OPIS PRZEDMIOTU ZAMÓWIENIA

I. Wymagania ogólne dotyczące zamawianych urządzeń.

1. Wszystkie urządzenia muszą być fabrycznie nowe. Przed dostawą sprzęt musi być zarejestrowany przez producenta, bezpośrednio na Zamawiającego, jako jedynego użytkownika po opuszczeniu fabryki. Jeśli producent nie prowadzi rejestracji sprzętu, to wymaga się deklaracji producenta, iż sprzęt jest fabrycznie nowy.
2. W momencie oferowania wszystkie elementy oferowanego systemu muszą być dostępne (dostarczane przez producenta) w dacie złożenia oferty i nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
3. Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
4. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
5. Do każdego urządzenia i oprogramowania musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku angielskim lub polskim.
6. Sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim.
7. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych
8. Korzystanie przez Zamawiającego z dostarczonego produktu nie może naruszać majątkowych praw autorskich osób trzecich.
9. Wszystkie urządzenia muszą posiadać oznakowanie CE produktu albo spełniać normy równoważne.
10. Wszystkie urządzenia, jeśli nie podano inaczej, muszą współpracować z siecią energetyczną o parametrach : 230 V ± 10% , 50 Hz.
11. Zamawiający może zażądać przed dostawą dokumentu zawierającego listę numerów seryjnych dostarczanego sprzętu w celu weryfikacji spełnienia warunków gwarancyjnych
12. Zamawiający sprawdzi spełnienie powyższych warunków w polskim biurze producenta na podstawie numeru seryjnego urządzenia – w przypadku niezgodności deklaracji Wykonawcy z opinią producenta - Zamawiający odmówi odbioru przedmiotu zamówienia, jako niezgodnego ze specyfikacją istotnych warunków zamówienia.
13. Wszystkie komponenty muszą pochodzić od producenta oraz być fabrycznie zainstalowane przez producenta.

Szczegółowa specyfikacja sprzętowa:

* 1. Router brzegowy - **2 sztuki**

**Nazwa producenta: ……………………………………………………………………………..**

**Typ produktu, model: …………………………………………………………………………..**

|  |  |  |  |
| --- | --- | --- | --- |
| **Wymagania minimalne** | | | **Parametry oferowane przez Wykonawcę** |
|  | Wymagania Ogólne | Dostarczony sprzęt musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były realizowane 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 z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu. |  |
|  | **Wymagania systemowe** | 1. Firewall. 2. Ochrona w warstwie aplikacji. 3. Dostępne 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. Rozwiązanie realizujący funkcję routera brzegowego musi dysponować minimum:  * 2 portami Gigabit Ethernet RJ-45 do zarządzania. * 16 portami GE RJ45 * 8 gniazdami GE SFP * 4 gniazdami 10 GE SFP+ * 4 gniazdami 25GE SFP28/ 10GE SFP+/ GE SFP  1. Router brzegowy musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. Router brzegowy powinien dawać 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. 4. System musi być wyposażony w lokalną przestrzeń dyskową o łącznej pojemności 480GB. 5. System musi być dostarczony z wkładkami:  * 25 GE Multimode – 8 szt. * 25 GE Singlemode – 8 szt. |  |
|  | Parametry wydajnościowe: | 1. W zakresie Firewall’a obsługa nie mniej niż 8 mln jednoczesnych połączeń oraz 550.000 nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 137 Gbps dla pakietów 512 B. 3. Przepustowość Stateful Firewall: nie mniej niż 70 Gbps dla pakietów 64 B. 4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 32 Gbps. 5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 55 Gbps. 6. 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 10 Gbps. 7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 10 Gbps. 8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 9 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, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe 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. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. 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.  1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |  |
|  | Połączenia VPN | 1. Rozwiązanie 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.  1. 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. |  |
|  | 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 oraz PIM.  1. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. |  |
|  | Zarządzanie pasmem | 1. Router brzegowy 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. |  |
|  | Kontrola Antywirusowa | 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). |  |
|  | Ochrona przed atakami | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Ochrana przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 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 2100 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. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 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. |  |
|  | Uwierzytelnianie użytkowników w ramach sesji | 1. Router brzegowy 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.  1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 2. 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 dwu-składnikowego dla dostępu administracyjnego. 4. Zaproponowane rozwiązanie 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. Router brzegowy musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |  |
|  | Logowanie | 1. 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. 2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 3. Musi istnieć możliwość logowania do serwera SYSLOG. |  |
|  | Kompatybilność | Możliwość integracji, z posiadanym przez Zamawiającego, systemem FortiSandbox w celu przesyłania zdefiniowanych typów plików do analizy pod kątem nieznanych zagrożeń. Rozwiązanie musi mieć możliwość korzystania z wewnętrznej bazy sygnatur przechowywanej na FortiSandbox. |  |
|  | Serwisy i licencje | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  a)     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 36 miesięcy. |  |
|  | Gwarancja oraz wsparcie | 1. Gwarancja: Urządzenie musi być objęty serwisem gwarancyjnym 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. 2. Oferent winien przedłożyć oświadczenie producenta, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań |  |
|  | Analiza logów | W ramach dostawy routera brzegowego należy dostarczyć centralny system 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 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.  **Interfejsy, Dysk:**  System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB.  **Parametry wydajnościowe:**   * 1. System musi być w stanie przyjmować minimum 10 GB logów na dzień.   2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 10000 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. Możliwość dostosowania widoku wyświetlanych logów poprzez dodawanie, usuwanie oraz zmianę kolejności kolumn zawierających elementy logowanego zdarzenia.   4. Możliwość wykrywania w sieci urządzeń, które zostały przejęte przez atakującego lub złośliwe oprogramowanie i stanowią zagrożenie dla wewnętrznych systemów. Funkcja pozwala dodatkowo przeskanować wcześniej wykryte urządzenia w celu weryfikacji skuteczności podjętych działań usuwających zagrożenie.   5. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia NGFW oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa na przestrzeni zadanego czasu.   Muszą one obejmować co najmniej:   * + - * 1. listę najczęściej wykrywanych ataków,         2. listę najbardziej aktywnych użytkowników/źródeł ruchu,         3. listę najczęściej wykorzystywanych aplikacji,   1. listę najczęściej odwiedzanych stron www,   2. listę krajów, do których nawiązywane są połączenia,   3. listę najczęściej wykorzystywanych polityk Firewall,   4. Informacje o realizowanych połączeniach IPSec i SSL VPN,   5. Listę najczęściej występujących zdarzeń systemowych.   6. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych za pomocą protokołu Syslog i/lub CEF. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.   7. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem portów UDP/514 oraz TCP/514.   8. System musi umożliwiać cykliczny eksport logów do zewnętrznego systemu w celu ich długoterminowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP i/lub SCP. Administrator musi mieć możliwość określenia, kiedy ma następować eksport logów.   9. System musi prezentować informacje na temat ilości przestrzeni dyskowej wykorzystanej na przechowywanie logów.   **Raportowanie**  W zakresie raportowania system musi zapewniać:   * 1. Generowanie raportów co najmniej w formatach: HTML, 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 oraz automatycznego przesłania raportu na zewnętrzny serwer za pomocą protokołu FTP lub SCP.   6. Możliwość filtrowania danych uwzględnianych w procesie tworzenia danego raportu, m.in. możliwość ograniczenia zakresu raportu do danych z wybranych urządzeń NGFW a także z wybranej adresacji IP.   7. Możliwość automatycznego usuwania raportów po określonym czasie.   **Korelacja logów**  W zakresie korelacji zdarzeń system musi zapewniać:   * 1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.   2. Możliwość tworzenia własnych reguł korelowania logów.   3. Konfigurację powiadomień poprzez: e-mail, SNMP oraz API http w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. W treści powiadomienia musi być możliwość przekazania dodatkowych informacji o zdarzeniu wywołującym dane powiadomienie, np. nazwa wykrytego zagrożenia.   4. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:      1. Malware/AV      2. Aplikacje sieciowe      3. Email      4. IPS      5. Web Filter      6. Traffic (logi z ruchu sieciowego)      7. Systemowe (m.in. utracone połączenie VPN, utracone połączenie sieciowe, zdarzenia związane z klastrem niezawodnościowym, zmiana w sieci SD-WAN)   5. Możliwość automatycznego, zwrotnego powiadomienia systemu bezpieczeństwa NGFW o wystąpieniu wybranych zdarzeń korelacji.   **Zarządzanie**   * 1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.   2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, Tacacs+, PKI.   3. System musi umożliwiać definiowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do wybranych modułów systemu logowania i raportowania.   4. System musi mieć możliwość podziału na wirtualne systemy logowania i raportowania (konteksty/domeny). Musi istnieć możliwość przypisywania administratorom praw dostępu do wybranych kontekstów. Dla każdego kontekstu musi być możliwość niezależnego przydzielania zasobów dyskowych oraz określania maksymalnego czasu przechowywania logów. |  |

1. **Usługa instalacji, uruchomienie, konfiguracja i szkolenie.**

**Zakres wdrożenia routera brzegowego:**

1. Fizyczna instalacja urządzeń w dwóch lokalizacjach Zamawiającego
2. Konfiguracja klastra active-active w oparciu o połączenia światłowodowe
3. Podstawowa konfiguracja urządzeń – adresacja IP, dostęp administracyjny
4. Aktualizacja systemu do najnowszej stabilnej wersji
5. Podłączenie do sieci Zamawiającego
6. Przeniesienie konfiguracji z obecnych, osobnych firewalli (do obsługi VPN i wewnętrznych sieci Zamawiającego) na nowy klaster z uwzględnieniem wymagań Zamawiającego oraz dobry praktyk m.in.
   * + routingu statycznego i dynamicznego
     + profili i polityk bezpieczeństwa, ochrony przed atakami typu DoS
     + serwerów autoryzacyjnych z wykorzystaniem protokołów Radius i LDAP
     + usługi VPN
     + integracji z serwerem logów
     + integracji z serwerem SIEM
     + integracji z systemem ochrony aplikacji webowych
     + integracji z systemem do monitorowania sieci
7. Wykonanie kopii bezpieczeństwa w siedzibie Zamawiającego
8. Wykonanie testów przed przełączeniem
9. Przełączenie produkcyjne nowych urządzeń
10. Wykonanie schematu i opisu podłączenia systemu w infrastrukturze Zamawiającego

**Zakres wdrożenia systemu do zbierania logów i raportowania:**

1. Instalacja systemu w najnowszej stabilnej wersji w wirtualnym środowisku Zamawiającego
2. Podstawowa konfiguracja – adresacja IP, dostęp administracyjny
3. Autoryzacja wszystkich urządzeń przesyłających logi
4. Migracja logów z obecnego systemu
5. Konfiguracja raportów i powiadomień
6. Wykonanie kopii bezpieczeństwa w siedzibie Zamawiającego
7. Wykonanie schematu i opisu podłączenia systemu w infrastrukturze Zamawiającego

**Osoby, które będą wykonywać zamówienie:**

• w związku z posiadanymi przez zamawiającego jednostkami FortiGate, który jest głównym elementem sieci LAN i WLAN, oraz koniecznością migracji polityk bezpieczeństwa z tych jednostek Zamawiający wymaga, aby Wykonawca dysponował odpowiednim potencjałem technicznym, tj. min. jednym akredytowanym inżynierem na poziomie min. NSE4