ZAŁĄCZNIK NR 1.1 do SIWZ
– Budowa infrastruktury ogólnodostępnej sieci bezprzewodowej na terenie gminy Czernikowo

Założenia techniczne

Przedmiotem projektu jest zbudowanie Sieci Bezprzewodowej na terenie gminy Czernikowo.
Budowana ogólnodostępna sieć bezprzewodowa służyć ma lokalnej społeczności i zwiększyć stopień informatyzacji gospodarstw domowych na terenie gminy.
Budowana sieć ma zapewnić usługi powszechnego dostępu do Internetu dla instytucji sektora publicznego, prywatnego, klientów indywidualnych, itp.
W szczególności sieć ma być zbudowana w oparciu o elementy o parametrach nie gorszych niż zaproponowane w projekcie.
I tak:

Lp.	***nazwa rzeczywista wynikająca z urządzeń przyjętych na etapie projektu***	***nazwa***	***ilość***
1	most RB433AH	most.bezprzewodowy	14
2	AP RB433AH	punkt.dostępowy	25
3	Juniper SRX 240H	FW.brzegowy	2
4	Astaro 120	FW1	2
5	Astaro 220 HA	FW2	7
6	Astaro 320 HA	FW3	3
7	Astaro virtual	FW4	2
8	Fujitsu RX100 s6 + LT20 + KVM	srv.adm	1
9	Fujitsu RX300 s6	srv.virt	2
10	Fujitsu DX60 FC	macierz	1
11	maszt 18m	maszt 18m	14
12	Ruckus Zone Director 1000	Kontroler.wifi	1
13	Ruckus ZoneFlex 27	punkt.dostepowy.kontroler.wifi	10
14	anteny	anteny	1 kpl.
15	Przełącznik sieciowy	Sw1	4

1. most.bezprzewodowy

Platforma sprzętowa wyposażona w
- minimum 3 złącza miniPCI dla kart bezprzewodowych (dołączyć należy komplet 2 kart pracujących w standardach 802.11a/b/g/n o mocy transmisyjnej równej co najmniej wartości dozwolonej przepisami prawa w Polsce).
- złącze micro SD na kartę pamięci o pojemności min. 2GB (dołączyć należy kartę o wskazanej pojemności minimalnej)
- minimum 3 złącza Ethernet 10/100 Mb, w tym jedno pozwalające na zasilanie urządzenia poprzez kabel ethernet (dołączony odpowiedni zasilacz PoE do zestawu)
- specyfikacja temperaturowa urządzenia powinna umożliwiać pracę w warunkach zewnętrznych bez specjalnego systemu chłodzenia/ogrzewania.

Zestaw składa się z pary urządzeń umożliwiających zestawienie mostu bezprzewodowego w paśmie 5GHz. Do każdego zestawu należy dołączyć parę anten dipolarnych umożliwiających pracę wyspecyfikowanemu zestawowi w trybie umożliwiającym podwojenie szybkości transmisji poprzez transmisję sygnału jedną kartą bezprzewodową, a odbiór sygnału drugą kartą bezprzewodową.
Urządzenia muszą być zamontowane w obudowie zewnętrznej z klasą szczelności min. IP67.
Każda platforma musi posiadać odgromniki na każdym kablu antenowym i ethernetowym wychodzącym z obudowy.

2. punkt.dostępowy

Platforma sprzętowa wyposażona w
- minimum 3 złącza miniPCI dla kart bezprzewodowych (dołączyć należy komplet 3 kart pracujących w standardach 802.11a/b/g/n o mocy transmisyjnej równej co najmniej wartości dozwolonej przepisami prawa w Polsce, każde wyprowadzone na zewnątrz obudowy ze złączem „N” do podłączenia anteny zewnętrznej).
- złącze micro SD na kartę pamięci o pojemności min. 2GB (dołączyć należy kartę o wskazanej pojemności minimalnej)
- minimum 3 złącza Ethernet 10/100 Mb, w tym jedno pozwalające na zasilanie urządzenia poprzez kabel Ethernet (dołączony odpowiedni zasilacz PoE do zestawu)
- specyfikacja temperaturowa urządzenia powinna umożliwiać pracę w warunkach zewnętrznych bez specjalnego systemu chłodzenia/ogrzewania.

Do każdego zestawu należy dołączyć anteny pracujące w paśmie 2,4GHz zgodnie z zestawieniem.
Urządzenia muszą być zamontowane w obudowie zewnętrznej z klasą szczelności min. IP67.
Każda platforma musi posiadać odgromniki na każdym kablu antenowym i ethernetowym wychodzącym z obudowy.

3. FW.brzegowy

1. Firewall musi być dedykowanym urządzeniem sieciowym o wysokości maksymalnie 1 U.

2. Urządzenie powinno być wyposażone w co najmniej 1 GB pamięci RAM, pamięć Flash o wielkości co najmniej 1 GB oraz port konsoli. Urządzenie powinno posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi istnieć możliwość uruchomienia systemu operacyjnego firewalla z nośnika danych podłączonego do slotu USB na module kontrolnym.
3. System operacyjny firewalla powinien posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł routingu IP, odpowiedzialny za ustalenie tras routingu i zarządzanie urządzeniem musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. System operacyjny firewalla musi śledzić stan sesji użytkowników (*stateful processing*), tworzyć i zarządzać tablicą stanu sesji. Musi istnieć opcja przełączenia urządzenia w tryb pracy bez śledzenia stanu sesji użytkowników, jak również wyłączenia części ruchu ze śledzenia stanu sesji.
4. Urządzenie powinno być wyposażone w nie mniej niż 16 wbudowanych interfejsów Ethernet 10/100/1000 (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji).
5. Urządzenie musi być wyposażone w minimum 4 sloty na dodatkowe karty z modułami interfejsów. Urządzenie musi obsługiwać co najmniej następującej rodzaje kart z modułami interfejsów: ADSL 2/2+, Serial, E1, Gigabit Ethernet (SFP).
6. Firewall musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż 32 strefami bezpieczeństwa z wydajnością nie mniejszą niż 500 Mb/s liczoną dla ruchu IMIX. Firewall musi przetworzyć nie mniej niż 200 000 pakietów/sekundę (dla pakietów 64-bajtowych). Firewall musi obsłużyć nie mniej niż 128 000 równoległych sesji oraz zestawić nie mniej niż 9 000 nowych połączeń/sekundę.
7. Firewall musi mieć możliwość zestawiania zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN musi być realizowany sprzętowo. Firewall musi obsługiwać nie mniej niż 1 000 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 250 Mb/s. Urządzenie musi posiadać możliwość udostępniania użytkownikom wbudowanego klienta IPSec VPN za pośrednictwem strony WWW.
8. Polityka bezpieczeństwa systemu zabezpieczeń powinna uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Firewall musi umożliwiać zdefiniowanie nie mniej niż 4 000 reguł polityki bezpieczeństwa.
9. Firewall musi posiadać funkcję wykrywania i blokowania ataków intruzów (IPS, *intrusion prevention*) realizowaną sprzętowo. System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące (D)DoS oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych ataków (intruzów, robaków) musi odbywać się w regułach polityki bezpieczeństwa. System firewall musi realizować zadania IPS z wydajnością nie mniejszą niż 250 Mb/s. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall. Baza sygnatur ataków musi być aktualizowana przez producenta codziennie. Dopuszcza się możliwość uruchomienia tego modułu za pomocą dodatkowej licencji.
10. Urządzenie zabezpieczeń musi posiadać wbudowany moduł kontroli antywirusowej kontrolujący pocztę elektroniczną (SMTP, POP3, IMAP), FTP oraz HTTP. Włączenie kontroli antywirusowej nie

może wymagać dodatkowego serwera. Kontrola antywirusowa musi być realizowana sprzętowo z wydajnością nie mniejszą niż 85 Mb/s dla ruchu HTTP. Musi istnieć możliwość wyboru działania mechanizmu kontroli antywirusowej w trybie sprzętowym i programowym. Dopuszcza się możliwość uruchomienia tego modułu za pomocą dodatkowej licencji.

11. Urządzenie zabezpieczeń musi posiadać wbudowany moduł kontroli antyspamowej działający w oparciu o mechanizm blacklist. Włączenie kontroli antyspamowej nie może wymagać dodatkowego serwera. Dopuszcza się możliwość uruchomienia tego modułu za pomocą dodatkowej licencji.
12. Urządzenie zabezpieczeń musi posiadać wbudowany moduł filtrowania stron WWW w zależności od kategorii treści stron. Włączenie filtrowania stron WWW nie może wymagać dodatkowego serwera. Dopuszcza się możliwość uruchomienia tego modułu za pomocą dodatkowej licencji.
13. Urządzenie zabezpieczeń musi posiadać funkcję filtrowania zawartości ruchu HTTP, FTP i protokołów poczty elektronicznej (SMTP, POP3, IMAP) w celu blokowania potencjalnie szkodliwych obiektów. Urządzenie musi filtrować ruch na podstawie kryteriów obejmujących co najmniej: typy MIME, rozszerzenia plików, elementy ActiveX, Java i cookies.
14. Urządzenie musi obsługiwać protokoły dynamicznego rutingu: RIP, OSPF oraz BGP. Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 20 wirtualnych ruterów.
15. Urządzenie musi posiadać możliwość uruchomienia funkcji MPLS z sygnalizacją LDP i RSVP w zakresie VPLS i L3 VPN.
16. Urządzenie musi obsługiwać co najmniej 512 sieci VLAN z tagowaniem 802.1Q. W celu zapobiegania zapętlania się ruchu w warstwie 2 firewall musi obsługiwać protokoły Spanning Tree (802.1D), Rapid STP (802.1W) oraz Multiple STP (802.1S). Urządzenie musi obsługiwać protokół LACP w celu agregowania fizycznych połączeń Ethernet.
17. Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p oraz parametrów z nagłówków TCP i UDP. Urządzenie musi posiadać możliwość tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach.
18. Firewall musi pracować w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń. Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
19. Zarządzanie urządzeniem musi odbywać się za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH. Firewall musi posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta.
20. Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji.
21. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone są w języku polskim.

22. Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przez okres 3 lat. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu, wymianę uszkodzonego sprzętu na następny dzień roboczy, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

4. FW1

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 (IPS/IDS)
- VPN zgodny z IPSec, PPTP, L2TP i SSL-VPN
- Antyspam
- Filtracja stron WWW
- Kontrola pasma (Traffic Management)

Typ urządzenia
Urządzenie typu UTM, zapewniające funkcjonalności: Firewall, Gateway VPN, ochrona przed wirusami, spyware, system IPS, filtrowanie treści, działające w klastrze wysokiej dostępności Active-Passive

Specyfikacja fizyczna urządzenia

Dedykowane rozwiązanie sprzętowe
Obudowa Standalone
Pamięć RAM: minimum 1 GB
Storage: rozwiązanie wyposażone w dysk twardy, przestrzeń dyskowa minimum 70 GB
Ilość interfejsów:
- nie mniej niż 4 konfigurowalnych interfejsów Ethernet
- nie mniej niż 2 interfejsy USB

Wydajność urządzeń pracujących w klastrze HA Active-Passive
Obsługa nielimitowanej ilości hostów w sieci chronionej
Przepustowość zapory sieciowej nie mniejsza niż 200 Mbps.
Przepustowość modułu VPN (AES) nie mniejsza niż 85 Mbps.
Ilość jednocześnie obsługiwanych sesji: nie mniej niż 85 000.

Funkcjonalności urządzeń w zakresie konfiguracji połączeń zdalnych VPN
- Minimalna ilość jednocześnie obsługiwanych połączeń SSL VPN: 10.
- Minimalna ilość klientów VPN SSL w cenie urządzenia: 40.

• Wspierane mechanizmy uwierzytelniania i szyfrowania: 3DES, AES (128, 192, 256-bit), MD5, SHA-1.
• Wspierane mechanizmy wymiany kluczy: Manual Key, PKI (X.509).
• Obsługa funkcjonalności: L2TP IPSec oraz DHCP over VPN.

Sieciowe funkcjonalności urządzeń

Możliwość pracy jako Router lub Bridge
• Obsługa nie mniej niż 512 sieci VLAN działających zgodnie ze standardem 802.1Q.
• Wbudowany serwer DHCP umożliwiający przydzielanie adresów statycznie, dynamicznie, przekierowanie zgłoszeń do zewnętrznego serwera DHCP.
• Wsparcie mechanizmów NAT: 1:1, 1:many, many:1, many:many.
• Możliwość kreowania reguł routingu statycznego
• Wsparcie dynamicznych protokołów routingu: OSPF i wsparcie dla routowania transmisji multicast.
• Wsparcie funkcjonalności QoS: DSCP-bits, 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 reguł równoważenia obciążeń dla ruchu przychodzącego do hostów znajdujących się w sieci chronionej.
• Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), pełna kompatybilność z większością urządzeń i serwerów VoIP.

Funkcjonalności urządzeń w zakresie uwierzytelniania użytkowników
Lokalna baza użytkowników umożliwiająca wykreowanie nie mniej niż 50 kont.
Uwierzytelnianie użytkowników w oparciu o: Active Directory, LDAP, lokalna baza użytkowników – system powinien oferować mechanizm Single Sign-On.

Funkcjonalności urządzeń w zakresie zarządzania i wysokiej dostępności
• Możliwość zarządzania urządzeniem poprzez wbudowany interfejs webowy dostępny przez HTTPS
• Praca w klastrze wysokiej dostępności w trybie Active – Passive.

Funkcjonalności urządzeń w zakresie mechanizmów filtrowania Deep Packet Inspection i Statefull Packet Inspection
• Możliwość kreowania reguł Firewall dla ruchu przychodzącego/wychodzącego z/do poszczególnej podsieci, 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:
• sonda IPS (detekcja i blokowanie wtargnięć do sieci) zapewniająca skanowanie ruchu w oparciu o sygnatury dostarczone przez producenta. System musi rozpoznawać i blokować ataki dla dedykowanych usług takich jak: serwery pocztowe, serwery webowe, ataki na aplikacje np. MS Office i inne.
• Wymagana jest możliwość włączenia lub wyłączenia usługi IPS dla poszczególnych maszyn/podsieci

• Wymagana jest możliwość skonfigurowania połączeń VPN (SSL lub IPSec) client-site, aby cały ruch z połączonych do urządzeń klientów przesyłany był poprzez urządzenia i możliwe było jego skanowanie przez mechanizmy bezpieczeństwa.

Rozwiązanie do raportowania
Wymagane jest aby dostarczone rozwiązanie zapewniało monitorowanie, rejestrację i graficzną prezentację danych dotyczących zdarzeń obsługiwanych przez mechanizmy bezpieczeństwa. Wymagane jest aby rozwiązanie oferowało zestaw zdefiniowanych typów raportów. Niezbędne dane to średnia zajętość łącza w podziale na dni i godziny, informacje dotyczące ataków, detekcji intruzów, zagrożeń antywirusowych. Wymagane jest aby rozwiązanie raportujące było tego samego producenta co oferowany system bezpieczeństwa. Dopuszcza się rozwiązania zintegrowane jak i narzędzia zewnętrzne.

Rozwiązanie do centralnego zarządzania
Dostawca zobowiązany jest dostarczyć system centralnego zarządzania wszystkim rozwiązaniami bezpieczeństwa. Wymagane jest aby system centralnego zarządzania był tego samego producenta co rozwiązania bezpieczeństwa i umożliwiał instalację na dowolnym serwerze lub na wirtualnej maszynie zgodnej z VMWare. System centralnego zarządzania powinien oferować monitorowanie wszystkich urządzeń w czasie rzeczywistym, pokazując stany urządzeń, obciążenie maszyn, stan aktualizacji. System powinien umożliwiać automatyczne konfigurowanie połączeń VPN Site-to-Site pomiędzy wybranymi urządzeniami oraz zapewniać dostęp do interfejsu zarządzającego oparty na rolach.

Gwarancja, wsparcie techniczne i aktualizacja systemu
Wymagane jest aby dostarczane urządzenia objęte były okresem gwarancji przez okres minimum 3 lat, z możliwością przedłużenia na dłuższy okres czasu. Wymagane jest, aby w ramach gwarancji uszkodzone urządzenie zostało naprawione w czasie nie dłuższym niż 10 dni roboczych od dostarczenia do wskazanego punktu serwisowego. Wymagane jest, aby urządzenia objęte było wsparciem technicznym minimum 8x5 (wraz z możliwością dokonywania aktualizacji oprogramowania up-to-date w ramach posiadanego wsparcia technicznego), realizowanym przez producenta przez okres minimum 3 lat z możliwością przedłużenia na dłuższy okres czasu.

5. FW2

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 (IPS)
• VPN zgodny z IPSec, PPTP, L2TP i SSL-VPN
• Antyspam
• Filtracja stron WWW

• Kontrola pasma (Traffic Management);

Typ urządzenia
Urządzenie typu UTM, zapewniające funkcjonalności: Firewall, Gateway VPN, ochrona przed wirusami, spyware, system IPS, filtrowanie treści, działające w klastrze wysokiej dostępności Active-Passive

Specyfikacja fizyczna urządzenia
Dedykowane rozwiązanie sprzętowe
Obudowa 1U przeznaczona do montażu w szafie RACK
Pamięć RAM: minimum 1 GB
Storage: rozwiązanie wyposażone w dysk twardy, przestrzeń dyskowa minimum 70 GB
Ilość interfejsów:
• nie mniej niż 8 konfigurowalnych interfejsów Gigabit Ethernet
• nie mniej niż 2 interfejsy USB

Wydajność urządzeń pracujących w klastrze HA Active-Passive
Obsługa nielimitowanej ilości hostów w sieci chronionej
Przepustowość zapory sieciowej nie mniejsza niż 1,6 Gbps.
Przepustowość modułu VPN (AES) nie mniejsza niż 250 Mbps.
Ilość jednocześnie obsługiwanych sesji: nie mniej niż 280 000.

Funkcjonalności urządzeń w zakresie konfiguracji połączeń zdalnych VPN
• Minimalna ilość jednocześnie obsługiwanych połączeń SSL VPN: 80.
• Minimalna ilość klientów VPN SSL w cenie urządzenia: 200.
• Wspierane mechanizmy uwierzytelniania i szyfrowania: 3DES, AES (128, 192, 256-bit), MD5, SHA-1.
• Wspierane mechanizmy wymiany kluczy: Manual Key, PKI (X.509).
• Obsługa funkcjonalności: L2TP IPSec oraz DHCP over VPN.

Sieciowe funkcjonalności urządzeń
Możliwość pracy jako Router lub Bridge
• Obsługa nie mniej niż 512 sieci VLAN działających zgodnie ze standardem 802.1Q.
• Wbudowany serwer DHCP umożliwiający przydzielanie adresów statycznie, dynamicznie, przekierowanie zgłoszeń do zewnętrznego serwera DHCP.
• Wsparcie mechanizmów NAT: 1:1, 1:many, many:1, many:many.
• Możliwość kreowania reguł routingu statycznego
• Wsparcie dynamicznych protokołów routingu: OSPF i wsparcie dla routowania transmisji multicast.
• Wsparcie funkcjonalności QoS: DSCP-bits, 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 reguł równoważenia obciążeń dla ruchu przychodzącego do hostów znajdujących się w sieci chronionej.
• Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), pełna kompatybilność z większością urządzeń i serwerów VoIP.

Funkcjonalności urządzeń w zakresie uwierzytelniania użytkowników
Lokalna baza użytkowników umożliwiająca wykreowanie nie mniej niż 200 kont.
Uwierzytelnianie użytkowników w oparciu o: Active Directory, LDAP, lokalna baza użytkowników – system powinien oferować mechanizm Single Sign-On.
Wymagane jest, aby uwierzytelnianie użytkowników odbywało się z lokalnej bazy, skonfigurowanej na urządzeniu lub z zewnętrznego serwera Active Directory.

Funkcjonalności urządzeń w zakresie zarządzania i wysokiej dostępności
- Możliwość zarządzania urządzeniem poprzez wbudowany interfejs webowy dostępny przez: HTTPS
- Praca w klastrze wysokiej dostępności w trybie Active – Passive.

Funkcjonalności urządzeń w zakresie mechanizmów filtrowania Deep Packet Inspection i Statefull Packet Inspection
- Możliwość kreowania reguł Firewall dla ruchu przychodzącego/wychodzącego z/do poszczególnej podsieci, 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:
- sonda IPS (detekcja i blokowanie wtargnięć do sieci) zapewniająca skanowanie ruchu w oparciu o sygnatury dostarczone przez producenta. System musi rozpoznawać i blokować ataki dla dedykowanych usług takich jak: serwery pocztowe, serwery webowe, ataki na aplikacje np. MS Office i inne.
- Wymagana jest możliwość włączenia lub wyłączenia usługi IPS dla poszczególnych maszyn/podsieci
- Wymagana jest możliwość skonfigurowania połączeń VPN (SSL lub IPSec) client-site, aby cały ruch z połączonych do urządzeń klientów przesyłany

Rozwiązanie do raportowania
Wymagane jest aby dostarczone rozwiązanie zapewniało monitorowanie, rejestrację i graficzną prezentację danych dotyczących zdarzeń obsługiwanych przez mechanizmy bezpieczeństwa. Wymagane jest aby rozwiązanie oferowało zestaw zdefiniowanych typów raportów. Niezbędne dane to średnia zajętość łącza w podziale na dni i godziny, informacje dotyczące ataków, detekcji intruzów, zagrożeń antywirusowych. Wymagane jest aby rozwiązanie raportujące było tego samego producenta co oferowany system bezpieczeństwa. Dopuszcza się rozwiązania zintegrowane jak i narzędzia zewnętrzne.

Rozwiązanie do centralnego zarządzania
Dostawca zobowiązany jest dostarczyć system centralnego zarządzania wszystkim rozwiązaniami bezpieczeństwa. Wymagane jest aby system centralnego zarządzania był tego samego producenta co rozwiązania bezpieczeństwa i umożliwiał instalację na dowolnym serwerze lub na wirtualnej maszynie zgodnej z VMWare. System centralnego zarządzania powinien oferować monitorowanie wszystkich urządzeń w czasie rzeczywistym, pokazując stany urządzeń, obciążenie maszyn, stan aktualizacji. System powinien umożliwiać automatyczne konfigurowanie połączeń VPN Site-to-Site

pomiędzy wybranymi urządzeniami oraz zapewniać dostęp do interfejsu zarządzającego oparty na rolach.

Gwarancja, wsparcie techniczne i aktualizacja systemu
Wymagane jest aby dostarczane urządzenia objęte były okresem gwarancji przez okres minimum 3 lat, z możliwością przedłużenia na dłuższy okres czasu. Wymagane jest, aby w ramach gwarancji uszkodzone urządzenie zostało naprawione w czasie nie dłuższym niż 10 dni roboczych od dostarczenia do wskazanego punktu serwisowego. Wymagane jest, aby urządzenia objęte było wsparciem technicznym minimum 8x5 (wraz z możliwością dokonywania aktualizacji oprogramowania up-to-date w ramach posiadanego wsparcia technicznego), realizowanym przez producenta przez okres minimum 3 lat z możliwością przedłużenia na dłuższy okres czasu.

6. FW3

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 (IPS)
- VPN zgodny z IPSec, PPTP, L2TP i SSL-VPN
- Antyspam
- Filtracja stron WWW
- Kontrola pasma (Traffic Management);

Typ urządzenia
Urządzenie typu UTM, zapewniające funkcjonalności: Firewall, Gateway VPN, ochrona przed wirusami, spyware, system IPS, filtrowanie treści, działające w klastrze wysokiej dostępności Active-Passive

Specyfikacja fizyczna urządzenia
Dedykowane rozwiązanie sprzętowe
Obudowa 1U przeznaczona do montażu w szafie RACK
Pamięć RAM: minimum 2 GB
Storage: rozwiązanie wyposażone w dysk twardy, przestrzeń dyskowa minimum 70 GB
Ilość interfejsów:
- nie mniej niż 8 konfigurowalnych interfejsów Gigabit Ethernet
- nie mniej niż 2 interfejsy USB

Wydajność urządzeń pracujących w klastrze HA Active-Passive
Obsługa nielimitowanej ilości hostów w sieci chronionej
Przepustowość zapory sieciowej nie mniejsza niż 3,0 Gbps.
Przepustowość modułu VPN nie mniejsza niż 320 Mbps.

Ilość jednocześnie obsługiwanych sesji: nie mniej niż 600 000.

Funkcjonalności urządzeń w zakresie konfiguracji połączeń zdalnych VPN

- Minimalna ilość jednocześnie obsługiwanych połączeń SSL VPN: 200.
- Minimalna ilość klientów VPN SSL w cenie urządzenia: 400.
- Wspierane mechanizmy uwierzytelniania i szyfrowania: 3DES, AES (128, 192, 256-bit), MD5, SHA-1.
- Wspierane mechanizmy wymiany kluczy: Manual Key, PKI (X.509).
- Obsługa funkcjonalności: L2TP IPSec oraz DHCP over VPN.

Sieciowe funkcjonalności urządzeń

Możliwość pracy jako Router lub Bridge

- 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.
- Wsparcie mechanizmów NAT: 1:1, 1:many, many:1, many:many.
- Możliwość kreowania reguł routingu statycznego
- Wsparcie dynamicznych protokołów routingu: OSPF i wsparcie dla routowania transmisji multicast.
- Wsparcie funkcjonalności QoS: DSCP-bits, 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 reguł równoważenia obciążeń dla ruchu przychodzącego do hostów znajdujących się w sieci chronionej.
- Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), pełna kompatybilność z większością urządzeń i serwerów VoIP.

Funkcjonalności urządzeń w zakresie uwierzytelniania użytkowników

Lokalna baza użytkowników umożliwiająca wykreowanie nie mniej niż 500 kont.
Uwierzytelnianie użytkowników w oparciu o: Active Directory, LDAP, lokalna baza użytkowników – system powinien oferować mechanizm Single Sign-On.
Wymagane jest, aby uwierzytelnianie użytkowników odbywało się z lokalnej bazy, skonfigurowanej na urządzeniu lub z zewnętrznego serwera Active Directory.

Funkcjonalności urządzeń w zakresie zarządzania i wysokiej dostępności

- Możliwość zarządzania urządzeniem poprzez wbudowany interfejs webowy dostępny przez: HTTPS
- Praca w klastrze wysokiej dostępności w trybie Active – Passive.

Funkcjonalności urządzeń w zakresie mechanizmów filtrowania Deep Packet Inspection i Statefull Packet Inspection

- Możliwość kreowania reguł Firewall dla ruchu przychodzącego/wychodzącego z/do poszczególnej podsieci, 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:

- sonda IPS (detekcja i blokowanie wtargnięć do sieci) zapewniająca skanowanie ruchu w oparciu o sygnatury dostarczone przez producenta. System musi rozpoznawać i blokować ataki dla dedykowanych usług takich jak: serwery pocztowe, serwery webowe, ataki na aplikacje np. MS Office i inne.
- Wymagana jest możliwość włączenia lub wyłączenia usługi IPS dla poszczególnych maszyn/podsieci
- Wymagana jest możliwość skonfigurowania połączeń VPN (SSL lub IPSec) client-site, aby cały ruch z połączonych do urządzeń klientów przesyłany

Rozwiązanie do raportowania

Wymagane jest aby dostarczone rozwiązanie zapewniało monitorowanie, rejestrację i graficzną prezentację danych dotyczących zdarzeń obsługiwanych przez mechanizmy bezpieczeństwa. Wymagane jest aby rozwiązanie oferowało zestaw zdefiniowanych typów raportów. Niezbędne dane to średnia zajętość łącza w podziale na dni i godziny, informacje dotyczące ataków, detekcji intruzów, zagrożeń antywirusowych. Wymagane jest aby rozwiązanie raportujące było tego samego producenta co oferowany system bezpieczeństwa. Dopuszcza się rozwiązania zintegrowane jak i narzędzia zewnętrzne.

Rozwiązanie do centralnego zarządzania

Dostawca zobowiązany jest dostarczyć system centralnego zarządzania wszystkim rozwiązaniami bezpieczeństwa. Wymagane jest aby system centralnego zarządzania był tego samego producenta co rozwiązania bezpieczeństwa i umożliwiał instalację na dowolnym serwerze lub na wirtualnej maszynie zgodnej z VMWare. System centralnego zarządzania powinien oferować monitorowanie wszystkich urządzeń w czasie rzeczywistym, pokazując stany urządzeń, obciążenie maszyn, stan aktualizacji. System powinien umożliwiać automatyczne konfigurowanie połączeń VPN Site-to-Site pomiędzy wybranymi urządzeniami oraz zapewniać dostęp do interfejsu zarządzającego oparty na rolach.

Gwarancja, wsparcie techniczne i aktualizacja systemu

Wymagane jest aby dostarczane urządzenia objęte były okresem gwarancji przez okres minimum 3 lat, z możliwością przedłużenia na dłuższy okres czasu. Wymagane jest, aby w ramach gwarancji uszkodzone urządzenie zostało naprawione w czasie nie dłuższym niż 10 dni roboczych od dostarczenia do wskazanego punktu serwisowego. Wymagane jest, aby urządzenia objęte było wsparciem technicznym minimum 8x5 (wraz z możliwością dokonywania aktualizacji oprogramowania up-to-date w ramach posiadanego wsparcia technicznego), realizowanym przez producenta przez okres minimum 3 lat z możliwością przedłużenia na dłuższy okres czasu.

7. FW4

System zabezpieczeń sprzętowo-programowych

System musi obsługiwać co najmniej 480 użytkowników w ramach realizowanych systemów zabezpieczeń i umożliwiać realizację następujących funkcji:

- Firewall klasy Stateful Inaspection
- Antywirus

- System detekcji i prewencji włamań (IPS)
- VPN zgodny z IPSec, PPTP, L2TP i SSL-VPN
- Antyspam
- Filtracja stron WWW
- Kontrola pasma (Traffic Management);

Typ urządzenia
Rozwiązanie typu UTM, zapewniające funkcjonalności: Firewall, Gateway VPN, ochrona przed wirusami, spyware, system IPS, filtrowanie treści, działające w klastrze wysokiej dostępności Active-Passive, dostępne na platformie software'owej jako wirtualna maszyna, kompatybilna z VMWare (potwierdzone certyfikatem VMWare Ready).

Specyfikacja fizyczna rozwiązania
Obsługa nie mniej niż 480 użytkowników.
Obsługa interfejsów sieciowych:
- nie mniej niż 8 kart Gigabit Ethernet z możliwością dowolnej ich konfiguracji

Funkcjonalności rozwiązania w zakresie konfiguracji połączeń zdalnych VPN
- Minimalna ilość jednocześnie obsługiwanych połączeń SSL VPN: 300.
- Minimalna ilość klientów VPN SSL w cenie urządzenia: 500.
- Wspierane mechanizmy uwierzytelniania i szyfrowania: 3DES, AES (128, 192, 256-bit), MD5, SHA-1.
- Wspierane mechanizmy wymiany kluczy: Manual Key, PKI (X.509).
- Obsługa funkcjonalności: L2TP IPSec oraz DHCP over VPN.

Sieciowe funkcjonalności urządzeń

Możliwość pracy jako Router lub Bridge
- 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.
- Wsparcie mechanizmów NAT: 1:1, 1:many, many:1, many:many.
- Możliwość kreowania reguł routingu statycznego
- Wsparcie dynamicznych protokołów routingu: OSPF i wsparcie dla routowania transmisji multicast.
- Wsparcie funkcjonalności QoS: DSCP-bits, 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 reguł równoważenia obciążeń dla ruchu przychodzącego do hostów znajdujących się w sieci chronionej.
- Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), pełna kompatybilność z większością urządzeń i serwerów VoIP.

Funkcjonalności urządzeń w zakresie uwierzytelniania użytkowników
Lokalna baza użytkowników umożliwiająca wykreowanie nie mniej niż 480 kont.

Uwierzytelnianie użytkowników w oparciu o: Active Directory, LDAP, lokalna baza użytkowników – system powinien oferować mechanizm Single Sign-On.
Wymagane jest, aby uwierzytelnianie użytkowników odbywało się z lokalnej bazy, skonfigurowanej na urządzeniu lub z zewnętrznego serwera Active Directory.

Funkcjonalności urządzeń w zakresie zarządzania i wysokiej dostępności
- Możliwość zarządzania urządzeniem poprzez wbudowany interfejs webowy dostępny przez: HTTPS
- Praca w klastrze wysokiej dostępności w trybie Active – Passive.

Funkcjonalności rozwiązania w zakresie mechanizmów filtrowania Deep Packet Inspection i Statefull Packet Inspection
- Możliwość kreowania reguł Firewall dla ruchu przychodzącego/wychodzącego z/do poszczególnej podsieci, 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:
- sonda IPS (detekcja i blokowanie wtargnięć do sieci) zapewniająca skanowanie ruchu w oparciu o sygnatury dostarczone przez producenta. System musi rozpoznawać i blokować ataki dla dedykowanych usług takich jak: serwery pocztowe, serwery webowe, ataki na aplikacje np. MS Office i inne.
- Wymagana jest możliwość włączenia lub wyłączenia usługi IPS dla poszczególnych maszyn/podsieci
- Wymagana jest możliwość skonfigurowania połączeń VPN (SSL lub IPSec) client-site, aby cały ruch z połączonych do urządzeń klientów przesyłany

Rozwiązanie do raportowania
Wymagane jest aby dostarczone rozwiązanie zapewniało monitorowanie, rejestrację i graficzną prezentację danych dotyczących zdarzeń obsługiwanych przez mechanizmy bezpieczeństwa. Wymagane jest aby rozwiązanie oferowało zestaw zdefiniowanych typów raportów. Niezbędne dane to średnia zajętość łącza w podziale na dni i godziny, informacje dotyczące ataków, detekcji intruzów, zagrożeń antywirusowych. Wymagane jest aby rozwiązanie raportujące było tego samego producenta co oferowany system bezpieczeństwa. Dopuszcza się rozwiązania zintegrowane jak i narzędzia zewnętrzne.

Rozwiązanie do centralnego zarządzania
Dostawca zobowiązany jest dostarczyć system centralnego zarządzania wszystkim rozwiązaniami bezpieczeństwa. Wymagane jest aby system centralnego zarządzania był tego samego producenta co rozwiązania bezpieczeństwa i umożliwiał instalację na dowolnym serwerze lub na wirtualnej maszynie zgodnej z VMWare. System centralnego zarządzania powinien oferować monitorowanie wszystkich urządzeń w czasie rzeczywistym, pokazując stany urządzeń, obciążenie maszyn, stan aktualizacji. System powinien umożliwiać automatyczne konfigurowanie połączeń VPN Site-to-Site pomiędzy wybranymi urządzeniami oraz zapewniać dostęp do interfejsu zarządzającego oparty na rolach.

Gwarancja, wsparcie techniczne i aktualizacja systemu

Wymagane jest aby dostarczane rozwiązania objęte były okresem gwarancji przez okres minimum 3 lat, z możliwością przedłużenia na dłuższy okres czasu. Wymagane jest, aby rozwiązanie objęte było wsparciem technicznym minimum 8x5 (wraz z możliwością dokonywania aktualizacji oprogramowania up-to-date w ramach posiadanego wsparcia technicznego), realizowanym przez producenta przez okres minimum 3 lat z możliwością przedłużenia na dłuższy okres czasu.

8. srv.adm

Parametry techniczne	**Wymagane minimum**
Obudowa	typu rack , wysokość nie więcej niż 1U
Procesor	procesor w architekturze x86, osiągające w testach wydajnościowych SPECint_rate2006 min. 110 pkt
Płyta główna	Dedykowana serwerowa, wyprodukowana i zaprojektowana przez producenta serwera, karty rozszerzeń - min 2 sloty PCI Express x8 generacji 2, minimum 4 gniazda pamięci RAM DDR3,
Pamięć RAM	-Nie mniej niż 8GB RAM DDR2-800MHz -możliwość rozbudowy do minimum 32 GB.
HDD	Dwa dyski twarde typu SATA, nie mniejsze niż 2TB 7.2K HOT PLUG 3.5" 7,2 tyś. obrotów, dysk wewnątrz serwera
Kontroler dysków	kontroler SAS z obsługą RAID 0, 1
Napęd optyczny	DVD +/- RW wewnętrzny
Karta graficzna	Zintegrowana z płytą główną
Karty sieciowe	-2 karty sieciowe (dopuszcza się zintegrowane), typu Ethernet 10/100/1000 (akceleracja TCP/IP), rozruch PXE przez sieć LAN z serwera PXE, rozruch iSCSI przez zintegrowaną kartę sieci LAN -1 dedykowana karta Ethernet 10/100 wyłącznie dla komunikacji z kontrolerem zdalnego zarządzania,redundancja interfejsu zarządzającego poprzez przejęcie jego funkcjonalności w przypadku usterki przez jedną z dwóch kart Ethernet 10/100/1000 - dodatkowa dwuportowa karta sieciowa Ethernet 10/100/1000
Zasilanie i chłodzenie	zasilacz o mocy max. 350W
Zarządzanie zdalne, inwentaryzacja	Zintegrowany z płytą główną kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzanie włącznie z przejęciem zdalnym konsoli tekstowej (możliwość dokupienia opcji przejęcia konsoli graficznej oraz zdalnego podłączenia napędów). Dedykowana karta LAN 10/100 Mb/s do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym serwera. Umieszczona z przodu chowana karta identyfikacyjna serwera zawierająca nazwę serwera, numer handlowy, numer seryjny, adresy

Parametry techniczne	Wymagane minimum
	kart sieciowych
Porty I/O	Minimum 8 portów USB 2.0 w tym 2 porty USB z przodu obudowy, port szeregowy, minimum dwa port RJ45 – nie dopuszcza się stosowania przejściówek, adapterów oraz rozgałęziaczy i przedłużaczy.
Oprogramowanie	Oprogramowanie zarządzające wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera macierzy, instalację systemów operacyjnych, zdalne zarządzanie, przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska, dostęp przez przeglądarkę WWW, szyfrowane połączenie HTTPS/SSL 128-bit, możliwość przekierowania alertów dla administratorów na sms lub mail, obsługa min 12 kont administratorów,
Obudowa	Obudowa typu Rack , wysokość nie więcej niż 1U, elementy montażowe do zabudowy w szafie rack, uchylne ramię dla prowadzenia kabli podczas wysuwania i wsuwania serwera w szafie rack
Wsparcie dla systemów operacyjnych	Wymagana kompatybilność i wspomaganie (support) serwera dla następujących systemów operacyjnych: Microsoft: Windows 2008 R2, SUSE LINUX SLES-10 X86, Red Hat LINUX RHEL5 X86
Certyfikaty producenta	Certyfikat producenta ISO 9001 w zakresie projektowania, produkcji i serwisu produktów, CE oraz ISO 14001.
Dokumentacja	Karty gwarancyjne, instrukcje, licencje oprogramowania, nośniki ze sterownikami
System Operacyjny	Microsoft Windows 2008 R2 Standard
Inne	Kable zasilające
Gwarancja	3 lata gwarancji na części i robociznę realizowana w siedzibie klienta z czasem reakcji telefonicznej na drugi dzień roboczy (wymagane oświadczenie producenta serwera)
Inne	Dostarczony sprzęt musi być fabrycznie nowy, pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Producent sprzętu musi potwierdzić dokumentami, że oferowany do przetargu sprzęt spełnia ten wymóg. (Wymagane oświadczenie producenta). Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane (wymagane oświadczenie producenta dołączone do oferty) oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne. Oferent zobowiązany jest dostarczyć wraz z ofertą, szczegółową specyfikację techniczną oferowanego sprzętu. Dostępność części zamiennych co najmniej 5 lat po zakończeniu produkcji serwera (potwierdzone przez producenta)
Dodatkowe interfejsy	Interfejs do podłączenia biblioteki taśmowej wyspecyfikowanej poniżej

Dodatkowo należy dołączyć współpracującą bibliotekę taśmową o poniższych parametrach minimalnych:

Typ napędu:	LTO-4 HalfHeight
Liczba napędów:	1 szt.
Liczba slotów:	8 szt.
Liczba magazynów:	2 szt. po 4 sloty
Liczba slotów Import/Export tzw. mail slot dla wymiany nośników bez przerywania pracy napędu	1 szt.
Wbudowany skaner kodów paskowych na nośnikach LTO	TAK
Pojemność bez kompresji:	do 6,4TB
Pojemność z kompresją:	do 12,8 TB
Maksymalny transfer bez kompresji:	288MB/h
Maksymalny transfer z kompresją:	576MB/h
Zakres zmian prędkości zapisu:	min.35MB/s do 80MB/s
Interfejs:	SAS 3Gb/s
Rozmiar bufora wewnętrznego:	128kB
Obudowa:	Rack 19” 1U
Zdalne zarządzanie:	TAK
Zintegrowany moduł ADI (Automation Driver Interface)	TAK
Lokalne zarządzanie za pomocą panelu/pulpitu operatora	TAK
Interfejs zdalnego zarządzania	Ethernet 10/100Mb/s złącze RJ-45
Zabezpieczenie dostępu panelu /pulpitu operatora hasłem/kodem	TAK
Zabezpieczenie hasłem lub kodem interfejsu zdalnego zarządzania	TAK
Obsługa przez moduł zdalnego zarządzania adresacji IP v4/v6	TAK
Obsługa protokołu SNMP przez	
modułu zarządzania	TAK
Obsługa szyfrowania danych na nośniku LTO-4	TAK
Możliwość zdalnego odłączenia magazynku z kasetami	TAK
Obsługa nośników LTO-4 WORM	TAK
Maksymalny pobór mocy	60W
Do urządzenia dołączyć należy:	- szyny do montażu w szafie rack 19” - zewnętrzny kabel SAS 3Gb/s - 1 kaseta czyszcząca LTO - 14 kaset z taśmami do wyspecyfikowanego napędu - Oprogramowanie pozwalające na wykonywanie kopii zapasowych na wyspecyfikowanej bibliotece taśmowej

Do zestawu należy dołączyć również konsole KVM z monitorem mim. 17”, klawiaturą i touchpadem. Konsola musie mieć możliwość podpięcia min. 8 serwerów. Dołączyć należy komplet kabli przyłączeniowych.

9. srv.virt

Element składowy dostawy	***Ilość i cechy techniczne***
Obudowa	typu rack , wysokość nie więcej niż 2U
Procesor	- dwa procesory czterordzeniowe w architekturze x86, osiągające w testach wydajnościowych SPECint_rate2006 min. 315 pkt wymagane dostarczenie dokumentu z testów SPEC lub wymagana obecność certyfikatu potwierdzającego osiągnięty wynik na stronie: www.spec.org (wydruk załączony do oferty) - maksymalny pobór mocy dla jednego procesora max 80W wg dokumentacji technicznej jego producenta
Płyta główna	Dedykowana płyta serwerowa, zaprojektowana i wyprodukowana przez producenta serwera, trwale oznaczona logo producenta oraz oznaczeniem modelu płyty głównej na etapie produkcji -minimum 18 gniazd pamięci RAM. -minimum 2 sloty PCI-Express Gen2 x8 typu low profile -minimum 5 slotów PCI-Express Gen2 x4 typu low profile -możliwość obsadzania w minimum 2 slotach kart PCIe x16 -dodatkowo minimum dwa gniazda PCI-Express Gen2 x4 muszą umożliwiać wykorzystanie jako gniazdo x8, jeśli sąsiednie gniazda x4 będą niewykorzystane -minimum 10 portów USB (w tym min. 3 z przodu, min. 4 z tyłu, min. 3 w środku), -możliwość instalacji pamięci flash wewnątrz serwera za pośrednictwem dedykowanego złącza na płycie głównej -1 port RS-232
Pamięć RAM	- nie mniej niż 24GB RAM typu registred DDR3-1333 z korekcją błędów Advanced ECC, funkcje scrubbing i SDDC, moduły o obniżony napięciu (Low Voltage) - możliwość konfiguracji aktywnej rezerwy i zapisu lustrzanego pamięci - obsadzone 6 gniazd pamięci w trybie wysokiej wydajności - możliwość rozbudowy do minimum 192 GB RAM - obsługa pamięci typu UDIMM, RDIMM i LVDIMM
HDD	- możliwość instalacji min. 12 szt. dysków,
Kontrolery	- kontroler dysków typu SAS 6G - kontroler RAID 0, 1 SAS 6G - kontroler FC min 2 kanałowy o prędkości min 8Gb/s
Karta graficzna	integrowana, w jednym module z kontrolerem zdalnego zarządzania i pamięcią 32MB na płycie głównej, rozdzielczość min. 1600 x 1200
Karty sieciowe	- 2 karty sieciowe typu Ethernet 10/100/1000

Element składowy dostawy	*Ilość i cechy techniczne*
	- dodatkowe 3 dwuportowe karty sieciowe Ethernet 10/100/1000 - wsparcie dla akceleracji TCP/IP, VT-c - rozruch PXE przez sieć LAN z serwera PXE - rozruch iSCSI przez zintegrowaną kartę sieci LAN, - dedykowana karta Ethernet 10/100 wyłącznie dla komunikacji z kontrolerem zdalnego zarządzania, redundancja interfejsu zarządzającego poprzez przejęcie jego funkcjonalności w przypadku usterki przez jedną z dwóch kart Ethernet 10/100/1000 zainstalowanych na płycie głównej
Zasilanie i chłodzenie	- redundantne dwa zasilacze zgodne ze standardem EPA typu hot-plug, o mocy maksymalnej 800W na 1 zasilacz, o sprawności min. 92% przy typowym obciążeniu 50% - nadmiarowe chłodzenie – redundantne wentylatory typu hot-plug
Oprogramowanie	Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
Zarządzanie	Zintegrowany z płytą główną kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzanie włącznie z przejęciem zdalnym konsoli tekstowej (możliwość dokupienia opcji przejęcia konsoli graficznej oraz zdalnego podłączenia napędów). Dedykowana karta LAN 10/100 Mb/s do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym serwera. Umieszczona z przodu chowana karta identyfikacyjna serwera zawierająca nazwę serwera, numer handlowy, numer seryjny, adresy kart sieciowych
Certyfikaty producenta	Certyfikat producenta ISO 9001 w zakresie projektowania, produkcji i serwisu produktów, CE oraz ISO 14001.
Dokumentacja	Karty gwarancyjne, instrukcje, licencje oprogramowania, nośniki ze sterownikami
Gwarancja	3 lata z gwarantowanym czasem reakcji w następnym dniu roboczym od zgłoszenia
Inne	-Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane (wymagane oświadczenie producenta dołączone do oferty) oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne. -Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg. -Oferent zobowiązany jest dostarczyć wraz z ofertą, szczegółową specyfikację techniczną oferowanego sprzętu. -Dostępność części zamiennych przez 5 lat od momentu zakupu serwera (oświadczenie producenta)

Element składowy dostawy	*Ilość i cechy techniczne*
	-Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji - Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera, Możliwość weryfikacji czasu obowiązywania i reżimu gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera
Oprogramowanie wirtualizacyjne	Oferowane oprogramowanie musi umożliwiać: - przenoszenie działających maszyn wirtualnych pomiędzy fizycznymi serwerami - oferować tryb wysokiej dostępności (HA) - oferować mechanizmy optymalizacji pamięci - oferować raportowanie i alerty związane z wydajnością System wirtualizacyjny musi być uruchamiany na samym sprzęcie, bez pośrednictwa dodatkowych systemów operacyjnych Do oprogramowania należy zapewnić min 3-letne wsparcie producenta

10. macierz

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
1.	Obudowa	- System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks 2U w tej szafie. - Obudowa musi zawierać układ nadmiarowy dla modułów zasilania i chłodzenia umożliwiający wymianę tych elementów w razie awarii bez konieczności wyłączania macierzy - Obudowa powinna posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii/macierzy. - Maksymalna moc zasilania nie może przekraczać 800W dla maksymalnej konfiguracji macierzy. - Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy - Moduły dla rozbudowy o dodatkowe dyski i przestrzeń dyskową muszą mieć obudowy o zajętości nie większej niż 2U, przy montażu w szafach przemysłowych standardu 19”

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
		- Moduły dla rozbudowy muszą być wyposażone w nadmiarowy układ zasilania i chłodzenia
2.	Pojemność	- System musi umożliwiać instalację min 12 dysków formatu 3,5” wykonanych jako dyski SAS lub NearLine-SAS. - System musi posiadać możliwość dołączania półek rozszerzeń umożliwiających uzyskanie sumarycznej liczby dysków min. 24. - Macierz powinna posiadać możliwość późniejszej rozbudowy wyłącznie poprzez zakup elementów sprzętowych. - macierz musi być wyposażona w przestrzeń dyskową pojemności minimum 15,6TB RAW w tym min. 3,6TB RAW na dyskach o prędkości obrotowej min. 15000 obr/min
3.	Kontrolery	- System musi posiadać 2 kontrolery w układzie nadmiarowym typu active-active, z minimum 1GB pamięci podręcznej każdy. - W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik nie wymagający stosowania zasilania zewnętrznego lub bateryjnego. - Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia – dotyczy konfiguracji z dwoma kontrolerami RAID. - Macierz powinna pozwalać na wymianę kontrolera RAID bez utraty danych zapisanych na dyskach nawet w przypadku konfiguracji z jednym kontrolerem RAID. - W układzie z zainstalowanymi dwoma kontrolerami RAID zawartości pamięci podręcznej obydwu kontrolerów musi być identyczna tzw. cache mirror. - Każdy z kontrolerów RAID powinien posiadać dedykowany min. 1 interfejs RJ-45 Ethernet obsługujący połączenia z prędkościami : 1000Mb/s, 100Mb/s, 10Mb/s - dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.
4.	Interfejsy FC	- Oferowana macierz musi mieć minimum 2 porty FC dla bezpośredniego podłączenia serwerów lub dla dołączenia do sieci SAN. - Porty powinny pracować z prędkością min. 4 Gb/s oraz umożliwiać poprawną pracę także z prędkością 2 Gb/s i 1 Gb/s. - Interfejsy FC nie mogą być wykorzystywane do innych transmisji (zarządzanie lub konfiguracja macierzy) niż dane do zapisu / odczytu danych na zdefiniowane woluminy
5.	Poziomy RAID	Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RADI: 0,1 ,1+0, 5 ,5+0, 6
6.	Wspierane dyski	Oferowana macierz musi wspierać minimum dyski: - dyski SAS wykonane w technologii hot-plug o pojemnościach min. 600GB i prędkości obrotowej min. 15000 obrotów na minutę, - dyski NL-SAS (NearLine SAS) wykonane w technologii hot-plug o pojemnościach min. 2 TB i prędkości obrotowej 7200 obrotów na minutę,

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
		- Macierz musi wspierać mieszaną konfigurację dysków SAS, NearLine-SAS, w obrębie pojedynczego modułu obudowy. - Macierz musi wspierać technologię energooszczędne typu Drive Spin Down lub wyłączanie dysków nieaktywnych.
7.	Opcje software'owe	- Macierz musi być wyposażona w system kopii migawkowych (snapshot) z licencją na min 8 kopii migawkowe z możliwością rozszerzenia licencji do min. 512 kopii migawkowych. - Macierz musi wspierać Microsoft Volume ShadowCopy Services (VSS) - Macierz musi wspierać Microsoft Virtual Disk Services (VDS) - Macierz musi umożliwiać zdefiniowanie min. 512 woluminów (LUN) dla konfiguracji dwukontrolerowej. - Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 64 ścieżek logicznych FC. - Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego i kontrolerów RAID bez konieczności wyłączania macierzy lub bez konieczności wyłączania ścieżek logicznych FC dla podłączonych stacji/serwerów. - Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacji: - zmiana rozmiaru woluminu, - zmiana poziomu RAID, - zmiana technologii dysków dla danej grupy RAID, - dodawanie nowych dysków do istniejącej grupy dyskowej, - Macierz musi posiadać wsparcie dla systemów operacyjnych : MS Windows Server 2003/2008, RedHat Linux, HP-UX, IBM AIX, SUN Solaris, VMWare Infarstructure i vSphere, Citrix XEN Server - Macierz musi umożliwiać wystawienie woluminu logiczne o maksymalnej pojemności min. 8TB.
8.	Konfiguracja, zarządzanie	- Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej bez konieczności dedykowania oddzielnego serwera do obsługi tego oprogramowania. - Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. - Pełne zdalne zarządzanie macierzą powinno być możliwe bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora - Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI. - Macierz musi wspierać protokół zarządzania SMI-S i SNMP. - Z macierzą musi być również dostarczone oprogramowanie (nośnik + licencja) pozwalające zarządzać kilkoma macierzami opisanymi niniejszą specyfikacją.

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
9.	Gwarancja i serwis	- Całe rozwiązanie musi być objęte minimum 36 miesięcznym okresem gwarancji z naprawą miejscu instalacji urządzenia z czasem reakcji na następny dzień roboczy. - Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia w ciągu 36 miesięcy od daty zakupu. - System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez protokół SNMP lub SMTP - Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia

11. maszt 18m

Maszt dostosowany do montażu wraz ze stopą betonową prefabrykowaną montowany każdorazowo w miejscu wskazanym w projekcie budowlanym sieci. Do każdego z masztów należy doprowadzić zasilanie w energię elektryczną. Każda z rozdzielni elektrycznych musi być opomiarowana.

12. Kontroler.wifi

- Urządzenie przeznaczone do montażu w szafie rack o wysokości max 1U
- możliwość zarządzania minimum 12 punktami dostępowymi
- możliwość dynamicznego zarządzaina pasmem i częstotliwościami
- wsparcie dal natywnego ActiveDirectory, RADIUIS, LDAP
- możliwość dynamicznego przydzielania VLAN
- możliwość uruchamiania sieci typy Gość
- możliwość dynamicznej generacji kluczy Pre-Shared Key
- obsługa standardu 802.1x, 802.1q,

13. punkt dostępowy. kontroler.wifi

- punkt dostępowy pracujący w standardzie 802.11 b/g
Punkt dostępowy powinien wspierać minimum następujące mechanizmy bezpieczeństwa: WEP, WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i
- punkt dostępowy powinien mieć mechanizm automatycznego wyboru kanału

- zewnętrzny punkt dostępowy powinien posiadać obudowę o charakterystyce co najmniej IP-65 oraz działać w przedziale temperatur od -20C do +65C
- powinien umożliwiać pomalowanie na dowolny kolor
- powinien dysponować wbudowaną, inteligentną anteną wieloelementową o zysku co najmniej 9 dBi oraz tłumieniu zakłóceń poza główną ścieżką komunikacyjną co najmniej -15dBi
- maksymalna moc transmisji dla standardów 802.11b i 802.11g powinna wynosić min. 27dBM z możliwością regulacji
- antena powinna dostosowywać parametry transmisji do położenia i warunków każdego z klientów osobno aby eliminować interferencje
- punkt dostępowy powinien umożliwiać podłączenie co najmniej 100 klientów
- system bezprzewodowy powinien automatycznie klasyfikować ruch sieciowy i priorytetyzować połączenia VoIP i video
- punkt dostępowy powinien umożliwiać obsługę co najmniej różnych 8 SSID oraz zapewniać określanie priorytetów dla każdego z nich, jak i ograniczeń w dostępnym paśmie
- system bezprzewodowy powinien łatwo integrować się z różnymi systemami uwierzytelniania użytkowników: Radius, 802.1x, ActiveDirectory, a także posiadać własną bazę użytkowników
- system bezprzewodowy powinien umożliwiać tworzenie sieci kratowych typu Wi-Fi Mesh bez ograniczania funkcji dostępu klienckiego
- punkt dostępowy powinien umożliwiać bezpośrednie podłączenie anteny zewnętrznej
- punkt dostępowy powinien być zgodny ze standardami 802.11e (cztery kolejki softwareowe na stację) oraz 802.1q
- punkt powinien być kontrolowany przez wyspecyfikowany powyżej kontroler bezprzewodowy
- system bezprzewodowy powinien posługiwać się architekturą distributed forwarding, gdzie ruch sieciowy nie przechodzi przez kontroler sieci dla zapewnienia wyższej niezawodności i dostępności sieci

14. anteny

Podane parametry są parametrami przykładowymi. Dopuszczalne są następujące tolerancje dla poszczególnych parametrów:

- zysk antenowy: nie mniejszy niż wyspecyfikowano
- kąt promieniowania w płaszczyźnie poziomy (kąt poziom): 10 stopni
- kąt promieniowania w płaszczyźnie pionowej(kąt pion): 10 stopni

anteny dla częstotliwości 2,4 GHz

Lp.	Typ	opis	ilość
1	ant.15.90/15H	15 dBi, kąt poziom 90st., kąt pion 15st, polaryzacja H	9
2	ant.15.360/11H	15 dBi, kąt poziom 360st., kąt pion 11st, polaryzacja H	15
3	ant.14.120/16H	14 dBi, kąt poziom 120st., kąt pion 16st, polaryzacja H	10
4	ant.15.360/11V	15 dBi, kąt poziom 360st., kąt pion 11st, polaryzacja V	0
5	ant.17.120/14V	17 dBi, kąt poziom 120st., kąt pion 14st, polaryzacja V	12
6	ant.17.90/6V	17 dBi, kąt poziom 90st., kąt pion 6st, polaryzacja V	4
7	ant.16.60/0V	16 dBi, kąt poziom 60st., polaryzacja V	9

anteny dla częstotliwości 5 GHz

1	ant.dipolar.5GHz.25	25 dBi, kąt poziom 6st., kąt pion 6st, polaryzacja H+V	28

15. SW1

Urządzenie typu HP2810-24G, każdy z modułami 2x SFP SX.

16. Inne urządzenia

Pozostałe urządzenia systemu wg załączonego kosztorysu ślepego.
Są to dodatkowe szafki krosowe i inne materiały, przewody, okablowanie, urządzenia, niezbędne do realizacji wdrożenia.