INFR.271.1.2025

Załącznik nr 2a do SWZ. Szczegółowy opis przedmiotu zamówienia

Dotyczy zamówienia publicznego pn. Dostawa rozwiązań z zakresu cyberbezpieczeństwa, w tym specjalistycznego sprzętu komputerowego i oprogramowania dla Gminy Borzechów w ramach projektu „Wzmocnienie systemu cyberbezpieczeństwa w Gminie Borzechów”

Część 1. Dostawa sprzętu i oprogramowania dla Urzędu Gminy Borzechów

Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostawy do siedziby Zamawiającego, tj. Urzędu Gminy Borzechów w zakresie i ilościach wskazanych w zestawieniach rzeczowo – ilościowych odpowiednio dla każdej części.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Dostarczany sprzęt i oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.
4. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
6. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaże adresy WWW, pod którymi można je pobrać.
7. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

Zestawienie rzeczowo - ilościowe

Lp.	Przedmiot dostawy	Ilość	Miejsce dostawy
1.	UTM do 60 użytkowników	2	Urząd Gminy Borzechów
2.	UTM do 30 użytkowników	2	Urząd Gminy Borzechów
3.	UPS Zasilacz awaryjny do szafy RACK	3	Urząd Gminy Borzechów
4.	NAS Dysk sieciowy wraz z 4 dyskami o pojemności 4TB każdy	1	Urząd Gminy Borzechów
5.	Serwer do wykonywania kopii zapasowych. 4 dyski o pojemności 4TB każdy	1	Urząd Gminy Borzechów
6.	Serwer dla jednostek podległych, z kontrolerem domeny, jeden procesor 4-rdzeniowy, 16 GB RAM	3	Urząd Gminy Borzechów

7.	Licencja CAL do Serwera dla jednostek podległych. 5 – pack	11	Urząd Gminy Borzechów
8.	Serwer dla UG, jeden procesor 16-rdzeniowy, 32 GB RAM, 6x 1.92TB SSD SATA	1	
9.	Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X	4	Urząd Gminy Borzechów

1.1. UTM do 60 użytkowników

Wymagania Ogólne

System bezpieczeństwa realizujący 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 powinien zapewniać pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System powinien 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 7 administratorów do poszczególnych instancji systemu.

System musi wspierać protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – rozwiązanie powinno zapewniać możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.

2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

3. Monitoring stanu realizowanych połączeń VPN.

4. System powinien umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall powinien dysponować co najmniej poniższą liczbą i rodzajem interfejsów:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
5. 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.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

8. Zarządzanie pasmem (QoS, Traffic shaping).

9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. 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.

11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.

12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

13. Rozwiązanie powinno posiadać 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).

Polityki, Firewall

1. Polityka Firewall uwzględniająca: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

2. System realizujecy 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.

3. W ramach systemu powinna istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.

5. Polityka firewall umożliwiająca filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

7. Element systemu realizujący funkcję Firewall integrujący się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

    - Amazon Web Services (AWS).

    - Microsoft Azure.

    - Cisco ACI.

    - Google Cloud Platform (GCP).

- OpenStack.
- VMware NSX.
- Kubernetes.

Połączenia VPN

1. System umożliwiający konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji powinien zapewniać:
   - 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 umożliwiający konfigurację połączeń typu SSL VPN. W zakresie tej funkcji powinien zapewniać:
   - 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 powinien posiadać 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.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie powinno zapewniać obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwiający wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspierający zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwiający zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System powinien dawać możliwość określania pasma dla poszczególnych aplikacji.
3. System powinien pozwalać na zdefiniowanie pasma dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewniający możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwiający skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewniający skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwiający 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.

4. System umożliwiający blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.

5. System dysponujący sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

7. System powinien 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.

8. System musi zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opierająca się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

2. System chroniący przed atakami na aplikacje pracujące na niestandardowych portach.

3. Baza sygnatur ataków zawierająca minimum 5000 wpisów. Aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4. Administrator systemu powinien mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

5. System zapewniający wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).

7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.

8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwiająca kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

2. Baza Kontroli Aplikacji zawierajaca minimum 2000 sygnatur. Aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

4. Baza sygnatur powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

5. Administrator systemu powinien mieć możliwość definiowania wyjątków oraz własnych sygnatur.

6. Możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).

7. System powinien umożliwiać określanie dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzystający z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra WWW dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

3. Filtr WWW powinien dostarczać kategorie stron zabronionych prawem np.: Hazard.

4. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. Filtr WWW umożliwiający statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).

6. Filtr WWW dający możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.

7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.

8. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.

9. System pozwalający określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwiający 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.

2. System dający możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.

3. System powinien 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.

4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. 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.

2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

3. Możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4. System współpracujący z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiający przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.

5. System dający możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. Element systemu pełniący funkcję Firewall posiadający wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

7. Element systemu realizujący funkcję Firewall umożliwiający wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).

9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. 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.

2. W ramach logowania element systemu pełniący funkcję Firewall zapewniający 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.

3. Logowanie obejmujące zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.

4. Możliwość włączenia logowania per reguła w polityce firewall.

5. System zapewnia możliwość logowania do serwera SYSLOG.

6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

a) 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 12 miesięcy.

Gwarancja oraz wsparcie

1. System objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, 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.

Rozszerzone wsparcie serwisowe

System objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy.

System objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

- Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
- Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
- Doradztwo w zakresie konfiguracji.
- Zdalne wsparcie techniczne.
- Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
- Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
- Przygotowanie urządzenia do zdalnej konfiguracji.
- Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
- Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
- Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
- Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący powinien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

Wymagania powinny być potwierdzone dokumentami dostarczonymi przed podpisaniem umowy:

- Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
- Certyfikat ISO 9001 podmiotu serwisującego.

Bezpieczeństwo łańcucha dostaw

1. Wymaga się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.)

oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. Dokument ten powinien zostać dostarczony wraz z dostawą urządzenia.

2. Wymaga się, aby został dostarczony dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym. Dokument ten powinien zostać dostarczony wraz z dostawą urządzenia.

1.2. UTM do 30 użytkowników

Wymagania Ogólne

System bezpieczeństwa powinien realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa muszą być realizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej powinny być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall powinien zapewniać pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System powinien 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 7 administratorów do poszczególnych instancji systemu.

System powinien wspierać protokoły IPv4 oraz IPv6 w zakresie:
• Firewall.
• Ochrony w warstwie aplikacji.
• Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – powinna istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall powinien zapewniać funkcję synchronizacji sesji.
2. Powinien być zapewniony monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Powinien być zapewniony monitoring stanu realizowanych połączeń VPN.
4. System powinien umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto powinien dawać możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall powinien dysponować co najmniej poniższą liczbą i rodzajem interfejsów:
   • 5 portami Gigabit Ethernet RJ-45.
2. System Firewall powinien posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalację oprogramowania z klucza USB.
3. System Firewall powinien pozwalać na skonfigurowanie co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System powinien być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a powinna być obsługiwana liczba nie mniejsza niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall powinna wynosić nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji powinna wynosić nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 powinna wynosić nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix powinna wynosić minimum 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus powinna wynosić minimum 500 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTP powinna wynosić minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu – zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych – połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami – Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Powinny być dostępne co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS oraz w ruchu przechodzącym przez system.
13. Rozwiązanie powinno posiadać 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)

Polityki, Firewall

1. Polityka Firewall powinna uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System powinien realizować 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.
3. W ramach systemu powinna istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa, np. DMZ, LAN, WAN.
4. Powinna istnieć możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall powinna umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Powinna istnieć możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall powinien integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu:
   • Amazon Web Services (AWS).
   • Microsoft Azure.
   • Cisco ACI.
   • Google Cloud Platform (GCP).
   • OpenStack.
   • VMware NSX.
   • Kubernetes.

Połączenia VPN

1. System powinien umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji powinien zapewniać:
   • Wsparcie dla IKE v1 oraz v2.
   • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   • Obsługę 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 powinien umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji powinien zapewniać:
   • Pracę w trybie Portal – gdzie dostęp do chronionych zasobów powinien być realizowany za pośrednictwem przeglądarki. W tym zakresie system powinien

zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
• Producent rozwiązania powinien posiadać w ofercie oprogramowanie klienckie VPN, które powinno umożliwiać realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie VPN powinno być dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie powinno zapewniać obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoring dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN powinien wspierać zarówno interfejsy fizyczne, jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall powinien umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System powinien dawać możliwość określania pasma dla poszczególnych aplikacji.
3. System powinien pozwalać na zdefiniowanie pasma dla wybranych użytkowników niezależnie od ich adresu IP.
4. System powinien zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy powinien zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System powinien umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych powinna istnieć możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.

4. System powinien umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System powinien dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System powinien 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.
8. System powinien zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Powinna istnieć możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Powinna istnieć możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu powinien mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System powinien zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych powinny obejmować ochronę co najmniej przed: CSS, SQL Injection, trojanami, exploitami, robotami.
7. Powinna istnieć możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu HTTP.
8. Powinno być zapewnione wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Powinna istnieć możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie powinny działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu powinien mieć możliwość definiowania wyjątków oraz własnych sygnatur.

6. Powinna istnieć możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System powinien 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).

Kontrola WWW

1. Moduł kontroli WWW powinien korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW powinien dostarczać kategorii stron zabronionych prawem, np.: Hazard.
4. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW powinien umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym powinien pozwalać na definiowanie stron z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW powinien dawać możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search powinna przeciwdziałać pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator powinien mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System powinien pozwalać na określenie, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall powinien umożliwiać weryfikację tożsamości użytkowników za pomocą:
   • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System powinien dawać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System powinien 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.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP powinno być zapewnione.

Zarządzanie

1. Elementy systemu bezpieczeństwa powinny mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania powinna być realizowana z wykorzystaniem szyfrowanych protokołów.

3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
4. System powinien współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz powinien umożliwiać przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System powinien dawać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent powinien udostępniać dokumentację.
6. Element systemu pełniący funkcję Firewall powinien posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podgląd pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall powinien umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Powinna istnieć możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Powinna istnieć możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa powinny realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub powinny wymagać zastosowania komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall powinien zapewniać przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto powinna istnieć możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie powinno obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Powinna istnieć możliwość włączenia logowania per reguła w polityce firewall.
5. System powinien zapewniać możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów powinno być możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

Wszystkie funkcje i parametry wydajnościowe systemu powinny być weryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są następujące licencje:
- 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 12 miesięcy.

Gwarancja oraz wsparcie

1. System objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent powinien zapewniać dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe AHB/SOS

a) System powinien być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy.

System powinien być objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

• Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
• Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
• Doradztwo w zakresie konfiguracji.
• Zdalne wsparcie techniczne.
• Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
• Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
• Przygotowanie urządzenia do zdalnej konfiguracji.
• Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
• Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
• Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
• Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący powinien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe powinny być przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji powinien wynosić nie dłużej niż 1 godzinę – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

Wymagania powinny być potwierdzone dokumentami dostarczonymi przed podpisaniem umowy:

• Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
• Certyfikat ISO 9001 podmiotu serwisującego.

Bezpieczeństwo łańcucha dostaw:

1. Wymaga, aby przed podpisaniem umowy został dostarczony dokument, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego

pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Wymaga, aby przed podpisaniem umowy został dostarczony dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

1.3. UPS Zasilacz awaryjny do szafy RACK

Nazwa	Wymagane minimalne parametry techniczne
Typ	Zasilacz awaryjny montowany w szafie rack
Zastosowanie	Zasilacz awaryjny do zabezpieczenia urządzeń aktywnych w szafie dystrybucyjnej w obudowie RACK.
Obudowa	Typu RACK 2u
Montaż	Dołączone do zestawu uchwyty montażowe
Złącza	Min. 4x IEC-C13
Komunikacja	Min. 1x USB typ B Min. 1x RS-232 Wyświetlacz LCD
Moc pozorna	Maks. 2200 VA
Moc czynna	Min. 1320 W
Nominalne napięcie wyjściowe	230 VAC
Przebieg fal	Czysta fala sinusoidalna
Czas podtrzymania (dla obciążenia 100%)	1.1 min.
Czas podtrzymania (dla obciążenia 50%)	7.1 min.
Sprawność w trybie LINE (pełne obciążenie) w %	98
Sprawność w trybie bateryjnym (pełne obciążenie) w %	80
Zakres napięcia wejściowego	165-290VAC
Czas przełączenia (z AC na baterie)	4 ms
Czas ładowania	4h do 90%
Architektura	Line-Interactive

Monitorowanie pracy	- monitorowania statusu zasilania - Zdalne zarządzanie poprzez sieć - Planowane wyłączanie / restart - Historia zdarzeń - Ustawienia akcji dla różnych zdarzeń
Wyposażenie	Instrukcja obsługi w języku polskim, kabel USB, kabel zasilający, 2x kabel IEC, kabel RS-232
Warunki gwarancji	24 miesiące gwarancji producenta

1.4. NAS Dysk sieciowy wraz z 4 dyskami o pojemności 4TB każdy

Typ urządzenia	Serwer NAS
Obudowa	Tower
Procesor	Czterordzeniowy procesor o taktowaniu 2.0 GHz (maksymalnie 2,7 GHz z przyspieszeniem) osiągający w teście PassMark wynik co najmniej 2950 punktów Obowiązująca tabela wyników testu PassMark znajduje się w załączniku nr 2c
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 2 GB pamięci non-ECC SODIMM z możliwością rozszerzenia do min. 6 GB
Możliwości rozbudowy	· Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap · Wbudowane 2 gniazda M.2 obsługujące dyski NVMe. Dyski NVMe mogą posłużyć do utworzenia pamięć podręcznej bądź przestrzeni dyskowej
Pamięć masowa	Zainstalowane dyski: Min. 4 zainstalowane dyski HDD 3,5“ 4 TB 5400 obr./min SATA III 6 Gb/s. przeznaczone do rozwiązań typu pamięć NAS. Średni czas bezawaryjnej pracy (MTBF, w godz.) min. 1 000 000 Zamawiający dopuszcza możliwość instalacji dysków przez Wykonawcę na etapie dostawy
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	Tak

Wentylator obudowy	Min. 2 wentylatory 92 mm x 92 mm
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu: 108 TB • Minimalny liczba wewnętrznych wolumenów: 64 • Minimalny liczba obiektów iSCSI Target: 128 • Minimalny liczba jednostek iSCSI LUN: 256 • Obsługa klonowania/migawek jednostek iSCSI LUN
Pamięć masowa	Zainstalowane dyski: Min. 4 zainstalowane dyski HDD 3,5“ 4 TB 5400 obr./min SATA III 6 Gb/s. Dyski muszą znajdować się na oficjalnej liście kompatybilności dysków dla oferowanego urządzenia przygotowanej przez producenta urządzenia. Zamawiający dopuszcza możliwość instalacji dysków przez Wykonawcę na etapie dostawy
Obsługiwane typy macierzy RAID	Synology Hybrid RAID (SHR), Podstawowy (Basic), JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	• Minimalna liczba kont użytkowników: 2048 • Minimalna liczba grup użytkowników: 256 • Minimalna liczba folderów współdzielonych: 512 • Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 500 • Minimalna liczba jednoczesnych połączeń protokołu SMB/AFP/FTP (z rozbudową pamięci RAM): 1500
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Citrix®, OpenStack®
Usługa katalogowa	Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP
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)
Obsługiwane systemy klienckie	Windows® 7 i nowsze, macOS® 10.12 i nowsze
Obsługiwane przeglądarki	Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w zasilacz maks. 90 W

Oprogramowanie	· 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 instalowanego z Centrum Pakietów · 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/MAC oraz aplikację mobilną na Android/iOS. 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 wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. · 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.
Gwarancja	Wykonawca udzieli gwarancji: · 3 lat na urządzenia główne z możliwością przedłużenia do 5 lat za pomocą dodatkowego pakietu gwarancyjnego

1.5. Serwer do wykonywania kopii zapasowych. 4 dyski o pojemności 4TB każdy

Typ urządzenia	Serwer NAS
Obudowa	Tower

Procesor	Dwurdzeniowy procesor o taktowaniu 2.6 GHz (maksymalnie 3,1 GHz z przyspieszeniem) osiągający w teście PassMark wynik co najmniej 3240 punktów Obowiązująca tabela wyników testu PassMark znajduje się w załączniku nr 2c
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 4 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	• Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 9 dysków łącznie przy użyciu dodatkowej jednostki rozszerzającej podłączanej do jednostki głównej za pomocą portu eSATA • Wbudowane 2 gniazda M.2 obsługujące dyski NVMe. Dyski NVMe mogą posłużyć do utworzenia pamięć podręcznej bądź przestrzeni dyskowej • Wbudowany slot 1x PCIe Gen3 x2 do podłączenia dodatkowej karty sieciowej 10GbE
Pamięc masowa	Zainstalowane dyski: Min. 4 zainstalowane dyski HDD 3,5“ 4 TB 5400 obr./min SATA III 6 Gb/s. przeznaczone do rozwiązań typu pamięć NAS. Średni czas bezawaryjnej pracy (MTBF, w godz.) min. 1 000 000 Zamawiający dopuszcza możliwość instalacji dysków przez Wykonawcę na etapie dostawy
Porty zewnętrzne	Minimum: • 2 porty USB 3.2.1 • 1 porty eSATA
Porty sieciowe	Minimum: • 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Funkcja Wake on LAN/WAN	Tak
Wentylator obudowy	Min. 2 wentylatory 92 mm x 92 mm
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT

Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu: 108 TB • Minimalny liczba wewnętrznych wolumenów: 64 • Minimalny liczba obiektów iSCSI Target: 128 • Minimalny liczba jednostek iSCSI LUN: 256 • Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Synology Hybrid RAID (SHR), Podstawowy (Basic), JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	• Minimalna liczba kont użytkowników: 2048 • Minimalna liczba grup użytkowników: 256 • Minimalna liczba folderów współdzielonych: 512 • Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 1000
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP
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)
Obsługiwane systemy klienckie	Windows® 7 i nowsze, macOS® 10.12 i nowsze
Obsługiwane przeglądarki	Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w zasilacz maks. 100 W

Oprogramowanie	• 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 instalowanego z Centrum Pakietów • 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/MAC oraz aplikację mobilną na Android/iOS. 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 wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. • 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.
Gwarancja	Wykonawca udzieli gwarancji na okres 3 lat na urządzenia główne z możliwością przedłużenia do 5 lat za pomocą dodatkowego pakietu gwarancyjnego

1.6. Serwer dla jednostek podległych, z kontrolerem domeny, jeden procesor 4-rdzeniowy, 16 GB RAM

Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3.5'' wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych bez organizera do kabli.
Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	Jeden procesor 4-rdzeniowy 8-wątkowy, 3.4GHz 12M cache obsługujący ddr5
Pamięć RAM	Minimum 16GB pamięci RAM ECC UDIMM o częstotliwości pracy 5600MT/s. Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Wbudowane porty	min. 4 porty USB w tym 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu, min. 1 port RS232
Gniazda PCI	Niewymagane
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Kontroler dysków	Sprzętowy kontroler dyskowy możliwe konfiguracje poziomów RAID: 0, 1, 10 Wsparcie dla dysków samo szyfrujących.
Dyski twarde	• Możliwość instalacji dysków SAS, SATA, SSD, NL SAS • Zainstalowane 2 dyski SSD o pojemności min. 480GB przeznaczone do intensywnego odczytu, wymieniane bez konieczności wyłączania systemu. • Zainstalowane dwa dyski M.2 NVMe o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
System diagnostyczny	Diody LED informujące o kondycji serwera.
Wentylatory	Minimum 4 wentylatory
Zasilacze	Dwa zasilacze o mocy maks. 700W.
System operacyjny/dodatkowe oprogramowani	Dostarczony system operacyjny przez wzgląd na kompatybilność z obecnie posiadaną infrastrukturą. Licencja na Windows Server 2022 Standard, licencja pokrywająca wszystkie fizyczne rdzenie w serwerze. Wymagania ogólne: • Licencje na zamawiany serwerowy system operacyjny muszą być bezterminowe, a Licencja cyfrowa musi posiadać klucz aktywacyjny umożliwiający aktywację produktu. • Licencje muszą obejmować najnowszą (najwyższą) wersję oprogramowania, dostępną na dzień dostawy, • Dostarczony typ licencji musi umożliwiać przeniesienie, instalację i aktywację oprogramowania na innych serwerach Zamawiającego

	• Wymagane jest zapewnienie możliwości korzystania z wcześniejszych wersji zamawianego oprogramowania (downgrading) Dwa serwery mają posiadać: • licencję przeznaczoną dla szkół Jeden serwer ma posiadać: • licencję przeznaczoną dla Gminnego Ośrodka Pomocy Społecznej
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS powinien mieć możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • monitoring wszystkich kluczowych komponentów (wentylatory, zasilacze, pamięć, procesor, RAID, karty sieciowe oraz dyski twarde) • informacje o aktualnym zużyciu energii oraz temperaturach • kontrola zasilania (włączenie, wyłączenie, restart • podstawowe funkcje diagnostyczne: podgląd dziennika systemowego, dziennika kontrolera cyklu życia • odtworzenie konfiguracji sprzętowej na podstawie kopii z innego serwera • możliwość skonfigurowania wielu kont o zróżnicowanym poziomie przywilejów (wg na ról)
Oprogramowanie do zarządzania (opcjonalnie)	• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w opraciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w opraciu 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.
Gwarancja	• Serwis gwarancyjny producenta realizowany przez okres 3 lata od daty zakupu, świadczony w miejscu użytkowania serwera, obejmujący wszystkie komponenty serwera.

	• Możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. • Czas reakcji autoryzowanego serwisu producenta: od dnia zgłoszenia awarii do końca następnego dnia roboczego. • Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Przed podpisaniem umowy wymagane dostarczenie oświadczenia potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Oświadczenie powinno być dodatkowo potwierdzone przez Producenta sprzętu. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft, Windows Server 2022, Windows Server 2019.
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta.

Wykonawca dokona konfiguracji serwera Active Directory do potrzeb Zamawiającego.

1.7. Licencja CAL do Serwera dla jednostek podległych. 5 – pack

Licencje CAL do serwerów dla jednostek podległych:

- 10 pakietów zawierających po 5 sztuk licencji (łącznie 50 szt. licencji) Microsoft CAL na użytkownika do dwóch serwerów dla jednostek podległych (szkoły)
- 1 pakiet zawierający 5 sztuk licencji (łącznie 5 szt. licencji) Microsoft CAL na użytkownika do serwera dla jednostki podległej (Gminny Ośrodek Pomocy Społecznej).

1.8. Serwer dla UG, jeden procesor 16- rdzeniowy, 32 GB RAM, 6x 1.92TB SSD SATA

Wymagania minimalne:

Zastosowanie	Serwer baz danych, archiwizacji, wirtualizacji.
Architektura	Obudowa maksymalnie 1U kompatybilna ze standardem szaf rack 19 cali, montowana na szynach. Obudowa z możliwością instalacji do 8 dysków 2.5" Hot-Plug.
Procesor	Zainstalowany jeden procesor 16-rdzeniowy, min. 2.4 GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem osiągający w teście PassMark wynik co najmniej 28900 punktów Obowiązująca tabela wyników testu PassMark znajduje się w załączniku nr 2c
Płyta główna	Płyta główna dedykowana do pracy w serwerach, zaprojektowana i wyprodukowana przez producenta serwera. Płyta główna zapewnia możliwość pracy 2 procesorów po minimum 24 rdzeni każdy. Płyta główna musi posiadać przynajmniej 16 slotów pamięci RAM typu DDR4 umożliwiających rozszerzenie pamięci do maksymalnie 1TB.
Pamięć RAM	Nie mniej niż 32GB pamięci DDR4 RDIMM, w minimum 2 kościach w celu zwiększenia wydajności oferowanego rozwiązania.
Karty HBA/NIC/PCIe	Zainstalowany sprzętowy kontroler dysków SAS/SATA z 8GB cache z podtrzymaniem oraz funkcjonalnością RAID 0,1,10,5,6,50,60. Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez zainstalowanie karty w wymaganych slotach PCIe).
Zamontowane dyski twarde	Min. 6 szt. jednakowych dysków Hot-Plug SATA3 SSD o pojemności minimum 1.92TB każdy. Konfiguracja RAID 5. Możliwość zainstalowania karty obsługującej co najmniej dwa dyski M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Karta graficzna	2D, zintegrowana z płytą główną.
Zewnętrzne porty wejścia / wyjścia	Przód obudowy co najmniej: 1 port USB 3.0; 1 port Video VGA; 1 port USB – dedykowany do zarządzania Tył obudowy co najmniej: 1 port USB 3.0; 1 port USB 2.0; 1 port Video VGA; 1 port RJ45 dedykowany do zarządzania
Zdalne zarządzanie	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej;

	• zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Zasilanie	2 zasilacze nadmiarowe o mocy co najmniej 1000W każdy, technologia Hot-Plug. W zestawie kable zasilające złącza C14 IEC320 o długości min. 1.8m.
System operacyjny	Dostarczony system operacyjny przez wzgląd na kompatybilność z obecnie posiadaną infrastrukturą. Licencja na Windows Server 2022 Standard, licencja pokrywająca wszystkie fizyczne rdzenie w serwerze. System zainstalowany na wymaganych nośnikach, preinstalowana partycja recovery. Wymagania ogólne: • Licencje na zamawiany serwerowy system operacyjny muszą być bezterminowe a Licencja cyfrowa musi posiadać klucz aktywacyjny umożliwiający aktywację produktu. • Licencje muszą obejmować najnowszą (najwyższą) wersję oprogramowania, dostępną na dzień dostawy, • Wymagane jest zapewnienie możliwości korzystania z wcześniejszych wersji zamawianego oprogramowania (downgrading) Dodatkowo 20 szt licencji Microsoft CAL na użytkownika.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz możliwość wyposażenia w ramkę panelu przedniego z blokadą, zamykaną na klucz służącą do ochrony nieautoryzowanego dostępu do dysków twardych. • 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. • Moduł TPM 2.0 • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Wspierane systemy operacyjne	• Canonical® Ubuntu® Server LTS. • Citrix® Hypervisor. • Microsoft Windows Server® z technologią Hyper-V.

	• Red Hat® Enterprise Linux. • SUSE® Linux Enterprise Server. • VMware® ESXi.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów x64, Microsoft Windows Server 2022, Microsoft Windows Server 2019.
Gwarancja	1. Serwis gwarancyjny producenta realizowany przez okres 3 lata od daty zakupu, świadczony w miejscu użytkowania serwera, obejmujący wszystkie komponenty serwera. 2. Możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 3. Czas reakcji autoryzowanego serwisu producenta: od dnia zgłoszenia awarii do końca następnego dnia roboczego. 4. Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Przed podpisaniem umowy wymagane dostarczenie oświadczenia potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Dokumentacja, inne	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta.

Wykonawca dokona konfiguracji serwera Active Directory do potrzeb Zamawiającego.

1.9. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X

Typ urządzenia	Przełącznik sieciowy Ethernet Smart Management rack 1Gbit
Porty	- minimum 24 porty 1G RJ45 10/100/1000BASE-T - Minimum 4 porty SFP+ z możliwością pracy 1G/10G Porty SFP+ muszą umożliwiać ich obsadzanie wkładkami 10 Gigabit Ethernet – minimum 10GBase-SR, LR, oraz Gigabit Ethernet – minimum 1000Base- SX, 1000Base LX
Parametry fizyczne	Wysokość maksymalnie 1U, montowany w szafie typu rack 19''
Pamięć	Co najmniej 512 MB SDRAM Co najmniej 256 MB pamięci flash Bufor pakietów co najmniej 1.5 MB CPU ARM Cortex-A9 @ 800 MHz

Wielkość tablicy adresów MAC	Co najmniej 16000
Ilość obsługiwanych sieci VLAN	Co najmniej 256
Wydajność	• Przepustowość przełączania: min. 128 Gbit/s • Przełączanie dla pakietów: min. 95.23 Mpps. • Opóźnienie: < 4.7 uSec dla 100 Mb < 2.4 uSec dla 1000 Mb <1.3 uSec dla 10 Gbps
Obsługa ramek Jumbo	O wielkości co najmniej 9216 bajtów
Funkcjonalność urządzenia	- obsługa agregacji portów zgodnie z LACP (IEEE 802.3ad), - obsługa protokołu SNTP, - Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), MSTP (802.1s) - Minimum 256 obsługiwanych sieci VLAN - Automatyczne przydzielanie klasy urządzenia PoE w oparciu o LLDP oraz LLDP-MED. - Minimum 50 możliwych do utworzenia list ACL, - CoS zgodna z 802.1p - Voice VLAN - Minimum 509 wpisów ARP - Możliwość przechowywania dwóch obrazów oprogramowania: aktywny I zapasowy - Port Security - DHCP Snooping - Klient Radius - Port mirroring, - DHCP Relay, - DoS Protection, - ARP Attack Protection, - Możliwość utworzenia minimum 32 statycznych wpisów w tablicy routingu
Zasilanie	Zasilacz 230V AC wbudowany
Temperatura pracy	0°C do 40°C
Maksymalny obór mocy	22.6 W
Wentylacja	bezwentylatorowy
Zarządzanie	WWW (GUI), SNMP Manager, cloud-based web portal
Akcesoria	Razem z przełącznikiem należy dostarczy: 1. Kabel ….. 2. Wkładkę …..
Gwarancja	Produkty są objęte 90-dniowym całodobowym telefonicznym wsparciem technicznym. Przez pozostały okres gwarancji, dostępne będzie tylko wsparcie techniczne za pomocą czatu. Ograniczona gwarancja dożywotnia, obowiązuje tak długo, jak produkt jest używany przez pierwszego właściciela, dodatkowo jest ograniczona do pięciu (5) lat od daty wycofania produktu ze sprzedaży Dostęp do wersji oprogramowania przez cały okres posiadania dotyczy wszystkich ogólnodostępnych wersji oprogramowania / systemów operacyjnych dla wymienionych produktów, gdy i jeśli są dostępne, przez cały okres posiadania produktu przez klienta.

Dokumenty	Wykonawca winien przedłożyć dokumenty: - Deklaracja zgodności CE oferowanego urządzenia – certyfikat potwierdzony za zgodność z oryginałem, - Oświadczenie producenta lub oświadczenie autoryzowanego przedstawiciela producenta potwierdzające zgodność wszystkich parametrów oferowanego urządzenia wskazanych w Opisie przedmiotu zamówienia.

Uwaga: - W puste pola w kolumnie nr 4 należy wpisać odpowiednio parametr określający oferowany produkt