

Porąbka, 05.06.2025 r.

## ZAPROSZENIE SZACOWANIE WARTOŚCI ZAMÓWIENIA

W związku z zamiarem przeprowadzenia postępowania publicznego pn.: **„Dostawa sprzętu informatycznego i oprogramowania – część 1”** będącego częścią projektu **„Cyberbezpieczna Gmina Porąbka”** finansowanego ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe” Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa”, **Wójt Gminy Porąbka**, jako Zamawiający zwraca się z prośbą o przedstawienie **szacunkowej wyceny dostaw** zgodnie z poniższą specyfikacją. **Oferowane dostawy muszą być zgodne z minimalnymi wymaganiami określonymi poniżej. Zakres zamówienia obejmuje dostawy wraz z transportem, rozładunkiem, instalacją i uruchomieniem:**

- 1) **Rozbudowa zapory sieciowej** - 1 sztuka
- 2) **Urządzenie UTM dla JO** - 1 sztuka

Zamawiający informuje, że niniejsze Zaproszenie nie stanowi:

- oferty w rozumieniu art. 66 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2023 r. poz. 1610, ze zm.),
- ani ogłoszenia o zamówieniu w rozumieniu ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (tj. Dz. U. z 2024 r. poz. 1320, ze zm.).

Celem Zaproszenia jest wyłącznie przeprowadzenie rozeznania rynku i uzyskanie informacji o szacunkowej wartości planowanego zamówienia publicznego.

Zamawiający prosi o przekazanie informacji na Formularzu szacowania zamówienia stanowiącym załącznik do Zaproszenia w terminie do **10 czerwca 2025 r.** za pośrednictwem poczty elektronicznej na adres: **anna.omasta@ug.porabka.pl**

Osobą uprawnioną do udzielania odpowiedzi na ewentualne pytania w zakresie przedmiotu szacowanych dostaw jest Główny Specjalista ds. **Informatyki Piotr Wojtusiak** tel. **510 258 304**, e-mail: [piotr.wojtusiak@ug.porabka.pl](mailto:piotr.wojtusiak@ug.porabka.pl)

**WÓJT GMINY PORĄBKA**

**Paweł Zemanek**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

L.P.	WYMAGANE MINIMALNE PARAMETRY JAKOŚCIOWE
<b>I.</b>	<b><i>Rozbudowa zapory sieciowej UTM</i></b>
<b>1</b>	<b>INFORMACJE OGÓLNE</b>
1)	Producent/Nazwa rozwiązania/Model
2)	Zamawiający obecnie używa zapory sieciowej UTM Fortigate 80f.
3)	W ramach rozbudowy należy dostarczyć kompatybilne urządzenie umożliwiające utworzenie klastra HA wraz z zapewnieniem jednolitej gwarancji na całość rozwiązania.
3)	Zamawiający dopuszcza rozwiązanie równoważne, w którym każde urządzenie musi spełniać minimalne wymagania parametrach zgodnie z pkt. 2 – pkt 18. Zamawiający zastrzega, że w przypadku oferowania rozwiązania równoważnego należy uwzględnić wdrożenie systemu, wraz z przeniesieniem całej konfiguracji i odzwierciedlenie usług na nowym rozwiązaniu – bez przerwy w dostępie do usług po stronie Zamawiającego i poza godzinami pracy urzędu.
<b>2</b>	<b>WYMAGANIA OGÓLNE</b>
1)	Rozwiązanie musi być dostarczone w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym.
2)	Musi być wyposażone w moduł TPM
3)	Rozwiązanie musi umożliwiać utworzenie klastra wysokiej dostępności HA co najmniej w trybie Active-Pasive
4)	Komunikacja klastra wysokiej dostępności musi być tworzona za pomocą redundantnych połączeń światłowodowych i odbywać się poprzez dwa interfejsy SFP
5)	System musi wspierać protokół LACP (Link Aggregation Control Protocol) zgodny z normą IEEE 802.3ad.
<b>3</b>	<b>INTERFEJSY</b>
1)	minimum 6 interfejsów 1 GbE RJ45
2)	minimum 2 interfejsy 1 GbE SFP
3)	Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1q.
<b>4</b>	<b>PAMIĘĆ</b>
1)	Dysk SSD o pojemności minimum 64GB
<b>5</b>	<b>ZASILANIE</b>
1)	Redundantny zasilacz o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujące w sieci 230V 50/60Hz.
<b>6</b>	<b>FUNKCJE BEZPIECZEŃSTWA</b>
1)	System ochrony musi realizować wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych: <ul style="list-style-type: none"> <li>– kontrola dostępu – zaporą ogniową klasy Stateful Inspection</li> <li>– kontrola stron Internetowych – Web Filter [WF]</li> <li>– kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3)</li> <li>– kontrola pasma oraz ruchu [QoS i Traffic shaping]</li> <li>– kontrola aplikacji oraz rozpoznawanie ruchu P2P</li> <li>– ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). Skanowanie AV dla plików typu: rar, zip;</li> <li>– ochrona przed atakami - Intrusion Prevention System [IPS/IDS]</li> <li>– poufność danych - IPSec VPN oraz SSL VPN</li> </ul> analiza ruchu szyfrowanego protokołem SSL
<b>7</b>	<b>FIREWALL</b>
1)	Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.

2)	Obsługa translacji NAT oraz PAT.
3)	Ochrona przed atakami DoS oraz DDoS (flood protection).
4)	Ochrona przed skanowaniem portów.
5)	Blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).
6)	Filtrowanie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów MAC.
7)	Możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
8)	Możliwość uwierzytelnienia i autoryzacji użytkowników w oparciu o bazę LDAP, zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
9)	Musi posiadać wbudowany posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10)	Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
<b>8</b>	<b>VPN</b>
1)	Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site.
2)	Wsparcie sieci VPN typu, minimum: PPTP VPN, IPSec VPN, SSL VPN
3)	Klient VPN producenta rozwiązania współpracujący z dostarczonym rozwiązaniem.
4)	Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
5)	Możliwość przełączania tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover)
6)	Praca w topologii Hub and Spoke oraz Mesh lub równoważnej.
7)	Obsługa mechanizmów minimum IPSec NAT Traversal, DPD, Xauth.
8)	Obsługa SSL VPN w trybach portal oraz tunel.
<b>9</b>	<b>IPS</b>
1)	Wykrywanie włamań oraz anomalii w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
2)	Usuwanie szkodliwej zawartości w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej bez blokowania dostępu do tej strony po usunięciu zagrożenia
3)	Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów.
4)	Wykrywanie anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS.
<b>10</b>	<b>ANTYWIRUS</b>
1)	Silnik antywirusowy musi zapewniać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2)	Możliwość pracy w trybie przezroczystego serwera poczty (Transparent Email Proxy)
3)	Automatyczna aktualizacja sygnatur zagrożeń.
4)	Ochrona przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.
5)	Inspekcja komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S.
6)	Wykrywanie, blokowanie i skanowanie załączników poczty email.
7)	Tworzenie białych i czarnych list adresów email.
8)	Wykrywanie spamu niezależnie od stosowanego języka.
9)	Musi korzystać minimum z dwóch różnych serwerów publikujących listy RBL.
<b>11</b>	<b>KONTROLA APLIKACJI</b>
1)	Kontrola ruchu na podstawie głębokiej analizy pakietów, nie bazującej jedynie na wartościach portów TCP/UDP.
2)	Wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook).
3)	Identyfikacja aplikacji niezależnie od wykorzystywanego portu, protokołu, szyfrowania.

<b>12</b>	<b>FILTR STRON WWW</b>
1)	Wbudowany filtr URL.
2)	Musi udostępniać kategorie minimum spam, hacking, malware, botnets.
3)	Baza filtra WWW musi umożliwiać grupowanie w kategorie tematyczne.
4)	Filtrowanie treści oraz szkodliwego oprogramowania w obrębie protokołów HTTP i HTTPS.
5)	Możliwość blokowania i wysyłania treści poprzez HTTP i HTTPS.
6)	Inspekcja z obsługą protokołu TLS 1.3.
7)	Filtrowanie plików na podstawie MIME.
<b>13</b>	<b>OBŚŁUGA ROUTINGU</b>
1)	Obsługa Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły minimum: RIPv2, OSPF, BGP.
2)	Możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.
3)	Trasowanie pakietów z poziomu wybranej reguły firewall (Policy Based Routing)
4)	Trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
5)	Możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).
6)	Możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza.
<b>14</b>	<b>WYDAJNOŚĆ</b>
1)	Przepustowość Firewall minimum 10 Gbps
2)	Przepustowość ochrony przed atakami (IPS) minimum 1 Gbps
3)	Wydajność VPN IPSec minimum 6 Gbps
4)	Minimalna liczba jednoczesnych połączeń: 1 500 000.
5)	Minimum 45.000 nowych połączeń na sekundę
<b>15</b>	<b>BEZPIECZEŃSTWO</b>
1)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
2)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
3)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych.
4)	Możliwość budowy architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.
5)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
<b>16</b>	<b>AKTUALIZACJA</b>
1)	Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
<b>17</b>	<b>ZARZĄDZANIE</b>
1)	Elementy systemu muszą zapewniać lokalne zarządzanie (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania.
2)	Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

3)	Interfejs administracyjny musi umożliwiać generowanie skryptów z czynności wykonywanych przez administratora.
4)	Interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
5)	Możliwość eksportowania logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
<b>18</b>	<b>CERTYFIKATY I DEKLARACJE</b>
1)	Element realizujący zadanie Firewall musi posiadać certyfikat ICSA lub EAL4+ lub równoważny dla rozwiązań kategorii Network Firewall.
2)	Deklaracja zgodności UE (certyfikat CE) potwierdzająca spełnienie wymagań dyrektywy „Nowego Podejścia”. Urządzenie musi posiadać oznakowanie CE.
3)	Certyfikat zgodności z dyrektywą RoHS lub dokument wystawiony przez niezależną, akredytowaną jednostkę potwierdzający spełnienie kryteriów środowiskowych zgodnych z dyrektywą RoHS o eliminacji substancji niebezpiecznych.
4)	Deklaracja zgodności z dyrektywą WEEE lub oświadczenie producenta o spełnieniu obowiązków w zakresie postępowania z odpadami WEEE i zgodności z Ustawą z 11 września 2015 o zużytym sprzęcie elektrycznym i elektronicznym (Dz.U. 2015 poz.1688). Urządzenie musi być oznaczone etykietą WEEE.
<b>II.</b>	<b>Urządzenie UTM dla JO</b>
<b>1</b>	<b>INFORMACJE OGÓLNE</b>
1)	Producent/Nazwa rozwiązania/Model
<b>2</b>	<b>WYMAGANIA OGÓLNE</b>
1)	Rozwiązanie musi być dostarczone w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym.
2)	Musi być wyposażone w moduł TPM
3)	Rozwiązanie musi umożliwiać utworzenie kanałów VPN pomiędzy urzędem a Jednostką organizacyjną.
4)	System ochrony musi realizować funkcjonalności minimum: <ul style="list-style-type: none"> <li>– poufność danych - IPSec VPN oraz SSL VPN</li> <li>– analiza ruchu szyfrowanego protokołem SSL</li> </ul>
5)	Rozwiązanie musi umożliwiać rozbudowę platformy o funkcjonalność bezpieczeństwa w zakresie (nie wymagane na etapie obecnego postępowania): <ul style="list-style-type: none"> <li>– kontrola dostępu – zapora ogniowa klasy Stateful Inspection</li> <li>– kontrola stron Internetowych – Web Filter [WF]</li> <li>– kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3)</li> <li>– kontrola pasma oraz ruchu [QoS i Traffic shaping]</li> <li>– kontrola aplikacji oraz rozpoznawanie ruchu P2P</li> <li>– ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). Skanowanie AV dla plików typu: rar, zip;</li> <li>– ochrona przed atakami - Intrusion Prevention System [IPS/IDS]</li> </ul>
6)	W przypadku potrzeby uruchomienia przez Zamawiającego funkcjonalności bezpieczeństwa jak w pkt 4, rozwiązanie musi spełniać wymagania funkcjonalne i wydajnościowe zgodne z pkt 8-15.
<b>3</b>	<b>INTERFEJSY</b>
1)	minimum 8 interfejsów 2,5GbE
2)	minimum 1 interfejs 1GbE SFP
<b>4</b>	<b>ZASILANIE</b>
1)	Zasilacze redundantne o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujące w sieci 230V 50/60Hz.
<b>5</b>	<b>VPN</b>

1)	Przepustowość VPN IPSec AES-GCM minimum 2 Gbps
2)	Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site.
3)	Wsparcie sieci VPN typu, minimum: PPTP VPN, IPSec VPN, SSL VPN
4)	Klient VPN producenta rozwiązania współpracujący z dostarczonym rozwiązaniem.
5)	Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
6)	Możliwość przełączania tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover)
7)	Praca w topologii Hub and Spoke oraz Mesh lub równoważnej.
8)	Obsługa mechanizmów minimum IPSec NAT Traversal, DPD, Xauth.
9)	Obsługa SSL VPN w trybach portal oraz tunel.
10)	Obsługa bezpłatnego mechanizmu uwierzytelniania dwuskładowego do generowania kodów jednorazowych np. Google Authenticator
<b>6</b>	<b>BEZPIECZEŃSTWO</b>
1)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
2)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
3)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych.
4)	Możliwość budowy architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.
5)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
<b>7</b>	<b>ZARZĄDZANIE</b>
1)	Elementy systemu muszą zapewniać lokalne zarządzanie (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania.
2)	Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3)	Interfejs administracyjny musi umożliwiać generowanie skryptów z czynności wykonywanych przez administratora.
4)	Interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
5)	Możliwość eksportowania logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
<b>8</b>	<b>FIREWALL</b>
1)	Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2)	Obsługa translacji NAT oraz PAT.
3)	Ochrona przed atakami DoS oraz DDoS (flood protection).
4)	Ochrona przed skanowaniem portów.
5)	Blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).
6)	Filtrowanie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów MAC.
7)	Możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
8)	Możliwość uwierzytelnienia i autoryzacji użytkowników w oparciu o bazę LDAP, zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.

9)	Musi posiadać wbudowany posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10)	Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
<b>9</b>	<b>IPS</b>
1)	Wykrywanie włamań oraz anomalii w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
2)	Usuwanie szkodliwej zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej bez blokowania dostępu do tej strony po usunięciu zagrożenia
3)	Wykrywanie anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS.
<b>10</b>	<b>ANTYWIRUS</b>
1)	Silnik antywirusowy musi zapewniać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2)	Możliwość pracy w trybie przezroczystego serwera poczty (Transparent Email Proxy)
3)	Automatyczna aktualizacja sygnatur zagrożeń.
4)	Ochrona przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.
5)	Inspekcja komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S.
6)	Wykrywanie, blokowanie i skanowanie załączników poczty email.
7)	Tworzenie białych i czarnych list adresów email.
8)	Wykrywanie spamu niezależnie od stosowanego języka.
9)	Musi korzystać minimum z dwóch różnych serwerów publikujących listy RBL.
<b>11</b>	<b>FILTR STRON WWW</b>
1)	Wbudowany filtr URL oparty o technologię w chmurze z możliwością tworzenia własnych kategorii.
2)	Filtr URL musi mieć możliwość korzystania z adresów WWW dostępnych w chmurze.
3)	Musi udostępniać kategorie minimum spam, hacking, malware, botnets.
4)	Baza filtra WWW musi umożliwiać grupowanie w kategorii tematyczne.
5)	Filtrowanie treści oraz szkodliwego oprogramowania w obrębie protokołów HTTP i HTTPS.
6)	Możliwość blokowania i wysyłania treści poprzez HTTP i HTTPS.
7)	Inspekcja z obsługą protokołu TLS 1.3.
8)	Filtrowanie plików na podstawie MIME.
<b>12</b>	<b>KONTROLA APLIKACJI</b>
1)	Kontrola ruchu na podstawie głębokiej analizy pakietów, nie bazującej jedynie na wartościach portów TCP/UDP.
2)	Wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook).
3)	Identyfikacja aplikacji niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
<b>13</b>	<b>OBŚŁUGA ROUTINGU</b>
1)	Obsługa Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły minimum: RIPv2, OSPF, BGP.
2)	Możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.
3)	Trasowanie pakietów z poziomu wybranej reguły firewall (Policy Based Routing)
4)	Trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
5)	Możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).
6)	Możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza.



<b>14</b>	<b>WYDAJNOŚĆ</b>
1)	Wydajność systemu Firewall minimum 8 Gbps
2)	Wydajność ochrony przed atakami (IPS) minimum 4 Gbps
3)	Minimalna liczba jednoczesnych połączeń: 300.000.
4)	Minimum 25.000 nowych połączeń na sekundę
<b>15</b>	<b>AKTUALIZACJA</b>
1)	Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
<b>16</b>	<b>CERTYFIKATY I DEKLARACJE</b>
1)	Deklaracja zgodności UE (certyfikat CE) potwierdzająca spełnienie wymagań dyrektywy „Nowego Podejścia”. Urządzenie musi posiadać oznakowanie CE.
2)	Certyfikat zgodności z dyrektywą RoHS lub dokument wystawiony przez niezależną, akredytowaną jednostkę potwierdzający spełnienie kryteriów środowiskowych zgodnych z dyrektywą RoHS o eliminacji substancji niebezpiecznych.
3)	Deklaracja zgodności z dyrektywą WEEE lub oświadczenie producenta o spełnieniu obowiązków w zakresie postępowania z odpadami WEEE i zgodności z Ustawą z 11 września 2015 o zużytym sprzęcie elektrycznym i elektronicznym (Dz.U. 2015 poz.1688). Urządzenie musi być oznaczone etykietą WEEE.
4)	Certyfikat ICSA Labs dla funkcji VPN IPsec lub urządzenie musi znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE
5)	Certyfikat Common Criteria lub oświadczenie producenta potwierdzające bezpieczeństwo systemu zgodnie z wymaganiami normy ISO 15408.
6)	Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall musi posiadać certyfikat ICSA lub EAL4+ lub równoważny dla rozwiązań kategorii Network Firewall.
<b>III.</b>	
<b>1</b>	<b>INSTALACJA I MONTAŻ</b>
1)	Zamawiający wymaga dostarczenia wszelkich komponentów potrzebnych do zamontowania dostarczonych urządzeń, wniesienia i instalacji urządzeń oraz do połączenia urządzeń do infrastruktury pasywnej (np. szyny montażowe, przewody krosowe RJ45 2m – po 2 sztuki dla każdego dostarczonego urządzenia sieciowego, przewody zasilające, osprzęt montażowy).
2)	Wymagana instalacja dostarczonych urządzeń posiadających obudowę przeznaczoną do montażu stelażowego, we wskazanej przez Zamawiającego szafie RACK 19”.
3)	Urządzenia muszą być montowane za pośrednictwem szyn montażowych lub uchwytów dostarczonych wraz z urządzeniami.
4)	Zamawiający wymaga wykonanie wszystkich połączeń urządzeń, niezbędnych do uruchomienia całości środowiska.
<b>2</b>	<b>KONFIGURACJA</b>
1)	Zamawiający wymaga konfigurację i uruchomienie dostarczonego urządzenia w trybie wysokiej dostępności z istniejącym urządzeniem Fortigate 80F. Po przeprowadzeniu konfiguracji wymagane jest przeprowadzenie testów poprawności działania. Konfiguracja i uruchomienie urządzeń nie może zakłócać i destabilizować pracy urzędu.
2)	System UTM dla JO musi zapewniać szyfrowaną wymianę danych z urządzeniem zainstalowanym w Urzędzie. Musi być skonfigurowany zgodnie z wytycznymi administratora Zamawiającego.