**Załącznik Nr 7: Szczegółowy opis przedmiotu zamówienia / Parametry techniczne**

**– Wykonawca składa wraz z ofertą**

**WARUNKI I PARAMETRY TECHNICZNE WYMAGANE ORAZ OFEROWANE**

# PAKIET NR 1

Przełącznik zarządzalny Warstwy L3 - 4 szt. (CPV: 32424000-1 – Infrastruktura sieciowa)*Wg. wskazanych poniższych funkcji i cech produktu równoważnego:*

Oferujemy model\*: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| podać nazwę, producenta, model, typ. itp. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowanego komponentu\*** |
|  | Warstwa | 3 |  |
|  | Przepustowość | 1,5Tbps |  |
|  | Porty | 48 portów SFP/SFP+/SFP28 1Gbit/10Gbit/25Gbit  8 portów QSFP+/QSFP28 40Gbit/100Gbit  Możliwość zwiększenia ilości portów do 80 portów SFP+ przy zastosowaniu kabli rozdzielających QSFP+-SFP+ – każdy port QSFP+ może być rozdzielony do 4 portów SFP+ |  |
|  | Zarządzanie | Możliwość połączenia co najmniej 2 switchów w STACK za pomocą przewodów DAC o przepustowości minimum 40Gbit lub innych dedykowanych przez producenta danego modelu i utworzenia jednego wirtualnego switcha o ilości dostępnych portów równych sumie wolnych portów każdego ze switchy wchodzących w STACK, z uwzględnieniem zastosowania kabli rozdzielających QSFP+-SFP+ na wszystkich wolnych portach QSFP+.  Dedykowany port RS-232 (lub poprzez dedykowany port RJ-45->RS-232) do zarządzania  Co najmniej 2 porty RJ-45 do zarządzania  przez protokół SSH.  Porty do zarządzania RJ-45 nie mogą być osiągane przez jakiekolwiek przejściówki czy wkładki SFP. |  |
|  | Pozostałe | Wsparcie dla modułów SFP (zarówno optycznych jak i miedzianych)/SFP+/SFP28/QSFP+/QSFP28 oraz kabli DAC  Montaż w szafie RACK. Wysokość switcha 1U.  2 redundantne zasilacze o napięciu zasilania 110V-240V z możliwością wymiany typu HOT-SWAP  Obsługa co najmniej 4092 Vlanów  Możliwość tworzenia agregacji portów pomiędzy dwoma urządzeniami pracującymi w STACKu ze wsparciem dla protokołu LACP  Obsługa Multiple Spanning Tree Protocol MSTP (lub odpowiednik producenta) (co najmniej 64 instancje) oraz VLAN Spanning Tree Protocol VSTP (lub odpowiednik producenta) (co najmniej 500 instancji)  Pamięć co najmniej 200 000 adresów MAC  Możliwość przypisywania adresów MAC do konkretnych interfejsów  Możliwość tworzenia statycznych tras routingu w warstwie 3 (Layer 3)  Wsparcie dla protokołów routingu: RIP, OSPF, BGP  Wsparcie dla QoS zarówno w warstwie 2 (Layer 2) oraz w warstwie 3 (Layer 3)  Wsparcie dla SNMP v1/v2/v3  Wsparcie dla standardów: IEEE 802.1D, IEEE 802.1w, IEEE 802.1, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1ad, IEEE 802.3ad, IEEE 802.1AB, IEEE 802.3x, IEEE 802.1Qbb, IEEE 802.1Qaz |  |
|  | Warunki gwarancji | 36-miesięczna gwarancja producenta świadczona na miejscu u klienta na zasadzie Next Business Day w trybie 24/7. W ramach gwarancji możliwa wymiana uszkodzonego urządzenia, dostęp do pomocy ze strony inżynierów producenta, aktualizacji, bazy danych producenta |  |
|  | Istniejące infrastruktura | Oferowane urządzenia muszą mieć możliwość dołączenia do już posiadanego przez Zamawiającego STACKA składającego się z dwóch switchy Juniper EX-4650. W przypadku zaoferowania urządzenia innego producenta lub innego modelu tego samego producenta, należy dostarczyć oświadczenie producenta posiadanych przez zamawiającego switchy Juniper EX-4650 że będzie możliwość dołączenia oferowanych switchy to posiadanego przez zamawiającego STACKA i zachowana zostanie pełna funkcjonalność STACKA. |  |

Moduły przekaźników sieciowych, kable DAC (CPV: 32424000-1 – Infrastruktura sieciowa)*Wg. wskazanych poniższych funkcji i cech produktu równoważnego:*

Oferujemy model\*: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| podać nazwę, producenta, model, typ. itp. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Liczba sztuk** | **Wymagane minimalne parametry techniczne** | **Parametry oferowanego komponentu\*** |
| **Wtyki** | | | |
|  | 4 | Kabel DAC o długości minimum 50 cm maksimum 1 metra 100Gbit kompatybilny ze przełącznikiem Warstwy L3 z niniejszej specyfikacji |  |
|  | 4 | Kabel DAC o długości minimum 50 cm maksimum 1 metra 40Gbit kompatybilny z jednej strony z przełącznikiem warstwy L3 z niniejszej specyfikacji oraz z drugiej strony z przełącznikiem Juniper EX4600 |  |
|  | 62 | 10Gbit SFP+ Single Mode Duplex minimum 10km kompatybilne ze przełącznikiem Warstwy L3 z niniejszej specyfikacji |  |
|  | 130 | 10Gbit SFP+ Multi Mode minimum 300m kompatybilne ze przełącznikiem Warstwy L3 z niniejszej specyfikacji |  |

# PAKIET NR 2

Oprogramowanie – System ochrony poczty (licencja na 3 lata) wraz z wdrożeniem*Wg. wskazanych poniższych funkcji i cech produktu równoważnego:*

Oferujemy model\*: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| podać nazwę, producenta, model, typ. itp. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowanego komponentu\*** |
|  | 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 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.  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 | System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 2 TB. |  |
|  | Ogólne funkcje systemu ochrony poczty | Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:  1. Wsparcie dla co najmniej 70 domen pocztowych.  2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 50 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. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention).  18. 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 200 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 200 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. |  |
|  | Funkcje pracy w trybie wysokiej dostępności (HA) | System ochrony poczty musi zapewniać poniższe funkcje:  1. Konfigurację HA w każdym z trybów: gateway, transparent.  2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.  3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.  4. Monitorowanie stanu pracy klastra.  5. W ramach postępowania wymaganym jest dostarczenie systemu w formie klastra realizującego funkcje podstawowe, gdzie każdy jego element charakteryzuje się parametrami fizycznymi i funkcjonalnymi opisanymi w tym dokumencie. |  |
|  | 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 3 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. niewykupienie 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 | System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. |  |
|  | Opisy do wymagań ogólnych | Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. |  |
|  | Wdrożenie | W ramach wdrożenia wykonawca zainstaluje oraz skonfiguruje zamawiany produkt zgodnie z najlepszymi praktykami oraz zaleceniami producenta.  W ramach wdrożenia zostanie również przeprowadzenie szkolenie administracyjne co najmniej 2 pracowników zamawiającego, trwające minimum 8 godzin.  W ramach szkolenia wybrani pracownicy zamawiającego zostaną przeszkoleni z konfiguracji, aktualizacji, backupu oraz konserwacji zakupionego rozwiązania.  Szkolenie może odbywać się w formie zdalnej za pomocą aplikacji typu Teams, Zooms |  |

# Wykonawca składa przedmiotowy załącznik wraz z ofertą.

**Brak złożenia przedmiotowego Załącznika skutkuje odrzuceniem oferty z postępowania.**

* 1. UWAGA: Ilekroć w dokumentacji, wskazano markę lub pochodzenie produktu lub urządzenia, należy przyjąć, że za każdą nazwą jest umieszczone słowo „lub równoważne”, tzn. że wbudowane materiały, urządzenia itp. będą posiadały (charakteryzowały się) wszystkimi parametrami nie gorszymi niż opisane w niniejszej dokumentacji, **dla danej pozycji.**
  2. **Jeżeli w opisie przedmiotu zamówienia wskazane są konkretne rozwiązania techniczne, dopuszcza się stosowanie rozwiązań równoważnych, co do ich cech i parametrów – określonych dla danej pozycji przedmiotu zamówienia, a wszystkie ewentualne nazwy firmowe urządzeń i wyrobów użyte w opisie przedmiotu zamówienia powinny być traktowane jako definicje standardowe, a nie konkretne nazwy firmowe urządzeń, wyrobów zastosowanych w niniejszej dokumentacji. Obowiązek udowodnienia równoważności leży po stronie Wykonawcy**.