

RNZ.271.2.14.2025

Załącznik nr 1a do SWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

„Cyberbezpieczna Gmina Tykocin” – Zakup i dostawa sprzętu IT wraz z oprogramowaniem i licencjami wraz z dostawą agregatu.

Zakup jest przewidziany do współfinansowanego w ramach zadania pn.: Cyberbezpieczny Samorząd" ze środków Europejskiego Funduszu na Rozwój Cyfrowy 2021-2027 (FERC) Priorytetu II Zaawansowane usługi cyfrowe, Działania 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa, konkursu grantowego w ramach Projektu grantowego „Cyberbezpieczna Gmina Tykocin” o numerze FERC.02.02-CS.01-001/23

CZĘŚĆ I: ZAKUP I DOSTAWA SPRZĘTU IT WRAZ Z OPROGRAMOWANIEM I LICENCJAMI NA POTRZEBY URZĘDU MIEJSKIEGO W TYKOCINIE ORAZ JEDNOSTEK ORGANIZACYJNYCH

- I. Aktualizacja (upgrade), nowych licencji systemu do wykonywania kopii zapasowych dla komputerów PC, serwerów.
- II. Licencja dostępowe CAL. (licencja bez ograniczeń czasowych (wieczysta)) lub równoważna, łączna ilość: 50 szt.
- III. Urządzenia typu UTM wraz z licencjami na potrzeby jednostek organizacyjnych Gminy Tykocin.
- IV. Zakup przetączyń zarządalnych na potrzeby Urzędu Miejskiego w Tykocinie oraz jednostek podległych.
- V. DOSTAWA UPS.

I. Aktualizacja (upgrade), nowych licencji systemu do wykonywania kopii zapasowych dla komputerów PC, serwerów:

- 1) Zamówienie polega na dostarczeniu aktualizacji systemu Ferro Backup System (FBS) lub równoważnego:
 - a) aktualizacji systemu Ferro Backup System (FBS) z wersji 5.x Standard do wersji 6.x Standard oraz rozszerzenie licencji o 3 licencje do backupu serwera (Urząd Miejski w Tykocinie),
- 2) Zamówienie polega na dostawie 3 szt. nowych licencji systemu Ferro Backup System (FBS) wersja 6.x Standard lub równoważnych na potrzeby jednostek organizacyjnych, w tym:
 - a) do Gminnego Zakładu Gospodarki Komunalnej w Tykocinie (10 stanowisk + 1 server),
 - b) do Zespołu Szkolno- Przedszkolnego w Tykocinie (5 stanowisk + 1 server),
 - c) do Szkoły Podstawowej w Radulach (5 stanowisk + 1 server),

- 3) Zamówienie polega na dostawie 2 szt. nowej licencji systemu Ferro Ferro Backup System (FBS) wersja 6.x Standard Backup System (FBS) wersja 6.x Standard dla Urzędu Miejskiego w Tykocinie tj. 2x (5 stanowisk + 1 server) lub równoważnych.
1. W przypadku dostępności wersji Ferro Backup System (FBS) wersja 7.x Standard należy dostarczyć licencje wersji 7.x oraz aktualizacje do wersji 7.x.
2. Zamawiający po podpisaniu umowy poda dostawcy wymagane dane posiadanych licencji.

Zasady równoważności: Ferro Backup System wersja 6x lub nowszy

1. Przez oprogramowanie równoważne Zamawiający rozumie oprogramowanie spełniające następujące warunki poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
- 1) Wszystkie elementy systemu oraz jego licencja pochodzą od tego samego producenta.
 - 2) Obsługa zarządzania systemem całkowicie w języku polskim.
 - 3) System powinien działać w oparciu o architekturę klient - serwer.
 - 4) Powinien posiadać dwa programy: serwer backupu oraz klient na stacji z której robiony jest backup.
 - 5) Program Server backupu powinien być uruchamiany w trybie usługi systemowej.
 - 6) Powinien zapewniać wykonywanie kopii zapasowych plików przechowywanych w komputerach biurowych, komputerach przenośnych i serwerach pracujących pod kontrolą systemów Windows, NetWare i Linux.
 - 7) System powinien przechowywać dane w PKZIP (wersja 64-bit) stworzonym przez firmę PKWARE, Inc. Format ten pozwala na tworzenie archiwów (pojedynczych plików .zip) o rozmiarach do 9 exabajtów (1 EB = 1 000 000 TB).
 - 8) Pliki kopii .zip powinno być można w przypadku awarii systemu przeglądać i rozpakowywać różnymi programami obsługującymi format PKZIP ZIP64, np. popularnym programem WinZip®.
 - 9) System powinien posiadać konsolę sterowania, obsługiwaną przez „thin client” przeglądarką internetową, dostęp do konsoli zarządzającej systemu backupu nie powinien wymagać konieczności instalacji dodatkowego oprogramowania. Powinien działać w oparciu o stronę internetową. Serwer www powinien być wbudowany bezpośrednio do modułu serwera backupu, bez potrzeby instalowania na serwerze backupu zewnętrznego serwera www, np. IIS czy Apache.
 - 10) System powinien obsługiwać kodowanie znaków Unicode, przez co możliwy jest backup plików zawierających w nazwie dowolne znaki narodowe.

- 11) System powinien mieć możliwość pracy w programie z dowolnego miejsca bez potrzeby korzystania z Pulpitu zdalnego, jednoczesnej pracy z danym serwerem przez kliku administratorów.
- 12) Powinien mieć wbudowane następujące funkcje:
 1. Możliwość wykonania backupu całego systemu operacyjnego, łącznie z zainstalowanymi programami, sterownikami i danymi użytkownika, tak aby w przypadku awarii możliwe było odzyskanie działającego systemu operacyjnego i wszystkich zainstalowanych komponentów.
 2. Zautomatyzowane przywracanie systemu operacyjnego ze stacji roboczych i serwerów (prosty sposób przywracania systemu operacyjnego z serwera kopii zapasowych poprzez sieć do uszkodzonego komputera). Możliwość przywrócenia po awarii systemu operacyjnego wraz z wszystkimi zainstalowanymi programami (ang. bare-metal restore), tak aby uruchomić system operacyjny bez potrzeby ponownej instalacji i konfiguracji
 3. Ochrona przed programami ransomware szyfrującymi pliki.
 4. Backup i odzyskiwanie maszyn wirtualnych Hyper-V oraz VMWare ESX, ESXi Program powinien wykonywać kopie zapasowe zarówno zatrzymanych jak i uruchomionych maszyn wirtualnych.
 5. Certyfikaty SSL dla połączeń HTTPS – możliwość obsługi samopodpisanych certyfikatów oraz stosowania własnych certyfikatów SSL.
 6. Zabezpieczanie połączeń sieciowych w systemach archiwizacji danych - typu klientserwer za pomocą reguł IPSec.
 7. Możliwość archiwizacja danych w chmurze.
 8. Backup plików PST (MS Outlook) - backup plików PST bez zamykania programu Outlook.
 9. Możliwość automatycznego backupu komputera przy zamykaniu systemu
 10. Wysoka wydajność serwera backupu - bezproblemowy backup serwerów i komputerów zawierających bardzo dużo plików
 11. Archiwizacja danych także na napędy taśmowe – możliwość replikacji na napędy taśmowe.
 12. Możliwość backupu na dysk sieciowy - składowanie kopii na urządzeniach typu NAS szybkim i wydajnym protokołem iSCSI.
 13. Możliwość instalacji serwera backupu pod systemem Linux i Mac OS X
 14. Możliwość wydajnego i pewnego backupu baz danych i plików poczty. (Microsoft SQL Server, Microsoft Exchange Server, Oracle, MySQL, InterBase, Firebird, Microsoft Access, dBase, Paradox oraz plików programów pocztowych: Microsoft Outlook, Outlook Express, Mozilla Thunderbird).

15. Możliwość archiwizacji otwartych i zablokowanych plików.

16. Możliwość szyfrowania archiwów (w tym AES 256)

17. Możliwość wykonywania archiwizacji pełnej i różnicowej, także różnicowej na poziomie fragmentów plików (archiwizowane są tylko te części plików, które zostały zmodyfikowane od czasu poprzednich archiwizacji a pozostałe są pomijane).

18. Możliwość generowania raportów i statystyk, które pomagają w analizie działania aplikacji (Raporty informujące o niewykonanych i opóźnionych zadaniach archiwizacji i statystyki zawierające informacje na temat szybkości i rozmiaru backupu z poszczególnych komputerów).

19. Możliwość wykonywania zadań archiwizacji w/g harmonogramu następującego typu:

- a. Na żądanie - zadanie archiwizacji będzie wykonywane tylko przez manualne uruchomienie zadania
- b. Codziennie - zadanie archiwizacji będzie uruchamiane codziennie o wskazanej godzinie
- c. Co określoną liczbę dni - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę dni.
- d. Co określoną liczbę godzin - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę godzin.
- e. Co określoną liczbę minut - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę minut.
- f. W dni tygodnia - zadanie archiwizacji będzie wykonywane automatycznie w wybrane dni tygodnia.
- g. Czas rozpoczęcia - umożliwia ustalenie terminu rozpoczęcia zadania archiwizacji z dokładnością do jednej minuty.
- h. Następny termin - umożliwia ustalenie daty kolejnej archiwizacji.
- i. Zadania opóźnione mogą być pominięte i wykonane w następnym terminie, wykonane natychmiast po podłączeniu komputera, serwera.
- j. Przy zamykaniu systemu.

20. Dziennik zdarzeń służący do sprawdzania poprawności działania systemu i wyszukiwania przyczyn ewentualnych problemów – możliwość na bieżąco śledzenia generowanych zdarzeń, dotyczących działania całego systemu (serwera jak i stacji roboczych), takie jak: błędy, ostrzeżenia i informacje. Wszystkie zapisane zdarzenia można filtrować co najmniej według typu zdarzenia oraz nazwy komputera, którego dana informacja dotyczy.

13) System powinien ponadto umożliwiać:

1. Podczas wyboru plików i katalogów do archiwizacji pozwalać określić woluminy ,maski lub pełne ścieżki do plików i katalogów, które mają być archiwizowane i te, które mają być wykluczone z archiwizacji
2. Obsługę co najmniej następujących rodzajów archiwizacji
 - a. archiwizacja pełna
 - b. archiwizacja różnicowa
 - c. archiwizacja różnicowa na poziomie fragmentów plików.
3. Obsługę kopii rotacyjnych (wersjonowanie, retencja danych - pozwala określić ile maksymalnie przechowywać archiwów na dysku, ile przechowywać kopii wstecz).
4. Obsługa replikacji archiwów - archiwa należące do wybranego zadania backupu mogą być powielane w inne miejsce, replikacja może być wykonywana na napędy dyskowe, optyczne i taśmowe.
5. Monitoring i kontrola pracy serwera backupu, powinna w łatwy i intuicyjny sposób umożliwić zatrzymanie i uruchomienie serwera backupu, możliwość wywołania wirtualnego wiersz poleceń na serwerze backupu i podłączonych stacjach roboczych.
6. Dziennik zdarzeń służy do sprawdzania poprawności działania Systemu i wyszukiwania przyczyn ewentualnych problemów. W zakładce Dziennik zdarzeń można na bieżąco śledzić wszystkie generowane zdarzenia dotyczące działania całego Systemu (serwera jak i stacji roboczych), takie jak: błędy, ostrzeżenia i informacje.

Wszystkie zapisane zdarzenia można filtrować według typu zdarzenia oraz nazwy komputera, którego dana informacja dotyczy.
7. Wysyłanie alertów administracyjnych, zawierających raporty lub wybrane komunikaty z dziennika zdarzeń, wg ustalonego harmonogramu na wskazany adres email lub np. do serwera syslog.
8. Możliwy dostęp do zasobów sieciowych przez np. definiowanie ścieżki UNC, dyski sieciowe i dyski serwerów FTP, które mogą być wykorzystywane przez system jako:
 - a. miejsce przechowywania archiwów,
 - b. katalog docelowy replikacji,
 - c. ścieżka zapisu alertów administracyjnych.
9. Możliwe używania poleceń lokalnych, służących do rozszerzania funkcjonalności programu. Dzięki nim można automatycznie uruchamiać na serwerze backupu zewnętrzne programy, skrypty lub pliki wsadowe,

wykonywać operacje na plikach, wykorzystywać komponenty ActiveX, sterować usługami Active Directory, itp.

10. Program może być uruchamiany w trybie Usługi systemowej lub awaryjnie, także w trybie aplikacji użytkownika.

11. Możliwe uruchomienie programu w trybie diagnostycznym oraz w trybie naprawy bazy danych.

II. Licence dostępne CAL. (licencja bez ograniczeń czasowych (wieczysta)) lub równoważna*
Łączna Ilość: 50 szt.

Parametr	Charakterystyka (wymagania minimalne)
Nazwa licencji	Microsoft Windows Server 2025 User CAL lub równoważne
Ilość licencji	40 szt. - Urząd Miejski w Tykocinie 10 szt. - Miejsko- Gminny Ośrodek Pomocy Społecznej w Tykocinie

***Za równoważność zamawiający uznaje:** licencje dostępową dla urządzenia umożliwiającą legalne podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2025 typu User Cal z wdrożoną rolą Active Directory.

Wszystkie opisane parametry wymagane są wymaganiami minimalnymi. Zamawiający akceptuje rozwiązania o parametrach lepszych lecz bez utraty funkcjonalności i wydajności opisanej w opisie przedmiotu zamówienia.

Przedmiot zamówienia musi być legalny, fabrycznie nowy, nigdy wcześniej nie używany, pochodzący z legalnego kanału dystrybucyjnego producenta oprogramowania, dopuszczony do obrotu, spełniający normy CE.

Licencje muszą być dostarczone elektronicznie. Stan licencji musi być widoczny na indywidualnym profilu Zamawiającego w portalu producenta oprogramowania przeznaczonym do zarządzania licencjami oprogramowania producenta.

III. Urządzenia typu UTM wraz z licencjami na potrzeby jednostek organizacyjnych Gminy Tykocin.

1) 4 szt. urządzeń typu FortiGate-40F z licencjami lub równoważne o poniższych parametrach:

LP.	Nazwa	Parametr
1	Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy

		<p>sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> •Firewall. •Ochrony w warstwie aplikacji. •Protokołów routingu dynamicznego.
2	Redundancja, monitoring i wykrywanie awarii	<p>1.W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.</p> <p>2.Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</p> <p>3.Monitoring stanu realizowanych połączeń VPN.</p> <p>4.System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.</p>
3	Interfejsy, Dysk, Zasilanie:	<p>1.System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:</p> <ul style="list-style-type: none"> •Min. 4 portami Gigabit Ethernet RJ-45. <p>2.System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</p>
4	Funkcje Systemu Bezpieczeństwa:	<p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci</p>

		<p>osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> 1.Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2.Kontrola Aplikacji. 3.Poufność transmisji danych - połączenia szyfrowane IPsec VPN oraz SSL VPN. 4.Ochrona przed malware. 5.Ochrona przed atakami - Intrusion Prevention System. 6.Kontrola stron WWW. 7.Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8.Zarządzanie pasmem (QoS, Traffic shaping). 9.Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10.Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11.Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12.Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13.Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wystanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
--	--	--

5	Polityki, Firewall	<p>1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</p> <p>2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:</p> <ul style="list-style-type: none"> • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. <p>3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.</p> <p>5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</p> <p>6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</p> <p>7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.</p> <ul style="list-style-type: none"> • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
6	Połączenia VPN	<p>1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> • Wsparcie dla IKE v1 oraz v2.

		<ul style="list-style-type: none"> •Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). •Obsługa protokołu Diffie-Hellman grup 19, 20. •Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. •Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. •Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. •Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. •Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. •Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. •Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. •Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. •Mechanizm „Split tunneling” dla połączeń Client-to-Site. <p>2.System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> •Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. •Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. •Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
7	Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę:

		<p>1. Routingu statycznego.</p> <p>2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).</p> <p>3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.</p> <p>4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.</p> <p>5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.</p> <p>6. BFD (Bidirectional Forwarding Detection).</p> <p>7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.</p>
8	Funkcje SD-WAN	<p>1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN.</p> <p>2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</p>
9	Zarządzanie pasmem	<p>1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>2. System daje możliwość określania pasma dla poszczególnych aplikacji.</p> <p>3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</p> <p>4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</p>
10	Ochrona przed malware	<p>1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</p>

		<p>3.System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.</p> <p>4.System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</p> <p>5.System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p> <p>6.Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>7.System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.</p> <p>8.System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.</p> <p>9.Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</p> <p>10.Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</p>
11	Ochrona przed atakami	<p>1.Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>2.System chroni przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>3.Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>4.System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p>

		<p>5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</p> <p>6. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.</p> <p>7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p> <p>8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.</p>
12	Kontrola aplikacji	<p>1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> <p>3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</p> <p>5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>6. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).</p>
13	Kontrola WWW	<p>1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p> <p>2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</p> <p>3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</p>

		<p>4.Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>5.Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</p> <p>6.Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</p> <p>7.Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</p> <p>8.Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</p> <p>9.System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</p>
14	Uwierzytelnianie użytkowników w ramach sesji	<p>1.System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:</p> <ul style="list-style-type: none"> •Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. •Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. •Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. <p>2.System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</p> <p>3.System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.</p> <p>4.Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p>

15	Zarządzanie	<p>1.Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.</p> <p>2.Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>3.Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.</p> <p>4.System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</p> <p>5.System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>6.Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>7.Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p> <p>8.Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</p> <p>9.Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</p>
16	Logowanie	<p>1.Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.</p> <p>2.W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o:</p>

		<p>zaakceptowanym ruchu, blokowaniem ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <p>3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>4. Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>5. System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p>
17	Certyfikaty	<p>Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:</p> <ul style="list-style-type: none"> • ICSA lub EAL4 dla funkcji Firewall.
18	Serwisy i licencje	<p>Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje z minimalnym okresem 1 rok</p>
19	Gwarancja oraz wsparcie	<p>1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.</p> <ul style="list-style-type: none"> • Wsparcie telefoniczne zespołu certyfikowanych inżynierów. • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. • Doradztwo w zakresie konfiguracji. • Zdalne wsparcie techniczne. • Pomoc w zakładaniu zgłoszeń serwisowych u producenta. • Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).

		<ul style="list-style-type: none"> • Przygotowanie urządzenia do zdalnej konfiguracji. • Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. • Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. • Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. • Certyfikat ISO 9001 podmiotu serwisującego.
--	--	--

IV. Zakup przełączników zarządzalnych na potrzeby Urzędu Miejskiego w Tykocinie oraz jednostek podległych:

1) Ilość : 9 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne przełącznika
Typ przełącznika	Zarządzalny
Porty	14) 48 RJ-45 10/100/1000 Mbps 15) 4x 10 Gigabit SFP+
Zasilanie	220-240V 50-60 Hz
Moc PoE+	Min. 700W
Montaż	Możliwość montażu w szafie Rack
Wydajność przełączania	Min. 130 Gb/s
Szybkość przekierowań pakietów	Min. 100Mp/s
Rozmiar tablicy adresów MAC	16k wpisów
Bufor pakietów	1,5 MB
DRAM	512MB



Niezawodność MTBF	800 000 godzin
Maks. Waga	6 kg
Cechy i funkcje przetącnika	<ul style="list-style-type: none"> • obsługa DHCP • obsługa ARP • obsługa VLAN • zapobieganie atakom typu DoS • obsługa protokołu Spanning Tree (STP) • obsługa protokołu Multiple Spanning Tree Protocol (MSTP) • obsługa list dostępu (ACL) • Quality of Service (QoS), • obsługa RADIUS, • serwer DHCP
Gwarancja	Min. 5-letnia gwarancja producenta

V. DOSTAWA UPS

1) UPS typu RACK na potrzeby serwerowni Urzędu – 1 szt.

- fabrycznie nowy, typu rack;
- moc wyjściowa pozorna: min. 2200 VA
- moc skuteczna - min 1,95 kW, jednofazowy;
- czas przełączania – max 8 ms,
- kształt przebiegu: czysty sinus,
- czas podtrzymania dla obciążenia 100% - min. 5 min.
- Zabezpieczenia: przeciwprzepięciowe, przed głębokim rozładowaniem i przeladowaniem baterii,
- ilość złączy IEC C13 do podłączenia zasilania urządzeń zewnętrznych: min 8.
- UPS zawiera w komplecie baterie (gotowy do rozruchu/pracy)
- Posiada odpowiednie certyfikaty
- gwarancja na UPS min 24 miesiące.

2) UPS typu rack dla jednostek organizacyjnych do zasilania NAS i urządzeń sieciowych – 4 szt.

- fabrycznie nowy, z wyświetlaczem LCD;
- typu rack 1U/2U do szafy 19”; jeżeli brak w komplecie i są wymagane – dołączyć szyny montażowe;
- Moc wyjściowa pozorna: min. 1500 VA;
- moc czynna - min 900 W;
- czas przełączania – max 6 ms;
- czas ładowania – max 4h;
- kształt przebiegu sinus: Pełna sinusoida na wyjściu;
- Zabezpieczenia: przeciwprzepięciowe, przed głębokim rozładowaniem i przeladowaniem baterii;

- i) ilość złączy do podłączenia zasilania urządzeń zewnętrznych: min 4 (IEC C13). Do UPS muszą być dołączone co najmniej 2 x kabel (2m) z wtykiem typu IEC C13;
- j) UPS zawiera w komplecie baterie (gotowy do rozruchu/pracy);
- k) posiada odpowiednie certyfikaty;
- l) gwarancja na UPS min 24 miesiące.

SZCZEGÓŁOWE WYTYCZNE DOTYCZĄCE CAŁEJ CZĘŚCI NR I

I. Ogólne zasady oceny równoważności

1. W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne (dotyczy równoważności we wszystkich wskazanych powyżej przypadkach) nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.
2. Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych, jako rozwiązania referencyjne, po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.
3. Wykonawca zobowiązany jest podać w ofercie co najmniej nazwę producenta, nazwę oferowanego Oprogramowania, identyfikator Oprogramowania nadawany przez jego producenta, rodzaj licencji (według oznaczenia producenta), w sposób umożliwiający Zamawiającemu jednoznaczną identyfikację i weryfikację zaoferowanego Oprogramowania oraz udowodnić, że oferowane rozwiązanie spełnia wskazane przez Zamawiającego kryteria stosowane w celu oceny równoważności.
4. Zamawiający nie dopuszcza dostarczenia licencji dla produktów równoważnych w formie upgradu czy licencji czasowej.
5. Zamawiający nie dopuszcza zaoferowania subskrypcji licencyjnej opartej o rozwiązania chmurowe.
6. W przypadku błędnego działania środowiska lub wykrytych niezgodności pod kątem spełnienia warunków OPZ po instalacji oprogramowania równoważnego Zamawiający ma prawo odstąpić od umowy.

UWAGI OGÓLNE

- II. Zamawiający wymaga fabrycznie nowego oprogramowania nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu. Zamawiający nie dopuszcza składania ofert zawierających sprzęt poserwisowy lub refabrykowany.
- III. Wykonawca gwarantuje, iż sprzęt i oprogramowanie dostarczone w ramach realizacji umowy pochodzi z legalnego źródła i nie jest częścią żadnego projektu oferowanego dla innych podmiotów
- IV. Zamawiający wymaga aby oprogramowanie było dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności, na przykład z tzw. naklejkami GML (Genuine Microsoft Label) lub naklejkami COA (Certificate of Authenticity) stosowanymi przez producenta sprzętu

lub inną formą uwiarygodniania oryginalności wymaganą przez producenta oprogramowania stosowną w zależności od dostarczanej wersji,

- V.** Zamawiający dopuszcza możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów komputerowych u Producenta oprogramowania w przypadku wystąpienia wątpliwości co do jego legalności.
- VI.** Warunki wymagane do spełnienia przez Wykonawcę zamówienia:
- VII.** Wykonawca dostarczy wszystkie elementy przedmiotu zamówienia do siedziby Urzędu Miejskiego w Tykocinie
- VIII.** Wykonawca zobowiązany jest do:
- dostawy elementów dołączanych przez producenta oraz dodawanych przez Wykonawcę, niezbędnym do w pełni funkcjonalnej pracy;
 - dostawy w przypadku elementów powtarzalnych, identycznych wersji i w identycznej specyfikacji;
 - pokrycia wszelkich kosztów dostawy do siedziby Zamawiającego.
- IX.** Wykonawca oświadcza, że oferowany towar jest nowy, nieużywany, nieuszkodzony, nieobciążony prawami osób trzecich oraz spełnia normy bezpieczeństwa. Towar, będący przedmiotem zamówienia, nie jest również refabrykowany, recertyfikowany, poleasingowy, a każdy oferowany element danej pozycji jest jednakowego producenta, modelu, wersji i specyfikacji.
- X.** Wykonawca oświadcza, że oferowane oprogramowanie pochodzi z oficjalnej, polskiej dystrybucji.

