Załącznik nr 8 do SIWZ

UMOWA
(wzór)

Zawarta w dniu ……. 2008 roku w Łodzi pomiędzy:

Łódzkim Oddziałem Wojewódzkim Narodowego Funduszu Zdrowia
z siedzibą w Łodzi, przy ul. Kopcińskiego 58,
reprezentowanym przez:
Pawła Paczkowskiego – Dyrektora
zwanym dalej **Zamawiającym**,
a
……
z siedzibą w ……..,
reprezentowaną przez:
……
wpisaną do …….
zwaną dalej **Wykonawcą,**

wybranym w wyniku postępowania o udzielenie zamówienia publicznego nr ZP/ŁOW NFZ/7/2008 prowadzonego w trybie przetargu nieograniczonego na podstawie przepisów ustawy Prawo zamówień publicznych z dnia 29 stycznia 2004 r. (Dz.U. z 2007 r., Nr 223, poz. 1655 z późn. zm.) o następującej treści:

§ 1
Definicje

Podsystem – to urządzenia i oprogramowanie dostarczone, skonfigurowane i uruchomione w ramach przedmiotu umowy.

Awaria – to taki stan podsystemu, który uniemożliwia wykonywanie podstawowych jego funkcji, nawet po zastosowaniu procedury awaryjnej.

§ 2
Przedmiot umowy

1. Przedmiotem zamówienia jest modernizacja infrastruktury sieciowej Łódzkiego Oddziału Wojewódzkiego Narodowego Funduszu Zdrowia w Łodzi.
2. Szczegółowy zakres zamówienia określa opis przedmiotu zamówienia stanowiący integralny załącznik nr 1 do Specyfikacji Istotnych Warunków Zamówienia, jak i niniejszej umowy.

§ 3
Zasady dostawy i odbioru przedmiotu zamówienia

1. Zamówienie Wykonawca zrealizuje w siedzibie Zamawiającego w terminie 60 dni, licząc od dnia podpisania niniejszej umowy.
2. Odbiór przedmiotu zamówienia odbywał się będzie w miejscu i terminie określonym w ust. 1, z udziałem upoważnionego przedstawiciela Zamawiającego oraz Wykonawcy i polegać będzie na sprawdzeniu zgodności realizowanego zamówienia z treścią opisu przedmiotu zamówienia określonego w załączniku nr 1do niniejszej umowy i treścią oferty Wykonawcy z dnia ……. r.
3. Po zakończeniu procedury odbioru określonej w ust. 2 upoważnieni przedstawiciele stron sporządzą i podpiszą protokół odbioru, w ilości po jednym egzemplarzu dla każdej ze stron.
4. Ewentualne zastrzeżenia Zamawiającego w odniesieniu do zgodności realizowanego zamówienia z opisem przedmiotu zamówienia, określonego w załączniku nr 1 do niniejszej umowy, zostaną odnotowane przez upoważnionego przedstawiciela Zamawiającego w treści protokołu. Wniesienie uzasadnionych zastrzeżeń przez Zamawiającego skutkować będzie odmową podpisania ostatecznego protokołu odbioru.
5. Protokół odbioru sporządzony i podpisany na zasadach określonych w ust. 3 stanowi podstawę do wystawienia faktury za wykonanie niniejszego zamówienia.

6. Realizacja zamówienia odbywała się będzie w dni robocze w godz.: 8:00-16:00, po uprzednim uzgodnieniu z koordynatorem Zamawiającego. W przypadkach uzasadnionych i po wcześniejszym uzgodnieniu z koordynatorem Zamawiającego uruchomienie może odbywać się poza w/w terminami.
7. Czynności modernizacyjne nie mogą powodować zakłóceń w pracy sieci Zamawiającego w godz.: 8:00-16:00 od poniedziałku do piątku.
8. Wykonawca przekaże Zamawiającemu wszelkie niezbędne do właściwego korzystania instrukcje i certyfikaty w języku polskim.
9. Serwis gwarancyjny Wykonawca sprawował będzie zgodnie z opisem przedmiotu zamówienia i swoją ofertą.
10. Wykonawca na dostarczony sprzęt komputerowy przekaże karty gwarancyjne o ile są one wymagane w celu realizacji zobowiązań gwarancyjnych.
11. Osobą odpowiedzialną za wykonanie postanowień niniejszej umowy ze strony Wykonawcy jest…… tel. ……..
12. Osobą odpowiedzialną za wykonanie postanowień niniejszej umowy ze strony Zamawiającego jest…… tel. ……..

§ 4

Zasady płatności

1. Zamawiający zapłaci Wykonawcy za wykonanie przedmiotu umowy wynagrodzenie w wysokości ……PLN (słownie: ……zł.), w tym podatek VAT na kwotę: ……. PLN.
2. Wynagrodzenie będzie płatne na podstawie prawidłowo wystawionej faktury VAT w terminie 30 dni od daty jej doręczenia Zamawiającemu w formie przelewu na konto wskazane na niej przez Wykonawcę.
3. Podstawę opłaty faktury stanowi ostateczny protokół odbioru sporządzony i podpisany na zasadach określonych w § 3 niniejszej umowy.
4. Za dzień zapłaty uważany będzie dzień obciążenia rachunku bankowego Zamawiającego.

§ 5

Kary umowne i gwarancje

1. Za opóźnienie w zapłacie wynagrodzenia Wykonawca ma prawo naliczyć odsetki ustawowe za okres od dnia wymagalności do dnia zapłaty.
2. Za opóźnienia w realizacji przedmiotu zamówienia Zamawiający naliczy karę umowną w wysokości 0,1% wartości przedmiotu zamówienia netto za każdy dzień opóźnienia.
3. Za pełne lub częściowe odstąpienie od umowy przez Wykonawcę z przyczyn, za które odpowiedzialność ponosi Wykonawca, zapłaci on Zamawiającemu karę w wysokości 10% wartości przedmiotu zamówienia netto.
4. Odstąpienie od umowy powinno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia i powinno zawierać uzasadnienie.
5. Strony mogą odstąpić od naliczania kar umownych w przypadku wystąpienia okoliczności obiektywnych wykluczających zawinienie.
6. Strony mogą dochodzić odszkodowania uzupełniającego w zakresie nie pokrytych karami umownymi strat na drodze postępowania sądowego.
7. Tytułem zapewnienia należytego wykonania umowy Wykonawca wniesie zabezpieczenie należytego wykonania umowy w wysokości 10% wartości przedmiotu zamówienia brutto podanej w ofercie Wykonawcy z dnia …… r., tj. ……PLN.
8. Zamawiający zwróci zabezpieczenie w terminie 30 dniu od dnia wykonania zamówienia i uznania przez Zamawiającego za należycie wykonane.
9. Wszelkie naprawy gwarancyjne powinny odbywać się na miejscu bez dodatkowych opłat za transport i dojazd.

§ 6

Usuwanie awarii

Po stwierdzeniu Awarii podsystemu, działanie Wykonawcy będzie przebiegało następująco:

1. Na wskazany adres poczty elektronicznej Wykonawcy zostanie przesłany Formularz Zgłoszenia, który stanowi załącznik nr 2 do niniejszej umowy.

2. Wykonawca w ciągu 1 godziny potwierdza przyjęcie Zgłoszenia poprzez odesłanie podpisanego formularza. Czas, w którym obowiązuje powyższy termin dotyczy ustawowych dni roboczych w godzinach 8-17. Poza wymienionymi wyżej okresami bieg czasu na potwierdzenie zostaje wstrzymany.
3. Wykonawca, na podstawie danych zawartych w Formularzu Zgłoszenia, dokonuje wstępnej oceny Awarii i jej przyczyn oraz niezwłocznie przystępuje do jej usunięcia poprzez wizytę w miejscu Awarii odpowiedniego specjalisty lub podjęcie pracy w sposób zdalny. Jeśli w wyniku oceny specjalisty przyczyną jest wada sprzętu dostarczonego w ramach umowy, niezwłocznie przekazuje tą informację Zamawiającemu, który powiadamia serwis producenta, w pozostałych przypadkach Awaria zostanie usunięta w ciągu 48 godzin od momentu Zgłoszenia.
4. Wykonawca zapewnia wsparcie w zakresie uzgodnień z serwisem producenta w celu koordynacji wspólnych działań mających na celu usunięcie Awarii.
5. Wykonawca nie odpowiada za termin usunięcia wady sprzętu przez producenta poza terminem wynikającym z gwarantowanego przez producenta standardowego czasu naprawy w ramach dostarczonego podsystemu, w związku z tym czas od zgłoszenia wady sprzętu do jego usunięcia przez serwis producenta nie wlicza się do gwarantowanego 48 godzinnego czasu usunięcia Awarii.
6. Po zakończeniu działań wykonywanych przez autoryzowany serwis producenta, wykonawca w ciągu 48 godzin od daty naprawy sprzętu, dokona rekonfiguracji urządzeń w taki sposób, aby została przywrócona funkcjonalność podsystemu będącego przedmiotem umowy.
7. Osobą upoważnioną do przesyłania zgłoszeń serwisowych po stronie Zamawiającego jest …… ……. .
8. W przypadku nie dotrzymania terminu naprawy Wykonawca zapewni sprzęt zastępczy (równoważny sprzętowi naprawianemu).
9. W okresie pogwarancyjnym Wykonawca zapewni możliwość odpłatnej (zgodnie z jego aktualnym cennikiem) naprawy urządzenia i zapewni materiały eksploatacyjne.

§ 7

Ochrona tajemnicy przedsiębiorstwa

1. Strony zobowiązują się do utrzymania w tajemnicy i nie przekazywania osobom trzecim informacji o warunkach niniejszej umowy oraz wszelkich danych o przedsiębiorstwie drugiej ze stron, jak również o jego klientach , na zasadach określonych w ustawie o zwalczaniu nieuczciwej konkurencji i o ochronie danych osobowych, o ile informacje takie nie są powszechnie znane lub strona nie uzyskała uprzednio pisemnej zgody drugiej ze stron.
2. Zakaz udostępnienia określonych informacji nie dotyczy informacji wynikających z obowiązujących przepisów prawa.

§ 8

Postanowienia końcowe

1. Wszelkie oświadczenia, zawiadomienia oraz zgłoszenia dokonywane przez strony, a wynikające z postanowień niniejszej umowy winny być dokonywane w formie pisemnej. Zawiadomienia i oświadczenia dokonane w innej formie nie wywołują skutków prawnych ani faktycznych.
2. Załącznik nr 1 oraz załącznik nr 2 stanowią integralną część niniejszej umowy.
3. Jeżeli przy realizacji niniejszej umowy okaże się, że jej klauzule nie obejmują problemów, które przy podpisaniu umowy były niemożliwe lub trudne do przewidzenia, wtedy strony zobowiązują się je rozwiązać ze wzajemną przychylnością, w drodze negocjacji i kompromisów.
4. Wszelkie spory wynikające z niniejszej umowy strony oddają pod rozstrzygnięcie Sądu właściwego dla Zamawiającego rzeczowo i miejscowo.
5. W sprawach nieuregulowanych niniejszą umową stosuje się przepisy Kodeksu Cywilnego i ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych.
6. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, w tym dwa dla Zamawiającego i jeden dla Wykonawcy.

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 1 do umowy

Opis przedmiotu zamówienia

1.1 Dwie sztuki przełączników do obsługi rdzenia sieci ŁOW NFZ

Minimalne wymagania, które powinny spełniać urządzenia:

1. Urządzenie musi mieć budowę modularną.
2. Urządzenie musi mieć możliwość montażu w szafie RACK 19", wysokość nie większą niż 12RU.
3. Urządzenie musi posiadać co najmniej 6 slotów na karty zarządzające oraz karty liniowe.
4. Urządzenie musi posiadać redundantne zasilacze o mocy nie mniejszej niż 4000 W każdy, awaria wyłączenie jednego z nich nie powinna powodować przerwy w pracy urządzenia.
5. Urządzenie musi być wyposażone w kartę zarządzającą o wydajności co najmniej 32 Gbps i przepustowości minimum 15 mpps wyposażoną w minimum 2 porty 10 Gigabit Ethernet definiowane przez moduły XENPAK lub równoważne (wymagane dostarczenie dwóch modułów 10GBASE-SR).
6. Urządzenie musi zapewniać możliwość zdublowania karty zarządzającej – w przypadku rozbudowy o drugą kartę przełączenie przy awarii nie może przekroczyć 2s; awaria jednej karty zarządzającej nie może powodować degradacji wydajności urządzenia.
7. Urządzenie musi posiadać minimum 512 MB pamięci DRAM oraz 256 MB pamięci Flash.
8. Oprócz portów wbudowanych w moduł zarządzający urządzenie musi być wyposażone w co najmniej:
   a. 48 portów Gigabit Ethernet 10/100/1000 RJ-45.
   b. 8 portów Gigabit Ethernet definiowanych przez moduły GBIC (wymagane dostarczenie dwóch modułów 1000BASE-SX).
9. Urządzenie musi współpracować natywnie z systemem Cisco Security MARS (Monitoring, Analysis and ResponseSystem) wykorzystywanym w sieci Zamawiającego do monitorowania zdarzeń i ich korelacji oraz aktywne wsparcie dla wszelkich mechanizmów bezpieczeństwa.
10. Urządzenie musi współpracować natywnie z systemem Cisco Works LMS wykorzystywanym w sieci Zamawiającego.
11. W ramach funkcjonalności oprogramowania urządzenie musi zapewniać:
    a. Obsługę minimum 4096 VLAN-ów 802.1Q.
    b. Obsługę protokołu Spanning Tree zgodnie ze standardami 802.1D, 802.1w, 802.1s,
    c. Możliwość grupowania portów zgodnie ze specyfikacją 802.3ad (LACP).
    d. Wykrywanie łączy jednokierunkowych (UDLD).
    e. Funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym.
    f. Obsługę routingu IP statycznego i dynamicznego (RIP, OSPF, BGP 4).
    g. Obsługę IPv6.
    h. Obsługę ruchu multicast (PIM, IGMPv3, IGMP snooping),
    i. Mechanizmy redundancji bramy (HSRP, VRRP lub równoważne, GLBP),
    j. Obsługę mechanizmów bezpieczeństwa w warstwach 2 - 7 (rozpoznawanie aplikacji na podstawie wzorców warstwy 7, 802.1x, DHCP snooping, dynamiczna inspekcja ARP, listy kontroli dostępu, kontrola ruchu broadcast, filtrowanie MAC per port / per VLAN, port security,)
    k. Możliwość zarządzania ruchem (QoS – klasyfikacja ruchu na podstawie rozpoznawania aplikacji, adresów, portów, oznaczeń TOS, IP Precedence, DSCP itp., kolejkowanie z obsługą kolejki priorytetowej, statyczne i dynamiczne ograniczanie pasma, RSVP),
    l. Obsługę mechanizmów bezpieczeństwa w warstwach 2 - 7 (rozpoznawanie aplikacji na podstawie wzorców warstwy 7, 802.1x, DHCP snooping, dynamiczna inspekcja ARP, listy kontroli dostępu, kontrola ruchu broadcast, filtrowanie MAC per port / per VLAN, port security,)
    m. Sprzętową obsługę tuneli GRE
    n. Możliwość wysyłania statystyk ruchu zgodnie z netFlow, J-Flow, S-Flow lub równoważnym.
    o. Możliwość lokalnej obserwacji ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu.

p. Możliwość zdalnej obserwacji ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN.
q. zarządzanie przez Telnet, konsolę szeregową, SNMPv3, SSHv2, RMON,
r. możliwość autoryzacji dostępu do przełącznika w oparciu o mechanizmy AAA.
s. możliwość zmiany konfiguracji „w locie", bez konieczności restartu urządzenia (dotyczy dowolnych zmian konfiguracji),
t. możliwość zapisu konfiguracji w pliku tekstowym i jej importu/eksportu za pomocą protokołu FTP lub TFTP,
u. obsługa mechanizmów bezpieczeństwa w warstwach 2 - 7 (rozpoznawanie aplikacji na podstawie wzorców warstwy 7, 802.1x, DHCP snooping, dynamiczna inspekcja ARP, listy kontroli dostępu, kontrola ruchu broadcast, filtrowanie MAC per port / per VLAN, port security,)
v. możliwość wysyłania statystyk ruchu zgodnie z netFlow, J-Flow, S-Flow lub równoważnym – w przypadku utraty połączenia z serwerem zbierającym statystyki wymagane jest lokalne cache'owanie min. 100 000 wpisów,

12. Urządzenie musi być objęte minimum 12 miesięczną gwarancją. Zgłoszenia awarii muszą być przyjmowane między godziną 8 - 16, od poniedziałku do piątku, wymiana sprzętu realizowana musi być następnego dnia roboczego po zdiagnozowaniu awarii.

1.2 Dwie sztuki przełączników warstwy serwerowej

Minimalne wymagania, które powinny spełniać urządzenia:

1. Przełącznik o zamkniętej konfiguracji, posiadający 48 portów Gigabit Ethernet 10/100/1000 RJ-45 oraz 2 gniazda typu X2 pozwalające na instalację wkładek z portami 10 Gigabit Ethernet: 10GBASE-CX4, 10GBASE-ER, 10GBASE-SR, 10GBASE-LX4, 10GBASE-LR (wymagane dostarczenie dwóch modułów 10GBASE-SR).
2. Przełącznik musi mieć możliwość montażu w szafie RACK 19", wysokość nie większą niż 1RU.
3. Przełącznik musi posiadać co najmniej 256 MB pamięci DRAM oraz 64 MB pamięci Flash.
4. Przełącznik musi posiadać matrycę przełączającą o szybkości min. 136 Gbps (wszystkie porty muszą mieć możliwość pracy z pełną szybkością – wirespeed) i wydajnością przełączania na poziomie min. 102 mpps (L 2/3/4, realizowane sprzętowo).
5. Przełącznik musi zapewniać obsługę 55.000 adresów MAC, 32.000 tras w tablicy routingu oraz 2048 sieci VLAN.
6. Przełącznik musi posiadać redundantny wewnętrzny zasilacz.
7. Przełącznik musi być wyposażony w moduł wentylatorów wymienianych na gorąco (hot-plug).
8. Przełącznik musi zapewniać przełączanie w warstwie drugiej, trzeciej i czwartej.
9. Przełącznik musi w standardowej wersji oprogramowania umożliwiać przełączanie w warstwie trzeciej oraz definiowanie routingu w oparciu o protokoły RIPv1v2 oraz routing statyczny .
10. Przełącznik musi posiadać możliwość rozszerzenia funkcjonalności routingu o obsługę protokołów OSPF ,BGPv4, IS-IS poprzez wymianę oprogramowania.
11. Przełącznik musi zapewniać podstawową obsługę ruchu IP Multicast, w tym funkcjonalność IGMP oraz IGMP Snooping.
12. Przełącznik musi posiadać możliwość rozszerzenia funkcjonalności IP Multicast o obsługę protokołów PIM Sparse oraz PIM Dense poprzez wymianę oprogramowania.
13. Przełącznik musi zapewniać obsługę mechanizmów redundancji bramy (VRRP, HSRP lub równoważne).
14. Przełącznik musi zapewniać wykrywanie łączy jednokierunkowych (UDLD).
15. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. IEEE 802.1s Rapid Spanning Tree.
    b. IEEE 802.1w Multi-Instance Spanning Tree.
    c. Możliwość grupowania portów zgodnie ze specyfikacją IEEE 802.3ad (LACP).
16. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.

b. Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Round Robin lub podobnego dla obsługi tych kolejek.
c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).
d. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.

17. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    a. Wiele poziomów dostępu administracyjnego poprzez konsolę.
    b. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1x oraz EAP.
    c. Możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2.
    d. Funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym.
18. Przełącznik musi współpracować natywnie z systemem Cisco Security MARS (Monitoring, Analysis and ResponseSystem) wykorzystywanym w sieci Zamawiającego do monitorowania zdarzeń i ich korelacji.
19. Urządzenie musi współpracować natywnie z systemem Cisco Works LMS wykorzystywanym w sieci Zamawiającego.
20. Przełącznik powinien umożliwiać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu.
21. Przełącznik powinien umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN.
22. Przełącznik powinien mieć możliwość synchronizacji zegara czasu za pomocą protokołu NTP.
23. Przełącznik powinien posiadać możliwość połączenia z innymi przełącznikami tego samego typu w klaster zapewniający możliwość zarządzania za pomocą pojedynczego adresu IP.
24. Urządzenie powinno umożliwiać zarządzania poprzez interfejs CLI (konsolę).
25. Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) powinien być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 4 plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
26. Urządzenie musi być objęte minimum 12 miesięczną gwarancją. Zgłoszenia awarii muszą być przyjmowane między godzinami 8-16, od poniedziałku do piątku, wymiana sprzętu realizowana musi być następnego dnia roboczego po zdiagnozowaniu awarii.

1.3 Sześć sztuk przełączników warstwy przyłączeniowej

Minimalne wymagania, które powinny spełniać urządzenia:

1. Przełącznik o zamkniętej konfiguracji, posiadający 48 portów Fast Ethernet 10/100 Base-T oraz 4 gniazda typu SFP pozwalające na instalację wkładek z portami Gigabit Ethernet 1000BASE-T, 1000BASE-SX, 1000BASE-ZX, 1000BASE LX/LH.
2. Przełącznik musi mieć możliwość montażu w szafie RACK 19”, wysokość nie większą niż 1RU.
3. Przełącznik musi posiadać co najmniej 128 MB pamięci DRAM oraz 16 MB pamięci Flash.
4. Dostępne w przełączniku gniazda SFP powinny umożliwiać instalację modułów dla zwielokrotnionej transmisji optycznej CDWM.
5. Przełącznik musi posiadać wydajność przełączania przynajmniej 13 Mpps dla 64-bajtowych pakietów.
6. Przełącznik musi zapewniać obsługę 12,000 adresów MAC, 11,000 tras w tablicy routingu oraz 1024 sieci VLAN.
7. Przełącznik musi zapewniać zasilanie Power over Ethernet na portach 10/100Base T, zgodnie ze standardem IEEE 802.3af.
8. Przełącznik musi współpracować z modułem redundantnego zewnętrznego zasilacza.
9. Przełącznik musi zapewniać przełączanie w warstwie drugiej,

10. Przełącznik musi w standardowej wersji oprogramowania umożliwiać przełączanie w warstwie trzeciej oraz definiowanie routingu w oparciu o protokoły RIPv1v2 oraz routing statyczny .
11. Przełącznik musi posiadać możliwość rozszerzenia funkcjonalności routingu o obsługę protokołów OSPF i BGPv4, poprzez wymianę oprogramowania.
12. Przełącznik musi zapewniać podstawową obsługę ruchu IP Multicast, w tym funkcjonalność IGMP oraz IGMP Snooping.
13. Przełącznik musi posiadać możliwość rozszerzenia funkcjonalności IP Multicast o obsługę protokołów PIM Sparse oraz PIM Dense, poprzez wymianę oprogramowania.
14. Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP: DHCP Server oraz DHCP Relay.
15. Przełącznik musi zapewniać wykrywanie łączy jednokierunkowych (UDLD).
16. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. IEEE 802.1s Rapid Spanning Tree.
    b. IEEE 802.1w Multi-Instance Spanning Tree.
    c. Możliwość grupowania portów zgodnie ze specyfikacją IEEE 802.3ad (LACP).
17. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.
    b. Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Round Robin lub podobnego dla obsługi tych kolejek.
    c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).
    d. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
    e. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting). Dla portu FastEthernet 10/100 wymagana możliwość skonfigurowania co najmniej 64 różnych ograniczeń, każde odpowiednio dla różnej klasy obsługi ruchu
18. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    a. Wiele poziomów dostępu administracyjnego poprzez konsolę.
    b. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1x oraz EAP.
    c. Możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2.
    d. Funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym.
19. Przełącznik musi współpracować natywnie z systemem Cisco Security MARS (Monitoring, Analysis and ResponseSystem) wykorzystywanym w sieci Zamawiającego do monitorowania zdarzeń i ich korelacji.
20. Urządzenie musi współpracować natywnie z systemem Cisco Works LMS wykorzystywanym w sieci Zamawiającego.
21. Przełącznik powinien umożliwiać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu.
22. Przełącznik powinien umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN.
23. Przełącznik powinien mieć możliwość synchronizacji zegara czasu za pomocą protokołu NTP.
24. Przełącznik powinien posiadać możliwość połączenia z innymi przełącznikami tego samego typu w klaster zapewniający możliwość zarządzania za pomocą pojedynczego adresu IP
25. Urządzenie powinno umożliwiać zarządzania poprzez interfejs CLI (konsolę).
26. Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) powinien być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 4 plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
27. Urządzenie powinno posiadać wbudowany zasilacz umożliwiający zasilanie prądem przemiennym 230 V.

28. Urządzenie powinno mieć możliwość podłączenia redundantnego zewnętrznego zasilania
29. Urządzenie musi być objęte minimum 12 miesięczną gwarancją. Zgłoszenia awarii muszą być przyjmowane między godzinami 8-16, od poniedziałku do piątku, wymiana sprzętu realizowana musi być następnego dnia roboczego po zdiagnozowaniu awarii.

Razem z przełącznikami należy dostarczyć:

a. cztery moduły 1000BASE-T.
b. dwa moduły 1000BASE-SX.
c. okablowanie o długości 50 cm, niezbędne do połączenia 4 przełączników w jeden stos oraz 2 przełączników w drugi stos.

2.1 Dwie sztuki routerów modularnych w konfiguracji 1

Minimalne wymagania, które powinny spełniać urządzenia:

Architektura

1. Powinno być urządzeniem modularnym posiadającym możliwość instalacji co najmniej:
   a. 2 modułów sieciowych z interfejsami lub modułów Voice over IP.
   b. 4 kart sieciowych z interfejsami lub kart Voice over IP.
   c. 2 modułów funkcyjnych.
   d. 4 modułów z układami DSP.
   lub 12 modułów ogólnego przeznaczenia.
2. Powinno posiadać wszystkie interfejsy „aktywne". Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów.
3. Powinno być wyposażone w co najmniej dwa interfejsy GigabitEthernet 10/100/1000 RJ-45, w tym jeden typu „combo" – z możliwością obsadzenia portu światłowodowego definiowanego przez GBIC lub SFP. Dopuszczalne jest zastosowanie urządzenia z portem definiowanym przez moduł SFP lub GBIC niezależnym od interfejsów RJ-45.
4. Sloty urządzenia przewidziane pod rozbudowę o dodatkowy moduł sieciowy powinny mieć możliwość obsadzenia modułami:
   a. Z portami szeregowymi – o gęstości co najmniej 4 porty na moduł.
   b. Ze zintegrowanymi modemami V.90 – o gęstości co najmniej 8 portów na moduł.
   c. Z interfejsami ISDN BRI (styk S/T) – o gęstości co najmniej 8 portów na moduł.
   d. Z interfejsami ISDN PRI.
   e. Z przełącznikiem Ethernet – o gęstości co najmniej 16 portów na moduł.
   f. Z interfejsem HSSI.
   g. Z interfejsem ATM OC3
   h. Z interfejsem ATM E3.
   i. Content engine o pojemności co najmniej 80 GB.
   j. Intrusion Detection System.
   k. Analizatora sieciowego.
   l. Poczty głosowej.
5. Sloty urządzenia przewidziane pod rozbudowę o dodatkową kartę sieciową powinny mieć możliwość obsadzenia kartami:
   a. Z portami szeregowymi – o gęstości co najmniej 2 porty na moduł.
   b. Ze zintegrowanym modemem V.90 – o gęstości co najmniej 2 porty na moduł.
   c. Ze zintegrowanym modemem ADSL.
   d. Ze zintegrowanym modemem SHDSL.
   e. Z interfejsem ISDN BRI (styk S/T).

f. Z przełącznikiem Ethernet – o gęstości co najmniej 4 portów na moduł.

6. Sloty urządzenia przewidziane pod rozbudowę o moduł funkcyjny powinny mieć możliwość obsadzenia modułami:
   a. Sprzętowego modułu wsparcia szyfracji.
   b. ATM IMA.
   c. Poczty głosowej.
7. Sloty urządzenia przewidziane pod rozbudowę o moduł z układami DSP powinny mieć możliwość obsadzenia modułami:
   a. O gęstości nie mniejszej niż 8 kanałów.
   b. Pozwalającymi na dynamiczne alokowanie DSP do różnych zadań (obsługa interfejsów głosowych, transcoding, conferencing) z granulacją do 1 DSP.
8. Powinno być wyposażone w zintegrowany wewnętrzny moduł sprzętowego wsparcia szyfracji DES, 3DES, AES128, AES192, AES256.
9. Powinno być wyposażone w dodatkowy wewnętrzny moduł sprzętowego wsparcia szyfracji DES, 3DES, AES128, AES192, AES256 instalowany w slocie dla modułów funkcyjnych lub w slocie uniwersalnym (dla rozwiązania z co najmniej 7 slotami na moduły).
10. Powinno posiadać minimum dwa porty dedykowane do zarządzania: port konsoli, port asynchroniczny dla podłączenia modemu.
11. Powinno posiadać minimum 2 porty USB.
12. Powinno posiadać co najmniej 64 MB pamięci FLASH i możliwość jej rozbudowy do minimum 256 MB.
13. Powinno posiadać co najmniej 256 MB pamięci DRAM i możliwość jej rozbudowy do minimum 1024 MB.

Zasilanie

1. Urządzenie powinno posiadać wbudowany zasilacz umożliwiający zasilanie prądem przemiennym 230 V.
2. Urządzenie powinno mieć możliwość podłączenia redundantnego zewnętrznego zasilania
3. Urządzenie powinno umożliwiać doprowadzenie zasilania do portów Ethernet – w modułach sieciowych dostępnych do urządzenia – bez stosowania dodatkowych zewnętrznych urządzeń (zasilacz, panele, etc.).

Oprogramowanie – funkcjonalność:

1. Powinno mieć możliwość routingu pakietów zgodnie z protokołami RIP, OSPF, BGP4, PIM.
2. Powinno wspierać Policy Based Routing.
3. Powinno wspierać protokoły HSRP lub VRRP.
4. Powinno mieć oprogramowanie z funkcjami bezpieczeństwa:
   a. Szyfrowanie połączeń 3DES oraz AES.
   b. Sondy IPS – wymagane jest wsparcie dla minimum 700 sygnatur ataków.
   c. Firewall (w trybie routed oraz transparent).
   d. Ochrona samego urządzenia (Control-Plane) przed atakami DDoS i nadużyciami.

   Funkcje opisane w tym punkcie powinny działać jednocześnie.
5. Powinno mieć możliwość uruchomienia oprogramowania współpracującego z dostępnymi systemami kontroli kondycji bezpieczeństwa hostów. Np. Network Access Protection, Network Admission Control, etc.
6. Powinno posiadać wsparcie dla protokołu IGMPv3.
7. Powinno obsługiwać funkcjonalność Network Address Translation.
8. Powinno mieć możliwość uruchomienia oprogramowania z funkcją procesowania telefonii IP (funkcja serwera zestawiającego połączenia).
9. Powinno mieć możliwość obsługi połączeń VoIP.
10. Powinno obsługiwać tzw. routing między sieciami VLAN w oparciu o 802.1Q.
11. Wydajność proponowanego urządzenia nie może być mniejsza niż 350 kpps.

Zarządzanie i konfiguracja

1. Powinno być zarządzane przez SNMP.
2. Powinno posiadać możliwość eksportu informacji przez NetFlow lub odpowiednik.
3. Powinno posiadać możliwość komunikacji z serwerami uwierzytelniania i autoryzacji za pośrednictwem protokołu RADIUS i TACACS+.
4. Powinno być konfigurowalne przez CLI oraz interfejs graficzny (oczekiwane są narzędzia dodatkowe w postaci kreatorów połączeń, etc.).

5. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych (ilość ograniczona tylko pojemnością pamięci). Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo – nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
6. Router musi współpracować natywnie z systemem Cisco Security MARS (Monitoring, Analysis and ResponseSystem) wykorzystywanym w sieci Zamawiającego do monitorowania zdarzeń i ich korelacji.
7. Router musi współpracować natywnie z systemem Cisco Works LMS wykorzystywanym w sieci Zamawiającego.

Obudowa

1. Powinna być wykonana z metalu. Ze względu na różne warunki, w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowanie plastikowej.
2. Powinna mieć możliwość montażu w szafie RACK 19".

Gwarancja

Urządzenie musi być objęte minimum 12 miesięczną gwarancją. Zgłoszenia awarii muszą być przyjmowane między godzinami 8-16, od poniedziałku do piątku, wymiana sprzętu realizowana musi być następnego dnia roboczego po zdiagnozowaniu awarii.

2.2 Jedna sztuka routera modularnego w konfiguracji 2

Minimalne wymagania, które powinny spełniać urządzenia:

Architektura

1. Powinno być urządzeniem modularnym posiadającym możliwość instalacji co najmniej:
    a. 1 modułu sieciowego z interfejsami lub modułu Voice over IP.
    b. 4 kart sieciowych z interfejsami lub kart Voice over IP.
    c. 2 modułów funkcyjnych.
    d. 2 modułów z układami DSP.

    lub 7 modułów ogólnego przeznaczenia.
2. Powinno posiadać wszystkie interfejsy „aktywne". Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów.
3. Powinno być wyposażone w co najmniej dwa interfejsy FastEthernet 10/100 RJ-45.
4. Sloty urządzenia przewidziane pod rozbudowę o dodatkowy moduł sieciowy powinny mieć możliwość obsadzenia modułami:
    a. Z portami szeregowymi – o gęstości co najmniej 4 porty na moduł.
    b. Ze zintegrowanymi modemami V.90 – o gęstości co najmniej 8 portów na moduł.
    c. Z interfejsami ISDN BRI (styk S/T) – o gęstości co najmniej 8 portów na moduł.
    d. Z przełącznikiem Ethernet – o gęstości co najmniej 16 portów na moduł.
    e. Z interfejsem HSSI.
    f. Z interfejsem ATM E3.
    g. Content engine o pojemności co najmniej 40 GB.
    h. Intrusion Detection System.
    i. Analizatora sieciowego.
    j. Poczty głosowej.
5. Sloty urządzenia przewidziane pod rozbudowę o dodatkową kartę sieciową powinny mieć możliwość obsadzenia kartami:
    a. Z portami szeregowymi – o gęstości co najmniej 2 porty na moduł.
    b. Ze zintegrowanym modemem V.90 – o gęstości co najmniej 2 porty na moduł.

c. Ze zintegrowanym modemem ADSL.
d. Ze zintegrowanym modemem SHDSL.
e. Z interfejsem ISDN BRI (styk S/T).
f. Z przełącznikiem Ethernet – o gęstości co najmniej 4 portów na moduł.

6. Sloty urządzenia przewidziane pod rozbudowę o moduł funkcyjny powinny mieć możliwość obsadzenia modułami:
    a. Sprzętowego modułu wsparcia szyfracji.
    b. ATM IMA.
    c. Poczty głosowej.
7. Sloty urządzenia przewidziane pod rozbudowę o moduł z układami DSP powinny mieć możliwość obsadzenia modułami:
    a. O gęstości nie mniejszej niż 8 kanałów.
    b. Pozwalającymi na dynamiczne alokowanie DSP do różnych zadań (obsługa interfejsów głosowych, transcoding, conferencing) z granulacją do 1 DSP.
8. Powinno być wyposażone w zintegrowany wewnętrzny moduł sprzętowego wsparcia szyfracji DES, 3DES, AES128, AES192, AES256.
9. Powinno być wyposażone w dodatkowy wewnętrzny moduł sprzętowego wsparcia szyfracji DES, 3DES, AES128, AES192, AES256 instalowany w slocie dla modułów funkcyjnych lub w slocie uniwersalnym (dla rozwiązania z co najmniej 7 slotami na moduły).
10. Powinno posiadać minimum dwa porty dedykowane do zarządzania: port konsoli, port asynchroniczny dla podłączenia modemu.
11. Powinno posiadać minimum 2 porty USB.
12. Powinno posiadać co najmniej 64 MB pamięci FLASH i możliwość jej rozbudowy do minimum 256 MB.
13. Powinno posiadać co najmniej 256 MB pamięci DRAM i możliwość jej rozbudowy do minimum 768 MB.

Zasilanie

1. Urządzenie powinno posiadać wbudowany zasilacz umożliwiający zasilanie prądem przemiennym 230 V.
2. Urządzenie powinno mieć możliwość podłączenia redundantnego zewnętrznego zasilania
3. Urządzenie powinno umożliwiać doprowadzenie zasilania do portów Ethernet – w modułach sieciowych dostępnych do urządzenia – bez stosowania dodatkowych zewnętrznych urządzeń (zasilacz, panele, etc.).
4. Urządzenie powinno mieć możliwość podłączenia zewnętrznego zasilacza redundantnego.

Oprogramowanie – funkcjonalność:

1. Powinno mieć możliwość routingu pakietów zgodnie z protokołami RIP, OSPF, BGP4, PIM.
2. Powinno wspierać Policy Based Routing.
3. Powinno wspierać protokoły HSRP lub VRRP.
4. Powinno mieć oprogramowanie z funkcjami bezpieczeństwa:
    a. Szyfrowanie połączeń 3DES oraz AES.
    b. Sondy IPS – wymagane jest wsparcie dla minimum 700 sygnatur ataków.
    c. Firewall (w trybie routed oraz transparent).
    d. Ochrona samego urządzenia (Control-Plane) przed atakami DDoS i nadużyciami.

    Funkcje opisane w tym punkcie powinny działać jednocześnie.
5. Powinno mieć możliwość uruchomienia oprogramowania współpracującego z dostępnymi systemami kontroli kondycji bezpieczeństwa hostów. Np. Network Access Protection, Network Admission Control, etc.
6. Powinno posiadać wsparcie dla protokołu IGMPv3.
7. Powinno obsługiwać funkcjonalność Network Address Translation.
8. Powinno mieć możliwość uruchomienia oprogramowania z funkcją procesowania telefonii IP (funkcja serwera zestawiającego połączenia).
9. Powinno mieć możliwość obsługi połączeń VoIP.
10. Powinno obsługiwać tzw. routing między sieciami VLAN w oparciu o 802.1Q.
11. Wydajność proponowanego urządzenia nie może być mniejsza niż 120 kpps.

Zarządzanie i konfiguracja

1. Powinno być zarządzane przez SNMP.
2. Powinno posiadać możliwość eksportu informacji przez NetFlow lub odpowiednik.

3. Powinno posiadać możliwość komunikacji z serwerami uwierzytelniania i autoryzacji za pośrednictwem protokołu RADIUS i TACACS+.
4. Powinno być konfigurowalne przez CLI oraz interfejs graficzny (oczekiwane są narzędzia dodatkowe w postaci kreatorów połączeń, etc.).
5. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych (ilość ograniczona tylko pojemnością pamięci). Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo – nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
6. Router musi współpracować z systemem Cisco Security MARS (Monitoring, Analysis and ResponseSystem) wykorzystywanym w sieci Zamawiającego do monitorowania zdarzeń i ich korelacji.
7. Urządzenie musi współpracować natywnie z systemem Cisco Works LMS wykorzystywanym w sieci Zamawiającego.

Obudowa
1. Powinna być wykonana z metalu. Ze względu na różne warunki, w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowanie plastikowej.
2. Powinna mieć możliwość montażu w szafie RACK 19".

Gwarancja
Urządzenie musi być objęte minimum 12 miesięczną gwarancją. Zgłoszenia awarii muszą być przyjmowane między godzinami 8-16, od poniedziałku do piątku, wymiana sprzętu realizowana musi być następnego dnia roboczego po zdiagnozowaniu awarii.

2.3 Trzy sztuki routerów modularnych w konfiguracji 3

Minimalne wymagania, które powinny spełniać urządzenia:

Architektura
1. Powinno być urządzeniem modularnym posiadającym możliwość instalacji co najmniej:
    a. 2 kart sieciowych z interfejsami lub kart Voice over IP.
    b. 1 modułu funkcyjnego.
    lub 3 modułów ogólnego przeznaczenia.
2. Powinno posiadać wszystkie interfejsy „aktywne". Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów.
3. Powinno być wyposażone w co najmniej dwa interfejsy FastEthernet 10/100 RJ-45.
4. Sloty urządzenia przewidziane pod rozbudowę o dodatkową kartę sieciową powinny mieć możliwość obsadzenia kartami:
    a. Z portami szeregowymi – o gęstości co najmniej 2 porty na moduł.
    b. Ze zintegrowanym modemem V.90 – o gęstości co najmniej 2 porty na moduł.
    c. Ze zintegrowanym modemem ADSL.
    d. Ze zintegrowanym modemem SHDSL.
    e. Z interfejsem ISDN BRI (styk S/T).
    f. Z przełącznikiem Ethernet – o gęstości co najmniej 4 portów na moduł.
5. Sloty urządzenia przewidziane pod rozbudowę o moduł funkcyjny powinny mieć możliwość obsadzenia modułami:
    a. Sprzętowego modułu wsparcia szyfracji.
    b. ATM IMA.
    c. Poczty głosowej.

6. Sloty urządzenia przewidziane pod rozbudowę o moduł z układami DSP powinny mieć możliwość obsadzenia modułami:
    a. O gęstości nie mniejszej niż 8 kanałów.
    b. Pozwalającymi na dynamiczne alokowanie DSP do różnych zadań (obsługa interfejsów głosowych, transcoding, conferencing) z granulacją do 1 DSP.
7. Powinno być wyposażone w zintegrowany wewnętrzny moduł sprzętowego wsparcia szyfracji DES, 3DES, AES128, AES192, AES256.
8. Powinno być wyposażone w dodatkowy wewnętrzny moduł sprzętowego wsparcia szyfracji DES, 3DES, AES128, AES192, AES256 instalowany w slocie dla modułów funkcyjnych lub w slocie uniwersalnym (dla rozwiązania z co najmniej 3 slotami na moduły).
9. Powinno posiadać minimum dwa porty dedykowane do zarządzania: port konsoli, port asynchroniczny dla podłączenia modemu.
10. Powinno posiadać minimum 2 porty USB.
11. Powinno posiadać co najmniej 64 MB pamięci FLASH i możliwość jej rozbudowy do minimum 128 MB.
12. Powinno posiadać co najmniej 256 MB pamięci DRAM i możliwość jej rozbudowy do minimum 384 MB.

Zasilanie

1. Urządzenie powinno posiadać wbudowany zasilacz umożliwiający zasilanie prądem przemiennym 230 V.

Oprogramowanie – funkcjonalność:

1. Powinno mieć możliwość routingu pakietów zgodnie z protokołami RIP, OSPF, BGP4, PIM.
2. Powinno wspierać Policy Based Routing.
3. Powinno wspierać protokoły HSRP lub VRRP.
4. Powinno mieć oprogramowanie z funkcjami bezpieczeństwa:
    a. Szyfrowanie połączeń 3DES oraz AES.
    b. Sondy IPS – wymagane jest wsparcie dla minimum 700 sygnatur ataków.
    c. Firewall (w trybie routed oraz transparent).
    d. Ochrona samego urządzenia (Control-Plane) przed atakami DDoS i nadużyciami.

    Funkcje opisane w tym punkcie powinny działać jednocześnie.
5. Powinno mieć możliwość uruchomienia oprogramowania współpracującego z dostępnymi systemami kontroli kondycji bezpieczeństwa hostów. Np. Network Access Protection, Network Admission Control, etc.
6. Powinno posiadać wsparcie dla protokołu IGMPv3.
7. Powinno obsługiwać funkcjonalność Network Address Translation.
8. Powinno mieć możliwość uruchomienia oprogramowania z funkcją procesowania telefonii IP (funkcja serwera zestawiającego połączenia).
9. Powinno mieć możliwość obsługi połączeń VoIP.
10. Powinno obsługiwać tzw. routingu między sieciami VLAN w oparciu o 802.1Q.
11. Wydajność proponowanego urządzenia nie może być mniejsza niż 75 kpps.

Zarządzanie i konfiguracja

1. Powinno być zarządzane przez SNMP.
2. Powinno posiadać możliwość eksportu informacji przez NetFlow lub odpowiednik.
3. Powinno posiadać możliwość komunikacji z serwerami uwierzytelniania i autoryzacji za pośrednictwem protokołu RADIUS i TACACS+.
4. Powinno być konfigurowalne przez CLI oraz interfejs graficzny (oczekiwane są narzędzia dodatkowe w postaci kreatorów połączeń, etc.).
5. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych (ilość ograniczona tylko pojemnością pamięci). Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo – nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
6. Router musi współpracować natywnie z systemem Cisco Security MARS (Monitoring, Analysis and ResponseSystem) wykorzystywanym w sieci Zamawiającego do monitorowania zdarzeń i ich korelacji.

7. Urządzenie musi współpracować natywnie z systemem Cisco Works LMS wykorzystywanym w sieci Zamawiającego.

Obudowa
1. Powinna być wykonana z metalu. Ze względu na różne warunki, w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowanie plastikowej.
2. Powinna mieć możliwość montażu w szafie RACK 19".

Gwarancja
Urządzenie musi być objęte minimum 12 miesięczną gwarancją. Zgłoszenia awarii muszą być przyjmowane między godzinami 8-16, od poniedziałku do piątku, wymiana sprzętu realizowana musi być następnego dnia roboczego po zdiagnozowaniu awarii.

3.1 Zestaw szaf RACK 19" 42U wraz z akcesoriami, na który muszą się składać następujące elementy:

3.1.1 Zestaw dwóch szaf typu RACK 19" o wysokości użytkowej 42U wraz z akcesoriami spełniające następujące wymagania:
a. Szerokość pojedynczej szafy: 600 mm,
b. Głęgokość pojedynczej szafy: 800 mm,
c. Wysokość pojedynczej szafy: maksymalnie 2100 mm,
d. Dopuszczalne obciążenie pojedynczej szafy: minimum 600 kg,
e. Wyposażenie pojedynczej szafy:
   - Drzwi przednie wykonane z blachy perforowanej z możliwością zmiany kierunku otwierania,
   - Drzwi tylne wykonane z blachy perforowanej z możliwością zmiany kierunku otwierania oraz demontażu,
   - Dwie osłony boczne blaszane z możliwością demontażu
   - Dach blaszany z otworami umożliwiającymi instalację przepustów kablowych oraz paneli wentylacyjnych,
   - Cokół z łącznikami perforowanymi zapewniający równomierny rozkład obciążenia na całym swym obwodzie, z możliwością zdejmowania łączników przy obciążonej szafie,
   - Listwa uziemiająca wraz z zestawem linek uziemiających do podłączenia zdejmowanych elementów szafy do listwy uziemiającej
f. Wyposażenie dodatkowe:
   - Komplet łączników do połączenia szaf,
g. Wykończenie powierzchni - szkielet, dach, osłony, drzwi, cokół malowane proszkowo w kolorze czarnym lub grafitowym.
h. Wszystkie elementy zestawu powinny pochodzić od jednego producenta.

3.1.2 Zestaw dwóch szaf typu RACK 19" o wysokości użytkowej 42U wraz z akcesoriami spełniające następujące wymagania:
a. Szerokość pojedynczej szafy: 800 mm,
b. Głęgokość pojedynczej szafy: 600 mm,
c. Wysokość pojedynczej szafy: maksymalnie 2100 mm,
d. Dopuszczalne obciążenie pojedynczej szafy: minimum 600 kg,
e. Wyposażenie pojedynczej szafy:
   - Drzwi przednie wykonane z blachy perforowanej z możliwością zmiany kierunku otwierania,
   - Drzwi tylne wykonane z blachy perforowanej z możliwością zmiany kierunku otwierania oraz demontażu,
   - Dwie osłony boczne blaszane z możliwością demontażu
   - Dach blaszany z otworami umożliwiającymi instalację przepustów kablowych oraz paneli wentylacyjnych,
   - Cokół z łącznikami perforowanymi zapewniający równomierny rozkład obciążenia na całym swym obwodzie, z możliwością zdejmowania łączników przy obciążonej szafie,

- Listwa uziemiająca wraz z zestawem linek uziemiających do podłączenia zdejmowanych elementów szafy do listwy uziemiającej

f. Wyposażenie dodatkowe:
   - Komplet łączników do połączenia szaf,

g. Wykończenie powierzchni - szkielet, dach, osłony, drzwi, cokół malowane proszkowo w kolorze czarnym lub grafitowym,
h. Wszystkie elementy zestawu powinny pochodzić od jednego producenta.

Powyższe zestawy powinny pochodzić od jednego producenta oraz posiadać jednolitą kolorystykę.

3.1.3 Miedziane kable krosowe z wtykiem RJ45 zatopionym w tworzywie stanowiącym osłonę, kategorii 5e o następujących długościach i kolorach:

Długość	Pomarańczowy (kabel krosowany)	Zielony (kabel prosty)	Niebieski (kabel prosty)	Żółty (kabel prosty)
0.5 m	5	5	30	20
1 m	5	5	20	20
2 m	5	40	170	20
3 m	5	50	20	20
5 m	5	10		10

Łącznie należy dostarczyć 465 szt.

3.1.4 Czternaście sztuk światłowodowych, wielodomowych kabli krosowych o następujących standardach złącz oraz długościach.

Światłowód krosowy, duplex MM 50/125 OM3 SC-SC, 2m	2
Światłowód krosowy, duplex MM 50/125 OM3 SC-ST, 2m	10
Światłowód krosowy, duplex MM 50/125 OM3 LC-ST, 2m	2

3.1.5 Jedna sztuka moduł GBIC wraz z już posiadanym pozwoli na dwuścieżkowe dołączenie switcha Cisco Catalyst 3500XL do rdzenia sieci.

WS-G5484	1000BASE-SX Short Wavelength GBIC (Multimode only)

Gwarancja
Wymienione wyżej elementy muszą być objęte minimum 12 miesięczną gwarancją.

Wymagania dodatkowe

1. Całość dostarczanego sprzętu musi być fabrycznie nowa, nie używana we wcześniejszych projektach. Sprzęt i oprogramowanie powinno pochodzić z autoryzowanego na Polskę kanału dystrybucyjnego producenta.
2. Ze względu na pożądaną pełną kompatybilność, cały sprzęt sieciowy dostarczany w ramach postępowania powinien pochodzić od jednego producenta; w przypadku oferowania urządzeń różnych producentów, należy dostarczyć oświadczenia ich producentów o pełnej wzajemnej kompatybilności oraz oświadczenia producentów o współpracy ich autoryzowanych placówek serwisowych w zakresie usuwania problemów powstających na styku urządzeń.
3. Zamawiający wymaga dołączenia do urządzeń dokumentacji - instrukcje obsługi w języku polskim lub angielskim (w wersji elektronicznej lub drukowanej).
4. Zamawiający wymaga, aby wszystkie prace, które mogą spowodować przestoje w pracy sieci produkcyjnej, były przeprowadzane w godzinach 16.30 – 7.30. Zamawiający dopuszcza prowadzanie prac wdrożeniowych w dni wolne od pracy po wcześniejszym uzgodnieniu terminu.

5. Zamawiający wymaga zapewnienia serwisu bezpłatnej aktualizacji dostarczonego oprogramowania (update'ów, sygnatur i innych) do najnowszej dostępnej wersji przez okres 12 miesięcy.
6. Zapewnienie samodzielnego dostępu do serwisu webowego producenta umożliwiającego:
   a. pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres 12 m-cy;
   b. dostęp do narzędzi konfiguracyjnych;
   c. dostęp do dokumentacji sprzętu i oprogramowania;
7.Do oferty należy dołączyć specyfikację zawierającą informację na temat producenta i modelu oferowanego przez Wykonawcę sprzętu oraz informację w postaci tabeli przedstawiającej parametry pożądane przez Zamawiającego oraz parametry, które posiada sprzęt oferowany przez Wykonawcę

Warunki wdrożenia i uruchomienia systemu

1.Całość systemu (rozwiązania) ma zostać zainstalowana, skonfigurowana, wdrożona i uruchomiona według uzgodnień z Zamawiającym zgodnie z jego wymaganiami i przy jego współudziale. Prace powinny obejmować następujące etapy:

a. Przeprowadzenie analizy aktualnej struktury oraz konfiguracji urządzeń sieciowych w węźle centralnym Zamawiającego,
b. Przedstawienie harmonogramu prac, zaakceptowanego przez Zamawiającego,
c. Opracowanie projektu technicznego obejmującego szczegóły implementacyjne rozwiązań, w porozumieniu z Zamawiającym.
d. Przeprowadzenia szkoleń pracowników Zamawiającego.
e. Dostawa i instalacja komponentów systemu.
f. Konfiguracja i uruchomienie urządzeń w środowisku testowym, ew. w ograniczonej grupie urządzeń.
g. Właściwa konfiguracja i uruchomienie całego systemu - przełączenia ruchu produkcyjnego na nową infrastrukturę.
h. Przeprowadzenie testów akceptacyjnych - walidacja rozwiązania (audyt konfiguracji względem opracowanego projektu implementacji) i opracowania dokumentacji powykonawczej.
i. Opracowanie dokumentacji powykonawczej i zaleceń powdrożeniowych, obejmującej:
   - procedury operacyjne dla administratorów;
   - instrukcje z zadaniami administracyjnymi;
   - procedury backupów i awaryjne (ratunkowe).

2. Zamawiający wyznaczy po swojej stronie Kierownika Projektu, który będzie koordynował wszystkie prace oraz działania wynikające z powyższego zamówienia po stronie Zamawiającego. Zamawiający wymaga by Wykonawca po swojej stronie wyznaczył osobę, która będzie pełniła nadzór nad wszystkimi pracami wdrożeniowymi.
3. W zespole wdrożeniowym będą uczestniczyć ze strony Zamawiającego administratorzy sieci i systemów.
4. W ramach wdrożenia Zamawiający wymaga zintegrowania całego środowiska z następującymi systemami i urządzeniami zamawiającego i uruchomienia ustalonych funkcjonalności :
   a. Cisco CS-MARS;
   b. Cisco PIX 515E (w konfiguracji failover);
   c. Cisco Catalyst – switche serii 3500XL;
   d. Routery Cisco serii 800 i 1800
5. Konfiguracja przełączników musi obejmować między innymi :
   a. uruchomienie funkcjonalności redundancji,
   b. konfigurację interfejsów serwerów wykorzystywanych przez Zamawiające do pracy w układzie redundantnym (3 szt działające pod kontrolą systemu IBM AIX, 4 szt działające pod kontrolą Linux, 10 szt działające pod kontrolą MS Windows 2003 Server).
   c. konfigurację VLAN'ów,
   d. konfigurację routingu pomiędzy VLAN'ami,
   e. konfigurację QoS,
6. Konfiguracja routerów musi obejmować między innymi:
   a. uruchomienie funkcjonalności redundancji,

b. konfigurację routingu,
c. konfigurację do obsługi łącza zapasowego,
d. tunelowanie GRE,
e. szyfrowanie w sieci WAN,
f. konfigurację QoS.

7. Zamawiający wymaga, aby w projekcie powykonawczym (części technicznej) całego systemu, znalazły się wszelkie składniki systemu, w tym także elementy, które były rekonfigurowane w celu poprawnej pracy całości rozwiązania.

Załącznik nr 2 do umowy

Formularz zgłoszenia awarii

Nr ewid. zgłoszenia: _____

Data zgłoszenia: _____

Godzina zgłoszenia: _____

Nr polisy serwisowej (lub) polis producenta sprzętu: _____

Potwierdzenie przyjęcia zgłosznia: Data _____ Podpis _____

Konatakty zgłaszającego:
Imię i nazwisko: _____

Telefony kontaktowe: _____

Adres e-mail: _____

Krótki opis problemu:

Podjęte działania i rezultaty:

Data	Działanie	Potwierdzenie wykonania podpis Zamawiającego	Potwierdzenie wykonania podpis Wykonawcy