**numer sprawy: OR-D-III.272.122.2023.AR**

**załącznik nr 2 do specyfikacji warunków zamówienia (SWZ)**

**Opis Przedmiotu Zamówienia**

na *„****Modernizację infrastruktury sieciowej Węzła Regionalnego*** ***w celu podniesienia bezpieczeństwa infrastruktury i systemów zainstalowanych w Węźle Regionalnym****”* w ramach realizacji projektu pn. *„****Regionalne partnerstwo samorządów Mazowsza dla aktywizacji społeczeństwa informacyjnego w zakresie e-administracji i geoinformacji****”* objętego Regionalnym Programem Operacyjnym Województwa Mazowieckiego na lata 2014-2020.

**Spis treści**

[1. Słownik pojęć i skrótów 3](#_Toc147917189)

[2. Informacje ogólne 3](#_Toc147917190)

[3. Przedmiot zamówienia 4](#_Toc147917191)

[4. Wymagania szczegółowe realizacji Przedmiotu zamówienia 4](#_Toc147917192)

[4.1 Opis realizacji Przedmiotu zamówienia 5](#_Toc147917193)

[4.2 Modernizacja infrastruktury sieciowej 6](#_Toc147917194)

[4.3 Dokumentacja powykonawcza 20](#_Toc147917195)

[5. Termin realizacji Przedmiotu zamówienia 21](#_Toc147917196)

[6. Kontekst prawny 21](#_Toc147917197)

[7. Gwarancja i Wsparcie techniczne 22](#_Toc147917198)

[8. Zobowiązania Wykonawcy 23](#_Toc147917199)

[9. Zobowiązania Zamawiającego 25](#_Toc147917200)

[10. Warunki weryfikacji i odbioru produktów Przedmiotu zamówienia 25](#_Toc147917201)

[10.1 Weryfikacja i odbiór dokumentu 25](#_Toc147917202)

[10.2 Weryfikacja i odbiór modernizacji infrastruktury sieciowej 26](#_Toc147917203)

[11. Warunki weryfikacji i odbioru Przedmiotu zamówienia 26](#_Toc147917204)

[12. Załączniki 27](#_Toc147917205)

**Spis tabel**

[Tabela 1. Słownik pojęć i skrótów. 3](#_Toc147400650)

[Tabela 2. Wymagania dla nowych urządzeń sieciowych. 11](#_Toc147400651)

[Tabela 3. Wymaganie dla zaawansowanego mechanizmy autentykacji użytkowników. 15](#_Toc147400652)

[Tabela 4. Wymagania dla zaawansowanego mechanizmu zbierania logów. 17](#_Toc147400653)

[Tabela 5. Wymagania dla zaawansowanego mechanizmu zarządzania dostępem do infrastruktury sieciowej. 19](#_Toc147400654)

# Słownik pojęć i skrótów

1. Pojęcia i sformułowania pisane w OPZ wielką literą mają następujące znaczenie:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Pojęcie lub skrót** | **Definicja** |
|  | DCGiK | Departament Cyfryzacji, Geodezji i Kartografii. |
|  | Dzień roboczy | Każdy dzień od poniedziałku do piątku z wyłączeniem sobót oraz dni ustawowo wolnych od pracy w Rzeczypospolitej Polskiej. |
|  | Godzina robocza | Okres trwający godzinę zegarową (60 minut) w ramach Godzin pracy Zamawiającego. |
|  | Godziny pracy Zamawiającego | Od 8:00 do 16:00, od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy w Rzeczypospolitej Polskiej. |
|  | Gwarancja | Świadczenie przez Wykonawcę gwarancji na produkty Przedmiotu zamówienia w zakresie i na zasadach określonych w Rozdziale 7 „Gwarancja i Wsparcie techniczne”. |
|  | OPZ | Opis Przedmiotu Zamówienia. |
|  | Przedmiot zamówienia | Zamówienie publiczne, którego przedmiot w sposób szczegółowy został opisany w niniejszym OPZ. |
|  | Strony | Zamawiający i Wykonawca. |
|  | Umowa | Umowa, wraz z załącznikami, zawarta pomiędzy Stronami na realizację Przedmiotu zamówienia, opisanego w sposób szczegółowy w niniejszym OPZ. |
|  | UMWM | Urząd Marszałkowski Województwa Mazowieckiego w Warszawie. |
|  | Wsparcie techniczne | Świadczenie przez Wykonawcę wsparcia technicznego na produkty Przedmiotu zamówienia w zakresie i na zasadach określonych w Rozdziale 7 „Gwarancja i Wsparcie techniczne”. |
|  | Wykonawca | Podmiot, wyłoniony w trybie zamówienia publicznego, który zawrze z Zamawiającym Umowę na realizację Przedmiotu zamówienia. |
|  | Zamawiający | Województwo Mazowieckie. |

Tabela 1. Słownik pojęć i skrótów.

1. W OPZ każde odesłanie do:
2. OPZ oznacza odesłanie do OPZ wraz ze wszystkimi załącznikami;
3. załącznika oznacza odesłanie do załącznika OPZ;
4. aktu prawnego oznacza odesłanie do tego aktu prawnego z uwzględnieniem wszelkich jego zmian oraz wydanych na jego podstawie aktów wykonawczych.
5. Rozdziały, ustępy, punkty, litery oraz tiret należy interpretować zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 29 lutego 2016 r. w sprawie „Zasad techniki prawodawczej” (Dz. U. 2016 r., poz. 283).
6. Nagłówki w OPZ zostały zamieszczone jedynie dla większej przejrzystości tekstu i nie mają wpływu na jego wykładnię.

# Informacje ogólne

1. Projekt pn. „*Regionalne partnerstwo samorządów Mazowsza dla aktywizacji społeczeństwa informacyjnego w zakresie e-administracji i geoinformacji*” (Projekt ASI) jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020, Priorytet II „*Wzrost e-potencjału Mazowsza*”, działanie 2.1 „*E-usługi*”.
2. Na treść założeń i celów Projektu ASI miały wpływ doświadczenia Zamawiającego z wcześniej zrealizowanych projektów, a także dokumenty programowe Samorządu Województwa Mazowieckiego, w szczególności dokument pn. „*Strategia Rozwoju Województwa Mazowieckiego do roku 2030*” oraz Inteligentne specjalizacje Mazowsza, czyli obszary o największych możliwościach rozwojowych, które zostały zidentyfikowane na podstawie diagnozy potencjału naukowego, gospodarczego oraz społecznego i które wskazują między innymi jako technologie wiodące, technologie informacyjno-komunikacyjne.
3. Celem strategicznym Projektu ASI jest wsparcie inteligentnego, zrównoważonego rozwoju zwiększającego spójność społeczną i terytorialną przy wykorzystaniu potencjału mazowieckiego rynku pracy, przez rozwój konkurencyjnej gospodarki regionu opartej na innowacyjności. Realizacja tego celu odbywa się poprzez rozwój e-usług dla obywateli i przedsiębiorców oraz zwiększanie dostępu do technologii informacyjno-komunikacyjnych.
4. Do podstawowych celów Projektu ASI należy m.in.:
5. uruchomienie elektronicznych usług na 3 i 4 poziomie dojrzałości oraz usług o których mowa w ustawie z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej (Dz. U. z 2018 r. poz. 1472 z późn. zm.);
6. zapewnienie interoperacyjności publicznych systemów teleinformatycznych poprzez opracowanie i wdrożenie nowych rozwiązań informatycznych z zakresu elektronicznej administracji oraz geoinformacji i cyfryzacji baz danych, niezbędna w celu osiągnięcia elektronicznej realizacji usług na 4 poziomie dojrzałości, w tym przez urządzenia mobilne, skierowanych do obywateli i przedsiębiorców oraz stworzenia warunków dla ich niezakłóconego, zharmonizowanego działania;
7. podniesienie sprawności urzędów w zakresie świadczenia elektronicznych usług;
8. ułatwienie warunków działania przedsiębiorcom, poprawa jakości życia obywateli poprzez rozwinięcie możliwości załatwiania spraw drogą elektroniczną oraz wspomaganie usprawniania funkcjonowania administracji samorządowej.

# Przedmiot zamówienia

1. Przedmiotem zamówienia ma na celu wykonanie modernizacji infrastruktury sieciowej Węzła Regionalnego Zamawiającego poprzez dostawę, instalacje oraz konfigurację urządzeń sieciowych wraz z zapewnieniem Gwarancji i Wsparcia technicznego.
2. Przedmiot zamówienia obejmuje:
3. opracowanie opisu realizacji Przedmiotu zamówienia, realizowane zgodnie z wymaganiami określonymi w Rozdziale 4.1 „Opis realizacji Przedmiotu zamówienia”;
4. modernizację infrastruktury sieciowej, w tym instalację oraz konfigurację urządzeń sieciowych, realizowaną zgodnie z wymaganiami określonymi w Rozdziele 4.2 „Modernizacja infrastruktury sieciowej”;
5. opracowanie dokumentacji powykonawczej, realizowane zgodnie z wymaganiami określonymi w Rozdziale 4.3 „Dokumentacja powykonawcza”;
6. świadczenie Gwarancji i Wsparcia technicznego, realizowane zgodnie z wymaganiami określonymi w Rozdziale 7 „Gwarancja i Wsparcie techniczne”.
7. Przedmiot zamówienia należy realizować:
8. z zachowaniem terminów realizacji Przedmiotu zamówienia, określonych w Rozdziale 5 „Termin realizacji Przedmiotu zamówienia”;
9. zgodnie z przepisami prawa polskiego i europejskiego, określonymi w Rozdziale 6 „Kontekst prawny”;
10. z uwzględnieniem zobowiązań Wykonawcy, określonych w Rozdziale 8 „Zobowiązania Wykonawcy”;
11. z uwzględnieniem zobowiązań Zamawiającego, określonych w Rozdziale 9 „Zobowiązania Zamawiającego”.
12. Produkty Przedmiotu zamówienia będą podlegały procedurze weryfikacji i odbioru na zasadach określonych w Rozdziale 10 „Warunki weryfikacji i odbioru produktów Przedmiotu zamówienia”.
13. Przedmiot zamówienia będzie podlegał procedurze weryfikacji i odbioru na zasadach określonych w Rozdziale 11 „Warunki weryfikacji i odbioru Przedmiotu zamówienia”.
14. Wszystkie Załączniki, wymienione w Rozdziale 12 „Załączniki”.

# Wymagania szczegółowe realizacji Przedmiotu zamówienia

1. Wykonawca w ramach realizacji niniejszego Przedmiotu zamówienia będzie odpowiedzialny za wykonanie modernizacji infrastruktury sieciowej Zamawiającego, w tym dostawę, instalacje oraz konfigurację urządzeń sieciowych oraz zapewnienie 48 miesięcznego okresu Gwarancji i Wsparcia technicznego.
2. Infrastruktura sieciowa, o której mowa w ust. 1, zlokalizowana jest w jednej z lokalizacji DCGiK na terenie m.st. Warszawy. Wyżej wymieniona Infrastruktura jest administrowana przez DCGiK.
3. Modernizacją infrastruktury sieciowej będą objęte posiadane przez Zamawiającego dwa urządzenia Fortigate 501E pracujące w klastrze (z aktywnym wsparciem producenta do 17 lipca 2026 roku), w tym:
4. FortiCare Support - Premium;
5. Firmware & General Updates;
6. Intrusion Prevention;
7. AntiVirus;
8. Web Filtering
9. Email Filtering;
10. Outbreak Prevention;
11. FortiSandbox Cloud.
12. Wykonawca zobowiązany jest do ustalenia z Zamawiającym szczegółowego zakresu modernizacji infrastruktury sieciowej.
13. Szczegółowy zakres modernizacji infrastruktury sieciowej Zamawiającego, o której mowa w ust. 1, Wykonawca uzgodni z Zamawiającym w ramach opracowania opisu realizacji, o którym mowa w Rozdziale 4.1 „Opis realizacji Przedmiotu zamówienia”**.**
14. Faktyczny zakres zrealizowanych prac związanych z modernizacją infrastruktury sieciowej Wykonawca przedstawi w dokumentacji powykonawczej, o której mowa w Rozdziale 4.3 „Dokumentacja powykonawcza”.
15. Wykonawca w celu uzyskania dostępu do infrastruktury sieciowej Zamawiającego będzie zobowiązany do złożenia stosownych oświadczeń dostępu do infrastruktury teleinformatycznej, których wzór zostanie Wykonawcy przekazany przez Zamawiającego na wniosek Wykonawcy po podpisaniu Umowy.
16. Wykonawca musi posiadać autoryzację producenta w zakresie sprzedaży oferowanych, w ramach niniejszego Przedmiotu zamówienia, rozwiązań – w celu potwierdzenia tego faktu Wykonawca przedłożyć Zamawiającemu oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski.

## Opis realizacji Przedmiotu zamówienia

1. Wykonawca, w ramach opracowania opisu realizacji Przedmiotu zamówienia, o którym mowa w ust. 2 pkt 1 w Rozdziale 3 „Przedmiot zamówienia” opracuje i przekaże Zamawiającemu dokument opisujący sposób realizacji Przedmiotu zamówienia.
2. Opis realizacji Przedmiotu zamówienia, o którym mowa w ust. 1, Wykonawca opracuje w postaci Dokumentu pn. „**Opis realizacji”**.
3. Dokument, o którym mowa w ust. 2, należy opracować z zachowaniem:
4. wymagań Zamawiającego przedstawionych w niniejszym OPZ;
5. wyjaśnień Zamawiającego do niniejszego OPZ, które Wykonawca jest zobowiązany zebrać na etapie realizacji prac;
6. uzgodnień z Zamawiającym.
7. Dokument, o którym mowa w ust. 2, będzie podlegał akceptacji przez Zamawiającego. W ramach opracowania dokumentu Wykonawca zobowiązany jest do uzgodnienia z Zamawiającym szczegółowej struktury dokumentu.
8. Uzgodnienia, o których mowa w ust. 4, będą przeprowadzone pomiędzy Stronami na spotkaniu roboczym w siedzibie Zamawiającego. Spotkanie odbędzie się na wniosek Wykonawcy, w terminie uzgodnionym z Zamawiającym.
9. **Opis realizacji**, o którym mowa w ust. 2, musi zawierać co najmniej:
10. spis treści;
11. wprowadzenie;
12. słownik pojęć i skrótów;
13. harmonogram prac;
14. koncepcję architektury logicznej i technicznej;
15. decyzje i założenia projektowo-architektoniczne;
16. opis proponowanej technologii realizacji;
17. opis procedur instalacyjnych i konfiguracyjnych (w tym przeniesienia dotychczasowej konfiguracji);
18. opis konfiguracji urządzeń sieciowych;
19. opis wydajności i pojemności;
20. opis skalowalności;
21. plan testów wraz ze scenariuszami testowymi;
22. bezpieczeństwo i ochrona danych:
23. opis mechanizmów utrzymania sprawności działania,
24. opis mechanizmów zapewniających bezpieczeństwo,
25. opis mechanizmów równoważenia obciążenia,
26. opis mechanizmów redundancji,
27. opis mechanizmów backupu danych,
28. opis systemu zabezpieczeń;
29. opis zakresu odpowiedzialności Zamawiającego;
30. opis sposobu postępowania w sytuacjach awaryjnych i nadzwyczajnych oraz ścieżkę eskalacji problemów lub zagadnień.
31. **Opis realizacji**, o którym mowa w ust. 2, musi w sposób jednoznaczny identyfikować sposób implementacji wszystkich wymagań funkcjonalnych i niefunkcjonalnych opisanych w sposób szczegółowy w niniejszym OPZ.
32. Dokument będzie podlegał bezpłatnej aktualizacji przez Wykonawcę w trakcie realizacji Przedmiotu zamówienia.
33. Wykonawca zobowiązany jest pisemnie poinformować Zamawiającego, o konieczności dokonania aktualizacji dokumentu, o którym mowa w ust. 2, oraz wykonania aktualizacji w terminie **2 Dni roboczych** od dokonania zgłoszenia.
34. Aktualizacja dokumentu, o której mowa w ust. 8, może zostać również zainicjowana na wniosek Zamawiającego. W takiej sytuacji Wykonawca wykona aktualizację dokumentu w terminie, o którym mowa w ust. 9.
35. Poprzez aktualizację dokumentu należy rozumieć utworzenie kolejnej nowych i aktualnej wersji dokumentu.
36. Weryfikacja i odbiór dokumentu, o którym mowa w ust. 2, będzie przeprowadzona zgodnie z procedurą weryfikacji i odbioru dokumentu określoną w Rozdziale 10.1 „Weryfikacja i odbiór dokumentu”.

## Modernizacja infrastruktury sieciowej

* 1. Wykonawca, w ramach modernizacji infrastruktury sieciowej, o której mowa w ust. 2 pkt 2 w Rozdziale 3 „Przedmiot zamówienia”, dostarczy Zamawiającemu nowe elementy infrastruktury sieciowej wraz z wykonaniem niezbędnej instalacji oraz konfiguracji.
	2. Wykonawca przystąpi do modernizacji infrastruktury sieciowej po akceptacji przez Zamawiającego, opracowanego przez Wykonawcę, opisu realizacji Przedmiotu zamówienia, o którym mowa w Rozdziale 4.1 „Opis realizacji Przedmiotu zamówienia”.
	3. Zakres prac realizowanych w ramach modernizacji infrastruktury sieciowej obejmuje m.in.:
1. dostarczenie nowych urządzeń sieciowych UTM;
2. instalacji nowych urządzeń sieciowych UTM w szafach serwerowych Zamawiającego;
3. konfiguracji nowych urządzeń sieciowy UTM;
4. przeniesienie konfiguracji z obecnie wykorzystywanych urządzeń sieciowych UTM, o których mowa w ust. 3 w Rozdziale 4 „Wymagania szczegółowe realizacji Przedmiotu zamówienia”, do dostarczonych nowych urządzenia UTM;
5. przeprowadzenie testów zmodernizowanej infrastruktury sieciowej.
	1. W wyniku przeprowadzonej modernizacji infrastruktury sieciowej Zamawiający powinien dysponować systemem składającym się z następujących elementów:
6. dwa nowe urządzenia sieciowe pracujące w klastrze, spełniające wymagania określone w ust. 5;
7. 5 letni dostęp do definicji zagrożeń (od listopada 2023 roku), w tym m.in.: kontrola aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych), analiza typu Sandbox, antyspam, web filtering, bazy reputacyjne adresów IP/domen;
8. 5 letni okres gwarancji (od listopada 2023 roku) dla urządzeń sieciowych UTM z serwisem 24h/7dni i wymianą uszkodzonego urządzenia w następnym Dniu roboczym wraz z możliwością pozostawienia uszkodzonych dysków u Zamawiającego;
9. zaawansowany mechanizm zbierania logów, spełniający wymagania określone w ust. 6;
10. zaawansowany mechanizm autentykacji użytkowników, spełniający wymagania określone w ust. 7;
11. zaawansowany mechanizm zarządzania dostępem do infrastruktury sieciowej, spełniający wymagania określone w ust. 8.
	1. Nowe urządzenia sieciowe muszą spełniać wszystkie wymienione poniżej wymagania:

| **Lp.** | **Rodzaj wymagania** | **Opis wymagania** |
| --- | --- | --- |
|  | Ogólne | Wsparcie protokołów IPv4 oraz IPv6, w zakresie:1. Firewall;
2. ochrony w warstwie aplikacji;
3. protokołów routingu dynamicznego.
 |
|  | Możliwość pracy w następujących trybach:* + 1. router z funkcją NAT;
		2. transparentny;
		3. monitorowanie na porcie SPAN.
 |
|  | Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji w zakresie:1. Routingu;
2. Firewall’a;
3. IPSec VPN;
4. Antywirus;
5. IPS.
 |
|  | Możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji. |
|  | Możliwość łączenia w klaster Active-Active lub Active-Passive dla funkcji:1. Firewall;
2. IPSec;
3. kontrola aplikacji;
4. IPS.
 |
|  | Monitorowanie i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |
|  | Możliwość statycznej agregacji linków w oparciu o protokół LACP. |
|  | Możliwość tworzenia interfejsów redundantnych. |
|  | Możliwość dostępu, przez okres 48 miesięcy, do aktualnych baz funkcji ochronnych producenta i serwisów, w zakresie:1. kontrola aplikacji;
2. IPS;
3. Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android);
4. analiza typu Sandbox;
5. Antyspam;
6. Web Filtering;
7. bazy reputacyjne adresów IP/domen.
 |
|  | Interfejsy | Minimalna liczbą gniazd (każde urządzenie osobno):1. 16x Gigabit Ethernet (RJ45);
2. 8x Gigabit Ethernet (SFP);
3. 4x 10 Gigabit Ethernet (SFP+);
4. 4x 25 Gigabit Ethernet (SFP28/10GE SFP+/GE SFP).
 |
|  | Minimalna liczb gniazd do zarządzania (każde urządzenie osobno):1. 2x Gigabit Ethernet (RJ45).
 |
|  | Wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalację oprogramowania z klucza USB. |
|  | Możliwość zdefiniowania min. 200 interfejsów wirtualnych. |
|  | Możliwość definiowania interfejsów wirtualnych jako VLAN’y w standardzie 802.1Q. |
|  | WAN | Możliwość obsługi min. trzech łącz WAN. |
|  | Mechanizm statycznego lub dynamicznego podziału obciążenia pomiędzy łączami. |
|  | Monitorowanie stanu połączeń WAN. |
|  | Zasilanie | Zasilanie AC 230V. |
|  | Dysk  | Lokalna przestrzeń dyskową o łącznej pojemności min. 480GB. |
|  | Routing | Urządzenie musi zapewniać obsługę następujących rodzajów routingu:1. Routingu statycznego;
2. Policy Based Routingu.
 |
|  | Obsługa dynamicznego routingu w oparciu o następujące protokoły:1. RIPv2;
2. OSPF;
3. BGP;
4. PIM.
 |
|  | VPN | Możliwość konfiguracji połączeń typu IPSec VPN. |
|  | IPSec VPN musi zapewniać:1. wsparcie dla IKE v1;
2. wsparcie dla IKE v2;
3. obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode (GCM);
4. obsługa protokołu Diffie-Hellman grup 19 i 20;
5. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE;
6. tworzenie połączeń typu Site-to-Site oraz Client-to-Site;
7. monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności;
8. możliwość wyboru tunelu przez protokoły:
9. dynamicznego routingu (np. OSPF),
10. routingu statycznego;
11. obsługa mechanizmów:
12. IPSec NAT Traversal,
13. DPD,
14. Xauth;
15. mechanizm „Split tunneling” dla połączeń Client-to-Site.
 |
|  | Możliwość konfiguracji połączeń typu SSL VPN. |
|  | Połączenia SSL VPN muszą zapewniać następujące tryby pracy:1. Portal;
2. Tunnel.
 |
|  | Dla trybu Portal dostęp do chronionych zasobów musi być realizowany za pośrednictwem przeglądarki za pośrednictwem strony komunikacyjnej działającej w oparciu o HTML 5.0. |
|  | Dla trybu Tunnel musi być możliwość włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. |
|  | Monitoring stanu realizowanych połączeń VPN. |
|  | Firewall | Firewall klasy Stateful Inspection. |
|  | Firewall musi uwzględniać:1. adresy IP;
2. użytkowników;
3. protokoły;
4. usługi sieciowe;
5. aplikacje lub zbiory aplikacji;
6. reakcje zabezpieczeń;
7. rejestrowanie zdarzeń.
 |
|  | Możliwość synchronizacji sesji firewall. |
|  | Musi zostać zapewniona translacja adresów NAT, w tym: 1. źródłowego i docelowego;
2. PAT;
3. jeden do jeden;
4. jeden do wielu;

oraz dedykowany ALG (Application Level Gateway) dla protokołu SIP. |
|  | Możliwość tworzenia wydzielonych stref bezpieczeństwa, w tym:1. DMZ;
2. LAN;
3. WAN.
 |
|  | Funkcje firewall muszą posiadać certyfikację EAL4.  |
|  | Wydajność | Przepustowość Firewall: min. 8 mln jednoczesnych połączeń oraz 550 000 nowych połączeń na sekundę. |
|  | Minimalna przepustowość Stateful Firewall:1. 137 Gbps dla pakietów 512 B;
2. 70 Gbps dla pakietów 64 B.
 |
|  | Minimalna przepustowość Firewall (z włączoną funkcją kontroli aplikacji): 32 Gbps. |
|  | Minimalna wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 - SHA256: 55 Gbps. |
|  | Minimalna wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach IPS) dla ruchu Enterprise Traffic Mix: 10 Gbps. |
|  | Minimalna wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami IPS, Application Control oraz Antywirus: 10 Gbps. |
|  | Minimalna wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http: 9 Gbps. |
|  | Bezpieczeństwo | Możliwość kontroli na poziomie dostępu.  |
|  | Możliwość kontrola na poziomie aplikacji.  |
|  | Możliwość zapewnienia poufność transmisji danych – szyfrowanie połączenia IPSec VPN oraz SSL VPN. |
|  | Możliwość ochrony przed malware, w tym dla protokołów:1. SMTP;
2. POP3;
3. IMAP;
4. HTTP;
5. HTTPS;
6. FTP.
 |
|  | Możliwość ochrony przed atakami – Intrusion Prevention System. |
|  | Możliwość kontroli stron WWW. |
|  | Możliwość kontroli zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. |
|  | Możliwość zarządzania pasmem – QoS oraz Traffic shaping. |
|  | Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). |
|  | Możliwość dwuskładnikowego uwierzytelniania z wykorzystaniem tokenów sprzętowych lub programowych na potrzeby dwuskładnikowego uwierzytelnienia administratorów oraz w ramach połączeń VPN typu Client-to-Site.  |
|  | Minimalna liczba dostarczonych i możliwych do wykorzystania tokenów: 100. |
|  | Możliwość analizy ruchu szyfrowanego protokołem SSL. |
|  | Możliwość analizy ruchu szyfrowanego protokołem SSH. |
|  | Uwierzytelnianie użytkowników | Możliwość weryfikacji tożsamości użytkowników za pomocą:1. haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia;
2. haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP;
3. haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych;

przy jednoczesnym zastosowaniu uwierzytelniania dwuskładnikowego. |
|  | Możliwość budowy architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów, w tym: RADIUS lub API. |
|  | Zarządzanie | Możliwość zarządzania lokalnego z wykorzystaniem protokołów:1. HTTPS;
2. SSH;

a także możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. |
|  | Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. |
|  | Możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. |
|  | Możliwość współpracy z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. |
|  | Możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. |
|  | Dostępne wbudowane narzędzia diagnostyczne, w tym:1. ping;
2. traceroute;
3. podgląd pakietów;
4. monitorowanie procesowania sesji;
5. stan sesji firewall.
 |
|  | Zarządzanie pasmem | Możliwość zarządzania pasmem poprzez określenie maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. |
|  | Możliwość określania pasma dla poszczególnych aplikacji. |
|  | Możliwość zarządzania pasmem dla wybranych kategorii URL. |
|  | Logowanie | Możliwość logowania i raportowania do aplikacji udostępnianej w chmurze. |
|  | Możliwość przekazywania danych, w zakresie:1. zaakceptowanego ruchu;
2. blokowanego ruchu;
3. aktywności administratorów;
4. zużyciu zasobów;
5. stanie pracy systemu.
 |
|  | Możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. |
|  | Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. |
|  | Musi istnieć możliwość logowania do serwera SYSLOG. |
|  | Ochrona przed atakami | Ochrona IPS musi opierać się na:1. analizie sygnaturowej;
2. analizie anomalii w protokołach sieciowych.
 |
|  | Możliwość ochrany przed atakami na aplikacje pracujące na niestandardowych portach. |
|  | Baza sygnatur ataków musi zawierać min. 5 000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |
|  | Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. |
|  | Możliwość wykrywania anomalii protokołów i ruchu sieciowego. |
|  | Możliwość ochrony przed atakami typu DoS oraz DDoS. |
|  | Możliwość ochrony aplikacji Web’owych na poziomie sygnaturowym, w tym:1. CSS;
2. SQL Injecton;
3. Trojany;
4. Exploity;
5. Roboty.
 |
|  | Możliwość ochrony aplikacji Web’owych poprzez kontrolowanie:1. długości nagłówka;
2. ilości parametrów URL;
3. Cookies.
 |
|  | Możliwość wykrywania i blokowania komunikacji Command & Controldo sieci botnet. |
|  | Kontrola Antywirusowa | Możliwość skanowania ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach. |
|  | Możliwość skanowania archiwów, w tym:1. ZIP;
2. RAR.
 |
|  | Dostęp do sygnatur ochrony dla urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). |
|  | Kontrola aplikacji | Możliwość kontroli ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. |
|  | Możliwość kontroli aplikacji chmurowych, w tym:1. Facebook;
2. Google Docs;
3. Dropbox;

pod względem wykonywanych czynności, w tym:1. pobieranie;
2. wysyłanie plików.
 |
|  | Baza kontroli aplikacji musi zawierać:1. minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora;
2. kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa:
3. proxy,
4. P2P.
 |
|  | Administrator musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.  |
|  | Kontrola WWW | Moduł filtrowania musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.  |
|  | W ramach modułu filtrowania muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, w tym:1. malware (lub inne będące źródłem złośliwego oprogramowania);
2. phishing;
3. spam;
4. Dynamic DNS;
5. proxy avoidance.
 |
|  | Moduł filtrowania musi dostarczać kategorii stron zabronionych prawem tzw. etykiety hazard. |
|  | Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków tzw. białe i czarne listy dla adresów URL. |
|  | Możliwość zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii.  |
|  | Możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. |
|  | Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. |

Tabela 2. Wymagania dla nowych urządzeń sieciowych.

* 1. Zaawansowany mechanizm autentykacji użytkowników musi spełniać wszystkie wymienione poniżej wymagania:

| **Lp.** | **Rodzaj wymagania** | **Opis wymagania** |
| --- | --- | --- |
|  | Architektura | Wszystkie funkcje oraz zastosowane technologie muszą pochodzić od jednego producenta. |
|  | Musi pozwalać na centralne zarządzenie kontami użytkowników i ich uwierzytelnianiem. |
|  | Musi być dostępny w formie zarówno urządzeń wirtualnych (virtual appliance), jak i sprzętowych. |
|  | Musi pracować w oparciu o dedykowany system operacyjny, wzmocniony (hardenend) z punktu widzenia bezpieczeństwa. |
|  | Musi być dostarczony jako urządzenie na utwardzonym przez jednego producenta systemie operacyjnym w formie gotowego i pełnego rozwiązania. |
|  | Musi zapewniać:1. obsługę nielimitowanej licencyjnie liczby wirtualnych procesorów;
2. maksymalnie 1TB pamięci operacyjnej;
3. 4 wirtualne interfejsy sieciowe;
4. obsługę min. 16TB powierzchni dyskowej.
 |
|  | Musi pozawalać na uruchomienie na platformach:1. Microsoft Hyper-V Server 2019 oraz 2022;
2. VMware ESXi / ESX 4 / 5 / 5 / 6;
3. chmury publicznej Microsoft Azure, Amazon AWS.
 |
|  | Ogólne | Musi pozwalać na zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki, bez konieczności stosowania zewnętrznej konsoli zarządzającej. |
|  | Musi pozwalać na pracę w konfiguracji HA (High Availability) z trybemActive-Passive lub Active-Active w celu zwiększenia niezawodności. |
|  | Musi pozwalać na odpytywanie o stan urządzenia w oparciu o protokół SNMP (v1, v2, v3) oraz wykorzystanie SNMP Trap celem monitorowania m.in. następujących elementów:1. obciążenia procesora/ów;
2. wykorzystania pamięci;
3. obciążenia dysku;
4. zmiany adresu IP interfejsu;
5. informacji o osiąganiu granicznej liczby użytkowników;
6. informacji o osiąganiu granicznej liczby grup użytkowników;
7. przekroczeniu liczby uwierzytelnień;
8. przekroczeniu liczby błędnych uwierzytelnień;
9. zmiana stanu HA.
 |
|  | Musi pozwalać na graficzną reprezentację statusu uwierzytelnień. |
|  | Musi pozwalać na logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia i nazwy użytkownika, w tym:1. lokalnie;
2. zdalnie w oparciu o protokół syslog.
 |
|  | Musi pozwalać na aktualizację systemu operacyjnego z poziomu graficznego interfejsu zarządzającego (GUI). |
|  | Musi pozwalać na tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI) w oparciu o harmonogram w cyklu:1. godzinowym;
2. dziennym;
3. tygodniowym;
4. miesięcznym;

wraz z określeniem godzin i minut. |
|  | Musi pozwalać na zapisywanie kopii bezpieczeństwa przy pomocy protokołu FTP/SFTP. |
|  | Musi pozwalać na szyfrowanie kopii bezpieczeństwa. |
|  | Musi pozwalać na konfigurację Captive Portal |
|  | Zarządzanie | Musi udostępniać graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS. |
|  | Musi udostępniać interfejs REST API. |
|  | Uwierzytelnianie | Musi zapewniać uwierzytelnianie dla 200 użytkowników. |
|  | Musi wspierać lokalną, wbudowaną bazę użytkowników wraz z możliwością wykonywania następujących akcji na użytkowniku:1. tworzenie;
2. przypisanie tokena;
3. zarządzanie tokenem;
4. blokowanie konta (locking);

usuwanie konta. |
|  | Możliwość przechowywanie następujących informacji o użytkowniku:1. nazwa (username);
2. imię/nazwisko;
3. adres email;
4. numer telefonu komórkowego;
5. numer telefonu;
6. adres;
7. kraj;
8. województwo.
 |
|  | Musi umożliwiać przechowywanie min. 3 indywidualnie konfigurowalnych pól dla każdego użytkownika. |
|  | Musi umożliwiać import informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV. |
|  | Musi wspierać konfigurowalną politykę haseł użytkowników wraz z możliwością określenia:1. poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych);
2. czasu życia hasła;
3. możliwości ponownego użycia tych samych haseł.
 |
|  | Musi wspierać konfigurowalną politykę blokowania kont:1. w oparciu o ilość nieudanych logowań;
2. czas blokowania;
3. okres nieaktywności po którym konto jest blokowane.
 |
|  | Możliwość odzyskiwania haseł z wykorzystaniem:1. adresu email;
2. pytania pomocniczego.
 |
|  | Musi wspierać uruchomienie portalu do samodzielnej rejestracji użytkowników, w tym:1. tworzenie kont z akceptacją administratora;
2. tworzenie kont bez akceptacji administratora.
 |
|  | Musi wspierać obsługę protokołu RADIUS zgodną z RFC, w tym:1. wbudowany serwer RADIUS;
2. konfigurację serwera pozwalającą na ograniczenie dostępu tylko do wskazanych urządzeń NAS;
3. integrację z zewnętrznymi serwerami RADIUS;
4. możliwość importowania użytkowników RADIUS z zewnętrznego serwera LDAP.
 |
|  | Musi wspierać obsługę protokołu TACACS+, w tym:1. konfigurację serwera pozwalającą na ograniczenie dostępu tylko dla wskazanych klientów;
2. możliwość importowania klientów z pliku CSV oraz przy pomocy API;
3. specyfikowanie listy dozwolonych/blokowanych poleceń powłoki i usług.
 |
|  | Musi wspierać obsługę protokołu LDAP, w tym:1. wbudowany serwer LDAP;
2. zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP).
 |
|  | Musi wspierać obsługę SAML – Identity Provider (IdP) proxy. |
|  | Musi wspierać realizacje funkcjonalności SSO (Single Sign On), w tym:* 1. integrację z Active Directory bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny;
	2. dedykowaną aplikację na stację robocze z systemem Windows;
	3. RADIUS;
	4. informacje uzyskiwane poprzez protokół syslog;
	5. dedykowany portal.
 |
|  | Uwierzytelnianie dwuskładnikowe | Musi obsługiwać uwierzytelnianie dwuskładnikowe dla min. 100 użytkowników nazwanych. Wykonawca dostarczy min. 100 tokenów, tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania. |
|  | Musi wspierać obsługę dla tokenów sprzętowych (hardware), ich działanie musi być realizowane w oparciu o protokół OAuth wraz ze wsparciem dla TOTP oraz HOTP. |
|  | Musi wspierać obsługę tokenów programowych (software token) dla następujących systemów operacyjnych:1. iOS;
2. Android;
3. Windows Phone (8 i 8.1);
4. Windows 10 Mobile.
 |
|  | Dla tokenów na system operacyjny iOS i Android muszą zostać spełnione wymagania, w zakresie:1. aktywacji z centralnego systemu uwierzytelniania (seed provisioning);
2. możliwości konfiguracji ilości generowanych cyfr (6 lub 8);
3. generowania kodu (cyfr) co 30 lub 60 sekund;
4. możliwości dezaktywacji tokena oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne);
5. ochrony dostępu poprzez konfigurowalny kod PIN;
6. aktywacji w oparciu o kod QR;
7. możliwość przypisania własnego logotypu organizacji widocznego w aplikacji tokena mobilnego.
 |
|  | Musi umożliwiać dostarczenie kodu (wskazania tokena) poprzez:1. email (wygaśnięcie kodu w czasie 10-3600 sekund);
2. SMS (wygaśnięcie kodu w czasie 10-3600 sekund).
 |
|  | Możliwość konfiguracji bramki SMS w oparciu o HTTP/S i/lub SMTP. |
|  | Musi umożliwiać wykorzystanie notyfikacji push (w przypadku tokenów programowy) przychodzących na urządzenie mobilne i zawierających szczegóły dotyczące żądania logowania (nazwa użytkownika, serwer/usługa docelowa, adres IP, data i godzina, rodzaj i wersja przeglądarki) w celu zaakceptowania ich jednym "kliknięciem". |
|  | Musi umożliwiać integracje z logowaniem do systemu Windows. |
|  | Musi posiadać wsparcie dla API. |
|  | Uwierzytelnianie z wykorzystaniem protokołu 802.1x | Musi umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x. |
|  | Musi obsługiwać następujące protokołu (dla sieci bezprzewodowych):1. PEAP;
2. EAP-TTLS;
3. EAP-TLS;
4. EAP-GTC.
 |
|  | Musi wspierać uwierzytelnianie w oparciu o adres MAC (MAC based authentication). |
|  | Musi wspierać zarządzanie certyfikatami (w oparciu o własne CA) w celu wykorzystania w ramach:1. PEAP;
2. TTL;
3. TLS EAP.
 |
|  | Musi umożliwiać samodzielną rejestrację urządzeń przez użytkowników w celu uwierzytelniania z wykorzystaniem certyfikatów. |
|  | Zarządzanie certyfikatami | Musi posiadać własne, samodzielne CA (Certificate Authority). |
|  | Musi wspierać CA pośredniczące (intermediary CA). |
|  | Musi umożliwiać ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego. |
|  | Musi umożliwiać pobranie wygenerowanych certyfikatów. |
|  | Musi umożliwiać podpisywanie certyfikatów z wykorzystaniem protokołu SCEP. |
|  | Musi pozwalać na automatyczne i ręczne generowanie certyfikatówz wykorzystaniem protokołu SCEP. |
|  | Musi umożliwiać generowanie certyfikatów typu wildcard. |
|  | Musi pozwalać na realizację CRL (Certificate Revocation List). |
|  | Musi wspierać dynamiczne odwoływanie certyfikatów z wykorzystaniem protokołu OCSP (RFC2560). |

Tabela 3. Wymaganie dla zaawansowanego mechanizmy autentykacji użytkowników.

* 1. Zaawansowany mechanizm zbierania logów musi spełniać wszystkie wymienione poniżej wymagania:

| **Lp.** | **Rodzaj wymagania** | **Opis wymagania** |
| --- | --- | --- |
|  | Architektura | Wszystkie funkcje oraz zastosowane technologie muszą pochodzić od jednego producenta. |
|  | Musi być dostępny w formie zarówno urządzeń wirtualnych (virtual appliance), jak i sprzętowych. |
|  | Musi pracować w oparciu o dedykowany system operacyjny, wzmocniony (hardenend) z punktu widzenia bezpieczeństwa. |
|  | Musi być dostarczony jako urządzenie na utwardzonym przez jednego producenta systemie operacyjnym w formie gotowego i pełnego rozwiązania. |
|  | Musi zapewniać:1. obsługę nielimitowanej licencyjnie liczby wirtualnych procesorów;
2. maksymalnie 1TB pamięci operacyjnej;
3. 4 wirtualne interfejsy sieciowe;
4. obsługę min. 10TB powierzchni dyskowej.
 |
|  | Musi pozawalać na uruchomienie urządzeń wirtualnych na platformach:1. Microsoft Hyper-V Server 2019 oraz 2022;
2. VMware ESXi / ESX 4 / 5 / 5 / 6;

chmury publicznej Microsoft Azure, Amazon AWS. |
|  | Wydajność | Musi przyjmować min. 25 GB logów dziennie. |
|  | Musi umożliwiać kolekcjonowanie logów dla min. 1 000 systemów. |
|  | Zarządzenie | Musi umożliwiać zarządzanie lokalne z wykorzystaniem szyfrowanych protokołów, w tym:1. HTTPS;
2. SSH.
 |
|  | Musi realizować proces uwierzytelniania administratorów w oparciu o:1. lokalną bazę;
2. Radius;
3. LDAP;
4. Tacacs+;
5. PKI.
 |
|  | Musi umożliwiać definiowanie min. 8 administratorów. |
|  | Musi pozwalać na określenie praw dostępu do wybranych modułów systemu logowania i raportowania. |
|  | Musi umożliwiać podziału na wirtualne systemy logowania i raportowania (konteksty/domeny).  |
|  | Musi umożliwiać przypisywanie administratorom praw dostępu do wybranych kontekstów.  |
|  | Musi umożliwiać niezależne przydzielanie, dla każdego kontekstu, zasobów dyskowych oraz określania maksymalnego czasu przechowywania logów. |
|  | Logowanie | Musi umożliwiać podgląd logowanych zdarzeń w czasie rzeczywistym. |
|  | Musi umożliwiać przeglądanie logów historycznych z funkcją filtrowania. |
|  | Musi umożliwiać dostosowanie widoku wyświetlanych logów poprzez dodawanie, usuwanie oraz zmianę kolejności kolumn zawierających elementy logowanego zdarzenia. |
|  | Musi zapewniać predefiniowane raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa, w tym:1. listę najczęściej wykrywanych ataków;
2. listę najbardziej aktywnych użytkowników/źródeł ruchu;
3. listę najczęściej wykorzystywanych aplikacji;
4. listę najczęściej odwiedzanych stron www;
5. listę krajów , do których nawiązywane są połączenia;
6. listę najczęściej wykorzystywanych polityk Firewall;
7. informacje o realizowanych połączeniach IPSec i SSL VPN;
8. listę najczęściej występujących zdarzeń systemowych.
 |
|  | Musi mieć możliwość konfiguracji predefiniowanych raportów graficznych lub tekstowych. |
|  | Musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych za pomocą protokołu Syslog i/lub CEF. |
|  | Musi zapewniać mechanizmy filtrowania dla przesyłania kopii logów do innych systemów logowania i przetwarzania danych. |
|  | Musi zapewniać komunikację systemów bezpieczeństwa, z których przesyłane są logi, z wykorzystaniem UDP/514 oraz TCP/514. |
|  | Musi umożliwiać cykliczny eksport logów do zewnętrznego systemu zbierania logów w celu ich długoterminowego składowania. |
|  | Musi umożliwiać eksport logów za pomocą protokołu SFTP i/lub SCP. |
|  | Musi umożliwiać określenie przez administratorów, kiedy ma następować eksport logów. |
|  | Musi prezentować informacje na temat ilości przestrzeni dyskowej wykorzystanej na przechowywanie logów. |
|  | Korelacje logów | Musi umożliwiać korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. |
|  | Musi umożliwiać tworzenie własnych reguł korelowania logów. |
|  | Musi umożliwiać konfigurację i wysyłanie powiadomień dot. wystąpienia określonych zdarzeń (sieciowych, systemowych oraz bezpieczeństwa), poprzez:1. e-mail;
2. SNMP;
3. API http.
 |
|  | Musi umożliwiać przekazywanie dodatkowych informacji o określonym zdarzeniu (sieciowych, systemowych oraz bezpieczeństwa) wywołującym dane powiadomienie, np. nazwa wykrytego zagrożenia. |
|  | Musi umożliwiać wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. |
|  | Musi korelować zdarzenia min. dla następujących kategorii zdarzeń:1. Malware/AV;
2. aplikacje sieciowe;
3. email;
4. IPS;
5. Web Filter;
6. Traffic (logi z ruchu sieciowego);
7. Systemowe, w tym:
8. utracone połączenie VPN,
9. utracone połączenie sieciowe,
10. zdarzenia związane z klastrem niezawodnościowym,
11. zmiana w sieci SD-WAN.
 |
|  | Możliwość automatycznego, zwrotnego powiadomienia systemu bezpieczeństwa NGFW o wystąpieniu wybranych zdarzeń korelacji. |
|  | Raportowanie | Musi posiadać predefiniowane zestawy raportów. |
|  | Musi umożliwiać modyfikowanie, przez administratorów, parametrów prezentowania wyników. |
|  | Musi umożliwiać generowanie raportów w następujących formatach:1. HTML;
2. PDF;
3. CSV.
 |
|  | Musi posiadać funkcję definiowania własnych raportów.  |
|  | Musi umożliwiać spolszczenia raportów. |
|  | Musi umożliwiać na generowanie raportów w sposób cykliczny lub na żądanie, z możliwością:1. automatycznego przesłania wyników na określony adres lub adresy email;
2. automatycznego przesłania raportu na zewnętrzny serwer za pomocą protokołu FTP lub SCP.
 |
|  | Musi umożliwiać filtrowanie danych uwzględnianych w procesie tworzenia danego raportu, m.in. możliwość ograniczenia zakresu raportu do danych z wybranych urządzeń NGFW, a także z wybranej adresacji IP. |
|  | Musi umożliwiać automatyczne usuwanie raportów po określonym czasie. |

Tabela 4. Wymagania dla zaawansowanego mechanizmu zbierania logów.

* 1. Zaawansowany mechanizm zarządzania dostępem do infrastruktury sieciowej musi spełniać wszystkie wymienione poniżej wymagania:

| **Lp.** | **Rodzaj wymagania** | **Opis wymagania** |
| --- | --- | --- |
|  | Architektura | Wszystkie funkcje oraz zastosowane technologie muszą pochodzić od jednego producenta. |
|  | Musi być dostępny w formie zarówno urządzeń wirtualnych (virtual appliance), jak i sprzętowych. |
|  | Musi pracować w oparciu o dedykowany system operacyjny, wzmocniony (hardenend) z punktu widzenia bezpieczeństwa. |
|  | Musi być dostarczony jako urządzenie na utwardzonym przez jednego producenta systemie operacyjnym w formie gotowego i pełnego rozwiązania. |
|  | Musi pozawalać na uruchomienie urządzeń wirtualnych na platformach:1. Microsoft Hyper-V Server 2019 oraz 2022;
2. VMware ESXi / ESX 4 / 5 / 5 / 6;

chmury publicznej Microsoft Azure, Amazon AWS. |
|  | Musi obsługiwać moduł vTPM (Virtual Trusted Platform Module) dla przechowywania kluczy prywatnych użytkowników. |
|  | Musi pozwalać na podłączenie min. 30 użytkowników do monitorowanych zasobów (w tym nagrywanie sesji wideo). |
|  | Ogólne | Musi umożliwiać zarządzanie uprzywilejowanym dostępem do zasobów sieciowych. Dostęp uprzywilejowany obejmują lokalne konta administracyjne, konta administracyjne domeny, konta usługi Active Directory lub domenowej oraz konta aplikacji. |
|  | Musi umożliwiać centralne zarządzanie kontami uprzywilejowanymi, w tym:1. konta administratorów;
2. konta z dostępem „root”;
3. konta serwisowe.
 |
|  | Musi umożliwiać tworzenie, usuwanie i modyfikowanie kont, zarządzanie hasłami oraz kontrolę dostępu i uprawnień. |
|  | Musi zapewniać bezpieczne przechowywanie danych uwierzytelniających, takich jak hasła, certyfikaty czy klucze prywatne. Dane te powinny być zaszyfrowane i chronione przed nieuprawnionym dostępem. |
|  | Musi umożliwiać kontrolę dostępu do zasobów sieciowych na podstawie zasad i polityk. |
|  | Musi umożliwiać definiowanie reguł i ograniczeń dostępu dla poszczególnych kont uprzywilejowanych, a także monitorować i rejestrować działania użytkowników. |
|  | Musi umożliwiać audyt i monitorowanie aktywności użytkowników posiadających uprzywilejowany dostęp. |
|  | Musi umożliwiać rejestrowanie i analizę logów związanych z operacjami wykonywanymi przez konta uprzywilejowane, w celu identyfikacji potencjalnych zagrożeń i śledzenia działań. |
|  | Musi wspierać uwierzytelnianie wieloskładnikowe (MFA), takie jak tokeny OTP, certyfikaty czy biometria. |
|  | Musi umożliwiać zarządzanie sesjami uprzywilejowanymi, w tym: 1. monitorowanie i kontrola aktywnych sesji;
2. automatyczne wylogowywanie nieaktywnych sesji;
3. zdalne przerwanie sesji w przypadku podejrzenia nadużyć.
 |
|  | Musi umożliwiać na integrację z innymi narzędziami i rozwiązaniami pozwalającymi na lepszą koordynację działań i wykorzystanie przygotowywanej infrastruktury bezpieczeństwa, w tym:1. systemy zarządzania tożsamościami (IAM);
2. narzędzia do zarządzania incydentami;
3. SIEM (Security Information and Event Management).
 |
|  | Musi umożliwiać monitorowanie aktywności użytkowników z kontami uprzywilejowanymi. |
|  | Musi umożliwiać generowanie szczegółowych raportów audytowych w celu analizy i śledzenia działań użytkowników. |
|  | Funkcjonalne | Musi zapewniać wysoki poziom bezpieczeństwa danych i poufności informacji. |
|  | Musi wspierać szyfrowanie danych w transmisji i przechowywanie haseł i kluczy. |
|  | Musi zapewniać elastyczność w zakresie skalowania infrastruktury w celu obsługi zwiększonego obciążenia. |
|  | Musi posiadać mechanizmy failover i redundancji, aby zapewnić ciągłość działania w przypadku awarii. |
|  | Musi posiadać przyjazny interfejs graficzny (GUI) umożliwiający łatwe zarządzanie kontami uprzywilejowanymi i monitorowanie działań użytkowników. |
|  | Musi wspierać, na potrzeby realizacji dostępu uprzywilejowanego, integrację z technologią Zero Trust Network Access (ZTNA) oraz umożliwiać działanie jako punkt wymuszania dla ZTNA. |
|  | Musi zapewniać możliwość sprawdzania silnikiem antywirusowym przesyłanych podczas sesji plików. Kontrola musi być realizowana co najmniej dla transferu plików poprzez WEB (Web SFTP, Web SAMBA) oraz SCP. |
|  | Musi zapewniać automatyczne blokowanie niebezpiecznych poleceń za pomocą profilu filtrowania SSH. |
|  | Musi monitorować komendy wydawane przez operatora sesji. |
|  | Musi pozwalać na obsługę połączeń bezpośrednich jak i proxy. |
|  | Musi obsługiwać niestandardowe protokoł np. poprzez dedykowane wyzwalacze (custom application launcher). |
|  | Musi ostrzegać użytkowników o nagrywaniu w celu zapewnienia zgodności z wymaganiami RODO. |
|  | Musi obsługiwać mechanizm awaryjnego dostępu do zaszyfrowanych haseł przechowywanych w systemie na zasadzie procedury „glass breaking”. Wszystkie działania w tym trybie muszą być logowane celem możliwości przeprowadzenia audytu. |
|  | Musi automatycznie nagrywać obraz podczas uruchomienia procedury awaryjnej (glass breaking). |
|  | Musi umożliwiać automatyczną zmiana hasła konta po poprawnym zalogowaniu. |
|  | Musi wspierać zaplanowane, według harmonogramu, zmiany haseł. |
|  | Musi umożliwiać tworzenie procedury żądania dostępu do haseł i zatwierdzania takich żądań poprzez konfigurowalną ilość administratorów. |
|  | Musi obsługiwać algorytmy szyfrowania SSH o wysokiej sile. |
|  | Musi obsługiwać zaawansowany protokół uwierzytelniania RDP, w tym CredSSP i TLS. |
|  | Musi posiadać kontrolę dostępu opartą na rolach (RBAC). |
|  | Musi posiadać kontrolę uprawnień opartą na użytkownikach oraz grupach użytkowników. |
|  | Musi posiadać kontrolę profili dostępowych w formie polityk. |
|  | Musi posiadać wsparcie dla Disaster Recovery. |
|  | Musi umożliwiać na pracę użytkowników uprzywilejowanych w następujących trybach:1. agentowy – dostępne wszystkie funkcjonalności (agent musi być dostępny bezpłatnie);
2. bezagentowy – za pomocą przeglądarki internetowej wraz z dedykowanym rozszerzeniem (metoda ta musi umożliwiać na uzupełnianie haseł oraz nagrywanie sesji);
3. bezagentowy – za pomocą przeglądarki internetowej bez dodatkowych rozszerzeń.
 |
|  | Uwierzytelnianie | Musi obsługiwać uwierzytelnianie użytkowników za pomocą certyfikatów. |
|  | Musi umożliwiać na korzystanie z lokalnej bazy danych użytkowników. |
|  | Musi obsługiwać uwierzytelnianie wieloskładnikowe opartego na SAML. |
|  | Musi obsługiwać openID Connect (OIDC) oraz SAML. |
|  | Musi obsługiwać wielu połączeń SAML SP. |
|  | Musi umożliwiać na integrację z istniejącymi usługami uwierzytelniania, w tym:1. Active Directory;
2. LDAP;
3. Radius.
 |
|  | Musi wspierać integrację z istniejącymi systemami zarządzania tożsamościami. |
|  | Musi obsługiwać, w miarę rozwoju organizacji, na większą liczbę kont uprzywilejowanych. |
|  | Musi umożliwiać na blokowanie dostęp do zasobów użytkowników uprzywilejowanych w oparciu o dodatkowe parametry, w tym:1. kontrola dostępu oparta na adresie źródłowym IP użytkownika;
2. ograniczanie dostępu oparte na harmonogramie użytkownika;
3. kontrola dostępu do docelowego serwera oparta o przypisane tagi ZTNA (stan stacji, z której następuje połączenie musi być badany przez mechanizmy ZTNA).
 |

Tabela 5. Wymagania dla zaawansowanego mechanizmu zarządzania dostępem do infrastruktury sieciowej.

* 1. Wymagania, o których mowa w ust. 5, ust. 6, ust. 7 oraz ust. 8, muszą zostać zapewnione niezależnie od dostawcy łącza internetowego.
	2. Dla zapewnienia bezpieczeństwa zmodernizowanej infrastruktury sieciowej oraz szybkiego wsparcia technicznego ze strony Wykonawcy wymaga się, aby wszystkie elementy zmodernizowanej infrastruktury sieciowej pochodziły od jednego producenta.
	3. Wszystkie dostarczone przez Wykonawcę elementy Przedmiotu zamówienia, o których mowa w Rozdziale 4.2 „Modernizacja infrastruktury sieciowej”, muszą być objęte kompletną licencją producenta.
	4. Nie dopuszcza się dodatkowych wymagań licencyjnych dla:
1. systemu operacyjnego, bazy danych, oprogramowania serwera WWW lub podobnych;
2. ilości zasobów do których realizowany jest nadzorowany dostęp;
3. ilości zajętego miejsca na dyskach przez m.in. zbierane logi, nagrania sesji wideo, itp.
	1. Dopuszcza się, aby poszczególne elementy wchodzące w skład zmodernizowanej infrastruktury sieciowej były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych w postaci maszyn wirtualnych na posiadanym przez Zamawiającego systemie zarządzania wirtualizacją Microsoft Hyper-V Server.
	2. W przypadku implementacji programowej, o której mowa w ust. 13, Wykonawca zobowiązany jest do przekazanie Zamawiającemu parametrów technicznych maszyn wirtualnych wymaganych do realizacji implementacji. Implementacja programowa będzie podlegała akceptacji przez Zamawiającego. W przypadku braku akceptacji Wykonawca jest zobowiązany do zaproponowania innego rozwiązania.

## Dokumentacja powykonawcza

1. Wykonawca, w ramach opracowania dokumentacji powykonawczej, o której mowa w ust. 2 pkt 3 w Rozdziale 3 „Przedmiot zamówienia”, opracuje i przekaże Zamawiającemu szczegółową dokumentację powykonawczą.
2. Szczegółowa dokumentacja powykonawcza, o której mowa w ust. 1 pkt 1, zostanie opracowana przez Wykonawcę w postaci dokumentu pn. **Dokumentacja powykonawcza**.
3. Dokument, o których mowa w ust. 2, należy opracować z zachowaniem:
4. wymagań Zamawiającego przedstawionych w niniejszym OPZ;
5. wyjaśnień Zamawiającego do niniejszego OPZ, które Wykonawca jest zobowiązany zebrać na etapie realizacji prac;
6. uzgodnień z Zamawiającym.
7. Dokument, o którym mowa w ust. 2, będzie podlegał akceptacji przez Zamawiającego. W ramach opracowania dokumentu Wykonawca zobowiązany jest do uzgodnienia z Zamawiającym szczegółowej struktury dokumentu. Uzgodnienia zostaną przeprowadzone pomiędzy Stronami na spotkaniu roboczym w siedzibie Zamawiającego. Spotkanie odbędzie się na wniosek Wykonawcy, w terminie uzgodnionym z Zamawiającym.
8. **Dokumentacja powykonawcza**, o której mowa w ust. 2, musi zawierać co najmniej:
9. spis treści;
10. wprowadzenie;
11. słownik pojęć i skrótów;
12. decyzje i założenia projektowo-architektoniczne;
13. opis architektury logicznej;
14. opis architektury technicznej;
15. opis technologii realizacji;
16. opis konfiguracji urządzeń sieciowych;
17. opis klastrowania urządzeń sieciowych;
18. opis mechanizmu zbierania logów z urządzeń sieciowych UTM i wykonywania analiz na logach, w tym:
19. opis rozwiązania,
20. opis zastosowanej technologii,
21. opis użytkowników, ich ról i uprawnień,
22. opis zastosowanej konfiguracji i parametryzacji;
23. opis mechanizmu autentykacji użytkowników, w tym:
24. opis rozwiązania,
25. opis zastosowanej technologii,
26. opis użytkowników, ich ról i uprawnień,
27. opis zastosowanej konfiguracji i parametryzacji;
28. opis mechanizmu zarządzania dostępem do infrastruktury sieciowej, w tym:
29. opis rozwiązania,
30. opis zastosowanej technologii,
31. opis użytkowników, ich ról i uprawnień,
32. opis zastosowanej konfiguracji i parametryzacji;
33. opis sposobu postępowania w sytuacjach awaryjnych i nadzwyczajnych oraz ścieżkę eskalacji problemów;
34. raport z prac instalacyjnych i konfiguracyjnych;
35. raport z przeprowadzonych testów.
36. Dokumenty, o których mowa w ust. 2, będą podlegały akceptacji przez Zamawiającego. W ramach opracowania dokumentów Wykonawca zobowiązany jest do uzgodnienia z Zamawiającym szczegółowej struktury dokumentów. Uzgodnienia zostaną przeprowadzone pomiędzy Stronami na spotkaniu roboczym w siedzibie Zamawiającego. Spotkanie odbędzie się na wniosek Wykonawcy, w terminie uzgodnionym z Zamawiającym.
37. Dokument, o którym mowa w ust. 2, będzie podlegał bezpłatnej aktualizacji przez Wykonawcę w trakcie realizacji Przedmiotu zamówienia.
38. Wykonawca zobowiązany jest pisemnie poinformować Zamawiającego, o konieczności dokonania aktualizacji dokumentu, o którym mowa w ust. 2, oraz wykonania aktualizacji w terminie **2 Dni roboczych** od dokonania zgłoszenia.
39. Aktualizacja dokumentu, o którym mowa w ust. 2, może zostać również zainicjowana na wniosek Zamawiającego. W takiej sytuacji Wykonawca wykona aktualizację dokumentu w terminie, o którym mowa w ust. 8.
40. Poprzez aktualizację dokumentu, o której mowa w ust. 5, należy rozumieć utworzenie kolejnej nowych i aktualnej wersji dokumentu.
41. Weryfikacja i odbiór dokumentu, o którym mowa w ust. 2, będzie przeprowadzona zgodnie z procedurą weryfikacji i odbioru dokumentu określoną w Rozdziale 10.1 „Weryfikacja i odbiór dokumentu”.

# Termin realizacji Przedmiotu zamówienia

1. Rozpoczęcie prac nastąpi z chwilą podpisania przez Strony Umowy.
2. Przedmiot zamówienia, o którym mowa w Rozdziale 3 „Przedmiot zamówienia” należy zrealizować w terminie 10 dni od daty podpisania Umowy, w nieprzekraczalnym terminie do **15 grudnia 2023 roku[[1]](#footnote-1).**
3. Gwarancja i Wsparcie techniczne, o którym mowa w Rozdziale 7 „Gwarancja i Wsparcie techniczne”, będzie świadczone, przez Wykonawcę, przez okres **48 miesięcy** od dnia podpisania przez Strony Protokołu Odbioru Przedmiotu Zamówienia, którego wzór stanowi Załącznik nr 7 do OPZ.

# Kontekst prawny

Przedmiot zamówienia musi być zgodny z następującymi przepisami prawa polskiego i europejskiego oraz normami i wytycznymi.

1. Ustawy:
2. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57 z późn. zm.);
3. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2022 r. poz. 2509 t.j.);
4. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 t.j.);
5. Ustawa z dnia 23 kwietnia 1964 r. Kodeks Cywilny (Dz. U. z 2023 r. poz. 1610 z późn. zm.);
6. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 z późn. zm.);
7. Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. z 2023 r. poz. 1440 t.j.).
8. Akty wykonawcze:
9. rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247 z późn. zm.);
10. rozporządzenie Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (Dz. U. z 2018 r. poz. 29);
11. rozporządzenie Ministra Cyfryzacji z dnia 10 marca 2020 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (Dz. U. z 2020 r. poz. 399);
12. rozporządzenie Komisji (WE) NR 976/2009 z dnia 19 października 2009 r. w sprawie wykonania dyrektywy 2007/2/WE Parlamentu Europejskiego i Rady w zakresie usług sieciowych (Dz. U.UE.L.274.9 z 20.10.2009 z późn. zm.);
13. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U.UE.L.119.1 z 04.05.2016).
14. Inne akty prawne (ustawy, akty wykonawcze, akty prawa organizacyjnego i wytyczne) dotyczące Przedmiotu zamówienia, które weszły w życie w trakcie realizacji Umowy.

# Gwarancja i Wsparcie techniczne

1. Gwarancja i Wsparcie techniczne musi być świadczone przez okres **48 miesięcy** od dnia podpisania przez Strony Protokołu Odbioru Przedmiotu Zamówienia dla wszystkich elementów dostarczonych i wdrożonych przez Wykonawcę w ramach Przedmiotu zamówienia.
2. Wykonawca jest odpowiedzialny względem Zamawiającego za wszelkie wady fizyczne i prawne Przedmiotu zamówienia, przy czym za wady fizyczne uznaje się niespełnienie wymagań określonych w niniejszym OPZ.
3. Gwarancja, o której mowa w ust. 1, musi obejmować:
4. naprawę lub wymianę urządzeń w przypadku ich wadliwości w trybie AHR (Advanced Hardware Replacement) najpóźniej w następnym Dniu roboczym od zgłoszenia;
5. odbiór i zwrot urządzenia (w przypadku awarii) do producenta bez dodatkowych kosztów po stronie Zamawiającego, realizowane przez Wykonawcę;
6. możliwość pozostawienia dysków twardych u Zamawiającego, bez dodatkowych kosztów po stronie Zamawiającego;
7. dostęp do aktualizacji oprogramowania, sterowników, itp. w celu utrzymania infrastruktury w aktualnym i bezpiecznym stanie.
8. Wsparcie techniczne, o którym mowa w ust. 1, musi obejmować:
9. obsługę w języku polskim;
10. wsparcie techniczne w trybie 24/7 z czasem reakcji 1h od zgłoszenia (w przypadku zgłoszeń krytycznych) oraz w ciągu następnego dnia roboczego (Next Business Day) w przypadku zgłoszenia niekrytycznego;
11. pomoc w obsłudze procesu RMA na portalu producenta;
12. pomoc w konfiguracji platformy realizowaną przez inżyniera z najwyższym dostępnym poziomem certyfikacji technicznej Wykonawcy;
13. dostęp do zdalnej zmiany konfiguracji;
14. dostęp do pomocy (zdalny oraz stacjonarny u Zamawiającego) w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producent;
15. dostęp do zdalnych konsultacji technicznych z inżynierem posiadającym najwyższy poziom certyfikacji technicznej Wykonawcy;
16. wsparcie w procesie upgrade firmware.
17. Jeżeli w czasie Gwarancji, o której mowa w ust. 1, wyjdą na jaw wady wyłączające lub ograniczające przydatność produktów zmodernizowanej infrastruktury sieciowej, Wykonawca dokona napraw gwarancyjnych polegających m.in. na:
18. naprawie wadliwego działania produktów Przedmiotu zamówienia;
19. rekonfiguracji wadliwych ustawień/konfiguracji produktów;
20. naprawie baz danych;
21. naprawie zawartości baz danych (w tym usunięcie braku spójności i integralności danych, ochronę danych przed utratą);
22. wspieraniu każdorazowo administratorów Zamawiającego w przywróceniu pełnej funkcjonalności produktów, niezależnie od przyczyny niesprawności;
23. wymianie elementów produktów w przypadku wystąpienia wady fizycznej lub prawnej;
24. innych działaniach koniecznych dla zapewnienia prawidłowego funkcjonowania produktów.
25. Wykonawca ponosi odpowiedzialność z tytułu rękojmi na zasadach określonych w Kodeksie Cywilnym, z zastrzeżeniem, że okres obowiązywania rękojmi z tytułu wad fizycznych jest równy okresowi obowiązywania Gwarancji, o którym mowa w ust. 1.
26. Wykonawca zapewni, aby Gwarancja, o której mowa w ust. 1, były świadczone przez producenta zmodernizowanej infrastruktury sieciowej. Wykonawca zapewni pojedynczy punkt kontaktu z pomocą techniczną dla wszystkich elementów dostarczonych i wdrożonych przez Wykonawcę w ramach Przedmiotu zamówienia.
27. Dostęp do pojedynczego punktu kontaktu, o którym mowa w ust. 7, musi być świadczony za pomocą:
28. infolinii (pod wskazanym numerem telefonu);
29. poczty elektronicznej (pod wskazanym adresem poczty elektrycznie);
30. dedykowanej platformy serwisowej (pod wskazanym adresem strony internetowej).

# Zobowiązania Wykonawcy

Pozostałe zobowiązania Wykonawcy niewskazane gdzie indziej.

1. Wykonawca wykona Przedmiot zamówienia z najwyższą starannością, efektywnością oraz zgodnie z najlepszą praktyką i wiedzą zawodową.
2. Wykonawca będzie ściśle współpracował z osobami odpowiedzialnymi za realizację Przedmiotu zamówienia po stronie Zamawiającego.
3. Zamawiający zastrzega sobie prawo m.in. do:
4. zgłaszania uwag do realizacji przez Wykonawcę:
5. Przedmiotu zamówienia,
6. Gwarancji;
7. proponowania zmian na każdym etapie realizacji Przedmiotu zamówienia i Wsparcia technicznego;
8. organizowania spotkań roboczych (w tym również na etapie weryfikacji i odbioru produktów Przedmiotu zamówienia) w siedzibie DCGiK lub w innym miejscu na terenie m.st. Warszawy, wskazanym przez Zamawiającego, w terminie określonym przez Zamawiającego;
9. organizowania telekonferencji lub wideokonferencji w terminie określonym przez Zamawiającego;
10. żądania od Wykonawcy przedstawiania wyników prac cząstkowych dotyczących realizacji Przedmiotu zamówienia oraz Gwarancji.
11. Wykonawca zobowiązany jest dokonać z Zamawiającym wszelkich koniecznych ustaleń mogących mieć wpływ na Przedmiot zamówienia.
12. Wszelkie działania Wykonawcy w ramach realizacji Przedmiotu zamówienia będą oparte o uznane standardy i metodyki wykorzystane w danym obszarze m.in. ITIL.
13. Wykonawca zobowiązany jest do współpracy z Zamawiającym na każdym etapie realizacji Przedmiotu zamówienia.
14. Wykonawca nie może odmówić wzięcia udziału w spotkaniach roboczych oraz telekonferencjach lub wideokonferencjach, o których mowa w ust. 3. W spotkaniach roboczych oraz telekonferencjach lub wideokonferencjach oprócz Wykonawcy i Zamawiającego uczestniczyć mogą, powoływanie przez Zamawiającego, Audytorzy zewnętrzni i/lub Eksperci zewnętrzni.
15. Wszelkie koszty Wykonawcy związane z dojazdem i udziałem w spotkaniach roboczych, telekonferencjach lub wideokonferencjach, o których mowa w ust. 3, nie będą dodatkowo płatne – ich koszt Wykonawca uwzględni w całkowitym wynagrodzeniu Wykonawcy za realizację Przedmiotu zamówienia (w tym m.in. koszty wynagrodzeń i diet dla pracowników, dojazdów do Zamawiającego oraz wszystkie inne koszty związane z udziałem Wykonawcy w spotkaniach roboczych, telekonferencjach lub wideokonferencjach).
16. Wszelkie zawiadomienia/zgody/decyzje/zatwierdzenia Zamawiającego lub Wykonawcy będą dokonywane w formie pisemnej lub za pomocą poczty elektronicznej.
17. Wszystkie dokumenty wytworzone przez Wykonawcę w ramach realizacji Przedmiotu zamówienia będą charakteryzowały się wysoką jakością, na którą mają wpływ takie czynniki jak:
18. struktura dokumentu, rozumiana jako podział danego dokumentu, w czytelny i zrozumiały sposób, na rozdziały, podrozdziały i sekcje;
19. kompletność dokumentu, rozumiana jako pełne, bez wyraźnych, ewidentnych braków, przedstawienie omawianego problemu obejmujące całość danego zakresu rozpatrywanego zagadnienia;
20. spójność i niesprzeczność dokumentu, rozumiane jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu;
21. zachowanie standardów, a także sposób pisania, rozumianych jako zachowanie spójnej struktury, formy i sposobu pisania dla poszczególnych dokumentów oraz fragmentów tego samego dokumentu;
22. użycie jednolitego słownika definicji i pojęć dla wszystkich dokumentów;
23. stosowanie Rozdziałów, ustępów, punktów, liter oraz tiret, interpretowanych zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej” (Dz. U. 2016 r., poz. 283);
24. pogrubianie czcionki dla tytułów poszczególnych Rozdziałów;
25. wyrównywanie wypunktowań do prawej strony;
26. używanie czcionki Arial, o wielkości 9 pkt;
27. równomierne wyrównywanie tekstu pomiędzy stronami (wyjustowanie);
28. stosowanie 1,15 odległości między wierszami;
29. stosowanie marginesów – dolny 2,5 cm, górny 2,5 cm, lewy 2,5 cm, prawy 2,5 cm;
30. umieszczanie w dokumentach ilustracji, rysunków, zdjęć z podpisem poniżej;
31. stosowanie wcięcia 1,25 cm dla nowych akapitów.
32. Zamawiający wymaga, o ile jest taka możliwość, aby przekazywane przez Wykonawcę dokumenty były w języku polskim.
33. Dokumenty wytworzone przez Wykonawcę w ramach realizacji Przedmiotu zamówienia nie będą oznaczone logiem Wykonawcy, ani żadnym innym elementem identyfikującym Wykonawcę.
34. Nagłówki wszystkich wytworzonych przez Wykonawcę dokumentów muszą zawierać graficzną identyfikację wizualną programu unijnego, logo UMWM oraz emblemat Unii Europejskiej, zgodnie z wytycznymi Mazowieckiej Jednostki Wdrażania Programów Unijnych.



Rysunek 1. Wzór nagłówka Dokumentu.

1. Wszelkie dane i informacje otrzymane od Zamawiającego i utrzymywane w ramach realizacji Przedmiotu zamówienia są własnością Zamawiającego. Wykonawca jest zobowiązany do zachowania poufności wszystkich danych i informacji, w których posiadanie wejdzie podczas realizacji Przedmiotu zamówienia.
2. W przypadku ujawnienia zagrożeń dla realizacji Przedmiotu zamówienia Wykonawca niezwłocznie poinformuje Zamawiającego o wystąpieniu takiego zagrożenia.
3. Wykonawca, na wniosek Zamawiającego, udzieli Zamawiającemu każdorazowo pełnej informacji na temat stanu realizacji Przedmiotu zamówienia.
4. Wykonawca będzie zobowiązany współdziałać z osobami wskazanymi przez Zamawiającego.

# Zobowiązania Zamawiającego

Pozostałe zobowiązania Zamawiającego niewskazane gdzie indziej.

1. Udostępnienie dokumentacji, materiałów i informacji będących w posiadaniu Zamawiającego, niezbędnych do realizacji Przedmiotu zamówienia.
2. Udzielanie Wykonawcy na bieżąco niezbędnych do realizacji Przedmiotu zamówienia wyjaśnień oraz przekazywanie niezbędnych informacji.
3. Informowanie Wykonawcy o wszelkich czynnościach podejmowanych w związku z realizacją Przedmiotu zamówienia, jeśli będą one miały związek z jego realizacją przez Wykonawcę.
4. Umożliwienie Wykonawcy dostępu do, posiadanych przez Zamawiającego, obiektów, infrastruktury teleinformatycznej, oprogramowania oraz dokumentacji, niezbędnych do realizacji Przedmiotu zamówienia, zgodnie z wewnętrznymi regulacjami Zamawiającego i w Godzinach pracy Zamawiającego.

# Warunki weryfikacji i odbioru produktów Przedmiotu zamówienia

1. Wszystkie produkty Przedmiotu zamówienia będą objęte procedurami weryfikacji i odbioru opisanymi w niniejszym rozdziale.
2. W ramach Przedmiotu zamówienia wyróżnia się m.in. następujące typy produktów:
3. dokumenty;
4. modernizacja infrastruktury sieciowych.
5. Wykonawca przekazuje do odbioru, przez Zamawiającego, produkty Przedmiotu zamówienia, o których mowa w ust. 2, w Dni robocze i w Godzinach pracy Zamawiającego.
6. Wykonawca dostarcza produkty Przedmiotu zamówienia do odbioru, przez Zamawiającego, zgodnie z terminami określonymi w Rozdziale 5 „Termin realizacji Przedmiotu zamówienia”.

## Weryfikacja i odbiór dokumentu

1. Wykonawca przekaże Zamawiającemu do odbioru dokument wytworzony w ramach realizacji Przedmiotu zamówienia.
2. Dokument, o którym mowa w ust. 1, zgłoszony do odbioru będzie poddany weryfikacji przez Zamawiającego, zgodnie z opisaną poniżej procedurą:
3. Wykonawca przekazuje dokument do odbioru Zamawiającemu wraz z Protokołem Przekazania Dokumentu, którego wzór stanowi Załącznik nr 1 do OPZ;
4. Zamawiający zapoznaje się z dostarczonym dokumentem w czasie nie dłuższym niż **3 Dni robocze**;
5. jeżeli Zamawiający nie zgłasza uwag do Dokumentu, to następuje podpisanie Protokołu Odbioru Dokumentu, którego wzór stanowi Załącznik nr 2 do OPZ, i tym samym zakończenie procedury odbioru dokumentu;
6. w przypadku kiedy Zamawiający zgłosi uwagi do przekazanego dokumentu, rejestruje uwagi w postaci komentarzy (lub w trybie „śledzenia zmian”) w treści dokumentu, który następnie przekazuje Wykonawcy i procedura przebiega zgodnie z poniższymi krokami:
7. w uzgodnionym z Zamawiającym terminie (nie dłuższym niż **2 Dni robocze** od dnia przekazania uwag), na pisemny wniosek Wykonawcy Zamawiający może zorganizować spotkanie robocze (w siedzibie DCGiK lub w innym miejscu na terenie m. st. Warszawy), telekonferencję lub wideokonferencję, w celu omówienia dostarczonego dokumentu i uwag Zamawiającego,
8. w uzgodnionym z Zamawiającym terminie (nie dłuższym niż **2 Dni robocze** od dnia przekazania uwag) Wykonawca przekazuje Zamawiającemu poprawiony dokument uwzględniający zgłoszone przez Zamawiającego uwagi,
9. Wykonawca zobowiązany jest przedłożyć Zamawiającemu poprawiony dokument, uzupełniony o informacje dotyczące sposobu, w jaki zostały one rozpatrzone – zaktualizowany dokument powinien być dostarczony w taki sposób, aby widoczne były w nim naniesione zmiany (np. w trybie „śledzenia zmian”) wraz z komentarzami,
10. jeżeli Zamawiający ponownie zgłosi uwagi do dokumentu następuje przejście procedury do kroku, o którym mowa w lit. a,
11. jeżeli Zamawiający nie zgłosi uwag, to następuje podpisanie Protokołu Odbioru Dokumentu, Wykonawca przekazuje Zamawiającemu ostateczną wersję dokumentu (bez komentarzy oraz trybu „śledzenia zmian”) i tym samym zakończenie procedury odbioru dokumentu.
12. W uzasadnionych przypadkach Strony uzgodnią terminy odbiegające od wyżej wymienionych.
13. Zmiany terminów, o których mowa w ust. 3, nie będą traktowane jako zmiany zapisów Umowy oraz nie mogą mieć wpływu na termin realizacji Przedmiotu zamówienia.
14. Wykonawca zobowiązany jest przekazywać Zamawiającemu dokument w wersji elektronicznej w postaci pliku PDF oraz w postaci pliku edytowalnego (np. DOCX).

## Weryfikacja i odbiór modernizacji infrastruktury sieciowej

1. Przed przystąpieniem do weryfikacji i odbioru modernizacji infrastruktury sieciowej Wykonawca przygotuje i uzgodni z Zamawiającym:
2. Plan Testów, którego wzór stanowi Załącznik nr 3 do OPZ;
3. Raport z Testów, którego wzór stanowi Załącznik nr 4 do OPZ.
4. Plan Testów, o którym mowa w ust. 1 pkt 1, będzie obejmował w szczególności czynności związane ze sprawdzeniem poprawności realizacji modernizacji z uzgodnieniami z Zamawiającym i szczegółowymi wymaganiami wynikającymi z zapisów niniejszego OPZ. Plan Testów będzie poddany weryfikacji przez Zamawiającego.
5. Raport z Testów, o którym mowa w ust. 1 pkt 2, musi zawierać m.in. informacje o pozytywnym lub negatywnym przejściu kolejnych kroków opisanych w Planie Testów. Raport z Testów będzie poddany weryfikacji przez Zamawiającego.
6. Jeżeli Zamawiający nie zgłasza uwag do dokumentów, o których mowa w ust. 1, to następuje akceptacja tych Dokumentów i przejście do procedury, o której mowa w ust. 5. W przypadku, kiedy Zamawiający zgłosi uwagi do któregokolwiek z dokumentów, zgłoszenie uwag następuje zgodnie z procedurą weryfikacji i odbioru dokumentu opisaną w Rozdziale 10.1 „Weryfikacja i odbiór dokumentu”.
7. Weryfikacja i odbiór modernizacji, będzie realizowana zgodnie z poniższą procedurą:
8. po zakończeniu prac związanych z modernizacją infrastruktury sieciowej Wykonawca poinformuje Zamawiającego Protokołem Przekazania Modernizacji, którego wzór stanowi Załącznik nr 5 do OPZ, o zakończeniu prac i zaproponuje termin przeprowadzenia testów;
9. Zamawiający w ciągu **2 Dni roboczych** uzgodni z Wykonawcą termin przeprowadzenia testów;
10. testy są przeprowadzane zgodnie z zaakceptowanym Planem Testów przez przedstawicieli Zamawiającego w obecności (na wniosek Zamawiającego) przedstawiciela Wykonawcy;
11. z przebiegu testów Zamawiający wypełnia, sporządzony przez Wykonawcę, Raport z Testów;
12. w przypadku negatywnego wyniku testów, Zamawiający uzgadnia z Wykonawcą termin usunięcia usterek i następuje przejście procedury do pkt 1;
13. po pozytywnym przejściu testów, Zamawiający i Wykonawca podpisują Protokół Odbioru Modernizacji, którego wzór stanowi Załącznik nr 6 do OPZ, i procedura odbioru zostaje zakończona.
14. W uzasadnionych przypadkach Strony uzgodnią terminy odbiegające od wyżej wymienionych.
15. Zmiany terminów, o których mowa w ust. 6, nie będą traktowane jako zmiany zapisów Umowy oraz nie mogą mieć wpływu na termin realizacji Przedmiotu zamówienia.

# Warunki weryfikacji i odbioru Przedmiotu zamówienia

1. W ramach weryfikacji i odbioru Przedmiotu zamówienia Wykonawca przedłoży Zamawiającemu Protokół Odbioru Przedmiotu Zamówienia, którego wzór stanowi Załącznik nr 7 do OPZ.
2. Podstawą przedłożenia Zamawiającemu Protokołu Odbioru Przedmiotu Zamówienia będzie pozytywne odebranie przez Zamawiającego wszystkich prac przewidzianych do realizacji w ramach Przedmiotu zamówienia.
3. Wykonawca przekazuje Przedmiot zamówienia do weryfikacji i odbioru, przez Zamawiającego, zgodnie z terminami określonymi w Rozdziale5 „Termin realizacji Przedmiotu zamówienia” w Dni robocze i w Godzinach pracy Zamawiającego.
4. Protokół Odbioru Przedmiotu Zamówienia, o którym mowa w ust. 1, będzie obejmował w szczególności potwierdzenie realizacji wszystkich prac przewidzianych do realizacji w ramach Przedmiotu zamówienia, z uzgodnieniami z Zamawiającym i szczegółowymi wymaganiami wynikającymi z zapisów niniejszego OPZ.
5. Protokół Odbioru Przedmiotu Zamówienia będzie poddany weryfikacji przez Zamawiającego i musi zawierać m.in.:
6. wykaz poszczególnych prac odebranych przez Zamawiającego w ramach Przedmiotu zamówienia;
7. wykaz produktów odebranych przez Zamawiającego w ramach poszczególnych prac;
8. terminy odbioru poszczególnych prac.
9. Jeżeli Zamawiający nie zgłasza uwag do Protokołu Odbioru Przedmiotu Zamówienia to Zamawiający i Wykonawca podpisują Protokół Odbioru Przedmiotu Zamówienia i procedura odbioru zostaje zakończona.
10. W przypadku, kiedy Zamawiający zgłosi uwagi do Protokołu Odbioru Przedmiotu Zamówienia (zgłoszenie uwag następuje zgodnie z procedurą weryfikacji i odbioru dokumentu opisaną w Rozdziale 10.1 „Weryfikacja i odbiór dokumentu”) to procedura odbioru przebiega zgodnie z poniższymi krokami:
11. Wykonawca w ciągu **1 Dnia roboczego** przekazuje Zamawiającemu poprawiony, zgodnie z uwagami Zamawiającego, Protokół Odbioru Przedmiotu Zamówienia;
12. Zamawiający w terminie **2 Dni roboczych** weryfikuje przekazany Protokół Odbioru Przedmiotu Zamówienia;
13. w przypadku negatywnego wyniku weryfikacji następuje przejście procedury do pkt 1;
14. jeżeli Zamawiający nie zgłasza uwag do Protokołu Odbioru Przedmiotu Zamówienia to Zamawiający i Wykonawca podpisują Protokół Odbioru Przedmiotu Zamówienia i procedura odbioru zostaje zakończona.
15. W uzasadnionych przypadkach Strony uzgodnią terminy odbiegające od wyżej wymienionych.
16. Zmiany terminów, o których mowa w ust. 8, nie będą traktowane jako zmiany zapisów Umowy oraz nie mogą mieć wpływu na termin realizacji Przedmiotu zamówienia.

# Załączniki

Wykaz załączników stanowiących integralną część OPZ:

1. Załącznik nr 1 – wzór Protokołu Przekazania Dokumentu;
2. Załącznik nr 2 – wzór Protokołu Odbioru Dokumentu;
3. Załącznik nr 3 – wzór Planu Testów;
4. Załącznik nr 4 – wzór Raportu z Testów;
5. Załącznik nr 5 – wzór Protokołu Przekazania Modernizacji
6. Załącznik nr 6 – wzór Protokołu Odbioru Modernizacji;
7. Załącznik nr 7 – wzór Protokołu Odbioru Przedmiotu Zamówienia.
1. Termin ten jest uzasadniony realizacją Umów w ramach projektu pn. „Regionalne partnerstwo samorządów Mazowsza dla aktywizacji społeczeństwa informacyjnego w zakresie e-administracji i geoinformacji” (Projekt ASI) objętego Regionalnym Programem Operacyjnym Województwa Mazowieckiego na lata 2014-2020. [↑](#footnote-ref-1)