Ministerstwo Rozwoju i Technologii **Warszawa, 17.04.2023 r.**

ul. Plac Trzech Krzyży 3/5

00-507 Warszawa

ZAPYTANIE O WYCENĘ DO OSZACOWANIA WARTOŚCI ZAMÓWIENIA

Ministerstwo planuje uruchomić postępowanie przetargowe o udzielenie zamówienia publicznego na dostawę Systemu Zabezpieczeń typu Next Generation Firewall wraz z wdrożeniem i gwarancją na okres minimum 36 miesięcy dla Ministerstwa Rozwoju i Technologii.

Uprzejmie prosimy o wycenę, poniżej opisanych minimalnych wymagań stanowiących przedmiot planowanego do wszczęcia postępowania przetargowego na dostawę Systemu Zabezpieczeń typu Next Generation Firewall wraz z wdrożeniem i gwarancją na okres minimum 36 miesięcy dla Ministerstwa Rozwoju i Technologii.

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem Zamówienia, jest dostawa Systemu Zabezpieczeń typu Next Generation Firewall wraz z wdrożeniem i gwarancją na okres minimum 36 miesięcy dla Ministerstwa Rozwoju i Technologii.

Zakres zamówienia obejmuje w szczególności:

1. dostawę Systemu Zabezpieczeń typu Next Generation Firewall, na który składają się:
   a) urządzenia typu Firewall wraz z gwarancją na okres minimum 36 miesięcy, w liczbie niezbędnej do uzyskania funkcjonalności opisanej w pkt III-VII,
   b) oprogramowanie, licencje w formie subskrypcji dla wymaganego do sprawnego działania urządzeń i uzyskania funkcjonalności, o których mowa w pkt III-VII, na okres 36 miesięcy,
2. wdrożenie dostarczonego Systemu Zabezpieczeń typu Next Generation Firewall, w tym:
   a) instalację dostarczonych urządzeń i subskrypcji oprogramowania,
   b) konfigurację, uruchomienie i testowanie, w tym dodatkowych elementów,
   c) wykonanie dokumentacji technicznej i eksploatacyjnej,
   d) przeprowadzenie instruktażu dla administratorów Systemu.
3. usługi asysty technicznej dla wdrożonego Systemu, świadczone na podstawie dodatkowych zleceń Zamawiającego.

II. TERMIN REALIZACJI ZAMÓWIENIA

Przedmiot zamówienia zostanie zrealizowany w terminie maksymalnie **do 60 dni** od daty podpisania przez strony umowy **(termin realizacji do uzupełnienia przez Wykonawcę w Formularzu Ofertowym).**

Realizacja przedmiotu zamówienia obejmować będzie dostawę Systemu Zabezpieczeń typu Next Generation Firewall wraz z wdrożeniem i gwarancją na okres minimum 36 miesięcy dla Ministerstwa Rozwoju i Technologii do siedziby Zamawiającego, przy Placu Trzech Krzyży 3/5 w Warszawie.

III. MINIMALNE WYMAGANIA DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. W ramach realizacji przedmiotu zamówienia zostanie zrealizowana dostawa Systemu Zabezpieczeń typu Next Generation Firewall (System NGFW) wraz z wdrożeniem i gwarancją na okres minimum 36 miesięcy dla Ministerstwa Rozwoju i Technologii.
2. W ramach realizacji przedmiotu zamówienia zostaną dostarczone urządzenia wraz z niezbędnymi elementami i licencjami oprogramowania składającego się na zaoferowany System Zabezpieczeń typu Next Generation Firewall.
3. Zaoferowane urządzenia oraz oprogramowanie nie może być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
4. Wszystkie elementy dostarczone z urządzeniami, będą pochodziły od jednego producenta. Stosowane elementy muszą być wspierane przez producenta urządzeń i być objęte możliwością analizy potencjalnych błędów w trakcie potencjalnych zgłoszeń serwisowych. Muszą pochodzić z autoryzowanego kanału sprzedaży producentów Urządzeń na rynek polski lub Unii Europejskiej
5. Zaoferowane urządzenia muszą być fabrycznie nowe przeznaczone do sprzedaży na rynku europejskim (zgodnie z ustawą z dnia 30.08.2002 r. o systemie oceny zgodności (Dz.U. z 2004 r., nr 204, poz. 2087 j.t. z późn. zm.) i z wydanymi na jej podstawie rozporządzeniami), wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia oraz objęte wymaganą przez Zamawiającego gwarancją w Polsce. Zamawiający nie dopuszcza produktów

„odnawianych" (ang. Refurbished). Zaoferowane urządzenia, oprogramowanie sterujące połączeniami oraz aplikacje zarządzające muszą pochodzić od tego samego producenta. Zamawiający wymaga, aby dostarczony System pochodził z oficjalnego kanału dystrybucyjnego danego producenta, a serwis gwarancyjny był autoryzowany przez producenta urządzeń i oprogramowania oraz świadczony przez producenta lub autoryzowanych partnerów w centrach serwisowych na terenie Unii Europejskiej.

6. Zamawiający wymaga, aby zaoferowane urządzenia były dostępne i serwisowane przez Producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne) – na dzień składania oferty.

IV. MINIMALNE WYMAGANIA TECHNICZNE SYSTEMU ZABEZPIECZEŃ TYPU NEXT GENERATION FIREWALL

1. System Zabezpieczeń typu Next Generation Firewall musi być dostarczony w postaci dedykowanych 2 sztuk, urządzeń pracujących w klastrach niezawodnościowych.
2. Każde z dostarczonych urządzeń musi minimalnie spełniać poniżej wymienione warunki techniczne:
   a) 40 Gbps przepustowości Firewall/kontroli aplikacji;
   b) 20 Gbps przepustowości Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware;
   c) 20 Gbps dla IPsec VPN;
   d) 3 000 000 jednoczesnych sesji;
   e) 200 000 nowych połączeń na sekundę;
   f) 5 000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN;
   g) 10 wirtualnych routerów posiadających odrębne tabele routingu;
   h) 10 wirtualnych instancji firewall (określanych jako kontekst/domena/system). Każda z instancji musi pozwalać na konfigurację niezależnych oraz odrębnych od innych instancji – polityk bezpieczeństwa (co najmniej dla IPS, AV i współpracy z sandboxem), tablicy routingu oraz realizacji zdalnego dostępu. Możliwość licencyjnego zwiększenia liczby wirtualnych instancji firewall do 20.
   i) 200 stref bezpieczeństwa;
   j) Protokołów routingu: OSPFv2 i OSPFv3, BGP4;
   k) Lokalnej przestrzeni na system operacyjny i logi co najmniej o pojemności 400GB
   l) Wysokość maksymalnie 3U wraz z zestawem montażowym do szafy RACK 19";
   m) dwa redundantne zasilacze AC 230V Hot-Swap z kompletami kabli;
   n) 8 portów 10-GigabitEthernet RJ45
   o) 12 portów 10 Gigabit Ethernet SFP+ obsługujące moduły optyczne SR oraz LR
   p) 4 porty 25 Gigabit Ethernet SFP28
   q) 4 porty 40/100 Gigabit Ethernet QSFP28 lub alternatywnie 4 porty 40
   r) Gigabit Ethernet QSFP+ i 4 porty 100 Gigabit Ethernet QSFP28
   s) 1 port 1-GigabitEthernet RJ45 wyłącznie do celów zarządzania; dopuszcza się realizację tego poprzez port 1-GigabitEthernet SFP z użyciem modułu SFP RJ45.
   t) Urządzenia muszą posiadać port (40GE lub szybsze) dla celów połączenia urządzeń w klaster (high availability). Porty te muszą być traktowane jako dodatkowe względem wymaganych przez Zamawiającego. Nie dopuszcza się wykorzystania do celu klastrowania portów opisanych w podstawowych wymaganiach.
3. Zamawiający dopuszcza, aby dostarczony System był zbudowany w oparciu o komponenty wraz z elementami dodatkowymi, których zastosowanie jest opcjonalne i dobrowolne, a decyzja o ich zastosowaniu leży w gestii Wykonawcy – jeżeli uzna on, iż dla osiągnięcia opisanych wymaganych funkcjonalności są niezbędne. Zamawiający zezwala na ich zastosowanie pod warunkami opisanymi w punktach 4 - 12.
4. Stosowanie dodatkowych systemów nie może dotyczyć funkcji ochronnych Systemu NGFW (np. wykrywania aplikacji, obsługi IPS, AV czy NAT);
5. Stosowanie dodatkowych systemów nie może powodować ominięcia reguł bezpieczeństwa (np. weryfikacja kondycji bezpieczeństwa stacji końcowej nie może odbywać się w oparciu o integrację z systemem logowania i raportowania, bez wykorzystania reguł bezpieczeństwa);
6. Stosowanie dodatkowych systemów jest dopuszczalne, jeśli są one konieczne dla:
   - weryfikacji tożsamości użytkowników – system uwierzytelniania;
   - realizacji funkcji zarządzania firewallem i uprawnieniami administratorów;
   - zatwierdzania i pracy na konfiguracji kandydackiej;
   - realizacji funkcji inspekcji ruchu SSL;
   - realizacji ochrony DNS
   - realizacji zaawansowanych funkcji ochrony wymagających pobierania danych z chmury Threat Intelligence producenta oferowanego rozwiązania.

7. Stosowanie dodatkowych systemów dopuszczalne jest wyłącznie przy zapewnieniu ich wysokiej dostępności, m.in. poprzez dostarczenie takiego systemu jako dedykowane rozwiązanie składające się z urządzenia z dedykowanym dla niego oprogramowaniem ze wsparciem świadczonym przez jednego producenta. System musi być dostarczony jako klaster niezawodnościowy – tzn. identyczne urządzenia pracujące równolegle w modelu 1+1 lub N+1, wyposażone w redundantne zasilacze z możliwością ich wymiany „na gorąco" (hot-swap). Jeżeli urządzenia wspomagające są wyposażone w dyski SSD/HDD to należy przewidzieć je w konfiguracji niezawodnościowej RAID1 z możliwością ich wymiany „na gorąco" (hot-swap).
8. Systemy wspomagające muszą być zaoferowane z pełnym wsparciem producenta co oznacza wymóg zaoferowania wszystkich pakietów wsparcia producenta dostępnych dla oferowanego rozwiązania i konieczne dla właściwego działania usług wymaganych przez Zamawiającego.
9. W przypadku stosowania systemów wspomagających Zamawiający wymaga by były one oferowane przez tego samego producenta co oferowany System Zabezpieczeń typu Next Generation Firewall, w tym ze wsparciem tego producenta. Zamawiający dopuszcza stosowanie rozwiązań innych producentów, lecz ich liczba nie może przekraczać 2 (dwóch) nie licząc producenta oferowanych urządzeń Systemu Zabezpieczeń typu Next Generation Firewall.
10. Zamawiający wymaga, aby wszystkie dostarczane systemy wspomagające spełniały wymagania określone w pkt III ppkt 3-6 Minimalne wymagania dotyczące realizacji zamówienia.
11. Wykonawca wraz z Systemem NGFW musi dostarczyć wszystkie niezbędne kable, wkładki światłowodowe zarówno do oferowanych urządzeń jak również do przełączników posiadanych przez Zamawiającego do prawidłowego uruchomienia sprzętu.
12. Wykonawca z oferowanymi urządzeniami musi dostarczyć min.:
    a) 8 szt. wkładek 40G/100G QSFP+/QSFP28;
    b) 8 szt. wkładek 25G SFP28;
    c) 8 szt. wkładek 40G/100G QSFP+/QSFP28 do posiadanych przez Zamawiającego przełączników Cisco Nexus
    d) 8 szt. wkładek 25G SFP28 QSFP28 do posiadanych przez Zamawiającego przełączników Cisco Nexus.

V. MINIMALNE WYMAGANIA FUNKCJONALNE SYSTEMU ZABEZPIECZEŃ TYPU NEXT GENERATION FIREWALL

1. Dostarczony System Zabezpieczeń typu Next Generation Firewall (System NGFW) musi spełniać następujące funkcjonalności:
   - ochronę zasobów serwerowych Zamawiającego przed ingerencją z zewnątrz;
   - ochronę zasobów serwerowych Zamawiającego przez atakami z wnętrza sieci własnej;
   - kontrolę korzystania z zasobów internetowych przez użytkowników;
   - kontrolę przesyłanych danych z podmiotów współpracujących z Zamawiającym;
   - zdalny dostęp do sieci.

   oraz wymagania i funkcje szczegółowo opisane w dalszych punktach.
2. System musi rozpoznawać aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji nie może wymagać podania w konfiguracji NGFW numeru lub zakresu portów, na których jest ona dokonywana. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. NFGW musi wykrywać co najmniej 3000 aplikacji predefiniowanych przez Producenta.
3. System musi realizować funkcjonalności na bazie profili przypisywanych na poziomie reguł bezpieczeństwa:
    a) Intrusion Prevention System (IPS),
    b) Antywirus (AV),
    c) Anty-Spyware/Anty-Malware,
    d) Ochrona DNS,
    e) URL Filtering, sandbox lokalny lub chmurowy tego samego producenta.
4. Bazy sygnatur IPS, AV, Anty-Spyware (lub Anty-Malware, jeżeli obejmuje on ochronę przed Spyware) muszą być przechowywane w systemie NGFW, regularnie aktualizowane w sposób automatyczny.
5. Aktualizacje sygnatur AV muszą odbywać się nie rzadziej niż raz na 24 godziny.
6. System musi zapewniać możliwość tworzenia własnych sygnatur IPS bez wykorzystania zewnętrznych narzędzi (dopuszcza się tworzenie sygnatur z wykorzystaniem dostarczanego systemu zarządzania) czy wsparcia producenta.
7. Urządzenie Systemu musi umożliwiać elastyczną konfigurację AV i IPS w szczególności Wykrywanie aktywności sieci typu Botnet.

8. System musi posiadać funkcjonalność deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS (Wymagane wsparcie co najmniej dla TLSv1.1, TLSv1.2 i TLSv1.3). Odszyfrowany ruch zostaje przekazany do zewnętrznych urządzeń bezpieczeństwa, które po przeprowadzeniu analizy zwrócą ruch do urządzenia Systemu NGFW, w celu jego dalszego przetwarzania. Urządzenie Systemu NGFW musi przy tym współpracować z zewnętrznymi urządzeniami bezpieczeństwa funkcjonującymi w trybie transparentnym lub w trybie L3 (funkcjonalność nazywana dalej inspekcją SSL/TLS). Dopuszcza się rozwiązanie zewnętrzne współpracujące z urządzeniem Systemu NGFW przy spełnieniu poniższych wymagań:
   STARTTLS (Wymagane wsparcie co najmniej dla TLSv1.1, TLSv1.2 i TLSv1.3). Odszyfrowany ruch zostaje przekazany do zewnętrznych urządzeń bezpieczeństwa, które po przeprowadzeniu analizy zwrócą ruch do urządzenia Systemu NGFW, w celu jego dalszego przetwarzania. Urządzenie Systemu NGFW musi przy tym współpracować z zewnętrznymi urządzeniami bezpieczeństwa funkcjonującymi w trybie transparentnym lub w trybie L3 (funkcjonalność nazywana dalej inspekcją SSL/TLS). Dopuszcza się rozwiązanie zewnętrzne współpracujące z urządzeniem Systemu NGFW przy spełnieniu poniższych wymagań:
   a) realizuje wymaganą funkcjonalność dla wydajności przetwarzania minimum 10 Gbps inspekcji TLS dla sesji http 64K,
   b) jest wyposażone w co najmniej 4 interfejsy 10GigabitEthernet SFP+
   c) zapewnia redundancję zasilaczy analogicznie do urządzeń firewall,
   d) musi być dostarczone w modelu redundancji 1:1 (analogicznie do urządzeń firewall) z potrzebnymi licencjami i gwarancją/wsparciem zgodnym z długością wsparcia firewalla
   e) obsługujące w chwili dostawy co najmniej 10 instancji wirtualnych pozwalających na powiązanie ich z wirtualnymi instancjami realizowanymi przez urządzenia firewall oraz umożliwiające docelowo obsługę 20 instancji (np. poprzez dokupienie odpowiedniej licencji)
   f) musi być dostarczone z potrzebnymi licencjami i gwarancją zgodną z długością wsparcia firewalla.
   g) w przypadku zewnętrznego urządzenia lub urządzeń innych niż NGFW wymagane jest dostarczenie opisu współpracy proponowanej integracji z NGFW wykonującym inspekcję wykrywania i zapobiegania włamaniom na rozszyfrowanym ruchu przez zewnętrzne urządzenia.
9. Możliwość blokowania transmisji plików, co najmniej następujących typów: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku na podstawie nagłówka i typu MIME.
10. Filtrowanie ruchu URL w oparciu o automatycznie aktualizowaną bazę kategorii stron WWW i bazę reputacji tych stron. Ocena strony musi obejmować określenie jej kategorii (np. finanse, zakupy, sport, itp.) oraz określenie ryzyka do niej przypisanego (co najmniej wysokie-średnie-niskie). Możliwość tworzenia własnych list stron (whitelist oraz blacklist) bez wykorzystania zewnętrznych narzędzi czy wsparcia producenta. Własne listy będą miały wyższy priorytet niż klasyfikacja na bazie kategorii dostarczanych przez producenta.
11. Dostarczony System NGFW musi posiadać możliwość wysyłania plików przesyłanych przez urządzenie do lokalnego lub chmurowego systemu Sandbox.
12. System Sandbox musi zostać dostarczony w postaci fizycznego urządzenia bądź usługi subskrypcji.
13. Urządzenie Systemu Firewall musi pozwalać na przesyłanie do systemu Sandbox plików zdefiniowanych przez administratora – co najmniej exe, dll, java, MS Office.
14. Urządzenie Systemu NGFW musi być aktualizowane o nowo wykryte (w sandbox) zagrożenia.
15. Administrator musi posiadać dostęp do raportów z sandboxa dotyczących plików wysłanych przez urządzenie Systemu Firewall oraz posiadać możliwość manualnego wysłania pliku do sandbox (np. poprzez upload poprzez stronę www)
16. Dopuszcza się zaoferowanie lokalnego rozwiązania sandbox (zapewnianego przez producenta Systemu Firewall) – należy wówczas przewidzieć urządzenie pozwalające na jednoczesną analizę co najmniej 30 próbek/plików (VM Sandboxing)
17. Dopuszcza się zaoferowanie chmurowego rozwiązania sandbox (realizowanego przez producenta Systemu Firewall). W przypadku, jeżeli producent realizuje dostęp do chmurowego sandboxa za pomocą licencji oprogramowania należy przewidzieć licencję, która będzie pozwalała na jednoczesną analizę minimum 30 próbek/plików (VM Sandboxing).
18. Wymagane jest by możliwa była analiza 30 próbek/plików jednocześnie bez względu na to czy pliki te wysłane będą automatycznie czy manualnie przez administratora czy też będzie

to „mix” plików pochodzących zarówno bezpośrednio z Systemu Firewall i od administratorów.

19. Ochrona DNS w modelu, gdzie dla każdego zapytania DNS przetwarzanego przez System Firewall musi zostać wykonana jego pełna analiza. Nie dopuszcza rozwiązania funkcjonującego wyłącznie w oparciu o weryfikację zapytania DNS w bazie danych rozpoznanych zagrożeń danego producenta, ponieważ taka metoda nie zapewnia ochrony tzw. pacjenta zero, który wykonuje zapytanie DNS o unikalną nazwę domenową, która jeszcze nie znajduje się w bazie. Analiza każdego zapytania musi obejmować co najmniej zakres detekcji jak poniżej:
    a) wykrywanie zapytań do domen złośliwych. Baza domen musi mieć co najmniej 10 milionów wpisów,
    b) możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing)
20. Zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site.
21. Zestawianie tuneli SSL VPN w konfiguracji remote-access-VPN.
    a) Wymagane jest zestawienie tuneli z wykorzystaniem klienta VPN dostarczanego przez producenta urządzenia Systemu NGFW obsługa co najmniej 5000 tuneli, możliwość instalacji klienta VPN dla 5000 urządzeń/użytkowników.
    b) Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows i MacOS oraz musi posiadać możliwość weryfikacji kondycji bezpieczeństwa stacji zdalnej (Windows, MacOS) co najmniej w zakresie sprawdzenia:
        i. Czy zainstalowane jest oprogramowanie antywirusowe i czy posiada ono aktualne sygnatury,
        ii. Czy jest włączony osobisty firewall (ang. Personal firewall),
        iii. Czy komputer jest zarejestrowany w domenie Active Directory (tylko Windows)
    c) Oprogramowanie klienta VPN musi być objęte wsparciem producenta w okresie zgodnym z długością wsparcia dostarczonego Systemu NGFW.
    d) Wymagane jest zestawienie tuneli bez konieczności zastosowania klienta VPN – tzw. praca w trybie Clientless VPN – dla co najmniej 2000 tuneli
22. Monitorowanie oraz podstawowe zarządzanie muszą być możliwe z linii poleceń (CLI) oraz przez Interfejs graficzny (GUI) realizowany przez przeglądarkę lub dedykowanego klienta instalowanego na stacji roboczej administratora – bez konieczności korzystania z centralnych narzędzi zarządzania.
23. Eksportowanie logów do zewnętrznych serwerów zgodnych z protokołem Syslog.
24. Obsługa 4094 VLAN zgodnych z 802.1q.
25. Obsługa tworzenia subinterfejsów na interfejsach pracujących w L2 i L3.
26. Obsługa stref bezpieczeństwa symbolizujących np. WAN, LAN, DMZ, interfejsy fizyczne, subinterfejsy L2 i L3 – jako nazwane strefy, na bazie których można budować polityki bezpieczeństwa przy regulacji ruchu pomiędzy strefami.
27. Translacja adresów IP (NAT) zarówno statyczna jak i dynamiczna. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak, aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
28. Transparentne ustalenie tożsamości w oparciu o:
    a) integrację z kontrolerem domeny Active Directory;
    b) integracji z serwerami Microsoft Exchange;
    c) integracji z serwerami terminalowymi;
    d) integracji bazującej na informacji z logów SYSLOG pozwalającej na uwierzytelnienie użytkowników korzystających z systemów UNIX.
29. System NGFW musi posiadać możliwość wymuszenia w procesie uwierzytelniania użytkownika podania przez niego drugiego czynnika uwierzytelniającego (tzw. MFA) w celu ochrony kluczowych systemów przed kradzieżą poświadczeń.
30. Uwierzytelnianie administratorów Systemu NGFW za pomocą:
    a) bazy lokalnej;
    b) zewnętrznej usługi katalogowej dostępnej po LDAPS;
    c) RADIUS lub TACACS+.
31. Budowanie reguł bezpieczeństwa opierające się na podstawowych selektorach takich jak: strefy bezpieczeństwa źródłowe/docelowe, adresy IP źródłowe/docelowe, aplikacje (w warstwie L7 OSI), użytkownicy/grupy z Active Directory.
32. Zarządzanie pasmem sieci (QoS) w zakresie ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Przydzielanie takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
33. Inspekcja szyfrowanej komunikacji SSH (Secure Shell) w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

34. Praca na Systemie NGFW musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w całości konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej. Musi istnieć możliwość porównania zmian (m.in. polityk, konfiguracji interfejsów, routingu itp.), ze wcześniejszymi wersjami konfiguracji. Funkcja ta musi być dostępna z CLI i z GUI.
35. Interpretacja parametrów wydajnościowych dla Firewall/kontroli aplikacji - rozwiązanie pozwalające na:
    a) wykrycie aplikacji,
    b) przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.
36. Interpretacja parametrów wydajnościowych dla Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware - rozwiązanie pozwalające na:
    a) wykrycie aplikacji,
    b) przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych,
    c) inspekcje IPS całego ruchu,
    d) inspekcję antywirusową całego ruchu,
    e) inspekcję Antymalware/AntySpyware całego ruchu,
    f) przesyłanie plików do sandboxa lokalnego i/lub chmurowego,
    g) przechwytywanie i blokowanie plików określonego typu.

    Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla rozwiązania sygnaturami IPS oraz ze wszystkimi funkcjami dostępnymi w urządzeniu dla silników antywirus i antyspyware/antymalware. Inspekcjom bezpieczeństwa musi podlegać cały ruch – sprawdzeniu musi podlegać każdy bajt danych przesyłany przez urządzenie. Zamawiający wymaga, aby podana została przepustowość urządzenia dla pełnego zakresu ochrony oferowanego przez urządzenie – jeżeli urządzenie pozwala na pracę w wielu trybach to należy podać przepustowość dla trybu z największą liczbą dostępnych inspekcji dla silników IPS, antywirus, antymalware/antyspyware.

VI. **MINIMALNE WYMAGANIA w zakresie charakterystyki ruchu sieciowego dla interpretacji parametrów wydajnościowych**

1. Wszystkie parametry dotyczące wydajności, pod kątem przepustowości (ang. throughput), wymaganej na zaoferowanym Systemie NGFW zakładają, iż będą to parametry wskazane przez producentów w kartach katalogowych jako sesje http 64K (lub mniejsze np. http 44K, http 32K), lub dla równoważnego modelu ruchu.
2. Przez równoważny model ruchu rozumie się taki ruch, dla którego wymagane parametry wydajnościowe są osiągane w ruchu całościowym (up/down) i jednocześnie - w którym rozkład procentowy ruchu wybranych protokołów wykorzystujących pakiety różnej wielkości, przy pomocy których realizowane są różne aplikacje (np. youtube, facebook, google, gmail, ssh, smtp z załącznikami) jest przedstawiony w tabeli poniżej:

Protokół	Udział w %
HTTP	25%
HTTPS	60%
SMTP, IMAP, POP3, FTP, SMB i inne	12%
DNS	3%

3. W przypadku gdy Wykonawca zaproponuje urządzenie, którego wydajność będzie oparta o model ruchu przedstawiony powyżej wówczas jest on zobowiązany do dodatkowego potwierdzenia spełnienia wymagań wydajnościowych. Zamawiający wymaga, aby potwierdzenie to zostało dołączone do oferty w postaci wyników testów przeprowadzonych przez publiczny ośrodek badawczo-rozwojowy w Polsce z wykorzystaniem dedykowanych testerów ruchu – IXIA lub Spirent lub Agilent.

VII. MINIMALNE WYMAGANIA FUNKCJONALNE w zakresie zarządzana i logowania

1. Dostarczony System NGFW musi umożliwiać centralne monitorowanie funkcjonowania wszystkich zaoferowanych urządzeń wchodzących w skład Systemu NGFW.
2. Jeżeli oferowany System NGFW nie jest wyposażony w taką funkcjonalność Zamawiający dopuszcza dostarczenie funkcjonalności jako dodatkowego Systemu zarządzania i logowania jako narzędzie/licencja/subskrypcja w zależności od formy w jakiej oferuje producent.
3. System zarządzania i logowania musi być w pełni kompatybilny z oferowanym Systemem NGFW.
4. System zarządzania i logowania musi pozwalać na centralne monitorowanie funkcjonowania wszystkich zaoferowanego Systemu NGFW i pochodzić od tego samego producenta co oferowane urządzenia Systemu NGFW i spełniać niżej opisane wymagania.
5. Musi pozwalać na zarządzanie:
   a) nie mniej niż 10 firewallami rozumianymi jako firewalle fizyczne
   b) nie mniej niż 50 firewallami rozumianymi jako wirtualne instancje firewall (określane jako kontekst/domena/system) i umożliwia docelowo rozbudowę do systemu dla 100 instancji wirtualnych.
6. Musi zarządzać obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium.
7. Musi zapewniać dystrybucję i zdalną instalację nowych sygnatur oraz wersji oprogramowania systemowego.
8. Musi przechowywać różne wersje konfiguracji zarządzanych Systemu NGFW.
9. Musi zbierać logi zdarzeń z oferowanych NGFW co najmniej o:
   a) ruchu sieciowym,
   b) użytkownikach,
   c) aplikacjach,
   d) zagrożeniach
   e) filtrowanych stronach WWW.
10. Musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli.
11. Musi umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w logach zebranych z zarządzanych urządzeń Systemu NGFW.
12. Musi pozwalać na tworzenie raportów na podstawie gromadzonych w logach informacji.
13. Musi pozwalać na tworzenie raportów na podstawie zbudowanych kontenerów/grup Systemu NGFW.
14. Musi pozwalać na zapisywanie stworzonych raportów, uruchamianie ich w sposób manualny lub automatyczny w określonych przedziałach czasu oraz eksport do formatu tekstowego.
15. Graficzny interfejs SZL (Web GUI) musi być realizowany z wykorzystaniem protokołu HTTPS przez przeglądarkę WWW w HTML5, bez wykorzystania technologii Java czy Flash.
16. Musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu.
17. SZL musi zapewniać gromadzenie logów inspekcyjnych (związanych z ruchem przechodzącym przez firewall) w zakresie co najmniej:
   a) 20 TB użytecznej przestrzeni dyskowej z możliwością jej rozbudowy (bez konieczności wymiany chassis urządzenia) do 40TB,
   b) Obsługuje co najmniej 150GB logów inspekcyjnych jako przyrost dzienny,
   c) Obsługuje minimum 5000 logów na sekundę.
18. SZL musi zapewniać gromadzenie logów administracyjnych (z ang. Management logs) w zakresie co najmniej:
   a) 2 TB użytecznej przestrzeni dyskowej z możliwością jej rozbudowy do 5TB (bez konieczności wymiany chassis urządzenia)
   b) Obsługuje co najmniej 5GB logów inspekcyjnych jako przyrost dzienny
   c) Obsługuje minimum 100 logów na sekundę
19. SZL musi być dostarczony w postaci sprzętowej - w postaci dedykowanego urządzenia.
   a) SZL musi być dostarczony w postaci dedykowanego rozwiązania sprzętowo programowego - jako dedykowane rozwiązanie tj. urządzenie z dedykowanym dla niego oprogramowaniem serwisowane w całości przez jednego producenta i zarazem producenta oferowanego systemu firewall).
   b) SZL musi posiadać minimum 2 interfejsy 10GE,
   c) Użyteczna przestrzeń dyskowa zapewniana przez sprzętowy SZL musi zostać zrealizowana w RAID-1,
   d) Urządzenie realizujące SZL musi posiadać redundantne zasilacze AC oraz zapewniać możliwość ich wymiany w czasie pracy – tzw. zasilacze Hot-Swap.

20. SZL może być zbudowany w oparciu o pojedyncze rozwiązanie lub oparciu o dwa osobne urządzenia, współpracujące pomiędzy sobą, gdzie:
    a) Jedno urządzenie jest dedykowane dla centralnego logowania zdarzeń i raportowania, obsługująca logi inspekcyjne,
    b) Drugie urządzenie jest dedykowane dla zarządzania urządzeniami, kontami administratorów i obsługująca logi administracyjne,
    c) W przypadku gdy SZL będzie składał się z dwóch urządzeń muszą zostać spełnione następujące warunki:
    i. Oba urządzenia muszą pochodzić od jednego producenta i zarazem producenta oferowanego Systemu NGFW,
    ii. Każde z urządzeń z osobna musi spełniać wymagania w zakresie liczby zarządzanych firewalli, liczby docelowo zarządzanych firewalli,
    iii. Każde z urządzeń z osobna musi spełniać wymagania dotyczące architektury sprzętowej tj. wymagania dotyczące interfejsów, przestrzeni dyskowej (wielkość i zabezpieczenie RAID), zasilanie etc.

VIII. MINIMALNE WYMAGANIA w zakresie licencji oprogramowania

1. Wraz z Systemem NGFW zostanie dostarczone niezbędne do zapewnienia wymaganych funkcjonalności i prawidłowego działania do którego jest przeznaczone, oprogramowanie w ilości umożliwiającej spełnienie wymagań funkcjonalnych. Oprogramowanie zostanie dostarczone, w postaci stałej licencji lub minimum 36 miesięcznej subskrypcji, o ile producent nie oferuje oprogramowania w innej formie niż subskrypcja.
2. Wraz z oprogramowaniem Wykonawca będzie zobowiązany dostarczyć dokument potwierdzający nabycie przez ministerstwo praw do dostarczonego oprogramowania ze wskazaniem nazwy, liczby i rodzaju licencji.
3. Dla Systemu NGFW muszą zostać dostarczone subskrypcje oprogramowania na okres 36 miesięcy – jeżeli są one wymagane przez producenta oferowanego rozwiązania - obejmujące aktualizacje sygnatur dla następujących funkcji:
    a) Aktualizacje bazy aplikacji;
    b) Aktualizacje baz sygnatur IPS;
    c) Aktualizacje baz sygnatur AV;
    d) Aktualizacje/dostęp do bazy URL z kategoryzacją stron;
    e) Możliwość współpracy z systemem sandbox;
    f) Aktualizacji baz dla ochrony DNS;
    g) realizację sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN).

IX. MINIMALNE WYMAGANIA w zakresie wdrożenia dostarczonego Systemu NGFW wraz z przeprowadzeniem instruktażu.

1. W ramach wdrożenia dostarczonego Systemu Zabezpieczeń typu Next Generation Firewall Wykonawca będzie zobowiązany do wykonania niżej opisanego zakresu.
2. Wykonawca utworzy i przekaże dokument - Projekt techniczny Systemu NGFW (w języku polskim) – zawierający co najmniej:
    a) architekturę rozwiązania,
    b) opis konfiguracji wstępnej,
    c) testy akceptacyjne systemu,
    d) opis elementów infrastruktury Systemu, obejmujący parametry sprzętowe,
    e) konfigurację oprogramowania,
    f) harmonogram zawierający terminy realizacji zadań w ramach poszczególnych Etapów przedmiotu zamówienia. Harmonogram zostanie sporządzony w uzgodnieniu z Zamawiającym oraz zatwierdzony przez Zamawiającego.
3. Projekt techniczny będzie podlegał zatwierdzeniu przez Zamawiającego.
4. Wykonawca dostarczy wszystkie urządzenia stanowiące przedmiot zamówienia, składające się na System NGFW do siedziby Zamawiającego oraz wdroży dostarczone elementy Systemu poprzez realizację następujących czynności:
    a) instalację i konfigurację sprzętu i licencji w środowisku Zamawiającego, zgodnie z projektem technicznym,
    b) przeprowadzenie testów akceptacyjnych.
5. Wykonawca opracuje i dostarczy dokumentację powdrożeniową zawierającą w swojej treści co najmniej:
    a) procedury i instrukcje dotyczące instalacji, konfiguracji oraz parametryzacji wdrożonego Systemu,

b) procedury i instrukcje wykonania kopii bezpieczeństwa i ich odtworzenia,
c) procedury i instrukcje aktualizacji i wdrażania poprawek,
d) procedury postępowania w razie wystąpienia błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów,
e) dokumentacja musi być dostarczona przed produkcyjnym uruchomieniem Systemu,
f) dokumentacja będzie podlegała akceptacji ze strony Zamawiającego.

6. Po wykonaniu wdrożenia Systemu Wykonawca zobowiązany będzie do przeprowadzenia instruktażu dla administratorów Zamawiającego na następujących zasadach:
   a) instruktaż zostanie przeprowadzony na rzecz Zamawiającego dla minimum 4 administratorów, w wymiarze minimum 2 dni roboczych po 6 godzin zajęć efektywnych dziennie;
   b) dokładny termin zostanie uzgodniony z Zamawiającym z co najmniej 3 dniowym wyprzedzeniem, instruktaż zostanie przeprowadzony w siedzibie Zamawiającego,
   c) Wykonawca zapewni przeprowadzenie instruktażu przez kadrę wykwalifikowaną posiadającą wiedzę teoretyczną i praktyczną z zakresu przedmiotu zamówienia, (wymagane posiadanie certyfikatu z oferowanej technologii przez inżyniera przeprowadzającego instruktaż),
   d) przed ustalonym terminem instruktażu Wykonawca prześle Zamawiającemu zakres tematyczny/programu instruktażu. Zamawiający będzie miał prawo do weryfikacji zakresu tematycznego/programu instruktażu i zgłoszenia ew. dodatkowego zakresu tematycznego, Instruktaż swoją tematyką będzie obejmował co najmniej:
      - instalację dostarczonego Systemu,
      - konfigurację podstawowych funkcjonalności,
      - weryfikację ruchu (wykrywanie sytuacji niepożądanych),
      - zarządzanie uprawnieniami,
      - backup i odtworzenie konfiguracji.

X. MINIMALNE WYMAGANIA w zakresie asysty technicznej

1. Wykonawca przez cały okres trwania umowy zobowiązany będzie do świadczenia usługi asysty technicznej na każde żądanie Zamawiającego, tj. każdorazowo na podstawie pisemnego zlecenia asysty technicznej, wystawianego przez Zamawiającego.
2. Zakres, sposób oraz termin realizacji zostanie uzgodniony na etapie przedstawienia wymagań przez Zamawiającego i wyceny pracochłonności przez Wykonawcę, poprzedzających zlecenie.
3. Zlecenia będą obejmować w szczególności:
   1) wsparcie pracowników Zamawiającego w użytkowaniu systemu NGFW zarówno techniczne jak i merytoryczne,
   2) implementację nowych funkcjonalności lub modyfikację już skonfigurowanych.
   3) Wsparcie w przypadku wystąpienia incydentu bezpieczeństwa.
      a. Wsparcie w zakresie wykonania analizy wykorzystanych podatności.
      b. Kontaktu z ekspertem w zakresie bezpieczeństwa dostarczonego systemu.
      c. Analizy zakresu kompromitacji systemu.
      d. Wsparcia w konfiguracji/rekomendacji w celu zabezpieczenia systemu,
      e. Wsparcia w zakresie usunięcia skutków oraz rozwiązania incydentu bezpieczeństwa,
   4) Wsparcie w planowanych pracach serwisowych,
      a. Przeprowadzenia standardowych prac serwisowych,
      b. Przeprowadzania aktualizacji komponentów systemu,
      c. Weryfikacji poprawności konfiguracji,
      d. Zmiany w topologii sieci,
      e. Wsparcia w okresie podwyższonej czujności (np. Monitoring środowiska w czasie biznesowo krytycznych wydarzeń),
   5) Wsparcie on-site w przypadku braku możliwości rozwiązania problemu zdalnie.
   6) usługi asysty technicznej muszą być realizowane przez inżyniera posiadającego Certyfikat z oficjalnej ścieżki producenta dostarczonego systemu na poziomie eksperckim.
4. Usługi asysty technicznej Wykonawca zobowiązuje się realizować w dwóch formach:
   a) w siedzibie Zamawiającego przez pracowników Wykonawcy na podstawie pisemnego zlecenia Zamawiającego określającego zakres oraz termin wykonania tych usług, uzgodnionych wcześniej z Wykonawcą. Usługi te będą świadczone, przez liczbę godzin wskazanych w zleceniu,

b) zdalnie przez pracowników Wykonawcy na podstawie pisemnego zlecenia Zamawiającego określającego zakres oraz termin wykonania tych usług, uzgodnionych wcześniej z Wykonawcą. Usługi te będą świadczone, przez określoną liczbę godzin w danym dniu. Wykonawca udostępni narzędzie umożliwiające zdalną komunikację, które w uzgodnieniu z Zamawiającym zostanie uruchomione na stacji roboczej pracownika Zamawiającego.

5. Po wykonaniu usług Wykonawca przedłoży Zamawiającemu protokół z wykonania usług asysty zawierający ich rodzaj, zakres oraz termin.
6. Maksymalna liczba roboczogodzin w trakcie trwania umowy wskazana jest w Formularzu Ofertowym.
7. Zamawiający zastrzega sobie prawo do nie udzielania zleceń na usługi asysty technicznej.

XI. MINIMALNE WYMAGANIA w zakresie gwarancji

Gwarancja dla oferowanego Systemu NGFW, w tym urządzeń i oprogramowania musi spełniać niżej opisane wymagania:

1. Minimalny okres gwarancji na urządzenia i oprogramowanie wynosi – 36 miesięcy.
2. Zamawiający wymaga, aby usługa gwarancyjna na wszystkie dostarczone w ramach zamówienia sprzęt była, przez cały okres jej trwania, świadczona na podstawie wykupionego wsparcia producenta dostarczonych urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta dostarczanego urządzeń i był jego autoryzowanym dostawcą.
3. Wszystkie urządzenia dostarczone i zastosowane przez Wykonawcę będą pochodziły z autoryzowanego kanału sprzedaży producentów Urządzeń na rynek polski lub Unii Europejskiej. Spełnienie powyższego wymogu zostanie potwierdzone oświadczeniem producenta Urządzeń lub jego polskiego przedstawicielstwa, które Wykonawca zobowiązuje się dostarczyć Zamawiającemu najpóźniej w dniu dostawy oferowanych Urządzeń.
4. Gwarancja będzie liczona od daty odbioru przedmiotu umowy i oparta na gwarancji producentów rozwiązania zgodnie z terminami obowiązywania wymaganymi w OPZ. Serwis gwarancyjny świadczony ma być w miejscu instalacji Sprzętów.
5. Gwarancja ma być świadczona w reżimie 8x5xNBD. Czas naprawy Awarii liczony jest od czasu przesłania zgłoszenia o awarii do Wykonawcy zgodnie z procedurą przyjmowania zgłoszeń serwisowych.
6. Zamawiający wymaga by serwis gwarancyjny był autoryzowany przez producenta urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części oryginalne zgodnie z metodyką i zaleceniami producenta.
7. Zamawiający dopuszcza świadczenie serwisu dla dostarczonych urządzeń Systemu NGFW poprzez zastosowanie zamienników wskazanych przez producenta tylko i wyłącznie w przypadku, gdy takiego wsparcia u producenta nie da się wykupić (np. produkty zostały wycofane przez producenta bez możliwości świadczenia serwisu).
8. W przypadku, gdy w okresie gwarancyjnym nastąpi trzykrotna naprawa wadliwego podzespołu lub jedna jego istotna naprawa (rozumiana jako naprawa o wartości przekraczającej 30% wartości naprawianego elementu) Wykonawca niezwłocznie tj. w terminie nie dłuższym niż 14 dni liczonych od dnia zgłoszenia awarii, dokona jego wymiany na sprzęt nowy, wolny od wad. Na czas potrzebny do wymiany podzespołu wykonawca dostarczy element zastępczy o parametrach tożsamych z podzespołem uszkodzonym.
9. Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub www) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych urządzeń w godzinach pracy Zamawiającego.
10. Zamawiający zastrzega sobie prawo do dodawania nowych modułów oraz wymiany zainstalowanych modułów samodzielnie lub z pomocą Wykonawcy, w zakresie przewidzianym przez producenta Urządzenia, bez utraty gwarancji na zakupione Urządzenia. Zamawiający będzie dokonywał wymiany modułów samodzielnie po wcześniejszym uzgodnieniu z Wykonawcą. W przypadku nieprawidłowego lub niezgodnego z zaleceniami Wykonawcy i producenta Urządzenia dodania modułów lub wymiany zainstalowanych modułów przez Zamawiającego Wykonawca nie jest obciążony gwarancją i rękojmią w tym zakresie.
11. W okresie gwarancji Wykonawca w ramach otrzymanego wynagrodzenia udostępni Zamawiającemu możliwość wielokrotnego uaktualniania całego dostarczonego Oprogramowania

do najnowszych wersji oferowanych przez producenta (włączając tzw. firmware) oraz patche i programy korekcji błędów, a także dostęp do usług wsparcia technicznego producenta właściwy dla danego Urządzenia lub Oprogramowania. W przypadku, gdy dostęp taki wymaga podania nazwy użytkownika, hasła lub numeru seryjnego Wykonawca dostarczy Zamawiającemu ww. przed podpisaniem protokołu odbioru Urządzeń.

12. W przypadku konieczności naprawy Urządzenia lub Oprogramowania poza Lokalizacją, Wykonawca pokrywa koszty transportu i ponosi ryzyko uszkodzenia lub przypadkowej utraty urządzenia lub oprogramowania Standardowego w przypadku konieczności naprawy poza siedzibą Zamawiającego.
13. Na okres przedłużającej się naprawy Wykonawca może stosować procedury zastępcze. Czas trwania procedur zastępczych nie może być dłuższy niż 45 dni kalendarzowe od chwili zgłoszenia awarii.
14. Przez usunięcie Awarii należy rozumieć przywrócenie pierwotnej funkcjonalności Systemu we wszystkich modułach i zaprzestanie stosowania w bieżącej prac rezerwowego Urządzenia i/lub procedur zastępczych.
15. Po usunięciu każdej Awarii, Wykonawca zobowiązuje się do doprowadzenia całego systemu do stanu integralnej całości w rozumieniu poprawnego działania wszystkich zainstalowanych komponentów.
16. W ramach gwarancji dla dostarczonego Systemu NGFW Wykonawca zapewni Zamawiającemu prawo do aktualizacji oprogramowania Systemu do najnowszych wersji dostępnych w trakcie użytkowania systemu w okresie 36 miesięcy od daty odbioru wdrożenia systemu NGFW.
17. W ramach gwarancji Zamawiający będzie miał prawo przez okres 36 miesięcy do:
    a) pobierania i instalowania nowych wersji oprogramowania, wchodzącego w skład Systemu NGFW,
    b) Dostępu do bazy wiedzy oraz dokumentacji komponentów Systemu,
    c) Dostępu do powiadomień/ogłoszeń/alarmów w zakresie komponentów Systemu,
    d) Zgłaszania nieograniczonej liczby awarii systemu w trybie 24x365x7 za pomocą dedykowanego portalu i/lub zgłoszenia telefonicznego,
    e) Wymiany uszkodzonych/wadliwych komponentów systemu w trybie NDB (Next-Bussines Day),
18. Czasy reakcji/naprawy na zgłoszenie będą na poziomie:
    a) 1 godzina/8 godzin - błąd krytyczny – tj. przerwa w działaniu usług w środowisku produkcyjnym, brak dostępnego obejścia problemu,
    b) 2 godziny/2 dni - błędy wysokie – tj. problem z poprawnym działaniem usługi znacząco utrudniający realizację procesów biznesowych, brak dostępnego obejścia problemu,
    c) 4 godziny/7 dni - błędy średnie - tj. problem z poprawnym działaniem usługi, utrudnienie realizacji procesów biznesowych, dostępne obejście problemu,
    d) 8 godzin/14 dni - błędy niskie – tj. problem z poprawnym działaniem usługi, brak wpływu na realizację procesów biznesowych.
19. Wykonawca do dostarczonych urządzeń, będących przedmiotem zamówienia, dołączy karty gwarancyjne zawierające numer seryjny, termin i warunki ważności gwarancji, adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjnej.
20. Wykonawca w terminie 7 dni od zawarcia Umowy dostarczy Zamawiającemu procedury zgłaszania i obsługi Awarii wraz z listą osób upoważnionych do kontaktów, wykazem adresów poczty elektronicznej i nr telefonów.
21. Wykonawca, najpóźniej w dniu zawarcia Umowy, przedstawi do akceptacji Zamawiającemu listę osób uprawnionych do wykonywania czynności serwisowych.
22. W okresie gwarancji Wykonawca ponosi odpowiedzialność za poprawne funkcjonowanie urządzeń i oprogramowania stanowiącego przedmiot zamówienia, z zastrzeżeniem, że Wykonawca nie ponosi odpowiedzialności za uszkodzenia urządzeń i oprogramowania powstałych z wyłącznej winy Zamawiającego lub osób trzecich działających w jego imieniu.

23. Wymagany tryb zgłaszania wszelkich awarii, wad i błędów. Zgłoszenie następuje w drodze pisemnej mailem na adres podany przez Wykonawcę lub za pośrednictwem telefonicznego zgłaszania awarii, wad i błędów dotyczących sprzętu i oprogramowania w dni robocze w godzinach 8:00-17:00.
24. Obsługa zgłoszeń w języku polskim.