Załącznik do zapytania o wycenę

Szczegółowy Opis Przedmiotu Zamówienia

1. **Przedmiotem zamówienia jest:**
   1) odnowienie subskrypcji i usługi wsparcia technicznego producenta dla posiadanych przez Zamawiającego produktów Fortinet, opisane szczegółowo w punkcie 2.
   2) zakup i dostawa systemu zabezpieczeń typu firewall (dalej jako „System"), opisanego szczegółowo w punkcie 3.
   3) wykonanie usługi wdrożenia Systemu, opisanej szczegółowo w punkcie 4.
   4) świadczenie usługi wsparcia w konfiguracji i administrowaniu Systemem, opisanej szczegółowo w punkcie 5.

2. **Odnowienie subskrypcji i usługi wsparcia technicznego producenta dla posiadanych przez Zamawiającego urządzeń Fortinet na okres do dnia 23.12.2029 r.:**

Produkt i Nr seryjny	Od dnia	Do dnia	Wymagana subskrypcja i wsparcie producenta
FortiAnalyzer VM FAZ-VMTM19010896	24.12.2026 r.	23.12.2029 r.	FortiAnalyzer-VM FortiCare Premium Support (for 1-6 GB/Day of Logs)
FortiGate 200F (pracujący w trybie HA) FG200FT922941334	09.05.2026 r.	23.12.2029 r.	FortiGate-200F Advanced Threat Protection (IPS, Advanced Malware Protection Service, Application Control, and FortiCare Premium)
FortiGate 200F (pracujący w trybie HA) FG200FT922941880	09.05.2026 r.	23.12.2029 r.	FortiGate-200F Advanced Threat Protection (IPS, Advanced Malware Protection Service, Application Control, and FortiCare Premium)

3. **Zakup i dostawa systemu zabezpieczeń typu firewall – 2 szt.:**

Lp.	Cecha	Wymagania minimalne
1.	Wymagania ogólne	1) Urządzenie musi być w obudowie RACK o wysokości maksymalnie 1U 2) Obudowa urządzenia musi być wykonana z metalu. Ze względu na różne warunki, w których pracować będzie urządzenie, nie dopuszcza się urządzenia w obudowie plastikowej 3) Urządzenie musi posiadać na obudowie kontrolki lub wyświetlacz LCD informujący o statusie urządzenia, parametrach Systemu oraz alarmach
2.	Wymagania HA	1) Możliwość pracy urządzenia w trybie HA 2) Obsługiwane tryby pracy dla klastra HA: a) active/passive b) active/active
3.	Wymagane moduły/funkcjonalności	1) Zapora sieciowa wraz z inspekcją SSL 2) NAT

		3) VPN IPSec 4) Routing oraz switching 5) Ochrona antywirusowa 6) SSL VPN
4.	Parametry wydajnościowe zapory	1) Wydajność nie mniejsza niż 39 000 000 Pakietów na sekundę 2) Obsługa sesji TCP – 40 000 000 3) Obsługa nowych sesji TCP na sekundę – 400 000 4) Obsługa co najmniej 3000 sieci VLAN 5) Element Systemu pełniący funkcję Firewall musi dysponować przynajmniej: a) 8 portami 1GbE BaseT b) 8 portami 5/2,5 GbE BaseT c) 8 portami 10GbE SFP+ d) 4 portami 1GbE SFP 6) Obsługa nie mniej niż: 2 000 tuneli IPSec site-to-site 7) Obsługa nie mniej niż: 16 000 tuneli client-to-site 8) Obsługa nie mniej niż: 10 000 reguł firewall 9) Przepustowość Stateful Firewall: nie mniej niż 26 Gbps 10) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 6 Gbps 11) Wydajność Systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 7 Gbps 12) Wydajność szyfrowania IPSec VPN: nie mniej niż 36 Gbps 13) Wydajność szyfrowania SSL_VPN: nie mniej niż 3 Gbps 14) Moduł TPM
5.	Funkcje modułu Firewall, router i switching	1) Mechanizm inspekcji SSL (ssl inspection) 2) Urządzenie musi funkcjonować w oparciu o interfejsy, adresy (IP i FQDN), grupy adresów (IP i FQDN), oraz użytkowników 3) Obsługa statycznych i dynamicznych adresów IP (DHCP i PPoE) na zewnętrznym interfejsie 4) Możliwość pracy jako router i bridge (transpartent mode) 5) Możliwość obsługi translacji adresów: SNAT, DNAT 6) Możliwość obsługi translacji portów: PAT 7) Możliwość obsługi VLAN 802.1Q 8) Możliwość ochrony przed atakami stosującymi techniki unikania wykrycia, np. fragmentacja pakietów 9) Możliwość uwierzytelniania użytkowników oraz identyfikacji odpowiadającego im ruchu sieciowego 10) Możliwość transparentnego uwierzytelniania użytkowników przy integracji z Active Directory 11) Brak możliwości ograniczania ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej 12) Możliwość sterowania przepustowością w oparciu o następujące parametry: użytkownik, grupa użytkowników, protokół, interfejs sieciowy, adres (IP oraz FQDN) i grupa adresów (IP oraz FQDN) 13) Możliwość pełnienia roli bramki VPN terminującej połączenia VPN site-to-site i client-to-site
6.	Wymagane funkcje VPN Systemu	1) Możliwość obsługi tuneli: Site-to-Site 2) Wsparcie dla algorytmów szyfrowania IKE: AES-GCM, AES256, AES128, 3DES,

		DES 3) Wsparcie dla algorytmów autentykacji IKE: MD5, SHA-1, SHA-256, SHA-512 4) Rodzaje autentykacji: Preshared key oraz PKI X.509 5) IPsec: wsparcie dla przynajmniej jednego z poniższych: a) Authentication Header (AH) b) Encapsulating Security Payload (ESP) 6) Wsparcie dla IKEv1 i IKEv2 7) Obsługa Perfect Forward Secrecy oraz Anti Reply (Reply Detection). 8) Obsługa Dead Peer Detection (DPD) 9) Obsługa połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec oraz SSL VPN 10) Możliwość jednoczesnego podłączenia przynajmniej 500 klientów poprzez SSL VPN. Zamawiający nie akceptuje limitowania klientów dla tej formy połączenia zdalnego (lub dostarczenia minimum 1200 licencji na takie połączenia)
7.	Polityki, Firewall	1) Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń 2) Firewall musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: a) Translację jeden do jeden oraz jeden do wielu b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP 3) W ramach Systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN
8.	Routing i obsługa łączy WAN	1) W zakresie routingu rozwiązanie musi zapewniać obsługę: a) Routingu statycznego b) Policy Based Routingu c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM 2) Firewall musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN 3) Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu
9.	Zarządzanie pasmem	1) Możliwość zarządzania pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu 2) Możliwość określania pasma dla poszczególnych aplikacji 3) Możliwość zarządzania pasmem dla wybranych kategorii URL
10.	Ochrona antywirusowa	1) Automatyczna aktualizacja baz sygnatur, nie rzadziej niż co 24 godzin 2) Skanowanie plików skompresowanych: zip, tar, gzip 3) Wsparcie dla głównych protokołów: http, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS 4) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) 5) 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
11.	Ochrona przed atakami	1) Automatyczna aktualizacja bazy sygnatur IPS 2) Automatyczne blokowanie znanych źródeł ataków 3) Mechanizmy ochrony przed atakami typu DoS i DDoS 4) Ochrona przed atakami na aplikacje pracujące na niestandardowych portach 5) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur 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
12.	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 2500 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
13.	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 3) Filtr WWW musi dostarczać kategorie stron zabronionych prawem: Hazard 4) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania 5) Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL
14.	Uwierzytelnianie użytkowników w ramach sesji	1) System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: a) haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie Systemu b) haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP c) haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych 2) Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego 3) System musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API

15.	Zarządzanie	1) Możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i 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) Musi istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego 4) Współpraca z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow 1) Możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację 2) Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podgląd pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall 3) Elementy Systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) 4) Urządzenie musi posiadać dedykowany interfejs Ethernet obsługujący połączenia z prędkością minimum 100 Mbit/s - dla zdalnego zarządzania 5) Urządzenie musi posiadać port konsolowy 6) Urządzenie musi posiadać port USB umożliwiający instalację oprogramowania z nośnika USB
16.	Wyposażenie dodatkowe	1) Dołączone 4 moduły SFP+ SR 10Gb/s kompatybilne z urządzeniem. 2) Dołączone 2 moduły SFP SR 1Gb/s kompatybilne z urządzeniem. 3) Komplet szyn umożliwiających montaż w szafie rack 4) Urządzenie musi być dostarczone z kompletem kabli umożliwiających podłączenie urządzenia w klaster HA
17.	Zasilanie	Dołączone dwa redundantne zasilacze AC 230 V
18.	Gwarancja, serwis i wsparcie techniczne producenta	1) Długość gwarancji: min. do dnia 23.12.2029 r. 2) Gwarancja i serwis realizowany w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany i zabezpieczony kanał komunikacji elektronicznej 3) Producent musi umożliwiać skuteczne zgłaszanie awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.) oraz system zgłoszeniowy producenta 4) Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej infrastruktury oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela 5) Dyski twarde naprawianego urządzenia pozostają w siedzibie Zamawiającego 6) Zakres wsparcia technicznego producenta: a) dostęp do pomocy technicznej b) dostęp do poprawek i nowych wersji oprogramowania i/lub Systemu c) dostęp do dokumentacji technicznej d) dostęp do konta wsparcia urządzenia, zawierającego dostęp do bazy

		wiedzy oraz systemu zgłoszeń producenta
19.	Dokumentacja	Dokumentacja urządzenia w języku polskim lub angielskim, dostępna na stronie producenta
20.	Licencje	Urządzenie musi być dostarczone wraz z licencjami/subskrypcjami na okres minimum do dnia 23.12.2029 r. upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Muszą one obejmować: 1) Kontrola Aplikacji, 2) IPS, 3) Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android, w wersji min. 12), 4) Analiza typu Sandbox, 5) Antyspam, 6) Web/URL Filtering, 7) bazy reputacyjne adresów IP/domen 8) SSLVPN oraz IPSecVPN Jeżeli którakolwiek opisana powyżej funkcjonalność wymaga dodatkowych licencji i/lub subskrypcji to należy je dostarczyć wraz z urządzeniem.
21.	Integracja	Urządzenie musi być kompatybilne z posiadanym przez Zamawiającego systemem FortiAnalyzer. W przypadku gdy zaoferowane rozwiązanie nie będzie kompatybilne z posiadanym przez Zamawiającego systemem FortiAnalyzer wymagane jest dostarczenie systemu do logowania, raportowania i korelacji logów, zgodnie z wymaganiami opisanymi w punkcie 6.[1]
22.	VPN	Urządzenie musi być kompatybilne z posiadaną przez Zamawiającego aplikacją FortiClient. W przypadku gdy zaoferowane rozwiązanie nie będzie kompatybilne z posiadaną przez Zamawiającego aplikacją FortiClient wymagane jest dostarczenie aplikacji, umożliwiającej połączenie VPN do zaoferowanego Systemu wraz z wdrożeniem, instalacją i konfiguracją na wszystkich stacjach roboczych Zamawiającego.[2]

4. Usługa wdrożenia Systemu

Wykonawca zapewni wykonanie usługi wdrożeniowej Systemu w terminie do 14 dni kalendarzowych od dnia podpisania protokołu odbioru Systemu bez zastrzeżeń.

Usługa wdrożenia Systemu obejmuje w szczególności:

1) Instalację i konfigurację firewalli zgodnie z wytycznymi Zamawiającego, w tym:
   a) migracja konfiguracji z posiadanych urządzeń Fortinet FortiGate 500E,
   b) rekonfiguracja interfejsów sieciowych,

[1] W przypadku dostarczenia rozwiązania, które nie jest kompatybilne z posiadanym przez Zamawiającego systemem FortiAnalyzer
[2] W przypadku dostarczenia rozwiązania, które nie jest kompatybilne z posiadaną przez Zamawiającego aplikacją FortiClient

c) przepięcie ruchu z urządzeń Fortinet FortiGate 500E, w terminie ustalonym przez Zamawiającego, z zastrzeżeniem, że prace będą wykonywane wyłącznie w soboty i niedziele;
d) przeprowadzenie testów działania oraz testów wysokiej dostępności rozwiązania,
e) opracowanie i przekazanie dokumentacji powykonawczej zawierającej w szczególności:
   - diagramy połączeń,
   - konfiguracje urządzeń,
   - konfiguracje interfejsów,
   - integracje z systemami Zamawiającego,
   - opis wdrożonych funkcjonalności,
   - wyniki testów.

5. Usługa wsparcia w konfiguracji i administrowaniu Systemem

Wykonawca zapewni świadczenie usługi wsparcia w konfiguracji i administrowaniu Systemem w maksymalnym wymiarze 20 roboczogodzin z możliwością wykorzystania przez okres od dnia odbioru Systemu do dnia 23.12.2029 r. lub do wykorzystania ww. puli roboczogodzin świadczonych usług. Do realizacji usługi wsparcia Wykonawca skieruje minimum 2 osoby posiadające aktualny certyfikat autoryzowany przez producenta Systemu, potwierdzający zaawansowaną wiedzę z Systemu.

Usługa wsparcia Wykonawcy obejmuje w szczególności:

1) w przypadku awarii urządzenia – zgłoszenie awarii producentowi, koordynacja zgłoszenia poprzez monitorowanie i posiadanie aktualnych informacji o statusie zgłoszenia oraz miejscu przebywania urządzenia na wymianę, jeżeli takie jest przewidziane. Konfiguracja urządzenia wymienianego w celu uzyskania funkcjonalności urządzenia uszkodzonego;
2) usuwanie usterek, prace rekonfiguracyjne, diagnostycznie, projektowe, usługi konsultacyjne w zakresie funkcjonalności, eksploatacji i administrowania Systemem, aktualizacja dokumentacji i inne zlecane przez Zamawiającego, mające na celu zapewnienie prawidłowego funkcjonowania sieci Zamawiającego;
3) wsparcie będzie świadczone zgodnie z zapotrzebowaniem zgłaszanym przez Zamawiającego w formie mailowej lub telefonicznej, albo w miejscu wskazanym przez Zamawiającego wedle wyboru Zamawiającego w terminach wskazanych przez Zamawiającego.

6. System centralnego logowania, korelacji i raportowania[3]

[3] W przypadku dostarczenia rozwiązania, które nie jest kompatybilne z posiadanym przez Zamawiającego systemem FortiAnalyzer

W ramach systemu logowania i raportowania dostawca musi dostarczyć spójny system, w pełni kompatybilny z dostarczonym Systemem, monitorujący, gromadzący logi, korelujący zdarzenia i generujący raporty na podstawie danych.

System centralnego logowania i raportowania musi być dostarczony w postaci komercyjnej platformy działającej w środowisku wirtualnym z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESXi /8.x, Hyperv 2019, 2022, 2025.

1) W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane przynajmniej poniższe funkcjonalności:

Lp.	Nazwa elementu / Parametr	Opis / minimalne wymagania
1.	Interfejsy, Dysk, Zasilanie	System musi obsługiwać co najmniej 2 interfejsy wirtualne oraz zapewniać powierzchnię dyskową min. 3 TB
2.	Parametry wydajnościowe:	Na podstawie analizy przeprowadzonych testów w zakresie ilości logów w ciągu sekundy, zastosowany system centralnego logowania musi umożliwiać zapis oraz analizę 3,5 milionów logów na dobę w ilości 3 GB na dobę
3.	Logowanie	Podgląd logowanych zdarzeń w czasie rzeczywistym. Zastosowane systemy logowania muszą umożliwiać cykliczny eksport zgromadzonych logów do zewnętrznych systemów przechowywania danych w celu ich długo czasowego składowania.
4.	Raportowanie	Platforma musi dysponować predefiniowanym zestawem przykładów raportów, dla których administrator systemu będzie mógł modyfikować parametry prezentowania wyników. Możliwość generowania raportów w zakresie wszystkich funkcjonalności bezpieczeństwa realizowanych przez system - na żądanie oraz w trybie cyklicznym, w postaci popularnych formatów min: PDF, CSV, HTML. Raporty muszą obejmować zagadnienie dotyczące całej sfery bezpieczeństwa.
5.	Korelacja logów	Konfigurowalne opcje powiadamiania o zdarzeniach jak: email, SNMP
6.	Serwisy i licencje	Licencje aktywacyjne na okres do dnia 23.12.2029 r.
7.	Gwarancja oraz wsparcie	Wsparcie: System zarządzania i monitorowania musi być objęty serwisem producenta przez do dnia 23.12.2029 r., upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego minimum w trybie 8x5.

2) Wykonawca zapewni wykonanie usługi wdrożeniowej centralnego systemu logowania, raportowania i korelacji obejmującej:
   a) instalację i konfigurację systemu centralnego logowania, korelacji i raportowania,
   b) konfigurację do 10 raportów,
   c) przeprowadzenie testów działania oraz testów wysokiej dostępności rozwiązania,
   d) opracowanie i przekazanie dokumentacji powykonawczej zawierającej w szczególności:
      – konfigurację systemu logowania, raportowania i korelacji;

- opis raportów i polityk logowania.