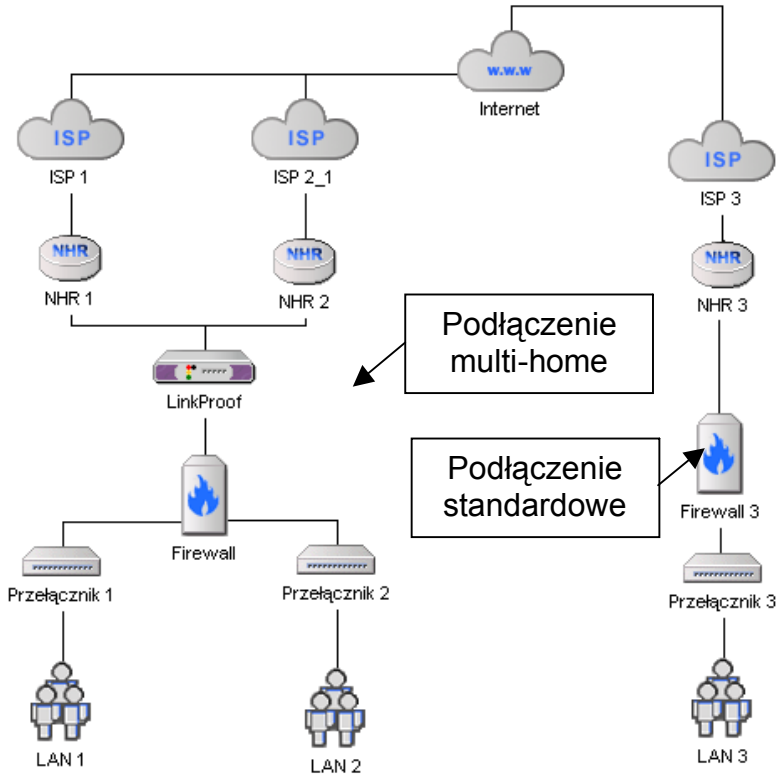
Efektywne wykorzystanie i ochrona łączy przed awariami

- na przykładzie praktycznej konfiguracji LinkProof

Ciągły rozwój usług dostępnych poprzez sieć komputerową wewnątrz korporacyjną czy też Internet lub jakąkolwiek inną sieć komputerową, pociąga za sobą rosnące wykorzystanie tych usług i integracje z codzienną pracą. Dotychczas stosowane rozwiązania zapewniające dostęp do sieci rozległej lub po prostu do zdalnej lokalizacji były i nadal często są realizowane w postaci pojedynczego połączenia. Rozwiązanie takie jest zapewne efektywne pod względem kosztów, ale nie zapewnia bezpieczeństwa wymaganego w przypadku rozwiązań biznesowych.

Ciągłe wykorzystywanie aplikacji łączących się do zdalnych lokalizacji wymusza zapewnienie odpowiedniego poziomu dostępności łącza jak również uniezależnienia od pojedynczego dostawcy zapewniającego podłączenie do np. Internetu. Lokalizacje posiadające więcej niż jedno podłączenie do Internetu są określane jako *multi-home*. Aby zapewnić prawidłową obsługę i wykorzystanie możliwości *multi-home* konieczne jest użycie rozwiązań, które dzięki zastosowanej technologii i rozwiązaniom potrafią kompleksowo obsłużyć ruch zarówno przychodzący jak i wychodzący.



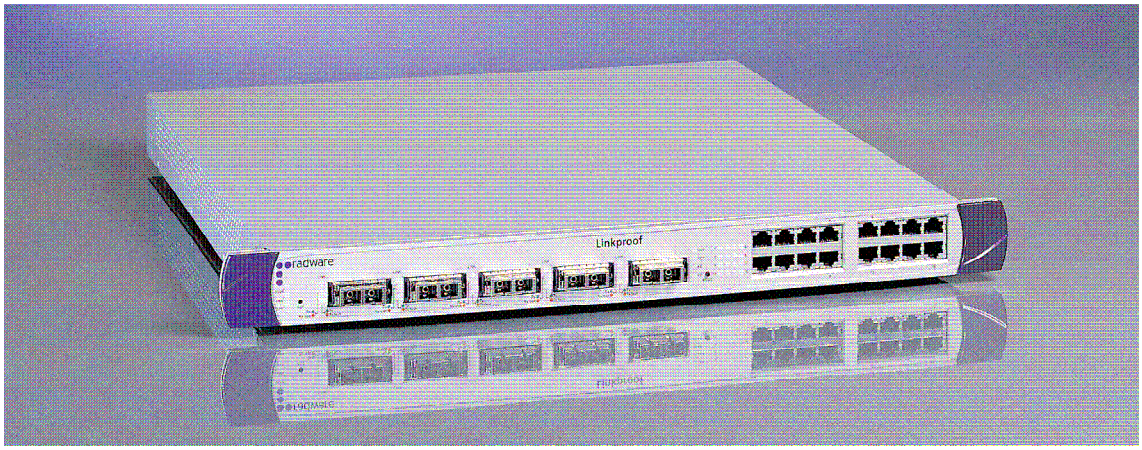
Rozwiązania podłączeń do sieci: typowe podłączenie oraz podłączenie klasy multi-home z wykorzystaniem dedykowanego urządzenia

Decydując się na wprowadzenie rozwiązania klasy *multi-home* należy pamiętać o tym, iż istnieje kilka problemów, których nie da się uniknąć. Pierwszym i najważniejszym są komplikacje związane ze schematem adresacji IP, które są spotykane w instalacjach *multi-home*.

Najczęściej przyjmowanym rozwiązaniem jest przyporządkowanie przez każdego dostawcę własnej, indywidualnej klasy adresów IP, przypisanej przez *Ripe* do operatora. Jednakże rozwiązanie takie powoduje, iż sieć wewnętrzna będzie musiała mieć przyporządkowane dwa różne zakresy adresów IP. Dodatkowo również istnieje kłopotliwa kwestia, jakiego użyć adresu źródłowego wysyłając ruch do Internetu. Problematyczne jest również zapewnienie równoważenia obciążenia łącz.

Drugim rozwiązaniem jest przyporządkowanie do sieci wewnętrznej, pojedynczej klasy adresów IP niezależnej od operatorów, od których wykupywane są łącza. Takie rozwiązanie wymaga jednak współpracy pomiędzy operatorami, dokonania i utrzymywania odpowiednich wpisów na *AS'ach* operatorów w celu zapewnienia wykorzystania dostępnych łącz. Rozwiązanie takie pociąga za sobą konieczność pokrywania kosztów utrzymywania takich wpisów, co z kolei generuje ciągłe koszty operacyjne. Również nie wszyscy dostawcy są chętni do realizacji takiej usługi.

Do obsługi ruchu w lokalizacjach posiadających dwa i więcej łącz do Internetu lub innej sieci powinno się używać dedykowanych urządzeń. Firma Radware posiada w swojej ofercie LinkProof, który jest dedykowany do takich zastosowań, posiada zestaw funkcji umożliwiający kompleksową obsługę sieci typu *multi-home*.



Radware LinkProof

Radware LinkProof eliminuje praktycznie wszystkie problemy związane z wykorzystaniem dwóch lub większej ilości łącz do Internetu lub innej zdalnej lokalizacji, a także pozwala zmaksymalizować korzyści wynikające z rozwiązania klasy *multi-home*. LinkProof zapewnia następujące korzyści dla podłączeń *multi-home*:

- inteligentnie zarządza zakresami adresów przypisanymi przez różnych dostawców,
- zapewnia optymalne wykorzystanie wszystkich dostępnych łącz dzięki inteligentnemu balansowaniu obciążeniem zarówno ruchu

wchodzącego jak i wychodzącego na dostępne łącza, jednocześnie zarządzając zakresami adresów IP ruchu wychodzącego,

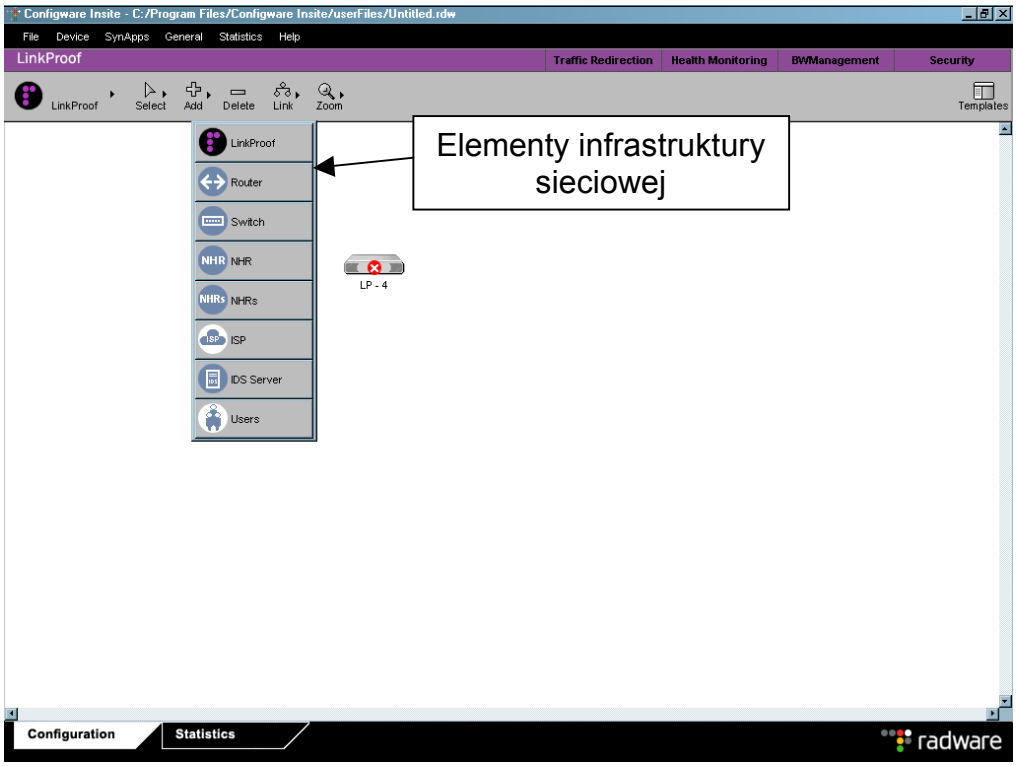
- LinkProof wyszukuje i wykorzystuje optymalną ścieżkę, którą osiągalna jest zdalna lokalizacja zarówno dla ruchu wchodzącego jak i wychodzącego,
- wykorzystywane jest zawsze najefektywniejsze łącze zapewniając tym samym maksymalne wykorzystanie inwestowanych w łącza środków finansowych

LinkProof został zaprojektowany z myślą o prostej instalacji i integracji w instalacjach typu *multi-home*.

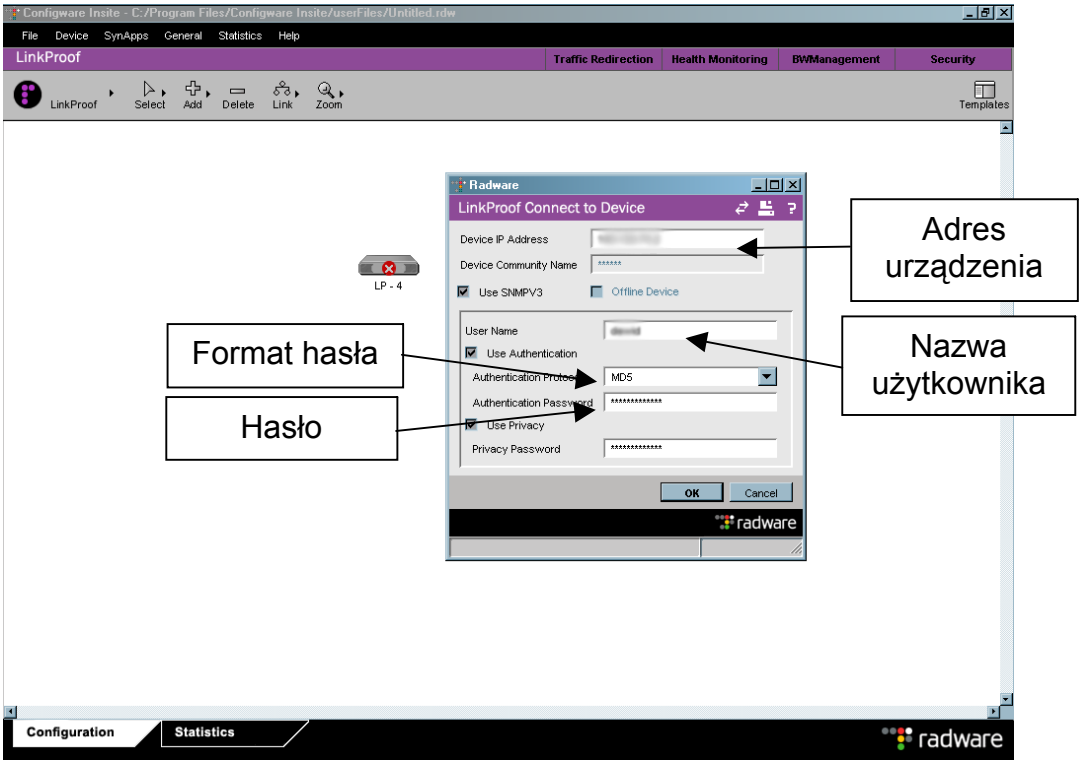
Istnieją również rozwiązania wykorzystujące protokół BGP do dystrybucji ruchu pomiędzy kilka dostępnych łącz. Jednakże rozwiązania takie są trudne we wdrożeniu i wymagają ciągłej obsługi. LinkProof może również współpracować z rozwiązaniami opartymi o BGP. LinkProof nie bazuje na statycznych wagach łącz, a sprawdza w czasie rzeczywistym obciążenie łącz i czas odpowiedzi w celu określenia, które z łącz zapewnia największą wydajność.

Konfiguracja LinkProof

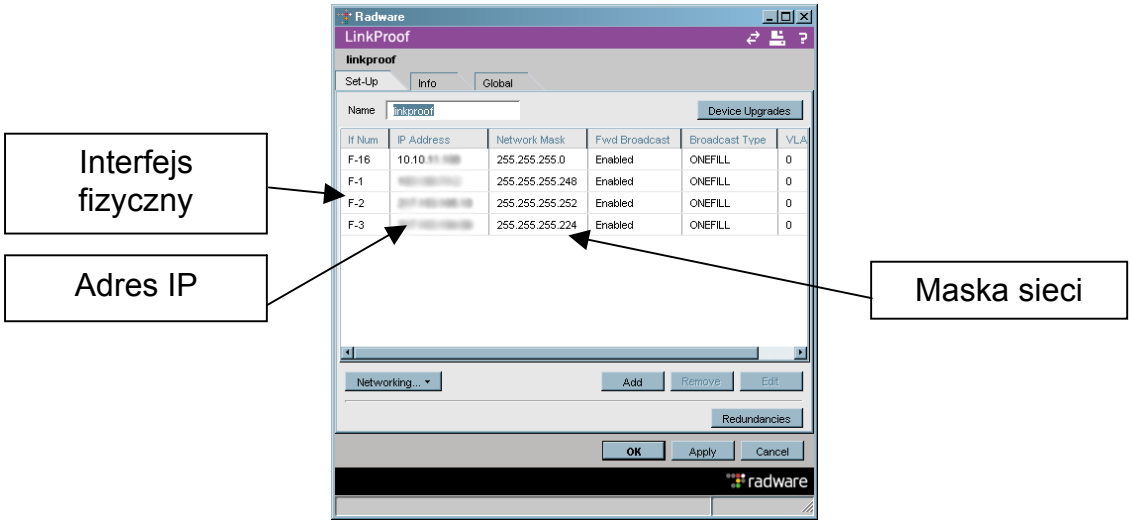
Po instalacji i uruchomieniu urządzenia w jego miejscu pracy. Instalujemy oprogramowania zarządzającego ConfigWare. Po instalacji, uruchamiamy Configware Insite i dodajemy urządzenie, tworząc tym samym odwzorowanie infrastruktury sieciowej.



W kolejnym kroku podłączamy się do urządzenia z użyciem protokołu np. SNMPv3 podając adres IP, nazwę użytkownika i niezbędne hasło (w formacie MD5 lub SHA1).

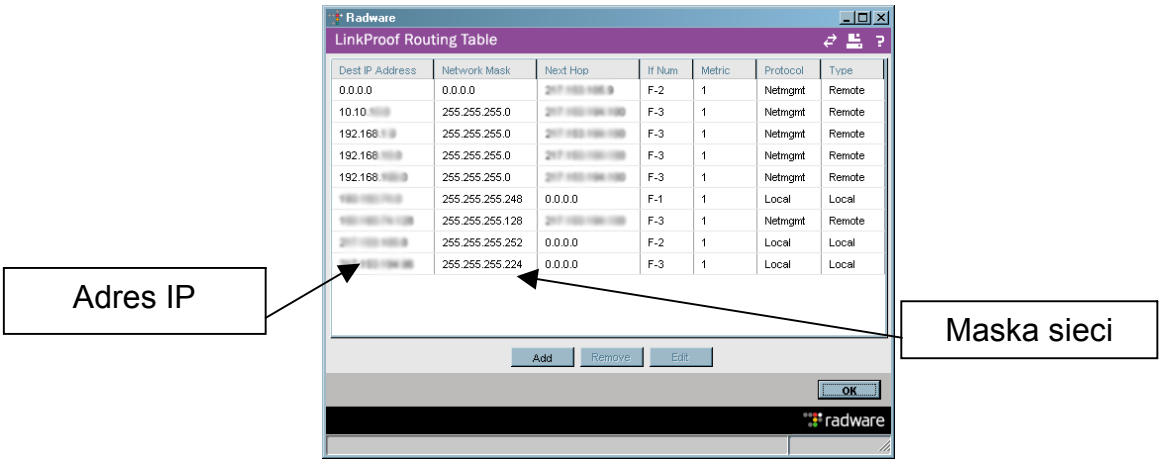


Po podłączeniu do urządzenia konieczne jest ustawienie adresacji IP na interfejsach. Dokonujemy tego wybierając pozycję **SetUp** z menu podręcznego urządzenia lub z menu **Device**

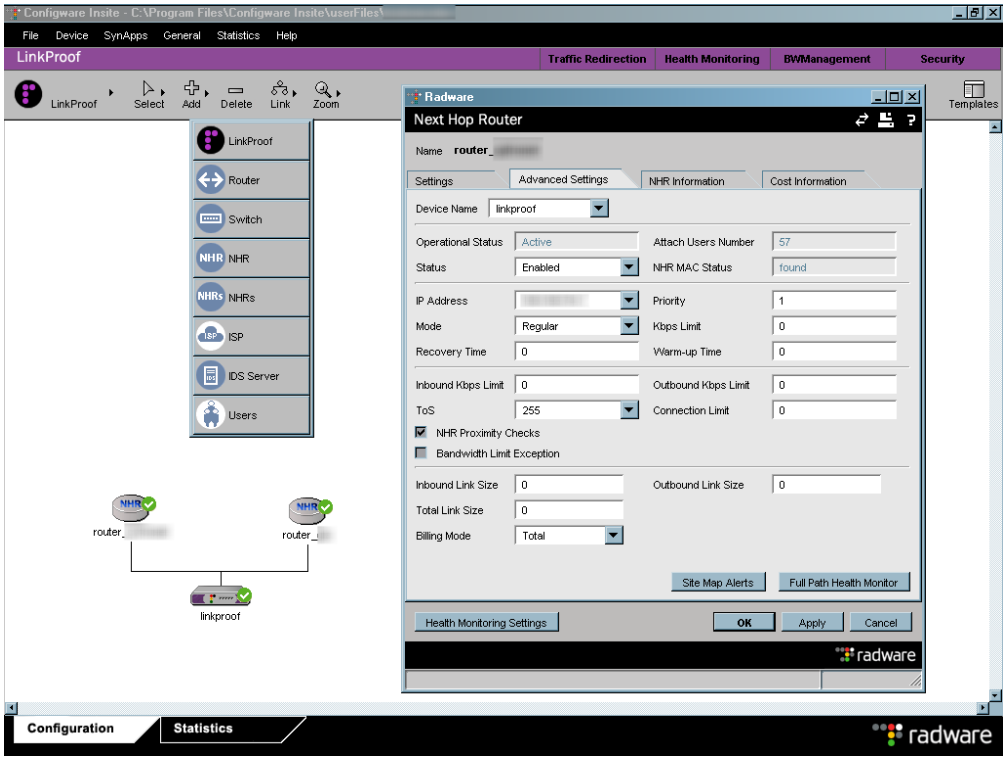


Następnie trzeba ustawić niezbędne wpisy w tablicy routingu. Obligatoryjne jest ustawienie dla każdego router'a do którego ma być równoważony ruch, wpisu *default route*. Jednakże w tablicy routingu widoczny jest zawsze tylko jeden wpis

default route. Jeśli zachodzi taka konieczność można również dodać ustawienia tras, które nie wynikają z ustawionych adresów IP na interfejsach – routing statyczny.



Do osiągnięcia kompletnej konfiguracji i prawidłowej wizualizacji konieczne jest jeszcze dodanie i opisanie routerów, których obciążenie będzie równoważone i przez które będziemy mieli dostęp do Internetu (tzw. *NHR*[1]).

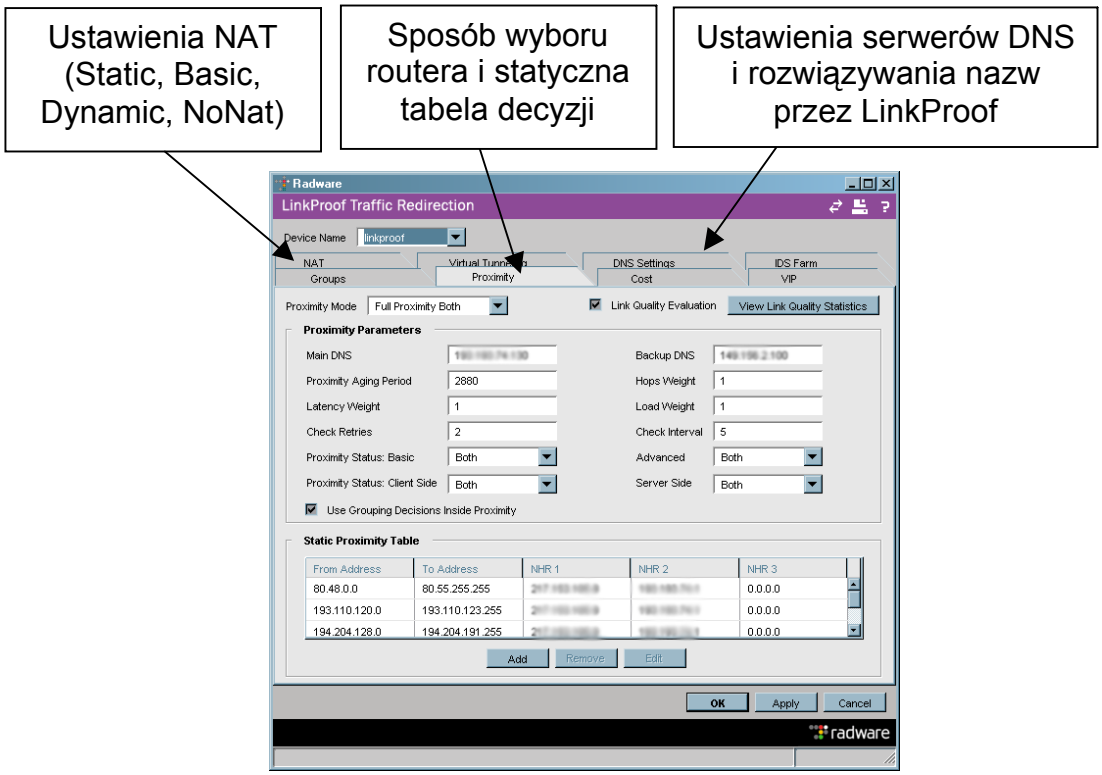


Dodanie *NHR* jest analogiczne do dodania urządzenia i odbywa się poprzez wybranie przycisku *Add* i wybór odpowiedniej pozycji z listy rozwijalnej. Po umieszczeniu *NHR* na schemacie konieczne jest jeszcze ich połączenie z *LinkProof*. W tym celu zaznaczamy elementy (*NHR i LinkProof*) i wybieramy z paska narzędziowego *Link*. Po tej operacji zostaniemy poproszeni o uzupełnienie niezbędnych informacji. Wraz z uzupełnianiem schematu i uzupełnianiem informacji

[1] NHR – Next Hop Router

o elementach, są dokonywane odpowiednie wpisy w konfiguracji *LinkProof*. Jak więc widać Konfiguracja urządzenia jest przeprowadzana w bardzo przystępny sposób wraz z tworzeniem czytelnego i przejrzystego odwzorowania infrastruktury.

Aby urządzenie mogło poprawnie realizować swoje funkcje konieczne jest ustawienie parametrów sterowania ruchem, tj. przekierowania ruchu do najlepszego router'a, ustawienia NAT, serwerów DNS i rozwiązywania nazw przez LinkProof. Ustawienia to możemy modyfikować wybierając *Traffic Redirection* z menu podręcznego lub z podmenu *Synapps*.



W zakładce **Proximity**, ustawiamy tryb pracy, jeden spośród: *No Proximity, Static Proximity, Full Proximity Inbound, Full Proximity Outbound, Full proximityBoth*. Najczęściej wybierana pozycja to *Full Proximity Both*, która zapewnia obsługę i sterowanie ruchem wchodzącym i wychodzącym. Istotnym elementem jest również *Static Proximity Table*, w której można zdefiniować statyczną kolejność wyboru, przez który router ma być przesyłany ruch dla określonych zakresów adresów IP.

Zakładka **NAT** zawiera tabele ma podstawie, której LinkProof dokonuje translacji adresów w sposób statyczny i dynamiczny, a także istnieje możliwość zdefiniowania zakresów adresów IP, które nie będą poddawane translacji przy przesyłaniu ruchu przez określony router.

Zdefiniowanie sposobu, w jaki ma być wykonywana translacja adresów jest bardzo prosta, gdyż w przystępny sposób podajemy zakres adresów źródłowych, docelowych i router. Adresy są zmieniane na podstawie tej tabeli w oparciu o router, którym ruch jest przesyłany.

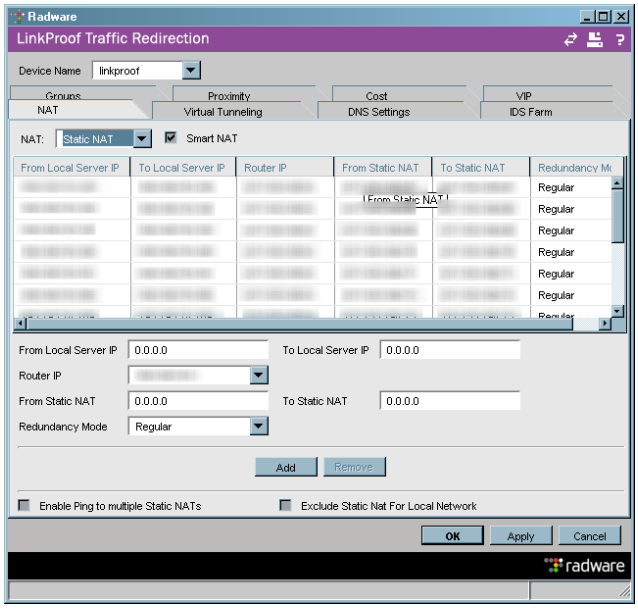
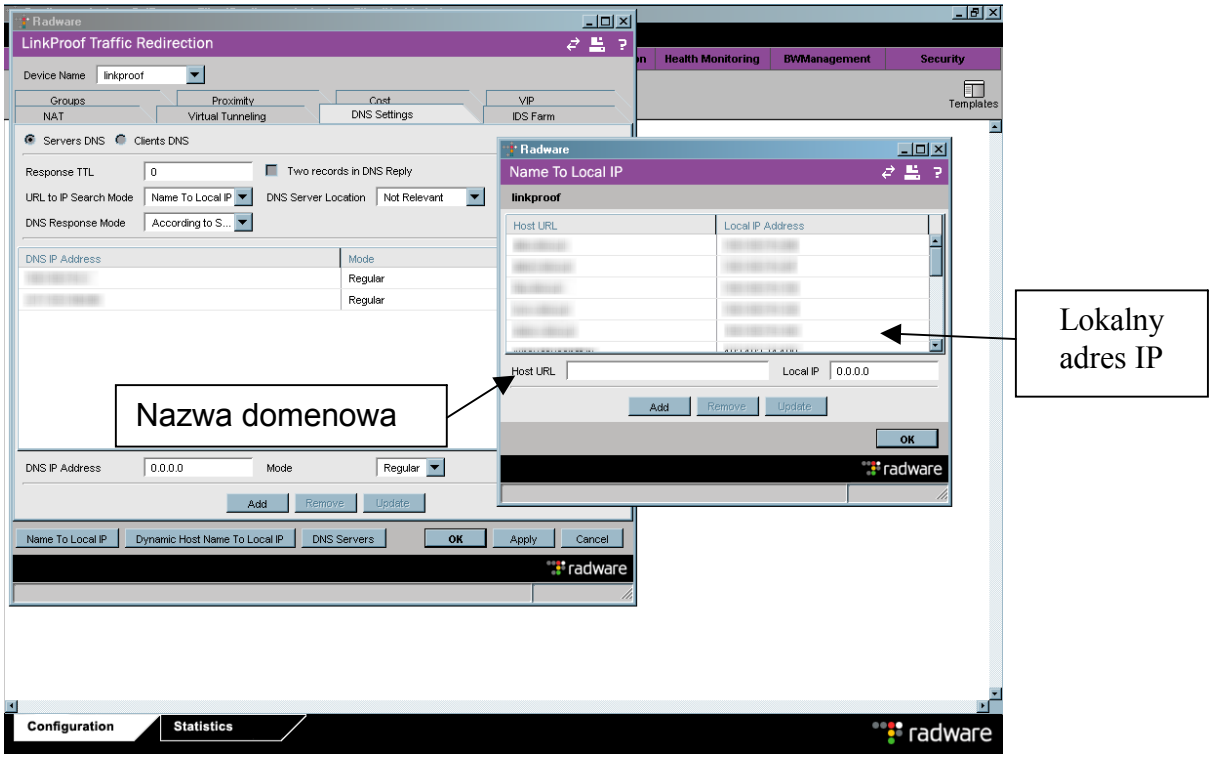


Tabela *No Nat* jest użyteczna w przypadku gdy za urządzeniem LinkProof jest np. sieć z adresami publicznymi z zakresu przyporządkowanego do jednego z routerów i jednocześnie komputery te mają być dostępne również z adresów publicznych z zakresu przyporządkowanego do innego router'a podłączonego do LinkProof. W takim przypadku definiujemy odpowiednie wpisy w tabeli *No Nat* i *Static Nat*.

LinkProof w celu zapewnienia równoważenia ruchu może również rozwiązywać nazwy hostów na adresy IP (rekordy *IN A*). Mechanizm ten umożliwia urządzeniu równoważenie ruchu pomiędzy podłączonymi łączami, wybierając optymalne łącze zgodnie z ustawieniami *Proximity*. Oczywiście istnieje również możliwość statycznego zdefiniowania łącza, którym ma zostać przesłany ruch do zdalnej lokalizacji. Do zdefiniowania parametrów związanych z serwerami DNS używanymi w sieci służy zakładka **DNS Settings**. Możemy tutaj ustawić parametry tj. czas ważności odpowiedzi (*TTL*), sposób odpowiedzi na zapytania DNS (jeden lub dwa adresy IP), rodzaj adresów zwracanych w odpowiedzi (lokalny adres IP, adres IP, na który jest translowany dany host lub też automatyczny wybór zgodnie z trybem *SmartNAT*). Zdefiniowanie listy nazw, które są rozwiązywane na określone adresy IP odbywa się w oknie *Name To Local IP*. Podawane tam są nazwy domenowe komputerów i adresy IP, które są osiągalne z *LinkProof*. Urządzenie przy odpowiedzi na zapytanie z zewnątrz, samo decyduje, jakim adresem odpowiedzieć zgodnie ze wcześniej ustawionym rodzajem adresu (lokalny, translowany, na podstawie *SmartNat*). Zazwyczaj używanym rodzajem odpowiedzi jest odpowiedź na podstawie *SmartNat*, gdyż zapewnia automatyczny wybór adresu IP, jaki jest zwracany na podstawie tabel translowania adresów i optymalnego router'a przez który będzie przesyłany ruch.



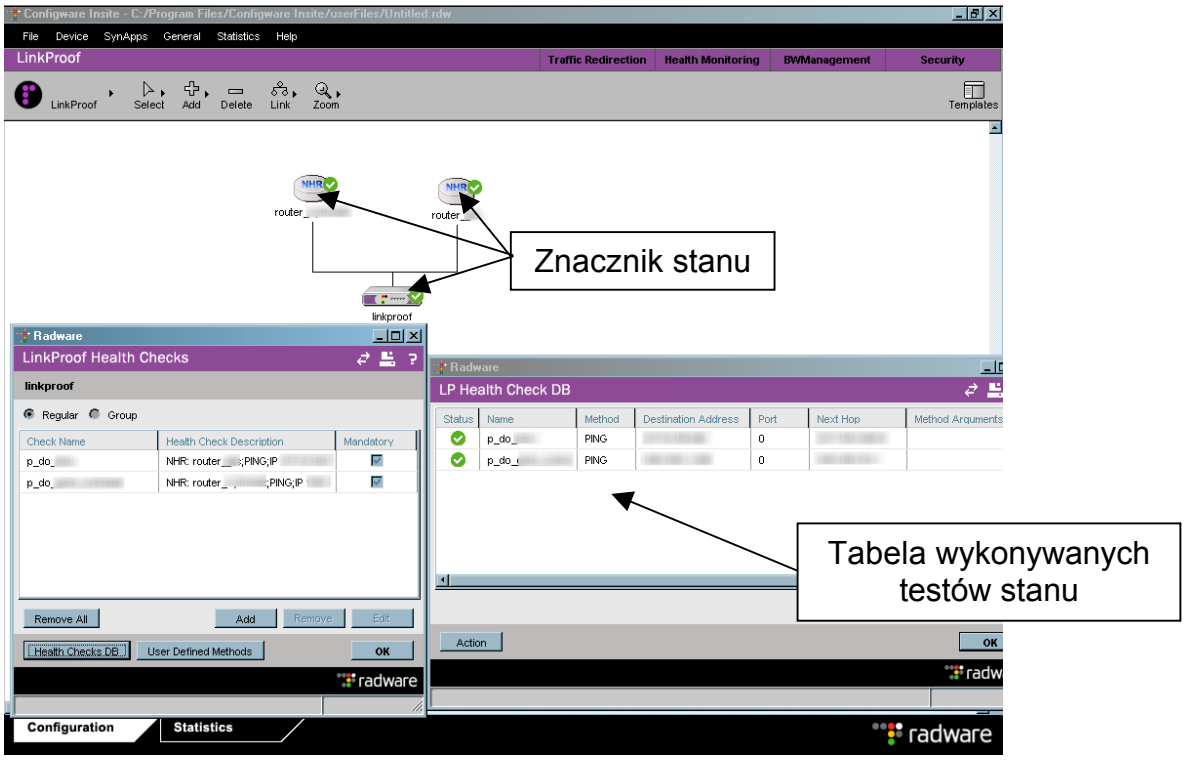
Zakładka **IDS Farms** służy do zdefiniowania urządzeń IDS, których obciążenie będzie równoważone i jednocześnie zostanie zapewnione to, iż do określonego urządzenia trafi cała sesja ruchu umożliwiają dwukierunkowe skanowanie ruchu.

Zastosowania operatorskie mogą wymagać zdefiniowania również kosztów związanych z kierowaniem ruchu przez określone łącza. Do tego celu służy zakładka **Cost**, w której możemy określić koszt przesyłanego ruchu z dokładnością do 10Kbps, 100Kbps i 1000Kbps.

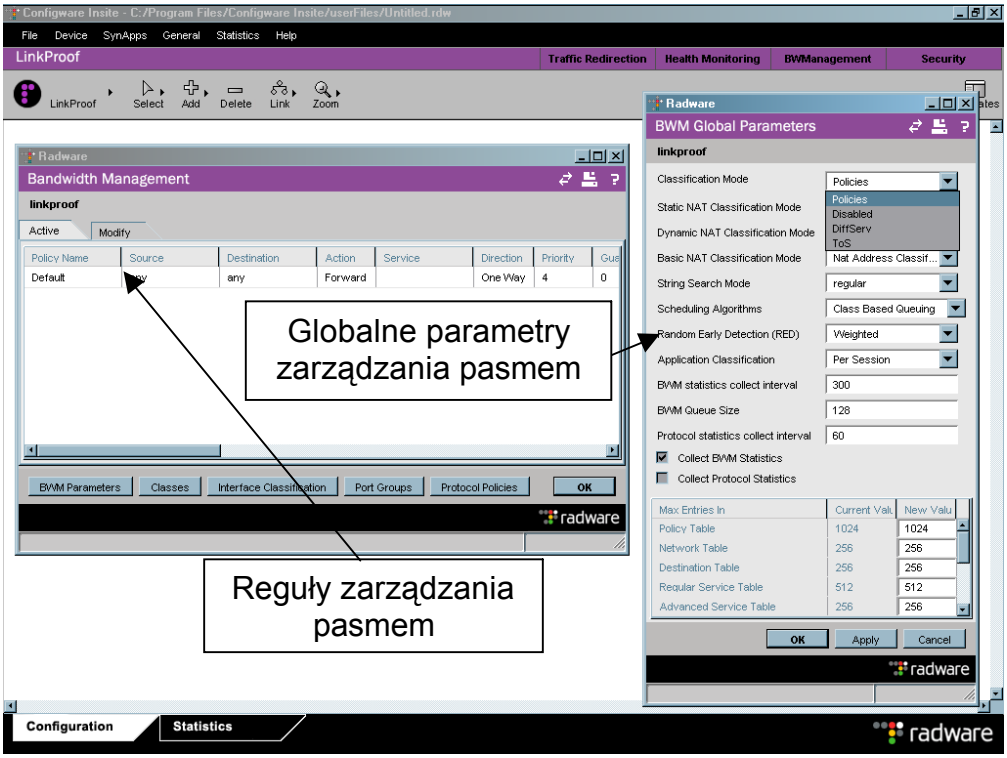
Istnieje również możliwość określenia, przez który router ma być przesyłany ruch określonego typu bazując na adresie źródłowym, docelowym a także aplikacji w oparciu o numer portu, np. http, https, dns, etc. Ustawienia te definiujemy w zakładce **Grouping**.

Kolejnym rozwiązaniem zastosowanym w LinkProof zapewniającym kompleksową obsługę jest monitorowanie stanu i dostępności łącz. Aby dodać i odpowiednio skonfigurować przeprowadzane testy wybieramy **HealthMonitoring** z menu podręcznego lub z menu *Synapps*. Sprawdzenie dostępności łącza może być wykonywane używając protokołu *ICMP* (echo request/reply), a także na wiele innych sposobów tj. arp, dns, ftp, http, imap4, ldap, nntp, pop3, Radius, rtsp, smtp, snmp, https, ssl hello, tcp port, udp port. Każda z metod charakteryzuje się innymi parametrami, ale w przypadku ogólnym sprowadza się do sprawdzenia dostępności hosta lub określonej usługi i poprawnego funkcjonowania usługi czy też hosta. Dzięki obecności takiego mechanizmu możliwe jest kompleksowe sprawdzenie funkcjonowania określonego łącza na całej drodze transmisji, a nie tylko biorąc pod uwagę najbliższy router dostępowy. Stwierdzenie, iż określony test nie spełnił wymogów (np. host nie odpowiedział na *icmp echo request*) umożliwia zapewnienie pełnej dostępności dostępu do sieci poprzez kierowanie ruchy pozostałymi, funkcjonującymi łączami i nie branie określonego router'a przy podejmowaniu decyzji o wyborze router'a. Zaraz po stwierdzeniu, iż określone łącze jest ponownie

dostępne, łącze będzie brane pod uwagę przy decyzji, którędy ma być transferowany określony ruch.

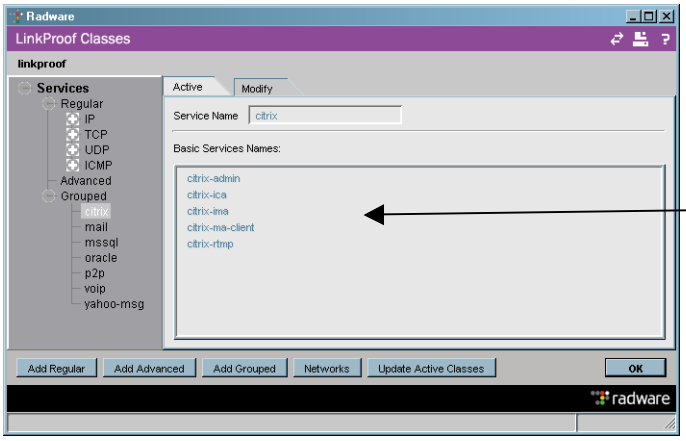


Stan monitorowanych elementów jest również przedstawiany online w ConfigWare Insite przy użyciu zrozumiałych symboli graficznych, dzięki czemu administrator ma stały podgląd aktualnej sytuacji.



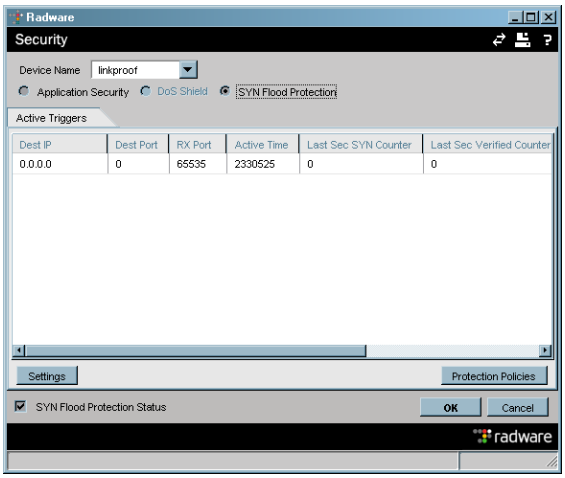
LinkProof może również zarządzać pasmem, gwarantując określony priorytet dla ruchu, który tego wymaga. Konfigurację parametrów związanych z zarządzaniem pasmem dokonujemy po wybraniu **Bandwidth Management** z menu podręcznego lub z menu *Synapps*.

Klasyfikacja ruchu może się odbywać na podstawie zdefiniowanych reguł podstawowych, zaawansowanych i grupach reguł opartych na wcześniej zdefiniowanych regułach. Dodawanie kolejnych klas i ich parametrów jest proste i przejrzyste, dzięki czemu modyfikacja parametrów jest prosta i przejrzysta.



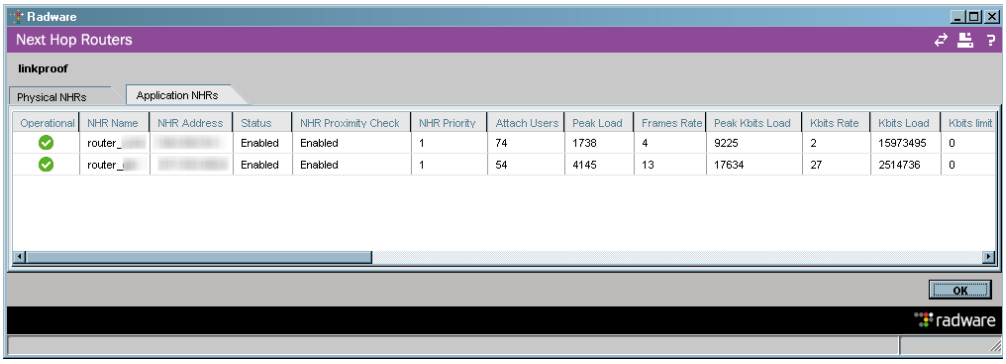
Reguły podstawowe na których oparta jest reguła grupowa

LinkProof może również być użyty do ochrony przed atakami DoS, SYN Flood. Konfiguracji tych zabezpieczeń dokonujemy po wybraniu **Security** z menu podręcznego lub z menu Synapps. Możliwość aktywacji zabezpieczeń zależy od typu zakupionej licencji.

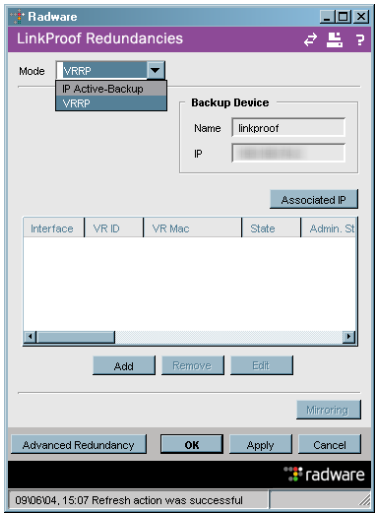


Radware oferuje w ramach wykupionej subskrypcji automatyczne uaktualnienia sygnatur ataków. Uaktualnienia mogą być wykonywane zgodnie z ustawionym harmonogramem.

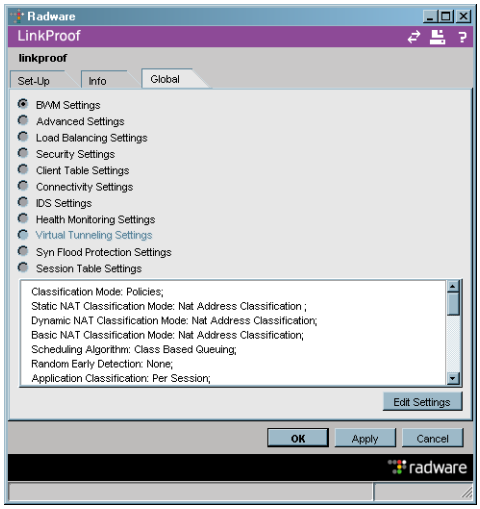
Podgląd wszystkich istotnych parametrów związanych z router'ami jest dostępny przez **Next Hop Routers** z menu podręcznego. Prezentowane informacje to stan router'a, jego nawa, adres IP, ilość sesji obsługiwanych przez router a także informacje dotyczące aktualnego jak i największego obciążenia router'a. Okno to umożliwia szybki wgląd w wiele interesujących szczegółów, które mogą wpływać na całokształt funkcjonowania łącz.



Istnieje także możliwość konfiguracji dwóch urządzeń LinkProof w taki sposób, iż eliminowany jest *Single Point of failure*. Urządzenia mogą pracować w trybie *IP Active-Backup* a także *VRRP*. Dostęp do konfiguracji tych parametrów jest możliwy po wyborze **Redundancy** z menu podręcznego.

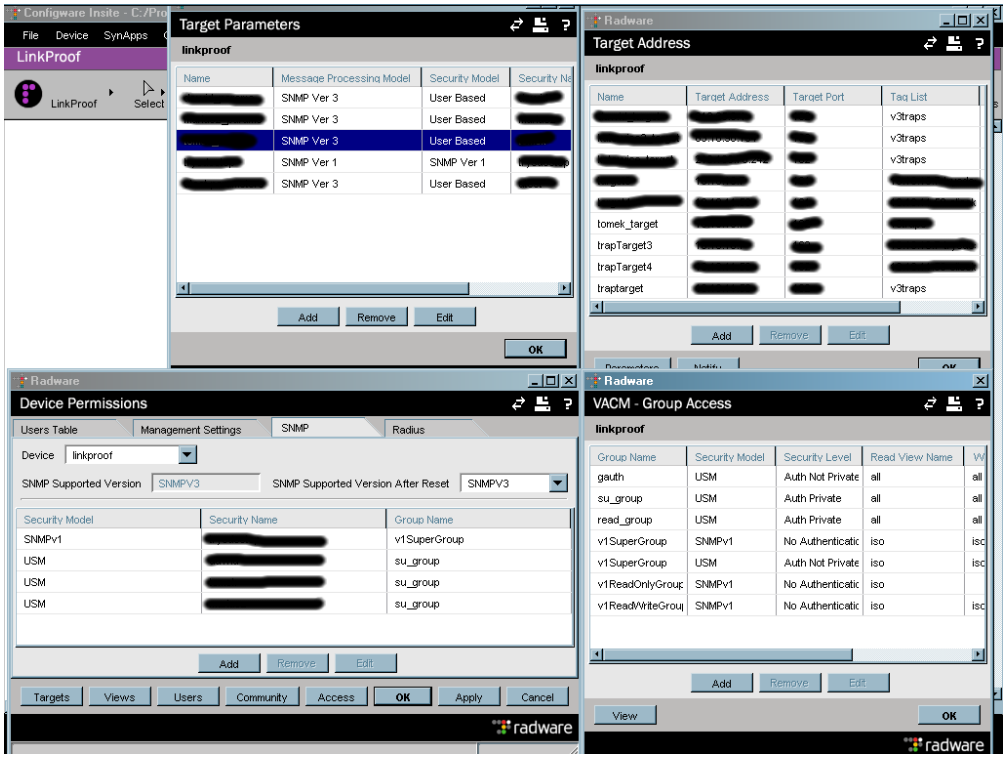


Istnieje również możliwość dokładnej kontroli nad wszystkimi aspektami pracy *LinkProof*. Aby zmienić lub sprawdzić zaawansowane ustawienia, wybieramy pozycję **SetUp** z menu podręcznego i zakładkę **Global**.



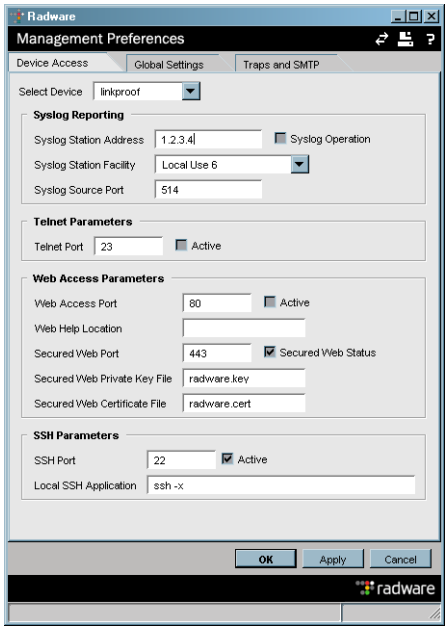
Konfiguracja dostępu do zarządzania

Konfiguracja dostępu do urządzenia jest wykonywana przez pozycję **Device Permissions** w menu *General*. Dostęp do urządzenia może być ograniczony w razie potrzeby do określonej liczby użytkowników, identyfikowanych przez nazwę i hasło. Dostęp do zarządzania urządzeniem może zostać ograniczony również jedynie do określonych fizycznych portów urządzenia, które mogą być różne w przypadku różnych protokołów dostępu do zarządzania tj. telnet, ssh, snmp, http, https. Użytkownicy mogą mieć dostęp tylko do odczytu konfiguracji lub też mieć możliwość zmian w konfiguracji.



Uwierzytelnianie użytkowników może być również realizowane w oparciu o Radius.

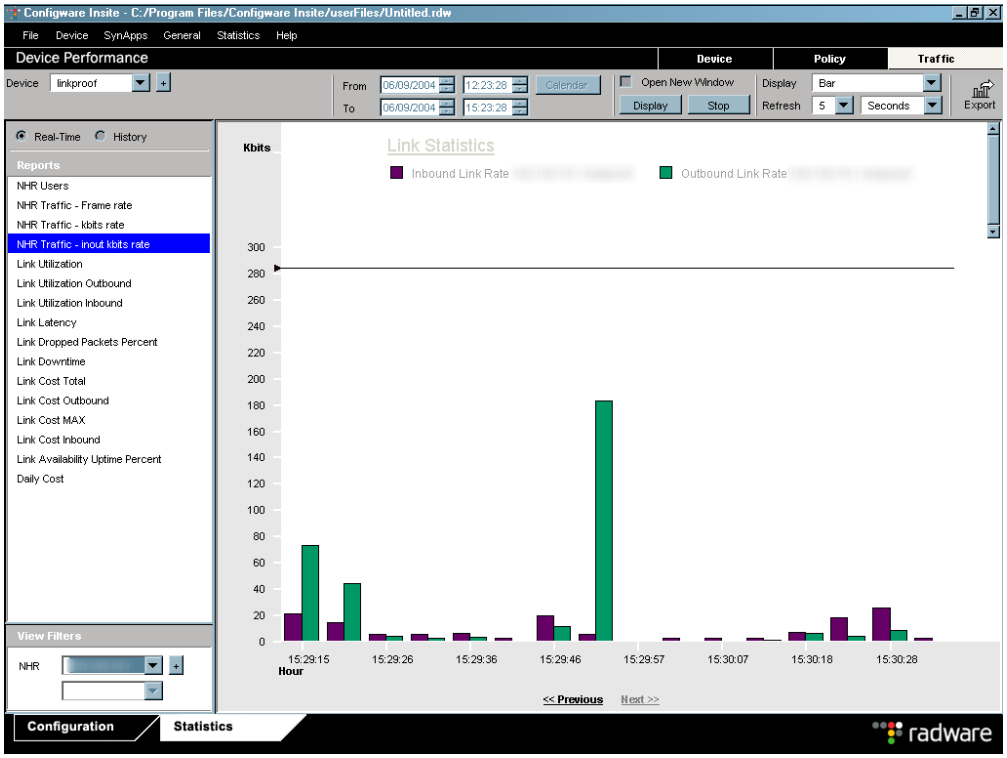
Istnieje także możliwość zmiany portów na różne od standardowych, na których urządzenie nasłuchuje, a także wyłączenie dostępu przez określony protokół. Dostęp do tych ustawień jest możliwy przez pozycję **Preferences** w menu *General*.



LinkProof ma również możliwość ustawienia adresu i portu serwera *Syslog*. Rozwiązanie takie umożliwia gromadzenie danych na dedykowanym do tego serwerze.

Monitorowanie parametrów

ConfigWare Insite zapewnia również możliwość gromadzenia statystyk jak i podglądu w czasie rzeczywistym wielu istotnych informacji w postaci wykresów. Wykresy są podzielone na trzy główne grupy: *Device, Policy, Traffic*. W każdej z grup zdefiniowane są domyślne raporty, niemniej jednak istnieje możliwość zdefiniowania własnych raportów na których mogą być wykonywane takie same operacje jak na raportach standardowych. Raporty definiują parametry jakie są pobierane z urządzenia i następnie wyświetlane w postaci wykresów w *ConfigWare Insite* w zakładce **Statistics**. Poniżej przedstawione są przykładowe wykresy generowane w czasie rzeczywistym.



Istnieje również możliwość otwarcia większej ilości wykresów jednocześnie, dzięki czemu można jednocześnie śledzić różne parametry pracy w dowolnie skomponowanym układzie i wielkości wykresów.