Załącznik 1 – Szczegółowy opis przedmiotu zamówienia do zapytania z dnia 4.11.2022 r. na dostawę oprogramowania wirtualnego firewall-a

Specyfikacja na wirtualny firewall w postaci licencji (subskrypcji) na klaster wysokiej dostępności HA (System Firewall)		
	Opis	**Wartość wymagana**
Parametry wydajnościowe dotyczące Systemu Firewall	1. System Firewall będzie pracował w trybie HA (2 sztuki). 2. System Firewall musi wspierać następujące rozwiązania „hypervisor": AWS, Azure, ESXi, GCP, Hyper-V, KVM, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, Cisco ENCS, NSX-T. 3. System Firewall będzie użytkowany na łącznie 8 vCPU (4 vCPU per NOD klastra). 4. System Firewall musi spełniać co najmniej następujące parametry wydajnościowe: a. Minimum 2,9 Gbps dla rozpoznawania i kontroli aplikacji, b. Minimum 1,4 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Anty-wirus, Anty-spyware, blokowanie typów plików, z włączonym logowaniem na dysk maszyny wirtualnej, c. Minimum 13 000 nowych sesji na sekundę, d. Minimum 230 000 równoległych sesji. 5. System Firewall musi obsługiwać nie mniej niż 3 wirtualne routery posiadające odrębne tabele routingu. 6. System Firewall musi umożliwiać zdefiniowanie nie mniej niż 1400 reguł polityki bezpieczeństwa.	TAK
Wymagania funkcjonalne dotyczące Systemu Firewall	1. Muszą to być specjalizowane maszyny wirtualne mogące pracować jako pojedynczy system oraz jako klaster wysokiej dostępności (HA) w trybach Active/Standby, Active/Active. 2. Całość oprogramowania musi być dostarczona i wspierana przez jednego producenta. Producent oferowanego rozwiązania musi być obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders przynajmniej od 5 lat. 3. System Firewall musi umożliwiać działanie w następujących trybach pracy: a. rutera (tzn. w warstwie 3 modelu OSI), b. mostu (tzn. w warstwie 2 modelu OSI), c. w trybie transparentnym (system nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych i musi pracować w trybie przezroczystego łączenia interfejsów w pary), d. w trybie pasywnego nasłuchu (sniffer/tap). 4. System Firewall musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu. 5. System Firewall musi posiadać separację logiczną zasobów służących do przetwarzania ruchu od zasobów służących do zarządzania systemem. 6. System Firewall musi posiadać dedykowane zasoby do funkcji zarządzania systemem lub możliwość ustawienia dedykowanego procesora do funkcji zarządzania systemem. 7. System Firewall musi wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Podinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. System Firewall musi obsługiwać 4000 znaczników VLAN. 8. System Firewall musi zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7). 9. System Firewall musi działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. System Firewall musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone. 10. Polityka zabezpieczeń firewall musi uwzględniać	

	a. adresy IP źródłowe i docelowe, b. protokoły i usługi sieciowe, c. aplikacje, d. kategorie URL, e. użytkowników aplikacji i grupy, f. reakcje zabezpieczeń, g. logowanie zdarzeń (początek i koniec sesji), h. strefa wejściowa i wyjściowa. 11. System Firewall musi automatycznie identyfikować aplikacje bez względu na numery portów (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. System Firewall musi wykrywać co najmniej 3300 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. Musi też pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI Systemu Firewall (bez użycia zewnętrznych narzędzi). 12. System Firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku. 13. System Firewall musi być zarządzany z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania Systemem. 14. System Firewall musi być wyposażony w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu maszyny wirtualnej bez użycia konsoli zarządzania lub linii poleceń (CLI). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy dostarczyć odpowiednie dla minimum 30 administratorów. 15. Dostęp do systemu i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. 16. System Firewall musi umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż: baza lokalna, serwer Radius, serwer TACACS+, serwer AD/LDAP. Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH a dla dostępu GUI za pomocą certyfikatów kryptograficznych. 17. System Firewall musi zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami: a. Active Directory, b. Terminal Services. 18. Polityka kontroli dostępu Systemu Firewall musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości musi odbywać się również transparentnie. 19. System Firewall musi pozwalać na lokalne zbieranie (na dysk maszyny wirtualnej) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL. 20. System Firewall musi umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. W systemie musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu. 21. System Firewall musi umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach, a proces oznaczania etykiet musi pozwalać na użycie: a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia), b. API.	

	22. System Firewall musi posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMware ESX i VMware vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można potem wykorzystywać w polityce bezpieczeństwa systemu. 23. System Firewall musi obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF dla IPv4 i IPv6. 24. System Firewall musi obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. 25. System Firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa. 26. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami NAT. 27. System Firewall musi pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju. 28. System Firewall musi obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3. 29. System Firewall musi posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa. 30. Wykonywanie operacji deszyfrowanie ruchu musi być odnotowywane w logach systemu w dedykowanej do tego celu sekcji. Musi zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu. 31. Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL. 32. Dla deszyfrowania ruchu TLS 1.3 wymagane jest wsparcie dla X25519, X448 oraz minimum dla zestawów protokołów: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384 oraz TLS_CHACHA20_POLY1305_SHA256. 33.System Firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. 34. System Firewall musi wspierać zarządzanie pasmem (QoS) i ustawiania dla aplikacji priorytetu oraz pasma. 35. System Firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. routing-based VPN). 36. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20. 37. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20. 38. System Firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tuneli SSH. 39. System Firewall musi posiadać funkcję filtrowania URL. 40. Funkcja filtrowania URL musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. 41. System Firewall musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „SandBox" plików wykonywalnych PE i DLL przechodzących przez firewall. Systemy sandbox, na podstawie przeprowadzonej analizy, muszą aktualizować System Firewall sygnaturami nowo wykrytych złośliwych plików, adresów IP, DNS i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik. Maksymalny interwał aktualizacji sygnatur 48 godzin. 42. System Firewall musi realizować ochronę DNS w zakresie: a. wykrywania zapytań do domen złośliwych (baza domen musi mieć co najmniej 10 milionów wpisów),	

	b. możliwości skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing), c. wykrywania domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA), d. wykrywanie domen dynamicznych Dynamic DNS, e. wykrywania nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych. 43. System Firewall musi obsługiwać funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta musi być realizowana na bazie technologii SSL VPN oraz IPSec. 44. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników. 45. Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows, MacOS, Android i iOS. 46. Jeżeli oprogramowanie klienta Remote Access VPN dla laptopów z systemem Windows wymaga licencji – należy dostarczyć licencję na maksymalną wydajność oraz maksymalną ilość dla oferowanego typu systemu firewall. 47. Oprogramowanie klienta VPN dla Windows i macOS musi posiadać możliwość weryfikacji kondycji bezpieczeństwa stacji końcowej co najmniej w zakresie sprawdzenia: a. czy zainstalowano oprogramowanie antywirusowe i czy posiada ono aktualne sygnatury, b. czy włączony jest osobisty firewall, c. czy włączone jest szyfrowanie dysku. 48. System Firewall musi posiadać funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (Machine Learning - ML) aktualizowanych dynamicznie przez producenta. 49. Wykrywanie za pomocą algorytmów musi odbywać się lokalnie w systemie jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antywirus oraz funkcji filtrowania URL. 50. Wymagane jest posiadanie funkcji wykrywania za pomocą ML (Machine Learning) dla następujących danych: złośliwych plików wykonywalnych (tzw. PE), złośliwych skryptów PowerShell, złośliwych stron / ataków Phishing, złośliwych skryptów JavaScript. 51. Dodatkowo rozwiązanie musi posiadać możliwość analizy, identyfikacji oraz blokowania wcześniej nieznanej komunikacji C2 (command-and-control) oraz spyware w oparciu o nauczanie maszynowe realizowane w chmurze producenta, przy czym: a. wymagana analiza i detekcja musi umożliwiać blokowanie wykrytej komunikacji C2 w czasie rzeczywistym, b. analiza i wykrywanie nieopisanych wcześniej w sygnaturach połączeń C2 muszą być możliwe minimum dla ruchu typu: http, http2, ssl oraz niezidentyfikowanych przez firewall aplikacji w oparciu o TCP i UDP. 52. W przypadku gdy jakakolwiek funkcjonalność lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres 36 miesięcy od daty odbioru. 53. Wsparcie serwisowe (techniczne) i gwarancja dla Systemu Firewall będzie świadczone przez producenta lub autoryzowane przez producenta centrum serwisowe lub Wykonawcę, realizowane we współpracy z producentem, przez okres 36 miesięcy od daty odbioru. 54. Zamawiający wymaga dostarczenia licencji w postaci subskrypcji na okres 36 miesięcy.	