Załącznik nr 1 – SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – SPECYFIKACJA TECHNICZNA

**System zabezpieczeń ruchu sieciowego**

1. **Wymagania ogólne dla systemu zabezpieczeń ruchu sieciowego**
   * 1. Przedmiotem zamówienia jest dostawa systemu zabezpieczeń ruchu sieciowego w postaci rozwiązań Next Generation Firewall (NGFW).
     2. Całościowy system bezpieczeństwa musi być zrealizowany poprzez dwa urządzenia (firewalle). Zamawiający dopuszcza realizację systemu bezpieczeństwa tylko jako dwa urządzenia (firewalle) połączone w klaster wysokiej dostępności.
     3. Przedmiot zamówienia musi być fabrycznie nowy, nigdy wcześniej nie używany, pochodzący z legalnego kanału dystrybucyjnego, dopuszczony do obrotu, spełniający normy CE.
     4. Zamawiający wymaga, aby zaoferowane urządzenia (firewalle) były dostępne i serwisowane przez Producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne).
2. **Wymagania dotyczące pojedynczego urządzenia typu firewall**
   1. **Wymagania dotyczące funkcjonalności zabezpieczeń:**
      1. Każdy z interfejsów musi mieć możliwość pracy w co najmniej następujących trybach: L2 (bridge), L3 (router), TAP (pasywny sniffer ruchu) oraz tryb transparentny. Działając w trybie transparentnym firewall nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne lub rozgłoszeniowe. Tryb transparentny musi umożliwiać analizę i filtrowanie przepuszczanego ruchu. Tryb pracy zabezpieczeń musi być ustalany w konfiguracji per interfejs. Musi istnieć możliwość jednoczesnej konfiguracji i pracy poszczególnych interfejsów sieciowych w różnych trybach.
      2. Firewall musi umożliwiać realizację zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.
      3. Reguły zabezpieczeń firewalla muszą uwzględniać co najmniej: strefy bezpieczeństwa, adresy IP źródłowe i docelowe, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (co najmniej: priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).
      4. Firewall musi umożliwiać identyfikację co najmniej 3000 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS, np.: SAP, Zoom, Google Meet, Google Classroom, Skype, Microsoft Update, Microsoft Samba v1/v2/v3, Microsoft Remote Desktop, Tor, BitTorrent, Facebook, Youtube. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall.
      5. Firewall musi umożliwiać ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
      6. Firewall musi umożliwiać zarządzanie, kontrolę i wgląd w ruch nierozpoznany przez polityki identyfikacji.
      7. Firewall musi umożliwiać identyfikowanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z Peer to Peer-P2P i IM-Instant Messaging). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.
      8. Firewall musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach. Polityki definiujące powinny umożliwiać wykorzystanie: adresów źródłowych, adresów docelowych, użytkowników, numerów portów usług, kategorie URL. System musi obsługiwać co najmniej następujące mechanizmy uwierzytelnienia RADIUS lub TACACS+, LDAP, SAML 2.0.
      9. Możliwość rozbudowy (wyłącznie w oparciu o zakup licencji) o funkcjonalność analizy plików wykonywalnych (exe, dll) przechodzących przez firewall współpracując z zewnętrznym systemem utrzymywanym przez producenta w Internecie, który instaluje i uruchamia przesłane pliki w wirtualnym środowisku oraz sprawdza czy dany plik nie zachowuje się w złośliwy sposób (np. kasuje lub zaraża inne pliki, zmienia ustawienia komputera, nawiązuje komunikację zwrotną, otwiera porty, zmienia ustawienia usług systemowych, itp). System zewnętrzny, na podstawie przeprowadzonej analizy, musi aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.
      10. Możliwość rozbudowy (wyłącznie w oparciu o zakup licencji) o funkcjonalności: filtrowania stron WWW (WWW/URL Filtering) w zależności od predefiniowanych kategorii, IDS/IPS, AntiSpyware, AntiVirus, DLP per reguła polityki bezpieczeństwa. Nie jest dopuszczalne, aby ww. moduły uruchamiane były per firewall lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). Bazy sygnatur ww. modułów muszą być przechowywane na urządzeniu, regularnie aktualizowane w sposób automatyczny, być w pełni kompatybilne z firewallem i posiadać nie mniej niż 200 milionów rekordów URL.
      11. Możliwość rozbudowy (wyłącznie w oparciu o zakup licencji) o funkcjonalność wykrywania i blokowania ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
      12. Firewall musi umożliwiać wykrywanie sieci Botnet na podstawie analizy behawioralnej oraz ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
      13. Firewall musi umożliwiać inspekcję komunikacji szyfrowanej HTTPS (SSL) dla ruchu wychodzącego i przychodzącego. Firewall musi umożliwiać deszyfrację niezaufanego ruchu HTTPS (szyfrowanego 3DES, AES (128-bit, 192-bit, 256-bit)) i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (Intrusion Prevention - IPS), wirusy i inny złośliwy kod (AntiVirus i AntiSpyware).
      14. Firewall musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
      15. Firewall musi umożliwiać uruchomienie modułu inspekcji antywirusowej, kontrolującego przynajmniej pocztę elektronicznej (SMTP, POP3, IMAP), FTP oraz HTTP i HTTPS bez konieczności dokupowania jakichkolwiek dodatkowych komponentów. Baza sygnatur AV musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Moduł AV musi być uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduł inspekcji antywirusowej uruchamiany był per cały firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).
      16. Firewall musi umożliwiać transparentnie ustalenie tożsamość użytkowników sieci (integracja z Active Directory, Citrix, LDAP i serwerami Terminal Services, syslog). Reguły zabezpieczeń firewalla precyzyjnie definiują prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
   2. **Wymagania dotyczące pozostałych funkcjonalności:**
      1. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów programowych firewall oraz łączy sieciowych.
      2. Wsparcie dla standardu 802.1q. Obsługa pełnego zakresu tagów od 1 do 4094 per interfejs. Obsługa pełnego zakresu tagów od 1 do 4094 per firewall (lub instancja).
      3. Wsparcie dla protokołów routingu OSPFv2/v3, BGP, RIP oraz dla Policy Based Routing (PBR).
      4. Wsparcie dla protokołów multicastowych: PIM-SM, PIM-SSM, IGMP v1, v2, v3
      5. Firewall musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu.
      6. Możliwość rozbudowy (wyłącznie w oparciu o zakup licencji) do obsługi nie mniej niż 6 wirtualnych firewalli/systemów/domen/kontekstów. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych: tablic routingu, polityk bezpieczeństwa obejmujących, system IPS, system ochrony antymalware/antyspyware, system ochrony antywirus, koncentratorów VPN dla zdalnego dostępu.
      7. Wsparcie dla mechanizmów NAT i PAT (Source i Destination NAT i PAT) dla protokołu IPv4, NAT64, możliwość rezerwowania dynamicznych i statycznych zakresów IP.
      8. Obsługa standardów wymiany klucza: Manual key, IKE v1 i v2.Obsługa standardów szyfrowania 3DES, AES (128-bit, 192-bit, 256-bit). Obsługa standardów uwierzytelniania: MD5, SHA-1, SHA-256, SHA-384, SHA-512.
      9. Firewall musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN.
      10. Zestawianie tuneli SSL VPN w konfiguracji remote-access-VPN musi posiadać możliwość weryfikacji kondycji bezpieczeństwa stacji końcowej (co najmniej dla Windows) co najmniej w zakresie obecności oprogramowania antywirusowego, przynależności do domeny Active Directory i stanu lokalnego firewalla.
      11. Firewall musi umożliwiać zestawianie tuneli VPN Client-to-Site z mechanizm „Split tunneling”.
      12. Producent firewalla musi zapewniać dostęp do aplikacji klienckiej VPN kompatybilnej z urządzeniami z systemem Windows, MacOS, Linux oraz urządzeniami mobilnymi iOS, Android.
      13. Firewall musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego.
      14. Zarządzanie musi odbywać się z linii poleceń (CLI), konsoli Web GUI dostępnej przez przeglądarkę WWW oraz przez SSH. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania firewallem.
      15. Firewall musi umożliwiać zdefiniowanie wielu administratorów o różnych uprawnieniach. Firewall musi umożliwiać uwierzytelnianie administratorów za pomocą:
          1. bazy lokalnej,
          2. serwera LDAP,
          3. RADIUS lub TACACS+
          4. SAML 2.0.
      16. Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
      17. Firewall musi umożliwiać edycję konfiguracji na urządzeniu bez jej jednoczesnego aplikowania (aplikowanie konfiguracji na żądanie).
      18. Firewall musi umożliwiać porównania bieżącej konfiguracji (wskazania różnic) z co najmniej 20 wcześniejszymi konfiguracjami.
      19. Firewall musi zapewniać interfejs API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).Firewall musi wspierać co najmniej jeden z poniższych standardów API:
          1. JSON,
          2. REST,
          3. XML.
      20. Firewall musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG.
      21. Firewall nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
      22. Licencje muszą zostać aktywowane przez zamawiającego, a nie automatycznie w momencie zakupu urządzenia. Czas trwania licencji musi być liczony od momentu aktywacji.
      23. Firewall musi być objęty minimum 5-letnim wsparciem obejmującym:
          1. dostęp do aktualnych wersji oprogramowania,
          2. realizacja zgłoszeń serwisowych w trybie 24x7,
          3. realizację zgłoszeń gwarancyjnych w trybie 24x7,
          4. wsparcie techniczne realizowane telefonicznie, mailowo oraz za pośrednictwem portalu www,
          5. aktualizację bazy ataków IPS i definicji wirusów (czas liczony jak w punkcie II.B.22),
          6. dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.
   3. **Wymagania wydajnościowe**
      1. Firewall musi być dostarczony jako dedykowane urządzenie typu appliance z dedykowanym dla niego oprogramowaniem systemowym. Obudowa wraz z kompletem mocowań umożliwiających montaż w szafie rack 19” i zajmować maksymalnie 2 RU. Całość sprzętu i oprogramowania musi pochodzić od jednego producenta.
      2. Zasilanie napięciem zmiennym 230V / 50Hz. Firewall musi być wyposażony w co najmniej 2 zasilacze typu AC pracujące redundantnie.
      3. Firewall musi posiadać co najmniej:
         1. 4 interfejsy 40GE QSFP+,
         2. 12 interfejsów 10/100/1000M Ethernet (RJ45),
         3. 8 interfejsów 1/10GE SFP/SFP+
      4. Do firewalla muszą być dołączone 4 współpracujące z nim interfejsy optyczne pracujące w standardzie 10GBASE-SX SFP+ oraz 4 współpracujące z nim interfejsy optyczne pracujące w standardzie 40GBASE-SR QSFP+
      5. Firewall musi posiadać co najmniej 1 dysk SSD o pojemności nie mniejszej niż 240 GB.
      6. Temperatura pracy firewalla w zakresie od 0 do 50 oC.
      7. Firewall musi zapewniać przepustowość co najmniej 8 Gbps dla kontroli ruchu z włączoną funkcją rozpoznawania aplikacji, nie mniej niż 4,5 Gbps dla kontroli zawartości (w tym kontrola AntiVirus, AntiSpyware, Intrusion Prevention System/ Intrusion Detection System i Web/URL Filtering).
      8. Firewall musi obsługiwać co najmniej 90 000 nowych sesji na sekundę.
      9. Firewall musi obsługiwać co najmniej 2,3 mln jednoczesnych sesji.
      10. Firewall musi spełniać co najmniej następujące parametry wydajnościowe funkcji VPN (IPSec i SSL):
          1. Minimum 4 Gbps dla IPSEC VPN,
          2. Minimum 6 000 tuneli IPSEC VPN (site-to-site),
          3. Minimum 2 000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN.
      11. Możliwość pracy w klastrze w trybie Active/Active i Active/Passive z synchronizacją konfiguracji i tablicy stanu sesji przy włączonych funkcjonalnościach.
      12. Firewall musi umożliwiać zdefiniowanie nie mniej niż 10 000 reguł polityki bezpieczeństwa oraz obsługę minimum 200 stref bezpieczeństwa.
      13. Firewall musi być objęty minimum 5 letnią gwarancją (nie krótszą niż gwarancja producenta).
3. **Platforma do centralnego zarządzania**
   1. Platforma ma pozwalać na zarządzanie z jednego miejsca każdym z urządzeń (firewalli) wchodzących w skład systemu zabezpieczeń ruchu sieciowego, co najmniej w zakresie:
      1. Tworzenia szablonów konfiguracji
      2. Zbieranie i analizowanie logów
      3. Korelowania zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o:
         1. ruchu sieciowym,
         2. aplikacjach,
         3. zagrożeniach
         4. filtrowaniu stron www.
      4. Tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
      5. Tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.
   2. Zgodność ze środowiskiem wirtualizacji VMware ESXi 6.7 i nowszym
   3. Platforma musi zapewniać interfejs AP,I za pomocą którego możliwa jest konfiguracja i monitorowanie stanu platformy bez użycia konsoli zarządzania lub linii poleceń (CLI). Platforma musi wspierać co najmniej jeden z poniższych standardów API:
      1. JSON,
      2. REST,
      3. XML.
   4. Platforma musi umożliwiać zdefiniowanie wielu administratorów o różnych uprawnieniach. Platforma musi umożliwiać uwierzytelnianie administratorów za pomocą:
      * 1. bazy lokalnej,
        2. serwera LDAP,
        3. RADIUS lub TACACS+
        4. SAML 2.0.