**Załącznik nr 2 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Zakup i wdrożenie systemu Backup i ochrony poczty dla Powiatowego Zespołu Szpitali**

**– szpital w Sycowie**

Minimalne parametry jakie zawierać muszą produkty będące przedmiotem zamówienia”

# Serwer pod backup

1 sztuka

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 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 jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych |
| **Procesor** | Zainstalowany jeden procesor, min. 16-rdzeniowy klasy x86, o prędkości min 3.0GHz z min. 128GB Cache, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 154 w teście SPECrate2017\_int\_base, dostępnym na stronie [www.spec.org](http://www.spec.org) dla proponowanego serwera. |
| **RAM** | Minimum 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do min. 2TB pamięci RAM. |
| **Zabezpieczenia pamięci RAM** | Memory demand and patrol scrubbing, Failed DIMM isolation, Memory Address Parity Protection |
| **Gniazda PCI** | - min. 2 sloty PCIe x16 generacji 3 oraz min. 2 sloty PCIe x16 generacji 4. |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (interfejsy nie mogą zajmować gniazda PCI) Wbudowane 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (interfejsy nie mogą zajmować gniazda PCI). Porty obsadzone modułami 10Gb/s SFP+ SR. 2 zewnętrzne interfejsy SAS 12Gbps  Serwer wyposażony w 2 światłowody OM3 LC-LC o długości minimum 3metrów. |
| **Dyski twarde** | Możliwość instalacji dysków SATA, SAS, SSD.  Zainstalowane 2 dyski SATA o pojemności min. 960GB z możliwością konfiguracji RAID 1.  Zainstalowanych 12 dysków NLSAS o pojemności min. 8TB z możliwością konfiguracji RAID 6.  Możliwość zainstalowania modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności min. 64GB. Rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający min. 2GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |
| **Wbudowane porty** | min. 2 porty USB 2.0, 1 port micro USB oraz 3 porty USB 3.0,  2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232 |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900 |
| **Wentylatory** | Redundantne |
| **Zasilacze** | Redundantne, Hot-Plug min. 1100W każdy wraz z kablami zasilającymi o długości min. 2m. |
| **Bezpieczeństwo** | Zainstalowany moduł TPM 2.0  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. |
| **Diagnostyka** | Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |
| **System operacyjny** | Windows Server 2022 Standard 16 core – 1 sztuka |
| **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-9001:2015 oraz ISO-14001.  Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019, Microsoft Windows 2022. |
| **Warunki gwarancji** | 36 miesięcy 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 9001:2015 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 sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.  Możliwość rozszerzenia gwarancji przez producenta do siedmiu 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. |

# Biblioteka taśmowa

1 sztuka

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Do zamontowania w szafie rack, maksymalnie 3U, wbudowany czytnik kodów kreskowych, redundantne zasilanie wraz z kablami zasilającymi. |
| **Napęd** | Jeden napęd LTO8 SAS. Możliwość rozbudowy do min. 21 napędów LTO. |
| **Interfejs** | SAS 6Gb/s wraz z dwoma kablami pozwalającymi na podłączenie do serwera dostarczonego wraz z biblioteką taśmową. |
| **Liczba slotów** | 40 w tym minimum pięć slotów we/wy, jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów  W komplecie minimum:   * 16 taśm LTO8 * 1 taśma czyszczące LTO8 * Etykiety do taśm LT08 o numerach 1-200 |
| **Dodatkowe** | * interfejs do zarządzania poprzez przeglądarkę WWW oraz możliwość zarządzania bezpośrednio z użyciem wbudowanych klawiszy i wyświetlacza LCD * wyjmowane magazynki kieszeni na taśmy w celu łatwego zarządzania większą ilością taśm * wsparcie dla nośników LTO WORM (Write Once, Read Many), umożliwiających spełnienie norm prawnych dotyczących odpowiednio długiego przechowywania nienaruszonych danych (archiwizacja) * Obsługa SNMP, TLS1.2 oraz IP6 * Wsparcie dla technologii szyfrowania backupowanych danych. |
| **Warunki gwarancji dla autoloadera** | 36 miesięcy gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.   * Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu. * W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych). * Wymagana instalacja urządzenia w szafie serwerowej rack. * Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty. * Oświadczenie producenta biblioteki, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. |

# Serwer pod system ochrony poczty

1 sztuka

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” 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 do 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 jeden procesor min. 16-rdzeniowy, min. 2.9GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 259 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| **RAM** | Minimum 128 GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| **Funkcjonalność pamięci RAM** | Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing |
| **Gniazda PCI** | - minimum jeden sloy PCIe x16 |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (interfejsy nie mogą zajmować gniazda PCI) Wbudowane 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (interfejsy nie mogą zajmować gniazda PCI). Porty obsadzone modułami 10Gb/s SFP+ SR.  Serwer wyposażony w 2 światłowody OM3 LC-LC o długości minimum 3metrów. |
| **Dyski twarde** | Możliwość instalacji dysków SAS, SATA, SSD  Zainstalowane 8 dysków SSD vSAS o pojemności min. 960GB, 12Gb, 2,5“ Hot-Plug.  Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.  Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |
| **Wbudowane porty** | 4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim. |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| **Zasilacze** | Redundantne, Hot-Plug min. 800W 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. |
| **System operacyjny** | Windows Server 2022 Standard 16 core – 1 sztuka |
| **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-9001:2015 oraz ISO-14001.  Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019, systemów Microsoft Windows 2022. |
| **Warunki gwarancji** | 36 miesięcy 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.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera |
| **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. |

# System ochrony poczty

**Wymagania ogólne**

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMWare ESX/ESXi 6.0/6.7/7.0, Citrix XenServer v5.6 SP2/6.0, Microsoft Hyper-V Server 2008 R2/2012/2012 R2/2016/2019, KVM qemu 2.12.1, AWS (Amazon Web Services), Microsoft Azure, Google Cloud Platform,

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

**Parametry fizyczne systemu antyspamowego**

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.

**Ogólne funkcje systemu ochrony poczty**

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

**Kontrola antywirusowa i ochrona przed malware**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.
10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w  plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.

**Kontrola antyspamowa**

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)
17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

**Ochrona przed atakami na usługę poczty**

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie  maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

**Funkcje logowania i raportowania**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

**Aktualizacje sygnatur, dostęp do bazy spamu**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

**Zarządzanie**

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

**Certyfikaty**

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

**Serwisy i licencje**

System musi być dostarczony w modelu „na własność” tj. Niewyku pienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta  i serwisów. Powinny one obejmować:

1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 36 miesięcy.

**Gwarancja oraz wsparcie**

1. System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

**Opisy do wymagań ogólnych**

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

# Wdrożenie

**Opis wdrożenie serwera backupu i biblioteki taśmowej:**

* instalacja dostarczonego sprzętu w miejscu wskazanym przez Zamawiającego.
* instalacja i konfiguracja systemu operacyjnego na dostarczonym serwerze pod backup
* konfiguracja biblioteki taśmowej oraz podłączenie jej do dostarczonego serwera pod backup
* Instalacja i konfiguracja na dostarczonym serwerze backupy oprogramowania Veeam Backup and Replication (Zamawiający posiada odpowiednią licencję ze wsparciem)
* Konfiguracja polityk backupu na systemie Veeam z wykonaniem kopii zapasowej na dysk lokalny serwera oraz na bibliotekę taśmową.
* Weryfikacja poprawności działania przez odzyskanie całej maszyny wirtualnej oraz pojedynczego pliku.
* przygotowanie dokumentacji powdrożeniowej
* przeprowadzenie szkolenie powdrożeniowego
* migracja 4 maszyn wirtualnych z obecnie posiadanego klastra VMware ESX 4.1 na serwer pod system ochrony poczty. Maszyny wirtualne zajmują w sumie 1.4 TB.

**Opis wdrożenie systemu ochrony poczty:**

* pobranie oprogramowania i instalacja jako maszyna wirtualna na dostarczonym serwerze pod system ochrony poczty. Licencje VMware ESX dla serwera posiada Zamawiający.
* konfiguracja interfejsów oraz adresacji
* konfiguracja routingu
* konfiguracja czasu
* konfiguracja ustawień głównych takich jak nazwa hosta domena główna
* konfiguracja domeny oraz subdomen
* konfiguracja Anty Spam i Anty Virus
* konfiguracja z blokowaniem plików typu exe
* konfiguracja i podłączenie z AD po LDAP
* Konfiguracja polityk IP
* konfiguracja polityki Recipient
* konfiguracja ograniczenia wielkości plików oraz wielkości wiadomości, czarnych i białych list
* Przegląd konfiguracji przed przepięciem
* Przepięcie ruchu mailowego na nowy system ochrony poczty
* przygotowanie dokumentacji powdrożeniowej
* przeprowadzenie szkolenie powdrożeniowego

**Wymagania dodatkowe dotyczące wdrożenia**

Zamawiający wymaga, żeby firma dostarczające i wdrażająca rozwiązanie posiadała zatrudnionych na etacie inżynierów posiadających następujące certyfikaty techniczne:

* Minimum VMware Certified Professional lub wyższy
* Minimum Veeam VMCE (Veeam Certified Engineer) w wersji min 2020 lub wyższej
* Minimum Fortinet NSE7 lub wyższy

Wymaganie to wynika z posiadanego przez Zamawiającego środowiska.

Szkolenia:

Zamawiający wymaga dostarczenia dwóch voucherów na szkolenia ważnych 12 miesięcy od daty dostarczenia.

Szkolenia muszą być przeprowadzone przez autoryzowane centrum szkoleniowe producenta.

Szkolenia muszą być w formie warsztatów ze znaczną liczbą praktycznych laboratoriów.

Uczestnik szkolenia musi otrzymać certyfikat imienny oraz firmowy.

Szkolenia muszą obywać się w języku polskim.

1. Dwa vouchery na szkolenie minimum dwudniowe po 8h z zarządzania i obsługi urządzeń UTM FortiGate.

Minimalna zawartość szkolenia:

* Produkty - rodzaje, pozycjonowanie, wymiarowanie
* Podstawowe czynności administracyjne

konfiguracja domyślna

update firmware

kopia zapasowa konfiguracji

serwisy licencyjne

* Wstępna konfiguracja

tryby pracy

konfiguracja interfejsów sieciowych

konfiguracja serwera DHCP

dodatkowe ustawienia sieciowe

dostęp administracyjny

* Logowanie - metody logowania i ich praktyczna konfiguracja

FortiAnalyzer

Syslog

pamięć RAM

* Konfiguracja zapory ogniowej - elementy podstawowe

obiekty i grupy

reguły zapory ogniowej

translacja adresów SNAT i DNAT

* Konfiguracja zapory ogniowej - uwierzytelnianie
* metody uwierzytelniania użytkowników

lokalna baza użytkowników

grupy użytkowników

* Routing statyczny

Ping Server

metryka i priorytety

* Zarządzanie zagrożeniami

moduł antywirusowy

moduł antyspamowy

filtrowanie stron WWW

kontrola aplikacj

i moduł IPS i DLP

* Wirtualne Sieci Prywatne VPN

SSL-VPN vs IPSec VPN

konfiguracja tuneli VPN

1. Dwa vouchery na szkolenie minimum dwudniowe po 8h z zarządzania i obsługi urządzeń UTM FortiGate.

Minimalna zawartość szkolenia:

* Routing i Load Balancing

Omówienie metod rozkładania ruchu

Wan-Link-Load-Balacing

Grupowanie interfejsów w Strefy

Potencjalne problemy z NAT

* Inspekcja ruchu SSL:

Zarządzanie certyfikatami

Praktyczna analiza ruchu zabezpieczonego protokołem SSL

Wpływ SSL na pracę modułów bezpieczeństwa

Potencjalne problemy

* High Availability

zasada działania HA

konfiguracja

tryby Active-Pasive vs Active-Active

* VDOMy
* Zaawansowane uwierzytelnianie - FSSO
* IPSec VPN:

konfiguracja topologi Hub-and-Spoke

Rozwiązanie problemu identycznej adresacji sieci lokalnych

* FortiGate jako kontroler sieci bezprzewodowych

1. Dostarczenie dwóch voucherów na autoryzowany egzamin producenta: Fortinet NSE 4 - FortiOS (FortiGate Security and FortiGate Infrastructure).

Vouchery muszą być ważne minimum 12 miesięcy od daty dostarczenia.

*Zatwierdziła*

*p.o. Dyrektora*

*Powiatowego Zespołu Szpitali*

*Agnieszka Cholewińska*