****

Załącznik nr 2 – formularz ofertowy techniczny

Dotyczy: postępowania**: Przyspieszenie procesów cyfryzacji w Specjalistycznym Szpitalu Wojewódzkim w Ciechanowie**

Numer pozycji/części: 5

**ZESTAWIENIE PARAMETRÓW GRANICZNYCH (ODCINAJĄCYCH)**

Przedmiot przetargu: **Pakiet V- Działania zwiększające poziom cyberbezpieczeństwa szpitala**

**realizowany poprzez przebudowę sieci informatycznej wraz z jej segmentacją**

**Obsługa środowiska sieciowego 24/7**

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
| **1** | **Wymagania ogólne** | **Przedmiotem zamówienia jest świadczenie kompleksowej usługi wsparcia, utrzymania środowiska sieciowego Zamawiającego, obejmującego infrastrukturę LAN (dot. sieci aktywnej) oraz urządzenia klasy UTM (Unified Threat Management). Usługa ma na celu zapewnienie wysokiej dostępności i bezpieczeństwa warstwy komunikacyjnej organizacji, a także bieżące reagowanie na incydenty sieciowe i potrzeby rozwojowe.**  **Wykonawca zapewni obsługę środowiska sieciowego Zamawiającego przez okres 36 miesięcy: 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.**   * **Czas przystąpienie do działań serwisowych na wezwanie Zamawiającego lub w przypadku wykrycia przez Wykonawcę incydentów w ramach świadczonego monitoringu:** * Generowanie raportów na wezwanie Zamawiającego: do 3 dni roboczych * Prace rekonfiguracyjne: do 8 godzin na przystąpienie do prac * Prace związane z awarią niekrytyczną: do 2 godzin na przystąpienie do prac * Prace związane z awarią krytyczną: do 30 minut na przystąpienie do prac * **Oznaczenie zastosowanych pojęć:** * **Prace rekonfiguracyjne –** prace związane z rekonfiguaracją urządzeń sieciowych, systemów sieciowych, nie wpływające na ciągłość działania pracy środowiska sieciowego. * **Awaria niekrytyczna -** to usterka lub problem techniczny w infrastrukturze sieciowej, systemach informatycznych lub usługach sieciowych, który nie powoduje całkowitego zatrzymania działania usług, lecz jedynie częściowe lub ograniczone utrudnienia. * **Awaria krytyczna –** to poważna usterka lub uszkodzenie infrastruktury sieciowej, systemów informatycznych lub usług sieciowych, które powoduje całkowitą niedostępność lub znaczące ograniczenie funkcjonowania kluczowych usług świadczonych użytkownikom.   **Zakres Usługi LAN/UTM**  Usługa obejmuje całościową opiekę nad środowiskiem sieciowym Zamawiającego, w tym:   * Monitorowanie stanu urządzeń sieciowych (switche, routery) oraz UTM * Zarządzanie konfiguracją urządzeń (w tym backupy, aktualizacje firmware, zmiany konfiguracji) * Obsługa incydentów sieciowych i bezpieczeństwa (awarie, wykryte zagrożenia, anomalia) * Reagowanie na zgłoszenia zespołu IT dotyczące problemów z łącznością, przepustowością lub dostępem * Wsparcie przy rozbudowie sieci (np. nowe lokalizacje, przełączniki, segmentacja VLAN) * Utrzymywanie polityk bezpieczeństwa na UTM (firewalle, VPN, IPS, filtrowanie treści, antywirus) * Rekomendowanie usprawnień i dobrych praktyk sieciowych   **Wymagania Funkcjonalne dla Infrastruktury LAN**  Środowisko sieciowe Zamawiającego musi być objęte usługą w sposób zapewniający:   * **Zarządzanie i monitoring aktywnych urządzeń sieciowych** (przełączniki warstwy 2/3, routery, kontrolery Wi-Fi, NAC, środowisko do zarządzania siecią) – bieżące monitorowanie parametrów wydajnościowych i stanu (CPU, RAM, port status, błędy transmisji) * **Zarządzanie konfiguracją VLAN**, routingiem, trunkami, agregacją łączy, listami ACL * **Diagnostyka i troubleshooting sieci** – np. analiza pętli, broadcast storm, błędnych konfiguracji STP/RSTP, problemów z DHCP * **Aktualizacja firmware** – planowanie i bezpieczne przeprowadzanie aktualizacji zgodnie z polityką producenta i praktykami change management * **Backup konfiguracji** – automatyczne i ręczne kopie konfiguracji urządzeń przechowywane zgodnie z zasadami bezpieczeństwa * **Raportowanie** – na wezwanie Zamawiającego przygotowanie zestawienia zdarzeń, wykorzystania portów i incydentów nie częściej niż raz na kwartał   **Komunikacja między Zamawiającym, a Wykonawcą odbywać się będzie telefonicznie, mailowo i/lub przez portal zgłoszeniowy Wykonawcy.**  **Wymagania Funkcjonalne dla UTM**  Usługa UTM (Unified Threat Management) obejmuje zarządzanie i bieżące utrzymanie następujących funkcjonalności:   * **Firewall i polityki dostępu** – tworzenie, modyfikacja, testowanie reguł zapory ogniowej (w tym polityk między VLAN, NAT, port forwarding) * **VPN** – zarządzanie tunelami IPsec i SSL VPN (zarówno site-to-site, jak i zdalny dostęp użytkowników) * **IPS/IDS** – konfiguracja, monitoring alertów, analiza fałszywych alarmów, aktualizacja sygnatur * **Web Filtering / Application Control** – definiowanie polityk dostępu do internetu, blokowanie niepożądanych treści, monitorowanie użycia aplikacji * **Antywirus** zarządzanie politykami AV, reagowanie na wykrycia * **Utrzymanie logów i raportów** – zapewnienie poprawnego logowania zdarzeń i integracji z systemami monitorującymi (np. system do analizy logów) * **Reagowanie na incydenty krytyczne**– np. blokowanie złośliwych adresów IP, analizowanie podejrzanego ruchu, izolacja stacji   **Komunikacja między Zamawiającym, a Wykonawcą odbywać się będzie telefonicznie, mailowo i/lub przez portal zgłoszeniowy Wykonawcy.** |  |

**Usługi wdrożenia segmentacji sieci**

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| **L.p.** | **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
| **1** | **Usługi wdrożenia segmentacji sieci** | Przedmiotem zamówienia jest wykonanie usługi segmentacji sieci teleinformatycznej Zamawiającego, obejmującej analizę istniejącej infrastruktury, zaprojektowanie, wdrożenie oraz przetestowanie segmentacji logicznej sieci LAN i WLAN w celu poprawy bezpieczeństwa, zwiększenia kontroli dostępu oraz ograniczenia ryzyka lateralnego przemieszczania się zagrożeń.  2.Usługa powinna obejmować co najmniej:  2.1 Audyt wstępny  Inwentaryzacja obecnej infrastruktury sieciowej (przełączniki, routery, firewalle, punkty dostępowe, serwery),  Identyfikacja istniejących stref funkcjonalnych i powiązań logicznych (np. administracja, systemy medyczne, IoT, pracownie, goście),  Ocena aktualnych mechanizmów bezpieczeństwa i polityk VLAN.  2.2 Opracowanie projektu segmentacji  Zaprojektowanie podziału sieci na logiczne segmenty/VLAN zgodnie z funkcją, poziomem zaufania i potrzebami biznesowymi,  Określenie zasad routingu i translacji między segmentami,  Wskazanie wymagań dotyczących konfiguracji urządzeń brzegowych, firewalli i przełączników,  Przygotowanie schematu logicznego oraz tabeli VLAN/segmentów.  2.3 Wdrożenie segmentacji  Konfiguracja urządzeń sieciowych (przełączniki L2/L3, routery, firewalle) zgodnie z przygotowanym projektem,  Wdrożenie VLAN, reguł ACL i reguł routingu między segmentami,  Konfiguracja sieci bezprzewodowej z podziałem na SSID przypisane do odpowiednich VLAN,  Wdrożenie mechanizmów kontroli dostępu (np. 802.1x, filtrowanie MAC, NAC – jeśli dotyczy).  2.4 Testy i dokumentacja  Przeprowadzenie testów poprawności działania komunikacji między i wewnątrz segmentów,  Weryfikacja poprawności izolacji ruchu i zgodności z założeniami bezpieczeństwa,  Przekazanie dokumentacji powykonawczej zawierającej schematy, konfigurację oraz opis wdrożonych rozwiązań.  3. Wymagania dodatkowe  Wykonawca zobowiązany jest do wykonania usługi w sposób minimalnie ingerujący w działanie sieci produkcyjnej,  Wdrożenie musi zostać przeprowadzone poza godzinami pracy użytkowników lub zgodnie z harmonogramem uzgodnionym z Zamawiającym,  W przypadku konieczności wykonania zmian konfiguracyjnych w urządzeniach, Wykonawca ma obowiązek uprzedniego wykonania kopii zapasowej konfiguracji i uzgodnienia zakresu zmian z Zamawiającym.  4. Wymagane rezultaty  Zrealizowana segmentacja sieci zgodna z przyjętym projektem,  Poprawna separacja ruchu między segmentami i kontrola dostępu,  Dokumentacja techniczna zawierająca:  Schemat segmentacji,  Tabela VLAN i przypisanych urządzeń/obszarów,  Konfiguracja urządzeń sieciowych w zakresie objętym pracami. |  |

**System do zarządzania infrastrukturą sieciową – 1 kpl.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Podać producenta oraz nazwę zaoferowanego systemu:**  **……………………………………………………………………………………………………………………………………………………….** | | | |
| **L.p.** | **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
| **1** | **Wymagania ogólne** | System służący do kompleksowego zarządzania infrastrukturą sieciową o poniższych parametrach.   * System musi być zbudowany w architekturze klient – serwer * Licencja na system powinna umożliwiać zarządzanie minimum 50 urządzeniami sieciowymi różnych producentów z możliwością rozbudowy do przynajmniej 5000 urządzeń sieciowych. * System musi umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych w celu uzyskania redundancji. System dostarczony musi być systemem redundantnym możliwym do zainstalowania na minimum 2 serwerach * System musi być zbudowany modułowo, tak aby możliwe było doinstalowanie modułów dających dodatkową funkcjonalność, minimalnie:   + Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA   + Zarządzanie siecią bezprzewodową WLAN   + Audyt użytkowników z wykorzystaniem informacji z logów, przepływów sieciowych sFlow, NetSream v5 oraz analizy zawartości pakietów SMTP, FTP, http   + Zarządzenie sieciami MPLS oraz sieciami VPN w oparciu o MPLS oraz VPLS   + Zarządzanie dostępem zdalnym IPsec/VPN   + Wbudowany serwer TACACS   + Funkcja monitorowania wydajności aplikacji * System musi zostać dostarczony w najnowszej dostępnej na rynku wersji na dzień ostatecznego odbioru Systemu * Licencja na System musi umożliwiać zarządzanie wszystkimi urządzeniami sieciowymi różnych producentów * System musi posiadać funkcje umożliwiać automatyczne wykrywanie topologii sieci z użyciem protokołów SNMP, Telnet * System musi posiadać funkcje monitorowania stanu urządzeń po protokole SNMP i wyświetlania informacji co najmniej o:   + Średnim wykorzystaniu CPU i pamięci RAM   + Średnim czasie odpowiedzi urządzenia   + Obciążeniu interfejsów (dla ruchu wchodzącego i wychodzącego)   + Ilość błędnych lub odrzuconych pakietów na interfejsie * System musi posiadać funkcje konfiguracji urządzeń po protokole SNMP i SSH * System musi posiadać funkcje zarządzania konfiguracją urządzeń, tworzenia backup’ów (ręcznie oraz automatycznie w określonych odstępach czasu) oraz grupowego implementowania konfiguracji na zarządzane urządzenia. System musi zachowywać historię tworzenia backup’ów (minimum 30 dni) wraz z informacją czy przebiegł on pomyślnie, a w przypadku, jeżeli nie, powinien także poinformować o przyczynie niepowodzenia * System musi pozwalać na tworzenie szablonów konfiguracji co najmniej w oparciu o cały plik konfiguracyjny, fragment konfiguracji, skrypt CLI, skrypt TCL. * System musi posiadać funkcje archiwizacji konfiguracji i zarządzania obrazami oprogramowania urządzeń, w tym możliwość przechowywania kilku wersji oprogramowania dla jednego modelu urządzenia, możliwość importowania obrazu z komputera do Systemu (tzw. Offline), możliwość pobrania obrazu do Systemu bezpośrednio z Internetu (tzw. Online/LiveUpdate) * System musi pozwalać na globalne zarządzanie VLAN, tzn. na tworzenie, modyfikowanie oraz usuwanie VLAN jednocześnie ze wszystkich lub wybranych przełączników zarządzanych przez System. Musi istnieć także możliwość automatycznego generowania map logicznej topologii sieci obrazującej konkretny VLAN a zarządzanych urządzeniach. * System musi posiadać funkcję zarządzania listami kontroli dostępu (ACL), w tym: możliwość importowania ACL z urządzeń i tworzenie na ich podstawie szablonu, tworzenie ACL w systemie zarządzania, możliwość pojedynczej lub grupowej implementacji przechowywanych w systemie ACL na urządzeniach * System musi posiadać możliwość wyświetlania zbiorczej tablicy routingu zbudowanej w oparciu o tablice zarządzanych urządzeń * System musi posiadać zcentralizowany mechanizm przeglądania zdarzeń w sieci, tzw. Dashboard (skonsolidowany, syslog, trapy snmp, zdarzenia i alarmy) * System musi generować alarmy na podstawie takich parametrów jak: wykorzystanie CPU, wykorzystanie RAM, temperatura urządzenia, obciążenie interfejsów fizycznych na wejściu i wyjściu, ilość odrzuconych pakietów; Muszą być dostępne co najmniej dwa poziomy alarmu dla pojedynczego parametru oraz muszą być one możliwe do zmiany. * System musi posiadać funkcje wysyłania alarmów np. e-mailem lub SMS’em wraz z możliwością konfiguracji konkretnego zakresu czasowego i dnia tygodnia, w którym wiadomości będą wysyłane. * System musi pozwalać na budowanie widoków przez administratora * System musi posiadać funkcje generowania raportów (co najmniej w formatach PDF, CSV, Excel, XLSX, Docx) w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta. Generowanie raportów musi się odbywać na życzenie (on demand) i w regularnych odstępach czasowych (scheduled, np. codziennie, raz w tygodniu, raz na kwartał itp.) * System musi posiadać narzędzia graficznej prezentacji topologii sieciowej wraz z dynamiczną prezentacją zmian stanu urządzeń oraz poziomem występujących na nich alarmów. Musi być też możliwość zmiany ikony reprezentującej urządzenie na topologii sieci wraz z możliwością wykorzystania różnych ikon dla różnych poziomów alarmów na urządzeniu. * System musi posiadać wbudowane narzędzie do przeprowadzenia inwentaryzacji sprzętu używanego w sieci. * System musi posiadać funkcje lokalizowania użytkowników przewodowych po adresie IP lub MAC. Wynikiem musi być wskazanie konkretnego portu zarządzanego urządzenia sieciowego, do którego podłączony jest użytkownik * System musi posiadać funkcję powiązywania konkretnego interfejsu fizycznego zarządzanego urządzenia z adresem MAC urządzenia końcowego, które będzie miało dostęp do sieci tylko na tym interfejsie. Po wykryciu nieautoryzowanej próby połączenia musi być możliwość wygenerowania alarmu, wyłączenia interfejsu po określonym czasie od zaistnienia zdarzenia (wartość konfigurowalna minimum w zakresie 10-1800 sekund) oraz ponownego włączenia interfejsu po określonym czasie od wyłączenia (wartość konfigurowalna minimum w zakresie 10-1800 sekund) * System musi posiadać predefiniowaną bazę zakresów adresów MAC dla urządzeń sieciowych oraz biurowych wiodących producentów. Baza musi być zbudowana co najmniej dla takich producentów jak: Cisco, Epson, Toshiba, NEC, Nortel, Canon, Sony, Samsung, 3Com, Siemens, Nokia, Apple, Lexmark, Xerox, Avaya, D-Link, LG, Dell, Alcatel, Netgear, HPE, TP-Link, Ruckus oraz Huawei. Musi istnieć możliwość ręcznego dodania wpisu do tej bazy. * System musi posiadać wbudowane mechanizmy wspomagające wyszukiwanie, izolację problemów i ich rozwiązywanie * System musi posiadać funkcje tworzenia mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym, w tym:   + Wykrywanie ataków między innymi takich jak: Duplicate ARP Address, ICMP Flood, TCP Port Scan, WinNuke, IP Spoofing, ICMP Redirect, Source Route, SYN Flood, UDP Port Scan, UDP Flood, Ping of Death, DHCP Server Detect   + Stworzenie topologii obrazującej logiczne połączenia między urządzeniami objętymi jednym lub kilkoma atakami sieciowymi, tzn. pokazuje urządzenie/urządzenia będące źródłem ataku i łączy je z urządzeniem/urządzeniami będącymi celem ataku.   + Stworzenie topologii obrazującej fizyczne połączenie między urządzeniami objętymi pojedynczym atakiem sieciowym, tzn. pokazuje całą ścieżkę fizyczną między źródłem, a celem ataku. * System musi posiadać funkcję Telnet/SSH oraz GUI proxy umożliwiającą zarządzanie CLI/Web przez przeglądarkę Internetową * System musi posiadać funkcje zarządzania za pomocą urządzeń mobilnych tj. iPhone oraz urządzeniami z systemem Android * System musi posiada funkcje dostępu do sytemu zarządzania realizowaną przez przeglądarkę internetową (min. Chrome i Firefox) * System musi posiadać funkcje zbierania informacji o konfiguracji urządzeń w sieci dzienników zdarzeń systemu, informacji o zasobach (np. mapy topologii sieci) i przesyłania tych informacji za pomocą FTP, SFTP, e-mail * System musi posiadać funkcje tworzenia kont administratorskich z różnymi poziomami uprawnień oraz z możliwością przypisywania administratorów do grup urządzeń. Dodatkowo musi być możliwość stworzenia kont jedynie z uprawnieniami do podglądu – bez możliwości dokonywania zmian w systemie ani na urządzenia. * System musi posiadać funkcję zarządzania VXLAN – tworzenie listy urządzeń wspierających VXLAN, tworzenie tuneli, tworzenie topologii sieci VXLAN, wyświetlanie informacji o statystykach ruchu w tunelach * System musi posiadać funkcje zarządzania siecią wirtualną poprzez integrację z VMware (minimum wersja 6.0) i Microsoft Hyper-V(minimum w wersji 2012). Między innymi musi pozwalać na:   + Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem VMware ESX z wykorzystaniem protokołu SOAP.   + Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem Microsoft Virtual Machine Manager z wykorzystaniem Windows PowerShell.   + Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem Microsoft Hyper-V z wykorzystaniem protokołu WMI.   + Zarządzanie siecią wirtualną, w tym serwerami VMware vCenter Server oraz Microsoft Virtual Machine Manager, wirtualnymi maszynami oraz wirtualnymi przełącznikami.   + Migrację wirtualnych maszyn pomiędzy fizycznymi serwerami.   + Przedstawienie wszystkich zasobów, szczegółowych informacji o nich oraz ich wzajemnych relacji w środowisku wirtualnym. Wymaga się, aby był wgląd minimum w:     - Listę wszystkich fizycznych serwerów VMware ESX oraz Microsoft Hyper-V dostępnych w sieci. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: producent, model, nazwa serwera, adres IP, informacje na temat Managera sieci wirtualnej, ilość pamięci RAM (wraz z poziomem wykorzystania), CPU (wraz z poziomem wykorzystania) oraz informację czy dany serwer wspiera funkcję migracji maszyn wirtualnych.     - Listę wirtualnych przełączników przyporządkowanych do konkretnych serwerów VMware ESX oraz Microsoft Hyper-V. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: nazwa przełącznika, ilość wirtualnych portów.     - Listę wirtualnych maszyn przyporządkowanych do konkretnych przełączników wirtualnych. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: nazwa wirtualnej maszyny, adres IP, stan maszyny (Running, Stopped, Suspended).   + Zmianę stanu (minimum: Start VM, Stop VM, Suspend VM, Reset VM) i parametrów wirtualnej maszyny takich jak: zasoby CPU, ilość pamięci RAM, ilość przestrzeni dyskowej.   + Dodawanie, klonowanie i usuwanie wirtualnych masz.   + Kreowanie szablonów służących do tworzenia nowych wirtualnych maszyn, gdzie można zdefiniować parametry początkowe takie jak: nazwę VMware ESX/Microsoft Hyper-V, zasoby CPU, ilość pamięci RAM, przestrzeń dyskową, system operacyjny wirtualnej maszyny.   + Dodawanie wirtualnych przełączników wraz z możliwością wyboru konkretnych kart sieciowych fizycznego serwera, do których będzie połączony wirtualny przełącznik. Dodatkowo musi istnieć możliwość „load balancingu” pomiędzy kartami sieciowymi co najmniej w oparciu o: IP hash, MAC hash, port fizyczny ruchu przychodzącego. Musi być także możliwość ustawienia kart sieciowych w trybie Active-Standby. * System musi posiadać funkcje zarządzania co najmniej dla 2000 predefiniowanych modeli urządzeń. Oprócz tego musi być możliwość wgrania dowolnej bazy MIB dla urządzeń sieciowych nie obsługiwanych domyślnie przez System * System musi posiadać funkcję automatycznej aktualizacji przez Internet. * System musi posiadać funkcje implementacji rozproszonej, wykorzystując różne serwery do instalacji swoich komponentów. * System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled) * System musi pozwalać na podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy * Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych. * Minimum 3 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. |  |
| **2** | **Spójny ekosystem – parametr opcjonalny** | **Parametr opcjonalny dodatkowo punktowany – 9 punków, jeśli zaoferowano**  - Zaoferowany system zarządzania w korelacji z systemem kontroli dostępu (NAC), przełącznikami rdzeniowymi, dostępowymi, i system zarządzania oferowanymi w niniejszym postępowaniu muszą tworzyć spójny ekosystem. W szczególności muszą posiadać wspólny, autoryzowany przez ich producentów punkt serwisowy realizujący kompleksową pomoc techniczną dla całego rozwiązania. |  |
| **3** | **Usługi wdrożeniowe i konfiguracyjne** | **Wymagania dotyczące wdrożenia systemu do centralnego zarządzania infrastrukturą sieciową:**   1. **Instalacja i konfiguracja systemu zarządzania:**    * Instalacja systemu zarządzania siecią w środowisku Zamawiającego.    * Konfiguracja podstawowych komponentów systemu, w tym bazy danych, modułów komunikacyjnych oraz interfejsu zarządzającego.    * Zapewnienie dostępu do interfejsu administracyjnego z wyznaczonych stacji roboczych w sieci Zamawiającego. 2. **Integracja z infrastrukturą sieciową:**    * Wykrycie i dodanie do systemu zarządzania dostarczanych w ramach niniejszego postępowania przełączników warstwy rdzeniowej i dostępowej.    * Konfiguracja połączeń zarządzających do urządzeń sieciowych oraz zabezpieczenie kanałów komunikacyjnych.    * Umożliwienie zdalnego monitorowania i zarządzania urządzeniami sieciowymi poprzez centralny system. 3. **Konfiguracja monitoringu i inwentaryzacji:**    * Uruchomienie mechanizmów automatycznego wykrywania zmian w konfiguracji urządzeń.    * Włączenie monitorowania parametrów pracy sieci, takich jak wykorzystanie portów, stan interfejsów, dostępność urządzeń, błędy transmisji itp.    * Konfiguracja alertów i powiadomień o zdarzeniach krytycznych oraz nieprawidłowościach w pracy urządzeń. 4. **Zarządzanie konfiguracją i wersjami:**    * Umożliwienie centralnego tworzenia, przechowywania i przywracania kopii konfiguracji urządzeń.    * Uruchomienie funkcji porównywania zmian konfiguracji oraz wersjonowania.    * Przygotowanie mechanizmu dystrybucji konfiguracji oraz aktualizacji oprogramowania urządzeń sieciowych z poziomu systemu zarządzającego. 5. **Raportowanie i analiza:**    * Skonfigurowanie zestawów raportów dotyczących wydajności, dostępności oraz zmian w konfiguracjach.    * Możliwość generowania raportów cyklicznych oraz na żądanie.    * Umożliwienie wizualizacji topologii sieci oraz śledzenia jej zmian w czasie. 6. **Dokumentacja:**    * Przygotowanie dokumentacji wdrożeniowej opisującej strukturę i sposób działania systemu zarządzania. |  |

**System kontroli dostępu (NAC) – 1 szt.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Podać producenta oraz nazwę zaoferowanego system:**  **……………………………………………………………………………………………………………………………………………………….** | | | |
| **L.p.** | **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
| **1** | **Wymagania ogólne** | **System do kontroli dostępu musi charakteryzować się następującymi cechami:**   * Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor) * System zostanie dostarczony w klastrze wysokiej dostępności z licencjami do obsługi minimum 2000 urządzeń klienckich (w tym gości). Zamawiający dopuszcza klaster dwóch maszyn wirtualnych. Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia * Musi posiadać wbudowany serwer Radius oraz TACACS + * Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym:   + Cisco Systems   + Fortinet   + Microsoft   + Alcatel-lucent Enterprise   + Huawei Networks   + Extreme Networks   + PaloAlto Networks   + Producenta urządzeń opisanych w tym dokumencie * System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera. * System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego. * Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych. * Ze względu na fakt, że system kontroli dostępu (NAC) jest systemem krytycznym dla działania sieci, system ten musi być komponentem całkowicie niezależnym i odseparowanym (niezależny, nie połączony kod) od innych systemów takich jak systemy zarządzania (nie dopuszcza się systemów, które pełnią funkcje łączone – np. system zarządzania siecią i system kontroli dostępu) * Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych   + Microsoft Active Directory   + Radius   + Kerberos   + LDAP   + ODBC   + Współpraca z serwerami tokenów * Musi obsługiwać metody profilowania   + DHCP   + TCP   + MAC OUI   + SNMP   + Cisco device sensor * Wspierać protokoły   + Radius, Radius CoA, TACACS +, web authentication, SAML v2.0   + EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)   + PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)   + TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)   + EAP-TLS   + PAP, CHAP, MSCHAPv1 i v2, EAP-MD5   + NAC, Microsoft NAP   + Windows machine authentication   + MAC Auth   + Audit (role oparte na porcie oraz skanowanie podatności)   + OCSP (Online Certificate Status Protocol)   + SNMP generic MIB, SNMP private MIB   + CEF (Common Event Format), LEEF (Log Event Extended Format)   + TLS 1.2 * Funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami * Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych:   + Co najmniej ESX 4.0, ESXi 4.1 do 6.0   + Co najmniej Hyper-V 2012 R2 oraz Windows 2012 R2 enterprise   - Musi posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (2000). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte.  System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności   * Samodzielna rejestracja klientów gościnnych w oparciu o:   + Adres e-mail   + Numer telefonu (wiadomość SMS)   + Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link) * Logowanie w oparciu o portale społecznościowe * Funkcja integracji z systemami trzecimi poprzez API * Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową * Wbudowany system reklamowy umożliwiający integrację z zewnętrznymi serwisami umożliwiającymi w prosty sposób promowanie ofert promocyjnych, materiałów multimedialnych oraz aplikacji mobilnych. * Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych. * Funkcja personalizacji strony gościnnej   - Musi posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.   * Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działo IT * System musi wspierać obsługę następujących systemów operacyjnych   + MS Windows   + Mac OS X   + iOS   + Android   + Chromebook   + Ubuntu * Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci * Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej * Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu. * Funkcja tworzenia unikalnych certyfikatów dla urządzeń. * Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń * Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID   - Musi posiadać moduł odpowiedzialny za kontrolę końcówek klienckich. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.  System kontroli końcówek klienckich musi mieć następujące funkcjonalności:   * System musi wspierać następujące systemy operacyjne   + Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis)   + Apple Mac OS X 10.7 i nowsze   + Red HAT Enterprise Linux 4 i nowsze   + CentOS 4 (Community Enterprise Operating System) i nowsze   + Fedora Core 5 i nowsze   + SUSE linux 10.x i nowsze * Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall * Wyświetlanie informacji on-line o statusie monitorowanych końcówek * System powinien obsługiwać agenta w formie   + Stałej (Presistent Agent)   + Tymczasowej (Dissolvabe Agent)   + Agenta NAP   - Minimum 3 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.  - Zaoferowane rozwiązanie musi być uznane przez firmę analityczną Gartner Research. To znaczy musi być wymienione w bieżącym na moment składania oferty raporcie Market Guide for Network Access Control lub musi być wymienione w Gartner Peer Insights w kategorii Network Access Control, gdzie musi posiadać przynajmniej 190 opinii i poziom „Would Recommend” mnie mniejszy niż 80%.  - Do rozwiązania musi być dostępna publicznie, na stronie producenta, dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań.  - Oferta musi zawierać kompletne zestawianie numerów katalogowych produktów i wszystkich jego dodatkowych składników umożliwiających ich jednoznaczną identyfikację u producenta sprzętu  - Zamawiający może zażądać przed dostawą przeprowadzenia testów wybranych funkcji sprzętu i oprogramowania wymaganych w niemniejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłużysz niż 2 tygodnie od chwili zażądania przez Zamawiającego ich przeprowadzenia. Nieprzystąpienie do testów lub nieskuteczne ich przeprowadzenie (brak potwierdzenia przez Zamawiającego, że testy zostały zakończone pomyślnie) skutkować będzie odrzuceniem oferty. |  |
| **2** | **Spójny ekosystem – parametr opcjonalny** | **Parametr opcjonalny dodatkowo punktowany – 9 punktów, jeśli zaoferowano**  - Zaoferowany system kontroli dostępu (NAC), w korelacji z przełącznikami rdzeniowymi i dostępowymi, oraz system zarządzania oferowanymi w niniejszym postępowaniu muszą tworzyć spójny ekosystem. W szczególności muszą posiadać wspólny, autoryzowany przez ich producentów punkt serwisowy realizujący kompleksową pomoc techniczną dla całego rozwiązania. |  |
| **3** | **Usługi wdrożeniowe i konfiguracyjne** | **Zakres usług dotyczących instalacji i konfiguracji systemu NAC w środowisku Zamawiającego:**   1. **Instalacja i konfiguracja systemu NAC:**    * Instalacja systemu NAC w środowisku Zamawiającego    * Utworzenie klastra wysokiej dostępności    * Aktualizacja oprogramowania systemu NAC do najnowszej zalecanej przez producenta wersji stabilnej. 2. **Integracja z infrastrukturą Zamawiającego:**    * Konfiguracja usług RADIUS na serwerze NAC oraz integracja z usługami katalogowymi Zamawiającego.    * Utworzenie polityk uwierzytelniania użytkowników końcowych i urządzeń, obejmujących segmentację dostępu oraz przypisywanie odpowiednich VLAN-ów na podstawie polityk NAC.    * Konfiguracja mechanizmów dynamicznej autoryzacji użytkowników (Change of Authorization - CoA). 3. **Konfiguracja polityk bezpieczeństwa NAC:**    * Utworzenie reguł i polityk dostępu w oparciu o role użytkowników oraz urządzeń końcowych (komputery, drukarki, telefony IP).    * Konfiguracja procedur reagowania na incydenty bezpieczeństwa, w tym automatyczna izolacja zagrożeń lub ograniczanie dostępu.    * Stworzenie dedykowanych polityk dla urządzeń gościnnych, uwzględniających ograniczony dostęp do zasobów sieciowych. 4. **Testowanie i optymalizacja:**    * Weryfikacja poprawności działania uwierzytelniania użytkowników i urządzeń końcowych.    * Przeprowadzenie testów integracyjnych, funkcjonalnych oraz bezpieczeństwa środowiska NAC.    * Optymalizacja działania systemu NAC w celu minimalizacji wpływu na użytkowników końcowych i zwiększenia efektywności procesu autoryzacji. 5. **Szkolenie i dokumentacja:**    * Przygotowanie dokumentacji powdrożeniowej, obejmującej konfigurację systemu NAC.    * Przeprowadzenie szkolenia technicznego dla wskazanych przez Zamawiającego administratorów sieci z zakresu obsługi i zarządzania wdrożonym systemem NAC. |  |

**Przełącznik warstwy rdzeniowej – 2 szt.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Podać producenta oraz nazwę zaoferowanego przełącznika:**  **……………………………………………………………………………………………………………………………………………………….** | | | |
| **L.p.** | **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
| **1** | **Wymagania ogólne** | 1. Typ i liczba portów:   Minimum 4 porty 10GbE/25GbE SFP28 ze wsparciem dla MACsec umieszczonych z przodu obudowy.  Minimum 22 porty 1GbE/10GbE/25GbE/50GbE SFP56 umieszczonych z przodu obudowy. Porty muszą wspierać co najmniej standardy: 50GBaseSR, 25GBase-SR, 25GBaseLR, 25GBase-eSR, 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-T, 1000Base-T, 1000BaseSX, 1000BaseLX, kable DAC i AOC. Musi być możliwe każdego portu SFP56 na 2 porty 25Gb SFP28.   1. Minimum 6 portow 40/100GbE QSFP28 umieszczonych z przodu obudowy, z czego minimum 2 z obsługą MACsec. Porty muszą wspierać co najmniej standardy: 100GBase-SR4, 100GBase-LR4, 100Gb BiDi, 100Gb CWDM4, 100Gb FR1,100Gb ER4L, 40GBase-SR4, 40GBase-eSR, 40Gb BiDi, 40GBase-LR4, 40BaseER4, kable DAC i AOC, kable typu split oraz adaptery QSFP28 do SFP28 2. Wszystkie wymienione porty muszą być od siebie niezależne, nie dopuszcza się portów typu Combo 3. Wbudowany, dodatkowy, dedykowany port Ethernet do zarządzania poza pasmem - out of band management 4. Port konsoli RS232 ze złączem DB9 lub RJ45 5. Port konsoli USB ze złączem USB-C 6. Port USB 2.0 (niezależny od portu konsoli USB) 7. Wydajność: minimum 4.8 Tbps (prędkość przełączania „wirespeed” dla każdego portu przełącznika) 8. Wydajność: minimum 1000 Mp/s 9. Przełączanie w warstwie 2 i 3 modelu OSI 10. Wielkość bufora pakietów (packet buffer): minimum 32MB 11. Modularny system operacyjny bazujący na jądrze Linux oraz wykorzystujący OVSDB 12. Minimum 32GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash). Nie dopuszcza się pamięci instalowanej na zewnątrz przełącznika (np. do zewnętrznego portu USB) 13. Oprócz uruchamiania systemu operacyjnego Bootloader musi pozwalać na: dostęp do logów, zrzutów pamięci (coredump) i konfiguracji, naprawę i formatowanie przestrzeni pamięci, wygrywanie i aktualizację systemu operacyjnego, czyszczenie konfiguracji, czyszczenie i zmianę haseł administratorskich, wybór wersji systemu operacyjnego 14. Minimum 16GB pamięci operacyjnej 15. Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów) 16. Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika do tyłu przełącznika. Nie dopuszczalne są rozwiązania, z mieszanym przepływem powietrza. 17. Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia. 18. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP) 19. Funkcja łączenia przełączników w grupy co najmniej 2 urządzeń, w sposób ciągły synchronizujących ze sobą konfiguracje przy zachowaniu niezależnych płaszczyzn zarządzani (control plane). Przełączniki połączone w grupę muszą zapewnić co najmniej: realizację łączy agregowanych w ramach różnych przełączników będących w grupie, architekturę, w której oba przełączniki są aktywne dla funkcji L2 i L3, funkcje typu ISSU lub Live Upgrade. 20. Tablica adresów MAC o wielkości minimum 210000 pozycji 21. Obsługa ramek Jumbo o wielkości co najmniej 9kB 22. Obsługa Quality of Service 23. Obsługa mechanizmów, co najmniej: strict priority (SP) queuing, Deficit weighted round robin (DWRR) queuing oraz SP+DWRR 24. Obsługa IEEE 802.1s Multiple SpanningTree (MSTP) oraz IEEE 802.1w Rapid Spanning Tree Protocol 25. Obsługa sieci IEEE 802.1Q VLAN – 4094 jednoczesnych sieci VLAN 26. Obsługa IGMP v2/v3, IGMP Snooping, PIM SM 27. Routing IPv4 – statyczny i dynamiczny (min. RIPv2, OSPF, BGP) 28. Routing IPv6 – statyczny i dynamiczny (min. RIPng, OSPFv3, MP-BGP) 29. Obsługa ECMP (Equal Cost Multi Path) 30. Obsługa VRRP 31. Obsługa tunelowania GRE 32. Obsługa Virtual Routing and Forwarding (VRF) 33. Obsługa funkcji VXLAN 34. Tablica routingu o pojemności co najmniej 600000 wpisów dla IPv4 oraz co najmniej 600000 wpisów dla IPv6 35. Obsługa funkcji klienta DHCP 36. Obsługa DHCP Relay dla IPv4 i IPv6 37. Obsługa list ACL (co najmniej 60000 dla IPv4 i 60000 dla MAC) na bazie informacji z warstw 2 i 3 modelu OSI.   Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia   1. Obsługa standardu 802.1p 2. Funkcja ograniczania ruchu typu multicast i broadcast 3. Możliwość zmiany wartości pola DSCP i/lub wartości priorytetu 802.1p 4. Funkcja kopiowania ruchu wejściowego i wyjściowego (port mirroring) lokalnego (w obrębie urządzenia) i zdalnego (na porty znajdujące się na innym urządzeniu) 5. Funkcja centralnego uwierzytelniania administratorów na serwerze RADIUS oraz TACACS+ 6. Zarządzanie poprzez port konsoli (CLI), SNMP 2c, SNMP 3, interfejs graficzny (WebGUI) znajdujący się bezpośrednio na urządzaniu oraz SSH v2 7. Obsługa Syslog 8. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) 9. Obsługa sFlow 10. Obsługa Network Time Protocol (NTP) 11. Obsługa Secure FTP (SFTP) oraz TFTP 12. Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona rekomendowana przez producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty. 13. Obsługa skryptów w języku Python 14. Obsługa REST API 15. Obsługa RMON (minimum grupy 1, 2, 3 i 9) 16. Obsługa funkcji diagnostycznych ping i traceroute dla IPv4 i IPv6 17. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego 18. Przechowywanie co najmniej dwóch wersji oprogramowania na przełączniku 19. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji). 20. Przełącznik musi posiadać mechanizm (automatycznego i ręcznego) tworzenia punktów szybkiego odtwarzania konfiguracji. Punkty szybkiego odtwarzania muszą zawierać aktualne zrzuty działającej konfiguracji oraz informacje dodatkowe (co najmniej: typ punktu, datę utworzenia, wersję oprogramowania, dane sprzętu, dane zapisującego punkt przywracania, opis). System musi umożliwiać ich kopiowanie i uruchamianie na innych urządzeniach tego samego typu. W urządzeniu musi być przechowywanych nie mniej niż 60 punktów przywracania konfiguracji. Przełącznik musi posiadać funkcję porównywania ze sobą (oraz prezentacji różnic) dwóch punktów odtwarzania konfiguracji oraz punktu odtwarzania konfiguracji z konfiguracją aktualnie działającą i konfiguracją zapisaną jako bieżąca. 21. Wysokość w szafie 19” – 1U o głębokości maksymalnie 60 cm 22. Minimalny zakres temperatur pracy od 0°C do 45°C 23. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania 24. Wszystkie wymagane na przełączniku funkcje muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji o ile nie wyspecyfikowano inaczej.      1. Producent sprzętu musi być sklasyfikowany co najmniej 5 ostatnich (w tym bieżącym) w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure” lub równoważnym i znajdować się w kwadracie liderów (Leaders). Za ranking równoważny Zamawiający uzna ranking klasyfikujący rozwiązania klasy 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 i publikowany był od co najmniej 10 lat. 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 2. Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. 3. Przełącznik musi być wyposażony w zestaw montażowy do szarfy rack 4. Dołączone kable 100GbE DAC QSFP28 o długości co najmniej 3 m – 2 szt. Kable muszą być w pełni kompatybilne z przełącznikami rdzeniowymi opisanymi w tym dokumencie. W szczególności muszą być wskazane jako dedykowane w oficjalnych kartach katalogowych przełączników oraz muszą być serwisowane przez serwis producentów przełączników. 5. Dołączone kable 25GbE DAC SFP28 o długości co najmniej 3 m – 2 szt. Kable muszą być w pełni kompatybilne z przełącznikami dostępowymi i rdzeniowymi opisanymi w tym dokumencie w tym dokumencie. W szczególności muszą być wskazane jako dedykowane w oficjalnych kartach katalogowych przełączników oraz muszą być serwisowane przez serwis producentów przełączników. |  |
| **2** | **Pobór mocy** | **Parametry punktowane - podać jeden z zaoferowanych parametrów:**  **Parametr 1 - Maksymalny pobór mocy do 750W lub mniejszy – 1 punkt**  **Parametr 2 - Maksymalny pobór mocy większy niż 750W – 0 punktów** |  |
| **3** | **Spójny ekosystem – parametr opcjonalny** | **Parametr opcjonalny dodatkowo punktowany: 9 punktów, jeśli zaoferowano**  Zaoferowane przełączniki rdzeniowe, w korelacji z przełącznikami dostępowymi, system kontroli dostępu (NAC) oraz system zarządzania oferowanymi w niniejszym postępowaniu muszą tworzyć spójny ekosystem. W szczególności muszą posiadać wspólny, autoryzowany przez ich producentów punkt serwisowy realizujący kompleksową pomoc techniczną dla całego rozwiązania. |  |
| **4** | **Wymagania dodatkowe** | 1. Zamawiający może zażądać przed dostawą przeprowadzenia testów wybranych funkcji sprzętu i oprogramowania wymaganych w niemniejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłuższym niż 2 tygodnie od chwili zażądania przez Zamawiającego ich przeprowadzenia. Nieprzystąpienie do testów lub nieskuteczne ich przeprowadzenie (brak potwierdzenia przez Zamawiającego, że testy zostały zakończone pomyślnie) skutkować będzie odrzuceniem oferty.  2. Sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim.  3. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych.  4. Wszystkie urządzenia muszą być fabrycznie nowe. Przed dostawą sprzęt musi być zarejestrowany przez producenta, bezpośrednio na Zamawiającego jako jedynego użytkownika po opuszczeniu fabryki. Jeśli producent nie prowadzi rejestracji sprzętu, to wymaga się deklaracji producenta, iż sprzęt jest fabrycznie nowy.  5. Zamawiający może zażądać przed dostawą dokumentu zawierającego listę numerów seryjnych dostarczanego sprzętu w celu weryfikacji spełnienia warunków gwarancyjnych. Zamawiający sprawdzi spełnienie powyższych warunków w polskim biurze producenta na podstawie numeru seryjnego urządzenia – w przypadku niezgodności deklaracji Wykonawcy z opinią producenta - Zamawiający odmówi odbioru przedmiotu zamówienia, jako niezgodnego ze specyfikacją istotnych warunków zamówienia.  6. Dostarczane urządzeni musi być zgodne z europejskimi normami ROHS lub równoważnymi. |  |
|  | **Usługi wdrożeniowe i konfiguracyjne** | **Wymagania dotyczące instalacji i konfiguracji dwóch przełączników rdzeniowych:**   1. **Fizyczna instalacja i uruchomienie:**    * Montaż urządzeń w szafach teleinformatycznych zgodnie z dokumentacją techniczną.    * Podłączenie zasilania z dwóch niezależnych źródeł (jeśli dostępne) w celu zapewnienia niezawodności zasilania.    * Podłączenie do infrastruktury okablowania światłowodowego i miedzianego zgodnie z planem połączeń. 2. **Konfiguracja podstawowa:**    * Ustawienie podstawowych parametrów urządzeń, takich jak adresacja IP, DNS, NTP, zarządzanie dostępem administracyjnym (SSH, SNMP, syslog).    * Wdrożenie polityk bezpieczeństwa dostępu do urządzeń zgodnie z wymaganiami Zamawiającego. 3. **Konfiguracja redundancji i wysokiej dostępności:**    * Skonfigurowanie mechanizmów zapewniających redundancję i ciągłość działania.    * Zapewnienie synchronizacji konfiguracji kluczowych elementów między urządzeniami rdzeniowymi.    * Konfiguracja automatycznego przełączania ruchu w przypadku awarii jednego z przełączników rdzeniowych. 4. **Integracja z siecią dostępową:**    * Przygotowanie i skonfigurowanie interfejsów uplink dla połączeń z przełącznikami dostępowymi.    * Konfiguracja odpowiednich VLAN-ów oraz routingu dla zapewnienia komunikacji w całym środowisku sieciowym.    * Implementacja mechanizmów kontroli pętli i redundancji warstwy drugiej (np. MSTP, RPVST, lub inne zgodne z architekturą). 5. **Testy funkcjonalne i awaryjne:**    * Przeprowadzenie testów poprawności działania funkcji routingu, VLAN, komunikacji z urządzeniami dostępowymi.    * Symulacja awarii jednego z urządzeń rdzeniowych w celu weryfikacji mechanizmów przełączania i zachowania ciągłości działania. 6. **Dokumentacja i przekazanie:**    * Opracowanie dokumentacji powdrożeniowej obejmującej schematy połączeń, konfigurację logiczną. |  |

**Przełącznik warstwy dostępowej- 45 sztuk**

|  |  |  |  |
| --- | --- | --- | --- |
| **Podać producenta oraz nazwę zaoferowanego przełącznika:**  **……………………………………………………………………………………………………………………………………………………….** | | | |
| **L.p.** | **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
| **1** | **Wymagania ogólne** | 1. Minimum 48 portów 1000BaseT z wsparciem dla standardów PoE (standardy 802.3af i 802.3at), umieszczone z przodu obudowy 2. Minimum 4 porty 1/10/25/50-gigabitowe SFP56 umieszczone z przodu obudowy 3. Przepustowość: minimum 496 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika) 4. Wydajność: minimum 360 Mp/s 5. Bufor pakietów: minimum 7.5 MB 6. Minimum 8GB pamięci operacyjnej 7. Minimum 30GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash). Pamięć musi być umieszczona wewnątrz urządzenia w sposób uniemożliwiający łatwe jej usunięcie (nie dopuszcza się pamięci podłączonej do portów (typu USB, czytnik kart SD, microSD, CF itp.) umieszczonych na obudowie przełącznika 8. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych 9. Dedykowany port konsoli USB 10. Port USB 2.0 (niezależny od portu konsoli USB) 11. Interfejs Bluetooth (dopuszcza się rozwiązanie w postaci adaptera Bluetooth, podłączanego do portu USB przełącznika, przy czym adapter musi pochodzić od tego samego producenta co przełącznik, nie musi być zaoferowany na tym etapie) 12. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 10 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. 13. Łączenie w stos z wykorzystaniem portów 10Gb, 25Gb, 50Gb i agregowanych portów 10Gb, 25Gb i 50Gb (w celu zwiększenia przepustowości w stosie). Musi być możliwe stworzenie stosu z urządzeń oddalonych od siebie o co najmniej 1000 metrów. 14. Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie 15. Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia. 16. Budżet mocy PoE przy zastosowaniu dwóch zasilaczy co najmniej 1440W 17. Modularne, redundantne wentylatory, podzielone na co najmniej dwa niezależne moduły. Moduły wentylatorów musi mieć możliwość wymiany „na gorąco” (na działającym urządzeniu) 18. Wielkość tablicy routingu: minimum 60000 wpisów IPv4, 60000 wpisów IPv6 19. Wielkość tablicy routingu multicast: minimum 8000 wpisów IPv4, 8000 wpisów IPv6 20. Tablica adresów MAC o wielkości minimum 32000 pozycji 21. Obsługa Jumbo Frames 22. Obsługa sFlow lub Netflow 23. Obsługa skryptów w języku Python 24. Obsługa REST API 25. Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona rekomendowana przez producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty. 26. Obsługa RMON (minimum grupy 1,2,3 i 9) 27. Obsługa 4094 tagów IEEE 802.1Q oraz 4094 jednoczesnych sieci VLAN 28. Obsługa standardu 802.1v 29. Obsługa protokołu MVRP 30. Wsparcie dla VXLAN 31. Obsługa Microsoft Network Load Balancer (NLB) 32. Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne 33. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s) 34. Obsługa Secure FTP lub SCP 35. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP) 36. Obsługa SNTPv4 lub NTP 37. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping) 38. Obsługa protokołów rutingu: ruting statyczny, RIPv2, RIPng, OSPF, OSPFv3, BGP, MP-BGP 39. Obsłyga ruchu multicast: IGMPv1/v2/v3, PIM-SM, PIM-DM, MSDP 40. Obsługa VRRP 41. Obsługa ECMP 42. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED) 43. Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED) 44. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting 45. Obsługa uwierzytelniania użytkowników zgodna z 802.1x 46. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS 47. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW 48. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie 49. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+ 50. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+ 51. Wbudowany serwer DHCP 52. Obsługa funkcji User Datagram Protocol (UDP) helper 53. Obsługa blokowania nieautoryzowanych serwerów DHCP 54. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego 55. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection) 56. Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP 57. Zakres pracy od 0 do 45°C 58. Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 40 cm. 59. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania 60. Wszystkie wymagane na przełączniku funkcje muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji o ile nie wyspecyfikowano inaczej. 61. Producent sprzętu musi być sklasyfikowany co najmniej 5 ostatnich (w tym bieżącym) w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure” lub równoważnym i znajdować się w kwadracie liderów (Leaders). Za ranking równoważny Zamawiający uzna ranking klasyfikujący rozwiązania klasy 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 i publikowany był od co najmniej 10 lat. 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 62. Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. |  |
|  | **Pobór mocy** | **Parametry punktowane - podać jeden z zaoferowanych parametrów:**  **Parametr 1 - Maksymalny pobór mocy do 180W bez obciążenia PoE lub mniejszy – 1 punkt**  **Parametr 2 - Maksymalny pobór mocy większy niż 180W bez obciążenia PoE – 0 punktów** |  |
|  | **Spójny ekosystem – parametr opcjonalny** | **Parametr opcjonalny dodatkowo punktowany – 10 punktów, jeśli zaoferowano**  Zaoferowane przełączniki dostępowe, w korelacji z przełącznikami rdzeniowymi, system kontroli dostępu (NAC) oraz system zarządzania oferowanymi w niniejszym postępowaniu muszą tworzyć spójny ekosystem. W szczególności muszą posiadać wspólny, autoryzowany przez ich producentów punkt serwisowy realizujący kompleksową pomoc techniczną dla całego rozwiązania. |  |
|  | **Wymagania dodatkowe** | 1. Zamawiający może zażądać przed dostawą przeprowadzenia testów wybranych funkcji sprzętu i oprogramowania wymaganych w niemniejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłużysz niż 2 tygodnie od chwili zażądania przez Zamawiającego ich przeprowadzenia. Nieprzystąpienie do testów lub nieskuteczne ich przeprowadzenie (brak potwierdzenia przez Zamawiającego, że testy zostały zakończone pomyślnie) skutkować będzie odrzuceniem oferty.  2. Sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim.  3. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych  4. Wszystkie urządzenia muszą być fabrycznie nowe. Przed dostawą sprzęt musi być zarejestrowany przez producenta, bezpośrednio na Zamawiającego jako jedynego użytkownika po opuszczeniu fabryki. Jeśli producent nie prowadzi rejestracji sprzętu, to wymaga się deklaracji producenta, iż sprzęt jest fabrycznie nowy.  5. Zamawiający może zażądać przed dostawą dokumentu zawierającego listę numerów seryjnych dostarczanego sprzętu w celu weryfikacji spełnienia warunków gwarancyjnych. Zamawiający sprawdzi spełnienie powyższych warunków w polskim biurze producenta na podstawie numeru seryjnego urządzenia – w przypadku niezgodności deklaracji Wykonawcy z opinią producenta - Zamawiający odmówi odbioru przedmiotu zamówienia, jako niezgodnego ze specyfikacją istotnych warunków zamówienia.  6. Urządzenie musi spełniać normę EN 60950-1:2006 lub równoważną. |  |
|  | **Usługi wdrożeniowe i konfiguracyjne** | **Wymagania dotyczące instalacji i konfiguracji przełączników dostępowych**   1. **Fizyczna instalacja:**    * Montaż przełączników w szafach teleinformatycznych w lokalizacjach wskazanych przez Zamawiającego.    * Podłączenie zasilania z dwóch niezależnych źródeł (jeśli dostępne) w celu zapewnienia niezawodności zasilania.    * Dokonanie połączeń sieciowych. 2. **Konfiguracja podstawowa:**    * Utworzenie stosu wysokiej dostępności w lokalizacjach wskazanych przez Zamawiającego wykorzystując dostarczane przełączniki dostępowe.    * Ustawienie parametrów zarządzania, takich jak adresy IP interfejsów zarządzających, maski podsieci, bramy domyślne, DNS, NTP.    * Konfiguracja zabezpieczonego dostępu administracyjnego (SSH, SNMPv3, syslog) oraz utworzenie kont użytkowników zgodnie z polityką bezpieczeństwa Zamawiającego.    * Wdrożenie mechanizmów zapobiegających nieautoryzowanemu dostępowi do urządzeń (m.in. listy kontroli dostępu, filtrowanie portów, itp.). 3. **Konfiguracja portów dostępowych:**    * Przydzielenie portów do odpowiednich VLAN-ów zgodnie z planem Wykonawcy ustalonym z Zamawiającym, dotyczącym adresacji i segmentacji sieci Zamawiającego.    * Konfiguracja portów do pracy w trybie access lub trunk    * Wdrożenie mechanizmów takich jak port security, BPDU Guard, storm control i innych zabezpieczeń warstwy drugiej. 4. **Integracja z systemami nadrzędnymi:**    * Przygotowanie portów do współpracy z systemem kontroli dostępu do sieci (NAC), w tym aktywacja funkcji 802.1X i dynamicznego przypisywania polityk VLAN.    * Konfiguracja interfejsów uplink i redundancji połączeń do przełączników rdzeniowych, w tym obsługa protokołów agregacji łączy 5. **Testy i weryfikacja:**    * Sprawdzenie poprawności działania połączeń uplink oraz komunikacji z innymi segmentami sieci.    * Weryfikacja działania przypisań VLAN-ów, dostępu użytkowników oraz poprawności działania zabezpieczeń.    * Testowanie funkcji zarządzania i monitoringu z poziomu systemów centralnych. 6. **Dokumentacja i przekazanie:**    * Sporządzenie dokumentacji powdrożeniowej zawierającej schematy połączeń, konfigurację logiczną, przypisania VLAN oraz zasady dostępu. |  |

**Okablowanie oraz wkładki komunikacyjne – 1 komplet**

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
| **1** | **Okablowanie DAC – TYP1** | **Wykonawca dostarczy:**  okablowanie DAC umożliwiające łączenie w stosy przełączników dostępowych na porach Uplink typu SFP56 o długości 0,50m – 30 szt. Kable muszą być w pełni kompatybilne z przełącznikami dostępowymi i rdzeniowymi opisanymi w tym dokumencie. W szczególności muszą być wskazane jako dedykowane w oficjalnych kartach katalogowych przełączników oraz muszą być serwisowane przez serwis producentów przełączników. |  |
|  | **Okablowanie DAC – TYP2** | **Wykonawca dostarczy:**  okablowanie DAC umożliwiające łączenie w stosy przełączników dostępowych na porach Uplink typu SFP56 o długości 3 m – 15 szt. Kable muszą być w pełni kompatybilne z przełącznikami dostępowymi i rdzeniowymi opisanymi w tym dokumencie. W szczególności muszą być wskazane jako dedykowane w oficjalnych kartach katalogowych przełączników oraz muszą być serwisowane przez serwis producentów przełączników. |  |
|  | **Wkładka SFP – TYP1** | **Wykonawca dostarczy**  wkładki SFP28 SR 850nm 100m LC DUAL RATE 10/25GbE Multi Mode- 100 szt. Wkładki muszą współpracować z przełącznikami dostępowymi i rdzeniowymi opisanymi w tym dokumencie. |  |
|  | **Wkładka SFP – TYP2** | Wykonawca dostarczy:  wkładki SFP+ SR 10Gbs 850nm LC DDM MMF 300m- 50 szt. Wkładki muszą współpracować z przełącznikami dostępowymi i rdzeniowymi opisanymi w tym dokumencie. |  |
|  | **Patchcordy światłowodowe** | **Wykonawca dostarczy:**  Patchcord LC/UPC-LC/UPC, Multimode min. OM3 Duplex, długość:1m- 50 szt.  Patchcord LC/UPC-LC/UPC, Multimode min. OM3 Duplex, długość:3m- 50 szt.  Patchcord LC/UPC-LC/UPC, Multimode min. OM3 Duplex, długość:5m- 50 szt. |  |
|  | **Patchcordy RJ45** | **Wykonawca dostarczy:**  Patchcord RJ45 kat. Minumum 5e UTP w ilości:   * 0,25m- 600 szt. * 0,5m- 600 szt. * 1m- 600 szt. * 1,5m- 50 szt. * 3m- 50 szt. * 5m- 50 szt. |  |
|  | **Informacje ogólne** | Wykonawca wykorzysta powyższe elementy celem dokonania wdrożenia i instalacji dostarczanych w niniejszym postępowaniu urządzeń sieciowych. |  |

**Licencja do posiadanego UTM Fortigate 60F SN FGT60FTK22035464 - 1 szt.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Podać producenta oraz nazwę zaoferowanej licencji:**  **……………………………………………………………………………………………………………………………………………………….** | | | |
| **L.p.** | **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
| **1** | **Licencja** | Wykonawca dostarczy licencję do obecnie pracującej jednostki FortiGate 60F na okres minimum 3 lat. Licencja musi być kontynuacją obecnie wykorzystywanej. |  |

**Urządzenie do zestawienia wysokiej dostępności dla posiadanego Fortigate 60F - 1 szt.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Podać producenta oraz nazwę zaoferowanego urządzania wraz z licencją:**  **……………………………………………………………………………………………………………………………………………………….** | | | |
| **L.p.** | **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
| **1** | **Zestaw wysokiej dostępności** | Wykonawca dostarczy urządzenie do zestawienia wysokiej dostępności (HA) dla posiadanego Fortigate 60F wraz z licencjami UTP na okres 3 lat. |  |
|  | **Usługi wdrożeniowe i konfiguracyjne** | Wykonawca utworzy klaster HA Active- Pasive za pomocą dostarczanego urządzenia oraz posiadanego. Licencje na obu urządzeniach muszą być skorelowane i posiadać tą samą date końca wsparcia. Wykonawca po dokonaniu konfiguracji przeprowadzi testy poprawności działania trybu wysokiej dostępności. Wykonawca dokona aktualizacji oprogramowania urządzeń do najnowszej stabilnej wersji. |  |

**UTM wysokiej wydajności (klaster HA składający się z dwóch urządzeń - zgodnie z wymogami zawartymi w tabeli) – 1 kpl.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Podać producenta oraz nazwę zaoferowanego rozwiązania UTM:**  **……………………………………………………………………………………………………………………………………………………….** | | | |
| **L.p.** | **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
| **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. |  |
| **2** | **Redundancja, monitoring i wykrywanie awarii** | 1. 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. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. 5. System ma pracować w postaci klastra wysokiej dostępności. |  |
| **3** | **Interfejsy, Dysk, Zasilanie:** | 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:  * 8 portami Gigabit Ethernet RJ-45. * 4 gniazdami SFP 1 Gbps. * 8 gniazdami SFP+ 10 Gbps. * 8 portami 10 Gigabit Ethernet RJ-45.  1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System jest wyposażony w zasilanie 2xAC. |  |
| **4** | **Parametry wydajnościowe** | 1. W zakresie Firewall’a obsługa nie mniej niż 10 mln jednoczesnych połączeń oraz 380 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 26 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 35 Gbps. 5. 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 9 Gbps. 6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 6 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 6 Gbps. |  |
| **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:  1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.  2. Kontrola Aplikacji.  3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.  4. Ochrona przed malware.  5. Ochrona przed atakami - Intrusion Prevention System.  6. Kontrola stron WWW.  7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.  8. Zarządzanie pasmem (QoS, Traffic shaping).  9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).  10. 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.  11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.  12. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.  13. 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). |  |
| **6** | **Polityki, Firewall** | 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  2. 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.  3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.  5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.  6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.  7. 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. |  |
|  | **Połączenia VPN** | 1. 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.  2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |  |
|  | **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie zapewnia obsługę:  1. Routingu statycznego.  2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).  3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.  4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.  5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.  6. BFD (Bidirectional Forwarding Detection).  7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |  |
|  | **Funkcje SD-WAN** | 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.  2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |  |
|  | **Zarządzanie pasmem** | 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.  2. System daje możliwość określania pasma dla poszczególnych aplikacji.  3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.  4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
|  | **Ochrona przed malware** | 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).  2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.  3. 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.  4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.  5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).  6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  7. 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.  8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.  9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.  10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |  |
|  | **Ochrona przed atakami** | 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.  2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.  3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.  5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.  6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).  7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.  8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.  9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |  |
|  | **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.  2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.  5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.  6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).  7. 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). |  |
|  | **Kontrola WWW** | 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.  2. 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.  3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.  4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.  5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).  6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.  7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.  8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.  9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |  |
|  | **Uwierzytelnianie użytkowników w ramach sesji** | 1. 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.  2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.  3. 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.  4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |  |
|  | **Pobór mocy** | **Parametry punktowane - podać jeden z zaoferowanych parametrów:**  **Parametr 1 - Maksymalny pobór mocy do 360W dla klastra lub mniejszy – 1 punkt**  **Parametr 2 - Maksymalny pobór mocy większy niż 360W dla klastra – 0 punktów** |  |
|  | **Zarządzanie** | 1. 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.  2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.  3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.  4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.  5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.  6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.  7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.  8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).  9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |  |
|  | **Logowanie** | 1. 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.  2. 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.  3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.  4. Możliwość włączenia logowania per reguła w polityce firewall.  5. System zapewnia możliwość logowania do serwera SYSLOG.  6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |  |
|  | **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. |  |
|  | **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 cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy. |  |
|  | **Gwarancja oraz wsparcie** | System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.  Urządzenia muszą spełniać obecne dyrektywy RoHS w UE. |  |
|  | **Wymagania pozostałe** | 1. Wymaga 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.  2. Wymaga się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży. |  |
|  | **Usługi wdrożeniowe i konfiguracyjne** | **Wykonawca dokona konfiguracji dostarczanego systemu UTM w trybie wysokiej dostępności (HA):**   1. **Fizyczna instalacja i połączenia sieciowe:**    * Montaż dwóch urządzeń UTM w szafie RACK.    * Zasilenie urządzeń.    * Podłączenie interfejsów sieciowych zgodnie z planem (interfejsy WAN, LAN, DMZ, synchronizacji HA).    * Dedykowane połączenie interfejsów HA (heartbeat/sync) pomiędzy urządzeniami w celu synchronizacji stanu i konfiguracji. 2. **Konfiguracja klastra HA:**    * Włączenie trybu wysokiej dostępności i skonfigurowanie jednego urządzenia jako głównego (primary) oraz drugiego jako zapasowego (secondary).    * Konfiguracja mechanizmu synchronizacji konfiguracji, sesji, i stanu pomiędzy urządzeniami.    * Testowanie przełączania (failover) i powrotu do pracy głównego urządzenia (failback) w celu potwierdzenia działania HA. 3. **Konfiguracja interfejsów i stref bezpieczeństwa:**    * Ustawienie stref bezpieczeństwa (LAN, WAN, DMZ, VPN, itp.) i przypisanie do nich odpowiednich interfejsów fizycznych.    * Konfiguracja adresów IP (w tym adresów wirtualnych używanych w HA), masek oraz bram domyślnych.    * Wdrożenie polityki routingu statycznego 4. **Zarządzanie dostępem i uwierzytelnianiem:**    * Konfiguracja dostępu administracyjnego do systemu (HTTPS/SSH),    * Integracja z usługami katalogowymi dla kontroli dostępu użytkowników do sieci i zasobów. 5. **Reguły bezpieczeństwa i inspekcji ruchu:**    * Stworzenie polityk zapory (firewall) definiujących ruch dozwolony i blokowany pomiędzy strefami.    * Włączenie inspekcji stanu połączeń oraz inspekcji aplikacyjnej    * Konfiguracja filtrowania treści (URL filtering), ochrony przed zagrożeniami (IPS/IDS), 6. **System VPN:**    * Konfiguracja połączeń VPN IPSec dla zdalnych pracowników oraz połączeń między oddziałami.    * Uruchomienie 2FA dla zdalnych pracowników 7. **Rejestrowanie, monitoring i alerty:**    * Włączenie mechanizmów logowania zdarzeń    * Konfiguracja monitoringu wydajności i zdarzeń bezpieczeństwa.    * Ustawienie powiadomień (e-mail/SNMP) o awariach, zmianach konfiguracji i wykrytych zagrożeniach. 8. **Testy końcowe i dokumentacja:**    * Weryfikacja działania systemu w trybie normalnym i awaryjnym.    * Sporządzenie dokumentacji wdrożeniowej zawierającej konfigurację, schematy sieciowe. |  |

**System do analizy logów – 1 szt.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Podać producenta oraz nazwę zaoferowanego rozwiązania:**  **……………………………………………………………………………………………………………………………………………………….** | | | |
| **L.p.** | **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
| **1** | **Wymagania Ogólne** | W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.  Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).  Urządzenie musi być w pełni kompatybilne z urządzeniami typu UTM opisanymi w tym dokumencie. |  |
| **2** | **Interfejsy, Dysk:** | 1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 20 TB. |  |
| **3** | **Parametry wydajnościowe:** | 1. System musi być w stanie przyjmować minimum 50 GB logów na dzień. 2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.   W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje: |  |
| **4** | **Logowanie** | 1. Podgląd logowanych zdarzeń w czasie rzeczywistym.  2. Możliwość przeglądania logów historycznych z funkcją filtrowania.  3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:  a. Listę najczęściej wykrywanych ataków.  b. Listę najbardziej aktywnych użytkowników.  c. Listę najczęściej wykorzystywanych aplikacji.  d. Listę najczęściej odwiedzanych stron www.  e. Listę krajów , do których nawiązywane są połączenia.  f. Listę najczęściej wykorzystywanych polityk Firewall.  g. Informacje o realizowanych połączeniach IPSec.  4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.  5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.  6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy. |  |
| **5** | **Raportowanie** | W zakresie raportowania system musi zapewniać:  1. Generowanie raportów co najmniej w formatach: PDF, CSV.  2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.  3. Funkcję definiowania własnych raportów.  4. Możliwość spolszczenia raportów.  5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. |  |
| **6** | **Korelacja logów** | W zakresie korelacji zdarzeń system musi zapewniać:  1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.  2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.  3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:  • Malware.  • Aplikacje sieciowe.  • Email.  • IPS.  • Traffic.  • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.  4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie. |  |
|  | **Zarządzanie** | 1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.  a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.  2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. |  |
|  | **Serwisy i licencje** | 1. System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. |  |
|  | **Wymagania pozostałe** | 1. Wymaga 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.  2. Wymaga się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży. |  |
|  | **Usługi wdrożeniowe i konfiguracyjne** | **Wykonawca dokona wdrożenia systemu analizy i korelacji zdarzeń bezpieczeństwa:**   1. **Środowisko instalacyjne:**    * Instalacja systemu w środowisku wirtualnym lub montaż w szafie rack, jeżeli zostanie dostarczony jako urządzenie fizyczne.    * Utworzenie stałej łączności sieciowej z urządzeniami generującymi logi oraz dostęp do serwerów NTP i DNS. 2. **Integracja ze źródłami logów:**    * Dokonać integracji z urządzeniami sieciowymi w celu odbioru i analizy logów.    * Skonfigurować funkcję syslog oraz podłączyć urządzenia wskazane przez zamawiającego. 3. **Konfiguracja polityk korelacyjnych i analitycznych:**    * Należy skonfigurować podstawowe reguły korelacyjne wykrywające potencjalne zagrożenia, nieprawidłowości lub anomalie w zachowaniu sieci i użytkowników.    * Wdrożenie powinno obejmować predefiniowane raporty oraz możliwość ich modyfikacji i tworzenia własnych zestawień. 4. **Zarządzanie incydentami:**    * Konieczne jest wdrożenie procedury eskalacji i powiadamiania (np. e-mail) w przypadku wykrycia zdarzeń krytycznych. 5. **Bezpieczeństwo i dostęp:**    * Dokonać integracji w procesie kontroli dostępu do systemu w oparciu o role użytkowników oraz integrację z systemem uwierzytelniania Zamawiającego (np. LDAP, RADIUS).    * Skonfigurowanie mechanizmów ochrony przed nieautoryzowanym dostępem oraz rejestrowanie wszystkich działań administracyjnych. 6. **Szkolenie i dokumentacja:**    * Opracowanie dokumentacji technicznej obejmującej konfigurację, schematy integracji i zasady eksploatacji systemu. |  |

**Licencja umożliwiająca dwuskładnikowe uwierzytelnianie w ramach połączeń IPsec VPN – 1kpl.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Podać producenta oraz nazwę zaoferowanego rozwiązania:**  **……………………………………………………………………………………………………………………………………………………….** | | | |
| **L.p.** | **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
| **1** | **Wymagania ogólne** | 1. W ramach postępowania powinny zostać dostarczone co najmniej 50 tokenów programowych współpracujące z posiadanym przez Zamawiającego urządzeniem oraz nowo dostarczanym UTM, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów oraz w ramach połączeń VPN typu client-to-site. 2. Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile. 3. Dla tokenów na system iOS i Android wymaga się: 4. aktywacji z systemu firewall FortiGate 5. generowania kodu (cyfr) co 30 lub 60 sekund, 6. możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), 7. ochrony dostępu poprzez konfigurowalny kod PIN, 8. Wsparcie/gwarancja producenta lub dostawcy min. 3 miesiące |  |
|  | **Usługi wdrożeniowe i konfiguracyjne** | **Wykonawca dokona:**   * Przypisanie tokenów do użytkowników końcowych oraz przeprowadzenie procesu ich aktywacji (np. za pomocą e-mail lub portalu samoobsługowego). * Weryfikacja poprawności działania tokenów w połączeniach IPSec VPN. |  |

**Szkolenia dla kadry kierowniczej oraz personelu medycznego i administracyjnego – podniesienie świadomości z zakresu Cyberbezpieczeństwa**

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Element**  **konfiguracji** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
| **1** | **Podniesienie świadomości z zakresu Cyberbezpieczeństwa** | **Wymaga się przeprowadzenia cyklicznych szkoleń dla personelu medycznego, administracyjnego oraz kadry kierowniczej:**   1. **Częstotliwość**     * Szkolenia mają odbywać się raz w roku przez okres 3 lat. 2. **Platforma szkoleniowa (portal internetowy):**    * Dostęp online 24/7 przez cały okres trwania umowy.    * Zamieszczenie wszystkich materiałów szkoleniowych (np. filmy, prezentacje, dokumenty PDF).    * Rejestracja uczestnictwa 3. **Materiały szkoleniowe:**    * Materiały powinny być dostępne do pobrania lub wydrukowania dla uczestników.    * Treści aktualizowane przynajmniej raz do roku zgodnie z aktualnymi standardami i przepisami. 4. **Monitoring:**    * Zamawiający musi mieć możliwość bieżącego monitorowania ilości osób, które przystąpiły do szkolenia    * Raportowanie powinno obejmować liczbę uczestników 5. **Potwierdzenie ukończenia szkolenia:**    * Każdy uczestnik po ukończeniu szkolenia powinien być oznaczony jako osoba, która zrealizowała obowiązek szkoleniowy. 6. **Wsparcie techniczne i organizacyjne:**    * Dostęp do wsparcia technicznego dla użytkowników platformy.    * Dostępność pomocy organizacyjnej w godzinach roboczych (telefonicznej i mailowej). 7. **Bezpieczeństwo i ochrona danych:**    * Wszystkie dane użytkowników muszą być odpowiednio zabezpieczone. |  |
| **2** | **Wdrożenie i szkolenie z platformy SZBI** | Do obowiązków Wykonawcy w ramach niniejszego zadania należy wdrożenie oprogramowania do audytu wraz ze szkoleniem i utrzymania SZBI spełniającego min. wymagania:   1. **Wymagane funkcjonalności** 2. Synchronizacja użytkowników systemu z Active Directory. 3. Możliwość nadawania użytkownikom różnych uprawnień. 4. Słowniki    1. Jednostki odzwierciedlające hierarchiczną strukturę organizacyjną.    2. Cele kontroli w ramach doskonalenia SZBI.    3. Dokumenty stanowiące SZBI (lista polityk, procedur, zasad i innych dokumentów, które będą poddawane cyklicznej kontroli pod kątem aktualności i adekwatności).    4. Mechanizmy kontrolne (lista stosowanych zabezpieczeń technicznych i organizacyjnych wraz z możliwością określenia ich rodzaju i roli w SZBI).    5. Usługi kluczowe 5. Checklisty    1. Predefiniowane checklisty pozwalające na przeprowadzenie audytu SZBI.    2. Tworzenie własnych wielopoziomowych checklist służących do przeprowadzania kontroli i udzielania jednoznacznych odpowiedzi na każde pytanie. 6. Plany kontroli    1. Tworzenie długoterminowych planów kontroli.    2. Proces akceptacji poszczególnych planów kontroli (możliwość akceptacji planów przez osobę tworzącą). 7. Programy testowania    1. Tworzenie programów testowania w podziale na obszary objęte kontrolą, okresy, systemy i osoby.    2. Proces akceptacji poszczególnych programów.    3. Definiowanie próby kontrolnej - możliwość zdefiniowania próby kontrolnej do badania. 8. Badanie    1. Przeprowadzanie badania na bazie checklisty - możliwość przeprowadzenia badania na bazie checklisty dla każdego przypadku testowego w ramach próby. Zabezpieczenie przed pominięciem odpowiedzi na pytania z checklisty podczas badania.    2. Możliwość weryfikacji wyników badania przez kontrolowanego pracownika.    3. Zamykanie badania przez kontrolera - kończenie badania i akceptacja wyników kontroli celem generowania nieprawidłowości i zaleceń. 9. Nieprawidłowości    1. Rejestr nieprawidłowości – prowadzenie ewidencji nieprawidłowości wykrytych podczas audytów SZBI.    2. Automatyczne generowanie nieprawidłowości z badania na podstawie udzielonych odpowiedzi - generowanie nieprawidłowości w oparciu o szablon treści nieprawidłowości powiązany z pytaniami na checkliście.    3. Możliwość ręcznego dodawania nieprawidłowości wykrytych podczas kontroli.    4. Proces zarządzania nieprawidłowościami (ewidencja, zatwierdzanie, zamykanie). 10. Zalecenia     1. Rejestr zaleceń – prowadzenie ewidencji zaleceń wydanych podczas audytów SZBI.     2. Automatyczne generowanie zaleceń po badaniu na podstawie udzielonych odpowiedzi - generowanie zaleceń w oparciu o szablon treści zaleceń powiązany z pytaniami na checkliście.     3. Możliwość ręcznego dodawania zaleceń.     4. Proces akceptacji poszczególnych zaleceń w zakresie zatwierdzenia ich realizacji (terminy, osoby odpowiedzialne, koszty).     5. Proces zatwierdzania poszczególnych zaleceń pod kątem sposobu ich realizacji (weryfikacja czy zalecenie zrealizowane zgodnie z wytycznymi).     6. Możliwość importu zaleceń z pliku.     7. Przypisywanie zaleceń do projektów. 11. Rejestry SZBI     1. Rejestr aktywów – prowadzenie ewidencji aktywów wraz z możliwością ewidencji danych dotyczących wsparcia serwisowego dla danego aktywa i zagrożeń związanych z jego brakiem.     2. Rejestr systemów – prowadzenie ewidencji systemów informatycznych wraz z możliwością klasyfikacji tych systemów według atrybutów poufności, integralności i dostępności.     3. Rejestr procesów - prowadzenie ewidencji procesów wraz z ewidencją danych dotyczących wpływu zakłóceń na proces, RTO, RPO, MTD oraz pozwalających na przeprowadzanie analizy BIA dla procesu.     4. Rejestr obszarów bezpiecznych – prowadzenie ewidencji obszarów bezpiecznych wraz z możliwością wskazywania stosowanych zabezpieczeń organizacyjnych i technicznych w danym obszarze.     5. Rejestr nośników – prowadzenie ewidencji nośników danych wraz z możliwością ewidencji informacji wynikających z procedury bezpiecznego usuwania nośników.     6. Rejestr kopii zapasowych – prowadzenie ewidencji kopii zapasowych wraz z możliwością ewidencji szczegółowych informacji o jej wykonywaniu, składowaniu i weryfikacji poprawności jej odtwarzania.     7. Rejestr informacji – prowadzenie ewidencji informacji wraz z możliwością klasyfikacji tych informacji według atrybutów poufności, integralności i dostępności.     8. Rejestr incydentów - prowadzenie ewidencji wykrytych incydentów wraz z jego oceną i klasyfikacją, określeniem rodzaju i skali incydentu oraz jego potencjalnego wpływu na jednostkę wraz z kontrolą poprawności i terminowości obowiązku informacyjnego dotyczącego zgłaszania incydentów.     9. Rejestr ryzyk - identyfikacja ryzyk wraz z możliwością szacowania i oceny, kontroli i monitorowania ryzyka.     10. Rejestr czynności przetwarzania danych osobowych - prowadzenie rejestru czynności przetwarzania realizowanych zarówno jako administrator danych, które w danej czynności są przetwarzane jak i jako podmiot przetwarzający dane osobowe (RODO).     11. Rejestr upoważnień - ewidencja nadanych uprawnień do systemów - prowadzenie ewidencji upoważnień do systemów informatycznych, do których użytkownik ma mieć dostęp, szkoleń dotyczących ochrony danych i podpisanych upoważnień do przetwarzania danych osobowych.     12. Rejestr zmian – prowadzenie ewidencji planowanych i realizowanych zmian w systemach informatycznych wraz z możliwością śledzenia poszczególnych etapów wdrożeń oraz analizy pod kątem planowanych i rzeczywistych terminów i kosztów realizacji.     13. Rejestr kluczowych dostawców – prowadzenie ewidencji kluczowych dostawców usług i sprzętu wraz z analizą ryzyka związanego z upadłością dostawcy i oceny zdolności dostawcy do zachowania ciągłości działa i jakości poziomu świadczonych usług 12. Raporty     1. Protokół pokontrolny - format doc lub pdf automatycznie generowany na podstawie danych z przeprowadzonego badania.     2. Raport z planów kontroli - format xls lub pdf z możliwością parametryzacji raportu     3. Raport z programów badań - format xls lub pdf z możliwością parametryzacji raportu     4. Raport z realizacji zaleceń - format xls lub pdf z możliwością parametryzacji raportu     5. Raport z nieprawidłowości - format xls lub pdf z możliwością parametryzacji raportu     6. Raport z rejestru systemów - format xls lub pdf z możliwością parametryzacji raportu     7. Raport z rejestru aktywów - format xls lub pdf z możliwością parametryzacji raportu     8. Raport z rejestru systemów - format xls lub pdf z możliwością parametryzacji raportu     9. Raport z rejestru procesów - format xls lub pdf z możliwością parametryzacji raportu     10. Raport z rejestru nośników - format xls lub pdf z możliwością parametryzacji raportu     11. Raport z rejestru kopii zapasowych - format xls lub pdf z możliwością parametryzacji raportu     12. Raport z rejestru obszarów bezpiecznych - format xls lub pdf z możliwością parametryzacji raportu     13. Raport z rejestru informacji - format xls lub pdf z możliwością parametryzacji raportu     14. Raport z rejestru zmian - format xls lub pdf z możliwością parametryzacji raportu     15. Raport z rejestru ryzyk- format xls lub pdf z możliwością parametryzacji raportu     16. Raport z rejestru czynności przetwarzania- format xls lub pdf z możliwością parametryzacji raportu     17. Raport z rejestru incydentów- format xls lub pdf z możliwością parametryzacji raportu     18. Raport z rejestru upoważnień- format xls lub pdf z możliwością parametryzacji raportu     19. Sprawozdanie z audytu – model porównawczy w stosunku do poprzedniego audytu oraz poprzedniego do poprzedniego. 13. **Wymagany model wdrożenia** 14. Oprogramowania do audytu i utrzymania SZBI powinno zostać wdrożone w modelu subskrypcyjnym SaaS (Software as a Service) na zasobach spełniających następujące wymagania bezpieczeństwa:     1. Certyfikat ISO 27001 - wymagania dotyczące systemu zarządzania bezpieczeństwem informacji     2. Certyfikat ISO 27018 - bezpieczeństwo przetwarzania i ochrony danych osobowych w chmurze 15. Oprogramowania wdrożone w modelu SaaS z prawem dostępu dla minimum 10 użytkowników Zamawiającego. 16. Minimalny okres trwania subskrypcji – 36 miesięcy. 17. Cena wdrożenia i zaoferowanego czasu subskrypcji powinna być zawarta w cenie oferty. 18. Zaoferowane rozwiązanie powinno charakteryzować się skalowalnością i odpornością na awarię. 19. Konieczne aktualizacje oprogramowania powinny dokonywać się automatyczne bez udziału Zamawiającego. 20. Minimalny poziom dostępności aplikacji – 99%. 21. Wykonawca dokona szkolenia z obsługi wdrożonego rozwiązania .   W ofercie należy podać nazwę zaoferowanego oprogramowania. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Wymaganie ogólne** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
|  | **Gwarancja i wsparcie techniczne** | Zamawiający wymaga zapewnienia min. 36 miesięcznej gwarancji oraz min. 36 miesięcznego nieodpłatnego wsparcia technicznego na wszystkie elementy składające się na przedmiot zamówienia.  Przez „okres gwarancji i wsparcia technicznego” Zamawiający rozumie okres, w którym Wykonawca zapewnia:  1) gwarancję jakości – obejmującą usuwanie wad sprzętu i oprogramowania w ramach gwarancji producenta lub równoważnej,  2) wsparcie techniczne – obejmujące nadzór autorski, aktualizacje, poprawki, łatki bezpieczeństwa, prawo do bezpłatnego korzystania z nowych wersji oprogramowania, zobowiązanie do ich usuwania zgłoszonych usterek i błędów oraz uzyskiwania pomocy i konsultacji dotyczących dostarczonego systemu..  Wsparcie techniczne musi być zapewnione:  – bezpośrednio przez producenta oferowanego systemu/sprzętu, lub  – przez wykonawcę, pod warunkiem posiadania autoryzacji producenta do świadczenia takiego wsparcia i zapewnienia równoważnego poziomu obsługi (SLA, aktualizacje, dostęp do baz wiedzy, poprawki).  Gwarancja sprzętowa i licencyjna musi być realizowana przez producenta (np. rejestracja urządzeń/licencji w systemie producenta).  Okres gwarancji oraz wsparcia technicznego na wszystkie elementy składające się na przedmiot zamówienia liczony jest od dnia podpisania końcowego protokołu odbioru, bez zastrzeżeń ze strony zamawiającego. |  |

|  |
| --- |
| kwalifikowany podpis elektroniczny |