## Załącznik nr 2.2 do SWZ

**Nr postępowania: 01/ZP/2024**

**Opis przedmiotu zamówienia**

**Pakiet 2**

## Firewall sprzętowy (UTM) – 1 szt.

**Oferujemy ................................................................... zgodnie z n/w parametrami:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowanego komponentu** |
| 1. | Obudowa | Rack 1U |   |
| 2. | Wymagane moduły/ funkcjonalności | 1. Zapora sieciowa wraz z inspekcją SSL. 2.NAT. 3. VPN IPSec. 4. Routing oraz switching. 5. Ochrona antywirusowa. 6. SSL VPN.7. Możliwość pracy urządzenia w trybie HA |   |
| 3. | Parametry wydajnościowe zapory | 1. Przepustowość Firewall-a (1518/512/64 bajtowe pakiety UDP) - 20/18/10 Gbps2. Opóźnienie Firewall-a (64 bajtowe pakiety UDP) - 4.97 μs3. Przepustowość Firewall-a (Pakiety na sekundę) - 15 Mpps4. Przepustowość IPsec VPN (512 bajtów) - 11.5 Gbps5. Tunele Gateway-to-Gateway IPsec VPN - 2,5006. Przepustowość SSL-VPN - 1 Gbps7. Równoczesna liczba użytkowników SSL-VPN – 5008. Przepustowość Kontroli SSL (IPS, HTTPS) - 1 Gbps9. Przepustowość Kontroli Aplikacji (HTTP 64K) - 2.2 Gbps10. Wirtualne Domeny – 1011. Element Systemu pełniący funkcję Firewall musi dysponowaćprzynajmniej:a) 12 portami 1GbE BaseT,b) 2 portami 10GbE SFP+,c) 4 portami Combo Rj45/SFP. |   |
| 4. | Funkcje modułu Firewall, router i switching | 1. Zapora sieciowa musi posiadać mechanizm inspekcji SSL (sslinspection).2. Zapora sieciowa musi funkcjonować w oparciu o interfejsy, adresy(IP i FQDN), grupy adresów (IP i FQDN), oraz użytkowników.3. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPoE) nazewnętrznym interfejsie.4. Musi umożliwiać pracę jako router i bridge (transpartent mode).5. Musi umożliwiać obsługę translacji adresów: SNAT, DNAT.6. Musi umożliwiać obsługę translacji portów: PAT.7. Musi umożliwiać obsługę VLAN 802.1Q.K2 - Informacja wewnętrzna (Internal)8. Musi zapewniać ochronę przed atakami stosującymi technikiunikania wykrycia, np. fragmentacja pakietów.9. Musi umożliwiać uwierzytelnianie użytkowników orazidentyfikacjęodpowiadającego im ruchu sieciowego.10. Musi umożliwiać transparentne uwierzytelnianie użytkownikówprzy integracji z Active Directory.11. Nie może ograniczać ilość urządzeń, adresów IP czy użytkownikówsieci wewnętrznej.12. Musi umożliwiać sterowanie przepustowością w oparciu onastępujące parametry: użytkownik, grupa użytkowników,protokół, interfejs sieciowy, adres (IP oraz FQDN) i grupa adresów(IP oraz FQDN).13. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-tosite i client-to-site. |   |
| 5. | Wymagane funkcje VPN Systemu | 1. Musi umożliwiać obsługę tuneli: Site-to-Site2. Wsparcie dla algorytmów szyfrowania IKE: AES-GCM, AES256,AES128, 3DES, DES.3. Wsparcie dla algorytmów autentykacji IKE: MD5, SHA-1, SHA-256,SHA-512.4. Rodzaje autentykacji: Preshared key oraz PKI X.509.5. IPsec: wsparcie dla przynajmniej jednego z poniższych:a) Authentication Header (AH)b) Encapsulating Security Payload (ESP)6. Wsparcie dla IKEv1 i IKEv2.7. Urządzenie musi obsługiwać Perfect Forward Secrecy oraz AntiReply (Reply Detection).8. Obsługa Dead Peer Detection (DPD).9. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec oraz SSL VPN. |   |
| 6. | Polityki, Firewall | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcjezabezpieczeń, rejestrowanie zdarzeń.2. Firewall musi zapewniać translację adresów NAT: źródłowego idocelowego, translację PAT oraz:a) Translację jeden do jeden oraz jeden do wielu.b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP.3. W ramach Systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |  |
| 7. | Ochrona antywirusowa | 1. Automatyczna aktualizacja baz sygnatur, nie rzadziej niż co 24 godzin.2. Skanowanie plików skompresowanych: zip, tar, gzip.3. Wsparcie dla głównych protokołów: http, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS |   |
| 8. | Ochrona przed atakami | 1. Automatyczna aktualizację bazy sygnatur IPS.2. Automatyczne blokowanie znanych źródeł ataków.3. Mechanizmy ochrony przed atakami typu DoS i DDoS. |   |
| 9. | Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall musi umożliwiać weryfikację tożsamościużytkowników za pomocą:a) haseł statycznych i definicji użytkowników przechowywanychw lokalnej bazie Systemu.b) haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.c) haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.3. Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innychmechanizmów: RADIUS lub API. |  |
| 10. | Zarządzanie | 1. Elementy Systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH).2. Urządzenie musi posiadać interfejs Ethernet obsługujący połączenia z prędkością minimum 100 Mbit/s - dla zdalnego zarządzania. |  |
| 11. | Wyposażenie dodatkowe | 1. Dołączone 2 moduły SFP+ SR 10Gb/s kompatybilne z urządzeniem.2. Komplet szyn umożliwiających montaż w szafie rack |   |
| 12. | Zasilanie | Dołączone dwa redundantne zasilacze AC 230V |  |
| 13. | Licencje | Urządzenie musi być dostarczone wraz z licencjami/subskrypcjami na okres 36 miesięcy upoważniające do korzystania z aktualnych bazfunkcji ochronnych producenta i serwisów.Jeżeli którakolwiek opisana powyżej funkcjonalność wymaga dodatkowych licencji i/lub subskrypcji to należy je dostarczyć wraz zurządzeniem. |  |
| 14. | Gwarancja | 1. Długość gwarancji 36 miesięcy.2. Gwarancja i serwis realizowany w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęciazgłoszenia, możliwość zgłaszania awarii poprzez ~~ogólnopolską~~ linię telefoniczną producenta lub dedykowany i zabezpieczony kanałkomunikacji elektronicznej.3. Producent musi umożliwiać skuteczne zgłaszanie awarii w trybie 24x7x365 poprzez ~~ogólnopolską~~ linię telefoniczną producenta(ogólnie dostępna linia telefoniczna producenta, preferowany kontakt w językuPolskim lub angielskim, ~~linia telefoniczna w polskiej strefie numeracyjnej - telefon~~~~stacjonarny.~~ Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.) oraz systemK2 - Informacja wewnętrzna (Internal)zgłoszeniowy producenta.4. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej infrastruktury oraz warunków gwarancji po podaniu numeruseryjnego bezpośrednio u producenta lub jego przedstawiciela.5. Gwarancja i serwis producenta z czasem reakcji na zgłoszenia usterki w następnym dniu roboczym ~~producenta realizowany w trybie 8x5 NBD Onsite Response Time lub równoważnym tj. następny dzień roboczy.~~6. Dyski twarde naprawianego urządzenia pozostają w siedzibieZamawiającego.7. Zakres wsparcia technicznego producenta:a) dostęp do pomocy technicznej;b) dostęp do poprawek i nowych wersji oprogramowania i/lubSystemu;c) dostęp do dokumentacji technicznej;d) dostęp do konta wsparcia urządzenia, zawierającego dostępdo bazy wiedzy oraz systemu zgłoszeń producenta |  |

Opis przedmiotu zamówienia musi być wypełniony i podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.