Załącznik nr 1 do Umowy nr [●]

– Opis przedmiotu zamówienia (OPZ)

**Opis przedmiotu zamówienia**

**cz. II – urządzenia sieciowe F5 do ośrodka zapasowego**

1. **Wstęp**

Zamawiający posiada i wykorzystuje w swojej infrastrukturze IT dedykowane rozwiązania w postaci urządzeń sieciowych o funkcjonalności load balancera, polegającej na równoważeniu obciążeń i rozdzielaniu ruchu pomiędzy aplikacje/serwery w celu optymalizacji wydajności, efektywności i przepustowości infrastruktury wraz z oprogramowaniem o funkcjonalności WAF oraz firewall firmy F5. Zamawiający do celów zarządzania oraz monitorowania posiadaną infrastrukturą wykorzystuje również rozwiązanie BIG-IQ firmy F5.

Przedmiotem zamówienia jest dostawa i uruchomienie rozwiązania klasy load balancer współpracujących z obecną infrastrukturą sieciowo / serwerowo / aplikacyjną Zamawiającego w celu rozbudowy środowiska na potrzeby budowy połączeń między ośrodkowych oraz wewnątrz ośrodkowych w centrach przetwarzania danych Ministerstwa Sprawiedliwości. Celem jest budowa jednej domeny zarządzania oraz monitorowania w ramach całej posiadanej infrastruktury load balancerów Zamawiającego.

1. **Przedmiot zamówienia** 
   1. Przedmiotem zamówienia jest:
      1. dostawa 2 szt. urządzeń klasy load balancer zgodnych z wymaganiami opisanymi w pkt 10 wraz z modułami optycznymi (dalej „Urządzenia”) oraz dedykowanego oprogramowania zgodnego z wymogami opisanymi w pkt 10 (dalej „Oprogramowanie”), wraz ze wsparciem producenta tego Oprogramowania, w ramach rozbudowy infrastruktury sieciowej Ministerstwa Sprawiedliwości , co obejmuje ich rozmieszczenie i instalację, w tym czynności, o których mowa w pkt 2.8;
      2. zorganizowanie i przeprowadzenie warsztatów opisanych w pkt 8;
      3. świadczenie usług asysty technicznej opisanych w pkt 7.
   2. Urządzenia muszą pochodzić z oficjalnego kanału sprzedaży ich producenta.
   3. Urządzenia muszą być fabrycznie nowe tj. nieużywane i wyprodukowane nie wcześniej niż 6 miesięcy przed terminem dostawy, kompletne, wolne od wad, bez śladów używania i bez uszkodzeń.
   4. Urządzenia muszą być oryginalne, przy czym pod pojęciem oryginalny należy rozumieć sprzęt dopuszczony do obrotu na terenie Rzeczpospolitej Polskiej, wprowadzony na rynek zgodnie z przepisami Ustawy o zużytym sprzęcie elektrycznym i elektronicznym z dnia 11 września 2015 r., posiadający wymagane prawem deklaracje zgodności, jak również instrukcje obsługi w języku polskim lub języku angielskim.
   5. W chwili dostarczenia (do czasu rozpakowania na potrzeby montażu), Urządzenia muszą znajdować się w opakowaniach fabrycznych zabezpieczających przed uszkodzeniem w trakcie transportu i składowania, posiadać zabezpieczenia (o ile zostały zastosowane przez producenta), oznaczenie CE oraz znaki identyfikujące Urządzenia, a w szczególności znak towarowy lub markę producenta Urządzeń.
   6. *celowo pominięto*
   7. Wykonawca zapewni, aby Urządzenia oraz sposób ich montażu, spełniały wymogi bezpieczeństwa określone przez przepisy Unii Europejskiej dotyczące bezpieczeństwa określonego produktu (Conformité Européenne) oraz szczegółowe wymagania dotyczące bezpieczeństwa produktu określone przepisami polskimi, a w przypadku ich braku, wymogi dobrowolnych norm krajowych państw UE innych niż normy uznane przez KE, Polskich Norm, zaleceń KE, zasad dobrej praktyki w zakresie bezpieczeństwa produktu obowiązujących w danym sektorze, aktualnego stanu wiedzy i techniki lub uzasadnionych oczekiwań użytkowników w zakresie bezpieczeństwa.
   8. W ramach dostawy Urządzeń, Wykonawca:
      1. opracuje projekt wdrożenia, zawierający co najmniej:
         1. diagramy połączeniowe Urządzeń z poszczególnymi komponentami istniejącej infrastruktury;
         2. opis konfiguracji dla dostarczanego Urządzenia;
         3. opis zmian w konfiguracji komponentów istniejącej infrastruktury;
         4. harmonogram prac (montażu i wdrożenia);
         5. koncepcję testów w ramach poszczególnych kroków powdrożeniowych;
         6. plan awaryjny tj. na wypadek niepowodzenia (ang. roll-back) dla każdego z kroków wdrożenia;
      2. dostarczy Urządzenie oraz wykona montaż (instalację fizyczną) Urządzeń w szafie RACK we wskazanej lokalizacji zgodnie z ustaleniami w trybie roboczym z Zamawiającym po podpisaniu Umowy;
      3. uruchomi je w porozumieniu z Zamawiającym, przy czym ewentualne przerwy w działaniu infrastruktury muszą zostać zaakceptowane przez Zamawiającego;
      4. uruchomi Urządzenia w porozumieniu z Zamawiającym w infrastrukturze Zamawiającego w tym aktywuje Oprogramowanie, podłączy Urządzenia do systemu zarządzania i monitorowania Zamawiającego, przeprowadzi testy wymagane projektem wdrożenia, aż do ich pozytywnego zakończenia;
      5. opracuje dokumentację powdrożeniową opisaną w pkt 9, zawierającą co najmniej:
         1. diagramy połączeń;
         2. opis funkcjonalności wdrożonych podczas uruchamiania urządzeń w infrastrukturze Zamawiającego;
         3. opis konfiguracji i pozostałych komponentów infrastruktury po rozbudowie;
         4. wyników testów;
      6. obsadzi wszystkie porty strony klienckiej wkładkami zgodnymi z wymaganiami producenta umożliwiającymi podłączenie z wykorzystaniem kabli światłowodowych ze złączem LC lub MPO oraz umożliwiających podłączenie infrastruktury sieciowej.
   9. Prace, o których mowa w pkt 2.8, muszą zostać przeprowadzone zgodnie z zasadami sztuki, zgodnie z wytycznymi wynikającymi z zawartych przez Zamawiającego umów serwisowych dotyczących eksploatowanego sprzętu, a przy tym w sposób bezpieczny, niezagrażający utracie danych i gwarantujący nieprzerwane funkcjonowanie infrastruktury (nieustanna praca w trybie biznesowym – etapowość prowadzonych prac). Dokładny przebieg realizacji tych zadań wymaga uzgodnienia z Zamawiającym.
   10. Montaż (instalacja fizyczna), uruchomienie i konfiguracja muszą zostać wykonane zgodnie z rekomendacjami producenta, a przy tym bez wpływu na działające środowiska i bez powodowania jakichkolwiek przerw czy opóźnień w dostępie do danych.
   11. Wszystkie elementy dodatkowe wymagane do montażu (instalacji fizycznej) Urządzenia (śrubki, kable, wkładki itp.) oraz do ich uruchomienia, konfiguracji poszczególnych komponentów muszą zostać dostarczone przez Wykonawcę w ramach przedmiotowego zamówienia.
   12. Wszelkie (np. trwale uszkodzone) nośniki danych w przypadku konieczności wymiany pozostaną w miejscu realizacji zamówienia we właściwości Zamawiającego.
   13. Wykonawca traktowany jest jako wytwórca odpadów powstałych w toku realizacji zamówienia i utylizuje je na własny koszt i ryzyko, zgodnie z właściwymi przepisami.
   14. Wytyczne i rekomendacje, o których mowa w pkt 2.9 i 2.10 zostaną przekazane Wykonawcy w trybie roboczym (w toku realizacji zamówienia).
   15. Stanowiące przedmiot dostawy (udzielenie, względnie zapewnienie udzielenia) licencje na Oprogramowanie wraz ze wsparciem producenta Oprogramowania, zostaną udzielone na okres poczynając nie później niż od daty uruchomienia Urządzenia w infrastrukturze Zamawiającego.
   16. Licencje na Oprogramowanie będą wieczyste (bezterminowe), niewyłączne, nieograniczone terytorialnie i zostaną udzielone zgodnie z warunkami licencyjnymi opublikowanymi przez producenta Oprogramowania, których aktualna treść dostępna jest na stronie internetowej, której adres Wykonawca wskaże Zamawiającemu nie później niż w dniu zawarcia Umowy, z tym zastrzeżeniem, że obejmą co najmniej następujące pola eksploatacji:
       1. prawo do instalowania Oprogramowania, na które udzielana jest licencja w liczbie kopii / stanowisk / serwerów / użytkowników charakterystycznej dla danego oprogramowania;
       2. prawo do korzystania ze wszystkich funkcjonalności Oprogramowania, na które udzielana jest licencja w dowolny sposób;
       3. prawo do aktualizowania Oprogramowania, na które udzielana jest licencja poprzez zamówienie i zainstalowanie nowszych wersji oprogramowania z zachowaniem wszystkich pól eksploatacji wymienionych w pkt 2.16.1 i 2.16.2 powyżej;
       4. prawo do instalowania wszelkich poprawek opublikowanych na stronach producenta Oprogramowania oraz na polach eksploatacji określonych w opublikowanych przez producenta Oprogramowania warunkach licencyjnych.

Licencje wieczyste oznaczają, że żadna ze Stron nie będzie mogła ich wypowiedzieć (pot. licencje dożywotnie). W razie zakwestionowania przez sąd skuteczności zrzeczenia się prawa do wypowiedzenia licencji, przyjmuje się, że licencje zostały udzielone na okres 10 lat z opcją automatycznego przedłużenia na kolejne 10 lat, o ile żadna ze Stron nie złoży oświadczenia na rok naprzód przed końcem danego 10-letniego obowiązywania licencji.

* 1. Wsparcie producenta będzie obowiązywać przez okres do upływu 48 miesięcy od daty protokolarnego odbioru dostawy Urządzeń bez zastrzeżeń Zamawiającego i obejmuje co najmniej:
     1. diagnostykę zdarzeń dotyczących Oprogramowania;
     2. dostarczanie rozwiązań błędów Oprogramowania;
     3. zapewnienie łat (ang. patches), tj. poprawek lub aktualizacji mających na celu usunięcie problemów, błędów, rozszerzenie funkcjonalności lub zwiększenie wydajności wcześniejszej wersji Oprogramowania;
     4. zapewnienie aktualizacji do nowych, wyższych wersji Oprogramowania (ang. upgrades);
     5. udzielanie odpowiedzi na zapytania związane z instalacją i eksploatacją dostarczonego Oprogramowania;
     6. dostęp do konta (profilu) utworzonego dla licencjobiorcy na stronie internetowej prowadzonej przez producenta Oprogramowania, zawierającego informacje dotyczące infrastruktury i oprogramowania sprzętowego i umożliwiającego dokonywanie zgłoszeń i zapytań w ramach wsparcia producenta Oprogramowania – o ile producent rozwiązania prowadzi taką stronę w powyżej przytoczonej formie.

1. **Termin realizacji dostawy** 
   1. Wykonawca dostarczy Urządzenia do lokalizacji Zamawiającego nie później niż 60 dni od dnia zawarcia Umowy.
   2. O planowanym terminie dostarczenia Urządzenia, Wykonawca poinformuje Zamawiającego z wyprzedzeniem co najmniej 7 dni.
   3. Projekt wdrożenia (pkt 2.8.1) musi zostać przedłożony Zamawiającemu do zatwierdzenia w ciągu 14 dni od dnia zawarcia Umowy. Wykonawca uwzględni ewentualne uwagi do projektu wdrożenia w ciągu 5 dni od ich zgłoszenia przez Zamawiającego.
   4. Czynności, o których mowa w pkt 2.8.2-2.8.4, muszą zostać wykonane zgodnie z projektem wdrożenia w ciągu 15 dni od dnia dostarczenia Urządzenia, w godzinach 8 – 16, natomiast uruchomienie powinno odbywać się po godzinach pracy urzędu lub w czasie wyznaczonych okien serwisowych, chyba że ustalono inaczej z Zamawiającym.
   5. Dokumentacja powdrożeniowa (pkt 2.8.5) zostanie opracowana i dostarczona Zamawiającemu nie później niż w ciągu 14 dni od daty zakończenia montażu Urządzenia, uruchomienia i dokonania wdrożenia oraz zakończenia testów wymaganych projektem wdrożenia, potwierdzonych pozytywną weryfikacją przez Zamawiającego, w oryginale (2 egz.) oraz w postaci elektronicznej (plik .doc lub .docx), wraz z wygenerowanymi w postaci elektronicznej wynikami testów przełączania i ich wydrukami – uwzględniając wymagania pkt 9 .
   6. W terminie do 5 dni od rozpoczęcia terminu obowiązywania licencji na Oprogramowanie wraz ze wsparciem producenta Oprogramowania, o którym mowa w pkt 2.15, Wykonawca dostarczy Zamawiającemu (i) wystawione przez producenta Urządzeń instrukcje ich użytkowania, atesty, deklaracje zgodności, itp., (ii) instrukcje oraz dane dostępowe (loginy i hasła), o których mowa w pkt. 6.8 OPZ, (iii) wystawione przez producenta Oprogramowania dokumenty w postaci elektronicznej, potwierdzające udzielenie licencjobiorcy licencji na Oprogramowanie wraz ze wsparciem producenta Oprogramowania, pocztą elektroniczną na adres [licencje@ms.gov.pl](mailto:licencje@ms.gov.pl) oraz [zs@ms.gov.pl](mailto:zs@ms.gov.pl). Wykonanie zobowiązania, o którym mowa w zdaniu poprzedzającym, może polegać na udostępnieniu stosownych informacji lub dokumentów (plików) na koncie (profilu) utworzonym dla licencjobiorcy na stronie internetowej prowadzonej przez producenta Oprogramowania.
2. **Miejsce realizacji dostawy:** 
   1. Miejscem realizacji dostawy Urządzeń jest obiekt, w którym zlokalizowana jest infrastruktura IT Ministerstwa Sprawiedliwości na terenie miasta stołecznego Warszawy – adres tej lokalizacji zostanie podany po zawarciu Umowy.
   2. Zamawiający zastrzega sobie możliwość zmiany miejsca realizacji dostawy na inną lokalizację w granicach województwa mazowieckiego, za zawiadomieniem Wykonawcy w formie pisemnej lub w formie elektronicznej z wyprzedzeniem co najmniej 10 dni.
   3. Zamawiający zastrzega sobie prawo do przeniesienia Urządzeń do innej lokalizacji, bez utraty uprawnień wynikających z gwarancji i rękojmi.
   4. Naprawy Urządzeń w ramach gwarancji i rękojmi, będą dokonywane w miejscu ich eksploatacji, wynikającym z pkt 4.1-4.2. W przypadku niemożności dokonania naprawy w miejscu eksploatacji Urządzeń, Wykonawca na swój koszt i ryzyko zapewnia dostarczenie i odbiór Urządzenia do/z autoryzowanego punktu serwisowego.
3. **Sposób realizacji dostawy** 
   1. Dostawa Urządzeń lub ich wymiana serwisowa, obejmuje każdorazowo również transport z wniesieniem oraz montaż (instalację fizyczną), uruchomienie i konfigurację w lokalizacji.
   2. Dokumentacja zostanie sporządzona w języku polskim.
   3. Komunikacja, warsztaty oraz wszelka korespondencja pomiędzy Stronami będzie odbywała się w języku polskim.
   4. W ramach realizacji zamówienia, Wykonawca przeniesie na Zamawiającego prawa autorskie majątkowe do dostarczonych lub wytworzonych utworów w zakresie wskazanym w § 8 Umowie.
4. **Serwis gwarancyjny**
   1. Wykonawca udzieli Zamawiającemu rękojmi za wady dostarczonych rzeczy, usług i dzieła (utworów) oraz gwarancji na prawidłowe działanie Urządzeń i Oprogramowania, co do ich jakości oraz zgodności z dokumentacją techniczną i dokumentacją powdrożeniową, stosownie do § 9 Umowy.
   2. Wykonawca opracuje i przekaże Zamawiającemu nie później niż w dniu podpisania protokołu odbioru przedmiotu zamówienia (dostawy), w formie pisemnej i w postaci elektronicznej, dokument pt. „Instrukcja zgłaszania, obsługi i eskalacji zgłoszeń serwisu gwarancyjnego”, zawierający:
      1. instrukcje zgłaszania awarii, w tym formularz – Zgłoszenia gwarancyjnego;
      2. procedury eskalacyjne (pod pojęciem procedury eskalacji Zamawiający rozumie tryb postępowania stron w sytuacji braku realizacji zgłoszenia lub reakcji na zgłoszenie);
      3. dane podmiotu świadczącego usługi gwarancyjne – adresy, numery telefonów i faksów, adresy poczty elektronicznej;
      4. instrukcje dotyczące przeglądania statusu Umowy oraz urządzeń nią objętych;
      5. wzór Raportu z naprawy urządzenia.

Instrukcje i procedury, o których mowa powyżej, nie mogą być sprzeczne lub niezgodne z postanowieniami Umowy. Zmiana dokumentów wymienionych w niniejszym punkcie wymaga powiadomienia Zamawiającego w formie pisemnej albo w formie elektronicznej. Wykonawca zobowiązuje się wdrożyć i stosować przez cały okres obowiązywania Umowy powyższe procedury i instrukcje. Przekazane przez Wykonawcę procedury i instrukcje podlegają akceptacji Zamawiającego. Zamawiający może zgłosić uwagi i poprawki do instrukcji i procedur przekazanych przez Wykonawcę, a Wykonawca jest zobowiązany do ich uwzględnienia i przedstawienia do ponownej akceptacji przez Zamawiającego.

* 1. Zgłoszenie awarii objętych gwarancją może być dokonywane w postaci: zgłoszenia telefonicznego, za pomocą faksu, z wykorzystaniem serwisu www udostępnionego przez Wykonawcę, za pomocą poczty elektronicznej oraz zgłoszeń generowanych automatycznie na koncie (profilu) producenta Urządzeń.
  2. Wykonawca będzie przyjmował zgłoszenia awarii całodobowo (24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku).
  3. Konsultacje techniczne w ramach serwisu gwarancyjnego mogą być przeprowadzane pomiędzy Wykonawcą a Zamawiającym osobiście, telefonicznie lub za pomocą poczty elektronicznej.
  4. Wykonawca jest zobowiązany do potwierdzenia przyjęcia zgłoszenia awarii (lub konsultacji technicznych) w terminie do 60 minut od jego zgłoszenia na adres poczty elektronicznej [popd@ms.gov.pl](mailto:popd@ms.gov.pl) lub telefonicznie – na numer podany podczas rejestracji zgłoszenia, niezwłocznie przesyłając potwierdzenie mailem na powyższy adres mailowy, przy czym za chwilę potwierdzenia przyjęcia zgłoszenia uważa się moment potwierdzenia telefonicznego. W przypadku braku potwierdzenia, po upływie 60 minut od zgłoszenia awarii przez Zamawiającego, Zamawiający wdroży procedurę eskalacji zgłoszenia, o której mowa w pkt. 6.7.
  5. Wykonawca zobowiązany jest do zapewnienia procedury eskalacyjnych zgłoszeń zawierających co najmniej dodatkowe dwa numery telefonów. Pod pojęciem procedury eskalacji Zamawiający rozumie tryb postępowania stron w sytuacji braku realizacji zgłoszenia lub reakcji na zgłoszenie, na zasadach określonych w procedurze eskalacji zgłoszenia, o której mowa w pkt. 6.6.
  6. Wykonawca zobowiązany jest do zapewnienia Zamawiającemu możliwości bieżącego śledzenia statusu zgłoszenia za pośrednictwem co najmniej strony www – Wykonawca przekaże Zamawiającemu login i hasło.
  7. Wykonawca zapewni Zamawiającemu dostęp do monitorowania statusu zgłoszeń gwarancyjnych na koncie (profilu), o którym mowa w pkt 2.16.6.
  8. Zamawiający wymaga zapewnienia ciągłości obsługi w ramach serwisu gwarancyjnego.
  9. Zgłoszenia awarii będą realizowane w następujący sposób:
     1. Zgłoszenie o priorytecie krytycznym tj. nieprawidłowe działanie urządzenia, powodujące albo całkowity brak możliwości korzystania z infrastruktury Ministerstwa Sprawiedliwości albo takie ograniczenie możliwości korzystania z infrastruktury Ministerstwa Sprawiedliwości, że przestaje ona spełniać swoje podstawowe funkcje – czas reakcji do 4 godzin serwisowych od chwili zgłoszenia, czas przywrócenia funkcjonalności do [●] godzin serwisowych od chwili zgłoszenia (zgodnie z ofertą Wykonawcy, nie dłużej jednak niż do 12 godzin serwisowych).
     2. Zgłoszenie o priorytecie niekrytycznym tj. inne niż krytyczne, np. zmniejszenie wydajności infrastruktury Ministerstwa Sprawiedliwości – czas reakcji nie później niż w następnym dniu roboczym od dnia zgłoszenia, czas przywrócenia funkcjonalności do 72 godzin serwisowych od chwili zgłoszenia.
  10. Wykonawca zobowiązany jest do realizowania czasów reakcji i napraw w następujących przedziałach czasu (godziny serwisowe):
      1. Zgłoszenia o priorytecie krytycznym w trybie non-stop, nie wyłączając dni ustawowo wolnych od pracy;
      2. Zgłoszenia o priorytecie niekrytycznym między godziną 7 a 17 od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy.
  11. W przypadku, gdy Wykonawca nie wykona obowiązku wynikającego z pkt. 6.11:
      1. Zamawiający ma prawo wypożyczyć, zainstalować i uruchomić na koszt Wykonawcy u dowolnego innego dostawcy urządzenie zastępcze, zachowując jednocześnie prawo do kary umownej i odszkodowania.
      2. Zamawiający ma prawo zlecić dowolnemu innemu dostawcy naprawę urządzenia, a kosztami naprawy obciążyć Wykonawcę zachowując jednocześnie prawo do kary umownej i odszkodowania.
  12. W przypadku wystąpienia okoliczności opisanych w pkt 6.13.1 lub 6.13.2 Zamawiający nie traci prawa do gwarancji.
  13. W ramach usunięcia awarii urządzenia, Zamawiający dopuszcza możliwość wymiany przez Wykonawcę po uzgodnieniu z Zamawiającym poszczególnych elementów i podzespołów Urządzenia lub całego Urządzenia na nowe takie samo lub inne, o co najmniej takich samych parametrach, funkcjonalności i standardzie.
  14. W przypadku, gdy z uwagi na awarię urządzenia Wykonawca zapewnił sprzęt zastępczy, a naprawa dotkniętego awarią sprzętu trwa dłużej niż 6 tygodni lub gdy ten sam element/podzespół/część będzie naprawiany trzykrotnie w okresie gwarancyjnym i nastąpi kolejna (czwarta) awaria, Zamawiający może żądać od Wykonawcy wymiany sprzętu na nowy, taki sam lub inny, uzgodniony z Zamawiającym, w terminie 30 dni od zgłoszenie takiego żądania przez Zamawiającego, o co najmniej takich samych parametrach, funkcjonalności i standardzie. Dostarczony w ramach wymiany sprzęt musi być fabrycznie nowy tj. wyprodukowany nie wcześniej niż 6 miesięcy przed wymianą, wolny od wad, bez śladów używania i bez uszkodzeń, wprowadzone na rynek zgodnie z przepisami Ustawy o zużytym sprzęcie elektrycznym i elektronicznym z dnia 11 września 2015 r., dostarczony Zamawiającemu w oryginalnych opakowaniach fabrycznych, zabezpieczających przed uszkodzeniem w trakcie transportu i składowania. W przypadku wymiany sprzętu na nowy, Wykonawca sporządzi protokół z wymiany.
  15. Wykonawca każdorazowo dostarczy Zamawiającemu sprawozdanie (raport) z naprawy, zawierający datę i godzinę zgłoszenia, informację co było przedmiotem naprawy. W przypadku przekroczenia limitów czasu usunięcia awarii, wynikających z pkt. 6.11, Wykonawca uwzględni w rzeczonym raporcie stosowne informacje w tym względzie.
  16. W okresie trwania gwarancji i rękojmi, Zamawiający ma prawo do instalowania, wymiany standardowych kart rozszerzeń/modułów i podzespołów (np. modułów optycznych itp.) oraz rozbudowy poszczególnych sprzętów/urządzeń oraz instalacji pobranych poprawek, aktualizacji, oprogramowania narzędziowego i nowych wersji systemu operacyjnego sprzętów/urządzeń (firmware) zgodnie z zasadami sztuki w tym zakresie przez wykwalifikowany personel Zamawiającego lub podmiotu zewnętrznego, któremu zleci te prace Zamawiający.
  17. W przypadku awarii powodującej konieczność wymiany nośnika danych, uszkodzone nośniki pozostają w gestii Zamawiającego.

1. **Usługi asysty technicznej**
   1. Wykonawca zapewni usługi asysty technicznej dla infrastruktury sieciowej Zamawiającego rozbudowanej o Urządzenia, w zakresie m.in.:
      1. konfiguracji sprzętowo-systemowej;
      2. zarządzania;
      3. rozwiązywania problemów eksploatacyjnych;
      4. konsultacji technicznych;
      5. asysty przy planowych przerwach w działaniu infrastruktury;
      6. asysty niezbędnej z uwagi na przerwy w działaniu infrastruktury, powodowane awarią, incydentem bezpieczeństwa, względnie innymi zdarzeniami losowymi.
   2. Usługi asysty technicznej nie obejmują czynności serwisowych ani innych świadczeń należnych się Zamawiającemu tytułem rękojmi lub gwarancji.
   3. Usługi asysty technicznej świadczone będą na warunkach określonych w Umowie oraz w poszczególnych zleceniach, po uzyskaniu wzajemnej akceptacji zgodnie z procedurą opisaną w pkt 7.8 i 7.9 poniżej, z zastrzeżeniem pkt. 7.10-7.12 poniżej. Usługi asysty technicznej świadczone będą w miejscu eksploatacji Urządzeń (patrz pkt. 4.1-4.3), względnie – po uzgodnieniu z Zamawiającym – zdalnie, z zastrzeżeniem pkt. 7.12.
   4. Termin realizacji usług asysty technicznej obejmuje do upływu 48 miesięcy od dnia zawarcia Umowy, z tym, że nie dłużej niż do wyczerpania puli wynoszącej 1000 roboczogodzin. W rzeczonym okresie, Zamawiający może składać Wykonawcy zlecenia, a Wykonawca zobowiązany jest takie zlecenia przyjąć do realizacji na zasadach opisanych w pkt. 7.8 i 7.9, oraz świadczyć w tym okresie usługi asysty technicznej w razie przerw w działaniu infrastruktury (ppkt. 7.1.5 i 7.1.6). Szczegółowe terminy realizacji poszczególnych zleceń w ramach usług asysty technicznej wynikać będą z treści danego zlecenia, bez uszczerbku dla pkt 7.10 i 7.11.
   5. Deklarowany przez Zamawiającego minimalny wymiar roboczogodzin do wykorzystania w okresie świadczenia usług asysty technicznej wynosi 30 (trzydzieści) roboczogodzin.
   6. Usługi asysty technicznej rozliczane będą w cyklu miesięcznym (okresem rozliczeniowym jest miesiąc kalendarzowy).
   7. Przy rozliczaniu czasu świadczenia usługi asysty technicznej nie ma znaczenia liczba osób wykonujących jednocześnie czynności wymagane/niezbędne dla należytego i sprawnego wykonania zadań / czynności powierzonych Wykonawcy do realizacji w ramach danej usługi asysty technicznej nie uwzględnia się czasu przeznaczonego przez te osoby na dojazd ani nocleg, itd.
   8. Z zastrzeżeniem postanowień pkt. 7.10-7.11 poniżej, Zamawiający będzie składał Wykonawcy zapytania, w których zawrze zakres usług (specyfikację czynności / zadań do wykonania), wraz z proponowanym terminem ich realizacji. W odpowiedzi na zapytanie, Wykonawca nie później niż w ciągu kolejnych 3 dni roboczych przedstawi szacowany nakład roboczogodzin oraz potwierdzi albo wskaże inne warunki zlecenia, w tym termin realizacji zlecenia. W odpowiedzi na tak złożoną propozycję, Zamawiający podpisze zlecenie, względnie zakwestionuje zaproponowane warunki realizacji zlecenia, zwracając się do Wykonawcy o stosowne wyjaśnienia. W przypadku rozbieżności między Stronami co do szacowanego nakładu godzinowego lub innych warunków realizacji zlecenia zaproponowanych przez Wykonawcę, Zamawiający zastrzega sobie prawo do powołania eksperta (podmiot lub jednostka organizacyjna biegła w usługach IT, a niezależna od dostawców usług IT), w celu rozstrzygnięcia sporu. Ustalenia tak powołanego eksperta będą ostatecznie wiążące dla Stron, przy czym w przypadku potwierdzenia stanowiska Zamawiającego, Wykonawca zwróci Zamawiającemu koszty i wydatki związane z powołaniem eksperta na jego pierwsze żądanie. Poza tym, jeżeli w wyniku ustaleń eksperta okaże się, że nakład godzinowy został przez Wykonawcę przeszacowany o co najmniej 30%, przyjmuje się, że to Wykonawca ponosi odpowiedzialność za opóźnienie w podpisaniu zlecenia (zwłoka Wykonawcy). Nie dotyczy to asysty technicznej, o której mowa w ppkt. 6.1.6 i ppkt. 6.1.7, które Wykonawca zobowiązany jest realizować na podstawie samego zgłoszenia przez Zamawiającego.
   9. Podstawą przyjęcia zlecenia do realizacji (świadczenia usług objętych zleceniem) będzie obustronne podpisanie w formie pisemnej albo w formie elektronicznej zlecenia, którego wzór określa Załącznik nr 7 do Umowy, przy czym Wykonawca zobowiązany jest podpisać zlecenie w ciągu 2 dni roboczych od otrzymania egzemplarza zlecenia podpisanego przez Zamawiającego, bez uszczerbku dla postanowień pkt. 7.10-7.12 poniżej.
   10. Asysta techniczna przy planowych przerwach w działaniu infrastruktury Ministerstwa realizowana będzie w miejscu ich eksploatacji, wynikającym z pkt 4.1-4.3 (ppkt. 7.1.5) i nie wymaga zlecenia. Wykonawca zostanie powiadomiony o planowanym wyłączeniu / włączeniu infrastruktury w miarę możliwości z wyprzedzeniem co najmniej 48 godzin.
   11. Asysta techniczna przy nieplanowanych przerwach w działaniu infrastruktury realizowana będzie w miejscu ich eksploatacji, wynikającym z pkt 4.1-4.3 (ppkt. 7.1.6) nie wymaga zlecenia.
   12. Asysta techniczna, o której mowa w pkt 7.10 i 7.11 może być realizowana w trybie zdalnym tylko w uzasadnionych przypadkach i dopiero po uzyskaniu zgody Zamawiającego. W takim przypadku, wyłączenie / włączenie urządzenia (bądź wybranych jego komponentów) przeprowadza Zamawiający przy wsparciu udzielanym przy użyciu środków porozumiewania się na odległość.
2. **Warsztaty** 
   1. Warsztaty muszą obejmować zagadnienia z następującego zakresu:
      1. Warsztaty **Typ I** – 3 dni szkoleniowe – zagadnienia uwierzytelniania i dostępu zdalnego:

* Konfigurowanie load balancera
* Dostęp do aplikacji w sieci Web
* Polityka dostępu
* Zarządzanie funkcjonalnościami APM rozwiązania
* Uwierzytelnianie
* Przypisywanie zasobów
* Dostęp do portalu
* Dostęp do sieci
* Macra i logowanie
* Kontrole po stronie klienta
* Kontrole po stronie serwera
* App Tunele
* Listy kontroli dostępu
* Pojedyncze logowanie (Single sign-on)
* Reguły zasad dostępu zaawansowanego
* SAML
* Webtop i Wizards
* Klient Edge BIP-IP
* Projekt konfiguracji
  + 1. Warsztaty **Typ II** – 4 dni szkoleniowe – ochrona aplikacji webowych;
* Ustawienie systemu w load balancerze z ochroną aplikacji
* Procesowanie ruchu w rozwiązaniu
* Pojęcia aplikacji sieci Web
* Luki w zabezpieczeniach aplikacji WWW
* Wdrożenie polityki bezpieczeństwa
* Dostrajanie reguł i naruszenia
* Sygnatury ataków
* Tworzenie pozytywnej polityki bezpieczeństwa
* Cookies i inne nagłówki
* Raportowanie i rejestrowanie
* Zaawansowana obsługa parametrów
* Porównywanie polityk i administracja
* Automatyczne budowanie polityki
* Integracja skanera podatności
* Korzystanie z polityk warstwowych
* Login Enforcement, Brute Force Mitigation oraz śledzenie sesji
* Web Scraping Mitigation and Geolocation Enforcement
* Ochrona przed atakami DoS w warstwie 7 oraz ochrona przed Botami
* F5 Adv. WAF i iRules
* Używanie profili zawartości
  1. Organizacja Warsztatów:
     1. Wykonawca przeprowadzi warsztaty w dwóch turach, jednocześnie dla 2 osób w każdej turze (tj. dla nie więcej niż 4 osób łącznie).
     2. Warsztaty dla jednej osoby muszą trwać odpowiednio dla Typ I co najmniej 24 godziny oraz dla Typ II co najmniej 32 godziny (tj. dla Typ I 3 kolejnych dni roboczych po 8 godzin i dla Typ II 4 kolejnych dni roboczych po 8 godzin). Termin przeprowadzenia warsztatów będzie podlegać akceptacji przez Zamawiającego.
     3. Wykonawca zobowiązany jest do przeprowadzenia warsztatów w terminie do 24 miesięcy od daty podpisania protokołu odbioru dostawy bez zastrzeżeń Zamawiającego. Termin przeprowadzenia każdej z tur warsztatów będzie podlegać akceptacji przez Zamawiającego.
     4. Wykonawca zobowiązany jest do przeprowadzenia warsztatów w lokalizacji na terenie Warszawy, z opcjonalnym udziałem on-line wybranych uczestników. Miejsce realizacji warsztatów będzie podlegać akceptacji przez Zamawiającego. Zastrzega się, że na 10 dni przed planowanym terminem danej tury warsztatów, Strony uzgodnią liczbę uczestników, którzy będą w niej uczestniczyć zdalnie.
     5. Każdy uczestnik otrzyma certyfikat jego ukończenia.
     6. Warsztaty muszą być prowadzone w języku polskim.
     7. Wykonawca musi dysponować odpowiednio wykwalifikowaną kadrą, której powierzy realizację przedmiotu zamówienia w zakresie warsztatów. Wymagane jest, aby trenerzy posiadali udokumentowane co najmniej 2-letnie doświadczenie w przedmiocie szkolenia z zakresu oferowanego rozwiązania.
     8. Wykonawca zobowiązuje się dysponować lub zapewnić na cele realizacji przedmiotu zamówienia bazą szkoleniową z odpowiednimi pomieszczeniami wraz z zapleczem do przeprowadzenia warsztatów dla osób dorosłych tj. sale dostosowane do prowadzenia zajęć, dobrze oświetlone (światło dzienne i sztuczne), wentylowane (z dostępem do świeżego powietrza), posiadające odpowiednie warunki sanitarne, bezpieczeństwa i higieny pracy, wyposażone w akustyczne i jakościowe narzędzia i urządzenia, a także oprogramowania i pomoce dydaktyczne niezbędne do wykonania zamówienia.
     9. Wykonawca w terminie do 30 dni od dnia podpisania protokołu odbioru dostawy bez zastrzeżeń Zamawiającego, przedstawi Zamawiającemu do akceptacji Program warsztatów. Program musi zawierać informacje dotyczące tematyki prowadzonych warsztatów z podziałem na zajęcia teoretyczne i praktyczne. Program musi zawierać również informacje dotyczące wiedzy i umiejętności jakie zdobędą uczestnicy po zakończeniu warsztatów.
     10. Wykonawca w uzgodnieniu z Zamawiającym przygotuje szczegółowe harmonogramy warsztatów – z rozpisaniem na dni i godziny i dostarczy je do 30 dni, od dnia podpisania protokołu odbioru dostawy bez zastrzeżeń Zamawiającego. Zamawiający zastrzega sobie możliwość korekty przedstawionych dokumentów. Harmonogram zajęć musi zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu.
     11. Zajęcia odbywać się będą w dni robocze od poniedziałku do piątku, w godzinach od 8:00 do 17.00, nie więcej niż 8 godzin zegarowych dziennie. Harmonogram i program muszą zostać wydrukowane i rozdane uczestnikom szkolenia na pierwszym spotkaniu.
     12. Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika do danego rodzaju warsztatu, pozwalające na samodzielną edukację z zakresu tematyki warsztatów (opracowania, wydruku materiałów szkoleniowych).
     13. Komplet materiałów szkoleniowych dla każdego uczestnika warsztatu obejmuje:
         1. papierową wersję materiałów szkoleniowych. Zamawiający dopuszcza dostarczenie materiałów w formie elektronicznej, np. dokumenty w standardzie PDF, w miejsce materiałów papierowych;
         2. materiały papiernicze (notatnik, długopis) i inne środki dydaktyczne niezbędne do realizacji szkolenia.
     14. Komplet materiałów musi zostać rozdany uczestnikom szkolenia w pierwszym dniu zajęć.
     15. Koszty opracowania, transportu i powielenia materiałów ponosi Wykonawca.
  2. Wykonawca zapewni:

1. W zakresie wyżywienia uczestników szkoleń Wykonawca zapewni dla każdego uczestnika warsztatów, w każdy dzień szkolenia, podczas przerwy obiadowej:
2. Obiad dwudaniowy dla wszystkich uczestników warsztatów obejmujący: zupę, gorące danie główne (mięsne, rybne lub wegetariańskie) z dodatkami skrobiowymi oraz surówką/sałatkami, deser (wyroby cukiernicze lub owoce sezonowe), kawę i herbatę wraz dodatkami, wodę mineralną gazowaną i niegazowaną; dany obiad nie powinien powtarzać się częściej niż raz na 5 dni szkoleniowych; miejsce posiłku oddalone nie więcej niż 10 minut drogi pieszo od miejsca szkolenia.
3. Wykonawca zapewni następujące gramatury wymienionych powyżej posiłków:

* Zupa – co najmniej 0,25l na uczestnika szkolenia,
* Danie gorące (mięsne lub rybne, opcja wegetariańska – warzywne) – co najmniej 150g na uczestnika szkolenia,
* Zestaw surówek/sałatek – co najmniej 150g na uczestnika szkolenia,
* Dodatki skrobiowe – porcja ziemniaków lub frytek / makaronu / ryżu / kaszy – co najmniej 200g na uczestnika szkolenia,
* Kawa, herbata, woda mineralna gazowana i niegazowana – co najmniej 0,5l na uczestnika szkolenia.

1. Dwie przerwy kawowe pomiędzy zajęciami dla wszystkich uczestników warsztatów podczas jego trwania:

* Serwis będzie dostępny przy Sali szkoleniowej;
* Serwis kawowy dla każdego uczestnika warsztatów obejmuje:
* Butelkowaną wodę mineralną gazowaną i niegazowaną (0,5l);
* Świeżo parzoną, gorącą kawę z ekspresu lub zaparzacza oraz kawę sypaną i rozpuszczalną;
* Herbatę – co najmniej 3 rodzaje herbat w torebkach;
* Dodatki – cukier, mleko do kawy, cytrynę;
* Dodatki – np. ciastka / wafelki i inne słodycze oraz ciasto

Czas na przerwy kawowe i obiadowe należy doliczyć do założonej liczby godzin dydaktycznych szkolenia.

* 1. Wszystkie koszty poniesione w związku z realizacją warsztatów w tym, m. in. przygotowaniem materiałów szkoleniowych (np. opracowanie, powielanie) koszty posiłków, koszty zabezpieczenia kadry szkoleniowej (trenerów), koszty zabezpieczenia urządzeń, obsługi i transportu ponosi Wykonawca.

1. **Dokumentacja**
   1. Dokumentacja powdrożeniowa musi zawierać techniczny opis konfiguracji implementacji urządzenia (co najmniej: nazwa, konfiguracja sieciowa, model, numer seryjny przełącznika, numery seryjne wkładek, informację o tym, gdzie urządzenie zostało zamontowane, informację o urządzeniach podpiętych do poszczególnych portów, jeżeli zostały zmienione jakieś parametry domyślne to powinna być informacja co zostało zmienione, jeżeli zagregowano porty to też powinna być taka informacja itp.).
   2. Dokumentacja powdrożeniowa powinna być dostarczona w formie elektronicznej (w wersji edytowalnej - DOC oraz w PDF) za pośrednictwem poczty elektronicznej na adresy email wskazane w § 4 ust. 1 Umowy oraz w co najmniej 1 egzemplarzu w wersji papierowej w zakresie obejmującym kompletację dostarczanych urządzeń.
   3. Do dokumentacji powdrożeniowej powinien być dołączony wykaz zawierający szczegółowy spis dokumentów wraz z opisem ich przeznaczenia.
   4. Dla każdego dostarczonego urządzenia i licencji Wykonawca dostarczy również pełną dokumentację standardowo dostarczoną przez producentów. Dokumentacja ta powinna być w języku polskim, jeżeli jest niedostępna w języku polskim to wówczas powinna być w języku angielskim.
2. **Szczegółowe wymagania dotyczące Urządzeń i Oprogramowania – wymagania dla pojedynczego urządzenia**

Przedmiotem zamówienia są urządzenia modularne pełniące funkcję load balancera oraz dodatkowe funkcje wymienione w OPZ. Komponenty urządzenia w tym obudowa musi umożliwiać wyposażenie jej w minimum 8 modułów obliczeniowych zwanych blade’ami. Urządzenie jako całość musi spełniać wymagania wyspecyfikowane poniżej.

Wszystkie wymienione funkcje oraz funkcjonalności nie mogą być licencjami ograniczonymi czasowe w ramach dostarczanego urządzenia (są tzw. licencjami wiecznymi). Urządzenie musi realizować co najmniej następujące funkcje (wszystkie wymienione funkcje, muszą być dostępne w obrębie nie więcej niż jednego urządzenia fizycznego (jednego chassis)):

* + - Rozkład ruchu pomiędzy serwerami;
    - Firewall stanowy;
    - System ochrony DNS oraz globalnego równoważenia obciążenia za pomocą̨ protokołu DNS;
    - Moduł uwierzytelnienia do aplikacji oraz SSL VPN;
    - Web Application Firewall;
    - Wysoka dostępność i analityka;

Zamawiający nie dopuszcza rozwiązania realizowanego w postaci:

* + - Maszyny (maszyn) wirtualnej w środowisku serwerowym (Vmware, Hyper-V, vcloud, KVM, Oracle VM, VirtualBox, itp.);
    - Urządzenia (urządzeń) wolnostojącego, które nie posiada możliwości powiększenia wydajności przez instalację w nim modułów typu Blade.

Szczegółowy opis funkcjonalności:

* 1. System musi umożliwiać realizację rozkładu ruchu pomiędzy serwerami:
     1. System musi umożliwiać realizację rozdziału ruchu w oparciu o informację z warstw 4-7 modelu ISO/OSI;
     2. System musi realizować obsługę inteligentnego równoważenia ruchu dla farm serwerów przy wsparciu dla protokołów: TCP, UDP, FTP, TFTP, http, SSL/TLS, DNS, RADIUS, SQL, RDP, SSH, PPTP, NTP, MQTT, MQTT-TLS, ISAKMP, SMTP, SIP;
     3. System musi mieć możliwość balansowania ruchu w oparciu o algorytmy:
     + Round Robin;
     + cykliczna dla usługi,
     + cykliczna dla serwera,
     + ważona dla usługi,
     + ważona dla serwera,
     + dynamiczna ważona dla usługi,
     + dynamiczna ważona dla serwera,
     + obserwowana,
     + przewidywana,
     + obciążenie serwerów,
     + ilość́ połączeń,
     + ważona ilość połączeń dla serwerów,
     + ważona ilość połączeń dla usługi,
     + czas odpowiedzi,
     + ilość sesji,
     + ważona dla ilości sesji do serwerów,
     + ważona dla ilości sesji do usługi,
     + hashing (URL, Domain, source IP, Destination IP);
     1. System musi umożliwiać mechanizm dowiązania sesji (session persistence) w oparciu o:
     + cookie (hash/passive/insert lub rewrite),
     + adres źródłowy,
     + adres docelowy,
     + identyfikator sesji SSL,
     + SESSIONID,
     + SIP call,
     + Hash,
     + Host,
     + Msrdp,
     + universal (wybranie dowolnego fragmentu payloadu i utworzenie na jego podstawie profilu persystencji);
     1. System ma umożliwiać monitorowanie stanów serwerów i na tej podstawie dokonywania decyzji o przełączaniu w oparciu o:
     + ICMP,
     + TCP,
     + UDP,
     + http,
     + HTTP/2,
     + HTTPS,
     + Inband,
     + SNMP DCA,
     + server (co najmniej: ServerBandwidth, CPUPercentUsage, MemoryUsage, TotalClientCount),
     + Skrypty własne;
     1. System ma wspierać content switching w oparciu o:
     + polityki: URL, URL query, URL wildcard Domain, Source IP, Destination IP, Nagłówek http, dane HTTP i TCP, UDP,
     + protokoły w przychodzących pakietach;
     1. System musi umożliwiać obsługę list kontroli dostępu dla 3 i 4 warstwy ISO/OSI;
     2. System musi umożliwiać zabezpieczenia przed atakami DNS, przynajmniej takimi jak DNS query floods, DNS amplification, zabezpieczenie przed atakami SYN flood;
     3. Selektywną kompresję danych;
     4. Terminację sesji SSL;
     5. Rozwiązanie musi pracować w trybie pełnego proxy;
     6. Praca w trybie pełnego proxy nie może powodować degradacji wydajności rozwiązania;
     7. Buforowanie połączeń TCP w przypadku osiągnięcia zadanej ilości sesji dla danego serwera;
     8. Wsparcie dla HTTP/2, w tym wsparcie dla kompresji nagłówków;
     9. System musi posiadać funkcję definiowania maksymalnej ilości obsługiwanych przez dany serwer połączeń, w przypadku przekroczenia zdefiniowanej wartości musi istnieć możliwość wysłania klientowi strony błędu lub przekierowania klienta na inny serwer;
     10. System musi zapewniać możliwość klonowania puli serwerów umożliwiając wysyłanie kopii ruchu do zewnętrznych systemów monitoringu lub urządzeń typu IDS/IPS;
     11. System musi umożliwiać obsługę sieci co najmniej w zakresie: Routingu statycznego, Routingu dynamicznego OSPF, RIP, BGP, IS-IS, Link Aggregation, 802.3ad, VLAN 802.1q Jumbo Frames, z wykorzystaniem integracji z Equal Cost Multi-Path (ECMP);
     12. System musi wspierać wysoką dostępność: Active/Passive, Active/Active Connection Mirroring;
     13. Urządzenie powinno implementować TCP proxy z mechanizmem zamykania okna w stronę serwera www w przypadku zbyt wolnego odbierania danych przez zdalnego klienta;
     14. Urządzenie musi mieć możliwość strojenia profili połączeń TCP, w tym co najmniej:
     + ustawienia timeout idle,
     + keep alive interval,
     + zero window timeout,
     + initial Receive Window Size,
     + wyboru algorytmu wykrywania natłoku,
     + wsparcia hybrydowych algorytmów wykrywania natłoku, opartych o stratę pakietów i round-trip-time,
     + mechanizmu rate pacing,
     + określenia maksymalnej wielkości bufora per połączenie TCP celem ochrony przed wysyceniem pamięci,
     + określenia maksymalnego bufora wysyłania i odbioru (send/receive buffer);
     1. Urządzenie musi mieć możliwość włączenia ignorowania nagłówków przeglądarki dotyczących cachowania (Cache-control);
     2. Urządzenie musi umożliwiać selektywne cachowanie zwracanego kontentu a cachowanie powinno być zależne od:
     + listy URN-ów i prefixów URN-ów z których zwracany jest kontent,
     + maksymalnej wielkości zwracanego obiektu,
     + minimalnej wielkości zwracanego obiektu;
     1. Powinna istnieć możliwość ograniczania wielkości cachu, ilości cachowanych obiektów celem ochrony pamięci urządzenia przed przepełnieniem;
     2. Urządzenie musi wspierać multipleksacje wielu zapytań http w tej samej sesji TCP;
     3. Urządzenie musi umożliwiać kompresję zwracanej zawartości http. Użycie kompresji powinno być zależne od:
     + listy dozwolonych URI,
     + listy wykluczonych URI,
     + listy możliwych do kompresji Content-Type,
     + listy wykluczonych Content-Type,
     + minimalnej wielkości zwracanego obiektu;
     1. Kierowanie ruchu do odpowiedniej pool’i zasobów:
     + Urządzenie powinno realizować mechanizm kierowania żądań od użytkowników końcowych do pool (grup) zasobów serwerowych na podstawie następujących atrybutów:
       - wartości http hostname, początku/końca nagłówka hostname, ciągu znaków znajdujący się w nagłówku hostname,
       - port,
       - metody http,
       - nazwy cookie, ciągu znaków na początku/końcu nazwy cookie, ciągu znaku zawartego w nazwie cookie,
       - URN-a, oraz ciągu znaków występujących na początku/końcu lub zawartych w URN-ie,
       - User agent,
       - dowolnego nagłówka lub kombinacji nagłówków,
       - wykorzystania cipherów w TLS,
       - Common Name Klienta, oraz ciągu znaków występujących na początku/końcu lub zawartych w Common Name;
     + Reguły kierowania żądań powinny wymuszać co najmniej następujące akcje:
       - wybór pool’i zasobów (grupy IP adresów i portów),
       - kierowania żądania do konkretnego adresu IP,
       - redyrekcji,
       - wyłączanie / włączanie ochrony aplikacyjnej,
       - wybór polityki ochrony aplikacyjnej,
       - włączania/ wyłączania cachowania,
       - włączania/ wyłączania kompresji,
       - dodania / usunięcia nagłówka / cookie http,
       - wyboru parametrów profilu (zestawu parametrów, w tym CA, certyfikatu, klucza) dla połączeń w stronę serwerów aplikacyjnych;
     + Powinna istnieć możliwość nadpisania statycznych reguł kierowania ruchu w języku skryptowym, na podstawie dowolnych atrybutów żądania http, oraz stanu sesji zapisanego w pamięci urządzenia;
     1. System musi zapewniać obsługę certyfikatów z kluczami typu ECDSA wykorzystującymi krzywe eliptyczne (ECC) zarówno od strony klienta, jak i od strony puli serwerów;
     2. Sprzętowe wsparcie dla algorytmów AES, AES-GCM, RSA, DSA, DH, ECDSA, ECDH, SHA2. Wsparcie dla Perfect Forward Secrecy;
     3. Dla protokołu TLS 1.2 wymagana jest obsługa AES-GCM zarówno od strony klienta, jak i od strony puli serwerów;
     4. Wsparcie dla protokołu TLS 1.3;
     5. System musi zapewniać obsługę certyfikatów podpisanych funkcją skrótu SHA-2 zarówno od strony klienta, jak i od strony puli serwerów;
     6. System musi posiadać funkcję walidacji certyfikatów klientów łączących się przy wykorzystaniu protokołu SSL;
     7. System musi obsługiwać sieci VLAN w standardzie 802.1q;
     8. System musi obsługiwać agregację linków w standardzie 802.3ad (LACP);
     9. System musi obsługiwać Jumbo Frames;
     10. System musi posiadać funkcjonalność bramy VXLAN oraz NVGRE;
     11. Klucze prywatne zapisane na dysku urządzenia muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej;
     12. Rozwiązanie musi posiadać wbudowany w system operacyjny język skryptowy, posiadający co najmniej następujące cechy:
     + analiza, zmiana oraz zastępowanie parametrów w nagłówku http oraz w zawartości pakietów
     + obsługa (parsowanie, modyfikacja, kreowanie odpowiedzi) protokołów: http, http2, WebSocket, DNS, RADIUS,
     + język skryptowy musi umożliwiać dynamiczne przypisanie polityki bezpieczeństwa aplikacyjnego w oparciu o dowolną kombinację atrybutów http, SSL/TLS. Parsowanie parametrów komunikacji TLS/SSL, w szczególności odczyt certyfikatów X.509 i wstrzykiwanie odczytanych parametrów w formie nagłówków http,
     + możliwość zdefiniowania reakcji na zagrożenie wykryte przez Web Application Firewall na podstawie danych dostarczonych przez WAF, odczytanych w komunikacji http, SSL, WebSocket oraz historycznych atrybutów konfiguracji (kontekstu),
     + język skryptowy oparty o Tool Command Language powinien mieć możliwość delegowania złożonych zadań do silnika NodeJS i użycia bibliotek „społecznościowych”, celem np. parsowania protokołów jeszcze nie zaimplementowanych w rozwiązaniu Application Delivery Controller
  2. System musi umożliwiać realizację firewall’a stanowego
     1. Konfigurację reguł firewall’owych za pomocą wbudowanego w system interfejsu graficznego;
     2. Rozwiązanie powinno śledzić i ograniczać wystąpienia anomalii warstw niższych, w tym: IPv4, IPv6, TCP, UDP, ICP;
     3. Rozwiązanie powinno zawierać system sztucznej inteligencji analizujący na bieżąco ruchu i wykrywające ilościowe anomalie ruchu;
     4. Rozwiązanie powinno zawierać w pełni funkcjonalny firewall warstwy 4 modelu OSI/ISO;
     5. Rozwiązanie powinno być wyposażone w system ochrony przed atakami DDoS realizowany przynajmniej częściowo za pomocą dedykowanych komponentów hardware;
     + Rozwiązanie powinno obsłużyć sprzętowo mitygację minimum 100 wektorów ataków DDoS
  3. System ochrony DNS:
     1. System ochrony DNS musi realizować co najmniej następujące funkcjonalności:
     + DNS Autorytatywny,
     + Global Server Load Balancing,
     + Dynamiczne podpisywanie domen DNS SEC,
     + DNS Caching,
     + DNS Resolver,
     + walidacja podpisów odpowiedzi DNS SEC,
     + rozkład ruchu pomiędzy serwerami DNS innych producentów,
     + ochrona przed atakami DDoS na protokół DNS;
     1. Ochrona przed atakami DDoS na niższe (niż DNS) protokoły w modelu ISO/OSI;
     2. System musi natywnie wspierać IPv4 i IPv6;
     3. System musi obsługiwać sieci VLAN w standardzie 802.1q;
     4. System musi obsługiwać agregację linków w standardzie 802.3ad (LACP);
     5. System nie może wykorzystywać bibliotek i kodu „bind” do obsługi ruchu od użytkowników końcowych;
     6. Rozwiązanie powinno wspierać rozrzucanie ruchu DNS na podstawie następujących algorytmów:
     + cykliczna,
     + ważona,
     + najmniejsza liczba połączeń,
     + najszybsza odpowiedź serwera,
     + najmniejsza liczba połączeń i najszybsza odpowiedź serwera,
     + najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie,
     + dynamicznie ważona oparta na SNMP/WMI,
     + definiowana na podstawie grupy priorytetów dla serwerów,
     + musi istnieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego,
     1. Rozwiązanie musi posiadać wbudowany w system operacyjny język skryptowy, posiadający co najmniej następujące cechy:
     + analiza, zmiana oraz zastępowanie parametrów DNS,
     + generowania odpowiedzi na podstawie zapytania DNS oraz stanu zapisanego w pamięci urządzenia (np. historyczne zapytania DNS od danego użytkownika),
     + powinna istnieć możliwość nadpisania statycznych reguł kierowania ruchu, na podstawie dowolnych atrybutów żądania DNS, oraz stanu sesji zapisanego w pamięci urządzenia,
     + język skryptowy powinien umożliwiać iteracje poprzez wszystkie rekordy odpowiedzi DNS, oraz odczytywanie, modyfikacje i usuwanie poszczególnych rekordów,
     + język skryptowy powinien umożliwiać odczyt, modyfikacje i wstawienie sekcji additional
     + język skryptowy powinien umożliwiać odczyt i modyfikację:
       - Typu rekordu,
       - TTL,
       - Nazwy rekordu,
       - Klasy (class);
     + język skryptowy powinien umożliwiać operacje porównania stringów: equals, contain, starts with, ends with,
     + język skryptowy powinien wspierać REGEXP,
     + język skryptowy powinien umożliwiać selektywne (per request) wyłączanie funkcji GSLB, DNS Resolver i Cache, autorytatywnego DNS,
     + język skryptowy powinien umożliwiać selektywne (per request) wyłączanie funkcji GSLB, DNS Cache;
     1. Powinna istnieć możliwość weryfikacji listy rekordów i reakcji / obsługi wyjątków, jeżeli domena lub zwracany adres IP znajduje się na liście;
     2. Powinna istnieć możliwość zaimportowania i użycia statycznej listy „wyjątków” powyżej 200 000 rekordów;
     3. Powinna istnieć możliwość definiowania obsługi ruchu zarówno dla żądań jak i odpowiedzi DNS;
     4. Rozwiązanie powinno pełnić funkcje serwera autorytatywnego;
     5. Celem podwyższenia wydajności, zony statyczne powinny być ładowane do pomięci i obsługiwane z pamięci RAM (to jest Autorytatywny DNS);
     6. Autorytatywny serwer DNS powinien działać zarówno jako primary/master jak i secondary/slave (to jest Autorytatywny DNS);
     7. Rozwiązanie powinno wspierać zone transfer (to jest Autorytatywny DNS, który robi DNS Express):
     + obsługiwać TSIG,
     + inicjować transfer zony po otrzymaniu notyfikacji (NOTIFY),
     + Powinna istnieć możliwość przekazania notyfikacji do innych serwerów DNS;
     1. Powinna istnieć możliwość definiowania nazw, dla których jest implementowany mechanizm GSLB (Global Server Load Balancing);
     2. Nazwy zwracające dynamiczne rekordy (GSLB) powinny nadpisywać statyczną definicje strefy (zony);
     3. Mechanizm GSLB powinien obsługiwać następujące typy rekordów:
     + A,
     + AAAA,
     + CNAME,
     + MX,
     + NAPTR,
     + SRV;
     1. Silnik GSLB powinien uwzględniać stan zasobów znajdujących się za adresami IP, do których może być skierowany użytkownik poprzez zwrócenie adresu IPv4 lub IPv6.
     2. Stan zasobów powinien być wymieniany asynchronicznie pomiędzy:
     + innymi autorytatywnymi serwerami DNS implementującymi GSLB,
     + urządzeniami ADC (Application Delivery Controller) pochodzącymi od tego samego producenta;
     1. Serwery autorytatywne powinny pracować w klastrze N+1, tak, że kompletne odcięcie jednego centrum przetwarzania danych nie spowoduje utraty synchronizowanych informacji pomiędzy pozostałymi;
     2. Rozwiązanie nie powinno wymuszać twardego limitu na liczbę jednostek w klastrze;
     3. Rozwiązanie powinno wspierać mechanizm Route Healt Injection (RHI);
     4. W przypadku, gdy nie jest możliwe otrzymanie stanu zasobów / serwerów virtualnych, powinna istnieć możliwość zdefiniowania i użycia monitora stanu aplikacji / serwera virtualnego;
     5. Rozwiązanie GSLB powinno wspierać co najmniej następujące metody monitorowania:
     + http, https,
     + IMAP,
     + LDAP,
     + MSSQL, MySQL, PostgresSQL,
     + NNTP,
     + POP3,
     + RADIUS i RADIUS Accounting,
     + SIP,
     + SNMP,
     + SMTP,
     + SOAP,
     + TCP,
     + UDP,
     + monitora skryptowego, definiującego sekwencje wymiany wiadomości,
     + monitora zewnętrznego, czyli uruchomienia procesu np. bash, perl, zwracającego stan zasobów na podstawie logiki zawartej w zewnętrznym programie / skrypcie;
     1. Silnik GSLB powinien wspierać co najmniej następujące algorytmy load balancingu:
     + cykliczna
     + ważona
     + na podstawie adresu IP resolvera, implementująca persystencje (przywiązywanie sesji),
     + do pierwszego dostępnego virtualnego serwera, przy czym rozwiązanie powinno umożliwiać zdefiniowanie kolejności virtualnych serwerów,
     + lokalizacji pytającego serwera, na podstawie zaszytej bazy geolokalizacji;
     1. Jeżeli wirtualny serwer jest zdefiniowany na urządzeniu ADC od tego samego producenta, silnik GSLB powinien wspierać co najmniej następujące algorytmy load balancingu:
     + na podstawie wolnych zasobów procesora urządzenia ADC,
     + ilości hopów pomiędzy LDNS a ADC,
     + na podstawie aktualnego wysycenia połączeń do serwera wirtualnego. Mniejsze wysycenie oznacza większe prawdopodobieństwo wyboru,
     + aktualnej ilości obsługiwanych połączeń przez ADC,
     + pakietów na sekundę,
     + Round Trip Time,
     + subiektywnej oceny wydajności przypisanej do wirtualnego serwera na urządzeniu ADC przez administratora,
     + średniej ważonej z powyższych metryk;
     1. Powinna istnieć możliwość grupowania obszarów geograficznych z dokładnością do poziomu województwa, tak aby zwiększyć prawdopodobieństwo połączenia Klienta z najbliższym CPD;
     2. Powinna istnieć możliwość grupowania prywatnych adresacji w obszary i wykorzystania tych obszarów do algorytmu load balancingu;
     3. Silnik GSLB powinien umożliwiać grupowanie zasobów / wirtualnych serwerów w Centra Przetwarzanie danych na podstawie ich rzeczywistej lokalizacji;
     4. System GSLB powinien wspierać mechanizmy oceny dostępności Centrum Przetwarzania Danych;
     5. W przypadku niedostępności Centrum Przetwarzania Danych, GSLB nie powinno zwracać adresów IP posadowionych w niedostępnym CPD, chyba że są one zdefiniowane statycznie;
     6. Powinna istnieć możliwość delegacji procesu monitorowania wirtualnych serwerów posadowionych na rozwiązaniach firm trzecich do urządzenia ADC od tego samego dostawcy znajdującego się w tym samym CPD co wirtualne serwery;
     7. Powinna istnieć możliwość delegacji procesu monitorowania wirtualnych serwerów, posadowionych na rozwiązaniach firm trzecich, do urządzenia ADC mającego routing do strefy, w której znajdują się monitorowane zasoby;
     8. Powinna istnieć możliwość grupowania nazw, tak żeby dany klient był obsługiwany z tego centrum przetwarzania danych dla wszystkich nazw ze zdefiniowanego zbioru;
     9. Rozwiązanie powinno umożliwiać implementacje cache’u wielopoziomowego;
     10. Rozwiązanie powinno wspierać trzy tryby pracy:
     + Cache transparentny, gdzie cachowane są pełne odpowiedzi. W przypadku potrzeby rozwiązania zapytania (cache miss), cache transparentny przesyła zapytanie do drugiego poziomu cache-u,
     + Resolvera z cachem,
     + Resolvera walidującego podpisy DNS SEC z cachem;
     1. Rozwiązanie powinno umożliwiać granularną konfigurację każdego typu cache’u, tak aby uzyskać optymalny stosunek czasu wyszukiwania rekordów do cache hit ratio. Rozwiązanie powinno umożliwiać strojenie przynajmniej następujących parametrów
     + dla cache’u transparentnego: dostępnej pamięci dla cache’u wiadomości i cachu rekordów
     + w trybie pracy resolver z cache’m: dostępnej pamięci dla cache’u wiadomości, cache’u rekordów i cache’u autorytatywnych serwerów nazw,
     + w trybie pracy resolver walidującego DNS SEC z cache’m: dostępnej pamięci dla cache’u wiadomości, cache’u rekordów, cache’u autorytatywnych serwerów nazw i cache’u kluczy DNS SEC;
     1. Resolver powinien zbierać i utrzymywać statystyki czasu odpowiedzi serwerów autorytatywnych i wykorzystywać te statystyki w celu skrócenia czasu rozwiązywania nazw;
     2. Rozwiązanie powinno wykorzystywać IPv4 i IPv6 do komunikacji z serwerami autorytatywnymi;
     3. Rozwiązanie powinno umożliwiać przeszukiwanie cache’owanych rekordów;
     4. Rozwiązanie powinno umożliwiać selektywne usuwanie cache’owanych rekordów;
     5. System powinien filtrować w oparciu o Response Policy Zone;
     6. System powinien filtrować w oparciu o pliki płaskie, gdzie w pliku płaskim do każdej domeny może być przypisana akcja, np. NX Domain, odpowiedź CNAME, A record itd.;
     7. Resolver powinien zbierać co najmniej następujące statystyki:
     + ilość zapytań,
     + ilość odpowiedzi,
     + wykorzystanych autorytatywnych serwerów,
     + odpowiedzi wygenerowanych lokalnie,
     + trafień w Response Policy Zone,
     + trafień / nietrafień w cache, per typ cache’u (cache wiadomości, resource rekord, autorytatywne serwery),
     + wyników rozwiązywań zapytań, np. sukces, timeout, przepełnienie kolejki,
     + odpowiedzi ze strony serwerów autorytatywnych;
     1. Statystyki powinny być dostępne za pomocą SNMP;
     2. Powinna istnieć możliwość definiowania wyjątków dla zapytań trafiających do systemu resolvera, przynajmniej dla następujących przypadków:
     + powinna istnieć możliwość przekazania zapytania dla predefiniowanych subdomen do pool’i serwerów DNS odpowiedzialnych za te domeny,
     + powinna istnieć możliwość przekazania zapytania dla predefiniowanych domen odwrotnych do pool’i serwerów DNS odpowiedzialnych za te domeny odwrotne,
     + generowania predefiniowanej odpowiedzi, jeżeli w oryginalnej odpowiedzi z serwera autorytatywnego znajdzie się IP adres o złej reputacji;
     1. Silnik systemu (resolvera) powinien mieć możliwość skorzystania z bazy reputacyjnej adresów IP celem usuwania tychże adresów z odpowiedzi od serwera autorytatywnego;
     2. Rozwiązanie powinno umożliwiać rozbudowę o system sygnatur IP;
     3. Rozwiązanie powinno filtrować po dowolnej kombinacji następujących typów zapytań:
     + a, axfr, dnskey, isdn, mb, naptr, nsec3param, rrsig, sshfp , a6, caa, ds, ixfr, md, nimloc, null, rt, tkey , aaaa, cert, eid, key, mf, ns, nxt, sig, tsig , afsdb, cname, gpos, kx, mg, nsap, opt, sink, txt , any, dhcid, hinfo, loc, minfo, nsap-ptr, ptr, soa, wks , apl, dlv, hip, maila, mr, nsec, px, spf, x25 , atma, dname, ipseckey, mailb, mx, nsec3, rp, srv, zxfr;
     1. Rozwiązanie powinno być odporne na ataki typu „Phantom domain attack”;
     2. Rozwiązanie powinno być odporne na ataki typu „Lock-up domain”;
     3. Rozwiązanie powinno być wyposażone w system ochrony przed atakami DDoS;
     4. Rozwiązanie powinno śledzić i ograniczać:
     + liczbę pakietów o nieprawidłowej składni;
     + liczbę pakietów per typ zapytania: A, PTR, NS, SOA, CNAME, MX, AAAA, TXT, SRV, AXFR, IXFR, ANY, NXDOMAIN, niemieszczących się w powyższych kategoriach,
     + występowanie ataków typu reflection;
     1. System musi posiadać moduł analizy ruchu DNS. Moduł powinien zbierać następujące metryki:
     + typy zapytań,
     + domeny,
     + najaktywniejsi Klienci per IP, Kraj,
     + typy ataków,
     + wektory ataków;
     1. Dla funkcjonalność GSLB system musi realizować co najmniej następujące funkcjonalności:
     + Global Server Load Balancing,
     + Dynamiczne podpisywanie domen DNS SEC,
     + DNS Caching,
     + walidacja podpisów odpowiedzi DNS SEC,
     + rozkład ruchu pomiędzy serwerami DNS innych producentów,
     + ochrona przed atakami DDoS na protokół DNS,
     + ochrona przed atakami DDoS na niższe (niż DNS) protokoły w modelu ISO/OSI;
     1. Rozwiązanie powinno wspierać cache transparentny, gdzie cache’owane są pełne odpowiedzi. W przypadku potrzeby rozwiązania zapytania (cache miss), cache transparentny przesyła zapytanie do drugiego poziomu cache-u;
     2. Rozwiązanie powinno umożliwiać granularną konfigurację cache’u, tak aby uzyskać optymalny stosunek czasu wyszukiwania rekordów do cache hit ratio. Rozwiązanie powinno umożliwiać strojenie dostępnej pamięci dla cache’u wiadomości i cache’u rekordów;
  4. System uwierzytelniania i autoryzacji musi zapewnić obsługę minimum 20 tysięcy jednoczesnych użytkowników.
     1. System musi mieć wsparcie dla następujących metod uwierzytelniania użytkowników w dostępie do systemów:
     + lokalna baza użytkowników – bez odwoływania się do zewnętrznych systemów certyfikatów cyfrowych,
     + LDAP / LDAPS,
     + SAML 2.0 - Security Assertion Markup Language Kerberos SSO / NTLM,
     + RSA SecureID,
     + Radius,
     + TACACS - Terminal Access Controller Access-Control System OAuth / OpenID,
     + wbudowany w rozwiązanie mechanizm generowania i wysyłania jednorazowych kodów OTP,
     + OCSP Responder,
     + obsługę dla SSO pomiędzy wieloma domenami,
     + możliwość wyodrębnienia i wykorzystania w polityce bezpieczeństwa ticketów Kerberos,
     + obsługę SAML 2.0 w trybach IDP oraz SP,
     + obsługę dedykowanych tuneli aplikacyjnych per aplikacja,
     + dynamiczną kontrolę dostępu użytkowników,
     + dynamiczne portale bazujące na tożsamości użytkownika,
     1. Moduł SSL VPN musi posiadać co najmniej następujące funkcje:
     + obsługa tuneli szyfrowanych SSL VPN z pomocą dedykowanego klienta lub client-less,
     + obsługa IPv6 ,
     + moduł SSL VPN musi obsługiwać tryb wymuszający nawiązanie połączenia VPN, tzw. tryb always-on dla systemu Windows,
     + wsparcie dla zewnętrznego uwierzytelnienia w dostępie SSL VPN tzw. captive portal,
     + system musi umożliwiać kompresję przesyłanych danych,
     + możliwość sprawdzania stacji końcowej pod kątem bezpieczeństwa,
       - sprawdzanie obecności pliku w systemie,
       - sprawdzanie aktywnego procesu w systemie,
       - sprawdzanie aktywnego systemu antywirusowego, antyspareware,
       - sprawdzanie stanu Firewalla systemowego,
       - sprawdzanie zainstalowanych poprawek systemowych,
       - w przypadku systemu Windows sprawdzanie wpisu do rejestru systemowego,
       - sprawdzanie certyfikatu,
       - sprawdzanie informacji o zasobach hardware urządzenia klienta;
     + system musi umożliwiać dynamic split-tunneling;
     1. Moduł SSL VPN musi posiadać mechanizm raportowy, uwzgledniający nie mniej niż:
     + błędne próby uwierzytelnienia,
     + informacje o użytkownikach,
     + zasoby, do których odwołują się użytkownicy,
     + geolokalizację użytkownika;
     1. System musi zapewniać obsługę nie mniej niż 500 jednocześnie pracujących użytkowników SSL VPN z możliwością licencyjnej rozbudowy do minimum 20 tysięcy licencji;
     2. System musi zapewniać obsługę 20 tysięcy jednocześnie pracujących użytkowników dla sesji uwierzytelniania typu:
     + Microsoft Exchange,
     + Outlook Anywhere, ActiveSync, Web Service,
     + Microsoft OWA (without a rewrite profile),
     + WebAuth,
     + SAML;
     1. Licencjonowanie musi odbywać się per ilość jednocześnie pracujących użytkowników z możliwością instalacji klienta SSL VPN na dowolnej ilości urządzeń/stacji roboczych;
     2. System musi umożliwiać metody dostępu poprzez:
        + portal użytkownika z funkcjonalnością SSO (webtop),
        + tunelu aplikacyjnego,
        + dostępu sieciowego (VPN);
     + obsługa Microsoft ActiveSync i Outlook Anywhere z client-side NTLM,
     + listy dostępu (ACL) dla warstwy 7 modelu OSI,
     + buforowanie poświadczeń oraz SSO proxy,
     + zewnętrzne strony logowania,
     + obsługa wielu platform użytkowników (iPadOS, IOS, MacOS, Windows, Linux, Android),
     + obsługa OAuth i OAuth 2.0,
     + obsługa JSON Web Token (JWT) z OAuth,
     + obsługa Google reCAPTCHA V2,
     + obsługa WebSockets dla dostępu przez portal,
     + obsługa integracji z ADFS Proxy (PIP),
     + integracja z MS Intune Device, Airwatch, MAAS360 dla wyniku weryfikacji stanu urządzeń końcowych,
     + obsługa OpenID Connect Support dla OAuth Resource Server i Client,
     + obsługa serwera uwierzytelnienia dla OpenID Connect,
     + konfiguracja proxy Identity-aware dla architektur Zero Trust. System musi realizować dynamiczną zmianę polityki bezpieczeństwa odpowiadającą zmianie warunków dostępu użytkownika,
     + system musi umożliwiać content i URL rewriting podczas bez agentowego dostępu do zasobów wewnętrznych w trybie reverse proxy,
     + obsługa walidacji dla modelu Zero Trust:
       - tożsamości użytkownika,
       - wynik kontroli bezpieczeństwa urządzenia,
       - MFA (multifactor authentication);
     + integracja z IDaaS,
     + możliwość integracji z systemami AAA firm trzecich za pomocą wywołań API,
     + wsparcie dla FIDO U2F via API (YubiKey),
     + wsparcie dla DTLS 1.2 dla klienta VPN,
     + wsparcie dla Microsoft Conditional Access rules (Azure AD),
     + obsługa OpenAPI 3.0 dla importu polityki bezpieczeństwa API w ramach AuthZ/AuthN,
     + dynamiczny Split Tunneling (Zoom, Office 365),
     + obsługa dla OpenID Connect protocol dla Duo MFA,
     + wsparcie dla Microsoft Identity Platform 2.0,
     + graficzny interfejs umożliwiający budowanie reguł dostępowych,
     + obsługa języka skryptowego opartego na języku TCL lub równoważnym,
     + system musi posiadać funkcję definiowania i edycji szablonów konfiguracji aplikacji. Szablony powinny służyć do optymalizacji procesu wdrażania systemu zarówno dla znanych aplikacji biznesowych, jak i własnych aplikacji klienta. W ramach opisanych szablonów musi istnieć możliwość automatycznej kontroli poszczególnych elementów konfiguracji szablonu i zabezpieczenie ich przed modyfikacją i usunięciem;
  5. Web Application Firewall musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji Web. Firewall aplikacyjny musi działać jednocześnie z wykorzystanie pozytywnego i negatywnego modelu bezpieczeństwa:
     1. Pozytywny model bezpieczeństwa powinien kontrolować co najmniej:
     + wystąpienie URL-i, długość URL-i,
     + typ servleta występujący pod danym url-em – format komunikacji (http form, JSON, XML, GWT),
     + przejścia pomiędzy URL-ami (servletami),
     + dopuszczalne metody http,
     + dopuszczalne cookie,
     + dopuszczalne parametry w polityce,
     + parametry dynamiczne,
     + typ/format parametrów (alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML, e-mail, telefon, plik upload’owany),
     + dopuszczalne parametry w danym servlecie,
     + długość zapytań,
     + nazwy hosta,
     + wystąpień i długość parametrów (per każdy parametr),
     + wystąpień i długości nagłówków,
     + wystąpień i długości cookies,
     + oczekiwanych typów znaków per każdy parametr,
     + typów rozszerzeń plików, w tym długości URL’a, requestu, query stringu, post data dla danego typu pliku URL-i podatnych na CSRF;
     1. Profil aplikacji web musi być tworzony na podstawie analizy ruchu sieciowego;
     2. WAF musi umożliwiać definiowania dopuszczalnego przepływu sekwencji zapytań w obrębie aplikacji z uwzględnieniem jej logiki biznesowej;
     3. Tworzenie profilu bezpieczeństwa Web Application Firewall dla danej aplikacji musi odbywać się na podstawie analizy ruchu sieciowego w szczególności na podstawie publicznego ruchu produkcyjnego;
     4. System musi posiadać funkcję definiowania i edycji szablonów konfiguracji aplikacji. Szablony powinny służyć do optymalizacji procesu wdrażania systemu zarówno dla znanych aplikacji biznesowych, jak i własnych aplikacji klienta. W ramach opisanych szablonów musi istnieć możliwość automatycznej kontroli poszczególnych elementów konfiguracji szablonu i zabezpieczenie ich przed modyfikacją i usunięciem;
     5. Algorytmy tworzenia profilu bezpieczeństwa WAF powinny odrzucać próby ataków w procesie nauki;
     6. Musi istnieć możliwość definicji zaufanych adresów źródłowych, z których algorytm tworzenia profilu bezpieczeństwa WAF będzie akceptować wszystkie zachowania jako prawidłowe, tak aby administrator mógł przyspieszyć proces tworzenia profilu bezpieczeństwa;
     7. Musi istnieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki bezpieczeństwa;
     8. Musi istnieć możliwość ochrony dynamicznych oraz ukrytych parametrów zapytań http;
     9. WAF musi automatycznie wykrywać false positive i wyłączać odpowiadające nim sygnatury dla danego parametru;
     10. WAF musi posiadać funkcjonalność automatycznego wykrywania stron logowania użytkowników oraz automatycznie włączać dla tych stron ochronę przed atakami „brute force”;
     11. Mechanizm zabezpieczenia przed manipulacją cookie serwera aplikacyjnego powinien być oparty o wstrzykiwanie cookie z podpisem oryginalnego cookie aplikacji;
     12. WAF powinien chronić przed kradzieżą sesji poprzez porównywanie „odcisku palca” (fingerprint) przeglądarki z sesją użytkownika. Mechanizm musi działać także dla TLS (TLS fingerprintig);
     13. Mechanizm zabezpieczenia przed Cross-Site Request Forgery powinien dodawać losowy token do odpowiedzi http zawierających odwołania do chronionego zasobu (servleta);
     14. System musi zapewniać możliwość wyboru polityki bezpieczeństwa na podstawie: Host, URL, Nagłówków, Cookie;
     15. Oprócz pozytywnego modelu zabezpieczeń WAF musi posiadać również funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń);
     16. WAF musi posiadać mechanizmy ochrony przed atakami: Broken Access Control, SQL Injection, Cross-Site Scripting, Cross-Site Request Forgery, Session hijacking, Command Injection, Cookie/Session Poisoning, Parameter/Form Tampering, Forceful Browsing, Brute Force Login, Web Scraping, Cookie manipulation/poisoning, Dynamic Parameter tampering, Buffer Overflow, Stealth Commanding, Unused HTTP Methods, Malicious File Uploads, Hidden Field Manipulation;
     17. Musi istnieć możliwość selektywnego włączania/wyłączania sygnatur per parametr;
     18. Dla każdej chronionej aplikacji internetowej urządzenie powinno umożliwiać wybór stosowanych technologii i systemu operacyjnego w celu poprawnego doboru wykorzystywanych sygnatur uwzględniając, ale nie ograniczając się do:
     + bazy danych: ORACLE, MySQL, Microsoft SQL Server, PostgreSQL, Sybase, IBM DB2, CouchDB, Elasticsearch, MongoDB, SQLite, Sybase/ASE,
     + system operacyjny: Windows, Linux, UNIX,
     + język aplikacji, frameworki, biblioteki: ASP, ASP.NET, PHP, Java Servlets, JavaScript, AngualrJS, Backbone.js, CodeIgniter, Django, Java Server Faces, BEA WebLogic, CGI, Elasticsearch, Front Page Server Extension, Lotus Domino, Macromedia ColdFusion, Outlook Web Access, SSI, WebDAV, jQuery, SSI, Apache Struts, ef.js, Ember.js, Express.js, GraphQL, Handlebars, JavaServer Faces, Laravel, MooTools, Moustache, Python, React, RequireJS, Ruby, Spring Boot, UIKit, Underscore.js, Vue.js, WebDAV, Zend, ZURB Fundation,
     + serwer WWW, silniki: Apache, Apache Tomcat, Microsoft IIS, serwerów proxy, Jenkins, Jetty, Joomla, Macromedia JRun, Nginx, Node.js, Oracle Application Server, Oracle Identity Manager, Redis, Typo3 CMS;
     1. WAF musi posiadać mechanizmy ochrony przed atakami DoS ukierunkowanymi na warstwę aplikacyjną (np. Slow Loris, http Smuggling);
     2. WAF musi rozróżniać rzeczywistych użytkowników od automatów podczas ataku (D)DoS poprzez:
     + wstrzykiwanie skryptu JavaScript i weryfikacji rezultatów jego wykonania,
     + mechanizmu browser fingerprinting, w celu wykrycia tzw. headless browser,
     + sygnatur botów,
     + wykorzystanie CAPTCHA (tylko w przypadku, gdy powyższe mechanizmy nie rozstrzygają czy podłączony jest rzeczywisty użytkownik);
     1. System powinien umożliwiać proaktywne wykrywanie i blokowanie botów (j.w.), zanim wywołają atak DDoS, web scraping lub „brute force”;
     2. System musi rozróżniać ruch generowany przez boty za pomocą zasobów lokalnych;
     3. System musi posiadać możliwość rozbudowy licencyjnej o wysyłanie części ruchu do dalszej analizy w scrubbing center, w celu ochrony przed botami;
     4. WAF musi zawierać moduł sztucznej inteligencji, który na bieżąco obserwuje ruch od użytkowników końcowych, celem budowy i utrzymania modelu prawidłowego ruchu do aplikacji. WAF na podstawie behawioralnej analizy ruchu bieżącego i zbudowanego modelu, powinien wykrywać i chronić aplikację przed atakiem DDoS w warstwie 7. W systemie nie może być żadnego licencyjnego limitu dla tej funkcji.
     5. System powinien kategoryzować boty i umożliwiać przepuszczanie ruchu od pożytecznych botów (np. search enginy), blokując ruch od szkodliwych botów;
     6. Moduł ochrony przed DDoS powinien wykrywać ataki per: Source IP, Urządzenie, na bazie „odcisku palca” urządzenia, Obszar geolokacyjny, URL, Globalnie – website;
     7. Powinna istnieć możliwość przypisania różnych poziomów detekcji ataków (D)DoS dla danych URL-i portala. Np. /infoportal/\* powinien posiadać luźniejszą politykę detekcji i zapobiegania ataków DDoS niż /portal/\*;
     8. System powinien wykrywać i chronić przed atakami DDoS na tzw. ciężkie servlety, czyli takie wywołujące złożone operacje obliczeniowe np. skomplikowane zapytania do baz danych;
     9. Wykrycie ataku na ciężkie servlety powinno opierać się przynajmniej o ilość zapytań (TPS) oraz czas odpowiedzi;
     10. System powinien umożliwiać definicję maksymalnego czasu próbki ruchu, maksymalnej pojemności próbki ruchu, interwału czasowego pomiędzy pobieraniem próbki ruchu;
     11. System powinien umożliwiać automatyczny zapis przykładowego ruchu do plików zgodnych z formatem TCP dump, w momencie wykrycia ataku (D)DoS;
     12. Powinna istnieć możliwość doboru odpowiedzi w zależności do rodzaju naruszenia;
     13. WAF musi posiadać możliwość uwzględniania w logach dotyczących incydentów informacji o uwierzytelnionym użytkowniku oraz blokowania określonej liczby incydentów wykonywanych w zdefiniowanym czasie przez tego użytkownika;
     14. WAF powinien umożliwiać usuwanie nagłówków serwera aplikacyjnego zdradzających technologię oraz wersję oprogramowania; bez uszczerbku na wydajności WAF’a;
     15. WAF powinien umożliwiać wstrzykiwanie nagłówków np. w celu ochrony przed Clickjack’iem;
     16. WAF powinien umożliwiać podmianę kodów statusów zwracanych przez serwer aplikacyjny;
     17. W obrębie licencji WAF dostarczony musi być moduł ochrony protokołu HTTP, SMTP oraz FTP, DNS, API;
     18. WAF musi mieć możliwość wgrania pliku swagger file (Open API) w celu budowy polityki typu whitelist dla API;
     19. WAF musi posiadać wsparcie dla aplikacji AJAX oraz JSON;
     20. WAF powinien wyświetlać strony blokowania (błędu) w technologiach AJAX i JSON;
     21. WAF musi posiadać wsparcie dla Google Web Toolkit;
     22. WAF musi posiadać wsparcie dla GraphQL;
     23. WAF musi posiadać możliwość ochrony komunikacji XML poprzez:
     + walidację Schema/WSDL,
     + wybór dozwolonych metod SOAP,
     + szyfrację /deszyfrację fragmentów wiadomości SOAP,
     + wsparcie dla WS-Security (szyfracja, deszyfracja, veryfikacja i podpisywanie),
     + definiowanie możliwości użycia załączników wiadomości SOAP,
     + włączanie/wyłączanie podążania za odnośnikami do schematów SOAP,
     + walidację SOAP Action Header,
     + włączanie/wyłączanie możliwości użycia DTD,
     + włączanie/wyłączanie możliwości użycia zewnętrznych referencji,
     + włączanie/wyłączanie możliwości użycia początkowych białych znaków,
     + włączanie/wyłączanie możliwości użycia numerycznych nazw,
     + włączanie/wyłączanie możliwości użycia Processing Instructions,
     + włączanie/wyłączanie możliwości użycia CDATA,
     + ograniczenie długości: dokumentu, elementu, nazwy, wartości atrybutu, Namespace,
     + ograniczenia ilości: zagnieżdżeń w dokumencie, dzieci per element, atrybutów per element, deklaracji NameSpace-ów,
     + definicję dopuszczalnych znaków,
     + definicję sygnatur;
     1. WAF musi umożliwiać blokowanie zapytań z danego obszaru geograficznego. Aktualizacje bazy geolokacyjnej powinny być dostępne w ramach podstawowych opłat wsparcia;
     2. WAF musi umożliwiać automatyczne budowanie polityk w oparciu o skanowanie przez zewnętrznych dostawców (przynajmniej trzech) np. Cenzic, HP WebInspect, IBM AppScan, Qualys Guard, WhiteHat Sentinel;
     3. WAF musi posiadać mechanizmy normalizacji w celu obrony przed technikami ukrywania ataku. Mechanizmy normalizacji muszą wspierać/wykrywać:
     + Directory traversal,
     + Kodowanie typu %u,
     + Kodowanie typu IIS backslash,
     + IIS Unicode codepoints,
     + Bare byte decoding,
     + Apache whitespace,
     + Bad unescape,
     + wstrzykiwanie komentarzy (np. <!-- -->);
     1. Mechanizm normalizacji powinien umożliwiać definiowanie maksymalnego zagnieżdżonego kodowania;
     2. Urządzenie musi wspierać następujące tryby pracy:
     + tryb wykrywania, logowania i blokowania ataków,
     + tryb wykrywania i logowania ataków bez blokowania,
     + tryb uczenia się bez blokowania,
     + tryb uczenia się z blokowaniem i logowaniem;
     1. WAF w trybie nauki, musi umożliwiać automatyczne, stopniowe przełączanie polityki bezpieczeństwa w tryb blokowania, np. servlety/parametry, dla których został zaobserwowany wystarczający ruch dla algorytmu nauki, zostaną przełączone w tryb blokowania, podczas gdy pozostałe pozostaną w trybie transparentnym;
     2. WAF musi umożliwiać integracje systemami antywirusowymi po protokole ICAP w celu wykrywania wirusów w przesyłanych plikach;
     3. WAF musi wykrywać i maskować numery kart kredytowych, wyciekających z chronionej aplikacji; oraz dowolnie inny ciąg znaków zdefiniowany poprzez PCRE regular expression;
     4. WAF musi chronić ruch przesyłany po IPv6 bez degradacji wydajności wynikającej z innych czynników niż różnice protokołów IPv4 i IPv6
     5. System musi umożliwiać szyfrowanie wskazanych pół (np. pole do wprowadzania danych typu hasło) w czasie rzeczywistym, wprowadzanym w przeglądarce internetowej;
     6. Szyfrowanie musi być również dostępne, jeżeli formularz logowania wykorzystuje technologię AJAX. Szyfrowanie tych pól musi odbywać się z wykorzystaniem klucza publicznego osadzanego przez rozwiązanie w odpowiedzi serwera aplikacyjnego. System nie może wymagać zmiany po stronie samej aplikacji ani wymagać instalacji dodatkowego oprogramowania na urządzeniu końcowym;
     7. System musi umożliwiać szyfrowanie w czasie rzeczywistym nazw wskazanych pól w kodzie HTML oraz dodawać dodatkowe pola typu input, by strona logowania www nie była statyczna (dodawanie dodatkowych pól typu input musi być niewidoczne dla użytkownika końcowego na stronie www);
  6. Wysoka dostępność i analityka
     1. System musi posiadać co najmniej następujące interfejsy administracyjne:
     + GUI przy wykorzystaniu protokołu https,
     + zarządzanie poprzez SSH,
     + zarządzanie poprzez API REST;
     1. System musi posiadać moduł analizy ruchu http. Moduł powinien zbierać następujące metryki:
     + czas odpowiedzi per serwer,
     + czas odpowiedzi per URI,
     + ilość sesji użytkownika,
     + przepustowość,
     + adres źródła,
     + kraj,
     + User Agent (wykorzystywana przez klienta aplikacja),
     + metoda dostępu;
     1. System musi posiadać następujące funkcje zarządzania siecią:
     + obsługa protokołu SNMP v1/v2c/v3,
     + możliwość budowania własnych zdarzeń SNMP z własnymi numerami OID,
     + zewnętrzny syslog,
     + możliwość wysyłania logów syslog do więcej niż jednego miejsca docelowego,
     + zbieranie danych i ich wyświetlanie,
     + zbieranie danych zgodnie z ustawieniami administratora,
     + osobna brama domyślna dla interfejsu zarządzającego,
     + wsparcie dla przynajmniej 2 wersji oprogramowania (multi-boot),
     + zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy),
     + dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu systemu;
     1. System musi umożliwiać weryfikację działającego na urządzeniu firmware, czy nie uległ on modyfikacji (TPM Chain of Custody);
     2. System musi posiadać funkcję integracji z zewnętrznymi serwerami uwierzytelnienia użytkowników LDAP, RADIUS, TACACS;
     3. Autoryzacja administratorów systemu musi bazować na rolach użytkowników;
     4. System musi posiadać funkcję definiowania i edycji szablonów konfiguracji aplikacji. Szablony powinny służyć do optymalizacji procesu wdrażania systemu zarówno dla znanych aplikacji biznesowych, jak i własnych aplikacji klienta;
     5. Rozwiązanie musi oferować podział na tzw. partycje administracyjne. Zdefiniowany użytkownik może zarządzać konfiguracją tylko i wyłącznie wewnątrz swojej partycji;
     6. Rozwiązanie musi oferować wsparcie dla tzw. domen routingu (Virtual Routing and Forwarding). Rozwiązanie takie oferuje separację ruchu sieciowego do różnych aplikacji. Musi umożliwiać poprawnie działanie rozwiązania, kiedy podłączone VLANy do urządzenia mają takie same podsieci i adresy IP;
     7. Rozwiązanie musi oferować stworzenie minimum 1000 partycji administracyjnych oraz 1000 jednoczesnych domen routingu. Partycje administracyjne i domeny routingu muszą być dostępne również, jeżeli urządzenie pracuje w formie klastra;
     8. Rozwiązanie musi być umożliwiać pracę w formie klastra wysokiej dostępności (HA) złożonego z dwóch urządzeń (dwóch chassis) tego samego typu pracujących w trybie active – standby z możliwością realizacji trybu active-active oraz rozbudowy do klastra N+1;
     9. W ramach klastra musi istnieć możliwość jednoczesnego wykorzystania różnych modeli urządzeń sprzętowych oraz maszyn wirtualnych;
     10. Klaster wysokiej dostępności musi zapewniać kopiowanie informacji o sesji SSL i stanu sesji TCP pomiędzy urządzeniami, aby uniknąć ponownej negocjacji po przełączeniu ruchu;
     11. Klaster wysokiej dostępności musi zapewniać synchronizację:
     + Konfiguracji,
     + stanu połączeń,
     + przywiązywania sesji (Session persistence),
     + polityk bezpieczeństwa aplikacyjnego;
     1. Wykrycie awarii urządzeń w klastrze odbywać się musi przy użyciu, co najmniej następujących metod:
     + weryfikacja stanu pracy urządzenia poprzez analizę aktywności w sieci (Network failover);
  7. Dostarczone urządzenie musi spełniać następujące wymagania:
     1. Chassis (obudowa) powinna być zgodna ze standardowym RACK 19 calowym;
     2. Wysokość chassis nie więcej niż 4RU;
     3. Chassis musi być wyposażone w co najmniej 4 redundantne zasilacze, umożliwiające zasilanie urządzenia z dwóch obwodów prądu przemiennego o mocy 3000W, 200-240 VAC;
     4. Konstrukcja układu zasilającego musi umożliwiać wymianę uszkodzonego zasilacza bez przerwy w pracy urządzenia (HotSwap);
     5. Chassis powinno umożliwiać instalacje do 8 modułów typu Blade, które zajmują się przetwarzaniem ruchu wraz z chassis oferent dostarczy 2 moduły typu Blade.
     6. Chassis powinno być wyposażone w redundantne moduły kontrolujące działanie całego systemu – System Controllers;
     7. System Controller powinien posiadać dysk twardy o pojemności nie mniejszej niż 960 GB NVMe SSD;
     8. System Controller powinien posiadać co najmniej 32 GB DDR4 pamięci RAM;
     9. System Controller powinien zapewniać zarządzanie stanem modułów Blade;
     10. System Controller powinien przechowywać oprogramowanie dla modułów wykonawczych Blade i instalować oprogramowanie na w/w modułach według ustawień operatora;
     11. System Controller powinien zapewniać komunikację pomiędzy modułami Blade;
     12. Pojemność „switch fabric” warstwy 2 System Controller’a powinna zapewniać komunikację w trybie non-blocking;
     13. System Controller powinien być wyposażony w interfejs do zarządzania typu out-of-band 10G Base-T, port konsolowy oraz port USB 3.0;
     14. Architektura software’owa System Controller’a powinna być oparta o Kubernetes;
     15. System Controller powinien zarządzać alokacją zasobów dla najemców (tenants) w ramach wydzielonych „galwanicznie” stref oraz alokacją maszyn wirtualnych zainstalowanych na modułach Blade.
     16. System Controller powinien umożliwiać grupowanie modułów Blade tak, że:
     + każda grupa modułów Blade ma oddzielne adresy administracyjne,
     + każda grupa modułów Blade może być zarządzana przez odrębnych administratorów,
     + grupa A modułów Blade jest odizolowana sieciowo od grupy B;
     1. Chassis w warstwie 2 powinno umożliwiać grupowanie modułów Blade w niezależne, odseparowane podsystemy, celem izolacji stref sieciowych i izolacji ruchu;
     2. Moduły Blade i chassis powinny umożliwiać wydzielenie środowisk wirtualnych ADC/systemów bezpieczeństwa w obrębie grup tych modułów, tak, że:
     + środowisko wirtualne może być rozciągnięte pomiędzy wieloma modułami Blade przetwarzającymi ruch;
     1. Chassis powinno być wyposażone w display LCD wyświetlający stan systemu;
  8. Każdy z dostarczonych modułów Blade, pracujących w urządzeniu oferowanego systemu, musi spełniać minimalne wymagania przedstawione poniżej:
     1. Pamięć RAM – nie mniej niż 128 GB;
     2. Dysk twardy – jeden dysk 960 GB M.2 NVMe SSD;
     3. Przepływność dla warstwy 4 – nie mniej niż 95 Gbps;
     4. Przepływność dla warstwy 7 – nie mniej niż 95 Gbps;
     5. Ilość transakcji SSL na sekundę dla klucza o długości 2048 – nie mniej niż 100 tysięcy;
     6. Ilość transakcji SSL na sekundę dla szyfru ECDSA P-256 – nie mniej niż 70 tysięcy;
     7. Przepływność ruchu szyfrowanego – nie mniej niż 50 Gbps;
     8. Ilość połączeń na sekundę w warstwie 4 – nie mniej niż 1 200 000;
     9. Kompresja sprzętowa – nie mniej niż 65 Gbps;
     10. Liczba vCPU dla wirtualnych instancji – nie mniej niż 22;
     11. Gęstość interfejsów - nie mniej niż dwa interfejsy z możliwością obsadzenia wkładkami 100Gbps QSFP28 lub 40Gbps QSFP+, oddzielny port USB 3.0.

Dla każdego z dostarczonych modułów Blade mają zostać dostarczone 2 wkładki 100Gbps SR QSFP28. Dopuszcza się tylko moduły w pełni wspierane przez producenta tego urządzenia.

Dodatkowo w ramach dostawy należy dostarczyć moduły optyczne QSFP-100G-SR4 do urządzeń sieciowych Zamawiającego Nexus 9508 oraz kable światłowodowe umożliwiające połączenie pomiędzy dostarczanym urządzeniem a urządzeniami sieciowymi Zamawiającego długości 10m i ułoży (montaż w peszlu). Dopuszcza się tylko moduły w pełni wspierane przez producenta wskazanego urządzenia.