***Załącznik Nr 1 do zaproszenia AZP.273.76.2019***

**Opis przedmiotu zamówienia**

**I. Zapora sieciowa (Firewall)**

1. Wymagania ogólne
	1. Przedmiotem zamówienia jest zakup systemu bezpieczeństwa, który zastąpi wycofywane z eksploatacji dwa urządzenia FortiGate-800C.
	2. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.
	3. 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.
	4. System realizujący funkcję Firewall musi dawać możliwość pracy w każdym z trzech trybów:
* Routera z funkcją NAT,
* Transparentnym,
* Monitorowania na porcie SPAN.
	1. 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. System ma umożliwiać dedykowanie co najmniej 9 administratorów do poszczególnych instancji systemu.
	2. System musi wspierać IPv4 oraz IPv6 w zakresie:
* Firewall,
* Ochrony w warstwie aplikacji,
* Protokołów routingu dynamicznego.
1. 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 musi być dostępna funkcja synchronizacji sesji firewall.
	2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
	3. System zapewnia monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
	4. System zapewnia monitoring stanu realizowanych połączeń VPN.
	5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP.
	6. System musi umożliwiać tworzenie interfejsów redundantnych.
2. Interfejsy, zasilanie:
	1. System realizujący funkcję Firewall musi dysponować minimum:
* 8 portami Gigabit Ethernet RJ-45,
* 8 gniazdami SFP 1 Gbps.
* 2 gniazdami SFP+ 10 Gbps.
	1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
	2. W ramach systemu Firewall musi być możliwe zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
	3. Każdy z elementów podsystemu firewall musi być wyposażony w dwa redundantne zasilacze AC.
1. Parametry wydajnościowe:
	1. W zakresie Firewall’a obsługa nie mniej niż 7 mln jednoczesnych połączeń oraz 400.000 nowych połączeń na sekundę.
	2. Przepustowość Stateful Firewall: nie mniej niż 30 Gbps.
	3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 14 Gbps.
	4. Wydajność szyfrowania VPN IPSec nie mniej niż 18 Gbps.
	5. Wydajność szyfrowania SSL-VPN nie mniej niż 6 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 9 Gbps.
	7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 6 Gbps.
	8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 6 Gbps.
2. 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.
	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 muszą zostać dostarczone 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. Analiza ruchu szyfrowanego protokołem SSL.
	12. Analiza ruchu szyfrowanego protokołem SSH.
1. 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.
1. 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.
	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.
1. Routing i obsługa łączy WAN
	1. W zakresie routingu rozwiązanie musi 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.
1. 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.
2. 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).
3. Ochrona przed atakami
	1. Ochrona IPS musi 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 musi 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.
4. Kontrola aplikacji
	1. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
	2. Baza Kontroli Aplikacji musi zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
	3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
	4. Baza musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
	5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
5. 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 muszą 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.
6. 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.
	1. Musi istnieć możliwość zastosowania uwierzytelniania dwu-składnikowego w procesie weryfikacji tożsamości użytkowników.
	2. Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
1. Zarządzanie
	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS i SSH oraz muszą 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. System musi umożliwiać włączenie mechanizmów uwierzytelniania dwu-składnikowego 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. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
2. Logowanie
	1. System musi mieć możliwość logowania do systemu logowania i raportowania będącego przedmiotem postępowania.
	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. System ma umożliwiać logowanie do serwera SYSLOG.
	5. Dodatkowo każdy z elementów firewall, musi posiadać, redundantne, lokalne zasoby dyskowe służące do przechowywania logów na urządzeniu.
3. Certyfikacje
	1. Poszczególne elementy oferowanego systemu bezpieczeństwa muszą posiadać następujące certyfikacje:
* ICSA lub EAL4 dla funkcji Firewall.
* ICSA lub NSS Labs dla funkcji IPS.
* ICSA dla funkcji IPSec VPN.
1. Serwisy i licencje

W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów obejmujące:

* Kontrolę Aplikacji,
* IPS,
* Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android),
* Analizę typu Sandbox,
* Antyspam,
* Web Filtering,
* bazy reputacyjne adresów IP/domen na okres minimum 12 miesięcy.
1. Gwarancja oraz wsparcie
	1. System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Zagwarantowana musi być wysyłka nowego urządzenia na następny dzień roboczy od potwierdzenia awarii. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
	2. Na potrzeby wdrożenia urządzeń oraz na czas trwania dostarczonych licencji Wykonawca zapewni wsparcie techniczne niezależne od producentów lub dystrybutorów oferowanych rozwiązań. Wsparcie ma obowiązywać w dni robocze w godzinach pracy Zamawiającego wymiarze minimum 4 godzin dziennie.
	3. Na etapie podmiany starych urządzeń FortiGate-800C Oferent zapewni dostępność Inżyniera, pod telefonem lub na miejscu, nawet poza standardowymi godzinami pracy Zamawiającego w łącznym wymiarze minimum 72 godziny.
2. Uwagi dodatkowe

Oferent winien przedłożyć przed podpisaniem umowy oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

# **II. System zbierania, przechowywania i analizy logów**

1. Wymagania Ogólne
	1. W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.
	2. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
2. Interfejsy, Dysk, Zasilanie:
	1. System musi dysponować co najmniej 2 portami Gigabit Ethernet RJ-45.
	2. Rozwiązanie musi dysponować powierzchnią dyskową min. 4 TB.
3. Parametry wydajnościowe:
	1. System musi być w stanie przyjmować minimum 90 GB logów na dzień.
	2. System musi być w stanie analizować minimum 3000 logów na sekundę.
	3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 10 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

1. Logowanie
	1. Podgląd logowanych zdarzeń w czasie rzeczywistym z możliwością zastosowania filtrów dla prezentowanych informacji.
	2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
	3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe - dla urządzeń, które logują informacje - obrazujące stan pracy urządzeń 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.

* 1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
	2. 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.
	3. 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.
1. 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.
1. 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 korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
* Malware,
* Aplikacje sieciowe,
* Email,
* IPS,
* Traffic,
* Systemowe: utracone połączenie VPN, utracone połączenie sieciowe, obciążenie zasobów.
1. 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.
	2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o:
* lokalną bazę,
* Radius,
* LDAP,
* PKI.
	1. System musi umożliwiać definiowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
1. Gwarancja oraz wsparcie
	1. System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Zagwarantowana musi być wysyłka nowego urządzenia na następny dzień roboczy od potwierdzenia awarii. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
	2. Na potrzeby wdrożenia urządzeń oraz na czas trwania dostarczonych licencji Wykonawca zapewni wsparcie techniczne niezależne od producentów lub dystrybutorów oferowanych rozwiązań. Wsparcie ma obowiązywać w dni robocze w godzinach pracy Zamawiającego wymiarze minimum 4 godzin dziennie.
2. Uwagi dodatkowe

Oferent winien przedłożyć przed podpisaniem umowy oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.