**Część IV SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENA/SPECYFIKACJA TECHNICZNA**

**Część I Dostawa Unified Threat Management wraz ze switchem i szkoleniem.**

|  |  |  |
| --- | --- | --- |
| NAZWA | WYMAGANIA | SPECYFIKACJA I PARAMETRY PROPONOWANEGO SPRZĘTU/ROZWIĄZANIA |
| Firewall typu UTM + AV + SANDBOX + SNS 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.  • Zamawiający wymaga dostarczenia dedykowanego systemu centralnego logowania i raportowania, obsługującego wszystkie dostarczone w ramach postępowania firewalle.  • W ramach systemu logowania i raportowania musi zostać dostarczony system monitorujący, gromadzący logi, korelujący zdarzenia i generujący raporty na podstawie danych z systemów bezpieczeństwa.  • System centralnego logowania i raportowania musi dostarczony w postaci maszyny wirtualnej instalowanej w środowisku VMware.  • System logowania i raportowania musi zapewniać przestrzeń dyskową o pojemności nie mniejszej niż 4 TB i i pozwalać na przechowywanie zarchiwizowanych danych w ramach systemu przez okres minimum 2 lat.  • System logowania i raportowania musi umożliwiać zbieranie minimum 6 GB logów dziennie.  • Logi nie mogą być przechowywane w chmurze.  • Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.  • System logowania i raportowania musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów firewalli.  • System logowania i raportowania musi posiadać narzędzia dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie.  • System logowania i raportowania musi mieć możliwość synchronizacji z serwerami czasu NTP.  • System logowania i raportowania musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta Firewalli, które będą dostarczone w ramach postępowania firewalle.  • System logowania i raportowania musi umożliwiać tworzenie statycznych raportów. Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.  • System logowania i raportowania musi umożliwiać zaplanowanie wykonania raportów.  • System logowania i raportowania musi mieć predefiniowany raport przez producenta Firewalli, które będą dostarczone w ramach postępowania na firewalle.  • System logowania i raportowania musi umożliwiać tworzenie własnych raportów.  • System logowania i raportowania musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) z funkcjonalnością „drill-down”.  • System centralnego logowania i raportowania musi być objęty serwisem gwarancyjnym na okres 60 miesięcy. |  |
| SZKOLENIE | • Stacjonarne szkolenie za zakresu obsługi i administracji UTM |  |
| SWITCH | • 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 |  |
| PROGRAM DO BACKUP | Oprogramowanie może być dostarczane w dwóch scenariuszach:   * + Cloud(Software as Service),   + On-premise. * Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud. * Interfejs systemu dostępny jest w języku:   + polskim,   + angielskim, * Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych, * Oprogramowanie może być uruchomione w kontenerze docker, * Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:   + Debian: 9+   + Ubuntu: 16.04+   + Fedora: 29+   + centOS: 7+   + RHEL: 6+   + openSUSE: 15+   + SUSE Enterprise Linux (SLES): 12 SP2+   + Windows Client: 7, 8.1, 10 (1607+)   + Windows Server: 2008 R2+, * System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji, * Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii(awaria jednego z komponentów nie spowoduje przestoju),   Wsparcie techniczne:   * Pomoc techniczna w językach:   + polskim,   + angielskim. * Materiały samopomocowe:   + Baza wiedzy:     - polski,     - angielski   Zarządzanie:   * Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli webowej, * Zarządzanie całym systemem poprzez dashboardy, * Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego, * System posiada wbudowane predefiniowane zadania backupowe, * System umożliwia tworzenie zadań backupowych w oparciu o kalendarz. * Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem, * Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem, * Monitorowanie postępu działania zadania, * Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach:   + Zadanie zostało zakończone pomyślnie,   + Zadanie zostało zakończone z ostrzeżeniami,   + Zadanie zostało zakończone z błędem,   + Zadanie zostało anulowane,   + Zadanie nie zostało uruchomione. * System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego. * Możliwość zdefiniowania okna backupowego dla każdego z zadań, * Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów, * System pozwala na klonowanie planów kopii zapasowych, * System umożliwia reset hasła administratora w przypadku jego utraty, * Oprogramowanie umożliwia definiowanie retencji według schematów:   + GFS(Grandfather-Father-Son),   + FIFO(First-In, First-Out). * Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami, * Konta użytkowników mogą być tworzone poprzez import pliku CSV, * Oprogramowanie umożliwia tworzenie grup urządzeń, * Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów). * System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.:   + System Administrator,   + Backup operator,   + Restore operator,   + Viewer.   Składowanie danych:   * Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie z poziomu jednej konsoli, * System umożliwia składowanie danych:   + Lokalnie:     - Zasób SMB,     - Zasób NFS,     - Zasób ISCSI,     - Zasób S3,     - Katalog zabezpieczonego urządzenia.   + W chmurze:     - Amazon Web Service,     - Magazyn zgodny z S3,     - Dostarczanej przez producenta. * System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji, * System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.   Odtwarzanie:   * Odtwarzanie granularne:   + Pojedynczych plików z kopii obrazu dysku,   + Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365, * Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:   + Windows: 7+,   + Windows Server: 2008 R2+, * Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika. * Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive’a, * Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V. * Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK), * Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL), * Odtwarzanie zasobów plikowych z prawami dostępu, * Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows), * Odtwarzanie danych według harmonogramu, * Przywracanie danych z określonego urządzenia/użytkownika, * Przywracanie kopii z wybranego magazynu. * Przywracanie danych Microsoft 365:   + do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku:     - pst,     - mbox.   + do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji), * System posiada możliwość nieodwracalnego kasowania danych, * Przywracanie repozytoriów GIT:   + Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket),   + przywracanie między kontami.   Backup:   * Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla:   + Systemów operacyjnych:     - Alpine 3.10+,     - Debian: 9+,     - Ubuntu: 16.04+,     - Fedora: 29+,     - centOS: 7+,     - RHEL: 6+,     - openSUSE: 15+,     - SUSE Enterprise Linux(SLES): 12 SP2+,     - macOS: 10.13+,     - Windows: 7, 8.1, 10(1607+),     - Windows Server: 2008 R2+,   + Środowisk wirtualnych:     - Hyper-V,     - VMware: 6.7+.     - Dowolne inne w sposób agentowy   + Repozytoriów GIT:     - GitHub,     - Bitbucket. * Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla:   + Baz danych**:**     - Microsoft SQL,     - MySQL,     - PostgreSQL,     - Firebird,     - Dowolnych innych przez podpięcie skryptów pre/post. * Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:   + 128 bit,   + 192 bit,   + 256 bit. * Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów:   + ZStandard,   + LZ4. * Oprogramowanie umożliwia zarządzanie poziomem kompresji, * Wykonywanie kopii zapasowej otwartych plików(VSS), * System umożliwia uruchamianie skryptów przed i po backupie, * System umożliwia uruchamianie skryptów po wykonaniu migawki VSS, * System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów, * Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT, * Backup plikowy, * Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe, * Oprogramowanie umożliwia konsolidację wersji kopii zapasowych, * Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia, * Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego. * Oprogramowanie pozwala na backup zaszyfrowanych partycji.   GIT   * Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych), * Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki).   Licencjonowanie:   * Sposób licencjonowania opiera się na:   + Ilości serwerów/endpointów- dla fizycznych urządzeń,   + Ilości fizycznych hostów - dla środowisk wirtualnych,   + Ilości repozytoriów - dla GIT. * Licencje powinny pozwalać na wieczyste zabezpieczenie:   + 2 fizycznych serwerów   + 40 fizycznych endpointów * Wsparcie techniczne: * Świadczone jest w języku polskim, bezpośrednio przez główną siedzibę producenta, * Zapewnia dostęp do aktualizacji oprogramowania, * Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego, * Obowiązuje przez okres minimum 12 miesięcy. |  |

**Część II Dostawa Ap Wi-Fi**

|  |  |  |
| --- | --- | --- |
| NAZWA | WYMAGANIA | SPECYFIKACJA I PARAMETRY PROPONOWANEGO SPRZĘTU/ROZWIĄZANIA |
| Access Point | • 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 |  |
| AP 60 Ghz | Nadajnik , odbiornik 60 Ghz x 2szt.  • praca w paśmie 60 GHz, standard 802.11ad  • urządzenie bezprzewodowe zintegrowane z anteną  • zapasowe radio 5 GHz (automatycznie przełącza się w przypadku błędu połączenia 60 GHz)  • 1x port Gigabit Ethernet  • zasilanie: pasywne PoE lub PoE 802.3af/at |  |

**Cześć III Dostawa serwera NAS wraz z dyskami oraz UPS-em**

|  |  |  |
| --- | --- | --- |
| NAZWA | WYMAGANIA | SPECYFIKACJA I PARAMETRY PROPONOWANEGO SPRZĘTU/ROZWIĄZANIA |
| SERWER NAS | • 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 |  |
| 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. |  |
| SERWER NAS | • Procesor AnnapurnaLabs Alpine AL314 32-bit ARM® Cortex-A15 4-core 1.7GHz processor  • Pamięć systemowa 4 GB SODIMM DDR3 RAM + dodatkowe 4 GB  • Pamięć flash 512 MB (ochrona systemu operacyjnego przed podwójnym rozruchem)  • Wnęka dysków 4 dyski 3,5-calowe SATA 6 Gb/s, 3 Gb/s  • Port Gigabit sieci Ethernet - 2  (RJ45)  • Port USB 3.2 Gen 1 – 3  • Kształt Tower |  |
| UPS - NAS | • 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 |  |
| 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 |  |

**Część IV Dostawa komputerów i monitorów**

|  |  |  |
| --- | --- | --- |
| NAZWA | WYMAGANIA | SPECYFIKACJA I PARAMETRY PROPONOWANEGO SPRZĘTU/ROZWIĄZANIA |
| STACJA KOMPUTEROWA | • Obudowa - Small Form Factor (SFF)  • Procesor - Intel® Core™ i5-10400 (2.9 GHz - 4.3 GHz, 6 rdzeni/ 12 wątków, 12 MB cache, 65 W)  • Pamięć RAM 8 GB (1 x 8 GB, DDR4, UDIMM, 2666 MHz, non-ECC)  • Maksymalna ilość pamięci - 64 GB  • Liczba gniazd pamięci (ogółem / wolne) - 2 / 1  • Chipset - Intel® B460  • Dysk - 256 GB (SSD, PCIe, NVMe, M.2)  • Grafika - Intel® UHD 630 (Zintegrowana, Pamięć współdzielona)  • Karta sieci LAN - Realtek RTL8111H (Zintegrowana, 1 Gb/s)  • Karta sieci WLAN - Intel® Wireless-AC 3165 (802.11ac)  • Bluetooth - Bluetooth 4.2  • Dźwięk - Karta dźwiękowa (Zintegrowana)  • Napęd optyczny - DVD+/-RW  • Czytnik kart pamięci - SD Card Reader  • System - Microsoft Windows 10/11 Pro (64 bit)  • Sloty PCIe / M.2  1 x PCIe x16  1 x PCIe x1  1 x M.2 22x80mm  • Złącza - panel przedni  2 x USB-A 3.2 Gen 1  2 x USB-A 2.0  1 x Gniazdo uniwersalne audio  • Złącza - panel tylni  1 x HDMI 1.4  1 x VGA  2 x USB-A 3.2 Gen 1  2 x USB-A 2.0  1 x RJ-45 (LAN)  1 x Wyjście liniowe audio  • Moc zasilacza - 200 W  • Wysokość - 29 cm  • Szerokość - 9.26 cm  • Głębokość - 29.28 cm  • Waga - 4.66 kg  • Bezpieczeństwo  • TPM 2.0  • Slot na linkę zabezpieczenia  • Akcesoria w zestawie  • Klawiatura przewodowa  • Przewód zasilający  • Mysz przewodowa  • Gwarancja - 3 lata gwarancji producenta |  |
| MONITOR | • Przekątna - 27″  • Typ matrycy - IPS  • Powłoka - Anti-Glare  • Rozdzielczość - FullHD  • Rozdzielczość w px - 1920 x 1080 px  • Format - 16:9  • Odświeżanie - 75 Hz  • Liczba wyświetlanych kolorów - 16.7 mln  • Pokrycie barw - 72% (NTSC)  • Kontrast statyczny - 3000:1  • Czas reakcji matrycy - 4 ms  • Kąty widzenia (Poziom) - 178˚  • Kąty widzenia (Pion) - 178˚  • Jasność - 250 cd/m2  • Wielkość plamki - 0.3108 mm  • Liczba pikseli na cal - 81 PPI  • Złącza - panel tylni  1 x HDMI  1 x VGA  • Regulacja Pochylenia - Tak  • Certyfikaty  ENERGY STAR  RoHS Compliant  • Pobór mocy praca - 20 W  • Pobór mocy spoczynek - 0.3 W  • Montaż na ścianie - VESA 100 x 100 mm  • Akcesoria w zestawie  Przewód zasilający  Przewód HDMI |  |
| 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. |  |

**Część V Opracowanie wzorów dokumentów elektronicznych**

|  |  |  |
| --- | --- | --- |
| NAZWA | WYMAGANIA | SPECYFIKACJA I PARAMETRY ROZWIĄZANIA |
| Wzory dokumentów elektronicznych CRWD | Przedmiotem zamówienia jest opracowanie 10 wzorów dokumentów elektronicznych,  gotowych do opublikowania w Centralnym Repozytorium Wzorów Dokumentów  Elektronicznych, o których mowa w art. 19b, ust. 1 Ustawy o informatyzacji działalności  podmiotów realizujących zadania publiczne (Dz.U.2021 poz. 2070 ze zm.), a także formularzy z  aplikacjami przeznaczonych do świadczenia przez Urząd Gminy Trzebiel e-Usług na platformie e-PUAP. Każda usługa musi umożliwiać udzielenie odpowiedzi Klientowi, poprzez wykorzystanie pisma ogólnego opartego o wzór dokumentu elektronicznego znajdujący się w CRWDE.  Do zadań Wykonawcy należy również udzielenie pomocy podczas instalacji usługi na platformie ePUAP i przygotowanie 10 opisów usług przeznaczonych do zgłoszenia, do publikacji w katalogu usług na platformie ePUAP. |  |

*…………..………………………… ………………………………………….*

*(miejscowość i data) (podpis Wykonawcy)*