Załącznik nr 1 do SWZ – SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – SPECYFIKACJA TECHNICZNA

**Dostawa systemu zabezpieczeń ruchu sieciowego dla Biblioteki Uniwersyteckiej w Warszawie.**

|  |  |
| --- | --- |
| **Wymagania ogólne dla systemu zabezpieczeń ruchu sieciowego** | |
|  | Przedmiotem zamówienia jest dostawa systemu zabezpieczeń ruchu sieciowego w postaci rozwiązań Next Generation Firewall (NGFW) w postaci dwóch maszyn wirtualnych w konfiguracji HA. |
|  | Dostarczone rozwiązanie musi być zgodne ze środowiskiem wirtualizacji VMware ESXi 6.7 i nowszym. |
|  | Całościowy system bezpieczeństwa musi być zrealizowany poprzez dwa wirtualne firewalle. Zamawiający dopuszcza realizację systemu bezpieczeństwa tylko jako dwa firewalle połączone w klaster wysokiej dostępności (HA). |
|  | Zamawiający wymaga, aby zaoferowane firewalle były dostępne i serwisowane przez Producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne). |
| **Wymagania dotyczące funkcjonalności zabezpieczeń:** | |
|  | Każdy z interfejsów musi mieć możliwość pracy w co najmniej następujących trybach: L2 (bridge), L3 (router), TAP (pasywny sniffer ruchu) oraz tryb transparentny. Działając w trybie transparentnym firewall nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne lub rozgłoszeniowe. Tryb transparentny musi umożliwiać analizę i filtrowanie przepuszczanego ruchu. Tryb pracy zabezpieczeń musi być ustalany w konfiguracji per interfejs. Musi istnieć możliwość jednoczesnej konfiguracji i pracy poszczególnych interfejsów sieciowych w różnych trybach |
|  | Firewall musi umożliwiać realizację zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji. |
|  | Reguły zabezpieczeń firewalla muszą uwzględniać co najmniej: strefy bezpieczeństwa, adresy IP źródłowe i docelowe, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (co najmniej: priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ). |
|  | Firewall musi umożliwiać identyfikację co najmniej 3000 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS, np.: Gada-Gadu, Tor, BitTorrent, eMule, Facebook, Youtube, SAP, Zoom, Google Meet, Google Classroom, Skype, Microsoft Update, Microsoft Samba v1/v2/v3, Microsoft Remote Desktop. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall. |
|  | Firewall musi umożliwiać ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |
|  | Firewall musi umożliwiać zarządzanie, kontrolę i wgląd w ruch nierozpoznany przez polityki identyfikacji. |
|  | Firewall musi umożliwiać identyfikowanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z Peer to Peer-P2P i IM-Instant Messaging). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. |
|  | Firewall musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach. Polityki definiujące powinny umożliwiać wykorzystanie: adresów źródłowych, adresów docelowych, użytkowników, numerów portów usług, kategorie URL. System musi obsługiwać co najmniej następujące mechanizmy uwierzytelnienia RADIUS lub TACACS+, LDAP, SAML 2.0. |
|  | Możliwość rozbudowy (wyłącznie w oparciu o zakup licencji) o funkcjonalność analizy plików wykonywalnych (exe, dll) przechodzących przez firewall współpracując z zewnętrznym systemem utrzymywanym przez producenta w Internecie, który instaluje i uruchamia przesłane pliki w wirtualnym środowisku oraz sprawdza czy dany plik nie zachowuje się w złośliwy sposób (np. kasuje lub zaraża inne pliki, zmienia ustawienia komputera, nawiązuje komunikację zwrotną, otwiera porty, zmienia ustawienia usług systemowych, itp). System zewnętrzny, na podstawie przeprowadzonej analizy, musi aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. |
|  | Możliwość rozbudowy (wyłącznie w oparciu o zakup licencji) o funkcjonalności: filtrowania stron WWW (WWW/URL Filtering) w zależności od predefiniowanych kategorii, IDS/IPS, AntiSpyware, AntiVirus, DLP per reguła polityki bezpieczeństwa. Nie jest dopuszczalne, aby ww. modułów uruchamiane były per firewall lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). Bazy sygnatur ww. modułów muszą być przechowywane na urządzeniu, regularnie aktualizowane w sposób automatyczny, być w pełni kompatybilne z firewallem i posiadać nie mniej niż 200 milionów rekordów URL. |
|  | Możliwość rozbudowy (wyłącznie w oparciu o zakup licencji) o funkcjonalność wykrywania i blokowania ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole). |
|  | Firewall musi umożliwiać wykrywanie sieci Botnet na podstawie analizy behawioralnej oraz ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. |
|  | Firewall musi umożliwiać inspekcję komunikacji szyfrowanej (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3) dla ruchu wychodzącego i przychodzącego. Firewall musi umożliwiać deszyfrację wskazanego ruchu HTTPS (szyfrowanego 3DES, AES (128-bit, 192-bit, 256-bit)) i poddania go właściwej inspekcji nie mniej niż: identyfikacja aplikacji, wykrywanie i blokowanie ataków typu exploit (Intrusion Prevention - IPS), wirusy i inny złośliwy kod (AntiVirus i AntiSpyware). |
|  | Firewall musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH. |
|  | Firewall musi zapewnić funkcjonalność inspekcji ruchu modułami IDS/IPS, AntiSpyware, AntiVirus, DLP bez konieczności dokupowania jakichkolwiek dodatkowych komponentów. Bazy sygnatur muszą być przechowywane na urządzeniu, regularnie aktualizowane w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduły inspekcji muszą być uruchamiane niezależnie per reguła polityki bezpieczeństwa. Nie jest dopuszczalne, aby moduły uruchamiane były per cały firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). |
|  | Firewall musi umożliwiać transparentnie ustalenie tożsamość użytkowników sieci (integracja z Active Directory, Citrix, LDAP i serwerami Terminal Services, syslog). Reguły zabezpieczeń firewalla precyzyjnie definiują prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. |
|  | Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów programowych firewall oraz łączy sieciowych. |
|  | Wsparcie dla standardu 802.1q. Obsługa pełnego zakresu tagów od 1 do 4094 per interfejs. Obsługa pełnego zakresu tagów od 1 do 4094 per urządzenie (lub instancja). |
|  | Wsparcie dla protokołów routingu OSPFv2/v3, BGP, RIP oraz dla Policy Based Routing (PBR). |
|  | Wsparcie dla protokołów multicastowych: PIM-SM, PIM-SSM, IGMP v1, v2, v3 |
|  | Wsparcie dla mechanizmów NAT i PAT (Source i Destination NAT i PAT) dla protokołu IPv4, NAT64, możliwość rezerwowania dynamicznych i statycznych zakresów IP. |
|  | Obsługa standardów wymiany klucza: Manual key, IKE v1 i v2.Obsługa standardów szyfrowania 3DES, AES (128-bit, 192-bit, 256-bit). Obsługa standardów uwierzytelniania: MD5, SHA-1, SHA-256, SHA-384, SHA-512. |
|  | Firewall musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. |
|  | Producent firewalla musi zapewniać dostęp do aplikacji klienckiej VPN kompatybilnej z urządzeniami z systemem Windows, MacOS, Linux oraz urządzeniami mobilnymi iOS, Android. |
|  | Firewall musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. |
|  | Zarządzanie musi odbywać się z linii poleceń (CLI), konsoli Web GUI dostępnej przez przeglądarkę WWW oraz przez SSH. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania firewallem. |
|  | I.C.10 Firewall musi umożliwiać zdefiniowanie wielu administratorów o różnych uprawnieniach. Firewall musi umożliwiać uwierzytelnianie administratorów za pomocą:   * bazy lokalnej, * serwera LDAP, * RADIUS lub TACACS+ * 4. SAML 2.0 |
|  | Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS) |
|  | Firewall musi umożliwiać edycję konfiguracji na urządzeniu bez jej jednoczesnego aplikowania (aplikowanie konfiguracji na żądanie). Zmiany konfiguracji wprowadzone przez administratora w panelu zarządzania (CLI lub GUI) nie będą aplikowane na urządzeniu w momencie dokonywania zmiany, a dopiero po zleceniu ich aplikacji. Administrator musi mieć możliwość: podglądu jakie zmiany zostaną wprowadzone, wycofania zmian, zapisania zmian oraz aplikacji zmian w zaplanowanym czasie. |
|  | Firewall musi umożliwiać porównania bieżącej konfiguracji (wskazania różnic) z co najmniej 20 wcześniejszymi konfiguracjami. |
|  | Firewall musi zapewniać interfejs API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Firewall musi wspierać co najmniej jeden z wymienionych standardów API: JSON, REST, XML. |
|  | Firewall musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG. |
|  | Firewall nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej |
|  | Licencje muszą zostać aktywowane przez zamawiającego, a nie automatycznie w momencie zakupu urządzenia. Czas trwania licencji musi być liczony od momentu aktywacji. |
|  | Firewall musi być objęty minimum 3-letnim wsparciem obejmującym:   * dostęp do aktualnych wersji oprogramowania, * realizacja zgłoszeń serwisowych w trybie 24x7, * realizację zgłoszeń gwarancyjnych w trybie 24x7, * wsparcie techniczne realizowane telefonicznie, mailowo oraz za pośrednictwem portalu www, * aktualizację silników i baz sygnatur modułów bezpieczeństwa (czas liczony jak w punkcie 38). * dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. |
|  | Liczba wspieranych wirtualnych interfejsów sieciowych nie mniejsza niż 4096. |
|  | Firewall musi zapewniać przepustowość co najmniej 8 Gb/s dla kontroli ruchu z włączoną funkcją rozpoznawania aplikacji, nie mniej niż 4 Gb/s dla kontroli zawartości (w tym kontrola AntiVirus, AntiSpyware, Intrusion Prevention System/ Intrusion Detection System. |
|  | Firewall musi obsługiwać co najmniej 60 000 nowych sesji na sekundę. |
|  | Firewall musi obsługiwać co najmniej 2 000 000 jednoczesnych sesji. |
|  | Firewall musi obsługiwać co najmniej 10 000 polityk bezpieczeństwa oraz obsługę minimum 200 stref bezpieczeństwa |
|  | Firewall musi obsługiwać co najmniej 32 000 wpisów w tablicy ARP |
|  | Firewall musi spełniać co najmniej następujące parametry wydajnościowe funkcji VPN (IPSec i SSL):  Minimum 4 Gbps dla IPSEC VPN,  Minimum 4 000 tuneli IPSEC VPN (site-to-site),  Minimum 1 500 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN. |
|  | Możliwość pracy w klastrze w trybie Active-Passive i Active-Active z synchronizacją konfiguracji i tablicy stanu sesji przy włączonych funkcjonalności. |
|  | Firewalle musza być dostarczone w konfiguracji z licencjami dla wymaganych funkcjonalności na 3 lata  Wymagane funkcjonalności:  Threat Prevention (Antivirus, anti-spyware, ochrona podatności),URL-Filtering, DNS Security |
|  | Dostarczone wirtualne firewalle muszą być zgodne ze środowiskiem wirtualizacji VMware ESXi 6.7 i nowszym oraz obsługiwać:  min. 8 interfejsów sieciowych fizycznych 10 Gb/s (zarzadzanie/obsługa ruchu)  min. 8 vCPU  min. 16 GB RAM  min. 60 GB dysk |
|  | Wykonawca przeprowadzi co najmniej 5 dniowe (40 godz.) szkolenie podczas, którego nastąpi wdrożenie w środowisku testowym dostarczonych wirtualnych firewalli w konfiguracji HA platformie VMware ESXi 6.7 i nowszym Zamawiającego.  Minimalny zakres szkolenia:  Architektura rozwiązania Next Generation Firewall  Przegląd funkcjonalności firewalla  Instalacje wirtualne oraz ochrona chmury  Konfiguracja podstawowa urządzenia  Konfiguracja interfejsów sieciowych  Polityki bezpieczeństwa oraz translacja adresów  Identyfikacja aplikacji  Ochrona przed DDos  Ochrona ruchu DNS  Podstawy ochrony Mechanizm IPS, AV, Anty-Spyware  Kategoryzacja stron Internetowych URL filtering  Deszyfracja ruchu szyfrowanego SSL  User-ID - identyfikacja użytkowników w sieci/ Integracja z AD  Dostęp zdalny  Konfiguracja tunelów Site2Site  Monitorowanie urządzenia oraz tworzenie raportów  Konfiguracja klastra niezawodnościowego Active/Passive, testy przełączenia węzłów  Najlepsze praktyki konfiguracyjne |
|  | Gwarancja min 36 miesięcy |