

Opis Przedmiotu Zamówienia

Oprogramowanie oraz

infrastruktura sprzętowa

SPIS TREŚCI

WSTĘP	3
I. WYMAGANIA OGÓLNE	4
RÓWNOWAŻNOŚĆ OFEROWANYCH ROZWIĄZAŃ	4
II. OBSZAR TECHNICZNY	6
1. USŁUGI INFORMATYCZNE - WYMAGANIA MINIMALNE	6
2. UTM UNIFIED THREAT MANAGEMENT - WYMAGANIA MINIMALNE	6
3. SERWER - WYMAGANIA MINIMALNE	13
4. NETWORK ATTACHED STORAGE NAS - WYMAGANIA MINIMALNE	21
5. ZARZĄDZALNE URZĄDZENIA SIECIOWE Z OBSŁUGĄ VLAN, MACSEC, STANDARDU 802.1X TYP 1 - WYMAGANIA MINIMALNE	23
6. ZARZĄDZALNE URZĄDZENIA SIECIOWE Z OBSŁUGĄ VLAN, MACSEC, STANDARDU 802.1X TYP 2 - WYMAGANIA MINIMALNE	25
7. OPROGRAMOWANIE DO WYKONYWANIA KOPII ZAPASOWYCH - WYMAGANIA MINIMALNE	27
III. OBSZAR KOMPETENCYJNY	30
1. SZKOLENIA DLA DZIAŁU IT TYP 1 - WYMAGANIA MINIMALNE	30
2. SZKOLENIA DLA DZIAŁU IT TYP 2 - WYMAGANIA MINIMALNE	31
3. SZKOLENIA DLA DZIAŁU IT TYP 3 - WYMAGANIA MINIMALNE	32
4. SZKOLENIA DLA DZIAŁU IT TYP 4 - WYMAGANIA MINIMALNE	32

Wstęp

Niniejszy załącznik określa minimalne wymagania dla dostawy/wdrożenia/uruchomienia oprogramowania oraz infrastruktury sprzętowej dla Gminy Lewin Kłodzki realizowanego w ramach „Cyberbezpieczny Samorząd” dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Celem projektu jest zwiększenia poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego.



I. WYMAGANIA OGÓLNE

RÓWNOWAŻNOŚĆ OFEROWANYCH ROZWIĄZAŃ

1) *w zakresie Oprogramowania*

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tę samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

Mając na uwadze powyższe w przypadku, jeżeli Wykonawcy nie mają możliwości uzyskania odpowiedniego do realizacji dostępu do oprogramowania firm trzecich, w celu zapewnienia zasady konkurencyjności, przejrzystości, jawności a także równego traktowania wykonawców w trakcie prowadzenia postępowania, Zamawiający dopuszcza każdorazowo wymianę Oprogramowania u Zamawiającego/Partnerów Projektu pod warunkiem, że:

- a) Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego systemy Wykonawca dostarcza i wdraża na swój koszt, z zachowaniem warunków licencjonowania wskazanych w niniejszym dokumencie.
- b) Wykonawca przeprowadzi migrację danych w zakresie wskazanym przez Zamawiającego na swój koszt, w sposób opisany w niniejszym OPZ a migracja musi objąć pełny zakres danych bieżących i archiwalnych.
- c) Wykonawca przeprowadzi instruktaże stanowiskowe, zapewni gwarancje i serwis gwarancyjny a także help desk oraz będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom Zamawiającego płynną obsługę Oprogramowania.
- d) Wymiana Oprogramowania nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy wynikającą z obowiązujących terminów, przepisów prawa i stosowanych procedur.
- e) Wszelkie uzgodnienia i konsultacje w zakresie transmisji danych powinny być dokonane w siedzibie Zamawiającego na podstawie zatwierdzonego harmonogramu.
- f) Proces migracji musi objąć pełne dane zawarte we wcześniej użytkowanym systemie.
- g) Nowe rozwiązania muszą realizować wszystkie wymienione wymagania względem Oprogramowania.

2) w zakresie Infrastruktury sprzętowej

W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.

W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.

Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w OPZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne, np. zapis: “Zainstalowane minimum dwa procesory minimum ośmiordzeniowe klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 131 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów” należy rozumieć jako:

“Zainstalowane co najmniej dwa procesory, posiadające co najmniej 8 rdzeni klasy co najmniej x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku minimum 131 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów”.

I. Obszar techniczny

1. Usługi informatyczne - wymagania minimalne

Nazwa	Wymagania minimalne dla usługi
Typ	Usługi informatyczne
Typ	<p>Zamawiający w ramach realizacji przedmiotu zamówienia wymaga wdrożenia usługi katalogowej o zakresie minimum:</p> <ul style="list-style-type: none"> uruchomienie nowej instancji systemu operacyjnego Windows Server będącego w posiadaniu Zamawiającego, wdrożenie, instalacja roli usługi katalogowej, konfiguracja struktury organizacyjnej, stworzenie podstawowych polityk GPO zgodnie z wymaganiami Zamawiającego, utworzenie przykładowego użytkownika, przygotowanie i dołączenie stacji roboczej/serwera do kontrolera domeny, podstawowe szkolenie administratorów w zakresie dodawania użytkowników i dodawania stacji roboczych, zarządzanie użytkownikami i stacjami, wykonawca wykona testowe dodanie do 5 urządzeń PC do pracy w domenie. przygotowanie dokumentacji powdrożeniowej. <p>Zamawiający wymaga, aby Wykonawca wykonał usługi w siedzibie Zamawiającego.</p>
Ilość	1 szt.

2. UTM Unified Threat Management - wymagania minimalne

Nazwa	Minimalne wymagania dla sprzętu
Typ	Urządzenie klasy UTM (Unified Threat Management)
Wymagania ogólne	<p>W ramach przedmiotu zamówienia wymagana jest dostawa systemu bezpieczeństwa, który 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.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System musi umożliwiać 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 5 administratorów do poszczególnych instancji systemu.</p> <p>System musi wspierać protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> Firewall.

	<ul style="list-style-type: none"> • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	<p>W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.</p> <p>Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.</p> <p>Monitoring stanu realizowanych połączeń VPN.</p> <p>System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.</p>
Interfejsy, Dysk, Zasilanie	<p>System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów:</p> <ul style="list-style-type: none"> • 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 Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. • System jest wyposażony w zasilanie AC.
Parametry wydajnościowe	<p>W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.</p> <p>Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.</p> <p>Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.</p> <p>Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.</p> <p>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.</p> <p>Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.</p> <p>Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.</p>
Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ul style="list-style-type: none"> • Kontrola dostępu - zaporę ogniową 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.

	<ul style="list-style-type: none"> 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, wystanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	<p>Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</p> <p>System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:</p> <ul style="list-style-type: none"> Translację jeden do jeden oraz jeden do wielu. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. <p>W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.</p> <p>Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</p> <p>Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</p> <p>Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.</p> <ul style="list-style-type: none"> Amazon Web Services (AWS). Microsoft Azure. Cisco ACI. Google Cloud Platform (GCP). OpenStack. VMware NSX. Kubernetes.
Połączenia VPN	<p>System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> 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.

	<ul style="list-style-type: none"> 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. <p>System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> 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.
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie musi zapewniać obsługę:</p> <ul style="list-style-type: none"> 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 RIPv2), 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.
Funkcje SD-WAN	<p>System musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</p> <p>SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</p>
Zarządzanie pasmem	<p>System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>System musi dawać możliwość określania pasma dla poszczególnych aplikacji.</p> <p>System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</p> <p>System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</p>
Ochrona przed malware	<p>Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</p> <p>System musi umożliwiać 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.</p> <p>System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</p> <p>System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p>

	<p>Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>System musi współpracować 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.</p> <p>System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.</p> <p>Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</p> <p>Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</p>
Ochrona przed atakami	<p>Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</p> <p>Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.</p> <p>Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p> <p>Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.</p>
Kontrola aplikacji	<p>Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> <p>Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</p> <p>Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 21).</p> <p>System musi dawać możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).</p>
Kontrola WWW	<p>Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p> <p>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.</p>

	<p>Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</p> <p>Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</p> <p>Filtr WWW musi dawać możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</p> <p>Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</p> <p>Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</p> <p>System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</p>
Uwierzytelnianie użytkowników w ramach sesji	<p>System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</p> <p>Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych.</p> <p>System musi dawać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</p> <p>System musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.</p> <p>Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p>
Zarządzanie	<p>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.</p> <p>Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.</p> <p>System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</p> <p>System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p> <p>Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</p> <p>Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</p>

Logowanie	<p>Elementy systemu bezpieczeństwa muszą realizować 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.</p> <p>W przypadku, kiedy usługa logowania i raportowania realizowana jest w chmurze, wymagane są stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.</p> <p>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.</p> <p>Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p>
Testy wydajnościowe oraz funkcjonalne	<p>Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.</p>
Serwisy i licencje	<p>Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:</p> <p>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 do daty minimum 06.05.2026r.</p>
Gwarancja oraz wsparcie	<p>System musi być objęty serwisem gwarancyjnym producenta do daty minimum 06.05.2026r. polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.</p> <p>System musi być objęty rozszerzonym wsparciem technicznym realizowanym przez producenta, rozwiązań lub autoryzowanego dystrybutora do daty minimum 06.05.2026r.</p> <p>Do zamawianego sprzętu Wykonawca musi zapewnić usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta świadczona w języku polskim w zakresie:</p> <ul style="list-style-type: none"> • pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu • konfiguracja urządzenia w miejscu instalacji przez certyfikowanego inżyniera zgodnie z wymaganiami użytkownika, najlepszymi praktykami i doświadczeniem inżynierów na podstawie szablonów i przeprowadzonych konsultacji • doradztwo w zakresie konfiguracji • rekonfiguracje urządzenia w związku ze zmianą środowiska lub wymagań klienta (maksymalnie do 10 zdalnych zmian w konfiguracji) • wsparcie telefoniczne zespołu certyfikowanych inżynierów • zdalne wsparcie techniczne • pomoc w zakładaniu zgłoszeń serwisowych u producenta

	<ul style="list-style-type: none"> • pomoc w procesie realizacji naprawy i wymiany w ramach posiadanej gwarancji • usługa jest dostępna w dni robocze 9:00 - 17:00 (8x5) • usługa musi być świadczona przez podmiot posiadający certyfikat ISO 9001 (lub równoważną) w zakresie świadczenia usług serwisowych. Na potwierdzenie wymogu wymagane jest dołączenie do oferty oświadczenia producenta lub Autoryzowanego Dystrybutora Producenta, że serwis oferowanego urządzenia będzie: <ul style="list-style-type: none"> - realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta; - firma serwisująca posiada autoryzację producenta oferowanego urządzenia;
Instalacja i konfiguracja	<p>Instalacja i konfiguracja musi odbyć się w siedzibie Zamawiającego. Musi obejmować w zakresie minimum:</p> <ul style="list-style-type: none"> • Instalacja sprzętu w szafie maksymalnie 19" • Podłączenie okablowania strukturalnego do urządzenia • Zmiana domyślnych haseł • Rejestracja urządzenia na stronie producenta • Aktualizacja oprogramowania • Konfiguracja urządzenia w trybie NAT • Konfiguracja domyślnych profili bezpieczeństwa (AV, IPS, WebFiltering, Application Control) • Konfiguracja portów LAN WAN (konfiguracja do 4 podsieci LAN) • Konfiguracja DDNS (w przypadku dynamicznego IP WAN) • Konfiguracja polityk bezpieczeństwa (do 30 polityk) • Utworzenie do 50 obiektów adresów bądź usług • Konfiguracja WiFi – wbudowanego lub 1 FortiAP zewnętrznego (2 SSID z uwierzytelnieniem PSK) • Konfiguracja do 10 obiektów Virtual IP (Port Forwarding) • Konfiguracja VPN IPSEC lub/i VPNSSL dla użytkowników – maksymalnie 2-3 konta w jednej grupie dostępu (OPCJA Konfiguracja Deep Inspection SSL pod warunkiem instalacji wskazanego certyfikatu CA na stacjach roboczych przez - zapobieganie wyświetlaniu komunikatu o błędnym certyfikacie)
Ilość	1 szt.

3. Serwer - wymagania minimalne

Nazwa	Wymagania minimalne dla sprzętu
Typ	Serwer - sprzęt serwerowy
Obudowa	<p>Obudowa Rack o wysokości maksymalnie 2U umożliwiającą instalację minimum 8 dysków 2,5" z kompletem wysuwanych szyn umożliwiającą montaż w szafie rack i wysuwanie serwera do celów serwisowych.</p> <p>Obudowa z możliwością instalacji karty umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.</p>
Płyta główna	<p>Płyta główna z możliwością zainstalowania dwóch procesorów.</p> <p>Płyta główna musi być zaprojektowana przez producenta serwera.</p>

Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane minimum dwa procesory minimum ośmio-rdzeniowe klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 131 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów. Wydruk z testu należy dołączyć do oferty. Zamawiający dopuszcza wydruk w języku angielskim.
RAM	Minimum 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 32 slotów przeznaczonych do instalacji pamięci. Płyta główna musi obsługiwać do 8TB pamięci RAM.
Zabezpieczenia pamięci RAM	Memory Health Check, Memory Page Retire
Gniazda PCIe	Minimum dwa sloty PCIe x8 generacji 4 oraz minimum cztery sloty PCIe x16 generacji 4.
Interfejsy sieciowe/FC/SAS	Dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ nie zajmujące slotów PCIe. Możliwość instalacji wymiennie modułów udostępniających: <ul style="list-style-type: none"> dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 dwa interfejsy sieciowe 10Gb Ethernet w standardzie BaseT cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT cztery interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.
Dyski twarde	Możliwość instalacji dysków SAS/SATA/NVMe Zainstalowane minimum 3 dyski minimum 600GB SAS 10k skonfigurowane fabrycznie w RAID 5. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde. Możliwość instalacji dwóch dysków hot-swap M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.
Kontroler RAID/HBA	Sprzętowy kontroler dyskowy z pojemnością cache 8GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60.
Wbudowane porty	Minimum port USB 2.0 oraz dwa porty USB 3.0, port VGA,
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości minimum 1600x900
Wentylatory	Redundantne Hot-Plug
Zasilacze	Minimum dwa zasilacze Hot-Plug maksymalnie 1100W Titanium
Bezpieczeństwo	Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardech. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą TPM 2.0

	<p>Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera</p> <p>Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.</p> <p>Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155 (lub równoważnymi).</p> <p>Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).</p>
Karta Zarządzania	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające:</p> <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z usługą katalogową • możliwość obsługi przez ośmiu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232. • możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. • Monitorowanie zużycia dysków SSD • możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, • Automatyczne zgłaszanie alertów do centrum serwisowego producenta • Automatyczne update firmware dla wszystkich komponentów serwera • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON • Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. • Możliwość wykrywania odchyłań konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera • Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać

	<p>możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI.</p> <p>Karta powinna posiadać możliwość rozszerzenia o poniższe funkcjonalności:</p> <ul style="list-style-type: none"> • możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych • kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania • Automatyczne odświeżanie certyfikatów SSL • możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielokrotnego przy logowaniu do karty zarządzającej • możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień • możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera • możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer • możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe • monitorowanie przepływu powietrza na bieżąco
Oprogramowanie do zarządzania	<p>Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniające poniższe wymagania:</p> <ul style="list-style-type: none"> • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z usługą katalogową • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów

- Możliwość importu plików MIB
- Przesyłanie alertów „as-is” do innych konsol firm trzecich
- Możliwość definiowania ról administratorów
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
- Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
- Zdalne uruchamianie diagnostyki serwera.
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

System Operacyjny

Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO.

Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.

SSO musi posiadać następujące, wbudowane cechy:

- a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,
- b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,
- c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych,
- d) 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,
- e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,
- f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,

g) 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),

i) wbudowane wsparcie instalacji i pracy na wolumenach, które:

- I. pozwalają na zmianę rozmiaru w czasie pracy systemu,
- II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
- III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
- IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL),

j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,

k) wbudowane szyfrowanie dysków

l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,

m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,

n) wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,

o) graficzny interfejs użytkownika,

p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),

s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,

t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,

u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

- I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
- II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
- III. zdalna dystrybucja oprogramowania na stacje robocze,
- IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
- V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - 1) dystrybucję certyfikatów poprzez http,
 - 2) konsolidację CA dla wielu lasów domeny,

	<p>3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,</p> <p>VI. szyfrowanie plików i folderów,</p> <p>VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),</p> <p>VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,</p> <p>IX. serwis udostępniania stron WWW,</p> <p>X. wsparcie dla protokołu IP w wersji 6 (IPv6),</p> <p>XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:</p> <ol style="list-style-type: none"> 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. <p>W ramach dostawy SSO mają zostać dostarczone także licencje dostępowe do serwera dla 25 użytkowników.</p>
Certyfikaty	<p>Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 (lub równoważną) lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.</p> <ul style="list-style-type: none"> • Serwer aplikacji musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub normami równoważnymi, • Serwer aplikacji musi posiadać deklarację CE lub równoważną • Serwer musi spełniać wymagania normy NIST SP 800-193 (lub równoważnej) ochrony przed cyberatakami- do oferty załączyć oświadczenie producenta potwierdzające spełnianie wymogu .

Normy Środowiskowe	<p>Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami rozporządzenia nr 1272/2008WE. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC.</p>
Warunki gwarancji	<ul style="list-style-type: none"> Gwarancja producenta na minimum 36 miesięcy, świadczona przez podmiot posiadający ISO 9001:2015 (lub równoważną) oraz ISO-27001 (lub równoważną) na świadczenie usług serwisowych. Na potwierdzenie wymogu wymagane jest dołączenie do oferty oświadczenia producenta, że serwis oferowanego serwera będzie: <ul style="list-style-type: none"> - realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta; - firma serwisująca posiada autoryzację producenta oferowanego serwera; - firma serwisująca posiada ISO 9001:2015 (lub równoważną) oraz ISO-27001 (lub równoważną) na świadczenie usług serwisowych. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Zamawiający w ramach gwarancji wymaga dodatkowo usługi, w ramach której, w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym

	wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Na potwierdzenie, że oferowany serwer będzie posiadał odpowiednią gwarancję, wymagane jest dołączenie oświadczenia producenta oferowanego sprzętu.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Wdrożenie	Wymagane jest uruchomienie fizyczne serwera w tym jego instalację w miejscu wskazanym przez Zamawiającego w zakresie minimum: - montaż serwera: serwer musi zostać podłączony w sposób redundantny do przełącznika, musi zostać zaktualizowany do najnowszej wersji oprogramowania układowego oraz systemowego na dzień wdrożenia. Należy skonfigurować interfejs niskopoziomowego zarządzania serwera. W ramach wdrożenia należy skonfigurować maksymalnie 2 maszyny wirtualne oraz maksymalnie 2 vlany. Wykonawca musi przygotować niezbędną dokumentację w zakresie dokumentacji powdrożeniowej zawierającej opis konfigurowanych opcji wdrożonego środowiska serwerowego. Wymaga się, aby wdrożenie było przeprowadzone przez inżynierów (minimum 1 osoba) posiadających wiedzę na temat dostarczanego modelu serii serwerów danego producenta.
Ilość	1 szt.

4. Network Attached Storage NAS - wymagania minimalne

Nazwa	Wymagania minimalne dla sprzętu
Typ	Network Attached Storage NAS
Obudowa	Tower
Procesor	Minimum czterordzeniowy procesor o taktowaniu minimum 2.0 GHz (maksymalnie 2,7 GHz z przyspieszeniem) osiągający w teście PassMark na co najmniej 2950 punktów.
Sprzętowy mechanizm szyfrowania	Minimum (AES-NI)
Pamięć RAM	Minimum 2 GB pamięci non-ECC SODIMM z możliwością rozszerzenia do minimum 6 GB
Możliwości rozbudowy	Sprzęt powinien być wyposażony w minimum 2 kieszenie na dyski twarde typu hot-swap. Obsługiwane dyski 3.5" oraz 2.5".
Porty zewnętrzne	Minimum: 2 porty USB 3.2.1
Porty sieciowe	Minimum: 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)

Funkcja Wake on LAN/WAN	Sprzęt powinien posiadać funkcje Wake on LAN/WAN
Wentylator obudowy	Minimum 1 wentylator 92 mm x 92 mm
Obsługiwane protokoły sieciowe	Minimum SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPS, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Minimum : <ul style="list-style-type: none"> • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	Maksymalny rozmiar pojedynczego wolumenu: 108 TB Minimalna liczba wewnętrznych wolumenów: 64 Minimalna liczba obiektów iSCSI Target: 128 Minimalna liczba jednostek iSCSI LUN: 256 Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Minimum SHR, Basic, JBOD, RAID 0, RAID 1
Funkcja udostępniania plików	Minimalna liczba kont użytkowników: 2 048 Minimalna liczba grup użytkowników: 256 Minimalna liczba folderów współdzielonych: 256 Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 500 Minimalna liczba jednoczesnych połączeń protokołu SMB/AFP/FTP (z rozbudową pamięci RAM): 1 500
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Usługa katalogowa	Serwer musi łączyć się z usługą katalogową, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń.
Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w zasilacz maks. 60 W
Oprogramowanie	<ul style="list-style-type: none"> • Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia. Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC oraz aplikację mobilną.

	<p>Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.</p> <ul style="list-style-type: none"> • Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Zainstalowane dyski	<p>Ilość: minimum 2 szt. Pojemność: minimum 16TB Obudowa: 3.5" Interfejs: minimum SATA 6Gb/s Prędkość obrotowa: minimum 7200 rpm Maksymalna stała prędkość przesyłu danych: 281 MB/s</p>
Gwarancja	Minimum 24 miesiące gwarancji producenta na sprzęt i minimum 36 miesięcy gwarancji producenta na dyski.
Ilość	1 szt.

5. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 1 - wymagania minimalne

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 1
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem uchwytów montażowych, wyposażona w zintegrowany zasilacz, chłodzona aktywnie.
Porty	<p>Minimum 48 portów 10/100/1000 Mbps RJ45 z obsługą PoE+ 802.3af/at, minimum 4 porty SFP/SFP+ 1/10GbE, Budżet mocy PoE minimum 400 W 1 port typu out-of-band management 1 port konsolowy RS232 RJ45 1 port typu USB A do transferu plików</p>
Wydajność przełącznika	<p>Minimum 16000 adresów MAC Switch fabric capacity minimum 176 Gbps Forwarding rate minimum 120 Mpps Pamięć flash minimum 128 MB Pamięć RAM minimum 512 MB</p>
Funkcjonalność warstwy II	<p>Obsługa minimum 4000 wirtualnych sieci Wsparcie dla agregacji statycznej oraz LACP (802.3ad) Obsługa 8 grup LACP i 8 portów fizycznych per grupa</p>

	Obsługa ramek Ethernet typu Jumbo minimum 9k
Funkcjonalność warstwy III	Obsługa routingu statycznego oraz dynamicznego RIPv2 oraz OSPFv2 Obsługa minimum 64 wpisów routingu statycznego Obsługa minimum 512 wpisów routingu dynamicznego
Inne Funkcjonalności	Obsługa list kontroli dostępu opartych o adresy MAC i IP Ochrona DoS Storm Control Broadcast/Multicast/Unknown Unicast DHCP Snooping DHCP Relay DHCP Server IGMP Snooping Querier IGMP Proxy PVST/PVRST BPDU Guard, BPDU filtering, Root Guard Authentication, Authorization, and Accounting (AAA) Private VLAN Port Mirroring Port Security/MAC Locking DiffServ support DSCP and 802.1p (CoS) Traffic shaping/metering OoS – kolejki priorytetowe oraz Weighted Round Robin (WRR), Strict Priority (SP) Narzędzia diagnostyczne PING, TRACEROUTE, ICMPv6 TFTP, FTP, Telnet, SSH v2 SNMP v1/v2/v3 Zarządzanie IPv6 Funkcjonalność typu autoinstall/autodeployment dla oprogramowania układowego oraz plików konfiguracyjnych Zero-touch deployment Zarządzanie przez CLI, wbudowane WebGUI (HTTP/HTTPS) oraz kontroler w wersji on-premise lub chmurowej
Zgodność z protokołami	802.1ab LLDP ANSI/TIA-1057- LLDP-MED 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority 802.1Q VLAN Tagging 802.1S Multiple Spanning Tree (MSTP) 802.1W Rapid Spanning Tree (RSTP) 802.1X Network Access Control, Auto VLAN 802.2 Logical Link Control 802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP 802.3u Fast Ethernet (100BASE-TX) 802.3x Flow Control RFC 768 UDP

	RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 2030 SNTP RFC 2132 DHCP options and BOOTP vendor extensions RFC 2865 RADIUS Client RFC 3579 RADIUS Support for EAP RFC 3164 Syslog
Inne	Przystosowanie do pracy w temperaturze 0-50 stopni Celsjusza
Gwarancja	Minimum 60 miesięcy gwarancji producenta
Ilość	2 szt.

6. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 2 - wymagania minimalne

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 2
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem uchwytów montażowych, wyposażona w zintegrowany zasilacz, chłodzona aktywnie.
Porty	Minimum 24 porty 10/100/1000 Mbps RJ45 z obsługą PoE+ 802.3af/at, minimum 4 porty SFP/SFP+ 1/10GbE, Budżet mocy PoE minimum 400 W 1 port typu out-of-band management 1 port konsolowy RS232 RJ45 1 port typu USB A do transferu plików
Wydajność przełącznika	Minimum 16000 adresów MAC Switch fabric capacity minimum 128 Gbps Forwarding rate minimum 120 Mpps Pamięć flash minimum 128 MB Pamięć RAM minimum 512 MB
Funkcjonalność warstwy II	Obsługa minimum 4000 wirtualnych sieci Wsparcie dla agregacji statycznej oraz LACP (802.3ad) Obsługa 8 grup LACP i 8 portów fizycznych per grupa Obsługa ramek Ethernet typu Jumbo minimum 9k
Funkcjonalność warstwy III	Obsługa routingu statycznego oraz dynamicznego RIPv2 oraz OSPFv2 Obsługa minimum 64 wpisów routingu statycznego Obsługa minimum 512 wpisów routingu dynamicznego

Inne Funkcjonalności

Obsługa list kontroli dostępu opartych o adresy MAC i IP

Ochrona DoS

Storm Control Broadcast/Multicast/Unknown Unicast

DHCP Snooping

DHCP Relay

DHCP Server

IGMP Snooping Querier

IGMP Proxy

PVST/PVRST

BPDU Guard, BPDU filtering, Root Guard

Authentication, Authorization, and Accounting (AAA)

Private VLAN

Port Mirroring

Port Security/MAC Locking

DiffServ support

DSCP and 802.1p (CoS)

Traffic shaping/metering

OoS – kolejki priorytetowe oraz Weighted Round Robin (WRR), Strict Priority (SP)

Narzędzia diagnostyczne PING, TRACEROUTE, ICMPv6

TFTP, FTP, Telnet, SSH v2

SNMP v1/v2/v3

Zarządzanie IPv6

Funkcjonalność typu autoinstall/autodeployment dla oprogramowania układowego oraz plików konfiguracyjnych

Zero-touch deployment

Zarządzanie przez CLI, wbudowane WebGUI (HTTP/HTTPS) oraz kontroler w wersji on-premise lub chmurowej

Zgodność z protokołami

802.1ab LLDP

ANSI/TIA-1057- LLDP-MED

802.1D Bridging, Spanning Tree

802.1p Ethernet Priority

802.1Q VLAN Tagging

802.1S Multiple Spanning Tree (MSTP)

802.1W Rapid Spanning Tree (RSTP)

802.1X Network Access Control, Auto VLAN

802.2 Logical Link Control

	802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP 802.3u Fast Ethernet (100BASE-TX) 802.3x Flow Control RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 2030 SNTP RFC 2132 DHCP options and BOOTP vendor extensions RFC 2865 RADIUS Client RFC 3579 RADIUS Support for EAP RFC 3164 Syslog
Inne	Przystosowanie do pracy w temperaturze 0-50 stopni Celsjusza
Gwarancja	Minimum 60 miesięcy gwarancji producenta
Ilość	1 szt.

7. Oprogramowanie do wykonywania kopii zapasowych - wymagania minimalne

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie do wykonywania kopii zapasowych
Zarządzanie systemem kopii zapasowych	<p>Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:</p> <ul style="list-style-type: none"> • Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www. • Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego). • Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych. • Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu). • Możliwość definiowania uprawnień dla administratorów systemu kopii zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.).

	<ul style="list-style-type: none"> • Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami. • Wsparcie dla Single Sign On dla logowania do systemu. • Możliwość zarządzania procesem tworzenia kopii zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT. • Możliwość definiowania planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem). • Możliwość tworzenia zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopii zapasowych. • Możliwość zdalnej instalacji agentów kopii zapasowych z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows. • Możliwość zdalnego uaktualniania agentów kopii zapasowych. • Możliwość zdalnego zarządzania procesem wykonywania kopii zapasowej i odzyskiwania danych. • Możliwość zdefiniowania dedykowanej maszyny, której agent kopii zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopii zapasowej). • Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych. • Centralny katalog wszystkich danych zapisanych w kopiach zapasowych. • Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.
Wykonywanie kopii zapasowych	<p>Kopie zapasowe całych dysków i partycji.</p> <ul style="list-style-type: none"> • Kopie zapasowe wybranych plików i folderów. • Kopia zapasowa udziałów sieciowych • Kopie zapasowe aplikacji • Zapis kopii zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczany przez producenta systemu kopii zapasowych. • Zapis kopii zapasowych na udział sieciowe. • Zapis kopii zapasowych na serwer SFTP. • Zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana. • Zapis kopii zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloaderzy). • Możliwość wyszukiwania plików w kopiach zapasowych. • Możliwość szyfrowania plików kopii zapasowych. • Wsparcia dla technologii VSS. • Deduplikacja kopii zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć. • Kompresja plików kopii zapasowych. • Możliwość replikacji kopii zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy). • Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopii zapasowych.
Odtwarzanie kopii zapasowych	<p>Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:</p> <ul style="list-style-type: none"> • Odtworzenie całej maszyny – tzw. Bare Metal Restore.

	<ul style="list-style-type: none"> • Odtworzenie całej maszyny na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową. • Odtworzenie poszczególnych plików i folderów. • Przywracanie przyrostu względem danych, które już się znajdują na dysku na który przywracana jest kopia zapasowa. • Automatyzacja procesu odtwarzania całych maszyn – np.: po zaboottowaniu maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonana kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania). • Wyszukiwanie i podgląd odtwarzanych wiadomości email. • Możliwość granularnego odtwarzania witryn i plików. • Odtwarzanie kontrolerów domeny usługi katalogowej.
Ochrona danych	<p>Dodatkowe (obowiązkowe) wymagania związane ochroną danych dostępne dla systemów Windows Server</p> <ul style="list-style-type: none"> • Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń. • Wbudowana ochrona antywirusowa i antymalware. • Mechanizm ochrony przed exploitami. • Filtrowanie adresów URL. • Zarządzanie produktem antywirusowym Windows Defender i Microsoft Security Essentials. • Funkcja otrzymywania informacji o nowych zagrożeniach wraz ze wskazaniem zadań do wykonania dla konkretnego zagrożenia (m.in instalacja poprawki, wykonanie skanowania stacji). • Mechanizm badania zdrowia dysku. • Mechanizm ciągłej ochrony (backupu) plików zapisywanych w wybranych aplikacjach lub lokalizacjach. Funkcja ta musi co najmniej wspierać aplikacje z kategorii dokumentów, inżynierii oraz z możliwością wskazania niestandardowej aplikacji. • Filtrowanie stron na podstawie kategorii stron. • Skanowanie oprogramowania celem poszukiwania podatności. Podatności wypisane muszą zawierać informacje w zakresie minimum nazwy produktu który zawiera podatność, maszyny na których znaleziono takie oprogramowanie, stopień ważności w skali CVSS. • Możliwość skanowania plików backupu w poszukiwaniu malware'u. • Bezpieczne odtwarzanie backupu - w trakcie odtwarzania backupu będzie wykonywane skanowanie w poszukiwaniu zagrożeń i ich usunięcie.
Przestrzeń chmurowa	<p>Przestrzeń chmurowa dostarczana wraz z oprogramowaniem musi spełniać poniższe wymagania:</p> <ul style="list-style-type: none"> • W przypadku uzyskania uzasadnionej pewności, że doszło do naruszenia bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki dostarczy informacje o takowym naruszeniu na adres e-mail podany podczas rejestracji konta. • W przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby udokumentować, naprawić i zminimalizować skutki naruszenia bezpieczeństwa w odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu.

	<ul style="list-style-type: none"> • Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich repliki muszą być przechowywane na terenie Polski. • Producent powinien przechowywać dane osobowe klienta (dane osobowe oraz kopie zapasowe) przy użyciu technik szyfrowania, minimum AES-256. • Producent powinien wykorzystywać danych osobowych klienta bez anonimizacji w środowiskach programistycznych lub testowych. • Producent oprogramowania powinien przeprowadzać okresowe oceny ryzyka i przeglądy co najmniej raz w roku. • Infrastruktura (chmurowy magazyn kopii zapasowych) jest zaprojektowana zgodnie z podejściem N+1 (to, co niezbędne +1). • Producent oprogramowania powinien być zgodny z standardem bezpieczeństwa ISO 27001 lub SOC 2 lub równoważnych, a magazyn kopii zapasowych powinien być zgodny z certyfikatami ISO 9001, ISO 27001 (lub równoważnymi) oraz powinien posiadać certyfikację DCOS (lub równoważną) na minimum 4 poziomie. • Przestrzeń chmurowa dostarczana wraz z oprogramowaniem powinna posiadać minimum 250GB w ramach jednej licencji, na cały okres jej trwania.
Licencja	Licencje muszą umożliwiać zabezpieczenie minimum 2 serwerów fizycznych. Licencje oraz dostęp do wsparcia technicznego producenta musi obowiązywać do daty minimum 06.05.2026r.
Ilość	2 szt.

II. Obszar kompetencyjny

1. Szkolenia dla działu IT typ 1- wymagania minimalne

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenia dla działu IT typ 1
Wymagania podstawowe	<p>Wykonawca zapewni certyfikowane szkolenie (minimum 2 dni) dla administratora Zamawiającego (1 osoba) z posiadanego rozwiązania antywirusowego ESET. Szkolenie w formie online.</p> <p>Szkolenie powinno zostać dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie do minimum 06.05.2026r.</p>
Wymagania szczegółowe	<p>Program szkolenia będzie obejmować w zakresie minimum:</p> <ul style="list-style-type: none"> • Omówienie dostępnych produktów, • Różnice pomiędzy konsolą ON-PREM a chmurową, • Różnice pomiędzy ochroną na poziomie antywirus i security, • Przydatne strony WWW, • Konto administratora -zarządzanie licencjami (ćwiczenie), • Konsola do zarządzania - architektura i omówienie komponentów, • Instalacja i aktualizacja serwera z konsolą do zarządzania (ćwiczenie), • konsola - omówienie funkcji serwera, • Zarządzanie administratorami i ich uprawnieniami (ćwiczenie), • Zarządzanie agentami- zdalna instalacja i omówienie możliwości (ćwiczenie),

	<ul style="list-style-type: none"> • Grupy statyczne i dynamiczne, • Zadania klienta, serwera oraz wyzwalacze, • Zdalna instalacja klienta antywirusa, • Typowe scenariusze (ćwiczenia), • Omówienie funkcji podstawowych i zaawansowanych klienta, • Ochrona antywirusowa, • Zarządzanie aktualizacją, • Polityki i dziedziczenie (ćwiczenie), • Zapora osobista (ćwiczenie), • Typowe scenariusze (ćwiczenia), • Moduł antyspamowy, • Powiadomienia, • Raportowanie (ćwiczenie), • Kontrola dostępu do stron internetowych (ćwiczenie), • Kontrola dostępu do urządzeń (ćwiczenie), • Migracja konsoli lokalnej do konsoli chmurowej (ćwiczenie), • Wdrożenie klienta antywirusa na urządzenia z systemem Android (ćwiczenie), • Rozwiązywanie problemów. • Administrator po kursie otrzymuje zaświadczenia ukończenia szkolenia.
Ilość	1 szt.

2. Szkolenia dla działu IT typ 2- wymagania minimalne

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenia dla działu IT typ 2
Wymagania podstawowe	<p>Wykonawca zapewni certyfikowane szkolenie (minimum 2 dni) dla administratora Zamawiającego (1 osoba) z wdrożonej w pkt. II. 1. usługi katalogowej.</p> <p>Szkolenie w formie online.</p> <p>Szkolenie powinno zostać dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie do minimum 06.05.2026r.</p>
Wymagania szczegółowe	<p>Program szkolenia będzie obejmować w zakresie minimum:</p> <ul style="list-style-type: none"> • Omówienie usługi katalogowej • Omówienie kontrolerów domeny • Wdrożenie kontrolera domeny • Zarządzanie kontami użytkowników • Zarządzanie grupami • Wdrożenie rozproszonego środowiska • Konfigurowanie lokacji • Konfigurowanie i monitorowanie replikacji usługi katalogowej • Wdrażanie szablonów administracyjnych • Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów • Konfiguracja preferencji zasad grupowych

Ilość	1 szt.
-------	--------

3. Szkolenia dla działu IT typ 3 - wymagania minimalne

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenia dla działu IT typ 3
Wymagania podstawowe	Wykonawca zapewni certyfikowane szkolenie (minimum 1 dzień) dla administratora Zamawiającego (1 osoba) z dostarczonego w pkt. II. 2. Rozwiązania klasy UTM. Szkolenie w formie online. Szkolenie musi być zrealizowane w okresie do minimum 06.05.2026r.
Wymagania szczegółowe	Program szkolenia będzie obejmować w zakresie minimum: <ul style="list-style-type: none"> • Omówienie wstępnej konfiguracji urządzenia - Tryby pracy - Konfiguracja sieci i routingu - System Dashboard i moduły systemu • Konfiguracje routingu • Polityki zapory sieciowej - Koncepcja firewall - Tworzenie obiektów dla reguł firewall - Translacja adresów NAT i Virtual IP • Konfiguracje funkcji ochronnych (profile bezpieczeństwa) - Ochrona antywirusowa - Filtrowanie antyspamowe - System IPS - Kontrola ruchu WWW / blokowanie URL - Kontrola aplikacji - Data Leak Prevention (DLP) - Wirtualne sieci prywatne – VPN IPsec • Bieżącą obsługę systemu - Tworzenie kopii zapasowej konfiguracji i jej odtwarzanie - Aktualizacja firmware • Filtry logów • Zewnętrzne mechanizmy logowania
Ilość	1 szt.

4. Szkolenia dla działu IT typ 4 - wymagania minimalne

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenia dla działu IT typ 4
Wymagania podstawowe	Wykonawca zapewni certyfikowane szkolenie (minimum 1 dzień) dla administratora Zamawiającego (1 osoba) z dostarczonego w pkt. II. 7. rozwiązania do wykonywania kopii zapasowych.

	Szkolenie w formie online. Szkolenie powinno zostać dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie do minimum 06.05.2026r.
Wymagania szczegółowe	<p>Program szkolenia będzie obejmować w zakresie minimum:</p> <ul style="list-style-type: none"> • Możliwości i zastosowanie produktu • Konsola chmurowa- omówienie i dostępne możliwości • Instalacja agentów: <ul style="list-style-type: none"> - Metody wdrożenia, automatyzacja wdrożenia - Sposoby aktualizacji agentów • Tworzenie planów kopii zapasowej: <ul style="list-style-type: none"> - Typy chronionych danych/zasobów/usług - Tworzenie planu backupu całego systemu - Lokalizacje przechowywania kopii zapasowych - Weryfikacja kopii zapasowej - Usuwanie planu kopii zapasowej • Metody odzyskiwanie kopii zapasowej • Administracja kontami i uprawnieniami w konsoli
Ilość	1 szt.