OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu komputerowego

CZĘŚĆ I Sprzęt sieciowy (Wymagania minimalne)

1	**Wkładki do przełączników Aruba – 50 szt.**	
	1	Dostawa do posiadanych przełączników (HP Switch 5406Rzl2 (J9850A)) wkładek światłowodowych „Aruba 10G SFP+ LC SR 300 mm MMF XCVR (J9150D)" **lub równoważnych** charakteryzujących się łącznie: - wszystkimi cechami wkładek „Aruba 10G SFP+ LC SR 300 mm MMF XCVR (J9150D), - „dożywotnią gwarancją" jakiej udziela producent na oryginalne wkładki „Aruba 10G SFP+ LC SR 300 mm MMF XCVR (J9150D)" stosowane do przełączników (HP Switch 5406Rzl2 (J9850A), - moduły SFP+ zaoferowane przez Wykonawcę które będą częścią składową urządzenia sieciowego (HP Switch 5406Rzl2 (J9850A)) muszą być objęte wsparciem serwisowym producenta dla tego urządzenia i przejmować jego wsparcie (https://support.hpe.com/hpesc/public/docDisplay?cc=uk&docId=emr_na-c02707631&lang=en-uk). - dla wkładki równoważnej zaoferowanej przez Wykonawcę wykorzystywanej w przełączniku Aruba (HP Switch 5406Rzl2 (J9850A)) wsparcie techniczne świadczone przez producenta dla tych przełączników nie może zostać zakwestionowane przez producenta przełącznika z uwagi na wykorzystanie wkładki równoważnej.
2	**Kable światłowodowe – 30 szt.**	
	1	Dostawa kabli światłowodowych LC-LC 50/125 OM3 MM duplex 7 m
3	**Licencje do serwerów HPE iLO – 3 szt.**	
	1	Dostawa licencji ILO Adwanced 3 lata do posiadanych 3 serwerów HPE DL 380 Gen 10 (BD505A)
4	**Maskownica do serwera – 3 szt.**	
	1	Dostawa maskownicy do 3 serwerów HPE DL 380 Gen 10 (HPE Gen10 2U Bezel Kit) P/N:(858790-001)
5	**Klaster urządzeń antyspamowych – 2 szt. (urządzenia)**	
	1	**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 były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
		Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o dedykowany system operacyjny oraz komercyjne bazy zabezpieczeń.
	2	**Parametry Fizyczne:**
		System musi być wyposażony w min 4 interfejsy Gigabit Ethernet RJ-45
		System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB - w przypadku awarii dysk twardy pozostaje u Zamawiającego.
		System musi posiadać wbudowany port konsoli szeregowej.
		Zasilanie z sieci 230V/50Hz.
	3	**Ochrona poczty:**

OPIS PRZEDMIOTU ZAMÓWIENIA
Dostawa sprzętu komputerowego
CZĘŚĆ I Sprzęt sieciowy (Wymagania minimalne)

		Wsparcie dla co najmniej 20 domen pocztowych
		System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 28 tys. wiadomości/godzinę.
		Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
		Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
		Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
		Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
		Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
		Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
		Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
		Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz POP3,
		Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
		Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
		Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
		Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
		Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
	4	**Kontrola antywirusowa i ochrona przed malware:**
		Skanowanie antywirusowe wiadomości SMTP.
		Kwarantanna dla zainfekowanych plików.
		Skanowanie załączników skompresowanych.
		Definiowanie komunikatów powiadomień w języku polskim.
		Blokowanie załączników w oparciu o typ pliku.
		Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
		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.
		Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu komputerowego

CZĘŚĆ I Sprzęt sieciowy (Wymagania minimalne)

	nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
	Ochronę typu wirus outbrake.
	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.
5	**Kontrola antyspam:**
	Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
	Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
	Szczegółowa kontrola nagłówka wiadomości.
	Analiza heurystyczna.
	Współpraca z zewnętrznymi serwerami RBL, SURBL.
	Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen.
	Możliwość dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
	Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
	Kontrola w oparciu o Greylisting oraz SPF.
	Filtrowanie treści wiadomości i załączników.
	Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
	Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
	Ochrona typu outbrake.
	Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
	Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
	Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)
	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.
6	**Ochrona przed atakami na usługę poczty:**
	Ochrona przed atakami na adres odbiorcy.
	Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
	Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
	Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
	Weryfikacja poprawności adresu e-mail nadawcy.

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu komputerowego

CZĘŚĆ I Sprzęt sieciowy (Wymagania minimalne)

7	**Funkcje dodatkowe:**
	Funkcje logowania i raportowania: 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): 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.
	Aktualizacje sygnatur, dostęp do bazy spamu: 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.
8	**Zarządzanie:**
	System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
	Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
	Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.
9	**Certyfikaty:**
	Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji: VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.
10	**Serwisy i Licencje:**
	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować co najmniej:
	Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake na okres 36 miesięcy.
	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.
11	**Gwarancja oraz wsparcie:**

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu komputerowego

CZĘŚĆ I Sprzęt sieciowy (Wymagania minimalne)

	System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości oraz objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy w następnym dniu roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
	Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.
	Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5.
	Oferent winien przedłożyć dokumenty przy dostawie:
	Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
12	**Wdrożenie:**
	Czynności w ramach usługi wdrożenia Systemu: 1. Instalacja i Konfiguracja przez Wykonawcę urządzeń służących do budowy całości Klastra urządzeń antyspamowych, przygotowanie i przeprowadzenie testów poprzedzających Odbiór jakościowy poszczególnych urządzeń, wdrożenie Systemu; 2. uruchomienie Systemu w Lokalizacji przez Wykonawcę; 3. wykonanie i przekazanie przez Wykonawcę Dokumentacji Powdrożeniowej i przeniesienie na rzecz Zamawiającego majątkowych praw autorskich do tej Dokumentacji w zakresie określonym Umową; 4. Instalacja i Konfiguracja Systemu w Lokalizacji przez Wykonawcę; 5. sprawdzenie funkcjonalności przez Wykonawcę; 6. zatwierdzenie powyższych czynności Protokołem Odbioru;
	1. Dokumentacja musi zawierać szczegółowy opis techniczny zaimplementowanego rozwiązania z opisem uruchomionych funkcjonalności. 2. Dokumentacja techniczna będzie stanowiła dokument na podstawie którego będzie możliwe odbudowanie architektury zaimplementowanego rozwiązania. 3. Dokumentacja techniczna będzie zawierała: 1) przedstawienie ogólnej architektury systemu. 2) ogólną architekturę wdrożenia, 3) wykorzystywane mechanizmy redundancji 4) przedstawienie szczegółowej architektury z konfiguracją redundancji (sposób pracy, komunikacja pomiędzy elementami klastra, zarządzenia i monitorowanie klastra urządzeń)
13	**Szkolenia:**

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu komputerowego

CZĘŚĆ I Sprzęt sieciowy (Wymagania minimalne)

		Wykonawca jest zobowiązany do dostarczenia w formie voucherów szkoleniowych szkolenia podstawowego autoryzowanego przez producenta dostarczonych urządzeń szkolenia dla trzech administratorów Zamawiającego. Szkolenia zostaną zrealizowane przez autoryzowany przez producenta dostarczanych Urządzeń podmiot szkoleniowy. Szkolenia zostaną przeprowadzone w języku polskim. Czas ważności voucherów nie może być krótszy niż 6 miesięcy od dnia wdrożenia Systemu. Przekazanie voucherów musi nastąpić nie później niż wdrożenie Systemu.
6		**Moduł dystrybucji zasilania (PDU) do montażu w szafie 19" wraz z czujnikiem monitorującym temperaturę – 2 szt.**
	1	Przeznaczony do montażu w szafie 19”:
		Możliwość montażu pionowo (ZeroU) i beznarzędziowo;
		Nominalne napięcie wejściowe: 200V, 208V, 230V;
		Częstotliwość na wejściu: 50/60 Hz;
		Typ elektrycznego wtyku wejściowego: IEC-320 C20;
		Maksymalny całkowity prąd wejściowy: 16A;
		Napięcie wyjściowe: 200V, 208V, 230V AC;
		Gniazda elektryczne wyjściowe: 21 x IEC-320 C13, 3 x IEC-320 C19 z blokadami wyposażone w niskoprofilowe wyłączniki automatyczne;
		Sygnalizacja za pomocą diody LED wykorzystania każdego z gniazd wyjściowych;
		Wskaźnik obciążenia LED wskazujący status całkowitego obciążenia listwy PDU na podstawie zdefiniowanych przez użytkownika progów alarmowych;
		Lokalny wyświetlacz umożliwiający monitorowanie poboru mocy;.
		Port 10/100 Base-T do zdalnego zarządzania listwą poprzez sieć TCP/IP;
		Obsługa protokołów IPv4 oraz IPv6;
		Obsługa protokołów DHCP i BOOTP;
		Obsługa Network Time Protocol (NTP);
		Możliwość definiowania reguł dla firewall’a;
		Port RJ-12 (wraz z potrzebnym przewodem) zapewniający dostęp lokalny za pomocą tekstowego terminalu szeregowego;
		Sonda do monitorowania wilgotności i temperatury w szafie podłączana do listwy PDU poprzez port monitorowania parametrów środowiskowych;
		Możliwość aktualizacji oprogramowania sprzętowego znajdującego się w pamięci flash listwy PDU poprzez sieć TCP/IP oaz wbudowany port USB (flash driver);
		Wbudowany port In/Out zapewniający sterowanie urządzeń poprzez oprogramowanie zarządzające;
		Obsługa Network Port Sharing (NPS);
		Możliwość zarządzania przez sieć za pomocą w pełni funkcjonalnych sieciowych interfejsów zarządzania, które umożliwiają zarządzanie w oparciu o standardy WWW, SNMP i Telnet. Umożliwiające użytkownikom uzyskiwanie zdalnego dostępu do urządzenia, konfigurowanie go i zarządzanie nim;

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu komputerowego

CZĘŚĆ I Sprzęt sieciowy (Wymagania minimalne)

	Zdalna kontrola pojedynczych wyjść umożliwiająca odłączenie wybranych, nieużywanych wyjść (zapobieganie przeciążeniu) lub załączenia zasilania dla Zamkniętego sprzętu (minimalizacja przestojów i eliminacja konieczności podejścia do sprzętu);
	Pomiar prądu zapewniający zdalne, realizowane w czasie rzeczywistym monitorowanie podłączonych obciążeń;
	Pomiar: mocy czynnej, mocy chwilowej, mocy biernej, energii, współczynnika mocy;
	Możliwość ustawienia wartości, przy których uruchamiany jest alarm (w celu uniknięcia przeciążenia obwodów) poprzez zdefiniowanie progów.
	Alarmy sieciowe i wizualne powinny informować użytkownika o potencjalnych problemach;
	Programowalne opóźnienie zasilania zapewniające użytkownikom możliwość skonfigurowania kolejności włączania i wyłączania zasilania na poszczególnych wyjściach w celu uniknięcia kumulacji momentu rozruchowego przy starcie urządzeń, który może być przyczyną przeciążenia obwodu i odłączenie obciążeń oraz zapewniające możliwości ustalania kolejności włączania sprzętu, tak by inne zależne od niego urządzenia mogły działać prawidłowo.
	Możliwość grupowania i wspólnego zarządzania wyjściami (również przy zastosowaniu kilku modułów PDU);
	Możliwość konfiguracji harmonogramu zdarzeń (jednorazowych, dziennych, tygodniowych);
	Możliwość tworzenia użytkowników oraz przypisania im różnych praw do sterowania poszczególnymi wyjściami,
	Logowanie zdarzeń, danych oraz firewall'a;
	Kopiowanie logów na zdalny komputer przy pomocy protokołów ftp lub scp;
	Informowanie o zdarzeniach poprzez e-mail;
	Szyfrowane połączenie przy logowaniu zdalnym;
	Możliwość zapisania i odtworzenia konfiguracji do / z pliku zewnętrznego;
	Przycisk reset listwy PDU;
	Maksymalna wysokość: 1830.00 mm;
	Czujnik uniwersalny, który monitoruje temperaturę w centrum danych lub pomieszczeniu sieciowym.
	Gwarancja producenta na bezawaryjne funkcjonowanie urządzenia na okres co najmniej 12 miesięcy na miejscu u Zamawiającego. Serwis urządzeń musi być realizowany przez Producenta lub przez Autoryzowanego Partnera Serwisowego Producenta