Załącznik nr 1 do SIWZ

Dostarczenie sprzętu informatycznego wraz z jego instalacją i modernizacją sieci informatycznej

A. Dostawa sprzętu informatycznego

1. Specyfikacja ilościowa oraz gwarancje.

	nazwa	*szt./kpl*	*gwarancja minimum*
1	serwer z wyposażeniem	1	60 miesięcy
2	router sprzętowy internetowy z wyposażeniem wersja 1	1	12 miesięcy
3	system antyspamowy sprzętowy pocztowy z wyposażeniem	1	12 miesięcy
4	router sprzętowy internetowy z wyposażeniem wersja 2	2	12 miesięcy
5	punkty dostępowe Wi-Fi	2	12 miesięcy
6	przełącznik sieciowy 1Gb POE 24 gniazda typu RACK	1	dożywotnia
7	przełącznik sieciowy 1Gb POE 8 gniazd	1	dożywotnia
8	Usługa rozbudowy sieci informatycznej		12 miesięcy

2. Serwer z wyposażeniem.
    a. wyposażenie:
        i. serwer jednostka centralna;
        ii. oprogramowanie wirtualizacyjne do serwera z licencjami i wsparciem;
        iii. oprogramowanie archiwizacyjne z licencjami i wsparciem.

    b. serwer jednostka centralna:

Parametr lub warunek	**Minimalne wymagania**
Obudowa	-Typu Rack, wysokość maksimum 2U; -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack;
Płyta główna	-Dwuprocesorowa, wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów 28-rdzeniowych; -Minimum 6 złącz PCI Express generacji 3, w tym minimum 3 złącza o prędkości x16 i 3 złącza o prędkości x8; -Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora (niezależne od dysków twardych) – minimum dwa sloty M.2;
Procesory	-Obsługa procesorów minimum 28-rdzeniowych; -Zainstalowane minimum 2 procesory 10-rdzeniowe, 20-wątkowe w architekturze x86, o bazowej częstotliwości taktowania 2,20 GHz, osiągające

	minimum 101 punktów w teście CPU2017 Integer Rates, wynik Peak Result dla układów dwuprocesorowych. Raport z testu musi być dostępny na stronie www.spec.org
Pamięć RAM	-Zainstalowane minimum 64 GB pamięci RAM typu DDR4 Registered, 2666Mhz w modułach o pojemności 32GB; -Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC; -Wsparcie dla konfiguracji pamięci w trybie „Rank Sparing"; -Minimum 24 gniazda pamięci RAM na płycie głównej, obsługa minimum 3072GB pamięci RAM DDR4 2666 Mhz;
Kontrolery dyskowe, I/O	-Zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,50,60 2GB pamięci podręcznej cache, -Możliwość doposażenia w technologię podtrzymania zawartości pamięci cache przy pomocy pamięci nieulotnej flash.
Dyski twarde	-Zainstalowane 5 dysków SSD SATA 6G minimum 960GB typu mixed – use, DWPD co najmniej 3, 2,5" dyski hotplug; -Zainstalowane 7 dysków SATA 6G minimum 1TB z 7,2k rpm, 2,5"; dyski hotplug; -możliwość zainstalowania sumarycznie 16 dysków twardych lub SSD w formacie szerokości 2,5"
Inne napędy zintegrowane	Brak
Kontrolery LAN	-Zainstalowana minimum dwuportowa karta 2x1Gbit/s ze wsparciem iSCSI (zintegrowane w obudowie serwera, nie zajmująca slotów PCIe); -Minimum jedna 4-portowa karta 1G LAN ze wsparciem iSCSI;
Porty	-zintegrowana karta graficzna ze złączem VGA; -5x USB, minimum 1 wewnętrzne, 2 dostępne z przodu serwera, 2 z tyłu serwera z czego 5 złącz w standardzie USB 3.0; Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera; -moduł TPM 2.0
Zasilanie, chłodzenie	-Minimum 2 redundantne zasilacze hotplug o mocy minimum 800W, o sprawności 94% (tzw klasa Platinum) -Redundantne wentylatory hotplug; -Zasilacze dostarczone z kablami (IEC 320 C14/C13) o długości min. 4m;

Zarządzanie minimalna konfiguracja	-Wbudowane diody informacyjne informujące o stanie serwera; -Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web (także SSL, SSH) • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) • Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 16Gbit/s oferowanych przez producenta serwera) • 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 (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
Wspierane OS	-Windows 2016 Hyper-V, Windows 2012 R2 Hyper-V, VMWare, Suse, RHEL
Gwarancja	-minimum 60 miesięcy gwarancji producenta serwera w trybie onsite z gwarantowanym czasem przyjęcia zgłoszenia najpóźniej w następnym dniu roboczym -Dostępność części zamiennych przez minimum 60 miesięcy od momentu zakupu serwera; -Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji;
wsparcie techniczne	-Wymagana jest bezpłatna dostępność poprawek i aktualizacji przez minimum 60 miesięcy BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji;

Dokumentacja, inne	-Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA -Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce -Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu - Telefoniczna infolinia/linia techniczna producenta serwera 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

c. oprogramowanie wirtualizacyjne do serwera z licencjami i wsparciem;

Licencje powinny umożliwiać uruchomianie wirtualizacji na serwerach fizycznych o łącznej liczbie 6 procesorów. Wszystkie licencje powinny być dostarczone wraz z rocznym wsparciem, świadczonym przez producenta oprogramowania.

Wymagania techniczne dot. oprogramowania

- Warstwa wirtualizacji powinna być rozwiązaniem systemowym tzn. powinna być zainstalowana bezpośrednio na sprzęcie fizycznym.
- Rozwiązanie powinno zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
- Oprogramowanie powinno posiadać centralną konsolę graficzną do zarządzania środowiskiem wirtualnym.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do 255GB pamięci operacyjnej.
- Rozwiązanie powinno umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
- Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
- Rozwiązanie powinno wspierać następujące systemy operacyjne: Windows XP, Windows Vista , Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012R2, Windows Server 2016, Centos 7 Linux.
- Rozwiązanie powinno umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągniecia maksymalnego współczynnika konsolidacji.
- Rozwiązanie powinno zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej.
- Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
- Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
- Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi Microsoft Active Directory.
- Rozwiązanie musi umożliwiać udostepnienie maszynie wirtualnej większej ilości zasobów dyskowych aniżeli fizycznie zarezerwowane.

- System powinien posiadać funkcjonalność wirtualnego przełącznika (switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej.

d. oprogramowanie archiwizacyjne z licencjami i wsparciem.

Parametr lub warunek	**Minimalne wymagania**
Wymagania ogólne	• Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2016. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej • Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. • Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. • Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V
Funkcje i właściwości	• Oprogramowanie musi być licencjonowanie w modelu “per-CPU”. Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone • Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej • Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków • Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji • Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. • Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania • Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia • Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość akutalizacji pola „notatki” na wirtualnej maszynie • Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware.

	• Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director 5.5, 5.6, 8.0, 8.10 i archiwizować również metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD • Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji • Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji • Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) • Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
Wymagania RPO	• Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej • Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora • Oprogramowanie musi wspierać kopiowanie plików na taśmy • Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server • Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej • Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) • Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu. • Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. • Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik • Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) • Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V • Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) • Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere

	Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)
Wymagania RTO	• Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dla srodowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania • Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować jaką migrację swoimi mechanizmami • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure. • Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików • Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. • Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: o **Linux** ▪ ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs o **BSD** ▪ UFS, UFS2 o **Solaris** ▪ ZFS, UFS o **Mac** ▪ HFS, HFS+ o **Windows** ▪ NTFS, FAT, FAT32, ReFS o **Novell OES** ▪ NSS • Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. • Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. • Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, grupy oraz pozwalać na odtworzenie haseł.

	• Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. • Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia. • Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych. • Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows • Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Wsparcie techniczne	Wszystkie licencje powinny być dostarczone wraz z minimum rocznym wsparciem, świadczonym przez producenta oprogramowania.

3. router sprzętowy internetowy z wyposażeniem wersja 1.

Parametr lub warunek	**Minimalne wymagania**
Wymagania ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji.

	• Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, dysk i zasilanie	1. System realizujący funkcję Firewall musi dysponować minimum: • 18 portami Gigabit Ethernet RJ-45. • 4 gniazdami SFP 1 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 135.000 nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 512 B. 3. Przepustowość Stateful Firewall: nie mniej niż 9 Gbps dla pakietów 64 B. 4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.5 Gbps. 5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 9 Gbps. 6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.2 Gbps. 7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps. 8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.
Funkcje systemu bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji.

	3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. Analiza ruchu szyfrowanego protokołem SSH.
Polityki bezpieczeństwa, firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie

	system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Kontrola antywirusowa	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Ochrana przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

	2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola www	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • 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. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

	2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall
Logowanie	1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall. • ICSA lub NSS Labs dla funkcji IPS. • ICSA dla funkcji IPSec VPN. • ICSA dla funkcji SSL VPN.
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: • Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Gwarancja oraz wsparcie	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz minimum roczne wsparcie techniczne w trybie 8x5
Rozszerzone wsparcie serwisowe	• System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres minimum 12 miesięcy. • Certyfikat ISO 9001 podmiotu serwisującego.
Opisy do wymagań ogólnych	1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): 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.

4. System antyspamowy sprzętowy pocztowy z wyposażeniem.

Parametr lub warunek	**Minimalne wymagania**
Wymagania ogólne	System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

	Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o dedykowany system operacyjny oraz komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów: 1. Tryb Gateway. 2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).
Parametry fizyczne systemu antyspamowego	1. System musi być wyposażony w interfejsy: • 4 porty Gigabit Ethernet RJ-45. 2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 500 GB. 3. System musi posiadać wbudowany port konsoli szeregowej. 4. Zasilanie z sieci 230V/50Hz.
Funkcje serwera poczty	W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 50 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych. W tym zakresie dostarczony system musi zapewniać: 1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP. 2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2). 3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników. 4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2). 5. Polski interfejs użytkownika przy dostępie przez WebMail. 6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP. 7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.
Ogólne funkcje systemu ochrony poczty	Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje: 1. Wsparcie dla co najmniej 2 domen pocztowych. 2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 2,5 tys. wiadomości/godzinę. 3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all). 4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP. 5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).

	6. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. 7. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. 8. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP. 9. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. 10. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz POP3. 11. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. 12. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. 13. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. 14. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. 15. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention).
Kontrola antywirusowa i ochrona przed malware	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Skanowanie antywirusowe wiadomości SMTP. 2. Kwarantannę dla zainfekowanych plików. 3. Skanowanie załączników skompresowanych. 4. Definiowanie komunikatów powiadomień w języku polskim. 5. Blokowanie załączników w oparciu o typ pliku. 6. Możliwość zdefiniowania nie mniej niż 15 polityk kontroli antywirusowej. 7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu. 8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
Kontrola antyspamowa	System musi zapewniać poniższe funkcje i metody filtrowania spamu: 1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. 2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. 3. Szczegółowa kontrola nagłówka wiadomości.

	4. Analiza Heurystyczna. 5. Współpraca z zewnętrznymi serwerami RBL, SURBL. 6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen. 7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników. 8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF. 9. Kontrola w oparciu o Greylisting oraz SPF. 10. Filtrowanie treści wiadomości i załączników. 11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. 12. Możliwość zdefiniowania nie mniej niż 15 polityk kontroli antyspamowej. 13. Ochrona typu outbrake. 14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking). 15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
Ochrona przed atakami na usługę poczty	System musi zapewniać poniższe funkcje i metody filtrowania: 1. Ochrona przed atakami na adres odbiorcy. 2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. 3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. 4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing). 5. Weryfikacja poprawności adresu e-mail nadawcy.
Funkcje logowania i raportowania	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Logowanie do zewnętrznego serwera SYSLOG. 2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. 3. Logowanie informacji na temat spamu oraz niedozwolonych załączników. 4. Możliwość podglądu logów w czasie rzeczywistym. 5. Możliwość analizy przebiegu sesji SMTP. 6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. 7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu. 8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności	System ochrony poczty musi zapewniać poniższe funkcje: 1. Konfigurację HA w każdym z trybów: gateway, transparent. 2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP. 3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. 4. Monitorowanie stanu pracy klastra.
Aktualizacje sygnatur, dostęp do bazy spamu	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. 2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
Zarządzanie	System ochrony poczty musi zapewniać poniższe funkcje: 1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. 2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy. 3. Powinna istnieć możliwość zdefiniowania co najmniej 6 lokalnych kont administracyjnych.
Certyfikaty	1. VBSpam and VB100 rated lub Common Criteria NDPP, FIPS 140-2 Certified.
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: 1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa na okres min. 12 miesięcy.
Gwarancja oraz wsparcie	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz minimum roczne wsparcie techniczne w trybie 8x5
Opisy do wymagań ogólnych	1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): 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.

5. Router sprzętowy internetowy z wyposażeniem wersja 2

Parametr lub warunek	**Minimalne wymagania**
Wymagania ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN.
Interfejsy, dysk, zasilanie	1. System realizujący funkcję Firewall musi dysponować minimum: • 10 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

	3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 1.3 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 3 Gbps dla pakietów 512 B. 3. Przepustowość Stateful Firewall: nie mniej niż 3 Gbps dla pakietów 64 B. 4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 650 Mbps. 5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 2 Gbps. 6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 400 Mbps. 7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 200 Mbps. 8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 175 Mbps.
Funkcje systemu bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL.

Polityki bezpieczeństwa, firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

	3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Kontrola antywirusowa	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Ochrana przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola www	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.

	3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • 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. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
Logowanie	1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania

	w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall. • ICSA lub NSS Labs dla funkcji IPS. • ICSA dla funkcji IPSec VPN. • ICSA dla funkcji SSL VPN.
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: • Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.
Gwarancja oraz wsparcie	• Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz minimum roczne wsparcie techniczne w trybie 8x5.
Opisy do wymagań ogólnych	1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): 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.

6. Punkty dostępowe Wi-Fi.

   Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej; jeżeli do zarządzania punktami dostępowymi potrzebny jest dodatkowy kontroler to należy go uwzględnić w ofercie.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
    a. Temperatura -20–50°C,
    b. Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington.
3. Urządzenie musi być wyposażone w dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
    a. 2.4 GHz 802.11b/g/n,
    b. 5 GHz 802.11a/n/ac,
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
5. Liczba interfejsów:
    a. Ethernet – 1 w standardzie 10/100/1000 Base-TX,
    b. USB – 1 Typ A.
6. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub zewnętrzny zasilacz, który należy uwzględnić w ofercie;
7. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
    a. Tunnel,
    b. Bridge,
    c. Mesh.
8. Wsparcie dla QoS: 802.11e, WME/WMM Multimedia Extensions, konfigurowalne polityki QoS per użytkownik/aplikacja.
9. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, Web Captive Portal, MAC blacklist & whitelist, 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
10. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    a. MIMO – 2x2,
    b. Transmit Beam Forming (TxBF),
    c. Maksymalna przepustowość dla poszczególnych modułów radiowych:
        i. 400 Mbps;
        ii. 867 Mbps;
    d. Wymagana moc nadawania:
        i. min. 25 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
        ii. min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
    e. Wsparcie dla 802.11n 20/40Mhz HT,
    f. Wsparcie dla kanału 80 MHz dla 802.11ac,
    g. Anteny – 4 wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.
    h. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
    i. Maksymalna deklarowana liczba klientów per moduł radiowy – 512.
11. Funkcje interfejsu radiowego:

a. Skaner częstotliwości 2.4 oraz 5 GHz,
b. Skanowanie w tle podczas obsługi klientów na pasmach 2.4 oraz 5 GHz,
c. Skaner częstotliwości 2.4 oraz 5GHz w trybie dedykowanego monitora,

12. Funkcje dodatkowe:
    a. Low-Density Parity Check (LDPC) Encoding,
    b. Maximum Likelihood Demodulation (MLD),
    c. Maximum Ratio Combining (MRC),
    d. A-MPDU and A-MSDU Packet Aggregation,
    e. MIMO Power Save,
    f. Short Guard Interval,
    g. WME Multimedia Extensions.
13. Punkt dostępowy musi być certyfikowanym urządzeniem WiFi Alliance: WiFi certified IEEE Std 802.11a/b/g/n (ac) oraz posiadać certyfikację DFS.
14. Gwarancja oraz wsparcie:
    Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz minimum roczne wsparcie techniczne w trybie 8x5.

7. Przełącznik sieciowy 1Gb POE 24 gniazda typu RACK.

    a. Minimum 24 porty 10/100/1000BaseT ze wsparciem dla standardu PoE+ (802.3at)
    b. Minimum 4 porty Gigabitowe SFP, niezależne od wymaganych portów 10/100/1000BaseT
    c. Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT
    d. Wydajność przełączania co najmniej 56 Gbps oraz przepustowość 41,6 Mpps dla pakietów 64 bajtowych
    e. - Obsługa 4094 tagów IEEE 802.1Q oraz minimum 512 jednoczesnych sieci VLAN
    f. Automatyczne wykrywanie punktów bezprzewodowych podłączonych do przełącznika, automatyczne konfigurowanie portów, do których są one podłączone (minimum sieć VLAN, CoS, budżet mocy PoE, priorytet PoE)
    g. Funkcja automatycznej aprowizacji i konfiguracji przełącznika przy jego pierwszym podłączeniu do sieci bez konieczności wykonywania wstępnej, ręcznej konfiguracji
    h. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
    i. Budżet mocy PoE nie może być mniejszy niż 190W
    j. Bufor pakietów nie mniejszy niż 1,5MB
    k. Minimum 128MB pamięci Flash
    l. Dostęp do urządzenia przez konsolę szeregową (linia komend umożliwiająca pełne zarządzanie przełącznikiem), HTTPS, SSHv2 i SNMPv3
    m. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
    n. Obsługa Secure FTP
    o. Obsługa 802.3ad Link Aggregation Protocol (LACP)
    p. Obsługa Simple Network Time Protocol (SNTP) v4
    q. Wielkość tablicy adresów MAC: minimum 16000
    r. Obsługa LLDP i LLDP-MED
    s. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting

t. Funkcja autoryzacji użytkowników zgodna z 802.1x
u. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+,
v. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
w. Obsługa list kontroli dostępu (ACL)
x. Obsługa protokołu TR-069
y. Obudowa wieżowa 1U umożliwiająca instalację w szafie 19" o głębokości nie większej niż 35 cm.
z. Maksymalny pobór mocy (bez PoE) nie większy niż 60W
aa. Minimalny zakres pracy od 0°C do 45°C
bb. Dożywotnia (tak długo jak Zamawiający posiada produkt, minimum 60 miesięcy od zakończenia produkcji urządzenia, gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez okres co najmniej 10 lat. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do minimum 5 letniego wsparcia technicznego producenta od zakończenia produkcji urządzenia.

8. Przełącznik sieciowy 1Gb POE 8 gniazd.

a. Co najmniej 10 portów gigabitowych w standardzie 10/100/1000BaseT z czego minimum 8 ze wsparciem dla standardu PoE+ (802.3at)
b. Co najmniej 2 porty 1000BaseX ze stykiem definiowanym przez SFP (dopuszcza się porty typu Combo, współdzielone z portami 10/100/1000BaseT).
c. Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT
d. Wydajność przełączania co najmniej 20 Gbps oraz przepustowość 14,8 Mpps dla pakietów 64 bajtowych
e. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 512 jednoczesnych sieci VLAN
f. Automatyczne wykrywanie i konfiguracja punktów bezprzewodowych tego samego producenta podłączonych do przełącznika
g. Funkcja automatycznej aprowizacji i konfiguracji przełącznika przy jego pierwszym podłączeniu do sieci bez konieczności wykonywania wstępnej, ręcznej konfiguracji
h. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
i. Bufor pakietów nie mniejszy niż 1,5MB
j. Minimum 128MB pamięci Flash
k. Budżet mocy PoE nie może być mniejszy niż 60W
l. Dostęp do urządzenia przez konsolę szeregową (linia komend umożliwiająca pełne zarządzanie przełącznikiem), HTTPS, SSHv2 i SNMPv3
m. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
n. Obsługa Secure FTP
o. Obsługa 802.3ad Link Aggregation Protocol (LACP)
p. Obsługa Simple Network Time Protocol (SNTP) v4

q. Wielkość tablicy adresów MAC: minimum 16000
r. Obsługa LLDP i LLDP-MED
s. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting
t. Funkcja autoryzacji użytkowników zgodna z 802.1x
u. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+,
v. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
w. Obsługa list kontroli dostępu (ACL)
x. Obsługa protokołu TR-069Wysokość w szafie 19" – 1U. Kompaktowa obudowa o szerokości nie większej niż 13" i głębokości nie większej niż 16 cm. Na wyposażeniu powinny również znajdować się elementy do montażu w standardowej szafie 19"
y. Pasywne chłodzenie – brak wentylatora
z. Minimalny zakres pracy od 0°C do 45°C
aa. Maksymalny pobór mocy (bez PoE) nie większy niż 20W
bb. Dożywotnia (tak długo jak Zamawiający posiada produkt, minimum 60 mieisięcy od zakończenia produkcji urządzenia, gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez okres co najmniej 10 lat. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do minimum 5 letniego wsparcia technicznego producenta od zakończenia produkcji urządzenia.

B. Instalacja sprzętu oraz modernizacja sieci komputerowej

1. Instalacja sprzętu oraz modernizacja sieci komputerowej dotyczy 3 lokalizacji:
    a. Gmachu Głównego MNP wraz z Muzeum Sztuk Użytkowych; pozycje 1, 2, 3 specyfikacji ilościowej;
    b. Muzeum Pałacu w Rogalinie; pozycja 4 (szt. 1) specyfikacji ilościowej;
    c. Zamku w Gołuchowie; pozycje 4 (szt. 1), 5, 6, 7 specyfikacji ilościowej;

2. Instalacja sprzętu i modernizacja sieci komputerowej w Gmachu Głównym oraz Muzeum Sztuk Użytkowych obejmuje:
    a. instalację oraz konfigurację serwera z pozycji 1 specyfikacji ilościowej;
        i. instalacja i konfiguracja mechanizmów wirtualizacji pozwalających na uruchomienie, współdzielenie i równoważenie obciążenia zasobów serwera fizycznego prze minimum 5 serwerów wirtualnych;
        ii. konfiguracja 2 serwerów wirtualnych pod serwery stron internetowych;
        iii. konfiguracja serwera wirtualnego pod serwer pocztowy;
        iv. konfiguracja serwera wirtualnego pod serwer FTP
        v. konfiguracja serwera wirtualnego pod serwer tzw. usług w chmurze;
        vi. przeniesienie minimum 6 portali internetowych;

vii. wdrożenie technologii SSL;

b. instalację oraz konfigurację routera z pozycji 2 specyfikacji ilościowej; wydzielenie strefy DMZ (tzw. zdemilitaryzowanej) pod instalację z poprzedniej pozycji
c. instalację oraz konfigurację systemu antyspamowego sprzętowego z pozycji 3 specyfikacji ilościowej;
d. konfigurację istniejących punktów dostępowych Wi-Fi; konfiguracja powinna obejmować funkcjonowanie minimum 2 podsieci Wi-Fi:
    i. muzealnej – z dostępem do sieci wewnętrznej i internetu;
    ii. dla gości – z dostępem do internetu odseparowanej logicznie od sieci muzealnej;

3. Instalacja sprzętu i modernizacja sieci komputerowej w Muzeum Pałacu w Rogalinie obejmuje:
    a. instalację oraz konfigurację routera z pozycji 4 specyfikacji ilościowej; konfiguracja powinna obejmować możliwość połączeń VPN do wybranych zasobów w Gmachu Głównym; zabezpieczenie dostępu z sieci internetowej oraz logowanie dostępu do sieci internetowej;
    b. konfigurację istniejących punktów dostępowych Wi-Fi; konfiguracja powinna obejmować funkcjonowanie minimum 2 podsieci Wi-Fi:
        i. muzealnej – z dostępem do sieci wewnętrznej i internetu;
        ii. dla gości – z dostępem do internetu odseparowanej logicznie od sieci muzealnej;

4. Instalacja sprzętu i modernizacja sieci komputerowej w Zamku w Gołuchowie obejmuje:
    a. instalację oraz konfigurację routera z pozycji 4 specyfikacji ilościowej; konfiguracja powinna obejmować możliwość połączeń VPN do wybranych zasobów w Gmachu Głównym; zabezpieczenie dostępu z sieci internetowej oraz logowanie dostępu do sieci internetowej;
    b. instalację oraz konfigurację przełączników sieciowych z pozycji 6 oraz 7 specyfikacji ilościowej tak aby zapewnić bezpieczeństwo sieci;
    c. instalację oraz konfigurację punktów dostępowych Wi-Fi z pozycji 5 specyfikacji ilościowej; konfiguracja powinna obejmować funkcjonowanie minimum 2 podsieci Wi-Fi:
        i. muzealnej – z dostępem do sieci wewnętrznej i internetu;
        ii. dla gości – z dostępem do internetu odseparowanej logicznie od sieci muzealnej;

C. Szczegółowy opis instalacji sprzętu oraz modernizacji sieci komputerowej.

1. Opis ogólny:

    Zastosowany program do wirtualizacji serwera i instalacji serwerów wirtualnych powinien zapewniać pełną wirtualizację tzn. żadna z usług nie będzie dzieliła zasobu systemu operacyjnego. Ze względu na kompatybilność z istniejącym zasobami wszystkie serwery wirtualne powinny funkcjonować w oparciu system operacyjny Centos 7 Linux.

2. Bezpieczeństwo:

    a. Bezpieczeństwo dla usług dostępnych w sieci Internet powinno być zapewnione zarówno w formie aktywnej jak i pasywnej. bezpieczeństwo pasywne realizowane powinno być przez sztywno określone parametry usług. Bezpieczeństwo aktywne powinno być realizowane przez zastosowanie narzędzi diagnostycznych pozwalających na wykrycie anomalii jak również podjęcie automatycznych działań zapobiegawczych.

    b. Forma aktywna powinna umożliwiać użycie na każdym z serwerów wirtualnych:
        i. firewalld – sztywne określenie dostępu wyłącznie do tych usług dla których przeznaczony jest dany serwer wirtualny;
        ii. maldet – dla usług www – skaner poszukujący niepożądanego kodu w ramach stron www;
        iii. fail2ban – analiza logów poszczególnych usług w locie wraz z automatycznym podjęciem blokady w ramach firewalld;
        iv. rkhunter – skanowanie systemu operacyjnego w poszukiwaniu anomalii konfiguracyjnych oraz rootkit-ów;

    c. Wszelkie usługi i dostępy powinny być przydzielane z zasadą minimalnych uprawnień.

3. Monitoring usług:

    Wszystkie serwery wirtualne powinny być monitorowane za pomocą odpowiedniego oprogramowania. Monitorowaniu powinna podlegać dostępność poszczególnych usług na wskazanych portach jak również aktualne wykorzystanie poszczególnych zasobów mających wpływ na wydajność oraz dostępność usług.

4. Usługa serwera pocztowego:

    a. W celu zapewnienia kompatybilności z innymi usługami istniejącymi w muzeum zakłada się wykorzystanie programów Postfix oraz Dovecot. Ochrona antywirusowa oraz antyspamowa serwera pocztowego powinna być realizowana za pomocą sprzętowego systemu antyspamowego wymienionego w specyfikacji ilościowej (punkt A.1.3); serwer pocztowy powinien wykorzystywać technikę SSL;
    b. Usługa powinna posiadać aktywną warstwę bezpieczeństwa analizującą logi w locie w celu ochrony przed nieuprawnionym dostępem;
    c. Usługa powinna posiadać konfigurowalne ograniczenie liczby odbiorców pojedynczej wiadomości, ograniczenie ilościowe możliwych do wysłania wiadomości w jednostce czasu oraz maksymalną wielkość odbieranej wiadomości;
    d. Powinna istnieć możliwość blokowania rozszerzeń potencjalnie niebezpiecznych plików min. exe, vb, bat, reg
    e. Usługa powinna wspierać protokoły IMAP/POP3/SMTP oraz ich bezpieczne wersje IMAPs/POP3s/SMTPs;
    f. Uwierzytelnienie poczty oraz jej wiarygodność powinno być realizowane za pomocą protokołów SPF, DKIM, DMARC;
    g. Powinna istnieć możliwość uruchomienia dodatkowego filtrowania przychodzącej i wychodzącej wiadomości;

h. Adresy usług pocztowych: pop.mnp.art.pl, smtp.mnp.art.pl oraz mail.mnp.art.pl, do zarządzania pocztą, który powinien być niedostępny publicznie i dostępny z sieci wewnętrznej VPN;

5. Serwer www:
    a. W celu zapewnienia kompatybilności z dotychczasowymi portalami www serwer powinien być zainstalowany w oparciu o Centos 7 Linux i wspierać wersję PHP 5.4 – 7.2 oraz wykorzystywać Apache 2.4 z repozytorium Centos; serwer powinien wykorzystywać technikę SSL;
    b. Warstwa bezpieczeństwa powinna być zrealizowana w formie statycznej oraz aktywnej (patrz punkt A.2) oraz:
        i. WAF – wsparcie dla reguł OWASP na poziomie serwera Apache – mod_security;
        ii. Reguły Files – blokujące domyślnie rozszerzenia potencjalnie zawierające dane krytyczne (xls, sql, csv) lub krytyczne adresy podatne na eksploitację np. wp-login.php;
        iii. Analiza logów serwera w poszukiwaniu nieudanych prób logowania wraz z aktywną czasowo blokadą;
    c. usługa www powinna oferować 2 protokoły http oaz https (wsparcie dla LetsEncrypt); dostęp do zasobów webowych powinien odbywać się za pośrednictwem protokołu SFTP;
    d. Interpreter PHP powinien być uruchamiany za pomocą modułu mod_fcgid z możliwością definiowania konfiguracji php.ini na poziomie użytkownika dla każdej z oferowanych wersji; zakłada się brak wsparcia dla funkcji podatnych na ataki m.in. exec, system, shell_exec, mail, phpinfo();
    e. zarządzanie serwerem powinno odbywać się za pomocą interfejsu graficznego; dostęp do panelu powinien odbywać się po uprzednim zalogowaniu do VPN;
    f. wykonywanie kopii bezpieczeństwa na zewnętrzny serwer (np. za pomocą programu rsync) powinno odbywać się w sposób automatyczny co najmniej raz na dobę.

6. Serwer bazodanowy do serwera www.
    a. W celu zapewnienia kompatybilności z dotychczasowymi portalami www serwer powinien być zainstalowany w oparciu o Centos 7 Linux; domyślnym silnikiem bazowym powinien być program MariaDB 10.x;
    b. Usługa nie może być dostępna publicznie w sieci Internet i ma stanowić zasób wewnętrzny, do którego będą się łączyć aplikacje i usługi wymagające dostępu do baz danych i znajdujące się w tej samej sieci.
    c. Każda z baz danych powinna posiadać swojego wydzielonego użytkownika;
    d. Zakłada się, że graficzny klient dostępny będzie w ramach serwera webowego pod adresem mysql.mnp.art.pl z dwustopniowym uwierzytelnieniem; klient powinien być dostępny wyłącznie w ramach połączenia szyfrowanego SSL; powinna istnieć możliwość zarządzania bazami danych oraz użytkownikami z tego samego panelu zarządzania co usługa www po uprzednim zalogowaniu się do sieci VPN;
    e. Wykonywanie kopii bezpieczeństwa na zewnętrzny serwer (np. za pomocą programu rsync) powinno odbywać się w sposób automatyczny co najmniej raz na dobę.

7. Usługa FTP.

a. W celu zapewnienia kompatybilności z dotychczasowymi zasobami MNP powinien być zainstalowany w oparciu o Centos 7 Linux;
b. Za pośrednictwem protokołu FTP dostęp do plików powinien być realizowany tylko w ramach sieci wewnętrznej MNP; Dla połączeń zewnętrznych dostęp będzie za pomocą protokołu SFTP.
c. Oprócz polityki bezpieczeństwa opisanej w punkcie C.2 powinna być realizowana analiza logów serwera w poszukiwaniu nieudanych prób logowania wraz z aktywną czasową blokadą;

8. Usługa chmura plików.
    a. W celu zapewnienia kompatybilności z dotychczasowymi zasobami serwer powinien być zainstalowany w oparciu o Centos 7 Linux; z tego powodu zaleca się również stosowanie rozwiązania NextCloud;
    b. Chmura plików powinna być dostępna z poziomu przeglądarki internetowej oraz aplikacji klienckiej;
    c. Domyślny protokół komunikacji dla aplikacji webowej – https;
    d. Możliwość przesyłania dużych plików do 1GB;

9. Relokacja dotychczasowych portali internetowych.
    a. Do serwera www należy przenieść następujące portale internetowe:
        i. mnp.art.pl;
        ii. monet.mnp.art.pl;
        iii. msu.mnp.art.pl;
        iv. rogalin.mnp.art.pl;
        v. bip.mnp.art.pl;
        vi. lenica.mnp.art.pl;
    b. Wszystkie portale należy wdrożyć w technice SSL (https);
    c. Należy przewidzieć konieczność modyfikacji portali w celu współpracy z aktualnymi komponentami serwera www;

10. Centralna archiwizacja serwera sprzętowego.
    a. Serwer sprzętowy powinien posiadać oprogramowanie archiwizacyjne pozwalające odtworzyć oprogramowanie serwera łącznie z systemem operacyjnym i jego konfiguracją;
    b. Powinna być możliwość wykonywania kopii pełnych, przyrostowych oraz różnicowych;
    c. Powinna być możliwość wykonywania kopii minimum na serwerze zewnętrznym, w bibliotece taśmowej, oraz w chmurze plików;
    d. Administrator powinien posiadać możliwość konfigurowania minimum zakresu konfiguracji, terminów, docelowej lokalizacji oraz automatyzacji procesu;
    e. Administrator powinien mieć możliwość konfigurowania użytkowników o zróżnicowanych uprawnieniach;

11. Uwagi ogólne:
    a. Wykonawca musi uwzględnić w swojej ofercie niezbędne materiały pomocnicze do prawidłowego montażu i podłączenia urządzeń;

b. Montaż, podłączenie urządzeń oraz dojazd do oddziałów są w gestii wykonawcy;
c. Oferowany sprzęt musi być fabrycznie nowy;
d. Wykonawca podaje w swojej ofercie producenta, typ oraz model wyżej wymienionego sprzętu oraz oprogramowania;
e. Wykonawca załącza karty katalogowe producenta potwierdzające parametry wyżej wymienionego sprzętu oraz oprogramowania; dopuszcza się wydruki ze strony internetowej producenta, na której widoczny jest link do jego strony; dopuszcza się karty katalogowe w języku polskim, angielskim, niemieckim i francuskim
f. Zamawiający zaznacza jednocześnie, że użyte w opisie przedmiotu zamówienia sformułowania z zakresu informatyki i elektroniki nie wskazują na konkretnego producenta urządzeń. Sformułowania te (np. „moc RMS", „wyjście do monitora VGA", „wejścia na złączach mini Jack i RCA") oznaczają jedynie powszechnie przyjęte na gruncie informatyki i elektroniki technologie, wykorzystywane zarówno w procesie produkcji, eksploatacji, jak i w określeniu parametrycznym danych typów urządzeń.