MINIMALNE WYMAGANIA SPRZĘTU INFORMATYCZNEGO

1. Serwer wraz z oprogramowaniem

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 2U RACK 19 cali wraz z szynami montażowymi.
Procesor	Intel® Xeon® Silver 4310 2.1G, 12C/24T, 10.4GT/s, 18M Cache, Turbo, HT (120W) DDR4-266
Liczba procesorów	1 procesor z możliwością rozszerzenia o drugi procesor w późniejszym czasie
Pamięć operacyjna	64 GB RDIMM 3200MT/s, Dual Rank, 16Gb BASE x8 Płyta główna z minimum 16 slotami na pamięć i umożliwiająca instalację do minimum 1TB.
Sloty rozszerzeń	Serwer musi być wyposażony w: 1 gniazdo na karty o połowie wysokości/długości
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania co najmniej 8 dysków 2,5in typu Hot Swap, zainstalowane 2 dyski 480GB SSD SATA Mix Use 6Gbps 512 2.5in Hot-plug zainstalowane 2 dyski 1.2TB Hard Drive SAS ISE 12Gbps 10k 512n 2.5in Hot-Plug
Kontroler	Serwer wyposażony w zainstalowany sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/5/6/10/50/60 z 8GB pamięci cache z podtrzymywaniem bateryjnym. Kontroler umożliwiający pracę z dyskami odpowiednimi szybkościami transferu zależnie od typu typu: 3 Gbps SATA, 6 Gbps SATA/SAS, 12 Gbps SAS
Interfejsy sieciowe	Serwer musi być wyposażony w: - minimum 2 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.
Karta graficzna	Zintegrowana karta graficzna
Porty	Min 2 x USB 3.0 VGA
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 800W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug

Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera
Element konfiguracji	Wymagania minimalne
	dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend; • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • zdalna aktualizacja oprogramowania (firmware) • wsparcie dla Microsoft Active Directory • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2022. Oferowany serwer musi się znajdować na liście Windows Server Catalog i posiadać certyfikację "Certified for Windows Server 2022"
Wsparcie techniczne	5-letnia gwarancja/wsparcie producenta serwera w miejscu instalacji świadczona z reakcją na miejscu instalacji. Wsparcie techniczne realizowane jest przez organizację serwisową producenta oferowanego serwera. Uszkodzone dyski twarde pozostają własnością Zamawiającego. Obsługa prowadzona w języku polskim.

2. Systemu backup razem z urządzeniami

Wymagania ogólne:

- Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.5 oraz nowszym.
- Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
- Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere.

Wymagania dotyczące architektury

- Rozwiązanie oprócz licencji powinno zawierać niezbędne zaplecze sprzętowe umożliwiające wykonanie kopi 5 maszyn wirtualnych oraz 2 TB danych netto.

- Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
- Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
- Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe.
- 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.
  Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
- Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
- Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia
- Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie
- Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
- Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL (w tym odtwarzanie point-in-time)
- 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 posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Wymagania dotyczące wykonywania kopii zapasowych

- Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
- 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
- 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

- Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej
- Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
- 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 dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere
- Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)
- 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 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
- Oprogramowanie musi wspierać odtwarzanie 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 umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
- Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat

  Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
- Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.

- Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
- Oprogramowanie musi pozwalać na odtworzenie maszyn wirtualnych z macierzowych snapshotów ze wspieranych macierzy.
- Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Wymagania dotyczące monitorowania i raportowania

- System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware bez potrzeby korzystania z narzędzi firm trzecich
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x oraz 7.x – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
- System musi mieć status „VMware Ready" i być przetestowany i certyfikowany przez VMware
- System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
- System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
- System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
- System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
- System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
- System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
- System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
- System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
- System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
- System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 6.x oraz 7.x vCenter Server 6.x oraz 7.x
- System musi być certyfikowany przez VMware i posiadać status „VMware Ready"
- System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi
- System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
- System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
  System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
- System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych

- System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
- System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
- System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
- System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.
- System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
- System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
- System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

3. Router sieciowy z wymaganymi licencjami

Urządzenie typu firewall spełniające następujące funkcjonalności:

1. Musi być dostarczone jako samodzielne, dedykowane fizyczne urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej rozwiązania musi występować moduł zarządzania i moduł przetwarzania danych.
2. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
3. Urządzenie musi być wyposażone w dedykowany port zarządzania out-of-band.
4. Brak ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
5. Urządzenie musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.
6. Obsługa dla IPv6.
7. Funkcjonalność statycznej i dynamicznej translacji adresów NAT między IPv4 i IPv6.
8. Reguły zabezpieczeń firewall muszą być tworzone zgodnie z ustaloną polityką opartą o profile oraz obiekty.
9. Polityka zabezpieczeń firewall musi uwzględniać przynajmniej takie parametry jak: adresy IP źródłowe i docelowe, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie.
10. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.
11. Interfejs administracyjny urządzenia musi być w języku polskim lub angielskim.
12. Firewall musi działać w następujących trybach:
    a. routera (tzn. w warstwie 3 modelu OSI),
    b. przełącznika (w warstwie 2 modelu OSI),
    c. transparentnym
    d. pasywnego nasłuchu.

Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych biorących udział w transmisji.

13. Zarządzanie firewallem musi odbywać się z linii poleceń (CLI) oraz z graficznej konsoli GUI. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Dopuszcza się, aby polityki mogły być tworzone tylko z graficznej konsoli GUI.
14. Musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP, mapowanie 1 adres publiczny na 1 adres prywatny oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
15. Musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenia muszą umożliwiać stworzenie co najmniej 6 klas dla różnego rodzaju ruchu sieciowego.
16. Firewall musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
17. Obsługa protokołu Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.
18. Obsługa protokołów routingu dynamicznego, nie mniej niż RIP, OSPF oraz BGP.
19. Firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
20. Musi posiadać osobny zestaw polityk definiujący ruch zaszyfrowany SSL oraz SSH, który należy poddać lub wykluczyć z operacji deszyfrowania rozdzielny od polityk bezpieczeństwa.
21. Musi posiadać funkcjonalność automatycznego pobierania listy stron WWW lub adresów IP z zewnętrznego systemu oraz używania ich w politykach bezpieczeństwa.
22. Ochrona przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony informującej użytkownika o próbie pobrania pliku i możliwości kontynuowania lub zaniechania pobrania.
23. Urządzenie zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
24. Firewall musi identyfikować co najmniej 2500 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS m.in.: Skype, Tor, BitTorrent, eMule.
25. Możliwość definiowania własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta.
26. System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie wyłącznie na podstawie rozszerzenia.
27. Urządzenie musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Urządzenie musi umożliwiać konfigurację tuneli VPN w trybie route-based VPN.
28. Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN oraz IPSec.

29. Firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną).
30. Producent urządzenia musi udostępniać dedykowanego klienta binarnego VPN przynajmniej dla platform Windows i Mac
31. Urządzenie musi transparentnie ustalać tożsamość użytkowników sieci w oparciu o Active Directory oraz Ms Exchange. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym Citrix oraz Windows Terminal Services, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
32. Musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach.
33. Urządzenie musi obsługiwać nie mniej niż 3 wirtualne routery posiadające odrębne tabele routingu.
34. Rozwiązanie musi możliwość wykrywanie domen DGA i ruchu tunelowanego przez DNS. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi **na okres minimum 5 lat.**
35. Musi mieć możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesję w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.
36. Musi mieć możliwość wyboru sposobu blokowania ruchu w politykach bezpieczeństwa. Musi istnieć możliwość ustawienia cichego blokowania ruchu bez wysyłania RST, blokowanie z wysłaniem RST tylko do klienta, blokowanie z wysłaniem RST tylko do serwera, blokowanie z wysłaniem RST do klienta i serwera jednocześnie.
37. Firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
38. Musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i kategorii stron WWW.
39. Urządzenie musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
40. Urządzenie musi być dostarczone w konfiguracji z minimum 8 portami Ethernet 1Gb/s
41. Firewall musi posiadać przepustowość w ruchu nie mniej niż 2,2 Gbps dla kontroli firewall z włączoną funkcją kontroli aplikacji. Przepustowość dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (ochrona IPS, antywirus, antyspyware, identyfikacja aplikacji) nie może być mniejsza niż 1 Gbps.
42. Urządzenie musi obsłużyć minimum 200 000 jednoczesnych sesji oraz 38 000 nowych połączeń na sekundę.
43. Urządzenie musi zapewniać wydajność przynajmniej 1,5 Gbps dla ruchu IPSec VPN i umożliwiać zestawienie przynajmniej 2500 równoczesnych tuneli site-to-site.
44. Urządzenie musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi umożliwiać deszyfracje niezaufanego ruchu HTTPS i poddania go dalszej inspekcji.
45. Musi umożliwiać wykluczenie z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie co najmniej: kategoryzacji stron URL oraz dodania własnych wyjątków.

46. Musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (IPS, AV, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
47. Urządzenie musi zapewniać zestawienie przynajmniej 1000 sesji SSL VPN.
48. Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność zestawienia tuneli VPN SSL bez konieczności instalowania klienta na stacji końcowej – clientless VPN.
49. Musi posiadać możliwość uruchomienia funkcji wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS). W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi **na okres minimum 5 lat.**
50. Urządzenie musi posiadać możliwość uruchomienia funkcji inspekcji antywirusowej, kontrolującej przynajmniej protokoły: SMTP, HTTP, POP3, IMAP oraz podstawowe rodzaje plików. Baza AV musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi **na okres minimum 5 lat.**
51. Firewall musi umożliwiać filtrowanie stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza przypisania URL do kategorii musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi **na okres minimum 5 lat.**
52. Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
53. Firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi **na okres minimum 5 lat.**
54. Urządzenie musi zapewniać moduł przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików (przynajmniej exe, dll, pdf, jar, apk, pliki MS Office, ELF, BAT, JS, VBS, PS1, shell script, HTA, linki w wiadomościach e-mail) przechodzących przez firewall w celu ochrony przed zagrożeniami typu zero-day. Informacja zwrotna na temat wykrytego złośliwego oprogramowania musi zostać dostarczona na firewall w czasie nie dłuższym jak 5 minut. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików. Jeżeli funkcjonalność wymaga wykupienia dodatkowej licencji wtedy Zamawiający wymaga jej dostarczeni**a na okres 5 lat.**
55. Musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive i Active-Active w przypadku pracy z drugim takim samym urządzeniem posiadającym taki sam zestaw licencji.
56. Urządzenie musi być rozwiązaniem o uznanej na rynku pozycji i musi znajdować się w kwadracie „Leaders" raportu Gartnera pt. „Magic Quadrant of Network Enterprise Firewalls" w raportach opublikowanych w przeciągu 2 ostatnich lat.
57. Urządzenie musi być fabrycznie nowe, aktualnie obecne w linii produktowej producenta.
58. Musi pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej.
59. Urządzenie nie może znajdować się na liście „end-of-sale" oraz „end-of-support" producenta.
60. Serwis dostępu do najnowszej wersji oprogramowania, serwis sprzętowy i ewentualne licencje/subskrypcje na aktualizacje bazy aplikacji muszą być ważne przynajmniej **przez okres 5 lat.**

61. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim.

4.Skanery (5 szt.)

Urządzenie skanujące spełniające następujące funkcjonalności:

Typ skanera

Skaner płaski

Rozdzielczość optyczna (automatyczny podajnik dokumentów)

600 DPI x 600 DPI (poziomo x pionowo)

Rozdzielczość skanowania

1.200 DPI x 1.200 DPI (poziomo x pionowo)

Obszar skanowania

210 mm x 297 mm (poziomo x pionowo)

Minimalny rozmiar dokumentu na ADF

89 mm x 127 mm (poziomo x pionowo)

Formaty papieru

A4 (21.0x29,7 cm), A5 (14,8x21,0 cm), A6 (10,5x14,8 cm), B5 (17,6x25,7 cm), Letter, Letter Legal

Głębia kolorów

Wejście: 30 Bit Kolor / 10 Bit Monochromatyczny , Wyjście: 24 Bit Kolor / 8 Bit Monochromatyczny

Prędkość skanowania

monochromatyczny 25 Str./min. - Kolor: 25 Str./min. , Rozdzielczość: 200 / 300 dpi,
monochromatyczny 10 obrazów/min - Kolor: 10 obrazów/min , Rozdzielczość: 200 / 300 dpi

Obsługa papieru / nośników

Pojemność

50 Arkusze

Gramatura papieru na ADF

Ładowanie automatyczne: 50 - 120 g/m²

Dzienna wydajność niezawodnej pracy

1.500 pages

Automatyczny podajnik dokumentów

50 pages

Skanowanie dwustronne (dupleks)

Tak

Funkcje skanowania

Funkcje

Spadek gęstości kolorów RGB, Zaawansowane usuwanie/wzmocnienie koloru, Pomijanie pustych stron, Usuwanie otworów po dziurkaczu, Rozszerzona edycja obrazu, Automatyczna korekta położenia ukośnego, Poprawa koloru RGB, Automatyczny obrót obrazu, Poprawa tekstu, Wygładzenie krawędzi, Maskowanie nieostrości, Derasteryzacja, Rozpoznawanie kodu kreskowego, Obsługa strefowego optycznego rozpoznawania znaków OCR A i B, Pełne strefowe rozpoznawanie tekstów OCR

Funkcje kompresji pliku

Sprzętowa kompresja JPEG, Kompresja TIFF (JPEG(7), CCITT G4, LZW), Kompresja PDF, Kompresja JPEG

Wolumen skanowania

1.500 Liczba stron dziennie

Przyłącza

USB 3.0

5. Laptop wraz z niezbędnym oprogramowaniem (5 szt.)

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Typ	Komputer przenośny z zasilaczem. W ofercie należy podać nazwę producenta, typ, model oferowanego sprzętu z uwzględnieniem dokładnego modelu oferowanego procesora, typu i modelu pamięci, typu, rodzaju i pojemności dysków twardych oraz modelu zintegrowanego układu graficznego. Cały oferowany sprzęt musi być fabrycznie nowy, wyprodukowany nie wcześniej niż w I kwartale 2022 r. **Zamawiający nie dopuszcza sprzętu refurbished.**
2.	Ekran	Matryca 15" z podświetleniem w technologii LED, matowa, IPS, rozdzielczość FHD (1920x1080)
3.	Chipset	Dostosowany do zaoferowanego procesora
4.	Płyta główna	Wyposażona w interfejs M.2 do obsługi dysków twardych.
5.	Procesor	Procesor min. 4 rdzeniowy, zaprojektowany do pracy w komputerach przenośnych, osiągający w teście PassMark – CPU Mark co najmniej 10,070 punktów (wynik zaproponowanego procesora ze strony http://www.cpubenchmark.net).
6.	Pamięć operacyjna	Minimum 8 GB RAM DDR4. Możliwość rozbudowy do 16 GB. Jeden slot musi pozostać wolny aby umożliwić dodanie drugiego modułu.
7.	Dysk twardy	Minimum 256 GB SSD M.2 zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
8.	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) z możliwością dynamicznego przydzielenia pamięci. Obsługująca funkcje: − DX12, − OGL 4.0, − OpenCL 1.2,
9.	Audio/Video	Wbudowana, zgodna z HD Audio, wbudowane głośniki, kamera, mikrofon.
10.	Karta sieciowa	10/100/1000 – RJ 45
11.	Porty/złącza	− 1 x USB 3.1 typu C z możliwością wyświetlania 4k − 1 x USB 3.0 typu A − 1 x USB 2.0 typu A − gniazdo zasilania − rozdzielne złącze słuchawek i mikrofonu lub typu − combo HDMI lub DisplayPort RJ-45. czytnik kart − multimedialnych. − ebook musi posiadać możliwość podłączenia dedykowanej stacji dokującej z zapewnieniem ładowania laptopa za jej

		pośrednictwem.
12.	Klawiatura	Klawiatura podświetlana, odporna na zachlapanie, układ US i touchpad z obsługą gestów.
13.	WiFi	Wbudowana karta sieciowa WIFI, pracująca w standardzie ac/b/g/n.
14.	Bluetooth	Wbudowany moduł Bluetooth 4.1.
25	System operacyjny	Windows 11 Professional