**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Część zamówienia nr 1 - Zadanie nr 1** – pn. **„Dostawa i wdrożenie sprzętu sieciowego do kolokacji”**

**Nr referencyjny sprawy: ZZP.261.ZO.23.2025**

### ZAMAWIAJĄCY:

### Polskie Wydawnictwo Muzyczne

Al. Krasińskiego 11a

31-111 Kraków

**Przedmiot zamówienia obejmuje:**

1. Zakup nowych urządzeń sieciowych:
   * 1. 2 szt. urządzeń UTM z zaawansowanym wsparciem technicznym producenta oraz kompleksową ochroną sieciową (Antywirusową w tym antymalware, Antyspam, IPS, filtrowanie URL, filtrowanie DNS, kontrolą aplikacji, bezpieczeństwo mobilne), przez okres 36 miesięcy
     2. 2 szt. przełączników sieciowych LAN typu switch z zaawansowanym wsparciem technicznym producenta przez okres 36 miesięcy.
2. Konfiguracja i wdrożenie nowych urządzeń sieciowych w kolokacji, konfiguracja polityk firewall, VPN z uwzględnieniem MFA, konfiguracja relokowanych serwerów i macierzy serwerowych w kolokacji.

**Poz. 1 – URZĄDZENIE KLASY UTM – 2 szt.**

|  |  |
| --- | --- |
| **Minimalne wymagane parametry** | |
| **Wymagania Ogólne:** | Dostarczone urządzenie dla systemu bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić 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. |
| **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. |
| **Parametry fizyczne systemu:** | 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:  * 10 portami Gigabit Ethernet RJ-45. * 8 gniazdami SFP 1 Gbps. * 4 gniazdami SFP+ 10 Gbps.  1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System musi być wyposażony w zasilanie AC. |
| **Parametry wydajnościowe:** | 1. W zakresie Firewall’a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 39 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 33 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 5 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 2.5 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps. |
| **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 oraz SSL 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). |
| **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.  1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, hash'e. 3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 5. 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 256 lub 512 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.  1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:  * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.  1. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |
| **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 Antywirusowa:** | 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.  1. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 2. 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. 3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| **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 funkcjonalne i wydajnościowe:** | 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:  a)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox realizowana inline, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Weryfikacja zgodności konfiguracji z dobrymi praktykami producenta (audyt konfiguracji i polityk urządzenia) na okres 36 miesięcy. |
| **Gwarancja oraz wsparcie:** | System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| **Termin realizacji** | Został wskazany w Zapytaniu ofertowym. |
| **Inne:** | Przed podpisaniem umowy lub maksymalnie w dniu jej podpisania, wykonawca zobowiązany jest przedłożyć szczegółowy opis oferowanego przedmiotu zamówienia.  Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.  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. |

**Poz. 2 – URZĄDZENIE SIECIOWE SWITCH – 2 szt.**

|  |  |
| --- | --- |
| **Minimalne wymagane parametry** | |
| **Wymagania Ogólne:** | W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej kolokowanej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.  W celu realizacji konfiguracji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o niżej wymienionych parametrach.  Zamawiający jest w posiadaniu rozwiązania sieciowego opartego o rozwiązania Fortinet. W ramach rozbudowy istniejącego systemu, której celem jest przeniesienie mechanizmów bezpieczeństwa na warstwę dostępową, wymaganym jest dostarczenie przełącznika współpracującego z istniejącym rozwiązaniem w zakresie opisanym w sekcjach: *"Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC"* oraz *"Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa".* |
| **Parametry fizyczne systemu:** | * Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. * Zasilanie AC 230V. * Minimalny zakres temperatury pracy: 0-40ᵒC. |
| **Interfejsy sieciowe - wymagania minimalne** | Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:  a) 24 porty GE RJ-45  b) 4 porty 10GE, SFP+ uplink |
| **Zarzadzanie:** | * Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. * Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). * Wsparcie dla SNMP w wersjach 1-3 * Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. * Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. * Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. * Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). * Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. * Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. * Automatycznie wykonywane rewizje konfiguracji. |
| **Parametry wydajnościowe:** | * Przepustowość urządzenia - min. 124 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 200 Mpps (pakiety na sekundę). * Tablica adresów MAC o pojemności co najmniej 16 k wpisów. * Opóźnienie wprowadzane przez przełącznik - poniżej 1 mikrosekundy. |
| **Wymagane Funkcje:** | * Automatycznej negocjacji prędkości i duplexu dla połączeń. * Obsługa Jumbo Frames. * Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). * Agregacja portów zgodna ze standardem 802.3ad. * Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. * Obsługa routingu statycznego. * Port-mirroring. * Uwierzytelnianie 802.1x na poziomie portu. * Uwierzytelnianie 802.1x w oparciu o adres MAC. * W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). * W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. * W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. |
| **Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC** | 1. Przełącznik musi wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:  * Centralne zarządzanie konfiguracją urządzenia * Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania * Centralne zarządzanie sieciami VLAN. * Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u * Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. * Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. * Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. * Automatyczna detekcja i rekomendacje konfiguracji. * Przesyłanie logów na zewnętrzny serwer syslog. * Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. * Obsługa białych i czarnych list adresów MAC. * Wykrywanie aplikacji komunikujących się w sieci.  1. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 2. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC. |
| **Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa** | * + - 1. System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.       2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing. |
| **Moduły sieciowe i okablowanie** | Wraz z przełącznikami należy dostarczyć następujące elementy:   1. 6 szt. - Moduły 10GE SFP+ transceiver module SR z portami typu LC prosty, tego samego producenta co oferowane przełączniki sieciowe LAN, kompatybilnych z światłowodami wielomodowymi typu OM3 lub OM4 o zasięgu pracy przynajmniej do 100m, kompatybilne z portami sieciowymi oferowanych przełączników i urządzeń klasy UTM z Poz. 1. 2. 4 szt. - Kable światłowodowe dwuwłóknowe wielomodowe OM4 o długości min 2 metry zakończone obustronnie wtykami typu LC prosty kompatybilne z wkładkami światłowodowymi opisanymi powyżej w kolorze fioletowym lub purpurowym. |
| **Gwarancja oraz wsparcie:** | System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.  Moduły SFP+ muszą posiadać3 letnią gwarancję, z wymianą do 5 dni roboczych od daty zgłoszenia awarii. |
| **Termin realizacji** | Został wskazany w Zapytaniu ofertowym. |
| **Inne:** | Przed podpisaniem umowy lub maksymalnie w dniu jej podpisania, wykonawca zobowiązany jest przedłożyć szczegółowy opis oferowanego przedmiotu zamówienia.  Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.  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. |

**Poz. 3 – KONFIGURACJA I WDROŻENIE NOWYCH URZĄDZEŃ SIECIOWYCH W KOLOKACJI, KONFIGURACJA POLITYK FIREWALL, VPN Z UWZGLĘDNIENIEM MFA, KONFIGURACJA RELOKOWANYCH SERWERÓW I MACIERZY SERWEROWEJ W KOLOKACJI.**

|  |  |
| --- | --- |
| **Wymagania** | |
| **Wprowadzenie** | Celem prac wdrożeniowych jest zbudowanie bezpiecznej i wydajnej sieci LAN/WAN w planowanej kolokacji PWM.  W ramach realizacji zadania wymagane jest :   1. konfiguracji i wdrożenia nowych urządzeń sieciowych, w pełnym zakresie funkcjonalności, dostarczone w ramach zadania nr 1, składającego się z:   - 2 szt. urządzeń sieciowych UTM,  - 2 szt. przełączników sieciowych LAN typu Switch,   1. modyfikacja konfiguracji polityk firewall z uwzględnieniem podwójnej autentykacji dla dostępu do zasobów serwerowych i aplikacyjnych z poziomu VPN, z użyciem obecnie używanego przez Zamawiającego rozwiązania MFA, 2. konfiguracja 3 tuneli VPN site-to-site z siedzibami biur Zamawiającego w Krakowie, w Warszawie oraz zewnętrznym magazynem Zamawiającego w Krakowie, 3. konfiguracja środowiska serwerowego relokowanego do kolokacji (w ramach usługi kolokacji w zadaniu 3) w zewnętrznym Data Center składającego się z:   - 6 szt. serwerów fizycznych  - 1 szt. macierzy serwerowej  - 2 szt. serwerów plików (NAS)  w zakresie uruchomienie usług oraz wirtualnych maszyn oraz fizycznych połączeń okablowania w szafie rack zamawiającego oraz logiczną konfigurację adresacji IP urządzeń zamawiającego.  Wdrożenie musi się odbyć na zasadzie modernizacji (migracji) obecnego stanu sieci przy zagwarantowaniu minimalnych przerw w dostępie do Internetu, serwerów, aplikacji oraz sieci w centrali PWM. Obecna konfiguracja urządzeń ma stanowić punkt wyjścia do konfiguracji nowych urządzeń (należy zachować adresacje IP, nr Vlan-ów, itp.).  Wymagania w zakresie zasad realizacji Zamówienia:   1. Prace inwazyjne polegające na wyłączaniu/włączaniu zasilania, wypięcia/wpięcia do sieci, podłączenia kabli dla sieciowych urządzeń aktywnych NIE mogą być wykonywane w godz. pracy Zamawiającego tj. w godzinach 8:00 – 16:00 w dni robocze, 2. Prace nieinwazyjne tj. audyt obecnego stanu sieci (topologia, połączenia, inwentaryzacja urządzeń, analiza konfiguracji) mogą odbywać się o dowolnej porze ale tylko i wyłącznie przy asyście pracownika działu IT Zamawiającego, 3. Wszelkie wizyty celem wykonania prac nieinwazyjnych lub inwazyjnych musze być zaplanowane w postaci harmonogramu wizyt i prac oraz zatwierdzone przez Zamawiającego, 4. Ze względów bezpieczeństwa, podczas prac nie dopuszcza się połączeń VPN i dostępu zdalnego realizowanych przez Wykonawcę, 5. Wgląd i analiza konfiguracji obecnych urządzeń może odbywać się tylko i wyłącznie w obecności pracownika IT Zamawiającego na jego urządzeniu bez możliwości skopiowania konfiguracji na własne urządzenia Wykonawcy, 6. Podczas prac w kolokacji należy dokonać okablowania w szafie rack (porty w patchpanelach, wszelkie krosy do portów RJ45, połączenia światłowodowe) i estetycznego ułożenia z wykorzystaniem dostępnych organizatorów i opasek, 7. Po wykonaniu migracji, Wykonawca udzieli 3-miesiecznego aktywnego wsparcia, z gwarancją SLA na poziomie 2 godz. w trybie 8/5 w godz. 8:00-16:00 (w przypadku potrzeby rozwiązania problemu, zdalnie poprzez doradztwo telefoniczne, a w sytuacji braku możliwości wykonania zdalnie, wymagany jest przyjazd do kolokacji w ciągu 2 godz.) |
| **Założenia techniczne** | 1. Siedziba PWM w Krakowie wraz ze swoim oddziałem w Warszawie i magazynem zewnętrznym w Krakowie musi posiadać bezpieczne i niezawodne połączenia WAN do kolokacji z szyfrowaniem danych IPSEC oraz pełną automatyką przełączania podczas awarii połączenia WAN. 2. Dostęp do Internetu musi być możliwy przy pomocy lokalnego wyjścia do Internetu jak i kolokacje z pełną automatyką przełączania podczas awarii WAN. 3. Konfiguracja musi umożliwiać sterowanie usługami (porty TCP/UDP, serwisy internetowe w tym aplikacje) wykorzystując różne porty WAN (mechanizm SD-WAN). 4. Przełączniki sieciowe LAN (Switch’e) muszą być podłączony (wdrożony) w sposób redundantny tj. w pełni odporny na przerwę (uszkodzenie) dowolnego połączenia. 5. W kolokacji muszą być dostępne sieci VLAN skonfigurowane obecnie na urządzeniach UTM w siedzibie Wydawnictwa (mechanizm VXLAN). 6. Na przełącznikach sieciowych LAN należy wdrożyć w sposób kompleksowy sieci VLAN wraz z właściwym przypisaniem portów. 7. Na urządzeniach UTM należy skonfigurować zaawansowaną politykę bezpieczeństwa zgodnie z polityką bezpieczeństwa obowiązującą u Zamawiającego. 8. Wszystkie urządzenia muszą przejść „utwardzenie” tj. zastosowanie wszelkich najlepszych praktyk bezpieczeństwa, w tym między innymi wyłączenie wszystkich zbędnych usług i portów.   Szczegółowy zakres wdrożenia i konfiguracji urządzeń ostatecznie zostanie ustalony podczas bezpośredniego kontaktu z działem IT Zamawiającego i spisany, po podpisaniu umowy na usługę z Wykonawcą zadania. Należy założyć, że wymagane będzie wdrożenie większości funkcji realizowanych przez urządzenia UTM klasy „enterpise” oraz switche LAN. |
| **Zakres prac** | W ramach wykonania usługi wdrożeniowej Wykonawca zobowiązany jest do wykonania:  **I. Projekt wdrożenia.**  1.Opracowanie dokumentacji uwzględniającej:   1. Harmonogram planowanych prac, uwzględniający **Harmonogram realizacji** opisany poniżej, 2. Audyt i analizę obecnej konfiguracji sieciowej, jej topologii oraz używanych mechanizmów, których konfiguracja ma stanowić punkt wyjścia do opracowania koncepcji wdrożenia nowych urządzeń. W zakresie filtracji ruchu należy założyć, że obecna polityka bezpieczeństwa jest uboga i winna być zbudowana praktycznie od nowa w rozszerzonym zakresie uwzględniając funkcje UTM, 3. Przygotowania koncepcji nowej topologii sieci, najbardziej optymalnej pod względem wydajności i szybkości działania, niezawodności oraz sporządzenie adekwatnych rysunków, 4. Przygotowanie koncepcji konfiguracji nowego sprzętu sieciowego uwzględniając aspekt współpracy/integracji z posiadanymi systemami i urządzeniami oraz przedstawione przez administratorów wymagania. Koncepcja wdrożenia poza tradycyjnymi elementami typu reguły filtracji oraz translacji powinna obejmować szczegółowe wdrożenie wszystkich obsługiwanych przez firewall funkcji UTM, tunele VPN (typu IPSec oraz SSL) z uwzględnieniem używanej przez Zamawiającego podwójnej autentykacji MFA, jak również identyfikację użytkowników z wykorzystaniem kont w Active Directory oraz inteligentne balansowanie obciążenia łącz do Internetu, 5. Opracowanie planowanych zmian konfiguracyjnych w zakresie polityk bezpieczeństwa firewall, 6. Komunikacji między segmentami sieci oraz mechanizmów zabezpieczeń, 7. Przygotowanie procedury awaryjnej "rollback" na wypadek niepowodzenia lub nieprzewidzianych problemów z wdrożeniem urządzeń w kolokacji, gwarantującej szybki powrót do stanu pierwotnego zapewniając podtrzymanie poprawnej pracy usług biznesowych Zamawiającego, 8. Inne zmiany konfiguracyjne.   **II. Wdrożenie:**   1. Wdrożenie firewalla UTM, przełącznika na styku z Internetem z uwzględnieniem wszystkich przedstawionych wymagań i zaakceptowanej przez Zamawiającego koncepcji. Należy w szczególności wykonać: 2. Instalacja i montaż nowych urządzeń UTM i switch w szafie serwerowej oraz wykonanie wszystkich wymaganych połączeń kablowych, 3. Konfigurację w celu dostosowania do zmian konfiguracyjnych związanych z kolokacją, z uwzględnieniem routingów statycznych na urządzeniach a w razie potrzeby wdrożenia routingu dynamicznego (OSPF, BGP), jeśli zaproponowana koncepcja sieci WAN będzie tego wymagać (sieci WAN typu „Hub and Spoke”, Leaf and Spine”, eVPN), 4. Integracja firewalla z systemem autoryzacji Microsoft Active Directory w trybie transparentnym lub przy użyciu dedykowanych agentów, tak aby możliwa była identyfikacja użytkowników przy pomocy SSO (polityka bezpieczeństwa winna być zbudowana w oparciu o grupy użytkowników). Jeśli będzie wymagana dodatkowa instalacja agentów SSO oraz rekonfiguracja polis GPO w AD należy wykonać to w sposób kompleksowy. 5. Konfiguracja dostępu zdalnego VPN (VPN Client, portal WebVPN) z użyciem autoryzacji MFA, przy pomocy certyfikatów oraz różnych poziomów dostępu dla różnych grup użytkowników AD.   2. Wykonania rekonfiguracji innych urządzeń i systemów w sieci w celu poprawnej współpracy z wdrażanymi urządzeniami sieciowymi (uruchomienie agregacji portów LACP, rekonfiguracja STP, integracja z AD itp).  3. Uruchomienie wszystkich usług świadczonych przez przenoszone do kolokacji urządzenia oraz wirtualne maszyny wraz z gwarancją poprawności ich działania.  4. Wykonania testów niezawodności i odporności na różne awarie i scenariusze zdarzeń (awaria linku, urządzenia, zapętlenie ruchu w switchu w dowolnej strefie, awaria dowolnego portu w firewallu, awaria dowolnego łącza do Internetu).  5. Uruchomienie innych rekomendowanych mechanizmów bezpieczeństwa.  6. Po zakończeniu prac, Wykonawca przekaże Zamawiającemu dokumentację wraz z plikami konfiguracyjnymi, które dotyczą przedmiotu zamówienia. Dokumentacja musi zawierać opis wykonanych prac konfiguracyjnych, w celu umożliwienia odtworzenia konfiguracji systemu (zgodnym z niniejszą specyfikacją). Dostarczona dokumentacja musi być dostarczona w wersji elektronicznej edytowalnej. |
| **Wymagania** | * + - 1. Prace wdrożeniowe muszą być wykonane przez zespół inżynierów sieciowych Wykonawcy (co najmniej dwóch pracowników dla zapewnienia zastępstwa w przypadku zdarzeń losowych), spełniającego następujące wymagania:   a) posiadać co najmniej 10 lat doświadczenia we wdrażaniu sieci komputerowych i systemów bezpieczeństwa typu zapory firewall oraz bardzo dobra znajomość bezpieczeństwa sieciowego,  b) posiadać certyfikat eksperta/specjalisty Fortinet na poziomie minimum NSE7 (Network Security Expert) lub FCSS (Fortinet Certified Solution Specialist) lub równoważny Cisco, Paloalto, Checkpoint,  c) uczestniczyć w co najmniej 5 wdrożeniach urządzeń UTM, gdzie wartość dostawy (sprzęt plus usługi) wynosiła co najmniej 200 tys. zł netto oraz dotyczyła firmy z minimum 150 użytkownikami w sieci.  2. Wykonawca musi posiadać co najmniej 5 pisemnych referencji na wdrożenie urządzeń klasy UTM o wartości min. 150 000 zł.  3. Posiadać aktualny status partnera producenta wdrażanych urządzeń na poziomie „Advanced” lub wyższy.  4. Nie dopuszcza się realizacji zadania przez podwykonawców lub użyczenia kompetencji inżynierów sieciowych z innych firm.  5. Zamawiający zastrzega sobie możliwość weryfikacji spełnienia wymagań przed podpisaniem umowy. |
| **Harmonogram realizacji** | * Etap 1: Analiza i przygotowanie projektu – do 2 tygodnia od podpisania umowy * Etap 2: Wdrożenie urządzeń UTM, konfiguracja środowiska serwerowego – do 1 tygodnia po zakończeniu Etapu 1 (planowane dni tygodnia – czwartek, piątek, sobota), przy założeniu posiadania przez Zamawiającego uruchomionych usług kolokacyjnych. W przeciwnym wypadku – do 1 tygodnia po udostępnieniu Zamawiającemu szafy RACK z usługami kolokacyjnymi. * Etap 3: Przekazanie dokumentacji i podpisanie protokołu odbioru prac – do 1 tygodnia po zakończeniu Etapu 2 (przy działających bez problemów usługach i urządzeń). |
| **Gwarancja** | Wykonawca udziela gwarancji na wykonane prace konfiguracyjne i wdrożeniowe, w okresie 12 miesięcy, po zakończeniu prac objętych tym zadaniem. |
| **Termin realizacji** | Został wskazany w Zapytaniu ofertowym. |