Załącznik 1b do SIWZ

**Szczegółowy opis przedmiotu zamówienia dla Cześć 2 : Dostawa i instalacja urządzeń sieciowych**– dotyczy przetargu nieograniczonego na Informatyzację w ZOZ Końskie w ramach projektu: „Informatyzacja Placówek Medycznych Województwa Świętokrzyskiego”

# Wymagania ogólne dla dostarczanych rozwiązań:

1. System powstały w wyniku niniejszego zamówienia musi funkcjonować zgodnie z obowiązującymi przepisami prawa w szczególności uwzględniać zmiany dotyczące przedmiotu realizacji projektu.
2. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów.
3. Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 9 miesięcy przed datą złożenia oferty) oraz by były nieużywane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji poprawności działania.
4. Zamawiający zastrzega sobie prawo żądania przeprowadzenia testów poszczególnych funkcjonalności przed wyborem oferty.
5. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
6. Oferowane urządzenia w dniu składania oferty nie mogą być przeznaczone przez ich producenta do wycofania z produkcji lub sprzedaży.
7. Oferowane oprogramowanie w dniu składania oferty nie może być przeznaczone przez jego producenta do wycofania z produkcji, sprzedaży lub wsparcia technicznego.
8. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień składania ofert.
9. Dla zaoferowanego oprogramowania należy dostarczyć: licencje, nośniki instalacyjne oraz instrukcje obsługi.
10. Zamawiający wymaga, aby cały dostarczony sprzęt został skonfigurowany, uruchomiony i przetestowany przez Wykonawcę pod nadzorem pracowników Zamawiającego
11. Dostawy wymaganego i opisanego poniżej sprzętu do lokalizacji Zamawiającego
12. Instalacji sprzętu
13. Uruchomienia i konfiguracji system ochrony danych (UTM).
14. Instalacji dostarczonych urządzeń sieciowych oraz konfiguracji sieci LAN, w tym podsieci VLAN zgodnie z wymaganiami Zamawiającego

# Warunki gwarancji

1. Zamawiający wymaga minimum 36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.

Maksymalny czas naprawy sprzętu - 30 dni.

1. Zgłaszanie awarii musi następować w trybie 8x5.
2. Serwis musi być świadczony bezpośrednio przez producenta sprzętu lub autoryzowany serwis w języku polskim.

Spis treści

[1. Przełącznik serwerowy 3](#_Toc10017323)

[2. Przełączniki LAN 8](#_Toc10017324)

[3. Firewall 16](#_Toc10017325)

[4. Przełącznik zarządzający 26](#_Toc10017326)

## Przełącznik serwerowy

|  |  |
| --- | --- |
| **Przełącznik serwerowy - ilość – 2 szt.**  **Karta katalogowa - TAK** | |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Obudowa** | Urządzenie przystosowane jest do montażu w szafie stelażowej 19”, wysokość – 1U. Głębokość nie większa niż 46cm |
| **Interfejsy** | * Minimum 40 portów 1G/10GbE SFP+ umieszczonych z przodu obudowy * Minimum 2 porty 40GbE QSFP+ umieszczone z przodu obudowy * Każdy przełącznik wyposażony w kabel DAC QSFP+ o długości co najmniej 1 metr. * Wbudowany, dodatkowy, dedykowany port Ethernet do zarządzania poza pasmem - out of band management * Port konsoli RS232 ze złączem DB9 lub RJ45 * Port USB 2.0 |
| **Wydajność** | * Przepustowość minimum 714 Mpps dla pakietów 64 bajtowych * Wydajność: minimum 960 Gbps (prędkość przełączania „wirespeed” dla każdego portu przełącznika) * Tablica routingu o pojemności co najmniej 1000 wpisów * Tablica adresów MAC o wielkości minimum 64000 pozycji * Obsługa ramek Jumbo o wielkości 10kB * Minimum 512MB pamięci typu Flash * Minimum 2GB pamięci operacyjnej * Wielkość bufora pakietów (packet buffer): minimum 9MB |
| **Środowisko** | * Minimalny zakres temperatur pracy od 0°C do 45°C |
| **Zasilanie** | * Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia. * Maksymalny pobór mocy nie większy niż 180W |
| **Funkcjonalność** | * Przełączanie w warstwie 2 i 3 modelu OSI * Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów) * Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika (porty) do tyłu przełącznika (zasilacze). Nie dopuszczalne są rozwiązania, z mieszanym przepływem powietrza. * Funkcja łączenia w stos grupy przełączników, urządzenia połączone w stos widziane jako jedno logiczne urządzenie ze wspólnym zarządzaniem. Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 360 portów 10GbE SFP+. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain)). * Łączenie w stos z wykorzystaniem portów 10Gb, 40Gb i agregowanych portów 10Gb (w celu zwiększenia przepustowości w stosie) * Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie * Obsługa Quality of Service * Obsługa mechanizmów: strict priority (SP) queuing, weighted fair queuing (WFQ), weighted random early discard (WRED), weighted deficit round robin (WDRR), explicit congestion notification (ECN), SP+WFQ oraz SP+WDRR * Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol * Obsługa sieci IEEE 802.1Q VLAN – 4094 sieci VLAN oraz IEEE 802.1ad QinQ * Obsługa IGMP Snooping v1/v2/v3, PIM Snooping, MLD snooping v1/v2 oraz IPv6 PIM Snooping * Wsparcie dla FibreChannel over Ethernet (FCF/Transit/NPV) * Wsparcie dla Data Center Bridging (DCB):   + IEEE 802.1Qbb Priority Flow Control (PFC)   + Data Center Bridging Exchange (DCBX) * Obsługa Transparent Interconnection of Lots of Links (TRILL) * Routing IPv4 – statyczny i dynamiczny (min. RIP, IS-IS, OSPF, BGP) * Routing IPv6 – statyczny i dynamiczny (min. RIPng, IS-ISv6, OSPFv3) * Obsługa ECMP (Equal Cost Multi Path) * Serwer DHCP, klient DHCP, obsługa opcji 82 (snooping i relay), DHCP snooping * Obsługa list ACL na bazie informacji z warstw 3/4 modelu OSI. * Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia * Obsługa standardu 802.1p * Możliwość zmiany wartości pola DSCP i/lub wartości priorytetu 802.1p * Funkcje mirroringu: 1 to 1 Port mirroring, Many to 1 port mirroring, remote mirroring * Obsługa funkcji logowania do sieci („Network Login”) zgodna ze standardem IEEE 802.1x * Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS * Zarządzanie poprzez port konsoli, SNMP v.1, 2c i 3, Telnet, SSH v.2 * Syslog * Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) oraz LLDP-MED * Obsługa sFlow * Obsługa NETCONF * Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3 * Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter * Obsługa Network Time Protocol (NTP), Simple Network Time Protocol (SNTP) oraz kompatybilność z Precision Time Protocol (PTP) RFC 1855 * Obsługa OAM (IEEE 802.3ah) * Obsługa CFD (IEEE 802.1ag) * Modularny system operacyjny ze wsparciem dla In Services Software Upgrade (ISSU) i skryptów w języku Python * Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania). * Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji). * Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji 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 nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. |
| **Wyposażenie dodatkowe** | Wraz z przełącznikiem sieciowym należy dostarczyć oraz zainstalować:   * Kompatybilne z przełącznikiem wkładki 10G SFP+ LR (na światłowód jednomodowy) – 16 sztuk/przełącznik * Każdy przełącznik wyposażony 10 x DAC 5m SFP+ to SFP+ umożliwiające podłączenie przełączników z dostarczanym sprzętem IT (serwerami wirtualizacji, backupu, bazy danych, macierzami, UTM-ami) * 16 sztuk kabli LC-LC co najmniej OS2 i długości min. 10m |
| **Gwarancja** | Minimum 3 letni serwis producenta obejmujący wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniający reakcję w miejscu instalacji maksymalnie na następny dzień roboczy. Wymagana jest dostępność usługi w trybie 8x5 w godzinach od 8:00 do 17:00. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. Aktualizacje oprogramowania i poprawki muszą być dostępne (bezpośrednio od producenta) przez cały czas użytkowania przełącznika, również po wygaśnięciu kontraktu serwisowego. |
| **Certyfikaty** | Przełącznik serwerowy musi być wyprodukowany zgodnie z normą ISO 9001.  Przełącznik serwerowy musi posiadać deklaracje CE.  **Na potwierdzenie złożyć** kopię certyfikatu zgodności. |

## Przełączniki LAN

|  |  |
| --- | --- |
| **Przełącznik LAN ilość – 7 szt.**  **Karta katalogowa - TAK** | |
| **Wymagane minimalne parametry techniczne** | |
| 1. Co najmniej 24 portów gigabitowych w standardzie 100/1000BaseT  2. Minimum 4 porty 10Gb SFP+. Dla zwiększenia niezawodności porty SFP+ powinny być umieszczone na module pozwalającym na ich wymianę. Dla zapewnienia przyszłej rozbudowy, musi być dostępny wymienny moduł zapewniający co najmniej jeden port 40Gb/s QSFP+ lub QSFP28  3. Minimum 2 dedykowane porty stackujące (niezależne od portów SFP+), pozwalające na połączenie w stos minimum 9 przełączników. Agregowana prędkość magistrali stackującej nie może być mniejsza niż 100Gb/s. Stos musi być widoczny jako jedno urządzenie (wspólne zarządzanie z jednej linii komend, analogiczne do przełącznika modularnego). Dopuszcza się rozwiązanie, w którym porty stackujące dostępne są w postaci opcjonalnego modułu (niezależnego od modułów 10Gb i 40Gb opisanych w punkcie 2), który jednak musi być dostępny w chwili składania oferty i zaoferowany. Do przełącznika musi być dołączony kabel służący do połączenia w stos o długości co najmniej 50cm.  4. Przepustowość: minimum 128 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika), nie licząc magistrali stackującej  5. Wydajność: minimum 95 Mp/s  6. Tablica adresów MAC o wielkości minimum 32000 pozycji  7. Obsługa ramek Jumbo  8. Minimum 4GB pamięci stałej typu Flash, minimum 1GB pamięci RAM  9. Minimum 12MB bufora pakietów  10. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych  11. Port USB  12. Jeden modularny wewnętrzny zasilacz prądu zmiennego, slot na drugi zasilacz. Przy wykorzystaniu obydwu źródeł zasilania możliwość pracy zasilaczy w trybie redundantnym oraz możliwość wymieniany na gorąco  13. Routing IPv4 – minimum: statyczny, RIPv2, OSPF  14. Routing IPv6 – minimum: statyczny, RIPng, OSPFv3  15. Obsługa protokołu VRRP  16. Wielkość tablicy rutingu: minimum 10000 wpisów dla IPv4, 5000 wpisów dla IPv6  17. IGMPv1/v2/v3 Snooping; MLDv1/v2 Snooping, PIM Dense Mode, PIM Sparse Mode  18. Obsługa VxLAN  19. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol  20. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN  21. Funkcja Root Guard oraz BPDU protection  22. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie  23. Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping  24. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI  25. Obsługa standardu 802.1p – min. 8 kolejek na porcie  26. Funkcja mirroringu portów  27. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)  28. Funkcja autoryzacji użytkowników zgodna z 802.1x  29. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+  30. RADIUS Accounting  31. Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3  32. OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic.  33. Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP)  34. Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow.  35. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az  36. Zarządzanie poprzez port konsoli (pełne) (RS-232 i USB), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https  37. Obsługa Syslog  38. Obsługa SNTPv4 lub NTP  39. Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku  40. Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej  41. Wsparcie dla funkcji Private VLAN lub równoważnego  42. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link Detection Protocol (DLDP) lub równoważnego  43. Minimalny zakres pracy od 0°C do 45°C  44. Wysokość w szafie 19” – 1U, głębokość nie większa niż 50 cm | |
| **Wyposażenie dodatkowe** | Wraz z przełącznikiem sieciowym należy dostarczyć oraz zainstalować:   * Kompatybilne z przełącznikiem wkładki 10G SFP+ LR (na światłowód jednomodowy) – 2 sztuki/przełącznik * 2 sztuki kabli LC-LC co najmniej OS2 i długości min. 5m – 2 sztuki/przełącznik |
| **Gwarancja** | MINIMUM3 letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez okres co najmniej 3 lat. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis - **na potwierdzenie złożyć** oświadczenie Wykonawcy. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. |
| **Certyfikaty** | Przełącznik LAN musi być wyprodukowany zgodnie z normą ISO 9001.  Przełącznik LAN musi posiadać deklaracje CE.  **Na potwierdzenie złożyć** kopię certyfikatu zgodności. |
|  |  |
| **Przełącznik LAN** | **Ilość – 19 szt.**  **Karta katalogowa - TAK** |
| **Wymagane minimalne parametry techniczne** | |
| 1. Co najmniej 48 portów gigabitowych w standardzie 100/1000BaseT  2. Minimum 4 porty 10Gb SFP+. Dla zwiększenia niezawodności porty SFP+ powinny być umieszczone na module pozwalającym na ich wymianę. Dla zapewnienia przyszłej rozbudowy, musi być dostępny wymienny moduł zapewniający co najmniej jeden port 40Gb/s QSFP+ lub QSFP28  3. Minimum 2 dedykowane porty stackujące (niezależne od portów SFP+), pozwalające na połączenie w stos minimum 9 przełączników. Agregowana prędkość magistrali stackującej nie może być mniejsza niż 100Gb/s. Stos musi być widoczny jako jedno urządzenie (wspólne zarządzanie z jednej linii komend, analogiczne do przełącznika modularnego). Dopuszcza się rozwiązanie, w którym porty stackujące dostępne są w postaci opcjonalnego modułu (niezależnego od modułów 10Gb i 40Gb opisanych w punkcie 2), który jednak musi być dostępny w chwili składania oferty i zaoferowany. Do przełącznika musi być dołączony kabel służący do połączenia w stos o długości co najmniej 50cm.  4. Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika), nie licząc magistrali stackującej  5. Wydajność: minimum 112 Mp/s  6. Tablica adresów MAC o wielkości minimum 32000 pozycji  7. Obsługa ramek Jumbo  8. Minimum 4GB pamięci stałej typu Flash, minimum 1GB pamięci RAM  9. Minimum 12MB bufora pakietów  10. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych  11. Port USB  12. Jeden modularny wewnętrzny zasilacz prądu zmiennego, slot na drugi zasilacz. Przy wykorzystaniu obydwu źródeł zasilania możliwość pracy zasilaczy w trybie redundantnym oraz możliwość wymieniany na gorąco  13. Routing IPv4 – minimum: statyczny, RIPv2, OSPF  14. Routing IPv6 – minimum: statyczny, RIPng, OSPFv3  15. Obsługa protokołu VRRP  16. Wielkość tablicy rutingu: minimum 10000 wpisów dla IPv4, 5000 wpisów dla IPv6  17. IGMPv1/v2/v3 Snooping; MLDv1/v2 Snooping, PIM Dense Mode, PIM Sparse Mode  18. Obsługa VxLAN  19. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol  20. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN  21. Funkcja Root Guard oraz BPDU protection  22. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie  23. Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping  24. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI  25. Obsługa standardu 802.1p – min. 8 kolejek na porcie  26. Funkcja mirroringu portów  27. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)  28. Funkcja autoryzacji użytkowników zgodna z 802.1x  29. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+  30. RADIUS Accounting  31. Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3  32. OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic.  33. Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP)  34. Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow.  35. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az  36. Zarządzanie poprzez port konsoli (pełne) (RS-232 i USB), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https  37. Obsługa Syslog  38. Obsługa SNTPv4 lub NTP  39. Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku  40. Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej  41. Wsparcie dla funkcji Private VLAN lub równoważnego  42. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link Detection Protocol (DLDP) lub równoważnego  43. Minimalny zakres pracy od 0°C do 45°C  44. Wysokość w szafie 19” – 1U, głębokość nie większa niż 50 cm | |
| **Wyposażenie dodatkowe** | Wraz z przełącznikiem sieciowym należy dostarczyć oraz zainstalować:   * Kompatybilne z przełącznikiem wkładki 10G SFP+ LR (na światłowód jednomodowy) – 2 sztuki/przełącznik * 2 sztuki kabli LC-LC co najmniej OS2 i długości min. 5m – 2 sztuki/przełącznik |
| **Gwarancja** | Minimum 3 letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez okres co najmniej 3 lata. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis - **na potwierdzenie złożyć** oświadczenie Wykonawcy. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. |
| **Certyfikaty** | Przełącznik LAN musi być wyprodukowany zgodnie z normą ISO 9001.  Przełącznik LAN musi posiadać deklaracje CE.  **Na potwierdzenie złożyć** kopię certyfikatu zgodności. |
|  |  |
| **UPS** | **Ilość – 15 szt.**  **Karta katalogowa - TAK** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Moc znamionowa | 1 kVA / 600 W |
| Topologia | Line Interactive |
| Typ przebiegu | sinusoida |
| Czas przełączenia | Max. 10ms |
| Napięcie wyjściowe | 230 V |
| Częstotliwość wyjściowa | 50/60Hz +/- 3 Hz |
| Napięcie wejściowe w trybie podstawowym | 180 - 287V |
| Częstotliwość wejściowa | Automatycznie wykrywana 50–60 Hz |
| Czas podtrzymania | 20 minut dla 300 W |
| Baterie | Szczelne, bezobsługowe, kwasowo-ołowiowe. |
| Czas ładowania (typowy) | 3h |
| Panel sterujący LCD | Wymagany |
| Złącze interfejsów | RJ-45 Serial, USB |
| Złącza wyjściowe | 4 x IEC 320 C19  2 x IEC Jumpers |
| Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa ,kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE  **Na potwierdzenie złożyć** | Wymagane |
| Certyfikat ISO 9001 oraz 14001 producenta zasilacza UPS  **Na potwierdzenie złożyć.** | Wymagane |
| Wymiary zasilacza UPS w szafie rack 19’’ | 2U |
| Elementy do montażu w szafie rack | Wymagane |
| Instrukcja w języku polskim lub angielskim | Wymagane |
| Zdalny monitoring | Wymagany |
| Gwarancja | Minimum 3 lata na elektronikę, minimum 2 lata na baterie |

## Firewall

|  |  |
| --- | --- |
| **Urządzenie do ochrony sieci – UTM - ilość – 1 komplet.**  **Karta katalogowa - TAK** | |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **OBSŁUGA SIECI** | * 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 * Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. * Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. * Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). * 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. * 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. * Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall’u. * Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). * 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). |
| **INTRUSION PREVENTION SYSTEM (IPS)** | * 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. * Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. * Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. * Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. * Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej. * Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. * 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. |
| **KSZTAŁTOWANIE PASMA (Traffic Shapping)** | * Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. * Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. * Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). * Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. |
| **OCHRONA ANTYWIRUSOWA** | * Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). * Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. * Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. * 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. |
| **OCHRONA ANTYSPAM** | * Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). * Ochrona antyspam ma działać w oparciu o:   + białe/czarne listy,   + DNS RBL,   + heurystyczny skaner. * 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. * Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. |
| **WIRTUALNE SIECI PRYWANTE (VPN)** | * Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). * Odpowiednio kanały VPN można budować w oparciu o:   + PPTP VPN,   + IPSec VPN,   + SSL VPN * SSL VPN musi działać w trybach Tunel i Portal. * W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN   współpracującego z oferowanym rozwiązaniem.   * Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). * Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. * Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. |
| **FILTR DOSTĘPU DO STRON WWW** | * Urządzenie ma posiadać wbudowany filtr URL. * Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. * Administrator musi mieć możliwość dodawania własnych kategorii URL. * Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. * Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. * Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:   + blokowanie dostępu do adresu URL,   + zezwolenie na dostęp do adresu URL,   + blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. * Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. * Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. * Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. * Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. * Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. * Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http. |
| **UWIERZYTELNIANIE** | * Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:   + lokalną bazę użytkowników (wewnętrzny LDAP),   + zewnętrzną bazę użytkowników (zewnętrzny LDAP),   + usługę katalogową Microsoft Active Directory. * Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. * Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:   + SSL,   + Radius,   + Kerberos. * Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. * Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta. * Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny. |
| **ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)** | * Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). * Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:   + równoważenie względem adresu źródłowego,   + równoważenie względem połączenia. * Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. * Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. * Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. * 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. * Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. * Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. * Rozwiązanie powinno wspierać technologię Link Aggregation. |
| **POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA** | * Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. * Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. * Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. * Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS * Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. * Urządzenie musi posiadać usługę DNS Proxy. |
| **ADMINISTRACJA URZĄDZENIEM** | * Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia. * Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. * Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. * Komunikacja może odbywać się na porcie innym niż https (443 TCP). * Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. * Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. * Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. * Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). * Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. * Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. * Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. |
| **RAPORTOWANIE** | * Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. * System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. * System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. * System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów. * System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. * W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. * Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy |
| **PARAMETRY SPRZĘTOWE** | * Urządzenie ma być wyposażone w dysk twardy o pojemności co najmniej 120 GB. * Liczba portów Ethernet 10/100/1000Mbps – min. 8. * Urządzenie musi pozwalać na podłączenie minimum jednej karty rozszerzeń z 8 interfejsami Ethernet 10/100/1000Mbps lub 4 światłowodowymi interfejsami 1Gbps lub 2 światłowodowymi interfejsami 10Gbps. Należy dostarczyć 2 portowe rozszerzenie 10 Gb SFP+ wraz z kompatybilnymi wkładkami. * Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. * Przepustowość Firewalla – min. 20 Gbps * Przepustowość Firewalla wraz z włączonym systemem IPS – min. 12 Gbps. * Przepustowość filtrowania Antywirusowego – min. 2,2 Gbps * Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 4 Gbps. * Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 1000 * Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 150 * Obsługa min. VLAN 512 * Liczba równoczesnych sesji - min. 1 500 000 i nie mniej niż 60 000 nowych sesji/sekundę. * Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. * Urządzenie jest nielimitowane na użytkowników. * Należy dostarczyć dwa urządzenia skonfigurowane w klastrze HA. |
| **Wymagane licencje / gwarancja** | Urządzenie ma być objęte gwarancją typu NBD tzn. w przypadku awarii podstawowego urządzenia wymiana na urządzenie zastępcze lub wymiana urządzenia na sprawne musi nastąpić na kolejny dzień roboczy od stwierdzenia awarii - **na potwierdzenie złożyć** oświadczenie Wykonawcy.  Urządzenie musi być objęte gwarancją producenta przez okres 5 lat. Wraz z urządzeniem należy dostarczyć pakiet subskrypcji na okres 5 lat od daty protokołu przekazania urządzenia. |
| **Certyfikaty** | Firewall musi być wyprodukowany zgodnie z normą ISO 9001.  Firewall musi posiadać deklaracje CE.  **Na potwierdzenie złożyć** kopię certyfikatu zgodności. |

## Przełącznik zarządzający

|  |  |  |
| --- | --- | --- |
| **Przełącznik zarządzający ilość – 1 szt.**  **Karta katalogowa - TAK** | | |
| **Wymagane minimalne parametry techniczne** | | |
| 1. Co najmniej 24 portów gigabitowych w standardzie 100/1000BaseT  2. Minimum 4 porty 10Gb SFP+. Dla zwiększenia niezawodności porty SFP+ powinny być umieszczone na module pozwalającym na ich wymianę. Dla zapewnienia przyszłej rozbudowy, musi być dostępny wymienny moduł zapewniający co najmniej jeden port 40Gb/s QSFP+ lub QSFP28  3. Przepustowość: minimum 128 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika), nie licząc magistrali stackującej  4. Wydajność: minimum 95 Mp/s  5. Tablica adresów MAC o wielkości minimum 32000 pozycji  6. Obsługa ramek Jumbo  7. Minimum 4GB pamięci stałej typu Flash, minimum 1GB pamięci RAM  8. Minimum 12MB bufora pakietów  9. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych  10. Port USB  11. Jeden modularny wewnętrzny zasilacz prądu zmiennego, slot na drugi zasilacz. Przy wykorzystaniu obydwu źródeł zasilania możliwość pracy zasilaczy w trybie redundantnym oraz możliwość wymieniany na gorąco  12. Routing IPv4 – minimum: statyczny, RIPv2, OSPF  13. Routing IPv6 – minimum: statyczny, RIPng, OSPFv3  14. Obsługa protokołu VRRP  15. Wielkość tablicy rutingu: minimum 10000 wpisów dla IPv4, 5000 wpisów dla IPv6  16. IGMPv1/v2/v3 Snooping; MLDv1/v2 Snooping, PIM Dense Mode, PIM Sparse Mode  17. Obsługa VxLAN  18. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol  19. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN  20. Funkcja Root Guard oraz BPDU protection  21. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie  22. Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping  23. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI  24. Obsługa standardu 802.1p – min. 8 kolejek na porcie  25. Funkcja mirroringu portów  26. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)  27. Funkcja autoryzacji użytkowników zgodna z 802.1x  28. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+  29. RADIUS Accounting  30. Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3  31. OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic.  32. Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP)  33. Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow.  34. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az  35. Zarządzanie poprzez port konsoli (pełne) (RS-232 i USB), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https  36. Obsługa Syslog  37. Obsługa SNTPv4 lub NTP  38. Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku  39. Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej  40. Wsparcie dla funkcji Private VLAN lub równoważnego  41. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link Detection Protocol (DLDP) lub równoważnego  42. Minimalny zakres pracy od 0°C do 45°C  43. Wysokość w szafie 19” – 1U, głębokość nie większa niż 50 cm  44. Do przełącznika należy dostarczyć dwa kompatybilne kable DAC SFP+ zgodne z 10GbE o długości min. 3m | | |
| **Gwarancja** | Minimum 3 letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez okres minimum 3 lata. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis - **na potwierdzenie złożyć** oświadczenie Wykonawcy. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. |  |
| **Certyfikaty** | Przełącznik zarządzający musi być wyprodukowany zgodnie z normą ISO 9001.  Przełącznik zarządzający musi posiadać deklaracje CE.  **Na potwierdzenie złożyć** kopię certyfikatu zgodności. |  |