Szczegółowy Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest:

1) Zakup i dostawa urządzeń typu firewall wraz z oprogramowaniem – 2 szt. (dalej jako „System")

Lp.	Cecha	Wymagane minimalne parametry techniczne
1.	Wymagania ogólne	1. Urządzenie musi być w obudowie RACK o wysokości maksymalnie 1U. 2. Obudowa urządzenia musi być wykonana z metalu. Ze względu na różne warunki, w których pracować będzie urządzenie, nie dopuszcza się urządzenia w obudowie plastikowej. 3. Urządzenie musi posiadać na obudowie kontrolki lub wyświetlacz LCD informujący o statusie urządzenia, parametrach systemu oraz alarmach.
2.	Wymagania HA	1. Możliwość pracy urządzenia w trybie HA 2. Obsługiwane tryby pracy dla klastra HA: a) active/passive b) active/active
3.	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.
4.	Parametry wydajnościowe zapory	1. Firewall musi obsługiwać 3 miliony jednoczesnych połączeń oraz przyjmować nowe połączenia z wydajnością minimalną 280 tysięcy nowych połączeń na sekundę. 2. Obsługa co najmniej 3000 sieci VLAN. 3. Element Systemu pełniący funkcję Firewall musi dysponować przynajmniej: a) 16 portami 1GbE BaseT, b) 4 portami 10GbE SFP+, c) 8 portami 1GbE SFP. 4. Obsługa nie mniej niż: 2 000 tuneli IPSec site-to-site. 5. Obsługa nie mniej niż: 16 000 tuneli client-to-site. 6. Obsługa nie mniej niż: 10 000 reguł firewall. 7. Przepustowość Stateful Firewall: nie mniej niż 16 Gbps. 8. Wydajność szyfrowania IPSec VPN: nie mniej niż 13 Gbps.
5.	Funkcje modułu Firewall, router i switching	1. Zapora sieciowa musi posiadać mechanizm inspekcji SSL (ssl inspection). 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) na zewnętrznym 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.

		8. Musi zapewniać ochronę przed atakami stosującymi techniki unikania wykrycia, np. fragmentacja pakietów. 9. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego. 10. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory. 11. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej. 12. Musi umożliwiać sterowanie przepustowością w oparciu o następujące 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-to-site i client-to-site.
6.	Wymagane funkcje VPN Systemu	1. Musi umożliwiać obsługę tuneli: Site-to-Site 2. 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 Anti Reply (Reply Detection). 8. Obsługa Dead Peer Detection (DPD). 9. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec oraz SSL VPN. 10. Możliwość jednoczesnego podłączenia przynajmniej 500 klientów poprzez SSL VPN. Zamawiający nie akceptuje limitowania klientów dla tej formy polaczenia zdalnego (lub dostarczenia minimum 1200 licencji na takie połączenia).
7.	Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. Firewall musi zapewniać translację adresów NAT: źródłowego i docelowego, 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.
8.	Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie musi zapewniać obsługę: a) Routingu statycznego. b) Policy Based Routingu. c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. Firewall musi umożliwiać obsługę kilku (co najmniej dwóch) łączy

		WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. 3. Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
9.	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.
10.	Ochrona przed atakami	1. Automatyczna aktualizację bazy sygnatur IPS. 2. Automatyczne blokowanie znanych źródeł ataków. 3. Mechanizmy ochrony przed atakami typu DoS i DDoS.
11.	Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: a) haseł statycznych i definicji użytkowników przechowywanych w 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 innych mechanizmów: RADIUS lub API.
12.	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.
13.	Wyposażenie dodatkowe	1. Dołączone 4 moduły SFP+ SR 10Gb/s kompatybilne z urządzeniem. 2. Komplet szyn umożliwiających montaż w szafie rack 3. Urządzenie musi być dostarczone z kompletem kabli umożliwiającym podłączenie urządzenia w klaster HA
14.	Zasilanie	Dołączone dwa redundantne zasilacze AC 230 V
15.	Gwarancja, serwis i wsparcie techniczne producenta	1. Długość gwarancji 36 miesięcy. 2. Gwarancja i serwis realizowany w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany i zabezpieczony kanał komunikacji elektronicznej. 3. Producent musi umożliwiać skuteczne zgłaszanie awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.) oraz system

		zgłoszeniowy producenta. 4. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej infrastruktury oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. 5. Gwarancja i serwis producenta realizowany w trybie 8x5 NBD Onsite Response Time. 6. Dyski twarde naprawianego urządzenia pozostają w siedzibie Zamawiającego. 7. Zakres wsparcia technicznego producenta: a) dostęp do pomocy technicznej; b) dostęp do poprawek i nowych wersji oprogramowania i/lub Systemu; c) dostęp do dokumentacji technicznej; d) dostęp do konta wsparcia urządzenia, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta.
16.	Dokumentacja	Dokumentacja urządzenia w języku polskim lub angielskim, dostępna na stronie producenta.
17.	Licencje	Urządzenie musi być dostarczone wraz z licencjami/subskrypcjami na okres 36 miesięcy upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Jeżeli którakolwiek opisana powyżej funkcjonalność wymaga dodatkowych licencji i/lub subskrypcji to należy je dostarczyć wraz z urządzeniem.
18.	Uwagi	Urządzenie musi być kompatybilne z posiadanym przez zamawiającego systemem FortiAnalyzer. Z uwagi na posiadane przez Zamawiającego urządzenia Fortinet AccessPoint FAP-221E, zaoferowane rozwiązanie musi posiadać pełną funkcjonalność zarządzania wymienionymi urządzeniami.

2) zapewnienie w ramach prawa opcji usługi wsparcia w konfiguracji i administrowaniu Systemem, w wymiarze 20 roboczogodzin z możliwością wykorzystania przez okres 36 miesięcy od dnia odbioru Systemu lub do wykorzystania ww. puli roboczogodzin świadczonych usług. Do realizacji usługi wsparcia Wykonawca skieruje minimum 2 osoby posiadające aktualny certyfikat autoryzowany przez producenta Systemu, potwierdzający zaawansowaną wiedzę z Systemu.
   Usługa wsparcia Wykonawcy obejmuje w szczególności:
   a) gotowość serwisową oznaczającą podjęcie działań naprawczych w terminie maksymalnie 6 godzin od chwili zgłoszenia, przy czym Zamawiający może dokonywać zgłoszeń w dni robocze w godzinach 8-17,
   b) w przypadku awarii urządzenia – zgłoszenie awarii producentowi, koordynacja zgłoszenia poprzez monitorowanie i posiadanie aktualnych informacji o statusie zgłoszenia oraz miejscu przebywania urządzenia na wymianę, jeżeli takie jest przewidziane. Konfiguracja urządzenia wymienianego w celu uzyskania funkcjonalności urządzenia uszkodzonego,

c) usuwanie usterek, prace rekonfiguracyjne, diagnostycznie, projektowe, usługi konsultacyjne w zakresie funkcjonalności, eksploatacji i administrowania systemami, aktualizacja dokumentacji i inne zlecane przez Zamawiającego, mające na celu zapewnienie prawidłowego funkcjonowania sieci Zamawiającego,

d) wsparcie będzie świadczone zgodnie z zapotrzebowaniem zgłaszanym przez Zamawiającego w formie mailowej lub telefonicznej, albo w miejscu wskazanym przez Zamawiającego wedle wyboru Zamawiającego w terminach wskazanych przez Zamawiającego.