Obraz zawierający tekst

Opis wygenerowany automatycznie

Załącznik nr 9

**OPIS PRZEDMIOTU ZAMÓWIENIA**

W ramach zamówienia Zamawiający wymaga dostarczenia:

1. Switch typ 1

Producent: …………………………………….

Model: …………………………………….

Ilość: 2 szt.

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowany parametr** |
| **Porty** | • min. 48 x 10/100/1000 Mb/s Ethernet  • min. 4 x SFP  • Automatyczne wykrywanie oraz automatyczna negocjacja parametrów połączenia |  |
| **Obsługiwane standardy** | • IEEE 802.3 10BASE-T  • IEEE 802.3u 100BASE-TX  • IEEE 802.3ab 1000BASE-T  • IEEE 802.3z 1000BASE-X  • IEEE 802.3x |  |
| **Obsługiwane protokoły** | • IEEE 802.1D  • IEEE 802.1W  • IEEE 802.1S  • Auto-voice VLAN  • SNMP v1, v2c, v3  • RFC 1213 MIB II  • RFC 1643 Ethernet Interface MIB  • RFC1493 Bridge MIB  • Jumbo Frame  • IEEE 802.1Q Tag VLAN  • 128 Static VLANs  • IEEE 802.1p  • DSCP - L3 QoS  • Ograniczanie pasma na wejściu  • IEEE 802.3ad  • DHCP client  • Broadcast storm control  • Port mirroring (many-to-one)  • Port setting  • IGMP snooping v1/v2  • IEEE 802.1x (RAIDUS)  • ACL - MAC, IP  • SNTP  • IEEE 802.1ab LLDP  • HTTP and HTTPS  • Ochrona przed DoS  • Syslog  • Ping & traceroute  • Konfiguracja przez www  • EEE802.3az  • Statyczny routing  • MLD Snooping |  |
| **Parametry wydajnościowe** | • Metoda przesyłania ramek: Store-and-forward  • Przepustowość magistrali: min. 100 Gb/s  • Wielkość bufora: min. 2Mb  • Ilość adresów MAC: min. 16000  • Czas bezawaryjnej pracy przełącznika min. 380 tys. godzin |  |
| **Gwarancja** | Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji. Update firmware wpierany do wyjścia urządzenia z produkcji. |  |

1. Switch typ 2

Producent: …………………………………….

Model: …………………………………….

Ilość: 1 szt.

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowany parametr** |
| **Ilość portów** | Min. 8 x MultiGigabit Ethernet 1/2,5/5/10Gb  Min. 4 x SFP+ |  |
| **Tablica MAC** | Min. 16K |  |
| **Przepustowość** | Min. 320 Gb/s |  |
| **Obsługiwane funkcje i protokoły** | • IEEE 802.3az Energy Efficient Ethernet  • Przekazywanie ramek: Store-and-forward  • IEEE 802.1Q  • Voice VLAN  • DoS attacks prevention  • IEEE 802.3ad - LAGs  • IEEE 802.3x  • IGMP Snooping (v1, v2 and v3)  • DHCP Client  • DiffServ QoS  • Interfejs www do zarządzania |  |
| **VLAN** | Min. ilość obsługiwanych VLAN 64 |  |
| **Ilość grup multicast IGMP** | min.: 128 |  |
| **Zasilacz** | Tak |  |
| **Gwarancja** | Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji. Update firmware wpierany do wyjścia urządzenia z produkcji. |  |

1. Oprogramowanie do backupu

Producent: …………………………………….

Model: …………………………………….

Ilość: 1 szt.

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowany parametr** |
| **Opis** | Możliwośc backupu 35 komputerów, 5 serwerów oraz 1 hosta wirtualizacji  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 XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology  Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, 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  Oprogramowanie musi być zainstalowane i wstępnie skonfigurowana na dostarczonym urządzeniu NAS.  Wsparcie techniczne producenta min. 3 lata. |  |

1. Serwer

Producent: …………………………………….

Model: …………………………………….

Ilość: 1 szt.

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowany parametr** |
| **Obudowa** | Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 3.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.  Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |  |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |  |
| **Procesor** | Zainstalowane dwa procesory 8-rdzeniowy, min. 2.1 GHz (Turbo Speed min. 3.2 GHz), klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 18000 w teście Average CPU Mark dostępnym na stronie <https://www.cpubenchmark.net/>. |  |
| **RAM** | 128GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 768GB pamięci RAM. |  |
| **Zabezpieczenia pamięci RAM** | Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling |  |
| **Gniazda PCI** | - minimum trzy sloty PCIe |  |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ |  |
| **Dyski twarde** | Możliwość instalacji dysków SAS, SATA, SSD  Zainstalowane:   * 2 dyski SSD SATA o pojemności min. 960GB każdy, 6Gb, Hot-Plug, * 3 dyski NLSAS o pojemności min. 2TB każdy, 12Gbps, Hot-Plug   Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |  |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy posiadający min. 4GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |  |
| **System operacyjny/System wirtualizacji** | Windows Serwer 2022 Standard lub równoważny system operacyjny do serwera administracji i monitorowania oraz zarządzania środowiskiem zwirtualizowanym (wymagana jest zgodność z oprogramowaniem już wykorzystywanym u Zamawiającego, m.in. w zakresie współpracy z Active Directory). System do serwerów powinien mieć możliwość postawienia 2 maszyn wirtualnych.  Równoważność  Zamawiający uzna, że zaoferowane rozwiązanie posiada równoważne cechy z przedmiotem zamówienia jeżeli będzie ono zawierało funkcjonalności co najmniej tożsame lub lepsze od określonych w niniejszym opisie przedmiotu zamówienia w zakresie posiadanej funkcjonalności i będzie kompatybilne w 100% z oprogramowaniem posiadanym przez Zamawiającego, o którym mowa w niniejszym opisie przedmiotu zamówienia. W przypadku zaproponowania wersji równoważnej Wykonawca zobowiązany jest załączyć do oferty opis i dane techniczne zaproponowanego rozwiązania umożliwiające porównanie go z wszystkimi parametrami wymaganymi niniejszym opisem przedmiotu zamówienia w tym zgodność posiadanego oprogramowania z zaproponowanym rozwiązaniem. Dodatkowo Zamawiający zastrzega sobie prawo do zweryfikowania funkcjonalności, wydajności i kompatybilności zaoferowanego rozwiązania równoważnego poprzez analizę jego możliwości. W przypadku skorzystania przez Zamawiającego z ww. uprawnienia wykonawca jest zobowiązany w terminie 5 dni od dnia otrzymania od Zamawiającego wezwania do dostarczenia testowej wersji zaproponowanego rozwiązania dostarczyć to rozwiązanie do siedziby Zamawiającego  Dodatkowo wykonawca dostarczy 50 szt. licencji dostępowych na urządzenie dla serwerowego systemu operacyjnego |  |
| **Wbudowane porty** | Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej,  Tylne: min. 1x VGA, min. 1x USB |  |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |  |
| **Zasilacze** | Redundantne, Hot-Plug min. 700W każdy |  |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem |  |
| **Diagnostyka** | Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |  |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; * możliwość podmontowania zdalnych wirtualnych napędów; * wirtualną konsolę z dostępem do myszy, klawiatury; * wsparcie dla IPv6; * wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z Active Directory; * możliwość obsługi przez dwóch administratorów jednocześnie; * wsparcie dla dynamic DNS; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. * możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera * możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera |  |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.  Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022. |  |
| **Warunki gwarancji** | 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.  Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Możliwość rozszerzenia gwarancji przez producenta do 7 lat. |  |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |

1. UTM

Producent: …………………………………….

Model: …………………………………….

Ilość: 1 szt.

|  |  |  |
| --- | --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** | **Oferowany parametr** |
| **Urządzenie** | 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 dawać możliwość 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 etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator musi 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 bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 6. Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).   INTRUSION PREVENTION SYSTEM (IPS)   1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator musi 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. 6. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 7. Administrator urządzenia 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 mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.   KSZTAŁTOWANIE PASMA (Traffic Shapping)   1. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 3. Rozwiązanie 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. Rozwiązanie ma zezwalać na 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 odrzucenia.   OCHRONA ANTYSPAM   1. Producent ma udostępniać 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. heurystyczny skaner. 3. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.   WIRTUALNE SIECI PRYWANTE (VPN)   1. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Odpowiednio kanały VPN można budować w oparciu o:    1. PPTP VPN,    2. IPSec VPN,    3. SSL VPN. 3. SSL VPN musi działać w trybach Tunel i Portal. 4. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 6. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 7. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.   FILTR DOSTĘPU DO STRON WWW   1. Urządzenie ma posiadać wbudowany filtr URL. 2. Administrator musi mieć możliwość dodawania własnych kategorii URL. 3. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 4. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 5. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: 6. blokowanie dostępu do adresu URL, 7. zezwolenie na dostęp do adresu URL, 8. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 9. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 10. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 11. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 12. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 13. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.   UWIERZYTELNIANIE   1. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:    1. lokalną bazę użytkowników (wewnętrzny LDAP),    2. zewnętrzną bazę użytkowników (zewnętrzny LDAP),    3. usługę katalogową Microsoft Active Directory. 2. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 3. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:    1. SSL,    2. Radius,    3. Kerberos. 4. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 5. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.   ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)   1. Urządzenie ma posiadać 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 łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 5. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 6. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 7. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 8. Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.   POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA   1. Urządzenie musi posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 2. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 3. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 4. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS. 5. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 6. Urządzenie musi posiadać usługę DNS Proxy.   ADMINISTRACJA URZĄDZENIEM   1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 3. Komunikacja może odbywać się na porcie innym niż https (443 TCP). 4. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 6. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 7. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 8. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 9. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 10. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. 11. Urządzenie musi posiadać funkcjonalność anonimizacji logów. 12. Urządzenie ma mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów.   RAPORTOWANIE   1. Urządzenie musi 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 musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 4. System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów. 5. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 6. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 7. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy.   PARAMETRY SPRZĘTOWE   1. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać z wbudowanej pamięci flash. 2. Liczba portów Ethernet 10/100/1000Mbps – min. 8. 3. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. 4. Przepustowość Firewall – min. 4 Gbps. 5. Przepustowość Firewall wraz z włączonym systemem IPS – min. 2,4 Gbps. 6. Przepustowość filtrowania Antywirusowego – min. 495 Mbps. 7. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 600 Mbps. 8. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 100. 9. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20. 10. Obsługa min. VLAN 64. 11. Liczba równoczesnych sesji - min. 300 000 i nie mniej niż 18 000 nowych sesji/sekundę. 12. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 13. Urządzenie jest nielimitowane na użytkowników. 14. Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci. Powyższy moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu. 15. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 65 kategorii tematycznych stron internetowy. W ramach filtra URL sklasyfikowanych jest co najmniej 100 milionów stron internetowych. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu. |  |
| **Gwarancja** | 1. Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres 60 miesięcy.  2. Wymaga się, aby dostawa obejmowała również 60-miesięczną gwarancję producentów na dostarczone urządzenie. |  |

1. Urządzenie do archiwizacji

Producent: …………………………………….

Model: …………………………………….

Ilość: 1 szt.

|  |  |  |
| --- | --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** | **Oferowany parametr** |
| **Obudowa** | Rack, max. 2U, szyny montażowe w zestawie |  |
| **Procesor** | Min. czterordzeniowy |  |
| **Pamięć RAM** | min. 8 GB RAM  Maksymalna pojemność pamięci min. 32GB |  |
| **Ilość kieszeni na dyski** | Min. 8 szt. |  |
| **Obsługiwane dyski** | 3.5" SATA HDD  2.5" SATA HDD  2.5" SATA SSD |  |
| **Interfejsy sieciowe** | Min. 4 x 1 Gigabit Ethernet (1G/100M/10M) lub  2 x 2,5 Gigabit Ethernet (2,5G/1G/100M/10M) |  |
| **Wymieniany dysków podczas pracy** | Tak |  |
| **Dyski** | Zatoki na min. 8 dysków SATA III  Zainstalowane min. 8 dysków SATAIII:  • o pojemności min. 6TB każdy,  • pamięć podręczna: min. 256MB,  • prędkość obrotowa: min. 5600RPM,  • MTBF: min. 1 000 000 h, |  |
| **Porty** | Min. 2x USB 3.0 |  |
| **Obsługa RAID** | Basic  JBOD  RAID 0  RAID 1  RAID 5  RAID 6  RAID 10 |  |
| **Zasilanie** | max. 350W |  |
| **Gwarancja** | Producenta min. 60 miesięcy |  |

1. Komputer z monitorem

Producent: …………………………………….

Model: …………………………………….

Ilość: 4 szt.

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane parametry techniczne komputerów** | **Oferowany parametr** |
| **Typ** | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |  |
| **Zastosowanie** | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. |  |
| **Wydajność obliczeniowa** | Procesor dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 12 000 punktów według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> |  |
| **Pamięć RAM** | 16GB DDR4 2666MHz. Możliwość rozbudowy do min 64GB. Jeden slot DIMM wolny. |  |
| **Pamięć masowa** | Dysk M.2 SSD 256GB PCIe NVMe  Obudowa musi umożliwać montaż dodatkowego dysku 2.5” lub 3.5” |  |
| **Wydajność grafiki** | Zintegrowana z procesorem |  |
| **Wyposażenie multimedialne** | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. port audio line out. |  |
| **Obudowa** | Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 700 mm.  Zasilacz o mocy min. 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych). Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany ]system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. |  |
| **Bezpieczeństwo** | Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej.  Procedura POST traktowana jest jako oddzielna funkcjonalność. |  |
| **BIOS** | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio.  Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie.  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo.  Możliwość dokonywania backup’u BIOS wraz z ustawieniami na dysku wewnętrznym.  Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS. |  |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |  |
| **Zgodność z systemami operacyjnymi i standardami** | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi |  |
| **System operacyjny** | Zainstalowany system operacyjny musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  - możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;  - Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu  - Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW;  - Internetowa aktualizacja zapewniona w języku polskim;  - Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;  - Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;  - Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi)  - Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;  - Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta.  - Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;  - Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.  - Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.  - Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych.  - Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.  - Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.  - Wbudowany system pomocy w języku polskim;  - Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);  - Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;  - Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;  - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;  - Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;  - System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;  - Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;  - Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;  - Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji za logowanego użytkownika celem rozwiązania problemu z komputerem;  - Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami.  Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową;  - Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;  - Graficzne środowisko instalacji i konfiguracji;  - Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;  - Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.  - Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;  - Możliwość przywracania plików systemowych;  - System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.)  - Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).  - klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. |  |
| **Certyfikaty i standardy** | Deklaracja zgodności CE (załączyć do oferty)  Urządzenia muszą być wyprodukowane szgodnie z normą PN-EN ISO 50001 oraz ISO 9001 – certyfikaty załączyć do oferty  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram.  Certyfikat EPEAT 2018 min. Silver dla Polski |  |
| Wymagania dodatkowe | Wbudowane porty: 2x Display Port 1.4, port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu, port audio-out na tylnym panelu obudowy, 1xRJ-45, 8 portów USB wyprowadzonych na zewnątrz obudowy, w tym min 2 porty USB na przednim panelu obudowy i min. 4 porty USB 3.2 gen. 1  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej.  Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługęWoL (funkcja włączana przez użytkownika),  Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen.3, 1 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 2 x SATA w tym min. 1 szt SATA 3.0.  Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej.  Klawiatura bezprzewodowa USB w układzie polski programisty  Mysz optyczna bezprzewodowa USB z dwoma przyciskami oraz rolką (scroll)  Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu. |  |
| **Ergonomia** | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy jałowej (IDLE) wynosząca maksymalnie 26 dB (załączyć raport akredytowanej jednostki badawczej lub oświadczenie producenta). |  |
| **Monitor** | |  |  | | --- | --- | | **Typ ekranu** | Ekran ciekłokrystaliczny z aktywną matrycą IPS min.23,8” | | **Rozmiar plamki (maksymalnie)** | 0,275 mm | | **Jasność** | Min. 250 cd/m2 | | **Kontrast** | Min. 1000: 1 | | **Kąty widzenia (pion/poziom)** | Min. 178/178 stopni | | **Czas reakcji matrycy**  **(maksymalnie)** | 8ms | | **Rozdzielczość maksymalna** | 1920 x 1080 przy 60Hz | | **Zakres regulacji** | Pochylenie w zakresie min. 25 stopni  Regulacja wysokości w zakresie min. 150 mm  Obrót monitora o 45 stopni w prawo i w lewo  PIVOT | | **Powłoka powierzchni ekranu** | Antyodblaskowa | | **Podświetlenie** | System podświetlenia LED | | **Bezpieczeństwo** | Monitor musi być wyposażony w slot na linkę zabezpieczającą | | **Złącza** | 1x 15-stykowe złącze D-Sub,  1x HDMI (v1.4),  1x złącze DisplayPort (v1.2)  Min. 4 Porty USB 3.2  Złące linki zabezpieczającej | | **Gwarancja** | 5-letnia gwarancja producenta świadczona na miejscu u klienta, możliwość zgłaszania awarii przez ogólnopolską linię telefoniczną oraz stronę internetową producenta  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta– dokumenty potwierdzające załączyć do oferty.  Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. | | **Inne** | Podstawa odłączana bez użycia narzędzi  Możliwość podłączenia do obudowy dedykowanych głośników producenta monitora lub głośniki wbudowane | |  |
| **Wsparcie techniczne producenta** | Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego). |  |
| **Warunki gwarancji** | 5-letnia gwarancja producenta świadczona na miejscu u klienta  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.  Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.  Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) |  |
| **Oprogramowanie dodatkowe** | Pakiet oprogramowania biurowego  Pakiet musi zawierać:  • edytor tekstów,  • arkusz kalkulacyjny,  • narzędzie do przygotowania i prowadzenia prezentacji,  • narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami  i zadaniami).  Wymagana pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej  pomocy w języku polskim. Pakiet powinien mieć system aktualizacji darmowych poprawek  bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim.  Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek  bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu  biurowego świadczonej w języku polskim w dni robocze w godzinach od 8 do 17 – cena połączenia nie większa niż cena połączenia lokalnego.  Wymagany publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia  technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 5 lat od daty zakupu.  Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo  widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0).  Wymagane dostarczenie nieograniczonej czasowo licencji odpowiedniej dla jednostki samorządu  terytorialnego.  Pakiet biurowy musi spełniać niżej wskazane wymagania poprzez wbudowane mechanizmy, bez  użycia dodatkowych aplikacji.  Wymagania ogólne:  • możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową - użytkownik  raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie  rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego  monitowania go o ponowne uwierzytelnienie się,  • oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w  ustalonym formacie, który spełnia następujące warunki:  o posiada kompletny i publicznie dostępny opis formatu,  o ma zdefiniowany układ informacji w postaci XML (standard uniwersalnego formatu  tekstowego służący do zapisu danych w formie elektronicznej),  o umożliwia wykorzystanie schematów XML,  o wspiera w swojej specyfikacji podpis elektroniczny,  • oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb  instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do  właściwych odbiorców,  • w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające  automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język  makropoleceń, język skryptowy),  • do aplikacji musi być dostępna pełna dokumentacja w języku polskim.  Edytor tekstów musi umożliwiać:  • 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.  • Wstawianie oraz formatowanie tabel.  • Wstawianie oraz formatowanie obiektów graficznych.  • Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).  • Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.  • Automatyczne tworzenie spisów treści.  • Formatowanie nagłówków i stopek stron.  • Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.  • Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.  • Określenie układu strony (pionowa/pozioma).  • Wydruk dokumentów.  • Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza  kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.  • Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  • Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi  umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy  pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.  Arkusz kalkulacyjny musi umożliwiać:  • Tworzenie raportów tabelarycznych.  • Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.  • Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły  przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na  danych finansowych i na miarach czasu.  • Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych  zgodne z ODBC, pliki tekstowe, pliki XML, webservice).  • Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych.  • Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie  problemów optymalizacyjnych.  • Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz  wykresów bazujących na danych z tabeli przestawnych.  • Wyszukiwanie i zamianę danych.  • Wykonywanie analiz danych przy użyciu formatowania warunkowego.  • Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.  • Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.  • Formatowanie czasu, daty i wartości finansowych z polskim formatem.  • Zapis wielu arkuszy kalkulacyjnych w jednym pliku.  • Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:  • Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu  projektora multimedialnego.  • Drukowanie w formacie umożliwiającym robienie notatek.  • Zapisanie jako prezentacja tylko do odczytu.  • Nagrywanie narracji i dołączanie jej do prezentacji.  • Opatrywanie slajdów notatkami dla prezentera.  • Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i  wideo.  • Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.  • Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu  kalkulacyjnym.  • Możliwość tworzenia animacji obiektów i całych slajdów.  • Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze  lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.  Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i  zadaniami) musi umożliwiać:  • Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.  • Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem  efektywnej kompresji danych.  • Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i  bezpiecznych nadawców.  • Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.  • Automatyczne grupowanie poczty o tym samym tytule.  • Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych  katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.  • Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla  nadawcy i adresatów.  • Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.  • Zarządzanie kalendarzem.  • Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień  użytkowników.  • Przeglądanie kalendarza innych użytkowników.  • Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne  wprowadzenie spotkania w ich kalendarzach.  • Zarządzanie listą zadań.  • Zlecanie zadań innym użytkownikom.  • Zarządzanie listą kontaktów.  • Udostępnianie listy kontaktów innym użytkownikom.  • Przeglądanie listy kontaktów innych użytkowników.  • Możliwość przesyłania kontaktów innym użytkowników. |  |

1. Usługa katalogowa

Producent: …………………………………….

Model: …………………………………….

Ilość: 1 szt.

|  |  |  |
| --- | --- | --- |
| **Nazwa** | **Wymagane parametry techniczne** | **Oferowane parametry techniczne** |
| **Usługa katalogowa** | Na wykonanie usługi, składają się elementy:  1. Instalacja, aktualizacja i konfiguracja systemów operacyjnych na serwerach wirtualnych obejmujących usługę. Musi zostać wykonana instalacja i konfiguracja kontrolerów domeny oraz usług DHCP, file serwer  2. Utworzenie domeny i konfiguracji lokalnego serwera DNS z odzwierciedleniem topologii sieci urzędu.  3. Utworzenie i konfiguracja serwerów usług katalogowych obejmujące:  a. przeniesienie topologii sieci i struktury organizacyjnej urzędu w usługach katalogowych (grupy, VLAN-y);  b. zdefiniowanie kont użytkowników;  c. zaimplementowanie struktury katalogowej: komputery i użytkownicy;  d. utworzenie i konfiguracja zasobów dyskowych dla profili użytkowników oraz pracy w obrębie grup;  e. wdrożenie mechanizmów zarządzania z poziomu usług katalogowych kluczowymi aplikacjami w sieci urzędu;  f. określenie polityk bezpieczeństwa na serwerach usług katalogowych (w domenie).  Opracowanie struktury Grup Zabezpieczeń i ustalenie praw dostępu do zasobów sieciowych;  g. wdrożenie opracowanej struktury Grup Zabezpieczeń (założenie grup i przypisanie im odpowiednich praw dostępu);  h. założenie kont użytkowników wraz z przypisaniem kont do odpowiednich grup zabezpieczeń;  i. przygotowanie procedury podłączania stacji roboczych do domeny usługi katalogowej;  j. przypięcie do domeny wszystkich stacji wskazanych przez zamawiającego;  k. opracowanie i wdrożenie skryptów logowania użytkowników, uwzględniających ustalone uprawnienia do zasobów sieciowych w tym implementacja polityki haseł i czasu pracy;  l. konfiguracja obiektów Zasad Grup dotyczących automatycznej aktualizacji stacji roboczych;  m. opracowanie i wdrożenie Zasad Grup, dla automatyzacji konfiguracji stacji roboczych oraz profili użytkowników;  n. stworzenie polityk dostępowych w oparciu o grupy użytkowników grupy katalogowej. |  |

1. Szkolenie typ 1

Producent: …………………………………….

Model: …………………………………….

Ilość: 1 szt.

|  |  |  |
| --- | --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** | **Oferowany parametr** |
| **Opis** | Autoryzowane szkolenie producenta urządzenia UTM min. 48 godzin obejmujące następujące zagadnienia:  1. Rozpoczęcie pracy z urządzeniem  2. Zbieranie logów i monitorowanie  3. Obiekty  4. Konfiguracja sieci  5. Translacja adresów sieciowych (NAT)  6. Translacja połączeń wychodzących (maskarada)  7. Translacja połączeń przychodzących (przekierowanie)  8. Translacja dwukierunkowa (jeden do jeden)  9. Filtrowanie ruchu sieciowego (Firewall)  10. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection)  11. Ochrona aplikacji  12. Użytkownicy i uwierzytelnianie  13. Konfiguracja usługi katalogowej  14. Wirtualne sieci prywatne (VPN)  15. SSL VPN  16. Szczegółowe omówienie działania modułu IPS od Stormshield  17. Infrastruktura klucza publicznego  18. SSL Proxy  19. GRE i GRETAP  20. Transparentne uwierzytelnianie użytkowników  21. Wysoka dostępność (HA) |  |
| **Realizacja** | Imienny certyfikat ukończenia szkolenia  Możliwość dostawy vouchera szkoleniowego z terminem ważności min. 1 rok. |  |

1. Szkolenie typ 2

Producent: …………………………………….

Model: …………………………………….

Ilość: 1 szt.

|  |  |  |
| --- | --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** | **Oferowany parametr** |
| **Opis** | Autoryzowane szkolenie producenta serwerowego systemu operacyjnego min. 40 godzin obejmujące następujące zagadnienia:   * Omówienie funkcji administracyjnych * Usługi dotyczące tożsamości * Usługi dotyczące infrastruktury sieci * Zarządzanie serwerami plików i pamięcią masową * Oprogramowanie do wirtualizacji i kontenery * Funkcje wysokiej dostępności * Usuwanie skutków awarii * Bezpieczeństwo * Technologia RDS * Zdalny dostęp i usługi WWW * Monitorowanie serwera i wydajności * Aktualizacje i migracje |  |
| **Realizacja** | Imienny certyfikat ukończenia szkolenia  Możliwość dostawy vouchera szkoleniowego z terminem ważności min. 1 rok. |  |