Załącznik nr 1 do Zapytania ofertowego

Szczegółowy Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest zakup i dostawa, jak również zainstalowanie, zintegrowanie i skonfigurowanie urządzeń elektronicznych oraz oprogramowania dla Wielkopolskiego Funduszu Rozwoju sp. z o.o. w ilościach i o konfiguracji wymienionej poniżej.

I CZĘŚĆ ZAMÓWIENIA

Cześć I zamówienia obejmuje zakup i dostawę, jak również zainstalowanie, zintegrowanie i skonfigurowanie urządzenia wielofunkcyjnego A3

Urządzenie wielofunkcyjne A 3 – 1 szt. - minimalne parametry techniczne

Technologia druku	technologia laserowa, czterobębnowa
Format oryginału i kopii	A3-A6
Prędkość drukowania	min. 30 stron A4 / min. w kolorze i mono
Rozdzielczość drukowania	1200x1200 dpi
Czas wydruku pierwszej strony	kolorowej maks. 8 sek., czarno-białej maks. 6 sek.
Czas nagrzewania	maks. 20 sek. od włączenia zasilania
Kopiowanie wielokrotne	do 999 kopii
Pamięć RAM	min. 4 GB
Dysk SSD	min. 32 GB SSD
Zoom	25-400%
Panel operatora	Panel wyposażony w kolorowy ekran dotykowy LCD, opisy na panelu oraz komunikaty na ekranie w języku polskim, panel z regulowanym położeniem w min. 2 pozycjach. Integracja z aplikacjami zewnętrznymi poprzez ekran dotykowy urządzenia.

Dupleks	automatyczny, obsługa papieru 70-250 g/m^2
Podajnik dokumentów	Dwustronny, pojemność tacy podającej min. 140 ark. 80 g/m2
Podajniki papieru	• podajnik automatyczny min. 2 x 500 ark., 60-300 g/m2 (w tym min. jeden obsługujący papier formatu A3); • taca boczna na min. 150 ark. A6-A3, 60-300 g/m2
Pamięć drukarki	Współdzielona z kopiarką (dotyczy pamięci RAM i HDD)
Język opisu strony	PCL 6, Post Script Level 3 (dopuszcza się emulacje)
Interfejsy	USB 2.0, Ethernet 10/100/1000 Mb
Funkcje skanowania	skanowanie do PC, do e-mail, do FTP, TWAIN (sieciowy), do pamięci przenośnej USB, WIA, SMB, do skrzynki dokumentów
Rozdzielczość skanowania	600 dpi
Prędkość skanowania	kolor: min. 80 str. / min. (300 dpi/A4)
Typy plików	PDF, PDF/A, PDF szyfrowany, PDF kompresowany, JPEG, TIFF, XPS
Podstawa	Oryginalna podstawa producenta urządzenia, z katalogu dostępnych opcji. Zamykana, na kółkach. Dopasowana kolorystycznie, wzorniczo i kształtem do oferowanego urządzenia.
Materiały eksploatacyjne jako wyposażenie standardowe (dostarczone w komplecie z urządzeniem)	**Tonery**: w ilości, która zapewni wydrukowanie min. 15 000 stron kolorowych A4 (zgodnie z ISO 19798) **Bębny**: w ilości, która zapewni wydrukowanie min. 200 000 stron kolorowych A4. Dostarczone materiały muszą być nowe i nieużywane, oraz wyprodukowane przez producenta oferowanych urządzeń.
Gwarancja	min. 36 miesięcy
Terminal	Wbudowany, zintegrowany z oprogramowaniem urządzenia; umożliwiający

	komunikację urządzenia z dostarczonym oprogramowaniem do zarządzania wydrukami
Funkcje terminala	Identyfikacja użytkownika; odblokowanie maszyny; funkcja samodzielnego przypisywania karty do konta użytkownika w systemie zarządzania wydrukami (zaczytanie numeru karty do zwolnienie wydruków na żądanie po przyłożeniu karty bądź wpisaniu kodu PIN przypisanego do użytkownika (wszystkich wysłanych prac); zliczanie kopii na użytkownika; odczyt karty ma powodować odblokowanie maszyny (w tym wyjście ze stanu uśpienia) i uruchomienie aplikacji zarządzania wydrukami
Czytnik kart zbliżeniowych	Zintegrowany z urządzeniem czytnik; odczyt karty sygnalizowany dźwiękiem; odległość zapewniająca pewny odczyt karty: min. 2 cm od obudowy urządzenia; odczyt posiadanej przez Zamawiającego karty Hi-Tag2, ATS1475 o częstotliwości pracy 125kHz Czytnik kart zbliżeniowych w formacie UNIQUE 125 kHz zgodne z EM4100 zlokalizowany wewnątrz obudowy urządzenia . Miejsce przyłożenia karty do urządzenia oznaczone odpowiednia naklejką.
Wydruk podążający	Dostarczone urządzenia muszą być wspierane przez jeden wspólny sterownik (wspólny dla urządzeń typu I, II i III) zgodny ze specyfikacją PCL, umożliwiający formatowanie i wysyłanie wydruku bez znajomości urządzenia docelowego (z punktu widzenia użytkownika widoczna jest tylko kolejka wydruków na serwerze, wybór drukarki jest realizowany dopiero poprzez zidentyfikowanie się przy niej kartą lub PIN¬-kodem). Sterownik musi być w języku polskim, jedna i ta sama wersja musi obsługiwać wykorzystywane przez Zamawiającego systemy operacyjne Microsoft Windows 7 lub nowsze i Microsoft Windows Server 2008 lub nowsze.
System zarządzania wydrukiem	Dostarczone urządzenie musi funkcjonować w systemie Printoscope

Produkt musi zostać zainstalowany, zintegrowany i skonfigurowany zgodnie z wymaganiami Zamawiającego.

II CZĘŚĆ ZAMÓWIENIA

Część II zamówienia obejmuje zakup i dostawę, jak również zainstalowanie, zintegrowanie i skonfigurowanie niszczarek oraz drukarek

1. **Niszczarki:**

    1) **niszczarka przeznaczona do pracy o średnim natężeniu – 1 szt.**

niszczarka – 1 szt.	
Typ cięcia	Ścinki
Stopień bezp. DIN-66399:	P-4
Niszczenie płyt CD / DVD	TAK
Rozmiar cięcia	szerokość ścinki ≤6mm; powierzchnia ścinki ≤160 mm^2
Ilość kartek niszczona jednorazowo A4/70g	min. 16
Auto-reverse w przypadku zacięcia papieru	Tak
Pojemność kosza	min. 55 l
Szerokość szczeliny wejściowej w mm	240
Cykl pracy	Ciągły
Automatyczny START/STOP + funkcja cofania	TAK
Zabezpieczenie termiczne	TAK
Cięcie zszywek	TAK
Cięcie małych spinaczy	TAK
Cięcie kart plastikowych	TAK
Automatyczne zatrzymanie pracy przy zacięciu	TAK

2) niszczarki przeznaczone do pracy o niskim natężeniu – 4 szt.

niszczarka – 4 szt.	
Stopień bezp. DIN-66399:	P-2
Rozmiar cięcia	3,9 mm
Ilość kartek niszczona jednorazowo A4/70g	min.12
Pojemność kosza	min.20 l
Szerokość szczeliny wejściowej w mm	225
Automatyczny START/STOP	TAK
Zabezpieczenie termiczne	TAK
Cięcie zszywek	TAK
Cięcie kart plastikowych	TAK
Zabezpieczenie przed przegrzaniem	TAK
Optyczny wskaźnik napełnienia worka	TAK

2. Drukarka – 2 szt.

drukarka – 2 szt.	
Technologia druku	Laserowa, monochromatyczna
Obsługiwany typ nośnika	Papier zwykły Papier fotograficzny Koperty Etykiety
Obsługiwany format nośnika	A4 A5 A6 B5
Podajnik papieru	min. 150 arkuszy
Odbiornik papieru	min. 100 arkuszy
Szybkość druku w mono	min. 22 str./min

Maksymalna rozdzielczość druku	1200 x 1200 dpi
Rozdzielczość skanowanie	1200 x 1200 dpi
Maksymalny format skanu	A4
Miesięczne obciążenie	min. 10000 str./miesiąc
Maksymalna gramatura papieru	163 g/m^2
Funkcja faksu	TAK
Interfejsy	USB Wi-Fi LAN (Ethernet) RJ-11
Wyświetlacz	Wbudowany
Dodatkowe informacje	Drukowanie bezpośrednio ze smartfonów i tabletów Automatyczny podajnik dokumentów (ADF)
Dołączone akcesoria	Kabel zasilający Kabel telefoniczny Kabel USB Toner startowy
Gwarancja	min.12 miesięcy (gwarancja producenta)

Produkty muszą zostać zainstalowane, zintegrowane i skonfigurowane zgodnie z wymaganiami Zamawiającego.

III CZĘŚĆ ZAMÓWIENIA

Część III zamówienia obejmuje zakup i dostawę, jak również zainstalowanie, zintegrowanie i skonfigurowanie urządzeń oraz oprogramowania wspierających bezpieczeństwo informatyczne

1. Urządzenie klasy UTM – 1 szt.

1) urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP;
2) urządzenie ma być wyposażone w Firewall klasy StatefulInspection;
3) urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT;
4) urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge);
5) interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie;
6) administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia;
7) administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u;
8) edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów);
9) Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos);
10) system detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe;
11) moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy;
12) moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń;
13) administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS;

14) moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej;

15) urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS;

16) administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP;

17) urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma;

18) ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP;

19) rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring);

20) urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch;

21) rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania);

22) co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji;

23) administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym;

24) administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia;

25) producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM);

26) achrona antyspam ma działać w oparciu o:

    a. białe/czarne listy,

    b. DNS RBL,

    c. heurystyczny skaner;

27) w przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL;

28) wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin;

29) urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja);
30) odpowiednio kanały VPN można budować w oparciu o:
    a. PPTP VPN,
    b. IPSec VPN,
    c. SSL VPN;
31) SSL VPN musi działać w trybach Tunel i Portal;
32) w ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem;
33) Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover);
34) urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf;
35) urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię RouteBased;
36) urządzenie ma posiadać wbudowany filtr URL;
37) filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych;
38) administrator musi mieć możliwość dodawania własnych kategorii URL;
39) urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora;
40) moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST;
41) administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:
    a. blokowanie dostępu do adresu URL,
    b. zezwolenie na dostęp do adresu URL,
    c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora;
42) administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony;
43) strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych;
44) filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS;
45) urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME;
46) urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane;
47) urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http;

48) urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:
    a. lokalną bazę użytkowników (wewnętrzny LDAP),
    b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
    c. usługę katalogową Microsoft Active Directory;
49) rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP;
50) rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:
    a. SSL,
    b. Radius,
    c. Kerberos;
51) urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory;
52) co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta;
53) autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny;
54) urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. LoadBalancing);
55) mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
    a. równoważenie względem adresu źródłowego,
    b. równoważenie względem połączenia;
56) mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu;
57) urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego;
58) urządzenie ma posiadać mechanizm statycznego trasowania pakietów;
59) urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego;
60) urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP;
61) rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP;

62) urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci;

63) urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay;

64) konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6;

65) urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS;

66) urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3;

67) urządzenie musi posiadać usługę DNS Proxy;

68) producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia;

69) konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego;

70) interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https;

71) komunikacja może odbywać się na porcie innym niż https (443 TCP);

72) urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami;

73) rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana;

74) interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https;

75) urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS);

76) rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX;

77) urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora;

78) urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora;

79) urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu;

80) system raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania;

81) system raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego;

82) system raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów;

83) system raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu;

84) w ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny;

85) dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy;

86) urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać z wbudowanej pamięci flash;

87) liczba portów Ethernet 10/100/1000Mbps – min. 8;

88) urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta;

89) przepustowość Firewalla – min. 3,5 Gbps;

90) przepustowość Firewalla wraz z włączonym systemem IPS – min. 2,4 Gbps;

91) przepustowość filtrowania Antywirusowego – min. 400 Mbps;

92) minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 600 Mbps;

93) maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 100;

94) maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20;

95) obsługa min. VLAN 64;

96) liczba równoczesnych sesji - min. 300 000 i nie mniej niż 18 000 nowych sesji/sekundę;

97) urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive;

98) urządzenie jest nielimitowane na użytkowników;

99) urządzenie musi mieć wykupioną licencję Premium UTM Security Pack na 1 rok

2. Switch–1 szt.

Parametry sprzętowe

Standardy i protokoły	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3z, IEEE 802.3ad, IEEE 802.3x, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, IEEE 802.1q, IEEE 802.1p, IEEE 802.1x
Porty	P-424 porty RJ45 10/100/1000Mb/s (Auto negocjacja/Auto MDI/MDIX) 4 gigabitowe sloty SFP
Okablowanie sieciowe	10BASE-T: Kabel UTP kat. 3, 4 lub 5 (do 100m) 100BASE-TX/1000Base-T: Kabel UTP kat. 5, 5e lub wyższej (do 100m) 1000BASE-X: MMF, SMF
Bezwentylatorowy	Nie - 2 wentylatory
Zasilanie	100~240VAC, 50/60Hz
Pobór mocy	Maksymalnie(PoE włączone): 264,8W (220V/50Hz) Maksymalnie (PoE wyłączone): 28,2W (220V/50Hz)
Porty PoE+ (RJ45)	Zgodność ze standardami:802.3at/af Liczba portów PoE+: 24 Maksymalna łączna moc podłączonych urządzeń: 192W
WYDAJNOŚĆ	
Przepustowość	56Gb/s
Szybkość przekierowań pakietów	41,7Mp/s
Tablica adresów MAC	16K
Ramki jumbo	9KB

FUNKCJE OPROGRAMOWANIA	
Funkcja Quality of Service	Priorytetywanie ruchu CoS/DSCP w oparciu o standard IEEE 802.1p 8 kolejek priorytetowania Ustalenie kolejek priorytetów: SP, WRR, SP+WRR Limotowanie transmisji w zależności od portu/przepływu danych IPv6 QoS* Voice VLAN
Funkcje L2 i L2+	Routing statyczny DHCP Relay IGMP Snooping V1/V2/V3 Agregacja portów - LACP (Do 14 grup agregacji obejmujących do 8 portów każda) STP/RSTP/MSTP LLDP, LLDP-MED Filtrowanie/ochrona BPDU Ochrona TC/Root Wykrywanie połączeń loopback Kontrola przepływu 802.3x
Sieci VLAN	jednoczesna obsługa do 4096 VLAN z 4096 identyfikatorów VLAN ID MAC/Protocol VLAN
Listy kontroli dostępu	Filtrowanie pakietów oparte o źródłowe i docelowe adresy MAC L2～L4 Adres IP, porty TCP/UDP IPv6 ACL*
Bezpieczeństwo transmisji	AAA Port Security DHCP Snooping IP-MAC-Port Binding ARP Inspection 802.1x and Radius Authentication SSH v1/v2 SSL v3/TLSv1 Broadcast/Multicast/Unknown-unicastStorm Control Dos Defend
IPv6	Podwójny stos IPv4/IPv6 MLD Snooping IPv6 ND Wykrywanie MTU ICMPv6 TCPv6/UDPv6
Zastosowania IPv6	Klient DHCPv6 Ping6

	Tracert6 Telnet(v6) IPv6 SNMP IPv6 SSH IPv6 SSL Http/Https IPv6 TFTP
Zarządzanie	Interfejs przeglądarki internetowej GUI SNMP v1/v2c/v3, zgodne z publicznymi bibliotekami MIB i prywatnymi bibliotekami MIB TP-LINK RMON (grupy 1, 2, 3, 9) Monitorowanie CPU Port Mirroring Aktualizacja firmware: poprzez przeglądarkę internetową oraz TFTP Diagnostyka: test VCT Logi systemu, publiczne biblioteki MIB Dual Image
INNE	
Certyfikaty	CE, FCC, RoHS

3. Media konwerter i moduł – 4szt.

1) Media konwerter i moduł – 2 szt.

Standardy i protokoły	IEEE 802.3z, CSMA/CD, TCP/IP
Długość fali	TX: 1310nm / RX: 1550nm
Zasilanie	3,3V
Certyfikaty	FCC, CE
Kabel	Światłowód jednomodowy
Typ światłowodu	9/125 umjednomodowy
Maks. długość kabla	10km
Prędkość transmisji	1,25Gb/s
Typ portu	LC/UPC

2) Media konwerter i moduł – 2 szt.

Standardy i protokoły	IEEE 802.3z, CSMA/CD, TCP/IP
Długość fali	TX: 1550nm / RX: 1310nm
Zasilanie	3,3V
Certyfikaty	FCC, CE
Kabel	Światłowód jednomodowy
Typ światłowodu	9/125 umjednomodowy
Maks. długość kabla	10km
Prędkość transmisji	1,25Gb/s
Typ portu	LC/UPC

4. UPS RACK – 1 szt.

Zalecana wilgotność otoczenia	20,00 - 90,00 %
Długość	410,00 mm
Poziom hałasu	50,00 dB
Napięcie baterii	12,00 V
Zakres częstotliwości wejściowej	- Hz
Czas ładowania baterii	4,00 H
Napięcie wejściowe	230,00 VAC
Maksymalny czas przełączania	0,00 ms
Szerokość	438,00 mm
Moc	1 600,00 W
Zalecana temperatura otoczenia	0,00 - 40,00 °C

Częstotliwość wyjściowa	50,00 Hz
Napięcie wyjściowe	230,00 V
Liczba gniazd rozszerzeń	1,00
Zakres napięcia wejściowego	- VAC
Pojemność baterii	9,00 Ah
Liczba baterii	4
Moc pozorna	2 000,00 VA
Regulacja częstotliwości wyjściowej	Sinusoida Hz
Gniazdo rozszerzeń	Tak
Oprogramowanie	ViewPower
Zabezpieczenie przeciwprzepięciowe	Tak
Postać fali	Sinusoida
Awaryjne wyłączenie (EPO)	Tak
Zabezpieczenie przeciwprzepięciowe	Tak
Złącza USB	2.0
Obsługiwane systemy operacyjne	Windows/MAC/Linux/Unix
Gniazda wyjściowe	Tak, IEC C13 (10A)x4
CZAS ZASILANIA AWARYJNEGO	
OBCIĄŻENIE [W]	CZAS [min]
100	135
200	60
300	37
400	26
500	19

750	11,5
1000	7,8
1500	4,3
2000+	Overload

5. Oprogramowanie do tworzenia kopii zapasowych - licencja na serwery Windows pracujące w środowiskach wirtualnych (Pakiet licencji z serwisem na rok) – 3 szt.

1) pełne wsparcie dla środowisk wirtualnych: VMware Workstation, VMware ESX/ESXi, Microsoft Hyper-V, Microsoft Virtual PC, Microsoft Virtual Server, Oracle VirtualBox, Citrix XenServer, Linux KVM, ProxMox, Red Hat Enterprise Virtualization (RHEV), Stratos everRun;
2) Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Storage Server 2012 R2 Essentials, Windows Server 2008 R2 (Foundation/Essentials), Windows Server 2008 (Foundation/Essentials) z SP2 lub wyższy;
3) wsparcie dla 32 i 64-bitowych systemów Microsoft;
4) wsparcie systemów plików: FAT16, FAT16X, FAT32, FAT32X, NTFS;
5) wsparcie dla dysków z tablicą partycji MBR oraz GPT;
6) program i wsparcie techniczne dostępne w języku polskim;
7) backup obejmuje kopie całego systemu operacyjnego wraz z konfiguracją oraz zainstalowanymi aplikacjami i plikami;
8) program umożliwia skonfigurowanie różnych schematów wykonywania backupu: w trybie pełnym, backupy przyrostowe lub tryb mieszany. Harmonogram przyrostowy powinien umozliwiać backup z częstotliwością min. co 15 minut;
9) istnieje możliwość wykonywania backupów pełnych i przyrostowych na dyski lokalne, dyski sieciowe, SAN, NAS, dyski USB, Firewire;
10) program wykonuje kopie zapasowe (backupy) na poziomie sektorów czyli backup przyrostowy zawiera tylko zmienione sektory na dysku a nie np. całe pliki;
11) program nie wymaga oddzielnego serwera zarządzającego backupem, a harmonogram zadań tworzenia backupów dla danej maszyny jest przechowywany bezpośrednio na tej maszynie;
12) możliwe jest tworzenie kopii zapasowej w automatycznym trybie hot backupu (bez korzystania ze skryptów zamykających i uruchamiających bazy czy programy). Hot backup

powinien pozwalać na backup systemu, aplikacji i baz danych takich MS SQL, MS Exchange, Active Directory, Share Point, Oracle od wersji 11g;

13) do wykonywania kopii zapasowej wykorzystywana jest technologia Microsoft VSS oraz certyfikowany sterownik Microsoftu;

14) program umożliwia wykonywanie kopii zapasowej dysku bez konieczności uruchamiania systemu operacyjnego za pomocą bootowalnej płyty lub pendrive'a z systemem i oprogramowaniem dostarczanym przez producenta rozwiązania backupowego;

15) rozwiązanie pozwala na okresową weryfikacje, konsolidację oraz retencję łańcucha backupu przyrostowego z możliwością konfiguracji po jakim czasie mają się one wykonać;

16) rozwiązanie musi umożliwiać tworzenie backupu przez łącze 3G i WiFi;

17) podczas tworzenia kopii zapasowej program generuje plik sumy kontrolnej (md5) dla pliku backupu w celu kontroli plików backupu;

18) program posiada narzędzie pozwalające na automatyczną weryfikację tworzonych plików backupu za pomocą okresowego uruchamiania backupowanego systemu operacyjnego w maszynie wirtualnej, oraz wysłanie zrzutu ekranu z tak uruchomionego systemu do administratora za pomocą wiadomości email;

19) program umożliwia konwersje kopii zapasowej do plików dysków maszyn wirtualnych w formacie VHD, VMDK, VHDX;

20) program umożliwia replikację wykonanych plików kopii zapasowych na dyski lokalnie, dyski sieciowe lub do lokalizacji zdalnych na serwer FTP;

21) możliwość przywrócenia backupu całego obrazu dysku/partycji na takim samym sprzęcie, jak ten który był backupowany jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników do nowego sprzętu lub możliwość dodania sterowników przez użytkownika. Komputer powinien zostać uruchomiony z bootowalnej płyty CD lub pendrive'a, z którego bezpośrednio zostaje uruchomiony proces odzyskiwania obrazu dysku z backupu;

22) program pozwala na dowolne odtwarzanie maszyn fizycznych na inną fizyczną lub do maszyny wirtualnej, oraz z maszyny wirtualnej do innej maszyny wirtualnej lub na fizyczną;

23) bez względu na rozmiar backupu, program umożliwia automatyczne uruchomienie systemu z backupu jako maszyny wirtualnej w środowiskach VirtualBox, VMwarevSphere lub Hyper-V bez konieczności wcześniejszej konwersji pliku backupu do postaci wirtualnej;

24) program umożliwia zamontowanie pliku backupu jako dysku wirtualnego w trybie odczyt/zapis lub tylko do odczytu. Tak podłączony dysk logiczny umożliwia przeglądanie, wyszukiwanie i odzyskiwanie plików, folderów a także modyfikowanie zawartości;

25) podczas przywracania obrazu dysku/partycji z kopii zapasowej, program umożliwia: uaktywnienie wybranej partycji, przywrócenia sektora MBR, przywrócenie sygnatur dysku, przywrócenie ukrytych ścieżek na dysku, dezaktywację licencji systemu Windows;

26) program pozwala na zdefiniowanie procesu tworzenia kolejnych backupów przyrostowych, które w sposób automatyczny będą odtwarzane po określonym przez

administratora czasie na innej maszynie fizycznej lub wirtualnej (VMDK, VHD, VHDX). Musi istnieć możliwość zdefiniowania opóźnienia z jakim kopie przyrostowe będą przenoszone na nowy wolumin w zakresie od 1 godziny do 30 dni;

27) program musi umożliwiać pełną konfigurację i pełne zarządzanie zadaniami wykonywania kopii zapasowej na innych komputerach w sieci lokalnej, w zakresie identycznym jak z lokalnej konsoli administracyjnej;

28) musi być dostępne narzędzie dające możliwość tworzenia zadań backupu za pomocą polityk dla grup stacji z poziomu konsoli webowej;

29) konsola webowa musi umożliwiać instalację oraz aktualizację zdalną oprogramowania na punktach końcowych;

30) konsola webowa musi umożliwiać podgląd dzienników zdarzeń na stacjach końcowych;

31) program musi umożliwiać wysłanie powiadomień w postaci wiadomości e-mail gdy: zadanie backupu zakończyło się niepowodzeniem, po zakończeniu zadania tworzenia backupu, oraz podsumowanie aktywności dziennej, tygodniowej i miesięcznej;

32) musi istnieć możliwość pobrania ze strony producenta konsoli zarządzającej w postaci pliku ISO;

6. Oprogramowanie do tworzenia kopii zapasowych - licencja na stacje robocze pracujące pod systemem MS Windows – 4 szt.

1) wsparcie dla 32 i 64-bitowych systemów Microsoft: Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10;

2) wsparcie systemów plików: FAT16, FAT16X, FAT32, FAT32X, NTFS;

3) wsparcie dla dysków z tablicą partycji MBR oraz GPT;

4) program i wsparcie techniczne dostępne w języku polskim;

5) backup obejmuje kopie całego systemu operacyjnego wraz z konfiguracją oraz zainstalowanymi aplikacjami i plikami;

6) program umożliwia skonfigurowanie różnych schematów wykonywania backupu: w trybie pełnym, backupy przyrostowe lub tryb mieszany. Harmonogram przyrostowy powinien umozliwiać backup z częstotliwością min. co 15 minut;

7) istnieje możliwość wykonywania backupów pełnych i przyrostowych na dyski lokalne, dyski sieciowe, SAN, NAS, dyski USB, Firewire;

8) program wykonuje kopie zapasowe (backupy) na poziomie sektorów czyli backup przyrostowy zawiera tylko zmienione sektory na dysku a nie np. całe pliki;

9) program nie wymaga oddzielnego serwera zarządzającego backupem, a harmonogram zadań tworzenia backupów dla danej maszyny jest przechowywany bezpośrednio na tej maszynie;

10) możliwe jest tworzenie kopii zapasowej w automatycznym trybie hot backupu (bez korzystania ze skryptów zamykających i uruchamiających bazy czy programy). Hot backup powinien pozwalać na backup systemu, aplikacji i baz danych takich MS SQL, MS Exchange, Active Directory, Share Point, Oracle od wersji 11g;

11) do wykonywania kopii zapasowej wykorzystywana jest technologia Microsoft VSS oraz certyfikowany sterownik Microsoftu;

12) program umożliwia wykonywanie kopii zapasowej dysku bez konieczności uruchamiania systemu operacyjnego za pomocą bootowalnej płyty lub pendrive'a z systemem i oprogramowaniem dostarczanym przez producenta rozwiązania backupowego;

13) rozwiązanie pozwala na okresową weryfikacje, konsolidację oraz retencję łańcucha backupu przyrostowego z możliwością konfiguracji po jakim czasie mają się one wykonać;

14) rozwiązanie musi umożliwiać tworzenie backupu przez łącze 3G i WiFi;

15) podczas tworzenia kopii zapasowej program generuje plik sumy kontrolnej (md5) dla pliku backupu w celu kontroli plików backupu;

16) program posiada narzędzie pozwalające na automatyczną weryfikację tworzonych plików backupu za pomocą okresowego uruchamiania backupowanego systemu operacyjnego w maszynie wirtualnej, oraz wysłanie zrzutu ekranu z tak uruchomionego systemu do administratora za pomocą wiadomości email;

17) program umożliwia konwersje kopii zapasowej do plików dysków maszyn wirtualnych w formacie VHD, VMDK, VHDX;

18) program umożliwia replikację wykonanych plików kopii zapasowych na dyski lokalnie, dyski sieciowe lub do lokalizacji zdalnych na serwer FTP;

19) możliwość przywrócenia backupu całego obrazu dysku/partycji na takim samym sprzęcie, jak ten który był backupowany jak również na zupełnie innym komputerze z automatycznym dopasowaniem sterowników do nowego sprzętu lub możliwość dodania sterowników przez użytkownika. Komputer powinien zostać uruchomiony z bootowalnej płyty CD lub pendrive'a, z którego bezpośrednio zostaje uruchomiony proces odzyskiwania obrazu dysku z backupu;

20) program pozwala na dowolne odtwarzanie maszyn fizycznych na inną fizyczną lub do maszyny wirtualnej;

21) bez względu na rozmiar backupu, program umożliwia automatyczne uruchomienie systemu z backupu jako maszyny wirtualnej w środowiskach VirtualBox, VMwarevSphere lub Hyper-V bez konieczności wcześniejszej konwersji pliku backupu do postaci wirtualnej;

22) program umożliwia zamontowanie pliku backupu jako dysku wirtualnego w trybie odczyt/zapis lub tylko do odczytu. Tak podłączony dysk logiczny umożliwia przeglądanie, wyszukiwanie i odzyskiwanie plików, folderów a także modyfikowanie zawartości;

23) podczas przywracania obrazu dysku/partycji z kopii zapasowej, program umożliwia: uaktywnienie wybranej partycji, przywrócenia sektora MBR, przywrócenie sygnatur dysku, przywrócenie ukrytych ścieżek na dysku, dezaktywację licencji systemu Windows;

24) program pozwala na zdefiniowanie procesu tworzenia kolejnych backupów przyrostowych, które w sposób automatyczny będą odtwarzane po określonym przez administratora czasie na innej maszynie fizycznej lub wirtualnej (VMDK, VHD, VHDX). Musi istnieć możliwość zdefiniowania opóźnienia z jakim kopie przyrostowe będą przenoszone na nowy wolumin w zakresie od 1 godziny do 30 dni;

25) program musi umożliwiać pełną konfigurację i pełne zarządzanie zadaniami wykonywania kopii zapasowej na innych komputerach w sieci lokalnej, w zakresie identycznym jak z lokalnej konsoli administracyjnej;

26) musi być dostępne narzędzie dające możliwość tworzenia zadań backupu za pomocą polityk dla grup stacji z poziomu konsoli webowej;

27) konsola webowa musi umożliwiać instalację oraz aktualizację zdalną oprogramowania na punktach końcowych;

28) konsola webowa musi umożliwiać podgląd dzienników zdarzeń na stacjach końcowych;

29) program musi umożliwiać wysłanie powiadomień w postaci wiadomości e-mail gdy: zadanie backupu zakończyło się niepowodzeniem, po zakończeniu zadania tworzenia backupu, oraz podsumowanie aktywności dziennej, tygodniowej i miesięcznej;

30) musi istnieć możliwość pobrania ze strony producenta konsoli zarządzającej w postaci pliku ISO.

Produkty muszą zostać zainstalowane, zintegrowane i skonfigurowane zgodnie z wymaganiami Zamawiającego.