OPIS PRZEDMIOTU ZAMÓWIENIA

1. **Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz uruchomienie urządzeń typu firewall następnej generacji (ang. Next-Generation Firewall (NGFW)) w konfiguracji wysokiej dostępności (ang. High Availability - HA) oraz dwóch urządzeń typu Switch + akcesoria wraz z przeszkoleniem pracowników.**
2. Zamawiający wymaga dostarczenia sprzętu (dwa urządzenia NGFW pracujących jako klaster w trybie Active-Active z Switch-ami) wraz z wymienionym osprzętem, montażem w siedzibie Zarządu Transportu Miejskiego w Warszawie (wskazane miejsce montażu i współpraca z działem IT) i instalacją niezbędnego oprogramowania, skonfigurowaniem, testami i uruchomieniem z minimalnymi skutkami na działanie innych systemów Zarządu Transportu miejskiego w Warszawie**.**
3. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. NGFW musi być zgodny z rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane wyłącznie w postaci zamkniętej platformy sprzętowej, oprogramowanie oraz sprzęt musi być dostarczony i wspierany przez jednego producenta.
4. Zarządzanie urządzeniami (administracja, konfiguracja) musi odbywać się za pośrednictwem linii poleceń (CLI) oraz w graficznej konsoli Web GUI, oba sposoby powinny zapewniać szyfrowane połączenia i możliwość wyboru dostępu dla konkretnej sieci, adresu IP, adresu MAC lub za pośrednictwem LDAP.
5. W ramach konfiguracji i uruchomienia urządzeń należy przenieść konfigurację z obecnie używanych systemów na nowe urządzenia ew. ją modyfikując w zależności od potrzeb. Instalacja i konfiguracja systemu musi być przeprowadzona przez uprawnioną osobę posiadającą aktualny certyfikat producenta w zakresie instalacji i konfiguracji urządzeń objętych niniejszym postępowaniem z obowiązującymi praktykami.
6. Oferowane rozwiązanie powinno posiadać certyfikat ICSA Labs dla funkcjonalności Network Firewall i oferowane rozwiązanie powinno zapewniać skuteczność zabezpieczeń (Security Effectiveness) powyżej 95% według raportu Next Generation Firewall Security Value Map z 2016 roku przeprowadzonego przez NSS Labs.
7. Wykonawca przeprowadzi autoryzowane przez producenta urządzeń szkolenia w zakresie konfiguracji i obsługi urządzeń dla 3 osób. Minimalny czas szkolenia 30 godzin zajęć. Minimalny zakres szkolenia:
   1) logowanie i monitoring zdarzeń,
   2) konfiguracja polityk firewall-a,
   3) lokalne uwierzytelnianie użytkowników,
   4) tworzenie i monitoring VPN SSL, IPSec-VPN, operacje oparte na certyfikatach,
   5) konfiguracja skanowania antywirusowego,
   6) konfiguracja filtrów WWW, tworzenie polityk,
   7) kontrola aplikacji,
   8) konfiguracja Routingu w tym BGP i OSPF,
   9) transparently tryb pracy,
   10) wysoka dostępność (Klaster HA - High Availability),
   11) Intrusion Prevention System - IPS,
   12) diagnostyka i rozwiązywanie problemów,
   13) zasoby systemowe - optymalizacja,
   14) rozwiązywanie problemów sieciowych, sniffer,
   15) rozwiązywanie problemów: z uwierzytelnianiem użytkowników

Wymagania dla urządzenia NGFW

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

1. Możliwość łączenia w klaster Active-Active oraz Active-Passive minimum 2 urządzeń,
2. Urządzenia powinno spełniać wszelkie normy, certyfikaty i być dopuszczone do użytku w ramach swojej funkcjonalności na terenie Unii Europejskiej z uwzględnieniem prawa polskiego.
3. Urządzenia powinny być wyposażone w redundantne zasilanie, wymiana nie powinna zakłócać pracy urządzenia, opcjonalnie pojedyncze zasilanie per urządzenie z możliwością wymiany samego zasilacza bez deinstalacji urządzenia.
4. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych, obsługa SMNPv3, powiadamianie email.
5. Specyfikacja minimalna urządzenia:

Tryby Pracy

- Routing (L3)
- Switch (L2)
- Transparentnym,
- Pasywnego nasłuchu (sniffer).

Porty

- 2x 10Gigabit SFP+ (2x GIBIC 10Gigabit kompatybilny z zamówionym sprzętem)
- 8x 1Gigabit RJ45
- 8x 1Gigabit SPF (2x GIBIC 1Gigabit kompatybilny z zamówionym sprzętem)
- 1x Interfejs Zarządzający

Wydajność/Przepustowość NGFW (Uruchomione wszystkie funkcje)

Firewall	10 Gbps
IPS	5 Gbps
AntyVirus/Anti-malware	2,5 Gbps
IPSec VPN	5 Gbps
Liczba Sesji jednocześnie	500 000
Nowe sesje/s	100 000
PołączeniaVPN (Site-to-Site,Client)	1000

Sieć

Zarządzanie Adresami IP	Static; DHCPv4/v6 Server,Client, Relay; DDNS, DNS Forwarding
IP Routing	BGAv4/v6; OSPFv2/v3; RIPv2; Static Routes; IP Policy
Enkapsulacja	Ethernet; 802.1Q VLANs; GRE; PPPoE; IP in IP; Bridging; Bonding (802.3ad)
VPN	OpenVPN; IPsec (IKEv1/v2, AES256, SHA256, 3DES); PPTP; L2TP; IPSec NAT Traversal
Dostępność HA	Firewall / NAT Failover; VRRP; IPSec VPN Clustering
Zarządzanie/Autoryzacja	CLI; WebGUI; SSHv2; Radius; LDAP; ActiveDirectory, RSA SecurlD, TACACS+, Kerberos

Zasilenie

- Dwa zasilacze HotSwap

6. System zabezpieczeń powinien współpracować ze środowiskami wirtualnymi Vmware i Hyper-V oraz systemami Windows, Linux, MacOS.
7. System, konfiguracja i bazy (AV/IPS) muszą znajdować się na szybkich dyskach SSD lub pamięciach Flash, Bazy AV i IPS powinny znajdować się lokalnie na urządzeniu. Aktualizacja systemu, konfiguracji i baz nie powinna wpływać na brak dostępności (rozwiązanie HA).
8. Urządzenie NGFW powinno mieć możliwość gromadzenia logów na dodatkowych Dyskach wbudowanych w urządzenie lub opcjonalnie na urządzeniu zewnętrznym (w tym przypadku dostawca dostarcza takie urządzenie). Dyski powinny pracować w trybie RAID, przestrzeń przeznaczona na logi powinna gwarantować zapis logów z okresu 2 lat. Urządzenie powinno mieć także możliwość przesyłania logów na Serwer Logów.
9. 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.
    - Ochrona przed wirusami - Antywirus (minimum dla protokołów SMTP, POP3, IM AP, HTTP, SFTP, FTP, HTTPS, SMB), 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 (IKE) oraz SSL VPN, kompresja VPN. Konfiguracja VPN w oparciu o ustawienia rutingu (routing-based VPN) i współpraca z OpenVPN.
    - 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 przechowywana na urządzeniu (min 10 milionów URL-i) i aktualizowana automatycznie. Tworzenie własnych polityk filtracji WWW, bez użycia zewnętrznego oprogramowania i dodatkowych licencji.
    - Kontrola pasma oraz ruchu [QoS, Traffic shaping] co najmniej określanie maksymalnej i gwarantowanej ilości pasma.
    - Kontrola aplikacji oraz rozpoznawanie ruchu P2P i IM na wszystkich portach przy użyciu mechanizmu ochrony firewall.
    - Możliwość analizy ruchu szyfrowanego protokołem SSL nie tylko HTTPS, SSH
    - Ochrona przed wyciekiem poufnej informacji (DLP).
10. 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).
11. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.

Wymagania dla Switch-y

12. Specyfikacja minimalna urządzenia:

Tryby Pracy

- L2/L3

Porty

- Mini 4 porty QSFP+ 40Gbps.
- Mini 16x 1/10Gigabit SFP+ (2x GIBIC 10Gigabit kompatybilny z zamówionym sprzętem oraz Switch musi być kompatybilny z HP J9281B, HP J4858C i HP J4859C)
- Mini 16x 1Gigabit RJ45
- 1x Interfejs Zarządzający
- 1x Port Konsoli

Wydajność/Przepustowość

Prędkość magistrali	900Gbps
Przepustowość	700Mpps
Rozmiar tablicy MAC	64000
Bufor	16Mb
Opóźnienie 10Gb	< 2us

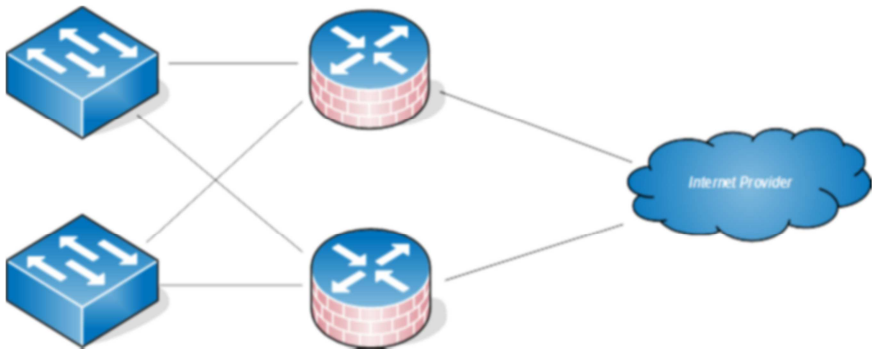
Sieć

- **Standardy:**
  - **IEEE 802.1d, IEEE 802.1p, IEEE 802.1q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3ae, IEEE 802.3azIEEE 802.3i, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z**
- **Zarządzanie:**
  - **CLI (Terminal)**
  - **HTTP**
  - **HTTPS**
  - **SNMP v1**
  - **SNMP v2c**
  - **SNMP v3**
  - **SSH**

Zasilanie

- Dwa zasilacze HotSwap
- Wentylatory HotWwap

Przykładowa architektura



Wymagania dotyczące wsparcia Technicznego oraz wdrożenia:

1) Pomoc techniczna oraz szkolenia z produktu powinny być dostępne w Polsce na terenie miasta stołecznego Warszawy. Usługi szkoleniowe muszą być dostępne w języku polskim w aut-oryzowanych ośrodkach edukacyjnych.
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) Wdrożenie produktu powinno obejmować wszystkie niezbędne funkcjonalności podane powyżej dla prawidłowego funkcjonowania systemu bezpieczeństwa.
4) 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.
5) Gwarancja i wsparcie powinno być realizowane przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego, z czasem reakcji na poziomie do 4 godzin od poniedziałku do piątku 7:00-20:00 i do 6 godzin w pozostałe dni i godziny. Zgłoszenia serwisowe powinny być przyjmowane w trybie 24-godzinnym od poniedziałku do niedzieli przez dedykowany portal lub mail wraz z potwierdzeniem przyjęcia oraz infolinię.
6) Zamawiający wymaga aby oferta zawierała cenę zakupu w/w rozwiązania, cenę wdrożenia i wsparcia w/w oraz szkoleniem.
7) Wdrożenie nastąpi po wcześniejszym uzgodnieniu szczegółowego harmonogramu działań oraz określeniu ryzyka i planu awaryjnego pomiędzy zamawiającym a dostawcą rozwiązania.