Załącznik nr 9 do SWZ

Spis treści

1. UTM

UTM	Ilość	1 kpl.
Wymagane minimalne parametry techniczne		
OBSŁUGA SIECI 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. ZAPORA KORPORACYJNA (Firewall) 2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). INTRUSION PREVENTION SYSTEM (IPS) 12. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 13. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 14. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 15. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 16. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 17. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 18. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 19. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 20. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). KSZTAŁTOWANIE PASMA (Traffic Shapping) 21. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną		

wartość pasma.
22. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
23. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
24. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

25. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
26. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
27. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
28. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

OCHRONA ANTYSPAM

29. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
30. Ochrona antyspam ma działać w oparciu o:
    a. białe/czarne listy,
    b. DNS RBL,
    c. Skaner heurystyczny.
31. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
32. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

33. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
34. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
    a. PPTP VPN,
    b. IPSec VPN,
    c. SSL VPN.
35. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
36. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
37. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
38. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
39. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

40. Urządzenie ma posiadać wbudowany filtr URL.
41. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
42. Administrator ma mieć możliwość dodawania własnych kategorii URL.
43. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
    a. blokowanie dostępu do adresu URL,
    b. zezwolenie na dostęp do adresu URL,
    c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

44. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
45. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
46. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
47. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
48. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

UWIERZYTELNIANIE

49. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
    a. lokalną bazę użytkowników (wewnętrzny LDAP),
    b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
    c. usługę katalogową Microsoft Active Directory.
50. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
51. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
    a. SSL,
    b. Radius,
    c. Kerberos.
52. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
53. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
54. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

55. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
56. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
    a. równoważenie względem adresu źródłowego,
    b. równoważenie względem połączenia.
57. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
58. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
59. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
60. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
61. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

62. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
63. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
64. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
65. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

66. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
67. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
68. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
69. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

70. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
71. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
72. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
73. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.
74. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
75. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
76. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
    a. manualnego eksportu do pliku w dowolnym momencie czasu,
    b. automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
77. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
78. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

RAPORTOWANIE

79. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
80. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
81. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
82. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
83. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
84. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
85. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
86. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

87. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
88. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
89. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
90. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
91. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny.
92. Urządzenie ma posiadać usługę DNS Proxy.
93. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
94. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

GWARANCJA I SERWIS

95. Urządzenie ma być objęte 36-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
96. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
97. Urządzenie ma być objęte gwarancją typu NBD tzn. w przypadku awarii urządzenia wymiana na urządzenie

zastępcze lub wymiana urządzenia na sprawne musi nastąpić na kolejny dzień roboczy od potwierdzenia awarii.

PARAMETRY SPRZĘTOWE

98. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 240 GB.
99. Liczba portów Ethernet 10/100/1000Mbps – min. 8, z możliwością rozszerzenia do 16.
100. Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:
    a. Moduł z 8 interfejsami miedzianymi 10/100/1000Mbps
    b. Moduł z 4 interfejsami miedzianymi 10Gbps
    c. Moduł z 8 interfejsami światłowodowymi 1Gbps
    d. Moduł z 4 interfejsami światłowodowymi 10Gbps
101. Zamawiający wymaga zainstalowania modułu z 2 interfejsami światłowodowymi 10Gbps wraz z wkładkami SFP+ SR.
102. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
103. Przepustowość Firewall (1518 bajtów UDP) – minimum 15Gbps.
104. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 8Gbps.
105. Przepustowość filtrowania Antywirusowego – minimum 2Gbps.
106. Przepustowość tunelu VPN przy szyfrowaniu AES-GCM – minimum 3Gbps.
107. Maksymalna liczba tuneli VPN IPSec – minimum 1 000.
108. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 150.
109. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 150.
110. Obsługa interfejsów 802.11q (VLAN) – minimum 256.
111. Liczba równoczesnych sesji – minimum 1 000 000 i nie mniej niż 50 000 nowych sesji/sekundę.
112. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
113. Urządzenie nie ma limitu na liczbę użytkowników.
114. Liczba reguł filtrowania – minimum 16 384.
115. Liczba tras statycznego routingu – minimum 2 048.
116. Liczba tras dynamicznego routingu – minimum 10 000.
117. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U.

2. Serwer

Serwer		Ilość	1 szt.
Wymagane minimalne parametry techniczne			
Obudowa	Obudowa Rack o wysokości max 2U. Możliwość instalacji minimum 2 dysków 2.5” oraz 12 dysków 3.5”. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.		
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów 3rd Generacji Intel Xeon. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.		
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych		
Procesor	Zainstalowane dwa procesory min. 8-rdzeniowe klasy x86, min. 2.8GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 131 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.		
RAM	Minimum 128GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.		
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing		

Gniazda PCI	Min. 5 slotów PCIe x16 generacji 4.
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Zainstalowana dodatkowa karta SAS umożliwiająca podłączenie dostarczanej biblioteki taśmowej. Zainstalowana dodatkowa karta posiadająca 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+. Wszystkie sloty SFP+ należy obsadzić kompatybilnymi wkładkami 10GB SR.
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 2 dyski SSD SATA o pojemności min. 480GB, 6Gb, 2,5“ Hot-Plug skonfigurowane w RAID1. Zainstalowane 5 dyski NLSAS o pojemności min. 4TB, 12Gb, 3,5“ Hot-Plug skonfigurowane w RAID5. Zainstalowane 2 dyski M.2 SATA o pojemności min. 240GB Hot-Plug skonfigurowane w RAID1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
Wbudowane porty	4xUSB, w tym min. 1 port USB 3.0 2 porty VGA z czego 1 na panelu przednim Możliwość rozbudowy o Serial Port
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 800W każdy.
Bezpieczeństwo	• Blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);

	• szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Firma serwisująca musi posiadać ISO 9001 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

3. Biblioteka taśmowa

Biblioteka taśmowa		**Ilość**	**1 szt.**
Wymagane minimalne parametry techniczne			
Obudowa	Do zamontowania w szafie rack, maksymalnie 2U.		
Napęd	LTO-7 SAS – 1 sztuka możliwość rozbudowy o drugi napęd. Zamawiający wymaga dostarczenia kabla do podłączenia z serwerem.		
Liczba slotów	Minimum 24 kieszenie na taśmy (urządzenie powinno być dostarczone z kompletem		

	magazynków). Jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów i magazynków zainstalowanych w urządzeniu. Wymagana ilość mail slot (I/E): min. 1. Wymiana taśm przez MailSlot powinna odbywać się bez konieczności wysuwania całego magazynka.
Pojemność	Wymagana pojemność bez kompresji – minimum 288 TB
Wyposażenie	Urządzenie musi być wyposażone w czytnik kodów kreskowych, kabel zasilający i sieciowy oraz kabel koniecznego do podłączenia do odpowiedniego kontrolera serwera (długość kabla min. 1m) umożliwiającego komunikację z urządzeniem oraz wszystkimi zainstalowanymi napędami. Wraz z urządzeniem należy dostarczyć także zestaw nośników danych o pojemności bez kompresji minimum 6TB każdy w ilości 15 szt. wraz z 1 nośnikiem czyszczącym, przy czym wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem oraz wyposażone w naklejki z kodami kreskowymi.
Gwarancja i oświadczenia	3 lata w miejscu instalacji urządzenia.

4. Przełącznik

Przełącznik		Ilość	1 kpl.
Wymagane minimalne parametry techniczne			
1.	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.		
2.	Wymagane parametry fizyczne: a) możliwość montażu w stelażu/szafie 19” b) wysokość maksymalna 6U c) minimum dwa wewnętrzne redundantne zasilacze 230V AC typu hot-swap (nie dopuszcza się rozwiązania zewnętrznego). Każde urządzenie musi zostać dostarczone z 2 zasilaczami umożliwiające wymianę w trakcie pracy urządzenia (ang. hot-swap). d) zakres temperatur pracy ciągłej co najmniej od -5 do +45 °C e) zakres wilgotności pracy co najmniej 10% - 95% f) port USB umożliwiający podłączenie zewnętrznej pamięci flash g) MTBF: minimum 300 000 godzin h) waga urządzenia nie większa niż 25kg		
3.	Urządzenie musi być wyposażone w 4 wentylatory z możliwością wymiany pojedynczego wentylatora lub całego modułu wentylatorów w trakcie pracy urządzenia (ang. hot-swap).		
4.	Przełącznik musi zostać dostarczony z następującymi interfejsami mogącymi działać równocześnie: ● 48 portów 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 10G-ER, 1G-LX, 1G-SX ● 6 portów 40G QSFP+ z obsługą modułów 40G-SR, 40G-LR Wszystkie porty muszą być dostępne od frontu urządzenia. Urządzenie musi umożliwiać w przyszłości zwiększenie przepustowości portów 40G do prędkości 100G poprzez zakup dodatkowej licencji bądź możliwość instalacji dodatkowego modułu z 6 portami 100G. W ramach postępowania Zamawiający nie wymaga dostarczenia niniejszej licencji lub dodatkowego modułu z 6 portami 100G. Zamawiający nie dopuszcza, aby realizacja portów 10G była realizowana poprzez tzw. rozszywanie portów 100G/40G na 4 porty		

	10G. Wszystkie interfejsy 10G, 40G/100G muszą być dostępne z przodu obudowy.
5.	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: a) Zarządzanie stosem poprzez jeden adres IP b) Do min. 2 jednostek w stosie c) Magistrala stackująca o wydajności 160Gb/s d) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation) e) Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree f) Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia. g) Zamawiający dopuszcza, aby możliwość łączenia w stosy była realizowana za pomocą portów typu uplink.
6.	Układ przełączający o wydajności min. 1,68 Tbps, wydajność przełączania przynajmniej 480 Mpps
7.	Obsługa min. 64 000 adresów MAC
8.	Wbudowana pamięć RAM min. 4 GB Procesor wielordzeniowy.
9.	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 2 GB
10.	Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
11.	Możliwość skonfigurowania min. 1000 interfejsów vlan interface SVI działających równocześnie.
12.	Obsługa standardów IEEE: - CFM zgodny z 802.1ag - EFM zgodny z 802.3ah
13.	Obsługa ramek jumbo o wielkości min. 9216 bajtów
14.	Obsługa protokołu GVRP lub VTP
15.	Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP. Wsparcie dla funkcjonalności PVST lub równoważnej z obsługą minimum 128 instancji VLAN.
16.	Obsługa min. 256 000 tras dla routingu IPv4
17.	Obsługa min. 80 000 tras dla routingu IPv6
18.	Obsługa protokołów routingu OSPF, OSPFv3, IS-IS, IS-ISv6, BGPv4, BGPv4+, RIP, RIPng, PIM-SM, PIM-DM i SSM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania
19.	Obsługa min. 256 instancji VPN (VRF)
20.	Obsługa protokołów LLDP i LLDP-MED
21.	Wsparcie dla technologii MPLS, w tym L3 VPN oraz L2 VPN. Jeżeli funkcjonalność MPLS wymaga licencji to należy ją dostarczyć w ramach niniejszego postępowania
22.	Przełącznik musi posiadać funkcjonalność DHCP Server
23.	Obsługa ruchu multicast: ● IGMP v1, v2 i v3 ● IGMP Snooping v1, v2 i v3
24.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: a) min. 4 poziomy dostępu administracyjnego poprzez konsolę b) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL c) możliwość utworzenia minimum 2000 list ACL d) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www

	e) zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6 f) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP g) obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny), h) możliwość synchronizacji czasu zgodnie z NTP i) wsparcie dla RMON, RMON2 j) wsparcie dla protokołu NETCONF
25.	Obsługa funkcjonalności UDLD lub równoważnej
26.	Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach: ● klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP ● wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ
27.	Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA). Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania.
28.	Wymagane opcje zarządzania: a) możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN b) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC) c) dedykowany port konsoli, zgodny ze standardem RS-232 d) dedykowany port zarządzający out-of-band Ethernet 10/100Base-T
29.	Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
30.	Wsparcie dla funkcjonalności VXLAN L2 i L3. Jeżeli obsługa powyżej funkcjonalności wymaga dodatkowej licencji to w ramach niniejszego postępowania Zamawiający nie wymaga jej dostarczenia.
31.	Przełącznik musi mieć możliwość pracy jako kontroler WLAN poprzez instalację dodatkowej licencji bądź modułu rozszerzeń instalowanego w obudowie urządzenia. Możliwość obsługi minimum 200 punktów dostępowych. Jeżeli funkcjonalność kontrolera WLAN wymaga dodatkowej licencji bądź modułu to w ramach niniejszego postępowania Zamawiający nie wymaga ich dostarczenia.
32.	Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski
33.	Wraz z przełącznikiem należy dostarczyć: 12x Wkładka SFP+ 10GB SR 12x Okablowanie OM3 LC-LC o długości min. 5 metrów 1x Karta SFP do serwera backup'u wraz z wkładkami
34.	Zamawiający wymaga, aby przełącznik posiadał 3-letni serwis gwarancyjny, świadczony przez Wykonawcę na bazie wsparcia serwisowego producenta. Wsparcie serwisowe na dostarczone urządzenia musi być

	zarejestrowane u producenta na Zamawiającego. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia.
35.	Urządzenie musi posiadać gwarancję producenta typu Limited Lifetime Warranty.
36.	Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzeń

5. Oprogramowanie backupowe

Oprogramowanie backupowe	Ilość	1 komplet
Wymagane minimalne parametry techniczne		
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,		
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		
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 z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.		
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 pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)		
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 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.		
Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania		
Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.		
Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu		
Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API		
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.
Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru
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 mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
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.
Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwosc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
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 wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
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.
Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
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
Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
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 pojedynczych plików z następujących systemów plików:
- Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs

- BSD: UFS, UFS2
- Solaris: ZFS, UFS
- Mac: HFS, HFS+
- Windows: NTFS, FAT, FAT32, ReFS
- Novell OES: NSS

Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.

Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników 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 nowszych

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA

Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.

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.

Oprogramowanie musi zostać dostarczone w licencjonowaniu wieczystym wraz z trzy letnim wsparciem producenta.

Oprogramowanie musi zostać dostarczone w licencjonowaniu umożlwiającym backup różnego rodzaju obciążeń w tym: maszyny wirtualne (Vmware, Hyper-V), serwery fizyczne (Windows, Linux), workstacje (Windows, Linux, Mac), instancje chmurowe (Azure, AWS, Google Cloud).

Zamawiający wymaga dostarczenie licencji umożliwiających backup 20 maszyn VM.

Minimum 3 lata gwarancji.

6. Serwerowy System Operacyjny

Serwerowy System Operacyjny		Ilość	1 szt.
Wymagane minimalne parametry techniczne			
Licencja musi uprawniać do uruchamiania SSO na dostarczanym serwerze w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.			
Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy.			
1	Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym		
2	Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.		
3	Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.		
4	Posiada 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	Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6	Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7	Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8	Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
9	Wbudowane wsparcie instalacji i pracy na wolumenach, które: • pozwalają na zmianę rozmiaru w czasie pracy systemu, • umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, • umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, • umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10	Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11	Posiada 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	Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13	Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14	Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15	Graficzny interfejs użytkownika.
16	Zlokalizowane w języku polskim, następujące elementy: • menu, • przeglądarka internetowa, • pomoc, • komunikaty systemowe.
17	Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
18	Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
19	Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
20	Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).

21	Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
	• Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	• Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
	  • Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
	  • Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na

	przykład typu certyfikatu użytego do logowania, • Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. • Zdalna dystrybucja oprogramowania na stacje robocze. • Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej • Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: • Dystrybucję certyfikatów poprzez http • Konsolidację CA dla wielu lasów domeny, • Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. • Szyfrowanie plików i folderów. • Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). • Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów. • Serwis udostępniania stron WWW. • Wsparcie dla protokołu IP w wersji 6 (IPv6), • Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtulne 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 zapewniają wsparcie dla: • Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, • Obsługi ramek typu jumbo frames dla maszyn wirtualnych, • Obsługi 4-KB sektorów dysków, • Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, • Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model)
22	Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
23	Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
24	Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
25	Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

7. Bramka SMS

Bramka SMS 4G		**Ilość**	**1 szt.**
Wymagane minimalne parametry techniczne			
Procesor	Minimum 4 rdzenie o taktowaniu 1.2GHz		
Pamięć wewnętrzna	Minimum 4GB		
Obsługiwane Częstotliwości	UMTS 800/850/900/AWS/1900/2100 MHz GSM/GPRS 850/900/1800/1900 MHz		
Interfejsy	1x HDMI, 2x USB, 1xRJ45		

Slot na kartę SIM	Tak
Przepustowość	odbiór wiadomości: do 30 SMS/min wysyłanie wiadomości: do 30 SMS/min
Funkcjonalność	• Wysyłanie, Odbiór SMS (foldery wiadomości: Skrzynka odbiorcza, Skrzynka nadawcza, Elementy wysłane) • Wysyłanie, Odbiór MMS • Wysyłanie SMS do pojedynczych użytkowników lub grup • Wysyłanie wiadomości o konkretnej porze (harmonogram wysyłek) • Ograniczanie wysyłania w określonych godzinach (np. między 08:00-18:00) • Tryb konwersacji w folderach (wiadomości są pogrupowane wg numeru telefonu). Łatwo śledzisz historię komunikacji z danym użytkownikiem • Obsługa różnych typów wiadomości (SMS/SMS wieloczęściowy/Flash SMS/MMS/SMS binarny/kody USSD/WAP Push link) • Szablony wiadomości • Książka adresowa (zarządzanie odbiorcami, grupami odbiorców) • Import odbiorców z pliku CSV • Monitoring usług i serwerów (np serwer WWW, serwer poczty emal) wysyłanie alertów sms i SNMP Traps • Automatyczna odpowiedź na odebrane wiadomości • Przekierowanie Email na SMS • Przekierowanie SMS na Email • Przekierowanie SMS przychodzących do zewnętrznego skryptu (callback URL) • Funkcja czarnej listy do wykluczania numerów • Plugin do Outlooka umożliwiający wysyłanie SMS-ów bezpośrednio z aplikacji • Cyfrowe wejście i wyjście sterowane przez SMS • Uwierzytelnianie wieloskładnikowe (MFA) • Funkcja eskalacji wiadomości • Kopia zapasowa na FTP • Okresowe czyszczenie folderów • Automatyczne tworzenie kopii zapasowych na FTP • Cykliczne wysyłanie SMS w określonych odstępach czasu • Wsparcie dla wielu użytkowników (użytkownicy zarządzają prywatnymi folderami: Skrzynka odbiorcza, Skrzynka nadawcza, Elementy wysłane) • Alerty SMS z czujnika Temperatury i wilgotności • Wsparcie dla Unicode (narodowe zestawy znaków) • Interfejs API do wysyłania i odbioru wiadomości z zewnętrznych programów • Wielojęzyczny (angielski, francuski, hiszpański, niemiecki, polski) interfejs webowy • Klient NTP • Klient SNMP • Wbudowany serwer www • Wbudowana baza danych • Wbudowany serwer email • Nowoczesny responsywny interfejs webowy • Wsparcie dla raportów doręczenia • Obsługa HTTPS • Mechanizm watchdog nadzorujący pracę modemu 4G • Obsługa Failover (możliwość utworzenia klaster HA dla 2 urządzeń) • Szybkość transmisji danych HSPA+ do 21 Mb/s przy pobieraniu i 5,7 Mb/s przy wysyłaniu (z możliwością wyłączenia/wyłączenia)

	• Obsługa zewnętrznych czujników temperatury
Gwarancja	Minimum 3 lata gwarancji

8. Monitoring zasobów krytycznych

Wymagania ogólne

Usługa polega na konfiguracji środowiska do monitorowania krytycznych zasobów infrastruktury IT a w szczególności infrastruktury środowiska HIS. Ma na celu zapobieganie, poprzez informowanie z odpowiednim wyprzedzeniem administratorów szpitala, o potencjalnych problemach oraz zagrożeniach w dostępności usług oraz serwisów (tj. brak miejsca na dysku, brak pamięci operacyjnej, błędy systemów operacyjnych, błędy usług środowiska HIS, brak dostępności do urządzeń sieciowych oraz usług).
Konfiguracja musi obejmować przygotowanie serwera monitorowania, przygotowanie oraz personalizację szablonów, konfigurację powiadomień, szkolenie z obsługi oraz podpięcie co najmniej 15 urządzeń/usług, w tym serwery/usługi środowiska HIS działającego u Zamawiającego. Dodatkowo, jeżeli zakupiona zostanie sprzętowa bramka SMS (oferowania z usługą), zostaną skonfigurowane niezależne powiadomienia SMS o najważniejszych błędach (karta SIM zostanie dostarczona przez Zamawiającego).

Wymagania szczegółowe

Zainstalowane w ramach konfiguracji usługi rozwiązanie musi spełniać następujące minimalne wymagania:

1	umożliwiać monitorowanie systemów operacyjnych, urządzeń sieciowych, łączy internetowych, baz danych, procesów
2	obsługiwać co najmniej systemy operacyjne rodziny Windows i Linux
3	posiadać mechanizmy monitorowania plików logów (plików tekstowych)
4	gromadzić dane w bazie danych i obsługiwać co najmniej MySQL, mariaDB, PostgreSQL,Oracle
5	posiadać prekompilowanych agentów na systemy rodziny Windows oraz Linux
6	umożliwiać weryfikację poprawności pracy agentów monitorowania
7	umożliwiać definiowanie odrębnych parametrów monitorowania oraz wartości progowych dla różnych rodzajów serwerów w zależności od ich konfiguracji i roli.
8	umożliwiać definiowanie grup serwerów w zależności od ich konfiguracji i roli
9	gromadzić i utrzymywać informacje historyczne monitorowanych elementów infrastruktury.
10	udostępniać za pośrednictwem interfejsu graficznego informacje o skonsolidowanym stanie serwerów w czasie rzeczywistym.
11	udostępniać za pośrednictwem interfejsu graficznego informacje o aktualnych listach problemów wymagających reakcji.
13	powiadamiać administratorów o niedostępności monitorowanych serwerów i urządzeń.
14	szyfrować komunikację pomiędzy serwerem monitorowania a agentami
15	mieć możliwość monitoringu zarówno agentowego jak i bezagentowego.
16	realizować dostęp do systemu monitorowania poprzez konta dla upoważnionych użytkowników i chronić je hasłem
17	umożliwiać elastyczne definiowanie widoków dla użytkowników w zależności od ich roli, potrzeb oraz uprawnień.
18	monitorować wydajność i pojemność zasobów sprzętowych serwerów: a) procesory, b) pamięć operacyjna, c) przestrzenie dyskowe, d) interfejsy sieciowe.

19	musi umożliwiać wysyłanie powiadomień o zdarzeniach zarówno przez email jak i SMS
20	musi umożliwiać prezentowanie danych historycznych w postaci wykresów
21	musi posiadać szablony konfiguracyjne zawierające predefiniowane ustawienia monitorowania
22	musi automatycznie wyliczać SLA dla wybranych serwisów
23	musi umożliwiać prezentacje wizualną infrastruktury np. za pomocą map sieci
24	musi umożliwiać budowania własnych szablonów monitorowania
25	musi mieć możliwość dynamicznego dodawania elementów do monitorowania (np. dynamicznie budować listę dysków systemu operacyjnego i dodawać do nich parametry do monitorowania)
26	musi monitorować zadane parametry i na podstawie zadanych granicznych wartości generować odpowiednio ostrzeżenia lub błędy
27	musi obsługiwać SNMP
30	musi monitorować usługi systemu HIS i ERP działającego u Zamawiającego
31	musi monitorować pracę systemu PACS działającego u Zamawiającego
32	musi monitorować bazy danych, co najmniej Oracle, MySQL, PostgreSQL
33	musi monitorować działania bramek HL7, działających u Zamawiającego
35	musi umożliwiać monitorowanie parametrów wydajnościowych systemu HIS działającego u zamawiającego
36	musi być możliwość uruchomienia serwera monitorowania jako maszyny wirtualnej

Wymagania dotyczące instalacji

Instalacja odbędzie się na infrastrukturze wskazanej przez Zamawiającego, spełniającej następujące minimalne wymagania:

- Procesor 6 rdzeniowy (vCPU)
- 16 GB RAM
- 300 GB miejsca na dysku

Zamawiający oczekuje instalacji środowiska w postaci maszyny wirtualnej. Dopuszczone jest zastosowanie oprogramowanie typu Open Source, pod warunkiem możliwości wykupienia wsparcia producenta.

Szkolenia

Wraz z wdrożeniem zostanie przeprowadzone szkolenie do 2 administratorów Zamawiającego z dostarczonego rozwiązania, po którym będą w stanie samodzielnie administrować rozwiązaniem, dodawać nowe usługi/urządzenia do kontrolowania oraz zarządzać otrzymywanymi powiadomieniami. Wykonawca musi również przekazać dokumentację administratora. W zakresie gotowych produktów, dopuszczalna jest dokumentacja w języku angielskim.

Gwarancja

Na dostarczone rozwiązanie, Wykonawca musi zapewnić 12 miesięcznej gwarancji, w ramach której będzie usuwał błędy dostarczonej usługi oraz wykonywał raz na kwartał wymagane aktualizacje. Błędy w działaniu usługi, muszą być usuwane w ciągu 6 dni roboczych.

9. Wykonanie skanów podatności systemów teleinformatycznych

Wykonywanie testów podatności infrastruktury teleinformatycznej uznanymi narzędziami mającymi na celu:

a) wykrycie wszystkich otwartych portów,

b) wyszukanie błędów konfiguracyjnych skutkujących powstaniem podatności,

c) analizę wykrytych słabości oraz oceny ich wpływu na infrastrukturę.

W ramach testów podatności wykonane zostaną następujące czynności:

a) wykonanie skanów otwartych portów w całej adresacji publicznej podmiotu,

b) wykorzystanie dedykowanego oprogramowania do wykrywania podatności zasilonego najnowszą bazą znanych podatności,

c) wykonanie skanów uwierzytelnionych i nieuwierzytelnionych,

d) wykonanie raportu końcowego.

W ramach testów podatności wyłączone ze skanowania będą urządzenia, aplikacje i bazy danych związane z zapewnieniem ciągłości działania podmiotu, urządzenia związane

z ratowaniem życia lub zdrowia i innych kluczowych dla prowadzonej działalności.

Uwzględniając zagrożenia z przeprowadzenia testów podatności podmiot przekaże w terminie 7 dni przed przystąpieniem do realizacji usługi zakresy numerów IP do skanowania.

Zamawiający wyłączy ze skanowania podatności urządzenia służące do gromadzenia danych kopii zapasowych w przypadku stwierdzenia braku bezpiecznych kopii dla tych urządzeniach.

10. Usługi

Usługi	Ilość	1 kpl.
Wymagane minimalne parametry techniczne		
1. Szczegóły dotyczące instalacji i uruchomienia Infrastruktury serwerowej zostaną ustalone w trakcie wdrożenia. 2. Na serwerze zostanie zainstalowane oraz skonfigurowane środowisko wirtualne (zamawiający dostarczy licencję). 3. W zakresie części serwerowej w ramach postępowania wymagane jest wykonanie następujących usług: ➢ Przygotowanie planu instalacji: - Zestawienie dostarczanych urządzeń ➢ Instalacja, montaż i uruchomienie infrastruktury backupowej: - Aktualizacja oprogramowania do najnowszej stabilnej wersji		

- Inicjalne uruchomienie urządzeń
- Uruchomienia oraz skonfigurowania urządzenia UTM wraz z przełącznikiem
- Instalacja oprogramowania wirtualizacyjnego i backupowego
- Konfiguracja oprogramowania wirtualizacyjnego i backupowego
- Aktywacja dostarczonego oprogramowania backupowego

➢ Przygotowanie dokumentacji powykonawczej. Winna zawierać:

- Zestawienie adresacji wdrożonych urządzeń
- Zestawienie danych dostępowych
- Zestawienie nazewnictwa poszczególnych elementów systemu
- Zestawienie wersji zainstalowanego oprogramowania

➢ Zamawiający wymaga przeszkolenia z obsługi dostarczanych urządzeń w ilości 2 godzin.

➢ Zamawiający wymaga przeszkolenia dwóch Administratorów z usług Usługi Active Directory w zakresie:

Omówienie usług AD DS

Omówienie kontrolerów domeny usług AD DS

Wdrożenie kontrolera domeny

Encrypted DNS – szyfrowana usługa rozpoznawania nazw w Windows Server 2022

Zarządzanie kontami użytkowników

Zarządzanie grupami w usługach AD DS

Zarządzanie obiektami typu komputer w AD DS

Wprowadzenie do zaawansowanych wdrożeń AD DS

Wdrożenie rozproszonego środowiska AD DS

Konfiguracja relacji zaufania AD DS.

Omówienie replikacji usług AD DS

Konfigurowanie lokacji usług AD DS

Konfigurowanie i monitorowanie replikacji usług AD DS.

Wprowadzenie do zasad grupy

Wdrażanie i zarządzanie obiektami GPO (Group Policy Object)

Konfiguracja zakresu i przetwarzania obiektów GPO

Rozwiązywanie problemów z GPO

Wdrażanie szablonów administracyjnych

Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów

Konfiguracja preferencji zasad grupowych

Zaoferowane szkolenie może odbywać się w formie online, minimalna długość szkolenia to 2 dni po 8 godzin.

Termin szkolenie zostanie ustalony na etapie wdrożenia.