Załącznik nr 4 do Zapytania ofertowego

Wymagania postawione w niniejszym opisie są wymaganiami minimalnymi (chyba że wskazano inaczej).

I. Zamawiający dostarczy identyczne - 2 szt (2 komplety) – fabrycznie nowe urządzenia typu NAS zapewniające konfigurację RAID 10 **wraz z minimum 6 dyskami o pojemności 20TB każdy klasy Enterprise.**

Urządzenie oraz dyski muszą być ze sobą kompatybilne. Dyski muszą być ze wsparciem producenta rozwiązania NAS. Urządzenie musi być dodatkowo wyposażone w przesuwne szyny rack oraz posiadać możliwość rozbudowy zgodnie z poniższym zestawieniem.

Zamawiający wymaga:

1. dostarczenia przez wykonawcę sprzętu na własny koszt i ryzyko wraz z jego wniesieniem w miejsce wskazane przez zamawiającego, tj. do siedziby Gminy Dębowa Łąka, Dębowa Łąka 38, 87-207 Dębowa Łąka,
2. przekazania zamawiającemu sprzętu na podstawie protokołu odbioru; protokół odbioru sporządzi wykonawca i przedstawi go do podpisu zamawiającemu po wykonanej dostawie.
3. Jeżeli w czasie odbioru jakościowego jakikolwiek sprzęt wybrany do odbioru jakościowego nie będzie działał poprawnie lub nie spełni wymagań konfiguracyjnych, cała partia przeznaczona do odbioru jakościowego zostanie zwrócona wykonawcy, a cała procedura odbioru zostanie powtórzona od początku.

Uwaga: W ramach procedury odbioru zamawiający zastrzega sobie prawo weryfikacji czy oprogramowanie i powiązane z nim elementy, takie jak certyfikaty/etykiety producenta oprogramowania dołączone do oprogramowania są oryginalne i licencjonowane zgodnie z prawem. W powyższym celu zamawiający może zwrócić się do przedstawicieli producenta danego oprogramowania z prośbą o weryfikację czy oferowane oprogramowanie i materiały do niego dołączone są oryginalne. W przypadku identyfikacji nielicencjonowanego lub podrobionego oprogramowania lub jego elementów, Zamawiający odstąpi od odbioru dostarczonego Sprzętu. Ponadto, powyższe informacje zostaną przekazane właściwym organom w celu wszczęcia stosownych postępowań

4. Dostarczany sprzęt musi być kompletny, oryginalny. W szczególności mieć okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie.
5. Dostarczany sprzęt powinien być przystosowany fabrycznie do zasilania z sieci energetycznej dostępnej w Polsce i wyposażone w obowiązującą w tym kraju wtyczkę sieciową. Nie dopuszcza się stosowania przejściówek/konektorów.
6. Sprzęt musi posiadać atesty oraz spełniać normy dopuszczające do obrotu, wymagane prawem polskim i UE.
7. Zamawiający nie dopuszcza sprzętu poleasingowego. Wymagana jest dostawa sprzętu fabrycznie nowego, nieużywanego, wolnego od obciążeń prawami osób trzecich, posiadających dołączone, niezbędne instrukcje i materiały dotyczące użytkowania w języku polskim wraz z niezbędnym wyposażeniem producenta.
8. Wszystkie wymagania określone w dokumentach stanowią wymagania minimalne, a ich spełnienie jest obligatoryjne. Niespełnienie ww. wymagań minimalnych będzie

skutkować odrzuceniem oferty.

Minimalne wymagania/parametry:

Typ urządzenia	Serwer NAS
Obudowa	Rack
Procesor	Czterordzeniowy procesor o taktowaniu 3,35 GHz (z przyspieszeniem do 3.6 GHz)
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 32 GB pamięci ECC UDIMM
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 12 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 24 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą gniazda rozszerze.
Porty zewnętrzne	Minimum: • 2 porty USB 3.2.1 • 1 gniazdo rozszerzenia
Porty sieciowe	Minimum: • 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) • 1 port 10GbE RJ45 **Dodatkowo urządzenie musi być wyposażone w dwa porty SFP+**
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 3.0	Min. 1x 4-liniowe gniazdo x8 Gen. 3
Wentylator obudowy	Min. 3 wentylatory 60 mm x 60 mm
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT

Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu:
	  ○ 200 TB (wymagana pamięć 32 GB)
	  ○ 108 TB
	• Minimalny liczba wewnętrznych wolumenów: 64
	• Minimalny liczba obiektów iSCSI Target: 128
	• Minimalny liczba jednostek iSCSI LUN: 256
	• Obsługa klonowania/migawek jednostek iSCSI LUN

Obsługiwane typy macierzy RAID	Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6,

	RAID 10
Funkcja udostępniania plików	• Minimalna liczba kont użytkowników: 2 048 • Minimalna liczba grup użytkowników: 256 • Minimalna liczba folderów współdzielonych: 512 • Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 2 000
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń.
Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane przeglądarki	Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach
Oprogramowanie	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać

	udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. • Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Konserwacja	• Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack
Zasilanie	• Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz
Gwarancja	Wykonawca udzieli gwarancji: • 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack • 3 lata na urządzenie główne (gwarancja producenta standardowa)
Inne	• wymagana certyfikacja ISO 9001:2015 dla obsługi serwisowej • wymagany certyfikat potwierdzający gwarancję producenta • Wykonawca dostarczy wszystkie niezbędne do podłączenia okablowanie oraz wkładki.

II. Oprogramowanie oraz wdrożenie typu DLP (Data Loss Prevention)

1. Zamawiający wymaga:
   1) dostarczenia przez wykonawcę licencji i oprogramowania na własny koszt i ryzyko wraz z jego wniesieniem w miejsce wskazane przez Zamawiającego, tj. do siedziby Gminy Dębowa Łąka, Dębowa Łąka 38, 87-207 Dębowa Łąka,
   2) dostarczenie wraz z kluczami aktywacyjnymi oprogramowania oraz dokumentów potwierdzających udzielenie licencji, w tym certyfikaty legalności oprogramowania. Licencje, o których mowa, są niewyłączne i nieograniczone czasowo,
   3) przekazania zamawiającemu licencji na podstawie protokołu odbioru; protokół odbioru sporządzi wykonawca i przedstawi go do podpisu zamawiającemu po wykonanej dostawie.
2. Dostarczane licencje, oprogramowanie musi być kompletne, zapewniające właściwą instalację i użytkowanie.
3. Wymagana jest dostawa licencji fabrycznie nowych, nieużywanych, wolnych od obciążeń prawami osób trzecich.
4. W ramach procedury odbioru zamawiający zastrzega sobie prawo weryfikacji czy oprogramowanie i powiązane z nim elementy, takie jak certyfikaty/etykiety producenta oprogramowania dołączone do oprogramowania są oryginalne i licencjonowane zgodnie z prawem. W powyższym celu zamawiający może zwrócić się do przedstawicieli producenta danego oprogramowania z prośbą o weryfikację czy oferowane oprogramowanie i materiały do niego dołączone są oryginalne. W przypadku identyfikacji nielicencjonowanego lub podrobionego oprogramowania lub jego elementów, Zamawiający odstąpi od odbioru dostarczonego oprogramowania. Ponadto, powyższe informacje zostaną przekazane właściwym organom w celu wszczęcia stosownych postępowań

Minimalne wymagania oprogramowania

1. Obsługa Systemów operacyjnych
   a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
   b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
   c. MacOS 12 lub nowszy.
2. Licencja wieczysta dla 35 użytkowników
3. Serwer administracyjny musi obsługiwać instalację na systemach Windows Server 2016
4. (64-bit) i nowszych.
   a. Serwer administracyjny musi obsługiwać bazy danych: MS SQL Server 2016 lub nowsze, MS SQL Express, AzureSQL, S3 lub nowsze.
5. Pomoc i dokumentacja programu dostępne w języku angielskim.
6. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.

7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
8. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na
9. stacjach roboczych.
10. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
11. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
12. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
13. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy
14. danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.
15. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
16. Administrator musi mieć możliwość, aby tworzyć, usuwać konta administratorów w konsoli programu.
17. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
18. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
19. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
20. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
21. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia,
22. odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.
23. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
24. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
25. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
26. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
27. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
28. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
29. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
30. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie

komunikatorami itp.

31. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.
32. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
33. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
34. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
35. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
36. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.
37. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft
38. SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
39. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach
40. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.)
41. System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych.

Wymagania Dodatkowe

- Wykonawca musi posiadać doświadczenie we wdrożeniach systemów DLP. Wymagane jest przedłożenie dokumentów potwierdzające takie wdrożenie - **wraz z ofertą.**
- Zapewnienie wsparcia technicznego przez minimum 12 miesięcy po wdrożeniu.
- Wszystkie prace muszą być wykonane zgodnie z najlepszymi praktykami bezpieczeństwa.

Zakres Prac

- Dostawa i instalacja systemu DLP
- Konfiguracja oprogramowania i instalacja do 40 użytkowników
- Integracja systemu z istniejącą infrastrukturą IT.
- Przeprowadzenie testów akceptacyjnych.

Kryteria Akceptacji

- System działa zgodnie z wymaganiami określonymi w OPZ.
- Wszystkie ustawione polityki działają prawidłowo
- Funkcjonalności DLP są w pełni operacyjne.
- Przeszkolenie pracownika Zamawiającego.
- Dostarczenie kompletnej dokumentacji powykonawczej.

III. Oprogramowanie oraz wdrożenie typu SIEM (Security Information and Event Management)

1. Zamawiający wymaga:
1) dostarczenia przez wykonawcę niezbędnych licencji i oprogramowania na własny koszt i ryzyko wraz z jego wniesieniem w miejsce wskazane przez Zamawiającego, tj. do siedziby Gminy Dębowa Łąka, Dębowa Łąka 38, 87-207 Dębowa Łąka,
   2) dostarczenie wraz z kluczami aktywacyjnymi oprogramowania oraz dokumentów potwierdzających udzielenie licencji, w tym certyfikaty legalności oprogramowania. Licencje, o których mowa, są niewyłączne i nieograniczone czasowo,
   3) przekazania zamawiającemu licencji na podstawie protokołu odbioru; protokół odbioru sporządzi wykonawca i przedstawi go do podpisu zamawiającemu po wykonanej dostawie.
2. Dostarczane licencje, oprogramowanie musi być kompletne, zapewniające właściwą instalację i użytkowanie.
3. Wymagana jest dostawa licencji fabrycznie nowych, nieużywanych, wolnych od obciążeń prawami osób trzecich.
4. W ramach procedury odbioru zamawiający zastrzega sobie prawo weryfikacji czy oprogramowanie i powiązane z nim elementy, takie jak certyfikaty/etykiety producenta oprogramowania dołączone do oprogramowania są oryginalne i licencjonowane zgodnie z prawem. W powyższym celu zamawiający może zwrócić się do przedstawicieli producenta danego oprogramowania z prośbą o weryfikację czy oferowane oprogramowanie i materiały do niego dołączone są oryginalne. W przypadku identyfikacji nielicencjonowanego lub podrobionego oprogramowania lub jego elementów, Zamawiający odstąpi od odbioru dostarczonego oprogramowania. Ponadto, powyższe informacje zostaną przekazane właściwym organom w celu wszczęcia stosownych postępowań

System ma zapewnić zaawansowane funkcje monitorowania, analizy i reagowania na incydenty bezpieczeństwa w środowisku IT, obejmującym do 10 dekoderów.
W szczególności

- Zapewnienie kompleksowego systemu monitorowania bezpieczeństwa informacji.
- Wykrywanie i analiza zagrożeń w czasie rzeczywistym.
- Szybkie reagowanie na incydenty bezpieczeństwa.
- Zwiększenie poziomu ochrony infrastruktury IT Zamawiającego.

Wymagania Techniczne

- Monitorowanie w czasie rzeczywistym.
- Możliwość instalacji agenta na systemach Linux, Windows, macOS, AIX, HP-UX.
- Automatyczna rejestracja agenta w systemie.

- Możliwość wdrożenia rozproszonej architektury (Skalowalność).
- Możliwość instalacji środowiska na systemach typu Linux - wolny system operacyjny.
- Zarządzanie podatnościami
- Zarządzanie zgodnością
- Wsparcie dla bez agentowej i agentowej architektury
- Monitorowanie kontenerów
- Automatyzacja zadań i reagowania na incydenty bezpieczeństwa.
- Monitorowanie integralności plików.
- Implementacja najnowszej stabilnej wersji oferowanego systemu SIEM .
- Nielimitowana ilość indeksowanych danych dziennie.
- Nielimitowana liczba użytkowników.
- Nielimitowana ilość punktów końcowych.
- Możliwość skalowania systemu w przyszłości.

Wymagania Funkcjonalne

- System musi umożliwiać real-time monitoring i alertowanie.
- Zapewnienie mechanizmów korelacji zdarzeń.
- Możliwość tworzenia niestandardowych reguł detekcji.
- Integracja z systemami powiadamiania (e-mail, SMS).
- Możliwość wdrożenia wysokiej dostępności, bez zmiany licencji.
- Konfiguracja dekoderów do zbierania i analizy logów z różnych źródeł.
- Integracja z istniejącymi systemami i urządzeniami sieciowymi.
- Zapewnienie kompatybilności z różnymi formatami logów.
- Optymalizacja wydajności dekoderów.
- Zapewnienie dashboardów i raportów dostosowanych do potrzeb Zamawiającego.
- Wdrożenie funkcjonalności Endpoint Detection and Response.

Kryteria Akceptacji

- System działa zgodnie z wymaganiami określonymi w OPZ.
- Wszystkie dekodery poprawnie zbierają i analizują logi.
- Funkcjonalności EDR (Endpoint Detection and Response) są w pełni operacyjne.
- Przeszkolenie pracownika Zamawiającego.
- Dostarczenie kompletnej dokumentacji powykonawczej.
- Dostarczone zostanie wieczyste oprogramowanie. Nie dopuszcza się dodatkowych subskrypcji, opłat abonamentowych za działanie systemu.

Wymagania Dodatkowe

- Wykonawca musi posiadać doświadczenie we wdrożeniach systemów SIEM. Wymagane jest przedłożenie dokumentów potwierdzające wykonanie takiego wdrożenia.
- Zapewnienie wsparcia technicznego przez minimum 18 miesięcy po wdrożeniu.
- Wszystkie prace muszą być wykonane zgodnie z najlepszymi praktykami bezpieczeństwa.

Zakres Prac

- Dostawa i instalacja systemu SIEM wraz z komponentem EDR.
- Konfiguracja do 10 dekoderów w środowisku Zamawiającego.
- Integracja systemu z istniejącą infrastrukturą IT.
- Przeprowadzenie testów akceptacyjnych.
- Dostarczenie kompletnej dokumentacji powykonawczej.

IV. Segmentacja sieci LAN, zabezpieczenie sieci wraz z dostawą niezbędnych urządzeń oraz audyt wraz z niezbędnymi poprawkami

Zamawiający wymaga:

1. dostarczenia przez wykonawcę sprzętu, licencji (gdy dotyczy) na własny koszt i ryzyko wraz z jego wniesieniem w miejsce wskazane przez zamawiającego, tj. do siedziby Gminy Dębowa Łąka, Dębowa Łąka 38, 87-207 Dębowa Łąka,
2. przekazania zamawiającemu sprzętu na podstawie protokołu odbioru; protokół odbioru sporządzi wykonawca i przedstawi go do podpisu zamawiającemu po wykonanej dostawie.
3. Jeżeli w czasie odbioru jakościowego jakikolwiek sprzęt wybrany do odbioru jakościowego nie będzie działał poprawnie lub nie spełni wymagań konfiguracyjnych, cała partia przeznaczona do odbioru jakościowego zostanie zwrócona wykonawcy, a cała procedura odbioru zostanie powtórzona od początku.

Uwaga: W ramach procedury odbioru zamawiający zastrzega sobie prawo weryfikacji czy oprogramowanie i powiązane z nim elementy, takie jak certyfikaty/etykiety producenta oprogramowania dołączone do oprogramowania są oryginalne i licencjonowane zgodnie z prawem. W powyższym celu zamawiający może zwrócić się do przedstawicieli producenta danego oprogramowania z prośbą o weryfikację czy oferowane oprogramowanie i materiały do niego dołączone są oryginalne. W przypadku identyfikacji nielicencjonowanego lub podrobionego oprogramowania lub jego elementów, Zamawiający odstąpi od odbioru dostarczonego Sprzętu. Ponadto, powyższe informacje zostaną przekazane właściwym organom w celu wszczęcia stosownych postępowań

4. Dostarczany sprzęt musi być kompletny, oryginalny. W szczególności mieć okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie.
5. Dostarczany sprzęt powinien być przystosowany fabrycznie do zasilania z sieci energetycznej dostępnej w Polsce i wyposażone w obowiązującą w tym kraju wtyczkę sieciową. Nie dopuszcza się stosowania przejściówek/konektorów.
6. Sprzęt musi posiadać atesty oraz spełniać normy dopuszczające do obrotu, wymagane prawem polskim i UE.
7. Zamawiający nie dopuszcza sprzętu poleasingowego. Wymagana jest dostawa sprzętu fabrycznie nowego, nieużywanego, wolnego od obciążeń prawami osób trzecich, posiadających dołączone, niezbędne instrukcje i materiały dotyczące użytkowania w języku polskim wraz z niezbędnym wyposażeniem producenta.
8. Wszystkie wymagania określone w dokumentach stanowią wymagania minimalne, a ich spełnienie jest obligatoryjne. Niespełnienie ww. wymagań minimalnych będzie skutkować odrzuceniem oferty.

Zakres prac

1. Audyt znajdującego się u zamawiającego firewall typu Fortigate 60F z poprawkami według ogólnie przyjętych norm bezpieczeństwa
2. Segmentacja sieci na vlan – ogółem 5 VLANów. Przygotowanie odpowiednich reguł z ograniczonych dostępem.
3. Dostarczenie dwóch przełączników sieciowych o parametrach

- Cechy zarządzania
- Typ przełącznika Zarządzany
- Przełącznik wielowarstwowy L2/L3
- Obsługa jakość serwisu (QoS) Tak
- Zarządzany w chmurze Tak
- Zarządzanie przez stronę www Tak
- Inspekcja ARP Tak
- Konfigurowanie ustawień lokalizacji (CLI) Tak
- Obsługa MIB Y
- Porty i interfejsyPodstawowe przełączanie RJ-45 Liczba portów Ethernet 48
- Podstawowe przełączania Ethernet RJ-45 porty typ Gigabit Ethernet (10/100/1000)
- Ilość slotów Modułu SFP+ 4
- Liczba portów USB 2.0
- Sieć
- Standardy komunikacyjne
- IEEE 802.1D, IEEE 802.1Q, IEEE 802.1ad, IEEE 802.1af, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3u
- Dublowanie portów Tak
- Blokowanie head-of-line (HOL) Tak
- Prędkość transferu danych przez Ethernet LAN 1000 Mbit/s
- Protokół drzewa rozpinającego Tak
- Automatyczne MDI/MDI-X Tak
- Kontrola wzrostu natężenia ruchu Tak
- Podpora kontroli przepływu Tak
- Obsługa sieci VLAN Tak
- Liczba VLANs 255
- Przesyłanie danych
- Wielkość tabeli adresów 8000 wejścia
- Zgodny z Jumbo Frames Tak
- Rozszerzenie Jumbo Frames 9000
- Ochrona
- Funkcje DHCP DHCP relay, DHCPv6 client
- Lista kontrolna dostępu (ACL) Tak
- Zasady Listy Kontroli Dostępu (ACL) 512
- IGMP snooping Tak
- Ochrona hasłem Tak
- obsługuje SSH/SSL Tak
- Filtrowanie adresów MAC Tak

- Szyfrowanie / bezpieczeństwo HTTPS, SSH, SSL/TLS
- Funkcje Multicast
- Obsługa Multicast Tak
- Protokoły
- Protokoły zarządzające SNMP
- Konstrukcja
- Możliwości montowania w stelażu Tak
- Kolor produktu Srebrny
- Przycisk reset Tak
- Diody LED Tak
- Wydajność
- Procesor wbudowany Tak
- Taktowanie procesora 800 MHz
- Pojemność pamięci wewnętrznej 512 MB
- Wielkość pamięci flash 256 MB
- Aktualizacje oprogramowania urządzenia Tak
- Moc
- Zasilacz dołączony Tak
- Częstotliwość wejściowa AC 50 - 60 Hz
- Warunki pracy
- Zakres temperatur (eksploatacja) -5 - 50 °C
- Zakres temperatur (przechowywanie) -25 - 70 °C
- Zakres wilgotności względnej 10 - 90%
- Dopuszczalna wilgotność względna 10 - 90%

4. Konfiguracji serwera Radius w oparciu o technologie Microsoft z integracją z Active Directory. Autentykacja użytkowników będzie wymagała konta Active Directory, będzie odbywała się automatycznie po wpisaniu loginu i hasła użytkownika.
5. Dostarczeniu 3 punktów dostępowych razem z centralnym kontrolerem w technologii Wifi 6 o parametrach

Kontroler sprzętowy sieci bezprzewodowej WiFi
Cechy fizyczne:

- Kontroler musi umożliwiać zarządzanie punktami dostępowymi w liczbie min 450.
- Kontroler musi mieć możliwość zarządzania zarówno urządzeniami odpowiadającymi za segment bezprzewodowy sieci (punkty dostępowe) jak i urządzeniami tworzącymi warstwę dostępową i szkielet sieci (przełączniki)
- Urządzenie musi być wyposażone w min. 2 porty RJ45 o prędkości 10/100/1000Mb/s
- Urządzenie musi być wyposażone w port USB umożliwiający podłączenie zewnętrznego nośnika danych
- Urządzenie musi mieć możliwość montażu w szafie rack 19”, elementy montażowe muszą być zawarte w zestawie.
- Urządzenie musi posiadać następujące certyfikaty: CE, RoHS
- Dopuszczana temperatura pracy urządzenia musi zawierać się w przedziale od 0 do 40 stopni Celsjusza

Cechy funkcjonalne:

- Urządzenie musi umożliwiać automatyczne wykrywanie wszystkich urządzeń w sieci lokalnej kompatybilnych z Kontrolerem
- Urządzenie musi zapewniać możliwość zdalnego zarządzania siecią w danej lokalizacji wykorzystując chmurę lub inny mechanizm pozwalający na dostęp do kontrolera z dowolnego miejsca
- W zakresie ogólnej funkcjonalności urządzenie musi wspierać funkcje:
    - Wyświetlania topologii sieci (wykorzystując urządzenia zarządzane przez kontroler)
    - Zarządzania wieloma lokalizacjami z poziomu pojedynczego kontrolera
    - ACL (listy kontroli dostępu) zarówno dla użytkowników łączących się do sieci przewodowo jak i bezprzewodowo
    - Uwierzytelniania użytkowników zarówno przewodowych jak i bezprzewodowych z wykorzystaniem strony powitalnej
- W zakresie konfiguracji sieci WiFi urządzenie musi umożliwiać konfigurację następujących funkcji:
    - Multi SSID
    - Sieć dla Gości (odizolowanie klientów w tej sieci od innych klientów lokalnych bez wykorzystania VLAN)
    - Powiązanie SSID do VLAN
    - Filtrowanie adresów MAC (tryby blacklist/whitelist)
    - Kanał transmisji/moc nadawania konkretnych AP
    - Równoważenie obciążenia punktów dostępowych
    - Sterowanie pasmem
    - Ograniczenie prędkości transmisji
    - Tworzenie harmonogramu sieci WiFi oraz resetu urządzeń
    - QoS
    - Harmonogramowanie sieci bezprzewodowej oraz restartu urządzenia

Punkt dostępowy sieci WiFi

- Urządzenie musi być wyposażone w min. 1 port RJ45 pracujący z prędkością 1Gb/s obsługujący standard PoE 802.3at
- Urządzenie musi być wyposażone w gniazdo umożliwiające zasilanie urządzenia bezpośrednio z wykorzystaniem zewnętrznego zasilacza
- Urządzenie musi być wyposażone w przycisk przywracania ustawień fabrycznych
- Urządzenie musi być wyposażone w min 2 anteny wewnętrzne dookólne o zysku min 4dBi dla sieci 2,4GHz oraz min 5dBi dla sieci 5GHz
- Urządzenie musi wspierać standardy IEEE 802.11a/b/g/n/ac/ax oraz częstotliwości pracy 2,4 oraz 5GHz
- Prędkość modułów radiowych musi wynosić min 2402Mbps dla częstotliwości 5GHz i 574Mbps dla częstotliwości 2,4Ghz
- Maksymalny pobór mocy urządzenia nie może być większy niż 14W
- Urządzenie powinno być dostosowane do montażu na ścianie lub suficie oraz posiadać dołączony zestaw montażowy

- Urządzenie musi pracować zarówno jako urządzenie typu stand-alone lub w trybie podłączonym do kontrolera sieci bezprzewodowej
- Kontroler sieci bezprzewodowej realizowany musi być jako oprogramowanie przeznaczone do instalacji na systemach operacyjnych Windows/Linux lub kontroler sprzętowy – oddzielne urządzenie
- Oprogramowanie kontrolera sieci bezprzewodowych musi być realizowane jako oprogramowanie bezpłatne, bez dodatkowych opłat licencyjnych
- Urządzenie musi posiadać funkcjonalność tworzenia wielu sieci WiFi – min. 14 SSID
- Urządzenie musi posiadać funkcjonalność: wyłącznik sieci bezprzewodowej, automatyczny wybór kanału, kontrola mocy transmisji, QoS (WMM), sterowanie pasmem, równoważenie obciążenia pasma, kontrola przepustowości, harmonogram resetu oraz harmonogram sieci bezprzewodowej.
- Urządzenie musi posiadać możliwość utworzenia strony powitalnej
- Urządzenie musi posiadać możliwość mapowania SSID do VLAN oraz tworzenia sieci dla gości
- Urządzenie musi posiadać możliwość wyłączenia diody LED na obudowie
- Urządzenie musi być zarządzane z poziomu przeglądarki internetowej, oraz obsługiwać zarządzanie poprzez HTTPS
- Urządzenie musi posiadać obsługę SNMP v1/v2c,v3
- Urządzenie musi posiadać certyfikat CE, FCC oraz RoHS
- W zestawie z urządzeniem powinien być zestaw montażowy
- Dopuszczalna temperatura pracy powinna zawierać się w przedziale od 0 do 40 stopni Celsjusza.

Wymagania Dodatkowe

- Wykonawca musi posiadać doświadczenie w administracji sieciami, min. 2 letnie, co potwierdzi odpowiednimi dokumentami – **wymagane do złożenia wraz z ofertą.**
- Zapewnienie wsparcia technicznego przez minimum 18 miesięcy po wdrożeniu.
- Wszystkie prace muszą być wykonane zgodnie z najlepszymi praktykami bezpieczeństwa
- Zamawiający wydeleguje do wykonania zadania certyfikowanego inżyniera firmy Fortinet z certyfikatem minimum NSE4, na co przedstawi odpowiedni dokument potwierdzający **po podpisaniu umowy.**
- Wykonawca wykona prace nie zakłócając pracy użytkownikom (normalna praca: pon-piątek 7:00-16:00).
- Wykonawca dostarczy:
    - Projekt powykonawczy sieci.
    - Opis zabezpieczeń i kontroli dostępów
- Wykonawca zapewni szkolenie z wprowadzonych zmian dla lokalnego IT

Signature Not Verified

Dokument podpisany przez Mateusz Rutkowski
Data: 2024.11.21 09:20:19 CET