



Fundusze  
Europejskie  
Polska Cyfrowa



Rzeczpospolita  
Polska

Unia Europejska  
Europejski Fundusz  
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Numer sprawy: ZP.271.21.2022.MK

## Szczegółowy Opis Przedmiotu Zamówienia

**„Zakup zapory sieciowej typu UTM, serwera, serwera NAS, licencji na oprogramowanie do backup-u, licencji Windows Serwer 2022 STD, licencji dostępowych Windows Server 2022 CAL oraz usług wdrożeniowych oraz konfiguracji w ramach projektu Grantowego Cyfrowa Gmina”**

## Zawartość

|   |          |
|---|----------|
| <b>I. Szczegółowy Opis Przedmiotu zamówienia – Zakup zapory sieciowej typu UTM, serwera, serwera NAS, licencji na oprogramowanie do backup-u, licencji Windows Serwer 2022 STD, licencji dostępowych Windows Server 2022 CAL oraz usług wdrożeniowych oraz konfiguracji. ....</b> | <b>3</b> |
| 1. Zestawienie ilościowe.....   | 3        |
| 1.1 Wymagania ogólne w zakresie dostawy sprzętu.....  | 3        |
| 1.2 Zasada równoważności rozwiązań. ....  | 4        |
| 1.3 Zakup i konfiguracja zapory sieciowej typu UTM.....   | 5        |
| 1.4 Zakup serwera .....   | 9        |
| 1.5 Zakup serwera NAS.....  | 13       |
| 1.6 Licencja na oprogramowanie do backup-u .....  | 14       |
| 1.7 Licencja Windows Serwer 2022 Standard .....   | 14       |
| 1.8 Licencje dostępne Windows Server 2022 CAL.....  | 15       |
| 1.9 Usługa wdrożenia oraz konfiguracji Firewalla/UTM, wdrożenia oraz konfiguracji serwera wraz z serwerem NAS, wdrożenia, konfiguracji wirtualizatora Hyper-V wraz z instalacją maszyn wirtualnych oraz implementacja mechanizmu backupu.....                                     | 15       |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## I. Szczegółowy Opis Przedmiotu zamówienia – Zakup zapory sieciowej typu UTM, serwera, serwera NAS, licencji na oprogramowanie do backup-u, licencji Windows Serwer 2022 STD, licencji dostępowych Windows Server 2022 CAL oraz usług wdrożeniowych oraz konfiguracji.

### 1. Zestawienie ilościowe.

Doposażenie serwerowni przez zakup serwera i przełącznika sieciowego oraz zakup laptopa.

| Lp. | Nazwa   | Ilość  |
|-----|---|--------|
| 1.  | Zakup i konfiguracja zapory sieciowej typu UTM  | 1 szt. |
| 2.  | Zakup serwera   | 1 szt. |
| 3.  | Zakup serwera NAS   | 1 szt. |
| 4.  | Licencja na oprogramowanie do backup-u  | 1 szt. |
| 5.  | Licencja Windows Serwer 2022 STD  | 2 szt. |
| 6.  | Licencje dostępowe Windows Server 2022 CAL - 5 User CALs (CAL'e per user dla 15 użytkowników)   | 3 szt. |
| 7.  | Usługa wdrożenia oraz konfiguracji Firewalla/UTM, wdrożenia oraz konfiguracji serwera wraz z serwerem NAS, wdrożenia, konfiguracji wirtualizatora Hyper-V wraz z instalacją maszyn wirtualnych oraz implementacja mechanizmu backupu. | 1 szt. |

#### 1.1 Wymagania ogólne w zakresie dostawy sprzętu.

1. Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nie noszący oznak użytkowania.
2. Dostarczony sprzęt musi być fabrycznie nowy (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą się znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzenia pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.

## 1.2 Zasada równoważności rozwiązań.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań, materiałów i urządzeń służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne.
5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całość systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.
9. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają

minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

### 1.3 Zakup i konfiguracja zapory sieciowej typu UTM

Minimalne parametry techniczne urządzenia:

#### 1. Wymagania Ogólne:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. System realizujący funkcję ochrony sieci musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Ochrony w warstwie aplikacji,
- Protokołów routingu dynamicznego.

#### 2. Redundancja, monitoring i wykrywanie awarii:

- W przypadku systemu pełniącego funkcje: IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klastrer active-active lub active-passive. W obu trybach powinna istnieć funkcja synchronizacji sesji ochrony sieci.
- Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.
- Monitoring stanu realizowanych połączeń VPN.

#### 3. Interfejsy, dysk, zasilanie:

- System realizujący funkcję ochrony sieci musi dysponować minimum 10 portami Gigabit Ethernet RJ-45.
- System ochrony sieci musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
- W ramach systemu ochrony sieci powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

#### 4. Parametry wydajnościowe:

- W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
- Przepustowość Stateful dla ochrony sieci: nie mniej niż 10 Gbps dla pakietów 512 B.

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

- Przepustowość ochrony sieci z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.8 Gbps.
- Wydajność szyfrowania IPsec VPN nie mniej niż 16,5 Gbps.
- Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
- Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
- Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 630 Mbps.

#### 5. Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

- Kontrola dostępu - zaporą ogniową klasy Stateful Inspection;
- Kontrola Aplikacji;
- Poufność transmisji danych - połączenia szyfrowane IPsec VPN oraz SSL VPN;
- Ochrona przed malware - co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS;
- Ochrona przed atakami - Intrusion Prevention System;
- Kontrola stron WWW;
- Kontrola zawartości poczty - Antyspam dla protokołów SMTP, POP3;
- Zarządzanie pasmem (QoS, Traffic shaping);
- Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP);
- Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site;
- Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
- Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

#### 6. Polityki, Firewall:

- Polityka ochrony sieci musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
- System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: Translację jeden do jeden oraz jeden do wielu; Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
- W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
- Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hashe złośliwych plików.
- Element systemu realizujący funkcję ochrony sieci musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu: Amazon Web Services (AWS); Microsoft Azure; Google Cloud Platform (GCP); OpenStack; VMware NSX;

#### 7. Połączenia VPN:

- System musi umożliwiać konfigurację połączeń typu IPsec VPN. W zakresie tej funkcji musi zapewniać: Wsparcie dla IKE v1 oraz v2; Obsługa szyfrowania protokołem AES z kluczem 128 i

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

256 bitów w trybie pracy Galois/Counter Mode(GCM); Obsługa protokołu Diffie-Hellman grup 19 i 20; Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE; Tworzenie połączeń typu Site-to-Site oraz Client-to-Site; Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności; Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego; Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth; Mechanizm „Split tunneling” dla połączeń Client-to-Site.

- System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0; Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta; Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

#### **8. Routing i obsługa łączy WAN:**

- W zakresie routingu rozwiązanie powinno zapewniać obsługę: Routingu statycznego; Policy Based Routingu; Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
- System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
- Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

#### **9. Zarządzanie pasmem:**

- System ochrony sieci musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
- Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
- System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

#### **10. Kontrola Antywirusowa:**

- Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
- System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
- System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
- System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
- System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

#### **11. Ochrona przed atakami:**

- Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
- System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
- Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
- System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

- Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
- Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

#### 12. Kontrola aplikacji:

- Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
- Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
- Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

#### 13. Kontrola WWW:

- Moduł kontroli WWW musi korzystać z bazy adresów URL pogrupowanych w kategorie tematyczne.
- W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
- Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
- Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
- Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
- Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
- W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

#### 14. Uwierzytelnianie użytkowników w ramach sesji:

- System ochrony sieci musi umożliwiać weryfikację tożsamości użytkowników za pomocą: Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu; Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP; Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
- Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
- Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
- Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

#### 15. Zarządzanie:

- Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
- Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
- Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

- System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
- System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
- Element systemu pełniący funkcję ochrony sieci musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji ochrony sieci.
- Element systemu realizujący funkcję ochrony sieci musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

#### 16. Logowanie:

- W ramach logowania system pełniący funkcję ochrony sieci musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
- Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
- Musi istnieć możliwość logowania do serwera SYSLOG.

#### 17. Serwisy i licencje:

- Z urządzeniem należy dostarczyć licencje upoważniające do korzystania w okresie gwarancji na urządzenie z aktualnych baz funkcji ochronnych producenta i serwisów w zakresie: kontrola aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), analiza typu Sandbox, antyspam, web filtering, bazy reputacyjne adresów IP/domen.
- Trzyletnia gwarancja producenta.
- Dostawa nowego urządzenia do 8 godzin od awarii. Wsparcie w reżimie 24x7 w językach angielskim i polskim.
- W ramach dostawy wykonawca dokona pełnego wdrożenia oferowanego przedmiotu zamówienia wg wytycznych Zamawiającego.

## 1.4 Zakup serwera

Minimalne parametry techniczne urządzenia:

### 1. Obudowa

- Obudowa Rack o wysokości max 1U z możliwością instalacji do 4 dysków 3.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
- Obudowa z możliwością wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.

### 2. Płyta główna

- Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

### 3. Chipset

- Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych

### 4. Procesor

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Zainstalowany jeden procesor 8-rdzeniowy, min. 2.8 GHz (Turbo Speed min. 3.6 GHz), klasy x86 dedykowany do pracy z zaferowanym serwerem umożliwiający osiągnięcie **wyniku min. 27350** w teście Average CPU Mark dostępnym na stronie <https://www.cpubenchmark.net/>.

5. RAM
  - 64GB DDR4 RDIMM 3200MT/s,
  - Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.
  - Płyta główna powinna obsługiwać do 1TB pamięci RAM.
6. Funkcjonalność pamięci RAM
  - Memory Rank Sparing,
  - Memory Mirror,
  - Failed DIMM isolation,
  - Memory Address Parity Protection,
  - Memory Thermal Throttling
7. Gniazda PCI
  - Minimum dwa sloty PCIe x16 generacji 4
8. Interfejsy sieciowe/FC/SAS
  - Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
9. Dyski twarde
  - Możliwość instalacji dysków SAS, SATA, SSD
  - Zainstalowane 4 dyski SSD SATA o pojemności min. 1,92 TB, 6Gb/s, 2,5" Hot-Plug.
  - Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.
  - Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde
10. Kontroler RAID
  - Sprzętowy kontroler dyskowy posiadający min. 4GB nieulotnej pamięci cache, umożliwiającą konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
  - Wsparcie dla dysków SED.
11. Wbudowane porty
  - Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej,
  - Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
12. Video
  - Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
13. Wentylatory
  - Redundantne
14. Zasilacze
  - Redundantne,
  - Hot-Plug maksymalnie 550W.
15. Bezpieczeństwo
  - Zatrzaszk górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej.
  - Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

- BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
  - Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
  - Moduł TPM 2.0
  - Możliwość dynamicznego włączania i wyłączenia portów USB na obudowie – bez potrzeby restartu serwera
  - Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
16. Diagnostyka
- Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
17. Karta Zarządzania
- Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:
- zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
  - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
  - szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;
  - możliwość podmontowania zdalnych wirtualnych napędów;
  - wirtualną konsolę z dostępem do myszy, klawiatury;
  - wsparcie dla IPv6;
  - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
  - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
  - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
  - integracja z Active Directory;
  - możliwość obsługi przez dwóch administratorów jednocześnie;
  - wsparcie dla dynamic DNS;
  - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
  - możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
  - możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
18. Oprogramowanie do zarządzania
- Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
  - integracja z Active Directory
  - Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
  - Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
  - Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
  - Szczegółowy opis wykrytych systemów oraz ich komponentów
  - Możliwość eksportu raportu do CSV, HTML, XLS, PDF
  - Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
  - Grupowanie urządzeń w oparciu o kryteria użytkownika
  - Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
  - Szybki podgląd stanu środowiska
  - Podsumowanie stanu dla każdego urządzenia
  - Szczegółowy status urządzenia/elementu/komponentu
  - Generowanie alertów przy zmianie stanu urządzenia.
  - Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
  - Integracja z service desk producenta dostarczonej platformy sprzętowej
  - Możliwość przejęcia zdalnego pulpitu
  - Możliwość podmontowania wirtualnego napędu
  - Kreator umożliwiający dostosowanie akcji dla wybranych alertów
  - Możliwość importu plików MIB
  - Przesyłanie alertów „as-is” do innych konsol firm trzecich
  - Możliwość definiowania ról administratorów
  - Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
  - Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
  - Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
  - Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
  - Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
  - Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
  - Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile.
  - Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
  - Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
  - Zdalne uruchamianie diagnostyki serwera.
  - Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
  - Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
19. Certyfikaty
- Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.
  - Serwer musi posiadać deklaracja CE.
  - Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
20. Warunki gwarancji
- 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.
  - Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

- Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
- Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
- Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.

#### 21. Dokumentacja użytkownika

- Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
- Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

## 1.5 Zakup serwera NAS

Protokoły sieciowe serwera plików zapewniające komunikację ze wszystkimi obecnymi na rynku systemami operacyjnymi jak i również systemami wirtualizacji VMware 4 vSphere4 (ESX 4.0 i nowsze), Citrix i Hyper-V. Serwer jest to idealne rozwiązanie dla gromadzenia i udostępniania danych w sieci lokalnej oraz w Internecie dla małych jak i średnich firm oraz użytkowników indywidualnych, w tym także poprzez protokół iSCSI. Urządzenie wspiera Microsoft Active Directory i linuxowy system plików NFS. Dodatkowo bezpieczeństwo zapewnia szyfrowanie danych kluczem AES 256bit.

Minimalne parametry techniczne urządzenia:

1. Procesor: Zainstalowany procesor 4-rdzeniowy/4-wątkowy, maksymalna częstotliwość 2.9 GHz, dedykowany do pracy z zaferowanym serwerem umożliwiający osiągnięcie wyniku min. 4000 w teście Average CPU Mark dostępnym na stronie <https://www.cpubenchmark.net/>.
2. Architektura procesora: 64-bitowy x86
3. Procesory graficzne: Tak
4. Koprocesor arytmetyczny FPU: Tak
5. Mechanizm szyfrowania: Tak (AES-NI)
6. Transkodowanie wspomagane sprzętowo: Tak
7. Pamięć systemowa: 4 GB SODIMM DDR4 (1 x 4 GB)
8. Maksymalna pojemność pamięci: 16 GB (2 x 8 GB)
9. Gniazdo pamięci: 2 x SODIMM DDR4
10. Pamięć flash: 4 GB (ochrona systemu operacyjnego przed podwójnym rozruchem)
11. Wnęka dysków: 4 dyski 3,5-calowe SATA 6 Gb/s, 3 Gb/s
12. Kompatybilność dysków:
  - 3,5-calowe dyski twarde SATA
  - 2,5-calowe dyski twarde SATA
  - 2,5-calowe dyski SSD SATA
13. Dysk serwerowy: 4x 8 TB 3.5" SATA III (6 Gb/s)
14. Wymieniany podczas pracy: Tak
15. Gniazdo M.2: 2 gniazda M.2 2280 PCIe Gen 3 x1
16. Obsługa przyspieszenia pamięci podręcznej SSD: Tak

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

17. Port 2,5 Gigabit Ethernet (2,5G/1G/100M): 2 (2,5G/1G/100M/10M)
18. Wake on LAN (WOL): Tak
19. Ramka Jumbo: Tak
20. Porty:
  - USB 2.0: 2x
  - Port USB 3.2 Gen 2 (10 Gb/s): 2x Type A USB 3.2 Gen 2
  - Wyjście HDMI: 1, HDMI 1.4b
21. Kształt: 1U, do montażu stelażowego
22. Wskaźniki LED: Zasilanie/stan, LAN, USB, HDD1-4, M.2 SSD 1-2
23. Przyciski: Zasilanie, reset
24. Zasilacz: 100W PSU, 100–240 V
25. Pobór mocy: Tryb uśpienia – HDD: 21,105 W
26. Pobór mocy: Tryb pracy, typowy: 35,297 W
27. Wentylator: 3 x 40mm
28. Ostrzeżenie systemowe: Brzęczyk
29. Maks. liczba połączeń współbieżnych (CIFS) — z maks. pojemnością pamięci: 1500
30. Co najmniej 24 miesięczna gwarancja producenta.

## 1.6 Licencja na oprogramowanie do backup-u

Rozwiązanie do ochrony danych w środowiskach VMware, Hyper-V oraz Cloud jak i również w chmurze Amazon EC2. Dzięki łatwemu i szybkiemu wdrożeniu pozwala w kilka minut rozpocząć wykonywanie backupu obrazów maszyn wirtualnych, a tym samym pozwala na szybkie przywrócenie systemu do działania w przypadku awarii.

Najważniejsze funkcje:

- backup bezagentowy,
- wsparcie dla najnowszych wersji systemów wirtualizacji – Microsoft Hyper-V 2016 oraz VMware vSphere 6.5,
- licencjonowanie per gniazdo fizycznego procesora,
- kompresja i deduplikacja w obrębie całego repozytorium backupu,
- łatwe wyszukiwanie i kasowanie niepotrzebnych backupów,
- weryfikacja backupu i migawek,
- ochrona kontenera,
- pomijanie plików tymczasowych i pliku wymiany,
- szyfrowanie przy użyciu AES256bit,
- replikacja backupu,
- przywracanie na poziomie plików,
- backup off-site, do Amazon Cloud i MS Azure,
- obsługa backupu on-line aplikacji krytycznych,
- kompatybilność z oferowanym serwerem NAS.

## 1.7 Licencja Windows Serwer 2022 Standard

Opis wymagań (wymagania minimalne dla równoważnego oprogramowania):

- ilość licencji – 2 szt.
- Polska wersja językowa
- współpraca z procesorami o architekturze 64 bit

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

- instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym
- w ramach dostarczonej licencji zawarta możliwość instalacji oprogramowania na serwerze wyposażonym w 2 rdzenie
- Jednostka licencjonowana na 16 rdzeni procesora
- praca w roli serwera domeny Microsoft Active Directory
- zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP)
- zawarta możliwość uruchomienia roli serwera DNS
- zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP)
- zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory
- zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory
- zawarta możliwość uruchomienia roli serwera stron WWW
- w ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera
- w ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych
- wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją wieczystą (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

## 1.8 Licencje dostępne Windows Server 2022 CAL

Opis wymagań (wymagania minimalne dla równoważnego oprogramowania):

- ilość licencji – 5 User CAL - 3 licencje (CAL'e per user dla 15 użytkowników dla Windows Server)
- Polska wersja językowa
- licencje dla użytkownika typu CAL uprawniająca do korzystania z usług takich jak drukowanie sieciowe, przechowywanie plików w systemie Windows Server 2020 (ActiveDirectory).

## 1.9 Usługa wdrożenia oraz konfiguracji Firewalla/UTM, wdrożenia oraz konfiguracji serwera wraz z serwerem NAS, wdrożenia, konfiguracji wirtualizatora Hyper-V wraz z instalacją maszyn wirtualnych oraz implementacja mechanizmu backupu.

### 1. Konfiguracja serwera fizycznego oraz maszyn wirtualnych HyperV z funkcjonalnością serwera backupu

- 1) Instalacja fizyczna elementów rozwiązania.
  - Krosowanie interfejsów Ethernet management, frontend i backend;
  - Konfiguracja interfejsów zarządzających serwerów;
  - Podłączenie zasilania;
  - Aktualizacja firmware.
- 2) Konfiguracja urządzeń sieciowych pod kątem rozwiązania wirtualizacji.

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

- 3) Instalacja systemów operacyjnych (min. Windows Server 2019); aktualizacja.
  - 4) Konfiguracja usług klastrowych Hyper-V.
    - Definicja sieci wirtualnych;
    - LiveMigration.
  - 5) Instalacja i konfiguracja maszyn wirtualnych (Windows Server).
  - 6) Utworzenie obrazu wzorcowego maszyny wirtualnej (Windows Server).
  - 7) Instalacja dostarczonego oprogramowania do tworzenia kopii zapasowych na dedykowanym serwerze NAS.
    - Konfiguracja lokalnych zasobów serwera jako repozytorium backupu;
    - Konfiguracja zadań backupowych dla nowego środowiska;
    - Weryfikacja bacupu - odtworzenie wybranej maszyny.
  - 8) Weryfikacja działania środowiska.
  - 9) Utworzenie dokumentacji powykonawczej.
  - 10) Konfiguracja i przeniesienie programów z poprzednich serwerów: BeSTi@, QNET, Płatnik, Mikrobot Akcyza, EGB-L GEOBAZA, Legislador, Program FK, Program Środki Trwałe, Program Podatki.
- 2. Konfiguracja usług Active Directory i zdalnego dostępu (RDS)**
    - 1) Uruchomienie funkcjonalności serwera AD na wybranej maszynie wirtualnej.
    - 2) Konfiguracja polityk Active Directory dotycząca urządzeń i użytkowników.
    - 3) Konfiguracja dostępu do wybranych zasobów.
    - 4) Instalacja usług serwera terminali na maszynie wirtualnej i konfiguracja usług RDS.
  - 3. Instalacja i konfiguracja urządzeń brzegowych sieci**
    - 1) Instalacja i konfiguracja urządzeń UTM.
      - Konfiguracja funkcjonalności UTM (firewall, AV, IPS, VPN, WebFiltering...);
      - Aktualizacja firmware i baz UTM;
      - Konfiguracja zdalnego dostępu i autentykacji poprzez token;
      - Konfiguracja VLAN i routingu.
  - 4. Konfiguracja urządzeń sieciowych - LAN**
    - 1) Konfiguracja switchy LAN.
  - 5. Konfiguracja serwera NAS**
  - 6. Szkolenia**
    - 1) Szkolenie z zakresu wybranego przez Zamawiającego obejmującego zainstalowane rozwiązanie – liczone w dniach roboczych, dostosowane do wymagań poszczególnych jednostek.