# **Szczegółowy opis przedmiotu zamówienia**

# **- Dostawa sprzętu i oprogramowania wraz z konfiguracją i szkoleniem w ramach: Projekt grantowy e-Tuchów w ramach projektu „Cyfrowa gmina”**

Dostawa sprzętu informatycznego (Serwerów, Przełączników, Macierzy dyskowej, UTM-a, UPS-a, Biblioteki taśmowej do archiwizacji danych), oprogramowania (zestawu licencji systemów operacyjnych, zestawu licencji oprogramowania do wirtualizacji, zestawu licencji oprogramowania do kopii zapasowych, zestawu licencji oprogramowania biurowego, zestawu licencji do zarządzania infrastrukturą) wraz z usługą wdrożeniową oraz szkoleniami dla pracowników urzędu w zakresie obsługi/administrowania zakupionego sprzętu i oprogramowania.

## Tabelaryczne zestawienie przedmiotu zamówienia:

# **Serwer – wymagania minimalne – 2 sztuki**

|  |  |  |
| --- | --- | --- |
|  |  | Parametr wymagany |
| 1 | Obudowa | RACK 19 cali, max. 1U, wraz z wszystkimi elementami niezbędnymi do zamontowania serwera w szafie serwerowej posiadanej przez Zamawiającego. Szyny muszą umożliwiać wysuwanie serwera w celach serwisowych |
| 2 | Procesor | Architektura x86 lub x64, TDP dla procesora – 155W. Minimalna ilość rdzeni dla procesora – 16, taktowanie zegara minimum 3.0GHz Osiągające wynik w testach wydajności SPECrate2017\_int\_base minimum 240 pkt. w konfiguracji dwuprocesorowej oferowanego modelu serwera. |
| 3 | Liczba procesorów zainstalowanych | dwa |
| 4 | Płyta główna | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD EPYC lub Intel Xeon) |
| 5 | Pamięć RAM | Zainstalowane 256GB pamięci RAM Minimum 16 slotów na pamięć dla serwera 2 procesorowego, wsparcie pamięci typu RDIMM. Pamięć o częstotliwości minimum 2933MHz. |
| 6 | Zabezpieczenie pamięci RAM | ECC, SDDC |
| 7 | Dyski | 2 dyski o pojemności minimum 240GB, hot swap SSD działające w RAID-1 |
| 8 | Gniazda rozszerzeń | Minimum 3 x PCIe 4.0 |
| 9 | Interfejsy sieciowe | 2 porty 10Gb SFP+, 2 porty RJ-45 o przepustowości 1GbE, 1 port RJ45 dedykowany dla karty zarządzającej. |
| 10 | Dodatkowe karty | Dodatkowo zainstalowane:  Min. 1 karta FC 16Gbps dwuportowa |
| 11 | Diagnostyka | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID. |
| 12 | Zarządzanie | * Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania * Monitoring statusu i zdrowia systemu * Logowanie zdarzeń * Umożliwiający Update systemowego firmware * Umożliwiający zdalną konfigurację serwera * Monitoring i możliwość ograniczenia poboru prądu * Zdalne włączanie/wyłączanie/restart * Przekierowanie konsoli szeregowej przez IPMI * Możliwość przejęcia zdalnego ekranu 1920x1200, 60 Hz,16 bpp * Zdalny dostęp do serwera * Możliwość zdalnej instalacji systemu operacyjnego * Alerty Syslog * Przekierowanie konsoli szeregowej przez SSH * Wyświetlanie danych aktualnych i historycznych dla użycia energii  i temperatury serwera * Możliwość mapowania obrazów ISO z lokalnego dysku operatora * Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS * Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę * Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API * Możliwość przełączenia frontowego portu USB w taki sposób, aby ten port służył serwisantowi (był podłączony do karty zarządzającej) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. |
| 13 | Grafika | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. Port VGA. |
| 14 | Zasilacze | 2 zasilacze Hot-Plug o mocy minimalnie 750W każdy dostosowane do dostarczanych procesorów. |
| 15 | Porty dodatkowe | Minimum:  z przodu obudowy: 1x USB 3.0, z tyłu obudowy: 2x USB 3.0, 1x VGA. |
| 16 | Systemy operacyjne | Kompatybilność z systemami : Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi. |
| 17 | Bezpieczeństwo | Hasło włączania, hasło administratora, moduł TPM 2.0. |
| 18 | Gwarancja | Minimum 24 miesięcy on-site NBD. |
| 19 | Pochodzenie | Dostarczony sprzęt musi być fabrycznie nowy, musi pochodzić  z oficjalnego kanału sprzedaży producenta. Wymagane oświadczenie producenta, że oferowany do przetargu sprzęt spełnia ten wymóg. Elementy, z których zbudowane są serwery musza być produktami producenta tych serwerów lub być przez niego certyfikowane (wymagane oświadczenie producenta dołączone do oferty) oraz musza być objęte gwarancja producenta, wymagane oświadczenie producenta. Wykonawca zobowiązany jest dostarczyć wraz z ofertą, szczegółową specyfikację techniczną oferowanego sprzętu. Serwer nie może być wyprodukowany później niż 6 miesięcy przed dostarczeniem. |
| 20 | Dodatkowe | Serwery muszą być dostarczone z kompletem kabli, szyn i innych akcesoriów umożliwiających bezproblemowe podłączenie w szafie rack.  - Urządzenie wyposażone w 2 szt. 2 metrowych kabli DAC SFP+ 10G  w celu podłączenia do przełącznika sieciowego, kabel musi być kompatybilny z serwerem oraz dostarczanym przełącznikiem. |

# **Przełącznik korowy – wymagania minimalne – 2 sztuki**

|  |  |  |
| --- | --- | --- |
|  |  | Parametr wymagany |
| 1 | Obudowa | Obudowa do montażu w szafie RACK 19” – 1U wraz z zestawem montażowym |
| 2 | Porty | - 24 x 1G/10G SFP+, 2x40GB QSFP+  Musi umożliwiać zestawienie stosu portami/magistralami minimum, 10GbE Full Duplex 10GbE. |
| 3 | Wydajność | - Przepustowość przełącznika minimum 640Gbps.  - Wydajność przełączania minimum 480Mpps.  - Obsługa minimum 96,000 adresów MAC.  - Bufor pakietów minimum 9MB |
| 4 | Zasilanie | Redundantne 2x 230V AC. |
| 5 | Funkcje i protokoły – wymagania minimalne: | - Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree  - Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9000 bajtów  - Urządzenie musi obsługiwać protokoły SNMPv1/2c, TACACS+, RADIUS, SSH  - Autoryzacja użytkowników w oparciu o IEEE 802.1X zmożliwością dynamicznego przypisania użytkownika do określonej sieci VLAN  - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC  - Możliwość implementacji listy kontroli dostępu (ACL)  - Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow lub równoważne)  - Obsługa multicastów z wykorzystaniem protokołów   * + IGMP   + IGMP Snooping   + PIM   - Routing statyczny dla IPv4 oraz IPv6  - Protokoły routingu dynamicznego: RIP, OSPFv2, BGP  - Musi obsługiwać standardy IEEE:   * 802.1D * 802.1X   Musi obsługiwać poniższe standardy w zakresie protokołu IPv4: IPv4, ARP |
| 6 | Zarządzanie i monitorowanie: | - Posiadający tekstowy interfejs zarządzania z podpowiedziami kontekstowymi  - Możliwość uzyskania dostępu do urządzenia przez protokoły SNMPv3, SSH,  - Umożliwiający bezpośredni dostęp do interfejsu zarządzania z wykorzystaniem dedykowanego portu szeregowego lub jego emulacji  - Obsługujący wysyłanie powiadomień o zdarzeniach z użyciem SNMP |
| 7 | Gwarancja | Oferowane urządzenie musi być objęte co najmniej 2-letnim wsparciem oraz gwarancją w dni robocze. |

# **Przełącznik do punktów dystrybucyjnych – 3 sztuki**

|  |  |  |
| --- | --- | --- |
|  |  | Parametr wymagany |
| 1 | Obudowa | Obudowa do montażu w szafie RACK 19” – 1U wraz z zestawem montażowym |
| 2 | Porty | - 24 x 100/1000Baset-t RJ45 , 4x10G SFP+  Musi umożliwiać zestawienie stosu portami/magistralami minimum, 10GbE Full Duplex 10GbE |
| 3 | Wydajność | - Przepustowość przełącznika minimum 120Gbps.  - Wydajność przełączania minimum 90Mpps.  - Obsługa minimum 16,000 adresów MAC.  - Bufor pakietów minimum 1,5MB |
| 4 | Zasilanie | Redundantne 2 x Zasilanie 230V AC. |
| 5 | Funkcje i protokoły – wymagania minimalne: | Funkcje i protokoły – wymagania minimalne:  - Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree  - Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9000 bajtów  - Urządzenie musi obsługiwać protokoły SNMP, RADIUS, SSH, NTP  - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC  - Możliwość implementacji listy kontroli dostępu (ACL) na poziomie co najmniej warstwy 2  - Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow lub równoważne)  - Obsługa multicastów z wykorzystaniem protokołów   * + IGMP   - Możliwość uruchomienia serwera DHCP dla IPv4 oraz IPv6  - Routing statyczny dla IPv4 oraz IPv6  - Musi obsługiwać standardy IEEE:   * 802.1D   Musi obsługiwać poniższe standardy w zakresie protokołu IPv4: IPv4, ARP |
| 6 | Zarządzanie i monitorowanie: | - Posiadający tekstowy interfejs zarządzania z podpowiedziami kontekstowymi  - Możliwość uzyskania dostępu do urządzenia przez protokoły SNMP, SSH,  - Umożliwiający bezpośredni dostęp do interfejsu zarządzania z wykorzystaniem dedykowanego portu szeregowego lub jego emulacji  - Obsługujący wysyłanie powiadomień o zdarzeniach z użyciem SNMP (trap)  - Umożliwiający przesyłanie dzienników zdarzeń z wykorzystaniem protokołu SYSLOG  - Obsługujący synchronizację czasu systemowego z użyciem protokołu NTP |
| 7 | Gwarancja | Oferowane urządzenie musi być objęte co najmniej 2-letnim wsparciem oraz gwarancją w dni robocze. |

# **Macierz dyskowa – wymagania minimalne – 1 sztuka**

|  |  |  |
| --- | --- | --- |
|  |  | Parametr wymagany |
| 1 | Obudowa | * Możliwość zainstalowania w standardowej szafie RACK 19”. * Urządzenie musi wykorzystywać półki dyskowe wysokiej gęstości upakowania - co najmniej 24 dyski na 2U wysokości dla dysków 2,5 cala oraz półki dyskowe zawierające co najmniej 12 dysków 3,5 cala na wysokości 2U. * Urządzenie musi wykorzystywać półki dyskowe wysokiej gęstości umożliwiające upakowanie co najmniej 90 dysków na maksymalnej wysokości 5U. |
| 2 | Zarządzanie | * Urządzenie musi umożliwiać zarządzanie za pomocą interfejsu Ethernet. * Możliwość zarządzania całością dostępnych zasobów dyskowych  z jednej konsoli administracyjnej. * Funkcjonalność bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje. * Interfejs zarządzający GUI, CLI, oraz zapewnienie możliwości tworzenia skryptów użytkownika. |
| 3 | Ilość portów | Wymagane jest nie mniej niż 2 porty 1Gb Ethernet Base-T oraz 8 portów 16Gb FC wyposażonych we wkładki SFP+ 16Gb. |
| 4 | Obsługa dysków | * Musi obsługiwać dyski SAS: * o prędkościach obrotowych 10000 obr./min. i pojemnościach 1.2TB, 1.8TB, 2.4TB; * o prędkościach obrotowych 7200 obr./min. i pojemnościach 2TB, 4TB, 6TB, 8TB, 10TB, 12TB, 14TB, 16TB; * musi obsługiwać dyski SSD o pojemnościach 800 GB, 1.92 TB , 3.84 TB, 7.68 TB, 15.36 TB, 30.72 TB. * Musi obsługiwać, co najmniej 390 dysków na parę kontrolerów  z zastosowaniem dodatkowych półek. Macierz musi umożliwiać rozbudowę o pojedyncze dyski fizyczne i pojedyncze półki rozszerzeń. * Musi umożliwiać konfigurację, która w jednym rozwiązaniu łączyć będzie półki rozszerzeń na dyski 2,5” z półkami na dyski 3,5”. |
| 5 | Pojemność dyskowa | Macierz dyskowa musi być wyposażona w minimum:  3 dysków SAS o pojemności 1.92TB SSD/Flash 12Gb SAS w RAID6 oraz 10 dysków 2.4 TB 10K 2.5 SAS |
| 6 | Dyski | Macierz musi zapewnić możliwość wymiany uszkodzonych dysków podczas pracy systemu (Hot-Swap). Macierz musi być umożliwiać stworzenie konfiguracji odpornej na awarię pojedynczego dysku oraz odporność na awarię dwóch dysków. Przestrzeń zapasowa powinna być realizowana za pomocą przestrzeni zapasowej rozmieszczonej na wszystkich dyskach w ramach grupy RAID lub w formie dysku nadmiarowego. |
| 7 | Obsługa pamięci Cache | Macierz musi być wyposażona w minimum 32GB pamięci Cache. |
| 8 | Wsparcie dla systemów operacyjnych | Macierz musi wspierać następujące systemy operacyjne i wirtualizatory: MS Windows Server, Vmware vSpere, RedHat Enterprise Linux |
|  |  | **Dodatkowe wymagania i funkcjonalności** |
| 9 | Funkcje niezawodnościowe | * Wszystkie krytyczne komponenty urządzenia takie jak: kontrolery dyskowe, pamięć cache, zasilacze i wentylatory muszą być zdublowane tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. * Komponenty te muszą być wymienialne w trakcie pracy macierzy. * Urządzenie musi cechować brak pojedynczego punktu awarii. * Wsparcie dla zasilania z dwóch niezależnych źródeł prądu poprzez nadmiarowe zasilacze typu Hot-Swap. * Wentylatory typu Hot-Swap. * Wbudowane co najmniej dwa kontrolery RAID. * Urządzenie musi posiadać pamięć typu Flash dla zapisu danych  z pamięci cache na wypadek zaniku zasilania oraz system podtrzymania zasilania pozwalający na zapis danych z cache do pamięci typu Flash. |
| 10 | Funkcjonalności inne | * Musi istnieć funkcjonalność Cache dla procesu odczytu. * Musi istnieć funkcjonalność Mirrored Cache dla procesu zapisu. * Możliwość wyłączenia cache dla poszczególnych wolumenów. * Funkcjonalność separacji przestrzeni dyskowych pomiędzy różnymi podłączonymi hostami. * Funkcjonalność dynamicznego zwiększania i zmniejszania rozmiaru wolumenów. * Funkcjonalność zarządzania ilością operacji wejścia / wyjścia wykonywanych na danym wolumenie – zarządzanie musi być możliwe zarówno poprzez określenie ilości operacji I/O na sekundę jak również przepustowości określonej w MB/s. * Urządzenie musi obsługiwać funkcjonalność ochrony przed skasowaniem lub odmapowaniem od hosta woluminu dyskowego, do którego były przesłane operacje wejścia/wyjścia w określonym przez użytkownika czasie. * Dostępne sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu dla podłączanych systemów operacyjnych (jeżeli jest wymagana licencja, należy dostarczyć licencje na całość oferowanych zasobów). |
| 11 | Obsługa wirtualnych dysków logicznych | * Minimalna ilość wspieranych wirtualnych dysków logicznych (LUN) dla całej (globalnej) puli dyskowej musi wynosić co najmniej 2000. Funkcjonalność LUN Masking i LUN Mapping. |
| 12 | Funkcjonalność thin provisioning | Urządzenie musi obsługiwać funkcjonalność thin provisioning dla wszystkich wolumenów. Musi istnieć możliwość wyłączenia tej funkcjonalności dla wybranych wolumenów. Należy dostarczyć licencję umożliwiającą korzystanie z funkcji thin provisioning na całą oferowaną pojemność urządzenia. |
| 13 | Kopie migawkowe | Urządzenie musi mieć możliwość wykonywania natychmiastowej kopii danych (point-in-time copy). Funkcjonalność ta powinna być realizowana w trybie copy-on-write. Licencja powinna umożliwiać utworzenie co najmniej 60 kopii danych. |
| 14 | Migracja wolumenów logicznych | Urządzenie musi mieć możliwość wykonania migracji wolumenów logicznych pomiędzy różnymi typami dysków wewnątrz macierzy bez zatrzymywania aplikacji korzystającej z tych wolumenów. Wymaga się, aby zasoby źródłowe podlegające migracji oraz zasoby do których są migrowane mogły być zabezpieczone różnymi poziomami RAID  i egzystować na różnych technologicznie dyskach stałych (SAS, SSD, SATA). |
| 16 | Replikacja macierzy | Urządzenie musi posiadać funkcjonalność replikacji danych przy użyciu synchronicznych oraz asynchronicznych transmisji danych przez łącza komunikacyjne IP oraz FC. Macierz musi przechowywać w pełni zsynchronizowaną kopię w odległości do 300km. Przy znacznie większej odległości, do 8000km, replikacje mogą działać asynchronicznie. Oba rodzaje replikacji muszą wspierać program Vmware Site Recovery Manager do odzyskiwania danych po awarii. Jeśli na obsługę powyższej funkcjonalności wymagana jest dodatkowa licencja, jest ona wymagana w tym postępowaniu. |
| 16 | Wirtualizacja zasobów | Macierz musi mieć możliwość wirtualizacji zasobów znajdujących się na innych niż oferowane macierze dyskowe na potrzeby migracji danych. Migracja musi się odbyć w trybie bezprzerwowym. |
| 17 | Wymagania | Macierz musi mieć możliwość dodawania kolejnych półek dyskowych oraz dysków bez przerywania pracy macierzy, dla dowolnej konfiguracji macierzy |
| 18 | Macierz musi mieć możliwość aktualizacji oprogramowania macierzy (firmware) w trybie online. |
| 19 | Macierz musi umożliwiać tworzenie wolumenów o pojemności nie mniejszej niż 250 TB |
| 20 | Do macierzy należy dołączyć przewody zasilające oraz 8 przewodów światłowodowych o długości 2m. |
| 21 | Macierz musi posiadać funkcjonalność optymalizacji wykorzystania dysków SSD/Flash poprzez automatyczną identyfikację najbardziej obciążonych fragmentów wolumenów w zarządzanych zasobach dyskowych oraz ich automatyczną migrację na dyski SSD/Flash. Macierz musi również automatycznie rozpoznawać obciążenie fragmentów wolumenów na dyskach SSD/Flash i automatycznie migrować z dysków SSD/Flash nieobciążone fragmenty wolumenów. Macierz musi posiadać możliwość wykorzystania mechanizmu optymalizacji umiejscowienia danych pomiędzy przynajmniej 3 rodzajami dysków – SSD/Flash, Enterprise (SAS 10k) oraz NL-SAS/SATA, jak również przy wykorzystaniu dwóch dowolnych z wyżej wymienionych typów. Opisany powyżej proces optymalizacji musi posiadać funkcję włączenia/wyłączenia na poziomie pojedynczego wolumenu. Jeśli na obsługę powyższej funkcjonalności wymagana jest dodatkowa licencja, jest ona wymagana w tym postępowaniu. |
| 22 | Pozostałe wymagania | Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu. |
| 23 | Oferowane produkty (urządzenia, sprzęty) w przedmiotowym postępowaniu o udzielenie zamówienia publicznego muszą spełniać wymagania norm CE, tj. muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE lub równoważne. |
| 24 | Urządzenia i ich komponenty muszą być oznakowane przez producenta  w taki sposób, aby możliwa była identyfikacja zarówno produktu jak  i producenta. |
| 25 | Urządzenie musi współpracować z siecią energetyczną o parametrach  w przedziale 200V- 230V, 50 Hz. |
| 26 | Macierz dyskowa musi być objęta gwarancją onsite świadczoną w reżimie  24x7 przez okres minimum 24 miesiące. |
| 27 | Zgłoszenia usterek muszą być akceptowane przez producenta zarówno drogą email jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności. Linia telefoniczna musi być czynna 24 godziny na dobę, 7 dni w tygodniu również w dni świąteczne. |
| 28 | Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia przez cały okres obowiązywania gwarancji. |

# **UTM – Wymagania minimalne – 1 sztuka**

|  |  |
| --- | --- |
|  | UTM - funkcjonalność |
| 1 | System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta. |
| 2 | System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 3 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 0,9 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS) i obsługiwać nie mniej niż 60 000 jednoczesnych połączeń. |
| 3 | System zabezpieczeń firewall musi być wyposażony w co najmniej 8 portów Ethernet 1G. |
| 4 | Interfejsy sieciowe systemu zabezpieczeń firewall muszą działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. |
| 5 | Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a system zabezpieczeń firewall musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.). |
| 6 | System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Interfejsy sieciowe pracujące w trybie transparentnym, L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać minimum 4094 znaczników VLAN. |
| 7 | System zabezpieczeń firewall musi obsługiwać nie mniej niż 3 wirtualne routery posiadające odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF. |
| 8 | System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7). |
| 9 | Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ). |
| 10 | System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone. |
| 11 | System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną. |
| 12 | Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 2,4 Gbit/s . |
| 13 | Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM). |
| 14 | Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall. |
| 15 | Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS. |
| 16 | System zabezpieczeń firewall musi wykrywać co najmniej 2000 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. |
| 17 | System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| 18 | System zabezpieczeń firewall musi zapewniać możliwość segmentacji aplikacji na standardowych dla nich portach usług w obrębie pojedynczej reguły polityki firewall, tj. musi istnieć możliwość takiej konfiguracji pojedynczej reguły firewall, która zezwoli na działanie kilku aplikacji, wyłącznie jeśli nawiązanie połączenia następuje na port właściwy dla danej aplikacji, np. jeśli pojedyncza reguła zezwala na ruch SMTP i DNS, to SMTP nie może być dozwolone na porcie 53 (właściwym dla DNS), a DNS na porcie 25 (właściwym dla SMTP). |
| 19 | System zabezpieczeń firewall powinien automatycznie weryfikować spójność konfiguracji polityk bezpieczeństwa z punktu widzenia kompletności użytych przez administratora sygnatur aplikacyjnych potrzebnych do prawidłowego działania polityki. Np. jeśli do prawidłowej obsługi dostępu do aplikacji „Facebook” potrzebne jest dodatkowo użycie aplikacji „SSL”, a administrator nie uwzględni tej aplikacji w polityce, to system powinien ostrzec o tym fakcie administratora w momencie zatwierdzania nowej polityki. |
| 20 | System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. |
| 21 | System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia. |
| 22 | System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji. |
| 23 | System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików. |
| 24 | System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |
| 25 | System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |
| 26 | System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. |
|  | System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji. |
| 27 | System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH. |
| 28 | System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. |
| 29 | System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. |
| 30 | System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia. |
| 31 | Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej. |
| 32 | System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. |
| 33 | System zabezpieczeń firewall musi umożliwiać kategoryzacje strony WWW za pomocą mechanizmu przypisującego do konkretnej strony kilka kategorii (np. portal finansowy i portal informacyjny). Kategoryzacja powinna zapewniać co najmniej cztery kategorie per strona. Dodatkowo, powinna istnieć możliwość budowania własnych kategorii bazujących na kombinacji kategorii standardowych (np. własna kategoria wiadomości finansowe zawierające wszystkie strony skategoryzowane jako portale finansowe i informacyjne) jak również budowanie kategorii na bazie ryzyka bezpieczeństwa danej strony (niskie, średnie, wysokie) i określenia czy dana strona jest stroną nowopowstałą. |
| 34 | System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| 35 | System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa. |
| 36 | System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| 37 | System zabezpieczeń musi umożliwiać deszyfrację ruchu SSL, przesłanie go w postaci rozszyfrowanej przez rozwiązania zewnętrzne firm trzecich (np. system DLP, system IPS, system Sand-box) i ponowne zaszyfrowanie protokołem SSL przed dalszą transmisją. |
| 38 | System zabezpieczeń musi umożliwiać wysyłanie kopii zdeszyfrowanego ruchu SSL na wskazany interfejs urządzenia. |
| 39 | System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| 40 | System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| 41 | System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| 42 | System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| 43 | System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| 44 | System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| 45 | System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| 46 | System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| 47 | System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. |
| 48 | System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole). |
| 49 | System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. |
| 50 | System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. |
| 51 | System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany. |
| 52 | System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. |
| 53 | System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, Ms-Offfice, jar, flash, apk, rar, MacOSX, Linux, JScript, PowerShell, Shell Scripts, VBScript) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 150 Mbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. |
| 54 | Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box". |
| 55 | Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”. |
| 56 | System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali. |
| 57 | System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. |
| 58 | System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa. |
| 59 | System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. |
| 60 | System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). |
| 61 | System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach. |
| 62 | System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0. |
| 63 | System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego. |
|  | System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników. |
| 64 | System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego. |
| 65 | System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla. |
| 66 | Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem. |
| 67 | System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu. |
| 68 | System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami. |
| 69 | System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji. |
| 70 | System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). |
| 71 | Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. |
| 72 | System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos. |
| 73 | System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS). |
| 74 | System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 128 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji. |
| 75 | System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu. |
| 76 | System zabezpieczeń firewall musi zapewniać mechanizm pozwalający na sprawdzenie podczas procesu instalacji nowej bazy sygnatur aplikacyjnych, które reguły bieżącej polityki bezpieczeństwa, polityki PBR (policy based routing) oraz polityki QoS wykorzystują sygnatury aplikacyjne modyfikowane w ramach bieżącej aktualizacji baz sygnatur. |
| 77 | System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa. |
| 78 | System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach. |
| 79 | System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia. |
| 80 | System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www. |
| 81 | System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. |
| 82 | System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni. |
| 83 | System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. |
| 84 | Całość objęta 24 miesięcznym wsparciem producenta. Wszystkie licencje dostarczone w ramach postępowania mają być objęte 24 miesięcznym wsparciem. |

# **Zasilacz awaryjny UPS do serwerowni – wymagania minimalne – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| Opis parametrów  techniczno-funkcjonalnych | | **wartości /funkcje** |
| **1** | Technologia | VFI (true on-line, podwójne przetwarzanie energii) |
| **2** | Moc znamionowa | 6kVA / 6kW |
| **3** | Wyjściowy współczynnik mocy (PF) | 1 |
| **4** | Wejściowy współczynnik mocy | cosφ ≥ 0,99 |
| **5** | Napięcie wejściowe | 208/220/230/240 VAC + N |
| **6** | Tolerancja napięcia wejściowego | 176 – 288 VAC |
| **7** | Częstotliwość wejściowa | 40-70 Hz |
| **8** | Minimalna sprawność AC-AC w trybie pracy on-line z obciążeniem 100% | 94% |
| **9** | Minimalna sprawność w trybie ECO | 98% dla 100% obciążenia |
| **10** | Możliwość rozbudowy mocy w okresie eksploatacji (praca równoległa) | do 4 jednostek |
| **11** | Napięcie wyjściowe | 208/220/230/240 VAC |
| **12** | Częstotliwość wyjściowa | 50/60Hz (programowalna) |
| **13** | Montaż | Wersja wolnostojąca TOWER lub RACK 4U (do wyboru) |
| **14** | Intuicyjny panel graficzny | tak |
| **15** | Zniekształcenia napięcia wyjściowego | ≤ 1% z obciążeniem liniowym  ≤ 4% z obciążeniem nieliniowym |
|  | Współczynnik szczytu przy obciążeniu znamionowym | 3:1 |
| **16** | Przeciążenie inwertera | 102%-110% przez 10 minut  110% -125% przez 1 minutę  125% -150% przez 30 sekund |
| **17** | Złącze interfejsów | RS232 + USB |
| **18** | Interfejs EPO (do wyłącznika ppoż.) | tak |
| **19** | Slot na dodatkowe karty komunikacyjne | tak |
| **20** | Możliwość pracy jako konwerter częstotliwości | tak |
| **21** | Baterie | Szczelne, bezobsługowe, w technologii AGM o żywotności projektowanej minimum 5 lat w temperaturze 25 stopni Celsjusza |
| **22** | Możliwość zainstalowania akumulatorów wewnątrz modułu zasilacza UPS | tak |
| **23** | Możliwość regulacji stosu bateryjnego | tak, 16-20 sztuk |
| **24** | Inteligentne zarządzanie baterią akumulatorów, zwiększające żywotnością baterii | tak |
| **25** | Test bateryjny | tak |
| **26** | Oprogramowanie zapewniające monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego | tak |
| **27** | Poziom hałasu w odległości 1m | ≤ 55 dBA |
| **28** | Spełnienie wszystkich obowiązujących norm bezpieczeństwa potwierdzone deklaracją zgodności CE | tak |
| **29** | Maks. wymiary modułu UPS (szer. x gł. x wys.) | 440 x 660 x 176 mm (4U) |
| **30** | Gwarancja | 24 miesiące na zasilacz UPS i akumulatory |

# **Biblioteka taśmowa do archiwizacji danych – wymagania minimalne – 1 sztuka**

|  |  |
| --- | --- |
| Lp. | Biblioteka taśmowa Parametr wymagany |
| 1 | Obudowa przystosowana do montażu w standardowej szafie rack 19’’. Maksymalna wysokość oferowanego rozwiązania - 3U. |
| 2 | Biblioteka taśmowa musi być wyposażona w min. 1 napędy taśmowe LTO7 z interfejsem FC min. 8 Gbit/s. |
| 3 | Biblioteka taśmowa musi mieć możliwość rozbudowy do min. 3 napędów taśmowych. |
| 4 | Biblioteka musi być wyposażona w nie mniej niż 32 sloty na taśmy z możliwością rozbudowy do 270 slotów, poprzez dodatkowe moduły rozszerzeń. |
| 5 | Biblioteka musi być wyposażona w przynajmniej 5 slotów wejścia/wyjścia (tzw. mail slot), umożliwiający wymianę taśm bez konieczności wyłączania urządzenia. |
| 6 | Biblioteka musi być wyposażona w czytnik kodów kreskowych. |
| 7 | Biblioteka musi być wyposażona w komplet magazynków na taśmy, tak by możliwa była pełna obsada biblioteki taśmami LTO. |
| 8 | Możliwość zdalnego zarządzania biblioteki poprzez interfejs WWW. |
| 9 | Możliwość monitorowania stanu biblioteki i napędów. |
| 10 | Biblioteka musi posiadać panel sterowania oraz wyświetlacz informujący o błędach urządzenia, aktywności napędów. |
| 11 | Macierz powinna umożliwiać partycjonowanie. Każda partycja powinna być prezentowana do hosta jako niezależna biblioteka. |
| 12 | Biblioteka musi posiadać redundantne zasilacze. |
| 13 | Razem z biblioteką oferent powinien dostarczyć min. 24 taśm LTO7 RW oznaczonych kodami kreskowymi oraz 2 taśmy czyszczące. |
|  | **Do biblioteki należy dostarczyć:** |
| 14 | Niezbędne kable zasilające. |
| 15 | Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu (najnowsza wersja firmware na dzień dostawy). |
| 16 | Wszystkie oferowane urządzenia muszą być fabrycznie nowe. |
| 17 | Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. |
| 18 | Urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz. |
| 19 | Oferowane produkty (urządzenia, sprzęty) w przedmiotowym postępowaniu o udzielenie zamówienia publicznego muszą spełniać wymagania norm CE, lub równoważne. |
| 20 | Gwarancja minimum 24 miesięcy on-site 24x7. |

# **System operacyjny do zarządzania pracą w sieci lokalnej – wymagania minimalne**

|  |  |
| --- | --- |
| Lp. |  |
| 1 | Oprogramowanie Systemu Operacyjnego (OSO):  Microsoft Windows Server 2022 Standard lub równoważne: 3 szt.  Licencja bezterminowa zgodna z liczbą fizycznych rdzeni procesorów zainstalowanych w dostarczanych w niniejszym postępowaniu serwerach. |
| 2 | Oprogramowanie Systemu Operacyjnego (OSO) licencje połączeniowe CAL na urządzenie: 50 szt. |
| 3 | Oprogramowanie Systemu Operacyjnego (OSO) licencje połączeniowe usług terminalowych RDS CAL na użytkownika: 10 szt. |
| 4 | **Opis równoważności dla Oprogramowania Systemu Operacyjnego:**  Cechy równoważnego oprogramowania typu Microsoft Windows Server 2019 Standard Edition:   1. Zamawiający dopuszcza zastosowanie oprogramowania równoważnego, poprzez które należy rozumieć oferowane oprogramowanie o parametrach nie gorszych od opisanych jako wymagane, umożliwiające wykorzystanie urządzeń, w takim samym zakresie i stopniu skomplikowania, co oprogramowanie określone w opisie przedmiotu zamówienia. 2. Oprogramowanie Systemu Operacyjnego (OSO) musi posiadać następujące cechy, funkcje i minimalne parametry:    1. Współpraca z procesorami o architekturze x86-64.    2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.    3. Obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu.    4. Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie minimum Microsoft Windows Server 2016.    5. Licencja musi uprawniać do uruchamiania wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.    6. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.    7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.    8. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.    9. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.    10. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.    11. Graficzny interfejs użytkownika. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.    12. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).    13. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.    14. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).    15. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  * Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC. * Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, * Pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe. * Zdalna dystrybucja oprogramowania na stacje robocze. * Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. * PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:   + Dystrybucję certyfikatów poprzez http,   + Konsolidację CA dla wielu lasów domeny,   + Automatyczne rejestrowania certyfikatów pomiędzy rożnymi lasami domen. * Szyfrowanie plików i folderów. * Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). * Serwis udostępniania stron WWW. * Wsparcie dla protokołu IP w wersji 6 (IPv6). * Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.   1. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.   2. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).   3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.   4. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF; W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania. |

# **Program do wirtualizacji – wymagania minimalne**

|  |  |
| --- | --- |
|  |  |
| 1 | Warstwa wirtualizacji powinna być rozwiązaniem systemowym tzn. powinna być zainstalowana bezpośrednio na sprzęcie fizycznym. |
| 2 | Oprogramowanie do wirtualizacji musi zapewniać możliwość obsługi 1 TB pamięci fizycznej  w serwerze. |
| 3 | Rozwiązanie powinno umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągniecia maksymalnego współczynnika konsolidacji. |
| 4 | Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych aniżeli fizycznie zarezerwowane. |
| 5 | System musi umożliwiać jednoczesną pracę wielu różnych maszyn wirtualnych (systemy operacyjne i działające w nich aplikacje) na współdzielonych zasobach serwera. |
| 6 | System musi umożliwiać tworzenie klonów działających wirtualnych maszyn bez potrzeby ich wyłączania. |
| 7 | Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi Microsoft Active Directory. |
| 8 | System musi umożliwiać tworzenie maszyn wirtualnych z 1, 2, 3, 4, 5, 6, 7, 8 wirtualnymi procesorami. |
| 9 | Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. |
| 10 | System musi umożliwiać tworzenie wielu migawek maszyn wirtualnych w celu późniejszego powrotu do określonego miejsca instalacji. |
| 11 | Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z dwóch ścieżek. |
| 12 | System musi wspierać następujące systemy operacyjne:   * Windows Server 2012 * Windows Server 2012 R2 * Windows Server 2016 * Windows Server 2019 * Ubuntu 18.04 LTS * Ubuntu 18.10 * SUSE Linux Enterprise Server 15 * Centos 7.x * Red Hat Enterprise Linux 7 * Oracle Linux 7.x |
| 13 | System musi umożliwiać automatyczne zarządzanie poprawkami dla infrastruktury. |
| 14 | System zarządzania wirtualnymi maszynami musi posiadać interfejs zarządzania. |
| 15 | Rozwiązanie musi posiadać system do zarządzania maszynami wirtualnymi. Musi zapewnić zarządzanie minimum 3 hostami fizycznymi. |
| 16 | Rozwiązanie powinno zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej. |
| 17 | Oprogramowanie musi zostać objęte wsparciem producenta na minimum 24 miesięcy. |

# **Program do archiwizacji danych – wymagania minimalne**

|  |  |
| --- | --- |
| Lp. |  |
|  | **Wymagania ogólne:**   1. Oprogramowanie powinno być przeznaczone dla małych, średnich i dużych firm, które mają rozbudowane środowisko informatyczne, powinien oferować elastyczną architekturę (serwer zarządzający/media-serwer/klient) celem sprostania rozwojowi środowiska informatycznego 2. System musi cechować bardzo efektywne wykorzystanie napędów taśmowych, tzn. system musi być zoptymalizowany do użycia jak najmniejszej ilości napędów taśmowych, wymagana jest możliwość wykonania backupu bezpośrednio na napęd taśmowy bez konieczności wykonania wcześniejszej kopii na dysk. 3. System musi zapisywać dane na taśmach tak zoptymalizowane, aby nie było potrzeby wykonywania żadnych dodatkowych działań (nawet automatycznych) celem ich optymalizacji 4. Powinien umożliwiać łatwą rozbudowę w miarę rozrastania się infrastruktury informatycznej 5. Brak preferowanego dostawcy hardware dla którego dostępna jest bogatsza funkcjonalność (macierze, biblioteki taśmowe…), musi istnieć możliwość zmiany producenta sprzętu bez utraty funkcjonalności backupu 6. Powinien być łatwy w instalacji, konfigurowaniu i zarządzaniu poprzez interface graficzny (GUI). Powinien umożliwiać pełne dostosowanie do środowiska klienta. 7. Powinien posiadać zaawansowane funkcje monitoringu, generator raportów. 8. Powinien umożliwiać backup po sieci LAN serwerów z Windows 2008/2012/2016/2019, Linuxy z rodziny Debian, RedHat, Suse, CentOS Oracle Linux oraz stacji roboczych z Windows 7/8/10 9. Do przechowywania danych wykorzystywane powinny być bezobsługowe biblioteki taśmowe bądź lokalne dyski. 10. Możliwość stosowania go w środowisku Storage Area Network, co zapewni dużą szybkość wykonywanych backupów oraz współdzielenie napędów taśmowych pomiędzy serwery backupowe w sieci SAN. 11. Powinien potrafić backupować online bazy danych i aplikacje taki jak. Oracle 10g/11g/12c, MS Exchange 2010/2013/2016/2019, MS SQL 2005/2008/2012/2014/2016/2017/2019, MS Sharepoint 2010/2013/2016/2019, Active Directory 2008/2012/2016/2019. 12. Backup i odtwarzanie serwera Exchange powinno umożliwiać odtworzenie na poziomie pojedynczej wiadomości w skrzynkach użytkowników. Opcja powinna umożliwiać odzyskiwanie z backupu bazy danych bez dodatkowego backupu skrzynek pocztowych w trybie MAPI. 13. Powinien posiadać również wbudowany mechanizm do backupowania otwartych plików 14. Powinien potrafić wykorzystywać do backupu mechanizm kopii migawkowych systemu Microsoft Windows (VSS) 15. Posiadać funkcje disaster–recovery dla systemu Windows umożliwiające proste i szybkie automatyczne odtworzenie serwera po awarii zapewniające integralność i spójność danych, opcja ta powinna być integralną częścią systemu backupowego. 16. Automatyczny backup bazujący na kalendarzu. Możliwość backupu typu: full, incremental, differential, forever incremental backup 17. Musi umożliwiać wykonywania skryptów przed i po backupie (np. uruchamianych przed backupem bazy oraz po wykonaniu backupu off-line bazy, kasowanie redo logów) 18. Możliwość szyfrowania danych przesyłanych przez sieć LAN. Opcja powinna być ściśle zintegrowana z produktem do backupu. 19. Możliwość kompresji na kliencie backupowym przed wysłaniem danych przez sieć. 20. Posiadać możliwość wykonywania backupów na urządzenia dyskowe, które następnie będą automatycznie powielane na nośniki taśmowe (D2D2T). System backupowy powinien, tak długo jak dane obecne są na dyskach, wykorzystywać je w procesach restore, znacznie skracając czas odtworzenia danych 21. Oprogramowanie powinno oferować funkcjonalność pozwalającą zminimalizować ilość koniecznych do wykonywania powtarzalnych pełnych kopii danych systemów plików. 22. System powinien mieć możliwość monitowania i alterowania poprzez email i SNMP 23. Powinien posiadać możliwość backupu online danych z systemu SharePoint Portal Server, wraz z odtwarzanie pojedynczych dokumentów z jednoprzebiegowego backupu. 24. Musi mieć możliwość zintegrowania się z technologią vStorage API celem wydajnego backupu danych z możliwością odtwarzania pojedynczych plików (zawartych w VMDK dla systemów Windows), backup musi być wykonywany jednoprzebiegowo (cały plik VMDK backupowany raz) 25. Musi wspierać najnowsze wersje środowisk Vmware vSphere 6.0/6.5/6.7/7.0 i wspierać backup za pomocą mechanizmu vstorage API. 26. Musi wspierać dla technologii wirtualizacyjnych firmy Microsoft (Hyper-V), z możliwością odtwarzania pojedynczych plików z maszyn wirtualnych Windows z jednoprzebiegowego backupu. Wsparcie musi uwzględniać najnowsze wersje oprogramowania Windows 2008 R2, 2012 R2 , 2016 oraz 2019 27. System powinien posiadać (jako opcja) możliwość wykonania backupu Active Directory a następnie odzyskania pojedynczych obiektów AD bez restartu i resynchronizacji systemu. Backup ten powinien być wykonywany jednoprzebiegowo. 28. System musi mieć możliwość centralnego zarządzania serwerami (Media Serwerami) systemu backupowego z pomocą nadrzędnej konsoli, zamawiający nie wymaga dostarczenia licencji na tą funkcjonalność. 29. Możliwość backupu poprzez sieć SAN zasobów z serwerów Linux, tak by tylko metadane były wysyłane przez sieć LAN 30. System musi posiadać jako opcję (komponent, włączany działający jako integralna część aplikacji backupowej) deduplikację danych. Funkcjonalność tego modułu musi opierać się na blokowej deduplikacji danych wykonywanej online a więc w trakcie wykonywania zadania backupowego. Proces deduplikacji danych musi odbywać się na kliencie (serwerze z danymi czy aplikacją) lub na media serwerze. Konfiguracja i zarządzanie całym procesem, przełączanie miejsca deduplikacji musi odbywać się za pomocą jednej konsoli zarządzającej systemem backupowym – jedna konsola dla konfigurowania i zarządzania całością procesów backupowych i odtwarzania danych. 31. Deduplikacja danych na kliencie (optymalizacja transferu danych przez siec LAN/WAN) musi być dostępna dla systemów Windows i Linux i nie może wymagać instalacji dodatkowych komponentów czy agentów poza oprogramowaniem klienckim systemu backupowego, 32. Włączenie funkcjonalności deduplikacji danych nie może powodować konieczności doinstalowania dodatkowego oprogramowania nie tylko po stronie klienta backupu ale także media serwera (serwera systemu backupowego) 33. System musi posiadać otwarte API umożliwiające podłączanie urządzeń deduplikacyjnych innych firm. Wymagane jest wsparcie dla EMC DataDomain, Quantum DXi, HPE StoreOnce 34. Musi umożliwiać odtwarzanie pojedynczych elementów (maili, elementów AD, plików czy baz danych ) z aplikacji Exchange, Active Directory, SharePoint i MS SQL zainstalowanych w środowiskach wirtualnych (Vmware, Hyper-V) poprzez backup całej maszyny wirtualnej – pojedynczy backup całego pliku vmdk a odtwarzanie różnego typu (cała maszyna, plik z systemu plikowego, element aplikacji/baza danych) 35. Musi mieć możliwość szyfrowania komunikacji pomiędzy klientem (serwerem produkcyjnym) a serwerem backupowym za pomocą SSL. 36. Funkcja disaster-recovery musi być dostępna dla systemów Windows i oprócz odtwarzania systemu operacyjnego musi umożliwiać zmianę sterowników minimum do urządzeń pamięci masowych czy kart sieciowych tak by było możliwe odtworzenie systemu na innym fizycznym sprzęcie 37. Musi istnieć możliwość wykonywania konwersji P2V, B2V oraz C2V systemów fizycznych (Windows) na maszyny wirtualne (Vmware i Hyper-V) na 3 sposoby: jeden P2V – pozwala na równoczesny backup danych i jednoczesną konwersję do pełnej maszyny wirtualnej, drugi sposób: B2V wykonuje zadanie konwersji po zakończeniu zadania backupowego oraz trzeci: C2V czyli konwersja bezpośrednia całego obrazu maszyny fizycznej w trakcie jej działania do maszyny wirtualnej bez tworzenia kopii zapasowej. Wszystkie sposoby konwersji są wewnętrznymi komponentami systemu backupowego i nie wymagają dodatkowych licencji czy instalacji dodatkowego oprogramowania. 38. Musi istnieć funkcjonalność uruchomienia wirtualnej maszyny z kopii backupowej bez konieczności kopiowania jej na system produkcyjny. Funkcjonalność ta musi być dostępna w poziomu interfejsu graficznego. Nie jest dopuszczalne uruchamianie tej funkcjonalności przez skrypty. 39. Musi istnieć model licencjonowania oparty o liczbę procesorów fizycznych w serwerach fizycznych na których uruchomiona wirtualizacja dzięki któremu jest możliwość backupu nieograniczonej liczby wirtualnych maszyn znajdujących się na tych serwerach. Tworzenie zadań backupowych dla nowych wirtualnych maszyn na tych serwerach fizycznych nie może powodować konieczności dokupienia dodatkowych licencji. Jednak zamawiający dopuszcza w tym postępowaniu inny model licencjonowania w tym subskrypcję mierzoną ilością obciążeń to znaczy maszyn fizycznych lub wirtualnych. 40. Musi istnieć możliwość **zarządzania** systemem backupowym z wykorzystaniem CLI (Command Line Interface) poprzez komponent Windows PowerShell obejmująca wszystkie zadania administracyjne pokrywające się możliwościami z interfejsem graficznym w 100%. 41. Wsparcie na oprogramowanie na 24 miesięcy |

# **Pakiet biurowy Microsoft Office – wymagania minimalne – 26 sztuk**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | **Nazwa** | **Wymagania dotyczące pakietu biurowego** |
| 1 | **Microsoft Office 2019 dla Użytkowników Domowych lub małych Firm lub równoważne** | Zintegrowany pakiet oprogramowania biurowego o parametrach minimum:  - w polskiej wersji językowej zawierający edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji, aplikację służącą do obsługi poczty elektronicznej i organizacji czasu, (dostarczenie produktów pochodzących od różnych producentów nie będzie uznane za ofertę zintegrowanego pakietu, pakiet biurowy musi spełniać wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji),  - całkowicie zlokalizowany w języku polskim system komunikatów, interfejsu użytkownika i podręcznej pomocy technicznej,  - prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych,  - ze względu na wdrożoną u Zamawiającego usługę katalogową Active Directory dostarczone oprogramowanie musi mieć możliwość zarządzania ustawieniami poprzez polisy GPO oraz umożliwiać centralne zarządzanie i dystrybuowanie aktualizacji,  - dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej  - pakiet musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:  a) posiada kompletny i publicznie dostępny opis formatu,  b) ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526),  c) pozwala zapisywać dokumenty w formacie XML.  - pakiet musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.  - do pakietu musi być dostępna pełna dokumentacja w języku polskim.  - w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy),  - umożliwiający pracę grupową na dokumentach stworzonych w MS Office w wersji co najmniej 2007, w pełni obsługujący wszystkie istniejące dokumenty Zamawiającego (utworzone przy pomocy Microsoft Word, Excel, PowerPoint w wersjach 2007, 2010, 2013, 2016, 2019, 2021 z zapewnieniem niezawodnej konwersji wszystkich elementów i atrybutów dokumentów - wspierający formaty plików .doc, .docx, .xls, .xlsx, .ppt, .pptx) oraz w pełni kompatybilny z posiadanym oprogramowaniem Zamawiającego wykorzystującym międzysystemową wymianę danych, bez utraty jakichkolwiek ich parametrów i cech użytkowych (korespondencja seryjna, wielokolumnowe arkusze kalkulacyjne zawierające makra i formularze, itp.) bez potrzeby stosowania dodatkowych narzędzi konwertujących,  - wydruk musi wyglądać identycznie bez konieczności dodatkowej jego edycji, wszystkie funkcje oraz makra muszą działać poprawnie a ich wynik musi być identyczny jak w przypadku MS Office 2016 PL bez konieczności dodatkowej edycji dokumentu,  - pełna wersja produktu, oprogramowanie nie może posiadać ograniczeń czasowych oraz funkcjonalnych (bezterminowa licencja na użytkowanie),  - oprogramowanie powinno być w wersji oficjalnej, niedopuszczalne jest dostarczenie w wersji typu alpha, beta, Community Preview (CP) lub innej, która zabrania używania oprogramowania przez urząd administracji publicznej,  - licencja – bezterminowa, musi umożliwiać bezpłatną aktualizację produktu w całym okresie wsparcia technicznego i pozostawania w ofercie rynkowej,  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  - sprawdzanie pisowni w języku polskim  - śledzenie i porównywanie zmian wprowadzonych przez użytkowników  - nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności  - określenie układu strony (pionowa/pozioma)  - wydruk dokumentów  - automatyczne wypisywanie hyperlinków  - wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną  - pracę na dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013, 2016, 2019, 2021 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu  - zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji  - wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem  - wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa  - wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.  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 )  - 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 zgodnie z polskim formatem  - zapis wielu arkuszy kalkulacyjnych w jednym pliku.  - zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013, 2016, 2019, 2021 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń  - zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji  Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:  - przygotowywanie prezentacji multimedialnych, które będą 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  - pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013, 2016, 2019, 2021  Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:  - pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego  - 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  - zarządzanie kalendarzem  - udostępnianie kalendarza innym użytkownikom  - zarządzanie listą zadań  - zlecanie zadań innym użytkownikom  - zarządzanie listą kontaktów  - możliwość przesyłania kontaktów innym użytkowników  Wymaga się, aby wersja instalacyjna pakietu została dostarczona na nośniku zewnętrznym lub w postaci pliku do pobrania z Internetu z autoryzowanej witryny (plik obrazu lub wersja instalacyjna). |

# **Program do zarządzania IT – wymagania minimalne**

|  |  |  |
| --- | --- | --- |
|  |  | Parametr wymagany |
| 1 | **Wymagania ogólne** | Oprogramowanie oraz dokumentacja dostępna w języku polskim.  Oprogramowanie posiadające konstrukcje modułową, zarządzane z jednej konsoli administracyjnej.  Oprogramowanie posiada agentów, instalowanych na systemach operacyjnych klienckich, agenci muszą być kompatybilni z systemami operacyjnymi:  Windows 7, Windows 8.1, Windows 10  Wbudowana funkcjonalność ochrony agenta przed usunięciem przez użytkownika.  Oprogramowanie pozwala na równoległa prace wielu administratorów w tym samym czasie. |
| 2 | **Zarządzanie siecią** | Funkcjonalności modułu zarządzania siecią:   1. Budowanie interaktywnej mapy sieci oraz połączeń sieciowych 2. Wykrywanie urządzeń sieciowych oraz serwisów poprzez skanowanie 3. Wykrywanie ruchu na portach sieciowych routerów oraz przełączników sieciowych 4. Obsługa pułapek SNMP v1/v2c/3 5. Możliwość dodawania nowych plików MIB 6. Obsługa serwera syslog 7. Monitorowanie serwisów sieciowych w tym: http/HTTPS/FTP/LDAP/IMAP 8. Generowanie alarmów na podstawie dostępności urządzenia lub serwisu   Monitorowanie systemów operacyjnych Windows poprzez WMI |
| 3 | **Inwentaryzacja** | Funkcjonalności modułu inwentaryzacji:   1. Automatyczne gromadzenie informacji o konfiguracji sprzętowej oraz oprogramowaniu stacji roboczych z zainstalowanym systemem operacyjnym Windows 2. Możliwość zdalnego dostępu do plików użytkownika i ich modyfikacji/usuwania 3. Audyt sprzętu oraz oprogramowania 4. Inwentaryzacja oraz zarządzenie środkami trwałymi 5. Możliwość generowania alarmów, podczas zmian sprzętowych   Możliwość instalacji oprogramowania wykorzystując pakiety MSI |
| 4 | **Obsługa użytkowników** | Funkcjonalności modułu do obsługi użytkowników:   1. Integracja z domeną MS Active Directory 2. Możliwość zablokowania uruchomionych aplikacji 3. Blokowanie stron www 4. Audyt czasu pracy 5. Audyt używanych i nie używanych aplikacji 6. Audyt informacji o odwiedzanych stronach www w tym (czas wizyty, adres strony) 7. Podgląd pulpitu zdalnego użytkownika 8. Możliwość zrealizowania zrzutu ekranu użytkownika 9. Audyt wydruków realizowanych przez użytkownika |
| 5 | **Pomoc zdalna** | Funkcjonalność modułu do pomocy zdalnej:   1. Integracja z domeną MS Active Directory 2. Wykonywanie zrzutów pulpitu 3. Podgląd pulpitu użytkownika 4. Wykonywanie zdalnych poleceń systemowych 5. Przypisywanie zgłoszeń pracownikom helpdesk 6. Planowanie nieobecności pracowników pomocy zdalnej 7. Dystrybucja plików przy pomocy agenta 8. Generowanie raportów obsługi helpdesk 9. Baza wiedzy dla pracowników |
| 6 | **Instalacja** | Oprogramowanie ma zostać zainstalowane na platformie wirtualizacji dostarczanej w ramach tego zamówienia. |
| 7 | **Licencja** | Obsługa minimum 50 użytkowników. |
| 8 | **Gwarancja** | 24 miesiące gwarancji oraz wsparcia technicznego producenta. |

# **Usługa wdrożeniowa sprzętu i oprogramowania – wymagania minimalne**

|  |  |
| --- | --- |
| Lp. |  |
|  | 1. Zamawiający wymaga przygotowania w porozumieniu z Zamawiającym „Planu wdrożenia” obejmującego min.:    * Opis wdrażanego rozwiązania    * Plan fizycznej instalacji komponentów sprzętowych    * Plan rozplanowania zasilana    * Plan implementacji przełączników sieciowych    * Graficzne zilustrowanie połączeń sieciowych z podziałem na typy mediów    * Tabelaryczne zestawienie połączeń fizycznych sieci Ethernet    * Adresację IP poszczególnych komponentów sprzętowych 2. Usługi w zakresie dostawy zasilacza awaryjnego UPS    * Instalacja urządzenia w szafie RACK    * Montaż opcjonalnych komponentów    * Rozruch zasilacza awaryjnego wraz z weryfikacją poprawności działania    * Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta    * Konfiguracja adresacji IP interfejsu zarządzania    * Instalacja oprogramowania służącego do wyłączania systemów w przypadku zaniku zasilania    * Weryfikacja działania automatycznego wyłączania systemów w przypadku zaniku zasilania 3. Usługi w zakresie konfiguracji przełączników    * Montaż przełączników sieciowych Typ 1 i Typ2 w ustalonych dla nich lokalizacjach    * Podłączenie zasilania z ustalonych źródeł zasilania    * Konfiguracja podstawowych parametrów sieciowych (adres, maska, brama sieciowa, serwer czasu) interfejsu(-ów) zarządzania    * Aktualizacja oprogramowania układowego do zalecanej przez producenta wersji    * Instalacja przewidzianych w urządzeniach modułów oraz połączeń kablowych    * Konfiguracja nadmiarowości urządzeń na parach przełączników sieciowych Typ 1 i Typ2    * Konfiguracja sieci VLAN i ewentualnej przynależności interfejsów sieciowych przełączników    * Weryfikacja poprawności działania nadmiarowości urządzeń i połączeń    * Podłączenie przełączników sieciowych Typ1 i Typ2 do infrastruktury sieciowej Zamawiającego zgodnie z Planem wdrożenia    * Weryfikacja poprawności konfiguracji sieciowej    * Zapisanie w formie elektronicznej konfiguracji poszczególnych przełączników sieciowych i przekazanie Zamawiającemu w celu zabezpieczenia. 4. Usługi w zakresie dostawy serwerów    * Montaż serwerów w ustalonej lokalizacji i szafie RACK    * Podłączenie okablowania sieci LAN/SAN    * Podłączenie zasilania    * Konfiguracja serwerów obejmująca min.:      + Konfigurację adresacji IP interfejsu zarządzania      + Synchronizację czasu urządzenia z serwerem NTP      + Instalację wszelkich niezbędnych licencji – o ile konieczne. Kopie licencji należy przekazać Zamawiającemu w celu zabezpieczenia      + Aktualizację oprogramowania układowego do rekomendowanej przez producenta wersji    * Weryfikacja poprawności działania połączeń LAN/SAN    * Wykonanie testu działania nadmiarowości zasilania i odporności na zanik napięcia w jednym źródle zasilania 5. Usługi w zakresie dostawy macierzy    * Montaż macierzy w ustalonej lokalizacji i szafie RACK    * Podłączenie okablowania sieci LAN/SAN    * Podłączenie zasilania    * Konfiguracja macierzy obejmująca min.:      + Konfigurację adresacji IP interfejsu(-ów) zarządzania      + Synchronizację czasu urządzenia z serwerem NTP      + Instalację wszelkich niezbędnych licencji – o ile konieczne. Kopie licencji należy przekazać Zamawiającemu w celu zabezpieczenia.      + Aktualizację oprogramowania układowego do rekomendowanej przez producenta wersji      + Konfigurację przestrzeni dyskowych zgodnie z Planem wdrożenia      + Konfiguracje mechanizmów zabezpieczeń przestrzeni dyskowych (snapshot)      + Integracja z Oprogramowaniem Systemu Wirtualizacji Serwerów      + Konfigurację powiadomień o awariach (min. e-mail)    * Wykonanie testów działania nadmiarowości komponentów i poprawności konfiguracji w zakresie połączeń Front-End i odporności na zanik napięcia w jednym źródle zasilania 6. Usługi w zakresie wdrożenia Oprogramowania Systemu Wirtualizacji Serwerów    * Instalacja systemu operacyjnego OSWS na dostarczanych serwerach.    * Konfiguracja systemu operacyjnego OSWS, obejmująca min.:      + Konfigurację adresu(-ów) IP zarządzania      + Synchronizację czasu z serwerem NTP      + Konfigurację wirtualnych przełączników sieciowych      + Konfigurację przestrzeni dyskowej udostępnionej z dostarczonej macierzy      + Wykonanie testu poprawności konfiguracji namiarowości połączeń wirtualnego przełącznika sieciowego poprzez odłączenie jednego z fizycznych interfejsów LAN serwera    * Wdrożenie i konfiguracja systemu zarządzania OSWS, obejmująca m.in.:      + Konfigurację adresu(-ów) IP      + Synchronizację czasu z serwerem NTP      + Konfigurację środowiska OSWS obejmującą instancję zainstalowanego oprogramowania serwera wirtualizacji      + Integracja uwierzytelniania systemu zarządzania OSWS z Active Directory      + Konfigurację powiadomień o awariach (min. e-mail)    * Integrację z systemem wyłączania systemów Zasilacza awaryjnego UPS w celu automatycznego wyłączenia wirtualnych maszyn w przypadku zaniku zasilania    * Przygotowanie 4 maszyn wirtualnych maszyn zgodnie z wymaganiami Zamawiającego 7. Usługi w zakresie wdrożenia Oprogramowania Systemu Operacyjnego    * Instalacja czterech instancji OSO na przygotowanych wirtualnych maszynach zgodnie z ustaloną konfiguracją, obejmująca m.in.:      + Instalacja i konfiguracja serwera kontrolera Domeny,      + Instalacja i konfiguracja serwera DNS, DHCP, serwer plików,      + Instalacja i konfiguracja zapasowego serwera kontrolera Domeny      + wdrożenie zarządzania Active Directory(konfiguracja kont administracyjnych, konfiguracja kont użytkowników, konfiguracja polityk bezpieczeństwa, konfiguracja kopii bezpieczeństwa, utworzenie schematu organizacyjnego, utworzenie folderów udostępnianych)      + Konfiguracja adresacji IP oraz nazwy sieciowej zgodnie z Planem wdrożenia,      + Konfiguracja przykładowej polityki GPO,      + Dodanie do domeny do 10 urządzeń,      + Weryfikacja poprawności konfiguracji sieciowej OSO ,      + Integracja uwierzytelniania z Active Directory,      + Aktualizacja wszystkich zalecanych dla OSO poprawek 8. Usługi w zakresie wdrożenia Oprogramowania do zarządzania komponentami infrastruktury    * Instalacja oprogramowania do zarządzania komponentami infrastruktury na wskazanej przez Zamawiającego maszynie wirtualnej,    * Integracja oprogramowania z domeną Active Directory.    * Konfiguracja kont użytkowników administracyjnych,    * Konfiguracja kont użytkowników pomocy zdalnej – helpdesk,    * Instalacja agentów na stacjach roboczych użytkowników,    * Integracja z serwerem poczty,    * Konfiguracja powiadomień e-mail.    * Konfiguracja w oprogramowaniu komponentów wdrażanych w ramach tego Zamówienia 9. Usługi w zakresie wdrożenia Oprogramowania Kopii Zapasowych:  * Weryfikacja spełnienia wymagań serwera posiadanego przez Zamawiającego pod kątem instalacji Oprogramowania Kopii Zapasowych. * Instalacja komponentów oprogramowania systemu backupu w najnowszej dostępnej wersji. * Konfiguracja przestrzeni dyskowych przeznaczonych do składowania danych. * Konfiguracja niezbędnych kont użytkowników systemu operacyjnego oraz Oprogramowania Systemu Wirtualizacji Serwerów. * Integracja z Oprogramowaniem Systemu Wirtualizacji Serwerów. * Integracja z istniejącą macierzą dyskową typu NAS. * Podłączenie i konfiguracja dostarczanej biblioteki taśmowej. * Przeprowadzenie testów wykonywania i odzyskiwania kopii zapasowych: * Wykonanie kopii zapasowej testowej wirtualnej maszyny. * Wykonanie odtworzenia testowej wirtualnej maszyny z kopii zapasowej. * Przygotowanie polityki backupowych dla kategorii serwerów określonych przez Zamawiającego względem krytyczności. * Konfiguracja zadań backupowych obejmujących poszczególne kategorie wirtualnych maszyn pod względem krytyczności. * Konfiguracja pul nośników taśmowych (polityki retencji nośników). * Konfiguracja kopiowania punktów przywracania kopii zapasowych na taśmy. * Konfiguracja powiadomień oprogramowania kopii zapasowych.  1. Usługi w zakresie wdrożenia urządzenia UTM    * Zainstalowane oraz okablowane w szafie RACK Zamawiającego    * Musi zostać wykonana integracja z posiadanym przez Zamawiającego środowiskiem w zakresie:      + Zasilania,      + Sieci WAN,      + Sieci zarządzania,      + Systemu DNS,      + Systemu synchronizacji czasu,      + Systemu poczty e-mail.    * Musi zostać wykonana konfiguracja topologii logicznej sieci w tym m.in.:      + Konfiguracja adresacji sieci IP,      + Konfiguracja sieci VLAN,      + Konfiguracja routing,    * Urządzenie musi zostać zintegrowane z domeną Active Directory    * Musi zostać wykonana konfiguracja polityki bezpieczeństwa zgodnie z wytycznymi Zamawiającego,    * Musi zostać wykonana konfiguracja tuneli VPN zgodnie z wytycznymi Zamawiającego,    * Musi zostawać skonfigurowany system logowania a wraz z nim:      + Konfiguracja raportów,      + Konfiguracja powiadomień e-mail |

# **Szkolenia stacjonarne dla pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania – wymagania minimalne**

|  |  |
| --- | --- |
| Lp. |  |
|  | 1. Szkolenie z zakresu obsługi, zarządzania i utrzymania dostarczanego sprzętu i oprogramowania    * Minimum dwa dni szkolenia (8 godzin lekcyjnych per dzień).    * Ćwiczenia praktyczne powinny zajmować nie mniej niż 50% przewidzianego czasu i muszą być realizowane na infrastrukturze Wykonawcy.    * Zamawiający przewidzenie 45 minutowej przerwy obiadowej w każdym dniu szkolenia.    * Prowadzący szkolenie powinien być inżynierem posiadającym aktualne certyfikaty potwierdzające znajomość zagadnień z zakresu wdrażania i administracji OSWS.    * Zamawiający po zakończonym szkoleniu wymaga przekazania materiałów dydaktycznych (prezentacja, skrypty ćwiczeń itp.) w języku polskim. Zamawiający dopuszcza przekazanie materiałów w formie nieedytowalnych plików PDF. 2. Szkolenie z zakresu zarządzania i utrzymania dostarczanego UTM:    * Minimum jeden dzień szkolenia (8 godzin lekcyjnych).    * Prowadzący szkolenie powinien być inżynierem posiadającym aktualne certyfikaty potwierdzające znajomość zagadnień z zakresu wdrażania i administracji UTM.    * Zamawiający po zakończonym szkoleniu wymaga przekazania materiałów dydaktycznych (prezentacja, skrypty ćwiczeń itp.) w języku polskim. Zamawiający dopuszcza przekazanie materiałów w formie nieedytowalnych plików PDF. 3. Szkolenie z zakresu zarządzania i utrzymania dostarczanego Oprogramowania Kopii Zapasowych:    * Minimum 4 godziny zegarowe.    * Prowadzący szkolenie powinien być inżynierem posiadającym aktualne certyfikaty potwierdzające znajomość zagadnień z zakresu wdrażania i administracji oferowanym Oprogramowaniem Kopii Zapasowych.    * Zamawiający po zakończonym szkoleniu wymaga przekazania materiałów dydaktycznych (prezentacja, skrypty ćwiczeń itp.) w języku polskim. Zamawiający dopuszcza przekazanie materiałów w formie nieedytowalnych plików PDF. |