Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu komputerowego i oprogramowania w ramach projektu Cyfrowa Gmina

RI.271.2.11.2022

Część 1 - Dostawa UTM wraz ze switch-em zarządzalnym

Minimalne parametry UTM

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać 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 – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 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 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 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

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

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 – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
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. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.

5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

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

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 być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi 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 na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

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 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 powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi 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 musi dostarczać kategorii stron zabronionych prawem: Hazard.

4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. 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.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
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 powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, Wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.

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

Certyfikaty
Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje
W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.
2. Licencja na usługę realizowaną w chmurze na okres 12 miesięcy umożliwiająca logowanie i raportowanie z czasem retencji logów minimum 1 rok.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe AHB/SOS

1. System musi 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 gwarancji.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Wykonawca winien przedłożyć dokumenty:
   - Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
   - Certyfikat ISO 9001 podmiotu serwisującego.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Minimalne parametry switch-a (przełącznika sieciowego)

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

Zamawiający jest w posiadaniu rozwiązania FortiGate model 60E. W ramach rozbudowy istniejącego systemu, której celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z istniejącym rozwiązaniem Fortigate, o następujących parametrach:

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 60 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
   - 48 porty GE RJ-45.
   - 4 porty 10 GE SFP+.

Zarządzanie

- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.

- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
   - Centralne zarządzanie konfiguracją urządzenia
   - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
   - Centralne zarządzanie sieciami VLAN.
   - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
   - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
   - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
   - Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
   - Automatyczna detekcja i rekomendacje konfiguracji.
   - Przesyłanie logów na zewnętrzny serwer syslog.
   - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
   - Obsługa białych i czarnych list adresów MAC.
   - Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.

- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres min. 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe

1. System musi 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 gwarancji.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Wykonawca winien przedłożyć dokumenty:
   - Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
   - Certyfikat ISO 9001 podmiotu serwisującego.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Część 2 - Dostawa serwera NAS wraz z dyskami

Minimalna specyfikacja sprzętowa:

Procesor	Procesor 64 bit Intel x86 o takowaniu nie mniejszym niż 2.0 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 8GB DDR4
Pamięć Flash	Nie mniej niż 4GB
Liczba zatok na dyski twarde	Minimum 4
Obsługiwane dyski twarde	3.5" oraz 2.5" SATA oraz 2.5" SATA SSD

Pojemność dysków twardych	minimum do 18TB
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Minimum 2
Diody LED	Minimum Status, LAN, HDD,
Porty USB 3.2 Gen 2	Minimum 2
Porty USB 2.0	Minimum 2
Port PCiE	Tak, minimum 1 Gen3
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 1U
Dopuszczalna temperatura pracy	od 0 do 40˚C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Zasilacz redundatny max. 2 x 250 W, 100-240 V

Specyfikacja oprogramowania	
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Szyfrowanie wolumenów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL

Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server. Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker

Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek

Gwarancja	Min. 36 miesięcy, świadczona przez producenta rozwiązania
Dodatki	Szyny montażowe do szafy rack
Dyski (4 szt)	4 dyski o pojemności 8TB Dyski musza być klasy serwerowej (enterprise) Dyski SATA 6 Gbit/s Obroty minimalnie 7200 / min Dyski musza posiadać MTTF (MTBF) nie mniejszy niż 2 000 000h Pojemność pamięci cache minimum 256 MB Znamionowe roczne obciążenie pracą 550TB (rocznie) Parametr maksymalnej utrzymywanej prędkość przesyłu danych (deklarowana przez producenta dysków) : Dla technologii sektorowej 512e: 248 MiB/s dla pojemności 8TB Gwarancja musi zawierać opcje pozostawienie dysków w razie awarii przez cały okres trwania gwarancji. Należy dostarczyć z oferta oficjalne dokumenty producenta dysków, spełniających wszystkie powyższe wymagania.

Część 3 - Dostawa serwera wraz z oprogramowaniem

Minimalna specyfikacja: Pamięć ram minimum 16GB DDR4 ze wsparciem ECC, taktowanie pamięci nie mniejsze niż 3200 Mhz, możliwość zainstalowanie łącznie do 128GB pamięci, płyta powinna posiadać minimum 4 sloty na pamięć RAM

- Zainstalowany dwa dyski SSD klasy enterpise o pojemności minimum 960GB oraz dwa dyski SATA3 o pojemności nie mniejszej niż 2TB każdy
- Wszystkie dyski muszą pracować w kieszeniach hot swap, z możliwością wyjęcia w trakcie pracy
- Zainstalowany dedykowany kontroler do obsługi RAID, wymagane poziomy RAID to minimum: 0,1,5,6,10,50,60, kontroler musi posiadać wsparcie dla minimum 8 dysków SATA/SAS/NVME, cache minimum 4GB

- Zainstalowany procesor, posiadający minimum 6 rdzeni / 12 wątków, o taktowaniu minimum 3.5 GHz, osiągający w teście passmark minimum 20000 pkt.
- Zasilacze o mocy minimum 700W przeznaczony do pracy ciągłej 24/7 i pozwalający na utrzymanie wszystkich podzespołów serwera,
- Obudowa RACK o wysokości maksymalnej 2U, do zestawu dołączone szyny montażowe
- Obudowa musi posiadać minimum 8 slotów hot swap dla dysków twardych 3.5 cala
- Serwer musi posiadać wszelkie kable lub adaptery– musi być gotowy do pracy w momencie dostawy
- Serwer wyposażony w moduł zdalnego zarządzania pozwalający na dostęp do serwera z innych lokalizacji niż fizyczne położenie serwera
- Płyta główna powinna być przygotowana do obsługi minimum 1 procesora
- Wbudowany napęd dvd slim
- Wymagane złącze karty graficznej: VGA
- Serwer musi posiadać min. 36 miesięcy gwarancji onsite z czasem reakcji 24h, realizowaną w siedzibie Zamawiającego z opcją pozostawienia uszkodzonego dysku twardego u Zamawiającego
- Serwis musi być realizowany przez producenta lub autoryzowanego serwis partnera producenta
- Serwer musi posiadać w BIOSIe wpisane informacje na temat numeru seryjnego, producenta oraz modelu sprzętu
- Wymagane certyfikaty dla producenta serwera: ISO 9001, ISO 14001, CE
- Możliwość sprawdzenia na stronie producenta po podaniu numeru seryjnego: Okresu gwarancji, konfiguracji sprzętu oraz pobrania sterowników
- Karta sieciowa posiadająca 2 porty 1gb ethernet, złącza wyjściowe 2x RJ45
- Zainstalowany moduł TPM dedykowany do płyty
- Dołączony system Windows Server 2022 w wersji standard obsługujący wymaganą ilość rdzeni
- Dołączone licencje CAL na użytkownika w wersji Windows Server 2022, wymagana ilość licencji: 30

Część 4 - Dostawa zestawów komputerowych i laptopów z oprogramowaniem

Zestawy komputerowe minimalna specyfikacja – ilość 15 zestawów:

Procesor:	6 rdzeni, 12 wątków, taktowanie bazowe 2,6GHz, w trybie turbo 4,4GHz, 12MB cache, TDP – 65W, ze zintegrowaną kartą graficzną, osiągający wynik minimum 17100 punktów w teście PassMark – CPU Benchmarks opublikowany na stronie https://www.cpubenchmark.net/cpu_list.php
Chłodzenie procesora	Dostosowane do obsługi procesorów z TDP 95W
Pamięć RAM	Minimum 8 GB (DIMM DDR4, 3200MHz)
Płyta główna	2 sloty pamięci, obsługa do 64GB RAM, wbudowana karta sieciowa 1Gbit z obsługą WOL/PXE, 1x PCI Express 4.0 x16, 2x PCI Express x1, złącza na tylnym panelu: 2x PS, 1x DVI-D, 1x HDMI, 1x DP, 1x VGA, 6x USB z czego min. 2x USB 3.2 Gen1
BIOS	Zapisana trwale w BIOS informacja dotycząca nazwy producenta, numeru seryjnego i modelu.
Dysk	SSD PCIe NVMe, minimum 500GB, prędkość odczytu min. 3500MB/s, zapisu min. 2300MB/s
Napęd ODD	brak
Karta graficzna	Zintegrowana
Multimedia	Wbudowana karta dźwiękowa 8-kanałowa zgodna z High Definition,

Łączność	LAN 10/100/1000 Mbps z obsługą WOL/PXE
Obudowa	MiniTower (obsługa kart o pełnym profilu), zaprojektowana i wyprodukowana na zlecenie producenta komputera, suma wymiarów nie większa niż 945mm, 2x USB 3.2 Gen1, Mic-In, Phone-out, możliwość instalacji wewnątrz napędów 2x 3,5” + 1x 2,5”
Zasilacz	O mocy minimum 350W, spełnia wymagania normy 80 Plus Bronze, aktywne PFC. Głośność pracy (przy obciążeniu 20%/50%/100%): 21,6dB(A) / 21,8dB(A) / 30,4dB(A)
Klawiatura, mysz	Myszka USB 1000dpi, klawiatura USB – obie oznaczone trwałym logo producenta komputera
Właściwości specjalne	Możliwość zabezpieczenia linką, TPM 2.0, Windows AutoPilot ready
System operacyjny	W pełni będzie integrował się z istniejącą usługą Active Directory, w tym GPO (m.in. automatyzacja procesów instalacji oprogramowania). Wykonawca ma obowiązek dostarczyć sprzęt z systemem operacyjnym Windows 10 Pro PL (wersja 64 – bitowa). Klucz systemu musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego z nośnika lub napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego.
Certyfikaty	CE, ISO 9001, ISO 14001 Zgodność: SMBios (DMI), EN62368-1, EN55032, EN55035, EN61000-3-2/3, EN62623, 89/336/ECC
Gwarancja	Min. 12 miesięcy. Gwarancja musi być realizowana przez producenta lub autoryzowanego serwis-partnera producenta. Możliwość sprawdzenia konfiguracji oraz okresu gwarancji na stronie producenta po podaniu numeru seryjnego sprzętu.
Wymagania dodatkowe:	Sprzęt fabrycznie nowy, oryginalnie zapakowany, bez śladów użytkowania, trwale oznaczony logo producenta. Możliwość pobrania sterowników oraz obrazu systemu ze strony producenta po podaniu numeru seryjnego. Sprzęt wyprodukowany w Europie, nie wcześniej niż w 2022 roku. Na sprzęcie powinien być umieszczony symbol legalności systemu operacyjnego w formie naklejki/hologramu potwierdzający jego autentyczność
Monitor	23,8”, matryca IPS, Full-HD, czas reakcji 5ms, kontrast dynamiczny – 30 000 000:1 (DCR), plamka 0,2745mm Złącza VGA, HDMI Wbudowane głośniki Możliwość pochylenia ekranu w zakresie -5 ° - 20 ° Funkcja Flicker-Free oraz Anti-Blue-Light VESA 100x100 Zużycie energii - <0,3W (wyłączony), <0,5W (standby) Opatrzony logiem producenta komputera Kabel HDMI i Audio w komplecie. Gwarancja min. 12 miesięcy – w przypadku usterki zawsze wymiana monitora na nowy na miejscu u klienta. Gwarancja musi być realizowana przez producenta lub autoryzowanego serwis-partnera producenta. Możliwość sprawdzenia okresu gwarancji na stronie producenta po podaniu numeru seryjnego sprzętu.

Pakiet biurowy	Microsoft Office 2021 Licencja komercyjna, wieczysta

Komputery przenośne – laptopy – ilość 3 szt.:

Typ:	Komputer przenośny
Zastosowanie:	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej.
Ekran:	15,6" o rozdzielczości FHD (min. 1920x1080 przy 60Hz) z powłoką przeciwodblaskową
Procesor:	4 rdzenie, 8 wątków, ze zintegrowaną grafiką, taktowanie bazowe 1,6GHz, w trybie turbo 4,2GHz, 6MB cache, osiągający w teście PassMark CPU Mark wynik min. 6350 punktów (należy dołączyć wydruk ze strony https://www.cpubenchmark.net z wynikiem testu dla oferowanego procesora). Pobór mocy TDP nie większy niż 15W.
Pamięć operacyjna:	min. 8GB, 1 slot wolny, możliwość rozbudowy pamięci do 32GB
Parametry pamięci masowej:	Dysk SSD PCIe/NVMe o pojemności min. 500GB, prędkość odczytu/zapisu: 3500/2300 MB/s
Karta graficzna:	Zintegrowana z procesorem z dynamicznie przydzielaną pamięcią współdzieloną.
Wyposażenie multimedialne:	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki
Płyta główna:	Wyposażona przez producenta w dedykowany chipset dla oferowanego procesora.
Napęd:	Wbudowany napęd DVD±RW
Komunikacja:	Wbudowana karta sieci bezprzewodowej 802.11 a/b/g/n/ac, moduł Bluetooth w wersji min. 5.0, karta sieciowa 10/100/1000 ze złączem RJ-45, możliwość instalacji modemu LTE wewnątrz obudowy (nie dopuszcza się modemu podłączanego do portu USB)
Klawiatura:	Układ klawiszy US, możliwość 4 stopniowej regulacji podświetlenia oraz zmiany koloru podświetlenia, wydzielony blok klawiszy numerycznych
Bateria i zasilanie:	Komputer wyposażony w baterię o pojemności min. 41Wh umożliwiającą pracę przez min. 360 minut (wg. danych producenta) oraz zasilacz. Możliwość wyjęcia i wymiany baterii bez otwierania laptopa.
Gwarancja:	Min. 12 miesięcy door-to-door. Gwarancja musi być realizowana przez producenta lub autoryzowanego serwis-partnera producenta. Możliwość sprawdzenia konfiguracji oraz okresu gwarancji na stronie producenta po podaniu numeru seryjnego sprzętu.
Certyfikaty:	Certyfikat CE, ISO14001, ISO9001 lub równoważne
System operacyjny:	W pełni będzie integrował się z istniejącą usługą Active Directory, w tym GPO (m.in. automatyzacja procesów instalacji oprogramowania). Wykonawca ma obowiązek dostarczyć sprzęt z systemem operacyjnym Windows 11 Pro PL (wersja 64 – bitowa). Klucz systemu musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego z nośnika lub napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego.

Wymagania dodatkowe:	Wbudowana kamera internetowa trwale zainstalowana w obudowie matrycy, wejście audio, wbudowany mikrofon, wbudowane głośniki, czytnik kart pamięci, złącza USB – min. 4 szt. w tym 1x USB 3.1 Type-C i 1x USB 3.1 Type-A, wyjście HDMI, wyjście VGA, Touchpad, TPM 2.0, gniazdo Kensington Lock, waga max 2,2 kg, sprzęt fabrycznie nowy, oryginalnie zapakowany, bez śladów użytkowania. Możliwość pobrania sterowników oraz obrazu systemu ze strony producenta po podaniu numeru seryjnego. Sprzęt wyprodukowany w Europie, nie wcześniej niż w 2022 roku. Laptop trwale oznaczony logo producenta. Mysz bezprzewodowa Na sprzęcie powinien być umieszczony symbol legalności systemu operacyjnego w formie naklejki/hologramu potwierdzający jego autentyczność
Pakiet biurowy	Microsoft Office 2021 Licencja komercyjna, wieczysta

Komputer przenośny – laptop – ilość 1 szt.:

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ:	Komputer przenośny
Zastosowanie:	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej.
Ekran:	15,6" o rozdzielczości FHD (min. 1920x1080 przy 60Hz) z powłoką przeciwodblaskową, matryca WVA, kąty widzenia $170^0/170^0$
Procesor:	4 rdzenie, 8 wątków, ze zintegrowaną grafiką, cache 12MB, osiągający w teście PassMark CPU Mark wynik min. 10400 punktów (należy dołączyć wydruk ze strony https://www.cpubenchmark.net z wynikiem testu dla oferowanego procesora)
Pamięć operacyjna:	min. 16GB z możliwością rozbudowy do 32GB, jeden slot wolny
Parametry pamięci masowej:	Dysk SSD PCIe NVMe o pojemności min. 500GB, prędkość odczytu/zapisu: 3500/2300 MB/s Dysk HDD 2,5” 2TB SATA3
Karta graficzna:	Zintegrowana z procesorem z dynamicznie przydzielaną pamięcią współdzieloną.
Wyposażenie multimedialne:	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki
Płyta główna:	Wyposażona przez producenta w dedykowany chipset dla oferowanego procesora.
Napęd ODD:	brak
Komunikacja:	Wbudowana karta sieci bezprzewodowej 802.11 a/b/g/n/ac/ax, moduł Bluetooth w wersji min. 5.2, karta sieciowa 10/100/1000 ze złączem RJ-45
Klawiatura:	Układ klawiszy US, możliwość 4 stopniowej regulacji podświetlenia oraz zmiany koloru podświetlenia, wydzielony blok klawiszy numerycznych
Bateria i zasilanie:	Komputer wyposażony w baterię o pojemności min. 73Wh (umożliwiającą pracę do 16 godzin wg. danych producenta) oraz zasilacz.
Gwarancja:	Min. 12 miesięcy door-to-door. Gwarancja musi być realizowana przez producenta lub autoryzowanego serwis-partnera producenta.

	Możliwość sprawdzenia konfiguracji oraz okresu gwarancji na stronie producenta po podaniu numeru seryjnego sprzętu.
Certyfikaty:	Certyfikat CE, ISO14001, ISO9001 lub równoważne
System operacyjny:	Zainstalowany i aktywowany system operacyjny z wieczystą licencją w polskiej wersji językowej zapewniający dostęp do domeny. Klucz systemu musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego z nośnika bezpośrednio z wbudowanego złącza lub napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. W pełni będzie integrował się z istniejącą usługą Active Directory, w tym GPO (m.in. automatyzacja procesów instalacji oprogramowania). System operacyjny ma pozwalać na uruchomienie i pracę z większością aplikacji biurowych dostępnych na rynku. Pełna polska wersja językowa. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników
Wymagania dodatkowe:	Wbudowana kamera internetowa trwale zainstalowana w obudowie matrycy, wbudowany mikrofon i głośniki, czytnik kart pamięci, czytnik linii papilarnych, złącza USB – min. 4 szt. w tym 1x USB 3.2 Gen2 Type-A, 1x USB 3.2 Gen2 Type-C i 1x Thunderbolt 4, wyjście HDMI, Touchpad, TPM 2.0, gniazdo Kensington Lock, waga max 1,7 kg, sprzęt fabrycznie nowy, oryginalnie zapakowany, bez śladów użytkowania. Możliwość pobrania sterowników oraz obrazu systemu ze strony producenta po podaniu numeru seryjnego. Sprzęt wyprodukowany w Europie, nie wcześniej niż w 2022 roku. Laptop trwale oznaczony logo producenta. Mysz bezprzewodowa. Na sprzęcie powinien być umieszczony symbol legalności systemu operacyjnego w formie naklejki/hologramu potwierdzający jego autentyczność
Pakiet biurowy	Microsoft Office 2021 Licencja komercyjna, wieczysta