Załącznik nr 1 do SIWZ

Sprawa numer: 34/ST/SPIS/PN/2019

Opis Przedmiotu Zamówienia – zmieniony 11-09-2019

 **Przedmiotem zamówienia jest dostawa systemu zabezpieczeń typu firewall wraz z wdrożeniem i usługami wsparcia technicznego w Centrum Przetwarzania Danych w GUS.**

1. **Ogólny opis przedmiotu zamówienia**

**Przedmiot zamówienia obejmuje następujące Zadania:**

**Zadanie I: Zakup i dostawa urządzeń wraz z oprogramowaniem, stacji zarządzającej oraz okablowania i modułów służących do wdrożenia systemu zabezpieczeń typu firewall**

**A1. Wymagania ogólne dla urządzeń służących do wdrożenia systemu zabezpieczeń typu firewall**

1. Sprzęt dostarczony w ramach realizacji zamówienia będzie fabrycznie nowy, wyprodukowany nie wcześniej niż na 6 miesięcy od daty dostarczenia urządzeń.
2. Sprzęt dostarczony w ramach realizacji zamówienia będzie pochodzić z autoryzowanego kanału sprzedaży producentów zaoferowanych urządzeń.
3. Sprzęt dostarczony w ramach realizacji zamówienia nie był w dniu składania ofert przeznaczony przez producenta do wycofania z produkcji.
4. Wraz z dostawą urządzeń Wykonawca dostarczy dokument wystawiony przez producenta sprzętu potwierdzający, że oprogramowanie w nim zawarte jest licencjonowane na Zamawiającego.
5. Wraz z dostawą urządzeń Wykonawca dostarczy dokument potwierdzający zarejestrowanie kontraktu i dokument potwierdzający bezpośredni dostęp Zamawiającego do bazy wiedzy, oprogramowania, zgłoszeń serwisowych i  dokumentacji, w ramach stron WWW producenta, dostępnych po zalogowaniu na indywidualne konto Zamawiającego.
6. Wraz z dostawą urządzeń Wykonawca dostarczy szczegółową dokumentację techniczną producenta oferowanych urządzeń, potwierdzającą spełnianie wymagań technicznych urządzeń będących przedmiotem zamówienia.

**A2. Wymagania dla urządzeń typu appliance (2 sztuki)**

1. Urządzenie typu firewall muszą być wyposażony w następujące interfejsy sieciowe:
	1. Minimum 4 porty Ethernet 1G,
	2. Minimum 16 portów 10G SFP+,
	3. Minimum 4 porty 40/100G QSFP28,

W celu osiągnięcia odpowiedniej ilości portów 10Gb dopuszcza się użycie spliterów, splitery nie mogą zmniejszyć dostępnej ilości portów 40 G

1. Urządzenie typu firewall musi być wyposażone w co najmniej jeden port konsoli,
2. Urządzenie typu firewall musi być wyposażony w co najmniej jeden port zarządzający Out-of-Band 10/100/1000 Mbps,
3. Urządzenie typu firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN,
4. Urządzenie typu firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 64 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji,
5. Urządzenie typu firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 23 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS),
6. Urządzenie typu firewall musi obsługiwać nie mniej niż 32 000 000 jednoczesnych połączeń i umożliwiać zestawianie nie mniej niż 340 000 połączeń na sekundę,
7. Urządzenie typu firewall musi umożliwiać realizację połączeń VPN z przepustowością nie mniejszą niż 22 Gbps,
8. Urządzenie typu firewall musi umożliwiać zdefiniowanie minimum 64 000 polityk bezpieczeństwa oraz minimum 8 000 polityk NAT,
9. Urządzenie typu firewall musi posiadać wbudowane w obudowę co najmniej 2 redundantne zasilacze umożliwiające podłączenie urządzenia do sieci energetycznej 230V,

**B. Wymagania dla systemu zabezpieczeń typu firewall (1 kpl.)**

1. System zabezpieczeń typu firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance).
2. Sprzęt i oprogramowanie musi być dostarczone i wspierane przez jednego producenta.
3. System zabezpieczeń typu firewall musi umożliwiać działanie w następujących trybach pracy:
	1. routera (tzn. w warstwie 3 modelu OSI),
	2. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych)
4. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.
5. System zabezpieczeń typu firewall musi umożliwiać pracę w modelu wysokiej dostępności poprzez pracę dwóch urządzeń w modelu failover. Wymagana jest praca firewall’i w modelach Active-Standby i Active-Active.
6. System zabezpieczeń typu firewall w dostarczanej konfiguracji musi obsługiwać nie mniej niż 25 wirtualnych firewalli / systemów / domen / kontekstów.
7. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych polityk bezpieczeństwa obejmujących:
	1. System IPS
	2. System ochrony antymalware / antyspyware
	3. System ochrony antywirus
	4. koncentratorów VPN dla zdalnego dostępu IPsec site-to-site
8. Musi posiadać możliwość licencyjnej rozbudowy do obsługi minimum 125 wirtualnych firewalli
9. System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
10. Polityka zabezpieczeń firewall musi uwzględniać:
	1. strefy bezpieczeństwa,
	2. adresy IP klientów i serwerów,
	3. protokoły i usługi sieciowe,
	4. aplikacje,
	5. kategorie URL,
	6. użytkowników aplikacji – poprzez integrację z Active Directory
	7. rejestrowanie zdarzeń i alarmowanie
11. zarządzanie pasmem w sieci w oparciu o priorytet, pasmo gwarantowane, pasmo maksymalne oraz oznaczenia DiffSery,
12. System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń musi blokować wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
13. System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania.
14. Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
15. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.
16. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać pole lub pola gdzie definiowane są aplikacje i gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Kontrola aplikacji musi być przeprowadzana w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych niż firewall (np. w IPS lub innym module UTM)
17. System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.
18. System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia wsparcia producenta.
19. System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, , doc, docx, ppt, pptx, xls, xlsx, rar, zip, exe, gzip, hta, pdf, tar. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
20. System zabezpieczeń firewall musi zapewniać integrację z usługami:
	1. Active Directory,
	2. LDAP
21. System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
22. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
23. System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
24. System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Wykorzystanie funkcji VPN (IPSec) nie wymaga zakupu dodatkowych licencji. System zabezpieczeń firewall musi obsługiwać minimum 12 000 tuneli Ipsec site-to-site
25. System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
26. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
27. System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
28. System zabezpieczeń firewall musi posiadać moduł wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
29. System zabezpieczeń firewall musi posiadać moduł antymalware lub antyspyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
30. System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
31. System zabezpieczeń firewall musi posiadać możliwość rozbudowy o moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. Subskrypcje nie są wymagane w ofercie.
32. System zabezpieczeń firewall musi zapewniać możliwość rozbudowy funkcjonalności o przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. Subskrypcje zapewniające taką możliwość nie są wymagane w ofercie.
33. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
34. System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 1 TB lub równoważny zewnętrzny system dyskowy dostarczony przez Wykonawcę.
35. System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
36. System zabezpieczeń firewall musi pozwalać na korelowanie zbieranych informacji oraz budowanie raportów na ich podstawie. Zbierane dane powinny zawierać informacje co
najmniej o:
	1. ruchu sieciowym,
	2. aplikacjach,
	3. zagrożeniach
	4. filtrowaniu stron www.
37. System zabezpieczeń firewall musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni. Do tego celu można wykorzystać zewnętrzny system do zbierania logów.
38. System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.

**C. Wymagania dotyczące oprogramowania (1kpl.)**

1. Zamawiający wymaga dostawy 2 urządzeń opisanych powyżej oraz stacji roboczej do zarządzania z:
	1. 5-letnim serwisem obejmującym naprawę sprzętu, usuwanie usterek w oprogramowaniu systemowym oraz aktualizacje tego oprogramowania przez okres 5 lat.
	2. 5-letnią subskrypcją rozpoznawania nowych aplikacji,
	3. 5-letnią subskrypcją na antywirus
	4. 5-letnią subskrypcją na antyspyware (lub antymalware jeżeli dla urządzenia nie jest dostępna licencja AS)
	5. 5-letnią subskrypcją na IPS
	6. 5-letnia subskrypcja oraz gwarancja liczone będą od daty podpisania odbioru ostatniego protokołu.
2. Zamawiający wymaga przez okres gwarancyjny możliwości rozbudowy o następujące subskrypcje/licencje, jednakże nie wymaga ich dostawy w ramach niniejszego postępowania:
3. Subskrypcja na URL Filtering
4. Subskrypcja umożliwiająca przesyłanie plików do chmurowego / lokalnego sandboxa

**D. Wymagania dotyczące stacji zarządzającej do systemu zabezpieczeń typu firewall (1 sztuka) oraz monitory (2 sztuki)**

1. procesor 4 rdzeniowy
2. 8 GB pamięci RAM
3. karta graficzna obsługująca DirectX 11 oraz mieć co najmniej 1 GB pamięci własnej
4. dysk twardy SSD o pojemności 2 T
5. 2 monitory min 28 cali
6. system operacyjny WIN 10

**E. 3. Moduły (32 sztuki), kable (2 sztuki) oraz patchcord (8 sztuk) – 1kpl.**

1. 2 sztuki kabli AOC 40G 10m
2. 8 sztuk patchcordów MPO12 OM4 25m
3. 8 sztuk modułów QSFP28 100G-SR4 MPO12
4. 12 sztuk modułów SFP+ 10G-SR
5. 12 sztuk modułów SFP+ 10G-LR

Moduły i kable AOC (Active Optic Cable) muszą być zapewnione przez Wykonawcę. Dopuszcza się zaoferowanie zamienników wkładek, gdy producent zapewnia użycie takich, które nie spowodują utraty gwarancji Wykonawcy w stosunku do Zamawiającego oraz nie spowodują utraty gwarancji producenta udzielonej Wykonawcy.

**F. Procedura odbioru sprzętu**

Przy odbiorze sprzętu Zamawiający zastrzega sobie prawo przeprowadzenia testów odbioru jakościowego (testy wydajnościowe urządzeń). Celem przeprowadzenia procedury testowej jest weryfikacja zgodności urządzeń i oprogramowania z wymaganiami zawartymi w OPZ/SIWZ. Wszelkie testy będą przeprowadzane przez Wykonawcę na jego koszt. Wszystkie testy odbywać się będą w obecności przedstawicieli Zamawiającego.

**F.1. Urządzenie testujące**

Testy muszą zostać wykonane dedykowanym urządzeniem umożliwiającym wygenerowanie ruchu o wymaganej charakterystyce i wolumenie, a także umożliwiające generowanie próbek na podstawie pliku zawierającego podsłuchany lub skopiowany rzeczywisty ruch sieciowy.

*Wymagania co do urządzenia testującego:*

1. Urządzenie generujące ruch musi mieć możliwość testowania parametrów wydajnościowych urządzeń sieciowych takich jak przełączniki, routery, firewalle.
2. Urządzenie generujące ruch musi symulować pracę zarówno klienta jak i serwera dla testowanych parametrów wydajnościowych (odbiornik, nadajnik).
3. Urządzenie musi mieć możliwość wygenerowania ruchu o wolumenie większym, niż wymagany przez Zamawiającego maksymalny wolumen dla oferowanego urządzenia.
4. Urządzenie powinno posiadać predefiniowane przez producenta próbki symulujące ruch generowany przez różnego rodzaju aplikacje, grupy aplikacji oraz protokoły np. Windows Update, Facebook, Google services, Microsoft Exchange, MS SQL, http oraz https itp.
5. W przypadku gdy urządzenie nie posiada predefiniowanych próbek Zamawiający dopuszcza wykorzystanie próbki dostarczonej przez Wykonawcę z zastrzeżeniem, że próbka ta zostanie szczegółowo opisana (procentowa ilość poszczególnych aplikacji i protokołów w próbce);
6. Opis próbki oraz sama próbka zostanie przekazana Zamawiającemu razem z raportem końcowym przeprowadzonych testów.
7. Urządzenie musi mieć możliwość wygenerowania ruchu dla wybranej grupy aplikacji, o określonym wolumenie i określonej liczbie symulowanych użytkowników.
8. Po zakończeniu testów urządzenie musi wygenerować raport z wykonanego testu zawierający informację o:
9. wolumenie wygenerowanego ruchu;
10. procentowym udziale poszczególnych aplikacji w wolumenie generowanego ruchu i w przypadku braku takiej funkcjonalności Zamawiający dopuszcza Opis próbki dostarczony przez Wykonawcę o którym mowa w pkt. 4.b;
11. ilości błędów w generowanych ruchu;
12. liczbie wygenerowanych sesji TCP.

**F.2. Procedura przeprowadzenia testów wydajnościowych (akceptacyjnych):**

1. Wykonawca w terminie wykonania testów musi przekazać Zamawiającemu kompletne środowisko testowe, w szczególności sprzęt i oprogramowanie składające się na oferowany system oraz wszelkie inne elementy konieczne do przeprowadzenia testów.
2. Testy odbędą się w siedzibie Zamawiającego w terminie do 3 dni od dostarczenia oferowanych urządzeń.
3. Czas trwania testów nie może być dłuższy niż 6 godzin zegarowych.
4. Wykonawca będzie miał obowiązek przygotowania środowiska testowego i konfiguracji urządzeń w miejscu testów dwie godziny zegarowe przed rozpoczęciem testów. Czas ten może zostać wykorzystany przez Wykonawcę do przygotowania się do testów.
5. W celu realizacji testów (podczas przygotowania oraz przeprowadzenia) Wykonawca może korzystać tylko i wyłącznie z dostarczonego przez siebie środowiska testowego. Wyjątek stanowią urządzenia prezentacyjne takie jak monitor czy projektor.
6. Podczas testów Wykonawca zobowiązany jest do udzielenia Zamawiającemu wszelkich wyjaśnień umożliwiających zbadanie, czy oferowane rozwiązanie posiada wymagane w OPZ funkcjonalności.
7. W przypadku wystąpienia podczas testów problemów lub błędów Wykonawca ma obowiązek podjęcia czynności zmierzających do ich usunięcia, w szczególności może dokonywać niezbędnych z jego punktu widzenia modyfikacji środowiska testowego , w ramach czasu przewidzianego na testy, tj. 6 godzin zegarowych. Zadania, które nie zostały wykonane w zadanym czasie zostaną uznane za niewykonane a test za niezaliczony.
8. Z przeprowadzonych testów Zamawiający sporządzi protokół.
9. Testy przeprowadzone zostaną w języku polskim, Zamawiający dopuszcza angielskojęzyczne raporty generowane z urządzeń pomiarowych.

**F.3. Przeprowadzone testy:**

*Funkcjonalne/* Wydajnościowe

1. Test rozpoznania aplikacji – podczas testu urządzenie powinno zidentyfikować aplikację generującą ruch. Potwierdzeniem zaliczenia testu będzie informacja w logu urządzenia z prawidłowo rozpoznaną aplikacją.
2. Test modułu AV – podczas testu nastąpi próba przesłania zainfekowanego pliku (Zamawiający zaleca wykorzystanie próbki ze strony www.eicar.org) za pomocą protokołu http. Następnie test zostanie powtórzony z przesłaniem tego samego pliku poddanego kompresji zip bez wprowadzenia hasła. Potwierdzeniem zaliczenia testu będzie informacja w logu urządzenia o zablokowanym ruchu zarówno dla pliku oryginalnego jak i skompresowanego.
3. Test IPS – test polega na wygenerowaniu dowolnego zdarzenia rozpoznanego przez moduł IPS. Potwierdzeniem zaliczenia testu będzie informacja w logu urządzenia.
4. Wydajność ruchu full-duplex nie mniej niż 23 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS). Zamawiający dopuszcza tolerancję błędu pomiarowego środowiska testowego wynoszącą +/- 5% tj. 1,15 Gbit/s. Potwierdzeniem zaliczenia testu będzie raport z generatora ruchu zawierający informację o przepływności ruchu nie mniejszej niż 21,85 Gbit/s.
5. Możliwość obsłużenia nie mniej niż 32 000 000 jednoczesnych połączeń. Zamawiający dopuszcza tolerancję błędu pomiarowego środowiska testowego wynoszącą +/- 5% tj. 1 600 000 połączeń. Potwierdzeniem zaliczenia testu będzie z raport z generatora ruchu zawierający informację o liczbie jednoczesnych sesji/połączeń nie mniejszej niż 30 400 000. Możliwość zestawienia nie mniej niż 340 000 połączeń na sekundę. Zamawiający dopuszcza tolerancję błędu pomiarowego środowiska testowego wynoszącą +/- 5% tj. 17 000 połączeń. Potwierdzeniem zaliczenia testu będzie raport z generatora ruchu zawierający informację o maksymalnej liczbie nowych sesji/połączeń na sekundę nie mniejszej niż 323 000.

**Zadanie II Wdrożenie dostarczonych elementów systemu zabezpieczeń typu firewall.**

**A1. Wymagania ogólne dotyczące wdrożenia systemu zabezpieczeń typu firewall**

1. Analiza przedwdrożeniowa obejmująca weryfikację logicznej konfiguracji sieci Zamawiającego niezbędna do przygotowania projektu technicznego; analiza będzie obejmować spotkania robocze na których Zamawiający przedstawi infrastrukturę sieciową, systemową oraz aplikacyjną w zakresie niezbędnym do realizacji przedmiotu zamówienia.
2. Opracowanie projektu technicznego opisującego szczegółową konfigurację urządzeń
i oprogramowania niezbędnego do realizacji wdrożenia.
3. Instalacja sprzętu wraz z okablowaniem w serwerowni określonej
w zaakceptowanym przez Zamawiającego projekcie technicznym, Wykonawca będzie zobowiązany do posprzątania miejsc instalacji urządzeń w siedzibie Zamawiającego, oraz pozostawienia tych miejsc w stanie nie gorszym od zastanego przed przystąpieniem do prac.
4. Opracowanie scenariuszy testowych potwierdzających zgodność dostarczonych rozwiązań z SIWZ, zatwierdzeniu scenariuszy przez Zamawiającego i przeprowadzenie testów zgodnie ze scenariuszami.
5. Opracowanie i przeprowadzenie raportu z testów.
6. Wykonanie dokumentacji powykonawczej opisującej szczegółową konfigurację wdrożonego rozwiązania.

**A2. Opis i warunki wdrożenia systemu zabezpieczeń typu firewall**

 Wdrożenie będzie polegało na instalacji dostarczonych urządzeń, konfiguracji, zabezpieczeniu oraz uruchomieniu nowego systemu zabezpieczeń typu firewall dla Centrum Przetwarzania Danych oraz integracji z usługą katalogową Active Directory.

W ramach wdrożenia Wykonawca zrealizuje następujące prace:

1. Analizę przedwdrożeniową obejmującą weryfikację logicznej konfiguracji sieci Zamawiającego niezbędną do przygotowania projektu technicznego; analiza będzie obejmować spotkania robocze na których Zamawiający przedstawi infrastrukturę sieciową, systemową oraz aplikacyjną w zakresie niezbędnym do realizacji przedmiotu zamówienia.
2. Opracuje projekt techniczny opisujący szczegółową konfigurację urządzeń i oprogramowania niezbędnego do realizacji wdrożenia;

Projekt techniczny podlegał będzie procedurze odbioru, na następujących warunkach:

1. Wykonawca przekaże Zamawiającemu drogą elektroniczną do akceptacji projekt techniczny w terminie nie dłuższym niż 14 dni od dnia zawarcia umowy;
2. Zamawiający w terminie nie dłuższym niż 5 dni od dnia dostarczenia przez Wykonawcę projektu technicznego, poinformuje Wykonawcę o jego akceptacji lub konieczności wprowadzenia zmian;
3. Wszystkie uwagi do projektu technicznego zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 3 dni od dnia ich otrzymania;
4. Zamawiający w terminie 3 dni od dnia powtórnego dostarczenia przez Wykonawcę poprawionego projektu technicznego, poinformuje Wykonawcę o jego akceptacji lub konieczności wprowadzenia zmian;

Zamawiający zastrzega sobie prawo do trzykrotnego zgłoszenia zmian w projekcie technicznym;

Komunikacja pomiędzy Zamawiającym a Wykonawcą w zakresie akceptacji projektu technicznego, następować będzie drogą mailową na adresy Wykonawcy i Zamawiającego wskazane w umowie;

1. Zatwierdzony projekt techniczny zostanie przekazany Zamawiającemu najpóźniej w dniu podpisania Protokołu odbioru projektu na pendrive w wersji edytowalnej i PDF oraz wydruk w 3 egzemplarzach,
	1. Potwierdzeniem odbioru projektu technicznego będzie Protokół odbioru projektu, którego wzór stanowi załącznik do Umowy, podpisany z wynikiem pozytywnym.
2. Wykonawca wykona instalację oraz konfigurację urządzeń typu firewall wraz z okablowaniem w serwerowni, określonej w zaakceptowanym przez Zamawiającego projekcie technicznym. Po wykonaniu prac związanych z instalacją sprzętu, Wykonawca będzie zobowiązany do pozostawienia miejsc, w których prowadzone były prace, w stanie nie gorszym od zastanego przed przystąpieniem do prac.
3. Wykonawca opracuje scenariusze testowe potwierdzające zgodność dostarczonych rozwiązań z SIWZ, Zamawiający zatwierdzi scenariusze, Wykonawca przeprowadzi testy zgodnie ze scenariuszami,
4. Wykonawca przeprowadzi testy oraz opracuje raporty z testów,
5. Wykonawca wykona dokumentację powykonawczą opisującą szczegółowo konfigurację wdrożonego rozwiązania;

Dokumentacja powykonawcza podlegała będzie procedurze odbioru, na następujących warunkach:

* 1. Wykonawca przekaże Zamawiającemu drogą elektroniczną do akceptacji dokumentację powykonawczą, nie później niż na 15 dni przez terminem zakończenia realizacji umowy;
	2. Zamawiający w terminie nie dłuższym niż 3 dni od dnia dostarczenia przez Wykonawcę dokumentacji powykonawczej, poinformuje Wykonawcę o jej akceptacji lub konieczności wprowadzenia zmian;
	3. Wszystkie uwagi do dokumentacji powykonawczej zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 2 dni od dnia ich otrzymania;
	4. Zamawiający w terminie 2 dni od dnia powtórnego dostarczenia przez Wykonawcę poprawionej dokumentacji powykonawczej, poinformuje Wykonawcę o jej akceptacji lub konieczności wprowadzenia zmian;
	5. Zamawiający zastrzega sobie prawo do dwukrotnego zgłoszenia zmian w dokumentacji powykonawczej;
	6. Komunikacja pomiędzy Zamawiającym a Wykonawcą w zakresie akceptacji dokumentacji powykonawczej, następować będzie drogą mailową na adresy Wykonawcy i Zamawiającego wskazane w umowie;
	7. Zatwierdzona dokumentacja powykonawcza zostanie przekazana Zamawiającemu najpóźniej w dniu podpisania Protokołu odbioru Zadania II, na pendrive w wersji edytowalnej i PDF oraz wydruk w 3 egzemplarzach,
	8. Potwierdzeniem odbioru zaakceptowanej przez Zamawiającego Dokumentacji powykonawczej będzie Protokół odbioru Dokumentacji, którego wzór stanowi załącznik do umowy, podpisany z wynikiem pozytywnym.

**B. Warunki gwarancji dla systemu zabezpieczeń typu firewall.**

1. Zamawiający wymaga, aby na wszystkie dostarczone w ramach realizacji zamówienia urządzenia
i oprogramowanie Wykonawca udzieli co najmniej 60 miesięcznej bezpłatnej gwarancji, której termin liczony będzie od dnia podpisania z wynikiem pozytywnym Końcowego protokołu odbioru. Ostateczny okres udzielonej przez Wykonawcę gwarancji określony zostanie na podstawie deklaracji złożonej w ofercie, z zastrzeżeniem, że nie będzie on krótszy niż 60 miesięcy.
2. Serwis w ramach udzielonej gwarancji, świadczony będzie w języku polskim, w siedzibie Zamawiającego.
3. Warunki udzielonej gwarancji będą zgodne z wymaganiami Zamawiającego, z zastrzeżeniem, że nie mogą być gorsze niż warunki gwarancji producenta(ów) urządzeń i oprogramowania.
4. Dopuszcza się kontakt mailowy i telefoniczny, pod warunkiem, że nie wpływa on na obniżenie jakości świadczenia usług.
5. Świadczenie usług gwarancyjnych odbywać się będzie w dni robocze od poniedziałku do piątku,
z wyłączeniem dni ustawowo wolnych od pracy w godzinach od 8:00 do 17:00
6. Zamawiający nie będzie ponosił żadnych kosztów związanych z pełnieniem gwarancji przez Wykonawcę (kosztów dojazdu, kosztów noclegu itp.).
7. Wykonawca gwarantuje maksymalny czas reakcji na zgłaszane problemy nie dłuższy niż 24 godziny.
8. W ramach gwarancji Wykonawca zapewni: cykliczne (dwa razy w roku) przeglądy systemu bezpieczeństwa będącego przedmiotem postępowania w siedzibie Zamawiającego zakończone raportem dotyczącym wykrytych problemów i nieprawidłowości oraz wskazaniem sposobu ich rozwiązania.
9. W okresie gwarancji Wykonawca musi zapewnić dostęp do bazy wiedzy, aktualnej wersji, aktualnych sygnatur oraz krytycznych poprawek producentów komponentów związanych z bezpieczeństwem i stabilnością działania systemu w całym czasie trwania gwarancji.
10. W ramach gwarancji Wykonawca zapewni wsparcie techniczne inżyniera Wykonawcy w sytuacji zagrażającej stabilnej pracy systemu;
11. W ramach gwarancji Wykonawca zapewni wsparcie techniczne inżyniera Wykonawcy w czasie wykonywania przez Zamawiającego planowanych instalacji poprawek, uaktualnień lub nowych wersji oprogramowania;
12. W ramach gwarancji Wykonawca zapewni wsparcie techniczne inżyniera Wykonawcy, w tym zdalną diagnozę, w przypadku wystąpienia nieprzewidzianych problemów z oprogramowaniem;
13. W ramach gwarancji Wykonawca zapewni konsultacje w zakresie eksploatacji, konfiguracji oraz funkcjonalności oprogramowania;
14. W czasie trwania gwarancji Wykonawca zapewni rozwiązywanie bieżących problemów technicznych związanych z funkcjonowaniem systemu oraz zapewni rozwiązywanie problemów bieżącego zarządzania;
15. Wady systemu objęte gwarancją klasyfikowane są jako: awarie, błędy i usterki:
16. Awaria: Uszkodzenie jednego lub więcej elementów Systemu (w tym sprzętu), ograniczające wydajność lub funkcjonalność systemu lub uniemożliwiająca Zamawiającemu korzystanie z systemu zgodnie z jego specyfikacją techniczną/instrukcją użytkowania.
17. Błąd: Błąd systemu, którego skutkiem jest zmiana funkcjonalności jednego lub więcej modułów systemu w sposób uniemożliwiający wykorzystanie go zgodnie z przeznaczeniem lub zakłócenie powodujące brak możliwości normalnego funkcjonowania jednego lub więcej istotnych procesów w przedsiębiorstwie Zamawiającego.
18. Usterka: Sytuacja, która nie jest przyczyną całkowitego zatrzymania pracy systemu lub zmiany funkcjonalności jednego lub więcej modułów systemu lub niedostępności systemu,
a skutkujący problemami w normalnej pracy systemu. W szczególności usterką będzie m.in.:

zakłócenie pracy systemu mogące mieć wpływ na funkcjonalności rozwiązania, natomiast nieograniczające zdolności operacyjnych rozwiązania,

spadek wydajności systemu (wydłużenie czasu odpowiedzi).

1. Czas reakcji Wykonawcy od momentu przyjęcia zgłoszenia w ramach gwarancji do podjęcia działań naprawczych wynosi maksymalnie:

dla awarii - 4 godziny,

dla błędów - 12 godzin,

dla usterki - 48 godzin.

1. Wady systemu objęte gwarancją mogą być zgłaszane wyłącznie przez osoby upoważnione ze strony Zamawiającego, drogą pisemną - pocztą elektroniczną, faksem lub telefonicznie.
2. Usunięcie wady systemu polega na przywróceniu pełnej poprawności działania systemu. Usunięcie wady w okresie trwania gwarancji następuje na wyłączny koszt i  ryzyko Wykonawcy. Wszystkie koszty związane z usunięciem wady w szczególności koszty gwarancji, transportu i naprawy obciążają Wykonawcę.
3. Czas na usunięcie zgłoszonych wad systemu od chwili podjęcia działań naprawczych wynosi maksymalnie:

 dla awarii - 48 godzin,

 dla błędów - 72 godzin,

 dla usterki -168 godzin.

1. W przypadku niewykonania naprawy gwarancyjnej w miejscu i w terminie, o którym mowa powyżej, Wykonawca zobowiązuje się dostarczyć na czas naprawy takie samo urządzenie wolne od wad i zapewni jego prawidłowe działanie. Ostateczny termin usunięcia usterki uszkodzonego urządzenia nie może być dłuższy niż 30 dni od dnia zgłoszenia jego wady lub usterki.
2. Wykonawca zobowiązuje się do wymiany urządzenia na sprawne w przypadku, gdy po trzech naprawach jakichkolwiek elementów urządzenia, będzie ono wykazywało nadal wady w działaniu.
3. W przypadku nie wywiązania się Wykonawcy ze swoich zobowiązań Zamawiający może dokonać tych czynności we własnym zakresie i kosztami obciążyć Wykonawcę.
4. Wykonawca pokrywa wszelkie koszty związane z naprawami gwarancyjnymi.
5. Zamawiający zobowiązany jest do udzielenia szczegółowych informacji o zewnętrznych objawach wady lub usterki oraz czasie jej wystąpienia.
6. Zamawiający ma prawo dokonywania rozbudowy sprzętu, zgodnie z dokumentacją techniczną, a także prawo do przemieszczenia zainstalowanego sprzętu bez utraty gwarancji.

**Zadanie III - Szkolenie dla Administratorów**

**A. Opis wymagań szkolenia dla Administratorów**

1. Wykonawca przeprowadzi szkolenie obejmujące zakresem. instalację, konfigurację, zarządzanie, troubleshooting (rozwiazywanie problemów) dostarczonego systemu bezpieczeństwa firewall przeprowadzone zgodnie z następującymi wymaganiami:
2. ilość uczestników – 4 osoby,
3. czas trwania szkolenia: 5 dni roboczych (40 godzin, 1 godzina to 45 minut),
4. szkolenie zostanie przeprowadzone na środowisku testowym poza siedzibą
Zamawiającego,
5. program szkolenia musi zawierać całość zagadnień obejmujących instalacje,
konfiguracje, administrowanie systemem oraz zapewnić umiejętności i wiedzę
niezbędną w tym zakresie,
6. wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku
polskim lub angielskim, w formie papierowej i elektronicznej w formacie PDF,
7. wszyscy uczestnicy szkolenia otrzymają zaświadczenia potwierdzające ukończenie
szkolenia.
8. Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz wyżywieniem
i zakwaterowaniem wykładowców, którzy będą prowadzili szkolenie.
9. Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz wyżywieniem
i zakwaterowaniem uczestników.
10. Wykonawca zapewni każdemu uczestnikowi szkolenia samodzielne stanowisko pracy, napoje w czasie przerw oraz posiłek (obiad).
11. Na co najmniej 14 dni przed rozpoczęciem szkoleń Wykonawca przedstawi Zamawiającemu do akceptacji – harmonogram szkoleń przygotowany w porozumieniu z Zamawiającym obejmujący:
12. programy szkoleń zawierające szczegółowe informacje o zakresie tematycznym i rozkładzie zajęć dla poszczególnych szkoleń,
13. metodę i formę prowadzenia szkoleń,
14. listę wykładowców i informacje o wykładowcach którzy przeprowadzą poszczególne
szkolenia.
15. Wykonawca zobowiązany będzie do przeprowadzenia szkolenia zgodnie
z zatwierdzonym przez Zamawiającego szczegółowym zakresem tematycznym i harmonogramem szkoleń.
16. Potwierdzeniem prawidłowo przeprowadzonego szkolenia jest pozytywna ocena minimum 3 w arkuszu indywidualnej oceny szkolenia.
17. Wykonawca w ramach prowadzonego szkolenia zobowiązany jest przekazać Zamawiającemu:
18. materiały szkoleniowe,
19. ankiety oceny szkoleń,
20. listy obecności.
21. Listę wydanych Zaświadczeń i komplet imiennych zaświadczeń dla wszystkich
uczestników, którzy ukończą szkolenie pod warunkiem uczestnictwa w pełnym
wymiarze zajęć.