Załącznik nr 1

Opis Przedmiotu Zamówienia Zintegrowany Pakiet Firewalle

I. Informacje podstawowe

Zamawiający planuje wdrożyć Zintegrowany System Firewall we wszystkich jednostkach miejskich Miasta Rydułtowy.

Pod względem wykorzystywania systemów teleinformatycznych, a także struktury sieci i zabezpieczeń, wszystkie jednostki organizacyjne są od siebie niezależne. Połączenie z siecią wewnątrz budynku, a także z siecią Internet realizowane jest z wykorzystaniem różnych modeli zabezpieczeń, różnej logiki zabezpieczeń oraz z wykorzystaniem różnego sprzętu brzegowego.

Na przestrzeni najbliższych kilku lat Miasto Rydułtowy zaplanowało realizację wielu przedsięwzięć z zakresu IT, które będą wymagały dostępu jednostek miejskich do sieci wewnętrznej Urzędu Miasta. Tym samym powstało zapotrzebowanie, aby zabezpieczyć wszystkie sieci komputerowe jednostek przed nieuprawnionym korzystaniem z zasobów serwerów Urzędu Miasta Rydułtowy. Mając to na uwadze przyjęto, że niezbędnym jest przygotowanie dla wszystkich jednostek wytycznych w zakresie logicznego i technicznego (sprzętowego) zabezpieczenia sieci, która będzie w pełni możliwa do zarządzania przez administratorów.

W ramach niniejszego postępowania Zamawiający wymaga od Wykonawcy dostarczenia, skonfigurowania, zainstalowania oraz uruchomienia 18 fabrycznie nowych urządzeń firewall (UTM).

Planuje się zakup fizycznych siedemnastu urządzeń zarządzalnych (programowalnych) pełniących funkcję zapory sieciowej (routera brzegowego) dla sieci we wszystkich jednostkach miejskich wraz z systemem operacyjnym producenta oraz jednego urządzenia dla jednostki nadrzędnej (UM Rydułtowy) do obsługi ruchu wszystkich jednostek oraz do pełnienia zapory sieciowej. Urządzenia winny być tak skonfigurowane, aby w sposób bezpieczny możliwe było dokonywanie połączeń z jednostek ze wskazanymi przez Zamawiającego podczas instalacji serwerami oraz usługami Urzędu Miasta Rydułtowy. Urządzenia dostarczone w ramach przedmiotu zamówienia muszą umożliwiać bezpieczne połączenie pomiędzy jednostkami miejskimi, a serwerami Urzędu Miasta Rydułtowy z wykorzystaniem obecnych połączeń internetowych wykazanych w punkcie II. Dodatkowo planuje się, że Wykonawca skonfiguruje urządzenia dla każdej jednostki indywidualnie oraz przygotuje dokumentację techniczną wskazującą metodologię konfigurowania urządzeń, uwzględniając charakterystykę jednostki, jej sieć oraz zasoby zachowując ustawienia obecnie posiadanych sieci i urządzeń.

Urządzenia muszą zostać skonfigurowane, dostarczone i zainstalowane w następujących jednostkach:

1. Urząd Miasta Rydułtowy, Rydułtowy ul. Ofiar Terroru 36
2. Zakład Gospodarki Komunalnej, Rydułtowy ul. Raciborska 150
3. Miejski Ośrodek Pomocy Społecznej, Rydułtowy ul. Raciborska 369
4. Miejski Zespół Obsługi Placówek Oświatowych (centrum usług wspólnych), Rydułtowy ul. Raciborska 369,
5. Rydułtowski Ośrodek Sportu i Rekreacji, Rydułtowy ul. Generała Józefa Bema 126c
6. Ognisko Pracy Pozaszkolnej, Rydułtowy ul. Adama Mickiewicza 33

7. Państwowe Ognisko Plastyczne im. Ludwika Konarzewskiego Seniora, Rydułtowy ul. Adama Mickiewicza 33
8. Biblioteka Publiczna Miasta Rydułtowy im. Henryka Mikołaja Góreckiego, Rydułtowy ul. Adama Mickiewicza 33,
9. Szkoła Podstawowa nr 1 im. Karola Miarki, Rydułtowy ul. Świętego Maksymiliana Kolbego 5
10. Szkoła Podstawowa nr 2, Rydułtowy ul. Raciborska 27
11. Szkoła Podstawowa nr 3 im. Arki Bożka, Rydułtowy ul. Radoszowska 3,
12. Szkoła Podstawowa nr 4, Rydułtowy ul, Strzelców Bytomskich 13,
13. Publiczne Przedszkole nr 1 im. Marii Kownackiej, Rydułtowy ul. Kochanowskiego 25,
14. Publiczne Przedszkole nr 2 im. Czesława Janczarskiego, Rydułtowy ul. Raciborska 216
15. Publiczne Przedszkole nr 3, Rydułtowy Osiedle Orłowiec 39
16. Publiczne Przedszkole nr 4 im. J. Brzechwy, Rydułtowy Osiedle Orłowiec 37
17. Miejski Żłobek, Rydułtowy Osiedle Orłowiec 39
18. Rydułtowskie Centrum Kultury FENIKS, Rydułtowy ul. Strzelców Bytomskich 9a

II. Informacje nt. posiadanych zasobów w jednostkach miejskich

L.P	Nazwa jednostki	Ilość użytkowników	Ilość komputerów	Inne urządzenia
1	Urząd Miasta Rydułtowy	120	142	94
2	Zakład Gospodarki Komunalnej Rydułtowy	13	15	15
3	Miejski Ośrodek Pomocy Społecznej w Rydułtowach	25	25	15
4	Miejski Zespół Placówek Oświatowych	11	15	10
5	Rydułtowski Ośrodek Sportu i Rekreacji	13	14	25
6	Ognisko Pracy Pozaszkolnej w Rydułtowach	6	19	15
7	Państwowe Ognisko Plastyczne im. Ludwika Konarzewskiego Seniora w Rydułtowach	4	5	10
8	Biblioteka Publiczna Miasta Rydułtowy	9	22	15
9	Szkoła Podstawowa nr 1 w Rydułtowach	60 (525 uczniów)	52	17
10	Szkoła Podstawowa nr 2 w Rydułtowach	48 (463 uczniów)	127	25
11	Szkoła Podstawowa nr 3 w Rydułtowach	39 (294 uczniów)	53	25
12	Szkoła Podstawowa nr 4 w Rydułtowach	34	71	25

		(319 uczniów)		
13	Publiczne Przedszkole nr 1 im. Marii Kownackiej w Rydułtowach	14	9	10
14	Publiczne Przedszkole nr 2 w Rydułtowach	9	6	10
15	Przedszkole Publiczne nr 3	9	7	10
16	Publiczne Przedszkole nr 4 w Rydułtowach	1	4	ok. 10
17	Miejski Żłobek w Rydułtowach	5	2	5
18	Rydułtowskie Centrum Kultury FENIKS	11	15	25

Ilość wykazanych urządzeń w okresie użytkowania zawianego pakietu firewall (przyjmuje się 24 miesiące) dla poszczególnych jednostek może wzrosnąć maksymalnie o 10%. Tym samym Wykonawca obowiązany jest zaproponować urządzenia o takich parametrach, które będzie umożliwiało wykorzystywanie jego zasobów z uwzględnieniem wzrostu ilości urządzeń o wskazaną wartość.

III. Wymagania ogólne

Każde z dostarczonych urządzeń musi zapewniać wszystkie wymienione poniżej funkcje. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa 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.

IV. Funkcjonalność urządzeń

1. Muszą umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa.
2. Muszą mieć możliwość uruchomienia w formie klastra wysokiej dostępności (HA) - co najmniej Active-Passive.
3. Muszą umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
4. Muszą obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.
5. Muszą obsługiwać Multicast routing.
6. Muszą obsługiwać Policy Based routing.
7. Muszą umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.
8. Muszą obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
9. Muszą obsługiwać DHPCv6 na zewnętrznym interfejsie.
10. Muszą obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
11. Muszą obsługiwać Dynamic DNS.

12. Muszą obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
13. Muszą obsługiwać translację portów: PAT.
14. Muszą obsługiwać IPSec NAT traversal.
15. Muszą obsługiwać mechanizm Policy Based NAT.
16. Muszą obsługiwać VLAN 802.1Q.
17. Muszą zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
18. Muszą umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
19. Muszą mieć możliwość obsługi zapasowego łącza sieciowego (np. poprzez podłączenie zewnętrznego modemu USB, dodatkowego złącza RJ-45 lub obsługę dodatkowe karty sieciowej USB).
20. Muszą mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
21. Muszą zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.
22. Muszą zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza.
23. Muszą zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
24. Muszą umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
25. Muszą umożliwiać dwuskładnikowe uwierzytelnianie użytkowników z wykorzystaniem wewnętrznej bazy użytkowników oraz ActiveDirectory, LDAP, Radius, Token (np. SecureID).
26. Urządzenia muszą posiadać co najmniej 3 mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Active Directory.
27. Co najmniej jedna metoda transparentnej autoryzacji nie powinna wymagać instalacji dedykowanego agenta na stacjach roboczych użytkowników.
28. Muszą umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft
29. Nie mogą ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
30. Muszą dostarczać mechanizmów identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
31. Muszą zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
32. Muszą zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
33. Muszą posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.
34. Muszą umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
35. Muszą dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych.
36. Muszą zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.
37. Muszą zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania http

38. Muszą zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.
39. Muszą i pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.

V. Dostarczony system bezpieczeństwa musi zapewniać:

1. Ochronę z wykorzystaniem mechanizmów IPS.
2. Ochronę antywirusową.
3. Ochronę przed niechcianą pocztą.
4. Kontrolę wykorzystywanych aplikacji.
5. Możliwość filtrowania URL.

VI. W ramach ochrony przed atakami system musi zapewniać:

1. Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 2000 definicji sygnatur.
2. Automatyczne blokowanie znanych źródeł ataków.
3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, CMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).
5. Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer OverFlow, Remote File Inclusions.
6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.

VII. W ramach kontroli antywirusowej system musi zapewniać

1. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 24 godziny.
2. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne lub usuwanie złośliwej zwartości w wiadomości email wraz z dodaniem do wiadomości e-mail informacji o przeskanowaniu przez silnik AV
3. Możliwość zdefiniowania rozmiaru skanowanego pliku.
4. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
5. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
6. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.
7. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.

VIII. W ramach kontroli antyspamowej system musi zapewniać:

1. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.
2. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
3. Blokowanie spamu w oparciu o język , format i zawartość wiadomości e-mail.
4. Możliwość tworzenia białych/czarnych list, w oparciu o które system zezwala lub odmawia wysyłania wiadomości e-mail dla określonych nadawców i odbiorców.
5. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.

IX. W ramach filtrowania zwartości URL system musi zapewniać:

1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
2. Baza filtra url powinna zawierać co najmniej 50 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
3. Odpytywanie bazy on-line w czasie rzeczywistym.
4. Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym dlaczego dostęp do strony www został zablokowany.
5. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
6. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
7. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.
8. Możliwość filtrowania treści w oparciu o typy MIME.
9. Możliwość blokowania plików cookies dla określonych domen.
10. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
11. Analizę treści dla protokołu HTTPS.
12. Wyłączenie inspekcji HTTPS dla wybranych kategorii stron www.

X. W ramach kontroli aplikacji system musi zapewniać:

1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
2. Ilość rozpoznawanych aplikacji: nie mniej niż 250, podzielonych na różne kategorie.
3. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, Spotify
4. Możliwość ograniczania wykorzystywanej przepustowości aplikacji lub kategorii aplikacji.

XI. W zakresie funkcji VPN system musi:

1. Obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
2. Musi współpracować z rozwiązaniami innych producentów w zakresie IPSec site-to-site VPN.
3. Musi wspierać mechanizmy szyfrowania 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
5. Musi obsługiwać Dead Peer Detection (DPD).
6. Musi wspierać IKEv1 i IKEv2.
7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
8. Urządzenia muszą wspierać VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
9. Urządzenia muszą zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.
10. Urządzenia muszą obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2, Open VPN, WineGuard.
11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, 11, MacOS, iOS i Android.
12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.
13. Urządzenia muszą umożliwiać zestawienia połączenia VPN np. poprzez zalogowanie się na stronę internetową wykorzystującą dwu etapową metodologię uwierzytelniania (np. google authenticator, sms lub inny ogólnodostępny system uwierzytelniania)

14. Możliwość ograniczenia ilości połączeń do wybranych adresów IP.

XII. Wymagania w zakresie zarządzania systemem

1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej, logów zawierających szczegółowe dane na temat urządzeń (MAC, IP,zagrożenia, systemu operacyjnego.
5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.
8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.
9. Interfejs do zarządzania urządzeniami / systemem musi być dostępny co najmniej w języku angielskim.

XIII. Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania

1. System musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
2. System musi umożliwiać przypisywane różnych ról dla poszczególnych administratorów.
3. System musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
4. System musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według zdefiniowanego harmonogramu.
5. System musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
6. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
7. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
8. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
9. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
10. System musi umożliwiać przeglądanie logów ruchu w czasie rzeczywistym.
11. System musi udostępniać narzędzie analizy całości ruchu.
12. System musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
13. System musi posiadać zestaw predefiniowanych typów raportów.
14. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
15. System musi mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.
16. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.

17. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
18. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
19. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
20. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
21. Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.

XIV. Licencje i wsparcie techniczne

1. W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować: Ochrona przed atakami (IPS), Kontrola aplikacji, Web Filtering, Antyspam, Antywirus, Bazy reputacyjne adresów. Licencja musi zostać udzielona na min. 24 miesięcy
2. System musi być objęty serwisem gwarancyjnym producenta na okres min. 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 5x8 (w dni robocze) - świadczone telefonicznie lub poprzez portal w języku polskim.

XV. Minimalne wymagania fizyczne i wydajnościowe dla urządzeń:

L.P	Nazwa jednostki	Ilość portów 1 GB RJ 45	Ilość portów 10GB SFP+	Możliwość rozbudowy o port 10Gb SFP+	Minimalna Przepustowość Firewall	Minimalna ilość jednoczesnych obsługiwanych tuneli VPN–IPSec site-to-site	Minimalna ilość obsługiwanej sieci VLAN
1	Urząd Miasta Rydułtowy	8	2	-	Min. 5.0 Gbps	Min. 100	100
2	Zakład Gospodarki Komunalnej Rydułtowy	5	-	Tak	Min. 3.0 Gbps	Min. 30	10
3	Miejski Ośrodek Pomocy Społecznej w Rydułtowach	5	-	Tak	Min. 3.0 Gbps	Min. 30	10
4	Miejski Zespół Placówek Oświatowych	5	-	Tak	Min. 3.0 Gbps	Min. 30	10
5	Rydułtowski Ośrodek Sportu i Rekreacji	5	-	Tak	Min. 3.0 Gbps	Min. 30	25
6	Ognisko Pracy Pozaszkolnej w Rydułtowach	5	-		Min. 1 Gbps	Min. 10	10
7	Państwowe Ognisko Plastyczne im. Ludwika Konarzewskiego Seniora w Rydułtowach	5	-		Min. 1 Gbps	Min. 10	10
8	Biblioteka Publiczna Miasta Rydułtowy	5	-		Min. 1 Gbps	Min. 10	10
9	Szkoła Podstawowa nr 1 w Rydułtowach	8	-		Min. 1 Gbps	Min. 50	50
10	Szkoła Podstawowa nr 2 w Rydułtowach	8	-		Min. 1 Gbps	Min. 50	50
11	Szkoła Podstawowa nr 3 w Rydułtowach	5	-		Min. 1 Gbps	Min. 10	10
12	Szkoła Podstawowa nr 4 w Rydułtowach	5	-		Min. 1 Gbps	Min. 10	10
13	Publiczne Przedszkole nr 1 im. Marii	5	-		Min. 1 Gbps	Min. 10	10

	Kownackiej w Rydułtowach						
14	Publiczne Przedszkole nr 2 w Rydułtowach	5	-	-	Min. 1 Gbps	Min. 10	10
15	Przedszkole Publiczne nr 3	5	-	-	Min. 1 Gbps	Min. 10	10
16	Publiczne Przedszkole nr 4 w Rydułtowach	5	-	-	Min. 1 Gbps	Min. 10	10
17	Miejski Żłobek w Rydułtowach	5	-	-	Min. 1 Gbps	Min. 10	10
18	Rydułtowskie Centrum Kultury FENIKS	5	-	Tak	3.0 Gbps	Min. 30	25

Dodatkowo wszystkie urządzenia muszą być wyposażone w następujące porty:

- Minimum 2 porty USB.
- Minimum 1 port typu Console.

XVI. Wymagania dotyczące dokumentacji

Wykonawca zobowiązany będzie do przygotowania i dostarczenia wraz z urządzeniami dokumentu wskazującego metodykę zabezpieczeń połączeń wewnątrz jednostek oraz na zewnątrz jednostek dla każdej jednostki osobno. Opisana metodyka musi uwzględniać instrukcję przywracania urządzeń do ustawień fabrycznych, opis konfiguracji urządzeń z uwzględnieniem logiki zastosowanej dla konkretnej jednostki, a także sposób konfiguracji urządzeń w sytuacji jeśli Zamawiający zdecydowałby się na zmianę połączeń sieciowych / Internetowych dla poszczególnych jednostek (np. połączenia realizowane za pomocą włókna światłowodowego z dostępem do Internetu od zewnętrznego dostawcy lub szarego włókna światłowodowego w relacji jednostka-Urząd Miasta Rydułtowy).

Wraz z dokumentem opisującym schemat konfiguracji urządzeń Wykonawca zobowiązany zostanie do dostarczenia instrukcji obsługi oraz zestawu haseł administracyjnych dla każdego urządzenia osobno.

Dokumentacja musi zostać przygotowana dla każdego urządzenia oddzielnie. Zamawiający dopuszcza dostarczenie dokumentacji w wersji elektronicznej (na dysku CD lub pendrive).

XVII. Wymagania dodatkowe

1. Wykonawca w ramach przedmiotu zamówienia zobowiązuje się do instalacji i konfiguracji systemów bezpieczeństwa w miejscu wskazanym przez zamawiającego.
2. Wykonawca w ramach przedmiotu zamówienia skonfiguruje wszystkie urządzenia zgodnie z najlepszymi praktykami w zakresie konfiguracji urządzeń tego typu.
3. Wykonawca w ramach przedmiotu zamówienia skonfiguruje urządzenie dostarczone do Urzędu Miasta Rydułtowy w taki sposób, aby zabezpieczało ono wszystkie usługi sieciowe, które są obecnie zabezpieczane przez urządzenie posiadane przez Urząd Miasta. -
4. Wykonawca w ramach przedmiotu zamówienia zobowiązuje się do zapewnienia i przeprowadzenia szkolenia z zakresu podstawowej obsługi zainstalowanych urządzeń dla maksymalnie 17 użytkowników. Szkolenie nie musi kończyć się zdobyciem certyfikatów przez uczestników szkolenia. Szkolenie może odbyć się w formie on-line (szkolenie niecertyfikowane).
5. Wykonawca w ramach przedmiotu zamówienia zobowiązuje się do zapewnienia i przeprowadzenia pełnego szkolenia z zakresu rozszerzonej obsługi dostarczonych urządzeń dla maksymalnie 3 użytkowników. Szkolenie musi kończyć się zdobyciem certyfikatów przez uczestników szkolenia. Szkolenie może odbyć się w formie on-line (szkolenie certyfikowane).
6. Zamawiający oczekuje skonfigurowania, dostarczenia i zainstalowania zamówionych urządzeń w ciągu maksymalnie 8 tygodni od momentu podpisania umowy.
7. Przeprowadzenie szkolenia niecertyfikowanego dla max. 17 użytkowników oraz pełnego szkolenia certyfikowanego dla max. 3 administratorów wskazanych przez Zamawiającego. Szkolenie musi zostać przeprowadzone przed uruchomieniem urządzeń.

Załącznik nr 1

Spis jednostek w których zainstalowane zostaną urządzenia

1. Urząd Miasta Rydułtowy, Rydułtowy ul. Ofiar Terroru 36
2. Zakład Gospodarki Komunalnej, Rydułtowy ul. Raciborska 150
3. Miejski Ośrodek Pomocy Społecznej, Rydułtowy ul. Raciborska 369
4. Miejski Zespół Obsługi Placówek Oświatowych (centrum usług wspólnych), Rydułtowy ul. Raciborska 369,
5. Rydułtowski Ośrodek Sportu i Rekreacji, Rydułtowy ul. Generała Józefa Bema 126c
6. Ognisko Pracy Pozaszkolnej, Rydułtowy ul. Adama Mickiewicza 33
7. Państwowe Ognisko Plastyczne im. Ludwika Konarzewskiego Seniora, Rydułtowy ul. Adama Mickiewicza 33
8. Biblioteka Publiczna Miasta Rydułtowy im. Henryka Mikołaja Góreckiego, Rydułtowy ul. Adama Mickiewicza 33,
9. Szkoła Podstawowa nr 1 im. Karola Miarki, Rydułtowy ul. Świętego Maksymiliana Kolbego 5
10. Szkoła Podstawowa nr 2, Rydułtowy ul. Raciborska 27
11. Szkoła Podstawowa nr 3 im. Arki Bożka, Rydułtowy ul. Radoszowska 3,
12. Szkoła Podstawowa nr 4, Rydułtowy ul, Strzelców Bytomskich 13,
13. Publiczne Przedszkole nr 1 im. Marii Kownackiej, Rydułtowy ul. Kochanowskiego 25,
14. Publiczne Przedszkole nr 2 im. Czesława Janczarskiego, Rydułtowy ul. Raciborska 216
15. Publiczne Przedszkole nr 3, Rydułtowy Osiedle Orłowiec 39
16. Publiczne Przedszkole nr 4 im. J. Brzechwy, Rydułtowy Osiedle Orłowiec 37
17. Miejski Żłobek, Rydułtowy Osiedle Orłowiec 39
18. Rydułtowskie Centrum Kultury FENIKS, Rydułtowy ul. Strzelców Bytomskich 9a