1. **arkusSerwer – 2 sztuki**

|  |  |
| --- | --- |
| **Element konfiguracji** | **Wymagania minimalne** |
| Typ urządzenia | Serwer do montażu w steleażu 19” (szafie rack 19”) |
| Obudowa | Maksymalnie 2U RACK 19 cali (wraz z szynami umożliwiającymi wysunięcie i wszystkimi elementami niezbędnymi do zamontowania serwera w szafie). |
| Procesor | Procesor osiągający w teście SPECrate®2017\_int\_base wynik co najmniej 151 punktów. Płyta główna wspierająca zastosowanie procesorów od 8 do 64 rdzeniowych, wymagających mocy 280W i obsługujących do 4TB RAM na procesor. |
| Liczba procesorów | 1 |
| Pamięć operacyjna | Min. Osiem modułów 32 GB Płyta główna z minimum 16 slotami na pamięć, umożliwiającainstalację do minimum 4TB pamięci RAM, obsługująca moduły 3200 MT/s. Obsługa zabezpieczeń: Advanced ECC. |
| Sloty rozszerzeń | Możliwość instalacji do 3 kart PCI-Express generacji 4, x16(szybkość slotu – bus width) pełnej wysokości (full height). |
| Dysk twardy | Możliwość instalacji do 26 dysków. Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD. Zainstalowane min. 2 dyski 240 GB SSD. |
| Interfejsy sieciowe | Zainstalowane min. 4 porty 10/100/1000 Mbit/s. Zainstalowane min. 4 porty 10Gb SFP+ wraz z modułami SFP+ |
| Karta graficzna | Zintegrowana karta graficzna z pamięcią min. 16 MB , umożliwiająca wyświetlenie obrazu min. 1920 x 1200@60Hz |
| Porty | Min. 4x USB 3.1 (w tym min. 1 port wewnętrzny i 1 z przodu obudowy)1x VGAMożliwość rozbudowy/rekonfiguracji o port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express1x port RJ-45 dedykowany dla interfejsu zdalnego zarządzania |
| Zasilacz | 2 szt., typu Hot-plug, redundantne, każdy o mocy maxmimum 500W, efektywność zasilaczy 94% |
| Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug |
| Zarządzanie i obsługa techniczna | Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) z dedykowanym portem RJ45 pozwalającą na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej oserwera niezależnie od jego stanu (także podczas startu, restartu OS). Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe i nie zajmująca wymaganych slotów PCI. Jeśli jest wymagana to załączona odpowiednia licencja. |
| Karta/moduł zarządzający i system zarządzania | 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
* praca 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

      dostęp do karty możliwy * + z poziomu przeglądarki webowej (GUI)
	+ z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)
	+ z poziomu skryptu (XML/Perl)
	+ poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)
* wbudowane narzędzia diagnostyczne
* zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego
* obsługa mechanizmu remote support  - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie
* wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
* przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)
* obsługa zdalnego serwera logowania (remote syslog)
* 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
* mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii  i ostatniego startu serwera a także nagrywanie na żądanie
* funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności
* monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji
* konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
* zdalna aktualizacja oprogramowania (firmware)
* zarządzanie grupami serwerów, w tym:
	+ tworzenie i konfiguracja grup serwerów
	+ sterowanie zasilaniem (wł/wył)
	+ ograniczenie poboru mocy dla grupy (power capping)
	+ aktualizacja oprogramowania (firmware)
	+ wspólne wirtualne media dla grupy
* możliwość równoczesnej obsługi przez 6 administratorów
* autentykacja dwuskładnikowa (Kerberos)
* wsparcie dla Microsoft Active Directory
* obsługa SSL i SSH
* enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli
* wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API
* wsparcie dla Integrated Remote Console for Windows clients
* możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
 |
| Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Microsoft Windows Server 2022Red Hat Enterprise Linux (RHEL) 8.0SUSE Linux Enterprise Server (SLES) 15VMware ESXi 6.7 U3 |
| Gwarancja | Minimum 5-letnia gwarancja producenta na części, robociznę i naprawę w miejscu instalacji typu On-Site, z 2 godzinnym czasem reakcji w godzinach 8:00-17:00, z czasem rozpoczęcia naprawy w następnym dniu roboczym (NBD) w miejscu instalacji.Usługa wsparcia technicznego musi być świadczona przez autoryzowany serwis producenta oferowanych urządzeń.Możliwość rozszerzenia usługi gwarancyjnej do 5 lat realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy 6 godzin i pozostawieniem uszkodzonych dysków u zamawiającego. |

1. **Macierz dyskowa – 2 sztuki**

|  |  |
| --- | --- |
| **Element konfiguracji** | **Wymagania minimalne** |
| Typ urządzenia | Serwer NAS |
| Obudowa | Rack |
| Procesor  | osiągający w teście PassMark na sierpień 2022 co najmniej 7 440 punktów |
| Sprzętowy mechanizm szyfrowania  | Tak (AES-NI) |
| Pamięć RAM | min. 8 GB pamięci ECC UDIMM z możliwością rozszerzenia do min. 64 GB |
| Możliwości rozbudowy | Sprzęt powinien być wyposażony w min. 12 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 36 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą gniazd rozszerzeń Infiniband |
| Dyski | Zainstalowanych min. 7 dysków 16TB. Oferowane dyski muszą znajdować się na liście kompatybilności, opublikowanej na stronie producenta serwera NAS.  |
| Porty zewnętrzne  | Minimum:* 2 porty USB 3.2.1
* 2 gniazda rozszerzenia
 |
| Porty sieciowe | Minimum:* 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
* 2 porty 10Gb SFP+
 |
| Funkcja Wake on LAN/WAN | Tak |
| Gniazdo rozszerzeń PCIe 3.0 | Min. 2x 8-liniowe gniazdo x8 (Gen.3) |
| Wentylator obudowy | Min. 4 wentylatory 80 mm x 80 mm |
| Obsługiwane protokoły sieciowe | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |
| Obsługiwane systemy plików | Min.:* Wewnętrzny: Btrfs, ext4
* Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
 |
| Zarządzanie pamięcią masową | * Maksymalny rozmiar pojedynczego wolumenu:
	+ 1 PB (wymagana pamięć 64 GB, tylko grupy RAID 6)
	+ 200 TB (wymagana pamięć 32 GB)
	+ 108 TB
* Minimalny liczba wewnętrznych wolumenów: 128
* Minimalny liczba obiektów iSCSI Target: 256
* Minimalny liczba jednostek iSCSI LUN: 512
* Obsługa klonowania/migawek jednostek iSCSI LUN
 |
| Obsługiwane typy macierzy RAID | Podstawowy (Basic), JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID F1 |
| Funkcja udostępniania plików | * Minimalna liczba kont użytkowników: 16 000
* Minimalna liczba grup użytkowników: 512
* Minimalna liczba folderów współdzielonych: 512
* Minimalna liczba jednoczesnych połączeń CIFS/AFP/FTP: 2 000
 |
| Uprawnienia | Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL) |
| Wirtualizacja | Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack® |
| Usługa katalogowa | Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP |
| Bezpieczeństwo | Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczneblokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) |
| Obsługiwane przeglądarki | Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach |
| Oprogramowanie | * Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych
* Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów
* Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.
* Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
 |
| Konserwacja | * Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack dostarczonych z zestawem
* Wymiana wentylatora systemowego ma przebiegać w szybki i bezpieczny sposób bez użycia narzędzi
 |
| Zasilanie | * Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz.
 |
| Gwarancja | Wykonawca udzieli gwarancji:* 5 lat na urządzenia główne
* 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack
 |

1. **Tablet mobilny – 5 sztuk**

|  |  |
| --- | --- |
| **Element konfiguracji** |  **Wymagania minimalne** |
| Typ urządzenia | Tablet |
| Ekran | Min. 10,1” 1280x800 IPS, jasność min. 600 nitów, wodoodporny |
| Procesor |  |
| System | Android min. 9.0 lub równoważnyZa system równoważny uważa się system operacyjny oferujący takie same funkcjonalności jakie oferuje system Android w min. Wskazanej przez Zamawiającego wersji współpracujący ze środowiskiem informatycznym Zamawiającego oraz o cechach: 1. System nie związany z jakimikolwiek ograniczeniami praw autorskich – dostępny np. na licencji Apache License 2. System operacyjny dedykowany dla urządzeń mobilnych typu tablet 3. Zintegrowana przeglądarka internetowa obsługujący przeglądanie na kartach 4. Wsparcie grafiki 3D poprzez OpenGL 5. Wsparcie dla języka Java umożliwiający dostęp do wszystkich urządzeń (kamery, ekranu dotykowego, GPS, kompasu, sensorów motorycznych i akceleratorów grafiki 3D) 6. Obsługa formatów multimedialnych: MPEG-4, H.264, MP3 oraz AAC, JPEG, PNG, GIF. 7. Obsługa technologii komunikacyjnych, m.in. GSM, CDMA, Bluetooth, EDGE, 3G oraz Wi-Fi. 8. Możliwość przełączania i wyboru uruchomionych aplikacji w postaci zrzutów ekranu (min. 6 aplikacji) 9. Środowisko programistyczne, które zawiera emulator urządzeń i biblioteki do debugowania |
| Pamięć RAM | Min. 2GB  |
| Pamięć ROM | Min. 16GB |
| Karta Pamięci | Slot obsługujący karty pamięci do min. 128GB |
| Łączność | WIFI wbudowane min. IEEE 802.11 a/b/g/n/ac, NFC, HF RFID |
| Czujniki | Akcelerometr, Żyroskop, czujnik światła otoczenia,  |
| Kamera | Wbudowana Tylnia min. 8 Mpx z lampą błyskowąWbudowana Przednia min. 8 Mpx |
| Mikrofon | Wbudowany min. 2 szt. wspierający redukcję szumów |
| Przyciski | Min. 2 szt. fizycznych programowalnych |
| Bateria | Min. 5500 mAh, oraz zapasowy min 250 mAh akumulator z możliwością wymiany podczas pracyŻywotność baterii min. 8h, potwierdzone w oficjalnych dokumentach producenta |
| VESA | Kompatybilny z VESA 100 x 200mm |
| Certyfikaty | Min. IP67, CE. |
| Środowisko | Temperatura pracy min. w zakresie: -10 stopni do +50 stopniTemperatura przechowywania min. w zakresie: -20 do +70 stopniWilgotność: min. w zakresie 0 – 95% |
| Stacja dokująca | Możliwość rozbudowania o ładującą stację dokującą dedykowaną przez producenta, jako stojak dla tabletu, z wbudowanymi portami min. RJ45, RS232, 2x USB |
| Gwarancja | Min. 12 miesięcy producenta |

1. **Urzadzenia sieci bezprzeowodowej:**
2. **Bezprzewodowe punkty dostępowe – 10 sztuk**

|  |  |
| --- | --- |
| **Element konfiguracji** |  **Wymagania minimalne** |
| Typ urządzenia | punkt dostępowy dwuradiowy (AP), w zamkniętej architekturze przeznaczone do montażu na ścianie, suficie podwieszanym lub suficie trwałym (z pomocą dodatkowych akcesoriów) |
| Wymagane porty | - urządzenie musi być w 100% kompatybilne z wyspecyfikowanym kontrolerem sieci bezprzewodowej;- minimum 2 porty 10/100/1000Base-T;- minimum 1 port szeregowy konsoli (interfejs RJ-45);- minimum 1 port USB 2.0;- temperatura pracy: minimalny zakres 0°C – 50°C- montaż: naścienny, na suficie- złącze zasilacza: 12V DC; |
| Zasilanie | Power over Ethernet IEEE 802.3af/at (pobór mocy max. 13W); zewnętrzny adapter (zasilanie:100-240V AC, napięcie wyjściowe 12V DC) |
| Pobór mocy | Max. nie większy niż 13W  |
| Tryby pracy | - możliwość pracy w trybie z kontrolerem (FIT), jak również w trybie samodzielnym (FAT); - sumaryczna prędkość przesyłania danych nie mniejsza niż 1,775Gb/s- równoczesna praca na częstotliwościach 2.4 GHz oraz 5 GHz;- komunikacja bezprzewodowa 2x2:2 MIMO |
| Anteny | wbudowane anteny 2.4 GHz zysk minimum 4dBi, wbudowane anteny 5GHz zysk minimum 5dBi; |
| Moc nadawcza | dla 2,4GHz minimum 23dBm, dla 5GHz minimum 23dBm (moc wyjściowa na złączu antenowym) |
| Regulacja mocy | z krokiem maksimum 1dBm |
| Wymagane tryby i częstotliwości pracy radia | - IEEE 802.11a/n/ac : 5.150 GHz - 5.850 GHz - IEEE 802.11b/g/n/ax: 2.4 GHz - 2.483 GHz - IEEE 802.11ax: 5.150 GHz – 5.250 GHz 5.250 GHz - 5.350 GHz 5.725 GHz – 5.850 GHz |
| Wymagane obsługiwane technologie modulacji | - IEEE 802.11b: BPSK,QPSK,CCK - IEEE 802.11a/g/n: BPSK, QPSK,16-QAM, 64-QAM - IEEE 802.11ac: BPSK, QPSK,16-QAM, 64-QAM, 256-QAM - IEEE 802.11ax: BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM |
| Stopień ochrony urządzenia | Min. IP41 |
| Obsługa wirtualnych punktów dostępowych (BSSID) | minimum 32 jednocześnie |
| Ilość obsługiwanych strumieni przestrzennych: | Min. 2 |
| Obsługa łączności bezprzewodowej | DCA (dynamiczne dostosowanie kanałów), TPC (kontrola mocy nadawania), wykrywanie martwych obszarów, ukrywanie SSID, RTS/CTS, skanowanie środowiska radiowego, limitowanie liczby użytkowników, eliminacja terminali ze zbyt słabym sygnałem, wymuszanie roamingu terminali o słabym sygnale, inteligentna kontrola terminali w oparciu o równomierne rozłożenie czasu transmisji, Okresowe włączanie i wyłączanie SSID; |
| Funkcje bezpieczeństwa | szyfrowanie 64/128 WEP, TKIP, CCMP; IEEE 802.11i; WAPI, autentykacja po adresie MAC; autentykacja LDAP; autentykacja PEAP; WIDS/WIPS; Ochrona widma w czasie rzeczywistym; zabezpieczenie przed atakami typu DoS; bezpieczeństwo przekierowywania: filtrowanie ramek, biała lista, statyczna czarna lista i dynamiczna czarna lista; izolowanie stacji bezprzedowodych, SAVI, Izolacja użytkownika; obsługa list kontroli dostępu; Kontrola dostępu do wolnych zasobów; kontrola dostępu terminali bezprzewodowych; ACL; bezprzerwowa praca urządzenia w przypadku utraty połączenia z kontrolerem; możliwość automatycznego wyłączania usług w przypadku przekroczenia zakładanego czasu dostępności usługi; |
| Funkcje sieciowe | statyczny adres IP, klient DHCP, obsługa pakietów IPv6, IGMP Snooping, roaming pomiędzy AP, roaming pomiędzy AC, WDS; kontrola dostępu do punktów dostępowych; |
| Obsługa funkcji QoS (jakości usługi) | IEEE 802.11e (WMM), mapowanie różnych sieci VLAN oraz SSID do różnych polityk QoS, mapowanie różnych strumieni danych (na podstawie różnych pól pakietów) do rożnych polityk QoS, load balancing w oparciu o liczbę użytkowników/ilość ruchu/zakres częstotliwości, limit przepustowości możliwy do zdefiniowania dla AP/SSID/terminali/strumieni danych, tryb oszczędzania energii, automatyczne odzyskiwanie komunikacji z AC, inteligentne identyfikowanie terminali; urządzenie musi umożliwiać początkową inicjalizację na paśmie 5GHz dla urządzeń odbiorczych pracujących w paśmie 2,4GHz oraz 5GHz; |
| Zarządzanie | zarządzanie centralne poprzez kontroler sieci bezprzewodowej (AC), lokalny log, syslog, eksport pliku log, funkcja AP Escape (w przypadku braku komunikacji z którymkolwiek z AC, AP pracują jako niezależne urządzenia wciąż obsługując obecnych i nowych użytkowników), Dual-image backup (podwójny OS), sprzętowy watchdog, możliwość zdalnej autentykacji do AC poprzez L3 i Internet (AC na publicznym adresie IP) bez użycia tuneli VPN; |
| Gwarancja | lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat. |

1. **Przełączniki sieciowe, dostępowe – 5 sztuk**

|  |  |
| --- | --- |
| **Element konfiguracji** |  **Wymagania minimalne** |
| Typ urządzenia | Przełącznik sieciowy z funkcją PoE dostępowy, gigabitowy |
| Wymagane porty | - minimum 24x 10/100/1000Base-T RJ45 PoE - minimum 4x 1/10GBase-X SFP+- minimum 1 port zarządzania RJ45 (RS-232)- minimum 1 port USB co najmniej w standardzie 2.0 |
| Szybkość przełączania | minimum 128Gb/s |
| Przepustowość | minimum 95Mp/s (dla pakietów 64Kb) |
| Bufor pakietów | minimum 1,5MB |
| Ramki Jumbo | minimum 10k |
| Tablica adresów MAC | minimum 16k |
| Adresy MAC – Multicast | minimum 1k |
| Tablica ACL | minimum 512 |
| Tablica VLAN | minimum 4094 |
| Taktowanie procesora | minimum 800MHz |
| Pamięć Flash | minimum 32MB  |
| Pamięć RAM | minimum 256MB |
| Obsługa technologii PoE | IEEE 802.3 af/at |
| Budżet mocy PoE | minimum 370W |
| Temperatura pracy | zakres minimum 0°C - 50°C |
| Wilgotność względna | zakres minimum 10% - 90% (bez kondensacji) |
| Zasilanie | zabudowany zasilacz 230V AC |
| Pobór mocy | maksymalnie 21W |
| Zabezpieczenie przeciwprzepięciowe | minimum 6kV |
| Wymiary | maksymalne: szerokość 440 mm, wysokość 44mm , głębokość 310mm |
| Certyfikaty bezpieczeństwa | CE, RoHS |
| Algorytm | Store and Forward |
| VLAN | Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ |
| DHCP | IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server |
| Spanning tree | IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding |
| Protekcja ringowa | ITU-T G.8032 – recovery time < 50ms, Fast Link, Loopback Detection |
| Agregacja łączy | IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balance |
| Bezpieczeństwo | Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN, |
| Multicast | : IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication |
| QoS | 8 queques per port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, Queuing Method: Strict Priority, Weighted Deficit Round Robin, Strict priority in Weighted Deficit Round Robin; DNS Client, DNS Relay |
| Lista kontroli dostępu | IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN |
| Diagnostyka | sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route, Dying GASP |
| Zarządzanie | TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (4 devices in one stack) – hardware stacking |
| Funkcje PoE | Support IEEE 802.3at for all ports, PD failure detection, PoE scheduling, Continuous powering during switches restart |
| Oprogramowanie oraz wsparcie techniczne | oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług |
| Gwarancja | lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat. |

1. **Stacja robocza z monitorem LCD – 20 sztuk**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów i monitorów** |
| **Komputer** | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. |
| Obudowa | Typu Small Form Factor z obsługą kart PCI Express wyłącznie o niskim profilu:- 1 x PCI Express x16,Wyposażona w min. 3 kieszenie z czego min. 1 szt. 5,25” (dopuszcza się zastosowanie jednej kieszeni 5,25” w wersji SLIM dla napędu optycznego) oraz 2 szt. pozwalające na montaż dysków 2,5”.Obudowa musi umożliwiać bez narzędziowe otwarcie, demontaż dysku M.2, napędu optycznego oraz kart rozszerzeń. Obudowa musi być wyposażona w czujnik otwarcia.Wbudowany głośnik o mocy min. 1WObudowa trwale oznaczona nazwą producenta, nazwą komputera, PN, numerem seryjnym |
| Chipset | Dostosowany do zaoferowanego procesora z fabrycznym wsparciem sprzętowym obsługi standardów DMTF oraz DASH (nie jest wymagana uruchomiona funkcjonalność software’owa) |
| Płyta główna | Płyta główna wyposażona w min. 2 złącza M.2 z czego 1 dedykowane dla dysku SSD PCIe. |
| Procesor | Procesor wielordzeniowy ze zintegrowaną grafiką klasy x86 ze wsparciem 64 bit osiągający w teście Passmark CPU min. 19 500 pkt. na podstawie Performance Test w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/.  |
| Pamięć operacyjna | 8GB, 3200MHz, 4 sloty na pamięć, z czego min. 3 wolne.Możliwość pracy pamięci w trybie dual channel. Obsługa do min. 128GB RAM.  |
| Dysk twardy | Dysk: Min 256 M.2 PCIe 4.0 wspierający sprzętowe szyfrowanie dysku, zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii |
| Napęd optyczny | Nagrywarka DVD +/-RW wyposażona w tackę z zaczepami umożliwiającymi pracę w poziomie i pionie |
| Karta graficzna | osiągająca w teście Passmark G3D Mark min. 1500 pkt. według wyników opublikowanych na https://www.videocardbenchmark.net/gpu\_list.php |
| Audio | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.  |
| Sieć | Karta sieciowa LAN obsługująca prędkości 10/100/1000, bezprzewodowa karta sieciowa standardu min. 802.11ax, Bluetooth min. 5.2 |
| Porty/złącza | Wbudowane porty: - 1 x HDMI min. 2.0, - 2 x DP 1.4, - 9 x USB w tym min.: 4x USB 3.2 z przodu obudowy oraz 1x USB-C; - port sieciowy RJ-45,- czytnik kart pamięci - porty słuchawek i mikrofonu na przednim panelu obudowy- możliwość doposażenia w porty szeregowe klawiatury/myszy PS/2 (bez udziału przejściówek, adapterów USB, dodatkowych kart, itp.) Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |
| Klawiatura/mysz | Klawiatura w układzie US + mysz z rolką |
| Zasilacz | Energooszczędny zasilacz o mocy nie większej niż 260W oraz sprawności na poziomie min. 85% posiadający certyfikat 80 PLUS.  |
| System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim.4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe.6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polski.9. Wbudowany system pomocy w języku polskim.10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."24. Wbudowany mechanizm wirtualizacji typu hypervisor."25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM.33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.34. Możliwość tworzenia wirtualnych kart inteligentnych.35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot).36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.38. Mechanizmy logowania w oparciu o:a. Login i hasło,b. Karty inteligentne i certyfikaty (smartcard),c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),d. Certyfikat/Klucz i PIN,e. Certyfikat/Klucz i uwierzytelnienie biometryczne,39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 540. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń.43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń |
| BIOS  | Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:- modelu komputera, PN- numerze seryjnym,- numerze inwentarzowym (AssetTag),- MAC Adres karty sieciowej,- wersja Biosu wraz z datą produkcji,- zainstalowanym procesorze, jego taktowaniu i ilości rdzeni- ilości pamięci RAM wraz z taktowaniem,- stanie pracy wentylatora na procesorze - stanie pracy wentylatora w obudowie komputera- napędach lub dyskach podłączonych do portów SATA (model dysku twardego i napędu optycznego)Możliwość z poziomu Bios:- wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy- wyłączenia selektywnego (pojedynczego) portów SATA,- wyłączenia karty sieciowej, karty audio, portu szeregowego,- możliwość ustawienia portów USB w jednym z dwóch trybów:1 użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB2 użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej - ustawienia hasła: administratora, Power-On, HDD,- blokady aktualizacji BIOS bez podania hasła administratora- wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów- alertowania zmiany konfiguracji sprzętowej komputera - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan)- ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - zdefiniowania trzech sekwencji bootujących (podstawowa, WOL, po awarii)- kontrola otwarcia i zamknięcia obudowy komputera za pomocą zamka elektromagnetycznego (jeżeli dotyczy)- załadowania optymalnych ustawień Biosbez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.  |
| Zintegrowany System Diagnostyczny | Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów:* wykonanie testu pamięci RAM
* test dysku twardego
* test monitora
* test magistrali PCI-e
* test portów USB
* test płyty głównej

Wizualna lub dźwiękowa sygnalizacja w przypadku uszkodzenia bądź błędów któregokolwiek z powyższych podzespołów komputera.Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie:* PC: Producent, model
* BIOS: Wersja oraz data wydania Bios
* Procesor : Nazwa, taktowanie
* Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci
* Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy
* Monitor: producent, model, rozdzielczość

System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera. |
| Certyfikaty i standardy | * Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty)
* Deklaracja zgodności CE (załączyć do oferty)

- Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności zdyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki- Certyfikat „TCO Certified Desktops 8” oferowana jednostka musi znajdować się na liście komputerów pod adresem: https://tcocertified.com/product-finder/index?category=Desktops lub równoważny, wg opisanych kryteriów w pkt. 2.0lub |
| Waga/rozmiary urządzenia | Wysokość urządzenia nie większa niż 35cm, waga nie większa niż 6 kg. |
| Bezpieczeństwo | * Złącze typu Kensington Lock lub równoważne
* Oczko na kłódkę
* Moduł TPM 2.0 z certyfikacją TCG
 |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji. |
| Oprogramowanie | Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym, kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie musi zapewniać również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca. |
| Gwarancja | 3 lata świadczona w miejscu użytkowania sprzętu (on-site)W przypadku awarii dysku twardego dysk uszkodzony pozostaje u Zamawiającego. |
| Wsparcie techniczne producenta | - możliwość weryfikacji u producenta konfiguracji fabrycznej i oferowanej zakupionego sprzętu - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji- możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego- Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |
| Pakiet biurowy | 1. Pełna polska wersja językowa interfejsu użytkownika.2. Wbudowany system pomocy w języku polskim.3. Możliwość dokonywania aktualizacji i poprawek oprogramowania przez Internet z możliwością wyboru instalowanych poprawek.4. Darmowe aktualizacje oprogramowania przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy serwera producenta systemu.5. Internetowa aktualizacja zapewniona w języku polskim.6. Licencja zezwalająca komercyjne użytkowanie pakietu – licencja biznesowa.7. Natywna, pełna integracja z posiadanym przez Zamawiającego systemem HIS AMMS Asseco.8. Natywne działanie na systemach z rodziny Windows (m.in. Windows 10 Professional 64bit, Windows Server 2019).9. Natywna obsługa drukarek sieciowych udostępnionych przez usługę Active Directory.10. Natywna obsługa skanerów (sterownik TWAIN), drukarek kodów kreskowych (język EPL) oraz czytników kodów kreskowych.11. Pakiet zintegrowanych aplikacji biurowych musi zawierać co najmniej:a) Edytor tekstub) Arkusz kalkulacyjnyc) Narzędzie do przygotowania i prowadzenia prezentacjid) Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)e) Narzędzie do tworzenia i organizowania notatek cyfrowych;12. Edytor tekstu musi umożliwiać:a) Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,b) Wstawianie oraz formatowanie tabel,c) Wstawianie oraz formatowanie obiektów graficznych,d) Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),e) Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,f) Automatyczne tworzenie spisów treści,g) Formatowanie nagłówków i stopek stron,h) Śledzenie zmian wprowadzonych przez użytkowników,i) Wydruk dokumentów,j) Eksport dokumentów do formatu PDFk) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatnąl) Pracę na dokumentach utworzonych w programie Microsoft Word, w wersjach 97-2019 oraz 365 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu. Zapewnienie po edycji i zapisaniu danego dokumentu jego dalszą, bezproblemową pracę w programie Microsoft Word, w wersjach 97-2019 oraz 365. Możliwość zapisu plików w formatach .doc oraz .docxm) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzeniem modyfikacji13. Arkusz kalkulacyjny musi umożliwiać:a) Tworzenie raportów tabelarycznych,b) Tworzenie wykresów liniowych (wraz z linią trendu), słupkowych, kołowych,c) Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,d) Tworzenie raportów z zewnętrznych źródeł danych, np. inne arkusze kalkulacyjne,e) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,f) Wyszukiwanie i zamianę danych,g) Wykonywanie analiz danych przy użyciu formatowania warunkowego,h) Nazywanie komórek arkusza i odwoływanie się w formułach po tej nazwie,i) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,j) Obsługę języka VBA,k) Formatowanie czasu, daty i wartości finansowych z polskim formatem,l) Zapis wielu arkuszy kalkulacyjnych w jednym pliku,m) Zachowanie pełnej zgodności z plikami utworzonymi w programie Microsoft Excel, w wersjach 97-2019 oraz 365 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. Zapewnienie po edycji i zapisaniu danego pliku jego dalszą, bezproblemową pracę w programie Microsoft Excel, w wersjach 97-2019 oraz 365. Możliwość zapisu plików w formatach .xls oraz .xlsx,n) Zabezpieczenie arkuszy i komórek hasłem przed odczytem i/lub modyfikacją.14. Narzędzie do przygotowania i prowadzenia prezentacji musi umożliwiać:a) Prezentowanie przy użyciu projektora multimedialnegob) Drukowanie w formacie umożliwiającym robienie notatekc) Zapisanie jako prezentacja tylko do odczytud) Nagrywanie narracji i dołączanie jej do prezentacjie) Opatrywanie prezentacji notatkami dla prezenteraf) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideog) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnegoh) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnymi) Możliwość tworzenia animacji obiektów i całych slajdówj) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezenterak) Zachowanie pełnej zgodności z plikami utworzonymi w programie Microsoft PowerPoint, w wersjach 97-2019 oraz 365. Zapewnienie po edycji i zapisaniu danego pliku jego dalszą, bezproblemową pracę w programie Microsoft PowerPoint, w wersjach 97-2019 oraz 365. Możliwość zapisu plików w formatach .ppt oraz .pptx15. Narzędzie do zarządzania informacją prywatną musi umożliwiaća) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego przez protokoły POP3 oraz IMAPb) Możliwość włączenia szyfrowania połączenia z serwerem pocztowymc) Automatyczne filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawcówd) Tworzenie katalogów pozwalających na organizowanie poczty elektroniczneje) Automatyczne grupowanie poczty o tym samym tytulef) Tworzenie reguł automatycznie przenoszących nowe wiadomości do odpowiednich folderów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcyg) Oflagowanie poczty elektronicznej z określeniem terminu przypomnieniah) Zarządzanie kalendarzemi) Udostępnianie kalendarza innym użytkownikomj) Przeglądanie kalendarza innych użytkownikówk) Zapraszanie użytkowników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzanie spotkania w ich kalendarzul) Zarządzanie listą zadańm) Zlecanie zadań innym użytkownikomn) Zarządzanie listą kontaktówo) Udostępnianie listy kontaktów innym użytkownikomp) Przeglądanie listy kontaktów innych użytkowników. |
|  |  |
| **Monitor** | Zastosowanie ogólne, biurowe |
| Typ matrycy | IPS LED |
| Rozmiar | Min. 23,8” |
| Kontrast statyczny/dynamiczny | Min. 1000:1/ 8 000 000:1 |
| Czas reakcji (GtG) | Maks. 4ms |
| Jasność | Min. 250 cd/m2 |
| Złącza/interfejsy | Min. VGA, HDMI, Displayport |
| Wbudowane głośniki | Min. 2 x 2W |
| Regulacja wysokości | Min. 150mm |
| Pivot | Min. 90 stopni |
| Funkcje dodatkowe | wysokość, obrót, pochył, pivot |
| Zużycie energii | Typowe maks. 16W |
| Certyfikaty | Min. TCO, CE, EAC, ROHS, WEEE, Energy Star |
| Waga bez opakowania | Maks. 6kg |
| Wyposażenie | Kabel zasilający, HDMI, USB, Displayport |

1. **System zbierania i analizy logów**

Centralny system logowania, raportowania i korelacji, umożliwiający centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń, obłsugujący wszystkie dostarczone w ramach postępowania firewalle.

1. W ramach systemu logowania i raportowania musi zostać dostarczony system monitorujący, gromadzący logi, korelujący zdarzenia i generujący raporty na podstawie danych z systemów bezpieczeństwa.
2. System centralnego logowania i raportowania musi zostać dostarczony w postaci maszyny wirtualnej instalowanej w środowisku VMware.
3. System logowania i raportowania musi zapewniać obsługę przestrzeni dyskowej o pojemności nie mniejszej niż 100 GB i pozwalać na przechowywanie zarchiwizowanych danych w ramach systemu przez okres minimum 2 lat.
4. System logowania i raportowania musi umożliwiać zbieranie minimum 1 MB logów dziennie.
5. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
6. System logowania i raportowania musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów firewalli.
7. System logowania i raportowania musi posiadać narzędzia dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie.
8. System logowania i raportowania musi mieć możliwość synchronizacji z serwerami czasu NTP.
9. System logowania i raportowania musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta Firewalli, które będą dostarczone w ramach postępowania firewalle.
10. System logowania i raportowania musi umożliwiać tworzenie statycznych raportów. Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.
11. System logowania i raportowania musi umożliwiać zaplanowanie wykonania raportów.
12. System logowania i raportowania musi mieć predefiniowany raport przez producenta Firewalli, które będą dostarczone w ramach postępowania na firewalle.
13. System logowania i raportowania musi umożliwiać tworzenie własnych raportów.
14. System logowania i raportowania musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) z funkcjonalnością „drill-down”.

**Wymagania dotyczące wsparcia technicznego:**

1. System centralnego logowania i raportowania musi być objęty serwisem gwarancyjnym na okres 36 miesięcy.
2. **System ochrony aplikacji sieciowych – 2 szt.**

System ochrony, podziału obciązenia dla ruchu przychodzącego i wychodzącego, pracujący w warstwach 2,4,7 modelu OSI. System musi pracować w trybie wysokiej dostępności. Niezależnie od kodu źródłowego aplikacji sieciowej lub aktualizacji system musi zabezpiczać przed :

1. Omijaniem kontroli dostępu poprzez modyfikację adresu URL, wewnętrznego stanu aplikacji lub strony HTML lub po prostu za pomocą niestandardowego narzędzia ataku API.
2. Umożliwieniem zmiany klucza podstawowego na rekord innego użytkownika, umożliwienie przeglądania lub edytowania konta innej osoby.
3. Podwyższeniem przywilejów. Działając jako użytkownik bez zalogowania lub działając jako administrator po zalogowaniu się jako użytkownik.
4. Manipulowaniem metadanymi, takie jak odtwarzanie lub manipulowanie tokenem kontroli dostępu JSON Web Token (JWT), plikiem cookie lub ukrytym polem manipulowanym w celu podniesienia uprawnień lub nadużywaniem unieważniania JWT.
5. Błędną konfiguracją CORS, która umożliwia nieautoryzowany dostęp do interfejsu API.
6. Wymuszeniem przeglądania stron uwierzytelnionych jako użytkownik nieuwierzytelniony lub stron uprzywilejowanych jako użytkownik standardowy. Dostęp do interfejsu API z brakującymi kontrolami dostępu dla POST, PUT i DELETE.

Niezależnie od kodu źródłowego aplikacji sieciowej lub aktualizacji system musi umożliwiać:

1. Monitorowanie API
2. Wykrywanie zagrożeń API
3. Zapobieganie zagrożeniom API
4. Wyszukiwanie niepożądanych, obcych komend :SQL, NoSQL, systemu operacyjnego; mapowania relacyjnych obiektów (ORM), LDAP i Expression Language (EL)
5. Przegląd kodu źródłowego w celu wykrycia podatności aplikacji na iniekcje
6. Automatyczne testowanie wszystkich parametrów, nagłówków, adresów URL, plików cookie, danych wejściowych JSON, SOAP i XML
7. Sprawdzenie aplikacji pod kątem przechowywania poufnych informacji
8. Sprawdzenie aplikacji pod kątem przechowywania niezabezpieczonych lub nieprawidłowo zabezpieczonych danych uwierzytelniających
9. Sprawdzenie poprawności konfiguracji uprawnień dla usług w chmurze
10. Sprawdzenie czy niepotrzebne funkcje są włączone lub zainstalowane (np. niepotrzebne porty, usługi, strony, konta lub uprawnienia)
11. Sprawdzenie czy domyślne konta i ich hasła są włączone i niezmienione
12. Sprawdzenie czy najnowsze dostępne funkcje zabezpieczeń są wyłączone lub czy są prawidłowo skonfigurowane
13. Sprawdzenie czy ustawienia zabezpieczeń w serwerach aplikacji, frameworkach aplikacji (np. Struts, Spring, ASP.NET), bibliotekach, bazach danych itp. są prawidłowo skonfigurowane
14. Sprawdzenie czy serwer nie wysyła nagłówków ani dyrektyw bezpieczeństwa oraz czy są one ustawione na bezpieczne wartości
15. Sprawdzenie czy oprogramowanie jest nieaktualne lub podatne na ataki
16. Sprawdzenie czy oprogramowanie używa nieobsługiwane komponenty, moduły innych firm
17. Sprawdzanie pod kątem nieużywane zależności, niepotrzebnych funkcji, komponentów
18. Sprawdzenie pod kątem wykorzystania komponentów z nieznanych źródeł oraz nie podpisanych pakietów
19. Sprawdzenie pod kątem niewłaściwej walidacji certyfikatu z niezgodnością hosta
20. Sprawdzenie pod kątem niewłaściwego uwierzytelniania i utrwalania sesji
21. Sprawdzenie podatności na aktualizacja bez podpisu
22. Sprawdzenie podatności na złośliwe aktualizacje
23. Sprawdzenie podatności na deserializację
24. Sprawdzenie pod kątem występowania znanych luk i błędnych zabezpieczeń
25. Sprawdzenie podatności na odwoływanie się do niezweryfikowanego adresu URL
26. Sprawdzenie czy oprogramowanie wysyła nieprzetworzone odpowiedzi do klientów
27. Sprawdzenie czy oprogramowanie wykonuje niezweryfikowane przekierowania HTTP
28. **System ochrony brzegu sieci typu UTM – 2 szt.**

Zintegrowany system bezpieczeństwa klasy UTM/NGFW wraz z subskrypcją zabezpieczeń i gwarancją, zgodną z opisem poniżej :

|  |
| --- |
| **ARCHITEKTURA SYSTEMU** |
| 1. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, umożliwiającej rozbudowę do dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności conajmniej Active-Passive, o specyfikacji opisanej poniżej.
2. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe.
3. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
 |
| 1. Metalowa obudowa o wysokości max. 1U przeznaczona do montażu w szafie RACK 19’’
2. Podwójne, redundantne, zintegrowane zasilanie.
3. Obsługa nielimitowanej ilości hostów w sieci chronionej.
4. Minimalna liczba i typ interfejsów fizycznych:

•System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 2,5 Gbps•System realizujący funkcję Firewall musi dysponować minimum 4 interfejsami optycznymi 10GbE (SFP+)•Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.1. Minimalna liczba nowych połączeń na sekundę: 50 000
2. Minimalna liczba jednoczesnych połączeń: 1 000 000
3. Minimalna przepustowość Firewall: 18 Gbps
4. Minimalna przepustowość IPS: 10 Gbps
5. Minimalna przepustowość Threat Protection: 3 Gbps
6. Minimalna przepustowość IPSec VPN: 4 Gbps
7. Minimalna liczba tuneli SSL VPN: 300
8. Minimalna liczba tuneli IPSEC VPN: 1000
9. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 200 GB SSD do celów logowania i raportowania
 |
| **PODSTAWOWE FUNKCJE SYSTEMU OCHRONY** |
| **Zarządzanie i utrzymanie** | 1. Rozwiązanie musi być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH.
2. Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej ping
3. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
4. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
5. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.
6. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego
7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników.
8. Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora.
9. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP
10. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3
11. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do chmury producenta lub własnego serwera. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, tygodniowo oraz miesięcznie.
12. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware)
 |
| **Zapora sieciowa, konfiguracja sieciowa oraz routing** | 1. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection.
2. Rozwiązanie musi umożliwiać budowanie reguł zapory sieciowych w oparciu o takie obiekty jak elementy jak host, sieć, interfejs, harmonogram, port, protokół, użytkownik, grupa użytkowników, metoda uwierzytelnienia
3. System musi umożliwiać budowanie reguł bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.
4. Rozwiązanie musi pozwolić na definiowanie własnych polityk NAT wraz z IP masquerading.
5. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
6. System musi zapewniać ochronę przed skanowaniem portów (portscan blocking).
7. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).
8. Rozwiązanie musi zapewniać obsługę routingu statycznego.
9. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, OSPF, BGP).
10. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z obsługą RSTP oraz MSTP.
11. System musi oferować funkcjonalność serwera DHCP lub DHCP Relay.
12. System musi oferować wsparcie dla IEEE 802.1Q VLAN z niezależnymi pulami DHCP.
13. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.
14. Rozwiązanie musi umożliwiać rozkładanie ruchu do Internetu w oparciu o wagi poszczególnych bram ISP.
15. Wymagane jest by rozwiązanie zapewniało obsługę modemu USB LTE np. jako łącze zapasowe .
16. Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).
17. Rozwiązanie musi dawać możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza.
18. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
19. Rozwiązanie musi dawać możliwość optymalizacji ruchu wychodzącego w dostępie do określonych usług.
20. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
21. System musi dawać możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.
 |
| **Podstawowe kształtowanie pasma oraz limity ilości danych** | 1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla użytkownika, hosta lub połączenia.
2. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
 |
| **Autoryzacja użytkowników** | 1. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont.
2. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP
3. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory
4. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.
5. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal.
6. Rozwiązanie musi posiadać wbudowany moduł zapewniający uwierzytelnianie na poziomie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
7. Metoda 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
 |
| **Samoobsługowy portal dla użytkowników** | 1. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).
2. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta OpenVPN dla Windows, Mac OS X, Linux, iOS, Android
3. Rozwiązanie musi umożliwiać zmianę hasła.
 |
| **Podstawowe opcje VPN** | System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:1. Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK)
2. Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
 |
| **OCHRONA SIECI** |
| **IPS** | 1. Dodatkowy moduł ochrony klasy IPS z bazą minimum 1000 sygnatur.
2. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS.
3. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.
4. Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur
5. System musi generować alerty w przypadku wykrycia ataku.
 |
| **OCHRONA I KONTORLA WEB ORAZ APLIKACJI** |
| **Ochrona i kontrola Web** | 1. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.
2. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.
3. Rozwiązanie musi zapewniać skanowanie AV plików w czasie rzeczywistym
4. Rozwiązanie musi oferować funkcję inspekcji z obsługą protokołu TLS 1.3 oraz z tzw. walidacją certyfikatów.
5. System musi filtrować pliki na podstawie MIME.
6. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.
7. Rozwiązanie musi zawierać przynajmniej 50 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www.
8. Rozwiązanie musi zapewniać możliwość blokowanie i wysyłania treści poprzez HTTP i HTTPS.
9. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego.
 |
| **Ochrona i kontrola aplikacji** | 1. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji.
2. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook)
3. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
 |
| **Kształtowanie pasma dla Web i Aplikacji** | 1. Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download.
2. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.
3. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym.
 |
| **OCHRONA ANTYWIRUSOWA** |
| **Ochrona i kontrola Email** | 1. Rozwiązanie musi oferować możliwość trybu pracy Transparent Email Proxy
2. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S.
3. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.
4. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń.
5. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników.
6. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL.
7. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów email.
8. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka.
 |
| **OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY** |
| **On-cloud Sandboxing** | Rozwiązaniem musi dawać możliwość rozbudowy o dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności:1. Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych np., .exe
2. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf.
3. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf.
4. Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym zip, arj, lha, rar, cab
5. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows.
 |
| **LOGOWANIE I RAPORTOWANIE** |
|  | 1. System musi umożliwiać składowanie oraz archiwizację logów.
2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.
3. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.
4. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).
5. Rozwiązanie musi generować raporty w HTML i CSV.
6. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog.
7. System musi zapewniać podgląd wykorzystania łącza internetowego.
8. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP
9. Rozwiązanie musi oferować możliwość zanonimizowania danych.
 |
| **POZOSTAŁE** |
| **Certyfikaty**  | Urządzenie musi posiadać:- certyfikat Common Criteria;- certyfikat ICSA Labs dla funkcji VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE; |
| **GWARANCJA I SERWIS** |
| Wymagania ogólne dla dostarczanych rozwiązań : |
| * Dostarczone urządzenia musza być fabrycznie nowe, nieużywane w innych projektach, nie wycofane z produkcji i pochodzić z legalnego, polskiego kanału dystrybucji.
* Całość dostarczanego sprzętu musi pochodzić z autoryzowanego kanału sprzedaży producentów na teren UE – ze względów gwarancyjnych niedopuszczalne jest dostarczanie sprzętu z tzw. brokerki,
* Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie zapisanym w specyfikacjach sprzętu,
* Całość dostarczonego sprzętu i oprogramowanie musi być ze sobą kompatybilna i pochodzić od jednego producenta,
* Wykonawca winien w momencie dostawy przedłożyć dokumenty potwierdzające, że posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.
 |
| Warunki gwarancji i serwisu : |
| * Na dostarczany sprzęt musi być udzielona **min. 36-miesięczna gwarancja**; Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była wymiana urządzeń zgodnie z metodyką i zaleceniami producenta dostarczonych rozwiązań,
* Wykonawca lub autoryzowany serwis ma obowiązek przyjmowania zgłoszeń serwisowych w języku polskim przez telefon (od poniedziałku do piątku, w godzinach 8-17), e-mail lub WWW (przez całą dobę),
 |
| Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiający:* bezpłatne pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres trwania gwarancji i licencji
* dostęp do dokumentacji sprzętu i oprogramowania,
* dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
* dostęp do pomocy technicznej producenta.

Zamawiający w momencie odbioru otrzyma:* licencje obejmujące wszystkie wymagane moduły na okres **min. 36 miesięcy**
* możliwość automatycznego pobierania subskrypcji dla wszystkich wymaganych modułów w okresie trwania licencji.
 |