*Załącznik nr 2 do SWZ*

**Opis Przedmiotu Zamówienia (OPZ)**

Przedmiot zamówienia, w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020 Działanie 5.1 Rozwój cyfrowy JST, obejmuje dostawę komputerów, sprzętu elektronicznego oraz oprogramowania zgodnego ze specyfikacją poniżej:

1. **Stacja robocza**

|  |  |
| --- | --- |
| Zastosowanie | Komputer stacjonarny będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej. |
| Obudowa | Obudowa typu tower, fabrycznie przystosowana do pracy w pionie. Możliwość otwarcia obudowy komputera i dołożenia komponentów bez utraty gwarancji. |
| Procesor | Procesor ośmiordzeniowy, zgodny z architekturą x86 z zintegrowaną kartą graficzną, osiągający w teście PassMark wynik min. 20000 punktów.  Do oferty należy załączyć wydruk ze strony potwierdzający spełnione wymaganie. |
| Płyta główna | - chipset dostosowany do oferowanego procesora lub równoważny  - wyposażona w sprzętowy moduł TPM 2.0  - minimum 4 złącza SATA III 6.0 Gb/s  - minimum 1 złącze PCIe 4.0 x 16  - minimum 2 złącza PCIe 3.0 x 1 |
| Pamięć operacyjna | - 16 GB RAM DDR4 3200 MHz  - Możliwość rozbudowy do 64 GB.  - Ilość banków pamięci, minimum: 2 szt.  - ilość wolnych banków pamięci, minimum: 1szt. |
| Dysk Twardy | 512 GB M.2 NVMe PCIe 3.0 SSD |
| Karta graficzna | -Zintegrowana z procesorem, -Z możliwością dynamicznego przydzielenia pamięci w obrębie pamięci systemowej, -Obsługiwana przez DirectX w wersji co najmniej 12.1 i OpenGL w wersji co najmniej 4.5.  -Posiadająca minimum 24 jednostki wykonawcze. |
| Napęd optyczny | Wbudowana w obudowę nagrywarka DVD x8 |
| Łączność | LAN 10/100/1000 Mbit/s Wi-Fi 6 (802.11ax) + Bluetooth 5.2 |
| Złącza zintegrowane z obudową - panel przedni | Minimum: 1x złącze audio słuchawek 1x złącze audio mikrofonu 2x złącza USB 2.0 Typ-A 2x złącza USB 3.2 Gen1 Typ-A Minimalna ilość złącz nie może być osiągnięta przy pomocy zewnętrznych HUB-ów lub przejściówek. |
| Złącza zintegrowane z obudową – panel tylny | Minimum: 1x złącze RJ45 Ethernet 1x złącze HDMI w wersji 1.4 1x złącze VGA 1x złącze DVI-D 2x złącza PS2 2x złącza COM 1x złącze równoległe (LPT)  2x złącza USB 2.0 Typ-A 2x złącza USB 3.2 Gen 1 Typ-A 3x port Audio 2x złącza SMA dla anteny Wifi  Minimalna ilość złącz nie może być osiągnięta przy pomocy zewnętrznych HUB-ów lub przejściówek. |
| Zasilacz | 500W spełniający normę minimum 80+ Bronze. |
| Wyposażenie | Myszka USB lub PS2 Klawiatura USB lub PS2 Kabel zasilający  Antena Wifi |
| BIOS | BIOS zgodny ze specyfikacją UEFI z pełnym wsparciem dla obsługi przy pomocy myszki i klawiatury.  Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS bieżących informacji o:  - aktualnej dacie  - wersji BIOS wraz z datą wydania  - producencie i modelu komputera  - zamontowanym procesorze wraz z taktowaniem, ilością rdzeni i wątków logicznych, pamięci cache L1/L2/L3  - zamontowanej pamięci RAM wraz z taktowaniem  - obłożeniu banków pamięci RAM  - zamontowanym dysku twardym wraz z modelem i pojemnością  - zamontowanej nagrywarce DVD wraz z modelem  - aktualnej prędkości pracy zamontowanego wentylatora  - temperaturze procesora  - temperaturze płyty głównej  - trybie pracy dysku SSD  - trybie pracy wbudowanego napędu optycznego  - sekwencji bootowania  BIOS musi oferować możliwość:  - włączenia i wyłączenia wirtualizacji  - włączenia i wyłączenia funkcji Hyper-Threding  - włączenia i wyłączenia funkcji Intel SpeedStep  - włączenia i wyłączenia wszystkich jak i pojedynczych portów SATA  - włączenia i wyłączenia wszystkich jak i pojedynczych portów USB  - włączenia i wyłączenia zintegrowanej karty audio - włączenia i wyłączenia zintegrowanej karty LAN - włączenia i wyłączenia karty Wi-fi wraz z Bluetooth - włączenia i wyłączenia portu COM 1 i COM 2 - włączenia i wyłączenia portu równoległego (LPT)  BIOS musi oferować możliwość ustawienia dwóch niezależnych haseł. Hasła dostępowego do ustawień BIOS i hasła powodującego blokadę rozruchu komputera. |
| System operacyjny | Zainstalowany Microsoft Windows 11 Pro PL 64-bit. Umieszczony na obudowie Certyfikat Autentyczności w postaci specjalnej naklejki zabezpieczającej lub załączone potwierdzenie producenta komputera o legalności dostarczonego oprogramowania systemowego. |
| Sterowniki | - Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w  najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem jednej strony www producenta komputera. |
| Oprogramowanie dodatkowe | Preinstalowane oprogramowanie producenta komputera umożliwiające pobieranie najnowszych sterowników i BIOS.  Pozwalające na regulację pracy wentylatora dla minimum 3 niezależnych trybów.  Pozwalające na przeprowadzenie diagnostyki w zakresie testu co najmniej:  -pamięci RAM -wbudowanego modułu Wi-fi/Bluetooth -dysku SSD  -systemu operacyjnego |
| Gwarancja | Minimum 36 miesięcy.  Gwarancja realizowana na miejscu u klienta.  Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych. |
| Wsparcie techniczne producenta: | Możliwość sprawdzenia telefonicznego bezpośrednio u producenta konfiguracji sprzętowej komputera oraz warunków gwarancji. |
| Certyfikaty i standardy: | CE dla oferowanego komputera.  ISO 9001:2015 dla autoryzowanego serwisu Producenta komputera. |

**Monitor komputerowy**

Wymiary matrycy : 23.8

Proporcjami obrazu : 16:9

Powierzchnia wyświetlacza : Non-Glare

Typ podświetlenia : Oświetlenie LED

Typ matrycy :IPS

Kąt widzenia :178°/ 178°

Rozdzielczość :1920 x 1080

Jasność :350 cd/㎡

Współczynnik kontrastu :1000:1

Wyświetlane kolory :16.7M

Czas reakcji : 5ms

Częstotliwość odświeżania : do 75 Hz

Flicker-free : Tak

Wybór temperatury kolorów :Tak( 4 tryby)

HDCP : Tak

Dark Boost : Tak

Niska emisja niebieskiego światła :Tak

Wbudowana w ramę monitora Kamera internetowa : TAK, 2.0M Pixels, regulwany obiektyw w zakresie min. 300 stopni

Cechy Audio

Głośniki :Tak 2Wx2

Mikrofon :Tak wbudowane 2 szt.

DisplayPort 1.2 x 1

HDMI(v1.4) x 1

VGA x 1

Gniazdo słuchawkowe :Tak

Wejście audio :Tak

Zamek Kensington :Tak

Konstrukcja z możliwością dostosowania nachylenia pod kątem +35° ~ -5°, obracania w poziomie pod kątem ±180°, obracania w pionie pod kątem ±90° (pivot) oraz regulacji wysokości do 130 mm

Monitor wyposażony w certyfikowane przez TÜV Rheinland technologie Flicker Free oraz Low Blue Light, dla zapewnienia komfortu podczas użytkowania.

1. **Przełączniki sieciowe (SWITCH)**

Wymaga się aby urządzenie obsługiwało następujące funkcje, protokoły oraz spełniało następujące wymagania:

* 24 portów PoE+ 10/100/1000 Mbps
* 4 dedykowane porty SFP
* IEEE® 802.3 10BASE-T
* IEEE 802.3u 100BASE-TX
* IEEE 802.3ab 1000BASE-T
* IEEE 802.3z 1000BASE-X
* IEEE 802.3x full-duplex flow control
* IEEE 802.3az (EEE)
* IEEE 802.3af (DTE Power via MDI)
* IEEE 802.3at (DTE Power via MDI Enhancements)
* IEEE 8021.Q VLAN (256 groups, Static)
* IEEE 802.1p Class of Service (CoS)
* 8 kolejek sprzętowych
* Port-based QoS
* IEEE 802.3ad Static or Dynamic Link Aggregation (LACP)
* IEEE 802.1D Spanning Tree Protocol
* IEEE 802.1w Rapid Spanning Tree Protocol
* IEEE 802.1s Multiple Spanning Tree Protocol
* SNMP v1, v2c, v3
* RFC 1213 MIB II
* RFC 1643 Ethernet Interface MIB
* RFC 1493 Bridge MIB
* RFC 2131 DHCP client
* IEEE 802.1x (RADIUS)
* RADIUS accounting
* IEEE 802.1x Dynamic VLAN Assignment
* HTTPS/SSL: Secure HTTP GUI
* Layer 3 (DSCP) Quality of Service (QoS)
* TACACS+
* Port-based security by locked MAC addresses
* TCP/UDP-based priority mapping
* IGMP snooping v1, v2, v3
* MLD snooping
* ACLs (MAC, IPv4, IPv6 and TCP/UDP based)
* Ograniczenie przepustowości na wejściu oraz wyjściu
* SNTP
* DNS
* Ochrona przed DoS oraz Auto DoS
* IPv6 management, multicast and QoS
* Static Routing
* DHCP snooping
* Protocol and MAC-based VLAN
* RMON group 1, 2, 3, 9
* Private Enterprise MIB
* Port mirroring – many-to-one
* IEEE 802.3ab LLDP
* LLDP-MED
* Protected ports
* Możliwość wykonania prostego testu okablowania
* Zgodność z EEE (Energy Efficient Ethernet)
* Obniżenie poboru energii w trybie bezczynności, lub krótkiego kabla
* Magistrala 56 Gbps
* Budżet PoE: min. 190W
* Bufor pakietów: 1,5MB
* Pamięć RAM min. 128 MB
* Ilość MAC: 8 K
* Ilość VLANs: min 256;
* Ilość kals 802.1p: 7
* Ilość LAGs: 8
* Ilość statycznych tras min.: 32
* Ilość wpisów ARP min.: 512
* Kolejek DiffServ min.: 7
* Ilość ACLs (IPv4/IPv6): min 100
* Ilość grup multicast min.: 512
* Czas bezawaryjnej pracy: min. 1250360
* Zgodność elektromagnetyczna oraz bezpieczeństwo: znak CE, FCC Part 15 Class A,

Urządzenie powinno być objęte ograniczoną wieczystą gwarancją producenta trwającą do 5 lat po ogłoszeniu zaprzestania produkcji wraz z wymianą na następny dzień roboczy przez cały okres gwarancji. Urządzenie powinno być objęte 90 dniowym wsparciem technicznym realizowanym przez producenta oraz pomocą techniczną w formie czat przez cały okres gwarancji.

1. **Signature pady**

Monochromatyczny panel LCD o przekątnej 4,5″, na którym zmieszczą się długie podpisy i przyciski oprogramowania

Bezprzewodowe, bezbateryjne piórko rejestrujące 1024 poziomy nacisku

Zaawansowane szyfrowanie RSA/AES do przeprowadzania bezpiecznych transakcji

Uchwyt na pióro oraz blokada kabla USB, która zapobiega jego przypadkowemu odłączeniu

Unikalny numer ID sprzętu, umożliwiający identyfikację urządzenia użytego do złożenia podpisu

Wbudowane gniazdo na blokadę bezpieczeństwa

Wzmocnione, odporne na zarysowania szkło chroniące panel LCD

Dane techniczne:

Wymiary: Min.162 x 174 x 11 mm

Połączenie: USB

Pobór prądu: 1.0 W

Ekran: F-STN ze szkła trawionego

Rozdzielczość Min. 320 x 200 pix

Technologia: Indukcja elektromagnetyczna (EMR)

Obszar podpisu: Min. 96 x 60 mm

Dokładnośc: ±0.5 mm

Transfer danych 200 punktów na sekundę

Poziomy nacisku 1024

Szyfrowanie: AES256 / RSA2048

Zabezpieczenie: Kensington

1. **Słuchawki z mikrofonem**

Łączność -Przewodowe

Budowa słuchawek - Nauszne otwarte

Pasmo przenoszenia słuchawek - 42 ~ 17000 Hz

Impedancja słuchawek - 32 Om

Czułość słuchawek - 95 dB

Wbudowany mikrofon - Tak

Charakterystyka mikrofonu - Wielokierunkowy

Pasmo przenoszenia mikrofonu - 90 ~ 15000 Hz

Złącze - Minijack 3,5 mm - 2 szt.

Długość kabla - 2,0 m

Zasilanie - Zewnętrzne

Dodatkowe informacje - Ruchomy mikrofon z funkcją eliminacji szumów z otoczenia

1. **UTM**
2. **Router**

OBSŁUGA SIECI

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

INTRUSION PREVENTION SYSTEM (IPS)

1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
9. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).

KSZTAŁTOWANIE PASMA (Traffic Shapping)

1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

1. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
4. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

OCHRONA ANTYSPAM

1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
2. Ochrona antyspam ma działać w oparciu o:
   1. białe/czarne listy,
   2. DNS RBL,
   3. Skaner heurystyczny.
3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
   1. PPTP VPN,
   2. IPSec VPN,
   3. SSL VPN.
3. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
5. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
6. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
7. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

1. Urządzenie ma posiadać wbudowany filtr URL.
2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
3. Administrator ma mieć możliwość dodawania własnych kategorii URL.
4. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
5. blokowanie dostępu do adresu URL,
6. zezwolenie na dostęp do adresu URL,
7. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
8. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
9. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
10. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
11. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
12. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

UWIERZYTELNIANIE

1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
   1. lokalną bazę użytkowników (wewnętrzny LDAP),
   2. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
   3. usługę katalogową Microsoft Active Directory.
2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
   1. SSL,
   2. Radius,
   3. Kerberos.
4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
   1. równoważenie względem adresu źródłowego,
   2. równoważenie względem połączenia.
3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

1. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
5. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
6. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
7. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
8. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
9. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
10. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
    1. manualnego eksportu do pliku w dowolnym momencie czasu,
    2. automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
11. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
12. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

RAPORTOWANIE

1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
6. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
7. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
8. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
2. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
3. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
4. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny.
5. Urządzenie ma posiadać usługę DNS Proxy.
6. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

GWARANCJA I SERWIS

1. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
2. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów.
3. Liczba portów Ethernet 10/100/1000Mbps – min.8.
4. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
5. Przepustowość Firewall (1518 bajtów UDP) – minimum 2Gbps.
6. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 1.6Gbps.
7. Przepustowość filtrowania Antywirusowego – minimum 400Mbps.
8. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 350Mbps.
9. Maksymalna liczba tuneli VPN IPSec – minimum 50.
10. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20.
11. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 20.
12. Obsługa interfejsów 802.11q (VLAN) – minimum 128
13. Liczba równoczesnych sesji – minimum 200 000 i nie mniej niż 15 000 nowych sesji/sekundę.
14. Urządzenie nie ma limitu na liczbę użytkowników.
15. Liczba reguł filtrowania – minimum 4 096.
16. Liczba tras statycznego routingu – minimum 512.
17. Liczba tras dynamicznego routingu – minimum 10 000.
18. Wymaga się, aby dostawa obejmowała również:

* Minimum 12-miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu.
* Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 12 miesięcy liczoną od dnia zakończenia wdrożenia całego systemu.
* Rozszerzoną gwarancję typu Next Business Day, czyli wymianę uszkodzonego urządzenia na drugi dzień roboczy na okres minimum 12 miesięcy

1. **Oprogramowanie biurowe**

1. Nowa licencja bezterminowa w najnowszej dostępnej wersji, nie używana nigdy wcześniej, wieczysta, w wersji pudełkowej (box) z kluczem do rejestracji produktu na stronie producenta.

2. Licencja przeznaczona dla użytkowników biznesowych.

3. Wymagania odnośnie interfejsu użytkownika - pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na język angielski,

4. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:

4.1. posiada kompletny i publicznie dostępny opis formatu,

4.2. ma zdefiniowany układ informacji w postaci XML (standard uniwersalnego formatu tekstowego służący do zapisu danych w formie elektronicznej),

4.3. umożliwia wykorzystanie schematów XML,

4.4. wspiera w swojej specyfikacji podpis elektroniczny,

5. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb użytkownika oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców,

6. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy),

7. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim,

8. Pakiet zintegrowanych aplikacji biurowych musi zawierać:

8.1. edytor tekstów

8.2. arkusz kalkulacyjny,

8.3. narzędzie do przygotowywania i prowadzenia prezentacji.

9. Edytor tekstów musi umożliwiać:

9.1. edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,

9.2. wstawianie oraz formatowanie tabel,

9.3. wstawianie oraz formatowanie obiektów graficznych,

9.4. wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),

9.5. automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,

9.6. automatyczne tworzenie spisów treści,

9.7. automatyczne tworzenie spisów treści,

9.8. formatowanie nagłówków i stopek stron,

9.9. sprawdzanie pisowni w języku polskim,

9.10. śledzenie zmian wprowadzonych przez użytkowników,

9.11. nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,

9.12. określenie układu strony (pionowa/pozioma),

9.13. wydruk dokumentów,

9.14. wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną,

9.15. pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007, 2010, 2013, 2016, 2019, 2021 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu,

9.16. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,

10. Arkusz kalkulacyjny musi umożliwiać:

10.1. tworzenie raportów tabelarycznych,

10.2. tworzenie wykresów liniowych (wraz z linią trendu), słupkowych, kołowych,

10.3. tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,

10.4. tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice),

10.5. obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych.

10.6. narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych,

10.7. tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,

10.8. wyszukiwanie i zamianę danych,

10.9. wykonywanie analiz danych przy użyciu formatowania warunkowego, 9) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,

10.10. nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,

10.11. formatowanie czasu, daty i wartości finansowych z polskim formatem,

10.12. zapis wielu arkuszy kalkulacyjnych w jednym pliku,

10.13. zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, 2007, 2010, 2013, 2016, 2019, 2021 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.

10.14. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

11. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

11.1. przygotowywanie prezentacji multimedialnych, które będą: a) prezentowanie przy użyciu projektora multimedialnego,

11.2. drukowanie w formacie umożliwiającym robienie notatek,

11.3. zapisanie jako prezentacja tylko do odczytu,

11.4. nagrywanie narracji i dołączanie jej do prezentacji,

11.5. opatrywanie slajdów notatkami dla prezentera,

11.6. umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,

11.7. umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,

11.8. odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,

11.9. możliwość tworzenia animacji obiektów i całych slajdów,

11.10. prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera,

11.11. zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, 2007, 2010, 2013, 2016, 2019, 2021

1. **Dysk NAS serwer plików**

**Sprzęt**

|  |  |
| --- | --- |
| **CPU** | Czterordzeniowy procesor min. 2,0 GHz |
| **Sprzętowy mechanizm szyfrowania** | Tak |
| **Pamięć** | Wbudowana pamięć 4 GB DDR4 z możliwością rozbudowy do 8 GB5 |
| **Zgodny typ dysków** | 4 dyski 3,5" lub 2,5" SATA HDD/SSD   1. 2 dyski M.2 2280 NVMe SSD |
| **Dyski w komplecie** | 4 szt. o minimalnych parametrach:  Pojemność - 4 TB  Wielkość pamięci podręcznej - 256 MB  Prędkość dysku (RPM) - 5400rpm  Interfejs - SATA  Szybkość transmisji - do 180MB/s  Technologia zapisu - SMR |
| **Napęd z możliwością wymiany podczas pracy** | Tak |
| **Port zewnętrzny** | 1. 2 porty USB 3.0 2. 1 porty eSATA |
| **Wymiary maksymalne (wys. × szer. × gł.)** | 170 × 200 × 230 mm |
| **LAN** | 2 x Gigabit (RJ-45) |
| **Funkcja Wake on LAN/WAN** | Tak |
| **Zaplanowane włączanie / wyłączanie** | Tak |
| **Wentylator obudowy** | 2 wentylatory (min. 92 × 92 mm) |

**Ogólne specyfikacje systemu**

|  |  |
| --- | --- |
| **Protokoły sieciowe** | SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) |
| **System plików** | 1. Wewnętrzny: Btrfs, ext4 2. Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT6 |
| **Obsługiwane typy macierzy RAID** | RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |
| **Zarządzanie pamięcią masową** | 1. Maksymalny rozmiar pojedynczego wolumenu: 108 TB |
| **Pamięć podręczna SSD** | 1. Obsługa pamięci podręcznej do odczytu i zapisu 2. Obsługa pamięci M.2 NVMe SSD |
| **Funkcja udostępniania plików** | 1. Liczba kont użytkowników lokalnych: do 2 048 2. Liczba grup lokalnych: do 256 3. Liczba folderów współdzielonych: do 512 4. Liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 1 000 |
| **Usługa katalogowa** | Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP |
| **Wirtualizacja** | VMware vSphere® 6,5, Microsoft Hyper-V®, Citrix®, OpenStack® |
| **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 |