Narodowe Centrum Badań i Rozwoju

Łukasiewicz
Instytut Technik
Innowacyjnych
EMAG

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa sprzętu komputerowego, serwerowego, sieciowego i oprogramowania”
– nr postępowania FH/ 04/ 11/ 22

Przedmiot zamówienia podzielony jest na 9 części. Zamawiający dopuszcza składanie ofert częściowych.

CZĘŚĆ NR 1. – Urządzenia sieciowe

1. Przełącznik brzegowy

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa przeznaczona do montażu w szafie Rack 19” (dostawa wraz z elementami mocującymi) Wysokość – maksymalnie 1U
Interfejsy sieciowe	Przełącznik musi być wyposażony w następujące porty: – co najmniej 12 portów 1/10 Gb/s SFP+ Ethernet – co najmniej 4 porty 1/10 Gb/s RJ45 Ethernet (1/10Base-T)
Kontrolki portów	Dla każdego portu kontrolka LED o statusach: speed/link/activity
Interfejs zarzadzania	Przełącznik musi być wyposażony w szeregowy port konsolowy do zarządzania RJ45, Ethernet In/Out Band
Zasilacz	Minimum jeden zasilacz AC/DC, przystosowany do zasilania z sieci 230V/50Hz.
Przepustowość non-blocking	Minimum 160 Gb/s
Zdolność przełączania	Minimum 320 Gb/s
Zgodność ze standardami	Certyfikaty CE, FCC, IC
Odporność na wibracje	Zgodnie z normą ETSI300-019-1.4
Temperatura pracy	Co najmniej od -5 do 40°C
Pobór mocy (maksymalny)	Nie więcej niż 40 W
Liczba sztuk	Zamawiający wymaga dostarczenia 1 sztuki przełącznika brzegowego.

Narodowe Centrum Badań i Rozwoju

2. Przełącznik dystrybucyjny

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa możliwa do montażu w szafie Rack 19” (dostawa wraz z elementami mocującymi) Wysokość – maksymalnie 1U
Interfejsy sieciowe	Przełącznik musi być wyposażony w następujące porty: – co najmniej 48 portów 1 Gb/s RJ45 Ethernet (Base-T) PoE 30W – co najmniej 4 porty 10 Gb/s SFP+ Ethernet
Budżet mocy PoE	375W
Interfejs zarzadzania	Przełącznik musi umożliwiać zdalne zarządzanie i współpracować z oprogramowaniem zarządzającym w chmurze.
Architektura	Przełącznik musi posiadać architekturę umożliwiającą przełączanie w warstwie 2 Ethernet i 3 IPv4 oraz IPv6.
Przepustowość	Minimum 130 Gb/s
Zdolność przełączania	Minimum 175 Gb/s
Rozmiar bufora pakietów	Co najmniej 1,5 MB
Rozmiar tablicy adresów sieciowych MAC	Co najmniej 16.000 wpisów
Pamięć wewnętrzna	– Flash – 32 MB – RAM – 512 MB
Zgodność ze standardami	Certyfikaty CE, FCC, BSMI EMC
Temperatura pracy	Co najmniej od 0 do 50°C
Pobór mocy (maksymalny)	Nie więcej niż 500 W
Głośność	Maksymalnie 29 dB(A) przy pracy w temperaturze 25°C
Liczba sztuk	Zamawiający wymaga dostarczenia 1 sztuki przełącznika dystrybucyjnego.

3. Urządzenie UTM

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa możliwa do montażu w szafie Rack 19” (dostawa wraz z elementami mocującymi) Wysokość – maksymalnie 1U
Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w

	skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły 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 – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie:	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: – 5 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps. 5. 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 1 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.
Funkcje Systemu Bezpieczeństwa:	W ramach systemu ochrony są 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.

	5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 25 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: 3. Translację jeden do jeden oraz jeden do wielu. 4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 5. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 6. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 7. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 8. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 9. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu: – Amazon Web Services (AWS). – Microsoft Azure. – Cisco ACI. – Google Cloud Platform (GCP). – OpenStack. – VMware NSX. – Kubernetes.
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: – Wsparcie dla IKE v1 oraz v2. – Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). – Obsługa protokołu Diffie-Hellman grup 19, 20. – Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. – 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.

	– Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. – Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. – Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. – Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. – Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: – Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. – Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. – Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.

	5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 10000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia 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). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 4000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.

	4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia 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. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie

	komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Certyfikaty	Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje: – ICSA lub EAL4 dla funkcji Firewall.
Uwierzytelnianie	Konieczne jest dostarczenie licencji umożliwiającej dwuskładnikowe uwierzytelnienie przez aplikację na urządzeniu mobilnym dla 25 użytkowników co najmniej przez okres trwania gwarancji.
Gwarancja oraz wsparcie	Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Rozszerzone wsparcie serwisowe AHB/SOS	1. System ma być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący ma posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe mają być przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. 2. System ma 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 60 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący ma posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. 3. System ma być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie, dostarczenie oraz instalację sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący ma posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe maja być przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. 4. System ma być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie, dostarczenie oraz instalację sprzętu zastępczego na czas naprawy

	sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący ma posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe mają być przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. 5. System ma być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy. System ma być objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: – Wsparcie telefoniczne zespołu certyfikowanych inżynierów. – Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. – Doradztwo w zakresie konfiguracji. – Zdalne wsparcie techniczne. – Pomoc w zakładaniu zgłoszeń serwisowych u producenta. – Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). – Przygotowanie urządzenia do zdalnej konfiguracji. – Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. – Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. – Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. – Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.
Opisy do wymagań ogólnych	1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), przed podpisaniem umowy należy dostarczyć 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. 2. Przed podpisaniem umowy należy dostarczyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.
Liczba sztuk	Zamawiający wymaga dostarczenia 1 sztuki urządzenia UTM.

Narodowe Centrum Badań i Rozwoju

4. Firewall

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa przeznaczona do montażu w szafie Rack 19” (dostawa wraz z elementami mocującymi) Wysokość – maksymalnie 1U
Zastosowanie	Firewall z funkcją routera L3 i routera IPsec VPN
Interfejsy sieciowe	Firewall musi być wyposażony w następujące porty: – co najmniej 8 przełączalnych portów 1 Gb/s RJ45 Ethernet (Base-T) – co najmniej 2 porty 10 Gb/s SFP+ Ethernet
Interfejs zarządzania	1 port mini-USB dla konsoli
Porty USB	min. 3 porty USB, z czego co najmniej jeden USB 3.0
Przepustowość	dla firewalla – 9 Gb/s dla routera L3 – 18 Gb/s dla routera IPsec VPN – 1,5 Gb/s
Pamięć RAM	8 GB DDR4 (zainstalowana)
Pamięć masowa	32 GB dysk eMMC (wbudowany)
Zgodność ze standardami	Certyfikaty CE, FCC, RoHS
Temperatura pracy	Co najmniej od 0 do 40°C
Liczba sztuk	Zamawiający wymaga dostarczenia 1 sztuki firewalla.

CZĘŚĆ NR 2. – Serwer NAS

Parametr	Charakterystyka (wymagania minimalne)
Sprzęt	
Procesor	Architektura 64 bit
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 4GB DDR4
Pamięć RAM liczba slotów	Minimum 1 slot
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 16GB

Pamięć Flash	Nie mniej niż 512MB
Liczba zatok na dyski twarde	Minimum 8
Obsługiwane dyski twarde	3.5" oraz 2.5" – SATA
Max. pojemność dysków twardych	Co najmniej do 18TB
Możliwości rozszerzeń	Możliwość podłączenia co najmniej dwóch modułów rozszerzających.
Porty LAN	Minimum 2 x 2,5 Gb/s lub 4 x 1 Gb/s
Porty LAN 10 Gb/s	Minimum 2 na złączu SFP+
Diody LED	Minimum: Status, LAN, HDD.
Porty USB 3.2	Minimum 4
Port PCiE	Minimum 1 port PCiE umożliwiający rozbudowę urządzenia o dodatkowe karty rozszerzeń.
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 2U
Dopuszczalna temperatura pracy	Co najmniej od 0 do 40˚C
Wilgotność względna podczas pracy	Co najmniej 5-95% R.H.
Zasilanie	Zasilacz 250 W, 100-240 V
Oprogramowanie	
Agregacja łączy	Możliwość agregacji łączy
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Możliwość podłączenia karty WLAN na USB	Możliwość podłączenia karty WLAN na USB
Szyfrowanie wolumenów	Możliwość szyfrowania wolumenów, min AES 256
Szyfrowanie dysków zewnętrznych	Możliwość szyfrowania dysków zewnętrznych

Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, 50, 60, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek woluminów i LUN blokowych Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUN na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring i zarządzanie urządzeniem Synchronizacja plików Obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP OpenVPN

Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Ustawienia: Back up, przywracania, resetowania systemu
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem oraz blokowanie na podstawie Geolokalizacji Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Możliwość pobrania oprogramowania ze sklepu z aplikacjami; możliwość instalacji z paczek
Zainstalowane dyski	4 dyski 3,5” SATA III przeznaczone do pracy w systemie NAS, o pojemności 12TB każdy, 7200 obr./min., cache 256MB
Ogólne	
Gwarancja	Minimum 36 miesięcy
Liczba sztuk	Zamawiający wymaga dostarczenia 1 sztuki serwera NAS.

Narodowe Centrum Badań i Rozwoju

CZĘŚĆ NR 3. – Zasilacze UPS

Parametr	Charakterystyka (wymagania minimalne)
Montaż	
Obudowa	Możliwość montażu w szafie rack (dostawa wraz z akcesoriami do montażu)
Parametry wyjściowe	
Moc wyjściowa	1600W / 2000VA
Topologia	Technologia Double Conversion (On-Line)
Typ przebiegu	Sinusoida
Złącza wyjściowe	4 x IEC 60320 C13
Częstotliwość na wyjściu	50/60Hz +/- 3 Hz (zsynchronizowana z siecią zasilającą)
Napięcia wyjściowe	220 V, 240 V
Czas przełączania	0 s
Układ obejściowy (bypass)	Wewnętrzny bypass (automatyczny i manualny)
Parametry wejściowe	
Złącze wejściowe	IEC 60320 C14
Częstotliwość wejściowa	40-70 Hz (automatyczne wykrywanie)
Zakres napięcia wejściowego w trybie podstawowym przy pełnym obciążeniu	160 – 280 V
Akumulatory i czas podtrzymania	
Typ akumulatora	Bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny
Typowy czas ładowania	5,5 godziny
Minimalny czas podtrzymania przy obciążeniu 100%	50 min
Minimalny czas podtrzymania przy obciążeniu 50%	1h 45 min
Automatyczny test akumulatora	Okresowy autotest akumulatora zapewnia wczesne wykrywanie konieczności wymiany.

Komunikacja i zarządzanie	
Interfejsy	DB-9, RS-232, Smart-Slot, USB
Smart-Slot	Umożliwia dołączenie karty SNMP pozwalającej na połączenie przez złącze RJ45 (TCP/IP, UDP, SNMP-V1, SNMP-V2, SNMP-V3) oraz złącze pozwalające na podłączenie czujników (np. temperatury) / karty ze stykiem bezpotencjałowym (Dry Contact) do zdalnego monitoringu i kontroli.
Panel sterowania	Wielofunkcyjna konsola sterownicza i informacyjna LCD. Tekst i schematy przedstawiające tryby działania, parametry systemu i alarmy.
Alarm dźwiękowy	Alarm przy zasilaniu akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: ciągły sygnał dźwiękowy sygnalizujący przeciążenie
Ochrona przed przepięciami i filtracja	
Klasa energetyczna sprzętu przeciwprzepięciowego	600J
Certyfikaty i zgodność z normami	
Potwierdzenia zgodności	CE, IEC 62040-1-1, IEC 62040-1-2
Oprogramowanie	
Dołączone oprogramowanie	Oprogramowanie umożliwiające łatwe monitorowanie zasilania sieciowego i zarządzanie zasilaczem UPS.
Wspierane systemy	Windows 2000/ XP/ 2003/ Vista/ 2008/ 2012 (32-bit & 64-bit)/ 7 / 8 / 10 (32-bit & 64-bit)
Wyposażenie dodatkowe	
Karta sieciowa	Zainstalowana karta SNMP umożliwiająca zdalne zarządzanie ze złączami Ethernet 10Base-T, Ethernet 100Base-TX, obsługująca protokoły TCP/IP, UDP/IP
Dodatkowa bateria	Dodatkowy moduł bateryjny 6/10kVa do montażu w szafie rack (dostawa wraz z akcesoriami do montażu), z funkcją powiadomienia o rozłączeniu akumulatora, alarmami dźwiękowymi i automatycznym testem
Ogólne	
Gwarancja	Minimum 24 miesiące gwarancji na naprawę lub wymianę
Liczba sztuk	Zamawiający wymaga dostarczenia 2 sztuk zasilaczy UPS.

Narodowe Centrum Badań i Rozwoju

CZĘŚĆ NR 4. – Terminale

1. Komputer stacjonarny

Parametr	Charakterystyka (wymagania minimalne)
Typ	Komputer stacjonarny (w ofercie wymagane jest podanie modelu, symbolu oraz producenta)
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 14100
Pamięć RAM	8GB DDR4 non-ECC możliwość rozbudowy do min 64GB, min. 1 slot wolny
Pamięć masowa	256GB M.2 NVMe PCIex4
Napęd optyczny	Nagrywarka DVD +/-RW o prędkości min. 8x
Wydajność grafiki	Zintegrowana karta graficzna
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, port audio combo (słuchawki + mikrofon)na panelu przednim, na tylnym audio out
Obudowa	Typu SFF z obsługą kart rozszerzeń o niskim profilu, napęd optyczny w dedykowanej wnęce zewnętrznej slim. Suma wymiarów mierzona po krawędziach obudowy nie może przekraczać 678 mm, waga max 6kg, Zasilacz o mocy max. 180W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 81% przy obciążeniu zasilacza na poziomie 100%, Wbudowany w zasilaczu system diagnostyczny do sprawdzenia zasilacza bez konieczności włączania komputera, zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx Dołączone oświadczenie producenta komputera iż wskazane zasilacze przez wykonawcę spełniają 80plus. Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED np. przycisku POWER [tzn. barw i miganie] W szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię procesora.

	Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wnęk zewnętrznych oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Zgodność z systemem operacyjnym	Potwierdzenie kompatybilności komputera na daną platformę systemową Zamawiający zastrzega sobie dostarczenia wyżej wymienionego dokument na wezwanie.
Bezpieczeństwo	Ukryty w laminacie płyty głównej dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. Działający w pełni, bez okrojonych funkcjonalności nawet w przypadku uszkodzonego dysku, braku dysku lub sformatowanym dysku, dostępu do sieci i internetu oraz bez konieczności podłączenia urządzeń wewnętrznych i zewnętrznych oraz bez konieczności pobierania i instalowania np. na ukrytej pamięci flash BIOS
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, nazwę producenta komputera, model komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych oraz dodatkowego oprogramowania typu system diagnostyczny odczytania z wewnętrznego menu BIOS informacji o: wersji BIOS, nr seryjnym komputera, dacie wyprodukowania komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, obecnej, minimalnej i maksymalnej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, MAC adresie zintegrowanej karty sieciowej, Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.

	Możliwość ustawienia hasła systemowego/użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym haśle administratora. Możliwość wyłączania portów USB w tym: – tylko portów USB znajdujących się na przednim panelu obudowy, – tylko portów USB znajdujących się na tylnym panelu obudowy. – wszystkich portów USB – pojedynczo
Certyfikaty i standardy	Certyfikat ISO9001 dla producenta sprzętu. Deklaracja zgodności CE. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia 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 Komputer musi spełniać wymogi normy Energy Star potwierdzony oświadczeniem przez producenta.
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 22 dB potwierdzony oświadczeniem przez producenta
Wsparcie techniczne producenta	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera.
System Operacyjny	Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny musi być zapisany trwale w BIOS.
Porty I/O	Wbudowane porty: – panel przedni : 2x USB 3.2 gen 1, 2x USB 2.0, 1x audio (dopuszcza się combo), – panel tylny: 1x audio out, 2x USB 3.2 gen 1, 2x USB 2.0, 1x DP 1.4, 1x HDMI 1.4b, 1x RJ45

	– karta WiFi zamontowana w złączu miniPCIe na płycie głównej, Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w: – 1x PCI Express x16, 1x PCI Express x1, – min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, – min. 2 złącza SATA w tym 1 szt. SATA 3.0, 1 złącze M.2 dla dysków SSD, 1 złącze M.2 dla bezprzewodowej karty WiFi
Wymagania dodatkowe	Klawiatura USB w układzie polski programisty Mysz USB z klawiszami oraz rolką (scroll) Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
Dodatkowe oprogramowanie	Dołączone do oferowanego komputera oprogramowanie z nieograniczoną licencją czasowo na użytkowanie umożliwiające: – upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, – możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: a) o poprawkach i usprawnieniach dotyczących aktualizacji b) dacie wydania ostatniej aktualizacji c) priorytecie aktualizacji d) zgodność z systemami operacyjnymi e) jakiego komponentu sprzętu dotyczy aktualizacja f) wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. – wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne – możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. – rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) – sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) – dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml – raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z

	dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
Gwarancja	Minimum 36 miesięcy gwarancji producenta świadczonej na miejscu u klienta. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera . Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego
Liczba sztuk	Zamawiający wymaga dostarczenia 5 sztuk.

2. Monitor

Parametr	Charakterystyka (wymagania minimalne)
Przeznaczenie	Monitor przeznaczony do współpracy z komputerami stacjonarnymi opisanymi w poprzedniej pozycji (należy dostarczyć wszelkie wymagane akcesoria umożliwiające podłączenie).
Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą min. 23,8” (16:9)
Technologia wykonania matrycy	IPS
Rozmiar plamki	Maksymalnie 0,275mm
Jasność	250 cd/m^2
Kontrast	Typowy 1000:1
Kąty widzenia (pion/poziom)	178/178 stopni
Czas reakcji matrycy	max. 8 ms
Rozdzielczość maksymalna	1920 x 1080 przy 60Hz
Paleta kolorów	83% (CIE 1976)
Głębia kolorów	16,7 miliona kolorów
Zużycie energii	Maks. 30W W trybie uśpienia maks. 0,3W
Powłoka powierzchni ekranu	Antyodblaskowa utwardzona

Podświetlenie	System podświetlenia LED
Bezpieczeństwo	Monitor musi być wyposażony w tzw. gniazdo zabezpieczenia przed kradzieżą. Wbudowane w monitor narzędzie diagnostyczne umożliwiające zdiagnozowanie problemu wyświetlania obrazu na ekranie.
Waga bez podstawy	Maksymalnie 3,3 kg
Pochylenie monitora	W zakresie min. 26 stopni
Kolor obudowy	Czarny
Złącza	1x D-Sub, 1x Display Port 1.2
Certyfikaty	TCO Certified Displays, Energy Star
Inne	Zdejmowana podstawa oraz otwory montażowe w obudowie VESA 100mm.
Gwarancja	Minimum 12 miesięcy, możliwość zgłaszania awarii przez ogólnopolską linię telefoniczną i stronę internetową producenta Czas reakcji serwisu – do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta.
Liczba sztuk	Zamawiający wymaga dostarczenia 5 sztuk monitorów.

Narodowe Centrum Badań i Rozwoju

CZĘŚĆ NR 5. – Szafa serwerowa i okablowanie

1. Szafa serwerowa (krosownicza)

Parametr	Charakterystyka (wymagania minimalne)
Rodzaj	Szafa serwerowa (krosownicza) typu Rack 19”, stojąca, 42U
Obudowa	Czarna, drzwi przednie i tylne z perforacją, zdejmowane panele boczne Klasa szczelności IP20
Wymiary	Głębokość: 1000 mm (głębokość montażowa – 860 mm) Szerokość: 800 mm
Udźwig maksymalny	800 kg
Zgodność ze standardami	– ANSI/EIA RS-310-D – DIN 41491/PART 1 – DIN 41494/PART 7 – ETSI – IEC297-2:1982
Wyposażenie	– panel wentylacyjny z 4 wentylatorami (230 V) – 2 pionowe szyny montażowe z pełną regulacją głębokości – 2 pionowe organizatory kabli – kółka z hamulcem – nóżki – śruby M6 – zamek przedni – zamek tylny – zamki boczne
Wyposażenie dodatkowe	– 4 poziome organizatory kabli o wysokości 1U – 2 Dwie listwy zasilające 230 V o wysokości 1U
Liczba sztuk	Zamawiający wymaga dostarczenia 1 sztuki szafy serwerowej (krosowniczej).

2. Okablowanie

Parametr	Charakterystyka (wymagania minimalne)
Kable światłowodowe	12 szt. kabli światłowodowych SFP+/SFP+, 10 Gb/s długość: 3 m
Moduły do konwersji sygnału	6 szt. modułów SFP+ / 10Base-T (RJ45 10Gb/s)

	Zasięg transmisji UTP/STP – 30 m Zasilanie – 3.3V Zgodność ze standardami – MSA Compliant Temperatura pracy – co najmniej 0°C do 70°C Waga – maksymalnie 20 g
Kable UTP, kat. 6.	20 szt. kabli UTP, kat. 6. w dwóch kolorach (po 10 szt. w każdym z kolorów) długość: 20 m
Kable krosujące UTP, kat. 6.	60 szt. kabli krosujących (podatnych) UTP, kat. 6. do użycia w szafie Rack w trzech kolorach: – 30 szt. żółtych – 20 szt. zielonych – 10 szt. czerwonych długość: 0,5 m
Kable krosujące UTP, kat. 6.	40 szt. kabli krosujących (podatnych) UTP, kat. 6. do użycia w szafie Rack w trzech kolorach: – 10 szt. żółtych – 20 szt. zielonych – 10 szt. czerwonych długość: 0,25 m

Narodowe Centrum Badań i Rozwoju

CZĘŚĆ NR 6. – Konsole KVM

1. Konsola KVM z lokalnym monitorem

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa możliwa do montażu w szafie Rack 19” (dostawa wraz z elementami mocującymi) Wysokość – maksymalnie 1U
Komponenty	Konsola musi posiadać składany monitor TFT-LCD o przekątnej min. 17” oraz dedykowaną klawiaturę.
Wyposażenie dodatkowe	6 przewodów KVM (SHPD+USB), 1,8 m
Interfejsy	Konsola musi być wyposażona w następujące porty: – 1 x SPHD-18 – port zewnętrzny konsoli – 8 x SPHD-17 – porty KVM – 1 x DB-25 – porty połączenia łańcuchowego – 1 x RJ-11 – port do aktualizacji oprogramowania układowego – 1 x RJ-45 – 2 x USB
Liczba obsługiwanych komputerów	– 8 bezpośrednio – do 128 podłączonych szeregowo (daisy-chain)
Rozdzielczość wideo	– 1280 x 1024 przy częstotliwości 75 Hz lokalnie – 1920 x 1200 przy częstotliwości 60Hz dla sesji zdalnych
Dodatkowe funkcje	– hot pluggable - możliwość dodawania i usuwania komputerów bez wyłączania przełącznika – wygodny wybór komputera za pomocą przycisków na przednim panelu, skrótów klawiszowych i wielojęzycznych menu ekranowych (OSD) – do 32 jednoczesnych zalogowań – zabezpieczona transmisja z klawiatury/myszy/wideo poprzez szyfrowanie 128-bitowe RC4 – obsługa szyfrowania danych TLS 1.2 i 2048-bitowych certyfikatów RSA do bezpiecznego logowania użytkownika do przeglądarki – dwupoziomowe zabezpieczenie hasłem – tylko autoryzowani użytkownicy mogą przeglądać i kontrolować komputery – do 64 kont użytkowników z osobnymi profilami dla każdego z nich
Temperatura pracy	Co najmniej od 0 do 50°C
Liczba sztuk	Zamawiający wymaga dostarczenia 1 sztuki konsoli KVM z monitorem.

Narodowe Centrum Badań i Rozwoju

2. Przełącznik KVM

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa możliwa do montażu w szafie Rack 19” (dostawa wraz z elementami mocującymi) Wysokość – maksymalnie 1U
Wyposażenie dodatkowe	6 przewodów KVM (SHPD+USB), 1,8 m
Interfejsy	Przełącznik musi być wyposażony w następujące porty: – 1 x SPHD-18 – port zewnętrzny konsoli – 8 x SPHD-17 – porty KVM – 1 x DB-25 – porty połączenia łańcuchowego – 1 x RJ-11 – port do aktualizacji oprogramowania układowego – 1 x RJ-45 – 1 x USB
Liczba obsługiwanych komputerów	– 8 bezpośrednio – do 128 podłączonych szeregowo (daisy-chain)
Rozdzielczość wideo	– 2048 x 1536 lokalnie – 1600 x 1200 przy częstotliwości 60Hz dla sesji zdalnych
Kompatybilność	Przełącznik musi współpracować z konsolą KVM z poprzedniego punktu.
Temperatura pracy	Co najmniej od 0 do 50°C
Liczba sztuk	Zamawiający wymaga dostarczenia 1 sztuki przełącznika KVM.

Narodowe Centrum Badań i Rozwoju

CZĘŚĆ NR 7. – Oprogramowanie - Serwerowy system operacyjny

Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

Licencja bezterminowa na 16 rdzeni procesorowych w serwerze.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Graficzny interfejs użytkownika.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
21. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
22. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        i. Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
    c. Zdalna dystrybucja oprogramowania na stacje robocze.
    d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        i. Dystrybucję certyfikatów poprzez http
        ii. Konsolidację CA dla wielu lasów domeny,
        iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
    f. Szyfrowanie plików i folderów.
    g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
    h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
    i. Serwis udostępniania stron WWW.
    j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
    k. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
    l. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
iii. Obsługi 4-KB sektorów dysków
iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model)

23. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
24. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
25. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
26. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji
27. Najnowsza wersja dostępna na dzień składania oferty
28. Możliwość zmiany wersji systemu operacyjnego na niższą (downgrade rights) o min. 1 wersję z zachowaniem wsparcia technicznego.

Zamawiający wymaga dostarczenia 3 licencji dla instytucji edukacyjnych/akademickich spełniających ww. wymagania.

Dodatkowo należy dostarczyć odpowiednie licencje dostępowe dla 12 użytkowników, jeśli system operacyjny tego wymaga.

CZĘŚĆ NR 8. – Oprogramowanie - Oprogramowanie do wirtualizacji

Cechy oprogramowania (wymagania minimalne):

1. Warstwa wirtualizacji oprogramowania powinna umożliwiać instalację bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2. Rozwiązanie musi zapewnić wymóg obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Wymagany jest wymóg przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna.
3. Oprogramowanie do wirtualizacji musi zapewnić wymóg skonfigurowania maszyn wirtualnych z możliwością dostępu do min. 4TB pamięci operacyjnej.
4. Oprogramowanie do wirtualizacji musi zapewnić wymóg przydzielenia maszynom wirtualnym do 64 procesorów wirtualnych.
5. Licencja dostarczonego oprogramowania powinna umożliwiać działanie na minimum trzech serwerach fizycznych.
6. Oprogramowanie do wirtualizacji zapewniać powinno możliwość skonfigurowania maszyn wirtualnych.
7. Oprogramowanie do wirtualizacji zapewniać powinno możliwość stworzenia dysku maszyny wirtualnej.

8. Rozwiązanie powinno umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
9. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
10. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna ma mieć możliwość działania na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna.
11. Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH. z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.
12. Rozwiązanie musi umożliwiać składowanie logów ze wszystkich serwerów fizycznych i konsoli zarządzającej.
13. Oprogramowanie do wirtualizacji powinno zapewniać możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
14. Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni.
15. Rozwiązanie powinno zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
16. Oprogramowanie do wirtualizacji musi zapewnić wymóg klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
17. Rozwiązanie powinno mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.

Zamawiający wymaga dostarczenia licencji na 3 serwery fizyczne (hosty).

CZĘŚĆ NR 9. – Oprogramowanie - Oprogramowanie do backupu

Cechy oprogramowania:

1. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie:
   - minimalna liczba referencji 150,
   - minimalna ocena z referencji 4,5,
2. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
3. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
4. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.

Narodowe Centrum Badań i Rozwoju

5. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
6. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
7. Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
8. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
9. 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
10. 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.
11. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
12. Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
13. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
14. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
15. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
16. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
17. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
18. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
19. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
20. 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
21. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
22. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
23. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
24. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
25. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
26. Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru

27. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
28. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage.
29. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
30. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
31. Oprogramowanie musi posiadać wsparcie dla NDMP
32. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
33. Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
34. Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
35. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
36. Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)
37. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
38. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
39. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
40. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
41. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
42. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
43. Oprogramowanie musi umożliwiać jednoczesne 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 dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
44. Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
45. 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 taką migrację swoimi mechanizmami

46. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
47. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
48. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
49. 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
50. 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.
51. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
    a) Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
    b) BSD: UFS, UFS2
    c) Solaris: ZFS, UFS
    d) Mac: HFS, HFS+
    e) Windows: NTFS, FAT, FAT32, ReFS
    f) Novell OES: NSS
52. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
53. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
54. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
55. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
56. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
57. Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
58. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
59. Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
60. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
61. Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
62. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
63. Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
64. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
65. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA
66. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
67. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.

Narodowe Centrum Badań i Rozwoju

68. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
69. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
70. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
71. Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
72. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Zamawiający wymaga dostarczenia licencji na minimum 3 lata w postaci subskrypcji na minimum 10 maszyn wirtualnych.