*Załącznik nr 1a do umowy projekt* *dla zadania nr 1*

**FORMULARZ RZECZOWY**

**OPIS OFEROWANEGO PRZEDMIOTU ZAMÓWIENIA**

**Zadanie 1**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **L.P.** | **Urządzenie** | | **Wymagane minimalne \*** | **Oferowane parametry**  **WYPEŁNIA WYKONAWCA** |
| 1 | UTM -Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS) | Wymagania Ogólne | Dostarczony system 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 musi dawać możliwość pracy w jednym trybów: Routera z funkcją NAT oraz transparentnym.  System musi wspierać 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 – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.  2.Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.  3.Monitoring stanu realizowanych połączeń VPN.  4.System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |  |
| Interfejsy, Dysk, Zasilanie | 1.System realizujący funkcję Firewall musi dysponować minimum:  •16 portami Gigabit Ethernet RJ-45.  •8 gniazdami SFP 1 Gbps.  •2 gniazdami SFP+ 10 Gbps.  2.System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.  3.W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.  4.System musi być wyposażony w dwa zasilania AC. |  |
| Parametry wydajnościowe | 1.W zakresie Firewall’a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 56 tys. nowych połączeń na sekundę.  2.Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.  3.Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 64 B.  4.Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 1518 B.  5.Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.2 Gbps.  6.Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.  7.Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.6 Gbps.  8.Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.  9.Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps. |  |
| Funkcje Systemu Bezpieczeństwa | W ramach dostarczonego systemu ochrony muszą być 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 – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS.  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.Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.  10.Analiza ruchu szyfrowanego protokołem SSL.  11.Analiza ruchu szyfrowanego protokołem SSH. |  |
| Polityki, Firewall | 1.Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  2.System musi zapewniać 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 musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  4.Element systemu realizujący funkcję Firewall musi integrować 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).  •Nuage Networks VSP.  •OpenStack.  •VMware vCenter (ESXi).  •VMware NSX. |  |
| Połączenia VPN | 1.System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  •Wsparcie dla IKE v1 oraz v2.  •Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).  •Obsługa protokołu Diffie-Hellman grup 19 i 20.  •Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.  •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.  •Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.  •Mechanizm „Split tunneling” dla połączeń Client-to-Site.  2.System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:  •Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać 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 musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |  |
| Routing i obsługa łączy WAN | 1.W zakresie routingu rozwiązanie powinno zapewniać obsługę:  •Routingu statycznego.  •Policy Based Routingu.  •Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP. |  |
| Zarządzanie pasmem | 1.System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.  2.Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.  3.System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
| Ochrona przed malware | 1.Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).  2.System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.  3.System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).  4.System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.  5.System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |  |
| Ochrona przed atakami | 1.Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.  2.System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.  3.Baza sygnatur ataków powinna zawierać minimum 1500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  4.Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.  5.System musi zapewniać 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) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.  7.Wykrywanie i blokowanie komunikacji C&C do sieci botnet |  |
| Kontrola aplikacji | 1.Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.  2.Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  3.Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  4.Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.  5.Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |  |
| Kontrola WWW | 1.Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.  2.Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.  3.Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.  4.Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.  5.System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.  6.Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.  7.W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |  |
| Uwierzytelnianie użytkowników w ramach sesji | 1.System Firewall musi umożliwiać 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.Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.  3.Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |  |
| Zarządzanie | 1.Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.  2.Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.  3.Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.  4.System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.  5.System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.  6.Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.  7.Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  |
| Logowanie | 1.Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania, raportowania, korelacji zdarzeń, powiadamiania o incydentach) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.  2.W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.  3.Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.  4.Musi istnieć możliwość logowania do serwera SYSLOG. |  |
| Certyfikaty | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall. |  |
| Asysta techniczna on-line | 1.Jednodniowa asysta techniczna przy wdrożeniu dostarczonego systemu bezpieczeństwa będzie wykonana przez inżyniera z certyfikatem producenta urządzenia. Inżynier przygotuje konfigurację bazową. Dystrybucja konfiguracji na urządzenia docelowe jest po stronie Zamawiającego. Samo podłączanie urządzeń będzie odbywało się z asystą inżyniera.  2.Zakres działań podczas wdrożenia:  •Analiza obecnych polityk bezpieczeństwa oraz infrastruktury sieciowej (optymalizacja zgodna z aktualnymi trendami panującymi w sferze zagrożeń sieciowych).  •Przygotowanie środowiska (rejestracja, aktualizacja oprogramowania, uruchomienie na rekomendowanej przez Wykonawcę wersji firmware ).  •Konfiguracja urządzeń zgodnie z założeniami polityki bezpieczeństwa Zamawiającego.  (interfejsy sieciowe, routing, polityki firewall, DNS, Web filtering, anti-spam, anti-virus, controla aplikacji, ips, ids, virtual private network, zarządzanie pasmem, uwierzytelnianie użytkowników, redundancja dostępu do internetu, logowanie oraz raportowanie, alerty administracyjne, dostosowanie do współpracy z zewnętrznym systemem logowania i raportowania)  •Weryfikacja poprawności implementacji (testy akceptacyjne).  •Kopia bezpieczeństwa konfiguracji wdrożonych urządzeń.  •Instruktarz obsługi urządzenia poprzez GUI (co najmniej 2 godziny) przeprowadzony przez inżyniera. |  |
| Serwisy i licencje | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres wskazany w ofercie. | **na okres …. miesięcy**  ***(wpisać to samo co   w pkt 4 oferty*** *i)* |
| Gwarancja oraz wsparcie | 1.System musi być objęty serwisem gwarancyjnym producenta przez okres wskazany w ofercie, 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.  2.Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim w trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji, to co najmniej jeden z inżynierów musi posiadać najwyższy stopień certyfikacji) oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych. Wszystkie certyfikaty należy dołączyć do oferty.  3.System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wskazany w ofercie. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji winien być nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.  4.Oferent winien przedłożyć dokumenty:  a. Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).  b. Certyfikat ISO 9001 podmiotu serwisującego. |
| Oferowany model Urządzenia  ***(wymienić również wszystkie oferowane z urządzeniem licencje i serwisy***) |  | |
| 2 | Wirtualna maszyna do zapisywania zdarzeń z UTM, analizowania i raportowania | Wymagania Ogólne | W ramach postępowania wymagane jest dostarczenie wirtualnej maszyny do zapisywania zdarzeń z UTM, analizowania i raportowania zdarzeń, zapewniającej współpracę z dostarczonym przez Wykonawcę urządzeniem opisanym w wierszu 1. – UTM - Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS).  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). |  |
| Interfejsy, Dysk | 1.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:  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. |  |
| 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. |  |
| 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 musi 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 dostarczyć dedykowaną konsolę 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. |  |
| Asysta techniczna on-line | 1. Asysta przy wdrożeniu będzie wykonana przez inżyniera z certyfikatem producenta.  2.Zakres działań podczas wdrożenia:  •Przygotowanie środowiska (rejestracja i instalacja maszyny wirtualnej, aktualizacja oprogramowania, uruchomienie na rekomendowanej przez Wykonawcę wersji firmware).  •Konfiguracja i podłączenie - logowanie oraz raportowanie, alerty administracyjne z konkretnych urządzeń (co najmniej 2 urządzenia, w tym zaoferowany przez Wykonawcę UTM). Ustawienia funkcji SOC oraz IoC  •Weryfikacja poprawności implementacji (testy akceptacyjne).  •Kopia bezpieczeństwa konfiguracji wdrożonych urządzeń.  •Instruktarz obsługi urządzenia poprzez GUI (co najmniej 2 godziny) przeprowadzony przez inżyniera. |  |
| Serwisy, licencje i gwarancja | System musi być objęty serwisem producenta przez okres wskazany w ofercie, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. | **na okres …. miesięcy**  ***(wpisać to samo co   w pkt 4 oferty*** *i)* |
| Oferowany model Urządzenia  ***(wymienić również wszystkie oferowane z urządzeniem licencje i serwisy***) |  | |

\* W Załączniku zawarto minimalne wymagania odnośnie produktów objętych zamówieniem co oznacza, że Wykonawca może zaoferować przedmiot zamówienia charakteryzujący się lepszymi parametrami technicznymi lub użytkowymi.

UWAGA: Niespełnienie wymagań minimalnych określonych w powyższym formularzu skutkować będzie odrzuceniem oferty

Wykonawca wypełnia tylko pola w kolorze białym, ze szczególnym uwzględnieniem pól dotyczących serwisów, licencji, gwarancji oraz wsparcia, gzie koniecznie musi podać tylko jeden okres ( np. 12 miesięcy). Inne zapisy będą interpretowane jako niespełnienie wymagań oraz spowodują odrzucenie oferty.

………………………………………………………………….

**.**

**Data,** ELEKTRONICZNY PODPIS WYKONAWCY lub

osoby uprawnionej do składania oświadczeń woli

w imieniu Wykonawcy, w postaci:

- kwalifikowanego podpisu elektronicznego,

- **LUB** podpisu zaufanego,

- **LUB** podpisu osobistego e-dowód