Załącznik nr 1 do Zapytania ofertowego

Załącznik nr 1 do Umowy CeZ/…/2023

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Część I**

**Zakup urządzenia typu firewall (NGFW) Palo Alto Networks PA-1410 wraz usługą wsparcia**

**na okres 12 miesięcy**

## **Przedmiot zamówienia obejmuje:**

## Dostawę 1 sztuki fabrycznie nowego urządzenia Palo Alto Networks PA-1410, wraz z zainstalowanymi następującymi licencjami umożliwiającymi uruchomienie odpowiednich zabezpieczeń:

1. Core Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, DNS Security And SD-WAN) (PAN-PA-1410-BND-CORESEC),
2. GlobalProtect Subscription (PAN-PA-1410-GP).

## Usługę wsparcia świadczoną przez okres 12 miesięcy od daty podpisania protokołu odbioru.

## Gwarancję oraz rękojmię w rozumieniu kodeksu cywilnego na urządzenia wskazane w pkt 1.1. na okres 12 miesięcy od dnia podpisania Protokołu Odbioru wnioskującego o rozliczenie finansowe.

## Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego wymagania wskazane do Załączniku nr 1 do OPZ. W przypadku dostarczania urządzenia równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie przedmiotu zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane urządzenie spełnia wszystkie wymagania i warunki określone w Opisie przedmiotu zamówienia.

## **Termin realizacji:**

## Dostawa nastąpi w terminie do 30 dni kalendarzowych od daty podpisania umowy.

## **Usługa wsparcia:**

## W ramach świadczenia usługi wymagany jest:

## dostęp do strony pomocy technicznej producenta,

## dostęp do aktualizacji oprogramowania,

## dostęp do nowych wersji oprogramowania oraz poprawek,

## dostęp do nowych sygnatur bezpieczeństwa,

## dostęp do bazy wiedzy producenta.

## Usługa musi być świadczona w języku polskim przez producenta lub oficjalnego partnera producenta w zakresie świadczenia pomocy serwisowej.

## Usługa musi być świadczona przez okres 12 miesięcy.

3.4 W ramach świadczenia usługi, w przypadku wystąpienia awarii Zamawiający otrzyma część zamienną/urządzenie objęte gwarancją w trybie następnego dnia roboczego.

**Załącznik nr 1 do OPZ:**

## Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego wymagania w szczególności w zakresie:

1. funkcjonalności rozwiązania równoważnego, która nie może być gorsza od funkcjonalności urządzenia typu firewall (NGFW) wymienionego w pkt 1.1 OPZ.
2. rozwiązanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego,
3. rozwiązanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie i systemy informatyczne,
4. rozwiązanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność rozwiązania równoważnego z wyspecyfikowanym systemem,
5. rozwiązanie równoważne, musi być rozwiązaniem istniejącym na rynku co najmniej 5 lat, pochodzącym z oficjalnego kanału sprzedaży. Jako potwierdzenie spełnienia wymagania uznane będzie zakwalifikowanie oferowanego rozwiązania firewall (NGFW) w niezależnym opracowaniu firmy badawczej Gartner, dotyczącym rozwiązań klasy Network Firewalls w obszarze liderów (w raportach najbardziej aktualnych na dzień składania ofert).

## Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego następujące wymagania:

1. Urządzenie musi być specjalizowanym urządzeniem sieciowym (tzw. appliance) mogącym pracować jako pojedyncze urządzenie oraz jako para wysokiej dostępności (HA) w trybach Active/Passive, Active/Active.
2. Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta.
3. Urządzenie musi umożliwiać działanie w następujących trybach pracy:
4. routera (tzn. w warstwie 3 modelu OSI),
5. mostu (tzn. w warstwie 2 modelu OSI),
6. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych. Musi pracować w trybie przezroczystego łączenia interfejsów w pary),
7. w trybie pasywnego nasłuchu (sniffer/tap).
8. Urządzenie musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
9. Urządzenie firewall musi posiadać separację logiczną zasobów służących do przetwarzania ruchu od zasobów służących do zarządzania urządzeniem.
10. Urządzenie musi posiadać dedykowane zasoby/rdzenie procesora/procesorów do funkcji zarzadzania urządzeniem lub możliwości ustawienia dedykowanych zasobów/rdzeni procesora/procesorów do funkcji zarządzania urządzeniem.
11. Urządzenie firewall musi wspierać protokół Ethernet z obsługa sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod0interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.
12. Urządzenie firewall musi wspierać protokół LACP.
13. Urządzenie firewall musi zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
14. Urządzenie firewall musi działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowane na firewall są wskazane jako dozwolone.
15. Polityka zabezpieczeń firewall musi uwzględniać:
16. adresy IP źródłowe i docelowe,
17. protokoły i usługi sieciowe,
18. aplikacje,
19. kategorie URL,
20. użytkowników aplikacji i grupy,
21. reakcje zabezpieczeń,
22. logowanie zdarzeń (początek i koniec sesji),
23. strefa wejściowa i wyjściowa.
24. Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włączenie P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65535 dostępnych portach. Przy tym wydajność kontroli firewalla stanowego i kontroli aplikacji całego ruchu nie może być mniejsza, niż wskazano w wymaganiach wydajnościowych urządzenia.

Urządzenie musi wykrywać co najmniej 3700 predefiniowanych aplikacji wspieranych przez producenta (takich jak DNS over HTTPS, Telegram, Skype, Tor, BitTorrent, MQTT, Modbus, DNP3, Siemens S7) wraz z aplikacjami tunelującymi się w http lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.

1. Urządzenie firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: .pdf, .scr, .cpl, .dll, .ocx, .exe, .class, .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.
2. Urządzenie firewall musi być zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji dedykowanego oprogramowania/klienta na stacji administratora/administratorów w celu zarządzania systemem.
3. Urządzenie firewall musi być wyposażone w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowane stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub kontraktu serwisowego, należy dostarczyć odpowiedni dostęp dla minimum 30 administratorów.
4. Dostęp do urządzenia i zarządzanie siecią musi być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
5. Urządzenie firewall musi umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż:
6. baza lokalna,
7. serwer Radius,
8. serwer TACACS+,
9. serwer AD/LDAP.

Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH a dla dostępu GUI za pomocą certyfikatów kryptograficznych.

1. Urządzenie firewall musi zapewniać możliwość automatycznego i transparentnego ustalania tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
2. Active Sirectory,
3. Terminal Services.
4. Polityka kontroli dostępu (urządzenia 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, ustalenie tożsamości musi odbywać się również transparentnie.
5. Urządzenie firewall musi 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.
6. Urządzenie musi dostarczać predefiniowane przez producenta raporty standardowe jak i możliwość tworzenia raportów niestandardowych. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu.
7. Urządzenie musi pozwalać na zapisanie raportów na urządzeniu i uruchomiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
8. Urządzenie firewall musi umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczenia etykiet musi pozwalać na użycie:
9. reakcji na zdarzenie/log (np. wystąpienie zagrożenia),
10. API.
11. Urządzenie firewall musi posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMware ESX i VMware vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można potem wykorzystywać w polityce bezpieczeństwa urządzeń.
12. Urządzenie firewall musi obsługiwać protokoły routingu dynamicznego, minimum BGP i OSPF.
13. Urządzenie firewall musi obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komponentów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
14. Urządzenie firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielony od polityk bezpieczeństwa.
15. Wykonywanie operacji translacji adresów NAT musi być odnotowane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami NAT.
16. Urządzenie firewall musi pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju.
17. Urządzenie firewall musi obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
18. Urządzenie firewall musi posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa.
19. Wykonanie operacji deszyfrowania ruchu musi być odnotowane w logach urządzenia 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 wykluczenia z szyfrowania problematycznych stron na bazie tego logu.
20. Wykonanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL.
21. 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 oraz TLS\_CHACHA20\_POLY1305\_SHA256.
22. Urządzenie firewall musi posiadać funkcję ochrony przed atakami DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
23. Urządzenie firewall musi wspierać zarządzanie pasmem (QoS) i ustawiania dla aplikacji priorytetu oraz pasma.
24. Urządzenie firewall musi umożliwiać zestawienie zabezpieczonych kryptografią tuneli VPN w oparciu o standardy IPSeci IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. Routing-based VPN).
25. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14, 19, 20.
26. Dla IPSec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14, 19, 20.
27. Urządzenie firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tuneli SSH.
28. Wszystkie funkcjonalności muszą pochodzić od producenta. W przypadku gdy jakakolwiek funkcjonalność lub parametr ilościowy wymaga licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres 12 miesięcy od daty odbioru sprzętu.
29. Wsparcie serwisowe (techniczne) i gwarancja dla urządzenia firewall (zwana dalej wsparciem) będzie świadczone przez producenta lub autoryzowane przez producenta centrum serwisowe, niezależne od Wykonawcy, realizowane we współpracy z producentem, przez okres 12 miesięcy od daty odbioru sprzętu.
30. Funkcjonalność ochrony Antywirusowej (ale nie równoważną z Sandbox), anti-spyware i przed podatnościami systemów. Musi ona zapewniać co najmniej:

## wykrywanie aktywności sieci typu Botnet na podstawie analizy behawioralnej,

## sygnatury antywirusowe - wykrywanie wirusów i złośliwego oprogramowania znajdującego się w plikach wykonywalnych i typach plików,

## sygnatury anti-spyware - wykrywanie aktywności typu Command-and-Control (C2), gdzie oprogramowanie szpiegowskie na zainfekowanym kliencie zbiera dane bez zgody użytkownika i/lub komunikuje się ze zdalnym napastnikiem,

1. sygnatury podatności – wykrywanie podatności systemowych, które napastnik mógłby próbować wykorzystać,
2. sygnatury Command-and-Control (C2) dla ruchu DNS,
3. informacje o adresach IP złośliwych hostów,
4. informacje o adresach IP podejrzanych hostów (wysokiego ryzyka).
5. 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 (przekierowane) za pomocą funkcji DNS Sinkholing.
6. Urządzenie musi posiadać i być dostarczone z funkcjonalnością systemu wykrywania i zapobiegania włamaniom (Intrusion Prevention System – IPS) wraz z aktyualizacją sygnatur w okresie gwarancji. System musi działać w warstwie 7 modelu OSI. Baza sygnatur systemu wykrywania i zapobiegania włamaniom musi być przechowywana w urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł systemu wykrywania i zapobiegania włamaniom musi mieć możliwość wykluczenia z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji lub zdefiniowanych serwisów, np. poprzez numer portu, protokół transportowy.
7. Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak co najmniej http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur AV musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent urządzenia na którym realizowana jest ta funkcja. Moduł AV musi mieć możliwość wykluczenia z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji lub zdefiniowanych serwisów, np. poprzez numer portu, protokół transportowy.
8. Urządzenie musi zapewniać ochronę przed atakiem typu spyware. Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub IPS lub antymalware lub dedykowany silnik antyspyware. Baza sygnatur antyspyware musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik antyspyware musi mieć możliwość wykluczenia z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji bez względu na numery portów, na których działa.
9. Urządzenie musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
10. Urządzenie firewall musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sandbox” plików wykonywalnych PE i DLL przechodzących przez firewall. Systemy Sandbox, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików, adresów IP, DNS i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik. Maksymalny interwał aktualizacji sygnatury 48 godzin.
11. System zabezpieczeń firewall musi dodatkowo oferować możliwość identyfikacji w ruchu sieciowym i przesyłania do zintegrowanej usługi analizy dynamicznej (tzw. „Sandbox”) plików następujących typów: wykonywalnych (PE), Microsoft Office, Adobe flash/PDF, archiwa: JAR, RAR, 7-ZIP, Android APK, Mac OSX, skrypty: BAT, JScript, PowerShell, VBS, Perl i Python. W przypadku potwierdzenia nieznanego ataku (tzw. „Zero-Day”), musi następować automatyczna aktualizacja systemu firewall nowymi sygnaturami opisującymi wykryte pliki malware lub ich zidentyfikowane złośliwe zachowania (np. wzorce komunikacji zwrotnej) w wyniku przeprowadzonej analizy.
12. Uruchomienie ochrony typu „Sandbox” dla systemu zabezpieczeń firewall musi być możliwe w następujących trybach:

## Subskrybcji – bez dokupywania jakichkolwiek komponentów sprzętowych wyłącznie w oparciu o usługę chmurową producenta urządzenia firewall, uruchamianą na terenie EU,

1. Prywatnym – po zakupieniu dodatkowego urządzenia do analizy lokalnej, pochodzącego od producenta urządzenia firewall,
2. Hybrydowym – z wykorzystanie zarówno Subskrypcji i po zakupieniu urządzenia do analizy lokalnej.
3. W każdym z powyższych trybów, administrator systemu firewall musi mieć możliwość konfiguracji rodzaju pliku, kontekstu użytej aplikacji, kierunku transmisji (wysyłanie/odbieranie) i miejsca analizy (chmura/urządzenie lokalne) dla celów definicji ruchu i klasyfikacji obiektów do analizy typu „Sandbox”.
4. Urządzenie firewall musi posiadać możliwość wysyłania plików do analizy w usłudze chmurowej „Sandbox” pochodzącą od producenta urządzenia firewall.
5. Urządzenie musi obsługiwać funkcjonalność zdalnych sesji VPN z wykorzystaniem każdej z poniższych metod:
6. z wykorzystaniem aplikacji klienckich zainstalowanych na stacjach roboczych (ang. desktop clients),
7. z wykorzystaniem aplikacji na platformy mobilne (ang. mobile clients),
8. z wykorzystaniem przeglądarki internetowej bez konieczności instalacji klienta (ang. clientless access).
9. Oprogramowanie klienta VPN musi posiadać możliwość weryfikacji kondycji bezpieczeństwa stacji zdalnej Windows i macOS co najmniej w zakresie sprawdzenia:
10. czy zainstalowano oprogramowanie antywirusowe I czy posiada ono aktualne sygnatury,
11. czy włączony jest osobisty firewall,
12. czy computer jest komputerem w domenie Active Directory (dla Windows).
13. Oprogramowanie klienckie zdalnego dostępu musi posiadać bezpłatne wsparcie producenta w rozumieniu możliwości zakładania spraw serwisowych.
14. Rozwiązanie musi pozwalać na odseparowanie zdalnego komputera w przypadku stwierdzenia jego kompromitacji.
15. Urządzenie firewall musi posiadać funkcję filtrowania URL.
16. 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.
17. Rozwiązanie musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania kategorii URL.
18. Urządzenie firewall musi umożliwiać zabezpieczenie działania protokołu DNS poprzez procesowanie zapytań DNS w celu wykrywania i blokowania: zagrożeń, wycieku danych (exfiltracja).
19. System zabezpieczeń firewall musi być wyposażony w mechanizm automatycznego wyboru optymalnego trasowania WAN dla zdefiniowanej aplikacji, przy zapewnieniu jak maksymalnej wydajności, dostępności oraz bezpieczeństwa. Dla różnych technologii połaczeń fizycznych WAN (np. LTE, 5G, DSL, MPLS, WiFi itd.) zakończonych w standardzie Ethernet, musi być możliwość ich ciągłego monitorowana w zakresie: straty pakietów, opóźnienia oraz odchylenia (tzw. jitter) jako parametrów decyzyjnych do dynamicznego wyboru najkorzystniejszej trasy. Zintegrowana funkcjonalność SD-WAN, musi działać bezpośrednio na urządzeniu, w oparciu o system centralnego zarzadzania, bez konieczności dokupywania dodatkowych komponentów, poza subskrypcją.
20. System zabezpieczeń firewall musi posiadać osobny zestaw polityk SD-WAN, definiujący najkorzystniejszy sposób dystrybucji kluczowego ruchu firmowego, rozdzielny od polityk bezpieczeństwa. Pojedyncza reguła SD-WAN musi uwzględniać następujące atrybuty ruchu: strefy bezpieczeństwa, adresy IP źródłowe i docelowe, aplikacje, porty usług, wartości klasyfikatorów jakościowych łącz (opóźnienie, strata pakietów, jitter) oraz metody korekcji błędów.
21. Cechy urządzenia firewall:
22. Wysokość maksymalnie 1U wraz z zestawem montażowym do szafy RACK 19”,
23. Możliwość podłączenia redundantnego źródła zasilania,
24. 8 portów 10 Mbps / 100 Mbps / 1 Gbps Ethernet RJ45,
25. 4 porty 10 Mbps / 100 Mbps / 1 Gbps / 2,5 Gbps / 5 Gbps Ethernet RJ45 z możliwością obsługi PoE,
26. 6 portów Gigabit Ethernet SFP oraz 4 porty 1/10 Gigabit Ethernet SFP/SFP+ obsługujące moduły optyczne SR oraz LR,
27. 1 port 1/10 Gigabit Ethernet SFP/SFP+ oraz 2 porty 10 Mbps / 100 Mbps / 1 Gbps Ethernet RJ45 lub 2 porty Gigabit Ethernet SFP dedykowane do obsługi HA.
28. Rozwiązanie musi być wyposażone w co najmniej jeden port konsoli szeregowej RJ45, w co najmniej jeden dedykowany port zarządzający realizowany jako port 10 Mbps / 100 Mbps / 1 Gbps Ethernet lub jako port SFP z wkładką 1000Base-T.
29. Minimalne parametry dostarczanego urządzenia firewall:
30. 6,6 Gbps przepustowości Firewall/kontroli aplikacji,
31. 3,2 Gbps przepustowości Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware,
32. 945 000 jednoczesnych sesji,
33. 100 000 nowych połączeń na sekundę,
34. 120 GB lokalnej przestrzeni na system operacyjny i logi.
35. Jako scenariusz Firewall/kontroli aplikacji Zamawiający rozumie, iż rozwiązanie pozwoli na:
36. wykrycie aplikacji,
37. przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.
38. Jako scenariusz Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware aplikacji Zamawiający rozumie, iż rozwiązanie pozwoli na:
39. wykrycie aplikacji,
40. przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonej aplikacji sieciowych, inspekcje IPS, Antywirus, Antyspyware.
41. Zakres kontroli musi też obejmować przesyłanie plików do Sandbox-a lokalnego i chmurowego w tym przechwytywanie i blokowanie plików określonego typu.
42. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony, tj. z włączonymi wszystkimi dostępnymi dla rozwiązania sygnaturami IPS oraz z wszystkimi funkcjami dostępnymi w rozwiązaniu dla silników antywirus i Antyspyware/antymalware.
43. Inspekcjom bezpieczeństwa musi podlegać cały ruch – sprawdzeniu musi podlegać każdy bajt danych przesyłany przez rozwiązanie.
44. Zamawiający wymaga, aby podana została przepustowość urządzenia dla pełnego zakresu ochrony oferowanego przez rozwiązanie – jeżeli rozwiązanie pozwala na pracę w wielu trybach, to należy podać przepustowość dla trybu z największą liczbą dostępnych inspekcji dla silników IPS, antywirus, antymalware/antyspyware.
45. Rozwiązanie musi spełniać co najmniej następujące parametry wydajnościowe odnośnie funkcjonalności site-to-site VPN:
46. minimum 4,6 Gbps dla IPsec VPN,
47. minimum 2 800 tuneli IPSec VPN (site-to-site).
48. Rozwiązanie musi spełniać co najmniej następujące parametry wydajnościowe odnośnie funkcjonalności remote access VPN:
49. minimum 1 500 tuneli remote access VPN z wykorzystaniem klienta VPN. Oprogramowanie klienta VPN musi być objęte wsparciem producenta,
50. minimum 200 tuneli tzw. Clientless VPN, bez konieczności zastosowania klienta VPN.
51. Rozwiązanie musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu. Musi mieć możliwość rozbudowy do przynajmniej 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, Antywirus i współpracy z Sandboxem), tablicy routingu oraz realizacji zdalnego dostępu.

## W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane rozwiązanie równoważne.

## Rozwiązanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie rozwiązania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie rozwiązania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w Jego nowszych wersjach.