**Załącznik nr 1.5 do SWZ**

**SPECYFIKACJA TECHNICZNA – UTM CENTRALNY – 1 SZT.**

• Nazwa: …  
• Typ/model/nr katalogowy: …  
• Producent / kraj pochodzenia: …  
• Rok produkcji: …

| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowanego sprzętu**  **PODAĆ** |
| --- | --- | --- | --- |
| **1** | **Wymagania ogólne:** | • System bezpieczeństwa musi realizować: Firewall, VPN (IPSec), IPS, Antywirus, Kontrola aplikacji, Web Filtering, Antyspam, DLP, QoS, SD-WAN, inspekcję SSL – niezależnie od dostawcy łącza, w formie sprzętowej lub programowej z zapewnieniem platformy sprzętowej oraz zabezpieczonego systemu operacyjnego. • Firewall musi wspierać tryby pracy: Router z NAT, Transparent, SPAN. • Możliwość konfiguracji minimum 2 instancji systemu (Routing, Firewall, VPN, IPS, Antywirus, Kontrola aplikacji). • Możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji. • Pełne wsparcie IPv4 i IPv6 dla: Firewall, aplikacyjna ochrona, dynamiczne protokoły routingu. |  |
| **2** | **Redundancja i monitoring:** | • Obsługa klastrów HA: Active-Active oraz Active-Passive z synchronizacją sesji. • Monitoring sprzętu, oprogramowania i stanu połączeń VPN. • Agregacja linków (statycznie i LACP), tworzenie interfejsów redundantnych. |  |
| **3** | **Interfejsy i zasilanie:** | • Min. 8 x 1GbE RJ-45, 2 x 10GbE SFP+ (wraz z 2 wkładkami MMF SFP+). • Port konsoli szeregowej oraz port USB. • Obsługa min. 200 interfejsów VLAN (802.1Q). • Min. 2 zasilacze AC (redundancja). |  |
| **4** | **Wydajność:** | • Min. 1,5 mln jednoczesnych sesji, 120 tys. nowych/s. • Stateful Firewall ≥ 28 Gbps (512B). • Z włączoną Kontrolą Aplikacji ≥ 6,5 Gbps. • IPSec VPN (AES-128) ≥ 25 Gbps. • IPS ≥ 4 Gbps (Enterprise Traffic Mix). • IPS+Antywirus+Aplikacje ≥ 2 Gbps. • SSL inspection (HTTPS) ≥ 2,5 Gbps. |  |
| **5** | **Funkcje bezpieczeństwa (wymagane wszystkie):** | • Stateful Firewall, IPSec VPN, IPS, Antywirus, Kontrola aplikacji, DLP, Antyspam SMTP, DNS filtering, Web Filtering (min. 40 mln URL, kategorie: malware, phishing, proxy, hazard, itp.), SD-WAN, QoS, SSL inspection (HTTP/S, SMTP, POP3, FTP), analiza anomalii i sygnatur (min. 5000). • Możliwość konfiguracji reguł opartych o: IP, aplikację, użytkownika, port, harmonogram, kraj pochodzenia IP. • Translacja NAT: SNAT, DNAT, PAT, 1:1, 1:N, ALG SIP. • Integracja z chmurami: AWS, Azure, GCP, OpenStack, Cisco ACI, NSX, Kubernetes. • Min. 2 tokeny do MFA. |  |
| **6** | **VPN:** | • Obsługa IPSec IKEv1/v2, AES 128/256 GCM, DH gr. 19/20, topologie Hub-Spoke i Mesh, NAT-T, DPD, Xauth, split tunneling, failover tuneli, monitoring stanu tuneli. • Możliwość określenia maksymalnej liczby równoczesnych tuneli. • Obsługa Site-to-Site i Client-to-Site. • VPN klient dostępny (opcja). |  |
| **7** | **Routing:** | • Obsługa: statycznego, PBR, RIPv2/ng, OSPF/v3, BGP, PIM. • ECMP, BFD, monitorowanie dostępności IP z interfejsu. |  |
| **8** | **Zarządzanie pasmem (QoS):** | Możliwość ustawienia limitów gwarantowanych i maksymalnych, DSCP, priorytetów ruchu, dla aplikacji, użytkowników, kategorii URL. |  |
| **9** | **Ochrona przed malware:** | • Skanowanie: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS, w tym na niestandardowych portach. • Obsługa archiwów z limitem zagnieżdżeń i czasu skanowania. • Wykrywanie nieskanowalnych plików (uszkodzone, zaszyfrowane). • Baza sygnatur z ochroną Android, automatyczna aktualizacja. • Integracja z Sandbox (lokalny lub chmurowy – UE). • AI engine producenta. |  |
| **10** | **IPS i ochrona aplikacji:** | • Analiza sygnaturowa i anomalii. • Ochrona na niestandardowych portach. • Własne sygnatury i wyjątki. • Ochrona WebApps (WAF): XSS, SQLi, trojany, C&C. |  |
| **11** | **Kontrola aplikacji:** | • DPI niezależne od portów TCP/UDP. • Min. 2000 sygnatur aplikacji. • Kontrola działań w chmurze (upload/download). • Własne sygnatury, możliwość blokowania port+protokół. |  |
| **12** | **Kontrola WWW:** | • Min. 40 mln URL, z kategoriami tematycznymi (malware, phishing, hazard). • Obsługa Regex, Whitelist/Blacklist, Warning Page, SafeSearch, brak inspekcji dla wybranych kategorii. |  |
| **13** | **Uwierzytelnianie:** | • Lokalna baza, LDAP, RADIUS, RSA SecurID, MFA. • Integracja SSO z AD, SAML, API, SYSLOG. |  |
| **14** | **Zarządzanie:** | •HTTPS, SSH, SNMP v2c/3, NetFlow/sFlow, lokalne i zdalne (centralne) zarządzanie. • Dokumentowane API. • Diagnostyka: ping, traceroute, packet capture, procesy. |  |

***należy podpisać***

***kwalifikowanym podpisem elektronicznym***

***lub podpisem zaufanym lub podpisem osobistym***