Budowa klastra HA firewall - wymagania minimalne

Uwaga: Zamawiający posiada urządzenie firewall PaloAlto PA-450.

id	Treść wymagania
FW-001	W ramach postępowania: – należy dostarczyć urządzenie, wraz z odpowiednimi zestawami licencji i supportu, pozwalające na stworzenie klastra HA z urządzeniem będącym w posiadaniu przez Zamawiającego, – dopuszcza się dostawę dwóch urządzeń z odpowiednimi zestawami licencji i supportu działających w klastrze HA spełniającym poniższe wymagania.
FW-002	Urządzenie musi być dostarczone jako samodzielne, dedykowane fizyczne urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej rozwiązania musi występować moduł zarządzania i moduł przetwarzania danych.
FW-003	Urządzenie musi być wyposażone w dedykowany port zarządzania out-of-band.
FW-004	Brak ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
FW-005	Urządzenie musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.
FW-006	Obsługa dla IPv6.
FW-007	Funkcjonalność statycznej i dynamicznej translacji adresów NAT między IPv4 i IPv6.
FW-008	Reguły zabezpieczeń firewall muszą być tworzone zgodnie z ustaloną polityką opartą o profile oraz obiekty.
FW-009	Polityka zabezpieczeń firewall musi uwzględniać przynajmniej takie parametry jak: adresy IP źródłowe i docelowe, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie.
FW-010	Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.
FW-011	Interfejs administracyjny urządzenia musi być w języku polskim lub angielskim.
FW-012	Firewall musi działać w następujących trybach: - routera (tzn. w warstwie 3 modelu OSI), - przełącznika (w warstwie 2 modelu OSI), - transparentnym,

	- pasywnego nasłuchu. Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych biorących udział w transmisji.
FW-013	Zarządzanie firewallem musi odbywać się z linii poleceń (CLI) oraz z graficznej konsoli GUI. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Dopuszcza się, aby polityki mogły być tworzone tylko z graficznej konsoli GUI.
FW-014	Urządzenie musi wykonywać 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, mapowanie 1 adres publiczny na 1 adres prywatny oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
FW-015	Urządzenie musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenia muszą umożliwiać stworzenie co najmniej 6 klas dla różnego rodzaju ruchu sieciowego.
FW-016	Firewall musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
FW-017	Obsługa protokołu Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.
FW-018	Obsługa protokołów routingu dynamicznego, nie mniej niż RIP, OSPF oraz BGP.
FW-019	Firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
FW-020	Urządzenie musi posiadać osobny zestaw polityk definiujący ruch zaszyfrowany SSL oraz SSH, który należy poddać lub wykluczyć z operacji deszyfrowania rozdzielny od polityk bezpieczeństwa.
FW-021	Urządzenie musi posiadać funkcjonalność automatycznego pobierania listy stron WWW lub adresów IP z zewnętrznego systemu oraz używania ich w politykach bezpieczeństwa.
FW-022	Ochrona przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony informującej użytkownika o próbie pobrania pliku i możliwości kontynuowania lub zaniechania pobrania.

FW-023	Urządzenie zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
FW-024	Firewall musi identyfikować co najmniej 2500 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS m.in.: Skype, Tor, BitTorrent, eMule.
FW-025	Urządzenie musi umożliwiać definiowanie własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta.
FW-026	System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie wyłącznie na podstawie rozszerzenia.
FW-027	Urządzenie musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Urządzenie musi umożliwiać konfigurację tuneli VPN w trybie route-based VPN.
FW-028	Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN oraz IPSec.
FW-029	Firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną).
FW-030	Producent urządzenia musi udostępniać dedykowanego klienta binarnego VPN przynajmniej dla platform Windows oraz macOS.
FW-031	Urządzenie musi transparentnie ustalać tożsamość użytkowników sieci co najmniej w oparciu o Active Directory oraz Ms Exchange. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować 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 Citrix oraz Windows Terminal Services, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
FW-032	Urządzenie musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach.
FW-033	Urządzenie musi obsługiwać nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu.

FW-034	Urządzenie musi mieć możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesje w przypadku, gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.
FW-035	Musi mieć możliwość wyboru sposobu blokowania ruchu w politykach bezpieczeństwa. Musi istnieć możliwość ustawienia cichego blokowania ruchu bez wysyłania RST, blokowanie z wysłaniem RST tylko do klienta, blokowanie z wysłaniem RST tylko do serwera, blokowanie z wysłaniem RST do klienta i serwera jednocześnie.
FW-036	Firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
FW-037	Urządzenie musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i kategorii stron WWW.
FW-038	Urządzenie musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
FW-039	Urządzenie musi być dostarczone w konfiguracji z minimum 8 portami Ethernet 1Gb/s
FW-040	Firewall musi posiadać przepustowość w ruchu nie mniej niż 2,9 Gbps (dla ruchu appmix) dla kontroli firewall z włączoną funkcją kontroli aplikacji. Przepustowość dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (ochrona IPS, antywirus, antyspyware, identyfikacja aplikacji) nie może być mniejsza niż 1,6 Gbps (dla ruchu appmix).
FW-041	Urządzenie musi obsłużyć minimum 270 000 jednoczesnych sesji oraz 50 000 nowych połączeń na sekundę.
FW-042	Urządzenie musi zapewniać wydajność przynajmniej 2,2 Gbps dla ruchu IPSec VPN i umożliwiać zestawienie przynajmniej 2500 równoczesnych tuneli site-to-site.
FW-043	Urządzenie musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi umożliwiać deszyfracje niezaufanego ruchu HTTPS i poddania go dalszej inspekcji.
FW-044	Urządzenie musi umożliwiać wykluczenie z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie co najmniej: kategoryzacji stron URL oraz dodania własnych wyjątków.
FW-045	Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (IPS, AV, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji

	pracujących na tym samym porcie.
FW-046	Urządzenie musi zapewniać zestawienie przynajmniej 1500 sesji SSL VPN.
FW-047	Urządzenie musi posiadać możliwość uruchomienia funkcji wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS). W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.
FW-048	Urządzenie musi posiadać możliwość uruchomienia funkcji inspekcji antywirusowej, kontrolującej przynajmniej protokoły: SMTP, HTTP, POP3, IMAP oraz podstawowe rodzaje plików. Baza AV musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.
FW-049	Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
FW-050	Urządzenie musi zapewniać moduł przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików wykonywalnych przechodzących przez firewall w celu ochrony przed zagrożeniami typu zero-day. Informacja zwrotna na temat wykrytego złośliwego oprogramowania musi zostać dostarczona na firewall w czasie nie dłuższym jak 1 dzień. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików.
FW-051	Urządzenie musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive i Active-Active w przypadku pracy z drugim takim samym urządzeniem posiadającym taki sam zestaw licencji.
FW-052	Urządzenie musi być fabrycznie nowe, aktualnie obecne w linii produktowej producenta.
FW-053	Urządzenie musi pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej.
FW-054	Urządzenie nie może znajdować się na liście „end-of-sale" oraz „end-of-support" producenta.
FW-055	Serwis dostępu do najnowszej wersji oprogramowania, serwis sprzętowy i ewentualne licencje/subskrypcje na aktualizacje bazy aplikacji muszą być ważne przynajmniej przez okres 12 miesięcy.
FW-056	Szkolenia z produktu muszą być dostępne w języku polskim.
FW-057	Warunki serwisu technicznego i procedura zgłoszeń: Wsparcie techniczne musi być świadczone w języku polskim przez producenta lub

	oficjalnego partnera producenta urządzeń w zakresie świadczenia pomocy serwisowej. Wsparcie techniczne musi być świadczone co najmniej przez okres 12 miesięcy. W ramach świadczenia gwarancyjnego, w wypadku wystąpienia awarii, Zamawiający otrzyma część zamienną/urządzenie objęte gwarancją w trybie następnego dnia roboczego. Wraz z dostarczonym sprzętem będzie świadczony dostęp do strony pomocy technicznej producenta oraz możliwość pobierania aktualizacji oprogramowania związanego z oferowanym sprzętem.