KOMENDA WOJEWÓDZKA POLICJI
z siedzibą w Radomiu

Radom, dnia 21.04.2010 r.

MODYFIKACJA

dot. modernizacja i rozbudowa dostępu do sieci Internet dla jednostek organizacyjnych garnizonu mazowieckiego Policji nr sprawy 31/2010

Na podstawie art. 38 ust. 4 ustawy Prawo zamówień publicznych (Dz. U. z 2007 roku Nr 223, poz. 1655 z późn. zm) Zamawiający dokonuje zmiany treści SIWZ w następującym zakresie:

1. Zamawiający dokonuje zmiany zapisu **Wymagania dla serwera pocztowego** zawartego w punkcie 2 Opisu przedmiotu zamówienia, w następującym zakresie:
   Parametr – kontroler dysków twardych, zmieniono zapis ***„cache 256 MB lub więcej"*** na „***cache 512 MB"***
   Parametr – dyski twarde, zmieniono zapis ***„dodatkowych 4 dysków"*** na „***dodatkowych 3 dysków"***
   Parametr – zdalne zarządzanie skreślono zapisy
   - ***wirtualną konsolę z dostępem do myszy, klawiatury***
   - ***wsparcie dla IPv6***
   - ***wsparcie dla WSMAN (Web Service for Managament); SNMP; IPMI2.0, VLAN tagging, Telnet, SSH***
   - ***możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer***
   - ***możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer***
   - ***integracja z Active Directory***

   oraz
   - ***wsparcie dla dynamic DNS***
   - ***wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej***

   możliwość podłączenia lokalnego poprzez złącze RS-232

   parametr – systemy operacyjne, skreślono **„NetWare 6.5"**
   parametr – diagnostyka zmieniono na zapis ***„Panel umożliwiający wyświetlenie informacji o stanie podzespołów serwera."***
   parametr - gwarancja, skreślono „***Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem."***

   W wymaganiach dla pozostałych serwerów wprowadzono identyczne zmiany z wyjątkiem parametru dyski twarde:

- dla serwera autentykacyjno-raportującego na „***dodatkowych 2 dysków"***
- dla serwera backupującego na ***„Zainstalowane 7 dysków SAS 146GB 10K 6G 2.5" typu HotPlug, możliwość instalacji dodatkowego 1 dysku twardego Hot-Plug".***

2. Zamawiający dokonuje zmiany zapisu **Stanowisko nadzoru mobilnego** zawartego w punkcie 2 Opisu przedmiotu zamówienia, w następującym zakresie:
   Parametr – dysk zmieniono na zapis „***Min. 320 GB SATA, 7200 obr./min."***
   Parametr – system operacyjny na zapis "***Microsoft Windows 7 Professional PL 64bit"***
   Parametr- gwarancja zmieniono na ***zapis "3 lata na miejscu u klienta NBD; naprawa przypadkowych uszkodzeń; w przypadku awarii dysków twardych, uszkodzone nośniki pozostają u Zamawiającego"***
   Parametr –urządzenia zewnętrzne, zapis ***„Zewnętrzny dysk min. 500 GB w technologii SATA 2,5 cala / 7200 obr/min – możliwość podłączenia poprzez interfejs USB 3.0 wraz z kontrolerem do tego interfejsu na Express Card"*** zmieniono na ***„Zewnętrzny dysk min. 500 GB w technologii SATA 2,5 cala / 7200 obr/min – interfejs USB 3.0. W przypadku braku interfejsu USB 3.0 w laptopie wykonawca dostarczy kontroler na Express Card. Zamawiający nie dopuszcza "składanych" dysków zewnętrznych (dysk+kieszeń)."***

3. Zamawiający dokonuje zmiany zapisu **System zabezpieczeń sprzętowo-programowych** zawartego w punkcie 2 Opisu przedmiotu zamówienia, w następującym zakresie:
   Skreślono: ***„Podstawowe funkcje systemu musza być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanego układu ASIC".***

   Zmieniony załącznik 1 Opis przedmiotu zamówienia stanowi załącznik do niniejszego modyfikacji

Kierownik
Sekcji Zamówień Publicznych
KWP zs. w Radomiu
Leszek Jaczyński

ZAŁĄCZNIK 1

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Sposób realizacji i odbioru przedmiotu zamówienia

Przedmiotem zadania jest sprzętowa rozbudowa węzła internetowego w KWP Radom. Rozbudowa realizowana będzie jako dostawa, instalacja, konfiguracja i uruchomienie sprzętu i oprogramowania wyszczególnionego w części 2 opisu zadania.

1. Wykonawca przedstawi harmonogram realizacji zadania w terminie 7 dni od podpisania umowy.
2. Wykonawca przeprowadzi wizję lokalną w KWP w Radomiu. W wizji lokalnej będzie uczestniczył przedstawiciel Zamawiającego.
3. Przeprowadzenie analizy przed wdrożeniowej dla określenia polityki bezpieczeństwa z uwzględnieniem wstępnych szczegółowych wymogów zamawiającego (dostosowanie do sprzętu i adresacji IP dla istniejącej infrastruktury internetu na Mazowszu) wdrażanego systemu;
4. Wykonanie dokumentacji wdrożeniowej proponowanego rozwiązania terminie 21 dni od podpisania umowy i przedstawienie do akceptacji;
5. Po zaakceptowaniu przez Zamawiającego dokumentacji wdrożeniowej Wykonawca dostarczy, zainstaluje, uruchomi i skonfiguruje urządzenia z uwzględnieniem ewentualnych potrzeb zmiany konfiguracji już pracujących urządzeń.
6. Wszystkie urządzenia zainstalowane będą w szafie o wysokości 42U – szafę wskaże Zamawiający, nie jest ona przedmiotem dostawy.
7. Przy instalacji i uruchomieniu urządzeń obecny będzie przedstawiciel Zamawiającego.
8. Po stwierdzeniu przez Zamawiającego zgodności dostarczonego rozwiązania z wymaganiami Zamawiającego, Wykonawca przekaże dokumentację powykonawczą (pozwalająca na odtworzenie całego systemu w przypadku uszkodzenia sprzętu lub zresetowania do ustawień fabrycznych itp.) i przeprowadzi wymagane instruktaże techniczne.
9. Warunkiem zgłoszenia przez Wykonawcę gotowości do odbioru zadania jest:
    - Dostawa, montaż, instalacja, uruchomienie i konfiguracja oferowanych urządzeń oraz oprogramowania zgodnie z wymaganiami Zamawiającego.
    - Przekazanie dokumentacji zgodnej z wymaganiami Zamawiającego.
    - Przeprowadzenie instruktażu technicznego zgodnego z wymaganiami Zamawiającego.
10. Wykonawca dostarczy wykaz zawierający nazwę produktu, jego ukompletowanie, ilość, numery seryjne oraz numer licencji na oprogramowanie jeśli jest wymagana oraz cenę jednostkową brutto urządzenia.

11. W trakcie odbioru, Komisja powołana do odbioru przedmiotu zamówienia sprawdzi zgodność dostarczonego rozwiązania z wymaganiami

12. W protokole odbioru umieszczone zostaną:
    - Ilościowe zestawione odbieranych urządzeń wraz z ich parametrami technicznymi oraz oprogramowania.
    - Potwierdzenie lub uwagi dotyczące zgodności dostarczonego rozwiązania z wymaganiami.
    - Potwierdzenie dostarczenia dokumentacji

Warunki ogólne dotyczące producenta sprzętu: gwarancje, pochodzenie

1. Sprzęt dostarczony w ramach realizacji umowy będzie sprzętem nowym, nie używanym wcześniej w innych projektach.
2. Sprzęt dostarczony w ramach realizacji umowy będzie posiadał świadczenia gwarancyjne oparte na gwarancji świadczonej przez producenta sprzętu.
3. Sprzęt dostarczony w ramach realizacji umowy będzie sprzętem zakupionym w oficjalnym kanale sprzedaży producenta na rynek polski, co zgodnie z punktem 1) i 2) oznacza, że będzie on sprzętem nowym i posiadającym stosowny pakiet usług gwarancyjnych kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej.

Wraz z dostawa sprzętu należy dostarczyć dokument wydany przez producenta, poświadczający datę produkcji sprzętu. Sprzęt powinien być nie starszy niż 4 miesiąc

Założenia Instalacji i Konfiguracji

<u>Dla Serwera poczty</u>

Instalacja i konfiguracja systemu operacyjnego: instalacja musi odbyć się bez użycia środowiska graficznego.
Oprogramowanie do zarządzania pocztą elektroniczną musi zapewniać:

- skonfigurowanie kont użytkowników pocztowych wraz z aliasami,
- hasła do skrzynek pocztowych muszą być zmienione przez użytkownika przy pierwszym logowaniu,
- zainstalowanie aktualnych poprawek oraz uaktualnień systemowych, wraz z bezpieczną konfiguracją systemu (wyłączenie zbędnych modułów, usług niezgodnych z przeznaczeniem serwera),
- zakłada się w specyfikacji konfigurację powierzchni dyskowej serwera pocztowego z określeniem wielkości miejsca dla skrzynki użytkownika - wielkość ustalona zostanie przed instalacją.

Konfiguracja zawiera przeniesienie danych i skrzynek z istniejącego już serwera pocztowego z zachowaniem serwera pocztowego Postfix.
Komunikacja musi odbywać się po szyfrowanych połączeniach (TLS/SSL). Odbiór poczty firmowej powinien być zapewniony na porcie 995, zaś wysyłanie na porcie standardowym 25, imaps na porcie 993.
Serwer musi mieć uruchomioną i skonfigurowaną obsługę IP Tables oraz posiadać dodatkowe zabezpieczenia.

Konfiguracja file systemu
Bezpieczna autoryzacja użytkowników po protokole LDAP w usłudze katalogowej Active Direktory
Instalacja oraz konfiguracja dodatków (SpamAssassin, DKIM, graylist, Antywirus, statystyk itp.). Zamawiający rozważy przeniesienie części funkcjonalności do System zabezpieczeń sprzętowo-programowych o ile będą takie możliwości i podniesie to bezpieczeństwo lub funkcjonalność.
Wygenerowanie certyfikatu SSL dla serwera, tak aby nie było konieczności instalowania certyfikatów w programach pocztowych na stacjach klienckich. Zamawiający dopuszcza zakup certyfikatu SSL o ważności minimum 3 lata tak, aby w/w wymóg został spełniony.

Dla Serwera WWW

Instalacja i konfiguracja serwera WWW (Apache, PHP, MySQL) z kodowaniem polskich znaków, instalacja musi odbyć się bez użycia środowiska graficznego.

Konfiguracja MySQL dla 2 użytkowników: administrator, gość,

Zainstalowanie aktualnych poprawek oraz uaktualnień systemowych, wraz z bezpieczną konfiguracją systemu

(wyłączenie zbędnych modułów, usług niezgodnych z przeznaczeniem serwera)

Konfiguracja zawiera przeniesienie danych z istniejącego już serwera webowego oraz uruchomienie istniejącej strony WWW. Serwer musi mieć uruchomioną i skonfigurowaną obsługę IP Tables, https oraz posiadać dodatkowe zabezpieczenia.

Konfiguracja file systemu

Uruchomienie i konfiguracja vhosts zgodnie z wymaganiami zamawiającego

Uruchomienie interfejsu webowego dla poczty pod adresem (url'em) wskazanym przez zamawiającego po połączeniu szyfrowanym

Instalacja serwera FTP (tylko połączenia szyfrowane dla konkretnych IP) i powiązania ich z vhostami

Wygenerowanie certyfikatu SSL dla serwera, tak aby nie było konieczności instalowania (akceptacji) certyfikatów w przeglądarkach na stacjach klienckich. Zamawiający dopuszcza zakup certyfikaty SSL o ważności minimum 3 lata tak, aby w/w wymóg został spełniony.

Dla serwera autentykacyjno – raportujący

Instalacja i konfiguracja systemu operacyjnego wraz z aktualnymi i dostępnymi poprawkami do systemu wraz z bezpieczną konfiguracją systemu (wyłączenie zbędnych modułów, usług niezgodnych z przeznaczeniem serwera)
Uruchomiona usługa Active Directory dla 500 użytkowników. Instalacja sprzętu, instalacja kontrolerów domeny, konfiguracja usług DNS, konfiguracja usługi DHCP, zabezpieczenie kontrolerów domeny (Microsoft SCW), stworzenie infrastruktury organizacyjnej w Active

Directory, stworzenie kont użytkowników, stworzenie i konfiguracja grup zabezpieczeń w Active Directory, stworzenie i implementacja polityk Active Directory, stworzenie logicznej infrastruktury plikowej oraz konfiguracja uprawnień, instalacja i konfiguracja serwisu aktualizacji zabezpieczeń i poprawek (WSUS 3.0). Dodatkowy wymóg, hasła użytkowników muszą być zmienione przez użytkownika przy pierwszym logowaniu, nowe hasło musi spełniać odpowiednią złożoność minimum 8 znaków w tym min. 1 cyfra i jedna duża litera. Instalacja zapasowego kontrolera domeny na serwerze zamawiającego (obecny serwer pocztowy). Zakup licencji serwera Windows 2008 oraz sprzętu potrzebnego na modernizacje leży po stronie Wykonawcy.

Dla serwera backupującego

Instalacja i konfiguracja oprogramowania do tworzenia kopii zapasowych dla 4 serwerów zainstalowanie aktualnych poprawek oraz uaktualnień systemowych, wraz z bezpieczną konfiguracją systemu (wyłączenie zbędnych modułów, usług niezgodnych z przeznaczeniem serwera). (Instalacja oprogramowania na serwerze backup'u, instalacja agentów na maszynach backup'owanych, konfiguracja mediów oraz urządzeń do tworzenia kopii bezpieczeństwa w oprogramowaniu, stworzenie polityk backupu, testowanie systemu kopii bezpieczeństwa).

Serwer musi mieć uruchomioną i skonfigurowaną obsługę IP Tables oraz posiadać dodatkowe zabezpieczenia
Konfiguracja streamera
Wdrożenie harmonogramu wykonywania kopii zapasowych
Konfiguracja file systemu

Dla systemu zabezpieczenia sprzętowo-programowego, urządzenia weryfikacji bezpieczeństwa sieci, routera, switch

Instalacja i konfiguracja wszystkich urządzeń z uwzględnieniem i dostosowaniem do adresacji Zamawiającego.
Powiązanie systemu z już pracującymi urządzeniami firewall na terenie Mazowsza z uwzględnieniem poprawności pracy poczty e-mail, usługi serwera WWW oraz innych związanych z projektem, dla jednostek policji posiadających innych dostawców Internetu niż KWP.
Skonfigurowanie polityki bezpieczeństwa zgodnie z ustaleniami poczynionymi z Zamawiającym. Polityka ma zapewniać kontrolę dostępu (firewall), ochronę przed atakami (IPS) i kontrolę pasma oraz ruchu (Traffic Shaping, Traffic Policing).
Zachowanie wszystkich adresów IP w domenie Zamawiającego bez zmian.
Wszystkie serwery maja być połączone za pomocą sieci skrętką kategorii 6 w różnej kolorystyce aby ułatwić identyfikacje.
Wszystkie serwery po wdrożeniu muszą zostać sprawdzone „Urządzeniem do weryfikacji bezpieczeństwa sieci" a wszelkie luki zostaną załatane przez Wykonawcę.
Wszystkie działania nie ujęte w założeniach instalacji i konfiguracji mające na celu połączenie wszystkich serwerów, urządzeń bezpieczeństwa i sieciowych w jeden działający system leży po stronie wykonawcy.

2 Wymagania techniczno-funkcjonalne

Switche (3 szt.)

Switche – przełączniki, urządzenia łączące segmenty sieci komputerowej. W projekcie umożliwią podłączenie zamawianych urządzeń.

Nazwa	Opis wymagań minimalnych
Porty	20 portów 10/100/1000BaseTX (RJ45)
Rozmiar tablicy adresów MAC	Min. 8000
Prędkość magistrali wew.	Min. 65 Gb/s
Przepustowość	Min. 50 mpps
Pamięć flash	16MB
Zarządzanie, monitorowanie i konfiguracja	WebUI, SSH, Telnet, SSL, SNMP v1/2c/3, Konsola lokalna (RS-232, DB-9)
Protokoły uwierzytelniania i kontroli dostępu	Secure Shell (SSH), RADIUS, TACACS+
Jumbo Frames	9K
Obsługiwane protokoły i standardy	IGMP, IEEE 802.1x, IEEE 802.3ad, VLAN support, QoS, IEEE 802.1p, IEEE 802.1Q, IEEE 802.3x, Flow control, full duplex capability, Layer 2 switching, DHCP support, auto-negotiation, Syslog support, port mirroring

Router (1 szt.)

Oferowany sprzęt będzie pochodzić od jednego producenta (jednolitość platformy sprzętowej) i pochodzić z legalnego kanału dystrybucyjnego. Zamawiający za oficjalny kanał dystrybucyjny uważa kanał uznany przez producenta oferowanego przez Wykonawcę sprzęt, zwłaszcza w aspekcie gwarancji, instalowania nowych wersji oprogramowania oraz serwisu na oferowany sprzęt.

Wymagane będzie w momencie instalacji, oświadczenie producenta sprzętu potwierdzające legalność sprzętu i oprogramowania. Router internetowy będzie wyposażony

w licencję na protokół BGP (Border Gateway Protocol).

W ramach umowy Zamawiający będzie mógł legalnie dokonywać uaktualnienia oprogramowania oraz sygnatur IPS przez okres 3 lat.

Wymagania funkcjonalne:

- Urządzenie modularne, posiadające min. 4 sloty do obsadzenia modułami rozszerzeń;
- Musi posiadać co najmniej 2 porty LAN 10/100/1000 BaseT;
- Musi posiadać co najmniej 2 routowalne porty WAN 10/100 BaseT
- Musi posiadać co najmniej 2 porty Serial oraz uwzględnić należy 2 kable (rs449, dte), z możliwością rozbudowy do 4 portów szeregowych
- Musi posiadać co najmniej 1 GB RAM oraz 256 MB FLASH;

- Urządzenie musi posiadać przepływność 500 000 pakietów na sekundę (pakiet 64 bajty)
- Musi posiadać co najmniej 2 porty USB;
- sloty urządzenia przewidziane pod rozbudowę o moduł funkcyjny sprzętowego wsparcia szyfracji,
- 2 porty dedykowane dla zarządzania: port konsoli, port asynchroniczny dla przyłączenia modemu,
- Musi być wyposażone w jeden zasilacz podstawowy oraz jeden zasilacz zapasowy (redundantny);
- Musi mieć możliwość montażu w szafie 19'', być zasilane prądem przemiennym o napięciu 230V oraz posiadać obudowę z metalu oraz wysokość urządzenie nie może przekraczać 3U;
- Urządzenie musi posiadać oprogramowanie i licencje realizujące funkcjonalność szyfrowania ruchu IPSec 3DES oraz AES z wydajnością nie mniejszą niż 180 Mbp. Wymagana jest obsługa protokołu AES z kluczem 128-bitowym, 192-bitowym lub 256-bitowym oraz obsługa co najmniej 700 tuneli IPsec;
- Urządzenie musi zapewniać współprace z serwerami certyfikatów cyfrowych: Entrust, Verisign, Microsoft i Baltimore Technologies;
- Urządzenie musi obsługiwać protokoły routingu dynamicznego: RIP/RIPv2, OSPF, EIGRP lub równoważny, IS-IS i BGP;
- Urządzenie musi obsługiwać ruch multicastowy w szczególności: PIM sparse/dense/SSM/Bi-directional, IGMP;
- Urządzenie musi obsługiwać RPF (Reverse Path Forwarding);
- Urządzenie musi obsługiwać następujące mechanizmy zarządzania pasmem: NBAR, WFQ, GTS, CAR i WRED
- Urządzenie musi obsługiwać następujące protokoły i mechanizmy bezpieczeństwa: SCEP, IKE keepalive, Radius, Tacacs, CHAP/PAP, MAC-MD5, MAC-SHA-1, NAC, CBAC, L2TP;
- Urządzenie musi posiadać funkcjonalność VRRP lub odpowiednik tej funkcjonalności;
- Zarządzenie musi być możliwie poprzez: CLI (Telnet, SSHv2, port konsoli), HTTPS, SNMPv3;
- Urządzenie musi posiadać niezbędne kable logiczne i energetyczne;

Przełącznik KVM (1 szt.)

Przełącznik KVM umożliwi podłączenie zainstalowanych serwerów do:

- zestawu klawiatury, myszy oraz monitora w szafie dystrybucyjnej,

- zdalnego stanowiska administratora.

Nazwa	Opis wymagań minimalnych
Porty	16 portów zarządzanych poprzez IP
Liczba zdalnych użytkowników IP	Min 2
Liczba lokalnych użytkowników	Min 1

Ilość niezależnych administratorów	Min 3
Obudowa	Obudowa typu rack, wysokość max. 1U
Porty lokalnej konsoli KVM	1 x (PS/2, PS/2, D-Sub-15) / (USB, USB, D-Sub-15)
Obsługiwane porty klawiatur/ myszy/monitorów	PS/2, PS/2, D-Sub-15, Sun (monitor 13W3, klawiatura i mysz DIN8), USB, USB, DSub-15 VT100
Inne	• WWW - wbudowany serwer webowy • możliwość konfiguracji BIOSu w podłączonych serwerach • Możliwość podłączenia urządzenia do zarządzania zasilaniem za pomocą portu DB-9 • Ochrona dostępu zdalnego za pomocą hasła i zaawansowanych technologii kodowania 1024 bit RSA, 256 bit AES, 56 bit DES i 128 SSL • Podłączenie serwerów przez interfejs RJ-45 • Możliwość połączeń kaskadowych zapewnia podłączenie do 128 komputerów • Do 64 kont użytkowników i 32 jednoczesnych logowań • Możliwość podglądu do 16 serwerów jednocześnie na jednym ekranie • Obsługa serwera RADIUS • Obsługa interfejsów sieciowych: TCP/IP, HTTP, HTTPS, UDP, RADIUS, DHCP, SSL, ARP, DNS, • Odłączalny przedni panel dla łatwego montażu w szafie serwerowej • Możliwość wyboru poszczególnych portów za pomocą: OSD, Hotkey, przycisków na urządzeniu • Rozdzielczość video 1280 x 1024 @ 60Hz • Dostarczone okablowanie ma zapewnić podłączenie serwerów ze specyfikacji oraz dodatkowo 2 serwerów z gniazdami PS2 oraz dwóch z gniazdami USB
Gwarancja	36 miesiące
Monitor	Kolorowy LCD 17` Min 1280 x 1024 pikseli, monitor LCD 16.2M kolorów, menu OSD, tego samego producenta co przełącznik w postaci wysuwanego panela 1U/19`` obsługa KVMów z portem lokalnym klaw. i myszy na PS/2
Obsługiwane porty klawiatur/myszy/monitorów	1 x (PS/2, PS/2, D-Sub-15)
Dołączone moduły	Umożliwiające podłączenie dostarczanych serwerów plus dwa dodatkowe na PS/2

Urządzenie do weryfikacji bezpieczeństwa sieci (1 szt.)

Urządzenie ma monitorować poziom bezpieczeństwa sieci. Wykrywać luki systemowe i podatności serwerów, stacji roboczych i wszystkich urządzeń sieciowych. Informuje o rodzaju błędu, określa poziom ryzyka oraz informuje administratora o sposobie jego usunięcia.

Wdrożenie systemu powinno obejmować:

- fizycznie podłączenie urządzenia do infrastruktury Zamawiającego w miejscu wskazanym przez Zamawiającego

- podstawową konfigurację w zakresie ustawień sieciowych urządzenia, ustawienia kont, na które będą kierowane powiadomienia, zgodnie z wytycznym Zamawiającego

- stworzenie na rozwiązaniu lokalnych kont pracowników z poziomami dostępu określonymi przez Zamawiającego

- przeprowadzenie pierwszego wykrycia maszyn pracujących w infrastrukturze Zamawiającego po fizycznej instalacji rozwiązania

- utworzenie 3 podstawowych profili audytowych dla maszyn Zamawiającego z zakresu: serwery, urządzenia sieciowe, stacje robocze.

Opis wymagań minimalnych
Rozwiązanie na platformie sprzętowej w obudowie umożliwiającej montaż w szafie rackowej. Wysokość obudowy urządzenia nie większa niż 1U.
Urządzenie musi zapewniać możliwość skanowania wszystkich urządzeń w infrastrukturze sieciowej. Licencja rozwiązania musi obejmować minimum 500 adresów IP.
Urządzenie musi posiadać co najmniej 3 interfejsy Gigabit, konfigurowalne (możliwość ustawienia: adresu IP, maski sieciowej, gatewaya i adresów serwerów DNS).
System musi posiadać wsparcie dla sieci VLAN. Rozwiązanie musi umożliwiać konfigurację (bez konieczności wymiany urządzeń sieciowych, ani instalowania dodatkowych aplikacji), która pozwoli na weryfikację bezpieczeństwa oraz ochronę przed nieautoryzowanym dostępem (poprzez moduł NAC) we wszystkich sieciach VLAN Zamawiającego.
Posiada certyfikat CVE
Działanie oparte na minimum trzech bazach w tym baza CVE i NVD
Możliwość wykrywania luk bezpieczeństwa w dowolnych systemach sieciowych bez instalowania dodatkowych aplikacji na tych systemach
Możliwość tworzenia i zarządzania polityką bezpieczeństwa sieci w oparciu o wbudowany system zawierający minimum 24 kategorie polityk bezpieczeństwa sieciowego
Możliwość weryfikacji bezpieczeństwa sieci w oparciu o normy bezpieczeństwa minimum: ISO27001/ISO17799, Sarbanes-Oxley, PCI
rozwiązanie musi posiadać wbudowany system zarządzania zagrożeniami, przydzielania zleceń naprawy systemów wybranym pracownikom z możliwością nadzorowania postępu prac
Urządzenie powinno oferować szczegółowe raporty zawierające opisy wykrytych luk bezpieczeństwa wraz z informacją o możliwości ich wyeliminowania z danego systemu

System musi posiadać wbudowany system raportowania z możliwością tworzenia podsumowań dla wskazanych systemów. system raportowania musi umożliwiać tworzenie raportów dla administratorów a także ogólnych raportów podsumowujących poziom bezpieczeństwa. Raporty muszą być dostępne minimum w formatach PDF oraz xml.
Możliwość blokowania hostów zawierających luki bezpieczeństwa w oparciu o mechanizmy integracji ze switchami zarządzalnymi
System musi umożliwiać wykrywanie i klasyfikowanie wszystkich urządzeń pracujących w infrastrukturze
System musi umożliwiać wykrywanie i automatyczne blokowanie nieautoryzowanego dostępu do infrastruktury sieciowej w oparciu o zintegrowany bezagentowy system NAC.
Rozwiązanie musi posiadać system wykrywania zmian w obrębie infrastruktury sieciowej i powiadamiania administratorów o każdej zanotowanej zmianie, powiadomienia nie mogą być wysyłane później niż 2 sekundy po zanotowaniu zdarzenia
System musi posiadać mechanizm automatycznego skanowania pod kątem występowania podatności i luk bezpieczeństwa zaufanych systemów podłączających się do infrastruktury sieciowej
System musi wykrywać wszelkie anomalia sieciowe związane z IP spoofing, MAC spoofing, system spoofing.
Możliwość integracji ze smartswitchami (HP, 3COM, CISCO lub Extreme Networks)
Rozwiązanie pozwala na tworzenie użytkowników mających dostęp do interfejsu webowego na dwóch różnych poziomach – managera oraz pracownika IT.
Możliwość wykrywania i powiadamiania o pojawieniu się w sieci hostów z danej puli adresów IP
System musi zapewniać bezpieczeństwo danych, przechowując informacje o wykrytych podatnościach w formie zaszyfrowanej
Możliwość monitorowania aktywności hostów i powiadamianie w przypadku braku łączności z monitorowanymi urządzeniami
Zarządzanie przez interfejs webowy, bez konieczności używania maszyny Javy ani dodatkowego oprogramowania instalowanego na maszynie zarządzającej.
Praca urządzenia powinna być możliwa w sieciach z adresacją statyczną oraz w środowisku DHCP
Urządzenie powinno umożliwiać określenie wykrytych luk bezpieczeństwa jako tzw. false positive dodatkowo powinna być możliwość generowania raportów podsumowujących a także zbiorczych raportów dla osób zarządzających
Minimum 3 tryby audytowe: pełny, porównawczy oraz inkrementalny
Minimum trzy letnią subskrypcją aktualizacji baz zagrożeń oraz firmware, zawierającą także suport techniczny wraz z maintenance'em dla urządzenia.

System zabezpieczeń sprzętowo-programowych

System musi obsługiwać nie limitowaną ilość użytkowników w ramach realizowanych systemów zabezpieczeń i umożliwiać realizację następujących funkcji:

- Firewall klasy *Stateful Inaspection*
- Antywirus
- System detekcji i prewencji włamań (IDP)
- VPN zgodny z IPSec,PPTP i L2TP z możliwością rozbudowy do SSL-VPN
- Antyspam

- Filtracja stron WWW
- Kontrola pasma (Traffic Management)

System ochrony musi być zbudowany przy użyciu minimalnej ilości elementów ruchomych, krytycznych dla jego działania. Dostawca jest zobowiązany zagwarantować wsparcie producenta dla każdej zaoferowanej funkcjonalności bezpieczeństwa. W przypadku zastosowania funkcjonalności sofware'owych dostawca powinien dostarczyć odpowiednio wydajna platformę sprzętową Uwaga: Dziennik zdarzeń lub inne działania wymagające systemów dyskowych musza być realizowane na zewnętrznym urządzeniu – serwerze autentykacyjno-raportującym i tam umożliwiać zbieranie logów i generowanie raportów.

Nazwa	Opis wymagań minimalnych
Typ urządzenia	Dwa urządzenia typu UTM, zapewniające funkcjonalności: Firewall, Koncentrator IPSec VPN, ochrona przed wirusami, spyware, sonda IPS, filtrowanie treści, działające w klastrze wysokiej dostępności Active-Passive z synchronizacją sesji jak również w trybie Active-Active UTM.
Specyfikacja fizyczna urządzenia	Dedykowane rozwiązanie sprzętowe Obudowa 1U przeznaczona do montażu w szafie RACK Zasilanie i wentylatory redundantne z możliwością wymiany hot-swap Pamięć RAM: minimum 1 GB Pamięć FLASH: minimum 512 MB Compact Flash Ilość interfejsów: • nie mniej niż 8 interfejsów GigabitEthernet • nie mniej niż 2 interfejsy USB • 1 interfejs GigabitEthernet dedykowany do połączenia dwóch jednakowych urządzeń w klaster HA • 1 interfejs konsoli
Wydajność urządzeń pracujących w klastrze HA Active-Passive	Obsługa nielimitowanej ilości hostów w sieci chronionej Przepustowość zapory sieciowej przy pracy w trybie Statefull Packet Inspection, mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 5 Gbps. Przepustowość zapory sieciowej pracującej jako sonda IPS, mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 2,3 Gbps. Przepustowość zapory sieciowej przy pracy w trybie Deep Packet Inspection, przy włączonych wszystkich usługach filtrowania i skanowania: nie mniejsza niż 1,5 Gbps. Przepustowość zintegrowanego z zaporą sieciową koncentratora połączeń IPSec VPN AES/3DES mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 2,5 Gbps. Maksymalna ilość jednocześnie obsługiwanych sesji: nie mniej niż 1000000. Obsługa nie mniej niż 20000 nowych sesji na sekundę. Ochrona przed atakami DoS i DdoS.
Funkcjonalności urządzeń w zakresie	• Minimalna ilość jednocześnie obsługiwanych połączeń IPSec VPN: 6000.

konfiguracji połączeń zdalnych VPN	• Minimalna ilość klientów IPSec VPN w cenie urządzenia: 2000. • Wspierane mechanizmy uwierzytelniania i szyfrowania: DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1. • Wspierane mechanizmy wymiany kluczy: IKE, IKEv2, Manual Key, PKI (X.509). • Wsparcie certyfikatów: Verisign, Thawte, Cybertrust, RSA Keon, Entrust, Microsoft CA dla połączeń site-to-site pomiędzy urządzeniami. • Obsługa funkcjonalności: L2TP IPSec, DHCP over VPN, redundantna brama zdalna w przypadku połączeń site-site VPN. • Minimalna ilość jednocześnie obsługiwanych połączeń SSL VPN: 50.
Sieciowe funkcjonalności urządzeń	• Możliwość pracy jako Router, Bridge L2 lub w trybie transparentnym. • Obsługa nie mniej niż 500 sieci VLAN działających zgodnie ze standardem 802.1Q. • Wbudowany serwer DHCP umożliwiający przydzielanie adresów statycznie, dynamicznie, przekierowanie zgłoszeń do zewnętrznego serwera DHCP. • Możliwość przesyłania komunikatów DHCP pomiędzy różnymi strefami. • Wsparcie mechanizmów NAT: 1:1, 1:many, many:1, many:many, PAT. • Możliwość scentralizowanego zarządzania nie mniej niż 128 punktami dostępowymi, wsparcie dla standardów 802.11 b/g, WEP, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS, IPSec over WLAN. • Możliwość kreowania reguł routingu statycznego • Wsparcie dynamicznych protokołów routingu: RIP v1/v2, OSPF i wsparcie dla routowania transmisji multicast. • Wsparcie funkcjonalności QoS: tagowanie/mapowanie 802.1p, DSCP, możliwość ustawienia przynajmniej 100 reguł określających maksymalne i gwarantowane pasmo. • Możliwość skonfigurowania przynajmniej 2 łączy WAN, działających w trybie redundantnym lub umożliwiających równoważenie obciążeń dla ruchu wychodzącego. • Możliwość konfiguracji monitorowania pracy łączy WAN w oparciu o połączenia TCP i ICMP i reguł przełączenia ruchu z łącza podstawowego na łącze redundantne. • Możliwość konfiguracji reguł równoważenia obciążeń dla ruchu przychodzącego do hostów znajdujących się w sieci chronionej. • Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń, pełna kompatybilność z większością urządzeń i serwerów VoIP.

Funkcjonalności urządzeń w zakresie uwierzytelniania użytkowników	• Lokalna baza użytkowników umożliwiająca wykreowanie nie mniej niż 2500 kont. • Uwierzytelnianie użytkowników w oparciu o: XAUTH/RADIUS, Active Directory, SSO, LDAP, lokalna baza użytkowników. • Wymagane jest, aby uwierzytelnianie użytkowników odbywało się zarówno z lokalnej bazy, skonfigurowanej na urządzeniu, jak i z zewnętrznego serwera Active Directory jednocześnie.
Funkcjonalności urządzeń w zakresie zarządzania i wysokiej dostępności	• Możliwość zarządzania urządzeniem poprzez: HTTP, HTTPS, CLI (SSH, konsola), SNMP v2. • Możliwość dokupienia dedykowanego oprogramowania do scentralizowanego zarządzania większą ilością urządzeń. • Praca w klastrze wysokiej dostępności w trybie Active – Passive z synchronizacją sesji oraz w trybie Active-Active UTM.
Funkcjonalności urządzeń w zakresie mechanizmów filtrowania Deep Packet Inspection i Statefull Packet Inspection	Możliwość kreowania stref bezpieczeństwa przydzielanych do danych interfejsów zarówno fizycznych, jak i wirtualnych (możliwość przypisania więcej niż jednego interfejsu do pojedynczej strefy bezpieczeństwa). Możliwość indywidualnej konfiguracji usług bezpieczeństwa dla każdej ze stref. Możliwość kreowania reguł Firewall dla ruchu przychodzącego/wychodzącego z/do zadanej strefy, w określonych przedziałach czasu, z uwzględnieniem użytkowników, dla których reguła ma być aktywna Możliwość włączania i wyłączania reguł Firewall i NAT bez konieczności ich usuwania Wymagane jest, aby na urządzeniach uruchomione były następujące usługi w subskrypcji na 3 lata: • sieciowa ochrona antywirusowa zapewniająca skanowanie ruchu na protokołach HTTP, FTP, POP3, SMTP, IMAP, ruch TCP oraz NetBios. Filtr antywirusowy powinien zapewniać skanowanie załączników poczty elektronicznej, plików skompresowanych ZIP i GZIP. Wymagane jest, aby możliwe było włączenie lub wyłączenie usługi antywirus w poszczególnych strefach bezpieczeństwa, oraz możliwość włączenia lub wyłączenia reagowania na określone sygnatury. • sonda IDP (detekcja i blokowanie wtargnięć do sieci) zapewniająca skanowanie ruchu w oparciu o sygnatury dostarczone przez producenta. Sygnatury powinny umożliwiać wykrywanie i blokowanie zdarzeń takich jak: korzystanie z programów do wymiany plików P2P (np. Limewire, BitTorrent, eMule, etc.), korzystanie z komunikatorów internetowych (np. Yahoo Messenger, Gadu-Gadu, Skype, etc.), ataki typu backdoor, exploit, SQL-Injection, etc. Wymagane jest, aby poza możliwością włączenia lub wyłączenia usługi IDP w poszczególnych strefach

	bezpieczeństwa możliwa była indywidualna konfiguracja każdej z sygnatur w celu uruchomienia bądź wyłączenia jej dla zadanych adresów IP, użytkowników lub przedziałów czasowych. • sieciowa ochrona antyspyware, zapewniająca skanowanie ruchu HTTP, FTP, SMTP, POP3, IMAP. Wymagane jest, aby poza możliwością włączenia lub wyłączenia usługi IDP w poszczególnych strefach bezpieczeństwa możliwa była indywidualna konfiguracja każdej z sygnatur w celu uruchomienia bądź wyłączenia jej dla zadanych adresów IP, użytkowników lub przedziałów czasowych. • usługa filtrowania treści stron WWW, zapewniająca blokowanie apletów Java, aplikacji Active-X, plików cookie, definiowanie białych i czarnych list stron www, definiowanie słów kluczowych umożliwiających zablokowanie strony w przypadku ich wystąpienia. Dodatkowo wymagane jest tworzenie reguł filtrowania treści dla poszczególnych grup użytkowników umożliwiających filtrowanie treści w oparciu o informacje z zewnętrznych serwerów zawierających bazę stron zestawionych w co najmniej 56 kategoriach. Wymagane jest, aby mechanizm filtrowania treści uwzględniał także filtrowanie stron HTTPS oraz możliwość włączenia lub wyłączenia mechanizmu filtrowania treści w poszczególnych strefach bezpieczeństwa i zdefiniowanie domyślnej reguły dla każdej ze stref działającej niezależnie od uprawnień poszczególnych użytkowników. • usługa Firewall aplikacji umożliwiająca definiowanie własnych sygnatur oraz reakcji urządzenia w przypadku wykrycia ruchu zgodnego z wprowadzonymi sygnaturami. • ochrona poczty elektronicznej w oparciu o białe/czarne listy nadawców oraz serwery RBL. Wymagana jest taka możliwość skonfigurowania połączeń IPSec VPN client-site, aby cały ruch z połączonych do urządzeń klientów przesyłany był poprzez urządzenia i możliwe było jego skanowanie przez mechanizmy antywirus, antyspyware, IDP, filtrowania treści. Wymaga się, aby na urządzeniach możliwe było włączenie blokowania ruchu przesyłanego pomiędzy strefami w przypadku, kiedy na stacjach roboczych lub serwerach nie będzie zainstalowanego odpowiedniego oprogramowania antywirusowego, lub oprogramowanie to będzie miało nieaktualne sygnatury. Wymaga się, aby mechanizmy antywirus, antyspyware i sonda IDP nie posiadały ograniczeń co do wielkości skanowanych plików
Zarządzanie pasmem	Wymagane jest dostarczenie dedykowanego oprogramowania (instalowanego na zewnętrznym serwerze) zapewniającego monitorowanie, rejestrację i graficzną (w postaci tabel i wykresów) prezentację danych przesłanych z urządzenia firewall dotyczących ruchu, oraz zagrożeń sieciowych. Niezbędne dane to średnia zajętość łącza w podziale na dni i godziny, wykorzystanie pasma przez każdego z użytkowników, informacje dotyczące przeglądanych witryn

	przez każdego z użytkowników sieci informatycznej, informacje dotyczące użytkowników łamiących zasady przeglądania witryn, informacje dot. ataków, detekcji intruzów, zagrożeń antywirusowych. Dane muszą mieć możliwość wydruku.
Wsparcie techniczne i gwarancja	Wymagane jest aby dostarczane urządzenia objęte były okresem gwarancji przez okres 3 lat, z możliwością przedłużenia na dłuższy okres czasu. Wymagane jest, aby w ramach gwarancji uszkodzone urządzenie zostało wymienione w ciągu jednego dnia roboczego. Wymagane jest, aby urządzenia objęte było wsparciem technicznym 24x7 (wraz z możliwością dokonywania aktualizacji oprogramowania up-to-date w ramach posiadanego wsparcia technicznego), realizowanym przez producenta przez okres 3 lat z możliwością przedłużenia na dłuższy okres czasu

Serwery (4 szt.)

Oferowany sprzęt będzie pochodzić od jednego producenta (jednolitość platformy sprzętowej) i pochodzić z legalnego kanału dystrybucyjnego. Zamawiający za oficjalny kanał dystrybucyjny uważa kanał uznany przez producenta oferowanego przez Wykonawcę sprzęt, zwłaszcza w aspekcie gwarancji, instalowania nowych wersji oprogramowania oraz serwisu na oferowany sprzęt.
Wymagane będzie w momencie instalacji, oświadczenie producenta sprzętu potwierdzające legalność sprzętu i oprogramowania. Oferowane serwery mają mieć możliwość wysunięcia po zamontowaniu ich w szafie.

Wymagania dla serwera pocztowego:

Nazwa elementu, parametru lub cechy	Opis wymagań minimalnych
Obudowa	Maksymalnie 2U do instalacji w standardowej szafie RACK 19”, dostarczona wraz z szynami i prowadnicą kabli.
Procesor	Jeden procesor czterordzeniowy klasy x86 dedykowany do pracy w serwerach zaprojektowany do pracy w układach dwuprocesorowych, taktowany zegarem co najmniej 2.26GHz, pamięć cache L3 8 MB lub procesor równoważny wydajnościowo według wyniku testów przeprowadzonych przez Oferenta. W przypadku zaoferowania procesora równoważnego Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.
Liczba procesorów zainstalowanych	Min. 1

Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów, dwu lub czterordzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Pamięć RAM	8 GB DDR3 RDIMM 1066 MHz, płyta główna powinna obsługiwać do 192GB, na płycie głównej powinno znajdować się minimum 18 slotów przeznaczonych dla pamięci.
Zabezpieczenia pamięci RAM	SBEC, Memory Mirror
Kontroler dysków twardych	Kontroler SAS RAID w wersji SAS 2.0, pozwalający na zbudowanie minimum poziomu RAID-0, 1, 10, 5 cache 512MB, podtrzymanie bateryjne
Dyski twarde	Możliwość instalacji dysków SATA, SAS lub SSD. Zainstalowane 5 dysków SAS 146GB 10K 6G 2.5'' typu HotPlug, możliwość instalacji dodatkowych 3 dysków twardych Hot-Plug
Liczba wszystkich wnęk na dyski twarde	Minimum 8 wnęk typu hot swap 2.5in
Napęd DVD	Min. CD-RW/DVD-ROM
Interfejsy sieciowe	Minimum 2 porty 10/100/1000
Zdalne zarządzanie	Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane złącze RJ-45 i umożliwiająca: ▪ zdalny dostęp do graficznego interfejsu Web karty zarządzającej ▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera,) ▪ szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika ▪ możliwość podmontowania zdalnych wirtualnych napędów ▪ możliwość obsługi przez dwóch administratorów jednocześnie
Grafika	Zintegrowana z płytą główną
Zasilacze	Minimum 2 zasilacze, redundantne typu hot plug
Wentylatory	Zestaw wentylatorów redundantnych typu hot plug
Porty dodatkowe	Minimum 4 porty USB 2.0, 1x port szeregowy, 1x VGA
Systemy operacyjne	Wspierane systemy: Windows 2000 Server, Windows 2003 Server, RedHat Linux 5, SUSE Linux 10
Diagnostyka	Panel umożliwiający wyświetlenie informacji o stanie podzespołów serwera.
Certyfikaty	ISO 9001 producenta serwera, deklaracja zgodności CE
Gwarancja	Przynajmniej trzy lata gwarancji z czasem reakcji 4 godziny od zgłoszenia.

	Zamawiający oczekuje możliwości przedłużenia czasu gwarancji do pięciu lat. W przypadku uszkodzenia dysków twardych naprawa w siedzibie zamawiającego i uszkodzone dyski pozostają u Zamawiającego
Zainstalowany system operacyjny	SUSE Linux Enterprise Server 11, 3 lata subskrypcji lub równoważny
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela

Wymagania dla serwera WWW

Nazwa elementu, parametru lub cechy	**Opis wymagań minimalnych**
Obudowa	Maksymalnie 2U do instalacji w standardowej szafie RACK 19", dostarczona wraz z szynami i prowadnicą kabli.
Procesor	Jeden procesor czterordzeniowy klasy x86 dedykowany do pracy w serwerach zaprojektowany do pracy w układach dwuprocesorowych, taktowany zegarem co najmniej 2.26GHz, pamięć cache L3 8 MB lub procesor równoważny wydajnościowo według wyniku testów przeprowadzonych przez Oferenta. W przypadku zaoferowania procesora równoważnego Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.
Liczba procesorów zainstalowanych	Min. 1
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów, dwu lub czterordzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Pamięć RAM	8 GB DDR3 RDIMM 1066 MHz, płyta główna powinna obsługiwać do 192GB, na płycie głównej powinno znajdować się minimum 18 slotów przeznaczonych dla pamięci.
Zabezpieczenia pamięci	

RAM	SBEC, Memory Mirror
Kontroler dysków twardych	Kontroler SAS RAID w wersji SAS 2.0, pozwalający na zbudowanie minimum poziomu RAID-0, 1, 10, 5 cache 512MB, podtrzymanie bateryjne
Dyski twarde	Możliwość instalacji dysków SATA, SAS lub SSD. Zainstalowane 4 dysków SAS 146GB 10K 6G 2.5" typu HotPlug, możliwość instalacji dodatkowych 4 dysków twardych Hot-Plug
Liczba wszystkich wnęk na dyski twarde	Minimum 8 wnęk typu hot swap 2.5in
Napęd DVD	Min. CD-RW/DVD-ROM
Interfejsy sieciowe	Minimum 2 porty 10/100/1000
Zdalne zarządzanie	Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane złącze RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej ▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera,) ▪ szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika ▪ możliwość podmontowania zdalnych wirtualnych napędów ▪ możliwość obsługi przez dwóch administratorów jednocześnie
Grafika	Zintegrowana z płytą główną
Zasilacze	Minimum 2 zasilacze, redundantne typu hot plug
Wentylatory	Zestaw wentylatorów redundantnych typu hot plug
Porty dodatkowe	Minimum 4 porty USB 2.0, 1x port szeregowy, 1x VGA
Systemy operacyjne	Wspierane systemy: Windows 2000 Server, Windows 2003 Server, RedHat Linux 5, SUSE Linux 10
Diagnostyka	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Certyfikaty	ISO 9001 producenta serwera, deklaracja zgodności CE
Gwarancja	Przynajmniej trzy lata gwarancji z czasem reakcji 4 godziny od zgłoszenia. Zamawiający oczekuje możliwości przedłużenia czasu gwarancji do pięciu lat. W przypadku uszkodzenia dysków twardych naprawa w siedzibie zamawiającego i uszkodzone dyski pozostają u Zamawiającego
Zainstalowany system operacyjny	SUSE Linux Enterprise Server 11, 3 lata subskrypcji lub równoważny
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji

	sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela

Wymagania dla serwera autentykacyjno – raportującego

Nazwa elementu, parametru lub cechy	Opis wymagań minimalnych
Obudowa	Maksymalnie 2U do instalacji w standardowej szafie RACK 19", dostarczona wraz z szynami i prowadnicą kabli.
Procesor	Jeden procesor czterordzeniowy klasy x86 dedykowany do pracy w serwerach zaprojektowany do pracy w układach dwuprocesorowych, taktowany zegarem co najmniej 2.66GHz, pamięć cache L3 8 MB lub procesor równoważny wydajnościowo według wyniku testów przeprowadzonych przez Oferenta. W przypadku zaoferowania procesora równoważnego Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.
Liczba procesorów zainstalowanych	Min 2
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów, dwu lub czterordzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Pamięć RAM	16 GB DDR3 RDIMM 1333 MHz, płyta główna powinna obsługiwać do 192GB, na płycie głównej powinno znajdować się minimum 18 slotów przeznaczonych dla pamięci..
Zabezpieczenia pamięci RAM	SBEC, Memory Mirror
Kontroler dysków twardych	Kontroler SAS RAID, pozwalający na zbudowanie minimum poziomu RAID-0, 1, 10, 5 , cache 256MB lub więcej, podtrzymanie bateryjne
Dyski twarde	Możliwość instalacji dysków SATA, SAS lub SSD. Zainstalowane 6 dysków SAS 146GB 15K 6G 2.5" typu HotPlug, możliwość instalacji dodatkowych 2 dysków twardych Hot-Plug
Liczba wszystkich wnęk na dyski twarde	Minimum 8 wnęk typu hot swap 2.5in

Napęd DVD	Min. CD-RW/DVD-ROM
Interfejsy sieciowe	Minimum 2 porty 10/100/1000
Zdalne zarządzanie	Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane złącze RJ-45 i umożliwiająca: ▪ zdalny dostęp do graficznego interfejsu Web karty zarządzającej ▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera,) ▪ szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika ▪ możliwość podmontowania zdalnych wirtualnych napędów ▪ możliwość obsługi przez dwóch administratorów jednocześnie
Grafika	Zintegrowana z płytą główną
Zasilacze	Minimum 2 zasilacze, redundantne typu hot plug
Wentylatory	Zestaw wentylatorów redundantnych typu hot plug
Porty dodatkowe	Minimum 4 porty USB 2.0, 1x port szeregowy, 1x VGA
Systemy operacyjne	Wspierane systemy: Windows 2000 Server, Windows 2003 Server, Novell NetWare 6.5, RedHat Linux 5, SUSE Linux 10
Diagnostyka	Panel umożliwiający wyświetlenie informacji o stanie podzespołów serwera.
Certyfikaty	ISO 9001 producenta serwera, deklaracja zgodności CE
Gwarancja	Przynajmniej trzy lata gwarancji z czasem reakcji 4 godziny od zgłoszenia. Zamawiający oczekuje możliwości przedłużenia czasu gwarancji do pięciu lat. W przypadku uszkodzenia dysków twardych naprawa w siedzibie zamawiającego i uszkodzone dyski pozostają u Zamawiającego
Zainstalowany system operacyjny	Microsoft Windows Server Enterprise R2 2008 w wersji anglojęzycznej lub równoważny (wymagane załączenie nośników instalacyjnych w wersji 2008 jak również 2003) Licencja systemu operacyjnego musi zawierać Windows Server CAL 2008 OLP Device CAL (Client Access License per device) dla 500 urządzeń.
Oprogramowanie dodatkowe	Wymagane jest dostarczenie dedykowanego oprogramowania (instalowanego na zewnętrznym serwerze) zapewniającego monitorowanie, rejestrację i graficzną (w postaci tabel i wykresów) prezentację danych przesłanych z systemu zabezpieczeń sprzętowo-programowego, urządzenia do weryfikacji zabezpieczeń sieci dotyczących ruchu, oraz zagrożeń sieciowych. Niezbędne dane to średnia zajętość łącza w podziale na dni i godziny, wykorzystanie pasma przez każdego z użytkowników, informacje dotyczące przeglądanych

	witryn przez każdego z użytkowników sieci informatycznej, informacje dotyczące użytkowników łamiących zasady przeglądania witryn, informacje dot. ataków, detekcji intruzów, zagrożeń antywirusowych. Dane muszą mieć możliwość wydruku. Wymagane jest, aby oprogramowanie posiadało minimum 40 zdefiniowanych typów raportów oraz zapewniało tworzenie raportów w oparciu o spersonalizowane wymagania. Oprogramowanie analizująco-raportujące dostarczane przez tego samego producenta, co system zabezpieczeń
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela

<u>Wymagania dla serwera backupującego</u>

Nazwa elementu, parametru lub cechy	**Opis wymagań minimalnych**
Obudowa	Maksymalnie 2U do instalacji w standardowej szafie RACK 19”, dostarczona wraz z szynami i prowadnicą kabli.
Procesor	Jeden procesor czterordzeniowy klasy x86 dedykowany do pracy w serwerach zaprojektowany do pracy w układach dwuprocesorowych, taktowany zegarem co najmniej 2.26GHz, pamięć cache L3 8 MB lub procesor równoważny wydajnościowo według wyniku testów przeprowadzonych przez Oferenta. W przypadku zaoferowania procesora równoważnego Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.
Liczba procesorów zainstalowanych	Min. 1
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów, dwu lub czterordzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych

Pamięć RAM	8 GB DDR3 RDIMM 1066 MHz, płyta główna powinna obsługiwać do 192GB, na płycie głównej powinno znajdować się minimum 18 slotów przeznaczonych dla pamięci.
Zabezpieczenia pamięci RAM	SBEC, Memory Mirror
Kontroler dysków twardych	Kontroler SAS RAID w wersji SAS 2.0, pozwalający na zbudowanie minimum poziomu RAID-0, 1, 10, 5 cache 512MB, podtrzymanie bateryjne
Dyski twarde	Możliwość instalacji dysków SATA, SAS lub SSD. Zainstalowane 7 dysków SAS 146GB 10K 6G 2.5'' typu HotPlug, możliwość instalacji dodatkowego 1 dysku twardego Hot-Plug
Liczba wszystkich wnęk na dyski twarde	Minimum 8 wnęk typu hot swap 2.5in
Napęd DVD	Min. CD-RW/DVD-ROM
Interfejsy sieciowe	Minimum 2 porty 10/100/1000
Zdalne zarządzanie	Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane złącze RJ-45 i umożliwiająca: ▪ zdalny dostęp do graficznego interfejsu Web karty zarządzającej ▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera,) ▪ szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika ▪ możliwość podmontowania zdalnych wirtualnych napędów ▪ możliwość obsługi przez dwóch administratorów jednocześnie
Grafika	Zintegrowana z płytą główną
Zasilacze	Minimum 2 zasilacze, redundantne typu hot plug
Wentylatory	Zestaw wentylatorów redundantnych typu hot plug
Porty dodatkowe	Minimum 4 porty USB 2.0, 1x port szeregowy, 1x VGA
Systemy operacyjne	Wspierane systemy: Windows 2000 Server, Windows 2003 Server, RedHat Linux 5, SUSE Linux 10
Diagnostyka	Panel umożliwiający wyświetlenie informacji o stanie podzespołów serwera
Certyfikaty	ISO 9001 producenta serwera, deklaracja zgodności CE
Gwarancja	Przynajmniej trzy lata gwarancji z czasem reakcji 4 godziny od zgłoszenia. Zamawiający oczekuje możliwości przedłużenia czasu gwarancji do pięciu lat. W przypadku uszkodzenia dysków twardych naprawa w siedzibie zamawiającego i uszkodzone dyski pozostają u Zamawiającego
Zainstalowany system	SUSE Linux Enterprise Server 11, 3 lata subskrypcji lub

operacyjny	równoważny
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela

Stanowisko nadzoru mobilnego (1 szt.)
Komputer przenośny o parametrach (wymagania minimalne):

Nazwa	Opis wymagań minimalnych
Typ komputera	Notebook
Procesor	Dwurdzeniowy, Częstotliwość min. 2,4 GHz, 4MB L3 cache
Dysk	Min. 320 GB SATA, 7200 obr./min..
Wyświetlacz	W zakresie 14”-15,6” matowy podświetlanie LED
Rozdzielczość	Powyżej 1280x800, ale poniżej 1920x1080
Grafika	Nie zintegrowana 1GB DDR3 128bit
Napęd	8x DVD±RW z oprogramowaniem
Pamięć	Min 4GB DDR3 (1 slot wolny) Dwa gniazda pamięci z możliwą obsługą o łącznej pojemności min 8GB
Sieć	Wbudowana karta sieciowa 10/100/1000Mbps, wbudowana karta sieciowa bezprzewodowa obsługująca standardy 802.11 a,g,n , bluetooth 2.0
System operacyjny	Microsoft Windows 7 Professional PL 64bit
Dodatkowe oprogramowanie	Microsoft Windows Office Professional 2007 PL
Bateria	Min 8-ogniw
Złącza zewnętrzne	• 3x USB 2.0 (lub nowsze) • 1x 15-stykowe D-Sub (wyjście na monitor) • 1x RJ-45 (LAN) • wejście na mikrofon • wyjście słuchawkowe • Wejście zasilania (DC-in) • Display port • FireWire
Typ gniazda rozszerzeń	• Co najmniej 1 x Express Card
Certyfikaty	Certyfikat zgodności CE
Bezpieczeństwo	Czytnik linii papilarnych Moduł zabezpieczający TPM 1.2
Inne	Obudowa trwale oznaczona logo producenta notebooka Torba do notebooka oznaczona logo producenta notebooka Mysz dwuprzyciskowa USB z rolką Zestaw nośników systemowych Etykieta wydajności energetycznej.

Gwarancja	3 lata na miejscu u klienta; w przypadku awarii dysków twardych, uszkodzone nośniki pozostają u Zamawiającego
Inne	Oprogramowanie: klient poczty - THE BAT (lub równoważny) spełniający poniższe wymagania: • obsługa protokołów: IMAP4, POP, APOP i SMTP • obsługa: PGP oraz S/MIME • możliwość szyfrowania bazy danych programu • obsługa wtyczek • możliwość tworzenia szablonów wiadomości, także z możliwością przypisania • szablonu do poszczególnych folderów • Obsługa uwierzytelniania: zwykle, MD5 APOP, MD5 CRAM-HMAC Oprogramowanie do nadzoru dostarczonego sprzętu WinRAR lub równoważny Wymagane załączenie nośników instalacyjnych systemu operacyjnego oraz sterowniki dla systemu
Urządzenia zewnętrzne	Zewnętrzny dysk min. 500 GB w technologii SATA 2,5 cala / 7200 obr/min – interfejs USB 3.0. W przypadku braku interfejsu USB 3.0 w laptopie wykonawca dostarczy kontroler na Express Card. Zamawiający nie dopuszcza "składanych" dysków zewnętrznych (dysk+kieszeń). Pendrive 16GB min. zapis 18MB/s czytnik kart mikroprocesorowych (na USB lub wbudowany) obsługujący karty CryptoCard multiSIGN modem (na USB lub wbudowany) obsługujący GPRS, EDGE, HSDPA (bez simlocka) mogący pracować u wszystkich polskich operatorów komórkowych Napęd FDD na USB

Instruktaż techniczny

Przeprowadzony w siedzibie Zamawiającego w zakresie obsługi, nadzoru i administracji wszystkich zainstalowanych urządzeń a zwłaszcza system zabezpieczeń sprzętowo-programowych i urządzenia do weryfikacji bezpieczeństwa sieci dla min. 5 osób. Po odbyciu szkolenia Wykonawca wystawi zaświadczenia uprawniające do samodzielnej obsługi, nadzoru, administracji oraz reinstalacji urządzeń/oprogramowania objętych przedmiotem zadania bez utraty gwarancji.
W przypadku przeprowadzenia instruktażu technicznego poza siedzibą Zamawiającego wszelkie koszty pokryje Wykonawca.