Swarzędz: Dostawa sprzętu teleinformatycznego w ramach realizacji projektu pt.: Ochrona najbiedniejszych mieszkańców Gminy Swarzędz przed wykluczeniem cyfrowym. Działanie 8.3 - przeciwdziałanie wykluczeniu cyfrowemu - enclusion.
Numer ogłoszenia: 155609 - 2009; data zamieszczenia: 14.09.2009
OGŁOSZENIE O ZAMÓWIENIU - dostawy

Zamieszczanie ogłoszenia: obowiązkowe.

Ogłoszenie dotyczy: zamówienia publicznego.

SEKCJA I: ZAMAWIAJĄCY

I. 1) NAZWA I ADRES: Gmina Swarzędz , Rynek 1, 62-020 Swarzędz, woj. wielkopolskie, tel. (061) 65 12 000, faks (061) 65 12 211.

- **Adres strony internetowej zamawiającego:** www.swarzedz.pl

I. 2) RODZAJ ZAMAWIAJĄCEGO: Administracja samorządowa.

SEKCJA II: PRZEDMIOT ZAMÓWIENIA

II.1) OKREŚLENIE PRZEDMIOTU ZAMÓWIENIA

II.1.1) Nazwa nadana zamówieniu przez zamawiającego: Dostawa sprzętu teleinformatycznego w ramach realizacji projektu pt.: Ochrona najbiedniejszych mieszkańców Gminy Swarzędz przed wykluczeniem cyfrowym. Działanie 8.3 - przeciwdziałanie wykluczeniu cyfrowemu - enclusion..

II.1.2) Rodzaj zamówienia: dostawy.

II.1.3) Określenie przedmiotu oraz wielkości lub zakresu zamówienia: Przedmiotem zamówienia jest dostawa i montaż sprzętu teleinformatycznego według poniższy wymagań 1.Przełącznik MPLS - 3 sztuki 1.1.Cechy Ogólne 1.1.1.12 portów 1GE Combo z możliwością instalowania modułów SFP 100Mbps (100Base-X SFP lub 1000Base-X SFP lub 10-100-1000Base-T), 1.1.2.hot- swappable SFP (na długie i krótkie dystanse, multi-rate, xWDM), 1.1.3.automatyczne rozpoznawanie rodzaju kabla miedzianego: Auto- MDI-MDIX, 1.1.4.porty zarządzające out-of-band RS-232 oraz Ethernet, 1.1.5.matryca: non-blocking wire-speed, 1.1.6.tablica adresów MAC: 16K, 1.1.7.obsługa ramek Jumbo (16 000 B) na wszystkich portach, 1.1.8.redundantne zasilanie AC, 1.1.9.temperatura pracy: 0oC - 45oC, 1.1.10.możliwość zamontowania w szafie Rack 19, 1.1.11.możliwość montażu na ścianie, 1.1.12.wysokość 1U, 1.2.Przełączanie 1.2.1.IEEE 802.1Q oraz 802.1ad: 1.2.1.1.możliwość zdefiniowania do 4K aktywnych VLANów, 1.2.1.2.mechanizm Q-in-Q na port + VLAN, 1.2.2.transparentny tryb cross-connect (no MAC learning), 1.2.3.Limit learning table na VLAN-port, 1.2.4.Ochrona przed awarią: 1.2.4.1.automatyczne przełączanie optyczne na łączach sieci (1+1) 1.2.4.2.IEEE 802.3ad Link Aggregation 1.2.4.3.IEEE 802.1s Multiple Instance Spanning Tree 1.2.4.4.kompatybilny z 802.1w-d 1.3.Zarządzanie ruchem (zgodne z MEF) 1.3.1.Zarządzanie ruchem inbound i outbound w obrębie strumienia, 1.3.2.Klasyfikacja na podstawie portu fizycznego, adresu MAC, polu Ethertype w ramce ethernetowej, VLAN, IP-TC-UDP, 802.1.p (VTP), DiffServe, 1.3.3.Oznaczanie- odznaczanie profili pomiędzy warstwami (802.1p ToS oraz MPLS EXP), 1.3.4.8 sprzętowych kolejek na port i konfigurowalny adaptacyjny bufor Cos, 1.3.5.Zastawy liczników pakietów In-profile & out-of-profile, 1.3.6.ograniczanie ruchu zależne od klasy, 1.3.7.HQoS (możliwość ograniczania ruchu na port/kolejkę jednocześnie), 1.4.Usługi warstwy 2- Tunelowanie 1.4.1.Q-in-Q - mapped mode or translation, 1.4.2.Layer 2 VPN - Martini MPLS pseudo-wire, 1.4.3.Spoke H-VPLS, 1.5.Usługi IP 1.5.1.RIP v1, v2, 1.5.2.OSPF, 1.5.3.Intermediate System to Intermediate System (IS - IS) Protocol, 1.5.4.BGPv4, 1.5.5.Virtual Router Redundancy Protocol (VRRP), 1.5.6.Network Address Translation (NAT), 1.5.7.DHCP Server-Client-Relay, 1.6.Bezpieczeństwo 1.6.1.Ochrona CPU Dos, 1.6.1.1.Kontrola prędkości ramek, 1.6.1.2.Kolejki dedykowane, 1.6.2.Wire-speed Access Control Lists, 1.6.3.Filtrowanie po MAC, ARP oraz BPDU, 1.6.4.Ograniczanie prędkości dla pakietów typu Unicast-Multicast-Broadcast,

1.6.5.IEEE 802.1x, 1.6.6.Stateful Firewall, 1.7.Zarządzanie 1.7.1.Zarządzanie out-of-band- EIA-232 console, 1.7.2.Zarządzanie out-of-band - dedykowany ethernetowy port Ethernet, 1.7.3.TELNET, SSH v2, SNMPv3, RMON (4 grupy), 1.7.4.Ping, Trace route, DNS lookup, TCP dump (wbudowany sniffer), 1.7.5.Port monitorujący (mirroring-monitoring) ruch przychodzący i wychodzący do portu analizującego, 1.7.6.Port miroring na ACL - Sniffer VLAN, 1.7.7.Zarządzanie ACL dla zaufanych połączeń (Telnet, SSH, SNMP), 1.7.7.1.RADIUS AAA dla zarządzania sesją (AAA- Authentication, Authorization and Accounting), 1.7.8.Możliwość ściągnięcia- zachowania konfiguracji na serwerze FTP, 1.7.9.NTP - Network Time Protocol, 1.7.10.Logging Syslog, 1.7.11.Skrypty dla konfiguracji macro i zarządzania, 1.7.12.Możliwość wydawania zestawów komend w zdefiniowane wcześniej dni-godziny, 1.8.OAM Service Assurance Tool 1.8.1.Zaawansowane narzędzia monitoringu i zarządzania SLA: 1.8.1.1.funkcjonalność lokalnej i zdalnej pętli zwrotnej (loopback), 1.8.1.2.loopback na VLAN oraz MAC swapping, 1.8.1.3.zaawansowane techniki mierzenia opóźnień-Jittera (QoS Verification), 1.8.2.Service end-to-end OAM - Connectivity Fault Management, 1.8.3.Link OAM - Auto-discovery zgodny z IEEE802.3ah, 1.8.4.OAM warstwy fizycznej - Cable Diagnostics: 1.8.4.1.Monitorowanie poziomów potycznych - Digital Diagnostics (SFP SFF - 8472), 1.8.4.2.sprawdzanie jakości torów miedzianych na portach RJ45, 1.8.5.Remote failure notification - reflaction- Link Integrity Notification (LIN), 1.9.Usługi MPLS 1.9.1.MPLS VC - LDP, 1.9.1.1.RSVP-TE, 1.9.1.2.CR-LDP, 1.9.1.3.OSPF-TE, 1.9.1.4.CSPF, 1.10.Zgodność ze standardami: 1.10.1.IEEE 1.10.1.1.IEEE 802.3z Gigabit Ethernet (1000Base-SX/LX) 1.10.1.2.IEEE 802.3ab Gigabit Ethernet Copper 1.10.1.3.IEEE 802.3ad Link Agregation 1.10.1.4.IEEE 802.3ah Ethernet in the First Mile 1.10.1.5.IEEE 802.1D Bridging and Spanning Tree 1.10.1.6.IEEE 802.1p Layer 2 priority QoS Support 1.10.1.7.IEEE 802.1Q VLAN Tagging 1.10.1.8.IEEE 802.1w Rapid STP 1.10.1.9.IEEE 802.1s MSTP 1.10.1.10.IEEE 802.1x Port-based Network Access Control 1.10.1.11.IEEE 802.1ad Provider bridges (partial draft) - Q-in-Q stacking per VLAN-port 1.10.2.IETF 1.10.2.1.RFC 1591 DNS client 1.10.2.2.RFC 1643 Ethernet MIB 1.10.2.3.RFC 1757 RMON 4 groups 1.10.2.4.RFC 1902 Structure of Management Information for SNMPv2 1.10.2.5.RFC 1907 SNMPv2 1.10.2.6.RFC 2030 SNTP 1.10.2.7.RFC 2131 BootP and DHCP Relay 1.10.2.8.RFC 2236 IGMP v2 1.10.2.9.RFC 2267 Network Ingress Filtering 1.10.2.10.RFC 2370 Opaque LSA support 1.10.2.11.RFC 2385 MD5 peer password authentication 1.10.2.12.RFC 2430 A Provider architecture for DiffServ and T 1.10.2.13.RFC 2475 DiffServ of DS field in IPv4 - IPv6 headers 1.10.2.14.RFC 2571 - 2575 SNMPv3 1.10.2.15.RFC 2597 DiffServ AF PHB 1.10.2.16.RFC 2598 DiffServ EF PHB 1.10.2.17.RFC 2702 Traffic Engineering over MPLS 1.10.2.18.RFC 2787 VRRP MIB 1.10.2.19.RFC 2819 RMON MIB 1.10.2.20.RFC 2865 RADIUS Authentication 1.10.2.21.RFC 2866 RADIUS Accounting 1.10.2.22.RFC 2925 Management SLA MIB - ping 1.10.2.23.RFC 3031 MPLS Architecture 1.10.2.24.RFC 3032 MPLS Label Stack Encoding 1.10.2.25.RFC 3036 LDP Specifications 1.10.2.26.RFC 3037 LDP Applicability 1.10.2.27.RFC 3063 MPLS loop prevention mechanism 1.10.2.28.RFC 3140 DiffServ PHB identification codes 1.10.2.29.RFC 3164 Syslog 1.10.2.30.RFC 3209 Extensions to RSVP for LSP tunnels (RSVP-TE) 1.10.2.31.RFC 3210 Applicability statement for extensions to RSVP for LSP tunnels (RSVP-TE) 1.10.2.32.RFC 3212 CR-LDP 1.10.2.33.RFC 3246 AF-PHB Group 1.10.2.34.RFC 3376 IGMP Ver. 3 1.10.2.35.RFC 3410 SNMP version 3 Framework 1.10.2.36.RFC 3411 An Architecture for Describing SNMP Management Frameworks 1.10.2.37.RFC 3412 Message Processing and Dispatching for SNMP 1.10.2.38.RFC 3413 SNMP Applications 1.10.2.39.RFC 3414 User-based Security Model (USM) for SNMPv3 1.10.2.40.RFC 3415 View-based Access Control Model (VACM) for SNMP 1.10.2.41.RFC 3416 Version 2 of the Protocol Operations for SNMP 1.10.2.42.RFC 3418 Management Information Base (MIB) for SNMP 1.10.3.IETF Drafts 1.10.3.1.draft-IETF-L2circuit-trans-MPLS-08 1.10.4.draft-IETF-L2circuit-encap-MPLS-04 2.Moduł SFP 100Base-FX - 24 sztuki 2.1.szybkość transmisji: 100Mbps, Fast Ethernet, 2.2.praca na dwóch włóknach jednomodowych, 2.3.zasięg 20km, 2.4.możliwość dynamicznego podglądu parametrów technicznych modułu z poziomu urządzenia, w którym jest zainstalowane, 2.5.w celu uzyskania pełnej kompatybilności moduły SFP muszą pochodzić od tego samego producenta co oferowane przełączniki MPLS. 3.Moduł SFP 1000Base-LX - 24 sztuki 3.1.szybkość transmisji: 1000Mbps, Gigabit Ethernet, 3.2.praca na dwóch włóknach jednomodowych, 3.3.zasięg 20km, 3.4.możliwość dynamicznego podglądu parametrów technicznych modułu z poziomu urządzenia, w którym jest zainstalowane, 3.5.w celu uzyskania pełnej kompatybilności moduły SFP muszą pochodzić od tego samego producenta co oferowane przełączniki MPLS. 4.Konwerter światłowodowy - 6 sztuk 4.1.szybkość transmisji: 100Mbps, Fast Ethernet, 4.2.praca na dwóch włóknach jednomodowych, 4.3.wejście RJ45 10-100Base-T, 4.4.zasięg 20km. 5.Sieciowy Punkt Dostępowy AP - 9 sztuk 5.1.Punkt Dostępowy typu thin Access Points, czyli Punkt w pełni zarządzalny przez kontroler, 5.2.konfiguracja

dystrybuowana na punkt dostępowy z kontrolera w sposób automatyczny, bazujący na regułach zdefiniowanych globalnie przez administratora, 5.3.Punkty Dostępowe pracujące dwukanałowo, obsługujące standardy 802.11a oraz 802.11b-g, 5.4.funkcja detekcji intruzów, w szczególności fałszywych punktów dostępowych, 5.5.Punkty dostępowe wyposażone w dwie wbudowane anteny dookolne, oraz wyjścia typu reverse-SMA, pozwalające na podłączenie co najmniej dwóch anten zewnętrznych, 5.6.Urządzenia obsługują Power over Ethernet w standardzie 802.3af, 5.7.obsługiwane prędkości transmisji danych: 1-2-5.5-6-9-11-12-18-24-36-48-54Mbps (dla 2.4GHz), 6 - 54 Mbps (dla 5GHz), 5.8.Obsługiwane modulacje: DSSS, OFDM, BPSK, QPSK, CCK, 16QAM, 64QAM, 5.9.Zaoferowane Punkty Dostępowe muszą współpracować z posiadanym przez Zamawiającego kontrolerem. 5.10.Punkty dostępowe należy zainstalować w obiektach wskazanych przez zamawiającego oraz podłączyć i uruchomić. Należy do montażu przyjąć konieczność ułożenia 60 m kabli LAN i zasilających w listwach PCV. 6.Antena dookólna - 9 sztuk 6.1.antena o charakterystyce dookolnej, 6.2.zysk energetyczny nie mniejszy niż 10dB, 6.3.kąt promieniowania w płaszczyźnie poziomej: 360o, 6.4.kąt promieniowania w płaszczyźnie pionowej nie mniej niż 14o, 6.5.polaryzacja fali: pozioma, 6.6.złącze typu N, 6.7.antena dostarczona z zestawem do montażu. 6.8.Anteny należy zainstalować na elewacji budynku i podłączyć do Punktu Dostepowego opisanego w pkt. 5 - wysokość montażu wymaga użycia podnośnika koszowego 7 Firewall-UTM sprzętowy - 1 sztuka 7.1 Urządzenie musi być wyposażone w co najmniej 1 GB pamięci RAM, pamięć Flash 1 GB oraz port konsoli. Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego firewalla z nośnika danych podłączonego do slotu USB na module kontrolnym. 7.2 System operacyjny firewalla musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł rutingu IP, odpowiedzialny za ustalenie tras rutingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. System operacyjny firewalla musi śledzić stan sesji użytkowników (stateful processing), tworzyć i zarządzać tablicą stanu sesji. Musi istnieć opcja przełączenia urządzenia w tryb pracy bez śledzenia stanu sesji użytkowników, jak również wyłączenia części ruchu ze śledzenia stanu sesji. 7.3 Urządzenie musi być wyposażone w nie mniej niż 2 wbudowane interfejsy Ethernet 10-100-1000 oraz 6 wbudowanych interfejsów Fast Ethernet 10-100 (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji). 7.4 Urządzenie musi być wyposażone w 1 slot na dodatkowe karty z modułami interfejsów. Urządzenie musi obsługiwać co najmniej następującej rodzaje kart z modułami interfejsów: ADSL 2-2+, Serial, E1, Gigabit Ethernet (SFP). Ponadto urządzenie musi posiadać slot na podłączenie karty 3G ExpressCard z modemem HSDPA. 7.5 Firewall musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż 12 strefami bezpieczeństwa z wydajnością nie mniejszą niż 250 Mb-s liczoną dla ruchu IMIX, oraz wydajnością maksymalną nie mniejszą niż 750Mb-s. 7.6 Firewall musi przetworzyć nie mniej niż 80 000 pakietów-sekundę (dla pakietów 64-bajtowych). 7.7 Firewall musi obsłużyć nie mniej niż 32 000 równoległych sesji (z w pełni włączonym silnikiem UTM) oraz nie mniej niż 64 000 równoległych sesji bez uruchomionej funkcjonalności UTM. 7.8 Firewall musi zestawiać nie mniej niż 2 000 nowych połączeń-sekundę. 7.9 Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN musi być realizowany sprzętowo. Firewall musi obsługiwać nie mniej niż 250 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 75 Mb-s. Urządzenie musi posiadać możliwość udostępniania użytkownikom wbudowanego klienta IPSec VPN za pośrednictwem strony WWW. 7.10 Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Firewall musi umożliwiać zdefiniowanie nie mniej niż 500 reguł polityki bepieczństwa. 7.11 Firewall musi posiadać funkcję wykrywania i blokowania ataków intruzów (IPS, intrusion prevention) realizowaną sprzętowo. System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące (D)DoS oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych ataków (intruzów, robaków) musi odbywać się w regułach polityki bezpieczeństwa. System firewall musi realizować zadania IPS z wydajnością nie mniejszą niż 80 Mb-s. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall przez okres minimum 3 lat. Baza sygnatur ataków musi być aktualizowana przez producenta codziennie. 7.12 Urządzenie zabezpieczeń

musi posiadać wbudowany moduł kontroli antywirusowej kontrolujący pocztę elektroniczną (SMTP, POP3, IMAP), FTP oraz HTTP. Włączenie kontroli antywirusowej nie może wymagać dodatkowego serwera. Kontrola antywirusowa musi być realizowana sprzętowo z wydajnością nie mniejszą niż 30 Mb-s dla ruchu HTTP. Musi istnieć możliwość wyboru działania mechanizmu kontroli antywirusowej w trybie sprzętowym i programowym. 7.13 Urządzenie zabezpieczeń musi posiadać wbudowany moduł kontroli antyspamowej działający w oparciu o mechanizm blacklist. Włączenie kontroli antyspamowej nie może wymagać dodatkowego serwera. 7.14 Urządzenie zabezpieczeń musi posiadać wbudowany moduł filtrowania stron WWW w zależności od kategorii treści stron. Włączenie filtrowania stron WWW nie może wymagać dodatkowego serwera. 7.15 Urządzenie zabezpieczeń musi posiadać funkcję filtrowania zawartości ruchu HTTP, FTP i protokołów poczty elektronicznej (SMTP, POP3, IMAP) w celu blokowania potencjalnie szkodliwych obiektów. Urządzenie musi filtrować ruch na podstawie kryteriów obejmujących co najmniej: typy MIME, rozszerzenia plików, elementy ActiveX, Java i cookies. 7.16 Urządzenie musi obsługiwać protokoły dynamicznego rutingu: RIP, OSPF oraz BGP. Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 10 wirtualnych ruterów. 7.17 Urządzenie musi posiadać możliwość uruchomienia funkcji MPLS z sygnalizacją LDP i RSVP w zakresie VPLS i L3 VPN. 7.18 Urządzenie musi obsługiwać co najmniej 64 sieci VLAN z tagowaniem 802.1Q. W celu zapobiegania zapętlania się ruchu w warstwie 2 firewall musi obsługiwać protokoły Spanning Tree (802.1D), Rapid STP (802.1W) oraz Multiple STP (802.1S). Urządzenie musi obsługiwać protokół LACP w celu agregowania fizycznych połączeń Ethernet. 7.19 Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS - wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków TCP i UDP. Urządzenie musi posiadać tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach. 7.20 Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. 7.21 Zarządzanie urządzeniem musi odbywać się za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH. Firewall musi posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta. 7.22 Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji. 7.23 Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone są w języku polskim. 7.24 Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przez okres trzech lat oraz aktualnej bazy sygnatur ataków, definicji wirusów, blacklist antyspamowych oraz bazy kategorii stron WWW przez okres trzech lat. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta (w języku polskim) i lub polskiego dystrybutora sprzętu, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. 7.25 Urządzenie należy zainstalować w szafie serwerowni i włączyć do sieci. 8 Komputer przenośny (Notebook) - 103 kpl. Poniższe wymagania są wymaganiami minimalnymi. 8.1 Procesor: dwurdzeniowy AMD Turion X2 RM-76, 2,3GHz, 1 MB pamięci podręcznej L2 lub procesor o równoważnej wydajności (np. Intel lub inny producent) zaprojektowany do pracy w urządzeniach przenośnych 8.2 Zainstalowana pamięć operacyjna: 2GB z wolnym slotem na rozszerzenie pamięci do 8GB 8.3 Rodzaj pamięci: DDR2 8.4 Płyta główna: jednoprocesorowa oparta o chipset rekomendowany przez producenta procesora i oznaczona trwałym logiem producenta. 8.5 Porty: 4x USB 2.0, 1x VGA, 1 x HDMI, wyjście audio(słuchawkowe), wejście audio (mikrofon),1 x RJ-45, 1 x ExpressCard-34 8.6 Sterownik dysku HDD: SATA II 8.7 Pojemność dysku HDD: 250GB SATAII 5400rpm 8.8 Napęd optyczny: DVD + -RW Dual Layer 8.9 Stacja dyskietek: bez FDD, wbudowany czytnik kart pamięci 7w1 8.10 Karta dźwiękowa: zintegrowana na płycie głównej, high definition, podłączona do 2 głośników stereo w obudowie, wbudowany mikrofon 8.11 Karta graficzna: zgodna z DirectX 10 8.12 Komunikacja: zintegrowana na płycie głównej karta sieciowa pracująca z szybkością 10-100-1000 Mbit-s, sieciowy moduł bezprzewodowy Wireless zgodny z 802.11a-b,g,n, zintegrowany Bluetooth 2.0 8.13 Bezpieczeństwo: osobne hasło do BIOS-u oraz startu systemu (Power-on password), wbudowana w bios

funkcjonalność pozwalająca na bezpieczne usuwanie danych z dysku twardego, możliwość startu systemu z urządzeń USB, możliwość blokowania zapisu i odczytu na dyskietkę i porty USB, Driver Lock Password, Kensington Lock Slot, mechanizm zabezpieczający dysk twardy przed uszkodzeniami poprzez parkowanie głowicy dysku w postaci czujnika wykrywającego przeciążenia, 8.14 Mysz: TouchPad z funkcją przewijania 8.15 Klawiatura: w obudowie notebooka w układzie US Standard z klawiaturą numeryczną 8.16 Waga: maksimum 2,6 kg - waga z baterią podstawową 8.17 Zasilacz: zewnętrzny, zasilany napięciem 100-240V 8.18 Zasilanie bateryjne: Litium-Ion pozwalające na pracę przez minimum 3 godziny. 8.19 System operacyjny: Microsoft Vista Business 32 PL (preload) i Microsoft Windows XP Pro PL; system operacyjny i nośniki muszą być dołączone przez producenta komputera; nie dopuszcza się dołączenia systemu operacyjnego przez Wykonawcę. 8.20 Certyfikaty: zgodny z Windows Vista, poświadczone w Windows Katalog, CE, Certyfikat ISO9001:2000 dla producenta oferowanego sprzętu na proces projektowania i produkcji, EnergyStar®, EPEAT® Gold 8.21 Wyświetlacz: w obudowie notebooka, LCD o przekątnej ponad 15,4 cala z podświetlaniem LED, o rozdzielczości min.1366x768 pikseli, wbudowana kamerka internetowa o rozdzielczości minimum 2MP. 8.22 Wyposażenie dodatkowe: do notebooka winna być dołączona specjalistyczna torba na notebook wraz z rączką i paskiem na ramie oraz zewnętrzna mysz optyczna. 8.23 Gwarancja: 5 lat gwarancji międzynarodowej na terenie Europy w serwisie producenta (poza siedzibą Zamawiającego); W Polsce gwarancja producenta obejmująca także koszty transportu z i do punktu serwisowego; Telefoniczne zgłaszanie uszkodzeń poprzez infolinię producenta (w języku polskim). 8.24 Dokumentacja: standardowa dostarczana przez producenta 9 Samodzielny Punkt Dostępowy - 45 kpl. Podane parametry są parametrami minimalnymi 9.1 Urządzenie typu plug-and play - umożliwiające podłączenie do sieci internet po włączeniu zasilania i podłączeniu kabla do złącza RJ45. 9.2 Urządzenie przystosowane do pracy w technologi CDMA 2000, 1xEV-DO Rev A i paśmie 450 MHz z możliwością instalacji karty mikroprocesorowej- aktywowane w sieci umożliwiającej dostęp do zasobów internetu - wymagany zasięg na terenie całej Gminy Swarzędz 9.3 Urządzenie musi być wyposażone w anteny lokalne (dołanczane bezpośrednio do urządzenia) pracujące w technologi Recive Diversity umożliwiające zwiększenie zasięgu i przepustowości, Po dwie anteny do pracy z siecią dostawcy oraz lokalnie w sieci Wi-FI 9.4 Zamawiający nie przewiduje montażu anten zewnętrznych dla potrzeb pracy urządzenia w sieci dostawcy. 9.5 Urządzenie musi posiadać port usb 9.6 Zintegrowany 4 portowy przełącznik 10-100 Ethernet -umożliwiające budowę lokalnej sieci LAN 9.7 Wbudowany protokół DHCP 9.8 Translacja adresu sieciowego NAT 9.9 Zintegrowany punkt dostępu bezprzewodowego pracujący w technologi Wi -Fi 802.11 b-g 9.10 Filtrowanie urządzeń po adresie MAC 9.11 Urządzenie wyposażone w zasilacz do pracy z napięciem sieciowym 230V oraz baterie umożliwiającą pracę po zaniku sieci min przez 2 h. 9.12 Zewnętrzna sygnalizacja LED - stanu pracy urządzenia 9.12.1 zasilania 9.12.2 siły sygnału sieci 9.12.3 połączenia z siecią 9.12.4 typu połączenia 9.12.5 stanu pracy sieci Ethernet z rozbiciem na poszczególne porty 9.12.6 stanu pracy sieci Wi-Fi 9.13 Administrowanie urządzeniem poprzez przeglądarkę internetową zabezpieczone loginem i hasłem umożliwiające: 9.13.1 Sprawdzenie aktualnych ustawień i statusu modemu 9.13.2 Skonfigurowanie funkcji rutera umożliwiających łączenie się z siecią przy ustawieniach zdefiniowanych przez Zamawiającego 9.13.3 Zmianę ustawień sieci, adres wewnętrzny IP ustawienia serwera DHCP 9.13.4 Ustawienia zapory sieciowej - port forwarding 9.13.5 Ustawienie zabezpieczeń sieci, blokada klientów, filtrowanie adresów MAC, szyfrowanie WEP i WPA 9.13.6 Ustawienie obszaru DMZ 9.13.7 Zmianę haseł 9.13.8 Ponowne uruchomienie 9.13.9 Uaktualnić oprogramowanie modemu 9.13.10 Ustawienie blokady WAN Ping 9.13.11 Ustawienie blokady HTTP Ping 9.13.12 Ustawienie rutingu statycznego 9.14 Oprogramowanie do instalacji na komputerze umożliwiające podłączenia urządzenia w sieci dostawcy oraz stwierdzenia stanu pracy urządzenia. 9.15 Urządzenie musi umożliwiać współprace z AP opisanego w pkt 5. 9.16 Urządzenie ma być przystosowane do montażu naściennego. 9.17 W komplecie należy dostarczyć kabel do podłączenia poprzez port USB i Ethernet. 9.18 Urządzenie ma być wyposażone w płytę instalacyjną ze sterownikami oraz instrukcje obsługi w języku polskim. 9.19 Urządzenie ma być zgodne ze standardami 9.19.1 Dyrektywa R & TTE 1999-5-WE 9.19.2 EN-60950-1 :2001 - Bezpieczeństwo 9.19.3 EN 50360: 2001, EN 5360: 2001 SAR 9.19.4 EN 301 489-1 V1.6.1 (2005-9) ETSI, EN 301 489-25 V2.3.2 (2005-07) Standard EMC 9.19.5 EN 301 526V1,1,1 (2006-07) Standard RF(z RSE).

II.1.4) Wspólny Słownik Zamówień (CPV): 30.23.12.00-9, 30.23.12.20-5, 32.58.10.00-9, 32.57.10.00-6.

II.1.5) Czy dopuszcza się złożenie oferty częściowej: nie.

II.1.6) Czy dopuszcza się złożenie oferty wariantowej: nie.

II.1.7) Czy przewiduje się udzielenie zamówień uzupełniających: nie.

II.2) CZAS TRWANIA ZAMÓWIENIA LUB TERMIN WYKONANIA: Okres w dniach: 30.

SEKCJA III: INFORMACJE O CHARAKTERZE PRAWNYM, EKONOMICZNYM, FINANSOWYM I TECHNICZNYM

III.1) WARUNKI DOTYCZĄCE ZAMÓWIENIA

Informacja na temat wadium: Zamawiający wymaga wniesienia wadium w wysokości 15000.00 zł

III.2) WARUNKI UDZIAŁU

- **Opis warunków udziału w postępowaniu oraz opis sposobu dokonywania oceny spełniania tych warunków:** 2.1.O udzielenie zamówienia publicznego mogą ubiegać się wyłącznie Wykonawcy, którzy spełniają następujące warunki: a)Posiadają uprawnienia do wykonywania przedmiotu zamówienia Prowadzą działalność gospodarczą w zakresie sprzedaży i serwisu sprzętu teleinformatycznego b)Posiadają niezbędną wiedzę i doświadczenie oraz dysponują potencjałem technicznym i osobami zdolnymi do wykonania zamówienia lub przedstawią pisemne zobowiązanie innych podmiotów do udostępnienia potencjału technicznego i osób zdolnych do wykonania zamówienia: Dysponują co najmniej jedną osobą z tytułem inżyniera, posiadającą przeszkolenie w zakresie oferowanych przełączników MPSL - do oferty należy dołączyć kserokopię dowodu odbycia szkolenia - zaświadczenie, certyfikat Wykonali w ciągu ostatnich trzech lat przed dniem wszczęcia postępowania o udzielenie zamówienia publicznego, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie minimum dwie dostawy sprzętu teleinformatycznego (w tym sprzęt transmisyjny) o wartości nie mniejszej niż 250.000,00 zł każda. Do oferty należy dołączyć referencje potwierdzające: datę wykonania dostawy, zakres przedmiotowy dostawy, jej wartość oraz stwierdzenie, iż dostawa ta została wykonana należycie. b)Znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia, tj.: spełniają następujące warunki: posiadają polisę ubezpieczeniową OC w zakresie prowadzonej działalności gospodarczej c)Nie podlegają wykluczeniu z postępowania o udzielenie zamówienia. d)Załączą do oferty dokumenty zgodnie z Rozdziałem 3. Zamawiający oceni spełnianie warunków udziału w postępowaniu na podstawie dokumentów złożonych wraz z ofertą, w skali spełnia - nie spełnia..
- **Informacja o oświadczeniach i dokumentach, jakie mają dostarczyć wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu:** Zamawiający żąda: 1.Wypełnionego i podpisanego DRUKU OFERTY (zgodnie z załączonym formularzem - ROZDZIAŁ 4); 2.Pełnomocnictwa dla jednego z wykonawców wspólnie ubiegających się o udzielenie zamówienia do reprezentowania ich w postępowaniu o udzielenie zamówienia i zawarcia umowy w sprawie zamówienia zgodnie z art. 23 ust. 2 ustawy Prawo zamówień publicznych. 3.Oświadczenia o spełnieniu warunków zawartych w art. 22 ust. 1 ustawy prawo zamówień publicznych (zgodnie z ZAŁĄCZNIKIEM NR 1); 4.Upoważnienia do podpisania oferty - jeżeli nie wynika z załączonego odpisu z właściwego rejestru albo aktualnego zaświadczenia o wpisie do ewidencji działalności gospodarczej. II. W celu potwierdzenia, że Wykonawca posiada uprawnienie do wykonywania określonej działalności lub czynności oraz nie podlega wykluczeniu, Zamawiający żąda: 1.Aktualnego odpisu z właściwego rejestru albo aktualnego zaświadczenia o wpisie do ewidencji działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub zgłoszenia do ewidencji działalności gospodarczej, wystawionego nie wcześniej niż 6 miesięcy przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert;

2.Oświadczenie, że Wykonawca nie zalega z opłaceniem podatków, opłat oraz składek na ubezpieczenie społeczne lub zdrowotne lub uzyskał zgodę na zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności, lub wstrzymanie w całości wykonania decyzji organu podatkowego (zgodnie z ZAŁĄCZNIKIEM Nr 2); III. W celu potwierdzenia opisanego przez Zamawiającego warunku posiadania przez Wykonawcę niezbędnej wiedzy i doświadczenia oraz dysponowania potencjałem technicznym i osobami zdolnymi do wykonania zamówienia, Zamawiający żąda: 1.Wykazu wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, dostaw w okresie ostatnich trzech lat przed dniem wszczęcia postępowania o udzielenie zamówienia, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, odpowiadających swoim rodzajem i wartością dostawom lub usługom stanowiącym przedmiot zamówienia, z podaniem ich wartości, przedmiotu, dat wykonania i odbiorców (zgodnie z ZAŁĄCZNIKIEM NR 3), oraz załączenia dokumentów potwierdzających, że te dostawy lub usługi zostały wykonane należycie; 2.Wykazu osób , którymi dysponuje lub będzie dysponował wykonawca i które będą uczestniczyć w wykonywaniu zamówienia, wraz z informacjami na temat ich kwalifikacji zawodowych, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia, a także zakresu wykonywanych przez nie czynności (zgodnie z ZAŁĄCZNIKIEM NR 4); 3.Pisemnego zobowiązania innych podmiotów do udostępnienia osób zdolnych do wykonania zamówienia, jeżeli w wykazie, o którym mowa w pkt 2, wykonawca wskazał osoby, którymi będzie dysponował (zgodnie z ZAŁĄCZNIKIEM NR 5) 4.Dokumentów stwierdzających, że osoby, które będą uczestniczyć w wykonywaniu zamówienia, posiadają wymagane uprawnienia, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień. IV. W celu potwierdzenia opisanego przez Zamawiającego warunku znajdowania się przez Wykonawcę w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia, Zamawiający żąda: 1.Polisy, a w przypadku jej braku innego dokumentu potwierdzającego, że wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, kwestię dokumentów składanych na potwierdzenie w/w faktów określa §2 Rozporządzenia Prezesa Rady Ministrów z dnia 19 maja 2006 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy oraz form, w jakich te dokumenty mogą być składane (DZ.U Nr. 87,poz. 605 z 2006r. i Dz.U. Nr.188, poz. 1155 z 2008r.).

SEKCJA IV: PROCEDURA

IV.1) TRYB UDZIELENIA ZAMÓWIENIA

IV.1.1) Tryb udzielenia zamówienia: przetarg nieograniczony.

IV.2) KRYTERIA OCENY OFERT

IV.2.1) Kryteria oceny ofert: najniższa cena.

IV.2.2) Wykorzystana będzie aukcja elektroniczna: nie.

IV.3) INFORMACJE ADMINISTRACYJNE

IV.3.1) Adres strony internetowej, na której dostępna jest specyfikacja istotnych warunków zamówienia: http://bip.swarzedz.eu.
Specyfikację istotnych warunków zamówienia można uzyskać pod adresem: Siedziba Zamawiającego Rynek 1 62-020 Swarzędz pok. 410.

IV.3.4) Termin składania wniosków o dopuszczenie do udziału w postępowaniu lub ofert: 23.09.2009 godzina 10:00, miejsce: Siedziba Zamawiającego Rynek 1 62-020 Swarzędz Biuro Obsługi Interesanta -

Kancelaria Urzędu.

IV.3.5) Termin związania ofertą: okres w dniach: 30 (od ostatecznego terminu składania ofert).

IV.3.13) Informacje dodatkowe, w tym dotyczące finansowania projektu/programu ze środków Unii Europejskiej: Zamówienie współfinansowane ze Środków Unii Europejskiej przez Ministerstwo Rozwoju Regionalnegow ramach Programu Operacyjnego Innowacyjna Gospodarka.