Załącznik nr 7

**Opis przedmiotu zamówienia**

Wymagania dotyczące wszystkich dostarczanych produktów:

* Wszystkie elementy składowe produktów muszą być fabrycznie nowe nieużywane oraz nieeksploatowane na wystawach lub imprezach targowych, nie wycofane z produkcji, sprawne techniczne bezpieczne, kompletne i gotowe do pracy, a także muszą spełniać wymagania techniczno-funkcjonalne wyszczególnione w opisie przedmiotu zamówienia.
* Przedmiot zamówienia musi spełniać wszystkie wymogi dotyczące bezpieczeństwa obowiązujące w Polsce.
* Zamawiający wymaga, aby każdy produkt dostarczony został w opakowaniu umożliwiającym jego identyfikację, bez konieczności naruszania opakowania. Uszkodzone i zniszczone opakowanie, upoważnia Zamawiającego do odmowy przyjęcia przedmiotu zamówienia.
* Wykonawca na własny koszt dostarczy sprzęt w siedzibie Zamawiającego, w opakowaniu firmowym odpowiadającym właściwościom sprzętu, zapewniającym jego całość i nienaruszalność.
* Odbiór sprzętu będącego przedmiotem umowy przez Zamawiającego nastąpi na podstawie protokołu odbioru.
* Serwis w trakcie trwania gwarancji bezpłatny dla Zamawiającego.
* Wykaz posiadanych urządzeń UTM oraz przełączników sieciowych zostanie udostępniony wykonawcom pod warunkiem złożenia oświadczenia o zachowaniu poufności informacji.
* Do oferty należy załączyć certyfikaty jakości CE oraz inne równoważne dokumenty potwierdzające wymagania jakościowe oferowanego sprzętu.
* Do oferty należy załączyć karty katalogowe / specyfikacje techniczne produktów.

1. **Urządzenie brzegowe UTM ze wsparciem technicznym i szkoleniem – 1 sztuka**

**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.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | |
|  | **Identyfikacja** | **Nazwa producenta i model oraz rodzaj licencji (jeśli dotyczy)** | **Wypełnić:** |
|  | Redundancja, monitoring i wykrywanie awarii | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. | |
| Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. | |
| Monitoring stanu realizowanych połączeń VPN. | |
| System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. | |
|  | Interfejsy | System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:   * 10 portami Gigabit Ethernet RJ-45, * 8 gniazdami SFP 1 Gbps, * 4 gniazdami SFP+ 10 Gbps. | |
| System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. | |
| System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. | |
|  | Zasilanie | System jest wyposażony w redundantne zasilanie AC. | |
|  | Wkładki | Dwie dedykowane wkładki 10GE SFP+ transceiver module, SR 10 GE SFP+ | |
|  | Wydajność | W zakresie Firewall’a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę. | |
| Przepustowość IPS nie mniej niż 5.3 Gbps | |
| Przepustowość NGFW (firewall + kontrola aplikacji + IPS) nie mniej niż 3 Gbps | |
| Przepustowość IPSeC VPN (512 bajtów) nie mniej niż 33 Gbps | |
| 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, POP3. 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. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i 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. 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 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.  1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:  * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. | |
|  | 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, oznaczeń Type of Service w nagłówkach IP). 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. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 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 chmurze. 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 dwuskładnikowego. 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 dwu-składnikowego 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 oraz wykonane testy. | |
|  | 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 do 30 czerwca 2026 roku. | |
|  | Gwarancja oraz wsparcie | * System jest objęty serwisem gwarancyjnym przez okres do 30 czerwca 2026 roku. * W przypadku wykrycia wadliwości urządzenia należy dokonać naprawy lub wymiany sprzętu w trybie AHR (Advanced Hardware Replacement), co oznacza szybką wymianę sprzętu w celu minimalizacji przestojów w działalności zamawiającego. * W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. | |
|  | Rozszerzone wsparcie serwisowe | * System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora do 30 czerwca 2026 roku. * Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Wymagania powinny być potwierdzone dokumentami: * Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). * Certyfikat ISO 9001 podmiotu serwisującego. | |
|  | Warunki realizacji zamówienia – wdrożenie | * Dostawca jest odpowiedzialny za dostarczenie urządzeń. Dostawa musi zawierać wszystkie niezbędne komponenty i akcesoria wymagane do pełnej funkcjonalności urządzeń. * Dostawca ma obowiązek zabezpieczyć i przenieść wszystkie obecnie działające polityki bezpieczeństwa z istniejącego urządzenia UTM (z kończącym się wsparciem i EOL) na nowo dostarczone urządzenie oraz wydzielenie sieci VLAN zgodnie z zapotrzebowaniem zamawiającego. Proces ten musi być wykonany w taki sposób, aby zapewnić ciągłość ochrony i minimalizować ryzyko wystąpienia luk w zabezpieczeniach podczas przejścia na nowe urządzenia. * Dostawca będzie odpowiedzialny za pełną integrację nowych urządzeń UTM z istniejącą infrastrukturą sieciową Zamawiającego, integracja z Active Directory oraz zakupionymi nowymi przełącznikami w tym postępowaniu, w tym integracja z przełącznikami typu I pracującymi w stacku. * Wykaz posiadanych urządzeń UTM oraz przełączników sieciowych zostanie udostępniony wykonawcom pod warunkiem złożenia oświadczenia o zachowaniu poufności informacji. * Migracja polityk bezpieczeństwa z urządzenia dotychczasowego (z kończącym się i wsparciem i EOL) na nowe (UTM zgodny ze specyfikacją); wydzielenie sieci VLAN oraz polityk przepływu danych pomiędzy sieciami VLAN – zgodnie z zapotrzebowanie zamawiającego. | |
|  | Szkolenie | Szkolenie dla 2 administratorów działu informatyki wskazanych przez Zamawiającego. Szkolenie w języku polskim, w wymiarze minimum 2 dni szkoleniowych po 8 godzin dziennie w siedzibie Zamawiającego.  Szkolenie zostanie zrealizowane w terminie do końca 2025 roku, w terminie do 30 dni od dnia powiadomienia Wykonawcy przez Zamawiającego o zamiarze skorzystania ze szkolenia. W przypadku niewykonania przez Wykonawcę zobowiązania do wykonania szkolenia Zamawiającemu przysługuje uprawnienie do zlecenia zastępczego do zrealizowania usługi przez podmiot trzeci – na koszt Wykonawcy.  Szkolenie z zakresu funkcjonalności oraz metod zarządzania UTM, minimum w tym:   * Podstawowe czynności administracyjne   + Konfiguracja domyślna,   + Aktualizacja firmware   + Kopia zapasowa konfiguracji   + Serwisy licencyjne * Konfiguracja wstępna,   + Tryby pracy   + Konfiguracja interfejsów sieciowych   + Konfiguracja DHCP   + Dostęp administracyjny * Logowanie – metody logowania i ich konfiguracja   + Syslog * Konfiguracja zapory ogniowej   + Obiekty i grupy   + Reguły   + Translacja adresów SNAT i DNAT   + Metody uwierzytelnienia użytkowników   + Grupy użytkowników * Konfiguracja modułów bezpieczeństwa   + Moduł antywirusowy   + Moduł antyspamowy   + Moduł IPS i DLP   + Kontrola aplikacji   + Kontrola WWW * Wirtualne sieci prywatne - VPN   + Konfiguracja tuneli VPN Site-to-Site IPsec   + Konfiguracja dostępu zdalnego SSL - VPN | |

1. **System centralnego składowania logów ze wsparciem technicznym i wdrożeniem**

**Wymagania ogólne:**

W ramach postępowania wymaganym jest dostarczenie i wdrożenie 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: 6.5, 6.7; Microsoft Hyper-V wersje: 2016, 2019, 2022,2025; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | |
|  | **Identyfikacja** | **Nazwa systemu / rozwiązania:** | **Wypełnić:** |
| 1. M | Interfejsy, dyski | System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB. | |
|  | Parametry wydajnościowe | 1. System musi być w stanie przyjmować minimum 5 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: | | | |
|  | 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 informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:    * Listę najczęściej wykrywanych ataków.    * Listę najbardziej aktywnych użytkowników.    * Listę najczęściej wykorzystywanych aplikacji.    * Listę najczęściej odwiedzanych stron www.    * Listę krajów , do których nawiązywane są połączenia.    * Listę najczęściej wykorzystywanych polityk Firewall.    * 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. | |
|  | Raportowanie | 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. | |
|  | Korelacja logów | 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.  1. 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.  * Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.  1. 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 | Wsparcie: System musi być objęty serwisem producenta do 30 czerwca 2026 roku, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. | |

1. **Zarządzalne przełączniki sieciowe – typ I – 2 sztuki**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Parametr oferowany** |
| 1. M | **Identyfikacja** | **Nazwa producenta i model** | **Wypełnić:** |
|  | Informacje ogólne | * Zarządzalny * Warstwa L2 i L3 * Montaż w szafie rack, wysokość 1U |  |
|  | Port konsoli | * Na przodzie obudowy * Dołączony kabel ze złączem USB |  |
|  | Ilość portów | Min. 12 portów SFP+ oraz 12 portów 1/2,5/5/10G niezależne |  |
|  | Dodatkowe wkładki | Wszystkie porty SFP+ z wkładkami 10GE SR SFP+ |  |
|  | Chłodzenie | od przodu do tyłu obudowy |  |
|  | ilość przełączników w stosie | Min. 8 |  |
|  | Gwarancja | Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (minimum do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji. |  |
|  | Przepustowość | min. 480 Gb/s |  |
|  | Wydajność | min. 356 Mp/s |  |
|  | MTBF | min. 150000 godzin |  |
|  | Pamięć bufora pakietów | 4MB |  |
|  | Łączenie w stos | możliwość łączenia w stos przełączników typu I, II i III |  |
|  | Warunki realizacji zamówienia – wdrożenie | * Stworzenie osobnego stacka z dwóch przełączników typu I – integracja z nowym UTM oraz istniejącą infrastrukturą Zamawiającego * Dostawca jest odpowiedzialny za dostarczenie urządzeń. * Dostawa musi zawierać wszystkie niezbędne komponenty i akcesoria wymagane do pełnej funkcjonalności urządzeń. |  |
|  | Wymagania dodatkowe | * Tablica MAC min. 16K * Tablica ARP min. 4K * Tablica NDP min. 512 * Port zarządzania Out-of-band; * Web GUI * HTTPs * CLI * Telnet * SSH * SNMP * MIB RSPAN * Radius * TACACS+ * DiffServ * Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram * Wymaga się aby interfejs web miał możliwość wykonywania poleceń tekstowych CLI bez potrzeby tworzenia oddzielnego połączenia Telnet lub SSH. * IPv4/IPv6 Multicast filtering * IGMPv3 MLDv2 Snooping * ASM & SSM * IGMPv1,v2 Querier * Policy-based routing (PBR) * LLDP-MED * Spanning Tree * Green Ethernet * STP * MTP * RSTP * EEE (802.3az) * GVRP/GMRP * Q in Q * Private VLAN * DOT1X * MAB * Captive Portal * DHCP Snooping * Dynamic ARP * Inspection * IP Source Guard * Min. ilość obsługiwanych VLAN 4K * DHCP Server min. 2K rezerwacji |  |

1. **Zarządzalne przełączniki sieciowe – typ II – 5 sztuk**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Parametr oferowany** |
| 1. 11 | **Identyfikacja** | **Nazwa producenta i model** | **Wypełnić:** |
|  | Informacje ogólne | * Zarządzalny * Warstwa L2 i L3 * Montaż w szafie rack, wysokość 1U |  |
|  | Port konsoli | * Na przodzie obudowy * Dołączony kabel ze złączem USB |  |
|  | Ilość portów | 48 PoE+ 1GBASE-T, 4 x SFP+ |  |
|  | Dodatkowe wkładki | Minimum 2 wkładki 10GE SR SFP+ |  |
|  | Gwarancja | Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (minimum do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji |  |
|  | Przepustowość | min. 176 Gb/s |  |
|  | Wydajność | min. 130 Mp/s |  |
|  | Pamięć bufora pakietów | 4 MB |  |
|  | MTBF | min. 150000 godzin |  |
|  | Zasilanie | Zasilanie redundantne |  |
|  | Łączenie w stos | możliwość łączenia w stos przełączników sieciowych typu I, II i III |  |
|  | Warunki realizacji zamówienia – wdrożenie | * Stworzenie osobnego stacka z pięciu przełączników, typu II, niższego poziomu – integracja z przełącznikami typu I oraz istniejącą infrastrukturą Zamawiającego. * Dostawca jest odpowiedzialny za dostarczenie urządzeń. * Dostawa musi zawierać wszystkie niezbędne komponenty i akcesoria wymagane do pełnej funkcjonalności urządzeń. |  |
|  | Wymagania dodatkowe | * Tablica MAC min. 16K * Tablica ARP min. 4K * Tablica NDP min. 512 * Port zarządzania Out-of-band * Web GUI * Wymaga się aby interfejs web miał możliwość wykonywania poleceń tekstowych CLI bez potrzeby tworzenia oddzielnego połączenia Telnet lub SSH. * HTTPs * SSH * Obsługa PTPv2 * STP, MTP, RSTP PV(R)STP * IPv4/IPv6 * PIM-SM * PIM-DM * SSM * Obsługa IEEE 802.1AS-2011 gPTP, IEEE 802.1Qav-2009 FQTSS, IEEE 802.1Qat-2010 MSRP, IEEE 802.1ak MMRP, IEEE 802.1ak MVRP * Kształtowanie ruchu na wejściu oraz wyjściu co 1 Kbps * Radius * TACACS+ * IGMPv1,v2 Querier * Min. ilość obsługiwanych VLAN 4K * DHCP Server min. 2K rezerwacji |  |

1. **Zarządzalne przełączniki sieciowe – typ III – 1 sztuka**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Parametr oferowany** |
| 1. M | **Identyfikacja** | **Nazwa producenta i model** | **Wypełnić:** |
|  | Informacje ogólne | * Zarządzalny * Warstwa L2 i L3 * Montaż w szafie rack, wysokość 1U |  |
|  | Port konsoli | * Na przodzie obudowy * Dołączony kabel ze złączem USB |  |
|  | Ilość portów | 24 PoE+ 1GBASE-T, 4 x SFP+ |  |
|  | Dodatkowe wkładki | Minimum 2 wkładki 10GE SR SFP+ |  |
|  | Bufor | 2MB |  |
|  | Gwarancja | Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (minimum do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji |  |
|  | Przepustowość | min. 128 Gb/s |  |
|  | Wydajność | min. 95 Mp/s |  |
|  | MTBF | 150000 godzin |  |
|  | Łączenie w stos | możliwość łączenia w stos przełączników sieciowych typu I, II i III |  |
|  | Warunki realizacji zamówienia – wdrożenie | * Dostawca jest odpowiedzialny za dostarczenie urządzeń. * Dostawa musi zawierać wszystkie niezbędne komponenty i akcesoria wymagane do pełnej funkcjonalności urządzeń. |  |
|  | Wymagania dodatkowe | * Tablica MAC min. 16K * Tablica ARP min. 4K * Tablica NDP min. 512 * Port zarządzania Out-of-band * Web GUI * Wymaga się aby interfejs web miał możliwość wykonywania poleceń tekstowych CLI bez potrzeby tworzenia oddzielnego połączenia Telnet lub SSH. * HTTPs * SSH * Obsługa PTPv2 * STP, MTP, RSTP PV(R)STP * IPv4/IPv6 * PIM-SM * PIM-DM * SSM * Obsługa IEEE 802.1AS-2011 gPTP, IEEE 802.1Qav-2009 FQTSS, IEEE 802.1Qat-2010 MSRP, IEEE 802.1ak MMRP, IEEE 802.1ak MVRP * Kształtowanie ruchu na wejściu oraz wyjściu co 1 Kbps * Radius * TACACS+ * IGMPv1,v2 Querier * Min. ilość obsługiwanych VLAN 4K * DHCP Server min. 2K rezerwacji |  |

1. **Zarządzalne przełączniki sieciowe – typ IV – 4 sztuki**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Parametr oferowany** |
| 1. M | **Identyfikacja** | **Nazwa producenta i model** | **Wypełnić:** |
|  | Informacje ogólne | * Zarządzalny * Warstwa L2 i L3 |  |
|  | Port konsoli | * Na przodzie obudowy * Dołączony kabel ze złączem USB |  |
|  | Ilość portów | 8 portów 1GBaseT PoE+, 2 x SFP+ |  |
|  | Dodatkowe wkładki | Minimum 1 wkładka 10GE SR SFP+ |  |
|  | Bufor | 2MB |  |
|  | Gwarancja | Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (minimum do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji |  |
|  | Przepustowość | min. 56 Gb/s |  |
|  | Wydajność | min. 41 Mp/s |  |
|  | MTBF | 150000 godzin |  |
|  | Wymagania dodatkowe | * Budżet PoE min. 220W * Tablica MAC min. 16K * Tablica ARP/NDP min. 4000 * Możliwość wyłączenia wentylatorów z poziomu interfejsu web wspierane przez producenta w celu wyeliminowania hałasu generowanego przez przełącznik * Port zarządzania Out-of-band * Web GUI * Wymaga się aby interfejs web miał możliwość wykonywania poleceń tekstowych CLI bez potrzeby tworzenia oddzielnego połączenia Telnet lub SSH. * HTTPs * SSH * Przełącznik powinien mieć możliwość montażu uchwytów rack z przodu lub z tyłu obudowy przełącznika. Dodatkowo w raz z przełącznikiem należy dostarczyć oryginalny zestaw do montażu w szafie rack, który umożliwi cofnięcie przełącznika o około 2 cale w celu zwiększenia przestrzeni na okablowanie sieciowe pomiędzy dziwami szafy a przełącznikiem. * Przełącznik powinien mieć możliwość montażu za pomocą uchwytów w standardzie VESA * Obsługa PTPv2 * STP, MTP, RSTP PV(R)STP * IPv4/IPv6: * PIM-SM * PIM-DM * SSM * Kształtowanie ruchu na wejściu oraz wyjściu co 1 Kbps * Radius * TACACS+ * Min. ilość obsługiwanych VLAN 4K * DHCP Server min. 2K rezerwacji |  |

1. **Okablowanie sieciowe**

* Patchcord LC/UPC-LC/UPC MMD 0,5m – 10 szt.
* Patchcord LC/UPC-LC/UPC MMD 10m – 3 szt.
* Patchcord LC/UPC-LC/UPC MMD 1m – 10 szt.
* Patchcord LC/UPC-LC/UPC MMD 20m – 3 szt.
* Patchcord Cat. 7; RJ45; 10Gbps 1m – 6 szt.
* Patchcord Cat. 7; RJ45; 10Gbps 2m – 6 szt.
* Patchcord Cat. 7; Rj45; 10Gbps 3m – 4 szt.