Załącznik nr 1 do SIWZ z dnia 26.04.2019r.

Szczegółowy Opis Przedmiotu Zamówienia (SOPZ)

1. Przedmiot przetargu.

Przedmiotem przetargu jest doprowadzenie, instalacja i udostępnianie połączeń internetowych w siedzibie Wojewódzkiego Urzędu Pracy w Toruniu, oraz dwóch Oddziałów.
Umowa obejmować będzie trzy punkty przyłączy:

1) Siedziba WUP Toruń – ul. Szosa Chełmińska 30/32, 87-100 Toruń, piętro IX, pokój nr 15 (serwerownia),
2) Oddział Zamiejscowy WUP w Bydgoszczy – ul. Paderewskiego 26, 85-075 Bydgoszcz, piętro II, pokój nr 23 (serwerownia),
3) Oddział Zamiejscowy WUP we Włocławku – ul. Bulwary 5b, 87-800 Włocławek, parter, pokój nr 8 (serwerownia).

Dokładne wyznaczenie miejsc dla punktów przyłącza określi Zamawiający, po uzgodnieniu z Wykonawcą. W przypadku zmiany lokalizacji któregoś z przyłączy, Zamawiający zastrzega sobie możliwość kontynuowania umowy w nowej lokalizacji, jeżeli Wykonawca wyrazi na to zgodę. W tym przypadku Wykonawca w ramach zamówienia uzupełniającego wykona przyłącze w nowej lokalizacji.

2. Specyfikacja techniczna połączeń internetowych.

1) Łącze dla Siedziby WUP Toruń (wymienionej w ustępie 1 pkt. 1) powinno mieć parametry:
   a) gwarantowana przepustowość do Zamawiającego (download): nie mniejsza niż **150 Mbit/s,**
   b) gwarantowana przepustowość od Zamawiającego (upload): nie mniejsza niż **150 Mbit/s,**
   c) gwarantowane pasmo (CIR) 150 Mbit/s (150Mbit/s pobieranie danych i 150Mbit/s wysyłanie danych),
   d) średni czas opóźnienia: nie większy niż 20 ms,
   e) współczynnik straty pakietów nie większy niż 10^{-3} (zgodnie z zaleceniem ITU-T Y.1541)
   f) udostępniona podsieć: co najmniej 16 stałych adresów IP (13 dla Zamawiającego),

g) brak limitów ruchu – brak ograniczenia w ilości przesyłanych danych, zarówno „do" jak i „od" Zamawiającego, brak limitów liczby sesji, itp.,

h) brak filtrowania ruchu – brak blokowania jakichkolwiek usług czy protokołów,

i) dopuszczalna technologia: Ethernet,

j) dopuszczalny interfejs styku Ethernet: złącze zgodne ze złączem WAN urządzenia UTM/NGFW w ustępie 6 pkt. 2,

2) Łącze dla Oddziału (wymienionego w ustępie 1 pkt. 2) powinno mieć parametry:

a) gwarantowana przepustowość do Zamawiającego (download): nie mniejsza niż **70 Mbit/s,**

b) gwarantowana przepustowość od Zamawiającego (upload): nie mniejsza niż **70 Mbit/s,**

c) gwarantowane pasmo (CIR) 70 Mbit/s (70 Mbit/s pobieranie danych i 70Mbit/s wysyłanie danych),

d) średni czas opóźnienia: nie większy niż 20 ms,

e) współczynnik straty pakietów nie większy niż 10^{-3} (zgodnie z zaleceniem ITU-T Y.1541)

f) udostępniona podsieć: co najmniej 8 stałych adresów IP (5 dla Zamawiającego),

g) brak limitów ruchu – brak ograniczenia w ilości przesyłanych danych, zarówno „do" jak i „od" Zamawiającego, brak limitów liczby sesji, itp.,

h) brak filtrowania ruchu – brak blokowania jakichkolwiek usług czy protokołów,

i) dopuszczalna technologia: Ethernet,

j) dopuszczalny interfejs styku Ethernet: złącze zgodne ze złączem WAN urządzenia UTM/NGFW w ustępie 6 pkt. 3,

3) Łącze dla Oddziału (wymienionego w ustępie 1 pkt. 3) powinno mieć parametry:

a) gwarantowana przepustowość do Zamawiającego (download): nie mniejsza niż **50 Mbit/s,**

b) gwarantowana przepustowość od Zamawiającego (upload): nie mniejsza niż **50 Mbit/s,**

c) gwarantowane pasmo (CIR) 50 Mbit/s (50 Mbit/s pobieranie danych i 50Mbit/s wysyłanie danych),

d) średni czas opóźnienia: nie większy niż 20 ms,

e) współczynnik straty pakietów nie większy niż 10^{-3} (zgodnie z zaleceniem ITU-T Y.1541)

f) udostępniona podsieć: co najmniej 8 stałych adresów IP (5 dla Zamawiającego),

g) brak limitów ruchu – brak ograniczenia w ilości przesyłanych danych, zarówno „do" jak i „od" Zamawiającego, brak limitów liczby sesji, itp.,

h) brak filtrowania ruchu – brak blokowania jakichkolwiek usług czy protokołów,

i) dopuszczalna technologia: Ethernet,

j) dopuszczalny interfejs styku Ethernet: złącze zgodne ze złączem WAN urządzenia UTM/NGFW w ustępie 6 pkt. 3.

3. Metodologia pomiaru parametrów łączy.

Metodologia pomiaru parametrów łączy internetowych (opisanych w ustępie 2) służących do pomiaru poziomu usług (SLA) opisanych w ustępie 7:

1) przepustowość – mierzona między punktami przyłączy zdefiniowanymi w ustępie 1, za pomocą pobierania pliku o wielkości co najmniej 500 MB, za pomocą protokołu http lub FTP,

2) średni czas opóźnienia – mierzony między punktami przyłączy zdefiniowanymi w ustępie 1, za pomocą narzędzia ping przy próbie wynoszącej 100 odpowiedzi,

3) straty pakietów są wyrażonym w % wynikiem pomiarów realizowanych przez co najmniej jednokrotne wysłanie co najmniej 500 pakietów ICMP (ping) o wielkości co najmniej 64-bajtów, co godzinę w 24-godzinnym okresie pomiaru przez internetową sieć szkieletową Dostawcy do OPP (Ostatni punkt pomiarowy – OPP oznacza ostatni router w sieci Dostawcy, który posiada bezpośredni styk z operatorem międzynarodowym). W celu uzyskania odpowiednich statystyk strat pakietów Wykonawca będzie monitorować drogę od routera brzegowego Zamawiającego do OPP,

4) miesięczna i roczna dostępność usługi – miedzy punktami przyłączy zdefiniowanymi w ustępie 1, za pomocą narzędzia Wykonawcy (opisanego w ustępie 9 pkt. 7), pakietów ICMP (np. narzędzia ping) oraz opcjonalnie (dla weryfikacji) mierzona z zewnętrznych serwerów (np. uptimerobot.com) lub udokumentowana za pomocą zgłoszeń awarii do służb technicznych Wykonawcy.

4. Termin obowiązywania.

1) Umowa na świadczenie usługi dostępu do Internetu zostanie podpisana na okres 36 miesięcy od daty uruchomienia usługi, z 6 miesięcznym okresem wypowiedzenia.
2) Zamawiający zastrzega sobie możliwość wypowiedzenia umowy dla każdego z przyłączy z osobna.
3) Termin realizacji (instalacji i uruchomienia usługi we wszystkich lokalizacjach): nie później niż **do 19 września 2019 roku**. Przy czym okres rozliczeniowy rozpocznie się od dnia 1 października 2019 roku.

4) Okres od 19 do 30 września 2019 roku **należy traktować jako testowe uruchomienie usługi,** w celu konfiguracji przez Zamawiającego urządzeń sieciowych i przeprowadzenia testów. Testowa usługa powinna być w pełni funkcjonalna tzn. zgodna z niniejszą specyfikacją. Koszty testowego uruchomienia nie mogą być dodatkowo płatne, tzn. koszty usługi Wykonawca wliczy w koszty miesięcznych abonamentów w ciągu całego czasu trwania umowy, zawartych w formularzu ofertowo-cenowym.

5. Koszt połączeń internetowych.

1) Wszystkie ewentualne koszty instalacji, wdrożenia, wsparcia technicznego, szkoleń i aktywacji usługi dostępu do Internetu powinny być wliczone do kosztów miesięcznych abonamentów, zawartych w formularzu ofertowo-cenowym.
2) Usługa dostępu do Internetu dla siedzib opisanych w punkcie 1 rozliczana będzie z dołu fakturami VAT wystawianymi na koniec każdego miesiąca abonamentowego. Wszystkie siedziby rozliczane będą na jednej fakturze. Każda z lokalizacji wymieniona w ustępie 1 będzie osobną pozycją na fakturze. Płatność za fakturę uiszczana będzie przelewem, w terminie 14 dni od dnia otrzymania faktury.

6. Urządzenia dostępowe i zabezpieczenia sieci typu UTM/NGFW.

1) Wykonawca dostarczy i zainstaluje urządzenia dostępowe – routery/modemy oraz urządzenia UTM/NGFW do zabezpieczenia i udostępniania połączenia internetowego, we wszystkich punktach przyłączy, wymienionych w ustępie 1. Ewentualne koszty dzierżawy urządzeń powinny być wliczone w abonament.

   Urządzenie dostępowe we Włocławku (ust. 1 pkt. 1) powinno być zabezpieczone przez Wykonawcę co najmniej za pomocą zasilacza awaryjnego (UPS-a możliwego do zamontowania w szafie RACK).

   Urządzenia dostępowe muszą być skonfigurowane w taki sposób, aby po utracie zasilania i jego powrocie możliwy był natychmiastowy dostęp do Internetu bez jakichkolwiek ingerencji Zamawiającego.

   Urządzenia dostępowe i zabezpieczania sieci pozostają własnością Wykonawcy i powinny być przez niego i na jego koszt serwisowane oraz ubezpieczone od kradzieży lub zniszczenia.

   Przy czym Zamawiający zastrzega sobie możliwość samodzielnego zarządzania urządzeniami UTM/NGFW.

   Urządzenia zabezpieczania sieci UTM/NGFW powinny mieć aktywne wsparcie i opisane poniżej mechanizmy ochrony sieci przez cały okres obowiązywania umowy.

2) **Urządzenia zabezpieczające sieć typu UTM/NGFW/NGFW dla lokalizacji opisanej w ustępie 1 pkt. 1, nie gorsze niż 2 szt. Fortigate 300E lub równoważne**, spięte w klaster HA typu active-active. Za równoważne traktowane są urządzenia posiadające co najmniej następujące funkcje i parametry oraz metody pomiaru wydajności:

a) Mechanizmy: Zapora korporacyjna – Firewall, NAT, Router z obsługa równoważenia obciążenia łączy (load balancing), Ochrona Antywirusowa, Ochrona Antyspamowa, Sandbox, Filtr adresów URL, Filtr aplikacji, Mechanizm Inspekcji połączeń SSL, Mechanizm zapobiegania wtargnięciom (IPS), Kształtowanie pasma (Traffic Shapping), Wirtualne sieci prywatne (VPN), Wysoka dostępność – możliwość pracy w klastrze HA (w trybie active-active),
b) UTM/NGFW musi posiadać możliwość współpracy z posiadanym przez Zamawiającego urządzeniem FortiAnalyzer 1000E do zbierania logów i raportowania. Musi być możliwość wykonywania okresowych predefiniowanych raportów z zaproponowanych urządzeń UTM/NGFW,
c) Przepustowość Firewall: 32 Gbps (dla UDP 512 byte) i 20 Gbps (dla UDP 64 byte),
d) Przepustowość IPS (http/enterprise mix): 5 Gbps,
e) Przepustowość inspekcji SSL: 3,9 Gbps,
f) Liczba sesji równoległych: 4.000.000,
g) Liczba nowych sesji na sekundę: 300.000,
h) Przepustowość IPSec VPN (512 byte): 20 Gbps,
i) Liczba tuneli IPSec VPN (Gateway to Gateway): 2.000,
j) Liczba tuneli IPSec VPN (Client to Gateway): 50.000,
k) Przepustowość SSL VPN: 2,5 Gbps,
l) Liczba tuneli SSL VPN: 5.000,
m) Liczba reguł firewall: 10.000,
n) Liczba VLAN 802.1q: 128,
o) W każdym z urządzeń w klastrze, liczba interfejsów sieciowych wspieranych przez dedykowane Network Processory: min 4x 1 GE RJ45, min 4x 1 GE SFP, ponadto Wykonawca dostarczy do każdego z urządzeń w klastrze: 2 szt. wkładek GBIC, oraz 2 szt. przejściówek, które pozwolą na użycie portów SFP jako portów RJ45, przy czym nie może to wpłynąć na ilość możliwych do wykorzystania dedykowanych portów RJ45, możliwość zdefiniowania 2x WAN zarówno na portach RJ45 jak i SFP,
p) Wysoka dostępność: zamówione dwa urządzenia muszą posiadać funkcjonalność pracy w klastrze HA (High Availability), do urządzeń należy dostarczyć pełne rozwiązanie umożliwiające spięcie w klaster (np. kable, moduły sprzętowe i programowe, itp.), tryb pracy active-active,
q) Zasilacz trwale wbudowany w urządzenie, Obudowa wielkość maks 2U oraz dostarczony zestaw do montażu w szafie rack,
r) Gwarancja urządzeń świadczona w trybie umożliwiającym wywiązanie się z poziomu świadczonej usługi (SLA) opisanego w ustępie 9,
s) Wszystkie moduły posiadają licencję i subskrypcję ważną w okresie trwania umowy,
t) Aktualizacja sygnatur antywirusa i IPS-a nie rzadziej niż raz dziennie.

3) **Urządzenia zabezpieczające sieć typu UTM/NGFW dla dwóch lokalizacji opisanych w ustępie 1 pkt, 2 i 3 nie gorsze niż Fortigate 50E lub równoważne**. Za równoważne traktowane są urządzenia posiadające co najmniej następujące funkcje i parametry oraz metody pomiaru wydajności:
   a) Mechanizmy: Zapora korporacyjna – Firewall, NAT, Router z obsługa równoważenia obciążenia łączy (load balancing), Ochrona Antywirusowa, Ochrona Antyspamowa, Sandbox, Filtr adresów URL, Filtr aplikacji, Mechanizm Inspekcji połączeń SSL,

Mechanizm zapobiegania wtargnięciom (IPS), Kształtowanie pasma (Traffic Shapping), Wirtualne sieci prywatne (VPN),

b) UTM/NGFW musi posiadać możliwość współpracy z posiadanym przez Zamawiającego urządzeniem FortiAnalyzer 1000E do zbierania logów i raportowania. Musi być możliwość wykonywania okresowych predefiniowanych raportów z zaproponowanych urządzeń UTM/NGFW,
c) Przepustowość Firewall: 2,5 Gbps,
d) Przepustowość IPS (http/enterprise mix): min 800 / 270 Mbps,
e) Przepustowość inspekcji SSL: 150 Mbps,
f) Liczba sesji równoległych: 1.800.000,
g) Liczba nowych sesji na sekundę: 21.000,
h) Przepustowość IPSec VPN(512 byte packet): 90 Mbps,
i) Liczba tuneli IPSec VPN (Gateway to Gateway): 200,
j) Liczba tuneli IPSec VPN (Client to Gateway): 250,
k) Przepustowość SSL VPN: 100 Mbps,
l) Liczba tuneli SSL VPN: 200,
m) Liczba reguł firewall: min 5.000,
n) Liczba VLAN 802.1q: min 128,
o) Liczba interfejsów sieciowych wspieranych przez dedykowane Network Processory: min 5x 1 GE RJ45, możliwość zdefiniowania 2x WAN na portach RJ45 oraz 1xUSB,
p) Zasilacz trwale wbudowany w urządzenie, Obudowa wielkość maks 2U oraz dostarczony zestaw do montażu w szafie rack,
q) Gwarancja urządzeń świadczona w trybie umożliwiającym wywiązanie się z poziomu świadczonej usługi (SLA) opisanego w ustępie 9,
r) Wszystkie moduły posiadają licencję i subskrypcję ważną w okresie trwania umowy,
s) Aktualizacja sygnatur antywirusa i IPS-a nie rzadziej niż raz dziennie.

4) Dodatkowe oprogramowanie

Softwareowe rozwiązanie (licencje oprogramowania), współpracujące z urządzeniami UTM/NGFW zabezpieczającymi sieć (opisanymi w ustępie 6), generujące hasła jednorazowe (OTP) dla w sumie **30 użytkowników**, pozwalające na użycie dwuskładnikowego uwierzytelniania do usług, np. SSL VPN, czy panelu administracyjnego. Oprogramowanie powinno być możliwe do zainstalowania na telefonach wyposażonych w system Android i iOS.

5) Wdrożenie

Wykonawca wdroży oferowane urządzenia w siedzibie zamawiającego oraz przeniesie istniejącą konfigurację na nowe urządzenia UTM/NGFW (posiadające najnowszą stabilną wersję firmware z linii 6.0) z posiadanych przez Zamawiającego urządzeń Fortigate: 2 szt. 300D (klaster HA) i 2 szt. 90D - pracujących na firmware w wersji 5.6.

Wdrożenie powinno objąć co najmniej:

a) Przeniesienie całych konfiguracji z istniejących urządzeń UTM/NGFW na nowe urządzenia UTM/NGFW z najnowszą stabilna wersją oprogramowania,
b) konfiguracja interfejsów sieciowych - WAN, LAN, DMZ,
c) konfiguracja loadbalancingu dla dwóch łączy WAN,
d) konfiguracja ogólna urządzeń - adresy IP, DNS, DHCP, routing, NTP,
e) integracja z Active Directory,
f) konfiguracja QoS oraz kształtowania pasma dla co najmniej 5 profili,

g) przeniesienie istniejących obiektów sieciowych – ok. 1.300 obiektów,
h) przeniesienie istniejących reguł firewall oraz NAT – ok. 350 reguł,
i) konfiguracja IPSec VPN pomiędzy siedzibą oraz oddziałami,
j) konfiguracja transparentnego uwierzytelniania użytkowników w sieci,
k) przeniesienie filtrów URL oraz SSL, konfiguracja inspekcji SSL – ok. 750 obiektów URL oraz ok. 300 obiektów SSL,
l) aktualizacja firmware na urządzeniu FortiAnalyzer 1000E do wersji zgodnej z dostarczonymi UTM/NGFW-ami,
m) konfiguracja logowania do 2 szt. urządzeń FortiAnalyzer ze wszystkich dostarczonych UTM/NGFW oraz zdefiniowanie co najmniej 3 raportów cyklicznych (automatycznych), w tym co najmniej dwa raporty niestandardowe (custom) i jeden predefiniowany, m.in. podsumowanie wykrytych przez IPS zagrożeń, wykorzystanie pasma per użytkownik, wykorzystanie pasma per strona internetowa / aplikacja, wykorzystanie pasma per host, ruch sieciowy per użytkownik/host - np skype, teamviewer etc., ruch www - jakie strony były odwiedzane, jakie zostały zablokowane, ruch ssl vpn - zestawione sesje, wykorzystanie pasma, ips - co zostało zablokowane / skąd pochodzą ataki / rodzaje: krytyczne, wysokie etc., top 50 blokowanych stron, top 50 stron per pasmo, top 50 stron per ilość połączeń, top 50 użytkowników per strony www / pasmo / ściągnięte pliki, top 50 hostów per strony www / pasmo / ściągnięte pliki,
n) Zamawiający może wymagać skonfigurowania dodatkowych parametrów urządzeń UTM/NGFW jeśli podczas wdrożenia zajdzie taka potrzeba w celu poprawnego uruchomienia dostarczonych w ramach niniejszej Umowy łączy internetowych.

Zamawiający wymaga, aby wdrożenie przeprowadził certyfikowany inżynier dla urządzeń UTM/NGFW do zabezpieczania sieci.

6) Dodatkowe wsparcie inżyniera dla urządzeń UTM/NGFW

Wykonawca zapewni w każdym roku umowy co najmniej 10 roboczo godzin wsparcia certyfikowanego inżyniera dla dostarczonych urządzeń UTM/NGFW w zakresie aktualizacji, konfiguracji urządzeń oraz modyfikacji funkcjonalności.

7) Szkolenie

a) Szkolenie podstawowe (wdrożeniowe) – odbywające się przy okazji wdrożenia i konfiguracji urządzeń UTM/NGFW w siedzibie Zamawiającego.
b) Szkolenie nieautoryzowane, minimum 3 dniowe, maksymalnie 5 dniowe, prowadzone przez certyfikowanego (z administracji dostarczonych urządzeń UTM/NGFW) inżyniera lub trenera, odbywające się po wdrożeniu, w siedzibie Zamawiającego lub w sali szkoleniowej. Szkolenie musi zawierać elementy warsztatowe i opierać się zadania praktyczne realizowane w przygotowanym Labie z urządzeniami UTM/NGFW. Szkolenie musi być prowadzone na wersji firmware zastosowanej podczas wdrożenia na urządzeniach Zamawiającego. Szkolenie musi być prowadzone przez praktyka posiadającego co najmniej 3-letnie doświadczenie w zakresie wdrażania zaproponowanymi urządzeniami UTM/NGFW.
W przypadku szkolenia poza siedzibą Zamawiającego Wykonawca pokryje koszty zakwaterowania i pełnego wyżywienia. Zamawiający pokrywa koszty dojazdu. W przypadku miejsca szkolenia, gdzie łączny czas dojazdu PKP/PKS/MZK jest dłuższy niż 3,5 godziny Wykonawca pokryje koszty zakwaterowania w dniu

poprzedzającym szkolenie. Zakwaterowanie w hotelu (co najmniej dwugwiazdkowym) nie może być oddalone od miejsca szkolenia więcej niż 15 min pieszo.
Szkolenie powinno zostać zrealizowane w dwóch turach/grupach: dla 2 osób i dla 3 osób.
Terminy szkoleń Wykonawca musi ustalić z Zamawiającym.
Zakres szkolenia:

- Fizyczna budowa urządzeń UTM/NGFW:
  - Tryby pracy NAT/Transparent,
  - Konfiguracja sieci i routingu,
  - System Dashboard i moduły systemu,
  - Administracja urządzeniem (WWW, CLI),
- Polityki zapory sieciowej:
  - Koncepcja firewall w urządzeniach UTM/NGFW,
  - Tworzenie obiektów dla reguł firewall,
  - Translacja adresów NAT i Virtual IP,
  - Internet Service Database,
- Inspekcja ruchu SSL i metody dystrybucji certyfikatów,
- Omówienie trybów pracy urządzenia – Proxy i Flow,
- Logowanie i powiadomienia, Konfiguracja przekazywania logów do FortiAnalyzera,
- Korzystanie z FortiCloud oraz FortiSandbox online,
- Omówienie FortiView,
- Konfiguracja funkcji ochronnych (profile bezpieczeństwa):
  - Ochrona antywirusowa,
  - Content Disarm and Reconstruction,
  - Filtrowanie antyspamowe,
  - System IPS / DoS Policy
  - Kontrola ruchu WWW / blokowanie URL / DNS Filter,
  - Kontrola aplikacji,
  - Reputacja klienta,
  - Data Leakage Prevention (DLP),
  - Web Application Firewall (WAF),
- Optymalizacja ruchu sieciowego (kształtowanie pasma),
- Konfiguracja połączeń SSL VPN,
- Wykorzystanie FortiClient do bezpiecznego łączenia z siecią FortiGate (m.in. IPsec),
- Konfiguracja rozwiązania FortiToken i zabezpieczanie dostępu do usług poprzez dwuskładnikowe uwierzytelnianie,
- Aktualizacja urządzeń UTM/NGFW. Konserwacja i bieżąca obsługa systemu.

7. Wymagania wobec Wykonawcy.

1) Przepustowość zdefiniowana dla poszczególnych przyłączy w ustępie 2 musi być gwarantowana przez Wykonawcę w punktach styku sieci IP Wykonawcy z sieciami IP operatorów Internetowych, z którymi Wykonawca posiada punkty styku.

2) Wykonawca musi posiadać, co najmniej 1 niezależny, bezpośredni punkty styku z Międzynarodowym Dostawcą Internetu.

3) Wykonawca musi posiadać, co najmniej 2 punkty styku z Krajowymi Dostawcami Internetowymi. Brak jakichkolwiek ograniczeń ruchu, w tym także do TPNET.

4) Wykonawca zabezpieczy przesyłane przez Zamawiającego dane w sposób zgodny z obowiązującymi aktualnie przepisami prawa.

5) Wykonawca musi ściśle współpracować przy aktualizacji i rozpropagowaniu nowych stref DNS Zamawiającego.

6) W celu odpowiedniego zabezpieczenia sieci Zamawiającego za pomocą urządzeń dostępowych i UTM/NGFW opisanych w ustępie 6, Wykonawca wyznaczy po swojej stronie inżyniera, który będzie współpracował z Zamawiającym w kwestiach odpowiedniej ochrony sieci za pomocą dostarczonych urządzeń UTM/NGFW. Do zadań inżyniera należeć będzie: pełnienie pierwszej linii wsparcia dla urządzeń UTM/NGFW, wsparcie przy aktualizacjach firmware, doradzanie Zamawiającemu w celu lepszego zabezpieczenia sieci i wprowadzania poprawek konfiguracyjnych do urządzeń UTM/NGFW, informowanie Zamawiającego o najnowszych zagrożeniach i metodach ochrony za pomocą urządzeń UTM/NGFW.

8. Dokumentacja powykonawcza.

Wykonawca dostarczy w formie papierowej i elektronicznej dokumentację powykonawczą. Dokumentacja powinna zawierać: schematy podłączenia sieci, informacje o przyznanej puli adresowej dla poszczególnych przyłączy, informacje potrzebnych do konfiguracji routingu do sieci Wykonawcy, informacje o serwerach DNS Dostawcy, konfiguracje urządzeń UTM/NGFW.

9. Poziom usług (SLA).

Poziom świadczonej usługi dostępu do Internetu dla wymienionych w ustępach 1 i 2 przyłączy nie może być niższy niż o poniższych parametrach:

1) Gwarantowana data aktywacji usługi, ustalona w SIWZ, umowie oraz w ustępie 4 niniejszej specyfikacji,

2) Gwarantowana miesięczna i roczna dostępność usługi na poziomie 99,8%,

3) Gwarantowane parametry połączenia:
   a) stała przepustowość, zgodnie ze specyfikacją określoną w ustępie 2,
   b) średni czas opóźnienia, zgodnie ze specyfikacją określoną w ustępie 2,
4) Gwarantowany czas reakcji na awarię: 1 godzina,

5) Gwarantowane usunięcie awarii w ciągu 8 godzin od momentu zgłoszenia lub wykrycia awarii przez Wykonawcę,

6) Dostępność służb technicznych 24 godziny/dobę, 7 dni w tygodniu przez wszystkie dni w roku,

7) Monitorowanie przez Wykonawcę łącza przez 24h/dobę, oraz zapewnienie Zamawiającemu możliwości całodobowego monitorowania łącza „online", jego wykorzystania i opisanych w niniejszym punkcie parametrów SLA,

8) Zamawiający zastrzega sobie możliwość stosowania kar umownych w wysokości 15% jednej miesięcznej opłaty abonamentowej danego przyłącza za każdorazowe niedotrzymanie uzgodnionych parametrów łącza internetowego (przepustowości i/lub czasu opóźnienia), mierzonych w sposób zdefiniowany w ustępie 3 formularza ofertowo-cenowego. Kara umowna w wysokości 15% jednej miesięcznej opłaty abonamentowej danego przyłącza liczona zostanie za każdą rozpoczętą godzinę ponad gwarantowany czas usunięcia usterki.

9) Zamawiający zastrzega sobie możliwość stosowania kar umownych w wysokości 15% jednej miesięcznej opłaty abonamentowej danego przyłącza za każdorazowe niedotrzymanie uzgodnionego w umowie terminu usunięcia awarii. Kara umowna w wysokości 15% jednej miesięcznej opłaty abonamentowej danego przyłącza liczona zostanie za każdą rozpoczętą godzinę ponad gwarantowany czas usunięcia usterki.

10) Zamawiający zastrzega sobie możliwość stosowania kar umownych w wysokości 15% jednej miesięcznej opłaty abonamentowej danego przyłącza za każdorazowe niedotrzymanie gwarantowanej miesięcznej dostępności mierzonej w sposób zdefiniowany w ustępie 3 formularza ofertowo-cenowego, rozliczana na koniec miesiąca. Kara umowna w wysokości 10% jednej miesięcznej opłaty abonamentowej danego przyłącza liczona zostanie za każdą rozpoczętą godzinę poniżej gwarantowanej dostępności miesięcznej.

11) Zamawiający zastrzega sobie możliwość stosowania kar umownych w wysokości 30% miesięcznej opłaty abonamentowej danego przyłącza za każdorazowe niedotrzymanie gwarantowanej rocznej dostępności mierzonej w sposób zdefiniowany w ustępie 3 formularza ofertowo-cenowego, rozliczana na koniec roku kalendarzowego. Kara umowna w wysokości 30% jednej miesięcznej opłaty abonamentowej danego przyłącza liczona zostanie za każdą rozpoczętą godzinę poniżej gwarantowanej dostępności rocznej.