Załącznik nr 1 d do OPZ Firewall duży

**Wymagania techniczne dot. Systemu Zabezpieczeń *dla lidera Projektu Urzędu Marszałkowskiego Województwa Podlaskiego*.**

**Definicje:**

* FW SZ – zapora ogniowa co najmniej typu NGFW, składająca się z minimum dwóch fizycznych zapór ogniowych pracujących w trybie niezawodnościowym, wchodząca w skład SZ.
* SZ - System Zabezpieczeń składający się z FW SZ oraz dodatkowych urządzeń i systemów wspierających ich pracę.

|  |  |
| --- | --- |
| **Opis wymagania** | **Parametry minimalne** |
| 1. Parametry fizyczne | * 1. FW SZ musi się składać z systemu połączonych, co najmniej dwóch dedykowanych, fizycznych urządzeń zabezpieczających sieć komputerową.   2. FW SZ musi być w formie appliance’u fizycznego tj. odrębnej, niezależnej platformy sprzętowej.   3. SZ musi być dedykowany przez producenta do montażu w 19” szafie RACK Zamawiającego.   4. Uszkodzenie SZ musi być raportowane na urządzeniu w formie wizualnej np. dioda, wyświetlacz LCD itp. |
| 1. Zasilacze | * 1. Każde z urządzeń wchodzących w skład SZ musi być wyposażone w minimum dwa zasilacze zapewniające redundancję zasilania w trybie hot-plug.   2. Połowa zainstalowanych zasilaczy musi zapewnić zasilanie wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości funkcjonalnych oraz wydajnościowych.   3. Zasilacze muszą pracować z siecią energetyczną Zamawiającego o parametrach AC 230V, 50Hz. |
| 1. Interfejsy | 1. Każde z urządzeń wchodzących w skład FW SZ musi być wyposażone w:    1. 16 interfejsów 10 Gbps SFP+, w tym:       * 1. 8 par wkładek światłowodowych SFP+, w każdej parze musi być jedna wkładka kompatybilna z FW SZ, a druga z Cisco Nexus 5596 Zamawiającego.         2. 8 par wkładek światłowodowych SFP+, w każdej parze musi być jedna wkładka kompatybilna z FW SZ, a druga z Cisco Nexus 5548UP Zamawiającego.       1. Jeśli urządzenie nie ma wbudowanych portów QSFP 40 Gbps, to musi mieć możliwość rozbudowy o porty QSFP 40 Gpbs,       2. 1 interfejs 1 Gbps wydzielony jako dedykowany do zarządzania out-of-band,       3. 1 port konsolowy RJ45.    2. FW SZ muszą obsługiwać agregowanie interfejsów fizycznych w obrębie pojedynczego urządzenia pracującego samodzielnie. |
| 1. Architektura systemu | * 1. Na SZ muszą składać się 2 fizyczne urządzenia typu appliance wykonujące kontrolę ruchu sieciowego.   2. Dla urządzeń appliance (FW SZ) musi występować sprzętowa separacja modułu zarządzania i modułu przetwarzania danych.   3. Dopuszcza się konfigurację, w której centralne zarządzanie, logowanie, raportowanie, archiwizacja logów i zdarzeń SZ zainstalowane jest na odrębnej platformie w postaci maszyny wirtualnej w środowisku Zamawiającego VMware – niezależnie od urządzeń appliance lub jako odrębny, wolnostojący serwer typu RACK.      1. Zamawiający przeznacza na ten cel środowisko VMware vSphere 5.5 z 1 hostem 4x CPU Intel Xeon E5-2620, 128GB RAM, 2TB HDD over 8Gbps FC.      2. Rozwiązanie musi spełniać wymogi wydajnościowe określone przez producenta oprogramowania.   4. FW SZ musi umożliwiać podział na niezależne logiczne instancje.      1. FW SZ musi umożliwiać uruchomienie minimum 6 w pełni funkcjonalnych, logicznych instancji systemu.      2. Musi istnieć możliwość rozbudowy FW SZ do osiągnięcia możliwości uruchomienia 7 logicznych instancji.   5. FW SZ musi mieć możliwość i być dedykowany przez producenta do zastąpienia obecnie pracujących fizycznych firewalli Zamawiającego:      1. 2 FW wewnętrznego ruchu sieciowego pracujących w trybie active/standby,      2. 1 FW wewnętrznego ruchu sieciowego (FW styku z siecią Internet),      3. 2 FW zewnętrznego ruchu sieciowego pracujących w trybie active/standby,      4. 1 FW zewnętrznego ruchu sieciowego (FW styku z siecią Internet).   6. Urządzenia fizyczne FW SZ muszą posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active/Standby.   7. W przypadku klastra Active/Standby wymagane jest objecie licencjami całego klastra, czyli wszystkich urządzeń fizycznych wchodzących w skład FW SZ. |
| 1. Wydajność: | * 1. Każde z urządzeń tworzących FW SZ musi posiadać następujące parametry wydajnościowe dla przetwarzanego ruchu sieciowego:      1. Całkowita wydajność urządzenia w trybie inspekcji Threat Prevention – rozumianym jako aktywna filtracja pakietów przy włączonych modułach bezpieczeństwa min. Firewall, Ochrona Antywirusowa, Ochrona Antymalware, Ochrona Antyspyware, System IPS, Kontrola Aplikacji, Filtracja Treści WWW/URL,– nie mniejsza niż 15 Gbps .      2. Maksymalna liczba obsługiwanych jednoczesnych połączeń - nie mniejsza niż 4 000 000 .      3. Maksymalna liczba obsługiwanych nawiązywanych połączeń - nie mniejsza niż 200 000 / sek. |
| 1. Tryby pracy Systemu | * 1. System musi realizować zadania kontroli i filtracji ruchu sieciowego, wykonując kontrolę na poziomie co najmniej warstw sieciowej, transportowej oraz aplikacji modelu ISO-OSI za pomocą modułów bezpieczeństwa:      1. Firewall,      2. System IPS,      3. Kontrola aplikacji,      4. Ochrona Antywirusowa,      5. Ochrona Antymalware,      6. Ochrona Antyspyware,      7. Filtracja Treści WWW/URL.   2. System musi wspierać funkcjonalności, co najmniej:      1. Realizacja połączeń VPN IPsec (Site-to-Site),      2. Dostęp zdalny użytkowników (RemoteAccess),      3. Inspekcja komunikacji szyfrowanej SSL/TLS,      4. Identyfikacja użytkowników,      5. Filtracja sieci BOTNET oraz TOR,      6. Translacja adresów,      7. Protokoły routingu,      8. Mechanizmy QoS,      9. Sieci VLAN.   3. FW SZ musi umożliwiać pracę w co najmniej 2 trybach:      1. routera (tzn. w warstwie 3 modelu OSI),      2. w trybie transparentnym.   4. Praca w trybach wymienionych powyżej musi być możliwa również w ramach podziału na pojedyncze logiczne instancje systemu. Poszczególne instancje logiczne systemu muszą pracować niezależnie od siebie, w trybie routera lub w trybie transparentnym. |
| 1. Moduł kontroli ruchu sieciowego:   Firewall | * 1. FW SZ musi mieć możliwość zabezpieczeń typu firewall zgodnie z określoną polityką tj. musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci tj. strefami bezpieczeństwa na poziomie warstwy sieciowej, transportowej oraz aplikacji modelu ISO-OSI.   2. Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP, protokoły, usługi sieciowe, użytkowników oraz logowanie ruchu sieciowego.   3. FW SZ musi zapewniać ochronę przed atakami typu DoS czy DDoS (flood protection).   4. FW SZ musi zapewniać ochronę przed skanowaniem portów.   5. FW SZ musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (GeoIP). |
| 1. Moduł kontroli ruchu sieciowego:   System IPS | * 1. FW SZ musi posiadać moduł wykrywania i blokowania ataków intruzów opartego o sygnatury, zdefiniowane wzorce ruchu sieciowego oraz parametry protokołów sieciowych.   2. Baza systemu IPS musi być regularnie aktualizowana w sposób automatyczny.   3. Musi być możliwość edytowania reguł Systemu IPS.   4. FW SZ musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów.   5. FW SZ musi generować alerty w przypadku wykrycia ataku.   6. FW SZ musi zapewniać wykrywanie i blokadę wszelkich prób nawiązywania połączenia z podejrzanymi serwerami Command & Control (Advanced Threat Prevention). |
| 1. Moduł kontroli ruchu sieciowego:   Kontrola aplikacji | * 1. FW SZ musi obsługiwać mechanizm wykrywania aplikacji w ruchu sieciowym.   2. FW SZ musi automatycznie identyfikować aplikacje bez względu na stosowane numery portów, protokoły i użyte szyfrowanie.   3. Rozpoznanie aplikacji musi odbywać się co najmniej poprzez sygnatury. |
| 1. Moduł kontroli ruchu sieciowego:   Ochrona antywirus  Ochrona antimalware  Ochrona antyspyware | * 1. FW SZ musi obsługiwać inspekcję ruchu pozwalającą na ochronę antywirusową, antimalware i antyspyware co najmniej dla protokołów: SMTP, POP3, HTTP i HTTPS oraz podstawowe rodzaje plików – minimum PDF, DOC, DOCX, XLS, XLSX, pliki wykonywalne oraz archiwa.   2. Bazy modułów antywirusowego, antimalware i antyspyware muszą być aktualizowane w sposób automatyczny.   3. System musi umożliwiać zablokowanie transferu plików w oparciu o ich rodzaj, protokół transmisji, kierunek transferu oraz zawierających złośliwy kod.   4. Musi być możliwość edytowania reguł ochrony, antimalware oraz antyspyware. |
| 1. Moduł kontroli ruchu sieciowego:   Filtracja treści WWW/URL | * 1. FW SZ musi obsługiwać mechanizm filtrowania stron WWW, adresów URL w zależności od kategorii treści stron internetowych.   2. FW SZ musi zapewnić możliwość dodania własnej kategorii.   3. Baza kategorii stron musi być aktualizowana w sposób automatyczny.   4. FW SZ powinien automatyczne odpytywać bazy producenta w trybie rzeczywistym.   5. FW SZ powinien zapewniać skanowanie plików w czasie rzeczywistym lub partiami.   6. FW SZ powinien filtrować pliki na podstawie nagłówków.   7. Administrator powinien mieć możliwość edytowania treści komunikatu i dodania logo organizacji. |
| 1. Wymagane funkcjonalności:   Realizacja połączeń VPN (site-to-site) | * 1. FW SZ musi obsługiwać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standard IPSec w konfiguracji site-to-site.   2. FW SZ musi wspierać zestawianie zabezpieczonych kryptograficznie tuneli VPN dla logicznych instancji systemu. |
| 1. Wymagane funkcjonalności:   Dostęp zdalny VPN użytkowników (client-to-site) | * 1. FW SZ musi umożliwiać tworzenie tuneli client-to-site opartych o technologię SSL oraz IPsec.   2. FW SZ umożliwia obsługę 100 użytkowników VPN jednocześnie.   3. Użytkownicy zdalni mogą autoryzować się za pomocą: RADIUS, LDAP, certyfikatów, dwu-składnikowego uwierzytelniania bądź lokalnej bazy użytkowników.   4. Klient VPN musi wspierać najnowsze systemy operacyjne: Windows, Android, iOS.   5. FW SZ musi mieć możliwość wykorzystania portalu do uwierzytelniania użytkowników tzw. Captive Portal i uwierzytelniać ich w oparciu o LDAP. |
| 1. Wymagane funkcjonalności:   Inspekcja komunikacji szyfrowanej | * 1. FW SZ musi zapewniać inspekcję komunikacji szyfrowanej HTTPS dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników przeglądających zasoby w sieci Internet) oraz ruchu przychodzącego z sieci Internet do serwerów wewnętrznych (przeglądanie stron WWW Zamawiającego).   2. FW SZ musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji Threat Prevention.   3. FW SZ musi zapewnić możliwość wykluczenia z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie co najmniej: kategoryzacji stron URL, dodania własnych wyjątków.   4. Inspekcja ruchu musi dopuszczać analizę ruchu w trybie monitorowania (bez podjęcia reakcji). |
| 1. Wymagane funkcjonalności:   Identyfikacja użytkowników | * 1. FW SZ musi transparentnie ustalać tożsamość użytkowników sieci w oparciu o Active Directory.   2. Polityka kontroli dostępu (FW SZ) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet, gdy użytkownik zmieni lokalizację i adres IP.   3. FW SZ nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów lub użytkowników w sieci wewnętrznej. |
| 1. Wymagane funkcjonalności:   Translacja adresów | * 1. FW SZ musi wykonywać statyczną i dynamiczną translację adresów NAT. |
| 1. Wymagane funkcjonalności:   Protokoły routingu | * 1. FW SZ musi zapewniać obsługę routingu statycznego.   2. FW SZ musi zapewniać obsługę protokołów routingu dynamicznego BGP, i OSPF.   3. FW SZ musi zapewniać obsługę IGMP. |
| 1. Wymagane funkcjonalności:   Mechanizmy QoS | * 1. FW SZ musi zapewniać klasyfikację ważności ruchu pakietów na bazie:      1. Protokołu sieciowego,      2. Źródłowego i docelowego adresu IP,      3. Numeru portu TCP lub UDP,      4. Ustawienia pasma maksymalnego ruchu sieciowego (QoS),      5. Tworzenie limitów ilości danych dla użytkowników w kierunku upload, download, |
| 1. Wymagane funkcjonalności:   Sieci VLAN | * 1. FW SZ musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q.   2. FW SZ musi obsługiwać co najmniej 1024 znaczników VLAN.   3. FW SZ musi obsługiwać ruch miedzy podsieciami VLAN. |
| 1. Zarządzanie: | * 1. Zarządzanie urządzeniami systemu musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW.   2. Interfejs SZ musi być w języku polskim lub angielskim.   3. Dostęp do SZ i zarządzanie z sieci muszą być zabezpieczone kryptograficznie poprzez szyfrowanie komunikacji.   4. SZ musi pozwalać na zdefiniowanie wielu administratorów o różnych poziomach uprawnień.   5. Komunikacja FW SZ z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS, LDAP.   6. FW SZ musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory.   7. FW SZ musi umożliwiać autoryzację dwustopniową za pomocą hasła jednorazowego (OTP) lub tokena (U2F).   8. Konsola zarządzająca, logująca i raportująca FW SZ musi umożliwiać centralne budowanie i dystrybucję polityk bezpieczeństwa, aktualizację oprogramowania i sygnatur oraz funkcje audytu i backupu konfiguracji.   9. FW SZ musi mieć wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego oraz do serwera FTP.   10. FW SZ powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w zdefiniowanych odstępach czasowych.   11. FW SZ musi mieć możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer, z możliwością wykorzystania ich do budowy polityk bezpieczeństwa.   12. FW SZ powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności.   13. FW SZ musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.   14. FW SZ powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu zarządzania. Liczba takich prób oraz czas blokady muszą być definiowane przez administratora.   15. FW SZ musi posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich. |
| 1. Logowanie i raportowanie: | * 1. SZ musi mieć możliwość korelowania zbieranych informacji oraz budowania raportów na ich podstawie.   2. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.   3. Konsola zarządzająca musi umożliwiać generowanie raportów i przesyłania ich na wskazany adres e-mail.   4. Logowanie działań administratora.   5. SZ musi zapewniać monitorowanie w czasie rzeczywistym stanu SZ (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych, połączenia sieciowe, czas trwania połączeń sieciowych, liczba przesłanych danych, lista ‘top talkers’, lista ‘top attackers’, lista ‘top blocked connections’). Podobne statystyki powinny być dostępne również dla danych historycznych w ramach webowego interfejsu graficznego urządzenia. Użyteczna przestrzeń na przechowywanie danych nie mniejsza niż 15TB.   6. FW SZ musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP.   7. FW SZ musi mieć wsparcie dla protokołów:      1. SNMP v1 lub v2 lub v3.      2. Netflow lub jFlow lub NetStream lub cflowd lub IPFIX lub NSEL lub sFlow.   8. SZ musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych celem długoterminowego przechowywania danych. |
| 1. Gwarancja: | * 1. Wykonawca musi zapewnić gwarancję SZ przez okres 36 miesięcy od dnia podpisania protokołu odbioru.   2. W okresie zaoferowanej gwarancji na SZ musi zostać zapewnione:      1. serwis wszystkich elementów sprzętowych SZ łącznie z wymianą urządzeń na nowe w przypadku awarii w trybie 5x8 NBD on-site.      2. serwis wszystkich elementów programowych SZ w trybie 5x8 NBD.      3. W sytuacji uszkodzenia dysku twardego w jakimkolwiek elemencie SZ i konieczności jego wymiany gwarancyjnej - dysk twardy pozostaje u Zamawiającego.      4. SZ musi mieć zaimplementowany RAID jako nadmiarowość dysków.      5. Obsługa zgłoszeń serwisowych przez inżynierów Producenta.      6. Dostęp do pomocy technicznej producenta.      7. Pomoc techniczna z SZ musi być dostępna w Polsce i świadczona w języku polskim lub angielskim.      8. Dostęp do najnowszej wersji oprogramowania dla urządzenia.      9. Licencje i subskrypcje na wszystkie wymagane funkcjonalności na okres wykupionej gwarancji.      10. SZ nie może posiadać ograniczeń licencyjnych dotyczących wydajności urządzenia.      11. SZ musi mieć pełne pokrycie licencyjne funkcjonalności w okresie gwarancyjnym.      12. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu, a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.      13. Urządzenia wchodzące w skład SZ muszą być fabrycznie nowe, aktualnie obecne w linii produktowej producenta i jednocześnie nie mogą znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.      14. Urządzenia SZ muszą pochodzić z autoryzowanego kanału sprzedażowego producenta. |
| 1. Reputacja | * 1. FW SZ muszą być oparte o urządzenia o uznanej na rynku pozycji i musiały znajdować się w kwadracie „Leaders” raportu Gartnera pt.      1. „Magic Quadrant for Network Firewalls – As of November 2020” lub      2. „Magic Quadrant for Network Firewalls – As of July 2019” lub      3. „Magic Quadrant for Enterprise Network Firewalls – As of September 2018”.   2. Potwierdzenie znajdowania się producenta FW SZ w kwadracie raportu Gartnera musi być dostarczone w dokumentacji. |
| 1. Dodatkowe wymagania | * 1. Wszelkie wymagane komponenty (kable, listwy, wkładki, interfejsy, karty, moduły, szyny, licencje, patchcordy itp.) niezbędne do uruchomienia SZ i podłączenia do infrastruktury Zamawiającego muszą być dostarczone w ramach postępowania i kompatybilne z infrastrukturą Zamawiającego. |
| 1. Szkolenia: | * 1. W ramach realizacji zamówienia Wykonawca zapewni uczestnictwo w autoryzowanych przez producenta szkoleniach w zakresie podstawowej i zaawansowanej konfiguracji SZ dla trzech pracowników Zamawiającego w terminie zaakceptowanym przez Zamawiającego.   2. W przypadku, gdy Wykonawca przeprowadzi szkolenie poza miejscem realizacji umowy tj. poza Białymstokiem, musi zapewnić dojazd do miejsca szkolenia, zakwaterowanie, wyżywienie oraz powrót.   3. Szkolenia z SZ muszą zostać przeprowadzone po zawarciu Umowy, ale przed jej zakończeniem.   4. Szkolenia z SZ muszą być dostępne w Polsce i świadczone w języku polskim. |
| 1. Wymagania dotyczące instalacji, konfiguracji i integracji urządzeń. | W ramach realizacji zamówienia Wykonawca zobowiązany jest do Wykonania następujących prac instalacyjnych i konfiguracyjnych Systemu:   * 1. Wykonanie i przedstawienie do akceptacji Zamawiającego projektu wdrożenia FW SZ.   2. Montaż urządzeń w szafie RACK wskazanej przez Zamawiającego. Montaż urządzeń FW SZ będzie polegał na rozłożeniu FW SZ w dwóch budynkach Zamawiającego, oddalonych od siebie w odległości ok. 2 km i połączonych ze sobą ciemnymi włóknami światłowodowymi.   3. Wykonanie okablowania oraz podłączenie do istniejącej infrastruktury Zamawiającego.   4. Konfiguracja klastra niezawodnościowego pracującego w trybie active-passive.   5. Konfiguracja podstawowych ustawień systemowych: serwer czasu, DNS, adres interfejsu zarządzającego, konto administracyjne.   6. Wykonanie projektu technicznego w zakresie wyodrębnienia i skonfigurowania logicznych instancji firewall. Po akceptacji Zamawiającego, przeniesienie konfiguracji fizycznych firewalli do logicznych instancji firewall.   7. Odwzorowanie konfiguracji obecnie używanych urządzeń bezpieczeństwa w zakresie:      1. Konfiguracji interfejsów sieciowych oraz tras routingu w poszczególnych logicznych instancjach.      2. Obiektów wraz z przypisanymi im adresami IP w poszczególnych logicznych instancjach.      3. Polityk bezpieczeństwa firewall (L4) oraz konfiguracji NAT w poszczególnych logicznych instancjach.      4. Bazy użytkowników dla autoryzacji połączeń zdalnych.      5. Identyfikacji użytkowników poprzez domenę Active Directory.   8. Aktywacja wymaganych licencji oraz konfiguracja pobierania aktualizacji baz dla modułów bezpieczeństwa.   9. Konfiguracja modułów bezpieczeństwa dla analizy i ochrony ruchu przychodzącego z sieci Internet do zasobów wewnętrznych.      1. Blokowanie ruchu z adresów IP na podstawie reputacji i geolokalizacji.      2. Blokowanie ruchu sieciowego na podstawie sygnatur IPS.   10. Konfiguracja modułów bezpieczeństwa dla analizy i ochrony ruchu wychodzącego z sieci wewnętrznej.       1. Blokowanie niedozwolonych treści WWW.       2. Blokowanie niedozwolonych aplikacji i protokołów sieciowych.       3. Skanowanie ruchu w celu zapobieganiu złośliwemu oprogramowaniu (antymalware, antywirus).   11. Konfiguracja raportów z ruchu sieciowego użytkowników.   12. Konfiguracja raportów dotyczących ruchu przychodzącego z sieci Internet.   13. Konfiguracja bramy umożliwiającej dostęp VPN dla użytkowników zdalnych.   14. Konfiguracja automatycznej kopii zapasowej SZ według określonego harmonogramu. |
| 1. Dokumentacja | * 1. Dokumentacja powykonawcza musi odzwierciedlać stan faktyczny SZ w momencie zakończenia prac wdrożeniowych. Musi zawierać:      1. Opis architektury połączeń fizycznych.      2. Opis architektury topologii logicznej sieci.      3. Opis uruchomionych modułów kontroli ruchu sieciowego wraz ze zdefiniowanymi politykami.      4. Opis skonfigurowanych wymaganych funkcjonalności podczas wdrożenia.      5. Opis wdrożonego systemu zarzadzania oraz raportowania zdarzeń wraz ze zdefiniowanymi raportami.   2. Dokumentacja musi być wykonana w formie minimum elektronicznej. |