

OPIS PRZEDMIOTU ZAPYTANIA (OPZ)

Przedmiotem zapytania jest:

Dostawa firewall-i z serwisem posprzedażnym i oprogramowaniem do archiwizacji i analizy logów

1. Podstawowe definicje:

- 1) awaria – stan niesprawności dostarczonych urządzeń, elementów, oprogramowania uniemożliwiający ich prawidłowe funkcjonowanie, występujący nagle i powodujący ich niewłaściwe działanie lub całkowite unieruchomienie,
- 2) dni robocze – dni od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy wskazanych w ustawie z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (Dz. U. z 2025 r. poz. 296) oraz dni przyjętych przez Zamawiającego za dni wolne od pracy, o których Zamawiający powiadomi niezwłocznie Wykonawcę w formie pisemnej z odpowiednim wyprzedzeniem,
- 3) nienależyte wykonanie Umowy – sytuacja, gdy świadczenie nie zostało spełnione w terminie lub nie zostało spełnione w całości albo gdy świadczenie zostało spełnione, ale interes Zamawiającego nie został zaspokojony w sposób odpowiadający treści Umowy,
- 4) niewykonanie Umowy – sytuacja, gdy świadczenie w ogóle nie zostało spełnione,
- 5) serwis posprzedażny – wszelkie czynności podejmowane przez Wykonawcę w celu zapewnienia realizacji serwisu gwarancyjnego zgodnie z wymaganiami określonymi w Opisie przedmiotu zapytania,
- 6) urządzenie – firewall zaoferowany z oprogramowaniem systemowym/sterującym i dostarczony przez Wykonawcę w ramach przedmiotu Umowy, fabrycznie nowy, wolny od jakichkolwiek wad fizycznych i prawnych oraz roszczeń osób trzecich, wyprodukowany nie wcześniej niż w 2025 roku,
- 7) usterka – stan, w którym dostarczone urządzenie, elementy, oprogramowanie sygnalizuje niepoprawne działanie hardware’u/software’u (oprogramowania) ale może dalej pracować,
- 8) Ustawa – Ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych Dz. U. z 2026 r. poz. 793),
- 9) elementy - akcesoria dodatkowe do urządzeń np. służące do mocowania urządzenia w szafie rackowej, itp.
- 10) instruktaż wstępny - zapoznanie pracowników z obsługą i konfiguracją urządzenia,
- 11) Oprogramowanie – oprogramowanie do archiwizacji i analizy logów.

2. Wykaz przedmiotu zamówienia:

- Cztery urządzenia UTM firewall z systemem IPS, anty malware oraz URL-filtering,
- Przepustowość łącza do urządzenia firewall z sieci WAN – minimum 1Gbps,
- Przepustowość łącza od urządzenia firewall do INTERNETU – minimum 500 Mbps.
- Oprogramowania do archiwizacji logów oraz analizowania danych wraz z wdrożeniem

Tabela nr 1. Minimalne wymagania dla każdego firewalla

Nazwa	Parametry minimalne
Opis urządzenia	1. Urządzenie musi pełnić rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej firewall-a Next-Generation (NGFW). 2. Urządzenie musi być wyposażone w: a) min. 12 portów 1 Gigabit Ethernet (każdy obsługujący prędkość 10/100/1000BaseT Gigabit Ethernet), b) min. 4 porty 1 GE SFP oraz c) min. 2 porty 10 GE SFP. d) zamiast pozycji lit. b i c Zamawiający dopuszcza 4 porty pracujące z prędkością 1/10 GE SFP/SFP+ e) lub równoważną konfigurację dla punktów lit. a, b, c, d 3. Urządzenie musi być wyposażone w dedykowany port konsoli oraz dedykowany port 1 Gigabit Ethernet do zarządzania MGMT.

	- Urządzenie musi posiadać redundantne wbudowane zasilacze zasilane prądem przemiennym 230V. - Urządzenie musi posiadać możliwość montażu w szafie RACK 19". Urządzenie będzie dostarczone wraz z elementami montażowymi do szafy RACK 19". - Urządzenie musi mieć wysokość nie większą niż 1U.
UTM Firewall	- Wydajność urządzenia dla uruchomionych modułów firewall-a oraz kontroli aplikacji (AVC) – min. 1,5 Gb/s. - Wydajność urządzenia dla uruchomionych modułów systemu IPS – min. 1,2 Gb/s. - Min. liczba obsługiwanych sesji równoległych (TCP): 250 000, z możliwością zestawiania min. 12 000 nowych połączeń na sekundę (TCP). - Urządzenie musi mieć możliwość pracy jako brama VPN z wydajnością min. 600 Mb/s dla IPSec VPN AES256-SHA256. - Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej. - Urządzenie musi obsługiwać routing statyczny i dynamiczny (RIP, OSPF, BGP). - Urządzenie musi zapewniać poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. - Urządzenie musi posiadać ochronę przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. - Urządzenie musi posiadać kontrolę zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. - Urządzenie musi posiadać kontrolę stron WWW oraz SSL Inspection - Urządzenie musi posiadać możliwość stworzenia/uruchomienia usługi Web-Proxy. - Urządzenie musi posiadać możliwość zarządzania pasmem (QoS, Traffic shaping). - Polityka firewall-a musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. - Firewall musi zapewniać translację adresów NAT: źródłowego i docelowego. - Urządzenie musi posiadać możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory. - Urządzenie musi zapewniać mechanizmy redundancji w tym możliwość konfiguracji urządzenia w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active-active, active-passive, clustering. - Urządzenie musi zapewniać funkcjonalność tzw. Firewall-a Next-Generation w zakresie: - systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control), - systemu IPS, - systemu antymalware, - filtracja treści URL.
IPS	- System IPS musi zapewniać: - możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system), - możliwość pracy w trybie pasywnym (IDS). - System IPS musi zapewniać możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym: - złośliwego oprogramowania, - ataków na usługę VoIP, - prób przepełnienia bufora, - ataków na aplikacje P2P,

	• zagrożeń dnia zerowego, itp. 3. System IPS musi zapewniać możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna). 4. System IPS musi zapewniać wiele sposobów wykrywania zagrożeń w tym: • sygnatur ataków opartych na exploitach, • reguł opartych o wzorce znanych zagrożeń, • mechanizmy wykrywania anomalii w protokołach. 5. System IPS musi zapewniać możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, jak również sprawdzania zawartości pakietów. 6. System IPS musi zapewniać mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives). lub inny mechanizm realizując podobną funkcjonalność. 7. System IPS musi zapewniać możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń lub możliwość wyeksportowania tego typu zdarzeń do zewnętrznego urządzenia typu SIEM. 8. System IPS musi zapewniać możliwość reakcji na zdarzenia min. takie, jak: • tylko monitorowanie, • blokowanie ruchu zawierającego zagrożenia, • zapisywanie pakietów. 9. System IPS musi zapewniać możliwość detekcji ataków i zagrożeń opartych na protokole IPv6. 10. System IPS musi zapewniać możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, SSH itp. 11. System IPS musi zapewniać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji. 12. System IPS musi zapewniać możliwość obrony przed atakami skonstruowanymi tak, aby uniknąć wykrycia przez IPS. W tym celu musi zapewnić możliwość blokowania każdego połączenia, które nosi znamiona manipulacji nr sekwencyjnymi segmentów TCP, bez względu do jakiego hosta docelowego kierowane jest to połączenie. 13. System IPS musi zapewniać mechanizm bezpiecznej aktualizacji sygnatur/reguł. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne. 14. System IPS musi umożliwiać definiowanie wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie. 15. System IPS musi zapewniać możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS.
Antymalware	1. Urządzenie musi zapewniać możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym: • pliki systemowe, • pliki graficzne, • pliki PDF, • pliki wykonywalne, • pliki multimedialne, • pliki pakietu Office, • pliki skompresowane. 2. Urządzenie musi posiadać możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download. 3. Urządzenie musi posiadać podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez: • sprawdzenie reputacji plików w systemie globalnym, • statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu.

URL filtering	System filtracji URL musi zapewniać: • kategoryzację stron – w co najmniej 50 kategoriach.
Wymagania dla oprogramowania do archiwizacji i analizy logów	1) Oprogramowanie w postaci dedykowanego urządzenia lub dedykowanej maszyny wirtualnej działającej na wirtualizatorze ESXi lub oprogramowaniu instalowanym na serwerze z systemem Windows lub systemem dostarczonym przez oferenta 2) Zapewni obsługę minimum 6 urządzeń UTM 3) Obecny wolumen danych to 0,8 GB/dzień 4) Licencja stała (perpetual) 5) Zapewni możliwości zbierania i analizowania logów z obecnie eksploatowanych przez Zamawiającego UTM-ów tj. a) Firmy Fortinet modele Fortigate 100F

- 1) Wykonawca w ramach dostawy przeprowadzi instruktaż wstępny w siedzibie Zamawiającego (ul. Pruszkowska 17, Warszawa) z obsługi firewall-i dla maksymalnie 4 pracowników (w tym samym czasie). Czas trwania instruktażu minimum 8 godzin. Merytoryczna zawartość instruktażu zostanie uzgodniona z Zamawiającym przed instruktażem i będzie zawierała minimum zapoznanie uczestników z architekturą, konfiguracją oraz administracją firewall-ami.
- 2) Dostarczone urządzenia, elementy i oprogramowanie muszą pochodzić z legalnego źródła i autoryzowanego kanału sprzedaży producenta na terytorium Rzeczypospolitej Polskiej. Na wezwanie Zamawiającego Wykonawca zobowiązany będzie udokumentować Zamawiającemu kanał dystrybucyjny zaoferowanych urządzeń i oprogramowania.
- 3) Wykonawca odpowiada za wszelkie wady prawne dostarczonych urządzeń, elementów i oprogramowania, w tym również za ewentualne roszczenia osób trzecich wynikające z naruszenia praw własności intelektualnej lub przemysłowej, w tym praw autorskich, patentów, praw ochronnych na znaki towarowe oraz praw z rejestracji na wzory użytkowe i przemysłowe, pozostające w związku z wprowadzeniem urządzeń oraz oprogramowania i licencji do obrotu na terytorium Rzeczypospolitej Polskiej; ewentualne roszczenia osób trzecich wynikające z praw autorskich lub patentowych, dotyczące przedmiotu dostawy, będą dochodzone bezpośrednio od Wykonawcy.
- 4) Zaoferowane i dostarczone urządzenie i elementy muszą być fabrycznie nowe, wolne od jakichkolwiek wad fizycznych i prawnych oraz roszczeń osób trzecich.
- 5) Wykonawca zobowiązuje się dostarczyć firewall-e wraz z niezbędnym oprogramowaniem, elementami, podzespołami, kablami i szynami RACK wymaganymi do podłączenia we wskazanych przez Zamawiającego lokalizacjach na terenie Warszawy.
- 6) Podmiot, który będzie świadczył serwis urządzenia musi posiadać autoryzację (w zakresie świadczenia usług serwisowych) producenta urządzeń.
- 7) Dostarczone firewall-e muszą być wyprodukowane nie wcześniej niż w 2025 roku.
- 8) Wykonawca zrealizuje dostawę urządzeń, elementów i oprogramowania, w tym niezbędnych licencji w terminie dni od dnia zawarcia umowy.

3. Warunki gwarancji, rękojmi i serwisu posprzedażnego w okresie gwarancji:

3.1. Warunki gwarancji

- 1) Okres gwarancji na każde z dostarczonych urządzeń i oprogramowanie wynosi 36 miesięcy.
- 2) Okres gwarancji rozpoczyna bieg od daty podpisania przez Zamawiającego, bez zastrzeżeń, Protokołu odbioru.
- 3) Dostarczone urządzenia, elementy i oprogramowanie muszą być objęte gwarancją producenta /autoryzowanego dystrybutora na Polskę/oficjalnego dystrybutora na Polskę.
- 4) W dniu dostawy urządzeń, elementów i oprogramowania Wykonawca doręczy Zamawiającemu poświadczenie producenta, autoryzowanego dystrybutora lub oficjalnego dystrybutora na Polskę, że dostarczone urządzenia, elementy i oprogramowanie będą objęte gwarancją producenta lub oficjalnego dystrybutora na Polskę na okres 36 miesięcy od dnia podpisania – bez zastrzeżeń Protokołu odbioru.

- 5) Wykonawca w terminie do 5 dni od dnia podpisania bez zastrzeżeń Protokołu odbioru, zobowiązany będzie dostarczyć prawidłowo wystawione karty gwarancyjne. W każdej karcie gwarancyjnej Wykonawca zamieści informacje zawierające nazwę, adres i telefony podmiotu wykonującego serwis gwarancyjny.
- 6) W okresie gwarancji Zamawiający będzie miał dostęp do bezpłatnych uaktualnień, poprawek oraz nowych wersji oprogramowania.
- 7) W okresie gwarancji Wykonawca zapewni, na życzenie Zamawiającego, weryfikację możliwości aktualizacji oprogramowania i pomoc w instalacji udostępnianych przez producenta oprogramowania uaktualnień i poprawek w jego działaniu.
- 8) Gwarantowany czas usunięcia usterki urządzenia, elementu i oprogramowania – w ciągu 10 dni roboczych od zgłoszeniu usterki w miejscach instalacji urządzenia.
- 9) Gwarantowany czas usunięcia awarii urządzenia, elementu i oprogramowania w ciągu dni roboczych (*w zależności od podanej wielkości w ofercie Wykonawcy*) od zgłoszenia awarii. Dotyczy to tylko urządzenia zaoferowanego przez Wykonawcę.
- 10) W przypadku konieczności wymiany urządzenia na nowe, bieg okresu gwarancji rozpoczyna się na nowo, od dnia jego wymiany przez Wykonawcę, potwierdzonej podpisaniem protokołu odbioru - bez zastrzeżeń.
- 11) Wykonawca w terminie do 5 dni od dnia podpisania bez zastrzeżeń protokołu odbioru nowego urządzenia, o którym mowa w ppkt 10 zobowiązany będzie dostarczyć prawidłowo wystawioną kartę gwarancyjną. W każdej karcie gwarancyjnej Wykonawca zamieści informacje zawierające nazwę, adres i telefony podmiotu wykonującego serwis gwarancyjny.

3.2. Warunki rękojmi

- 1) Wykonawca udziela rękojmi na dostarczone urządzenia/elementy na okres obowiązywania gwarancji, której bieg rozpoczyna się w dniu podpisania przez Strony bez zastrzeżeń Protokołu odbioru.
- 2) Zamawiający zastrzega sobie prawo dochodzenia roszczeń z tytułu rękojmi, zgodnie z przepisami Kodeksu cywilnego.
- 3) Informacje o awariach/usterkach Zamawiający będzie zgłaszał do Wykonawcy w dni robocze w godzinach 8:15-16:15, w formie pisemnej na adres do korespondencji lub za pośrednictwem poczty e-mail.

3.3. Warunki serwisu posprzedażnego

- 1) W okresie gwarancji Wykonawca zobowiązuje się do zapewnienia ciągłości realizacji serwisu gwarancyjnego, w miejscu instalacji urządzeń, na warunkach określonych w ppkt 2-13.
- 2) Serwis gwarancyjny obejmuje naprawę dostarczonych przez Wykonawcę urządzeń, elementów i oprogramowania przez producenta/autoryzowanego partnera serwisowego producenta.
- 3) Wykonawca odpowiada za prawidłową obsługę zgłoszeń serwisowych w tym za dotrzymanie terminu naprawy określonego w pkt 3.1 w ppkt 8 – 9.
- 4) Wykonawca w ramach serwisu posprzedażnego zapewni możliwość przyjmowania zgłoszeń o usterekach i awariach w działaniu urządzeń, elementów i oprogramowania w dni robocze w godz. 8:15-16:15.
- 5) Zamawiający będzie dokonywał zgłoszeń drogą elektroniczną lub pisemnie.
- 6) Zgłoszenia o usterekach i awariach w działaniu urządzeń, elementów i oprogramowania doręczone Wykonawcy w dni robocze po godz. 16:15 lub w dni ustawowo wolne od pracy traktowane będą jako zgłoszenia otrzymane o godz. 8:15 kolejnego dnia roboczego.
- 7) W przypadku niemożności naprawy urządzenia/elementu w terminie określonym w pkt 3.1 w ppkt 8-9, na żądanie Zamawiającego, Wykonawca następnego dnia roboczego – na czas naprawy – dostarczy, na własny koszt, urządzenie, element o parametrach nie gorszych od zaoferowanego oraz o porównywalnej funkcjonalności, a także dokona jego instalacji i konfiguracji celem zapewnienia poprawnej pracy. Dotyczy to tylko urządzenia/elementów zaoferowanych przez Wykonawcę.
- 8) Wykonawca zobowiązany będzie do wymiany urządzenia/elementu na nowy (dotyczy to tylko urządzenia/elementów zaoferowanych przez Wykonawcę) w terminie 5 dni roboczych, od dnia zgłoszenia przez Zamawiającego takiego żądania w formie pisemnej, w przypadkach:
 - a) wystąpienia kolejnej awarii, wady lub usterki urządzenia, elementu po wcześniejszym wykonaniu 3 napraw gwarancyjnych,
 - b) niewykonania naprawy w terminie do 30 dni.

- 9) W przypadku wymiany urządzenia/elementu na nowe, na warunkach określonych w ppkt 8, Zamawiający wymaga, aby nowe urządzenie/element posiadało parametry nie gorsze od zaoferowanego.
- 10) W przypadku wymiany urządzenia/elementu na nowe (*dotyczy to tylko urządzenia/elementu zaoferowanego przez Wykonawcę*), bieg okresu gwarancji rozpoczyna się na nowo, od dnia jego wymiany przez Wykonawcę, potwierdzonej protokołem odbioru,
- 11) W okresie gwarancji Wykonawca zapewnia Zamawiającemu wsparcie konsultacyjne w zakresie obsługi oprogramowania, drogą telefoniczną i e-mailową.
- 12) Wykonawca zapewni serwis posprzedażny w zakresie dostarczonego oprogramowania na okres obowiązywania gwarancji.
- 13) W okresie gwarancji Wykonawca będzie świadczyć na rzecz Zamawiającego pierwszą linię wsparcia w języku polskim w zakresie pomocy w rozwiązywaniu problemów i diagnozowania niesprawności oprogramowania, drogą telefoniczną i e-mailową na podany w Umowie nr telefonu i adres e-mail.
- 14) Podmiot, który będzie świadczył serwis gwarancyjny, musi posiadać autoryzację producenta w zakresie świadczenia usług serwisowych.
- 15) W przypadku uszkodzenia dysku pozostaje on u Zamawiającego.
- 16) W przypadku awarii urządzenia i potrzeby jego zabrania w celu naprawy dysk pozostaje u Zamawiającego.