OPIS PRZEDMIOTU ZAMÓWIENIA

1. **Przedmiotem zamówienia jest dostawa siedmiu urządzeń typu firewall następnej generacji (ang. Next-Generation Firewall (NGFW)) z wbudowaną komunikacją GSM.**

2. Zamawiający wymaga dostarczenia sprzętów (siedem urządzeń NGFW) do siedziby Zarządu Transportu Miejskiego w Warszawie w terminie uzgodnionym z kierownikiem działu Informatyki.

3. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza internetowego i posiadanej infrastruktury w ZTM. NGFW musi być zgodny z rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, wymagane jest aby elementy wchodzące w skład systemu ochrony były zrealizowane wyłącznie w postaci zamkniętej platformy sprzętowej, dotyczy to również modemu GSM. Oprogramowanie oraz sprzęt musi być dostarczony i wspierany przez jednego producenta.

4. Zarządzanie urządzeniami wchodzącymi w pakiet zamówienia (administracja, konfiguracja, aktualizacja) powinny zapewniać bezpieczne szyfrowane połączenia. Urządzenia powinny mieć możliwość zarządzanie oraz monitorowanie logów centralne za pośrednictwem dodatkowych nie wchodzących w skład zamówienia narzędzi.

5. Dostarczone urządzenia powinny być zapakowane w oryginalne opakowanie, przetransportowane w bezpieczny sposób. Urządzenia powinny być jak najbardziej aktualne z ostatniej serii danego modelu (dotyczy daty rozstrzygnięcia postępowania). Produkt nie powinien być starszy niż rok od produkcji.

6. Oferowane rozwiązanie powinno posiadać certyfikat ICSA Labs dla funkcjonalności Network Firewall 2018.

Wymagania techniczne dla urządzenia NGFW.

Urządzenie NGFW musi spełniać minimum poniższe wymagania (parametry podane są dla pojedynczego urządzenia):

1. Urządzenie powinno spełniać wszelkie normy, certyfikaty i być dopuszczone do użytku w ramach swojej funkcjonalności na terenie Unii Europejskiej z uwzględnieniem prawa polskiego: (UL, CB, FCC , CE).

2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych, obsługa SMNPv3, powiadamianie.

3. System zabezpieczeń powinien współpracować ze systemami Windows, Linux.

4. Wbudowany w urządzenie modem GSM/GPRS/EDGE [850/900/1800/1900 MHz] działający na terenie Polski i kompatybilny z kartami SIM polskich operatorów.

5. Specyfikacja minimalna urządzenia:

Tryby Pracy

- Routing (L3)
- Switch (L2)
- Transparentnym

Porty

- Mini. 5x Gigabit Ethernet w tym port WAN (RJ45 100BASE-TX / 1000BASE-T)
- 1x Interfejs Terminalowy (USB/RJ45)

Wydajność/Przepustowość NGFW

Firewall	950 Mbps
IPS	300 Mbps
NGFW	200 Mbps
IPSec VPN	75 Mbps
Liczba Sesji jednocześnie	800 000
Nowe sesje/s	15 000
Virtual Router	4

Sieć

Zarządzanie Adresami IP	-	Static ; DHCPv4 Server, Client, DHCP Relay ; DNS Forwarding.
IP Routing	-	BGPv4/v6; OSPFv2/v3; RIPv2; Static Routes; IP Policy.
Enkapsulacja/Protokoły	-	Ethernet; 802.1Q VLANs; GRE; QoS
VPN	-	IPsec (IKEv1/v2, AES256, SHA256, 3DES); IPSec NAT Traversal; SSL VPN
NAT	-	1:1, x:x, x:y, SNAT, DNAT
Zarządzanie/Autoryzacja	-	CLI; WebGUI HTTPS; SSHv2; SNMPv2/v3; Radius
Możliwość współpracy	-	MS Active Directory.
Parametry GSM	-	LTE, UMTS/HSPA+

6. System, konfiguracja i bazy (AV/IPS, Threat Prevention, URL Filtering) muszą znajdować się na szybkich pamięciach Flash. Bazy powinny znajdować się lokalnie na urządzeniu i być aktualizowane sekwencyjnie (tylko zmiany).

7. W ramach dostarczonego urządzenia muszą być realizowane wszystkie z poniższych funkcjonalności:
   - Firewall - zapora ogniowa klasy Stateful Packet Inspection, system zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrole ruchu sieciowego pomiędzy obszarami sieci na poziomie warstwy sieciowej, transportowej oraz aplikacji. Możliwość rejestracji zdarzeń. Identyfikacja aplikacji bez względu na numery portów czy szyfrowanie (Inspekcja ruchu

SSL/HTTPS). Kontrola aplikacji oraz rozpoznawanie ruchu P2P i IM na wszystkich portach przy użyciu mechanizmu ochrony firewall.

- Ochrona przed wirusami - Antywirus (minimum dla protokołów SMTP, POP3, IMAP, HTTP, SFTP, FTP, HTTPS), Anty-Spyware. Bazy sygnatur Antywirus-a i Anty-Spyware-a powinny być przechowywane na urządzeniu i aktualizowane automatycznie. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
- Poufność transmisji danych – możliwość tworzenia połączeń szyfrowanych IPSec VPN (IKEv1/v2) oraz SSL VPN.
- Ochrona przed atakami - Intrusion Prevention System/Intrusion Detection System [IPS/IDS] (L7 OSI) powinna opierać się co najmniej na analizie protokołów i sygnatur. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos, Bazy powinny być aktualizowane automatycznie i przechowywane na urządzeniu
- Kontrola stron internetowych WWW pod kątem rozpoznawania i blokowania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących, udostępniających treści typu SPAM, oraz pornografię. Baza URL powinna być aktualizowana automatycznie. Tworzenie własnych polityk filtracji WWW, bez użycia zewnętrznego oprogramowania i dodatkowych licencji.
- Kontrola ruchu sieciowego na podstawie rodzaju aplikacji, zdefiniowanego urządzenia lub użytkownika.
- Kontrola pasma oraz ruchu [QoS, Traffic shaping] co najmniej określanie maksymalnej i gwarantowanej ilości pasma.
- Możliwość analizy ruchu szyfrowanego protokołem SSL nie tylko HTTPS, SSH oraz transferu plików.
- Integracja systemów ochrony z Microsoft Active Directory (LDAP, Radius)
- Technologia ochrony przed wyciekiem poufnej informacji (DLP).

8. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
9. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ, Servers, LAN, It.

Wymagania dotyczące wsparcia Technicznego:

1) Pomoc techniczna produktu powinny być dostępne w Polsce na terenie miasta stołecznego Warszawy.
2) Zamawiający wymaga dostarczenia wszystkich niezbędnych licencji i subskrypcji na okres minimum 2 lat (24 miesięcy), w tym okresie bezpłatne wsparcie techniczne producenta oraz wszelkie aktualizacje (łatki, poprawki, update oprogramowania i firmware-u oraz aktualizacje sygnatur dla wszystkich wymaganych funkcjonalności).
3) System bezpieczeństwa powinien być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzeń w przypadku ich wadliwości oraz uszkodzenia. W okresie gwarancji wymagane jest bezpłatne usuwanie awarii oraz bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii.
4) Gwarancja i wsparcie powinno być realizowane przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego. Zgłoszenia serwisowe powinny być przyjmowane w trybie 12-godzinnym (8:00-20:00) od poniedziałku do piątku przez dedykowany portal lub mail wraz z potwierdzeniem przyjęcia oraz infolinię.