GKPII.271.3.2022

Załącznik Nr 7 do SWZ – **Opis przedmiotu zamówienia**

Minimalne wymagania dla sprzętu i oprogramowania:

1. Laptop 14 Cali

- matryca 14 cali z podświetleniem LED
- powłoka ekranu błyszcząca, dotykowa
- zawias o zakresie odchylenia 360°
- rozdzielczość FullHD, 1920x1080, IPS
- procesor Intel Core i7-1165G7, 4.7GHz
- pamięć RAM 8GB – 16GB DDR4-3200
- szybki dysk 512GB SSD
- grafika Intel Iris Xe Graphics
- WiFi 802.11 b/g/n/ac/ax (1x2)2.4/5GHz MU-MIMO
- moduł Bluetooth 5.2
- wbudowany czytnik kart pamięci
- podświetlana klawiatura
- czytnik linii papilarnych
- porty SuperSpeed USB Typ-A (zgodne z 3.0 i 2.0)
- port SuperSpeed USB Typ-C (3.1 Gen 2)
- cyfrowe złącze HDMI 2.0
- kamerka internetowa
- system operacyjny Windows 10 64 bit

---

2. Laptop 17 cali

- Procesor Intel Core i5 i7
- Karta graficzna: Intel
- Pamięć RAM: 16 GB
- Dysk twardy: 1TB HDD
- Dysk SSD: 256 GB M.2 PCIe NVMe
- Typ ekranu: 17,3", 1920 x 1080 (FullHD), Matowy, IPS
- Napęd optyczny: Nagrywarka DVD
- Dźwięk: Zintegrowana karta dźwiękowa, Wbudowane głośniki, Wbudowany mikrofon
- Kamera internetowa
- Łączność: Wi-Fi 6 (802.11 ax), Bluetooth 5.0, LAN 10/100/1000 Mb/s
- Zainstalowany system operacyjny: Microsoft Windows 10 , 11 Profesionall
- czytnik linii papilarnych

- podświetlana klawiatura

---

3. Program do backupu danych

- Licencja na 40 stacji roboczych + 2 serwery
- Możliwosc backupu do N komputerów (np. 300)
- Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich
- Program serwerowy kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, Linux, BSD, Mac OS X, QNAP, Synology
- Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, Linux, BSD, Mac OS X, QNAP, Synology
- Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików)
- Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)
- Automatyczny backup przy wyłączaniu komputera
- Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ?
- Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)
- Backup baz danych i plików poczty w trybie online i offline
- Kopie rotacyjne (wersjonowanie)
- Zapis archiwów w otwartym formacie (ZIP 64-bit)
- Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi
- Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)
- Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej
- Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych
- Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO
- Kompresja po stronie stacji roboczej
- Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP,
- Replikcacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows)
- Centralne sterowanie całym Systemem z jednego miejsca
- Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników
- Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN

- Wysyłanie Alertów administracyjnych na e-mail
- Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych
- Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki
- Automatyczna aktualizacja oprogramowania na komputerach zdalnych
- Bezterminowa licencja - licencja nie może być ograniczona czasowo
- Interfejs, instrukcja i pomoc techniczna w języku polskim

---

4. Dyski 8TB 7200obr. 256MB CMR
   - Format 3.5"
   - Interfejs SATA III (6.0 Gb/s)
   - Pamięć podręczna cache 256 MB
   - Prędkość obrotowa 7200 obr./min
   - Niezawodność MTBF 1 000 000 godz.

   8 szt.

---

5. Serwer plików
   - Procesor Intel® Celeron® J4125 4-core/4-thread processor, burst up to 2.7 GHz
   - Architektura procesora 64-bitowy x86
   - Intel® HD Graphics 600
   - Pamięć systemowa 4 GB SO-DIMM DDR4 (1 x 4 GB) + 4GB DODATKOWE
   - Gniazdo pamięci 2 x SO-DIMM DDR4
   - Pamięć flash 4 GB (ochrona systemu operacyjnego przed podwójnym rozruchem
   - Wnęka dysków 8 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s
   - Kompatybilność dysków 3,5-calowe wnęki:
     3,5-calowe dyski twarde SATA
     2,5-calowe dyski twarde SATA
     2,5-calowe dyski SSD SATA
   - Port 2,5 Gigabit Ethernet
     (2,5G/1G/100M)
     - 2 (także obsługa 10M)
   - Gniazdo PCIe 1
     Gniazdo 1: PCIe Gen 2 x2
   - Port USB 2.0 - 2
   - Port USB 3.2 Gen 1 - 2
   - Wyjście HDMI 1, HDMI 1.4b
   - Kształt 2U, do montażu stelażowego
   - Zasilacz 300W (x2), 100-240V

---

6. UPS

- UPS (1500VA/900W, 4x IEC, AVR, LCD, RACK) x 2 szt
- Topologia - Line-interactive
- Kształt napięcia wyjściowego - Sinusoidalny
- Gniazda wyjściowe
  - IEC 320 C13 - 4 szt.
  - RJ-45
  - USB
- Zabezpieczenia
  - Przeciwzwarciowe
  - Przeciążeniowe
  - Przeciwprzepięciowe
  - Termiczne
  - Zabezpieczenie przed przeładowaniem

---

7. UPS

- Zastosowanie - wolnostojący
- Moc wyjściowa pozorna 700 VA
- Moc wyjściowa czynna 390 W
- Napięcie wejściowe - 230 V
- Zakres napięcia wyjściowego - 230 V
- Kształt napięcia wyjściowego - aproksymowana sinusoida
- Czas ładowania - 6 godz.
- Rodzaj gniazd - schuko
- Ilość gniazd wyjściowych - 3 szt.
- Sygnalizacja optyczno-akustyczna

---

8. Firewall typu UTM + AV + SANDBOX licencja 5 lat

- 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.
- Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
- Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.

- Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
- 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.
- 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.
- Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
- Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
- Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
- Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
- Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
- 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.
- Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
- Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
- Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
- 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.
- Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
- 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.
- Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
- 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).

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

- Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
- Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
- Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
- 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.
- Urządzenie ma być dostarczone wraz z komercyjnym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o Sandboxing zlokalizowany w Internecie na serwerach producenta. Nie dopuszcza się aby analiza była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza była przeprowadzana przez firmy trzecie.
- Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
- Ochrona antyspam ma działać w oparciu o:
  białe/czarne listy,
  DNS RBL,
  Skaner heurystyczny.
- W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
- Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
- Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
- Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
- PPTP VPN,
- IPSec VPN,

- SSL VPN.
- SSL VPN ma działać co najmniej w trybach tunelu i portalu.
- Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
- Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
- Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
- Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
- Urządzenie ma posiadać wbudowany filtr URL.
- Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
- Administrator ma mieć możliwość dodawania własnych kategorii URL.
- Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
- blokowanie dostępu do adresu URL,
- zezwolenie na dostęp do adresu URL,
- blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
- Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
- Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
- Filtr URL musi uwzględniać komunikację po protokole HTTPS.
- Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
- Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
- Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
- lokalną bazę użytkowników (wewnętrzny LDAP),
- zewnętrzną bazę użytkowników (zewnętrzny LDAP),
- usługę katalogową Microsoft Active Directory.
- Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
- Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
- SSL,
- Radius,
- Kerberos.
- Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
- Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
- Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

- Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
- Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
- równoważenie względem adresu źródłowego,
- równoważenie względem połączenia.
- Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
- Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
- Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
- W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
- Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
- Urządzenie ma umożliwiać statyczne trasowanie pakietów.
- Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
- Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
- Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
- Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
- Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
- Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
- Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
- Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
- Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
- Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
- Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.
- Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
- Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
- Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:

- manualnego eksportu do pliku w dowolnym momencie czasu,
- 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
- Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
- Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
- Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
- System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
- System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
- System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
- System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
- W ramach posiadanej licencji urządzenie ma umożliwiać skorzystanie z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
- Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
- Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
- Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
- Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
- Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
- Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny.
- Urządzenie ma posiadać usługę DNS Proxy.
- 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.
- Urządzenie ma być objęte 60-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
- W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal

- Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
- Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów.
- Liczba portów Ethernet 10/100/1000Mbps – min.8.
- Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
- Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
- Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2.4Gbps.
- Przepustowość filtrowania Antywirusowego – minimum 495Mbps.
- Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 600Mbps.
- Maksymalna liczba tuneli VPN IPSec – minimum 100.
- Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20.
- Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
- Obsługa interfejsów 802.11q (VLAN) – minimum 128
- Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż
- 18 000 nowych sesji/sekundę.
- Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
- Urządzenie nie ma limitu na liczbę użytkowników.
- Liczba reguł filtrowania – minimum 8 192.
- Liczba tras statycznego routingu – minimum 512.
- Liczba tras dynamicznego routingu – minimum 10 000.

---

9. Serwer

- Procesor Xeon E-2224 4x3,4GHz Turbo 4,5GHz, 8MB cache
- SERWER RACK 1U
- pamięć 16GB DDR4 ECC 2666MHz, maks. 128GB
- dyski 2 x 240GB SSD M.2 RAID1 DELL BOSS + 4 x 1TB SATA 7.2k DELL RAID10 NHP
- kontroler RAID 0,1,5,10 PERC S140
- zarządzanie iDRAC9 Basic, dedykowany port
- sieć 2 x GbLan
- Wymiary Szer: 434 mm Wys: 42,80 mm Głębokość: 551 mm
- Szyny
- zasilacz 450W
- Windows Server 2022 Essentials z licencją dla 25 użytkowników. zainstalowany Windows Server 2022 Essentials, w zestawie nośnik USB lub DVD z oprogramowaniem, klucz licencji
- 36 miesięcy gwarancji producenta

10. Program do Inwentaryzacji i monitoringu

- MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) ma obejmować serwery Windows, Linux, Unix, Mac; routery,
- przełączniki, urządzenia VoIP i firewalle w zakresie:
- wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
- wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją
- o OU)
- wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku.
- wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach
- o dowolnym rozmiarze i kolorze.
- wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie.
- wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny.
- zablokowania mapy urządzeń przed przypadkową edycją.
- serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów.
- serwerów pocztowych:
- program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty,
- program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),
- program ma możliwość wykonywania operacji testowych,
- program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.
- monitorowania serwerów WWW i adresów URL.
- cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie
- internetowej i statusu protokołu HTTPS.
- obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.

- obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID.
- obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych.
- monitoringu routerów i przełączników wg:
- zmian stanu interfejsów sieciowych,
- ruchu sieciowego,
- podłączonych stacji roboczych – graficzna prezentacja panelu switcha,
- ruchu generowanego przez podłączone do portów stacje robocze.
- serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie.
- wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu.
- wydajności systemów Windows:
- - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.
- Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Program posiada również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.
- Program umożliwia również definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie.
- Program ma możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).
  W ZAKRESIE INWENTARYZACJI program automatycznie gromadzi informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

- Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów,
- kart itp.
- Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
- Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.

- Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
- Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania
- programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
- Umożliwia odczytanie numeru seryjnego (klucze licencyjne).
- Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez
- określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
- Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
- Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
- Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania
- administratorów wykonywane w tej funkcji są logowane.
- Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:
- przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz
- automatycznego aktualizowania zgromadzonych informacji,
- tworzenia powiązań między zasobami a urządzeniami,
- tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak
- i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
- wskazania osób uprawnionych do użycia zasobów,
- definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości
- dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
- określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
- definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- importu danych z zewnętrznego źródła (.CSV),

- przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
- tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
- oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
- ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
- generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich
- oprogramowania,
- generowania protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
- archiwizacji i porównywania audytów zasobów,
- tworzenia kodów kreskowych dla zasobów,
- drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
- inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej na system Android,
- inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
- definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data"
- z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja").
- Dodatkowo dostępny jest Agent inwentaryzacji na system Android.
- Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji
- o oprogramowaniu i audycie licencji poprzez:
- Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
- Informacje o aplikacjach używanych w organizacji.
- Tworzenie własnych wzorców aplikacji.
- Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
- Informacje o komputerach, na których aplikacja została wykryta.
- Zarządzanie posiadanymi licencjami.
- Wskazywanie osób odpowiedzialnych za licencję.
- Wskazanie użytkowników licencji.
- Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
- Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.

- Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
- Zarządzanie posiadanymi licencjami: raport zgodności licencji.
- Możliwość przypisania do programów numerów seryjnych, wartości itp.

W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW program umożliwia monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

- Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
- Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz
- informacją o uruchomieniu na podwyższonych uprawnieniach,
- Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
- Informacji o edytowanych przez użytkownika dokumentach,
- Historii pracy (cykliczne zrzuty ekranowe),
- Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
- Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez
- użytkownika),
- Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
- Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.
- Program ponadto posiada możliwość:
- blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu
- WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen
- tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy
- grupami lub kontami.
- blokowania ruchu na wskazanych portach TCP/IP,

- blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
- wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze
- lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje
- określoną ilość stron w ciągu dnia,
- przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
- definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.
-
- Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich
- komputerach pracowali w danym czasie.
- Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.
- Program posiada Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.
  PROGRAM UMOŻLIWIA REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM. W ramach kontroli stacji użytkownika dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Moduł umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach") oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Moduł ten zawiera również komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów) oraz bazę wiedzy

pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program umożliwia informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy.

- Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.
- Moduł pomocy zdalnej umożliwia również:
- pobieranie listy użytkowników z Active Directory,
- zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji
- uprawnień, resetu hasła, edycji kont,
- zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
- zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej,
- tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii
- w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,
- automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w
- określonych kategoriach lub pochodzących od określonych grup użytkowników,
- procesowanie zgłoszeń użytkowników z wiadomości e-mail,
- tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do
- wybranych kategorii zgłoszeń,
- wykonywanie operacji na wielu zgłoszeniach równocześnie,
- dołączanie załączników do zgłoszeń,
- rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
- szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
- wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
- zrzuty ekranowe (podgląd pulpitu),
- dystrybucję oprogramowania przez Agenty,
- dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
- zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji
- następuje kolejkowanie zadania dystrybucji pliku,
- możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
- planowanie nieobecności pracowników helpdesk,

- obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np.
- przekroczeń SLA wraz z podsumowaniem,
- generowanie raportów obsługi helpdesk,
- zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego
- użytkownika systemu),
- zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
- wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera
- Blokowanie urządzeń i nośników danych.
- Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
- Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski
- przenośne, napędy CD/DVD, stacje dyskietek.
- Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
- Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
- Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
- Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
- Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków
- BitLocker.
- Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM. Zarządzanie prawami dostępu do urządzeń:
- Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
- Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. -
- urządzenia prywatne są blokowane.
- Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
- Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
- Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.
- Audyt operacji na plikach na urządzeniach przenośnych:
- Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
- Podłączenie/odłączenie urządzenia przenośnego.
- Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.
- Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup

- domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.

Program WSPIERA ZARZĄDZANIE CZASEM I ANALIZOWANIE AKTYWNOŚCI UŻYTKOWNIKÓW poprzez

- dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji może oznaczyć sesję aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Może również uzyskać dostęp do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni mogą uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły pozwalają zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania.
- Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.
- Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.
- Statystyki aktywności podwładnych widoczne dla przełożonego.
- Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.
- Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.
- Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.
- Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na
- stronach internetowych.
- Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne
- i nieproduktywne.
- Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.
- Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia
- (kategoryzowanie).
- Wskaźnik czasu poświęconego na aktywność produktywną.
- Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.
- Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka -
- predefiniowana lista kategorii z możliwością edycji.

- Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji.

---

11. Switch x 6

- Zarządzanie - Zarządzalny L2
- Dostęp - Narzędzie oparte na kliencie lub Przeglądarka WWW (GUI)
- Architektura sieci - Gigabit Ethernet
- Obudowa - Metalowa, typu desktop
- Rodzaje wejść / wyjść - 8x RJ-45 10/100/1000 Mb/s
- Obsługiwane standardy - IEEE 802.3, IEEE 802.3u, IEEE 802.3x, IEEE 802.3ab, IEEE 802.3az
- Rozmiar tablicy MAC - 4 k
- Przepustowość - 16 Gb/s
- Bufor pakietów - 1.5 Mbits
- Dodatkowe informacje - Auto MDI-MDIX, Praca w trybie half i full-duplex IGMP Snooping, Bandwidth Control, IEEE 802.1Q VLAN traffic segregation, Port-based VLAN, IEEE 802.1p Quality of Service, Surveillance VLAN, Voice VLAN

---

12. Access Point x 3

- Interfejs sieciowy - 1x gigabitowy Port Ethernet 10/100/1000
- Anteny - 2,4 GHz: antena z potrójną polaryzacją, 3 dBi , 5 Ghz: 6 dBi
- Standardy WiFi - 802.11 a/b/g/n/ac
- Sposób zasilania - Pasywne PoE 24 V (Pairs 4, 5+; 7,8 Return) lub PoE 802.3af/A 48 V
- Zasilanie - Gigabitowy adapter PoE 24 V, 0.5 A
- Maks. pobór mocy - 6,5 W
- Maksymalna moc TX - 2,4 GHz: 24 dBm , 5 GHz: 22 dBm
- BSSID Do 4
- Oszczędzanie energii - Wspierane
- Zabezpieczenia transmisji bezprzewodowej - WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
- Certyfikaty - CE, FCC, IC
- Montaż - Na ścianie lub suficie (uchwyty w zestawie)
- Dopuszczalna temperatura pracy Od -10 do 70 st. C
- Dopuszczalna wilgotność powietrza 5%-95% niekondensująca
- VLAN - 802.1Q

- Zaawansowane QoS - Limitowanie przepustowości na użytkownika
- Guest Traffic Isolation - Wspierane
- WMM - Voice, Video, Best Effort, Background
- Liczba klientów podłączonych jednocześnie - 200+
- Wspierane przepustowości

  802.11a - 6, 9, 12, 18, 24, 36, 48, 54 Mb/s
  802.11n - 6,5 - 450 Mb/s (MCS0 - MCS23, HT 20/40)
  802.11ac - 6,5 - 867 Mb/s (MCS0 - MCS9 NSS1/2, VHT 20/40/80)
  802.11b - 1, 2, 5.5, 11 Mb/s
  802.11g - 6, 9, 12, 18, 24, 36, 48, 54 Mb/s