Nr sprawy: BF-IV.2370.12.2024
Załącznik nr 1 do SWZ/ Załącznik nr 2 do umowy

Opis Przedmiotu Zamówienia (OPZ)

Przedmiot Zamówienia **„Dostawa urządzeń infrastruktury sieci SD-WAN dla Platformy Chmurowej Integracji Danych KG PSP"** realizowany jest w ramach projektu **„Rozbudowa systemu ostrzegania i alarmowania”**.
Całe zadanie jest częścią **Krajowego Planu Odbudowy i Zwiększania Odporności**, w ramach którego maksymalnie 4060 punktów systemu alarmowania i ostrzegania ludności będzie zmodernizowanych w ramach środków dostępnych z Krajowego Planu Odbudowy i Zwiększania Odporności celem osiągnięcia wskaźnika C26G: Mobilna infrastruktura na rzecz systemu zarządzania kryzysowego".
Zamówienie to stanowi dostawę opisanego sprzętu i oprogramowania wraz z montażem, konfiguracją, integracją z infrastrukturą teleinformatyczną ZAMAWIAJĄCEGO, poszczególnych Odbiorców wskazanych w komparycji Umowy dla lokalizacji określonych w załączniku nr 2a do Umowy (wykaz lokalizacji dostaw i instalacji urządzeń dla poszczególnych Odbiorców), jak również opracowanie dokumentacji projektowej i powykonawczej przedmiotowego rozwiązania.

Wstęp.

Celem tego zamówienia jest stworzenie na bazie dostarczonych urządzeń, spójnego i zintegrowanego systemu komunikacyjnego, który umożliwi efektywny, szybki i bezpieczny przepływ krytycznych informacji w ramach działań Państwowej Straży Pożarnej i innych służb odpowiedzialnych za bezpieczeństwo publiczne. Przedmiotowe zadanie obejmuje dostawę i wyposażenie 553 lokalizacji PSP w urządzenia w ilości 605 sieci SD-WAN w celu stworzenia zaawansowanego i zintegrowanego systemu komunikacyjnego opartego na technologii SD-WAN.

Opis stanu obecnego.

Obecnie wszystkie jednostki PSP mają dostęp do sieci OST112 oraz sieci operatorów ISP z dostępem do Internetu. Zabezpieczenia ruchu sieciowego są zdecentralizowane i nie mają ustandaryzowanej konfiguracji zabezpieczeń sieci, nie są agregowane logi w kontekście całej organizacji i jej bezpieczeństwa. W powyższej konfiguracji nie jest możliwe zorganizowanie implementacji wspólnej polityki dostępu, zabezpieczeń sieci i jej automatycznej analizy dla realizacji szybkiej reakcji na potencjalne ataki z zewnątrz itp.
Ruch sieciowy wewnątrz organizacji do systemów centralnych i pomiędzy jednostkami odbywa się poprzez sieć OST 112. Nie jest wykorzystywana sieć dostępu do Internetu jako zapasowe łącze.

Próby organizacji zapasowych połączeń wykorzystujących jako medium transmisyjne sieć Internet były wdrażane na poziomach Komend Wojewódzkich PSP w relacji połączenia z podległymi Komendami, co w korelacji dostępu do usług centralnych nie stanowi poprawy dostępności dodatkowego kanału połączeniowego wdrażanego lokalnie.
Urządzenia zabezpieczające dostęp do sieci Internet mają różny poziom implementacji rozwiązań bezpieczeństwa i są kupowane przez każdą Jednostkę Organizacyjną z osobna, co stanowi bardzo duże koszty utrzymania poziomu zabezpieczeń.
W dotychczasowych połączeniach z siecią OST 112 brak jest mechanizmów ukierunkowanych na usługę, aplikacje i ich dostępność, co skutkuje losowym poziomem jakości dostępu.
Zamawiający dysponuje urządzeniami brzegowymi w siedzibie KG PSP oraz personel posiadający certyfikowane szkolenia oraz doświadczenie w zakresie zarządzania konfiguracji NG firewall.

Główne cele:

- Umożliwienie efektywnego współdziałania różnorodnych systemów i technologii używanych przez Państwową Straż Pożarną oraz inne służby ratunkowe, co umożliwi szybką i skoordynowaną reakcję w sytuacjach kryzysowych,
- Zapewnienie odporności rozwiązania na różnego rodzaju awarie i zagrożenia, co jest kluczowe dla utrzymania ciągłości komunikacji w trakcie działań ratunkowych i sytuacji kryzysowych,
- Wymiana danych musi spełniać najwyższe standardy bezpieczeństwa, aby zapobiegać nieautoryzowanemu dostępowi i utracie ważnych informacji,
- Rozwiązanie musi być projektowane z myślą o łatwej rozbudowie i integracji nowych jednostek oraz użytkowników, co umożliwi elastyczne dostosowanie do zmieniających się potrzeb,
- Wszelkie działania i rozwiązania muszą być zgodne z obowiązującymi przepisami prawnymi dotyczącymi ochrony danych i bezpieczeństwa informacji,
- Stworzenie zaawansowanego nadzoru i kontroli nad polityką dostępu do zasobów sieci Internet i innych sieci,
- Wdrożenie centralnego systemu bezpieczeństwa przed potencjalnymi atakami z sieci Internet poprzez wprowadzenie centralnych punktów styku,
- Możliwość szybkiego reagowania administratorów IT na lokalne, bieżące potrzeby w zakresie polityki dostępu,
- Centralna archiwizacja konfiguracji i możliwość jej audytu przez administratorów Komendy Głównej PSP pod kątem zgodności z centralną polityką dostępu,
- Sieć SD-WAN przystosowana do obsługi i świadczenia usług na każdym poziomie wszystkich jednostek podległych w tym m.in. takich jak łączność wideo, voip, dostęp do zasobów chmury prywatnej, publicznej etc.
- Wizualizacja ruchu sieciowego i jego analiza dla zapewnienia wysokiej dostępności usług, aplikacji,

- połączenie wszystkich Podmiotów wymienionych w **załączniku nr 2a** do umowy (wykaz lokalizacji dostaw i instalacji urządzeń dla poszczególnych Odbiorców) poprzez sieć SD-WAN przy wykorzystaniu istniejącej infrastruktury technicznej i jej rozbudowa o kolejne moduły sprzętowe.

Wymagania stawiane sieci SD-WAN:

- Wysoka dostępność i niezawodność połączeń,
- Zaawansowane mechanizmy zabezpieczeń tj. m.in. szyfrowanie, firewall, IDS/IPS,
- Możliwość centralnego zarządzania i monitorowania sieci,
- Kompatybilność z obecnymi systemami teleinformatycznymi KG PSP,
- Elastyczność w konfiguracji połączeń zależnie od aktualnych potrzeb operacyjnych.
- Projekt ten jest niezbędny dla zwiększenia efektywności operacyjnej i bezpieczeństwa w działaniach Państwowej Straży Pożarnej.

W ramach wskazanych Podmiotów (załącznik nr 2a) zakłada się budowę 3 poziomów węzłów komunikacyjnych:

- Centralnych (CWK), obsługiwanych przez urządzenia Typ nr 1,
- Pośrednich (PWK), obsługiwanych przez urządzenia Typ nr 2,
- Końcowych (KWK), obsługiwanych przez urządzenia Typ nr 4.

Przyjęty podział zakłada gradacje wymagań wydajnościowych i funkcjonalnych dla sprzętu i oprogramowania w zależności od ustalonego przydziału wynikającego z **załącznika nr 4 do umowy** (wykaz ilościowy urządzeń przeznaczonych dla poszczególnych Odbiorców). Zamawiający wymaga dostawy i wdrożenia sprzętu i oprogramowania spełniającego niżej wymienione wymagania techniczne. Oferent jest zobowiązany dołączyć do oferty niezbędne dane informacyjne, dane katalogowe (w j. polskim lub j. angielskim), z których będzie wynikać, że oferowane rozwiązanie jest zgodne z wymaganiami technicznymi (linki do stron materiałów publikowanych przez producentów sprzętu). Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na rynek europejski i musi być objęta serwisem oraz wsparciem przez okres minimum 60 miesięcy od daty dostawy. Całość dostarczanego sprzętu musi być nowa i nieużywana we wcześniejszych projektach (nie dopuszcza się zastosowania urządzeń tzw. Refurbished).

Na cały okres wdrożenia ze strony Zamawiającego oraz Wykonawcy zostaną wyznaczone osoby, pełniące rolę Koordynatorów wdrożenia, odpowiedzialne za kontakty i ustalania pomiędzy Zamawiającym, a Wykonawcą. Dane kontaktowe przedstawicieli poszczególnych Odbiorców umowy- koordynatorów zostaną przekazane na etapie realizacji przedmiotu umowy.

Zakres zamówienia obejmuje:

- Implementację ogólnokrajowej sieci SD-WAN,
- Dostarczenie niezbędnego sprzętu i oprogramowania na poziomie Komendy Głównej PSP, komend wojewódzkich PSP, komend powiatowych/miejskich PSP w tym JRG oraz posterunków JRG, jak również szkół PSP i ośrodków szkolenia PSP.
- Integrację z istniejącą infrastrukturą IT PSP,
- Zapewnienie wsparcia technicznego i serwisu.

Dostarczone urządzenia muszą być w pełni kompatybilne z urządzeniami Zamawiającego, w tym z systemem zarządzania, tak aby można było zaimplementować polityki bezpieczeństwa oraz konfigurację polityk routingu na dostarczone urządzenia bez konieczności ich modyfikacji. Kompatybilność musi obejmować obszary, takie jak:

- kompatybilność sprzętowa: zgodność na poziomie fizycznym, w tym złącza, interfejsy i protokoły komunikacyjne.
- kompatybilność programowa: zgodność z systemami operacyjnymi, oprogramowaniem zarządzającym oraz politykami bezpieczeństwa.
- kompatybilność operacyjna: możliwość implementacji polityk bezpieczeństwa i routingu bez konieczności modyfikacji dostarczonych urządzeń.

W przypadku dostawy rozwiązania innego niż funkcjonujące u Zamawiającego, Wykonawca dodatkowo, na własny koszt, dostarczy, skonfiguruje i wdroży równoważne rozwiązanie oparte na urządzeniach pracujących jako para wysokiej dostępności (HA) w trybach Active/Standby i Active/Active, wyposażone w system centralnego zarządzania i monitorowania NG Firewall.

Rozwiązanie to musi obejmować:

- odpowiednią ilość licencji i oprogramowania, przeniesienie i implementację wszystkich polityk i konfiguracji z pełnym odwzorowaniem funkcjonalności i bezpieczeństwa,
- zapewnić serwis gwarancyjny oraz wsparcie na okres co najmniej 60 miesięcy,
- zapewnić pełne wsparcie techniczne przez okres 60 miesięcy w trybie 24/7/365 z czasem reakcji do 2 godzin od zgłoszenia oraz maksymalnie 6 godzin na usunięcie awarii dla całego dostarczonego rozwiązania opisanego w niniejszym postępowaniu,
- zapewnić certyfikowane szkolenia dla personelu Zamawiającego wraz ze wsparciem technicznym opisanym poniżej z uwagi na doświadczenie i samodzielne utrzymanie systemu przez personel Zamawiającego.

Rozwiązanie funkcjonujące u Zamawiającego zawiera m.in.:

- klaster dwóch urządzeń firewall nowej generacji Palo Alto PA 1420 wraz z pakietem subskrypcji Core Security: zaawansowane zapobieganie zagrożeniom, zaawansowane filtrowanie adresów URL, zaawansowany Wildfire, zabezpieczenia DNS i SD-WAN (PAN-PA-1420-BND-CORESEC-5YR) na okres 60 miesięcy,
- wsparcie premium (PAN-SVC-BKLN-1420-5YR) na okres 60 miesięcy,

- oprogramowanie do centralnego zarządzania Panorama dla 100 urządzeń (PAN-PRA-100) ze wsparciem na okres 60 miesięcy,
- licencje na wirtualne systemy (10 szt.) dla 2 urządzeń,
- subskrypcje GlobalProtect z funkcją HIP (dla 2000 urządzeń końcowych) dla 2 urządzeń Palo Alto PA- 1420 pracujących w klastrze HA na okres 60 miesięcy.

Zamówienie obejmuje dostawę urządzeń infrastruktury sieci SD-WAN zgodnie z poniższą specyfikacją. W przypadku wskazania znaków towarowych, patentów lub pochodzenia, Zamawiający dopuszcza składanie ofert równoważnych, pod warunkiem że oferowane urządzenia spełniają minimalne wymagania określone w opisie przedmiotu zamówienia.
Wszelkie odwołania do znaków towarowych, patentów, pochodzenia lub konkretnych modeli urządzeń mają charakter informacyjny i nie mają na celu celem ograniczenia konkurencji. Zamawiający dopuszcza oferty równoważne, które spełniają powyższe wymagania i zapewniają osiągnięcie tych samych celów funkcjonalnych i jakościowych.

Opis Techniczny:

Pkt 1. Ogólne wymagania na sprzęt i oprogramowanie urządzeń brzegowych typu NG Firewall.

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

4. Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45, w co najmniej jeden dedykowany port zarządzający realizowany jako port Ethernet 10/100/1000 lub jako port SFP z wkładką 1000BASE-T.
5. Urządzenia muszą być wyposażone w minimum 2 zasilacze AC 230V pracujące redundantnie.
6. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia (tzw. Hot Plug).
7. 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 cores) do obu z funkcji lub alternatywnie za pomocą oddzielnych dedykowanych procesorów (tzw. CPU) dla każdej z funkcji.
8. 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.
9. Urządzenia firewall muszą wspierać protokół LACP.
10. 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).
11. 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.

12. Polityka zabezpieczeń firewall musi uwzględniać
    a. adresy IP źródłowe i docelowe,
    b. protokoły i usługi sieciowe,
    c. aplikacje,
    d. kategorie URL,
    e. użytkowników aplikacji i grupy,
    f. reakcje zabezpieczeń,
    g. logowanie zdarzeń (początek i koniec sesji)
    h. strefa wejściowa i wyjściowa
13. 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 4200 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP i HTTPS oraz z aplikacjami przemysłowymi (tzw. ICS/OT).
14. Urządzenia muszą pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia (bez użycia zewnętrznych narzędzi).
15. 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.
16. 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.
17. 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 20 administratorów dla wszystkich oferowanych urządzeń.
18. 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.
19. 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.
20. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
    a. Microsoft Active Directory,

b. Microsoft Exchange,
c. Terminal Services,
d. Syslog,
e. Cisco ISE,
f. Wykorzystywać posiadaną funkcję Captive Portal,
g. Wykorzystywać posiadaną funkcję API,
h. Integracja z Aruba ClearPass (informacja o zautoryzowanym użytkowniku, nazwie hosta, jego IP),

21. 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.
22. Urządzenia firewall muszą pozwalać na lokalne zbieranie (na dysk/nośnik 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.
23. 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 zakresu czasu.
24. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
b. API
25. 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. Pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można następnie wykorzystywać w polityce bezpieczeństwa urządzeń.
26. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.
27. 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.
28. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

29. 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.
30. 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.
31. Urządzenia firewall muszą obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
32. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji - rozdzielny od polityk bezpieczeństwa.
33. 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.
34. Wykonywanie operacji deszyfrowanie 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.
35. Wykonywanie operacji deszyfrowania 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).
36. Urządzenie firewall musi posiada 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.
37. 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.
38. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości sesji w odniesieniu do źródłowego lub docelowego adresu IP.
39. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) dla aplikacji i użytkowników.
40. 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).
41. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.

42. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
43. Urządzenia firewall muszą zapewniać inspekcję komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu blokowania tuneli SSH.
44. Urządzenie firewall muszą obsługiwać Post-Quantum Crypto dla IKE2 zgodnie z RFC 8784.
45. Urządzenia firewall muszą obsługiwać funkcję DNS proxy.
46. 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 wspieraną ilość dla oferowanego modelu urządzeń.
47. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.
48. Urządzenia firewall dla zdalnego dostępu VPN muszą umożliwiać następujące funkcjonalności:
    a. Dostępność oprogramowania klienta VPN dla stacji/laptopów dla następujących systemów operacyjnych: Windows 7/8.1/10/11; MacOS od 10.11 do 14.
    b. Jeżeli rozwiązanie danego producenta przewiduje oddzielne wsparcie serwisowe na klienta VPN, należy takie wsparcie przewidzieć na taki sam okres jak wsparcie dla urządzeń dla maksymalnej ilości wspieranych połączeń klienckich VPN dla każdego z urządzeń.
49. Producent oferowanego rozwiązania musi być obecny w najnowszym rynkowym raporcie „Gartner Magic Quadrant for SD-WAN”.
50. Dostarczane razem z urządzeniami subskrypcje, licencje, gwarancje muszą funkcjonować 60 miesięcy.
51. Wszystkie dostępne porty dostarczonych urządzeń i ich przepustowość, dostępność, aktywacja nie mogą być ograniczane poprzez dodatkowe licencje, subskrypcje.

Pkt 2. Wymagania precyzujące sprzęt i oprogramowanie ze względu na wydajność, rodzaj i ilość portów wej./wyj.:

Pkt 2.1. Wymagania dodatkowe dla urządzeń Typ nr 1 – 4 sztuki (2 pary HA) (urządzenia obsługujące Centralne Węzły Komunikacyjne (CWK)).
Należy dostarczyć 4 szt. urządzeń, które będą pracowały jako 2 pary w różnych lokalizacjach geograficznych w układzie HA.
Razem z urządzeniami muszą zostać dostarczone następujące typy i ilości modułów połączeniowych. Ilość dla zestawu 2 urządzeń tj. jedna para HA:
1. Na potrzeby połączeń HA: 2 szt. SFP+ 10GE wariant SR + 2 szt. QSFP+ 40GE kabel AOC

2. Do LAN: 8 szt. SFP+ 10GE wariant SR lub inne.

- Wkładki światłowodowe oryginalne producenta urządzeń

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

1. Urządzenie musi być wyposażone w minimum:
   a. minimum 12 portów Ethernet RJ45 wspierających 10G/5G/2.5G/1GE/100Mbps;
   b. minimum 10 portów Ethernet SFP+ (akceptujących moduły 10GE SFP+ oraz 1GE SFP);
   c. minimum 4 porty Ethernet SFP28 (akceptujących moduły 25G SFP28 oraz 10GE SFP+ oraz 1GE SFP);
   d. minimum 2 porty Ethernet QSFP+/QSFP28 (akceptujących moduły 40GE QSFP+ oraz 100GE QSFP28);
   e. minimum 1 port dla celów połączenia urządzeń w HA: minimum 1x 10GE SFP+ (lub szybszy) oraz minimum 2x 1GE (SFP lub RJ45) (lub szybszy). Porty te muszą być traktowane jako dodatkowe względem wymaganych powyżej. Nie dopuszcza się liczenia jako HA, portów wymaganych wcześniej.
2. Musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 450 GB na potrzeby systemu operacyjnego i logów.
3. W przypadku procedury wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby zasób dyskowy zostały wymontowany z urządzenia i pozostał w jego siedzibie w celu bezpiecznej utylizacji.
4. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
   a. Minimum 33 Gbps dla rozpoznawania i kontroli aplikacji,
   b. Minimum 17 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Antywirus, Antyspyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia.
   c. Minimum 13 Gbps wydajności IPSec VPN.
   d. Minimum 250 000 nowych sesji na sekundę.
   e. Minimum 2,8M równoległych sesji
   f. Minimum 2000 tuneli klienckich VPN
   g. Minimum 4000 sąsiedztw IKE (IPSec)
5. Musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń.
6. Musi obsługiwać nie mniej niż 10 wirtualnych kontekstów urządzenia (kontekst rozumiany jako logiczna, niezależna, oddzielnie zarządzana zapora ogniowa wydzielona wewnątrz urządzenia).
7. Musi umożliwiać zdefiniowanie nie mniej niż 10 000 reguł polityki bezpieczeństwa oraz 3 000 reguł NAT.
8. Musi umożliwiać tworzenia nazwanych stref bezpieczeństwa np. DMZ, LAN, WAN w ilości minimum 200.

9. Urządzenie musi być wyposażone w minimum 2 zasilacze typu AC 230V pracujące redundantnie. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.
10. Urządzenie musi być przeznaczone do montażu w szafie Rack 19”.
11. 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.
12. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur oraz powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.
13. Urządzenie musi posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.
14. 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 32h) i pochodzić od tego samego producenta co firewall.
15. Urządzenie musi posiadać funkcję anty-spyware. Baza sygnatur musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.
16. Urządzenie musi posiadać funkcję filtrowania URL.
17. Urządzenie musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (a nie tylko filtrującego) ruch w politykach bezpieczeństwa.
18. 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.
19. Wymagane jest posiadanie oddzielnych kategorii URL dla zagrożeń typu malware, phishing, C2C oraz dla ostatnio zarejestrowanych domen.
20. Ocena URL musi obejmować również określenie ryzyka do niego przypisanego (co najmniej wysokie/średnie/niskie).
21. Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania kategorii URL.
22. Urządzenie musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sandbox” (tego samego producenta) plików różnych typów (Windows Portable Executable (m.in. exe, dll), MacOS (MachO, DMG, PKG), Linux ELF, pdf, MS Office, JAR, APK, JS, VBS, PowerShell Script, HTA) w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez

złośliwy plik po zainstalowaniu na komputerze końcowym. Interwał aktualizacyjny to maksymalnie 2 godziny.

23. Administrator musi mieć możliwość konfiguracji jakiego rodzaju typy plików z listy wspieranych przez funkcję Sandbox zostaną wysłane do skanowania przez „Sandbox".

24. Musi istnieć możliwość wysyłania plików do systemu Sandbox w chmurze obliczeniowej producenta oraz do fizycznych (lokalnych) urządzeń Sandbox gdyby takie zostały zainstalowane w przyszłości w sieci Zamawiającego.

25. Zewnętrzny sandbox producenta musi być zlokalizowany w Polsce. W przypadku braku dostępności polskiej lokalizacji takiego systemu należy dostarczyć lokalne urządzenia typu sandbox do zainstalowania w sieci Zamawiającego w ilości odpowiadającej ilości urządzeń NG Firewall zawartych w ofercie.

26. Urządzenie musi wykrywać i blokować zagrożenia DNS w ruchu przechodzącym przez urządzenie bez potrzeby rekonfiguracji serwera DNS i bez potrzeby ustawiania firewall jako serwera DNS. Wykrywający i blokujący ruch do domen uznanych za złośliwe musi być sterowany (przekierowanie) za pomocą funkcji DNS Sinkholing.

27. Urządzenia muszą posiadać ciągły (on-line) dostęp do centralnego repozytorium zagrożeń DNS, który będzie wykorzystywany w procesie decyzyjnym ochrony DNS.

28. Urządzenie musi zabezpieczać działania protokołu DNS poprzez procesowanie zapytań DNS w celu wykrywania i blokowania:

a. wykrywanie domen dynamicznych Dynamic DNS;
b. wykrywanie zapytań do domen złośliwych;
c. wykrywanie domen generowanych przez algorytmy DGA;
d. wykrywanie tunelowania złośliwej komunikacji w protokole DNS;
e. wykrywanie DNS Exfiltration or DNS Inflitration;

29. Urządzenia firewall dla zdalnego dostępu VPN muszą dodatkowo umożliwiać następujące funkcjonalności:

a. Realizacja VPN dla aplikacji HTML/HTML5 w trybie przeglądarkowym (tzw. Clientless VPN)
b. Zestawianie zdalnego dostępu dla urządzeń mobilnych tzw. smart devices. Telefony/tablety bazujące na systemach operacyjnych: Apple iOS i Google Android.
c. Dostępność oprogramowania klienta VPN dla stacji/laptopów dla następujących systemów operacyjnych: Windows 10 UWP; iOS 10-17; Google Android 6-14; Linux CentOS, RHEL, Ubuntu;
d. Sprawdzanie informacji o systemie operacyjnym, aktualizacji poprawek OS, aktualizacji oprogramowania antywirusowego itp. (dla systemów PC z Windows).
e. Sprawdzanie obecności konta urządzenia w systemie katalogowym Windows AD dla systemów PC z Windows.

f. Możliwość pomijania tunelu zdalnego dostępu VPN dla specyficznych aplikacji, domeny DNS, aplikacji video. Dla podłączających się stacji/laptopów Windows i MacOS.
g. 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.

Pkt 2.2. Wymagania dodatkowe dla urządzeń Typ nr 2 – 32 sztuki (16 par HA) (urządzenia obsługujące Pośrednie Węzły Komunikacyjne (PWK)).

Należy dostarczyć 32 szt. urządzeń, które będą pracowały jako 16 par w układzie HA.

Razem z urządzeniami muszą zostać dostarczone następujące typy i ilości modułów połączeniowych. Ilość dla zestawu 2 urządzeń tj. 1 pary HA:
1. Na potrzeby połączeń HA: 2 szt. SFP+ 10GE wariant SR
2. Do LAN: 8 szt. SFP+ 10GE wariant SR lub SFP/1GE inne warianty.

Każde z urządzeń musi (poza wymaganiami wspólnymi), spełniać dodatkowo wymagania:
1. Urządzenie musi być wyposażone w minimum:
   a. minimum 4 portów Ethernet RJ45 wspierających 1GE/100Mbps;
   b. minimum 8 portów Ethernet RJ45 wspierających 5G/2.5G/1GE/100Mbps;
   c. minimum 2 porty Ethernet SFP (akceptujących moduły 1GE SFP);
   d. minimum 8 portów Ethernet SFP+ (akceptujących moduły 10GE SFP+ oraz 1GE SFP);
   e. minimum 1 port dla celów połączenia urządzeń w HA: minimum 1x 10GE SFP+ (lub szybszy) oraz minimum 2x 1GE (SFP lub RJ45) (lub szybszy). Porty te muszą być traktowane jako dodatkowe względem wymaganych powyżej. Nie dopuszcza się liczenia jako HA, portów wymaganych wcześniej.
2. Musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 220 GB na potrzeby systemu operacyjnego i logów.
3. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
   a. Minimum 9 Gbps dla rozpoznawania i kontroli aplikacji,
   b. Minimum 5,5 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Antywirus, Antyspyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia.
   c. Minimum 6 Gbps wydajności IPSec VPN.
   d. Minimum 120 000 nowych sesji na sekundę.
   e. Minimum 1,2M równoległych sesji
   f. Minimum 1500 tuneli klienckich VPN

g. Minimum 2500 sąsiedztw IKE (IPSec)

4. Musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń.
5. Musi obsługiwać nie mniej niż 6 wirtualnych kontekstów urządzenia (kontekst rozumiany jako logiczna, niezależna, oddzielnie zarządzana zapora ogniowa wydzielona wewnątrz urządzenia).
6. Musi umożliwiać zdefiniowanie nie mniej niż 4500 reguł polityki bezpieczeństwa oraz 3 000 reguł NAT.
7. Musi umożliwiać tworzenia nazwanych stref bezpieczeństwa np. DMZ, LAN, WAN w ilości minimum 50.
8. Urządzenie musi być wyposażone w minimum 2 zasilacze typu AC 230V pracujące redundantnie. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.
9. Urządzenie musi być przeznaczone do montażu w szafie Rack 19”.
10. Urządzenie musi pozwalać na budowanie sieci w modelu SD-WAN (Software-Defined Wide Area Network) z wykorzystaniem wielu interfejsów/łączy tworząc dynamicznie sterowaną i inteligentną szyfrowaną sieć WAN. Do usługi SD-WAN musi umożliwiać monitorowanie parametrów jakości łącza (opóźnienie, zmienność opóźnienia, utrata pakietów) oraz umożliwiać rozkładanie ruchu i kierowanie wybranych aplikacji na wybrane łącza.

Pkt 2.3. Wymagania dodatkowe dla urządzeń Typ nr 3 – 3 sztuki. (urządzenia obsługujące Węzły VPN).
Należy dostarczyć 3 szt. urządzenia.
Każde z urządzeń musi (poza wymaganiami wspólnymi), spełniać dodatkowo wymagania:

1. Urządzenie musi być wyposażone w minimum:
   a. minimum 8 portów Ethernet RJ45 wspierających 1GE/100Mbps/10Mbps;
2. Musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 120 GB na potrzeby systemu operacyjnego i logów.
3. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
   a. Minimum 4 Gbps dla rozpoznawania i kontroli aplikacji,
   b. Minimum 2 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Antywirus, Antyspyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia.
   c. Minimum 2,5 Gbps wydajności IPSec VPN.
   d. Minimum 60 000 nowych sesji na sekundę.
   e. Minimum 0,35M równoległych sesji
   f. Minimum 1400 tuneli klienckich VPN
   g. Minimum 2400 sąsiedztw IKE (IPSec)

4. Musi obsługiwać nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń.
5. Musi obsługiwać nie mniej niż 5 wirtualnych kontekstów urządzenia (kontekst rozumiany jako logiczna, niezależna, oddzielnie zarządzana zapora ogniowa wydzielona wewnątrz urządzenia).
6. Musi umożliwiać zdefiniowanie nie mniej niż 2200 reguł polityki bezpieczeństwa oraz 2400 reguł NAT.
7. Musi umożliwiać tworzenia nazwanych stref bezpieczeństwa np. DMZ, LAN, WAN w ilości minimum 100.
8. Urządzenie musi być wyposażone w minimum 2 zasilacze typu AC 230V pracujące redundantnie. Zasilacze muszą być wymienne/odłączalne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.
9. Urządzenie musi być zbudowane bez użycia wentylatorów (tzw. Fan-less design).
10. Urządzenia firewall dla zdalnego dostępu VPN muszą dodatkowo umożliwiać następujace funkcjonalności:

a. Realizacja VPN dla aplikacji HTML/HTML5 w trybie przeglądarkowym (tzw. Clientless VPN)
b. Zestawianie zdalnego dostępu dla urządzeń mobilnych tzw. smart devices. Telefony/tablety bazujące na systemach operacyjnych: Apple iOS i Google Android.
c. Dostępność oprogramowania klienta VPN dla stacji/laptopów dla następujących systemów operacyjnych: Windows 10 UWP; iOS 10-17; Google Android 6-14; Linux CentOS, RHEL, Ubuntu;
d. Sprawdzanie informacji o systemie operacyjnym, aktualizacji poprawek OS, aktualizacji oprogramowania antywirusowego itp. (dla systemów PC z Windows).
e. Sprawdzanie obecności konta urządzenia w systemie katalogowym Windows AD dla systemów PC z Windows.
f. Możliwość pomijania tunelu zdalnego dostępu VPN dla specyficznych aplikacji, domeny DNS, aplikacji video. Dla podłączających się stacji/laptopów Windows i MacOS.
g. 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.

Pkt 2.4. Wymagania dodatkowe dla urządzeń Typ nr 4 – 533 sztuk (urządzenia obsługujące Końcowe Węzły Komunikacyjne (KWK)).
Należy dostarczyć 533 szt. urządzeń.
Każde z urządzeń musi (poza wymaganiami wspólnymi), spełniać dodatkowo wymagania:

1. Urządzenie musi być wyposażone w minimum:
    a. minimum 8 portów Ethernet RJ45 wspierających 1GE/100Mbps;

2. Musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 120 GB na potrzeby systemu operacyjnego i logów.
3. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
   a. Minimum 2,2 Gbps dla rozpoznawania i kontroli aplikacji,
   b. Minimum 1 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: blokowanie typów plików, z włączonym logowaniem na dysk urządzenia.
   c. Minimum 1 Gbps wydajności IPSec VPN.
   d. Minimum 30 000 nowych sesji na sekundę.
   e. Minimum 180 000 równoległych sesji
   f. Minimum 900 tuneli klienckich VPN
   g. Minimum 2400 sąsiedztw IKE (IPSec)
4. Musi obsługiwać nie mniej niż 3 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń.
5. Musi obsługiwać nie mniej niż 2 wirtualnych kontekstów urządzenia (kontekst rozumiany jako logiczna, niezależna, oddzielnie zarządzana zapora ogniowa wydzielona wewnątrz urządzenia).
6. Musi umożliwiać zdefiniowanie nie mniej niż 2200 reguł polityki bezpieczeństwa oraz 2200 reguł NAT.
7. Musi umożliwiać tworzenia nazwanych stref bezpieczeństwa np. DMZ, LAN, WAN w ilości minimum 100.
8. Urządzenie posiadać minimum 2 zasilacze typu AC 230V pracujące redundantnie. Zasilacze muszą być wymienne/odłączalne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.
9. Urządzenie musi być zbudowane bez użycia wentylatorów (tzw. Fan-less design).
10. Urządzenie musi pozwalać na budowanie sieci w modelu SD-WAN (Software-Defined Wide Area Network) z wykorzystaniem wielu interfejsów/łączy tworząc dynamicznie sterowaną i inteligentną szyfrowaną sieć WAN. Do usługi SD-WAN musi umożliwiać monitorowanie parametrów jakości łącza (opóźnienie, zmienność opóźnienia, utrata pakietów) oraz umożliwiać rozkładanie ruchu i kierowanie wybranych aplikacji na wybrane łącza.

Pkt 2.5. Wymagania dodatkowe dla urządzeń Typ nr 5 – 33 sztuki (urządzenia zapasowe dla Końcowe Węzły Komunikacyjne (KWK)).
Należy dostarczyć 33 szt. urządzeń.

Każde z urządzeń musi (poza wymaganiami wspólnymi), spełniać dodatkowo wymagania:
1. Urządzenie musi być wyposażone w minimum:
   a. minimum 8 portów Ethernet RJ45 wspierających 1GE/100Mbps;

2. Musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 120 GB na potrzeby systemu operacyjnego i logów.
3. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
   a. Minimum 2,2 Gbps dla rozpoznawania i kontroli aplikacji,
   b. Minimum 1 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: blokowanie typów plików, z włączonym logowaniem na dysk urządzenia.
   c. Minimum 1 Gbps wydajności IPSec VPN.
   d. Minimum 30 000 nowych sesji na sekundę.
   e. Minimum 180 000 równoległych sesji
   f. Minimum 900 tuneli klienckich VPN
   g. Minimum 2400 sąsiedztw IKE (IPSec)
4. Musi obsługiwać nie mniej niż 3 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń.
5. Musi obsługiwać nie mniej niż 2 wirtualnych kontekstów urządzenia (kontekst rozumiany jako logiczna, niezależna, oddzielnie zarządzana zapora ogniowa wydzielona wewnątrz urządzenia).
6. Musi umożliwiać zdefiniowanie nie mniej niż 2200 reguł polityki bezpieczeństwa oraz 2200 reguł NAT.
7. Musi umożliwiać tworzenia nazwanych stref bezpieczeństwa np. DMZ, LAN, WAN w ilości minimum 100.
8. Urządzenie posiadać minimum 2 zasilacze typu AC 230V pracujące redundantnie. Zasilacze muszą być wymienne/odłączalne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.
9. Urządzenie musi być zbudowane bez użycia wentylatorów (tzw. Fan-less design).
10. Urządzenie musi pozwalać na budowanie sieci w modelu SD-WAN (Software-Defined Wide Area Network) z wykorzystaniem wielu interfejsów/łączy tworząc dynamicznie sterowaną i inteligentną szyfrowaną sieć WAN. Do usługi SD-WAN musi umożliwiać monitorowanie parametrów jakości łącza (opóźnienie, zmienność opóźnienia, utrata pakietów) oraz umożliwiać rozkładanie ruchu i kierowanie wybranych aplikacji na wybrane łącza.

Pkt 3. System Centralnego Zarządzanie i Monitorowania NG Firewall i SD-WAN.

1. Zamawiający oczekuje dostarczenia systemu zarządzania i monitorowania zrealizowanego w modelu redundancji zbieranych logów oraz z możliwością dokupienia w przyszłości redundancji HA (zapasowej instancji) dla modułu funkcji zarządzania.
2. Należy dostarczyć centralny, zunifikowany system zarządzania, logowania zdarzeń i raportowania pochodzący od tego samego producenta co dostarczone urządzenia NG Firewall.

3. System ten ma być realizowany w postaci dodania do już działającego w KG PSP systemu Panorama Firmy Paloaltonetworks tj. oprogramowania serwerów wirtualnych (tzn. dedykowanego VM Appliance a nie system operacyjny ogólnego przeznaczenia) kompatybilnej co najmniej z VMware ESX, Hyper-V, KVM oraz umożliwiać zarządzanie co najmniej 1000 urządzeń NG Firewall sprzętowymi pochodzącymi od tego samego producenta.
Zamawiający zapewni potrzebne zasoby serwerowe, dyskowe dla realizacji systemu zarządzania i monitorowania.
4. System ma pełnić rolę systemu logowania dla zarządzanych firewalli i systemu centralnego raportowania. W tym celu moduły odpowiedzialne za zbieranie logów muszą zostać zrealizowane z wykorzystaniem protokół konsensusu posiadającego mocne gwarancje spójności (tzw. consensus protocol). Każdy z węzłów musi obsługiwać przestrzeń dyskową o pojemności nie mniejszej niż 22 TB oraz minimum 20 000 logów na sekundę.
5. System musi posiadać zunifikowany, wspólny graficzny interfejs użytkownika (tzw. GUI) i być zgodny z indywidualnym interfejsem zarządzania NG firewall.
6. System musi pozwalać na przełączenie się w kontekst pojedynczego firewalla lub logicznego systemu na firewallu z poziomu centralnej konsoli zarządzającej.
7. System musi umożliwiać import obecnej konfiguracji używanej przez firewalle.
8. System musi umożliwiać zbieranie logów zdarzeń z firewalli. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
9. System musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli. Musi również oferować łatwe przeszukiwanie skorelowanych logów zebranych z zarządzanych firewalli.
10. Musi być możliwe tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych.
11. System musi umożliwiać tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego. Musi istnieć możliwość zapisania stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.
12. System musi umożliwiać tworzenie dynamicznych raportów w czasie rzeczywistym dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down” (pozyskiwania coraz większej ilości informacji o danym zdarzeniu).
13. System musi umożliwiać centralne budowanie i dystrybucję polityk bezpieczeństwa o zasięgu zarówno Lokalnym (dla wybranych firewalli lub logicznych systemów firewalla) jak i Globalnym (dla grup firewalli lub kilku systemów logicznych wybranych firewalli).
14. System musi umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów).

15. System musi umożliwiać tworzenie raportów na podstawie zbudowanych logicznych kontenerów.
16. System musi umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium.
17. System musi umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi. Przy tworzeniu obiektów musi być możliwość określenia ich zasięgu (lokalne, globalne).
18. System musi umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych.
19. System musi umożliwiać dystrybucję i zdalną instalację nowych sygnatur ataków, nowych wersji systemu oraz poprawek do niego.
20. Musi umożliwiać konwersję sygnatur IPS, co pozwala na zautomatyzowane przekształcanie reguł innych firm IPS, takich jak Snort lub Suricata, w niestandardowe sygnatury zagrożeń sieciowych. Te sygnatury będą następnie rejestrowane i implementowane w zgrupowanych firewallach w profilach zabezpieczeń, ochrony przed lukami w zabezpieczeniach oraz ochrony przed programami szpiegującymi.
21. System musi umożliwiać tworzenie kopii zapasowych zarządzanych firewalli
22. Musi być możliwość przesłania kopii zapasowych na zewnętrzny zasób za pomocą protokołów FTP lub SCP.
23. System musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego firewalla lub grupy firewalli/logicznych systemów na firewallach.
24. System musi informować o zmianach konfiguracji systemu.
25. System musi umożliwiać audytowanie/sprawdzanie poprawności konfiguracji firewalla przed jej zatwierdzeniem.
26. System musi umożliwiać zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów.
27. System musi umożliwiać wykonanie procedury wymiany uszkodzonego firewalla na nowy tak, aby system zarządzania, logowania i raportowania rozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone.
28. System musi umożliwiać rozbudowę konfiguracji w przyszłości do wysokiej dostępności w trybie Active-Passive (dwóch maszyn wirtualnych). Synchronizacja konfiguracji między węzłami HA (High Availability) musi być szyfrowana.
29. Taki w przyszłości uruchomiony układ HA w przypadku awarii jednego z nodów, musi zapobiegać zarówno utracie kontroli nad funkcjami zarządzania firewallami jak również utracie logów przesyłanych z podłączonych urządzeń.
30. System musi oferować funkcję automatycznego przywracania konfiguracji, w przypadku utraty łączności między firewallem a centralnym systemem zarządzania wskutek błędnej zmiany polityki bezpieczeństwa i jej rozpropagowania do zarządzanych firewalli.

Pkt. 4. Warunki gwarancji i wdrożenia

Wszystkie wymagane, oferowane funkcjonalności muszą być dostępne lub/i licencjonowane i mieć gwarancje na okres minimum 60 miesięcy.

Prowadzone prace wdrożeniowe i instalacyjne nie mogą zakłócać prawidłowej pracy istniejącej sieci. Wszystkie konieczne przerwy w pracy systemu muszą być zgłoszone najpóźniej na 24 godziny przed planowaną przerwą i powinny mieć miejsce poza godzinami pracy (tj. poza 7:30-16:15 w dni robocze od poniedziałku do piątku).

W trakcie realizacji przedmiotu umowy Wykonawca przeprowadzi szkolenia zgodne z zakresem producenta dostarczonego rozwiązania dla wyznaczonych pracowników Zamawiającego (cztery osoby) w zakresie administracji, zarządzania i użytkowania w wymiarze min. 40 godzin. Minimalny zakres szkoleń będzie obejmował:

- Szkolenie z zakresu VPN, Routingu,
- Za awansowego zarządzania urządzeniami firewall,
- Szkolenie z zakresu rozwiązywania problemów,
- Szkolenie analizy, zapobiegania i wdrażania rozwiązań bezpieczeństwa w skali przedsiębiorstwa,
- Szkolenia z automatyzacji i orchiestracji konfiguracji,
- Szkolenie z projektowania i działania sieci SD-WAN.

Usługa konfiguracji i instalacji będzie obejmowała dostawę i instalację urządzeń we wskazanych lokalizacjach zgodnie z infrastrukturą sieci i adresacją przygotowaną przez Zamawiającego (zostanie przekazana Wykonawcy w początkowym etapie wdrożenia).

Dostawa i podłączenie wstępnie skonfigurowanego sprzętu do wymaganych lokalizacji zgodnie z harmonogramem i listą dostaw (załącznik nr 5 do umowy)

Wstępna konfiguracja obejmuje:

- Dostawa sprzętu do wskazanej lokalizacji,
- Montaż w szafie rack,
- Konfiguracja portu zarządzania MGMT (ustawienie hasła, konfiguracja IP, konfiguracja trasy routingu, tak aby urządzenie było widoczne w systemie zarządzania
- Podpięcie urządzenia do systemu zarządzania.
- Wsparcie techniczne i pomoc w zakresie konfiguracji SD-WAN na urządzeniach dostarczonych.

Wsparcie i pomoc w zakresie konfiguracji styku LAN/WAN oraz implementacji polityk bezpieczeństwa z uwzględnieniem zabezpieczenia komunikacji ze wszystkich zainstalowanych urządzeń.

Ostateczne ustalenia z Zamawiającym dotyczące realizacji całego projektu zostaną opisane przez Wykonawcę w dokumencie projektowym (dokumentacja projektowa), który będzie zawierał szczegóły konfiguracyjne. Dokument zostanie następnie uzgodniony z Zamawiającym.

Wykonawca/cy po zakończeniu wdrożenia protokolarnie przekaże Zamawiającemu dokumentację powykonawczą konfiguracji dostarczonych i uruchomionych elementów systemu.

Wykonawca będzie świadczył wsparcie i pomoc techniczną przez okres 60 miesięcy od momentu odbioru przedmiotu umowy w trybie 8/5/365. Zgłoszenia 24 godziny na dobę z czasem reakcji 6 godzin. Zgłoszenia po godzinie 15.00 z obsługą w następnym dniu roboczym.