

## OPIS PRZEDMIOTU ZAMÓWIENIA

### ZAPORA SIECIOWA CZĘŚĆ 3

1. **Nazwa zamówienia:** Zapora sieciowa.
2. **Ilość:** 2 szt.
3. **Wymagania ogólne:** Wymagane jest wznowienie na okres 1 roku niżej wymienionych subskrypcji zabezpieczeń i serwisów dla posiadanych przez Zamawiającego 2-ch urządzeń FortiGate 200E (numery seryjne: FG200ETK18919582, FG200ETK18919438) działających jako osobne, niezależne systemy:
  - a. IPS, Malicious/Botnet URLs,
  - b. Anti-Malware Protection (AMP): AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct, AI-based Heuristic AV, FortiGate Cloud Sandbox,
  - c. URL, DNS and Video Filtering, Malicious Certificate
  - d. Anti-Spam,
  - e. AI-based Inline Malware Prevention,
  - f. Data Loss Prevention (DLP),
  - g. Attack Surface Security: IoT Device Detection, IoT Vulnerability, Correlation and Virtual Patching, Security Rating, Outbreak Check,
  - h. Application Control,
  - i. Inline CASB,
  - j. FortiCare Premium 24x7: Hardware, Firmware & General Updates, Enhanced Support, Telephone Support,  
(oznaczenie producenta: Fortinet FortiGate-200E Enterprise Protection, SKU: FC-10-00207-809-02-12),lub systemy o równoważnej funkcjonalności, w liczbie 2-ch kompletów, cechujące się co najmniej możliwościami opisanymi w pkt 4 – „Wymagania dla systemu równoważnego”. W przypadku zaoferowania wznowienia wyżej opisanych subskrypcji Zamawiający dopuszcza wymianę obecnie posiadanych urządzeń na nowsze warianty, pod warunkiem zapewnienia, że parametry zaoferowanych urządzeń będą nie gorsze niż urządzeń obecnie wykorzystywanych przez Zamawiającego.
4. **Wymagania dla systemu równoważnego:**
  - a. Systemy równoważne muszą być dostarczone w postaci dedykowanych urządzeń przeznaczonych do montażu w szafie rack 19 cali, w obudowie o wysokości 1U.
  - b. System musi wykorzystywać dedykowany system operacyjny, nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia.
  - c. System musi posiadać funkcje filtrowania pakietów oparte na kontroli stanu połączenia (stateful inspection).
  - d. Wymagana jest obsługa protokołów minimum IPv4, IPv6, ARP.
  - e. Wymagana jest ochrona przed atakami DoS/DDoS, IP spoofing, SYN flooding, ochrona oparta na filtrach DNS, ochrona oparta na filtrach URL na stronach www i w poczcie elektronicznej, ochrona przed botnetami, ochrona przed skanowaniem portów i adresów, ochrona bazująca na subskrypcjach zewnętrznych list niebezpiecznych domen, ochrona oparta o filtry wykorzystujące kategoryzację stron.

- f. Wymagana jest obsługa filtrowania pakietów dla protokołów dynamicznych co najmniej z wykorzystaniem funkcji Application Control (warstwa 7).
- g. Wymagana jest obsługa filtrowania pakietów dla protokołów statycznych.
- h. Wymagana jest obsługa wielu łącz internetowych z możliwością automatycznego ich przełączania w momencie awarii, jak również z możliwością wykorzystywania kilku łącz równocześnie, z możliwością ręcznego określenia priorytetów dla łącz oraz użycia algorytmów uwzględniających opóźnienia, stabilność, utratę pakietów, przepustowość.
- i. Wymagana jest obsługa pakietów o zwykłej wielkości jak i tzw. jumbo frame o wielkości minimum 9000B.
- j. Wymagana jest obsługa funkcjonalności proxy i inspekcji dla protokołów HTTP, HTTPS.
- k. Wymagana jest obsługa IPv4 NAT (co najmniej source i destination), PAT.
- l. Wymagana jest obsługa VPN w zakresie zestawiania połączeń za pomocą protokołu IPSec, obsługa algorytmów szyfrowania minimum AES128, AES256, 3DES, wraz z możliwością zestawienia minimum 500 tuneli VPN jednocześnie (Client to Gateway VPN Tunnels).
- m. Wymagana jest obsługa klienta do zestawiania tuneli Client to Gateway dla minimum systemów Windows i Linux. Wymagana jest obsługa klienta dla systemów Windows ze zintegrowanym firewallem oraz funkcją oceny stanu bezpieczeństwa komputera przed podłączeniem komputera przez VPN.
- n. Wymagana jest możliwość autoryzacji połączeń VPN Client to Gateway przy użyciu wewnętrznej bazy użytkowników, zewnętrznego serwera Radius, LDAP oraz możliwość użycia do autoryzacji techniki MFA wykorzystującej system FortiAuthenticator Zamawiającego.
- o. Wymagana jest obsługa zarządzania ruchem w obrębie sieci VPN za pomocą technologii traffic shaping, z obsługą min. 3 priorytetów, obsługą gwarantowanej i maksymalnej przepustowości oraz DSCP.
- p. Wymagana jest możliwość zestawiania tunelu VPN Site to Site przy wykorzystaniu kilku łącz, na zasadzie wykorzystywania kilku kanałów fizycznych, wchodzących w skład danego tunelu VPN. Wymagana jest obsługa minimum 2 kanałów na jeden tunel, możliwość wyznaczania kanałów zapasowych, detekcja uszkodzenia danego kanału i automatyczne przełączenie ruchu na sprawne kanały w przypadku uszkodzenia.
- q. Wymagana jest możliwość zestawiania tuneli VPN zarówno na łączach internetowych, jak i łączach dedykowanych do transmisji danych.
- r. Wymagana jest możliwość wykorzystania certyfikatów do uwierzytelniania tuneli VPN Site to Site.
- s. Wymagana jest funkcja monitoringu ruchu sieciowego na konsoli graficznej zarządzania, w tym zbliżone do czasu rzeczywistego monitorowanie ruchu wg. zadanego filtra (minimum wg. interfejsu sieciowego, aplikacji, sesji, stron www, kategorii www, użytkowników VPN, reguł zapory, hostów źródłowych, hostów docelowych, użytkowników, kwarantanny, punktów dostępowych sieci Wi-Fi, obcych sieci Wi-Fi, urządzeń podłączonych do sieci LAN i do sieci Wi-Fi).
- t. Wymagana jest obsługa funkcji IPS i IDS wraz z aktualizacją sygnatur i możliwością tworzenia własnych polityk i sygnatur oraz definiowania, w ramach własnych polityk, sposobów reakcji systemu na pakiety zawierające poszczególne sygnatury będące w bazie systemu.

- u. Wymagana jest obsługa funkcji inspekcji (IPS oraz aplikacyjna) ruchu w protokołach nieszyfrowanych, jak i w protokołach szyfrowanych minimum SSL/TLS.
- v. Wymagana jest obsługa funkcji filtrowania ruchu w warstwie 7 protokołu TCP/IP dla minimum 2000 zdefiniowanych aplikacji min. typu: P2P, Remote Access, Proxy, Storage/Backup, Generative AI, Video/Audio, Games, Mobile, Social Media, Cloud/IT.
- w. Wymagana jest funkcjonalność serwera DHCP, serwera DNS.
- x. Wymagana jest obsługa filtrowania URL wraz z aktualizacją zbiorów URL utrzymywanych przez producenta oraz możliwość definiowania własnych polityk, w ramach których wskazane grupy adresów URL są blokowane. Wymagana jest możliwość zdefiniowania własnych URL. Zdefiniowane polisy filtrowania URL muszą być możliwe do przypisania do poszczególnych reguł firewalla.
- y. Wymagane jest uwierzytelnianie klientów za pomocą protokołów i technologii minimum x.509, NTLM, Radius, LDAP/LDAPS, Active Directory w tym integracja z AD w celu nasłuchiwania logowań użytkowników, aby firewall mógł mapować adresy IP na konkretnych użytkowników.
- z. Wymagana jest możliwość tworzenia własnych obiektów sieciowych (minimum definiowane przez adresy IP, grupy adresów IP, zakresy adresów IP, grup użytkowników AD) wraz z możliwością nazywania zdefiniowanych obiektów i ich wykorzystywania w regułach.
- aa. Wymagana jest możliwość tworzenia dynamicznych reguł firewalla opartych o przypisanie użytkownika do grupy, przedział czasowy, w jakim dana reguła ma działać.
- bb. Wymagana jest możliwość generowania wykresów ruchu przepływającego przez system w czasie zbliżonym do rzeczywistego. Wymagana jest możliwość generowania raportów ruchu przepływającego przez system w postaci zestawień generowanych zgodnie z zadaniem harmonogramem.
- cc. Wymagana jest obsługa routingu z trasami definiowanymi zarówno statycznie, jak i dynamicznie wraz z obsługą protokołów OSPF i RIP.
- dd. Rozwiązanie równoważne musi posiadać pełną zgodność ze standardami IETF dla protokołu IPsec (w tym obsługa algorytmów szyfrowania: AES 128, 256, 256GCM, 3DES, obsługa algorytmów uwierzytelniania: SHA-2 (256, 384, 512), metody wymiany kluczy Diffie-Hellman grupy 1, 2, 5, 14, 15, 19, 20, 21, 31, 32).
- ee. Rozwiązanie musi spełniać wymagania normy ISO 15408 Common Criteria na poziomie EAL 4+ lub musi posiadać certyfikat ICSSA Labs minimum w zakresie Corporate Firewall lub producent rozwiązania równoważnego musi być wymieniony na aktualnym raporcie „Magic Quadrant” firmy Gartner, w co najmniej jednej z kategorii dotyczących zapór sieciowych.
- ff. Urządzenia równoważne muszą mieć możliwość zestawienia tuneli VPN między sobą, jak również w razie potrzeby muszą mieć możliwość pracy w połączeniu w trybie wysokiej dostępności (HA) jako jedno wirtualne urządzenie, jeśli taka będzie potrzeba Zamawiającego.
- gg. W przypadku zaoferowania rozwiązania równoważnego, urządzenie musi być wyposażone w minimum 12 niezależnych portów Ethernet zakończonych złączem RJ-45 o wydajności 10/100/1000, obsługujących funkcję 802.1q VLAN oraz minimum 2 porty Gigabit ze złączem SFP. Urządzenia muszą posiadać min. 2 porty WAN RJ-45 lub musi być możliwość zdefiniowania 2 portów WAN w konfiguracji urządzenia.

- hh. W komplecie z każdym urządzeniem musi być dostarczona min. 1 wkładka optyczna do portu SFP oraz kabel optyczny o długości min. 2 m, zakończony złączem LC do połączenia do portu optycznego 1Gbps w przełączniku Zamawiającego.
- ii. Urządzenie takie musi zapewniać obsługę co najmniej 20 segmentów sieci.
- jj. Wydajność urządzenia w zakresie filtrowania pakietów nie może być mniejsza niż 9 Gbps, w zakresie filtrowania IPS wydajność nie może być mniejsza niż 2 Gbps.
- kk. Urządzenie musi posiadać minimum 2 zasilacze 230V zapewniające pracę urządzenia po awarii jednego z zasilaczy lub zaniku zasilania z jednego obwodu, diody sygnalizacyjne.
- ll. Do urządzenia muszą być dołączone akcesoria montażowe do montażu urządzenia w szafie 19 cali.
- mm. Urządzenia muszą być wyposażone w port konsoli oraz port zarządzania.
- nn. Dla rozwiązania równoważnego należy zapewnić w okresie co najmniej 1 roku od daty aktywacji prawo do aktualizacji sygnatur i baz, prawo do aktualizacji oprogramowania oraz aktualizacji opisanych funkcji zabezpieczeń (przez 24 godziny na dobę), dostęp do wsparcia technicznego minimum w języku angielskim lub polskim. Dodatkowo należy zapewnić 2-letnią gwarancję na urządzenia, wymianę urządzenia w przypadku jego awarii w ciągu jednego dnia roboczego.
- oo. Aktywacja licencji, wsparcia, aktualizacji sygnatur i baz na rozwiązanie równoważne musi być możliwa do przeprowadzenia w okresie minimum do 2 miesięcy od dnia dostawy, tak aby wykorzystać maksymalnie okres wsparcia do posiadanego przez Zamawiającego rozwiązania.
- pp. System musi być w pełni kompatybilny z urządzeniami i systemami Zamawiającego: FortiAnalyzer, FortiSandbox, FortiAuthenticator, FortiMail, FortiAP.
- qq. Proces uwierzytelniania administratorów musi być realizowany co najmniej w oparciu o: lokalną bazę, RADIUS, LDAP, PKI oraz dostawcę tożsamości z wykorzystaniem SAML SSO.
- rr. Wymagana jest możliwość wykorzystania funkcji SAML SSO w celu integracji z zewnętrznym dostawcą tożsamości, co najmniej z systemem FortiAuthenticator Zamawiającego.
- ss. Obsługa systemu powinna być możliwa zarówno za pomocą graficznego interfejsu użytkownika (WebGUI) jak i z wiersza poleceń (CLI). Komunikacja z konsolą graficzną zarządzania powinna wykorzystywać szyfrowane połączenie (HTTPS). Komunikacja z konsolą tekstową powinna być możliwa co najmniej przez protokół Secure Shell (SSH).
- tt. W przypadku, gdy zaoferowany przez Wykonawcę system równoważny nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem sprawnego działania infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego.
- uu. System zaoferowany przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie systemu równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie systemu równoważnego, dla którego producent

oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.

- vv. W przypadku zaoferowania systemu równoważnego Wykonawca zobowiązany jest przeprowadzić szkolenie w Łodzi dla 6 administratorów Zamawiającego z zakresu instalacji, konfiguracji i zarządzania systemem równoważnym, umożliwiającym pełne poznanie produktu równoważnego. Szkolenie musi być przeprowadzone w terminie 10 dni od daty dostawy urządzeń.
  - ww. Dla systemu równoważnego wymagane jest przeprowadzenie migracji konfiguracji z istniejących urządzeń, migracji po godzinach pracy urzędu, w razie potrzeby Zamawiający udostępni kopie konfiguracji posiadanych urządzeń. W przypadku zaoferowania systemu równoważnego Wykonawca zobowiązany jest do zainstalowania systemu równoważnego w środowisku Zamawiającego oraz dokonania poprawnej migracji i konfiguracji wymaganych połączeń systemu i zapewnienia poprawnego działania funkcji ochrony i komunikacji nie później niż do 3 czerwca 2026 r.
- 5. **Gwarancja:** w przypadku urządzeń równoważnych min. 2 letnia gwarancja producenta systemu, w ramach gwarancji w przypadku awarii wymagana jest możliwość wymiany wadliwego urządzenia w następnym dniu roboczym.
  - 6. **Okres wznowienia:** 1 rok, koniec aktualizacji oferowanego wznowienia i funkcji zabezpieczeń nie może być wcześniejszy niż 03 czerwca 2027 r.