**Opis przedmiotu zamówienia.**

Województwo Podlaskie jest operatorem regionalnej sieci szkieletowo-dystrybucyjnej SSPW WP. Przedmiotem zamówienia jest świadczenie usługi wsparcia technicznego urządzeń Juniper Networks serii MX i ACX, urządzeń DWDM ZTE ZXONE 8000 oraz dostawa i instalacja 20 urządzeń dostępowych  
o niskim poborze energii, 3 kart liniowych do routerów mx960 oraz urządzenia bezpieczeństwa sieci według wymagań opisanych w dalszej części opisu, we wskazanych węzłach dystrybucyjnych sieci.

Usługi i dostawy będą wykonywane zgodnie z poniższymi warunkami i wykazami:

Przedmiot zamówienia będzie realizowany od daty zawarcia umowy przez okres 12 miesięcy, zapewniając zamawiającemu nieprzerwaną usługę wsparcia technicznego wymienionych urządzeń.

1) Obsługa wszelkich zgłoszeń serwisowych musi odbywać się w języku polskim.

2) Wykonawca zobowiązany jest zapewnić możliwość zgłaszania awarii w trybie 24h na dobę 365 dni w roku. Zamawiający wprowadza następujące kategorie zgłoszeń:

a. Zgłoszenie Krytyczne – awaria urządzenia lub jego elementów powodująca brak możliwości świadczenia usług.

b. Zgłoszenie Poważne – awaria urządzenia lub jego elementów powodująca ograniczenie możliwości świadczenia usług (np. zmniejszenie dostępnej przepustowości lub niepełna funkcjonalność) lub ograniczenie niezawodności działania urządzenia.

c. Zgłoszenie Podstawowe – pozostałe awarie.

3) Maksymalny czas reakcji wykonawcy na zgłoszenie awarii nie może przekraczać 1 godziny od momentu zgłoszenia.

**Dla urządzeń Juniper Networks:**

Routery szkieletowe Juniper MX960:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| lp | nazwa sprzętu | Lokalizacja | nr seryjny urządzenia | karta liniowa | nr seryjny karty liniowej |
| 1 | MX960 | BIAŁYSTOK | JN125ACCDAFA | MPC4E 3D 32XGE | CAFB1521 |
| 2 | MX960 | GRAJEWO | JN125D419AFA | MPC4E 3D 32XGE | CAEY1424 |
| 3 | MX960 | HAJNÓWKA | JN125D33DAFA | MPC4E 3D 32XGE | CAEY1229 |
| 4 | MX960 | ŁOMŻA | JN125A890AFA | MPC4E 3D 32XGE | CAEV9193 |
| 5 | MX960 | SIEMIATYCZE | JN125764CAFA | MPC4E 3D 32XGE | CAGA8618 |
| 6 | MX960 | SOKÓŁKA | JN125A74DAFA | MPC3E NG PQ & FLEX Q | CAGA8438 |
| 7 | MX960 | SUWAŁKI | JN125DF8CAFA | MPC4E 3D 32XGE | CAEY1251 |
| 8 | MX960 | WYSOKIE MAZOWIECKIE | JN125C0F4AFA | MPC4E 3D 32XGE | CAHE6844 |

Routery dystrybucyjne Juniper MX 104 oraz Juniper ACX5048:

|  |  |  |  |
| --- | --- | --- | --- |
| lp | Nazwa | Lokalizacja | Nr seryjny urządzenia |
| 1 | MX104 | Mońki | AL919 |
| 2 | MX104 | Narew | AL710 |
| 3 | MX104 | Bakałarzewo | G8068 |
| 4 | MX104 | Przerośl | G8012 |
| 5 | MX104 | Czyżew | AJ975 |
| 6 | MX104 | Rutki Kossaki | AL673 |
| 7 | MX104 | Kołaki Kościelne | AK184 |
| 8 | MX104 | Rydzewo | AL726 |
| 9 | MX104 | Dobrzyjałowo | AJ037 |
| 10 | MX104 | Narewka | AW309 |
| 11 | ACX5048 | Suwałki NGA2 | WB3715340121 |

4) Czas całkowitej i skutecznej naprawy urządzeń objętych usługą wsparcia i ich elementów:

a. Dla zgłoszeń Krytycznych – nie dłuższy niż 12 godzin od zgłoszenia przez zamawiającego do przywrócenia pełnej funkcjonalności urządzenia;

b. Dla zgłoszeń Poważnych - następny dzień roboczy od zgłoszenia przez zamawiającego do przywrócenia pełnej funkcjonalności urządzenia.

c. Dla zgłoszeń Podstawowych - 7 dni roboczych od zgłoszenia przez zamawiającego do przywrócenia pełnej funkcjonalności urządzenia.

5) Wykonawca do obsługi Zgłoszeń musi zapewnić osoby posiadające certyfikat wystawiony przez producenta sprzętu objętego usługą wsparcia.

6) Awarie będą usuwane przez wykonawcę w miejscu instalacji urządzeń. Jeżeli naprawa będzie polegała na dostarczeniu elementu zamiennego, to jego wymiana za element należący do Zamawiającego może nastąpić tylko w takim terminie, na który wyrazi zgodę Zamawiający. Dostawa elementu zamiennego za uszkodzony/zniszczony nastąpi w ramach wynagrodzenia określonego w ofercie wykonawcy.

7) Koszty wsparcia technicznego obejmują również wykonanie przez wykonawcę wszelkich czynności związanych z transportem i ubezpieczeniem elementów zamiennych na czas transportu   
i instalacji.

8) W okresie wsparcia technicznego wykonawca w ramach otrzymanego wynagrodzenia udostępni Zamawiającemu możliwość wielokrotnego uaktualniania całego oprogramowania sterującego serwisowanych urządzeń do najnowszych wersji oferowanych przez producenta tych urządzeń (włączając tzw. firmware), a także dostęp do usług wsparcia technicznego producenta tych urządzeń. W przypadku, gdy dostęp taki wymaga podania nazwy użytkownika, hasła lub numeru seryjnego Wykonawca dostarczy Zamawiającemu te informacje w ciągu 7 dni kalendarzowych od daty zawarcia umowy. Nie jest wymagana możliwość otwierania zgłoszeń serwisowych w serwisie producenta bezpośrednio przez Zamawiający, jeżeli producent wymaga w tym celu posiadania wydawanych przez producenta certyfikatów kwalifikacyjnych. Natomiast Wykonawca musi posiadać bezpośredni dostęp do zgłaszania do producenta problemów technicznych związanych  
z oprogramowaniem lub sprzętem wraz z możliwością pobierania aktualizacji oraz prowadzenia  
z producentem bezpośredniej korespondencji w sprawach technicznych dotyczących zgłoszonych awarii.

**Dla urządzeń ZTE:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| lp | Typ węzła | lokalizacja | Nazwa urządzenia | ilość kierunków DWDM 100G |
| 1 | Węzeł szkielet. | Białystok | ZTE DWDM ZXONE 8000 | 4 |
| 2 | Węzeł szkielet. | Grajewo | ZTE DWDM ZXONE 8000 | 2 |
| 3 | Węzeł szkielet. | Hajnówka | ZTE DWDM ZXONE 8000 | 2 |
| 4 | Węzeł szkielet. | Łomza | ZTE DWDM ZXONE 8000 | 3 |
| 5 | Węzeł szkielet. | Siemiatycze | ZTE DWDM ZXONE 8000 | 2 |
| 6 | Węzeł szkielet. | Sokółka | ZTE DWDM ZXONE 8000 | 2 |
| 7 | Węzeł szkielet. | Suwałki | ZTE DWDM ZXONE 8000 | 2 |
| 8 | Węzeł szkielet. | Wysokie Maz. | ZTE DWDM ZXONE 8000 | 3 |
| 9 | Węzeł pośredni | Nowa Kamienna | ZTE DWDM ZXONE 8000 | 2 |
| 10 | Węzeł pośredni | Zawady | ZTE DWDM ZXONE 8000 | 2 |

9) W celu dokonania naprawy uszkodzenia sprzętowego urządzeń ZTE Zamawiający udostępni moduły zamienne Zamawiającego w miarę ich dostępności. W szczególności mogą to być moduły zamienne pozyskane z innych w węzłów Zamawiającego, które nie świadczą usług krytycznych  
w sieci. W przypadku braku wyżej wymienionych komponentów Zamawiający dopuszcza wymianę urządzeń ZTE na równoważne, na zasadzie wypożyczenia przez Wykonawcę dla Zamawiającego  
w okresie trwania umowy, w poniższym zakresie:

- przepustowość nowego urządzenia musi zapewniać działanie istniejących usług,

- system operacyjny i konfiguracja urządzenia zastępującego muszą być możliwe do przeniesienia 1:1 z dopuszczalnymi różnicami w zakresie nazw i numeracji interfejsów,

- urządzenie zastępujące musi być obsługiwane przez obecnie używany system zarządzania Juniper Networks Junospace.

10) Wykonawca do obsługi Zgłoszeń musi zapewnić osoby posiadające certyfikat wystawiony przez producenta sprzętu objętego usługą wsparcia.

11) Awarie będą usuwane przez wykonawcę w miejscu instalacji urządzeń. Jeżeli naprawa będzie polegała na dostarczeniu elementu zamiennego, to jego wymiana za element należący do Zamawiającego może nastąpić tylko w takim terminie, na który wyrazi zgodę Zamawiający.

Pozostałe Wymagania:

12) Zamawiający ma prawo do dodawania do urządzeń objętych wsparciem technicznym dodatkowych komponentów takich jak karty z interfejsami sieciowymi lub modułów CFP, CFP2, XFP, SFP+ oraz SFP (pochodzących od dowolnych producentów) oraz wymiany zainstalowanych komponentów samodzielnie bez utraty gwarancji wynikających z usługi wsparcia technicznego.

13) Zamawiający ma prawo do przenoszenia modułów i elementów objętych usługą wsparcia technicznego, pomiędzy posiadanymi urządzeniami (również nie objętymi niniejszą usługą wsparcia technicznego) bez utraty gwarancji wynikających z tej usługi.

14) Zamawiający może udostępnić Wykonawcy na jego prośbę zdalny dostęp do urządzeń   
i systemów zarządzania w celach diagnostycznych. Jednak nie jest do tego zobowiązany i każdą tego typu prośbę będą rozpatrywać indywidualnie mając na uwadze bezpieczeństwo sieci   
i charakter prac diagnostycznych.

15) Wykonawca zobowiązuje się do udzielenia zamawiającemu gwarancji jakości:

a. na wykonane w ramach przedmiotu zamówienia prace (czynności serwisowe); gwarancja ta obowiązuje każdorazowo od daty wykonania danej czynności serwisowej uwidocznionej  
w systemie Zgłoszeń Problemowych; gwarancja jest udzielana każdorazowo na okres 1 roku,

b. na dostarczone elementy zamienne; gwarancja ta obowiązuje każdorazowo od daty wymiany danego elementu uwidocznionej w systemie Zgłoszeń Problemowych lub protokole wymiany (o ile taki zostanie sporządzony); gwarancja jest udzielana każdorazowo do końca obowiązywania umowy zawartej w wyniku niniejszego postępowania o udzielenie zamówienia publicznego.

16) Wykonawca zobowiązuje się, że przez cały czas realizacji przedmiotu zamówienia będzie posiadał ważny i aktualny (aktywny) status partnerski w programie Service Partners Program producenta Juniper Networks; Wykonawca na każde żądanie Zamawiającego przedstawi stosowne oświadczenie wystawione przez lokalne biuro Juniper Network w Polsce. Utrata tego statusu uprawnia Zamawiającego do rozwiązania umowy z wykonawcą bez zachowania okresu wypowiedzenia.

17) W ostatnim tygodniu trwania umowy wykonawca dostarczy raport zamknięcia zawierający: potwierdzenie pełnej sprawności i funkcjonalności urządzeń objętych usługą wsparcia technicznego oraz potwierdzenie wykonania aktualizacji oprogramowania o ile takie były wykonywane.

18) W ramach zamówienia Zamawiający będzie mógł skorzystać z konsultacji i wsparcia dotyczącego serwisowanego sprzętu. Czas konsultacji określa się na maksymalnie 30 godzin miesięcznie. Godziny te będą rozliczane kwartalnie.

19) Wykonawca zobowiązuje się wykonać czynności związane z przedmiotem zamówienia,   
w szczególności obsługę zgłoszeń oraz wykonywanie czynności serwisowych za pomocą pracowników zatrudnionych na podstawie umowy o pracę.

**Dostawa i instalacja urządzeń dostępowych:**

20) urządzenia dostępowe o niskim poborze energii muszą spełniać poniższe wymagania:

|  |
| --- |
| Wymiary przełącznika nie mogą przekraczać: 200 x 166 x 45 mm.  Przełączniki muszą być dostarczony z dodatkowymi uchwytami do instalacji w standardowych 19” szafach teleinformatycznych (EIA-310). Przełączniki muszą posiadać wszystkie elementy potrzebne do zainstalowania go w szafie. |
| Przełącznik musi być przystosowany do pracy w temperaturach od -40stC do +70 stC |
| Urządzenie musi być wyposażone w min.:   * RAM 256MB * Flash 16GB |
| Urządzenie musi obsługiwać dostęp do interfejsu CLI za pomocą protokołu SSHv2 oraz obsługiwać transfer plików za pomocą protokołu SFTP (wymagana jest obsługa funkcji serwera) |
| Urządzenie musi być wyposażone w port konsolowy do dołączenia konsoli RS-232 z gniazdem RJ45. |
| Wymagania szczegółowe |
| Urządzenie musi wspierać następujące funkcjonalności:   * Wsparcie dla VLAN 802.1q min. 100VLAN * Wsparcie dla VLAN-filering wspomagae sprzętowo * Routing L3 |
| Każdy z przełączników wchodzących w skład urządzenia o architekturze rozproszonej musi spełniać następujące wymagania: |
| Przełącznik musi być wyposażony co najmniej w następującą liczbę i typy interfejsów:  i. 9 interfejsy pracujące w następujących trybach w zależności od zainstalowanego modułu optycznego:  · 4 w trybie 10GE po zainstalowaniu modułu typu SFP+  · 5 w trybie 1GE po zainstalowaniu modułu typu SFP |
| Przełącznik musi być wyposażony zasilacz przystosowane do zasilania napięciem 230V AC. Maksymalny pobor mocy nie może przekraczać 20W. Zasilanie musi być możliwe przez styk typu jack z zewnętrznego zasilacza lub z zasilacza napięcia gwarantowanego 48V DC. |

21) Ilość urządzeń dostępowych o niskim poborze energii podlegających dostawie wynosi 20 sztuk.

22) W ramach umowy Wykonawca dokona instalacji i konfiguracji w sieci dostarczonych urządzeń dostępowych o niskim poborze energii, zapewniającej poprawną komunikację z urządzeniami kontroli dostępu w sieci.

**Uruchomienie transmisji 100G w relacjach Siemiatycze - Hajnówka i Siemiatycze – Wysokie Maz. wraz z dostawą kart liniowych oraz niezbędnych modułów optycznych w tych węzłach.**

23) Dostawa 3 kart liniowych MPC7E-MRATE-IR z portami 2x100G wraz z 4 modułami optycznymi 100G-ZR4 80km z rocznym wsparciem producenta do routerów Juniper MX960 w następujący sposób:

- węzeł Siemiatycze – jedna karta MPC7E z 2 modułami optycznymi;

- węzeł Wysokie Mazowieckie - jedna karta MPC7E z 1 modułem optycznym;

- węzeł Hajnówka - jedna karta MPC7E z 1 modułem optycznym;

24) Uruchomienie transmisji 100G z użyciem kart MPC7E w relacjach:

Siemiatycze – Wysokie Mazowieckie;

Siemiatycze – Hajnówka.

**Rozbudowa systemu bezpieczeństwa sieci opartego na klastrze HA 2xPalo Alto PA-5060  
o kompatybilny firewall zabezpieczający Centrum Nadzoru Sieci SSPW WP w zakresie dostępu do Internetu i dwóch Centrów Zarządzania Siecią SSPW WP.**

25)oferowany firewall musi posiadać następujące funkcjonalności:

a) Musi być dostarczone jako samodzielne, dedykowane fizyczne urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej rozwiązania musi występować moduł zarządzania i moduł przetwarzania danych.

b) Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.

c) Urządzenie musi być wyposażone w dedykowany port zarządzania out-of-band.

d) Brak ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.

e) Urządzenie musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.

f) Obsługa dla IPv6.

g) Funkcjonalność statycznej i dynamicznej translacji adresów NAT między IPv4 i IPv6.

h) Reguły zabezpieczeń firewall muszą być tworzone zgodnie z ustaloną polityką opartą o profile oraz obiekty.

i) Polityka zabezpieczeń firewall musi uwzględniać przynajmniej takie parametry jak: adresy IP źródłowe i docelowe, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie.

j) Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.

k) Interfejs administracyjny urządzenia musi być w języku polskim lub angielskim.

l) Firewall musi działać w następujących trybach:

- routera (tzn. w warstwie 3 modelu OSI),

- przełącznika (w warstwie 2 modelu OSI),

- transparentnym (bez skonfigurowanych adresów IP na interfejsach sieciowych biorących udział w transmisji0,

- pasywnego nasłuchu.

m) Zarządzanie firewallem musi odbywać się z linii poleceń (CLI) oraz z graficznej konsoli GUI. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Dopuszcza się, aby polityki mogły być tworzone tylko z graficznej konsoli GUI.

n) Musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP, mapowanie 1 adres publiczny na 1 adres prywatny oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.

o) Musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenia muszą umożliwiać stworzenie co najmniej 6 klas dla różnego rodzaju ruchu sieciowego.

p) Firewall musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.

q) Obsługa protokołu Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.

r) Obsługa protokołów routingu dynamicznego, nie mniej niż RIP, OSPF oraz BGP.

s) Firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

t) Musi posiadać osobny zestaw polityk definiujący ruch zaszyfrowany SSL oraz SSH, który należy poddać lub wykluczyć z operacji deszyfrowania rozdzielny od polityk bezpieczeństwa.

u) Musi posiadać funkcjonalność automatycznego pobierania listy stron WWW lub adresów IP z zewnętrznego systemu oraz używania ich w politykach bezpieczeństwa.

v) Ochrona przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony informującej użytkownika o próbie pobrania pliku i możliwości kontynuowania lub zaniechania pobrania.

x) Urządzenie zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.

y) Firewall musi identyfikować co najmniej 2500 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS m.in.: Skype, Tor, BitTorrent, eMule.

z) Możliwość definiowania własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta.

aa) System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie wyłącznie na podstawie rozszerzenia.

bb) Urządzenie musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN  
w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Urządzenie musi umożliwiać konfigurację tuneli VPN w trybie route-based VPN.

cc) Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN oraz IPSec.

dd) Firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci,  
z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną).

ee) Producent urządzenia musi udostępniać dedykowanego klienta binarnego VPN dla platform Windows, Mac oraz Android.

ff) Urządzenie musi transparentnie ustalać tożsamość użytkowników sieci w oparciu o Active Directory oraz Ms Exchange. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym Citrix oraz Windows Terminal Services, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.

gg) Musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction)  
i zastosowanie tego mechanizmu w politykach.

hh) Musi mieć możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka  
X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesje  
w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.

ii) Musi mieć możliwość wyboru sposobu blokowania ruchu w politykach bezpieczeństwa. Musi istnieć możliwość ustawienia cichego blokowania ruchu bez wysyłania RST, blokowanie z wysłaniem RST tylko do klienta, blokowanie z wysłaniem RST tylko do serwera, blokowanie z wysłaniem RST do klienta i serwera jednocześnie.

jj) Firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.

kk) Musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i kategorii stron WWW.

ll) Urządzenie musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.

mm) Urządzenie musi być dostarczone w konfiguracji z minimum 8 portami Ethernet 1Gb/s

nn) Firewall musi posiadać przepustowość w ruchu nie mniej niż 2,2 Gbps dla kontroli firewall z włączoną funkcją kontroli aplikacji. Przepustowość dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (ochrona IPS, antywirus, antyspyware, identyfikacja aplikacji) nie może być mniejsza niż 1,2 Gbps.

oo) Urządzenie musi obsłużyć minimum 200 000 jednoczesnych sesji oraz 30 000 nowych połączeń na sekundę.

pp) Urządzenie musi zapewniać wydajność przynajmniej 1,1 Gbps dla ruchu IPSec VPN  
i umożliwiać zestawienie przynajmniej 2500 równoczesnych tuneli site-to-site.

qq) Urządzenie musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi umożliwiać deszyfracje niezaufanego ruchu HTTPS i poddania go dalszej inspekcji.

rr) Urządzenie musi posiadać funkcjonalność weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci lub wybranych jej zasobów. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania.

ss) Musi posiadać możliwość uruchomienia funkcji wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS). W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.

tt) Urządzenie musi posiadać możliwość uruchomienia funkcji inspekcji antywirusowej, kontrolującej przynajmniej protokoły: SMTP, HTTP, POP3, IMAP oraz podstawowe rodzaje plików. Baza AV musi być przechowywana na urządzeniu i regularnie aktualizowana  
w sposób automatyczny. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.

uu) Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.

vv) Musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive i Active-Active w przypadku pracy z drugim takim samym urządzeniem posiadającym taki sam zestaw licencji.

xx) Urządzenie musi być rozwiązaniem o uznanej na rynku pozycji i musi znajdować się  
w kwadracie „Leaders” raportu Gartnera pt. „Magic Quadrant of Network Enterprise Firewalls” w raportach opublikowanych w przeciągu 2 ostatnich lat.

yy) Urządzenie musi być fabrycznie nowe, aktualnie obecne w linii produktowej producenta.

zz) Musi pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej.

aaa) Serwis dostępu do najnowszej wersji oprogramowania, serwis sprzętowy i ewentualne licencje/subskrypcje na aktualizacje bazy aplikacji muszą być ważne przynajmniej przez okres 12 miesięcy.

26) Dostarczane urządzenie nie mogą znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.

27) Pomoc techniczna oraz szkolenia z dostarczanych rozwiązań muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim.