

PZOZ/DZP/382/21PN/12

Płock, dnia 28 listopada 2012 roku

**Do wszystkich uczestników postępowania
o udzielenie zamówienia publicznego**

**WYJAŚNIENIE TREŚCI SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA
WRAZ ZE ZMIANĄ JEJ TREŚCI**

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego, którego przedmiotem jest **„Wykonanie sieci teleinformatycznej w części pasywnej i aktywnej oraz budowa bezpiecznego połączenia pomiędzy Szpitalem Świętej Trójcy w Płocku (Oddziałem PZOZ), a Przychodniami (Placówkami PZOZ), realizowanego w ramach projektu: „Kompleksowa informatyzacja Płockiego Zakładu Opieki Zdrowotnej dzięki budowie infrastruktury teleinformatycznej oraz platform elektronicznych, zwiększeniu poziomu wykorzystania technologii TIK oraz wdrożeniu zintegrowanego systemu zarządzania”, współfinansowanego z Europejskiego Funduszu Rozwoju Regionalnego w ramach Priorytetu II „Przyspieszenie e-Rozwoju Mazowsza”, Działania 2.1 „Przeciwdziałanie wykluczeniu informacyjnemu” Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2007-2013”**

W związku z wnioskami o wyjaśnienie treści Specyfikacji Istotnych Warunków Zamówienia, zwanej dalej „SIWZ”, złożonymi przez Wykonawców, działając na podstawie art. 38 ust. 1 i 2 ustawy z dnia 29 stycznia 2004 roku – Prawo zamówień publicznych (Dz. U. z 2010 r. Nr 113, poz. 759 z późn. zm.) Zamawiający – Płocki Zakład Opieki Zdrowotnej Sp. z o.o. wyjaśnia, co następuje:

Pytanie Nr 1

W § 3 ust. 8 Wykonawca wnosi o dopisanie na końcu zdania: „biegnie na nowo na nowo wymieniony element”.

Odpowiedź: Zamawiający wyraża zgodę na powyższe i dokona zmiany treści SIWZ.

Pytanie Nr 2

W § 4 ust. 1 i 4 Wykonawca wnosi o zmianę „opóźnienia” na „zwłokę” oraz o wprowadzenie zmiany poprzez wskazanie kwotowej wartości ograniczenie w ust. 4 górnej granicy odpowiedzialności.

Odpowiedź: Zamawiający podtrzymuje zapisy SIWZ.

Pytanie Nr 3

W § 5 ust. 1 Wykonawca wnosi o zmianę „opóźnienia” na „zwłokę”.

Odpowiedź: Zamawiający podtrzymuje zapisy SIWZ.

Pytanie Nr 4

Proszę o wskazanie, dokumentu na podstawie którego Zamawiający dokona oceny minimalnych parametrów oferowanego sprzętu, oprogramowania, oraz usług przez Oferenta, w związku z rozbieżnościami występującymi w niżej wymienionych dokumentach opublikowanych przez Zamawiającego:

- Załącznik nr 1 do SIWZ „Opis przedmiotu zamówienia”
- Załącznik nr 7 do SIWZ „Wykaz i parametry progowe oferowanego sprzętu, systemu zarządzania i monitoringu sieci komputerowej oraz usług”
- „Projekt sieci teleinformatycznej dla Płockiego Zakładu Opieki Zdrowotnej Sp. z o.o.”

Odpowiedź: Dokumentami na których wykonawca powinien się opierać to dokumenty zawarte w SIWZ tj:

- Załącznik nr 1 do SIWZ "Opis przedmiotu zamówienia",
- Załącznik nr 7 do SIWZ "Wykaz i parametry progowe oferowanego sprzętu. systemu zarządzania i monitoringu sieci komputerowej oraz usług".

Dokument "Projekt sieci teleinformatycznej dla Płockiego Zakładu Opieki Zdrowotnej Sp. z o.o." jest dokumentem pomocniczym i winien on być traktowany jako uzupełnienie, zatem jeśli opisy lub jakiegokolwiek specyfikacje i parametry techniczne występujące równocześnie w SIWZ i "Projekcie sieci teleinformatycznej dla Płockiego Zakładu Opieki Zdrowotnej Sp. z o.o." są niespójne lub niejednoznaczne, zawsze priorytet przyjmuje Załącznik Nr 1 i Nr 7 do SIWZ, a nie "Projekt sieci teleinformatycznej dla Płockiego Zakładu Opieki Zdrowotnej Sp. z o.o."

Pytanie Nr 5

Zamawiający w Załączniku nr 7 do SIWZ „Wykaz i parametry progowe oferowanego sprzętu, systemu zarządzania i monitoringu sieci komputerowej oraz usług” pkt. 15 „System Telewizji Dozorowej – CCTV” oraz w dokumencie „Projekt sieci teleinformatycznej dla Płockiego Zakładu Opieki Zdrowotnej Sp. z o.o.” pkt. 13 „SYSTEM TELEWIZJI DOZOROWEJ CCTV” wymaga dostawy Krosownicy wizyjnej w celu przełączania i obsługi bieżącej obrazu z kamer w portierni. Czy w przypadku zastosowania manipulatora i rejestratorów pozwalających na uzyskanie takich samych możliwości przełączania i obsługi bieżącej obrazu z kamer bez stosowania dodatkowego urządzenia jakim jest krosownica wizyjna Zamawiający dopuszcza możliwość braku dostawy Krosownicy wizyjnej przez Oferenta?

Odpowiedź: Zamawiający dopuszcza użycie krosownicy wizyjnej lub rozwiązania równoważnego zapewniającego taką samą funkcjonalność.

Pytanie Nr 6

Zamawiający w Załączniku nr 7 do SIWZ „Wykaz i parametry progowe oferowanego sprzętu, systemu zarządzania i monitoringu sieci komputerowej oraz usług” pkt.1 „Przełącznik typu BACKBONE” wymaga przepustowości urządzenia wyrażonej w Mbps, czy Zamawiający nie miał na myśli wartości wyrażonej w mpps?

Odpowiedź: W Załączniku nr 7 do SIWZ "Wykaz i parametry progowe oferowanego sprzętu, systemu zarządzania i monitoringu sieci komputerowej oraz usług" pkt.1 "Przełącznik typu BACKBONE" wymaga przepustowości urządzenia powinna być wyrażona w **mpps**.

Pytanie Nr 7

Zamawiający w Załączniku nr 7 do SIWZ „Wykaz i parametry progowe oferowanego sprzętu, systemu zarządzania i monitoringu sieci komputerowej oraz usług” pkt.1 „Przełącznik typu BACKBONE” wymaga rozmiaru tablicy MAC min. 120 000 adresów, czy Zamawiający dopuszcza zastosowanie przez Oferenta urządzenia z rozmiarem tablicy MAC 32 000 adresów?

Odpowiedź: Zamawiający podtrzymuje zapisy SIWZ.

Pytanie Nr 8

Zamawiający w Załączniku nr 7 do SIWZ „Wykaz i parametry progowe oferowanego sprzętu, systemu zarządzania i monitoringu sieci komputerowej oraz usług” pkt.2 „Przełącznik typu DISTRIBUTION” wymaga przepustowości urządzenia wyrażonej w Mbps, czy Zamawiający nie miał na myśli wartości wyrażonej w mpps?

Odpowiedź: Wymagana przepustowość urządzenia powinna być wyrażona w **mpps**.

Pytanie Nr 9

Zamawiający w Załączniku nr 7 do SIWZ „Wykaz i parametry progowe oferowanego sprzętu, systemu zarządzania i monitoringu sieci komputerowej oraz usług” pkt.3 „Przełącznik typu ACCESS I” wymaga przepustowości urządzenia wyrażonej w Mbps, czy Zamawiający nie miał na myśli wartości wyrażonej w mpps?

Odpowiedź: Wymagana przepustowość urządzenia powinna być wyrażona w **mpps**.

Pytanie Nr 10

Zamawiający w Załączniku nr 7 do SIWZ „Wykaz i parametry progowe oferowanego sprzętu, systemu zarządzania i monitoringu sieci komputerowej oraz usług” pkt.4 „Przełącznik typu ACCESS II” wymaga przepustowości urządzenia wyrażonej w Mbps, czy Zamawiający nie miał na myśli wartości wyrażonej w mpps?

Odpowiedź: Wymagana przepustowość urządzenia powinna być wyrażona w mpps.

Pytanie Nr 11

Zamawiający w Załączniku nr 7 do SIWZ „Wykaz i parametry progowe oferowanego sprzętu, systemu zarządzania i monitoringu sieci komputerowej oraz usług” pkt.6 „Firewall w GPD” wymaga ilości jednocześnie obsługiwanych połączeń min. 900 000, czy Zamawiający dopuszcza zastosowanie przez Oferenta urządzenia z ilością jednocześnie obsługiwanych połączeń min. 800 000?

Odpowiedź: Zamawiający podtrzymuje zapisy SIWZ.

Pytanie Nr 12

Zamawiający w Załączniku nr 7 do SIWZ „Wykaz i parametry progowe oferowanego sprzętu, systemu zarządzania i monitoringu sieci komputerowej oraz usług” pkt.6 „Firewall w GPD” wymaga ilości jednocześnie obsługiwanych tuneli IPsec min. 1 800, czy Zamawiający dopuszcza zastosowanie przez Oferenta urządzenia z ilością jednocześnie obsługiwanych tuneli IPsec min. 1 000?

Odpowiedź: Zamawiający podtrzymuje zapisy SIWZ.

Pytanie Nr 13

Zamawiający w Załączniku nr 7 do SIWZ „Wykaz i parametry progowe oferowanego sprzętu, systemu zarządzania i monitoringu sieci komputerowej oraz usług” pkt.8 „VPN centrala router w GPD (zaawansowany)” wymaga aby urządzenie umożliwiała na instalację dodatkowych modułów sieciowych w ilości min. 5, czy Zamawiający dopuszcza aby urządzenie oferowane przez Oferenta pozwalało na instalację 4 dodatkowych modułów sieciowych?

Odpowiedź: Zamawiający podtrzymuje zapisy SIWZ.

Pytanie Nr 14

Zamawiający w Załączniku nr 7 do SIWZ „Wykaz i parametry progowe oferowanego sprzętu, systemu zarządzania i monitoringu sieci komputerowej oraz usług” pkt.8 „VPN centrala router w GPD (zaawansowany)” wymaga aby urządzenie wyposażone było w min. 4 GB pamięci flash, czy Zamawiający dopuszcza aby urządzenie oferowane przez Oferenta wyposażone było w 1 GB pamięci flash?

Odpowiedź: Zamawiający podtrzymuje zapisy SIWZ.

Pytanie Nr 15

W serwerowni wymagany jest sejf na nośniki magnetyczne. Proszę określić odporność ogniową (60/120 minut), oraz pojemność w litrach (proponujemy podać przedział od...do...).

Odpowiedź: Wymagane progowe parametry techniczne sejfu:

- Sejf z zamkiem elektronicznym na nośniki magnetyczne
- Minimalna pojemność to 18 Litrów.

Wymagania zgodne z normami:

- Atest przeciwwłamaniowy zgodny z normą europejską EN 1143-1 (klasa I odporności na włamanie).
- Atest ognioodporności zgodny z normą EN 1047-1 w klasie 60P (60 minut odporności ogniowej).
- Wkładka na nośniki danych spełnia atest ognioodporności zgodny z normą EN 1047-1 w klasie S60 DIS (60 minut odporności ogniowej) dla CD/DVD, kaset DAT, DTL/LTO, dyski 3.5" oraz zgodna z klasą ognioodporności 60 Diskette wg. NT Fire 017 dla nośników magnetycznych i optycznych.

Pytanie Nr 16

W związku z ogłoszeniem o zamówieniu opublikowanym w dniu 31.10.2012 pod numerem 2012/S 210-345807, firma DATA NET Jarosław Jagodziński i Wspólnicy Spółka Jawna pragnie zgłosić prośbę o usunięcie zapisu z punktu III 2.3) podpunkt f.

Niniejszy punkt dotyczy kwalifikacji technicznych wykonawców zamówienia, a dokładnie posiadania osoby będącej:

"audytorem informatycznym, posiadającym certyfikat CISA, zdolnym do przeprowadzenia niezależnego audytu informatycznego zgodności przedmiotu zamówienia z wymaganiami SIWZ i zawartą umową, z uwzględnieniem standardów ISACA. Usługa audytu może być pozyskana na zewnątrz, z zachowaniem warunków niezależności i zapewnienia obiektywizmu badania audytowego ... "

Swoją prośbę motywujemy możliwością podważenia niezawisłości ww. osoby jeżeli dany specjalista jest wynajmowany przez firmę wykonawczą. Prosimy o wykreślenie obowiązku posiadania niniejszej osoby bądź przeniesienia obowiązku posiadania audytora na Zamawiającego*.

Odpowiedź: Zamawiający odpowiadając na pytanie informuje, że wymóg audytora informatycznego posiadającego certyfikat CISA jest zgodny z interesami zamawiającego i nie jest sprzeczny z zachowaniem warunków niezależności i zapewnienia obiektywizmu badania audytowego. Wynika to ze specyficznej roli jaką przyjmuje na siebie audytor informatyczny posiadający certyfikat CISA.

Certified Information Systems Auditor, CISA (Certyfikowany Audytor Systemów Informatycznych) - certyfikat zawodowy dla osób zajmujących się audytem systemów informatycznych wydawany przez ISACA.

Deklarowane cele powstania tego certyfikatu to:

- "rozwijać i utrzymywać narzędzie testowania, które może być używane do oceny indywidualnych kompetencji w zakresie audytu systemów informatycznych,
- dostarczyć mechanizmu motywującego audytorów systemów informatycznych do utrzymywania swoich kompetencji i monitorowania efektów programów szkoleniowych,
- pomagać kierownictwu w rozwijaniu funkcji kontroli systemów informatycznych, dostarczając kryteria dla doboru i szkolenia personelu."

Proces egzaminacyjny CISA uzyskał certyfikację American National Standards Institute (ANSI) zgodnie z normą ISO/IEC 17024:2003.

Wymagania

Aby uzyskać certyfikat **CISA** konieczne jest:

- Zdanie egzaminu organizowanego przez ISACA dwa razy w roku.
- Potwierdzone 5 lat doświadczenia w audycie informatycznym, lub pracy w kontroli w obszarze informatyki lub w pracy w obszarze bezpieczeństwa, z uwzględnieniem, iż:
 - 1 rok można zastąpić 1 rokiem doświadczenia w pracy przy systemach informatycznych lub w audycie finansowym/operacyjnym,
 - odpowiednio 1 albo 2 lata uzyskuje się posiadając tytuł licencjata lub magistra (3 lata jeśli program studiów zgodny z programem ISACA),
 - 2 lata w roli pełnoetatowego wykładowcy w obszarach takich jak informatyka, księgowość, audyt itp., równoważy 1 rok wymaganego doświadczenia.
- Deklaracja przestrzegania kodeksu etyki.
- Deklaracja prowadzenia ustawicznego kształcenia w obszarach związanych z audytem, kontrolą lub bezpieczeństwem informacji.
- Deklaracja stosowania standardów zawodowych publikowanych przez ISACA.

Powyższe wymagania przy uzyskaniu powyższego certyfikatu praktycznie wykluczają jakąkolwiek stronniczość podczas wykonywania audytu, zatem zapis w punkcie III.2.3. - f "1 audytorem informatycznym, posiadającym certyfikat CISA, zdolnym do przeprowadzenia niezależnego audytu informatycznego zgodności przedmiotu zamówienia z wymaganiami SIWZ i zawartą umową, z uwzględnieniem standardów ISACA. Usługa audytu może być pozyskana na zewnątrz, z zachowaniem warunków niezależności i zapewnienia obiektywizmu badania audytowego ... " w ogłoszeniu 2012/S 210-345807 pozostaje w niezmienionej formie.

Biorąc pod uwagę powyższe odpowiedzi, na podstawie art. 38 ust. 4 ustawy z dnia 29 stycznia 2004 roku – Prawo zamówień publicznych (Dz.U. z 2010 r. Nr 113, poz. 759 z późn. zm.) Zamawiający – Płocki Zakład Opieki Zdrowotnej Sp. z o.o., wprowadza do treści SIWZ następujące zmiany:

§ 3 ust. 8 istotnych postanowień umowy otrzymuje brzmienie:

W przypadku wymiany elementu, stanowiącego część lub całość przedmiotu umowy, okres gwarancji biegnie na nowo na nowo wymieniony element.

Załącznik Nr 7 do SIWZ „Wykaz i parametry progowe oferowanego sprzętu, systemu zarządzania i monitoringu sieci komputerowej oraz usług” **otrzymuje nowe brzmienie:**

„Wykonanie sieci teleinformatycznej w części pasywnej i aktywnej oraz budowa bezpiecznego połączenia pomiędzy Szpitalem Świętej Trójcy w Płocku (Oddziałem PZOZ), a Przychodniami (Placówkami PZOZ), realizowanego w ramach projektu: *Kompleksowa informatyzacja Płockiego Zakładu Opieki Zdrowotnej dzięki budowie infrastruktury teleinformatycznej oraz platform elektronicznych, zwiększeniu poziomu wykorzystania technologii TIK oraz wdrożeniu zintegrowanego systemu zarządzania*”, współfinansowanego z Europejskiego Funduszu Rozwoju Regionalnego w ramach Priorytetu II „Przyspieszenie e-Rozwoju Mazowsza”, Działania 2.1 „Przeciwdziałanie wykluczeniu informacyjnemu” Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2007-2013”

PZOZ/DZP/382/21PN/12

**WYKAZ I PARAMETRY PROGOWE
oferowanego sprzętu, systemu zarządzania i monitoringu sieci komputerowej oraz usług**

Nazwa Wykonawcy

Adres Wykonawcy

Oświadczamy, że oferowany przez nas sprzęt i oprogramowanie charakteryzuje się poniższymi parametrami:

1. Przełącznik typu BACKBONE

<i>Parametry progowe (minimalne wymagania)</i>	<i>Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK</i>
Podać Producenta / Typ / Model / Rok produkcji (data produkcji sprzętu nie może być starsza niż 13 miesięcy licząc od dnia ogłoszenia niniejszego SIWZ-u)	Producent: Typ: Model: Rok produkcji:
Wymagania podstawowe	
Budowa typu Rack 19"	
Przełącznik wspierający standard 10 Gigabit Ethernet	
Minimum 22 porty z wkładkami SFP+ 10GBase-SR bez nadsubskrypcji	
Minimum 2 porty z wkładkami 1GBase-LX bez nadsubskrypcji	
Prędkość magistrali wewnętrznej nie mniej niż : 450Gbps	
Przepustowość nie mniej niż: 340 mpps	
Warstwa przełączania : 2,3	
Możliwość rozbudowy o funkcjonalność łączenia dwóch przełączników fizycznych w jeden przełącznik wirtualny, traktowany jako jedno urządzenie logiczne z punktu widzenia protokołów routingu, LACP i Spanning Tree	
Konfiguracja : konsola, SSH	
Port konsoli : 1szt.	
Standard IEEE 802.1ad (Q-in-Q)	
Standard IEEE 802.1d (STP)	
Możliwość separacji portów w warstwie L 2,3	
Rozmiar tablicy MAC min. 120 000 adresów	
Minimum 4000 aktywnych sieci VLAN	
Mechanizm kolejkowania procesora zapobiegający atakom DoS	
Port security: zezwalający na dostęp tylko specyficznym adresom MAC	
Urządzenie musi być odporne na ataki typu Denial of service takich jak SYN	

Flood attacks, Land attacks, Smurf attacks, oraz ICMP Flood attacks	
IEEE 802.1X– dynamiczne dostarczanie polityk QoS, ACLs i sieci VLANs: zezwalające na nadzór nad dostępem użytkownika do sieci	
Monitorowanie : SNMPv1/v2/v3	
Obsługa i znakowanie sieci VLAN IEEE 802.1q	
Protokół umożliwiający tworzenie szybkobieżnych sieci w topologii pierścieni w których czas przełączenia transmisji na ścieżkę zapasową jest mniejszy niż 50ms	
RIP	
Zasilanie	
Zasilacz 1 sztuka	
Możliwość podłączenia zasilaczy redundantnych.	
Dodatkowe wyposażenie	
Komplet przewodów połączeniowych do zastosowanych portów o właściwej długości.	
Komplet montażowy do szafy Rack.	
Serwis gwarancyjny	
Gwarancja nie mniej niż 3 lata na miejscu w siedzibie Zamawiającego.	
Czas realizacji zgłoszenia liczony od momentu zgłoszenia w godz. 7.00 – 17.00 wynosi nie więcej niż 120 min.	
Min. 5-cio letni okres zagwarantowania dostępności części zamiennych od daty upływu terminu gwarancji.	
Koszt części zamiennych na poziomie średnich cen rynkowych.	
Autoryzowany przez producenta serwis pogwarancyjny.	

2. Przełącznik typu DISTRIBUTION

Parametry progowe (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Podać Producenta / Typ / Model / Rok produkcji (data produkcji sprzętu nie może być starsza niż 13 miesięcy licząc od dnia ogłoszenia niniejszego SIWZ-u)	Producent: Typ: Model: Rok produkcji:
Wymagania podstawowe	
Budowa typu Rack 19"	
Minimum 24 portów Ethernet 1000BaseT z auto-negocjacją 10/100/1000	
Minimum 2 - porty 10GE wyposażone we wkładki 10GBase-SR do połączenia z przełącznikami rdzeniowymi	
Możliwość podłączenia modułu uplink – nie mniej niż 2x10GbE	
Prędkość przełączania nie mniej niż : 80 Gb/s	
Przepustowość nie mniej niż : 60 mpps	
Warstwa przełączania : 2,3	
Możliwość łączenia przełączników fizycznych w jeden przełącznik wirtualny, jako jedno urządzenie logiczne z punktu widzenia protokołów routingu, LACP i Spanning Tree. Maksymalna liczba przełączników obsługiwanych w stosie co najmniej 9szt.	
Konfiguracja : konsola, SSH	
Port konsoli : 1szt.	
Standard IEEE 802.1ad (Q-in-Q)	
Standard IEEE 802.1d (STP)	
Możliwość separacji portów w warstwie L 2,3	
Przypisywanie adresu MAC do pojedynczego portu	
Pojemność tablicy MAC adresów nie mniej niż 12K	
Nie mniej niż 4000 aktywnych sieci VLAN	
Protokół umożliwiający tworzenie szybkobieżnych sieci w topologii pierścieni w których czas przełączenia transmisji na ścieżkę zapasową jest mniejszy niż 50ms	
DHCP snooping	
IEEE 802.1X– dynamiczne dostarczanie polityk QoS, ACLs i sieci VLANs:	

zezwalające na nadzór nad dostępem użytkownika do sieci	
Port security: zezwalający na dostęp tylko specyficznym adresom MAC	
MAC-based authentication	
Urządzenie musi być odporne na ataki typu Denial of service takich jak SYN Flood attacks, Land attacks, Smurf attacks, oraz ICMP Flood attacks	
Monitorowanie : SNMPv1/v2/v3	
Obsługa i znakowanie sieci VLAN IEEE 802.1q	
RIP	
Zasilanie	
Zasilacz 1 sztuka	
Możliwość podłączenia zasilaczy redundantnych.	
Dodatkowe wyposażenie	
Komplet przewodów połączeniowych do zastosowanych portów o właściwej długości.	
Komplet montażowy do szafy Rack.	
Serwis gwarancyjny	
Gwarancja nie mniej niż 3 lata na miejscu w siedzibie Zamawiającego.	
Czas realizacji zgłoszenia liczony od momentu zgłoszenia w godz. 7.00 – 17.00 wynosi nie więcej niż 120 min.	
Min. 5-cio letni okres zagwarantowania dostępności części zamiennych od daty upływu terminu gwarancji.	
Koszt części zamiennych na poziomie średnich cen rynkowych.	
Autoryzowany przez producenta serwis pogwarancyjny.	

3. Przełącznik typu ACCESS I

Parametry progowe (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Podać Producenta / Typ / Model / Rok produkcji (data produkcji sprzętu nie może być starsza niż 13 miesięcy licząc od dnia ogłoszenia niniejszego SIWZ-u)	Producent: Typ: Model: Rok produkcji:
Wymagania podstawowe	
Budowa typu Rack 19"	
Minimum 24 portów Ethernet 1000BaseT z auto-negocjacją 10/100/1000	
Minimum 2 - porty 10GE wyposażone we wkładki 10GBase-SR do połączenia z przełącznikami rdzeniowymi	
Możliwość podłączenia modułu uplink – nie mniej niż 2x10GbE	
Prędkość przełączania nie mniejsza niż: 80 Gb/s	
Przepustowość nie mniejsza niż : 60 mpps	
Warstwa przełączania : 2,3	
Możliwość łączenia przełączników fizycznych w jeden przełącznik wirtualny, jako jedno urządzenie logiczne z punktu widzenia protokołów routingu, LACP i Spanning Tree. Maksymalna liczba przełączników obsługiwanych w stosie co najmniej 9szt.	
Konfiguracja : konsola, SSH	
Port konsoli : 1szt.	
Standard IEEE 802.1ad (Q-in-Q)	
Standard IEEE 802.1d (STP)	
Możliwość separacji portów w warstwie L 2,3	
Przypisywanie adresu MAC do pojedynczego portu	
Pojemność tablicy MAC adresów nie mniej niż 12K	
Nie mniej niż 4000 aktywnych sieci VLAN	
Protokół umożliwiający tworzenie szybkobieżnych sieci w topologii pierścieni w których czas przełączenia transmisji na ścieżkę zapasową jest mniejszy niż 50ms	
DHCP snooping	
IEEE 802.1X– dynamiczne dostarczanie polityk QoS, ACLs i sieci VLANs:	

zezwalające na nadzór nad dostępem użytkownika do sieci	
Port security: zezwalający na dostęp tylko specyficznym adresom MAC	
MAC-based authentication	
Urządzenie musi być odporne na ataki typu Denial of service takich jak SYN Flood attacks, Land attacks, Smurf attacks, oraz ICMP Flood attacks	
Monitorowanie : SNMPv1/v2/v3	
Obsługa i znakowanie sieci VLAN IEEE 802.1q	
RIP	
Zasilanie	
Zasilacz 1 sztuka	
Możliwość podłączenia zasilaczy redundantnych.	
Dodatkowe wyposażenie	
Komplet przewodów połączeniowych do zastosowanych portów o właściwej długości.	
Komplet montażowy do szafy Rack.	
Serwis gwarancyjny	
Gwarancja nie mniej niż 3 lata na miejscu w siedzibie Zamawiającego.	
Czas realizacji zgłoszenia liczony od momentu zgłoszenia w godz. 7.00 – 17.00 wynosi nie więcej niż 120 min.	
Min. 5-cio letni okres zagwarantowania dostępności części zamiennych od daty upływu terminu gwarancji	
Koszt części zamiennych na poziomie średnich cen rynkowych.	
Autoryzowany przez producenta serwis pogwarancyjny.	

4. Przełącznik typu ACCESS II

Parametry progowe (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Podać Producenta / Typ / Model / Rok produkcji (data produkcji sprzętu nie może być starsza niż 13 miesięcy licząc od dnia ogłoszenia niniejszego SIWZ-u)	Producent: Typ: Model: Rok produkcji:
Wymagania podstawowe	
Budowa typu Rack 19"	
Minimum 48 portów Ethernet 1000BaseT z auto-negocjacją 10/100/1000	
Minimum 2 - porty 10GE wyposażone we wkładki 10GBase-SR do połączenia z przełącznikami rdzeniowymi	
Możliwość podłączenia modułu uplink – nie mniej niż 2x10GbE	
Prędkość przełączania nie mniejsza niż : 160 Gb/s	
Przepustowość nie mniejsza niż : 100 mpps	
Warstwa przełączania : 2,3	
Możliwość łączenia przełączników fizycznych w jeden przełącznik wirtualny, jako jedno urządzenie logiczne z punktu widzenia protokołów routingu, LACP i Spanning Tree. Maksymalna liczba przełączników obsługiwanych w stosie co najmniej 9szt.	
Konfiguracja : konsola, SSH	
Port konsoli : 1szt.	
Standard IEEE 802.1ad (Q-in-Q)	
Standard IEEE 802.1d (STP)	
Możliwość separacji portów w warstwie L 2,3	
Przypisywanie adresu MAC do pojedynczego portu	
Pojemność tablicy MAC adresów nie mniej niż 12K	
Nie mniej niż 4000 aktywnych sieci VLAN	
Protokół umożliwiający tworzenie szybkobieżnych sieci w topologii pierścieni w	

których czas przełączenia transmisji na ścieżkę zapasową jest mniejszy niż 50ms	
DHCP snooping	
IEEE 802.1X– dynamiczne dostarczanie polityk QoS, ACLs i sieci VLANs: zezwalające na nadzór nad dostępem użytkownika do sieci	
Port security: zezwalający na dostęp tylko specyficznym adresom MAC	
MAC-based authentication	
Urządzenie musi być odporne na ataki typu Denial of service takich jak SYN Flood attacks, Land attacks, Smurf attacks, oraz ICMP Flood attacks	
Monitorowanie : SNMPv1/v2/v3	
Obsługa i znakowanie sieci VLAN IEEE 802.1q	
RIP	
Zasilanie	
Zasilacz 1 sztuka	
Możliwość podłączenia zasilaczy redundantnych.	
Dodatkowe wyposażenie	
Komplet przewodów połączeniowych do zastosowanych portów o właściwej długości	
Komplet montażowy do szafy Rack.	
Serwis gwarancyjny	
Gwarancja nie mniej niż 3 lata na miejscu w siedzibie Zamawiającego.	
Czas realizacji zgłoszenia liczony od momentu zgłoszenia w godz. 7.00 – 17.00 wynosi nie więcej niż 120 min.	
Min. 5-cio letni okres zagwarantowania dostępności części zamiennych od daty upływu terminu gwarancji	
Koszt części zamiennych na poziomie średnich cen rynkowych.	
Autoryzowany przez producenta serwis pogwarancyjny.	

5. Przełącznik dla przedsięci bezpieczeństwa

Parametry progowe (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Podać Producenta / Typ / Model / Rok produkcji (data produkcji sprzętu nie może być starsza niż 13 miesięcy licząc od dnia ogłoszenia niniejszego SIWZ-u)	Producent: Typ: Model: Rok produkcji:
Wymagania podstawowe	
Budowa typu Rack 19"	
Minimum 48 portów Ethernet 1000BaseT z auto-negocjacją 10/100/1000	
Minimum 2 - porty 10GE wyposażone we wkładki 10GBase-SR do połączenia z przełącznikami rdzeniowymi	
Możliwość podłączenia modułu uplink – nie mniej niż 2x10GbE	
Prędkość przełączania nie mniejsza niż 160 Gb/s	
Przepustowość nie mniejsza niż 100 Mbps	
Warstwa przełączania : 2,3	
Możliwość łączenia przełączników fizycznych w jeden przełącznik wirtualny, jako jedno urządzenie logiczne z punktu widzenia protokołów routingu, LACP i Spanning Tree. Maksymalna liczba przełączników obsługiwanych w stosie co najmniej 9szt.	
Konfiguracja : konsola, SSH	
Port konsoli : 1szt.	
Standard IEEE 802.1ad (Q-in-Q)	
Standard IEEE 802.1d (STP)	
Możliwość separacji portów w warstwie L 2,3	

Przypisywanie adresu MAC do pojedynczego portu	
Pojemność tablicy MAC adresów nie mniej niż 12K	
Nie mniej niż 4000 aktywnych sieci VLAN	
Protokół umożliwiający tworzenie szybkobieżnych sieci w topologii pierścieni w których czas przełączenia transmisji na ścieżkę zapasową jest mniejszy niż 50ms	
DHCP snooping	
IEEE 802.1X– dynamiczne dostarczanie polityk QoS, ACLs i sieci VLANs: zezwalające na nadzór nad dostępem użytkownika do sieci	
Port security: zezwalający na dostęp tylko specyficznym adresom MAC	
MAC-based authentication	
Urządzenie musi być odporne na ataki typu Denial of service takich jak SYN Flood attacks, Land attacks, Smurf attacks, oraz ICMP Flood attacks	
Monitorowanie : SNMPv1/v2/v3	
Obsługa i znakowanie sieci VLAN IEEE 802.1q	
RIP	
Zasilanie	
Zasilacz 1 sztuka	
Możliwość podłączenia zasilaczy redundantnych.	
Dodatkowe wyposażenie	
Komplet przewodów połączeniowych do zastosowanych portów o właściwej długości.	
Komplet montażowy do szafy Rack.	
Serwis gwarancyjny	
Gwarancja nie mniej niż 3 lata na miejscu w siedzibie Zamawiającego.	
Czas realizacji zgłoszenia liczony od momentu zgłoszenia w godz. 7.00 – 17.00 wynosi nie więcej niż 120 min.	
Min. 5-cio letni okres zagwarantowania dostępności części zamiennych od daty upływu terminu gwarancji	
Koszt części zamiennych na poziomie średnich cen rynkowych.	
Autoryzowany przez producenta serwis pogwarancyjny.	

6. Firewall w GPD (urządzenie chroniące styk sieci LAN z internetem)

Parametry progowe (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Podać Producenta / Typ / Model / Rok produkcji (data produkcji sprzętu nie może być starsza niż 13 miesięcy licząc od dnia ogłoszenia niniejszego SIWZ-u)	Producent: Typ: Model: Rok produkcji:
Wymagania podstawowe	
Urządzenie fabrycznie nowe, nieużywane	
Obudowa przeznaczona do montażu w szafie 19".	
minimum 2 porty 1GE wyposażone we wkładki SFP 1GBase-LX	
Wymagane jest aby wszystkie powyższe porty mogły działać jednocześnie.	
Urządzenie wyposażone w zasilacz 230V/AC	
Przepustowość urządzenia nie mniej niż 800 Mbps	
Ilość jednocześnie obsługiwanych połączeń 900 000	
Minimalna efektywność IPSec VPN 280 Mbps	
Minimalna ilość jednocześnie obsługiwanych tuneli IPSec 1 800	
Obsługa trzech trybów pracy: routing mode, transparent mode, composite mode	
Funkcje warstwy 3	
Obsługa routingu IPv6.	

Techniki tunelowania IPv6: Dual-stacks, Manual tunnel, Automatic tunnel, GRE tunnel, 6over4 tunnel, 4over6 tunnel	
Protokoły routingu IPv6 : IS-IS, RIPng.	
MPLS VPN	
Firewall	
Obsługa pełnej funkcjonalności NAT a w szczególności: source IP address NAT, destination IP address NAT, static IP address NAT, IP pool NAT i expansion NAT.	
Wsparcie dla następujących protokołów : FTP ALG, H323(including T.120) ALG, SIP ALG, ICMP ALG, RTSP, NetBios ALG, ILS ALG, PPTP ALG, QQ ALG, MSN ALG, ICQ ALG, SQL.NET ALG, MMS ALG .	
Kontrola dostępu oparta na: adresie IP, porcie, typie protokołu, czasie i domenie ToS.	
Detekcja status ASPF: FTP, SMTP, HTTP, RTSP, H323, SIP, QQ, MSN, portów zdefiniowanych przez użytkownika, blokowanie Java/ActiveX, mapowania portów (PAM) i fragmentacji pakietów	
Ochrona przed atakami: SYN flood, ICMP flood, UDP flood, IP Spoofing, LAND attack, Smurf attack, Fraggle attack, WinNuke attack, Ping of Death attack, Tear Drop attack, address scanning attack, port scanning attack, IP Option control attack, IP packet fragmentation control attack, TCP label validity check attack, super ICMP packet control attack, ICMP redirection packet attack, ICMP unreachable packet attack i TRACERT packet	
Możliwość kontroli ruchu P2P: protocol-based P2P , policies-based p2p dla konkretnego klienta.	
Wsparcie dla: Xunlei, BT, Flashget, programów P2P oraz Torrent, KooWo, KuGoo, PPLive, PPStream, PP365, PPGou, PPFilm, QQdownload, QQLive, BaiBao, BBsee, BearShare, CCIPTV, CoolStreaming, DC, Dopool, FastTrack, Filetopia, Fs2you, GnuTella, Kazaa, Maze, Mysee, Poco, SopCast, Soulseek, UUSee, TVAnts, TVkoo, TVU, Vagaa	
Wsparcie dla: static blacklist, dynamic blacklist, blacklist relate z attack defense, blacklist relate.	
Wsparcie dla: routing statycznego, RIP, IS-IS, wsparcie dla polityk routing.	
Wsparcie dla: L2TP VPN, IPSEC VPN, L2TP VPN, GRE VPN, MPLS VPN, L2TP over IPsec VPN, GRE over IPsec VPN	
IPS	
Wsparcie detekcji niestandardowego zachowania protokołów: HTTP, SMTP, FTP, POP3, IMAP4, MSRPC, NETBIOS, SMB, MS_SQL, TELNET, IRC, DNS	
Wsparcie identyfikacji następujących protokołów: HTTP, SMTP, FTP, POP3, IMAP4, MSRPC, NETBIOS, SMB, MSSQL, TELNET, IRC, TFTP, programów P2P oraz Torrent, DNS	
Wsparcie dla powiązania pomiędzy politykami IPS a regułami ACL	
Możliwość całkowitego wyłączenia funkcji IPS	
Antywirus	
Skanowanie na obecność wirusów dla plików przesyłanych za pomocą protokołów HTTP, SMTP, POP3 i FTP	
Możliwość automatycznego upgrade bazy danych wirusów z możliwością ustawienia czasu upgrade.	
Możliwość ręcznego upgrade baz danych wirusów	
Możliwość usuwania wirusów, wyświetlania ostrzeżenia o wirusach i znaczenia emaili	
Możliwość całkowitego wyłączenia funkcji antywirusowych	
Filtrowanie URL	
Możliwość filtrowania dla list dozwolonych i zabronionych adresów URL	
Filtrowanie adresów URL w oparciu o kategorie	
Wsparcie dla URL category query ze zdalnego serwera	
Logowanie dostępu do URL	
Zarządzanie	

Zdalna konfiguracja i zarządzanie przez Web (https) oraz SSL	
Dostęp poprzez CLI i SSH	
Wsparcie dla funkcji debugowania za pomocą portu serialowego	
Wsparcie dla Syslog i logów w postaci binarnej. Funkcjonalność urządzenia nie może być zmniejszona w przypadku włączenia logowania binarnego	
Serwis gwarancyjny	
Gwarancja nie mniej niż 3 lata na miejscu w siedzibie Zamawiającego	
Czas realizacji zgłoszenia liczony od momentu zgłoszenia w godz. 7.00 – 17.00 wynosi nie więcej niż 120 min.	
Min. 5-cio letni okres zagwarantowania dostępności części zamiennych od daty upływu terminu gwarancji	
Koszt części zamiennych na poziomie średnich cen rynkowych.	
Autoryzowany przez producenta serwis pogwarancyjny.	

7. Firewall w przychodniach (urządzenie chroniące styk sieci LAN z internetem)

Parametry progowe (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Podać Producenta / Typ / Model / Rok produkcji (data produkcji sprzętu nie może być starsza niż 13 miesięcy licząc od dnia ogłoszenia niniejszego SIWZ-u)	Producent: Typ: Model: Rok produkcji:
Wymagania podstawowe	
urządzenie fabrycznie nowe, nieużywane	
obudowa przeznaczona do montażu w szafie telekomunikacyjnej 19".	
Urządzenie musi być przystosowane do pracy w temperaturze otoczenia od 5 do 45 stopni Celsjusza.	
Urządzenie musi być wyposażone w minimum 1 port FE typu WAN i co najmniej 8 portów FE typu LAN.	
Wymagane jest aby wszystkie powyższe porty mogły działać jednocześnie.	
Wydajność routingu minimum. 420 Kbps	
Port konsoli - szeregowy RS-232	
Funkcje warstwy 2	
Agregacja portów statyczna i przy pomocy protokołu LACP	
Obsługa VLANów zgodnie ze standardem 802.1q	
Obsługa Voice VLAN	
GARP VLAN Registration Protocol (GVRP)	
Port security	
Obsługa standardów STP, RSTP, MSTP	
Minimum 100 aktywnych sieci VLAN	
Funkcje warstwy 3	
Obsługa protokołów IPv4 i IPv6	
dynamic ARP, static ARP, proxy ARP, oraz ARPing	
DNS klient. DNS proxy/relay, Dynamic DNS	
NAT, PAT, NAT Serwer, NAT ALG (dla protokołów DNS, FTP, RSTP, SIP)	
DHCP Serwer, DHCP Relay, DHCP/BOOTP Klient	
Obsługa protokołów routingu statycznego i dynamicznego dla protokołów RIP, RIPng	
Obsługa wirtualnych tablic routingu.	
Obsługa co najmniej 5 tysięcy wpisów w tablicy routingu	
Bezpieczeństwo	
Ochrona protokołu STP: BPDU Protection, TC protection, Root Guard,	

Obsługa uwierzytelniania AAA, RADIUS oraz TACACS.	
Możliwość zarządzania urządzeniem poprzez protokół HTTPS	
Firewall typu "statefull inspection"	
Firewall oparty o strefy bezpieczeństwa	
Firewall musi rozpoznawać aplikacje co najmniej takie jak: FTP, HTTP, RSTP i SIP	
Obsługa ochrony CPU urządzenia przed atakami	
Obsługa protokołu 802.1x	
obsługa DHCP Snooping obejmującego ochronę przed atakami typu: Man-in-the-middle, IP/MAC spoofing, DoS poprzez podmianę adresu MAC, DoS poprzez zmianę wartości CHADDR	
Ochrona przeciwko atakom ARP typu spoofing i flood	
Ochrona przed atakami protokołem ICMP	
Obsługa mechanizmów IP Source Guard i URPF	
Obsługa ACL na podstawie adresów źródłowych i docelowych MAC i IP, portów źródłowych i docelowych protokołów TCP/UDP, znaczników DSCP i 802.1p, typów ICPM, protokołu TCP, VLANu.	
Możliwość przypisywania dla reguł ACL zakresów czasowych	
Obsługa PKI	
Obsługa protokołu SSL	
Obsługa protokołu VRRP	
Obsługa interfejsów zapasowych dla ruchu z możliwością wykrycia awarii w warstwie IP	
Moduły interfejsów muszą mieć możliwość wymiany w trakcie pracy urządzenia (funkcja Hot-Swap)	
Obsługa funkcji mirroringu ruchu na interfejsach lokalnego i zdalnego urządzenia	
Obsługa protokołu IPSec	
Tunelowanie typu GRE i L2TP	
Mechanizm Dynamic VPN typu Point to Multipoint i typu Mesh	
Obsługa SSL VPN	
Plik konfiguracyjny urządzenia musi być edytowalny w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych (ilość ograniczona tylko pojemnością pamięci). Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo – nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.	
Quality of Service (QoS)	
Obsługa mechanizmu QoS z zachowaniem gwarancji pasma, opóźnień i Jitter.	
Obsługa kolejkowania typu: PQ, WFQ, PQ+WFQ	
Limitowanie prędkości na portach z funkcją traffic shaping	
Obsługa klasyfikacji ruchu w oparciu o adres źródłowy MAC, adres docelowy MAC, źródłowy adres IP, docelowy adresu IP, interfejs warstwy 4, typ protokołu IP, VLAN, typu protokołu Ethernet oraz QoS.	
Obsługa hierarchicznego QoS	
Obsługa mechanizmów zapobiegania zatorów w sieci	
Obsługa mechanizmów RED, WRED	
Zarządzenie	
Zdalna konfiguracja i zarządzanie przez Web (https) oraz linię komend (CLI)	
IEEE 802.1ab LLDP	
Serwisy DHCP: serwer (RFC 2131), klient i relay	
SNMPv1, v2, v3	

Syslog	
Serwis gwarancyjny	
Gwarancja nie mniej niż 3 lata na miejscu w siedzibie Zamawiającego.	
Czas realizacji zgłoszenia liczony od momentu zgłoszenia w godz. 7.00 – 17.00 wynosi nie więcej niż 120 min.	
Min. 5-cio letni okres zagwarantowania dostępności części zamiennych od daty upływu terminu gwarancji	
Koszt części zamiennych na poziomie średnich cen rynkowych.	
Autoryzowany przez producenta serwis pogwarancyjny.	

8. VPN Centrala - router w GPD (zaawansowany)

Parametry progowe (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Podać Producenta / Typ / Model / Rok produkcji (data produkcji sprzętu nie może być starsza niż 13 miesięcy licząc od dnia ogłoszenia niniejszego SIWZ-u)	Producent: Typ: Model: Rok produkcji:
Wymagania podstawowe	
urządzenie fabrycznie nowe, nieużywane	
obudowa przeznaczona do montażu w szafie telekomunikacyjnej 19".	
Obudowa musi być wykonana z metalu. Ze względu na różne warunki, w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.	
Urządzenie musi być przystosowane do pracy w temperaturze otoczenia od 5 do 45 stopni Celsjusza.	
Urządzenie musi być modułarne z możliwością instalacji minimum 5 dodatkowych modułów sieciowych.	
Urządzenie musi być wyposażone w minimum 3 porty GE typu WAN, w tym co najmniej jeden port typu Combo (możliwość bezpośredniego podłączenia za pomocą styku miedzianego lub wykorzystania optycznej wkładki SFP).	
Wymagane jest aby wszystkie powyższe porty mogły działać jednocześnie.	
Wydajność routingu minimum. 1 Mbps	
Port konsoli - szeregowy RS-232	
Urządzenie musi być wyposażone w pamięć flash o pojemności minimum 4 GB	
Funkcje warstwy 2	
Agregacja portów statyczna i przy pomocy protokołu LACP	
Obsługa VLANów zgodnie ze standardem 802.1q	
Obsługa Voice VLAN	
GARP VLAN Registration Protocol (GVRP)	
Port security	
Obsługa standardów STP, RSTP, MSTP	
Funkcje warstwy 3	
Obsługa protokołów IPv4 i IPv6	
dynamic ARP, static ARP, proxy ARP, oraz ARPing	
DNS klient. DNS proxy/relay, Dynamic DNS	
NAT, PAT, NAT Serwer, NAT ALG (dla protokołów DNS, FTP, RSTP, SIP)	
DHCP Serwer, DHCP Relay, DHCP/BOOTP Klient	
Obsługa protokołów routingu statycznego i dynamicznego dla protokołów RIP, RIPng, IS-IS	
Obsługa wirtualnych tablic routingu.	
Obsługa co najmniej 30 tysięcy wpisów w tablicy routingu	
Bezpieczeństwo	

Ochrona protokołu STP: BPDU Protection, TC protection, Root Guard,	
Obsługa uwierzytelniania AAA, RADIUS oraz TACACS.	
Możliwość zarządzania urządzeniem poprzez protokół HTTPS	
Firewall typu "statefull inspection"	
Firewall oparty o strefy bezpieczeństwa	
Firewall musi rozpoznawać aplikacje co najmniej takie jak: FTP, HTTP, RSTP i SIP	
Obsługa ochrony CPU urządzenia przed atakami	
Obsługa protokołu 802.1x	
obsługa DHCP Snooping obejmującego ochronę przed atakami typu: Man-in-the-middle, IP/MAC spoofing, DoS poprzez podmianę adresu MAC, DoS poprzez zmianę wartości CHADDR	
Ochrona przeciwko atakom ARP typu spoofing i flood	
Ochrona przed atakami protokołem ICMP	
Obsługa mechanizmów IP Source Guard i URPF	
Obsługa ACL na podstawie adresów źródłowych i docelowych MAC i IP, portów źródłowych i docelowych protokołów TCP/UDP, znaczników DSCP i 802.1p, typów ICPM, flah protokołu TCP, VLANu.	
Możliwość przypisywania dla reguł ACL zakresów czasowych	
Obsługa PKI	
Obsługa protokołu SSL	
Obsługa protokołu VRRP	
Obsługa interfejsów zapasowych dla ruchu z możliwością wykrycia awarii w warstwie IP	
Moduły interfejsów muszą mieć możliwość wymiany w trakcie pracy urządzenia (funkcja Hot-Swap)	
Obsługa funkcji mirroringu ruchu na interfejsach lokalnego i zdalnego urządzenia	
LDP, MPLS L3 VPN, static LSP, dynamic LSP	
Obsługa protokołu IPSec	
Tunelowanie typu GRE i L2TP	
Mechanizm Dynamic VPN typu Point to Multipoint i typu Mesh	
Obsługa SSL VPN	
Plik konfiguracyjny urządzenia musi być edytowalny w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych (ilość ograniczona tylko pojemnością pamięci). Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo – nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.	
Quality of Service (QoS)	
Obsługa mechanizmu QoS z zachowaniem gwarancji pasma, opóźnień i Jitter.	
Obsługa kolejkowania typu: PQ, WFQ, PQ+WFQ	
Limitowanie prędkości na portach z funkcją traffic shaping	
Obsługa klasyfikacji ruchu w oparciu o adres źródłowy MAC, adres docelowy MAC, źródłowy adres IP, docelowy adresu IP, interfejs warstwy 4, typ protokołu IP, VLAN, typu protokołu Ethernet oraz QoS.	
Obsługa hierarchicznego QoS	
Obsługa mechanizmów zapobiegania zatorów w sieci	
Obsługa mechanizmów RED, WRED	
Zarządzenie	
Zdalna konfiguracja i zarządzanie przez Web (https) oraz linię komend (CLI)	
IEEE 802.1ab LLDP	
Serwisy DHCP: serwer (RFC 2131), klient i relay	

SNMPv1, v2, v3	
Syslog	
Serwis gwarancyjny	
Gwarancja nie mniej niż 3 lata na miejscu w siedzibie Zamawiającego.	
Czas realizacji zgłoszenia liczony od momentu zgłoszenia w godz. 7.00 – 17.00 wynosi nie więcej niż 120 min.	
Min. 5-cio letni okres zagwarantowania dostępności części zamiennych od daty upływu terminu gwarancji	
Koszt części zamiennych na poziomie średnich cen rynkowych.	
Autoryzowany przez producenta serwis pogwarancyjny.	

9. VPN jednostki terenowe - router w przychodniach

Parametry progowe (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Podać Producenta / Typ / Model / Rok produkcji (data produkcji sprzętu nie może być starsza niż 13 miesięcy licząc od dnia ogłoszenia niniejszego SIWZ-u)	Producent: Typ: Model: Rok produkcji:
Wymagania podstawowe	
urządzenie fabrycznie nowe, nieużywane	
obudowa przeznaczona do montażu w szafie telekomunikacyjnej 19".	
Urządzenie musi być przystosowane do pracy w temperaturze otoczenia od 5 do 45 stopni Celsjusza.	
Urządzenie musi być wyposażone w minimum 1 port FE typu WAN i co najmniej 8 portów FE typu LAN.	
Wymagane jest aby wszystkie powyższe porty mogły działać jednocześnie.	
Wydajność routingu minimum. 420 Kbps	
Port konsoli - szeregowy RS-232	
Funkcje warstwy 2	
Agregacja portów statyczna i przy pomocy protokołu LACP	
Obsługa VLANów zgodnie ze standardem 802.1q	
Obsługa Voice VLAN	
GARP VLAN Registration Protocol (GVRP)	
Port security	
Obsługa standardów STP, RSTP, MSTP	
Minimum 100 aktywnych sieci VLAN	
Funkcje warstwy 3	
Obsługa protokołów IPv4 i IPv6	
dynamic ARP, static ARP, proxy ARP, oraz ARPing	
DNS klient. DNS proxy/relay, Dynamic DNS	
NAT, PAT, NAT Serwer, NAT ALG (dla protokołów DNS, FTP, RSTP, SIP)	
DHCP Serwer, DHCP Relay, DHCP/BOOTP Klient	
Obsługa protokołów routingu statycznego i dynamicznego dla protokołów RIP, RIPng, IS-IS	
Obsługa wirtualnych tablic routingu.	
Obsługa co najmniej 5 tysięcy wpisów w tablicy routingu	
Bezpieczeństwo	
Ochrona protokołu STP: BPDU Protection, TC protection, Root Guard,	
Obsługa uwierzytelniania AAA, RADIUS oraz TACACS.	
Możliwość zarządzania urządzeniem poprzez protokół HTTPS	
Firewall typu "statefull inspection"	
Firewall oparty o strefy bezpieczeństwa	
Firewall musi rozpoznawać aplikacje co najmniej takie jak: FTP, HTTP, RSTP i SIP	
Obsługa ochrony CPU urządzenia przed atakami	
Obsługa protokołu 802.1x	

obsługa DHCP Snooping obejmującego ochronę przed atakami typu: Man-in-the-middle, IP/MAC spoofing, DoS poprzez podmianę adresu MAC, DoS poprzez zmianę wartości CHADDR	
Ochrona przeciwko atakom ARP typu spoofing i flood	
Ochrona przed atakami protokołem ICMP	
Obsługa mechanizmów IP Source Guard i URPF	
Obsługa ACL na podstawie adresów źródłowych i docelowych MAC i IP, portów źródłowych i docelowych protokołów TCP/UDP, znaczników DSCP i 802.1p, typów ICPM, protokołu TCP, VLANu.	
Możliwość przypisywania dla reguł ACL zakresów czasowych	
Obsługa PKI	
Obsługa protokołu SSL	
Obsługa protokołu VRRP	
Obsługa BFD dla VRRP	
Obsługa interfejsów zapasowych dla ruchu z możliwością wykrycia awarii w warstwie IP	
Możliwość konfiguracji BFD typu Multi-Hop	
Moduły interfejsów muszą mieć możliwość wymiany w trakcie pracy urządzenia (funkcja Hot-Swap)	
Obsługa funkcji mirroringu ruchu na interfejsach lokalnego i zdalnego urządzenia	
Obsługa protokołu IPSec	
Tunelowanie typu GRE i L2TP	
Mechanizm Dynamic VPN typu Point to Multipoint i typu Mesh	
Obsługa SSL VPN	
Plik konfiguracyjny urządzenia musi być edytowalny w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych (ilość ograniczona tylko pojemnością pamięci). Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo – nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.	
Quality of Service (QoS)	
Obsługa mechanizmu QoS z zachowaniem gwarancji pasma, opóźnień i Jitter.	
Obsługa kolejkowania typu: PQ, WFQ, PQ+WFQ	
Limitowanie prędkości na portach z funkcją traffic shaping	
Obsługa klasyfikacji ruchu w oparciu o adres źródłowy MAC, adres docelowy MAC, źródłowy adres IP, docelowy adresu IP, interfejs warstwy 4, typ protokołu IP, VLAN, typu protokołu Ethernet oraz QoS.	
Obsługa hierarchicznego QoS	
Obsługa mechanizmów zapobiegania zatorów w sieci	
Obsługa mechanizmów RED, WRED	
Zarządzenie	
Zdalna konfiguracja i zarządzanie przez Web (https) oraz linię komend (CLI)	
IEEE 802.1ab LLDP	
Serwisy DHCP: serwer (RFC 2131), klient i relay	
SNMPv1, v2, v3	
Syslog	
Serwis gwarancyjny	
Gwarancja nie mniej niż 3 lata na miejscu w siedzibie Zamawiającego.	
Czas realizacji zgłoszenia liczony od momentu zgłoszenia w godz. 7.00 – 17.00 wynosi nie więcej niż 120 min.	
Min. 5-cio letni okres zagwarantowania dostępności części zamiennych od daty upływu terminu gwarancji	
Koszt części zamiennych na poziomie średnich cen rynkowych.	
Autoryzowany przez producenta serwis pogwarancyjny.	

10. System Zarządzania i Monitoringu Sieci Komputerowej

Parametry progowe (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Podać Producenta / Nazwa programu/Numer wersji	Producent: Nazwa programu: Numer wersji:
Wymagania podstawowe:	
Obsługa minimum 110 urządzeń sieciowych	
Wymagana jest architektura serwer-klient z dostępem do systemu poprzez przeglądarkę WWW (MS Internet Explorer 8, Firefox 3.6 lub nowsze)	
Wymagany interfejs użytkownika w języku polskim lub angielskim	
Obsługiwana lokalna baza użytkowników systemu	
Czasowe blokowanie możliwości logowania użytkownika systemu w przypadku 5-krotnego podania błędnego hasła	
Możliwość stworzenia kopii zapasowej danych systemu zarządzania i odtworzenia tych danych z kopii	
W przypadku gdy oprogramowania korzysta z systemu licencjonowania powinna być zapewniona możliwość sprawdzenia zainstalowanej licencji oraz zmiany licencji	
Monitorowanie wykorzystania licencji i informowanie użytkownika systemu o zbliżającej się dacie wygasania licencji, bądź przekroczenia limitów zainstalowanej licencji (np. Ilość obsługiwanych urządzeń)	
Dostępna w systemie zarządzającym dokumentacja w języku polskim lub angielskim	
Zarządzenie alertami	
Możliwość automatycznego alarmowania opartego o zadane progi alarmowe, w tym	
możliwość definiowania dwóch progów – ostrzegawczy i alarmowy	
Możliwość automatycznego alarmowania opartego o profil ruchu	
Możliwość automatycznego alarmowania o przekroczeniu obciążenia interfejsu z uwzględnieniem dwóch progów - ostrzegawczy i alarmowy	
Możliwość określenia listy osób i grup osób powiadamianych przy poszczególnych	
Możliwość wykorzystania następujących kanałów powiadomienia dla poszczególnych poziomów alarmów :	
konsola operatora	
SMS na numer telefonu wskazanego operatora	
e-mail	
Monitorowanie	
Możliwość monitorowania zdarzeń związanych z funkcjonowaniem monitorowanych urządzeń w czasie rzeczywistym (CPU, pamięć)	
Możliwość monitorowania urządzeń sieciowych oraz ruchu sieciowego w oparciu o protokoły SNMP	
Możliwość zbierania danych z urządzeń firmy Cisco generowanych w oparciu o protokół SNMP	
Możliwość zapisywania niezagregowanych danych pochodzących z monitorowanych urządzeń przez okres 30 dni.	
Możliwość archiwizacji dostępnych danych niezagregowanych.	
Możliwość monitorowania obciążenia całkowitego urządzeń oraz ich interfejsów z zachowaniem:	
Wartości aktualnych	
Wartości szczytowych	
Możliwość pozyskania informacji o statusie monitorowanych urządzeń sieciowych	
Możliwość pozyskania informacji o statusie portu	
Możliwość ręcznego definiowania progów czułości alarmów	

Możliwość przesyłania powiadomień o alarmach za pomocą mechanizmu SNMP trap	
Możliwość monitorowania obciążenia całkowitego urządzeń oraz ich interfejsów z zachowaniem rozgraniczenia dla ruchu wchodzącego i wychodzącego	
Możliwość wyświetlania 95 percentyla dla raportów obciążenia interfejsów niezależnie dla kierunku wejściowego i wyjściowego	
Zarządzanie konfiguracją	
Możliwość współpracy z urządzeniami sieciowymi różnych producentów	
Wsparcie dla protokołu NetFlow (wersja 1, 5, 7, 9) lub równoważnego oraz SNMP (wersja 1,2,3)	
Możliwość konfigurowania zarządzanych urządzeń	
Możliwość automatycznego wykrywania urządzeń sieciowych	
Możliwość automatycznego odczytywania z monitorowanych i zarządzanych urządzeń ich nazw, listy interfejsów wraz z ich nazwami i prędkościami. System zarządzania i monitorowania sieci powinien umożliwiać dokonywanie automatycznego odczytu o zdefiniowanej g	Możliwość stworzenia mapy topologii fizycznej i logicznej sieci
Możliwość tworzenia i zarządzania sieciami VLAN (niezależnie od fizycznej lokalizacji urządzeń)	
Możliwość pełnego dostępu i zarządzania systemem monitorowania i zarządzania siecią zarówno lokalnie jak i zdalnie	
Możliwość uzyskania zdalnego dostępu do urządzeń sieciowych i dokonania zmian w ich konfiguracji.	
Możliwość definiowania w systemie monitorowania i zarządzania siecią użytkowników z nadawaniem uprawnień na poziomie poszczególnych urządzeń oraz grupy urządzeń, do odczytu konfiguracji urządzenia, zarządzania urządzeniem.	
Możliwość stworzenia kopii zapasowej ustawień urządzeń	
Możliwość przywrócenia kopii zapasowej ustawień urządzeń	
Możliwość ręcznego dodawania opisów do poszczególnych interfejsów monitorowanych urządzeń	
Możliwość logowania i uwierzytelniania w oparciu o lokalną bazę użytkowników	
Możliwość wymuszenia logowania się wszystkich użytkowników systemu monitorowania i zarządzania siecią.	
Możliwość przeprowadzenia testów dostępności urządzenia	
Liczby przeprowadzonych udanych oraz nieudanych odpytań SNMP	
Możliwość tworzenia szablonów konfiguracji dla danego modelu urządzenia	
Raportowanie	
Możliwość raportowania na poziomie pojedynczego urządzenia oraz grupy urządzeń obejmującego dostępne w Systemie - parametry sieciowe i wydajnościowe	
Możliwość raportowania zdarzeń w trybie rzeczywistym - czasie zbliżonym do rzeczywistego, dla urządzeń (na bieżąco wobec wpływających raportów NetFlow)	
Możliwość raportowania w formie graficznej (wykresy) jak i tekstowej (tabela z wszystkimi konwersacjami)	
Możliwość raportowania obciążenia całkowitego urządzeń oraz ich interfejsów z zachowaniem :	
Wartości aktualnych	
Wartości szczytowych	
Możliwość tworzenia raportów dostępności urządzeń	
Możliwość przeglądania raportów za pośrednictwem przeglądarki WWW	
Możliwość eksportu raportów do plików płaskich lub ustrukturyzowanych	
Możliwość automatycznego generowania, zapisywania i wysyłania raportów pocztą email	
Administracja systemem i Bezpieczeństwo	
Możliwość tworzenia unikalnych kont użytkowników	

Możliwość zabezpieczenia Dostępu do kont użytkowników przy pomocy haseł	
Możliwość logowania zdarzeń i aktywności użytkowników narzędzia	
Możliwość zarządzania uprawnieniami na poziomie grup - pojedynczych użytkowników	
Możliwość przypisywania użytkownikom - grupom uprawnień na poziomie:	
czynności	
elementów konfiguracji (np. urządzenie sieciowe, grupa urządzeń sieciowych)	
Możliwość definiowania wielu użytkowników, w tym możliwość różnicowania uprawnień odczytu oraz różnicowania uprawnień administracyjnych z podziałem na grupy urządzeń	
Możliwość tworzenia widoków dla użytkowników w zależności od zakresu uprawnień	
Możliwość tworzenia widoków jedynie do podglądu	
Możliwość archiwizacji i odtwarzania danych narzędzia, w tym konfiguracji oraz informacji o licencji	
Możliwość importu całej lub fragmentu konfiguracji narzędzia	
Możliwość konfigurowania, zarządzania oraz monitorowania usług VPN (IPSec)	
Serwis gwarancyjny	
Wymagany jest serwis gwarancyjny świadczony przez minimum 3 lata.	
Dostępność serwisu 8x5xNBD	
Rozwiązywanie problemów ze sprzętem i oprogramowaniem	
Gwarantowany czas naprawy platformy sprzętowej aplikacji – 48h od momentu zgłoszenia	
Dostęp do poprawek i nowych wersji oprogramowania	
Wykonawca wraz z systemem zarządzania i monitoringu musi dostarczyć platformę serwerową, która obsłuży system wyspecyfikowany powyżej przy założeniu obsługi maksimum 500 urządzeń	

11. Homogeniczność sieci i urządzeń (przełączników i firewall)

Parametry progowe (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Podać producenta: Jeden producent wszystkich urządzeń aktywnych sieci (przełączniki i firewall)	Producent:

12. System Okablowania Strukturalnego

Parametry progowe (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Podać Producenta (Elementy toru transmisyjnego: kabel, patchpanel, patchcord, powinny pochodzić od tego samego producenta).	Producent:
Kable oparte o system miedziany, faktyczna instalacja powinna być wykonana kablami F/UTP kat.6	
Instalacja kabli w powłoce LSOH wg przepisów budynkowych, p.poż i BHP	
Gwarancja: 1. Wydanie Certyfikatu i karty urządzeń 2. Zapewnienie 25 letniej gwarancji na system okablowania strukturalnego licząc od dnia podpisania protokołu zdawczo-odbiorczego przez obydwie strony.	1. 2.

13. Serwis, konserwacja i nadzór nad połączeniem VPN

Parametry progowe (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Gwarancja: Nie mniej niż 36 miesięcy kalendarzowych licząc od dnia podpisania protokołu zdawczo-odbiorczego przez obydwie strony.	
Wykonanie kopii ustawień konfiguracyjnych wszystkich urządzeń aktywnych na nośniku zewnętrznym, oraz przekazanie ich z hasłami dostępowymi w sposób jednoznacznie i wyraźnie opisany: 1. Urządzenie (Producent, Model, Typ) 2. Data kopii konfiguracji: DD.MM.RRRR 3. Użytkownik: 4. Hasło dostępowe:	1. 2. 3. 4.
Support: Czas podjęcia naprawy od momentu zgłoszenia w godz. 7.00 – 18.00 wynosi nie więcej niż 90 min..	

14. Przyłączenie i konfiguracja urządzeń aktywnych w sieci LAN oraz na styku WAN / LAN

Wykonanie czynności i usługi (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Konfiguracja urządzeń aktywnych na styku LAN / WAN w sposób zapewniający optymalne i bezawaryjne działanie wszystkich urządzeń w sieci.	
Zestawienie (konfiguracja i parametryzacja) łączy VPN między Szpitalem a Placówkami: 1. Budynek Przychodni na ul Miodowej 2 2. Budynek Przychodni na ul Tysiąclecia 13 3. Budynek Przychodni na ul Reja 15 4. Budynek Przychodni na ul Zielonej 40 (łącze radiowe) 5. Budynek Przychodni na ul Góry 7	1. 2. 3. 4. 5.
Konfiguracja urządzeń aktywnych w sieci LAN sposób zapewniający optymalne i bezawaryjne działanie wszystkich urządzeń w sieci.	
Wykonanie kopii ustawień konfiguracyjnych wszystkich urządzeń aktywnych na nośniku zewnętrznym, oraz przekazanie ich z hasłami dostępowymi w sposób jednoznacznie i wyraźnie opisany: 1. Urządzenie (Producent, Model, Typ) 2. Data kopii konfiguracji: DD.MM.RRRR 3. Użytkownik: 4. Hasło dostępowe:	1. 2. 3. 4.

15. System Telewizji Dozorowej – CCTV

Parametry progowe (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Kamery: Podać Producenta / Typ / Model / Rok produkcji (data produkcji sprzętu nie może	Producent: Typ:

być starsza niż 13 miesięcy licząc od dnia ogłoszenia niniejszego SIWZ-u)	Model: Rok produkcji:
Zastosować kamery dualne 1/3", o minimalnej liczbie linii 540	
Rejestratory: Podać Producenta / Typ / Model / Rok produkcji (data produkcji sprzętu nie może być starsza niż 13 miesięcy licząc od dnia ogłoszenia niniejszego SIWZ-u)	Producent: Typ: Model: Rok produkcji:
Zastosować rejestratory 16-kanałowe, do 400 kl/sek, MPEGCCTV, cyfrowy zapis z prędkością 25 kl/sek, wbudowana karta sieciowa.	
Krosownica: Podać Producenta / Typ / Model / Rok produkcji (data produkcji sprzętu nie może być starsza niż 13 miesięcy licząc od dnia ogłoszenia niniejszego SIWZ-u)	Producent: Typ: Model: Rok produkcji:
Zastosować krosownicę z min. 32 złączami przelotowymi, 4 wyjścia monitorowe, wejścia sygnałów alarmowych, sterowanie z manipulatora.	
Główny punkt obserwacji zlokalizować w budynku portierni. Rejestratory umieścić w dedykowanej szafie 19" GPD w serwerowni głównej.	
Gwarancją objęte są wszystkie urządzenia i elementy systemu CCTV na okres nie krótszy niż 24 miesiące licząc od dnia podpisania protokołu zdawczo-odbiorczego przez obydwie strony.	
Min. 5-cio letni okres zagwarantowania dostępności części zamiennych od daty upływu terminu gwarancji	
Koszt części zamiennych na poziomie średnich cen rynkowych.	
Autoryzowany przez producenta serwis pogwarancyjny.	

16. System Kontroli Dostępu – KD

Parametry progowe (minimalne wymagania)	Potwierdzone spełnienie wymagań przez Wykonawcę - wymagana odpowiedź TAK
Kontroler: Podać Producenta / Typ / Model / Rok produkcji (data produkcji sprzętu nie może być starsza niż 13 miesięcy licząc od dnia ogłoszenia niniejszego SIWZ-u)	Producent: Typ: Model: Rok produkcji:
System obsługiwany ma być za pomocą kart dostępu.	
Centrala sterująca KD: Podać Producenta / Typ / Model / Rok produkcji (data produkcji sprzętu nie może być starsza niż 13 miesięcy licząc od dnia ogłoszenia niniejszego SIWZ-u)	Producent: Typ: Model: Rok produkcji:

Powyższe informacje należy traktować, jako integralną część SIWZ.

Treść niniejszego pisma dostępna jest na stronie internetowej Zamawiającego: www.szpitalplock.pl.

Jednocześnie Zamawiający, na podstawie art. 38 ust. 4 przedłuża termin składania ofert do dnia 21.12.2012 r., do godz. 09:30. Otwarcie ofert nastąpi tego samego dnia o godz. 10:00.

Wyjaśnienie treści specyfikacji istotnych warunków zamówienia wraz ze zmianą jej treści

z dnia 28 listopada 2012 roku

PZOZ/DZP/382/21PN/12

Zgodnie z art. 27 ust. 2 ustawy – Prawo zamówień publicznych Zamawiający prosi o niezwłoczne potwierdzenie otrzymania niniejszego pisma na nr faxu 24 364 51 02.

Otrzymano dnia Ilość stron Podpis i pieczęć Wykonawcy