

I

PARAMETRY PRZEDMIOTU ZAMÓWIENIA DO PRZETARGU NR 9/2016

1. Komputer stacjonarny - 10 szt., dane techniczne:

1	Nazwa	
2	Producent	
3	Model	
4	Obudowa	Typu ALL IN ONE
5	System operacyjny	polska wersja językowa, preinstalowany najnowszy stabilny system operacyjny w języku polskim, w pełni obsługujący pracę w .domenie i kontrolę użytkowników w technologii ActiveDirectory System musi być kompatybilny z obecnie posiadanymi systemami operacyjnymi: MS Windows 10 Professional w wersjach 32 i 64 bitowych (m.in. umożliwiać swobodne korzystanie z drukarek udostępnianych w sieci przez wyżej wymienione systemy). System musi być w pełni legalny, spełniać dotyczące go postanowienia licencyjne producenta systemu. Warunki końcowe do zapoznania się oraz akceptacji przez użytkownika końcowego
6	Procesor	min. 2 rdzenie Procesor musi uzyskiwać min. 5089 punktów w teście Passmark
7	USB	4 porty USB z boku ekranu (w tym min. 1 gniazdo USB3)
8	Klawiatura	USB przewodowa z układem US-QWERTY zawierająca część numeryczną
9	Mysz	ergonomiczna laserowa USB, przewodowa z minimum dwoma klawiszami oraz kółkiem przewijania
10	Pamięć o dostępie swobodnym (RAM)	4GB (w organizacji 2x2 GB lub 1x4GB z możliwością rozszerzenia do 8GB) o taktowaniu szyny nie mniejszym niż 1333 MHz, obsługiwana przez procesor opisywany powyżej
11	Obsługa pamięci	minimum 1333 MHz
12	Dysk HDD	7200rpm
13	Napęd optyczny	DVD-RW
14	Karta sieciowa	100/1000
15	Karta graficzna	z pamięcią min. 1GB

16	Wymagania dodatkowe	urządzenie fabrycznie nowe, bez śladów eksploatacji, oznakowane znakiem CE lub równoważnym, zgodnie z właściwymi certyfikatami
17	Gwarancja podstawowa	min. 24 miesiące (od daty odbioru sprzętu przez Zamawiającego)
		pakiet obejmuje serwis na miejscu u klienta w następnym dniu roboczym wraz z możliwością wyboru wysyłki części i interwencji technika w ciągu tego samego dnia, po podjęciu próby rozwiązania problemu przez telefon
18	Wymagania dodatkowe	w przypadku awarii dysku wymiana dysku bez konieczności odsyłania hdd do punktu serwisowego
19	Gwarancja	minimum 24 miesiące gwarancji producenta

2. Drukarka laserowa mono - 6 szt., dane techniczne

1	Nazwa	
2	Producent	
3	Model	
4	Rodzaj drukarki	monochromatyczna
5	Rodzaje nośników	papier ekologiczny, papier gruby, papier cienki, papier zwykły, papier lekki
6	Prędkość druku - czern [str/min]	20
7	Praca w sieci	LAN
8	Interfejs	USB 2.0
9	Wydajność [str/mies]	10000
10	Obsługiwane formaty	A4, Oficio, Letter, Koperty, A5, Legal, Executive, Folio, ISO-B5, B5 JIS
11	Gwarancja	minimum 24 miesiące gwarancji producenta

3. Serwer - 1 szt., dane techniczne

1	Nazwa	
2	Producent	
3	Model	

4	Procesor	Intel® Xeon® E5-2650 v3 2.3GHz, 25M Cache, 9.60GT/s QPI, Turbo, HT, 10C/20T (105W) Max Mem 2133MHz
5	HDD	300GB SAS 6Gb/s 10 tys. obr./min.
6	Napęd	DVD+/-RW napęd SATA wewnętrzny 1 SR
7	Ram	4 szt. – 4x16 GB RDIMM, 2133MT/s, Dual Rank, x4 Data Width 16G2R
8	Kontroler RAID	1 szt. – 1GB NV Cache, obsługa do 8 dysków, RAID 0,1,5,6,10,50,60
9	Karta zdalnego zarządzania	karta zarządzania i monitorowania eliminująca konieczność stosowania monitora, myszy, klawiatury oraz KVM
10	Zasilanie	zasilanie redundantne, dwa zasilacze
11	Karta sieciowa	4 portowa 1GBE
12	Opcje	wymiana uszkodzonych dysków w ramach gwarancji bez zwrotu dysku uszkodzonego
13	Gwarancja	3 lata gwarancji producenta, zgłoszenia 7 dni w tygodniu, 24h na dobę

4. Switch Gigabit Ethernet - 2 szt., dane techniczne

1	Nazwa	
2	Producent	
3	Model	
4	Typ przełącznika	zarządzalny
5	Liczba portów 10/100/1000	48
6	Liczba zainstalowanych modułów SFP+	2
7	Liczba portów 10/100/1000/10000	2
8	Warstwa przełączania	L3
9	Procesor	minimum 800MHz, 512M RAM, 128M Flash
10	Wielkość tabeli adresów	minimum 16000
11	Liczba grup multitemisji filtrowanych	minimum 512
12	Liczba grup multitemisji filtrowanych	minimum 32

13	Prędkość magistrali	minimum 170 Gbps
14	Liczba VLAN	minimum 14
15	Opis	<p>przełącznik musi obsługiwać następujące protokoły:</p> <p>IEEE 802.3 Ethernet:</p> <ul style="list-style-type: none"> • IEEE 802.3i 10BASE-T • IEEE 802.3u 100BASE-T • IEEE 802.3ab 1000BASE-T • IEEE 802.1Q VLAN Tagging • IEEE 802.3x Full-Duplex Flow Control • IEEE 802.1Qav • IEEE 802.3z Gigabit Ethernet 1000BASE-SX/LX • IEEE 802.3ae 10-Gigabit Ethernet Over Fiber (10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-LX4) • IEEE 802.3an 10GBASE-T 10 Gbit/s Ethernet Over Copper Twisted Pair Cable <p>IEEE 802.3ad Trunking (LACP)</p> <p>IEEE 802.1AB LLDP with ANSI/TIA-1057 (LLDP-MED)</p> <p>IEEE 802.1p Class of Service</p> <p>IEEE 802.1Qat</p> <p>IEEE 802.1D Spanning Tree (STP)</p> <p>IEEE 802.1s Multiple Spanning Tree (MSTP)</p> <p>IEEE 802.1w Rapid Spanning Tree (RSTP)</p> <p>IEEE 802.1x RADIUS Network Access Control</p> <p>jednocześnie przełącznik powinien mieć pełen duplex, agregację połączenia, podporę kontroli przepływu, kontrolę wzrostu natężenia ruchu, dublowanie portów, ICMP snoping, obsługę SSH/SSL oraz moduł zarządzania przez www</p>
16	Gwarancja	<p>wymaga się, aby urządzenie i zainstalowane zasilacze oraz wentylatory były objęte wieczystą gwarancją producenta realizowaną w systemie door-to-door przez serwis producenta</p> <p>urządzenie powinno być objęte 90-dniową pomocą techniczną telefoniczną świadczoną przez producenta urządzenia. Dodatkowo producent winien zapewnić pomoc w formie czat pracujący minimum 8 godzin dziennie w dni robocze w języku polskim przez cały okres gwarancji</p> <p>urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii nie później niż na następny dzień roboczy przez cały okres gwarancji</p>

5. Multipower DSPMP 6kVA - 1 szt., dane techniczne

1	Nazwa	
2	Producent	
3	Model	
4	Szczegóły	jeden moduł dodatkowej baterii 440x132x680 -3U 9Ah/240V plus karta sieciowa
5	Zasilanie	1L+N + PE
6	Moc	6kVA
7	Zarządzanie	karta sieciowa
8	Sprawność Sprawność (AC ÷ AC) praca w trybie normalnym [%]	> 91%
9	Sprawność Sprawność (AC ÷ AC) praca w trybie ECO [%]	> 97%
10	BATERIE AKUMULATORÓW	VRLA
11	Statyczny układ obejściowy	baypas elektroniczny z liczbą faz 1L+N + PE
12	Tolerancja napięcia	-0,1
13	Czas przełączenia	0 ms
14	Stabilizacja napięcia wyjściowego (praca z sieci i z baterii, obciążenie liniowe)	< 1%
15	Możliwości przeciążeniowe:	minimalne wymagania: 2 minuty 110% obciążenia; 1 minuta 125 % obciążenia; 30 sekund 150% obciążenia
16	Współczynnik szczytu	03:01
17	Czas podtrzymania przy obciążeniu 50%	minimum 23 minuty
18	Bateria zewnętrzna	9Ah/240V
19	Gwarancja	minimum 24 miesiące gwarancji producenta

6. Serwer plików - 1 szt., dane techniczne

1	Nazwa	
2	Producent	

3	Model	
4	Wielkość dysków	4 TB x 12 sztuk
5	Procesor	Intel Pentium Dual Core G3250 3.1GHz
6	Pamięć	4 GB DDR3 ECC RAM (rozbudowa do 32GB)
7	Ilość dysków	12 x 3.5" SATAIII - kieszenie z funkcją hot-swap
8	Pamięć cache SSD	2 x mSATA wewnątrz obudowy, dla dysków SSD 2.5"
9	Sieć	4 x Gigabit LAN (opcja dodatkowo 4 x 10Gbit)
10	Złącza dodatkowe	4 x USB 3.0, 4 x USB 2.0
11	Gniazdo rozszerzeń	2
12	Wskaźniki LED	LAN, HDD, 10GbE
13	Obsługa trybów RAID	RAID 10+spare, 10, 6+spare, 6, 5+spare, 5, 1, 0, JBOD, Single Disk
14	Funkcje RAID	rozbudowa i zmiana trybu RAID "on-line" bez restartu urządzenia
15	Zasilanie	zasilacz redundantny 2 x 400W
16	Pobór mocy	88W uśpienie, 173 W praca
17	Wake on LAN	tak
18	Systemy operacyjne	Windows, Mac OSX, Linux, Unix
19	Wspierane systemy wirtualne	VMware ESX 4.x, Citrix Xen 5.x, Hyper-V Windows 2008R2
20	Protokoły sieciowe	CIFS, SMB, AFP, NFS, HTTP, FTP, HTTPS, SNMP, Telnet, SSH
21	Konfiguracja sieci	TCP / IP, stały lub dynamiczny adres
22	Port trunking	balance, active backup, balance XOR, broadcast, IEE 802.3ad, adaptacyjny rozkład obciążenia, balance TLB, balance ALB
23	Multi IP	tak – możliwe oddzielne adresy IP na każdym porcie sieciowym
24	Serwer DHCP, dyn. DNS	tak
25	Jumbo Frame	tak
26	Service Network Discovery	UPnP, Bonjour

27	Windows Active Directory	tak
28	Bezpieczeństwo sieciowe	filtr IP, FPT over SSL, tryb pasywny, szyfrowana replikacja
29	Szyfrowanie wolumenów	AES 256 bitowe (FIPS 140-2)
30	Zarządzanie dyskami	skanowanie złych sektorów, SMART
31	Inne usługi	iSCSI target / LUN (do 256), Virtual Disk
32	Serwer plików i FTP	FTP over SSL, TLS, tryb pasywny, kontrola pasma FTP
33	Dodatkowe opcje serwerowe	Serwer RADIUS, Serwer Syslog, Klient LDAP
34	Kopie zapasowe	kopia na nośnik zewn., szyfrowana replikacja, QNAP Replicator
35	Powiadomienie awaryjne	e-mail, SMS, LED
36	Inne usługi	kosz sieciowy, monitor zasobów on-line, harmonogram wł/wył
37	Zarządzanie systemem	poprzez przeglądarkę internetową
38	Przycisk reset	kasowanie hasła administracyjnego / ustawień sieciowych
39	Logi systemowe	użytkownicy, alarmy, błędy, połączenia, przydziały DHCP
40	Wbudowany serwer www	PHP, MySQL, phpMyAdmin, Joomla
41	Multimedialne usługi	UPnP, radio internetowe, galeria www, iTunes serwer
42	Pobieranie plików	zarządzanie przez aplikacje Windows lub przeglądarkę
43	Stacja monitoringu	zapis, odtwarzanie, podgląd na żywo, detekcja ruchu, alarmy
44	Ilość obsługiwanych kamer	4
45	ilość użytkowników	4000 lub więcej
46	ilość grup	500 lub więcej
47	ilość folderów	500 lub więcej
48	ilość połączeń	1300 lub więcej
49	Program antywirusowy	tak
50	Gwarancja	minimum 24 miesiące gwarancji producenta

7. Firewall: - 1 szt., dane techniczne

1	Nazwa	
2	Producent	
3	Model	
4	Wymagania	urządzenie z roczną licencją Bundle
5	Architektura systemu ochrony	system ochrony musi być zbudowany przy użyciu minimalnej ilości elementów ruchomych, krytycznych dla jego działania, dlatego główne urządzenie ochronne [gateway] nie może posiadać twardego dysku, w zamian używać pamięci FLASH
		podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanego układu ASIC
		jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego, wymaga się, aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny, pochodziły od jednego producenta, który udzieli licencji bez limitu chronionych użytkowników (licencja na urządzenie)
6	System operacyjny	dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia
7	Ilość/rodzaj portów	nie mniej niż 20 portów Ethernet 10/100/1000 Base-TX oraz 2 porty SFP/Ethernet [SharedPort]
8	Funkcjonalności podstawowe i uzupełniające	system ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych:
		– kontrolę dostępu – zaporę ogniową klasy Stateful Inspection
		– ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM, SMTPS, POP3S, IMAPS, HTTPS)
		– poufność danych – IPSec VPN oraz SSL VPN
		– ochronę przed atakami – Intrusion Prevention System [IPS/IDS] oraz funkcjonalności uzupełniających
		– kontrolę treści – Web Filter [WF]
		– kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
		– kontrolę pasma oraz ruchu [QoS i Traffic shaping]
		– kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM oraz P2P)
– zapobieganie przed wyciekami informacji poufnej DLP (Data Leak Prevention)		

9	Zasada działania (tryby)	urządzenie powinno dawać możliwość ustawienia jednego z dwóch trybów pracy:
		– jako router/NAT (3.warstwa ISO-OSI) lub
		– jako most /transparent bridge/ . Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu
10	Polityka bezpieczeństwa (firewall)	polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe użytkowników sieci, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem (m.in. pasmo gwarantowane i maksymalne, priorytety, oznaczenia DiffServ)
11	Wykrywanie ataków	wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP:
		– nie mniej niż 4000 sygnatur ataków
		– aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie
		możliwość wykrywania anomalii protokołów i ruchu
12	Translacja adresów	statyczna i dynamiczna translacja adresów (NAT)
		translacja NAT
13	Wirtualizacja i routing dynamiczny	możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne ustawienia wszystkich funkcji bezpieczeństwa i dostęp administracyjny
		obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego
		protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM
14	Połączenia VPN	Wymagane nie mniej niż:
		– tworzenie połączeń w topologii Site-to-site oraz Client-to-site
		– udostępnianie klienta VPN własnej produkcji realizującego następujące mechanizmy ochrony końcówki:
		· o firewall
		· o antywirus
		· o web filtering
· o antyspam		
		– monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności

14 (cd)	Połączenia VPN (cd)	– konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN)
		– obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
15	Uwierzytelnianie użytkowników	system zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
		· haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia
		· haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
		· haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych
		rozwiązanie powinno umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych
16	Wydajność	obsługa nie mniej niż 3 000 000 jednoczesnych połączeń i 22 000 nowych połączeń na sekundę
		przepływność nie mniejsza niż 2500 Mbps dla ruchu nieszyfrowanego i 450 Mbps dla VPN (3DES) oraz 260 Mbps dla ruchu szyfrowanego
		obsługa nie mniej niż 2 000 jednoczesnych tuneli VPN
17	Funkcjonalność zapewniająca niezawodność	monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łącz sieciowych
		możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive
18	Konfiguracja i zarządzanie	możliwość konfiguracji poprzez terminal i linię komend oraz wbudowaną konsolę graficzną (GUI). Administratorzy muszą być uwierzytelniani za pomocą:
		· dostępu do urządzenia i zarządzania z sieci poprzez szyfrowanie komunikacji
		· możliwości definiowania wielu administratorów o różnych uprawnieniach
		· możliwości definiowania wielu administratorów o różnych uprawnieniach
		· haseł statycznych
		· haseł dynamicznych (RADIUS, RSA SecureID)
		system powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB
		jednocześnie, dla systemu bezpieczeństwa powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta

19	Zarządzanie	system powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem centralnego zarządzania umożliwiającym:
		· przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej
		· wersjonowanie polityk w taki sposób, aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości
		· zarządzanie wersjami firmware'u na urządzeniach oraz zdalne uaktualnienia
		· zarządzanie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia
		· monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM)
		· zapis i zdalne wykonywanie skryptów na urządzeniach
20	Raportowanie	system powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym:
		· zbieranie logów z urządzeń bezpieczeństwa
		· generowanie raportów
		· skanowanie podatności stacji w sieci
		· zdalną kwarantannę dla modułu antywirusowego
21	Integracja systemu zarządzania	zgodnie z zaleceniami normy PN-ISO/17799 zarówno moduł centralnego zarządzania, jak i raportowania muszą być zrealizowane na osobnych urządzeniach sprzętowych
		jednocześnie administrator powinien mieć do dyspozycji jedną konsolę zarządzającą do kontroli obu podsystemów
22	Serwis oraz aktualizacje	licencje aktywacyjne dla funkcji bezpieczeństwa na okres 1 roku
23	Gwarancja	minimum 12 miesięcy gwarancji producenta

8 System operacyjny - 11 szt., dane techniczne:

1	Oprogramowanie Windows 10	64 bit pro
2	Gwarancja	minimum 12 miesięcy gwarancji producenta

9 Oprogramowanie monitorujące pracę sieci - 1 szt., dane techniczne:

1	Oprogramowanie Gfi LanGuard	licencja na 4 lata, 60 adresów IP/nodów
2	Gwarancja	4 lata gwarancji producenta

10. Oprogramowanie monitorujące pracę sieci - 1 szt., dane techniczne:

1	Oprogramowanie GFI Events Manager Plus Edition	licencja na 4 lata, 10 stanowisk serwerowych i 150 stacji roboczych (windowsowych)
2	Gwarancja	4 lata gwarancji producenta

II. Jeżeli w treści opisu przedmiotu zamówienia doszło o użycia nazw własnych, patentów lub pochodzenia, Zamawiający dopuszcza rozwiązania równoważne. Za ofertę równoważną należy rozumieć taką, która przedstawia opis przedmiotu zamówienia o takich samych parametrach lub zbliżonych do tych, jakie zostały określone w specyfikacji istotnych warunków zamówienia, lecz oznaczoną innym znakiem towarowym, patentem lub pochodzeniem. W przypadku oprogramowania musi ono współdziałać z oprogramowaniem obecnie funkcjonującym w firmie, a zwłaszcza z systemami operacyjnymi oraz pakietami biurowymi i oprogramowaniem graficznym.

III. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest zobowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W tym celu Wykonawca powinien złożyć wraz z ofertą opisy producenta oprogramowania i sprzętu, tabele porównawcze oraz wyniki testów potwierdzających równoważność.

IV. Zamawiający wymaga gwarancji na zakupiony sprzęt, zgodnie z danymi podanymi w parametrach technicznych.

V. Szczegółowe warunki sprawowania serwisu gwarancyjnego określa karta gwarancyjna załączona przez Wykonawcę do wydanego sprzętu.

.....
Podpis Wykonawcy