Opis przedmiotu zamówienia

na

„Odnowienie wsparcia dla urządzeń sieciowych (firewalle) PaloAlto”

Warszawa, sierpień 2026 r.

Rozdział I - Definicje

Lp.	Termin	Definicja
1.	**Awaria krytyczna**	Zdarzenie powodujące całkowite unieruchomienie Platformy, uniemożliwiające jej zarządzanie oraz wykorzystywanie.
2.	**Błąd**	Każde z poniżej opisanych zdarzeń, polegające na: 1) znacznym spadku wydajności Platformy; 2) niedostępności wybranych funkcjonalności Platformy, istotnych dla Zamawiającego pozwalającej jednak na dalszą realizację ochrony przed atakami; 3) braku możliwości korzystania z Platformy, ale uzyskanie oczekiwanych efektów jest możliwe w inny sposób (np. przez zastosowanie rozwiązania obejściowego).
3.	**Dni robocze**	Dni od poniedziałku do piątku za wyjątkiem dni wolnych od pracy zgodnie z ustawą z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (Dz. U. z 2020 r. poz. 1920).
4.	**Informacje poufne**	Wszelkie informacje uzyskane w związku z wykonywaniem Umowy przez jedną ze Stron od drugiej Strony niezależnie od formy przekazania tych informacji i ich źródła, w szczególności dane osobowe, informacje techniczne (w szczególności dotyczące Platformy i infrastruktury teleinformatycznej Zamawiającego), technologiczne, prawne i organizacyjne dotyczące drugiej Strony mające charakter poufny.
5.	**Infrastruktura**	Całokształt rozwiązań sprzętowo-programowych i organizacyjnych stanowiących środowisko działania Platformy.
6.	**Oferta**	Oferta Wykonawcy stanowiąca Załącznik nr 2 do Umowy.
7.	**OPZ**	Opis przedmiotu zamówienia, niemniejszy dokument.
8.	**Platforma**	Rozwiązania sprzętowo-programowe PaloAlto będące w posiadaniu Zamawiającego, zgodne z wykazem w Załączniku nr 1 do OPZ, w skład którego wchodzą: 1) System firewall zewnętrznych PA-3220 zwane dalej PA-3220 2) System firewall wewnętrznych PA-3250 zwane dalej PA-3250 3) System Panorama zwane dalej Panorama. 4) subskrypcje i usługi wsparcia technicznego niezbędne do prawidłowego działania ochrony zasobów Zamawiającego.
9.	**Produkt**	Wymagana przez Zamawiającego licencja w modelu subskrypcyjnym uprawniająca do korzystania z pełnej funkcjonalności Platformy, jej utrzymania i aktualizacji oraz możliwość korzystania ze wsparcia technicznego, tj.: 1) licencja w modelu subskrypcyjnym wraz ze wsparciem technicznym producenta dla Systemu PA-3220 (kod producenta dla posiadanych (Klaster HA - High Availability Cluster) urządzeń: Serial nr 016201042786, 016201043051), obejmująca subskrypcje: Advanced URL Filtering, DNS Security, GlobalProtect Gateway, PAN-DB URL Filtering, Threat Prevention, na okres od dnia 29.10.2026 r. do dnia 31.08.2028 r., lub równoważny, dalej jako: **Produkt nr 1;** 2) licencja w modelu subskrypcyjnym wraz ze wsparciem technicznym producenta dla Systemu PA-3250 (kod producenta

		(Klaster HA - High Availability Cluster): Serial nr 016301004854, 016301004817), obejmująca subskrypcję: Threat Prevention, na okres od dnia 29.10.2026 r. do dnia 31.08.2028 r., lub równoważny, dalej jako: **Produkt nr 2**;
10.	**Protokół Odbioru**	Dokument potwierdzający dostarczenie Produktu nr 1 – 2 zgodnie z Umową.
11.	**System PA-3250**	System zaawansowanej analizy, detekcji i prewencji zagrożeń pochodzących z sieci wewnętrznych i będący komponentem Platformy - PaloAlto, posiadany przez Zamawiającego.
12.	**System PA-3220**	System zaawansowanej analizy, detekcji i prewencji zagrożeń pochodzących z sieci zewnętrznych i będący komponentem Platformy - PaloAlto, posiadany przez Zamawiającego.
13.	**System Panorama**	System do zaawansowanego zarządzania Systemem PA-3220, oraz System PA-3250 oraz PA-440 posiadanym przez Zamawiającego.
14.	**Umowa**	Formalno-prawna umowa zawarta między Zamawiającym i Wykonawcą uwzględniająca zakres i warunki realizacji przedmiotu zamówienia.
15.	**Wykaz**	Opis dostarczanych przez Wykonawcę Produktów wraz z informacją o okresie ich świadczenia, stanowiący Załącznik nr 8 do Umowy.

Rozdział II - Wprowadzenie

1. Niniejszy dokument opisuje warunki i wymagania funkcjonalne Zamawiającego dotyczące przedmiotu zamówienia w postępowaniu zakupowym na „Odnowienie wsparcia dla urządzeń sieciowych (firewalle) PaloAlto”.
2. Zamawiający informuje, że posiada Platformę składającą się z Infrastruktury (fizycznych i wirtualnych komponentów) oraz licencji (wieczystych i czasowych) i usług wsparcia technicznego zgodnie z wykazem w Załączniku nr 1 do OPZ.
3. W załączniku nr 2 do OPZ opisuje rozwiązanie równoważne do Systemu PA-3220 wraz z licencjami w postaci subskrypcyjnej które przypisane są do urządzeń.
4. W załączniku nr 3 do OPZ opisuje rozwiązanie równoważne do Systemu PA-3250 wraz z licencją w postaci subskrypcyjnej które przypisane są do urządzeń.

Rozdział III - Przedmiot zamówienia

1. Przedmiotem zamówienia jest:
    1) dostarczenie Produktu nr 1 oraz Produktu nr 2 na okres od dnia 29.10.2026 r. do dnia 31.08.2028 r.,

Rozdział IV - Realizacja przedmiotu zamówienia

1. Wykonawca zobowiązuje się do:
    1) dostarczenia lub uruchomienia Produktów nr 1, 2 na okres od dnia 29.10.2026 r. do dnia 31.08.2028 r., nie później niż do 5 Dni roboczych od dnia podpisania Umowy. Bieg terminu licencji w modelu subskrypcyjnym wraz ze wsparciem technicznym producenta w ramach

Produktów nr 1, 2 rozpocznie się w dniu 29.10.2026 r. w taki sposób, aby zapewnić ciągłość działania usług.

2. Miejscem realizacji przedmiotu zamówienia jest siedziba Zamawiającego, tj. budynek przy ul. ks. Ignacego Jana Skorupki 4 w Warszawie (lokalizacja podstawowa), lokalizacja zapasowa znajdująca się na terenie Warszawy oraz planowane centrum danych znajdujące się na terenie Polski.
3. Wykonawca, a także osoby występujące w jego imieniu podczas realizacji przedmiotu zamówienia, będą zobowiązane do zachowania w tajemnicy wszelkich Informacji poufnych pozyskanych w związku z przystąpieniem do zamówienia i jego wykonywaniem, w szczególności dotyczących skonfigurowanej Platformy i innej infrastruktury teleinformatycznej Zamawiającego oraz informacji prawnie chronionych. W tym celu każda osoba występująca w imieniu Wykonawcy i biorąca udział w realizacji zamówienia będzie zobowiązana do podpisania zobowiązania o zachowaniu poufności informacji.
4. Wszelkie dokumenty elektroniczne przekazywane pomiędzy Zamawiającym i Wykonawcą zawierające Informacje poufne (np. informacje o infrastrukturze lub konfiguracji Platformy Zamawiającego) muszą być przekazywane w formie zaszyfrowanej. Zamawiający i Wykonawca ustalą pomiędzy sobą bezpieczny kanał komunikacji oraz metodę szyfrowania informacji.
5. Potwierdzeniem dostarczenia licencji i świadczenia usług wsparcia technicznego będzie podpisany przez Zamawiającego i Wykonawcę bez zastrzeżeń Protokół Odbioru.
6. Zamawiający może w trakcie realizacji przedmiotu zamówienia korzystać z usług osób trzecich w celu kontroli jakości i sposobu prowadzenia prac Wykonawcy. Wykonawca będzie zobowiązany do udzielenia takim osobom wszelkich informacji, danych lub wyjaśnień dotyczących realizacji przedmiotu zamówienia.
7. Dostarczone przez Wykonawcę Produkty, muszą pochodzić z legalnych źródeł oraz zostać dostarczone Zamawiającemu ze wszystkimi składnikami niezbędnymi do potwierdzenia legalności ich pochodzenia.
8. Dostarczone subskrypcje i oprogramowanie muszą być nowe i nigdy wcześniej niezarejestrowane.
9. Zamawiający nie dopuszcza zaoferowania licencji i oprogramowania pochodzących z odsprzedaży (tj. nie dopuszcza licencji pochodzących z rynku wtórnego).
10. Wykonawca ponosi odpowiedzialność za straty i szkody powstałe wskutek prowadzenia przez siebie prac związanych z realizacją przedmiotu zamówienia w sposób zawiniony, niezgodny z postanowieniami Umowy, przepisami prawa i ustaleniami z osobą kierującą pracami po stronie Zamawiającego, do pełnej wysokości szkody.
11. Wykonawca ponosi pełną odpowiedzialność za wszystkie prace oraz ich skutki wykonywane przez podwykonawców, tak jak za działania własne.

12. Zamawiający będzie współpracował z Wykonawcą przy realizacji przedmiotu zamówienia w zakresie określonym w Umowie.
13. Na podstawie Umowy i na warunkach w niej opisanych Wykonawca zobowiązuje się wykonać wszystkie prace będące przedmiotem Umowy terminowo z zachowaniem staranności wynikającej z zawodowego charakteru działalności oraz zgodnie z obowiązującymi przepisami prawa, normami i najwyższymi standardami technicznymi.

Rozdział V - Wymagania w zakresie produktu równoważnego

1. W przypadku zaoferowania produktu równoważnego Wykonawca zobowiązany jest w ofercie udowodnić, że funkcjonalność oferowanego produktu jest równoważna w stosunku do Produktu wskazanego w niniejszym OPZ oraz zaoferowane produkty równoważne spełniają wszystkie wymagania i warunki określone w OPZ.
2. Rozwiązanie równoważne nie może naruszać warunków licencyjnych producenta Platformy oraz musi zapewniać bez dodatkowych nakładów finansowych bezkonfliktowe działanie posiadanej Platformy zbudowanej w oparciu o Infrastrukturę sprzętowo-programowe wskazane w wykazie o którym mowa w Załączniku nr 1 do OPZ.
3. W przypadku oferowania równoważnej licencji lub równoważnego wsparcia technicznego względem wskazanego przez Zamawiającego, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że zaoferowane produkty spełniają wszystkie wymagania i warunki jakimi charakteryzuje się produkt wskazany w niemniejszym dokumencie, w szczególności w zakresie:
    1) warunki licencji i wsparcia technicznego zaoferowanych produktów równoważnych w każdym aspekcie nie mogą być gorsze niż dla Produktów wymienionych w OPZ;
    2) funkcjonalności zaoferowanych Produktów równoważnych, które nie mogą być ograniczone i gorsze względem funkcjonalności posiadanej Platformy;
    3) zakresu kompatybilności i współdziałania zaoferowanych produktów równoważnych ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego, który nie może być gorszy niż dla posiadanej Platformy;
    4) poziomu współpracy zaoferowanych produktów równoważnych z Platformą Zamawiającego, które nie może być gorszy niż dla Produktów wymienionych w OPZ;
    5) zapewnienie pełnej, równoległej współpracy w czasie rzeczywistym i pełnej funkcjonalnej zamienności zaoferowanych produktów równoważnych z Produktami wymienionymi w OPZ;
    6) warunków i zakresu usług gwarancji, wsparcia technicznego i konserwacji dla zaoferowanych produktów równoważnych, które nie mogą być gorsze niż dla Produktów wymienionych w OPZ;
    7) dostępności wersji bitowych zaoferowanych produktów równoważnych, które nie może być mniejsza niż dla Produktów wymienionych w OPZ.

4. W przypadku, gdy zaoferowany przez Wykonawcę produkt równoważny nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującymi w Infrastrukturze Zamawiającego stanowiącym Platformę, Wykonawca na własny koszt przywróci środowisko do stanu poprawnego funkcjonowania w przeciągu 24 godzin od stwierdzenia przez Zamawiającego niepoprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego (przywrócenie właściwego działania środowiska Platformy Zamawiającego) dostarczy inne rozwiązanie spełniające wymagania OPZ w terminie do 3 Dni roboczych.
5. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcie w jego nowszych wersjach.
   W przypadku zaoferowania rozwiązania równoważnego Wykonawca jest zobowiązany uwzględnić w ofercie wszelkie koszty jego wdrożenia i integracji z posiadaną przez Zamawiającego Infrastrukturą sprzętowo-programową Platformy, w tym koszty ewentualnych instruktaży oraz migracji danych oraz pokryje również wszelkie udokumentowane koszty po stronie Zamawiającego, związane z wdrożeniem rozwiązania równoważnego.
6. Zaoferowane rozwiązanie równoważne dla Produktów nr 1-2 musi posiadać wsparcie techniczne producenta o parametrach nie gorszych niż:
   a) Wsparcie przy rozwiązywaniu problemów związanych z działaniem posiadanej Platformy trybie 24x7, czas reakcji na zgłoszony drogą mailową lub telefoniczną problem –maks. 1 godzina w przypadku awarii krytycznych (np. uszkodzenie urządzenia) zgłoszonych telefonicznie maks. 8 godzin w przypadku pozostałych zgłoszeń przy wystąpieniu awarii urządzenia, któregokolwiek z jego komponentów lub wyposażenia, w tym modułów optycznych – wymiana lub naprawa (RMA) w terminie NBD (następny dzień roboczy) przy zgłoszeniu awarii do godziny 15:00 w dniu roboczym. W ciągu dwóch dni roboczych przy zgłoszeniu awarii po godzinie 15:00 w dniu roboczym
   b) W przypadku wymiany urządzenia, któregokolwiek z jego komponentów lub wyposażenia, w tym modułów optycznych – wymiana następuje na sprzęt tożsamy lub równoważny (w przypadku gdy producent dokonałby zmian w swoim portfolio produktowym)
   c) W przypadku wymiany nośników danych, które uległy awarii, uszkodzone nośniki pozostają w całości u zamawiającego. Nie są konieczne działania np. w postaci demontażu dysku i pozostawienia u zamawiającego fragmentów dysku z nośnikami danych

w terminie NBD (następny dzień roboczy) przy zgłoszeniu awarii do godziny 15:00 w dniu roboczym w ciągu dwóch dni roboczych przy zgłoszeniu awarii po godzinie 15:00 w dniu roboczym

d) Zapewnienie wsparcia technicznego świadczonego przez autoryzowane przez producenta centrum serwisowe niezależne od Integratora/Wykonawcy i realizowane we współpracy z producentem dla Platformy.
e) dostęp do poprawek dla Platformy udostępnionych przez producenta;
f) dostęp do nowych wersji dla Platformy udostępnionych przez producenta;
g) dostęp do nowych sygnatur bezpieczeństwa
h) dostęp do portalu producenta Platformy z bazą wiedzy, dokumentacją do Systemu oraz nośnikami do instalacji nowych wersji oprogramowania i poprawek;
i) dostęp do pomocy technicznej producenta Platformy dla Systemu świadczonej drogą elektroniczną (email, portal producenta, telefon) z nielimitowaną liczbą zgłoszeń;
j) dostęp 24x7x365 on-line do inżynierów technicznych zapewniających pomoc w diagnozowaniu problemów z konfiguracją i awariami krytycznymi Systemu.

Opis równoważności dla Produktu w poz. nr 1 (kod producenta Serial nr 016201042786, 016201043051) znajduje się w załączniku nr 2 do OPZ.
Opis równoważności dla Produktu w poz. nr 2 (kod producenta Serial nr 016301004854, 016301004817) znajduje się w załączniku nr 3 do OPZ.

Załączniki:

Załącznik nr 1 - Wykaz posiadanych elementów wchodzących w skład Platformy

Załącznik nr 2 – Opis sprzętu równoważnego dla Systemu PA-3220 wraz z licencjami w modelu subskrypcyjnym.

Załącznik nr 3 – Opis sprzętu równoważnego dla Systemu PA-3250 wraz z licencjami w modelu subskrypcyjnym.

Załącznik nr 1 do OPZ

Wykaz posiadanych elementów wchodzących w skład Platformy

1) Lista komponentów:

Lp.	Nazwa komponentu	Kod producenta/numery seryjne	Typ urządzenia	Ilość
1	PA-3220 (Advanced URL Filtering, DNS Security, GlobalProtect Gateway, PAN-DB URL Filtering, Threat Prevention)	016201042786 016201043051	maszyna fizyczna	2
2	PA-3250 Threat Prevention)	016301004854 016301004817	maszyna fizyczna	2
3	Panorama	000702134065	maszyna wirtualna	1
4	PA-440	021201091702	maszyna fizyczna	1

2) Lista licencji i wsparcia technicznego:

Lp.	Nazwa licencji/produktu	Kod producenta	Ilość
1	Advanced URL Filtering (PA-3220)		1
2	DNS Security (PA-3220)		1
3	GlobalProtect Gateway (PA-3220)		1
4	Threat Prevention (PA-3220)		1
5	Threat Prevention (PA-3250)		1
6	PAN-DB URL Filtering (PA-3220)		1

Opis sprzętu równoważnego dla Systemu PA-3220 wraz z licencjami w modelu subskrypcyjnym.

Wymagania podstawowe

1.1. Muszą to być specjalizowane urządzenia sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako para wysokiej dostępności (HA) w trybach Active/Standby, Active/Active.
1.2. Całość sprzętu i oprogramowania musi być dostarczona i zapewniać wsparcie serwisowe przez jednego tego samego producenta.
1.3. Urządzenia muszą umożliwiać działanie w następujących trybach pracy:
- routera (tzn. w warstwie 3 modelu ISO OSI),
- mostu (tzn. w warstwie 2 modelu ISO OSI),
- w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; musi pracować w trybie przezroczystego łączenia interfejsów w pary),
- w trybie pasywnego nasłuchu (tzw. sniffer/tap).

System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
1.4. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.
1.5. Urządzenia firewall muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu (tzw. data plane) od zasobów służących do zarządzania urządzeniem (tzw. management plane). Akceptowana jest separacja logiczna zasobów zrealizowana za pomocą przypisania dedykowanej ilości rdzeni zasobów procesorów (tzw. CPU core's) do obu z funkcji lub alternatywnie za pomocą oddzielnych dedykowanych procesorów (tzw. CPU) dla każdej z funkcji.
1.6. Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.
1.7. Urządzenia firewall muszą wspierać protokół LACP.
1.8. Urządzenia firewall muszą zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
1.9. Urządzenia firewall muszą działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.
1.10. Polityka zabezpieczeń firewall musi uwzględniać:
- adresy IP źródłowe i docelowe,
- protokoły i usługi sieciowe,
- aplikacje,
- kategorie URL,
- użytkowników aplikacji i grupy,
- reakcje zabezpieczeń,
- logowanie zdarzeń (początek i koniec sesji)
- strefa wejściowa i wyjściowa

1.11. Urządzenia firewall muszą automatycznie identyfikować aplikacje bez względu na numery portów (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Urządzenie musi wykrywać co najmniej 3500 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz z aplikacjami przemysłowymi (tzw. ICS/OT) np. DNP3, Modbus.

Urządzenia muszą pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia (bez użycia zewnętrznych narzędzi).

1.12. Urządzenia firewall muszą pozwalać na blokowanie transmisji plików wybranego typu, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .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.

1.13. Urządzenia firewall muszą być zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji lub pobierania dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.
1.14. Urządzenia firewall muszą być wyposażone w 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). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy przewidzieć odpowiednie licencje dla minimum 30 administratorów na wszystkie oferowane urządzenia.
1.15. Dostęp do urządzeń i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
1.16. Urządzenia firewall muszą 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.
1.17. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
- Microsoft Active Directory,
- Microsoft Exchange
- Terminal Services
- Syslog
- Cisco ISE

1.18. Polityka kontroli dostępu (urządzeń 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.
1.19. Urządzenia firewall muszą pozwalać na lokalne zbieranie (na dysk urządzenia) 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, połączeniach VPN.
1.20. Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu 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. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.
1.21. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
- reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
- API

1.22. Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESXi i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można następnie wykorzystywać w polityce bezpieczeństwa urządzeń.
1.23. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.
1.24. Urządzenia firewall muszą 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.
1.25. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
1.26. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami informacji o NAT.

1.27. Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju. Konieczna jest obsługa Syslog za pomocą transportu UDP, TCP, SSL oraz obsługa formatów IETF oraz BSD.
1.28. Urządzenia firewall muszą obsługiwać możliwość deszyfracji ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
1.29. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji - rozdzielny od polityk bezpieczeństwa.
1.30. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS który nie ma zostać odszyfrowany, ale poddany sprawdzeniu czy certyfikat serwera nie wygasł oraz sprawdzeniu czy certyfikat nie pochodzi od zaufanego wystawcy. W takim przypadku urządzenie musi umożliwiać blokadę takiej sesji użytkownika.
1.31. Wykonywanie operacji deszyfracji ruchu musi być odnotowywane w logach urządzeń 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.
1.32. Wykonywanie operacji deszyfracji ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL (w przypadku, gdy jest wymagane jego dostarczenie) albo możliwość wykorzystania własnej utworzonej na urządzeniu listy URL które mają podlegać deszyfracji albo być z niej wykluczone (tzw. wyjątek).
1.33. Urządzenie firewall 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.
1.34. 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, TLS_CHACHA20_POLY1305_SHA256.
1.35. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości sesji w odniesieniu do źródłowego lub docelowego adresu IP.
1.36. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) dla aplikacji i użytkowników.
1.37. Urządzenia firewall muszą 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).
1.38. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
1.39. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
1.40. Urządzenia firewall muszą zapewniać inspekcję komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu blokowania tuneli SSH.
1.41. Urządzenia firewall muszą obsługiwać funkcję DNS proxy.
1.42. Urządzenia firewall muszą obsługiwać funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta musi być realizowana na bazie technologii SSL VPN oraz IPSec. Jeżeli oprogramowania klienta Remote Access VPN dla laptopów z systemem klienckim Windows wymaga licencji – należy dostarczyć licencję na maksymalną wydajność oraz maksymalną ilość dla oferowanego typu urządzeń.
1.43. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.
1.44. Urządzenia firewall dla zdalnego dostępu VPN muszą umożliwiać następujące funkcjonalności:
- Realizacja VPN dla aplikacji HTML/HTML5 w trybie przeglądarkowym (tzw. Clientless VPN)
- Zestawianie zdalnego dostępu dla urządzeń mobilnych tzw. smart devices. Telefony/tablety bazujące na systemach operacyjnych: Apple iOS i Google Android.
- Dostępność oprogramowania klienckiego VPN dla urządzeń mobilnych z systemami: Apple iOS (10-16), Android (6-13), Win UWP
- Dostępność oprogramowania klienta VPN dla stacji/laptopów dla następujących systemów operacyjnych: Windows 8-11; Windows 10 UWP; iOS 10-14; MacOS 10.15-13; Google

Android 6-11; Linux CentOS, RHEL, Ubuntu;
- Sprawdzanie informacji o systemie operacyjnym, aktualizacji poprawek OS, aktualizacji oprogramowania antywirusowego itp. dla systemów Windows.
- Sprawdzanie obecności konta urządzenia w systemie katalogowym Windows AD dla systemów Windows.
- Możliwość pomijania tunelu zdalnego dostępu VPN dla specyficznych aplikacji, domeny DNS, aplikacji video. Dla podłączających się stacji/laptopów Windows i MacOS.
- Dodatkowa identyfikacja urządzeń użytkownika na bazie unikalnego identyfikatora innego niż adres IP (Windows – MachineGuid, Android – Android ID, iOS – UDID) pozwalająca na blokadę dostępu VPN dla wybranego urządzenia. Np. blokada dostępu VPN dla urządzenia zainfekowanego.
- Możliwość automatycznego (bez ingerencji administratora) zablokowania dostępu poprzez RA VPN urządzenia skompromitowanego do chronionych zasobów.

1.45. Producent oferowanego rozwiązania musi być obecny w najnowszym rynkowym raporcie Gartner Magic Quadrant for Enterprise Network Firewalls w części (tzw. ćwiartce) Leaders.
1.46. Dostarczane razem z urządzeniami subskrypcje, licencje, gwarancje muszą obowiązywać w okresie od dnia 29.10.2026 r. do dnia 31.08.2028 r.
1.47. W przypadku potrzeby wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby dyski zostały wymontowane z urządzenia i pozostały w jego siedzibie w celu bezpiecznej utylizacji.

Wymagania dodatkowe

Należy dostarczyć 2 szt. urządzeń, które będą pracowały jako 1 para w układzie HA.
Razem z urządzeniami muszą zostać dostarczone następujące typy i ilości modułów połączeniowych. Ilość dla zestawu 2 urządzeń głównych:
1. Do HA: 4 szt. SFP+ 10GE wariant SR
2. Do LAN: 20 szt. SFP+ 10GE wariant SR

Każde z urządzeń musi (poza wymaganiami wspólnymi), spełniać dodatkowo wymagania:
1. Urządzenie musi być wyposażone w minimum:
   1.1. dedykowany port Ethernet do zarządzania urządzeniem o prędkościach 10/100/1000Mbps
   1.2. dedykowany port konsoli do zarządzania urządzeniem w standardzie RJ45 bądź Micro USB,
   1.3. 12 wbudowanych interfejsów Ethernet (RJ45) pracujących z prędkościami 10/100/1000Mbps.
   1.4. 4 wbudowane gniazda pozwalające na obsadzenie modułami 1Gbps SFP.
   1.5. 4 wbudowane elastyczne gniazda pozwalających na obsadzenie modułami 1Gbps SFP oraz 10Gbps SFP+. Jeżeli urządzenie nie wspiera gniazd elastycznych, musi posiadać 4 gniazda 1Gbps SFP oraz 4 gniazda 10Gbps SFP+.
   1.6. 1 wbudowany dedykowany interfejs HA w formie gniazda 10Gbps SFP+.
   1.7. Musi być wyposażone w zasób dyskowy (niemechaniczny) o wielkości co najmniej 220 GB na potrzeby systemu operacyjnego. W przypadku procedury wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby zasoby dyskowe zostały wymontowane z urządzenia i pozostały w jego siedzibie w celu bezpiecznej utylizacji.
   1.8. Musi być wyposażone w co najmniej 2 zasilacze typu AC 230V pracujące redundantnie. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.
   1.9. Urządzenie musi być przeznaczone do montażu w szafie Rack 19”.
2. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
   2.1. 4,1 Gbps dla rozpoznawania i kontroli aplikacji.
   2.2. 2,1 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: włączone wszystkie sygnatury IPS, antywirus, antyspyware, blokowanie typów plików, z włączonym logowaniem na dyski urządzenia.
   2.3. 2,3 Gbps dla IPSec VPN,
   2.4. 45000 nowych sesji na sekundę.
   2.5. 950000 równoległych sesji
3. Musi obsługiwać nie mniej niż 10 wirtualnych routerów, posiadających odrębne tabele routingu i

umożliwiać uruchomienie więcej niż jednej tablicy routingu, w pojedynczej wirtualnej instancji firewall. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia.

4. Urządzenie musi posiadać co najmniej 180 stref bezpieczeństwa.
5. Urządzenie musi posiadać możliwość licencyjnego ustanowienia co najmniej 6 wirtualnych instancji firewall (określanych jako kontekst/domena/system). Każda z instancji musi pozwalać na konfigurację niezależnych oraz odrębnych od innych instancji – polityk bezpieczeństwa (co najmniej dla IPS, AV i współpracy z sandboxem), tablicy routingu oraz realizacji zdalnego dostępu.
6. Urządzenie musi posiadać architekturę z odseparowanymi zasobami. Procesory zarządzające oraz pamięć (tzw. Management Plane) muszą być oddzielne od procesorów i pamięci przetwarzających ruch sieciowy (tzw. Data Plane).
7. Nadmierne obciążenie ruchem sieciowym (Data Plane) urządzenia nie może blokować funkcjonowania części zarządzającej (Management Plane). Nie może powodować problemów z konfigurowaniem czy monitorowaniem urządzenia, dostępem do interfejsu GUI i CLI.
8. Musi umożliwiać zdefiniowanie nie mniej niż 9900 reguł polityki bezpieczeństwa oraz 2900 reguł NAT.
9. Urządzenie musi posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
10. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur oraz powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.
11. Urządzenie musi posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.
12. Urządzenie musi posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół minimum: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny (nie rzadziej niż raz na 48h) i pochodzić od tego samego producenta co firewall.
13. Urządzenie musi posiadać funkcję anty-spyware. Baza sygnatur musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.
14. Urządzenie musi posiadać funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (Machine Learning - ML) aktualizowanych dynamicznie przez producenta.
15. Wykrywanie za pomocą algorytmów musi odbywać się lokalnie na urządzeniu jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antywirus oraz funkcji filtrowania URL.
16. 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.
17. 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:
18. Wymagana analiza i detekcja musi umożliwiać blokowanie wykrytej komunikacji C2 w czasie rzeczywistym,
19. 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,
20. Urządzenie musi posiadać funkcję filtrowania URL.
21. Urządzenie musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (a nie tylko filtrującego) ruch w politykach bezpieczeństwa.
22. 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.
23. Wymagane jest posiadanie oddzielnych kategorii URL dla zagrożeń typu malware, phishing, C2C oraz dla ostatnio zarejestrowanych domen.

a. 24.Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania kategorii URL.
b. 25.Funkcjonalność musi zapewniać możliwość blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (Machine Learning, ML) aktualizowanych dynamicznie przez producenta. Wykrywanie za pomocą algorytmów ML musi odbywać się lokalnie na urządzeniu jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antivirus oraz funkcji filtrowania URL.

Opis sprzętu równoważnego dla Systemu PA-3250 wraz z licencjami w modelu subskrypcyjnym.

Wymagania podstawowe

1.1. Muszą to być specjalizowane urządzenia sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako para wysokiej dostępności (HA) w trybach Active/Standby, Active/Active.
1.2. Całość sprzętu i oprogramowania musi być dostarczona i zapewniać wsparcie serwisowe przez jednego tego samego producenta.
1.3. Urządzenia muszą umożliwiać działanie w następujących trybach pracy:
- routera (tzn. w warstwie 3 modelu ISO OSI),
- mostu (tzn. w warstwie 2 modelu ISO OSI),
- w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; musi pracować w trybie przezroczystego łączenia interfejsów w pary),
- w trybie pasywnego nasłuchu (tzw. sniffer/tap).

System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
1.4. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.
1.5. Urządzenia firewall muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu (tzw. data plane) od zasobów służących do zarządzania urządzeniem (tzw. management plane). Akceptowana jest separacja logiczna zasobów zrealizowana za pomocą przypisania dedykowanej ilości rdzeni zasobów procesorów (tzw. CPU core's) do obu z funkcji lub alternatywnie za pomocą oddzielnych dedykowanych procesorów (tzw. CPU) dla każdej z funkcji.
1.6. Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.
1.7. Urządzenia firewall muszą wspierać protokół LACP.
1.8. Urządzenia firewall muszą zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
1.9. Urządzenia firewall muszą działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.
1.10. Polityka zabezpieczeń firewall musi uwzględniać:
- adresy IP źródłowe i docelowe,
- protokoły i usługi sieciowe,
- aplikacje,
- kategorie URL,
- użytkowników aplikacji i grupy,
- reakcje zabezpieczeń,
- logowanie zdarzeń (początek i koniec sesji)
- strefa wejściowa i wyjściowa

1.11. Urządzenia firewall muszą automatycznie identyfikować aplikacje bez względu na numery portów (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Urządzenie musi wykrywać co najmniej 3500 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz z aplikacjami przemysłowymi (tzw. ICS/OT) np. DNP3, Modbus.
Urządzenia muszą pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia (bez użycia zewnętrznych narzędzi).
1.12. Urządzenia firewall muszą być zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji lub pobierania dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.
1.13. Urządzenia firewall muszą być wyposażone w 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). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy przewidzieć odpowiednie licencje dla minimum 30 administratorów na wszystkie oferowane urządzenia.

1.14 Dostęp do urządzeń i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.

1.15. Urządzenia firewall muszą 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.

1.16. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
- Microsoft Active Directory,
- Microsoft Exchange
- Terminal Services
- Syslog
- Cisco ISE

1.17. Polityka kontroli dostępu (urządzeń 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.

1.18. Urządzenia firewall muszą pozwalać na lokalne zbieranie (na dysk urządzenia) 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, połączeniach VPN.

1.19. Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu 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. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.

1.20. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
- reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
- API

1.21. Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESXi i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można następnie wykorzystywać w polityce bezpieczeństwa urządzeń.

1.22. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.

1.23. Urządzenia firewall muszą 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.

1.24. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

1.25. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami informacji o NAT.

1.26. Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju. Konieczna jest obsługa Syslog za pomocą transportu UDP, TCP, SSL oraz obsługa formatów IETF oraz BSD.

1.27. Urządzenia firewall muszą obsługiwać możliwość deszyfracji ruchu użytkowników w celu

inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.

1.28. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji - rozdzielny od polityk bezpieczeństwa.

1.29. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS który nie ma zostać odszyfrowany, ale poddany sprawdzeniu czy certyfikat serwera nie wygasł oraz sprawdzeniu czy certyfikat nie pochodzi od zaufanego wystawcy. W takim przypadku urządzenie musi umożliwiać blokadę takiej sesji użytkownika.

1.30. Wykonywanie operacji deszyfracji ruchu musi być odnotowywane w logach urządzeń 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.

1.31. Urządzenie firewall 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.

1.32. 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, TLS_CHACHA20_POLY1305_SHA256.

1.33. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości sesji w odniesieniu do źródłowego lub docelowego adresu IP.

1.34. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) dla aplikacji i użytkowników.

1.35. Urządzenia firewall muszą 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).

1.36. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.

1.37. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.

1.38. Urządzenia firewall muszą zapewniać inspekcję komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu blokowania tuneli SSH.

1.39. Producent oferowanego rozwiązania musi być obecny w najnowszym rynkowym raporcie Gartner Magic Quadrant for Enterprise Network Firewalls w części (tzw. ćwiartce) Leaders.

1.40. Dostarczane razem z urządzeniami subskrypcje, licencje, gwarancje muszą obowiązywać w okresie od dnia 29.10.2026 r. do dnia 31.08.2028 r.

1.41. W przypadku potrzeby wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby dyski zostały wymontowane z urządzenia i pozostały w jego siedzibie w celu bezpiecznej utylizacji.

4. 2. Wymagania dodatkowe

Należy dostarczyć 2 szt. urządzeń, które będą pracowały jako 1 para w układzie HA.
Razem z urządzeniami muszą zostać dostarczone następujące typy i ilości modułów połączeniowych. Ilość dla zestawu 2 urządzeń głównych:

1. Do HA: 4 szt. SFP+ 10GE wariant SR
2. Do LAN: 12 szt. SFP+ 10GE wariant SR

Każde z urządzeń musi (poza wymaganiami wspólnymi), spełniać dodatkowo wymagania:

1. Urządzenie musi być wyposażone w minimum:
   1.1. dedykowany port Ethernet do zarządzania urządzeniem o prędkościach 10/100/1000Mbps
   1.2. dedykowany port konsoli do zarządzania urządzeniem w standardzie RJ45 bądź Micro USB,
   1.3. 12 wbudowanych interfejsów Ethernet (RJ45) pracujących z prędkościami 10/100/1000Mbps.
   1.4. 4 wbudowane gniazda pozwalające na obsadzenie modułami 1Gbps SFP.
   1.5. 4 wbudowane elastyczne gniazda pozwalających na obsadzenie modułami 1Gbps SFP oraz 10Gbps SFP+. Jeżeli urządzenie nie wspiera gniazd elastycznych, musi posiadać 4 gniazda

1Gbps SFP oraz 4 gniazda 10Gbps SFP+.

1.6. 1 wbudowany dedykowany interfejs HA w formie gniazda 10Gbps SFP+.
1.7. Musi być wyposażone w zasób dyskowy (niemechaniczny) o wielkości co najmniej 220 GB na potrzeby systemu operacyjnego. W przypadku procedury wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby zasoby dyskowe zostały wymontowane z urządzenia i pozostały w jego siedzibie w celu bezpiecznej utylizacji.
1.8. Musi być wyposażone w co najmniej 2 zasilacze typu AC 230V pracujące redundantnie. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.
1.9. Urządzenie musi być przeznaczone do montażu w szafie Rack 19".

2. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
   2.1. 5 Gbps dla rozpoznawania i kontroli aplikacji.
   2.2. 2,5 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: włączone wszystkie sygnatury IPS, antywirus, antyspyware, blokowanie typów plików, z włączonym logowaniem na dyski urządzenia.
   2.3. 2,5 Gbps dla IPSec VPN,
   2.4. 58000 nowych sesji na sekundę.
   2.5. 2000000 równoległych sesji
3. Musi obsługiwać nie mniej niż 10 wirtualnych routerów, posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu, w pojedynczej wirtualnej instancji firewall. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia.
4. Urządzenie musi posiadać co najmniej 180 stref bezpieczeństwa.
5. Urządzenie musi posiadać możliwość licencyjnego ustanowienia co najmniej 6 wirtualnych instancji firewall (określanych jako kontekst/domena/system). Każda z instancji musi pozwalać na konfigurację niezależnych oraz odrębnych od innych instancji – polityk bezpieczeństwa (co najmniej dla IPS, AV i współpracy z sandboxem), tablicy routingu oraz realizacji zdalnego dostępu.
6. Urządzenie musi posiadać architekturę z odseparowanymi zasobami. Procesory zarządzające oraz pamięć (tzw. Management Plane) muszą być oddzielne od procesorów i pamięci przetwarzających ruch sieciowy (tzw. Data Plane).
7. Nadmierne obciążenie ruchem sieciowym (Data Plane) urządzenia nie może blokować funkcjonowania części zarządzającej (Management Plane). Nie może powodować problemów z konfigurowaniem czy monitorowaniem urządzenia, dostępem do interfejsu GUI i CLI.
8. Musi umożliwiać zdefiniowanie nie mniej niż 9900 reguł polityki bezpieczeństwa oraz 2900 reguł NAT.
9. Urządzenie musi posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
10. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur oraz powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.
11. Urządzenie musi posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.
12. Urządzenie musi posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół minimum: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny (nie rzadziej niż raz na 48h) i pochodzić od tego samego producenta co firewall.
13. Urządzenie musi posiadać funkcję anty-spyware. Baza sygnatur musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.
14. Urządzenie musi posiadać funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (Machine Learning - ML) aktualizowanych dynamicznie przez producenta.
15. Wykrywanie za pomocą algorytmów musi odbywać się lokalnie na urządzeniu jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antywirus

16. 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.
17. 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:
18. Wymagana analiza i detekcja musi umożliwiać blokowanie wykrytej komunikacji C2 w czasie rzeczywistym,
19. 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.