**OPIS PRZEDMIOTU ZAMÓWIENIA załącznik nr 1**

na czerwono są dopisane zmiany i wykreślenie wymagań

**Serwer**

1. **Serwer z oprogramowaniem serwerowym – 1 szt.**

|  |  |
| --- | --- |
| **Komponent** | **Opis minimalnych parametrów** |
| Obudowa | Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 3.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.  Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI. |
| Płyta główna | Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera  i oznaczona jego znakiem firmowym. |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| Procesor | Zainstalowany jeden procesor szesnasto-rdzeniowy min. 2.4GHz klasy x86 dedykowany do pracy z zaoferowanym serwerem osiągający wynik minimum  19000 w teście Average CPU Mark opublikowanym na stronie cpubenchmark.net |
| Pamięć RAM | Pamięci o parametrach 32GB DDR4 RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do minimum 1TB pamięci RAM. |
| Gniazda PCIe | Minimum trzy sloty generacji 4 i jeden slot generacji 3. |
| Interfejsy sieciowe/FC/SAS | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT |
| Dyski twarde | Możliwość instalacji dysków SATA, SAS, SSD. zainstalowane dyski: 2x 480GB SSD SATA Hot-Plug Read Intensive oraz 3x 2TB NLSAS 7200obr/min 12Gb/s, możliwość zainstalowania modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego  w dwa nośniki typu flash o pojemności min. 32GB z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| Kontroler RAID | Sprzętowy kontroler dyskowy, posiadający min. 4GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących |
| Wbudowane porty | Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane  dla karty zarządzającej, tylne: min. 1x VGA, min. 1x USB 3.0, min. 1x USB 2.0, min. 2 porty RJ45, port wewnętrzny: min. 1x USB 3.0, dodatkowo jeden dedykowany port RJ45 do karty zarządzającej |
| Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| Wentylatory | Redundantne |
| Zasilacze | Redundantne, Hot-Plug maksymalnie 800W każdy z dedykowanymi przewodami zasilającymi. |
| Bezpieczeństwo | Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą, wbudowany moduł TPM 2.0 |
| System operacyjny | Microsoft Windows Server 2022 Standard lub nowszy |
| Diagnostyka | Możliwość zainstalowania panelu LCD umieszczonego na froncie obudowy, umożliwiającego wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |
| Karta zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego:  zdalny dostęp do graficznego interfejsu Web karty zarządzającej szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika możliwość podmontowania zdalnych wirtualnych napędów wirtualną konsolę z dostępem do myszy, klawiatury wsparcie dla IPv6 wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.  Monitorowanie zużycia dysków SSD możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, automatyczne zgłaszanie alertów do centrum serwisowego producenta automatyczne update firmware dla wszystkich komponentów serwera możliwość przywrócenia poprzednich wersji firmware możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych |
| Gwarancja | Minimum 24 miesięcy gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii ogólnopolską linię telefoniczną producenta.  Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. |
| Minimalne wymagania oprogramowania serwerowego | Minimalne wymagane funkcjonalności:  - możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;  - możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;  - wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;  - możliwość uruchomienia kontrolera domeny będącego w pełni zgodnym z domeną AD pracującą w oparciu o minimum system Windows Server 2008 R2 (poziom funkcjonalności AD DS Windows Server 2008 R2);  - możliwość uruchomienia kontrolera domeny tylko do odczytu;  - możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;  - możliwość uruchomienia serwera usług terminalowych (RemoteApp) zgodnego z min. Windows Server 2008 R2;  - obsługa zdalnego pulpitu;  - możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;  - obsługa PowerShell 4.0;  - obsługa certyfikatów w AD;  - obsługa drzewa katalogowego Microsoft Active Directory. |
| Ilość procesorów fizycznych na które udzielona zostanie licencja na oprogramowanie serwerowe | 1 |
| Ilość rdzeni w procesorach fizycznych na które udzielona zostanie licencja na oprogramowanie serwerowe | 16 |
| Ilość możliwych do uruchomienia maszyn wirtualnych z systemem operacyjnym Windows Server Standard w ramach jednej licencji oprogramowania serwerowego | 2 |
| Licencje dostępowe do oprogramowania serwerowe | Licencje zapewniające dostęp do zasobów serwera. Licencje muszą pozwalać na dostęp dla każdego nazwanego użytkownika. Ilość licencji: 15 |
| Licencje dostępowe do środowiska pulpitu zdalnego | Licencje zapewniające dostęp do pulpitu graficznego systemu operacyjnego Microsoft Windows Server 2022. Licencje muszą pozwalać na dostęp do pulpitu zdalnego dla nazwanych użytkowników. Ilość licencji 5 |
| Przykładowy model | Dell EMC PowerEdge R550 |

1. **Switch 48-portowy zarządzalny – 1 szt.**

|  |  |
| --- | --- |
| Komponent | Opis minimalnych parametrów |
| Architektura sieci LAN | GigabitEthernet |
| Zarządzalny | TAK |
| Liczba portów 1000BaseT (RJ45) | 48 |
| Liczba gniazd SFP+ 10G | 4 |
| Liczba gniazd QSFP+ 40G | 2 |
| Zarządzanie, monitorowanie i konfiguracja | Poprzez interfejs WEB |
| Obsługiwane protokoły i standardy | IEEE 802.1Q |
| Zdolność przełączania | 336Gb/s |
| Rozmiar tablicy adresów MAC | 16000 |
| Warstwa przełączania | L3 |
| System operacyjny | Tryb dual możliwość uruchomienia dedykowane oprogramowania dla funkcji switch a także dla funkcji router |
| Pamięć RAM | 64MB |
| Typ obudowy | Montaż w szafie RACK |
| Gwarancja | Minimum 12 miesięcy gwarancji producenta, łącznie minimum 36 miesięcy gwarancji |
| Przykładowy model | Mikrotik CRS354-48G-4S+2Q+RM |

1. **Zasilacz UPS do szafy RACK**

|  |  |
| --- | --- |
| Komponent | Opis minimalnych parametrów |
| Moc wyjściowa (pozorna / czynna) | 3000 VA |
| 3000 W |
| Architektura UPS-a | On-line |
| Liczba faz na wejściu | 1 (230V) |
| Napięcie | 230 V |
| Liczba akumulatora | 6 |
| Pojemność akumulatorów | 9Ah |
| Napięcie akumulatora | 12V |
| Zabezpieczenia | Przeciwprzepięciowe / przeciwzwarciowe |
| Porty zasilania wejściowe | IEC-C20 |
| Porty zasilania wyjściowe | 8 x IEC-C13 |
| Czas przełączenia (maks.) | 0 ms |
| Czas podtrzymania (obciążenie 100%) | 3.5 min |
| Czas ładowania | 3 h |
| Typ obudowy | Rack |
| Gniazda we/wy | 1 x USB 2.0, 1x RS-232 |
| Wymagania środowiskowe | Temperatura robocza (°C) – 0-40  Sprawność maks. (dla VFI) [%] - 90 |
| Gwarancja | Minimum 24 miesiące gwarancji producenta |
| Przykładowy model | EVER UPS POWERLINE RT PLUS 3000 |

1. **serwer plików NAS – 1szt**.

|  |  |
| --- | --- |
| Typ obudowy | Rack |
| Obsługiwana pojemność | 64 TB |
| Procesor | Min. czterordzeniowy o taktowaniu min. 2,7 GHz osiągający wynik min. 2994 w teście Average CPU Mark na stronie cpubenchmark.net |
| Architektura procesora | 64-bitowy x86 |
| Mechanizm szyfrowania | AES-NI |
| Pamięć RAM | Min. 4 GB DDR4 |
| Maksymalna pojemność pamięci | 8 GB (2 x 4 GB) |
| Gniazdo pamięci | 2 x SO-DIMM DDR4 |
| Pamięć flash | 4 GB (ochrona systemu operacyjnego przed podwójnym rozruchem) |
| Wnęka dysków | 4 dyski 3,5-calowe SATA 6 Gb/s, 3 Gb/s |
| Kompatybilność dysków | 3,5-calowe dyski twarde SATA 2,5-calowe dyski twarde SATA 2,5-calowe dyski SSD SATA |
| RAID | 0, 1, 5, 6, 10, JBOD, Single Disk |
| Rodzaje wyjść / wejść | USB 3.0 – min. 2 szt.  USB 2.0 – min. 2 szt.  RJ-45 2.5GbE (LAN) – min. 2 szt.  HDMI-out – min. 1 szt.  ~~PCIe Gen2 (x2) - min. 2 szt.~~ |
| Protokoły sieciowe | HTTP, HTTPS, iPv4/iPv6, iSCSI, Klient DHCP lub statyczny adres IP, Klient VPN, Obsługa ramek typu jumbo, Przekierowywanie portów UPnP, Serwer CIFS/SMB, Serwer DNS, Serwer DHCP, Serwer DLNA, Serwer FTP, NFS, Serwer VPN, SNMP, SSH, Telnet, Wake-On-LAN, SMTP, SMSC, FTPS, TFTP, WebDAV |
| System plików dla dysków zewnętrznych | FAT32, NTFS, HFS+, EXT3, EXT4 |
| System plików | EXT4 |
| Dodatkowe informacje | Funkcja Wake on LAN/WAN  Obsługa serwera DLNA  Obsługa serwera FTP   |  |  | | --- | --- | | Volume Snapshot |  | | LUN Snapshot |  | | Maximum Snapshot (Per System) | Check maximum number of snapshots of your NAS | | Maximum Snapshot (Per Volume / LUN) | Check maximum number of snapshots of your NAS | | MinimumSnapshotInterval | 5 minutes | | Snapshot Retention Policy |  | | Self-serve Snapshot Recovery |  | | Application Consisted Snapshot |  | | Snapshot Full Clone |  | | Snapshot Replica / Vault  Obsługa przyspieszenia pamięci podręcznej SSD |  | |
| Wskaźniki LED | Zasilanie/stan, LAN, USB, HDD |
| Przyciski | Zasilanie, ~~kopiowanie USB~~, reset |
| Złącze bezpieczeństwa | Kensington |
| System Operacyjny | QTS 5.0.0 (embedded Linux) |
| Wspierane systemy operacyjne klientów | 1. Apple Mac OS 10.10 or later 2. Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 or later Linux 3. IBM AIX 7, Solaris 10 or later UNIX 4. Microsoft Windows 7, 8, 10 and 11 5. Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, and 2019 |
| Autoryzacja domenowa | Microsoft Active Directory (AD) oraz wsparcie dla kontrolera domeny  LDAP serwer i klient  Logowanie użytkownika domeny (AFP, CIFS/SMB, FTP, and File Station) |
| Obsługiwany język | Polski |
| Gwarancja | Minimum 24 miesiące |

1. **Dyski HDD współpracujące z zaproponowanym wyżej modelem serwera plików NAS – 4szt.**

|  |  |
| --- | --- |
| Rodzaj dysku | HDD |
| Pojemność dysku | 10 TB |
| Pamięć podręczna cache | 256 MB |
| Typ dysku | Wewnętrzny |
| Format | 3.5" |
| Interfejs | SATA III (6 Gb/s) |
| Maksymalna prędkość odczytu [MB/s] | 215 |
| Prędkość obrotowa [obr/min] | 7200 |
| Technika zapisywania danych | CMR |
| Gwarancja | Minimum 24 miesiące |

1. **UTM**

|  |  |
| --- | --- |
| **Komponent** | **Opis minimalnych parametrów** |
| Konstrukcja | System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania. Rozwiązanie powinno być wyposażone w moduł kryptoraficzny zgodny ze standardem FIPS 140-2. |
| Tryby pracy | Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca) |
| Możliwość budowy klastra | Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie Active-Passive lub Active-Active. |
| Ilość chronionych hostów | System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej. |
| Przechowywanie danych logów | Rozwiązanie musi być wyposażone w co najmniej jeden dysk SSD służący m.in. do przechowywania logów i raportów bezpośrednio na urządzeniu. |
| Zasilanie | Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy (drugi zasilacz jako wyposażenie opcjonalne). |
| Pamięc wewnętrzna | Zainstalowany dysk SSD minimum 64GB |
| Liczba fizycznych interfejsów 1000Base-T | Minimum 10 |
| Liczba fizycznych interfejsów SFP | Minimum 2 |
| Wydajność Firewall nie mniej niż (Gbps) | 10Gbps |
| Wydajność Firewall IMIX nie mniej niż (Gbps) | 4.7 |
| Wydajność IPS nie mniej niż (Gbps) | 3.3 |
| Liczba równoczesnych połączeń nie mniejsza niż: | 6400000 |
| Liczba nowych połączeń na sekundę nie mniejsza niż: | 74500 |
| Interfejs | Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. |
| Certyfikat SSL interfejsu | Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). |
| Uwierzytelnianie | Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. |
| Diagnostyka | Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter.  Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. |
| Zarządzanie | Rozwiązanie powinno oferować wiersz poleceń dostępny z poziomu graficznego interfejsu administraotra, portu konsolowego oraz za pośrednictwem protokołu SSH z uwierzytelnianiem przy użyciu kluczy RSA, DSA lub ECDSA o długości min. 2048 bitów. |
| Aktualizacja oprogramowania | Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). Informacja o dostępności nowej wersji powinna pojawiać się w Web GUI. Producent powinien oferować mechanizm automatycznego łatania wykrytych w oprogramowaniu systemowym podatności przez tzw. hotfixies, przy czym administrator powinien móc funkcjonalność tą wyłączyć. |
| Zarządzanie licencjami | Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu licencyjnego a synchronizacja subskrypcji powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami. |
| Zarządzanie interfejsami | Rozwiązanie powinno zapewniać możliwość zmiany nazw interfejsów sieciowych. |
| Ochrona IPS | Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur. Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS. Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS. |
| Ochrona ATP (Advanced Threat Protection) | System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet. |
| Zabezpieczenie sieci Web | Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP. |
| Silniki antywirusowe | Rozwiązanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania. Dodatkowo rozwiązanie powinno umożliwiać uruchomienie silnika antywirusowego firmy trzeciej. System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek. |
| Inspekcja ruchu SSL/TLS | Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów. Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2. Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP. Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443). Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web. Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen. |
| Filtr WEB | Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron Web oraz umożliwiać dodawanie własnych kategorii stron. Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól. System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowania treści komunikatu w tym dodania logo organizacji. |
| Lista aplikacji | Rozwiązanie powinno oferować bazę danych opisująca co najmniej 3000 aplikacji. Rozwiązanie powinno umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp. |
| Inne zagrożenia | Sprzęt powinien zapewnić rozwiązanie klasy Sanbox do ochrony przez zadrożeniami typu Zero-Day. Rozwiązanie będzie ofertować statyczną i dynamiczną analizę kody przesyłanego w ramach ruchu web czy email. Rozwiązanie umożliwi dodatkową inspekcję i detonację plików wykonywalnych (.exe, .com, .dll) oraz dokumentów (.doc, .docx, .docm, .rtf), plików PDF a także archiwów. |
| Przykładowy model | Sophos XGS 136 |