Załącznik nr 5 do SIWZ

Część 1. Przełączniki sieciowe.

Przełącznik (typ – 48 G10) 21 sztuk	Zgodność/Model
Wymagania podstawowe	
1. Przełącznik posiadający min 48 portów 10/100/1000BASE-T PoE+	
2. Przełącznik posiadać musi minimum 2 porty SFP z możliwością obsadzenia wkładkami SFP o przepustowości 10Gb/s	
3. Budżet mocy dla PoE+ min. 370W	
4. Wysokość urządzenia 1U	
5. Nieblokująca architektura o wydajności przełączania min. 108 Gb/s (216Gb/s full duplex)	
6. Szybkość przełączania min. 130 Milionów ramek na sekundę dla pakietów 64 bajtowych	
7. Możliwość łączenia do 8 przełączników w stos. Wydajność połączenia w stosie min. 40 Gb/s	
8. Jeżeli realizacja funkcji stackowania wymaga dodatkowych modułów/kabli itp. ich dostarczenie w ramach tego postępowania nie jest wymagane	
9. Tablica MAC adresów min. 16k	
10. Pamięć operacyjna: min. 512MB pamięci DRAM	
11. Pamięć flash: min. 128MB pamięci Flash	
12. Obsługa sieci wirtualnych IEEE 802.1Q	
13. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)	
14. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB	
15. Obsługa LLDP Media Endpoint Discovery (LLDP-MED) lub Cisco Discovery Protocol (CDP)	
16. Przełącznik musi posiadać możliwość dołączenia redundantnego systemu zasilania	
17. Wbudowany DHCP Serwer i klient	
18. Możliwość instalacji min. dwóch wersji oprogramowania - firmware	
19. Możliwość przechowywania min. wielu wersji konfiguracji w plikach tekstowych w pamięci Flash	
20. Możliwość monitorowania zajętości CPU	
21. Lokalny lub lokalny i zdalny port mirroring	
22. Obsługa transferu plików SCP/SFTP/TFTP i HTTP	
23. Urządzenie musi być wyposażone w port USB umożliwiający podłączenie pamięci flash. Musi być dostępna opcja uruchomienia systemu operacyjnego z nośnika danych podłączonego do portu USB	
24. Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego	
25. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 5	

plików konfiguracyjnych	
Bezpieczeństwo	
26. Bezpieczeństwo MAC adresów	
a. ograniczenie liczby MAC adresów na porcie	
b. zatrzaśnięcie MAC adresu na porcie	
c. możliwość wpisania statycznych MAC adresów na port/vlan	
27. Możliwość wyłączenia MAC learning	
Bezpieczeństwo sieciowe	
28. Możliwość konfiguracji portu głównego i zapasowego	
29. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D	
30. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w	
31. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s	
32. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP lub PAGP – minimum 6 grup po minimum 6 portów w grupie. Możliwość konfiguracji połączenia Link Aggregation z różnych przełączników w stosie.	
Zarządzanie	
33. Obsługa synchronizacji czasu NTP	
34. Zarządzanie przez SNMP v1/v2/v3	
35. Zarządzanie przez przeglądarkę WWW – protokół http i https	
36. Telnet Serwer/Klient dla IPv4	
37. SSH2 Serwer/Klient dla IPv4	
38. Ping dla IPv4	
39. Traceroute dla IPv4	
40. Obsługa SYSLOG	
41. Obsługa RMON	
42. Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli	
43. Podłączenie do portu konsoli przy użyciu adapatera RJ45 -> DB9 bez użycia dodatkowych elementów pośredniczących.	
Gwarancja	
Gwarancja wieczysta	
Sprzęt fabrycznie nowy	
Wykonawca musi być autoryzowanym partnerem producenta oferowanych rozwiązań, mogącym świadczyć serwis oparty na świadczeniach producenta - do oferty należy załączyć dokument potwierdzający autoryzacje (certyfikat lub pisemne potwierdzenie producenta lub jego polskiego przedstawicielstwa); · Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów – do oferty należy dołączyć odpowiednie oświadczenie Wykonawcy; · Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 4 miesięce przed ich dostarczeniem) oraz by były nieużywane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym Wykonawca jest zobowiązany do	

poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem); · Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producenta w okresie wymaganym w SIWZ – do oferty należy dostarczyć odpowiednie oświadczenia Wykonawcy;	

Przełącznik typ – 48 F1, 100 sztuk	**Zgodność/Model**
Wymagania podstawowe	
1. Przełącznik posiadający min 48 portów 10/100 PoE+	
2. Przełącznik posiadać musi minimum 4 porty SFP z możliwością obsadzenia wkładkami SFP o przepustowości 1Gb/s	
3. Budżet mocy dla PoE+ min. 370W	
4. Wysokość urządzenia 1U	
5. Nieblokująca architektura o wydajności przełączania min. 88 Gb/s (176 Gb/s full duplex)	
6. Szybkość przełączania min. 13,1 milionów ramek na sekundę dla pakietów 64 bajtowych	
7. Możliwość łączenia do 4 przełączników w stos. Wydajność połączenia w stosie min. 20 Gb/s	
8. Jeżeli realizacja funkcji stackowania wymaga dodatkowych modułów/kabli itp. ich dostarczenie w ramach tego postępowania nie jest wymagane	
9. Tablica MAC adresów min. 8k	
10. Pamięć operacyjna: min. 128MB pamięci DRAM	
11. Pamięć flash: min. 64MB pamięci Flash	
12. Obsługa sieci wirtualnych IEEE 802.1Q	
13. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)	
14. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB	
15. Obsługa LLDP Media Endpoint Discovery (LLDP-MED) lub Cisco Discovery Protocol (CDP)	
16. Przełącznik musi posiadać możliwość dołączenia redundantnego systemu zasilania	
17. Wbudowany DHCP Serwer i klient	
18. Możliwość instalacji min. dwóch wersji oprogramowania - firmware	

19. Możliwość przechowywania min. wielu wersji konfiguracji w plikach tekstowych w pamięci Flash	
20. Możliwość monitorowania zajętości CPU	
21. Lokalny lub lokalny i zdalny port mirroring	
22. Obsługa transferu plików SCP/SFTP/TFTP i HTTP	
23. Urządzenie musi być wyposażone w port USB umożliwiający podłączenie pamięci flash. Musi być dostępna opcja uruchomienia systemu operacyjnego z nośnika danych podłączonego do portu USB	
24. Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego	
25. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 5 plików konfiguracyjnych.	
Bezpieczeństwo	
26. Bezpieczeństwo MAC adresów	
d. ograniczenie liczby MAC adresów na porcie	
e. zatrzaśnięcie MAC adresu na porcie	
f. możliwość wpisania statycznych MAC adresów na port/vlan	
27. Możliwość wyłączenia MAC learning	
Bezpieczeństwo sieciowe	
28. Możliwość konfiguracji portu głównego i zapasowego	
29. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D	
30. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w	
31. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s	
32. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP lub PAGP – minimum 6 grup po minimum 6 portów w grupie. Możliwość konfiguracji połączenia Link Aggregation z różnych przełączników w stosie.	
Zarządzanie	
33. Obsługa synchronizacji czasu NTP	

34. Zarządzanie przez SNMP v1/v2/v3	
35. Zarządzanie przez przeglądarkę WWW – protokół http i https	
36. Telnet Serwer/Klient dla IPv4	
37. SSH2 Serwer/Klient dla IPv4	
38. Ping dla IPv4	
39. Traceroute dla IPv4	
40. Obsługa SYSLOG	
41. Obsługa RMON	
42. Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli	
43. Podłączenie do portu konsoli przy użyciu adapatera RJ45 -> DB9 bez użycia dodatkowych elementów pośredniczących.	
Gwarancja	
Gwarancja wieczysta	
Sprzęt fabrycznie nowy	
Wykonawca musi być autoryzowanym partnerem producenta oferowanych rozwiązań, mogącym świadczyć serwis oparty na świadczeniach producenta - do oferty należy załączyć dokument potwierdzający autoryzacje (certyfikat lub pisemne potwierdzenie producenta lub jego polskiego przedstawicielstwa); · Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów – do oferty należy dołączyć odpowiednie oświadczenie Wykonawcy; · Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 4 miesięce przed ich dostarczeniem) oraz by były nieużywane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym Wykonawca jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem); · Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producenta w okresie wymaganym w SIWZ – do	

oferty należy dostarczyć odpowiednie oświadczenia Wykonawcy;	

Część 2. Serwery

Serwer Rack – 16 sztuk

Komponent	Minimalne wymagania	
Obudowa	Obudowa Rack o wysokości maks. 2U z możliwością instalacji min. 16 dysków 2.5" Hot Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem kabli Posiadająca dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera.	Zgodność/Model
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Możliwość instalacji dedykowanego przez producenta serwera i znajdującego się w jego ofercie moduły GPU.	
Procesor	Dwa procesory sześciordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 443 punktów w teście SPECint_rate_base2006 dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej. Do oferty należy załączyć wynik testu dla oferowanego modelu serwera.	
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych	
Pamięć RAM	32 GB pamięci RAM typu LV RDIMM o częstotliwości pracy 1333MHz. Płyta powinna obsługiwać do 768GB pamięci RAM, na płycie głównej powinno znajdować się minimum 24 sloty przeznaczonych dla pamięci. Możliwe zabezpieczenia pamięci: Memory Rank Sparing, Memory Mirror, SBEC, Lockstep	
Sloty PCI Express	Min. 3 sloty x16 generacji 3 o prędkości x8 LowProfile, min. 2 sloty x16 generacji 3 o prędkości x8 , min. 1 slot x16 generacji 3 pełnej długości i wysokości, min. 1 slot x16 generacji 3 o prędkości x8 pełnej długości i wysokości	
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024	
Wbudowane porty	min. 5 portów USB 2.0 , 2 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232	
Interfejsy sieciowe	Minimum 4 porty typu Gigabit Ethernet Base-T z wsparciem dla protokołu IPv6 oraz możliwością iSCSI boot. Interfejsy sieciowe nie mogą zajmować żadnego z dostępnych slotów PCI-Express. Możliwość instalacji wymiennie modułów udostępniających 2 porty Gigabit Ethernet Base-T oraz 2 porty 10Gb Ethernet SFP+ oraz 2 porty Gigabit Ethernet Base-T oraz 2 porty 10Gb Ethernet BaseT Dodatkowa dwuportowa karta HBA FC 4Gb/s	
Kontroler dysków	Sprzętowy kontroler dyskowy, posiadający min. 512MB nieulotnej pamięci cache , możliwe konfiguracje poziomów RAID : 0, 1, 5, 6, 10, 50, 60	
Dyski twarde	Możliwość instalacji dysków twardych SATA, SAS, NearLine SAS i SSD. Zainstalowane 8 dysków twardych o pojemności min. 300GB SAS 10k RPM każdy. Możliwość instalacji wewnętrznego modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w 2 jednakowe nośniki typu flash z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.	
Napęd optyczny	Wbudowany napęd DVD+/-RW	
System diagnostyczny	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.	

Zasilacze	Redundantne zasilacze Hot Plug o mocy maks. 750W każdy	
Wentylatory	Minimum 6 redundantnych wentylatorów Hot-Plug	
Bezpieczeństwo	Zintegrowany z płytą główną moduł TPM. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.	
Karta zarządzająca	Możliwość instalacji niezależnej od zainstalowanego na serwerze systemu operacyjnego karty zarządzającej posiadającej dedykowany port RJ-45 Gigabit Ethernet umożliwiającej: - 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 - 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 - możliwość obsługi przez dwóch administratorów jednocześnie - wsparcie dla dynamic DNS - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej - możliwość podłączenia lokalnego poprzez złącze RS-232	
Gwarancja	Trzy lata gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do czterech godzin od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365. W przypadku awarii, dyski twarde pozostają własnością Zamawiającego. W przypadku awarii diagnostyka przeprowadzona w miejscu instalacji przez pracownika autoryzowanego serwisu producenta. 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 – dokumenty potwierdzające załączyć do oferty.	
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2008 R2 x64, x86, Microsoft Windows Server 2012	
Dokumentacja	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.	

Część 3. UTM.

UTM typ 1	
ilość	6
Proponowany model	

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

1. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.	
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.	
3. Monitoring stanu realizowanych połączeń VPN oraz automatyczne przekierowanie pakietów zgodnie z trasą definiowaną przez protokół OSPF.	
4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.	
5. System realizujący funkcję Firewall powinien dysponować minimum 6 portami Ethernet 10/100 Base-TX oraz 2 portami Ethernet 10/100/1000 Base-TX	
6. Możliwość tworzenia min 230 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.	
7. W zakresie Firewall'a obsługa nie mniej niż 90 tysięcy jednoczesnych połączeń oraz 5 tys. nowych połączeń na sekundę	
8. Przepustowość Firewall'a: nie mniej niż 300 Mbps	
Wydajność szyfrowania 3DES: nie mniej niż 60 Mbps	
9. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:	
• kontrola dostępu - zapora ogniowa klasy Stateful Inspection	

• ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS, SMTPS, POP3S). W celu zapewnienia wysokiej skuteczności mechanizmu antywirusowego wymaga się aby mechanizm skanowania działał w oparciu o technologię proxy. umożliwiającą analizę dowolnego typu załączników	
• poufność danych - połączenia szyfrowane IPSec VPN oraz SSL VPN	
• ochrona przed atakami - Intrusion Prevention System [IPS]	
• kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.	
• kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)	
• kontrola pasma oraz ruchu [QoS, Traffic shaping]	
• Kontrola aplikacji oraz rozpoznawanie ruchu P2P	
• Możliwość analizy ruchu szyfrowanego protokołem SSL	
• Ochrona przed wyciekiem poufnej informacji (DLP) z funkcją archiwizowania informacji na lokalnym dysku	
10. Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 300 Mbps	
11. Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączonymi funkcjami: Antivirus, WebFilter - min. 40 Mbps	
12. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:	
• Tworzenie połączeń w topologii Site-to-site oraz Client-to-site	
• Producent oferowanego rozwiązania VPN powinien dostarczać klienta	

VPN współpracującego z proponowanym rozwiązaniem.	
• .Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności	
• Praca w topologii Hub and Spoke oraz Mesh	
• Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF	
• Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth	
13. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.	
14. Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.	
15. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.	
16. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)	
17. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ	
18. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)	
19. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 6500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących	

podstawową ochronę przed atakami typu DoS oraz DDos.	
20. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP	
21. Baza filtra WWW o wielkości co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.	
22. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.	
23. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:	
• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu	
• haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP	
• haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych	
• Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania a kontrolerze domeny.	
24. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:	
• ICSA dla funkcjonalności SSLVPN, IPS, Antywirus	
• ICSA lub EAL4 dla funkcjonalności Firewall	

25. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami wchodzącymi w skład systemu. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	
26. Serwisy i licencje	
• Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres1 ROKU.	
27. Gwarancja oraz wsparcie	
• System powinien być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej	
• System powinien być objęty serwisem gwarantującym udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym . Serwis powinien być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego (oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Polski), mających swoją siedzibę na terenie Polski. Zgłoszenia serwisowe przyjmowane w trybie 24x7 przez dedykowany serwisowy moduł internetowy (należy podać adres www) oraz infolinię 24x7 (należy podać numer infolinii).	
28. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z	

późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.	
29. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.	

UTM typ 2	
ilość	2
Proponowany model	

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

1. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu. W ramach postępowania dostawca powinien dostarczyć system w formie redundantnej w postaci klastra urządzeń.	
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.	
3. Monitoring stanu realizowanych połączeń VPN.	
4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.	
5. System realizujący funkcję Firewall powinien dysponować minimum 16 portami Ethernet 10/100/1000 Base-TX	

6. Możliwość tworzenia min 254 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.	
7. W zakresie Firewall'a obsługa nie mniej niż 2 miliony jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę	
8. Przepustowość Firewall'a: nie mniej niż 1 Gbps dla pakietów 512 B	
9. Wydajność szyfrowania VPN IPSec: nie mniej niż 400 Mbps	
10. System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 16GB do celów logowania i raportowania. W przypadku kiedy system nie posiada dysku do poszczególnych lokalizacji musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.	
11. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:	
• kontrola dostępu - zapora ogniowa klasy Stateful Inspection	
• ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS).	
• poufność danych - połączenia szyfrowane IPSec VPN oraz SSL VPN	
• ochrona przed atakami - Intrusion Prevention System [IPS]	
• kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.	
• kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)	
• kontrola pasma oraz ruchu [QoS, Traffic shaping]	

• Kontrola aplikacji oraz rozpoznawanie ruchu P2P	
• Możliwość analizy ruchu szyfrowanego protokołem SSL	
• Ochrona przed wyciekiem poufnej informacji (DLP) z funkcją archiwizowania informacji	
12. Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 500 Mbps	
13. Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączoną funkcją: Antivirus min. 300 Mbps	
14. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:	
• Tworzenie połączeń w topologii Site-to-site oraz Client-to-site	
• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności	
• Praca w topologii Hub and Spoke oraz Mesh	
• Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF	
• Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth	
15. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.	
16. Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.	
17. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.	
18. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP,	

interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)	
19. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ	
20. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)	
21. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 6500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.	
22. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP	
23. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.	
24. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.	
25. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:	
• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu	
• haseł statycznych i definicji użytkowników przechowywanych w bazach	

zgodnych z LDAP	
• haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych	
• Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania a kontrolerze domeny.	
26. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:	
• ICSA dla funkcjonalności SSL VPN, IPSec, IPS, Antywirus	
• ICSA lub EAL4 dla funkcjonalności Firewall	
27. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	
28. Serwisy i licencje	
• Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 1 roku .	
29. Gwarancja oraz wsparcie	
• System powinien być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej	
• System powinien być objęty serwisem gwarantującym udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym . Serwis powinien być realizowany przez producenta rozwiązania lub	

autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego (oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Polski), mających swoją siedzibę na terenie Polski. Zgłoszenia serwisowe przyjmowane w trybie 24x7 przez dedykowany serwisowy moduł internetowy (należy podać adres www) oraz infolinię 24x7 (należy podać numer infolinii).	
30. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.	
31. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.	

UTM typ 3	
ilość	1
Proponowany model	

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku

implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

1. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.	
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.	
3. Monitoring stanu realizowanych połączeń VPN oraz automatyczne przekierowanie pakietów zgodnie z trasą definiowaną przez protokół OSPF.	
4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.	
5. System realizujący funkcję Firewall powinien dysponować minimum 8 portami Ethernet 10/100/1000 Base-TX	
6. Możliwość tworzenia min 230 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.	
7. W zakresie Firewall'a obsługa nie mniej niż 500 tysięcy jednoczesnych połączeń oraz 15 tys. nowych połączeń na sekundę	
8. Przepustowość Firewall'a: nie mniej niż 5 Gbps	
Wydajność szyfrowania 3DES: nie mniej niż 2 Gbps	
9. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:	
• kontrola dostępu - zapora ogniowa klasy Stateful Inspection	
• ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS). W celu zapewnienia wysokiej skuteczności mechanizmu antywirusowego wymaga się aby mechanizm skanowania działał w oparciu o technologię proxy. umożliwiającą analizę dowolnego	

typu załączników	
• poufność danych - połączenia szyfrowane IPSec VPN oraz SSL VPN	
• ochrona przed atakami - Intrusion Prevention System [IPS]	
• kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.	
• kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)	
• kontrola pasma oraz ruchu [QoS, Traffic shaping]	
• Kontrola aplikacji oraz rozpoznawanie ruchu P2P	
• Możliwość analizy ruchu szyfrowanego protokołem SSL	
• Ochrona przed wyciekiem poufnej informacji (DLP) z funkcją archiwizowania informacji na lokalnym dysku	
10. Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 500 Mbps	
11. Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączonymi funkcjami: Antivirus, WebFilter, min. 90 Mbps	
12. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:	
• Tworzenie połączeń w topologii Site-to-site oraz Client-to-site	
• Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem.	
• .Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności	
• Praca w topologii Hub and Spoke oraz Mesh	

• Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF	
• Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth	
13. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.	
14. Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.	
15. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.	
16. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)	
17. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ	
18. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)	
19. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 6500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.	
20. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP	

21. Baza filtra WWW o wielkości co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.	
22. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.	
23. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:	
• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu	
• haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP	
• haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych	
• Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania a kontrolerze domeny.	
24. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:	
• ICSA dla funkcjonalności SSLVPN, IPS, Antywirus	
• ICSA lub EAL4 dla funkcjonalności Firewall	
25. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami wchodzącymi w skład systemu. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	

26. Serwisy i licencje	
• Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 1 roku .	
27. Gwarancja oraz wsparcie	
• System powinien być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej	
• System powinien być objęty serwisem gwarantującym udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym . Serwis powinien być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego (oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Polski), mających swoją siedzibę na terenie Polski. Zgłoszenia serwisowe przyjmowane w trybie 24x7 przez dedykowany serwisowy moduł internetowy (należy podać adres www) oraz infolinię 24x7 (należy podać numer infolinii).	
28. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.	

29. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.	

UTM typ 4	
ilość	1
Proponowany model	

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

1. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.	
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.	
3. Monitoring stanu realizowanych połączeń VPN.	
4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.	
5. System realizujący funkcję Firewall powinien dysponować minimum 10 portami Ethernet 10/100/100 BaseTX	
6. Możliwość tworzenia min 254 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.	
7. W zakresie Firewall'a obsługa nie mniej niż 1,5 miliona jednoczesnych połączeń oraz 40 tys. nowych połączeń na sekundę	

8. Przepustowość Firewall'a: nie mniej niż 6 Gbps	
9. Wydajność szyfrowania 3DES: nie mniej niż 3 Gbps	
10. System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 30 GB do celów logowania i raportowania. W przypadku kiedy system nie posiada dysku do poszczególnych lokalizacji musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.	
11. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:	
• kontrola dostępu - zapora ogniowa klasy Stateful Inspection	
• ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS).	
• poufność danych - połączenia szyfrowane IPSec VPN oraz SSL VPN	
• ochrona przed atakami - Intrusion Prevention System [IPS]	
• kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.	
• kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)	
• kontrola pasma oraz ruchu [QoS, Traffic shaping]	
• Kontrola aplikacji oraz rozpoznawanie ruchu P2P	
• Możliwość analizy ruchu szyfrowanego protokołem SSL	
• Ochrona przed wyciekiem poufnej informacji (DLP) z funkcją	

archiwizowania informacji	
12. Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 1 Gbps	
13. Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączoną funkcją: Antivirus min. 400 Mbps	
14. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:	
• Tworzenie połączeń w topologii Site-to-site oraz Client-to-site	
• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności	
• Praca w topologii Hub and Spoke oraz Mesh	
• Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF	
• Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth	
15. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.	
16. Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.	
17. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.	
18. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)	
19. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ	

20. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)	
21. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 6500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.	
22. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP	
23. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.	
24. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.	
25. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:	
• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu	
• haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP	
• haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych	
• Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania	

typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania a kontrolerze domeny.	
26. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:	
• ICSA dla funkcjonalności SSLVPN, IPS, Antywirus	
• ICSA lub EAL4 dla funkcjonalności Firewall	
27. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	
28. Serwisy i licencje	
• Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 1 roku .	
29. Gwarancja oraz wsparcie	
• System powinien być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej	
• System powinien być objęty serwisem gwarantującym udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym . Serwis powinien być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego (oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Polski), mających swoją siedzibę na terenie Polski. Zgłoszenia serwisowe przyjmowane w trybie 24x7 przez dedykowany serwisowy moduł internetowy (należy podać	

adres www) oraz infolinię 24x7 (należy podać numer infolinii).	
30. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.	
31. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.	

Część 4. Pozostałe (macierze dyskowe, komputery, procesory, półki dyskowe)

	Ilość	Parametr oferowany
Macierz dyskowa z wyposażeniem (Typ: SRL)	**1**	**Zgodnośc/model**
Przez macierz dyskową Zamawiający rozumie zestaw dysków twardych i/lub SSD kontrolowanych przez pojedynczą parę kontrolerów macierzowych (bez dodatkowych kontrolerów zewnętrznych, serwerów wirtualizujących, etc). Dostęp do macierzy realizowany jest poprzez redundantną sieć iSCSI 10Gb z wykorzystaniem min. dwóch kontrolerów o podręcznej pamięci cache nie mniejszej niż 4GB każdy. Pojedyńczy kontroler wyposażony jest w min. 2 iSCSI (min. 10Gbit/s)		
System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” tj. szyny, przewody do komunikacji -min 4szt kabli Twinax 1m, przewody zasilające		
Obudowa macierzy		
Obudowa musi zawierać układ nadmiarowy dla modułów zasilania i chłodzenia umożliwiający wymianę tych elementów w razie awarii bez konieczności wyłączania macierzy, max wysokość 2U.		
Obudowa musi posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii/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”		
Moduły dla rozbudowy muszą być wyposażone w nadmiarowy układ zasilania i chłodzenia		
Pojemność macierzy		
Moduły systemu muszą umożliwiać instalację 12 dysków formatu 3,5", wykonanych jako dyski SAS lub NearLine-SAS lub SolidStateDrive		
Macierz musi umożliwiać instalacje dysków 2,5” oraz 3,5” w obrębie pojedynczego rozwiązania.		

Macierz musi umożliwiać zainstalowanie minimum 120 dysków 3,5 " w pojedynczym rozwiązaniu	
Macierz powinna posiadać możliwość późniejszej rozbudowy wyłącznie poprzez zakup elementów sprzętowych	
Oferowana macierz musi zawierać dyski: - min. 4 szt. dysków NL-SAS 3.5” min. 2TB każdy	
Kontrolery macierzy	
System musi posiadać min. 2 kontrolery pracujące w układzie nadmiarowym typu active-active, z minimum 4GB 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 korzystania z podtrzymania jego zasilania – tj. zasilania zewnętrznego lub bateryjnego	
Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia	
Macierz musi pozwalać na wymianę kontrolera RAID bez utraty danych zapisanych na dyskach	
W układzie z zainstalowanymi min. dwoma kontrolerami RAID zawartości pamięci podręcznej obydwu kontrolerów musi być identyczna tzw. cache mirror	
Każdy z kontrolerów RAID musi 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	
Interfejsy macierzy	
Oferowana macierz musi mieć minimum 2 porty iSCSI 10Gbps do dołączenia serwerów bezpośrednio lub do dołączenia do sieci wyprowadzone na każdy kontroler RAID	
Macierz musi umożliwiać instalacje min. 2 dodatkowych portów w każdym kontrolerze obsługujących protokoły transmisji : iSCSI 1 Gb/s, iSCSI 10Gb/s, SAS 2.0, FC 8Gb/s, FC 16Gb/s lub FCoE 10Gb/s	

Instalacja portów j.w. nie może wymagać zmiany modelu kontrolerów RAID w oferowanym rozwiązaniu, w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych	
Poziomy RAID macierzy	
Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID min: 0, 1 ,1+0, 5 ,5+0, 6	
Wspierane dyski macierzy min:	
Dyski w technologii SAS 2.0 (6Gb/s), wspierające operacje hot-plug, o pojemnościach min. 300GB/450GB/600GB i prędkości obrotowej min. 15000 obrotów na minutę; Dyski w technologii SAS 2.0 (6Gb/s), wspierające operacje hot-plug, o pojemnościach min. 300GB/450GB/600GB/900GB i prędkości obrotowej min. 10000 obrotów na minutę	
Dyski NL-SAS (NearLine SAS) z interfejsem SAS 2.0 6Gb/s, wspierające operacje hot-plug, o pojemnościach min. 1TB/2TB /3TB/4TB i prędkości obrotowej 7200 obrotów na minutę	
Macierz musi obsługiwać dyski elektroniczne SolidStateDrive wykonane w technologii hot-plug o pojemnościach 200GB/400GB/800GB	
Interfejsy obsługiwanych dysków muszą być wyposażone w min. 2 porty SAS 2.0 6Gb/s, pracujące w reżimie full-duplex (jednoczesną transmisję danych przez dwa porty)	
Macierz musi wspierać mieszaną konfigurację dysków SAS, NearLine-SAS i SSD w obrębie każdego pojedynczego modułu obudowy pozwalającego na instalacje dysków	
Macierz musi wspierać dla min jednej z obsługiwanych technologii dyskowych mechanizm automatycznej przedawaryjnej migracji zapisów i składowanych danych na dysk zapasowy	
Macierz musi umożliwiać definiowanie i obsługę dysków zapasowych tzw. hot-spare w trybach min: - hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID -hot-spare dla zabezpieczania dowolnej grypy dyskowej RAID	

Macierz musi umożliwiać zadeklarowanie dowolnego dysku w rozwiązaniu jako globalnego dysku zapasowego tj. global hot-spare. Macierz musi umożliwiać obsługę minimum 32 dysków global hot-spare w rozwiązaniu	
Obsługa dysków szamoszyfrujących SED	
Oprogramowanie macierzy	
Macierz musi być wyposażona w system kopii migawkowych (snapshot) z licencją na min. 8 kopii migawkowych, z możliwością rozbudowy do min 2048 kopii.	
Macierz musi umożliwiać zdefiniowanie min. 4096 woluminów (LUN)	
Macierz musi wspierać szyfrowanie danych na obsługiwanych woluminach z wykorzystaniem algorytmu szyfrującego o długości klucza minimum 128-bitów, jeżeli taka funkcjonalność wymaga aktywacji odrębnej licencji bądź dostarczenie oprogramowania to należy je uwzględnić w ofercie	
Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego i kontrolerów RAID bez konieczności wyłączania macierzy	
Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) min. operacji: - zmiana rozmiaru woluminu, - zmiana poziomu RAID, - zmiana technologii dysków dla danej grupy RAID, - dodawanie nowych dysków do istniejącej grupy dyskowej, - zmiana alokacji woluminu logicznego pomiędzy grupami dyskowymi o różnym poziomie zabezpieczenia RAID Jeżeli którakolwiek z wymienionych w tym punkcie funkcjonalności wymaga odrębnej licencji należy ją uwzględnić w ofercie	
Macierz musi umożliwiać definiowanie woluminów o wielkośći 60TB.	
Macierz musi posiadac wsparcie dla systemów operacyjnych min: MS Windows Server 2003/2008, SuSE Linux, RedHat Linux, HP-UNIX, IBM AIX, SUN Solaris, VMWare, Citrix XEN Server	

Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem).	
Macierz musi umożliwiać uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, z drugą macierzą tego typu lub modelem wyższym i z wykorzystaniem transmisji danych po protokołach FC oraz iSCSI, bez konieczności stosowania zewn. urządzeń konwersji wymienionych protokołów transmisji . Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication. Nie jest wymagane dostarczenie aktywnej licencji dla obsługi tej funkcjonalności.	
Macierz musi umożliwiać obsługę wirtualizacji całej przestrzeni dyskowej dla hostów , tzw. Thin Provisioning. Nie jest wymagane dostarczenie aktywnej licencji dla obsługi tej funkcjonalności.	
Macierz musi umożliwiać uruchomienie automatycznej reloakacja zasobów pomiędzy grupami dysków wykonanymi w różnych technologiach. Nie jest wymagane dostarczenie aktywnej licencji dla obsługi tej funkcjonalności.	
Konfiguracja i zarządzanie macierzą	
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 musi 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	

Inne	
Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia	
Urządzenie fabrycznie nowe wyprodukowane nie wcześniej niż w 2013 roku	
Gwarancja 3 lata w miejscu instalacji z gwarantowanym czasem naprawy w następnym dniu roboczym od zgłoszenia	

	Ilość	**Parametr oferowany**
Macierz dyskowa z wyposażeniem (Typ:SRS)	**1**	**Zgodnosc/Model**
Przez macierz dyskową Zamawiający rozumie zestaw dysków twardych i/lub SSD kontrolowanych przez pojedynczą parę kontrolerów macierzowych (bez dodatkowych kontrolerów zewnętrznych, serwerów wirtualizujących, etc). Dostęp do macierzy realizowany jest poprzez redundantną sieć FC z wykorzystaniem min. dwóch kontrolerów o podręcznej pamięci cache nie mniejszej niż 4GB każdy.		
System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” tj. szyny, przewody do komunikacji min 8szt. przewodów FC 5m, przewody zasilające		
Obudowa macierzy		
Obudowa musi zawierać układ nadmiarowy dla modułów zasilania i chłodzenia umożliwiający wymianę tych elementów w razie awarii bez konieczności wyłączania macierzy, max wysokość 2U.		
Obudowa musi posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii/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”		

Moduły dla rozbudowy muszą być wyposażone w nadmiarowy układ zasilania i chłodzenia	
Pojemność macierzy	
Moduły systemu muszą umożliwiać instalację 24 dysków formatu 2,5", wykonanych jako dyski SAS lub NearLine-SAS lub SolidStateDrive	
Macierz musi umożliwiać instalacje dysków 2,5” oraz 3,5” w obrębie pojedynczego rozwiązania.	
Macierz musi umożliwiać zainstalowanie minimum 240 dysków 2,5 " w pojedynczym rozwiązaniu	
Macierz powinna posiadać możliwość późniejszej rozbudowy wyłącznie poprzez zakup elementów sprzętowych	
Oferowana macierz musi zawierać dyski: - min. 8 szt. dysków SAS 2.5” 10K min. 600GB każdy	
Kontrolery macierzy	
System musi posiadać min. 2 kontrolery pracujące w układzie nadmiarowym typu active-active, z minimum 4GB 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 korzystania z podtrzymania jego zasilania – tj. zasilania zewnętrznego lub bateryjnego	
Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia	
Macierz musi pozwalać na wymianę kontrolera RAID bez utraty danych zapisanych na dyskach	
W układzie z zainstalowanymi min. dwoma kontrolerami RAID zawartości pamięci podręcznej obydwu kontrolerów musi być identyczna tzw. cache mirror	
Każdy z kontrolerów RAID musi 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	
Interfejsy macierzy	
Oferowana macierz musi mieć minimum 4 porty FC 8Gbps do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN wyprowadzone na każdy kontroler RAID	

Macierz musi umożliwiać wymianę zainstalowanych portó FC w każdym kontrolerze obsługujących na porty obsługujące protokoły transmisji : iSCSI 10Gb/s, SAS 2.0, FC 8Gb/s, FC 16Gb/s lub FCoE 10Gb/s.	
Instalacja portów j.w. nie może wymagać zmiany modelu kontrolerów RAID w oferowanym rozwiązaniu, w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych	
Poziomy RAID macierzy	
Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID min: 0, 1 ,1+0, 5 ,5+0, 6	
Wspierane dyski macierzy min:	
Dyski w technologii SAS 2.0 (6Gb/s), wspierające operacje hot-plug, o pojemnościach min. 300GB/450GB/600GB i prędkości obrotowej min. 15000 obrotów na minutę; Dyski w technologii SAS 2.0 (6Gb/s), wspierające operacje hot-plug, o pojemnościach min. 300GB/450GB/600GB/900GB i prędkości obrotowej min. 10000 obrotów na minutę	
Dyski NL-SAS (NearLine SAS) z interfejsem SAS 2.0 6Gb/s, wspierające operacje hot-plug, o pojemnościach min. 1TB/2TB /3TB/4TB i prędkości obrotowej 7200 obrotów na minutę	
Macierz musi obsługiwać dyski elektroniczne SolidStateDrive wykonane w technologii hot-plug o pojemnościach 200GB/400GB/800GB	
Interfejsy obsługiwanych dysków muszą być wyposażone w min. 2 porty SAS 2.0 6Gb/s, pracujące w reżimie full-duplex (jednoczesną transmisję danych przez dwa porty)	
Macierz musi wspierać mieszaną konfigurację dysków SAS, NearLine-SAS i SSD w obrębie każdego pojedynczego modułu obudowy pozwalającego na instalacje dysków	
Macierz musi wspierać dla min jednej z obsługiwanych technologii dyskowych mechanizm automatycznej przedawaryjnej migracji zapisów i składowanych danych na dysk zapasowy	

Macierz musi umożliwiać definiowanie i obsługę dysków zapasowych tzw. hot-spare w trybach min: - hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID -hot-spare dla zabezpieczania dowolnej grypy dyskowej RAID	
Macierz musi umożliwiać zadeklarowanie dowolnego dysku w rozwiązaniu jako globalnego dysku zapasowego tj. global hot-spare. Macierz musi umożliwiać obsługę minimum 32 dysków global hot-spare w rozwiązaniu	
Obsługa dysków szamoszyfrujących SED	
Oprogramowanie macierzy	
Macierz musi być wyposażona w system kopii migawkowych (snapshot) z licencją na min. 8 kopii migawkowych, z możliwością rozbudowy do min 2048 kopii.	
Macierz musi umożliwiać zdefiniowanie min. 4096 woluminów (LUN)	
Macierz musi wspierać szyfrowanie danych na obsługiwanych woluminach z wykorzystaniem algorytmu szyfrującego o długości klucza minimum 128-bitów, jeżeli taka funkcjonalność wymaga aktywacji odrębnej licencji bądź dostarczenie oprogramowania to należy je uwzględnić w ofercie	
Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego i kontrolerów RAID bez konieczności wyłączania macierzy	
Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) min. operacji: - zmiana rozmiaru woluminu, - zmiana poziomu RAID, - zmiana technologii dysków dla danej grupy RAID, - dodawanie nowych dysków do istniejącej grupy dyskowej, - zmiana alokacji woluminu logicznego pomiędzy grupami dyskowymi o różnym poziomie zabezpieczenia RAID Jeżeli którakolwiek z wymienionych w tym punkcie funkcjonalności wymaga odrębnej licencji należy ją uwzględnić w ofercie	
Macierz musi umożliwiać definiowanie woluminów o wielkości 60TB.	

Macierz musi posiadac wsparcie dla systemów operacyjnych min: MS Windows Server 2003/2008, SuSE Linux, RedHat Linux, HP-UNIX, IBM AIX, SUN Solaris, VMWare, Citrix XEN Server	
Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem).	
Macierz musi umożliwiać uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, z drugą macierzą tego typu lub modelem wyższym i z wykorzystaniem transmisji danych po protokołach FC oraz iSCSI, bez konieczności stosowania zewn. urządzeń konwersji wymienionych protokołów transmisji . Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication. Nie jest wymagane dostarczenie aktywnej licencji dla obsługi tej funkcjonalności.	
Macierz musi umożliwiać obsługę wirtualizacji całej przestrzeni dyskowej dla hostów , tzw. Thin Provisioning. Nie jest wymagane dostarczenie aktywnej licencji dla obsługi tej funkcjonalności.	
Macierz musi umożliwiać uruchomienie automatycznej reloakacja zasobów pomiędzy grupami dysków wykonanymi w różnych technologiach. Nie jest wymagane dostarczenie aktywnej licencji dla obsługi tej funkcjonalności.	
Konfiguracja i zarządzanie macierzą	
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 musi 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	
Inne	
Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia	
Urządzenie fabrycznie nowe wyprodukowane nie wcześniej niż w 2013 roku	
Gwarancja 3 lata w miejscu instalacji z gwarantowanym czasem naprawy w następnym dniu roboczym od zgłoszenia.	

	DODATKOWA PÓŁKA DO MACIERZY DYSKOWEJ Sztuk 1	
	Wymagania funkcjonalne	**Zgodność/model**
Obudowa	Dodatkowa półka dyskowa poprawnie współpracująca, zapewniająca poprawne działanie wszystkich funkcji i pasująca do posiadanej przez zamawiającego macierzy Fujitsu DX90S2 1) Półka musi być dostarczona ze wszystkimi komponentami do montażu w standardowej szafie rack 19" z zajętością maks. 2U i posiadać wszystkie niezbędne kable potrzebne do podłączenia i poprawnej pracy urządzenia. 2) Obudowa musi zawierać układ nadmiarowy dla modułów zasilania i chłodzenia umożliwiający wymianę tych elementów w razie awarii bez konieczności wyłączania macierzy 3) 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 lub powinna te elementy zawierać. 4) Obudowa musi zawierać dwa moduły I/O zapewniające redundantne połączenie do macierzy. 5) Musi umożliwiać instalację minimum 12 dysków formatu 3,5" wykonanych jako dyski SAS, NearLine-SAS lub SolidStateDisk. 6) Musi zapewniać możliwość dołączania następnych półek rozszerzeń 7) Musi zawierać 12 dysków 600 GB SAS 2.0 3.5" o prędkości obr. 15.000 obr/min	
Gwarancja i serwis	1) Dostarczane rozwiązanie musi być objęte minimum 36 miesięcznym okresem gwarancji z gwarantowanym czasem naprawy w miejscu instalacji urządzenia w następnym dniu roboczym od zgłoszenia. 2) Dostarczany sprzęt musi pochodzić z legalnego kanału sprzedaży producenta w Polsce i musi reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych 3) Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia	

Biblioteka taśmowa (autoloader) **Ilość 1 szt**

Opis wymagań (minimum)		Zgodność/model
Obudowa	Typu rack, maksymalnie 2U, wbudowany czytnik kodów kreskowych,	
Napęd	1x LTO6 SAS, możliwość instalacji 2go napędu	
Interfejs sieciowy		
Liczba slotów	24 obsługujących taśmy LTO 6, jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów,	
Interfejs użytkownika	Dwa interfejsy użytkownika: Interfejs dla administratora na obudowie biblioteki z możliwością zarządzania bezpośrednio z użyciem wbudowanych klawiszy i wyświetlacza LCD: pozwalający odczytywać informacje o stanie urządzenia, przeprowadzać diagnostykę, przeglądać dzienniki systemu, sprawdzać i modyfikować ustawienia konfiguracyjne, weryfikować działanie napędu oraz przeprowadzać inwentaryzację i zarządzać systemem. Interfejs dla administratora pozwalający na zdalne zarządzanie przez stronę www: Internetowy panel administracyjny, z którego można korzystać za pośrednictwem dowolnej przeglądarki internetowej po połączeniu się z urządzeniem przez sieć. Administrator może odczytywać informacje o stanie urządzenia, przeprowadzać diagnostykę, przeglądać dzienniki systemu, sprawdzać i modyfikować ustawienia konfiguracyjne, weryfikować działanie napędu oraz przeprowadzać inwentaryzację i zarządzać systemem, możliwość uaktualniania oprogramowania sprzętowego napędu i biblioteki	
Certyfikaty	Zgodność z Normami Europejskimi (Znak CE). Certyfikat Energy Star 5.0, certyfikat należy dołączyć do oferty w formie oryginału bądź kopii poświadczonej za zgodność z oryginałem przez Wykonawcę.	
Kompatybilność	Biblioteka musi znajdować się na liście: Backup Exec 2012 Hardware Compatibility List (HCL).	
Inne	Zestaw do montażu w szafie RACK, wszystkie niezbędne kable do uruchomienia urządzenia	

Gwarancja	36 miesięcy gwarancji z gwarantowanym czasem naprawy następny dzień roboczy. Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu. Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu. W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).	

Rozbudowa licencji Symantec Backup Exec

Nazwa	Liczba licencji	Zgodność
Rozbudowa posiadanego przez Sąd oprogramowania Symantec Backup Exec o moduł: SYMC BACKUP EXEC V-RAY EDITION/SYMC BACKUP EXEC 2012 PROMO V-RAY EDITION WIN 8 PLUS CORES PER CPU BNDL STD LIC GOV BASIC 12 MONTHS PN - 21274755	2	

Procesor – 2 sztuki	
Opis	Zgodność/model
Procesor dedykowany do serwera Fujitsu PRIMERGY TX300 S4 sn YK7W008979 w architekturze x86 osiągające w oferowanym serwerze w testach wydajności SPECint_2006 min. 30 pkt. Wymagana obecność certyfikatu potwierdzającego osiągnięty wynik na stronie: www.spec.orq (wydruk załączony do oferty). Nie dopuszcza się sprzętu pochodzącego z rynku wtórnego.	
Inne warunki	Sprzęt fabrycznie nowy

Terminal – 1 sztuka			
Nazwa		**Minimalne wymagane parametry**	**Zgodność/model**
Typ ekranu		32", z podświetleniem LED	
Jasność		350 cd/m2	
Ilość kolorów		min. 16,7 mln	
Kontrast statyczny		5000:1	
Kąty widzenia (pion / poziom)		178º/178º	
Czas reakcji matrycy (GtG)		max. 8 ms	
Rozdzielczość		1920x1080	
Proporcje ekranu		16:9	
Pobór energii: max / max BTU		71W / 410	
Złącze		DVI-D, D-Sub, Display Port 1.2, HDMI, RS232C (in/out), RJ45	
Waga monitora		max. 6,5 kg	
Maksymalna szerokość ramki		17 mm	
Montaż ścienny (zgodny z VESA)		tak, 200x200 mm	
Gwarancja		3-letnia gwarancja producenta.	
Zewnętrzny player	Taktowanie procesora min.	2,1GHz	
	Pamięć RAM min.	2GB	
	Złącza	USB 2.0, HDMI, D-Sub, RS232	
	Ethernet min.	1GB	
Nakładka dotykowa		Pasująca do otworów fabrycznych producenta	
Ilość dotyków min.		6	
Grubość szkła max.		3mm	
Materiał ramki		Aluminium	
Pozostałe		Sprzęt fabrycznie nowy, objęty minimum 2 letnią gwarancją producenta.	

Stacja robocza typ 1		Zgodność/model
Ilość: 4		
Procesor	Taktowanie >=2500 MHz; L3 cache >= 8 MB; liczba rdzeni >= 4; liczba wątków >= 8; obsługa 64 bitów; wsparcie dla sprzętowej wirtualizacji; Wyniki w testach: PCMark 7 – co najmniej 5700 3DMark11 I Extreme co najmniej 2450	
Płyta główna	Możliwość obsługi do min. 16GB RAM. Wsparcie dla sprzętowej wirtualizacji.	
Dysk na system operacyjny	SSD min. 32 GB	
Dysk dodatkowy	SATA min. 1 TB 7200 obr/min	
Pamięć operacyjna RAM	min. 16 GB dwukanałowej pamięci SDRAM DDR3 1333 MHz	
Karta graficzna	Min. 1.5 GB pamięci DDR5. Dostępne złącza 2xDVI, HDMI, Display Port. Wydajność w 3Dmark11 powyżej 6200	
Porty	min. 4x USB 3.0, 1 port szeregowy RS-232 (lub adapter umożliwiający podłączenie do portu konsolowego), porty audio (line-out, line-in)	
Czytnik kart	SD, MMC, Comapact Flash	
Karta sieciowa	10/100/1000 MBit/s. Wspierająca funkcję Wake on LAN i PXE 2.0. Umożliwiająca tworzenie i obsługę wirtualnych interfejsów.	
Napęd optyczny	Napęd Blu-ray combo (odczyt z nośników BD i zapis na nośnikach DVD/CD)	
Obudowa	Z przodu obudowy: co najmniej 2 porty USB, porty audio (line-out, mic.)	
System	MS Windows 8 Pro x64 PL	

operacyjny		
Pozostałe warunki	Sprzęt fabrycznie nowy, objęty minimum 2 letnią gwarancją producenta.	

Stacja robocza typ 2		Zgodność/model
Ilość: 4		
Płyta główna	Zaprojektowana przez producenta jednostki centralnej komputera, wyposażona w min. 2 sloty PCI i 1 slot PCI-Express x16 (ze wsparciem dla PCIe x1, nie dopuszcza się złącz Low Profile), 2 złącza DIMM, obsługa do 4GB DDR3 pamięci RAM, kontroler SATA II (dla min. 3 urządzeń)	
Chipset	Dostosowany do oferowanego procesora, min. G41 lub równoważny	
Procesor	Procesor klasy x86 intel Core 2 Duo E7500 (2,93GHz, 1066MHz, 3MB) lub równoważny	
Pamięć RAM	4GB DDR3 1066MHz (2x1024MB)	
Dysk twardy	Min. 160 GB SATAII 7200rpm, 8MB pamięci Cache	
Karta graficzna	Zintegrowana, z możliwością dynamicznego przydzielenia pamięci w obrębie pamięci systemowej do 512MB ze wsparciem dla DirectX 10, API i OpenGL 2.0, np. Intel GMA X4500 lub równoważna	
Karta dźwiękowa	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition (min. ALC269Q), 4 kanałowa lub równoważna, wewnętrzny głośnik w obudowie komputera	
Karta sieciowa	Wbudowana: 10/100/1000Mbit/s, Ethernet RJ 45	
Porty	Wbudowane: 1 x LPT; 1 x RS232, 1 x VGA; min. 8 x USB w tym min. 2 z przodu obudowy; wymagana ilość portów nie może być uzyskana poprzez stosowanie przejściówek lub kart PCI	
Klawiatura	Klawiatura USB w układzie polski programisty	
Mysz	Mysz laserowa USB z sześcioma klawiszami oraz rolką (scroll) min 1000dpi	
Napęd optyczny	Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania płyt	

System operacyjny	Microsoft Windows 7 Profesional PL 32-bit, fabrycznie zainstalowany system operacyjny niewymagający aktywacji za pomocą telefonu lub Internetu w firmie Microsoft. Dołączony nośnik z oprogramowaniem	
Obudowa	– Minitower w standardzie uBTX lub uATX, posiadająca min. 2 wnęki 5.25" i 1 wnękę 3.5" zewnetrzne oraz 2 wnęki 3.5" wewnętrzne (wnęki pełnej wysokości, nie dopuszcza się napędów typu slim) – Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń i napędów bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych); – Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych; Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) oraz kłódki (oczko w obudowie do założenia kłódki) – Zasilacz max 400W	
BIOS	1. Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) 2. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń 3. Możliwość odczytania z BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych , informacji na temat: zainstalowanego procesora, pamięci operacyjnej RAM wraz z informacją o obsadzeniu slotów pamięci, obsadzeniu slotów PCI. 4. Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, portu równoległego, portu szeregowego z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. 5. Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. 6. Możliwość wyłączania portów USB w tym: wszystkich portów, tylko portów znajdujących się na przodzie obudowy. 7. Możliwość zmiany trybu pracy dysku twardego: na	

	pracę zapewniającą największą wydajność, na pracę zmniejszającą poziom hałasu generowanego przez dysk twardy.	
Certyfikaty i standardy	1. Certyfikat ISO 9001:2000 dla producenta jednostki centralnej (załączyć do oferty oświadczenie producenta potwierdzające spełnianie wymogu) 2. Certyfikat ISO 14001 dla producenta jednostki centralnej (załączyć do oferty oświadczenie producenta potwierdzające spełnianie wymogu) 3. Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Vista i Windows 7 (załączyć do oferty oświadczenie producenta potwierdzające spełnianie wymogu) 4. Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie jałowym (IDLE) wynosząca maksymalnie 24,5dB (załączyć do oferty oświadczenie producenta potwierdzające spełnianie wymogu) 5. Deklaracja CE (załączyć do oferty doświadczenie producenta potwierdzające spełnianie wymogu) 6. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia wykonawcy wystawionego na podstawie dokumentacji producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram (załączyć do oferty oświadczenie producenta potwierdzające spełnianie wymogu)	
Gwarancja na cały zestaw	3 lata on-site producenta jednostki centralnej w następnym dniu roboczym Czas reakcji serwisu - do końca następnego dnia roboczego Uszkodzony dysk twardy pozostaje u Zamawiającego Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera (załączyć do oferty oświadczenie producenta potwierdzające spełnianie wymogu)	

	W przypadku nie wywiązywania się z obowiązków gwarancyjnych przez wykonawcę lub firmę serwisującą, producent jednostki centralnej przejmie na siebie wszelkie zobowiązania związane z serwisem gwarancyjnym na warunkach wymaganych w niniejszym postępowaniu (załączyć do oferty oświadczenie producenta potwierdzające spełnianie wymogu)	
Inne	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela Dołączony nośnik ze sterownikami. UWAGA: W przypadku uzasadnionych wątpliwości zamawiającego co do spełniania przez zaoferowany sprzęt w/w wymogów lub posiadania w/w certyfikatów, zamawiający zastrzega sobie prawo zażądać od wykonawcy przedstawienia dokumentów uwiarygodniających, np. kopii stosownych certyfikatów, wydruków, raportów itp. UWAGA: Oświadczenie producenta o którym mowa powyżej, musi być wystawione z dedykacją dla wykonawcy składającego ofertę oraz wystawione ściśle na potrzeby niniejszego postępowania, tzn. opatrzone nazwą i znakiem postępowania, nazwą Zamawiającego oraz nazwą wykonawcy składającego ofertę, a także oznaczeniem oferowanego w postępowaniu typu/modelu produktu, którego oświadczenie dotyczy. Oświadczenie winno być podpisane przez osobę lub osoby prawnie umocowane do składania oświadczeń woli w imieniu producenta. Oświadczenie należy złożyć w oryginale lub kopii poświadczonej za zgodność z oryginałem przez wykonawcę. UWAGA: Zamawiający zastrzega sobie prawo zażądać przedstawienia oryginałów lub notarialnie poświadczonych kopii w/w wymaganych oświadczeń i dokumentów, jeżeli złożone kopie będą nieczytelne lub będą budzić wątpliwości co do ich prawdziwości.	

Komputer przenośny		Zgodność/model
Ilość: 4		
Typ	Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości: HD (1366x768) w technologii LED przeciwodblaskowy, jasność min 200 nitów, kontrast min 300:1	
Procesor	Procesor zaprojektowany do pracy w komputerach przenośnych, Zaoferowany procesor musi uzyskiwać jednocześnie w teście Passmark CPU Mark min.: 3190pkt (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net – wydruk ze strony należy dołączyć do oferty.	
Pamięć operacyjna RAM	Min. 4GB (1x4GB) możliwość rozbudowy do min 16GB	
Parametry pamięci masowej	Min. 320 GB 7200RPM	
Karta graficzna	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej, ze sprzętowym wsparciem dla DirectX 10.1, OpenGL 3.0 oraz Dual HD HW Decode	
Wyposażenie multimedialne	Karta dźwiękowa zgodna z HD, wbudowane głośniki stereo Wbudowany w obudowę matrycy mikrofon.	
Wymagania dotyczące baterii i zasilania	6-cell, o wydłużonej żywotności. Czas pracy na baterii wg dokumentacji producenta min. 7 godzin.	
Zgodność z systemami operacyjnymi i standardami	Zgodność z 64-bitową wersją systemu operacyjnego Microsoft Windows 7 Professional PL	
System operacyjny	Licencja dla Windows 7 Professional 64bit PL OEM (preinstalowany na dysku twardym) wraz z nośnikiem pozwalającym na ponowną instalację systemu niewymagającą wpisywania klucza rejestracyjnego lub rejestracji poprzez Internet czy telefon, płyta przygotowana przez producenta komputera do automatycznej instalacji na danej jednostce (system wraz ze sterownikami). Nośnik do wersji 32 oraz 64-bit	
Bezpieczeństwo	BIOS w standardzie UEFI musi posiadać następujące cechy: - możliwość ustawienia hasła na dysku (drive lock) - dostępna opcja włączenia/wyłączenia portów: USB, eSATA, karty sieciowej, karty audio, czytnika kart pamięci, kamerki internetowej, mikrofonów, głośników,	

	możliwość blokady/wyłączenia gniazda Express Card, modułu bluetooth, WLAN - kontrola sekwencji boot-ącej; - możliwość startu systemu z urządzenia USB oraz karty SD - funkcja blokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń - blokowanie zapisu na dyskach wymiennych USB - BIOS musi zawierać nieulotną informację z nazwą producenta, nazwą produktu, jego numerem seryjnym, datę startu gwarancji, wersji BIOS i data wydania BIOS, a także informację o: typie zainstalowanego procesora, ilości i typie pamięci RAM, rodzaju układu graficznego, dysku HDD oraz baterii wraz z ich numerami seryjnymi. 2. Możliwość zapięcia linki typu Kensington 3. Wbudowana w BIOS funkcjonalność pozwalająca na bezpieczne usuwanie danych z dysku twardego 4. Udostępniona bez dodatkowych opłat, pełna wersja oprogramowania, szyfrującego zawartość twardego dysku zgodnie z certyfikatem X.509 oraz algorytmem szyfrującym AES 128 bit oraz AES 256bit 5. Złącze typu Kensington Lock 6. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 1.2)	
Zarządzanie	Dołączone dedykowane oprogramowanie producenta komputera umożliwiające zdalną inwentaryzację sprzętu, monitorowanie stanu jego pracy, aktualizację i zmianę ustawień BIOS'u oraz na aktualizację sterowników.	
Waga	Waga max 2.9 kg z baterią.	
Wymagania dodatkowe	1. Wbudowane porty i złącza: 1 x VGA, 1 x Display Port v1.2, 2 szt USB 2.0, 1 szt USB 3.0, 1 szt eSATA/USB 2.0, RJ-45, 1 x złącze słuchawkowe stereo/liniowe wyjście , 1 x złącze mikrofonowe, czytnik kart multimedialnych SD/MMC, Express Card 54mm 2. Karta sieciowa LAN 10/100/1000 Ethernet RJ 45 zintegrowana z płytą główną oraz WLAN 802.11 b/g/n, zintegrowany z płytą główną lub w postaci wewnętrznego modułu mini-PCI Express z	

	dedykowanym przełącznikiem do uruchamiania modułu WLAN 3. Wbudowany moduł Bluetooth 4.0 4. Napęd optyczny DVD +/- RW DL.. Dołączony nośnik ze sterownikami.	
Warunki gwarancji	3-letnia gwarancja producenta on site z czasem reakcji Next Business Day i pozostawieniem uszkodzonego dysku. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Wykonawcy potwierdzonego przez Producenta, że serwis będzie realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta	
Certyfikaty i standardy	– Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty) – Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty) – Deklaracja zgodności CE (załączyć do oferty) – Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki – Potwierdzenie kompatybilności komputera na stronie Microsoft Windows Hardware Compatibility List na daną platformę systemową (wydruk ze strony) – Certyfikat EnergyStar 5.0 – komputer musi znajdować się na liście zgodności dostępnej na stronie www.energystar.gov oraz http://www.eu-energystar.org – Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera – Możliwość weryfikacji czasu obowiązywania i reżimu gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera	
Akcesoria	Torba dedykowana do transportu komputera przenośnego	