Załącznik nr 1 do SWZ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Spis treści

[I. WSTĘP 1](#_Toc169510938)

[II. DEFINICJE 2](#_Toc169510939)

[III. PRZEDMIOT ZAMÓWIENIA 3](#_Toc169510940)

[IV. SPRZĘT KOMPUTEROWY WRAZ Z OPROGRAMOWANIEM 4](#_Toc169510941)

[V. SZKOLENIA 27](#_Toc169510942)

# WSTĘP

1. Celem niniejszego dokumentu jest przedstawienie wszystkich wymagań funkcjonalnych, systemowych oraz technicznych jakie muszą spełniać rozwiązania informatyczne dostarczane w ramach przedmiotowego postępowania.
2. W ramach realizacji przedmiotu zamówienia Wykonawca zapewni spełnienie wszystkich wymagań ujętych w Specyfikacji Warunków Zamówienia.
3. Wykonawca zobligowany jest do dostarczenia Zamawiającemu dokumentacji dostarczanych w ramach zamówienia rozwiązań.
4. Wykonawca dostarczy wymagane oprogramowanie i przekaże niezbędne licencje Zamawiającemu w ilościach wymaganych do prawidłowej pracy wdrażanych systemów.
5. Wszelkie prace związane z dostarczeniem przedmiotu zamówienia, jego konfiguracji oraz montażu stanowią koszt własny Wykonawcy.
6. Po zgłoszeniu przez Wykonawcę zakończenia prac Zamawiający przeprowadzi procedurę Odbioru Końcowego, podczas której dokona weryfikacji i potwierdzenia wypełnienia przez Wykonawcę wszystkich zobowiązań, jakie były przedmiotem realizacji zamówienia.

# DEFINICJE

|  |  |
| --- | --- |
| **Definicja/skrót** | **Opis** |
| OPZ | Opis przedmiotu zamówienia. |
| PDF | (ang. Portable Document Format) – format plików służący do prezentacji, przenoszenia i drukowania treści tekstowo-graficznych, stworzony przez firmę Adobe Systems. |
| RAM | (ang. random-access memory) - podstawowy rodzaj pamięci cyfrowej. |
| SWZ | Specyfikacja Warunków Zamówienia. |
| TCP | (ang. Transmission Control Protocol) - Protokół sterowania transmisją, protokół kontroli transmisji, połączeniowy, niezawodny, strumieniowy protokół komunikacyjny stosowany do przesyłania danych między procesami uruchomionymi na różnych maszynach. |
| CPD | Centrum Przetwarzania Danych |

# PRZEDMIOT ZAMÓWIENIA

1. Na realizację zadania składają się następujące elementy :
2. dostawa, wdrożenie i konfiguracja dwóch serwerów wraz z niezbędnym oprogramowaniem;
3. dostawa, wdrożenie i konfiguracja macierzy dyskowej produkcyjnej wraz z niezbędnym oprogramowaniem;
4. dostawa, wdrożenie i konfiguracja urządzenia brzegowego UTM;
5. Utworzenie klastra wysokiej dostępności HA w oparciu o dostarczone serwery i macierz dyskową oraz posiadany przez zamawiającego serwer.
6. dostawa, wdrożenie i konfiguracja wirtualizatora niezbędnego do budowy klastra HA;
7. Migracja posiadanych przez zamawiającego serwerów wirtualnych na nowo utworzone środowisko klastra HA;
8. przeprowadzenie szkoleń dla personelu Zamawiającego w zakresie administrowania i użytkowania wdrażanych rozwiązań
9. Szczegółowy opis wymagań wyżej wymienionych elementów został przedstawiony w dalszej części niniejszego dokumentu.
10. Produkty lub usługi określają minimalne parametry jakościowe i cechy użytkowe, jakim muszą odpowiadać produkty lub usługi oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego.
11. Z uwagi na zachowanie ciągłości działania pracy Zamawiającego Przedmiot Zamówienia realizowany będzie poza godzinami pracy urzędu lub w dni wolne od pracy (np. weekend).

Wyjątek stanowi szkolenie dla personelu Zamawiającego w zakresie administrowania i użytkowania wdrażanych rozwiązań, które mogą odbyć się w godzinach pracy urzędu.

# SPRZĘT KOMPUTEROWY WRAZ Z OPROGRAMOWANIEM

1. Wymagania ogólne :
2. Zamawiający w ramach realizacji przedmiotu zamówienia wymaga dostarczenia infrastruktury teleinformatycznej pozwalającej na uruchomienie wdrażanych rozwiązań. Zamawiający wymaga aby Wykonawca dostarczył wyspecyfikowany sprzęt i systemy wraz z wszystkimi niezbędnymi elementami pozwalającymi na jego instalację i uruchomienie w siedzibie Zamawiającego. Wykonawca zobowiązany jest dostarczyć wszystkie urządzenia do miejsca wskazanego w siedzibie Zamawiającego, a następnie zainstalować je, odpowiednio skonfigurować oraz sprawdzić poprawność ich działania. Wykonawca we własnym zakresie zapewni transport i rozładunek dostarczonych elementów zgodnie z wytycznymi Zamawiającego. Dostarczony sprzęt musi być fabrycznie nowy, nie starszy niż 6 miesięcy od daty produkcji i musi pochodzić z legalnego kanału dystrybucji producenta znajdującej się na terenie Polski. Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych oraz roszczeń osób trzecich. Wykonawca wraz z dostarczonymi urządzeniami musi przekazać Zamawiającemu dokumenty uzyskane od producenta, że sprzęt jest fabrycznie nowy i pochodzi z oficjalnego kanału sprzedaży na rynek Polski (ze względu na wymagania gwarancyjno-serwisowe opisane niżej), i że wraz ze wszystkimi komponentami objęty jest gwarancją, potwierdzoną przez producenta. Dla firm nie mających siedziby na terenie Rzeczpospolitej Polskiej, dopuszcza się urządzenia pochodzące z oficjalnego kanału sprzedaży producenta w UE, pod warunkiem, że spełnione zostaną wymagania gwarancyjno-serwisowe, co do czasu reakcji na zgłoszenie i całkowitej obsługi w języku polskim, potwierdzone odpowiednią umową z punktem serwisowym w Polsce producenta tych urządzeń, którą należy przekazać wraz z dostarczonym sprzętem. Wszystkie wymagane parametry są parametrami minimalnymi, Zamawiający dopuszcza zaproponowanie sprzętu z parametrami wyższymi niż wymienione poniżej.
3. W przypadku zmiany, modyfikacji lub rozbudowy sieci logicznej LAN zamawiającego na którą zamawiający posiada 25 letnią gwarancję, na zmienione elementy sieci Wykonawca udzieli gwarancji nie krótszej niż posiadana przez Zamawiającego.
4. Serwer produkcyjny – 2 sztuki (wraz z drobnymi akcesoriami)

Akcesoria:

Mysz bezprzewodowa ergonomiczna **1 szt.**

* Typ: optyczna, pionowa, dla praworęcznych,
* Komunikacja z myszą: bezprzewodowa,
* Liczba przycisków: 5 szt,
* Rolka przewijania Nano odbiornik,
* Rozdzielczość do 2400 dpi,
* Ergonomiczna, pozwalająca podtrzymać dłoń w wyprostowanej, neutralnej postawie, zapobiegając skręcaniu przedramienia.

Przewód 5-metrowy USB KVM z 3w1 SPHD i wbudowanym konwerterem PS/2 na USB

**– 6 szt.**

* Złącze PC: HDB i USB,
* Złącze konsoli: SPHD 3 w 1 (klawiatura/mysz/grafika),
* Długość: 5 m,
* wbudowany konwerter PS/2 na USB

Dostarczany kabel ma być kompatybilny z konsolą KVM CL5708N-ATA-AG 19"

Model: CL5708N posiadaną przez Zamawiającego.

Obudowa:

* Typu RACK, wysokość nie więcej niż 2U;
* Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
* Możliwość zainstalowania 10 dysków twardych hot plug;
* Zainstalowane 2 szt. dysków SSD SATA 480GB Hot-Plug skonfigurowane w RAID podpięte do sprzętowego kontrolera;
* Zainstalowany wewnętrzny napęd DVD-RW;
* Możliwość zainstalowania dedykowanego przez producenta serwera wewnętrznego napędu blu-ray

Płyta główna:

* Dwuprocesorowa;
* Wyprodukowana i zaprojektowana przez producenta serwera;
* Możliwość instalacji procesorów 38-rdzeniowych;
* Możliwość zainstalowania modułu TPM 2.0;
* 7 złącz PCI Express generacji 4 w tym:
  + 4 fizyczne złącza o prędkości x16;
  + 3 fizyczne złącza o prędkości x8;
  + Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
  + Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e;
* 32 gniazda pamięci RAM;
* Obsługa minimum 4 TB pamięci RAM DDR4;
* Obsługa 10 TB pamięci operacyjnej w konfiguracji RAM DDR4 + pamięć nieulotna;
* Wsparcie dla technologii:
  + Memory Scrubbing;
  + SDDC;
  + ECC;
  + Memory Mirroring;
  + ADDDC;
* Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci);
* Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug.

Procesory:

* Dwa procesory 12-rdzeniowe
* Taktowanie 3,2GHz
* architektura x86\_64
* osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base minimum 187 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wyniki testów stanowią załącznik do opisu przedmiotu zamówienia.

Pamięć RAM:

* 256 GB pamięci RAM
* DDR4 Registered
* 3200Mhz

Kontrolery LAN:

* Interfejsy LAN nie zajmujące dostępnych slotów PCI Express, minimum 2x 1Gbit Base-T + 2x 10Gbit SFP+ ;
* Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;
* Do każdego interfejsu LAN należy dołożyć wymaganą ilość wkładek SFP+, tak aby żaden port nie pozostał bez wkładki

Kontrolery I/O:

* Kontroler SAS RAID dla dysków wewnętrznych posiadający 8GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania;

Porty:

* Zintegrowana karta graficzna ze złączem VGA z tyłu i z przodu serwera;
* 1 port USB 3.0 wewnętrzny;
* 2 porty USB 3.0 dostępne z tyłu serwera;
* 2 porty USB 3.0 na panelu przednim
* Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
* Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;

Zasilanie, chłodzenie:

* Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy minimalnej 900W;
* Redundantne wentylatory hotplug;

Zarządzanie:

* Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii
* informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
  + karty rozszerzeń zainstalowane w dowolnym slocie PCI Express
  + procesory CPU
  + pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM
  + wbudowany na płycie głównej nośnik pamięci M.2 SSD
  + status karty zrządzającej serwera
  + wentylatory
  + bateria podtrzymująca ustawienia BIOS płyty główne
  + zasilacze
* system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym)
* Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
  + Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
  + Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
  + Dostęp poprzez przeglądarkę Web, SSH;
  + Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
  + Zarządzanie alarmami (zdarzenia poprzez SNMP)
  + Możliwość przejęcia konsoli tekstowej
  + Możliwość zarządzania przez 2 administratorów jednocześnie
  + Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)
  + Obsługa serwerów proxy (autentykacja)
  + Obsługa VLAN
  + Możliwość konfiguracji parametru Max. Transmission Unit (MTU)
  + Wsparcie dla protokołu SSDP
  + Obsługa protokołów TLS 1.2, SSL v3
  + Obsługa protokołu LDAP
  + Synchronizacja czasu poprzez protokół NTP
  + Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej
* Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
* Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

Wspierane systemy:

* Microsoft Windows Server 2022, 2019, 2016
* VMWare vSphere 6.7
* Hyper-V Server
* Suse Linux Enterprise Server 12,
* Red Hat Enterprise Linux 7, 8,

Gwarancja:

* 3 lata gwarancji producenta serwera w trybie on-site z gwarantowanym przyjazdem technika serwisu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.
* Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
* Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
* Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;

Dokumentacja, inne:

* Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy do oferty oraz producenta do protokołu odbioru sprzętu;
* Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w PL lub UE – wymagane oświadczenie wykonawcy do oferty oraz producenta do protokołu odbioru sprzętu;
* Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, na etapie zawierania umowy należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;
* W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
* Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

1. Macierz dyskowa 1 sztuka

System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie Rack 19” z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii. Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy lub musi być dostarczona licencja na dwukrotność dostarczanej pojemności. Dostarczana macierz musi umożliwiać takie podłączenie półek aby awaria lub/i usunięcie jednej z półek nie powodowało utraty dostępu do danych znajdujących się na pozostałych modułach. Oferowana macierz musi obsługiwać min. 260 dysków wykonanych w technologii hot-plug. Wszystkie zainstalowane dyski hot-plug, z wyłączeniem dysków SSD stosowanych jako rozszerzenie pamięci Cache kontrolerów, muszą być dostępne dla zapisu danych Zamawiającego. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów (tzw. „półek dyskowych”) w rozmiarze 2U pozwalająca umieścić do 24 dysków 2,5” typu hot-plug dla dysków SAS i SSD oraz w rozmiarze 2U dla 12 dysków 3,5” typu hot-plug NL-SAS i SSD oraz półki gęstego upakowania dla 60 dysków typu hot-plug SAS, NL-SAS i SSD; Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych (tj. 2,5” + 3,5” + gęstego upakowania).

**Pojemność macierzy:**

Minimum 12 TB powierzchni dostępnej dla hostów na dyskach SSD SAS w konfiguracji minimum RAID-6 + minimum 1szt. dysk typu hot spare. (16 dysków 960 GB SSD SAS)

**Wydajność macierzy:**

Oferowana konfiguracja musi osiągać minimum 150 000 IOPS przy czasie odpowiedzi nie większym niż 0,40 ms przy zachowaniu parametrów:

Stosunek odczytów do zapisów: 80:20

Wielkość bloku: 4KB

Trafienia w cache przy odczycie: nie więcej niż 40%

Trafienia w cache przy zapisie: nie więcej niż 10%

Oferowana wydajność musi być potwierdzona przez dedykowane narzędzie producenta (do oferty należy dostarczyć potwierdzony przez producenta wydruk z narzędzia, który umożliwi zweryfikowanie wymaganej wydajności macierzy)

**Kontrolery:**

* Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami;
* Każdy z kontrolerów macierzy musi posiadać po minimum 64 GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych przeznaczonych do zapisu;
* Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 800 GB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD;
* W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk.
* Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia;
* Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach;
* Każdy z kontrolerów RAID powinien posiadać dedykowany minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy;
* Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej z minimum 4 rdzeniami;
* Kontrolery macierzy muszą obsługiwać do 70 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów;
* Oferowana macierz musi mieć wyprowadzone 2 porty iSCSI 10 Gb/s SFP+ MMF LC do dołączenia serwerów bezpośrednio lub do sieci SAN (Storage Area Network), na każdy kontroler RAID;
* Do każdego interfejsu LAN należy dołożyć wymaganą ilość wkładek SFP+ MMF LC, tak aby żaden port nie pozostał bez wkładki;
* Macierz musi umożliwiać dołożenie do każdego z kontrolerów portów do transmisji danych (bez konieczności usuwania istniejących):
* 4 x FC 16 Gb/s,
* 2 x iSCSI 10 Gb/s SFP+,
* 2 x SAS 12 Gb/s,
* 2 x FC 32 Gb/s;
* Dołożenie portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu, a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych;
* Macierz musi posiadać obsługę operacji plikowych I/O w sieci NAS w obrębie zainstalowanych kontrolerów. Protokoły dostępu: CIFS, NFS. W przypadku obsługi protokołów CIFS i NFS wymagana jest funkcjonalność agregacji przepustowości dla interfejsów dedykowanych do obsługi tych protokołów. Obsługa protokołów CIFS i NFS musi odbywać się jednocześnie (nie jest wymagane dostarczenie tej funkcjonalności - opcja rozbudowy).

**Poziomy RAID:**

Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:

* Raid-1;
* Raid-10;
* Raid-5;
* Raid-50;
* Raid-6.

**Dyski:**

* Oferowana macierz musi wspierać dyski hot-plug:
* dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS 12 Gb/s
* dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm,
* Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania;
* Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex
* Macierz musi obsługiwać min. 260 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami;
* Możliwość rozbudowy oferowanego modelu macierzy do minimum 520 dysków bez migracji i przenoszenia danych - jedynie poprzez wymianę modułu kontrolerów macierzy (bez konieczności wymiany posiadanych dysków, półek dyskowych, bez konieczności przenoszenia danych/ istniejącej struktury grup dyskowych/LUN, jak również z zachowaniem istniejącej gwarancji producenta na półki dyskowe i dyski;
* Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug, jako wirtualną przestrzeń zapasową lub jako dysk hot spare (dysk zapasowy) i mieć możliwość:
* konfiguracji dysku hot spare dla zabezpieczenia dowolnej grupy dyskowej RAID,
* konfiguracji dysku hot spare dedykowanego dla zabezpieczenia tylko wybranej grupy dyskowej RAID;
* W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego, wymiana uszkodzonego dysku na sprawny, nie może powodować powrotnego kopiowania danych z dysku hot spare na wymieniony dysk lub nie wymaga zwolnienia zapasowej przestrzeni wirtualnej;
* Macierz musi pozwalać na zaszyfrowanie danych zapisanych na wszystkich obsługiwanych dyskach SSD-SAS, HDD-SAS oraz HDD NL-SAS minimum kluczem AES256-bit dla danych blokowych – jeżeli w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą. Macierz musi umożliwiać zaszyfrowanie całej dostępnej powierzchni użytkowej minimum kluczem AES256-bit.

**Opcje programowe:**

* Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 2048 kopii migawkowych;
* Macierz musi umożliwiać zdefiniowanie min. 8000 woluminów (LUN);
* Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów;
* Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową;
* Macierz musi posiadać wsparcie dla systemów operacyjnych: Microsoft Windows Server 2012R2, 2016, 2019, 2022, SuSE Linux Enterprise Server, Red Hat Linux Enterprise Server, Vmware Vsphere, Hyper-V Server;
* Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI;
* Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy;
* Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy;
* Macierz musi obsługiwać mechanizm ochrony priorytetów obsługi wybranych zasobów – za taki mechanizm uznaje się funkcję typu ‘cache partitioning’ lub ‘storage partitioning’;
* Macierz musi obsługiwać adresację IP v.4 i IP v.6;
* Wraz z macierzą należy dostarczyć oprogramowanie lub moduły programowe typu plug-in pozwalające na integracje macierzy w środowiskach Vmware w zakresie obsługi mechanizmów: Vmware VAAI, Vmware VVOL, Vmware MultiPath IO – z subskrypcją do bezpłatnej aktualizacji w całym okresie obowiązywania gwarancji;
* Macierz musi obsługiwać mechanizmy przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy ( tzw. Thin Provisioning);
* Macierz musi obsługiwać mechanizmy automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy ( tzw. AST (Automated Storage Tiering). Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SSAS, NLSAS. Macierz musi pozwalać na definiowanie różnych polityk i zasad migrowania danych w obrębie tej samej macierzy. Mechanizm AST musi pozwalać na definiowanie okna czasowego dla zbierania pomiarów wydajności operacji I/O oraz okna czasowego dla migrowania danych wg ustalonych zasad i polityk – minimalny definiowany czas trwania w/w operacji (długość okna czasowego) nie może być dłuższy niż 4 godziny. Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy;
* Mechanizm AST musi być obsługiwać funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) mierzonej jako maksymalny czas opóźnień operacji I/O wykonywanych przez serwer/środowisko/aplikację (nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy);
* Macierz musi wspierać usługi VSS (Volume ShadowCopy Services) w systemach klasy Microsoft Windows Server – wymagane jest dostarczenie niezbędnego oprogramowania / sterowników VSS pozwalających na obsługę VSS przy maksymalnej pojemności i liczbie dysków obsługiwanych przez oferowaną. W czasie trwania gwarancji wymaga się bezpłatnego dostępu do nowych wersji oprogramowania i sterowników;
* Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy tej klasy, z zachowaniem obsługi operacji I/O dla serwerów podłączonych do migrowanej macierzy tj. do migrowanych zasobów LUN;
* Macierz musi wspierać rozwiązania klasy ‘klastra macierzowego’ tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami protokołami FC oraz iSCSI. Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC oraz iSCSI, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy. Pod użytym pojęciem ‘wysoka dostępność zasobów dyskowych’ należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzą, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Funkcjonalność ‘klastra macierzowego’ musi pozwalać na automatyczne i ręczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. Automated/manual failover). Nie jest wymagane dostarczenie tej funkcjonalności, jest to opcja rozbudowy.
* Macierz w dostarczonej konfiguracji musi obsługiwać deduplikację i kompresję danych na dyskach wbudowanych w macierzy (nie dopuszcza się główek, kompresji zewnętrznej, programowej itp.) w następujących trybach równocześnie oraz niezależnie na poziomie każdego LUN:
  + Sama deduplikacja wybranego LUN;
  + Sama kompresja wybranego LUN;
  + Kombinacja technologii kompresji i deduplikacji wybranego LUN;
  + Brak użycia technologii kompresji i deduplikacji dla wybranego LUN;

**Zarządzanie:**

* Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej;
* Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.
* Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora;
* Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI.

**Gwarancja i serwis:**

* Całe rozwiązanie musi być objęte minimum 36 miesięcznym okresem gwarancji producenta z całkowitą obsługą w języku polskim (wraz z obsługą zgłoszenia awarii do producenta) oraz naprawą w miejscu instalacji urządzenia i gwarantowanym czasem przyjazdu serwisanta na miejsce awarii do końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy;
* Uszkodzone dyski nie podlegają zwrotowi organizacji serwisowej;
* Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia;
* Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania, bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy oraz do kolejnych wersji oprogramowania zarządzającego w okresie minimum 2 lat;
* System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół. Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA. Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta – musi być do tego wykorzystany dedykowany system serwisowy macierzy;
* Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia;
* Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy macierzy najpóźniej w następnym dniu roboczym od zgłoszenia usterki;
* Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – na etapie zawierania umowy należy podać adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje.

1. UTM na potrzeby klastra HA – 1 sztuka

Zamawiający posiada zainstalowany i skonfigurowany UTM SonicWall 3600 wraz z wykupionym wsparciem. Zamawiający wymaga dostarczenia nowego urządzenia oraz skonfigurowania go w identyczny sposób jak posiadane, zapewniając działanie wszystkich systemów w sposób nie gorszy niż zastany. W przypadku zmiany konfiguracji na lepszą/wydajniejszą/bezpieczniejszą, wszystkie wprowadzone zmiany musza zostać zaakceptowane przez zamawiającego.

Wymagane parametry UTM:

Funkcjonalność:

* Firewall musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2)
* Firewall musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF i BGP
* Firewall musi obsługiwać policy based routing
* Firewall musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPoE) na zewnętrznym interfejsie
* Firewall musi obsługiwać DHPC v6 na zewnętrznym interfejsie
* Firewall musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP, jako bridge (transpartent mode) lub z tym samym adresem IP na wszystkich portach.
* Firewall musi mieć możliwość obsługi wielu łączy zewnętrznych z opcją balansowania ruchu.
* Firewall musi mieć możliwość obsługi łącza zapasowego typu LTE
* Firewall musi obsługiwać Dynamic DNS
* Firewall musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1
* Firewall musi obsługiwać translację portów: PAT
* Firewall musi obsługiwać IPSec NAT traversal
* Firewall musi obsługiwać mechanizm policy-based NAT
* Firewall musi obsługiwać VLAN 802.1Q
* Firewall musi zapewniać ochronę przed atakami stosującymi techniki unikania wykrycia, np. fragmentacja pakietów
* Firewall musi obsługiwać pracę jako serwer DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
* Firewall musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP
* Firewall musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
* Firewall musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP,SecureID oraz wewnętrznej bazy użytkowników.
* Firewall musi umożliwiać transparentne uwierzytelnianie użytkowników przez Active Directory.
* Urządzenie musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z Microsoft Terminal Services
* Urządzenie nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
* Firewall musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji
* Firewall musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
* Firewall musi obsługiwać mechanizmy Protocol Anomaly Detection (PAD) dla najpopularniejszych protokołów.
* Firewall musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: http, https, ftp, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP
* Firewall musi zapewniać ochronę z wykorzystaniem mechanizmów IPS
* Firewall musi zapewniać ochronę antywirusową dla obsługiwanych protokołów
* Firewall musi zapewniać możliwość filtrowania URL
* Firewall musi zapewniać inspekcję ruchu szyfrowanego https
* Firewall musi zapewniać ochronę przed niechcianą pocztą (AntySPAM)
* Firewall musi zapewniać rozpoznawanie aplikacji w oparciu o analizę ruchu sieciowego a nie wyłącznie nr portu.
* Urządzenie musi mieć możliwość filtrowania treści według typu MIME
* Urządzenie musi umożliwiać sterowanie przepustowością w oparciu o następujące parametry: użytkownik, grupa, protokół, polisa, interfejs sieciowy, adres IP, sieć VLAN, aplikacja i kategoria aplikacji
* Firewall musi udostępniać mechanizmy limitowania dostępu do sieci użytkownikom w oparciu o kwoty czasowe lub transferu danych.
* Firewall musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site

Wydajność:

Firewall musi zapewnić obsługę na poziomie minimalnym:

* 5.8 Gpbs dla pracy w trybie firewall,
* 1.18 Gbps dla pracy w trybie UTM (z włączonymi mechanizmami AV and IPS)

Firewall musi obsługiwać 3 500 000 jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną 34 tys. nowych połączeń na sekundę

* Ilość obsługiwanych sieci VLAN: min 100
* Minimalna ilość portów 10/100/1000 BaseT: 8 z możliwością rozbudowy

Funkcje VPN:

* Urządzenie musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz TLS
* Urządzenie musi w zakresie IPSec site-to-site VPN współpracować z rozwiązaniami innych producentów
* Rozwiązanie musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256
* Rozwiązanie musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, 3rd Party Cert.
* Wsparcie dla Dead Peer Detection (DPD)
* Urządzenie musi obsługiwać IKEv1 i IKEv2
* Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman do wymiany kluczy przez email i web
* Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego) z podtrzymaniem zestawionych połączeń TCP
* Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu
* Urządzenie musi obsługiwać statyczne i dynamiczne (routowane) połaczenia VPN do dostawców chmury obliczeniowej (AWS i MS Azzure)
* Urządzenie musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP.
* Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android
* Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu
* Urządzenie ma zapewnia funkcję portalu dostępowego chronionego przez szyfrowanie https (TLS)

Wydajność VPN:

* Przepustowość IPSec VPN nie mniejsza niż 800 Mbps
* Obsługa nie mniej niż: 75 tuneli IPSec site-to-site
* Obsługa nie mniej niż: 75 tuneli client-to-site

Filtrowanie zawartości URL:

* Urządzenie musi umożliwiać filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji
* Funkcjonalność filtrowania zawartości powinna dawać możliwość filtrowania stron według minimalnie 120 kategorii
* Rozwiązanie musi pozwalać na tworzenie białych list wyjątków dla filtrowania zawartości
* Baza zawartości URL powinna być dostępna on-line lub do ściągnięcia i zainstalowania miejscowo
* Funkcja powinna filtrować treści w wielu językach, w tym w języku polskim
* Filtrowanie musi obsługiwać również protokół https
* Urządzenie musi umożliwiać wyłączenie inspekcji https dla wybranych kategorii stron www
* System kategoryzacji stron musi posiadać kategorie: Command&control, Proxy avoidance, Botnets, Malicious sites, Phishing, Spyware

Kontrola aplikacyjna:

* System kontroli aplikacyjnej musi rozpoznawać aplikacje oraz kategorie aplikacji
* Aplikacje muszą być rozpoznawana w oparciu o analizę ruchu a nie przez porty i protokoły
* Ilość rozpoznawanych aplikacji nie mniejsza niż 1800
* W ramach konkretnej aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe)
* Kontrola aplikacyjna musi rozpoznawać co najmniej aplikacje: Tor, CryptoAdmin, Proxy service, Peer-to-peer, VoIP, MS Office 365, Gry online

Antywirus:

* System musi mieć możliwość uruchomienia co najmniej 2 skanerów antywirusowych
* Aktualizacja plików sygnatur antywirusowych musi się odbywać automatycznie
* Aktualizacja plików sygnatur antywirusowych musi się odbywać nie rzadziej niż co 12 godzin.
* Antywirus musi mieć możliwość przeprowadzania kwarantanny e-mail.
* Jeden ze skanerów antywirusowych musi bazować na mechanizmach bezsygnaturowych
* Rozwiązanie musi mieć możliwość tworzenia wyjątków w białej liście, aby umożliwić nieblokowany dostęp do poczty z określonych domen
* Wykrywanie i blokowanie spyware’u
* Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji
* Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS
* System musi zapewniać możliwość zablokowania ransomware uruchomionego na stacjach roboczych i serwerach.
* Przepustowość AV w urządzeniu nie mniejsza niż 1.47 Gbps

Antyspam:

* Antyspam powinien być oparty na technologii RPD - Recurrent Pattern Detection
* Antyspam powinien zapewnić możliwość kwarantanny e-mail
* Antyspam powinien posiadać zintegrowaną antywirusową analizę spamu
* Rozwiązanie powinno umożliwić blokowanie spamu w wielu językach w tym w języku polskim
* Możliwość blokowania spamu opartego na obrazach graficznych.

IPS:

* Automatyczna aktualizacja sygnatur IPS
* IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy
* Automatyczne blokowanie znanych źródeł ataków
* System musi pozwalać na blokowanie ataków typu DoS i DDoS
* Przepustowość IPS w urządzeniu nie mniejsza niż 1,3 Gbps

Antymalware:

* System musi zapewniać ochronę przed nieznanym złośliwym oprogramowaniem, na zasadzie analizy behawioralnej (sandbox).
* System musi pracować w trybie lokalnym lub z wykorzystaniem mechanizmów chmury (w granicach Unii Europejskiej)
* Analizie muszą podlegać pliki ściągane przez http(s) i przesyłane pocztą elektroniczną.
* System musi zapewniać ogólne oszacowanie poziomu ryzyka dla analizowanych plików oraz udostępniać szczegółowe informacje o wykrytych działaniach niebezpiecznych.
* System musi mieć możliwość blokowania poczty zawierającej podejrzane załączniki do czasu zakończenia ich analizy
* Skuteczność wykrywania malware’u – minimum 98% (potwierdzone zewnętrznymi testami)

Ochrona przed phishingiem:

* System musi zapewniać dedykowaną (poza ochroną przed SPAMem) ochronę przed phishingiem
* System winien blokować możliwość dostępu do spreparowanych stron.
* System musi blokować dostęp niezależnie od użytego protokołu czy portu komunikacyjnego
* Zablokowanie dostępu musi być odpowiednio notyfikowane użytkownikowi, którego dotyczy, niezależnie od logów i raportów
* System musi chronić przed nadużyciem protokołu DNS

Zarządzanie:

* Administracja urządzenia musi być możliwa poprzez graficzny interfejs zarządzania w czasie rzeczywistym.
* Urządzenie musi umożliwiać zarządzanie za pomocą linii poleceń poprzez port szeregowy lub poprzez SSH.
* Urządzenie musi umożliwiać zarządzanie za pomocą wbudowanego interfejsu www.
* Interfejs WWW do zarządzania urządzeniem powinien mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
* Urządzenie może być zarządzane jednocześnie z wielu platform przez różnych administratorów.
* Rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
* Rozwiązanie musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
* Rozwiązanie musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według harmonogramu
* System powinien zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
* Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
* System powinien posiadać metodę porównywania różnych wersji konfiguracji.
* Obsługa różnych ról administratorów.
* Umożliwia monitorowanie logów ruchu w czasie rzeczywistym.
* System powinien posiadać możliwość stworzenia mapy sieci wewnętrznej zawierającej szczegółowe dane urządzenia (MAC, IP, System operacyjny, otwarte porty)
* Urządzenie musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
* System zarządzania musi zapewniać korelację zdarzeń dotyczących konkretnych komputerów pochodzących z systemów ochrony sieciowej i z chronionych komputerów
* System zarządzania musi posiadać graficzną konsolę do zarządzania systemem VPN działającą w trybie drag-and-drop

Dzienniki i raporty:

* Rozwiązanie musi umożliwiać zbieranie i przechowywanie dzienników i raportów.
* Rozwiązanie musi umożliwiać przesyłanie logów do co najmniej 2 serwerów dziennika
* Dzienniki transmisji muszą być szyfrowane.
* Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
* Rozwiązanie musi udostępniać narzędzie analizy całości ruchu
* Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa
* Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów czy rozmiaru bazy danych
* Rozwiązanie musi umożliwiać zapis logów w zewnętrznej bazie danych oraz stały dostęp w celu analizy i generowania raportów.
* Rozwiązanie musi posiadać minimum 90 predefiniowanych typów raportów.
* Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie
* System powinien mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.
* System powinien być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania tych sprawozdań pocztą e-mail.
* Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
* System raportowania powinien być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów i dzienników.
* System powinien wspierać automatyczne wysyłanie wszystkich typów raportów pocztą elektroniczną.
* Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
* System musi umożliwiać pseudoanonimizację użytkowników z prawem do deanonimizacji tylko dla wybranych administratorów
* System powinien zapewniać wizualizację, opisującą w trybie graficznym stan przepustowości systemu.
* System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.

**Gwarancja i serwis:**

* Urządzenie musi być objęte serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia. W przypadku jego wadliwości urządzenie musi być wymieniane na nowe na koszt producenta na drugi dzień roboczy po zgłoszeniu uszkodzenia wraz z pełną konfiguracją nowego urządzenia. W ramach przedmiotu zamówienia musi zostać dostarczona licencja aktywacyjna dla wszystkich wymaganych funkcji, upoważniająca do pobierania pełnej aktualizacji, oraz do korzystania z wsparcia producenta przez okres 36 miesięcy.
* **Możliwość odpłatnego wydłużenia gwarancji producenta do 5 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy najpóźniej w następnym dniu roboczym od zgłoszenia usterki;**
* Wsparcie producenta jest świadczone 24 godziny na dobę i 7 dni w tygodniu  
  Czas reakcji na zgłoszenia wg priorytetu:
* w przypadku błędów krytycznych uniemożliwiających pracę urzędu – natychmiastowo
* w przypadku błędów ważnych – 1h
* w przypadku błędów standardowych utrudniających pracę urzędu - 4h
* Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia;
* w okresie udzielonej gwarancji, w przypadku braku możliwości usunięcia awarii w ciągu 1 dnia roboczego zobowiązuję się dostarczyć sprzęt zastępczy na czas naprawy o nie gorszych parametrach niż uszkodzony;
* Producent oferowanego UTM musi posiadać dedykowaną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu gwarancyjnym należy podać adres internetowy strony producenta UTM, gdzie można zweryfikować wymagane informacje.
* naprawa dostarczonego sprzętu będzie wykonywana przez producenta macierzy lub autoryzowanego partnera producenta (firma serwisująca posiada ISO 9001:2000 na świadczenie usług serwisowych);
* serwis gwarancyjny będzie świadczony w siedzibie zamawiającego;
* serwis gwarancyjny obejmuje dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia;
* system zapewnia możliwość samodzielnego i automatycznego powiadamiania administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół.
* po wykonaniu naprawy, UTM zostanie przywrócony do stanu pełnej gotowości do pracy, tj. zgodnie ze stanem jak przed wystąpieniem awarii;

1. System operacyjny serwera – uprawniającego do postawienia 4 maszyn wirtualnych na każdym z 2 serwerów

* Ze względu na spójność środowiska i zapewnienie niezawodności platformy wirtualizacyjnej oraz uniknięcie zagrożeń mogących powstać na styku produktów różnych producentów serwerowy system operacyjny musi być kompatybilny z posiadanymi przez Zamawiającego serwerami, macierzami, oprogramowaniem do wirtualizacji oraz oprogramowaniem do tworzenia kopii zapasowych i ściśle ze sobą współpracować.

Zamawiający podaje, iż posiada stacje robocze podłączone do wewnętrznej sieci komputerowej pracujące na systemie operacyjnym Microsoft Windows 11, Microsoft Windows 10 oraz Microsoft Windows 7 zarządzalne domeną Active Directory.

Dostarczony serwerowy system operacyjny musi być w wersji najnowszej na dzień złożenia oferty, z uwzględnieniem specyfiki oferowanego sprzętu przez Wykonawcę.

* Zamawiający wymaga dostarczenia licencji na każdy dostarczany serwer, licencja musi obejmować wszystkie rdzenie fizycznych procesorów zainstalowanych w dostarczanych serwerach.
* Licencje na zamawiany serwerowy system operacyjny muszą być bezterminowe.
* Licencje muszą obejmować najnowszą (najwyższą) wersję oprogramowania, dostępną na dzień złożenia oferty.
* Z uwagi na szeroki zakres funkcjonalny planowanego wdrożenia na bazie zamawianego oprogramowania oraz konieczności minimalizacji kosztów związanych z wdrożeniem, szkoleniami i eksploatacją systemów, Zamawiający wymaga aby zaoferowane licencje, umożliwiały wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania i monitorowania.
* Wymagane jest zapewnienie możliwości korzystania z wcześniejszych wersji zamawianego oprogramowania (umożliwia downgrading)
* Wymagane jest udostępnienie podstawowych informacji na temat instalacji i użytkowania oprogramowania na witrynie producenta systemu
* Możliwość uruchomienia oprogramowania serwerowego firm trzecich dedykowanego na system Windows Serwer 2019 lub nowszy
* Możliwość wykorzystania co najmniej 2 logicznych procesorów oraz co najmniej 3 GB pamięci RAM w środowisku fizycznym
* Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
* Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez instytucję lub firmę upoważnioną do wydawania certyfikatu bezpieczeństwa danych. Za równoważny Zamawiający uzna certyfikat potwierdzający bezpieczeństwo danych.
* Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
* Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
* Graficzny interfejs użytkownika
* Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
* Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
* Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa
* Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
  + Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
  + Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe) z możliwością wykorzystania następujących funkcji:
    - Podłączenie SSOW do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
    - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
    - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
  + Zdalna dystrybucja oprogramowania na stacje robocze,
  + Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
  + Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego, umożliwiające:
    - Dystrybucję certyfikatów poprzez http,
    - Konsolidację CA dla wielu lasów domen,
    - Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen.
  + Szyfrowanie plików i folderów,
  + Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
  + Możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów,
  + Serwis udostępniania stron WWW,
  + Wsparcie dla protokołu IP w wersji 6 (IPv6),
  + Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, posiadanymi przez Zamawiającego,
  + Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 2 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
* Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
* Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
* Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
* Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
* Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
* Nabycie licencji oprogramowania pozwala na legalne używanie posiadanych przez Zamawiającego licencji oprogramowania w tym na serwerowy system operacyjny maszyn wirtualnych
* Ważność licencji na serwer fizyczny i serwerowy system operacyjny maszyn wirtualnych nie jest ograniczona czasowo.

1. Licencje dostępowe do systemu operacyjnego serwera – 70 licencji

Zamawiający wymaga dostarczenia wraz z systemem operacyjnym serwera, o którym mowa w pkt. 5) licencji dostępowych „na użytkownika” i dla urządzeń w ilości 70 licencji.

Licencje dostępowe muszą być dedykowane do danej wersji dostarczanego systemu operacyjnego.

1. System do backupu – licencja na 2 hosty

Wykonawca dostarczy zainstaluje, skonfiguruje oraz przeniesienie na zamawiającego własność licencji na oprogramowanie do backupu środowiska wirtualizacyjnego - licencje na 2 hosty wraz z 36 miesięcznym wsparciem.

Wymagania ogólne oprogramowania do backupu środowiska wirtualnego:

* Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk Data Center.
* Oprogramowanie musi współpracować z dostarczoną infrastrukturą.
* Oprogramowanie musi współpracować z hostami zarządzanymi przez wirtualizator oraz pojedynczymi hostami.
* Oprogramowanie musi współpracować z hostami zarządzanymi przez system centralny, klastrami hostów oraz pojedynczymi hostami.
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych.

Całkowite koszty posiadania licencji:

* Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
* Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
* Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: pełny, przyrostowy.
* Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
* Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu.
* Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej.
* Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków

Wymagania Recovery Point Objective:

* Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
* Oprogramowanie musi wspierać kopiowanie plików na taśmy
* Oprogramowanie musi mieć możliwość tworzenia retencji
* Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
* Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc

Wymagania Recovery Time Objective

* Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny.
* Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
* Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
* Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
* Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć.
* Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
  + Linux
  + ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
  + BSD
  + UFS, UFS2
  + ZFS, UFS
  + HFS, HFS+
  + Windows
  + NTFS, FAT, FAT32, ReFS
* Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
* Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
* Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.

Monitoring:

* System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego
* System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej
* System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
* System musi dawać możliwość podłączenia się do kilku instancji i serwerów jednocześnie, w celu centralnego monitorowania wielu środowisk
* System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
* System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
* System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
* System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
* System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

Raportowanie:

* System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej,
* System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
* System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
* System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
* System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
* System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
* System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
* System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
* System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
* System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy
* System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
* System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

1. System do wirtualizacji środowiska serwerowego – 3 fizyczne serwery

* Licencja producenta na oprogramowanie do wirtualizacji dla minimum 3 serwerów fizycznych bez limitu na ilość rdzeni wraz z licencją na oprogramowanie do centralnego zarzadzania klastrem serwerów
* Wykonawca dostarczy, zainstaluje, skonfiguruje oraz przeniesienie na zamawiającego własność licencji na oprogramowanie do wirtualizacji wraz z wsparciem na okres 36 miesięcy
* Warstwa wirtualizacji musi być instalowana bezpośrednio na sprzęcie fizycznym bez potrzeby instalowania dodatkowego systemu operacyjnego.
* Oprogramowanie musi umożliwiać budowanie klastrów wysokiej dostępności.
* Oprogramowanie do wirtualizacji musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i musi się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
* Oprogramowanie do wirtualizacji umożliwiać przenoszenie maszyn wirtualnych bez konieczności ich wyłączania
* Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do min 4TB pamięci operacyjnej.
* Oprogramowanie do wirtualizacji musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych, niż fizyczne zasoby RAM serwera, w celu osiągniecia konsolidacji.
* Oprogramowanie do wirtualizacji musi być niezależne od producenta platformy sprzętowej.
* Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich sprawnego odtwarzania.

1. Wdrożenie infrastruktury

Obecne zasoby systemowe zainstalowane są na dwóch różnych serwerach z działających w oparciu o Windows Serwer 2012 R2, przy użyciu wirtualizatora Hyper-V. W obecnej chwili Zamawiający posiada 7 pracujących maszyny wirtualnych z przeznaczeniem m.in. na: SyriuszSTD (system dziedzinowy urzędu), eDOK (system obieg dokumentów), Płatnik.

Zamawiający informuje też, że posiada zaawansowane urządzenie UTM w pełni skonfigurowane pod działanie całego CPD.

Zamawiający posiada również dwa łącza internetowe wymagające rekonfiguracji podczas wykonywanych prac instalacyjnych.

Zamawiający po podpisaniu umowy z Wykonawcą przekaże posiadaną dokumentację dotyczącą infrastruktury, oraz wymagane hasła dostępowe. **Zamawiający informuje że infrastruktura jest modyfikowana w trybie ciągłym i dokumentacja może nie odzwierciedlać stanu faktycznego. Dlatego przeprowadzenie wszelkich prac należy dokonać w oparciu o stan faktyczny infrastruktury, który Wykonawca musi zweryfikować przed rozpoczęciem wdrożenia.**

Zamawiający zastrzega sobie prawo do zmiany w infrastrukturze podczas realizacji wdrożenia, jeżeli zajdzie taka konieczność.

Zamawiający w ramach usługi wymaga:

* Przekonfigurowania całej struktury sieci tak, aby zwolnić miejsce w szafie Rack na montaż całości dostarczanego sprzętu, usunąć zbędne okablowanie oraz odkurzyć sprzęt serwerowy i sieciowy.
* Przed przystąpieniem do powyższej czynności, **Wykonawca opracuje koncepcję reorganizacji, omówi z Zamawiającym i uzyska jego aprobatę.**

**Dodatkowo Wykonawca przed przystąpieniem do wykonywania czynności wdrożenia infrastruktury przedstawi analizę ryzyka utraty integralności, dostępności lub poufności informacji w związku z wprowadzeniem w ramach niniejszego postępowania istotnych zmian w systemach informatycznych wykorzystywanych u Zamawiającego. Powyższa analiza powinna przede wszystkim zawierać: listę zagrożeń, ich prawdopodobieństwo wystąpienia oraz potencjalne następstwa, a także sposób postępowania w przypadku ich wystąpienia.**

Zamawiający informuje, że może się to wiązać z przebudowaniem struktury w CPD i przeniesieniem istniejących zasobów pomiędzy szafami RACK.

* Wymiany urządzenia UTM na nowo dostarczone, zgodnie z wytycznymi ustalonymi z Zamawiającym.
* Dokonania przez Wykonawcę rekonfiguracji łączy internetowych tak, aby zachować wszystkie dotychczasowe funkcjonalności i usługi.
* Dokonania przez Wykonawcę zmian w konfiguracji polis, które będą wymagane po zmianie VLAN –ów i dopisania nowych, gdyby zaszła taka potrzeba.
* Utworzenia klastra HA z dostarczonych serwerów w taki sposób aby podczas awarii jednego z serwerów, pracę wszystkich systemów przejął drugi serwer.
* Instalacji macierzy dyskowej i podłączenie jej jako produkcyjnej do klastra HA, oraz przebudowanie starej macierzy na backupową.
* Utworzenia takiej ilości maszyn wirtualnych alby odzwierciedlić środowisko zamawiającego, następnie migracji wszystkich posiadanych przez niego zasobów na nowe serwery i macierze. **Migracja wszystkich aktualnie używanych systemów w tym m.in. SyriuszSTD, eDOK oraz Płatnik na nowe maszyny wirtualne.**
* Utworzenia 5 nowych maszyn wirtualnych na potrzeby zamawiającego.
* Zmigrowanie domeny Active Directory i zmigrowanie (lub utworzenia na nowo) wszystkich danych z obecnie używanej domeny, dostosowanie jej do aktualnych potrzeb Zamawiającego.
* Zainstalowania i skonfigurowania systemu do backupu tak, aby wykonywał kopię wszystkich zmigrowanych i wdrożonych systemów przynajmniej raz dziennie, raz tygodniowo, raz miesięcznie i raz rocznie. System backupu nie może kolidować z obecnie posiadanymi systemami backupowymi.
* Przekonfigurowanie obecnego mechanizmu backupu tak aby nie kolidował z nowo wdrożonym.
* Przeanalizowania zapotrzebowania urządzeń w serwerowni pod kątem zabezpieczenia zasiania awaryjnego, tak aby dostępne UPS-y były obciążone w miarę równomiernie i zostały wykorzystane w optymalny sposób.
* **Zapewnienia nieprzerwanej pracy i usług świadczonych przez CPD podczas wdrożenia projektu**. Tym samym, samo wdrożenie, jak też wszelkie prace z nim związane, (w tym konfiguracyjne i testowe), nie mogą wpływać na ciągłość pracy instytucji obsługiwanych przez CPD.
* Udostępnienia odpowiednim użytkownikom, wszystkich zasobów w ramach stworzonej struktury. Wykonawca musi wdrożyć nowe środowisko w taki sposób aby odzwierciedlić dotychczasowe i przy okazji poprawić organizację danych i ich bezpieczeństwo.
* Naniesienia wszystkich dokonanych zmian i uaktualnienia dokumentacji CPD, tak aby odzwierciedlała stan faktyczny całej infrastruktury.

Wykonawca w ramach usługi wdrożenia musi:

* Zapoznać się z obecnym stanem infrastruktury zamawiającego;
* Porównać stan faktyczny z dokumentacją zamawiającego, nanieść w niej wszelkie zmiany i odstępstwa od tego, co jest w rzeczywistości.
* Sprawdzić poprawność działania wszystkich usług obecnie działających i porównać je z dokumentacją zamawiającego.
* **Przeanalizować obecną organizację infrastruktury CPD, systemów oraz urządzeń**, pod kontem ich wydajności, występujących zagrożeń i odkrytych niezgodności (np. programowych), optymalizacji działania całego systemu informatycznego **i zaproponować Zmawiającemu** stosowne zmiany.
* Przygotować koncepcję nowego podziału szaf Rack i sieci LAN, przekonfigurowania: VLAN –ów, polis bezpieczeństwa, Active Directory, systemów operacyjnych, zasilania awaryjnego, przedstawić ją Zamawiającemu. Prace związane z jej wdrożeniem, należy prowadzić w taki sposób aby nie wpływały one na ciągłość pracy jednostek, kładąc przy tym szczególny nacisk na bezpieczeństwo we wszystkich aspektach.
* Przygotowaną koncepcję należy zaprezentować Zamawiającemu, omówić z nim proponowane rozwiązania i uzyskać jego akceptację.
* Wykonać kopię bezpieczeństwa całości infrastruktury przed wykonaniem usługi.
* Dokonać zmian w zabudowie docelowej szafy Rack zgodnie z przedstawioną koncepcją.
* Dokonać podłączenia i konfiguracji posiadanych łączy zgodnie z przedstawioną koncepcją.
* Dokonać instalacji dostarczonych urządzeń i systemów.
* Skonfigurować środowisko do wykonania migracji posiadanych systemów zgodnie z zaakceptowana koncepcją (utworzenie klastrów HA, instalacja systemu do wirtualizacji).
* Dokonać zmian podziału sieci zgodnie z zaakceptowaną koncepcją.
* Zmigrować na nowe środowisko wszystkie dane wskazane przez Zamawiającego.
* Zinwentaryzować wszystkie serwery wirtualne i sprawdzić poprawność ich działania w stosunku do założeń. W przypadku rozbieżność zaproponować rozwiązanie zastępcze spełniające wymagania i założenia.
* Uruchomić i skonfigurować nowe dedykowane serwery wirtualne, niezbędne do działania wdrażanych usług, lub takie których potrzeba wynika np. z usprawnienia działania systemu informatycznego posiadanego przez Zamawiającego pod kontem działających usług.
* Uruchomić infrastrukturę Zamawiającego na dostarczonych serwerach i macierzach, sprawdzając poprawność działania zainstalowanego oprogramowania.
* Zainstalować i skonfigurować w porozumieniu z Zamawiającym, system kopii bezpieczeństwa danych, wykorzystując do tego celu, nowe i dotychczas używane macierze dyskowe.
* Zmigrować lub zainstalować na nowo domenę Active Directory, przenosząc wszystkie dotychczasowe polisy oraz tworząc nowe polisy w zależności od potrzeby.
* Przygotować i przekazać kompletną dokumentacje techniczną powykonawczą infrastruktury.
* Przeszkolić z zakresu wdrożonych rozwiązań, pracowników wskazanych przez Zamawiającego.

W celu zapewnienia ciągłości działania urzędu wdrożenie i konfiguracja muszą być wykonane poza godzinami pracy Urzędu.

# SZKOLENIA

Wykonawca zobligowany jest do przeprowadzenia szkoleń dla 2 osób z zakresu obsługi wdrażanych systemów. Szkolenia będą realizowane w formie stacjonarnej, w siedzibie Zamawiającego, na sprzęcie komputerowym udostępnionym przez Wykonawcę. Zamawiający wymaga aby dla każdego z systemów Wykonawca przeprowadził oddzielne szkolenia z zakresu administrowania oraz użytkowania dostarczanych systemów. Szkolenie powinno trwać 2 dni każdy po min. 7 godzin.