OPIS PRZEDMIOTU ZAMÓWIENIA I PARAMETRY TECHNICZNE

# Informacje ogólne

Przedmiotem zamówienia jest dostawa, wdrożenie migracja i uruchomienie w środowisku DataCenter klastra wysokiej dostępności (HA) 2 urządzeń klasy Next‑Generation Firewall (NGFW) wraz z pakietem zaawansowanych funkcji bezpieczeństwa (UTM), licencjami/subskrypcjami oraz wsparciem producenta, a także usługami projektowymi, wdrożeniowymi i szkoleniowymi.

Dodatkowo wymagana jest dostawa, wdrożenie i uruchomienie systemu centralnego zarządzania urządzeniami bezpieczeństwa sieci (dalej: „System Zarządzania”) umożliwiającego jednolite zarządzanie konfiguracją, politykami i cyklem życia (w tym aktualizacjami) dla infrastruktury dostarczanych urządzeń NGFW do Zamawiającego.

|  |  |  |
| --- | --- | --- |
| Zakres ilościowy | paRAMETR wYMAGANY | oDPOWIEDŹ OFERENTA |
| Dostawa 2 szt. urządzeń firewall przeznaczonych i skonfigurowanych do pracy w klastrze HA (redundancja/ nadmiarowość na poziomie sprzętowym). | TAK |  |
| System Zarządzania może być dostarczony jako:   * + rozwiązanie wirtualne (VM) uruchamiane w środowisku wirtualizacyjnym Zamawiającego lub   + urządzenie sprzętowe (appliance) lub równoważne. | TAK  TAK |  |
| Wymagania techniczne (minimalne) |  |  |
| Interfejsy:   * + - min. 16× 1GbE RJ45     - min. 4× 10GbE SFP+     - min. 8 × 1 GbE SFP | TAK |  |
| Porty dedykowane: osobne interfejsy dla zarządzania oraz dla komunikacji HA (heartbeat) – min. po 1 na funkcję (odseparowane od portów danych). | TAK |  |
| Zasilanie: redundantne zasilacze AC (dual PSU) w każdym urządzeniu. | TAK |  |
| Montaż: przystosowanie do instalacji w szafie 19” (akcesoria montażowe w komplecie). | TAK |  |
| Funkcje sieciowe: firewall L3/L4, NAT, VLAN 802.1Q, routing (statyczny i dynamiczny, jeśli wymagany), IPsec VPN (jeśli dotyczy), logowanie i eksport logów (np. syslog). | TAK |  |
| Oprogramowanie: wersja wspierana przez producenta w całym okresie wsparcia. | TAK |  |
| W zakresie Firewall’a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę. | TAK |  |
| Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B. | TAK |  |
| Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. | TAK |  |
| Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 33 Gbps. | TAK |  |
| Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) - minimum 5 Gbps. | TAK |  |
| Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.5 Gbps. | TAK |  |
| Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps. | TAK |  |
| Wysoka dostępność i redundancja |  |  |
| Praca w klastrze HA min. Active‑Passive z automatycznym przełączeniem w przypadku awarii. | TAK |  |
| Co najmniej dwa niezależne połączenia heartbeat (podstawowe i zapasowe). | TAK |  |
| Synchronizacja konfiguracji oraz (jeżeli wspierane) stanów sesji pomiędzy węzłami klastra. | TAK |  |
| Rozwiązanie ma eliminować pojedynczy punkt awarii w warstwie firewall (2 urządzenia, każde z podwójnymi zasilaczami (PSU), redundancja łączy). | TAK |  |
| Funkcje Systemu Bezpieczeństwa: |  |  |
| Kontrola Aplikacji | TAK |  |
| Poufność transmisji danych - połączenia szyfrowane IPSec VPN | TAK |  |
| Ochrona przed malware. | TAK |  |
| Ochrona przed atakami - Intrusion Prevention System. | TAK |  |
| Kontrola stron WWW. | TAK |  |
| Kontrola zawartości poczty – Antyspam dla protokołów SMTP. | TAK |  |
| Zarządzanie pasmem (QoS, Traffic shaping). | TAK |  |
| Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP) | TAK |  |
| Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site | TAK |  |
| Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3 | TAK |  |
| Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system | TAK |  |
| Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). | TAK |  |
| Routing i obsługa łączy WAN |  |  |
| W zakresie routingu rozwiązanie zapewnia obsługę:   1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. | TAK |  |
| Połączenia VPN |  |  |
| System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: | TAK |  |
| * Wsparcie dla IKE v1 oraz v2. | TAK |  |
| * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). | TAK |  |
| * Obsługa protokołu Diffie-Hellman grup 19, 20. | TAK |  |
| * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. | TAK |  |
| * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. | TAK |  |
| * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. | TAK |  |
| * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. | TAK |  |
| * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. | TAK |  |
| * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. | TAK |  |
| * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. | TAK |  |
| * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. | TAK |  |
| * Mechanizm „Split tunneling” dla połączeń Client-to-Site. | TAK |  |
| Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. | TAK |  |
| Funkcje SD-WAN |  |  |
| System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. | TAK |  |
| SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). | TAK |  |
| Zarządzanie pasmem |  |  |
| System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. | TAK |  |
| System daje możliwość określania pasma dla poszczególnych aplikacji. | TAK |  |
| System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. | TAK |  |
| System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. | TAK |  |
| Ochrona przed malware |  |  |
| Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). | TAK |  |
| Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. | TAK |  |
| W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. | TAK |  |
| System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. | TAK |  |
| System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). | TAK |  |
| Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. | TAK |  |
| System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. | TAK |  |
| System zapewnia usuwanie aktywnej zawartości plików Microsoft Office bez konieczności blokowania transferu całych plików. | TAK |  |
| Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. | TAK |  |
| Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. | TAK |  |
|  | TAK |  |
| Ochrona przed atakami |  |  |
| 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. | TAK |  |
| 1. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. | TAK |  |
| 1. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. | TAK |  |
| 1. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. | TAK |  |
| 1. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. | TAK |  |
| 1. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). | TAK |  |
| 1. Możliwość kontrolowania długości nagłówka, ilości parametrów URL dla protokołu http. | TAK |  |
| 1. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. | TAK |  |
| 1. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. | TAK |  |
| Kontrola aplikacji |  |  |
| 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. | TAK |  |
| 1. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. | TAK |  |
| 1. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. | TAK |  |
| 1. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. | TAK |  |
| 1. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. | TAK |  |
| 1. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). | TAK |  |
| 1. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). | TAK |  |
| Kontrola WWW |  |  |
| 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. | TAK |  |
| 1. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. | TAK |  |
| 1. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. | TAK |  |
| 1. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. | TAK |  |
| 1. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). | TAK |  |
| 1. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. | TAK |  |
| 1. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. | TAK |  |
| 1. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. | TAK |  |
| 1. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. | TAK |  |
| Uwierzytelnianie użytkowników w ramach sesji |  |  |
| System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:   * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. | TAK |  |
| System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. | TAK |  |
| System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. | TAK |  |
| Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. | TAK |  |
| Logowanie |  |  |
| Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. | TAK |  |
| W ramach logowaia element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania | TAK |  |
| Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. | TAK |  |
| Możliwość włączenia logowania per reguła w polityce firewall. | TAK |  |
| System zapewnia możliwość logowania do serwera SYSLOG. | TAK |  |
| Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. | TAK |  |
| Gwarancja i wsparcie producenta |  |  |
| Wymagane jest zapewnienie wsparcia producenta i objęcie urządzeń serwisem gwarancyjnym przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego uszkodzenia (wykrycia wady). W ramach tego serwisu producent zapewni dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię. | Poniżej 24 miesięcy – 0 pkt.  24 miesiące – 5 pkt.  25-36 miesiące – 10 pkt.  36- 60 miesięcy – 15 pkt |  |
| Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen. | Poniżej 24 miesięcy – 0 pkt.  24 miesiące – 5 pkt.  25-36 miesiące – 10 pkt.  36- 60 miesięcy – 15 pkt |  |
| Usługi projektowe |  |  |
| 1. Wykonawca przygotuje i uzgodni z zamawiającym dokumentację projektową (HLD/LLD) zawierającą co najmniej:  * Schematy logiczne, adresację, VLAN, routing, strefy bezpieczeństwa i zasady segmentacji. * Macierz reguł/polityk (rulebase) oraz zasady NAT/VPN (jeśli dotyczy). * Plan wdrożenia, plan migracji, plan testów i plan wycofania (rollback). | TAK |  |
| Usługi wdrożeniowe |  |  |
| Wykonawca wykona co najmniej:   * Montaż w szafie RACK w DataCenter i uruchomienie połączeń HA oraz uplinków. * Konfigurację: interfejsy, VLAN/routing, polityki bezpieczeństwa, NAT, VPN (jeśli dotyczy), konta/role administracyjne. * Uruchomienie HA * Integrację logów z istniejącym środowiskiem (syslog/SIEM). * Wykonanie kopii konfiguracji i przekazanie procedur backup/restore. * Podłączenie do dostarczonego Systemu Zarządzania urządzeniami Firewall | TAK |  |
| Usługi migracyjne |  |  |
| Migracja konfiguracji z obecnego rozwiązania, obejmująca co najmniej: obiekty, reguły, NAT, routing, VPN (jeśli dotyczy), listy wyjątków. | TAK |  |
| Weryfikacja spójności i uporządkowanie reguł (m.in. eliminacja duplikatów) oraz uruchomienie w uzgodnionym oknie serwisowym. | TAK |  |
| Zapewnienie planu rollback umożliwiającego powrót do stanu sprzed migracji. | TAK |  |
| Testy, odbiór i dokumentacja |  |  |
| Testy funkcjonalne oraz testy HA (symulacja awarii węzła, przełączenie, powrót). | TAK |  |
| Protokół odbioru. | TAK |  |
| Dokumentacja powdrożeniowa: schematy, opis HA, zestaw reguł, procedury eksploatacyjne i awaryjne. | TAK |  |
| Uruchomienie Systemu Zarządzania oraz (w ramach odbioru) testy:   * Dodanie i autoryzacja co najmniej 2 urządzeń (lub wszystkich dostępnych, nie więcej niż 10). * Wdrożenie przykładowej zmiany konfiguracyjnej z Systemu Zarządzania na wskazane urządzenie i potwierdzenie jej zastosowania. * Weryfikacja działania uprawnień (co najmniej 2 role) oraz rejestrowania operacji administracyjnych. Wykonawca dostarczy dokumentację powdrożeniową obejmującą minimum: opis architektury, instrukcję dodawania urządzeń, procedurę wykonywania zmian i procedurę aktualizacji. * Testy działania HA | TAK |  |
| Szkolenie |  |  |
| Szkolenie administracyjne dla wskazanych osób obejmujące zarządzanie politykami, diagnostykę, logi, obsługę HA, kopie konfiguracji, aktualizacje i podstawowe dobre praktyki. | TAK |  |
| Warunki równoważności |  |  |
| Dopuszcza się rozwiązania równoważne, pod warunkiem spełnienia wszystkich minimalnych wymagań określonych powyżej; wykonawca musi wykazać równoważność dokumentacją producenta (karty katalogowe/opisy funkcji/licencji) oraz potwierdzić 5‑letni okres wsparcia i subskrypcji UTM. | TAK |  |
| Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni. | TAK |  |