Złącznik nr 3 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

I. WSTĘP - wymagania ogólne

W ramach zamówienia, zamawiający oczekuje dostarczenia kompletnego i w pełni funkcjonalnego systemu do backupu , klastra wysokiej dostępności (HA), środowiska odtworzeniowego oraz elementów infrastruktury sieciowej które spełnią wszystkie wymagania techniczne i operacyjne wskazane w dalszej części specyfikacji. Zadaniem wykonawcy będzie zapewnienie zarówno dostawy sprzętu i oprogramowania, jak i pełnej integracji wszystkich elementów systemu, ich konfiguracji oraz testów w środowisku zamawiającego. W efekcie końcowym dostawca jest zobowiązany dostarczyć rozwiązanie, które będzie gotowe do użytku, w pełni operacyjne i zdolne do realizacji zadań zgodnie z określonymi wymaganiami wydajnościowymi, bezpieczeństwa oraz dostępności danych.

Cele nadrzędne, które musi realizować klaster wysokiej dostępności (HA), obejmują kluczowe aspekty zapewnienia nieprzerwanego dostępu do zasobów i minimalizacji ryzyka przestojów. Do głównych celów należy:

Zapewnienie ciągłości działania systemu – Klaster HA musi gwarantować nieprzerwaną pracę systemów kluczowych dla funkcjonowania organizacji, minimalizując ryzyko przestojów w przypadku awarii sprzętu, oprogramowania lub sieci. W razie awarii jednego z węzłów, system powinien automatycznie przenieść obciążenie na inne, sprawne węzły klastra.

Automatyczne przełączanie awaryjne (failover) – W przypadku wykrycia awarii jednego z komponentów, klaster HA musi natychmiast automatycznie przekierować ruch i operacje na zdrowe węzły, zapewniając płynne i szybkie odzyskanie dostępności bez ingerencji użytkowników końcowych.

Minimalizacja przestojów (downtime) – System powinien dążyć do zapewnienia maksymalnej dostępności usług (powyżej 99,99%) i minimalizacji czasu przestojów, zarówno planowanych (np. konserwacje) jak i nieplanowanych (np. awarie sprzętu).

Zachowanie integralności danych – Klaster HA musi zagwarantować, że w przypadku przełączenia awaryjnego (failover) dane są bezpieczne i żadne operacje nie zostaną utracone. Synchronizacja danych pomiędzy węzłami klastra powinna odbywać się w czasie rzeczywistym lub z minimalnym opóźnieniem, zapewniając spójność danych.

Skalowalność – System powinien umożliwiać łatwe skalowanie poprzez rozbudowę lub dodawanie nowych węzłów, co pozwoli na dostosowanie infrastruktury do zmieniających się potrzeb organizacji i zwiększającego się obciążenia.

Monitoring i zarządzanie – Klaster HA musi być wyposażony w narzędzia do monitorowania stanu wszystkich węzłów i komponentów oraz do szybkiego diagnozowania i rozwiązywania problemów. System zarządzania powinien umożliwiać centralne sterowanie klastrem, z możliwością zdalnej administracji.

Redundancja zasobów – Klaster musi zapewniać redundancję wszystkich krytycznych komponentów aby wyeliminować pojedyncze punkty awarii (SPOF), zapewniając jednocześnie wysoką dostępność infrastruktury.

Cele nadrzędne, które musi realizować środowisko backupowe i odtworzeniowe:

Zapewnienie bezpieczeństwa i integralności danych – Środowisko backupowe musi gwarantować, że wszystkie dane są bezpiecznie przechowywane i zabezpieczone przed uszkodzeniem, utratą lub nieuprawnionym dostępem. Dane muszą być regularnie kopiowane w sposób, który zapewnia ich spójność i integralność, niezależnie od rodzaju przechowywanej informacji (pliki, bazy danych, maszyny wirtualne).

Automatyzacja procesu tworzenia kopii zapasowych – System backupowy powinien automatycznie wykonywać kopie zapasowe zgodnie z wcześniej ustalonym harmonogramem lub wyzwalanymi zdarzeniami, minimalizując ręczną ingerencję i ryzyko błędów ludzkich. Automatyzacja powinna obejmować pełne, przyrostowe i różnicowe kopie zapasowe.

Szybkie i niezawodne odtwarzanie danych (restore) – W przypadku awarii, system odtworzeniowy musi umożliwić szybkie, łatwe i niezawodne przywrócenie danych do stanu sprzed awarii. Czas odtwarzania musi być minimalny

Redundancja i dywersyfikacja lokalizacji przechowywania kopii zapasowych – Dane backupowe powinny być przechowywane w więcej niż jednej lokalizacji, aby zminimalizować ryzyko ich utraty w przypadku awarii sprzętowej, klęski żywiołowej lub ataku cybernetycznego. Kopie powinny być również szyfrowane i chronione przed nieuprawnionym dostępem.

Skalowalność – System backupowy powinien umożliwiać łatwe skalowanie wraz ze wzrostem ilości danych, które podlegają backupowi. Środowisko musi być elastyczne, pozwalając na zwiększenie pojemności pamięci masowej i mocy obliczeniowej bez zakłócania bieżących operacji.

Łatwość zarządzania i monitorowania – System musi zapewniać intuicyjne narzędzia do zarządzania procesami backupowymi oraz monitorowania stanu kopii zapasowych. Powinny one obejmować raportowanie, powiadomienia o błędach oraz centralne zarządzanie, umożliwiając szybkie wykrywanie i rozwiązywanie problemów.

Zgodność z regulacjami i politykami firmy – Środowisko backupowe musi spełniać wymagania dotyczące retencji danych, szyfrowania oraz zgodności z przepisami prawa, takimi jak RODO czy inne regulacje branżowe. System powinien umożliwiać dostosowanie polityk przechowywania danych do wymogów audytowych i prawnych.

Ochrona przed zagrożeniami cybernetycznymi – W kontekście rosnącego zagrożenia cyberatakami (np. ransomware), system backupowy powinien oferować funkcje ochrony przed tego typu zagrożeniami, takie jak niezmienność kopii zapasowych (immutable backups), aby zapewnić, że dane mogą być bezpiecznie odtworzone, nawet jeśli produkcyjne środowisko zostało zaatakowane.

Dostarczenie zasobów do awaryjnego uruchomienia środowiska produkcyjnego - w przypadku wyłączenia/utraty/uszkodzenia środowiska produkcyjnego, środowisko backupowe musi umożliwić awaryjne uruchomienie kluczowych systemów

Cele wdrożenia urządzeń UTM oraz oprogramowania antywirusowego w jednostkach podległych:

Ochrona przed złośliwym oprogramowaniem (malware) – oprogramowanie antywirusowe musi zapewnić aktywną ochronę przed różnorodnym złośliwym oprogramowaniem, w tym wirusami, trojanami, robakami, ransomware oraz spyware.

Zapobieganie atakom sieciowym - poprzez integrację różnorodnych funkcji ochrony, takich jak: zapory ogniowe (firewall), systemy wykrywania i zapobiegania włamaniom (IDS/IPS), filtrowanie ruchu, VPN oraz kontrolę dostępu. System musi zapewniać ochronę przed atakami zewnętrznymi (np. DDoS, brute force) oraz chronić wewnętrzne zasoby przed nieautoryzowanym dostępem.

Zarządzanie i kontrola dostępu do zasobów internetowych – umożliwiające filtrowanie treści i kontrolowanie dostępu do określonych stron internetowych oraz aplikacji. System musi ograniczać ryzyko wynikające z odwiedzania stron zainfekowanych lub niedozwolonych.

Centralne zarządzanie bezpieczeństwem IT - we wszystkich jednostkach podległych. Rozwiązanie antywirusowe musi zapewniać centralne monitorowanie stanu systemów, zdalne aktualizacje oprogramowania oraz szybkie reagowanie na wykryte zagrożenia i incydenty.

Bezpieczny dostęp do zasobów w oparciu o VPN – we wszystkich jednostkach musi zostać wdrożony tunel vpn w oparciu o protokół IPsec umożliwiający dostęp do zasobów zlokalizowanych w zasobach Zamawiającego.

II. Fizyczne rozlokowanie zasobów i ich montaż.

W serwerowni podstawowej wykonawca zamontuje w istniejącej szafie serwerowej następujące elementy:

- serwery dla klastra HA – 2szt
- macierz dyskową – 1szt
- zasilacze UPS – 2szt
- switche 48 port – 2szt
- UTM – 1szt

W serwerowni zapasowej wykonawca zamontuje szafę serwerową a w niej następujące elementy:

- serwer backupowy
- bibliotekę taśmową (autoloader)
- NAS udostępniony przez Zamawiającego
- zasilacz UPS – 1szt
- switch 24 porty – 1szt

Pomieszczenie serwerowni zapasowej znajduje się nad pomieszczeniem serwerowni głównej (1 piętro). Do serwerowni zapasowej należy doprowadzić odpowiednie okablowanie sieciowe (telekomunikacyjne) konieczne do działania systemu backupowego (min 2x10Gb). Niezbędne okablowanie zasilające (instalację elektryczną) wykona Zamawiający we własnym zakresie.

Wszystkie niezbędne do montażu i podłączenia urządzeń kable, uchwyty, przełącznice, śruby, itp. zapewnia wykonawca.

Urządzenia UTM zostaną zamontowane i skonfigurowane przez Wykonawcę w następujących jednostkach podległych :

- Ośrodek Pomocy Społecznej w Byczynie
- Zespół Szkół w Byczynie
- Publiczne przedszkole w Byczynie
- Publiczny Żłobek Nr 2 w Byczynie
- Szkoła podstawowa w Roszkowicach
- Szkoła podstawowa w Biskupicach
- Centrum Integracji Społecznej w Polanowicach
- Ośrodek Kultury w Byczynie

III. Szczegółowe wymagania techniczne.

1. Biblioteka taśmowa – 1szt

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1.	Wykorzystana technologia	LTO Ultrium wspierająca technologię partycjonowania nośników.
2.	Obudowa	Typu rack 19”. Wysokość maksymalnie 2U - wszystkie elementy do montażu muszą być dostarczone wraz z urządzeniem.
3.	Wbudowany napęd	LTO-8 wyposażony w dwa złącza mSAS SFF-8088. Urządzenie musi wspierać technologię LTFS (Linear Tape File System) umożliwiającą kopiowanie danych na taśmę bez konieczności użycia oprogramowania do backupu kompatybilną z systemami Linux i Microsoft. Prędkość zapisu pojedynczego napędu bez kompresji – minimum 300 MB/sek. Zainstalowany napęd musi mieć możliwość dynamicznego i płynnego dopasowania prędkości do napływających danych w przedziale od 100 do 300 MB/sek. stosować szyfrowanie danych metodą AES 256-bit.
4.	Ilość slotów i magazynki	Minimum 8 kieszeni na taśmy
5.	Pojemność	Pojemność bez kompresji – minimum 96TB przy obsadzeniu wszystkich slotów na taśmy wyłącznie nośnikami LTO-8
6.	Zarządzanie	Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalne przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu FastEthernet. Wymagane wsparcie SNTP, protokołów SSL/TLS i IPv6 oraz definiowanie minimum 4 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji. Operacja powinna być możliwa zarówna poprzez web GUI jak i poprzez panel kontrolny urządzenia. Wymagana możliwość zdalnego,restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI.
7.	Dodatkowe interfejsy	Biblioteka musi być wyposażone w interfejs sieciowy
8.	Obsługa urządzenia	Wymagana możliwość wymiany napędu, zasilacza, modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej. Możliwość wyjmowania nośników z urządzenia nawet przy braku zasilania. Zarówno napęd jak i zasilacz oraz moduł portów zarządzania powinny być wyposażone w lampki kontrolne, informujące o stanie technicznym.
9.	Wyposażenie	Urządzenie musi być standardowo wyposażone w czytnik kodów kreskowych, zestaw kabli: 1x zasilając, 1x komunikacyjny konieczny do podłączenia urządzenia do odpowiedniego kontrolera serwera i umożliwiającego komunikację z urządzeniem – długość kabla min. 2m. W przypadku, gdyby serwer nie dysponował odpowiednim kontrolerem, należy taki dostarczyć wraz z urządzeniem. Wraz z urządzeniem należy dostarczyć także zestaw 10-ciu identycznych nośników na dane o pojemności natywnej pojedynczego nośnika min. 12TB oraz jeden nośnik czyszczący wyposażonych w unikalne naklejki z kodem kreskowym. Wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem, co należy potwierdzić odpowiednim oświadczeniem producenta urządzenia dołączonym do oferty.

10.	Kompatybilność	Urządzenie musi być w pełni kompatybilne z oferowaną aplikacją do backupu – kompatybilność musi być potwierdzona odpowiednim oświadczeniem producenta urządzenia dołączonym do oferty
11.	Gwarancja	24 miesiące z szybkiej wymiany całego urządzenia lub komponentów w czasie do 48 godz. (dni robocze) od momentu zgłoszenia uszkodzenia. Czas przyjmowania zgłoszeń serwisowych w trybie 5x8 z czasem reakcji do 12 godzin od zgłoszenia. Do oferty należy dołączyć pisemne oświadczenia wystawione przez producenta o gwarancji świadczonej w rygorze 5x8xNBD realizowanej przez producenta lub jego autoryzowany serwis posiadający ISO9001 na usługi serwisowe.

2. Macierz – 1szt

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1	Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 4U z możliwością instalacji min. 24 dysków 2.5”
2	Przestrzeń dyskowa	Zainstalowane: 8x dysk SAS 12Gb/s o pojemności min. 2.4TB, 10 tyś. obr./min, Hot-Plug 4x dysk SSD SAS MU o pojemności min. 1.6TB, Hot-Plug
3	Obsługa dysków	Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.
4	Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy. Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
5	Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
6	Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii.
7	Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
8	Interfejsy	Macierz musi posiadać, co najmniej 8 portów 12Gb SAS (4 porty na kontroler)
9	Kable	Kabel SAS Mini do HD-Mini, min. 2m
10	Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
11	Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 256 wolumenów logicznych w ramach oferowanej macierzy dyskowej.
12	Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

13	Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
14	Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
15	Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
16	Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
17	Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
18	Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
19	Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.

20	Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
21	Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union),
22	Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego urządzenia, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
23	Warunki gwarancji	3-letnia gwarancja producenta świadczona na miejscu u klienta Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie min: w dni robocze (8h) następującymi kanałami: telefonicznie oraz przez Internet . Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

3. Serwer do backupu – 1szt

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1	Obudowa	Maksymalnie 2U RACK 19 cali wraz z szynami montażowymi. Serwera wyposażony w ramię do prowadzenia kabli. Serwer wyposażony w zdejmowany panele przedni z zamkiem. Serwer wyposażony w czujnik otwarcia obudowy współpracującego z BIOS/UEFI/kartą zdalnego zarządzania. Serwer wyposażony w TPM 2.0.
2	Procesor	Jeden procesor 16-rdzeniowy, x86 - 64 bity, osiągający w testach SPECrate2017_int_base powyżej 346 punktów w konfiguracji dwuprocesorowej z zaoferowanym serwerem. Wynik testu musi być opublikowany na stronie www.spec.org.
3	Liczba procesorów	Min. 1 procesor, możliwość zamontowania drugiego procesora.
4	Pamięć operacyjna	128GB RDIMM DDR5 min.4800 MT/s w modułach o pojemności min. 32GB każdy. Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację minimum 6TB. Obsługa zabezpieczeń: Advanced ECC lub równoważne.
5	Sloty rozszerzeń	minimum trzy sloty PCIe

6	Dysk twardy	Zatoki dyskowe gotowe do zainstalowania min. 8 dysków 3.5” typu Hot Swap, SAS/SATA/SSD oraz zatoki dyskowe gotowe do zainstalowania min. 2 dysków 2.5” typu Hot Swap, SAS/SATA/SSD Wszystkie zatoki dyskowe dostępne z przodu serwera. Zainstalowane: 2 x dysk 960GB SSD Read Intensive 2.5” typu hot swap 6 x dysk 8TB SAS 7,2k 3,5” typu hot swap
7	Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych NVMe/SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60.
8	Interfejsy sieciowe	Karta, minimum 2 porty Ethernet 10Gb SFP+ które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”, wszystkie porty obsadzone wkładkami SFP+ 10Gb. Min 2 porty Ethernet (10/100/1000Mbit)
9	Karta graficzna	Zintegrowana karta graficzna
10	Porty	4 x USB w tym min. 2 porty USB 3.0 1x VGA
11	Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy niezbędnej do prawidłowej pracy serwera przy pełnej rozbudowie i obciążeniu
12	Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
13	Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne) wsparcie dla pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy z poziomu przeglądarki webowej (GUI) oraz z poziomu linii komend Management Command Line Protocol (SM CLP) wbudowane narzędzia diagnostyczne zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników przesyłanie alertów poprzez e-mail
14	Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2019, 2022 Red Hat Enterprise Linux (RHEL) 8.6 SUSE Linux Enterprise Server (SLES) 15 SP4 VMware ESXi 7.0 U3, 8.0
15	Wsparcie techniczne	2-letnia gwarancja producenta w miejscu instalacji. Czas reakcji w miejscu instalacji to kolejny dzień roboczy. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera. Uszkodzone dyski pozostają własnością Zamawiającego.
16	Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta

		oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.

4. Serwer do klastra HA – 2 szt.

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1	Obudowa	Maksymalnie 2U RACK 19 cali wraz z szynami montażowymi. Serwera wyposażony w ramię do prowadzenia kabli. Serwer wyposażony w zdejmowany panele przedni z zamkiem. Serwer wyposażony w czujnik otwarcia obudowy współpracującego z BIOS/UEFI/kartą zdalnego zarządzania. Serwer wyposażony w TPM 2.0.
2	Procesor	Jeden procesor 16-rdzeniowy, x86 - 64 bity, osiągający w testach SPECrate2017_int_base powyżej 346 punktów w konfiguracji dwuprocesorowej z zaoferowanym serwerem.Wynik testu musi być opublikowany na stronie www.spec.org.
3	Liczba procesorów	Min. 1 procesor, możliwość zamontowania drugiego procesora.
4	Pamięć operacyjna	128GB RDIMM DDR5 min.4800 MT/s w modułach o pojemności min. 32GB każdy. Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację minimum 6TB. Obsługa zabezpieczeń: Advanced ECC lub równoważny
5	Sloty rozszerzeń	minimum trzy sloty PCIe
6	Dysk twardy	Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5”. Serwer wyposażony w 2 dyski 960GB SSD SATA Read Intensive.
7	Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych NVMe/SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60.
8	Interfejsy sieciowe	Serwer musi być wyposażony w: - 2 sztuki dwuportowych kart 10Gb Ethernet SFP+, do każdej z kart należy dołączyć 2 sztuki wkładek 10Gb SFP+ ;Min 2 porty Ethernet (10/100/1000Mbit)
9	Karta graficzna	Zintegrowana karta graficzna
10	Porty	4 x USB w tym min. 2 porty USB 3.0 1x VGA
11	Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy niezbędnej do prawidłowej pracy serwera przy pełnej rozbudowie i obciążeniu
12	Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
13	Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne) wsparcie dla pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy z poziomu przeglądarki webowej (GUI) oraz z poziomu linii komend

		Management Command Line Protocol (SM CLP) wbudowane narzędzia diagnostyczne zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników przesyłanie alertów poprzez e-mail
14	Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2019, 2022 Red Hat Enterprise Linux (RHEL) 8.6 SUSE Linux Enterprise Server (SLES) 15 SP4 VMware ESXi 7.0 U3, 8.0
15	Wsparcie techniczne	2-letnia gwarancja producenta w miejscu instalacji. Czas reakcji w miejscu instalacji to kolejny dzień roboczy. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera. Uszkodzone dyski pozostają własnością Zamawiającego.
16	Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.

5. Zarządzalny przełącznik sieciowy – 24 porty

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1	Porty	24 porty RJ45 10/100/1000 Mb/s 4 sloty SFP+ 10G 1 port konsolowy RJ45
2	Zasilanie	Dwa wewnętrzne zasilacze (100–240 VAC, 50/60 Hz) (redundancja zasilania)
3	Montaż	montaż w szafie Rack
4	Wydajność przełączania	100 Gb/s
5	Stackowanie	min 8 urządzeń, porty stackowania: 4 Slot SFP+ 10G lub porty dedykowane o równoważnej przepustowości
6	Wydajność pakietowa	90 Mp/s
7	Tablica adresów MAC	16K
8	Ramki jumbo	9KB
9	Cechy L3	statyczny routing, RIP, OSPF, Serwer DHCP, DHCP Relay
10	Funkcje L2 i L2+	agregacja łączy, STP, wykrywanie pętli (loopback),port mirroring
11	Sieci VLAN	802.1Q VLAN (1024), port-based VLAN, MAC-based VLAN,
12	Bezpieczeństwo	802.1x, Wiązanie IP-MAC-Port, Filtr DHCP, Storm Control Broadcast, zarządzanie webowe poprzez HTTPS z szyfrowaniem SSLv3/TLS 1.2, CLI z szyfrowaniem SSHv2, kontrola dostępu bazująca na IP/Port/MAC
13	Funkcje zarządzania	Interfejs graficzny GUI, Interfejs wiersza poleceń CLI przez port konsolowy, telnet, SNMP v1/v2c/v3, monitorowanie obciążenia procesora, diagnostyka kabli, SNTP, Logi systemowe
14	zawartość dostawy	Switch,2 Przewody zasilające, kabel konsolowy RJ45,instrukcja instalacji, zestaw montażowy do szafy Rack
15	Wymagania systemowe	Windows 10,11,Linux
16	Gwarancja	24 m-ce, w przypadku uszkodzenia naprawa na w siedzibie zamawiającego lub wymiana na nowy w ciągu 5 dni.

6. Zarządzalny przełącznik sieciowy – 48 portów – 2szt.

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1	Porty	48 portów RJ45 10/100/1000 Mb/s 4 sloty SFP+ 10G 1 port konsolowy RJ45
2	Zasilanie	Dwa wewnętrzne zasilacze (100–240 VAC, 50/60 Hz) (redundancja zasilania)
3	Montaż	montaż w szafie Rack
4	Wydajność przełączania	200 Gb/s
5	Stackowanie	min 8 urządzeń, porty stackowania: 4 Slot SFP+ 10G lub porty dedykowane o równoważnej przepustowości
6	Wydajność pakietowa	150 Mp/s
7	Tablica adresów MAC	16K
8	Ramki jumbo	9KB
9	Cechy L3	statyczny routing, RIP, OSPF, Serwer DHCP, DHCP Relay
10	Funkcje L2 i L2+	agregacja łączy, STP, wykrywanie pętli (loopback),port mirroring
11	Sieci VLAN	802.1Q VLAN (1024), port-based VLAN, MAC-based VLAN,
12	Bezpieczeństwo	802.1x, Wiązanie IP-MAC-Port, Filtr DHCP, Storm Control Broadcast, zarządzanie webowe poprzez HTTPS z szyfrowaniem SSLv3/TLS 1.2, CLI z szyfrowaniem SSHv2, kontrola dostępu bazująca na IP/Port/MAC
13	Funkcje zarządzania	Interfejs graficzny GUI, Interfejs wiersza poleceń CLI przez port konsolowy, telnet, SNMP v1/v2c/v3, monitorowanie obciążenia procesora, diagnostyka kabli, SNTP, Logi systemowe
14	zawartość dostawy	Switch,2 Przewody zasilające, kabel konsolowy RJ45,instrukcja instalacji, zestaw montażowy do szafy Rack
15	Wymagania systemowe	Windows 10,11,Linux
16	Gwarancja	24 m-ce, w przypadku uszkodzenia naprawa na w siedzibie zamawiającego lub wymiana na nowy w ciągu 5 dni.

7. UTM – 1 szt

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1	Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
2	Redundancja, monitoring i wykrywanie awarii	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

3	Interfejsy, Zasilanie	System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 10 portami Gigabit Ethernet RJ-45. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.System jest wyposażony w zasilanie AC
4	Parametry wydajnościowe	W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 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 1.3 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.
5	Funkcje Systemu Bezpieczeństwa	Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. Kontrola Aplikacji. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. Ochrona przed malware. 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). Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
6	Polityki, Firewall	Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System realizuje 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 istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7	Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: - Wsparcie dla IKE v1 oraz v2. - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). - Obsługa protokołu Diffie-Hellman grup 19, 20.

		- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. - 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. - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. - Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia 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 posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
8	Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: - Routingu statycznego. - Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. - Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. - ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. - BFD (Bidirectional Forwarding Detection). - Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
9	Zarządzanie pasmem	System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. System daje możliwość określania pasma dla poszczególnych aplikacji. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
10	Ochrona przed malware	- Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). - Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. - System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.

		- System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. - System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). - Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. - System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. - System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. - Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. - Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
11	Ochrona przed atakami	- Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. - System chroni przed atakami na aplikacje pracujące na niestandardowych portach. - Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. - Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. - System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. - Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). - Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. - Wykrywanie i blokowanie komunikacji C&C do sieci botnet. - Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
12	Kontrola aplikacji	- Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. - Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. - Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. - Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. - Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. - Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). - System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
13	Kontrola WWW	- Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. - W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. - Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.

		- Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. - Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). - Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. - Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. - Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. - System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
14	Uwierzytelnianie użytkowników w ramach sesji	System Firewall umożliwia 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. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 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 mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. - Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. - Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. - System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. - System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. - Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. - Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. - Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). - Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
16	Logowanie	- Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. - W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu.

		Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. - Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. - Możliwość włączenia logowania per reguła w polityce firewall. - System zapewnia możliwość logowania do serwera SYSLOG. - Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
17	Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje dla funkcjonalnośc: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.
18	Gwarancja oraz wsparcie	System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7

8. UTM – 8 szt

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1	Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
2	Redundancja, monitoring i wykrywanie awarii	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
3	Interfejsy, Zasilanie	System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 5 portami Gigabit Ethernet RJ-45. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.System jest wyposażony w zasilanie AC
4	Parametry wydajnościowe	W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 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 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.
5	Funkcje Systemu Bezpieczeństwa	Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. Kontrola Aplikacji. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. Ochrona przed malware. 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). Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
6	Polityki, Firewall	Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System realizuje 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 istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7	Połączenia VPN	System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: - Wsparcie dla IKE v1 oraz v2. - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). - Obsługa protokołu Diffie-Hellman grup 19, 20. - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. - 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. - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.

		- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. - Mechanizm „Split tunneling" dla połączeń Client-to-Site. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia 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 posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
8	Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: - Routingu statycznego. - Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. - Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. - ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. - BFD (Bidirectional Forwarding Detection). - Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
9	Zarządzanie pasmem	System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. System daje możliwość określania pasma dla poszczególnych aplikacji. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
10	Ochrona przed malware	- Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). - Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. - System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. - System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. - System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). - Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. - System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.

		- System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. - Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. - Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
11	Ochrona przed atakami	- Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. - System chroni przed atakami na aplikacje pracujące na niestandardowych portach. - Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. - Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. - System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. - Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). - Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. - Wykrywanie i blokowanie komunikacji C&C do sieci botnet. - Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
12	Kontrola aplikacji	- Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. - Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. - Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. - Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. - Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. - Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). - System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
13	Kontrola WWW	- Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. - W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. - Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. - Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. - Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). - Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. - Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.

		- Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. - System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
14	Uwierzytelnianie użytkowników w ramach sesji	System Firewall umożliwia 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. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 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 mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. - Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. - Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. - System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. - System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. - Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. - Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. - Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). - Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
16	Logowanie	- Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. - W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. - Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. - Możliwość włączenia logowania per reguła w polityce firewall. - System zapewnia możliwość logowania do serwera SYSLOG. - Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
17	Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje dla funkcjonalnośc: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem

		sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.
18	Gwarancja oraz wsparcie	System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7

9. UPS – 3 szt.

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1	Minimalne wymagania techniczne dla jednostki UPS	- Moc znamionowa jednostki nie mniej niż 3000VA / 2700W - Jednostka do montażu w szafie Rack - Klasa VFI-SS-111 zgodnie z PN-EN62040-1 - Temperatura eksploatacji 0 - 40 °C - Wilgotność względna podczas pracy 0 - 90 % - Wysokość n.p.m. podczas pracy 0-3000metry - Sprawność ≥ 93,5% przy pełnym obciążeniu - Klasa ochrony IP 20
2	Parametry wejściowe	- Nominalne napięcie wejściowe 230V_{AC} - Częstotliwość wejściowa 50 Hz - Zmienny zakres napięcia wejściowego w trybie podstawowym 100 – 275V_{AC} (połowa obciążenia), 160 – 275V_{AC} (pełne obciążenie)
3	Parametry wyjściowe	- Napięcie wyjściowe 230VAC - Zniekształcenia napięcia wyjściowego ≤2% - Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50Hz ±3 Hz - Typ przebiegu sinusoida - Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny)
4	Akumulatory i czas podtrzymania	- Czas autonomii: ≥ 75 minut dla pełnego obciążenia ≥ 160 minut dla połowy obciążenia - Typowy czas ładowania ≤3 godziny - Oczekiwana żywotność akumulatora (lata) 3 – 5 - Rozszerzalny czas podtrzymania za pomocą dodatkowych modułów - Baterie wymieniane na gorąco
5	Komunikacja i zarządzanie	- Gniazdo do montażu karty WEB/SNMP- Smart Slot x1 (karta w zestawie) - Moduł WEB/SNMP obsługiwane protokoły komunikacyjne: IP v.6 SNMP v.3 ,Modbus TCP, HTTPS/SSL, SSH z kluczem do 2048 bit SMTP, NTP, FTP, Telnet - Port uniwersalny do podłączenia np. czujnika temperatury (jeden czujnik temperatury dostarczyć w komplecie z UPS) - Porty komunikacyjne: RJ45 Serial, Smart-Slot, USB - Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD - Awaryjny wyłącznik zasilania (EPO) Tak - Darmowe oprogramowanie do zamykania systemów operacyjnych
6	Certyfikaty, zgodności oraz gwarancja	- CE, Znak CE, EAC, EN/IEC 62040-1, EN/IEC 62040-2, ENERGY STAR (UE), RCM, VDE - 3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulatory.

10. Oprogramowanie do backupu.

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
	Wymagania ogólne	Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oprogramowanie musi współpracować z infrastrukturą Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022 oraz dostarczaną w ramach obecnego

		postępowania. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. Licencja wieczysta dla min. 5 serwerów (fizycznych i VM) z 24 miesięcznym wsparciem producenta oprogramowania.
	Wymagania szczegółowe	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 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. Metadane deduplikacji muszą być przechowywane w plikach backupu. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, oraz PostgreSQL (w tym odtwarzanie point-in-time) Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
	Wymagania RPO	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

		Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru **Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.** Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
	Wymagania RTO	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 uruchomienie zasobów plikowych SMB oraz baz danych MS SQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień 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 pojedynczych plików z systemów Windows, Linux. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. 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, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.

		Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
	Ograniczenie ryzyka	Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender oraz ESET NOD32. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
	Środowiska fizyczne	Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów Rozwiązanie musi wspierać backup podłączonych dysków USB Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone Rozwiązanie musi wspierać kontrolę pasma sieciowego Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft Rozwiązanie musi wspierać technologię BitLocker Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Active Directory 2008 i nowszych, Microsoft SQL 2008 i nowszychoraz PostgreSQL 12 i nowszych Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych

		Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu. Rozwiązanie musi wspierać szyfrowanie Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
	Monitoring	System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego bez potrzeby korzystania z narzędzi firm trzecich System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel System musi dawać możliwość podłączenia się do kilku instancji środowisk virtualnych, w celu ich centralnego monitorowania System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów 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 integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
	Raportowanie	System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Adobe PDF System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc 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 generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

11. System operacyjny ze środowiskiem do wirtualizacji.

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1	Opis funkcjonalny, wymagania licencyjne	- Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej ilości środowisk serwerowych systemów operacyjnych za pomocą wbudowanych mechanizmów wirtualizacji. - Licencja musi umożliwiać równoczesne uruchomienie na dwóch w pełni wyposażonych serwerach fizycznych opisanych w punkcie 4. - Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. - Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. - Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. - Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. - Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. - Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. - Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading; - Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. - Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. - Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. - Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. - Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. - Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. - Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.

12. System operacyjny.

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
	opis funkcjonalny, wymagania licencyjne	• Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowych systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. • Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. • Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

		• Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. • Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. • Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. • Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading; • Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. • Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. • Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. • Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. • Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.

13. Oprogramowanie antywirusowe -200 stanowisk

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1.	Administracja zdalna	1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD. 2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. 3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. 4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. 5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów. 6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. 7. Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android. 8. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci. 9. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe). 10. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. 11. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.

		12. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 13. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 14. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora. 15. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. 16. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
2.	Ochrona stacji roboczych	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11). 2. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 3. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 5. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 6. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 7. Rozwiązanie musi zapewniać skanowanie plików spakowanych i kompresowanych oraz dysków sieciowych i dysków przenośnych. 8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików,katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 9. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 10. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 11. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 12. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 13. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 14. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: a) tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, b) tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, c) tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

		d) tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasuprogram musi samoczynnie przełączyć się w tryb pracy oparty na regułach, e) tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 15. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 16. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 17. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 18. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 19. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
3	Ochrona serwera	1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty Dodatkowe wymagania dla ochrony serwerów Windows: 9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów,

		drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux: 18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu
4	Ochrona urządzeń mobilnych opartych o system Android	1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: a. usunięcie zawartości urządzenia, b. przywrócenie urządzenie do ustawień fabrycznych, c. zablokowania urządzenia, d. uruchomienie sygnału dźwiękowego, e. lokalizację GPS. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła.

14. Szafa serwerowa – 1 szt.

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1		Szafa serwerowa szerokość 800mm, głębokość 1000 mm, wysokość 15U. Zamawiający dopuści szafę serwerową o wysokości od 15U do 18U - Drzwi przednie szklane - szkło hartowane, zamykane na klucz - Drzwi tylne: pojedyncze - pełna stal, zamykane na klucz - Drzwi boczne zatrzaskowe z zamknięciem na klucz (możliwość demontażu) - Otwory na przewody: od dołu - Możliwość zamontowania dwóch wentylatorów w suficie - Ocynkowany stelaż do instalacji sprzętu, dodatkowe środkowe słupki montażowe - Kółka o nośności co najmniej 500 kg wraz z niezbędnymi elementami instalacyjnymi (szyny albo cokół) z hamulcem + regulowane nóżki, - Komplet elementów do zabezpieczenia wszystkich otworów do wprowadzania okablowania – szczotkowy - Sufit pełny z perforacją boczną - Jeden kluczyk do wszystkich zamków - Min. trzy klucze do szafy

IV. Testy funkcjonalne.

Zamawiający przeprowadzi przy udziale Wykonawcy testy polegające na:

- sprawdzeniu czasu podtrzymania zasilania awaryjnego (UPS)
- sprawdzeniu działania klastra HA przy wyłączeniu jednego z zasilaczy UPS
- sprawdzeniu poprawności działania klastra HA przy odłączeniu jednej ścieżki komunikacyjnej pomiędzy serwerami a macierzą
- sprawdzeniu automatycznego przenoszenia maszyn virtualnych w przypadku wyłączenia jednego z serwerów w klastrze
- sprawdzeniu możliwości wykonania kopii całej maszyny wirtualnej i jej odtworzenia na środowisku odtworzeniowym (serwer backupowy)
- sprawdzeniu możliwości wykonania kopii maszyny virtualnej na bibliotece taśmowej oraz możliwości jej odtworzenia
- sprawdzeniu możliwości zestawienia połączenia RDP w bezpiecznym tunelu z dowolnej jednostki podległej do wystawionej w infrastrukturze Zamawiającego usługi RDS