**Opis przedmiotu zamówienia**

1. **Serwer NAS A – 2 kompletne urządzenia gotowe do pracy**
2. **Serwer A**
3. **Switch dostępowy A – 18 kompletnych urządzeń gotowych do pracy**
4. **Switch CORE (rdzeniowy) A – 2 kompletne urządzenia gotowe do pracy w klastrze niezawodnościowym**
5. **Router brzegowy A (UTM) – 2 kompletne urządzenia gotowe do pracy w klastrze niezawodnościowym**

|  |  |  |
| --- | --- | --- |
| 1. **Serwer NAS A – 2 kompletne urządzenia gotowe do pracy** | | |
| *Wymagane minimalne parametry techniczne* | | *Oferowane urządzenie*  *…………………………………………….*  *Producent, model* |
| *Parametry oferowane*  *WYPEŁNIA WYKONAWCA* \*/\*\* |
| 1. | Urządzenie w obudowie do montażu w szafie rack 19”, wysokość maksymalnie 2U. W komplecie zestaw szyn umożliwiających wysuwanie serwera do celów serwisowych. | tak/nie |
| 2. | Urządzenie wyposażone w procesor czterordzeniowy 64-bitowy o taktowaniu nie niższym niż 2.2GHz  Minimalna liczba rdzeni procesora – 4 | tak/nie |
| 3. | Obudowa serwera musi mieć możliwość instalacji od frontu minimum 8 dysków | tak/nie |
| 4. | Pamięć RAM Minimum 8GB DDR4 ECC - RAM tego samego producenta, co serwer NAS, w konfiguracji 1 x 8GB.  Pamięć RAM zgodna z listą kompatybilności producenta oferowanego serwera.  Możliwość rozszerzenia RAM do 32GB. | tak/nie |
| 5. | Całkowita liczba gniazd pamięci – minimum 2 | tak/nie |
| 6. | Dyski twarde:  3.5" SATA HDD  Zamawiający wymaga dostarczenia minimum 4 dysków 3.5” SATA HDD o pojemności 8TB każdy o parametrach nie gorszych niż:  Prędkość obrotowa: 7200 RPM  MTTF: 2 500 000  Obciążenie roczne: 550 TB  Gwarancja producenta dysku: 5 lat  Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego serwera.  Dyski zgodne z listą kompatybilności producenta oferowanego serwera. | tak/nie |
| 7. | Wymagana możliwość podłączenia modułu rozszerzającego | tak/nie |
| 8. | Wymagany port na kartę rozszerzeń min. Minimum 1 x Gen3 x8 slot (x4 link) | tak/nie |
| 9. | Porty sieciowe LAN:  Wbudowane min. 4 x RJ-45 1GbE  Dodatkowo min. 2 x SFP+ 10GbE, wraz z wkładkami współpracujące z przełącznikami CORE z dalszej części zamówienia, dodatkowo do wkładek SFP+ należy dołączyć niezbędne przewody światłowodowe do połączenia urządzenia z przełącznikiem CORE o długości min. 3m | tak/nie |
| 10. | Serwer musi posiadać wbudowane porty w ilości przynajmniej:  - min. 2 porty USB 3.2,  - min. 1 port eSATA,  Nie dopuszcza się stosowania rozwiązań typu adaptery, przejściówki lub dodatkowych kart w celu uzyskania wymaganych ilości portów. | tak/nie |
| 11. | Zasilanie:  Wymagany redundantny zasilacz o mocy minimalnej 350W | tak/nie |
| 12. | Wymagany mechanizm szyfrowania sprzętowego min. AES-NI | tak/nie |
| 13. | Wewnętrzny system plików:  EXT4 | tak/nie |
| 14. | Obsługiwane tryby RAID: JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 lub równoważny | tak/nie |
| 15. | Uprawnienia listy kontroli dostępu systemu Windows (ACL) | tak/nie |
| 16. | Usługa katalogowa: Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/FTP/WebDAV/File Station | tak/nie |
| 17. | Bezpieczeństwo:  Obsługa WORM (Write Once Read Many - jeden zapis, wiele odczytów) dla folderów współdzielonych i migawek, zapora sieciowa, szyfrowanie folderu współdzielonego, szyfrowanie całego woluminu, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania), dwuetapowa weryfikacja logowania (2FA), adaptacyjna metoda logowania dla konta administratora (AMFA), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail. | tak/nie |
| 18. | Oferowany serwer powinien mieć oprogramowanie do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów.  Minimalne wymagane funkcje oprogramowania do backupu:  - kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal,  - kopia zapasowa środowisk MacOS  - kopia zapasowa maszyn wirtualnych (VMware, Hyper-V)  - kopia zapasowa serwerów fizycznych (Windows, Linux)  - obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania,  - obsługa wielu wersji i retencji,  - możliwość wyzwalania kopii zapasowej według harmonogramu,  - obsługa klastra przełączania awaryjnego Microsoft Hyper-V,  - automatyczna weryfikacja utworzonych kopii zapasowych maszyn wirtualnych i serwerów fizycznych, za pomocą utworzonego nagrania wideo z odtworzenia w formie maszyny wirtualnej,  - centralne zarządzanie,  - konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań,  - portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora),  - delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora,  - kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace  Zgodność współpracy oprogramowania do kopii zapasowej z oferowanym serwerem, potwierdzona przez producenta serwera. | tak/nie |
| 19. | Oprogramowanie:   * Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych, 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 * 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. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników. * Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego. * Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync * Obsługa minimum 1024 migawek na folder współdzielony i minimum 65000 migawek na cały system   Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 40jednoczesnych połączeń | tak/nie |
| 20. | Zamawiający wymaga, aby serwery NAS posiadały **2-letni serwis gwarancyjny** świadczony przez Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. | tak/nie |

|  |  |  |
| --- | --- | --- |
| 1. **Serwer A** | | |
| *Wymagane minimalne parametry techniczne* | | *Oferowane urządzenie*  *…………………………………………….*  *Producent, model* |
| *Parametry oferowane*  *WYPEŁNIA WYKONAWCA* \*/\*\* |
| 1. | Urządzenie w obudowie do montażu w szafie rack 19”, wysokość maksymalnie 1RU. W komplecie zestaw szyn umożliwiających wysuwanie serwera do celów serwisowych. | tak/nie |
| 2. | Obudowa serwera musi posiadać dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera | tak/nie |
| 3. | Obudowa serwera musi mieć możliwość instalacji od frontu minimum 10 dysków 2.5” HotPlug. | tak/nie |
| 4. | Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | tak/nie |
| 5. | Chipset dedykowany przez producenta procesora do pracy w serwerach | tak/nie |
| 6. | Zainstalowany min. jeden procesor min. 16-rdzeniowy, 32 wątki, dedykowany do pracy z zaoferowanym serwerem, pracujące z prędkością min. 3.0GHz oraz min. 3.6GHz w trybie zapotrzebowania na podwyższoną wydajność, posiadający pamięć cache o wielkości min. 64MB, osiągający w teście PassMark dostępnym na stronie https://www.cpubenchmark.net/ wynik nie mniejszy niż 44.000. | Model procesora:  *……………………………………*  *(podać model oferowanego procesora)* |
| 7. | Urządzenie wyposażone w minimum 256GB pamięci RAM typu RDIMM o częstotliwości pracy 5600MHz w modułach 64GB każdy. Na płycie głównej powinna znajdować się wolna ilość slotów przeznaczonych dla pamięci w ilości umożliwiającej rozbudowę o dodatkowe co najmniej 512GB RAM. | Ilość pamięci RAM (GB):  *……………………………………*  *(podać wielkość oferowanej pamięci)* |
| 8. | Wymagana zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024. | tak/nie |
| 9. | Urządzenie musi posiadać min. 2 sloty PCI Express min. generacji 4 o prędkości x16 | tak/nie |
| 10. | Serwer musi posiadać wbudowane porty w ilości przynajmniej:  - 3 porty USB (z czego minimum 1 w technologii 3.0),  - 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym),  Nie dopuszcza się stosowania rozwiązań typu adaptery, przejściówki lub dodatkowych kart w celu uzyskania wymaganych ilości portów. | tak/nie |
| 11. | Serwer musi posiadać następujące interfejsy sieciowe Ethernet: | |
| przynajmniej 2 interfejsy 1GbE w standardzie BaseT zintegrowane na płycie głównej  przynajmniej 2 interfejsy sieciowe 25GbE w standardzie SFP28  Dla każdego portu SFP28 należy dostarczyć kabel podłączeniowy o długości 3m przystosowany do pracy z przełącznikami CORE z dalszej części zamówienia oraz wkładki 25GbE współpracujące z przełącznikami CORE z dalszej części zamówienia | Model:  *……………………………………*  *(podać model / kod oferowanej karty)* |
| 12. | Zainstalowany kontroler dedykowany przez producenta serwera obsługujący poziomy RAID 0, 1, 5, 6, 10, 50, 60 oraz do min. 10 dysków twardych o prędkości min. 6Gb/s SATA i min. 12Gb/s SAS, wyposażony w min. 8GB pamięci cache z podtrzymaniem bateryjnym i wsparciem funkcjonalności write back, write through, no read Ahead, and read Ahead. | Model:  *……………………………………*  *(podać model / kod oferowanej karty)* |
| 13. | Zainstalowane minimum sześć dysków Hot-Plug SAS 12 Gb/s, każdy o pojemności przynajmniej 2.4TB.  Dyski muszą być oznaczone logo producenta serwera | Ilość dysków:  *……………………………………*  *(wpisać ilość dysków)*  Pojemność jednego dysku:  *……………………………………*  *(wpisać pojemność)* |
| 14. | Zainstalowane minimum cztery dyski Hot-Plug SATA SSD 6 Gb/s, każdy o pojemności przynajmniej 1.92TB.  Dyski muszą być oznaczone logo producenta serwera | Ilość dysków:  *……………………………………*  *(wpisać ilość dysków)*  Pojemność jednego dysku:  *……………………………………*  *(wpisać pojemność)* |
| 15. | Płyta główna musi być wyposażona w zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). Musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera. | tak/nie |
| 16. | Zainstalowane redundantne zasilacze Hot-Plug klasy Platinum o mocy min. 700W każdy. | tak/nie |
| 17. | Musi posiadać redundantne wentylatory Hot-Plug zapewniające bezpieczne warunki pracy | tak/nie |
| 18. | Wymagane posiadanie przynajmniej następujących funkcjonalności z zakresu bezpieczeństwa:  - panel LCD i/lub LED umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze,  - zintegrowany z płytą główną moduł TPM,  - wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą,  - fabryczne oznaczenie urządzenia, wykonane przez producenta serwera informujące Zamawiającego m.in. o numerze serwisowym serwera, pełnej nazwie podmiotu Zamawiającego, modelu serwera,  - fizyczne zabezpieczenie dedykowane przez producenta serwera uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników. | tak/nie |
| 20. | Musi posiadać kartę zarządzającą niezależną od zainstalowanego systemu operacyjnego, zintegrowaną z płytą główną lub jako dodatkowa karta rozszerzeń (Zamawiający dopuszcza zastosowanie karty instalowanej w slocie PCI Express jednak nie może ona powodować zmniejszenia minimalnej ilości wymaganych slotów w serwerze), posiadającą minimalną funkcjonalność:  - dedykowany port RJ45,  - zdalny dostęp do graficznego interfejsu Web karty zarządzającej,  - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera),  - szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika,  - możliwość podmontowania zdalnych wirtualnych napędów,  - wirtualną konsolę z dostępem do myszy, klawiatury,  - wsparcie dla Ipv6,  - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, VLAN tagging, Telnet, SSH,  - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer,  - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer,  - integracja z Active Directory,  - możliwość obsługi przez dwóch administratorów jednocześnie,  - wsparcie dla dynamic DNS,  - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej,  - możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy,  - monitorowanie zużycia dysków SSD  - możliwość monitorowania z jednej konsoli min. 50 serwerów fizycznych,  - automatyczne zgłaszanie alertów do centrum serwisowego producenta  - automatyczne update firmware dla wszystkich komponentów serwera  - możliwość przywrócenia poprzednich wersji firmware  - automatyczne przywracanie ustawień serwera, kart sieciowych, BIOS, wersji firmware’u w przypadku awarii i wymiany któregoś z komponentów z dedykowanej pamięci flash (w tym kontrolera RAID, kart sieciowych, płyty głównej) | tak/nie  *……………………………………*  *(podać model / kod oferowanej karty)* |
| 21. | Wraz z serwerem należy dostarczyć oprogramowanie zarządzające umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:  - możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;  - wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH;  - możliwość oskryptowywania procesu wykrywania urządzeń;  - możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;  - szczegółowy opis wykrytych systemów oraz ich komponentów;  - możliwość eksportu raportu do CSV, HTML, XLS;  - grupowanie urządzeń w oparciu o kryteria użytkownika;  - automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń;  - szybki podgląd stanu środowiska;  - podsumowanie stanu dla każdego urządzenia;  - szczegółowy status urządzenia/elementu/komponentu;  - generowanie alertów przy zmianie stanu urządzenia;  - filtry raportów umożliwiające podgląd najważniejszych zdarzeń;  - integracja z service desk producenta dostarczonej platformy sprzętowej;  - możliwość przejęcia zdalnego pulpitu;  - możliwość podmontowania wirtualnego napędu;  - kreator umożliwiający dostosowanie akcji dla wybranych alertów;  - możliwość importu plików MIB;  - przesyłanie alertów „as-is” do innych konsol firm trzecich;  - aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);  - możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta;  - możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;  - moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych. | tak/nie |
| 22. | Urządzenie musi posiadać certyfikat CE oraz certyfikat zgodności z dyrektywą RoHS lub równoważne. | tak/nie |
| 23. | Zamawiający wymaga, aby serwer posiadał **3-letni serwis gwarancyjny** świadczony przez Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanego urządzenia.  Gwarancja z wymianą lub naprawą na następny dzień roboczy od zgłoszenia usterki w miejscu użytkowania sprzętu u Zamawiającego.  Wymagane zachowanie dysków twardych przy wymianie gwarancyjnej u Zamawiającego. Możliwość samodzielnego pobierania bezpłatnych aktualizacji i nowych wersji oprogramowania oraz bezpośredni kontakt z inżynierami wsparcia technicznego producenta w języku polskim. Możliwość zgłaszania awarii w trybie 24x7x365 z pominięciem dostawcy poprzez ogólnopolską linię telefoniczną producenta w języku polskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | tak/nie  *……………………………………*  *(wpisać rodzaj lub kod oferowanej gwarancji)* |
| 24. | Wymagana dokumentacja w języku polskim lub angielskim. | tak/nie |
| 25. | Serwer należy dostarczyć wraz z kablami zasilającymi IEC320 C13 o długości przynajmniej 1.5m. | tak/nie |
| 26. | Certyfikaty | |
| Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. | tak/nie |
| Serwer musi posiadać deklarację CE. | tak/nie |
| Producent serwera nie może pochodzić z kraju objętego sankcjami dowolnego członka NATO. | tak/nie |

|  |  |  |
| --- | --- | --- |
| 1. **Switch dostępowy A – 18 kompletnych urządzeń gotowych do pracy** | | |
| *Wymagane minimalne parametry techniczne dla 1 urządzenia* | | *Oferowane urządzenie*  *…………………………………………….*  *Producent, model* |
| *Parametry oferowane*  *WYPEŁNIA WYKONAWCA* \*/\*\* |
| 1. | Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej. | tak/nie |
| 2. | **Wymagane parametry fizyczne:**   * możliwość montażu w stelażu/szafie 19” * wysokość maksymalna 1U * minimum jeden wewnętrzny zasilacz 230V AC * zakres temperatur pracy ciągłej co najmniej od -5 °C do +50 °C * zakres wilgotności pracy co najmniej 5% - 95% * głębokość urządzenia maksymalnie 24 cm (z racji ograniczonego miejsca w szafach teleinformatycznych Zamawiający nie dopuszcza urządzenie o większej głębokości niż 24 cm) | tak/nie |
| 3. | **Przełącznik musi posiadać minimum:**   * 48 portów 10/100/1000BASE-T PoE+ zgodne z IEEE 802.3at * 4 porty 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 1G-SX, 1G-LX, moduły 1G DWDM i CWDM, moduły 10G DWDM i CWDM * 2 dedykowane porty do łączenia przełączników w stos. Porty nie mogą być współdzielone z wymaganymi 4 portami 10GE SFP+ * Port konsoli RS232/RJ45 * Port USB umożliwiający podłączenie zewnętrznej pamięci flash * Z racji ograniczonego miejsca w szafach teleinformatycznych nie ma fizycznego dostępu do „tyłu” urządzenia dlatego wszystkie powyższe porty muszą być dostępne od frontu urządzenia. | tak/nie |
| 4. | * Maksymalny pobór mocy przez przełącznik (bez uwzględniania urządzeń PD): 100W * Budżet mocy (łączna moc dostarczana przez urządzenie PSE) nie mniejszy niż 350W. | tak/nie |
| 5. | **Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:**   * Zarządzanie stosem poprzez jeden adres IP * Do min. 9 jednostek w stosie * Magistrala stackująca o wydajności minimum 48Gb/s * Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation) * Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree | tak/nie |
| 6. | Układ przełączający o wydajności min. 224 Gbps, wydajność przełączania przynajmniej 160 Mpps | tak/nie |
| 7. | Obsługa min. 32 000 adresów MAC | tak/nie |
| 8. | Wbudowana pamięć RAM min. 2GB | tak/nie |
| 9. | Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1GB | tak/nie |
| 10. | Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ) | tak/nie |
| 11. | Możliwość skonfigurowania min. 1023 interfejsów vlan interface SVI działających równocześnie | tak/nie |
| 12. | Obsługa ramek jumbo o wielkości min. 9200 bajtów | tak/nie |
| 13. | Obsługa mechanizmów ERPS: G.8032 v1 G.8032 v2 | tak/nie |
| 14. | Obsługa protokołu BFD oraz LACP | tak/nie |
| 15. | Obsługa protokołu HSRP IPv4 i IPv6 lub VRRP IPv4 i IPv6 | tak/nie |
| 16. | Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP). Wymagane wsparcie dla min. 63 instancji protokołu MSTP. Wsparcie dla mechanizmu PVST lub równoważnego (innego niż wymagany standard STP/RSTP/MSTP) | tak/nie |
| 17. | Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania | tak/nie |
| 18. | Obsługa min. 4 000 tras dla routingu IPv4 | tak/nie |
| 19. | Obsługa min. 1 000 tras dla routingu IPv6 | tak/nie |
| 20. | **Obsługa protokołów związanych z obsługą ruchu typu multicast:**   * IGMP v1, v2 i v3 * IGMP Snooping v1, v2 i v3 * PIM-SM, PIM-DM, PIM-SSM | tak/nie |
| 21. | Minimalny rozmiar tablicy ARP 2 048 wpisów | tak/nie |
| 22. | Obsługa wirtualnych tablic routingu-forwardingu (VRF) minimum 60 | tak/nie |
| 23. | Obsługa protokołów LLDP i LLDP-MED | tak/nie |
| 24. | Przełącznik musi być zgodny z IEEE 802.3az | tak/nie |
| 25. | Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client | tak/nie |
| 26. | **Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:**   * min. 4 poziomy dostępu administracyjnego poprzez konsolę * autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL * obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 2000 reguł ACL * możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC * zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 i SSHv2 * możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP * obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard * obsługa mechanizmów związanych z ochroną protokołu STP: BPDU Protection, Root Protection, Loop Protection * możliwość synchronizacji czasu zgodnie z NTP IPv4 i IPv6 * możliwość uwierzytelnienia wielu użytkowników na jednym porcie z możliwością przydzielenia różnych VLANów dla każdego użytkownika z osobna | tak/nie |
| 27. | **Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:**   * klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP * wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR | tak/nie |
| 28. | Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania | tak/nie |
| 29. | **Wymagane opcje zarządzania:**   * możliwość lokalnej obserwacji ruchu na określonym porcie * plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC) * możliwość zarządzania urządzeniem z wykorzystaniem protokołu Netconf/Yang lub RESTCONF * wsparcie dla skyptów python uruchamianych na urządzeniu * wsparcie dla RMON | tak/nie |
| 30. | Przełącznik musi mieć opcję szybkiego przywrócenie konfiguracji do poprzedniej wersji (tzw. funkcjonalność rollback). Przywrócenie konfiguracji do poprzedniej wersji nie może wymagać restartu urządzenia (całego bądź częściowego) bądź ręcznego odwoływania konfiguracji. Administrator systemu musi mieć możliwość utworzenia znacznika/etykiety dla danej konfiguracji tak aby podczas wykonywania procesu przywrócenia można było wskazać ustawiony wcześniej znacznik/etykietę jako punkt do którego ma zostać przywrócona konfiguracja. | tak/nie |
| 31. | **Wraz z urządzeniami muszą zostać dostarczone:**   * pełna dokumentacja w języku polskim lub angielskim * dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana * Wkładka SFP+ 10GbE * Patchcord światłowodowy połączeniowy wkładkę z przełącznicą światłowodową | tak/nie |
| 32. | Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy | tak/nie |
| 33. | Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski | tak/nie |
| 34. | Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń | tak/nie |
| 35. | Zamawiający wymaga, aby przełączniki **posiadały 3-letni serwis** gwarancyjny świadczony przez Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).  W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca/autoryzowany serwis producenta musi posiadać status autoryzowanego partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim. | tak/nie |
| 36. | **Montaż oraz konfiguracja**   * wymaga się montażu urządzeń w istniejącej szafie rack Zamawiającego * wymaga się wykonanie konfiguracji dostarczanych urządzeń w celu uzyskania klastra niezawodnościowego oraz połączenie z dostarczaną i istniejącą infrastrukturą sieciową Zamawiającego | tak/nie |
| 37. | **Wykonawca zobowiązany jest do wykonania dokumentacji powykonawczej zawierającej następujące dane:**   * schemat połączeń * wykaz adresacji IP * informacja dot. Autoryzacji do poszczególnych urządzeń – zawarta oraz przekazana w szyfrowanym pliku np. w oprogramowaniu Keepass * informacja dot. Autoryzacji do portalu producenta sprzętu sieciowego – zawarta oraz przekazana w szyfrowanym pliku np. w oprogramowaniu Keepass * wykonanie pełnego backupu urządzeń oraz przekazanie na wymiennym nośniku pamięci | tak/nie |

|  |  |  |
| --- | --- | --- |
| 1. **Switch CORE (rdzeniowy) A – 2 kompletne urządzenia gotowe do pracy w klastrze niezawodnościowym** | | |
| *Wymagane minimalne parametry techniczne dla 1 urządzenia* | | *Oferowane urządzenie*  *…………………………………………….*  *Producent, model* |
| *Parametry oferowane*  *WYPEŁNIA WYKONAWCA* \*/\*\* |
| 1. | Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack oraz stworzenie klastra niezawodnościowego HA 100GE QSFP28. Przełącznik musi posiadać system operacyjny (firmware) dostarczony przez producenta urządzenia; zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej. | tak/nie |
| 2. | **Wymagane parametry fizyczne:**   * możliwość montażu w stelażu/szafie 19” * dwa wewnętrzne redundantne zasilacze 230V AC typu hot-swap (nie dopuszcza się rozwiązania zewnętrznego). Każde urządzenie musi zostać dostarczone z 2 zasilaczami umożliwiające wymianę w trakcie pracy urządzenia (ang. hot-swap). * Wysokość maksymalna 1U * zakres temperatur pracy ciągłej co najmniej od -5 do +45 °C * zakres wilgotności pracy co najmniej 5% - 95% * port USB umożliwiający podłączenie zewnętrznej pamięci flash * MTBF: minimum 40 lat * maksymalny pobór mocy: 400W * waga urządzenia nie większa niż 10kg | tak/nie |
| 3. | **Przełącznik musi zostać dostarczony z następującymi interfejsami mogącymi działać równocześnie:**   * 24 porty 10/100/1000BASE-T * 16 portów 10GE SFP+ * 8 portów 25GE SFP28 * 2 porty 100GE QSFP28 * Wszystkie interfejsy 10G/25G, 40G/100G muszą być dostępne z przodu obudowy. * Przełącznik musi umożliwiać obsługę modułów firm 3cich bez utraty gwarancji na urządzenie. | tak/nie |
| 4. | Układ przełączający o wydajności min. 2.3 Tbps, wydajność przełączania przynajmniej 450 Mpps | tak/nie |
| 5. | Obsługa min. 256 000 adresów MAC | tak/nie |
| 6. | Wbudowana pamięć RAM min. 4 GB | tak/nie |
| 7. | Procesor wielordzeniowy | tak/nie |
| 8. | Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 2 GB | tak/nie |
| 9. | Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ) | tak/nie |
| 10. | Możliwość skonfigurowania min. 1023 interfejsów vlan interface SVI działających równocześnie | tak/nie |
| 11. | Możliwość tworzenie połączeń agregowanych (link aggregation). | tak/nie |
| 12. | Obsługa ramek jumbo o wielkości min. 9216 bajtów | tak/nie |
| 13. | Obsługa mechanizmów ERPS: G.8032 v1 G.8032 v2 | tak/nie |
| 14. | Obsługa protokołu BFD oraz LACP | tak/nie |
| 15. | Obsługa protokołu VRRP dla IPv4 i IPv6 | tak/nie |
| 16. | Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP). Wymagane wsparcie dla min. 63 instancji protokołu MSTP. Wsparcie dla mechanizmu PVST lub równoważnego (innego niż wymagany standard STP/RSTP/MSTP) | tak/nie |
| 17. | Obsługa Multi-Switch Link Access Group, umożliwiającej realizację połączenia urządzenia dostępowego do dwóch niezależnych przełączników bez wykorzystania protokołu STP. | tak/nie |
| 18. | Obsługa min. 128 000 tras dla routingu IPv4 | tak/nie |
| 19. | Obsługa min. 64 000 tras dla routingu IPv6 | tak/nie |
| 20. | Wsparcie dla mechanizmu ECMP (ang. Equal Cost Multi-Path) z obsługą minimum 32 tras w pojedynczej grupie. | tak/nie |
| 21. | Obsługa protokołów routingu OSPF, OSPFv3, IS-IS, IS-ISv6, BGPv4, BGPv4+, RIP, RIPng, PIM-SM, PIM-DM i SSM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania | tak/nie |
| 22. | Obsługa min. 1023 wirtualnych tablic routingu-forwardingu (VRF) | tak/nie |
| 23. | Obsługa protokołów CDP lub LLDP | tak/nie |
| 24. | Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client. | tak/nie |
| 25. | **Obsługa ruchu multicast:**   * IGMP v1, v2 i v3 * IGMP Snooping v1, v2 i v3 | tak/nie |
| 26. | **Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:**   * min. 2 poziomy dostępu administracyjnego poprzez konsolę * autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL * możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC * wsparcie mechanizmu Private VLAN lub równoważnego * obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 4000 reguł ACL * zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 i SSHv2 * możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP * obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard * obsługa mechanizmów związanych z ochroną protokołu STP: BPDU Protection, Root Protection, Loop Protection * możliwość synchronizacji czasu zgodnie z NTP lub SNTP dla IPv4 i IPv6 * możliwość uwierzytelnienia wielu użytkowników na jednym porcie z możliwością przydzielenia różnych VLANów dla każdego użytkownika z osobna | tak/nie |
| 27. | Minimalny rozmiar tablicy ARP 64 000 wpisów | tak/nie |
| 28. | **Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:**   * klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP * wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ | tak/nie |
| 29. | **Wymagane opcje zarządzania:**   * możliwość lokalnej obserwacji ruchu na określonym porcie * plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC) * możliwość zarządzania urządzeniem z wykorzystaniem protokołu Netconf/Yang lub RESTCONF * wsparcie dla skyptów python uruchamianych na urządzeniu * wsparcie dla RMON * dedykowany port konsoli, zgodny ze standardem RS-232 * dedykowany port zarządzający Ethernet 10/100Base-T | tak/nie |
| 30. | Wsparcie dla funkcjonalności VXLAN L2 i L3. Jeżeli obsługa powyżej funkcjonalności wymaga dodatkowej licencji to w ramach niniejszego postępowania Zamawiający wymaga jej dostarczenia. | tak/nie |
| 31. | Przełącznik musi mieć opcję szybkiego przywrócenie konfiguracji do poprzedniej wersji (tzw. funkcjonalność rollback). Przywrócenie konfiguracji do poprzedniej wersji nie może wymagać restartu urządzenia (całego bądź częściowego) bądź ręcznego odwoływania konfiguracji. Administrator systemu musi mieć możliwość utworzenia znacznika/etykiety dla danej konfiguracji tak aby podczas wykonywania procesu przywrócenia można było wskazać ustawiony wcześniej znacznik/etykietę jako punkt do którego ma zostać przywrócona konfiguracja. | tak/nie |
| 32. | **Wraz z urządzeniami muszą zostać dostarczone:**   * pełna dokumentacja w języku polskim lub angielskim * dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE) * do przełącznika należy dodać wkładki SFP, SFP28, QSFP28 w ilości oferowanych portów przez przełącznik * wszystkie niezbędne przewody połączeniowe światłowodowe dla infrastruktury światłowodowej jednomodowej. | tak/nie |
| 33. | **Montaż oraz konfiguracja:**   * wymaga się montażu urządzeń w istniejącej szafie rack Zamawiającego * wymaga się wykonanie konfiguracji dostarczanych urządzeń w celu uzyskania klastra niezawodnościowego oraz połączenie z dostarczanymi i posiadanymi przełącznikami dostępowymi | tak/nie |
| 34. | **Połączenie pomiędzy dwoma switchami rdzeniowymi:**   * wymaga się połączenia pomiędzy urządzeniami o prędkości 100GE * Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja oraz dodatkowy osprzęt to należy je dostarczyć w ramach niniejszego postępowania | tak/nie |
| 35. | Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy | tak/nie |
| 36. | Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski | tak/nie |
| 37. | Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancyjny urządzeń | tak/nie |
| 38. | Zamawiający wymaga, aby przełączniki posiadały **3-letni serwis gwarancyjny** świadczony przez Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).  W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca/autoryzowany serwis producenta musi posiadać status autoryzowanego partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim. | tak/nie |
| 39. | **Wykonawca zobowiązany jest do wykonania dokumentacji powykonawczej zawierającej następujące dane:**   * schemat połączeń * wykaz adresacji IP * informacja dot. Autoryzacji do poszczególnych urządzeń – zawarta oraz przekazana w szyfrowanym pliku np. w oprogramowaniu Keepass * informacja dot. Autoryzacji do portalu producenta sprzętu sieciowego – zawarta oraz przekazana w szyfrowanym pliku np. w oprogramowaniu Keepass * wykonanie pełnego backupu urządzeń oraz przekazanie na wymiennym nośniku pamięci | tak/nie |
| 40. | Producent oferowanych urządzeń musi znajdować się w kwadracie „Leaders” raportu Gartner pt. „Magic Quadrant for Enterprise Wired and Wireless LAN” w roku 2024 r. lub równoważnym. Jako ranking równoważny Zamawiający uzna ranking klasyfikujący rozwiązania enterprise przewodowych i bezprzewodowych sieci LAN, prowadzony i publikowany przez podmiot niezależny od producentów tych rozwiązań. Zamawiający wymaga, aby ranking taki był aktualizowany w okresach nie dłuższych niż 1 rok. Podstawą do sporządzenia raportów muszą być badania polegające na sprawdzeniu jakości oferowanych usług i rozwiązań. Ocena jest prowadzona według kryteriów dotyczących kompletności wizji oferowanych usług, rozwiązań oraz prognoz na przyszłość w tym segmencie rynku oraz zdolności ich realizacji do wdrożenia, są to możliwości finansowe, biznesowe i organizacyjne. Wynik oceny wyznacza miejsce w rankingu, w którym znajduje się konkretny dostawca i jego rozwiązanie. Ranking musi uwzględniać co najmniej 4 kategorie, każda z nich ma określać jaką rolę na rynku spełnia dane rozwiązanie/dostawca.  Liderzy – najwyższa kategoria gdzie znajdują się liderzy/producenci danego rozwiązania.  Kandydaci – pretendenci pozostający bardzo wysoko w rankingu ze względu na swoje działania i potencjał do dominacji na rynku w którym działa.  Wizjonerzy- firmy rozwiązania posiadający wizję możliwości rynkowych, jednak poprzez realizowane działania nie są oni skuteczni na rynku.  Niszowi gracze – rozwiązania skupiające się na niewielkiej części rynku lub nie mających możliwości innowacyjnych do osiągnięcia większych sukcesów rynkowych.  Ranking równoważny nie może być wystawiony przez Wykonawcę lub podmiot zależny od Wykonawcy | tak/nie |

|  |  |  |
| --- | --- | --- |
| 1. **Router brzegowy A (UTM) – 2 kompletne urządzenia gotowe do pracy w klastrze niezawodnościowym** | | |
| *Wymagane minimalne parametry techniczne dla 1 urządzenia* | | *Oferowane urządzenie*  *…………………………………………….*  *Producent, model* |
| *Parametry oferowane*  *WYPEŁNIA WYKONAWCA* \*/\*\* |
| 1. | **Wymagania ogólne:**   * System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. * System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. * System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. * Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. * System wspiera protokoły IPv4 oraz IPv6 w zakresie: * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego | tak/nie |
| 2. | **Redundancja, monitoring i wykrywanie awarii:**   * W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. * Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. * Monitoring stanu realizowanych połączeń VPN. * System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych | tak/nie |
| 3. | **Interfejsy, Dysk, Zasilanie:**   * System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: * 10 portami Gigabit Ethernet RJ-45. * 8 gniazdami SFP 1 Gbps. * 4 gniazdami SFP+ 10 Gbps. * System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. * System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. * System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności fizycznej min. 480GB na potrzeby wymagających tego funkcji np. DLP, Antywirus, Proxy, Lokalnego przechowywanie bieżących log-ów. * System jest wyposażony w zasilanie AC. | tak/nie |
| 4. | **Parametry wydajnościowe:**   * W zakresie Firewall’a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę. * Przepustowość Stateful Firewall: nie mniej niż 39 Gbps dla pakietów 512 B. * Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. * Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 33 Gbps. * Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 5 Gbps. * Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.5 Gbps. * Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps. | tak/nie |
| 5. | **Funkcje Systemu Bezpieczeństwa:**  W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   * Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. * Kontrola Aplikacji. * Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. * Ochrona przed malware. * Ochrona przed atakami - Intrusion Prevention System. * Kontrola stron WWW. * Kontrola zawartości poczty – Antyspam dla protokołów SMTP. * Zarządzanie pasmem (QoS, Traffic shaping). * Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). * Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. * Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. * Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. * Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). | tak/nie |
| 6. | **Polityki, Firewall**   * Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. * System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP. * W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. * Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. * Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. * Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. * Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. * Amazon Web Services (AWS). * Microsoft Azure. * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. * Kubernetes. | tak/nie |
| 7. | **Połączenia VPN**   * System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19, 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site. * System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. | tak/nie |
| 8. | **Routing i obsługa łączy WAN**  W zakresie routingu rozwiązanie zapewnia obsługę:   * Routingu statycznego. * Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. * Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. * ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. * BFD (Bidirectional Forwarding Detection). * Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. | tak/nie |
| 9. | **Funkcje SD-WAN**   * System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. * SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). | tak/nie |
| 10. | **Zarządzanie pasmem**   * System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. * System daje możliwość określania pasma dla poszczególnych aplikacji. * System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. * System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL | tak/nie |
| 11. | **Ochrona przed malware:**   * Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). * Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. * W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. * System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. * System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). * Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. * System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. * Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. * Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. | tak/nie |
| 12. | **Ochrona przed atakami**   * Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. * System chroni przed atakami na aplikacje pracujące na niestandardowych portach. * Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. * System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. * Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). * Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. * Wykrywanie i blokowanie komunikacji C&C do sieci botnet. * Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. | tak/nie |
| 13. | **Kontrola aplikacji**   * Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. * Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. * Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. * Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. * Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). * System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). | tak/nie |
| 14. | **Kontrola WWW**   * Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. * W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. * Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. * Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. * Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). * Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. * Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. * Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. * System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. | tak/nie |
| 15. | **Uwierzytelnianie użytkowników w ramach sesji**   * System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. * System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. * System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. * Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. | tak/nie |
| 16. | **Zarządzanie**   * Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. * Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. * Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. * System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. * System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. * Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. * Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. * Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). * Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. | tak/nie |
| 17. | **Logowanie**   * Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. * W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. * Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. * Możliwość włączenia logowania per reguła w polityce firewall. * System zapewnia możliwość logowania do serwera SYSLOG. * Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. | tak/nie |
| 18. | **Testy wydajnościowe oraz funkcjonalne**  Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni. | tak/nie |
| 19. | **Serwisy i licencje**  Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:  Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na **okres 60 miesięcy**. | tak/nie |
| 20. | **Gwarancja oraz wsparcie**  System jest objęty serwisem gwarancyjnym producenta przez **okres 60 miesięcy**, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. | tak/nie |
| 21. | Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. | tak/nie |
| 22. | Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym. | tak/nie |
| 23. | **Wraz z urządzeniami muszą zostać dostarczone:**   * pełna dokumentacja w języku polskim lub angielskim * dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE) * wszystkie niezbędne przewody połączeniowe światłowodowe dla infrastruktury światłowodowej jednomodowej. | tak/nie |
| 24. | **Montaż oraz konfiguracja**   * wymaga się montażu urządzeń w istniejącej szafie rack Zamawiającego * wymaga się wykonanie konfiguracji dostarczanych urządzeń w celu uzyskania klastra niezawodnościowego oraz połączenie z dostarczanymi i posiadanymi przełącznikami rdzeniowymi oraz urządzeniami operatora dostawcy usług internetowych * Wymaga się wykonania pełnej konfiguracji urządzeń w klastrze niezawodnościowym oraz dostosowanie do istniejącej konfiguracji obecnie zainstalowanych UTM tj. CISCO FirePower 3105, StormShield SN710 | tak/nie |
| 25. | Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancyjny urządzeń | tak/nie |
| 26. | Wykonawca zobowiązany jest do wykonania dokumentacji powykonawczej zawierającej następujące dane:  - schemat połączeń  - wykaz adresacji IP  - informacja dot. Autoryzacji do poszczególnych urządzeń – zawarta oraz przekazana w szyfrowanym pliku np. w oprogramowaniu Keepass  - informacja dot. Autoryzacji do portalu producenta sprzętu sieciowego – zawarta oraz przekazana w szyfrowanym pliku np. w oprogramowaniu Keepass  - wykonanie pełnego backupu urządzeń oraz przekazanie na wymiennym nośniku pamięci | tak/nie |

*\* Wykonawca pozostawia właściwą odpowiedź "tak" lub "nie" przy pytaniach wyboru.  
\*\* W przypadku konieczności wypełnienia pól Wykonawca wpisuje zaproponowane rozwiązanie*

Jeżeli oferowany sprzęt spełnia wyższe wymagania – Wykonawca wpisuje oferowany parametr.

Jeżeli zaproponowane urządzenie spełnia wymagane parametry techniczne poprzez instalację dodatkowych kart rozszerzeń/modułów czy opcji gwarancyjnych (niebędących na wyposażeniu standardowym) należy je wyszczególnić przy pozycji oraz wpisać model lub symbol tego elementu.

Niespełnienie wszystkich minimalnych parametrów lub funkcji, podanych w rubryce „Wymagane minimalne parametry techniczne” spowoduje odrzucenie oferty.

Wykonawca oświadcza, że oferowane powyżej urządzenia są kompletne i po uruchomieniu będą gotowe do pracy, bez żadnych dodatkowych zakupów i inwestycji.