Unified Managera, gdzie należy wybrać w lewym menu opcję **Intrusion Prevention.** Poniżej przedstawiono głowne okno konfiguracji modułu IPS.

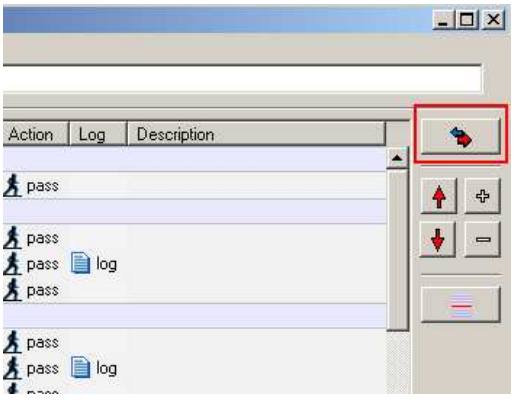


Dla konfiguracji ASQ dostępne są 4 profile ustawień. Profile można przyporządkować dla danego ruchu, który jest określony regułą na firewallu:

	Status	Interface	DSCP Service	Protocol	Message	Source	Source Port	Destination	Destination Port	Action	Routing	QoS	Log	ASQ options	Rule name
1	On	auto		all		Network_bridge	<Any>	<Any>	<Any>	pass				02 (Profile2)	
2	On	auto		all		<Any>	<Any>	<Any>	<Any>	pass				03 (Profile3)	

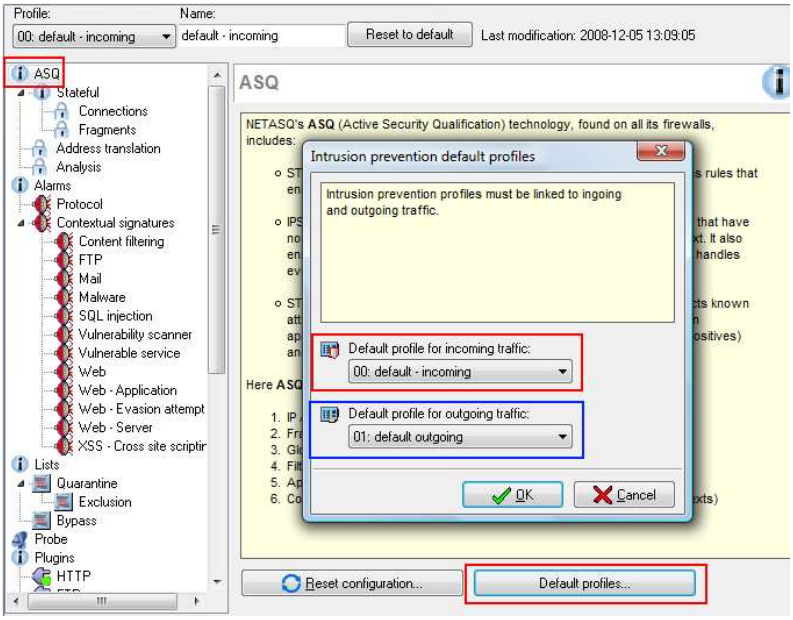
Wskazówka

Jeżeli nie pojawia się kolumna ASQ Options to należy wybrać przycisk **ADVANCED**, który odpowiedzialny jest za wyświetlenie widoku reguł w postaci zaawansowanej:



Domyślnie NETASQ przyporządkowuje odpowiedni profil w zależności od kierunku ruchu pakietów :

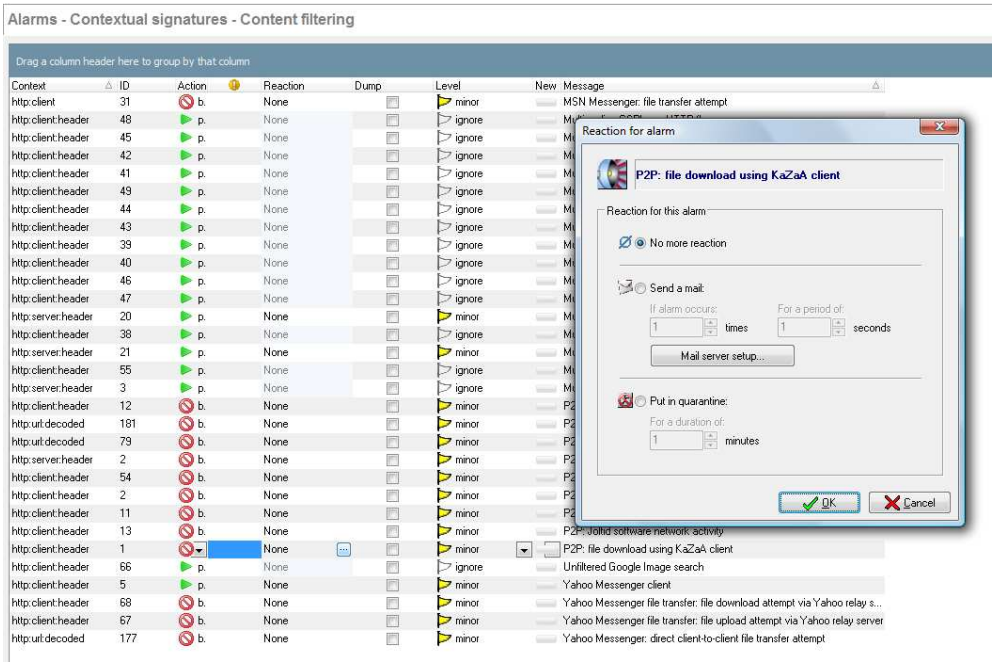
- **OUTGOING** – ruch przychodzący od strony « protected interfaces » (internal, private)
- **INCOMING** – ruch przychodzący od strony « *unprotected interfaces* » (external)



Po wybraniu opcji **ASQ->DEFAULT PROFILES** można określić, który z czterech profili będzie działał dla ochrony danego typu ruchu.

Opcja **ASQ->RESET CONFIGURATION** pozwala na przywrócenie domyślnych ustawień poszczególnych opcji IPSa. W lewym menu konfiguracji IPS można skonfigurować akcje ze względu na wywołane alarmy przez IPS. Alarmy IPS wyświetlane są w sekcji **ALARM** aplikacji NETASQ Real Time Monitor lub w logach, które można zobaczyć w sekcji NETASQ Event Reporter.

Dla każdego z alarmów można definiować następujące opcje:



Context – oznacza w jakim kontekście wystąpił alarm. Czyli przez jaki plugin został on zakwalifkowany jako niebezpieczny.

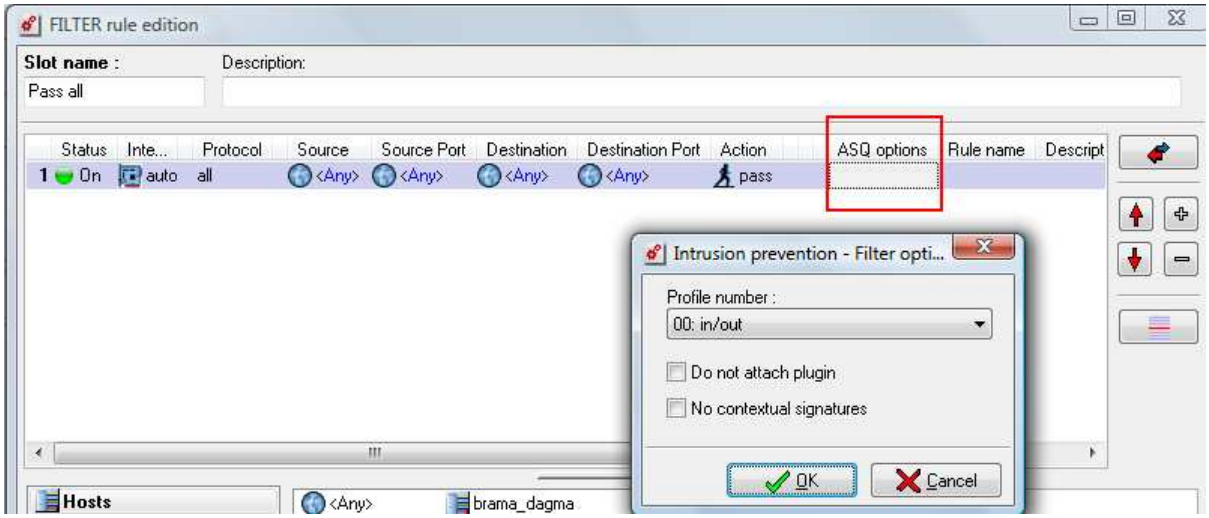
Action – oznacza akcje jaka zostanie wykonana po wykryciu alarmu – PASS/BLOCK.

Reaction – oznacza reakcje na wystąpienie konkretnego alarmu. Reakcja następuje po akcji (Pass/Block). Reakcją może być:

- Brak reakcji,
- Wysłanie wiadomości e-mail do administratora,
- Umieszczenie adresu IP hosta generującego alarm w kwarantannie. Czyli wszystkie połączenie wychodzące dlatego hosta będą zablokowane przez okreslony czas.

Wykluczenia z analizy IPS, ale zarazem też firewalla można skonfigurować w sekcji BYPASS. Dodając odpowiednio host i peer określa się dla jakich połączeń analiza systemu wykrywania włamań będzie wyłączona. Automatycznie jednak wszystkie pakiety dla tych połączeń przechodzą z pominięciem firewalla w obie strony.

Dołączenie odpowiedniego profilu IPS dla połączeń firewall określa się w konfiguracji zapory. **Policy->Filtering->SLOT XX**, gdzie XX określna jeden z 10 zestawów reguł. Rysunek poniżej prezentuje kolumnę *ASQ Option,* w której to można określić stworzony profil dla konkretnego połączenia wyznaczony ze względu na parametry reguły firewalla.



Wskazówka

Z poziomu CLI można wyświetlić informacje na temat aktywnych połączeń wraz z informacją o podłączonym pluginie.

F60-XA313360800404>**sfctl -s conn**

conn:

client	server	proto	sport	dport	state	bytes	plugin
172.16.7.7	172.16.7.254	TCP	53350	22	DATA	18.8KB	stream
172.16.7.7	172.16.7.254	TCP	55460	1300	DATA	988KB	stream
172.16.7.7	192.168.34.222	UDP	137	137	DATA	112 B	packet
172.16.7.7	192.168.34.222	TCP	53157	1026	DATA	2.49KB	stream
172.16.7.7	192.168.34.222	TCP	53182	40850	DATA	61.9KB	stream
172.16.7.7	192.168.34.222	TCP	53189	445	DATA	29.7KB	stream
172.16.7.7	192.168.34.222	TCP	53339	445	DATA	1.80KB	stream
172.16.7.7	192.168.34.222	UDP	55053	53	DATA	66.0 B	dns
192.168.101.165	192.168.34.225	UDP	12192	53	DATA	546 B	
192.168.101.165	195.187.245.55	UDP	123	123	DATA	8.16KB	

11.

Wskazówka

Konfiguracja ASQ znajduje się w osobnych plikach dla każdego profilu w pliku: */usr/Firewall/ConfigFiles/ASQ/XX*, gdzie XX to numer profile.

12.

13.

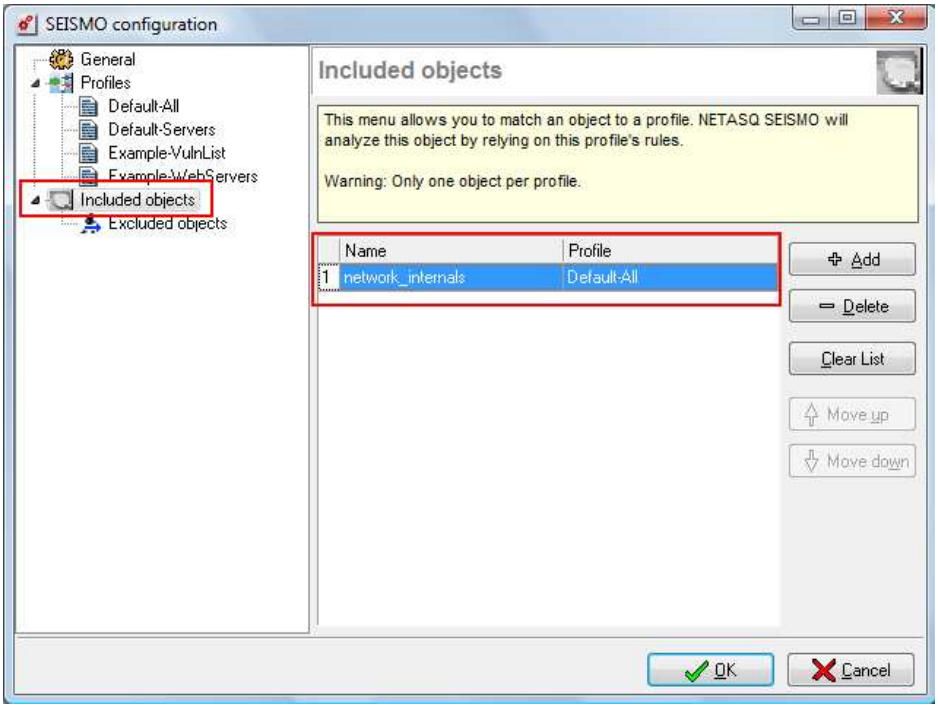
14. Konfiguracja SEISMO

SEISMO to pasywny skaner wnętrza sieci. Skanuje on ruch w kontekście luk w aplikacjach używanych do tych połączeń. Skaner pasywny to znaczy taki, który nie generuje dodatkowego ruchu w sieci. SEISMO wymaga zakupu dodatkowej licencji. Konfiguracja SEISMO odbywa się przez NETASQ Unified Managera. Z lewego menu nalezy wybrać opcję **SEISMO**. Jeśli opcja jest wyszarzona oznacza to, iż zainstalowana w urządzeniu licencja nie ma aktywnej funkcji pasywnego skanera sieci.

W przypadku konfiguracji dla SEISMO istotne jest :

- Określenie komputerów, serwerów które mają być monitorowane.
- Określenie zakresu chroniony pod kątem typu zagrożeń komputerów.
- Wykluczenia ze skanowania.

Domyślnie skanowany jest cały ruch generowany przez grupę *Network_Internals,* czyli wszystkie stacje podłączone do tzw. *Protected Interfaces.*

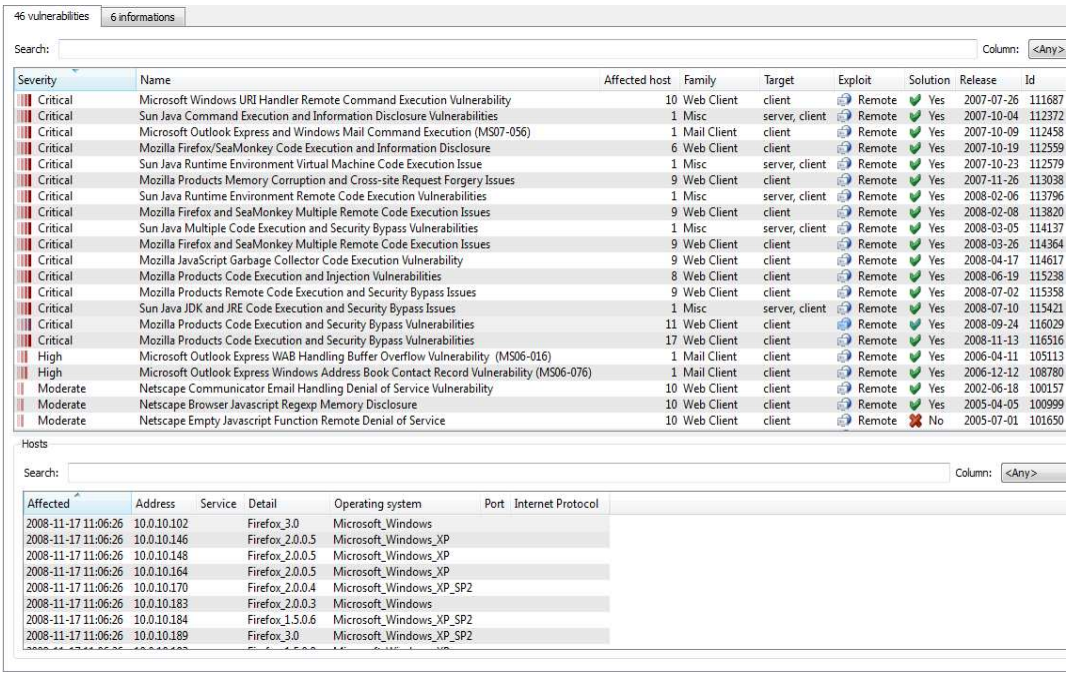


Informacje wyświetlone przez SEISMO znajdują się w NETASQ Real Time Monitor. Po zaznaczeniu konkretnej luki w systemie, prezentowana jest lista stacji których to dotyczy. SEISMO nie blokuje żadnego ruchu, a jednie wyświetla informacje na temat zagrożeń.

W górnej części wybranie opcji **SHOW HELP**.

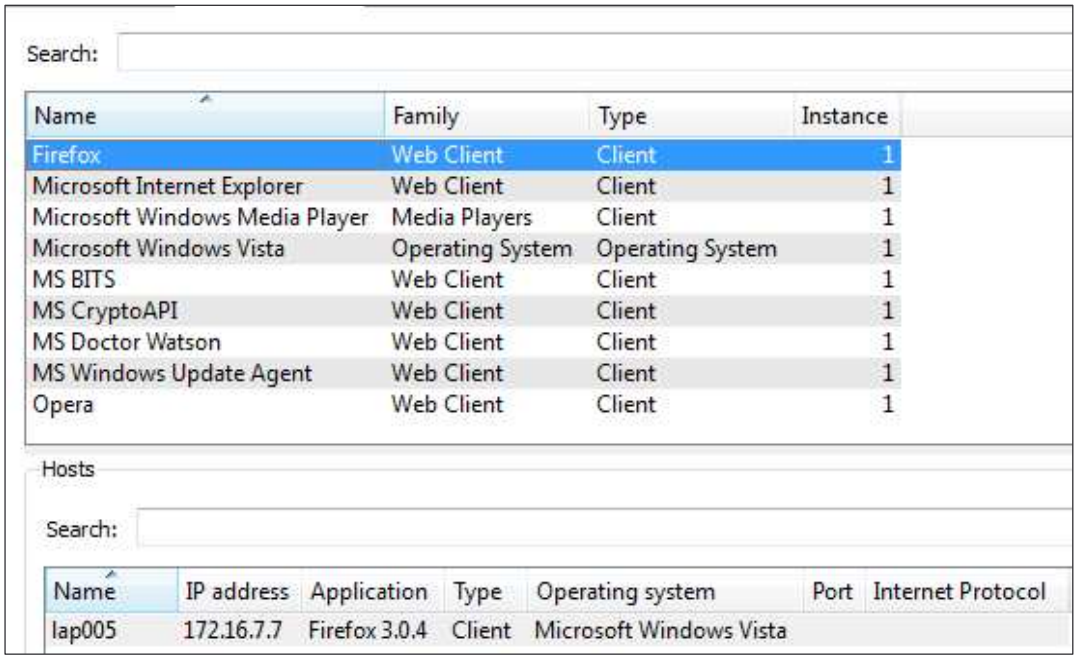
<fdsfdsfdsFDSF?>

Poniżej zaprezentowano przykładowy wynik skanowania pasywnego przez SEISMO:



Po uruchomieniu pomocy dostępna jest informacja na temat szczepionki dla danego zagrożenia. W przypadku dziur w oprogramowaniu rozwiązaniem w większości przypadków jest zainstalowanie nowszej wersji aplikacji.

SEISMO jest także doskonałym narzędziem do monitorowania zainstalowanych aplikacji, które łączą się na zewnętrz firmy. Od wersji firmware 8 taka informacja jest wyświetlana bezpośrednio w konsoli NETASQ Real Time Monitora :



15.

16. Wirtualne sieci prywatne (VPN)

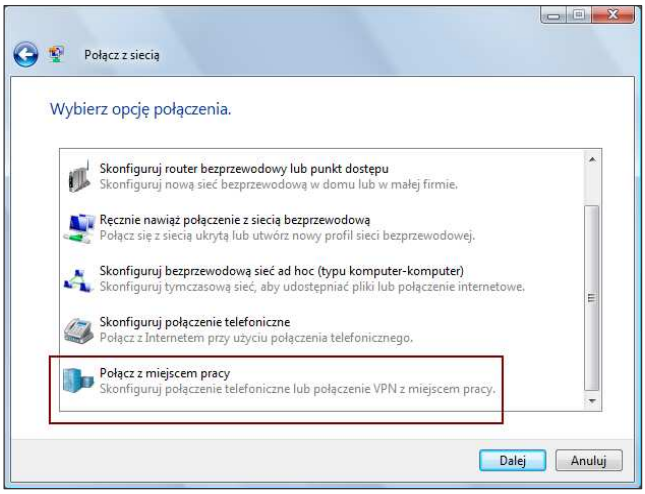
W przypadku urządzeń NETASQ dostępne są trzy możliwości tworzenia kanałów VPN:

- Protokół PPTP VPN – wszystkie modele,
- Protokół SSL VPN – od modelu U70 (SERIA F: od modelu F60),
- Protokół IPSec VPN – wszystkie modele.

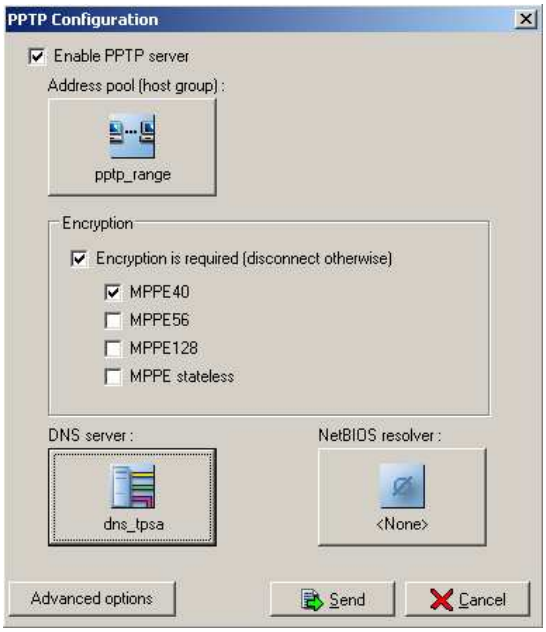
Urządzenia NETASQ różnią się, ze względu na wydajności, liczbę obsługiwanych równoczesnych kanałów VPN. Zastosowanie wybranego protokołu VPN powinno być podyktowane przede wszystkim poziomem zastosowanego bezpieczeństwa oraz kwestiami związanymi z funkcjonalnością protokołu.

PPTP VPN (eng. Point to Point Tunneling Protocol)

PPTP jest protokołem najprostszym w konfiguracji jednak najmniej bezpiecznym. Pozwala on na stworzenie tunelu pomiędzy użytkownikiem mobilnym, a centralą (zwany CLIENT-to-GATEWAY lub MOBILE-to-SITE). Klientem dla tego protokołu jest połączenie sieciowe systemu Windows, które można utworzyć po przejściu przez kreatora systemu Windows.



Następnie w NETASQ Unified Managerze wybieramy opcję **VPN->PPTP** z lewego menu.



W wyświetlonym oknie określamy:

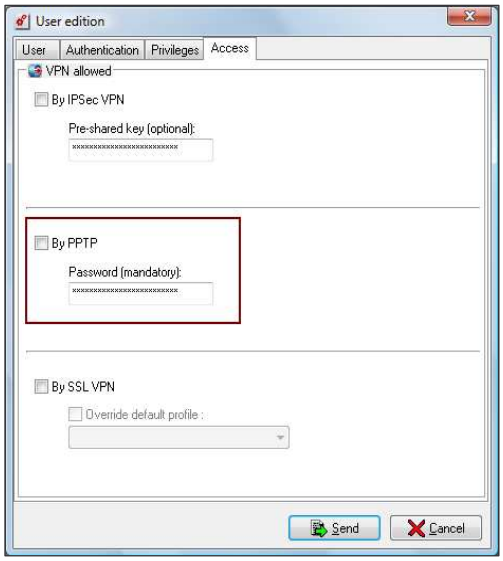
Enable PPTP Server – włączenie/wyłącznie serwera PPTP VPN;

Address Pool – zakres (*RANGE*) adresów IP dla klientów VPN;

Encryption – określa poziom szyfrowania;

DNS – określa adres IP serwera przydzielanego klientowi VPN.

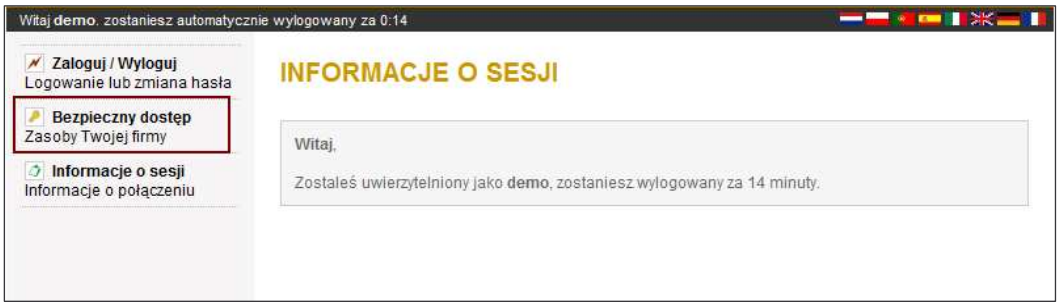
Po określeniu odpowiednich pól należy zatwierdzić zmiany przyciskiem **SEND**. Aby użytkownicy mogli się zalogować poprzez VPN PPTP należy jeszcze określić im dostęp do tej usługi. Opcje z tym związane dostępne są w ustawieniach każdego z użytkowników.



Baza użytkowników może znajdować się na urządzeniu NETASQ lub może być ustawiona synchronizacja z bazą Microsoft Active Directory lub LDAP. W przypadku integracji z AD wymagana jest zmiana schematu AD ze względu na pola wykorzystywane przez NETASQ. Do tych pól należy zaliczyć określenie dostępu przez PPTP. Dokładny opis integracji z AD znajduje się w bazie wiedzy na stronie http://en.knowledgebase.netasq.com/index.php/LDAP_%26_Active_Directory).

SSL VPN

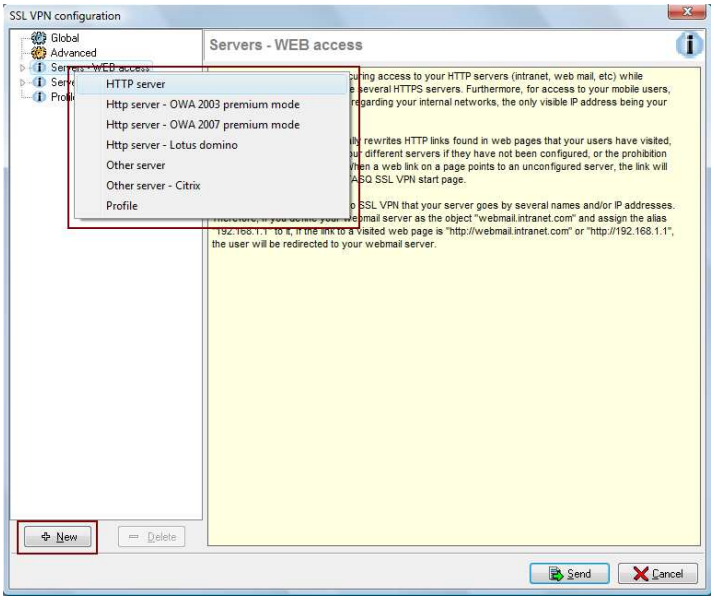
W przypadku SSL VPN klientem jest przeglądarka (IE, Firefox). Użytkownik uruchamia witrynę z adresem https://publiczny_adres_ip_netasq. Po uwierzytelnieniu na stronie, użytkownik będzie miał dostępną opcje:



Następnie pokaże się lista serwerów i usług do których użytkownik ma mieć dostęp.

W przypadku SSL VPN każdy z kanałów jest tworzony dla pojedynczej usługi w odniesieniu do konkretnego serwisu.

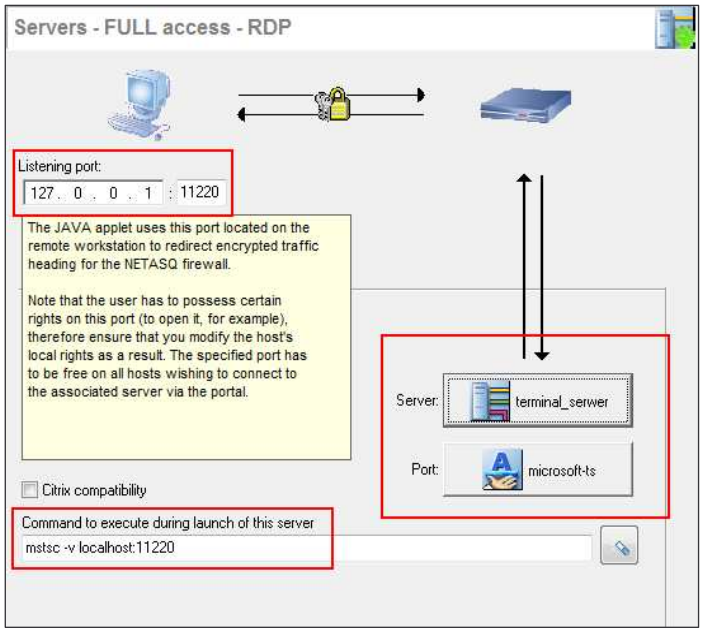
Konfiguracja SSL VPN odbywa się przy pomocy aplikacji NETASQ Unified Manager. Należy wybrać w lewym menu **VPN->SSL VPN**. Okno konfiguracji wygląda następująco:



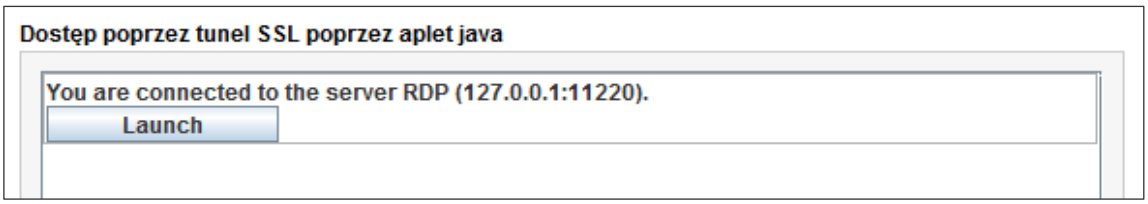
Ze względu na typ serwera jaki jest udostępniony będzie przez VPN wybieramy odpowiedni tryb. Jeśli jest to serwer www wybieramy **NEW->HTTP server**. W przypadku gdy usługa na serwerze nasłuchuje na porcie innym niż 80 to można wykorzystać opcję **NEW->Other server**.

W SSL VPN uruchamia się aplet javy który uruchomiony nasłuchuje na adresie loopback (127.0.0.1) na wskazanym porcie. A następnie wszystko jest przekierowane do serwera SSL VPN (w tym przypadku NETASQ), który inicjuje połączenie do wskazanego serwera.

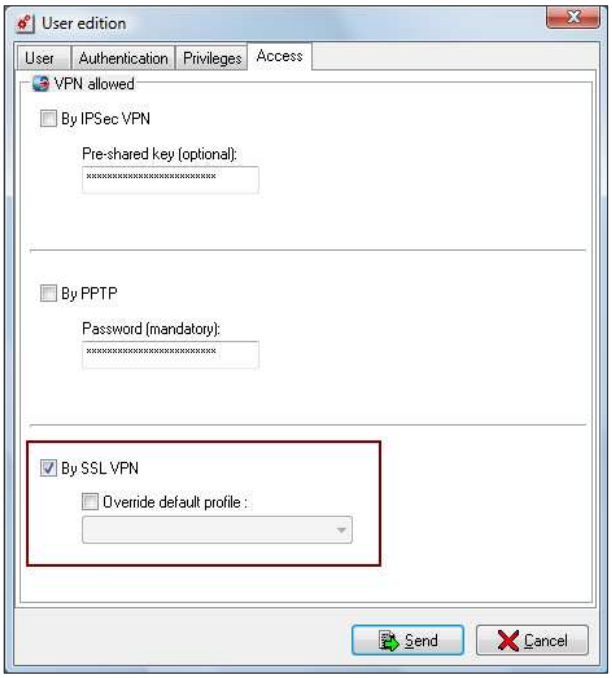
Poniżej poniższy przykład został stworzony dla przypadku w którym przekierowane zostaje połączenie dla zdalnego pulpitu. Czyli wszystkie połączenia kierowane do adresu loopback na port 11220 będą przekierowane do urządzenia NETASQ w postaci szyfrowanej, a następnie od urządzenia NETASQ do docelowego serwera na port 3389.



Dodatkowym polem jest *Command to execute during launch of this server* które pozwala na określenie polecenia, które zostanie wykonane po uruchomieniu apletu javy i wybraniu odpowiedniego przycisku *Launch*. W tym wypadku polecenie **mstsc –v localhost 11220** wywołuje klienta zdalnego pulpitu i uruchamia połaczenie do adresu 127.0.0.1 stacji lokalnej. Dzięki temu użytkownik po zalogowaniu się nie musi uruchamiać klienta RDP i wpisywać adresu. Wystarczy, że wybierze przycisk **Launch** co spowoduje uruchomienie się klienta (mstsc).



Do pełnej konfiguracji SSL VPN należy, analogicznie jak w przypadku PPTP VPN, ustawić dostęp użytkownikowi w zakłace ACCESS.



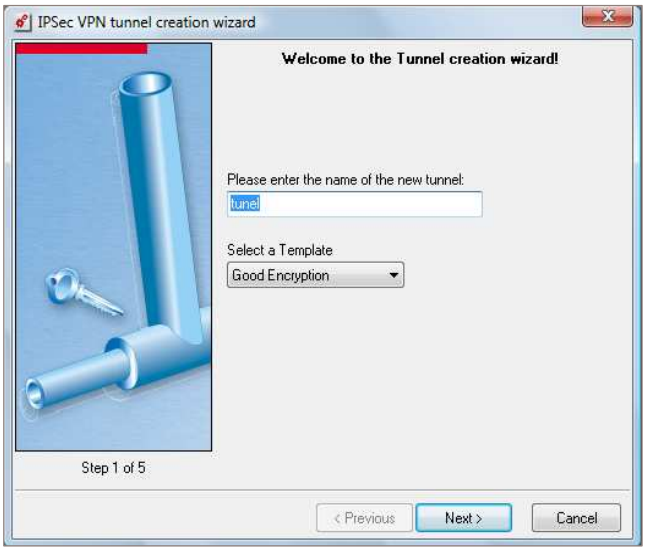
IPSec VPN

Protokół IPSec jest wykorzystywany na urządzeniach NETASQ do budowania dwóch typów tuneli:

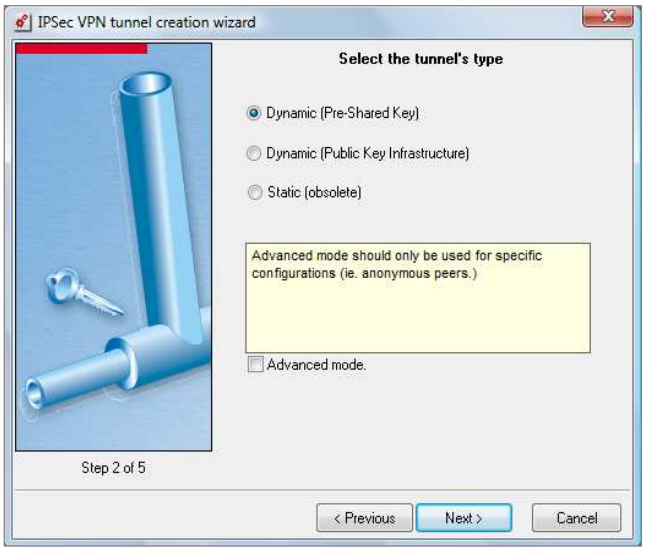
- Clinet-To-Site, zwany inaczej Mobile-to-Site lub Mobile-To-Gateway
- Site-To-Site, zwany inaczej Gateway-To-Gateway

Pierwszych z nich służy do udostępnienia zasobów sieci firmy dla użytkowników zdalnych, logujących z poza obszaru firmy. Użytkownicy posiadają zainstalowanego na stacji klienta IPSec VPN (dla użytkowników posiadających numer licencji do pobrania z http://vpn.netasq.com/). W drugim przypadku tunel tworzony jest pomiędzy dwoma lokalizacjami np. Centralą firmy i jej oddziałem zamiejscowym. Czyli w przypadku Site-To-Site połączone są dwa urządzenia. Zazwyczają połączenie to utrzymywane jest przez cały czas.

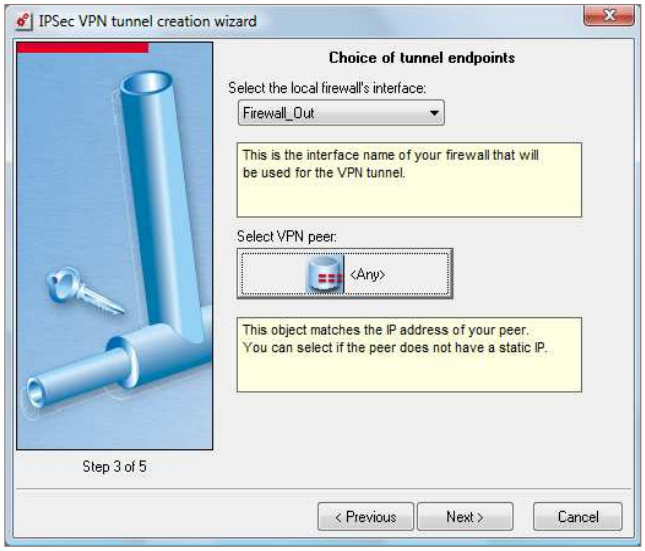
Konfiguracja IPSec VPN odbywa się poprzez wybranie **VPN->IPSec Tunnels** w lewym menu NETASQ Unified Managera. Do wybrania jest kilka zestawów tuneli. W domyślnej konfiguracji wszystkie są puste (*empty*). Tak więc aby zbudować tunel vpn należy wybrać dowolny, pusty zestaw i rozpocząć od przejścia kreatora tunelu VPN. Każdy kolejny tunel VPN w ramach danego zestawu dodaje się poprzez przejście przez właśnie kreatora. W podanym przykładzie zostanie przedstawiona konfiguracja tunelu Client-to-Site z wykorzystaniem (metoda autoryzacji) klucza współdzielonego (*preshared key*). W pierwszym kroku nadajemy nazwę dla wybranego tunelu, a tym samym nazwę dla zestawu (slot):



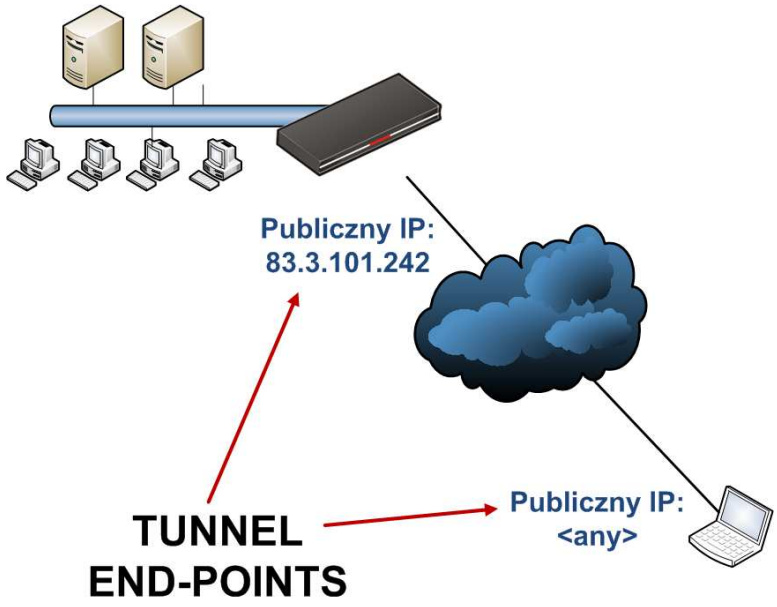
Template określa schamat ustawień, które będą dotyczyły poszczególnych parametrów faz tworzenia tunelu IPSec. Fazy oczywiście będzie można edytować po zakończeniu działania kreatora. Tak więc na tym etapie wybrać należy **NEXT**.



W kolejnym kroku należy określić typ autoryzacji tunelu. W omawianym przykładzie będzie to wymiana współdzielonego klucza (*Dynamic*). Drugą opcją, znaczenie bezpieczeniejszą, jest wykorzystanie infrastruktury klucza publicznego (PKI) i wymuszanie przedstawiania się przez klientów ważnym certyfikatem. Opcja PKI jest dostępna od modelu U120 (w serii F od F200). W przykładzie należy wybrać należy opcje *Dynamic (Pre-Shared Key)* i zatwierdzić przyskiem **NEXT**. Kolejne okno wymaga określenia tzw. *Tunnel Endpoints:*

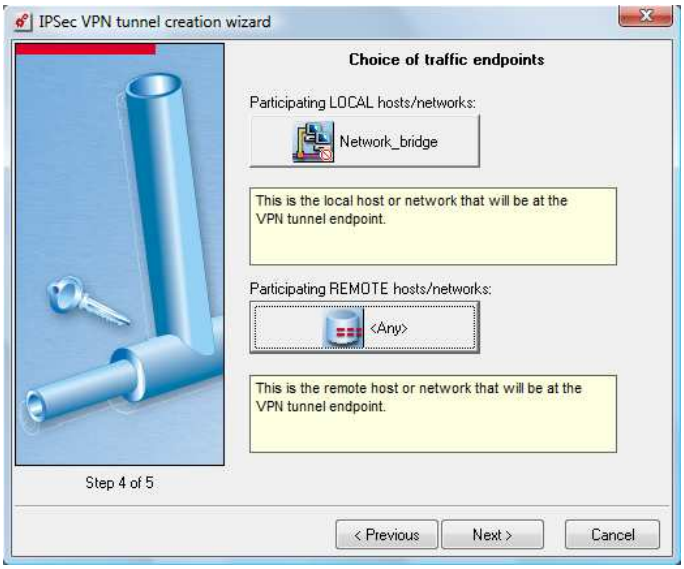


Dla odzwierciedlenie przypadku gdy tworzony jest tunel pomiędzy użytkownikiem mobilnym, a centralą (gdzie NETASQ jest serwerem IPSec VPN), zaprezentować można następującą topologię.

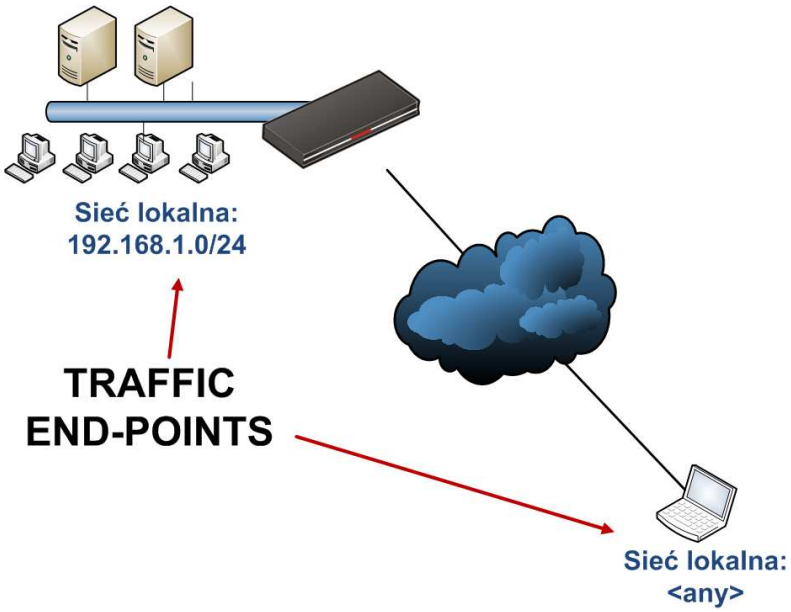


W przypadku połączenia klienta mobilnego do siedziby firmy (Clinet-To-Site) jako *LOCAL FIREWALL INTERFACE należy* wybrać zewnętrzny (external) interfejs NETASQ. *Select VPN peer* to adres drugiego końca tunelu. Z racji, iż adres IP nie będzie znany należy wybrać obiekt o nazwie *<any>*. W przypadku site-to-site, czyli pomiędzy dwoma lokalizacjami, określamy jako *Select VPN peer* obiekt symbolizujący adres IP urządzenia w drugiej lokalizacji. Po określeniu stronu tunelu wybieramy **NEXT**.

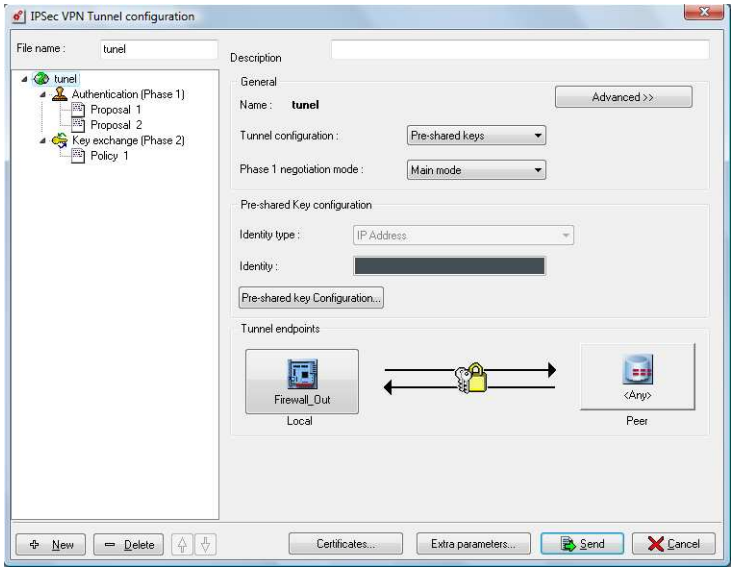
W kolejnym kroku określamy tzw. *TRAFFIC ENDPOINTS*. W tej części określa się sieci, hosty którę będą dostępne dla obu końców tunelu VPN. Odpowiednio *LOCAL* określają sieci po stronie firewalla, natomiast *REMOTE* określa sieci durgiej strony tunelu (zdalnej). W przypadku tunelu pomiędzy klientem mobilnym, a centralą zdalna sieć określona jest przez obiekt *<any>*.



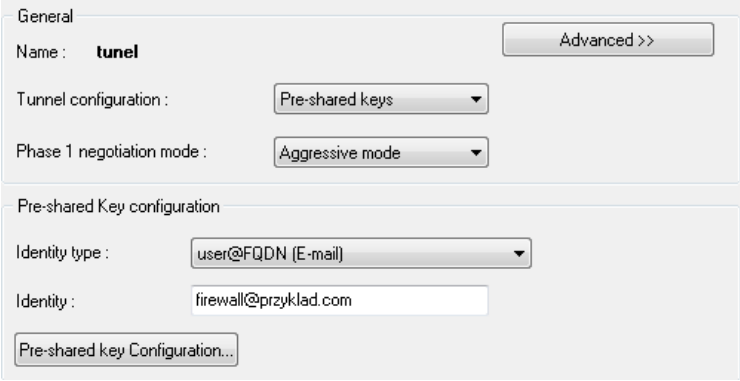
Poniższa topologia odzwierciedla czym są *Traffic Endpoints :*



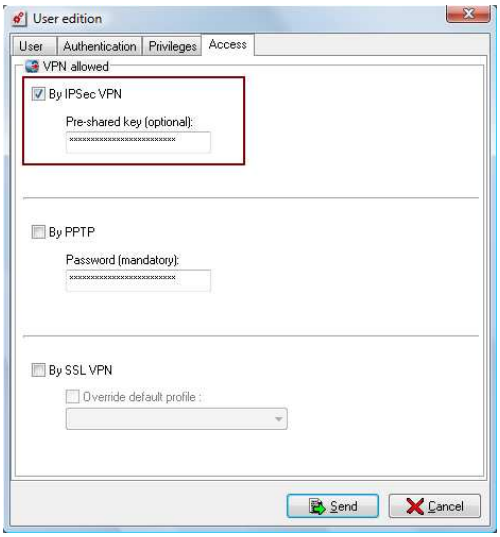
Po zakończeniu kreatora otworzy się okno z pełną konfiguracją VPN w danym zestawie (slocie). W tym oknie można dodać nowe tunele przez przycisk **NEW**. Kolejna możliwość to edycja konfiguracji istniejących tuneli. Następnym etapem jest konfiguracja dostępu użytkownika do serwera VPN.



W przypadku konfiguracji VPN dla połączeń z zdalnym klientem ustawiamy konfigurację dotyczącą współdzielonego klucza (preshared key):



Dla użytkownika ustalamy hasło w sekcji **ACCESS** właściwości użytkownika **OBJECTS->USERS** w lewym menu NETASQ Unified Manager:



W polu *pre-shared key* określamy hasło do autoryzacji użytkownika przy budowaniu tunelu. Następnie należy skonfigurować klienta NETASQ IPSec VPN. Dla użytkowników posiadających licencje klient dostępny jest pod adresem **vpn.netasq.com**. Do autoryzacji potrzebny jest numer seryjny licencji klienta VPN.

Wskazówka

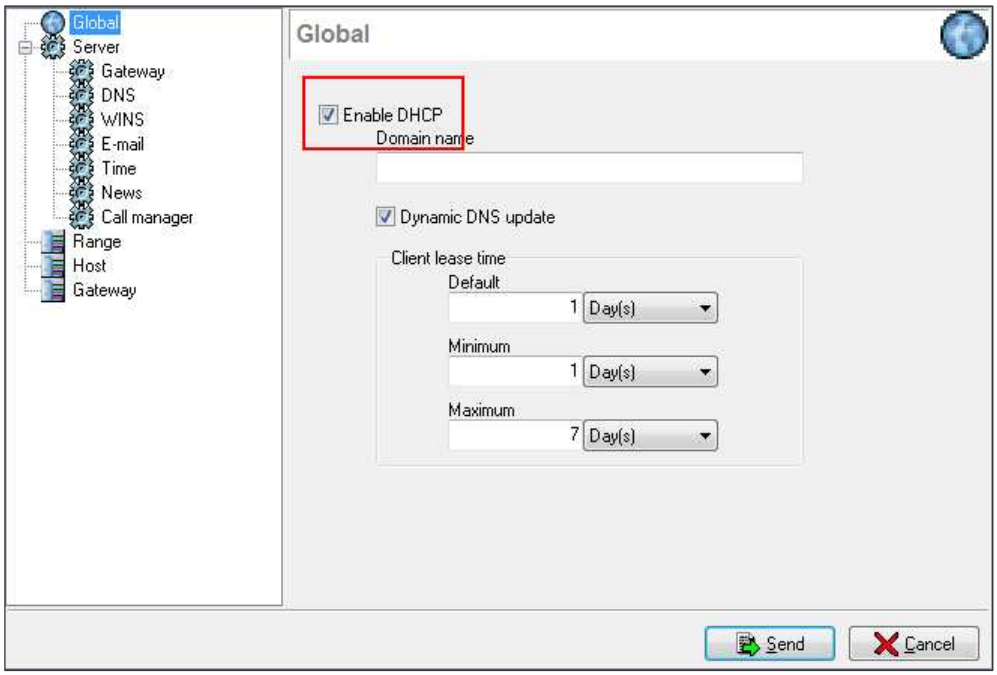
Jeżeli są Państwo zainteresowani testowanie klienta VPN prosimy o kontakt na: netasq@dagma.pl. Istnieje możliwość otrzymania bezpłatnej 30 dniowej wersji.

17. Konfiguracja serwera DHCP

Konfiguracji DHCP można dokonać z poziomu NETASQ Unified Manager w sekcji **SERVICES->DHCP**.

> Uwaga
> W domyślnej konfiguracji NETASQ (default configuration) serwer DHCP jest włączony. W przypadku posiadania drugiego serwera DHCP (uruchomionego w tej samej sieci) można spodziewać się zachwiania stabilności całej sieci.

Główne okno serwera DHCP wygląda następująco:



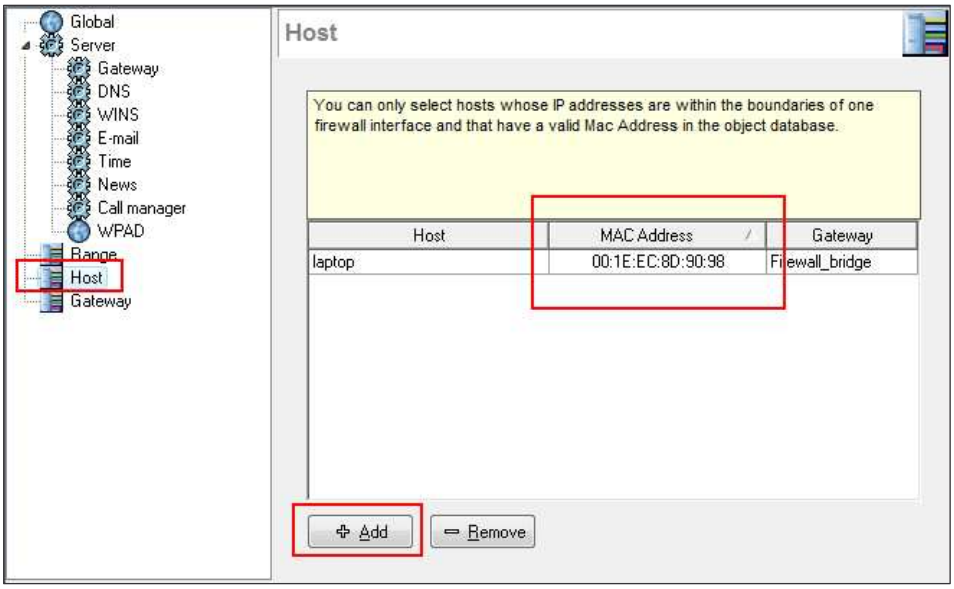
Opcja **ENABLE DHCP** pozwala na włączenie/wyłączenie serwera DHCP. **Dynamic DNS update** pozwala na to, by NETASQ modyfikował dynamicznie wpisy na serwerze DNS (jeśli oczywiście serwer DNS na to pozwala). Chodzi o hosty dotycząc komputerów, którym przydzielono dynamicznie adresy IP przez serwer DHCP.
W sekcji **SERVER** należy ustawić reprezentantów rozgłaszanych parametrów:
DNS – rozgłaszane serwery DNS (podstawowy, zapasowy).
WINS – rozgłaszany adres serwera WINS.

W sekcji **RANGE** wskazujemy, z jakiego zakresu adresów IP serwer DHCP będzie przydzielał adresy.
W sekcji **HOST** możemy ustawić aby dany komputer, o konkretnym adresie MAC mógł dostać zawsze ten same adres IP. Aby to uzyskać muszą być spełnione następujące warunki:

- Komputer musi mieć reprezentanta w obiektach (obiekt typu HOST)
- Adres IP tego komputera nie może być objęty zakresem (obiekt typu RANGE) rozgłaszanym przez serwer DHCP.

- Dodatkowo obiekt typu HOST musi mieć dodany adres MAC we właściwościach.

W sekcji **Gateway** należy określić (zweryfikować ustawienia) czy odpowiednie sieci skonfigurowane w ramach DHCP mają określoną prawidłowo domyślną bramę. Rysunek poniżej prezentuje konfiguracje DHCP z dodanym jednym obiektem typu HOST.



Po zakończonej konfiguracji wybieramy przycisk **SEND**.

Wskazówka

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

18. Konfiguracja proxy http, smtp, pop3, ftp

Proxy na urządzeniach NETASQ są transparentne z punktu widzenia użytkownika. To znaczy, iż nie wymagają konfiguracji przeglądarki internetowej na stacjach roboczych np. dla **HTTP PROXY**. Funkcjonalność każdego z proxy jest następująca.

http proxy

- klasyfikacja URL (filtrowanie dostępu do wybranych grup stron www),
- skanowanie antywirusowe dla ruchu http,
- konfiguracja strony informującej o zablokowaniu dostępu do strony www (Block page),
- uruchomienie http Proxy jest wymagane przy ustawieniu transparentnego uwierzytelniania użytkowników (wymaga także integracji z AD),
- określenie maksymalnego rozmiaru pliku pobieranego przez http,
- ustawienie QoS dla ruchu http.

pop3 proxy

- skaner antyspam (wiadomość SPAM jest oznaczana przez zmianę tematu wiadomości),
- skaner antywirusowy,
- ustawienie QoS dla ruchu pop3,
- kontrola komend w ramach protokołu pop3.

smtp proxy

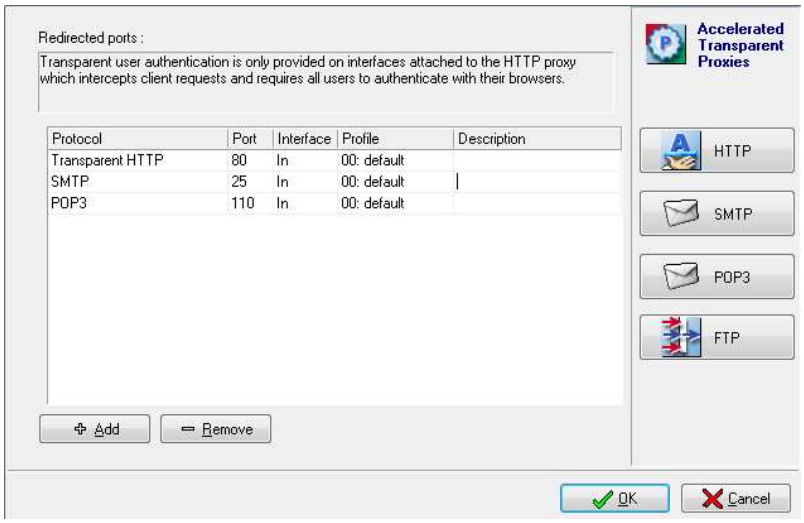
- skaner antyspam (wiadomość SPAM jest oznaczana przez zmianę tematu wiadomości lub może być blokowana[3]),
- skaner antywirusowy,
- filtr SMTP określający reguły filtrowania wiadomości e-mail w odniesieniu do nadawcy lub odbiorcy,
- określenie limitów wielkości poczty i liczby odbiorców.

ftp proxy

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

[3] Blokowanie wiadomości e-mail dla ruchu smtp od wersji firmware 8.

Aby rozpocząć konfigurację proxy należy w NETASQ Unified Manager wybrać **PROXY->GENERAL:**



W oknie tym określić należy, na jakich interfejsach proxy ma być ustawione i z jakim profilem ustawień ma działać. Po prawej stronie widoczne są opcje konfiguracji poszczególnego Proxy. Jeśli ustawienia ogólne Proxy są prawidłowe można przystąpić do konfiguracji każdego z nich. Konfiguracja Proxy może nastąpić zarówno z tego miejsca jak i z **PROXY->*Nazwa_Proxy*** (smtp, pop3, http, ftp[4]).

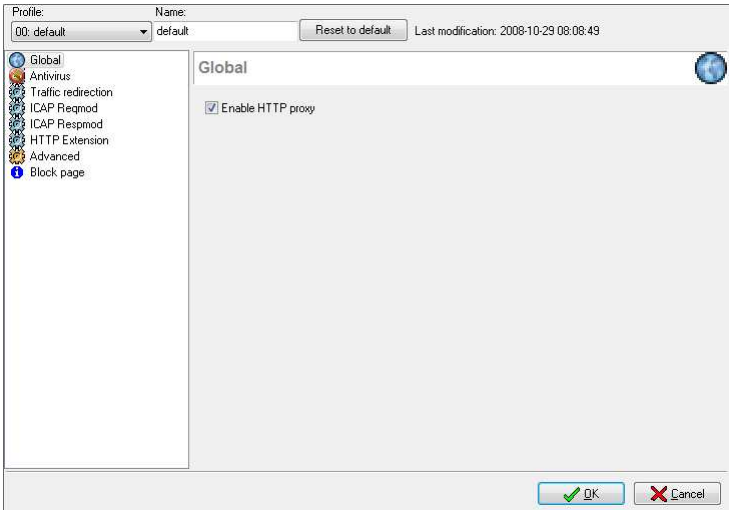
Uwaga

Po przejściu pakietów przez Proxy, adres źródłowy pakietu jest zastępowany adresem NETASQa.

[4] Proxy FTP jest dostępne od wersji firmware 8.

http proxy

Okno ustawień proxy http wygląda następująco (**PROXY -> PROXY HTTP**):



Enable http proxy – oznacza włączenie Proxy. Automatycznie wszystkie połączenia (określone w **PROXY->GENERAL**) http będą przekierowane do Proxy.

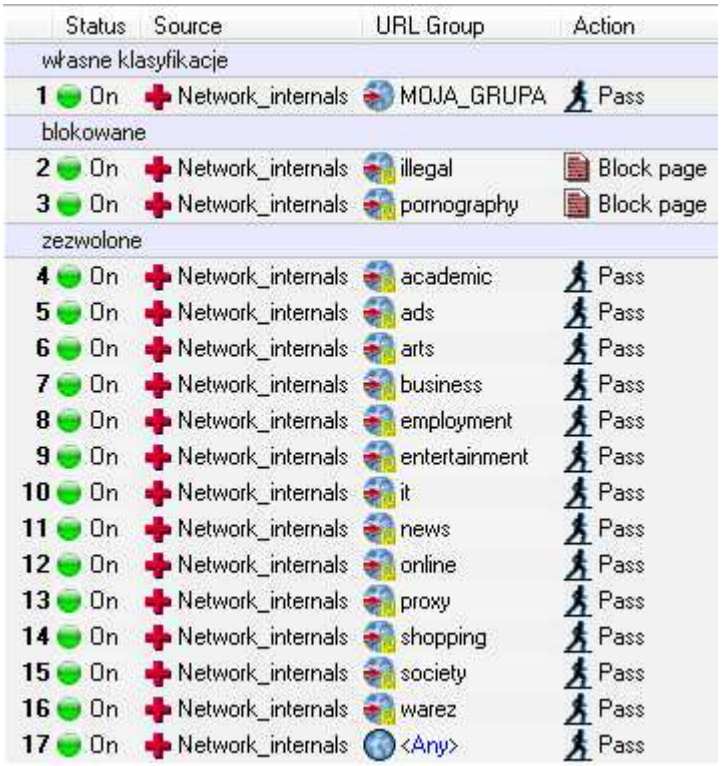
Uwaga

Jeśli po załączeniu tej opcji wysłane zostaną ustawienia, automatycznie zablokowany zostaje dostęp do wszystkich stron www. Aby ustawić przepuszczanie wszystkich stron należy przejść do: CONTENT ANALYSIS -> URL FILTERING -> FILTER RULES i aktywować zestaw (slot) o nazwie PASS ALL.

Po lewej stronie w menu ustawień http PROXY można ustawić:

ANTIVIRUS – włączenie ochrony antywirusowej dla ruchu http. Aby ją włączyć wymagane jest, aby urządzenie miało zaktualizowane bazy AV oraz musi być włączony skaner AV - **CONTENT ANALYSIS ->ANTIVIRUS**.

BLOCK PAGE – pozwala na ustawienie strony URL która pojawi się użytkownikowi jeśli akcja blokowania URL jest **BLOCK PAGE.** Ustawienia dotyczące reguł dla URL znajdują się w **CONTENT ANALYSIS -> URL FILTERING -> FILTER RULES.** Konfiguracja reguł filtrowania URL może wyglądać następująco:



	Status	Source	URL Group	Action
	własne klasyfikacje			
1	On	Network_internals	MOJA_GRUPA	Pass
	blokowane			
2	On	Network_internals	illegal	Block page
3	On	Network_internals	pornography	Block page
	zezwolone			
4	On	Network_internals	academic	Pass
5	On	Network_internals	ads	Pass
6	On	Network_internals	arts	Pass
7	On	Network_internals	business	Pass
8	On	Network_internals	employment	Pass
9	On	Network_internals	entertainment	Pass
10	On	Network_internals	it	Pass
11	On	Network_internals	news	Pass
12	On	Network_internals	online	Pass
13	On	Network_internals	proxy	Pass
14	On	Network_internals	shopping	Pass
15	On	Network_internals	society	Pass
16	On	Network_internals	warez	Pass
17	On	Network_internals	<Any>	Pass

Dostępne są trzy akcje dla blokowania konkretnej grupy URL:

PASS – grupa stron nie jest blokowana

BLOCK – grupa stron zostanie zablokowana z komunikatem BLOCK PAGE

BLOCK PAGE – grupa stron zostanie zablokowana z komunikatem określonym przez stronę html konfigurowaną w **PROXY->http PROXY-> BLOCK PAGE**

Wskazówka

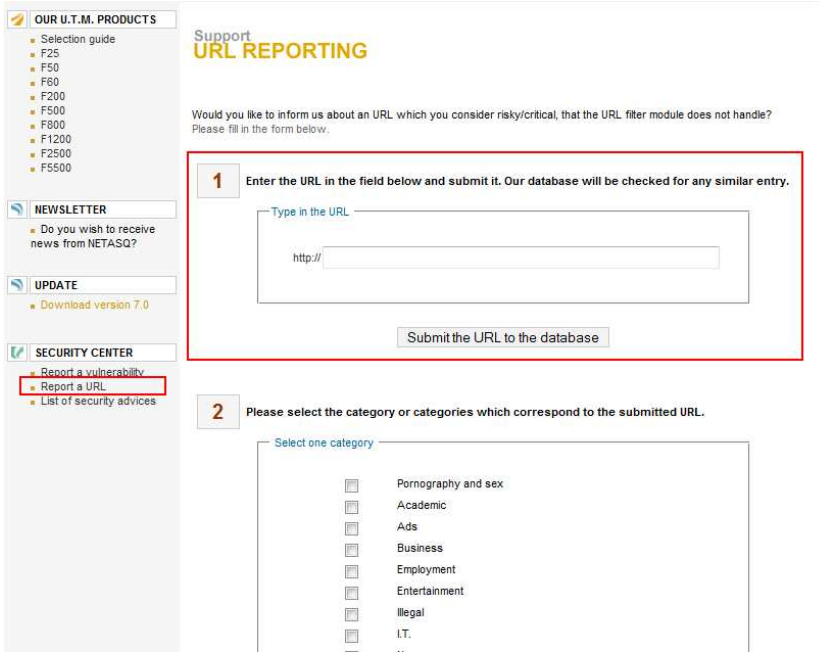
Poniżej zaprezentowano przykładowy kod html dla blokowany kategorii URL.

```
  <!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 www.netasq.com w sekcji Client Area. Poniżej przedstawiono wygląd menu opcji *Report a URL*:



Tworzenie własnych grup URL z dowolnymi adresami dodaje się w NETASQ Unified Managerze: **CONTENT ANALYSIS->URL FILTERING->URL GROUPS.**

Tworzenie własnych grup polega na określeniu łańcucha znaków, które są porównywane z określonym adresem URL w przeglądarce. Tak więc przykładowo by zablokować wszystkie strony w których adresie pojawi się łańcuch moto to podany filtr w grupach powinien wyglądać następująco: **moto**.

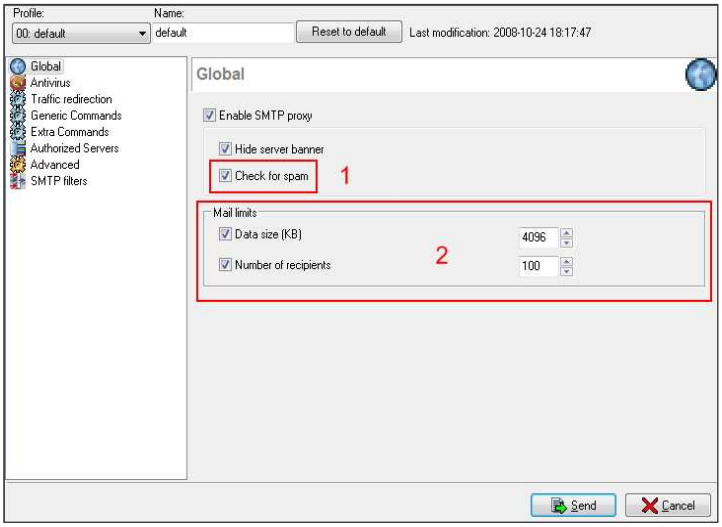
Poniżej przykład dla kilku adresów wchodzących w skład grupy *PRZYKŁAD*:

Wspomniany wyżej wpis **moto** będzie określał np. takie adresy jak: *www.motoryzacja.pl*; *www.moto.de*; motory.com.pl; itp.

Drugi przykład **.pdf* określa pliki z rozszerzeniem PDF. Może to być wykorzystane do blokowania/zezwolenia pobierania plików tego typu.

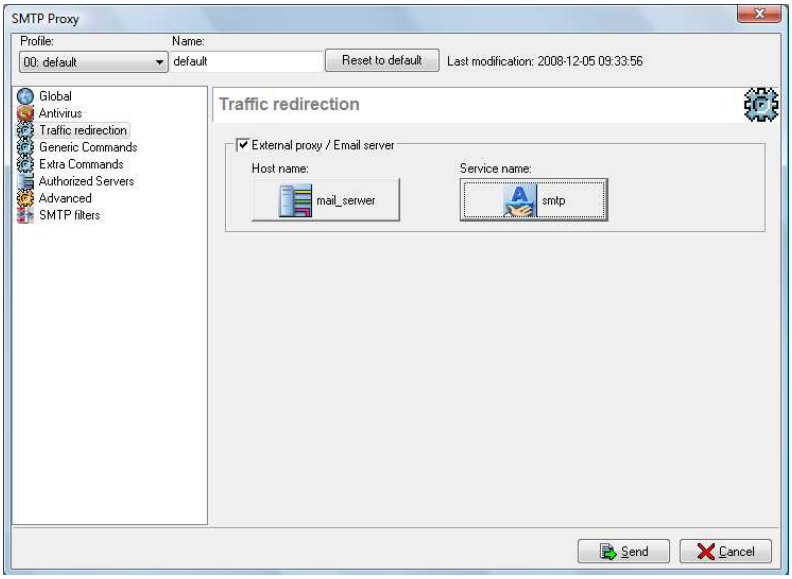
smtp i pop3 proxy

Analogia w konfiguracji dotyczy wszystkich proxy. Dlatego w dalszej części opisane zostaną tylko istotne różnice. Rysunek poniżej pokazuje ogólne ustawienia **smtp PROXY:**



W **sekcji 1** zaznaczanie **Check for Spam** uruchamia skanowanie wiadomości pod kontem poczty niechcianej dla ruchu SMTP. Dodatkowo w **sekcji 2 - Mail limits** można określić limit rozmiaru poczty jak i limit dotyczący liczby odbiorców danej wiadomości.

W przypadku ustawienia ochrony antyspamowej dla serwera pocztowego znajdującego się w sieci lokalnej (lub DMZ) należy ustawić SMTP Proxy na interfejsie zewnętrznym, a następnie w konfiguracji SMTP proxy w sekcji **TRAFFIC REDIRECTION** określić obiekt symbolizujący serwer pocztowy. Nie jest już wymagane ustawienie na NAT akcji **redirect** dla połączeń na porcie 25 (smtp).

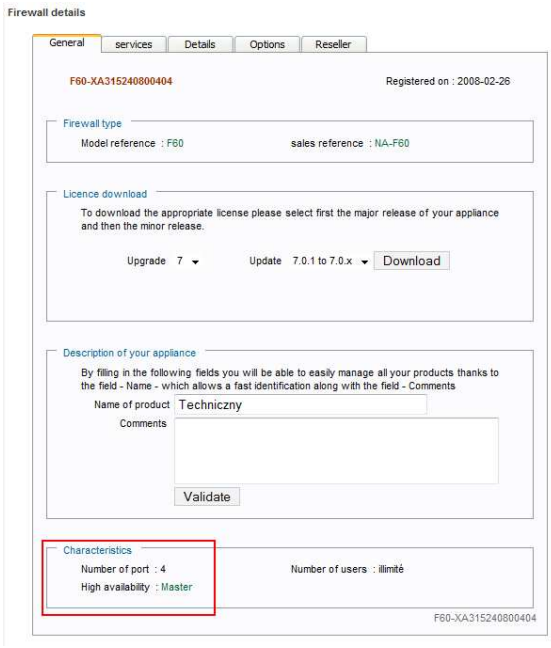


19.

20. Klaster High Availability

Klaster HA określa dwa połączone ze sobą urządzenia NETASQ w celu zapewnienia ciągłości pracy sieci w przypadku awarii jednego z urządzeń.

Aby podłączyć dwa urządzenia w klaster Active/Pasive wymagane jest aby na każdy z dwóch urządzeń była wygenerowana odpowiednia licencja Master/Slave. Aby sprawdzić czy urządzenie ma licencje master lub slave można zalogować się do *Client Area* na www.netasq.com. Poniżej przykład takiej licencji:

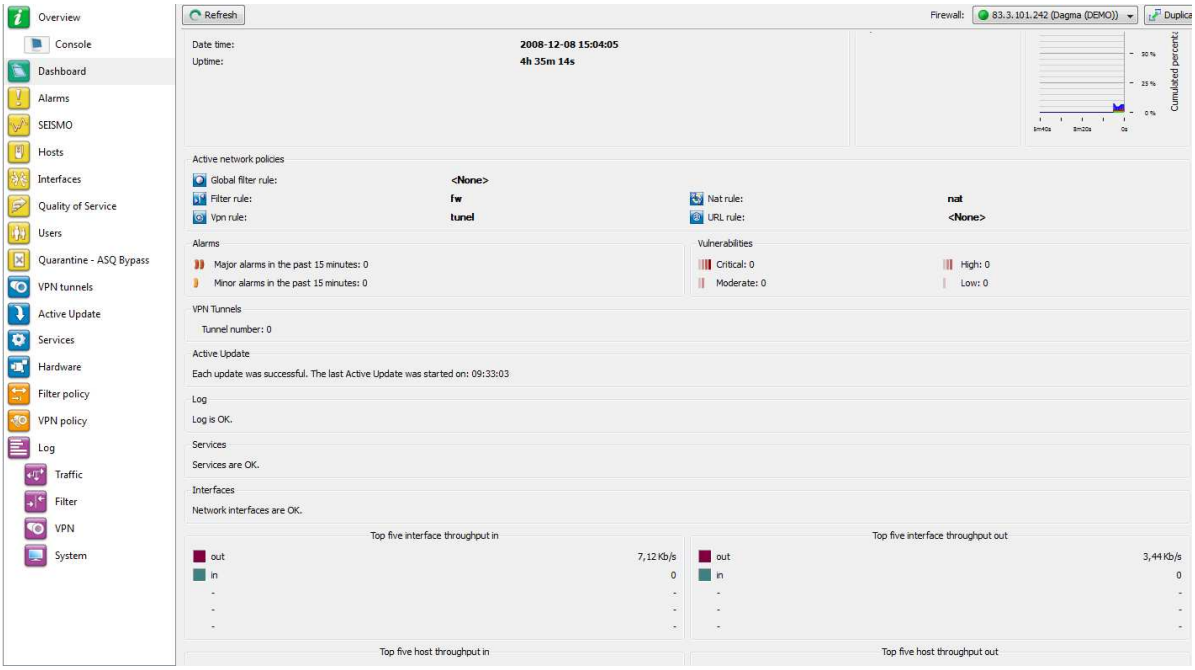


Aby połączyć ze sobą dwa urządzenia należy wykonać następującą procedurę:

a. Podłączyć się NETASQ Unified Managerem do urządzenia MASTER,
b. Skonfigurować interfejsy i trase domyślną odpowiednio w **NETWORK->INTERFACES** i **NETWORK -> ROUTING**,
c. Przejść przez HA wizzard (górne menu NETASQ Unified Managera) w FIREWALL -> HIGH AVIABILITY...,
d. Podłączyć się NETASQ Unified Managerem do urządzenia SLAVE,
e. Skonfigurować interfejsy i trasę domyślną w NETWORK->INTERFACES i NETWORK -> ROUTING analogicznie jak w przypadku pkt. 2,
f. Przejść przez HA wizzard (górne menu NETASQ Unified Managera) w FIREWALL->HIGH AVIABILITY....,
g. Wyłączyć oba urządzenia,
h. Podłączyć oba urządzenia kablem typu cross przed dedykowany interfejs,
i. Podłaczyć reszte infrastruktury w topologi sieci (switch, modem lub inne routery),
j. Załączyć oba urządzenia.

21. NETASQ Real-Time Monitor

Aplikacja NETASQ Real Time Monitor (RTM) służy do monitorowania w czasie rzeczywistym pracy urządzenia. Dostępne informacje w RTM związane z przeglądem aktywnych połączeń dla wybranych hostów, poziomu obciążenia interfejsów sieciowych, kontroli stanu tuneli VPN itp. Główne okno RTM wygląda następująco:



W sekcji **OVERVIEW** można zdefiniować do wiele połączeń do różnych monitorowanych urządzeń NETASQ. Każde połączenie może odbywać się w trybie **READ/WRITE** lub domyślnie tylko w trybie READ. Opcja **R/W** umożliwia umieszczenie danej stacji w kwarantannie (sekcja HOSTS), a także usunięcie aktywnego tunelu VPN (**flush tunel**), lub np. usunięcie zautoryzowanego użytkownika (sekcja USERS).

Wskazówka

W przypadku blokowania ruchu przez IPS (ASQ) należy w pierwszej kolejności należy zweryfikować wyświetlane alarmy w sekcji **RTM->ALARMS**. Następnie proszę odszukać wybrany alarm w **NETASQ Unified Manager->Intrusion Prevention** i zmienić domyślną akcje BLOCK na PASS. Oczywiście należy dokładnie przeanalizować czy ewentualna zmiana nie spowoduje obniżenia poziomu bezpieczeństwa.

22. NETASQ Event Reporter

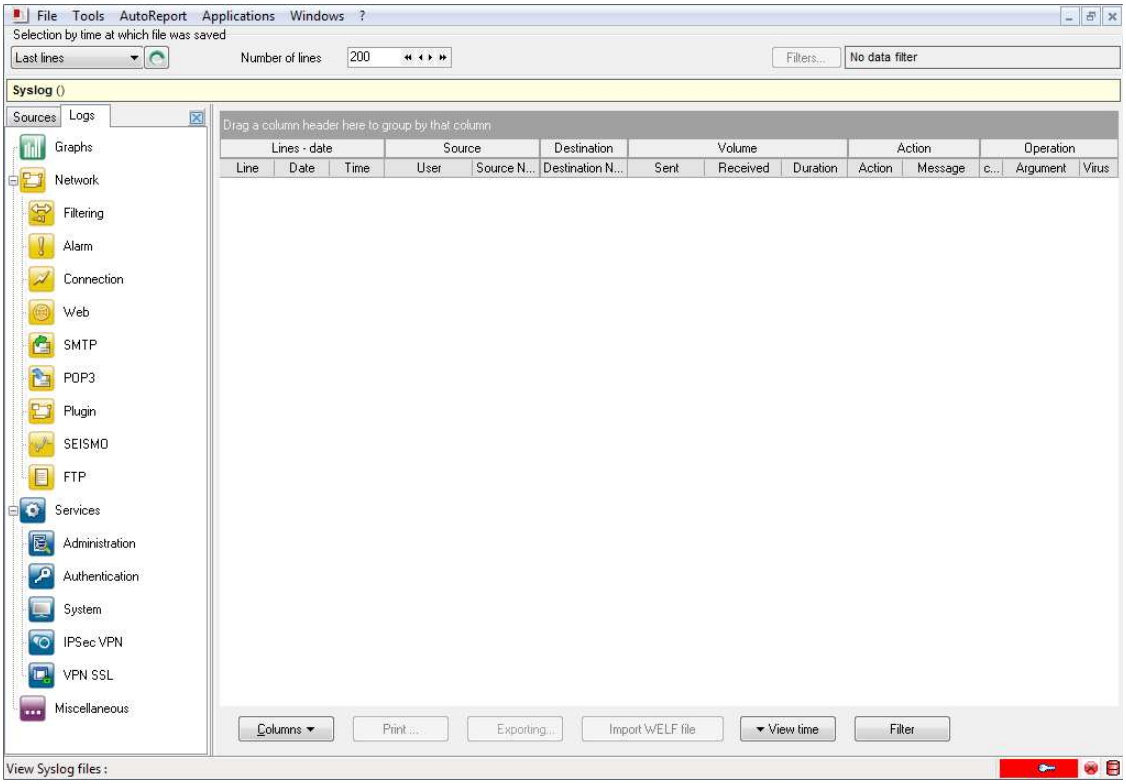
Aplikacja NETASQ Event Reporter służy do przeglądania logów i uruchomienia automatycznego generowania raportów. Logi mogą być przechowywane w trzech różnych lokalizacjach:

- Na urządzeniu NETASQ (U120,U250,U450,U1100,U1500,U6000)
- Na dysku lokalnym stacji roboczej z zainstalowanym syslogiem (wszystkie urządzenia)
- W bazie danych PostgreSQL.

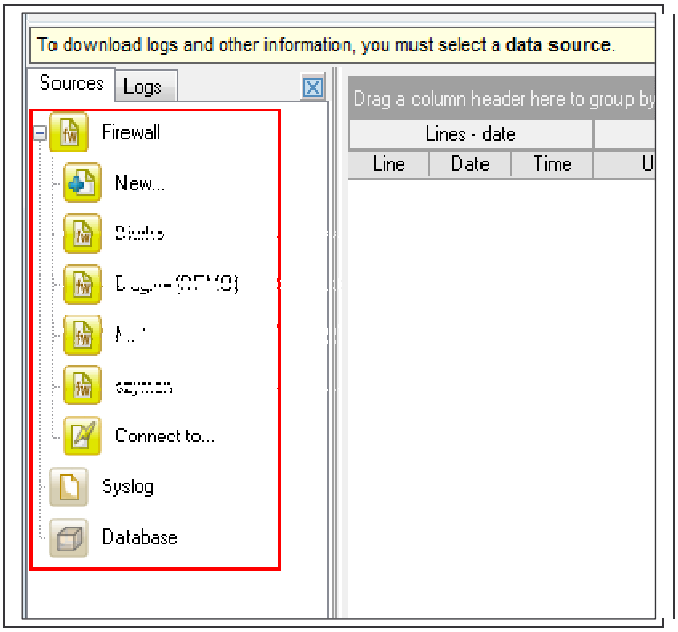
Na urządzeniu przechowywane są tylko i wyłącznie logi w przypadku urządzeń wyposażonych w dysk twardy. Dla pozostałych urządzeń należy ustawić przesyłanie logów na zewnętrzny serwer logów (syslog serwer). Opcja ta dostępna jest w NETASQ Unified Managerze **LOGS->SYSLOG->FORWARD LOGS TO EXTERNAL SYSLOG SERVER.**

Logi przechowywane są w bazie danych (PostgreSQL), zainstalowanej na dedykowanej maszynie, po wcześniejszym ich zaimportowaniu przez aplikację NETASQ Collector. NETASQ Collector może pobierać logi bezpośrednio z urządzenia wyposażonego w dysk twardy lub z plików zgromadzonych przez NETASQ Syslog service dla urządzeń bez dysku twardego.

Główne okno aplikacji NETASQ Event Reporter zaprezentowano poniżej:



W lewym menu znajdują się odpowiednie typy logów. Po ich wybraniu w głównym oknie zostaną wyświetlone wszystkie logi związane z danym typem. Aby określić źródło pobierania logów należy wybrać odpowiednie ich źródło (SOURCE) tak jak pokazano na rysunku poniżej:



Wybierając opcje **DATABASE** nastąpi połączenie z bazą danych skonfigurowaną w książce adresowej NETASQ Event Reportera (*File->Address book*). Źródło **SYSLOG** będzie odwoływać się do fizycznej lokalizacji plików określonej w konfiguracji **NETASQ Syslog Service**. W przypadku urządzeń wyposażonych w dysk twardy można się podłączyć do nich bezpośrednio wybierając konkretne urządzenie z listy (żółte ikony). Lista urządzeń pobierana jest z książki adresowej.

Aplikacja NETASQ Collector konfigurowana jest z górnego menu **TOOLS->MANAGE COLLECTOR**. Natomiast konfiguracja automatycznych raportów odbywa się przez aplikację **NETASQ AUTOREPORTER** dostępnej przez górne menu **AUTOREPORTER->CONFIGURE SERVICE.**

23. Najczęściej zadawane pytania (FAQ)

Jak wygląda procedura aktualizacji firmware?

- Zaloguj się na stronę www.netasq.com
- Pobierz najnowszy firmware (zgodnie z release info) przeznaczony dla twojego urządzenia.
- Zapoznaj się z plikiem opisu aktualizacji (release info).
- Podłącz się do urządzenia aplikacją NETASQ Unified Manager zgodną z firmware urządzenia. Oznacza to, że jeśli urządzenie posiada firmware 7.0.5.1 to należy podłączyć się aplikacją w wersji 7.0.
- Zalecane jest podłączenie się także przez port serial na czas aktualizacji. Ma to na celu kontrolę przebiegu aktualizacji.
- W górnym menu przejdź do MAINTANACE -> UPDATE FIRMWARE.
- Wskaż pobrany plik firmware (*.maj)
- Po wgraniu pliku na urządzenie (upload) rozpocznie się proces aktualizacji.

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

Aby restartować urządzenie do ustawień fabrycznych należy wykonać polecenie „defaultconfig". Polecenie to można wywołać z odpowiednimi parametrami. Opis tych parametrów jest dostępny po wpisaniu polecenia „*defaultconfig –h*". Po restarcie do ustawień fabrycznych należy ponownie uruchomić urządzenie (komenda „reboot").

Gdzie znajdują się pliki konfiguracyjne na dysku urządzenia?

Pliki konfiguracyjne znajdują się w:
„/usr/Firewall/ConfigFiles/"
Dla przykładu reguły firewall'a wchodzące w skład slotu (zestawu reguł) o numerze 10 będą w pliku:
„/usr/Firewall/ConfigFiles/Filter/10"

Nie można aktualizować firmware – "*active update failed*"?

Najczęściej może to dotyczyć małych urządzeń – grupa S – F25, F50, F60. W celu przeprowadzenia aktualizacji firmware należy usunąć w tym przypadku sygnatury antywirusa i klasyfikację URL. Aby to wykonać należy:
1. Podłączyć się do urządzenia przez SSH (np. przez PUTTY)
2. Wydać kolejno polecenia:
> cd /usr/Firewall/Data/AntiVIRUS/Clamav/Base/ (jeśli AV to ClamAV)
> rm * (usuwamy wszystkie pliki)
> cd /usr/Firewall/Data/URLGroups/URLFiltering/Download/
> rm * (usuwamy wszystkie pliki)
Po tych operacjach należy zaktualizować firmware. Wymuszenie aktualizacji sygnatur antywirusa, ips, antyspam, klasyfikacji url na urządzeniu można zrealizować poleceniem : « autoupdate ».

Skąd mogę pobrać najnowszą wersję firmware?

Strefa dla klientów na www.netasq.com to miejsce skąd można pobrać najnowszą wersje firmware jak i najnowsze oprogramowanie Administration Suite. W serwisie tym znajduję się także informacja o aktualizacji zawierająca dokładny opis zmian dla wersji.

W ustawieniach kanału IPSec VPN nie widać algorytmów AES, Blowfish, 3DES?

W podstawowej wersji urządzenie dostarczane jest z tzw. podstawowym szyfrowaniem. Aby móc szyfrować wymienionymi algorytmami należy skontaktować się z firmą DAGMA sp. z o.o. lub naszym partnerem handlowym. Można także przesłać maila na pomoc@dagma.pl z tematem „Silne szyfrowanie". W mailu prosimy podać dane kontaktowe.

Łączenie klientem PPTP na Windows VISTA nie udaje się, a na Windows XP wszystko działa poprawnie. Co sprawdzić?

W przypadku braku możliwości zestawienia tunelu PPTP VPN należy sprawdzić czy urządzenie jest wyposażone w firmware obsługujący silne szyfrowanie. Jest to tzw. Branch EUROPE. W celu weryfikacji posiadanego typu firmware należy wygenerować *Technical Support.* Wymuszenie łączenie kanału PPTP z Windows Vista do urządzenia ze słabym szyfrowaniem polega na zmianie wartości klucza w rejestrze systemu na wartość 1 (true):

HKLM\System\CurrentControlSet\Services\Rasman\Parameters\AllowPPTPWeakCrypt

Jak uruchomić dostęp przez SSH do urządzenia NETASQ?

Dostęp do urządzenia przez SSH można włączyć przez aplikację NETASQ Unified Manager. W górnym menu programu wybrać należy **FIREWALL->SECURITY->SSH ACCESS**. Następnie zaznaczyć pole *Activate SSH Access to firewall* oraz opcję *Enable password Access.* Druga opcja nie jest zalecana ze względów bezpieczeństwa. Należy więc wykorzystać do autoryzacji certyfikaty, które można wyeksportować z urządzenia w tym samym oknie.

Uruchomienie SSH z poziomu CLI to zmiana flagi *State* w sekcji *SSH,* w pliku: /usr/Firewall/ConfigFiles/system.

Co to jest TECHNICAL REPORT i jak go wygenerować?

Technical Report to plik zawierający ustawienia urządzenia oraz informacje na temat jego stanu bieżącego. Można go wygenerować poleceniem z CLI: *sysinfo.*

Istnieje także możliwość utworzenia raportu z poziomu NETASQ Unified Managera. W górnym menu programu należy wybrać **FIREWALL-> TECHNICAL REPORT**. Następnie zapisać plik na dysku. Jest to plik tekstowy więc można do jego podglądu użyć windowsowego notatnika. Raport ten jest niezbędny przy zgłaszaniu zapytań do wsparcia technicznego NETASQ pod adres: pomoc@dagma.pl.

Jak zbierać logi z urządzeń klasy S (F25, F50, F60, U30, U70)?

Urządzenia klasy S nie posiadają dysku twardego. W związku z tym należy wskazać w sieci lokalnej stację, która będzie pełniła rolę serwera logów, miejsca ich składowania. Wymagane jest by zainstalować na tej stacji aplikacje wchodzące w skład Administration Suite:

- NETASQ syslog service,
- NETASQ EVENT REPORTER,
- NETASQ Autoreport,
- NETASQ Collector.

W opcjach konfiguracji aplikacji NETASQ Syslog service można ustawić w jakiej lokalizacji na dysku będą zapisywane logi przesyłane przez urządzenie. Urządzenie zacznie wysyłać pliki logów w chwili gdy w menu NETASQ Unified Managera **LOGS->SYSLOG** ustawiona będzie opcja *Forward logs to external syslog Server.* Jako syslog serwer należy wskazać obiekt symbolizujący stacje na której zainstalowano wyżej wspomnianą aplikację.

Aplikacja NETASQ Collector służy to przesyłania logów z plików tekstowych do bazy danych (PostgreSQL). Konfiguracja Collectora jest dostępna z poziomu aplikacji NETASQ Event Reporter.

Aplikacja NETASQ Autoreporter służy do generowania raportów w oparciu o logi zgromadzone w bazie danych.

Gdzie mogę sprawdzić do kiedy ważna jest licencja?

Informacja o ważności licencji znajduje się na stronie www.netasq.com w tzw. CLIENT AREA. Aby się zalogować do tej strefy należy użyć nazwy użytkownika i hasła otrzymanego po rejestracji. Data ważności licencji jest dostępna też w *Technical Report* oraz w głównym oknie Unified Manager. Znajduje się także na menu ACTIVE UPDATE w NETASQ Real-Time Monitor.

Dane licencji wyświetlane w NETASQ Unified Manager/Real-Time Monitor nie są zgodne. Co mam robić?

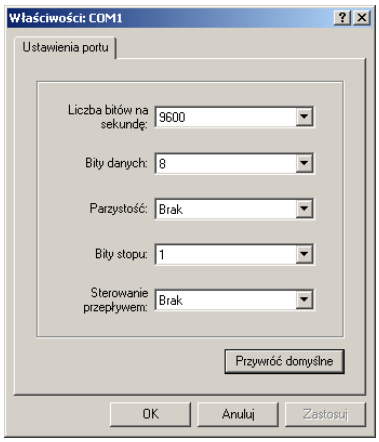
W takim przypadku należy wysłać maila na pomoc@dagma.pl. W tytule wiadomości napisać „nieprawidłowa licencja". Do wiadomości proszę dołączyć *Technical Support*.

Czy dla urządzeń NETASQ dostępny jest tzw. KNOWLEDGE BASE?

Na stronie www.netasq.com każdy z zarejestrowanych klientów ma możliwość skorzystania z bazy wiedzy. Po zalogowaniu się na stronie należy przejść do **TECHNICAL SUPPORT->KNOWLEDGE BASE** w górnym menu**.**

Jak powinna wyglądać konfiguracja Windows Terminala by podłączyć się do urządzenia przez port serial?

Rysunek poniżej przedstawia ustawienia jakie powinny być określone podczas podłączenia się do urządzenia NETASQ przy użyciu portu SERIAL. Ustawienia te dotyczą aplikacji Windows Terminal. Do podłączenia można też wykorzystać aplikację PUTTY.



Po zestawieniu połączenia należy wybrać przycisk ENTER aby uzyskać dostęp do znaku zachęty. Logować można się na użytkownika „admin". W przypadku, gdy urządzenie jest w ustawieniach domyślnych logowanie to zakończy się niepowodzeniem, chyba że zostanie nadane hasło według procedury restartu hasła lub gdy przynajmniej raz podłączymy się przy użyciu NETASQ Unified Managera.

Zapomniałem hasła dla użytkownika „admin". Czy istnieje procedura restartu hasła?

Podłącz się do urządzenie przez port serial, zrestartuj urządzenie – poleceniem „reboot",

Po uruchomieniu się urządzenia pojawi się opcja wyboru, z której partycji ma startować system NS-BSD:

NETASQ Firewall – BOOT

1) main slot

2) backup slot

choose:

zaraz po wybraniu opcji (lub przycisk **ENTER**) należy wybrać kilkukrotnie przycisk spacji.

Po uzyskaniu znaku zachęty wpisujemy: „**boot –s**" i przyciskamy **ENTER**.

Po pojawieniu się komunikatu „Enter full pathname or RETURN for /bin/sh:" przyciskamy ENTER.

Następnie wpisujemy: „**/usr/Firewall/sbin/swpasswd**" i wybieramy **ENTER**.

po chwili ukaże się prośba o nadanie nowego hasła. Nastąpi restart i nowe hasło zostanie nadane.

Jakie jest przeznaczenie portu USB w urządzeniach NETASQ?

W urządzeniach NETASQ port USB pełni dwie role:

- Umożliwia wczytanie poprzez dysk USB pliku konfiguracyjnego (pod warunkiem, że urządzenie jest przywrócone do ustawień fabrycznych).
- Umożliwia zabezpieczenie urządzenia specjalnym kluczem USB, dzięki czemu restart (reboot) urządzenia nie wykona się jeśli nie włożymy odpowiedniego klucza USB.

Aby użyć dysku USB należy się upewnić, iż jest on rozpoznawany przez system operacyjny FreeBSD.

Aby uzyskać więcej informacji proszę pisać na adres pomoc@dagma.pl.