

Opis Przedmiotu Zamówienia
Zakup internetowego, brzegowego systemu bezpieczeństwa

Przedmiotem zamówienia jest dostawa systemu służącego do zabezpieczenia infrastruktury teleinformatycznej ze strony zagrożeń sieci Internet, filtrowaniem treści i filtrowaniem WWW oraz konsoli zarządzającej służącej do zarządzania, monitorowania i raportowania wraz z instalacją, konfiguracją i wdrożeniem oraz ich integracją z systemami istniejącymi w infrastrukturze informatycznej Zamawiającego a także ze wsparciem technicznym i gwarancją na okres 36 miesięcy wraz ze szkoleniami administratorów.

Realizacja przedmiotu Umowy obejmuje wykonanie czterech zadań:

Zadanie 1 - Wykonanie projektu technicznego obejmującego całość wdrożenia oraz przygotowanie procedur eksploatacyjnych i scenariuszy testowych.

Zadanie 2 – Dostawę systemu/oprogramowania i urządzeń do wskazanej przez Zamawiającego lokalizacji wraz ze wszystkimi niezbędnymi komponentami oraz instalację i wdrożenie systemu zapory brzegowej.

Zadanie 3 - Wykonanie Dokumentacji powykonawczej.

Zadanie 4 - Przeprowadzenie szkoleń dla administratorów.

I. Definicje

Na potrzeby niniejszego dokumentu, określenia poniższe będą miały następujące znaczenie:

Aktualizacje	jakiegokolwiek uaktualnienia Oprogramowania, dostarczone w związku z zapewnieniem Wsparcia Technicznego, w tym wyższe wersje (update/upgrade), niższe wersje (downgrade), wydania uzupełniające, patche, zmiany, nowe wersje, poprawki oraz inne dostosowania, w tym wskazane w OPZ, zapewniające prawidłowe korzystanie z takiego oprogramowania
Awaria	nieprawidłowe działanie Urządzeń lub oprogramowania, w szczególności brak możliwości używania Urządzeń lub oprogramowania w sposób zgodny z ich przeznaczeniem lub z dokumentacją producenta i dokumentacją powykonawczą
Asysta techniczna	gwarantowana pomoc w eksploatacji zakupionych w ramach postępowania urządzeń i oprogramowania udzielana Zamawiającemu przez Wykonawcę
Czas naprawy	okres od dokonania zgłoszenia awarii do momentu, w jakim zostanie przywrócona pierwotna funkcjonalność i efektywność działania urządzeń.
Czas reakcji	maksymalny czas, jaki może upłynąć pomiędzy zgłoszeniem do Serwisu Wykonawcy a czasem potwierdzenia przyjęcia zgłoszenia do naprawy przez Serwis Wykonawcy
Dokumentacja	oznacza dokumentację wykonaną przez Wykonawcę i dostarczoną Zamawiającemu w ramach realizacji Umowy, podlegająca zatwierdzeniu przez Zamawiającego, materiały w formie papierowej, jak również informacje zapisane na innych nośnikach, w tym nośnikach elektronicznych.
Dzień roboczy	Oznacza każdy dzień od poniedziałku do piątku w godzinach 8:00 – 16:00, z wyłączeniem dni ustawowo wolnych od pracy.

GUS	Główny Urząd Statystyczny
GUS-WAN	Cała sieć WAN statystyki publicznej oparta o technologię MPLS.
Lokalizacja	Oznacza wskazane przez Zamawiającego miejsce na terytorium Polski, do którego Wykonawca dostarczy wymagane przez Zamawiającego w ramach dostawy urządzenia.
Procedura zastępcza	Procedura zastosowana przez Wykonawcę do czasu docelowego usunięcia Awarii, zapewniająca funkcjonalność i wydajność systemu nie gorszą niż przed awarią.
System/oprogramowanie	Zespół współpracujących ze sobą urządzeń i oprogramowania zabezpieczenia sieciowego, które na bieżąco filtruje ruch sieciowy i blokuje połączenia mogące stanowić potencjalne zagrożenie wraz z systemem zarządzania, monitorowania i raportowania
Urządzenie	Sprzęt wraz z niezbędnym wyposażeniem i odnoszącą się do niego dokumentacją techniczną Producenta będące przedmiotem niniejszego zamówienia.
<u>Wsparcie techniczne</u>	<u>Usługi lub inne świadczenia, zapewniane przez Producenta lub podmiot przez niego autoryzowany w zakresie kompetencji związanych z przedmiotem dostawy, oferowane razem z dostawą, obejmujące co najmniej świadczenia opisane w niniejszym Opisie Przedmiotu Zamówienia.</u>
<u>Wykonawca</u>	<u>Podmiot odpowiedzialny za realizację przedmiotu zamówienia z którym Zamawiający podpisuje umowę.</u>
<u>Zamawiający</u>	<u>Centrum Informatyki Statystycznej dalej CIS</u>

Pozostałe pojęcia użyte w dokumencie należy rozumieć zgodnie z ich ogólnie przyjętym znaczeniem.

II. Opis infrastruktury Zamawiającego

Sieć teleinformatyczna w siedzibie Głównego Urzędu Statystycznego zbudowana jest z przełączników warstwy 3, z przełączników warstwy 2, routerów dostępowych oraz zapor sieciowych i podzielona jest na następujące segmenty:

1. Dostęp do Internetu

Strefa ta składa się z dwóch łączy do niezależnych operatorów oraz dwóch routerów, dwóch przełączników L2 oraz redundantnego firewall'a brzegowego, który będzie podlegał wymianie w ramach przetargu.

2. Strefy DMZ (strefa zdemilitaryzowana)

W strefie tej zainstalowane są serwery służące do komunikacji z systemami oraz użytkownikami zewnętrznymi. Poszczególne strefy DMZ są od siebie odseparowane na poziomie logicznym. Zabezpieczenia stref DMZ realizowane jest przez firewall brzegowy. Reguły na zaporze sieciowej pozwalają jedynie na konkretne połączenia pomiędzy DMZ a siecią wewnętrzną.

3. Sieci GUS-WAN

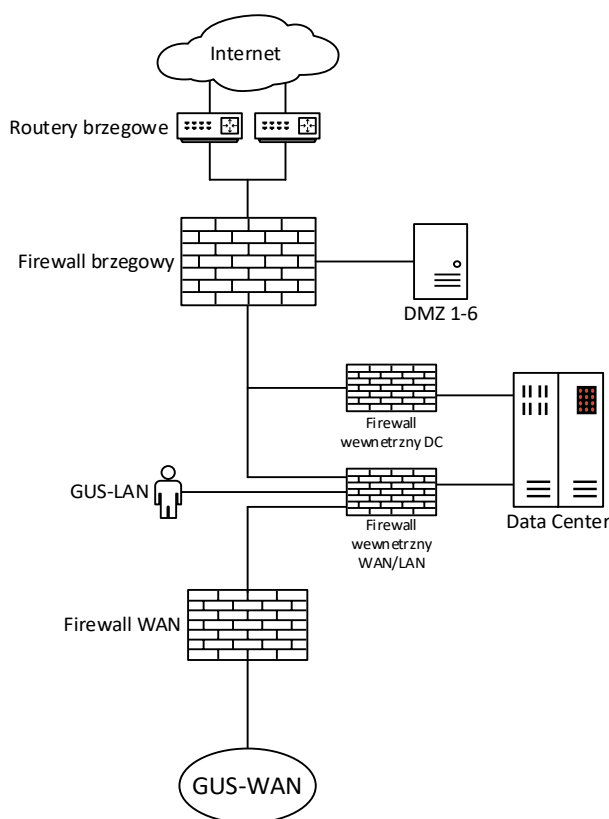
Sieć teleinformatyczna WAN zbudowana jest w oparciu o routery zlokalizowane w siedzibie GUS oraz routery w Urzędach statystycznych i ich Oddziałach.

4. Sieci GUS-LAN

Do tej strefy należą wszystkie zasoby znajdujące się w sieci LAN GUS, w tym: przełączniki szkieletowe, przełączniki agregacyjne, przełączniki dostępowe oraz komputery, laptopy, drukarki i urządzenia wielofunkcyjne.

5. Data Center

Sieć logiczna jest zbudowana w architekturze sieci programowalnych SDN. Zamawiający wykorzystuje oprogramowanie wirtualizacyjne VMware Cloud Foundation Advanced. Dodatkowo, na styku sieci DC, zainstalowany jest firewall wewnętrzny. Logicznie strefa ta jest podzielona na kilkadziesiąt podsieci. W skład tych podsieci wchodzi serwer aplikacji, serwery bazodanowe, serwery BackOffice oraz urządzenia balansujące ruch.



Zamawiający posiada wdrożone rozwiązania typu SIEM oraz system monitorowania infrastruktury oparty o protokół SNMP (v2, v3) do którego podłączone obecnie zainstalowane urządzenia i oczekuje, że nowe rozwiązania (bez ponoszenia dodatkowych kosztów po stronie Zamawiającego) również będzie mogły być zaimplementowane do tego środowiska. Zamawiający realizuje kontrolę dostępu w sieci w oparciu o protokoły Radius, Tacacs oraz Active Directory.

III. Wymagania ogólne

1. W przypadku istnienia wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający,

iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Dostarczone oprogramowanie nie może być zabronione do stosowania przez administrację któregośkolwiek z Państw członkowskich NATO (North Atlantic Treaty Organization).
3. Urządzenia dostarczone przez Wykonawcę muszą być fabrycznie nowe, pochodzić z bieżącej produkcji, nieużywane i niezarejestrowane na innego klienta w bazie klientów producenta sprzętu. Zaoferowany sprzęt nie może być starszy niż 6 miesięcy od daty złożenia oferty oraz by nie był używany w innych projektach, przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania urządzenia.
4. Wykonawca przedstawi Zamawiającemu najpóźniej w dniu dostawy oferowanych urządzeń oświadczenie Producenta lub jego polskiego przedstawicielstwa potwierdzające datę produkcji urządzeń.
5. Sprzęt zaoferowany i dostarczony przez Wykonawcę w ramach realizacji zamówienia będzie pochodzić z autoryzowanego kanału sprzedaży Producenta na rynek Unii Europejskiej i nie będzie w dniu składania oferty przeznaczony przez Producenta do wycofania z produkcji.
6. Wraz z dostawą systemu/oprogramowania i urządzeń Wykonawca dostarczy:
 - a) dokument potwierdzający, że oprogramowanie w nim zawarte jest licencjonowane na Zamawiającego,
 - b) dokument potwierdzający zarejestrowanie kontraktu i dokument potwierdzający bezpośredni dostęp Zamawiającego do bazy wiedzy, do najnowszych wersji oprogramowania i jego aktualizacji, poprawek, zgłoszeń dotyczących awarii, usterek oprogramowania i wsparcia technicznego i dokumentacji, w ramach stron WWW Producenta, dostępnych po zalogowaniu na indywidualne konto Zamawiającego,
 - c) szczegółową dokumentację techniczną producenta oferowanych urządzeń, potwierdzającą spełnianie wymagań technicznych urządzeń będących przedmiotem zamówienia.
7. Zamawiający zastrzega sobie możliwość zwrócenia się do Producenta oferowanych produktów o potwierdzenie, że oferowany sprzęt i licencje nie były przeznaczone dla innego odbiorcy (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację) jak również zastrzega sobie prawo sprawdzenia u Producenta warunków gwarancyjnych i wsparcia na oferowane rozwiązanie.
8. Wykonawca w terminie 7 dni od zawarcia umowy dostarczy Zamawiającemu (do akceptacji i stosowania) procedury zgłaszania i obsługi awarii wraz z listą osób upoważnionych do kontaktów, wykazem adresów poczty elektronicznej, nr telefonów.
9. Strony zobowiązują się do wzajemnego przekazywania sobie niezwłocznie wszelkich informacji mogących mieć wpływ na realizację zamówienia. Wykonawca niezwłocznie udzieli odpowiedzi w formie pisemnej na zgłaszane przez Zamawiającego uwagi dotyczące realizacji zamówienia, w terminie nie dłuższym niż 2 dni robocze.

10. Wskazane osoby skierowane przez Wykonawcę do realizacji umowy zobowiązane są do przestrzegania postanowień regulaminów wewnętrznych i stosowania odpowiednich procedur obowiązujących u Zamawiającego. Powyższe zostanie potwierdzone pisemnym oświadczeniem każdej z osób wyznaczonych do realizacji umowy.
11. Nośniki informacji takie jak, np. dyski twarde, pamięci flash, mogą być naprawiane jedynie w miejscu ich użytkowania, a w przypadku konieczności wymiany uszkodzonych nośników na nowe, wolne od wad, nośniki informacji pozostają u Zamawiającego. W przypadku konieczności dokonania naprawy sprzętu wyposażonego w nośniki informacji poza miejscem użytkowania, nośniki pozostają w siedzibie Zamawiającego.
12. Wykonawca zobowiązuje się, że nie będzie dokonywał żadnych modyfikacji sprzętu bez wcześniejszego uzgodnienia ich z Zamawiającym. Zamawiający zastrzega sobie prawo do samodzielnej modyfikacji sprzętu i dokonywania zmian w konfiguracji.
13. Odbiór systemu zapory brzegowej nastąpi po sprawdzeniu kompletności urządzeń, oprogramowania, dokumentacji powykonawczej oraz po osiągnięciu przez dostarczone urządzenia pełnej wymaganej funkcjonalności po ich instalacji i konfiguracji.

IV. Gwarancja – poziom usług serwisowych

1. Gwarancja Producenta na dostarczone w ramach zamówienia Urządzenie musi obejmować okres 36 miesięcy od daty podpisania protokołu odbioru wdrożenia systemu zapory brzegowej. W tym okresie Wykonawca zobowiązuje się zapewnić dostęp do wszelkich aktualizacji i oprogramowania oraz sygnatur bezpieczeństwa rozwiązania będącego przedmiotem umowy.
2. Gwarancja powinna zawierać wsparcie techniczne świadczone przez producenta urządzenia lub jego autoryzowanego przedstawiciela i obejmować wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, aktualizację sygnatur, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.
3. Wykonawca udzieli Zamawiającemu gwarancji na wykonaną usługę instalacji, konfiguracji i wdrożenia z istniejącą infrastrukturą obejmującą poprawę wykrytych ewentualnie błędów konfiguracji realizowanych wg założeń Zamawiającego na okres 36 miesięcy od daty podpisania protokołu odbioru wdrożenia systemu zapory brzegowej.
4. Dla zapewnienia możliwie największego bezpieczeństwa i wysokiego poziomu pewności usługi gwarancyjnej Zamawiający wymaga aby:
 - a) serwis gwarancyjny dla zaoferowanych urządzeń umożliwiał obsługę zgłoszeń awarii i zapytań o pomoc techniczną nawet w przypadku, gdy Wykonawca utraci autoryzację producenta - wymagane pakiety serwisowe mają dać gwarancję zachowania podstawowych praw serwisowych dla sprzętu niezależnie od przyszłej kondycji Wykonawcy,
 - b) serwis gwarancyjny zapewniał możliwość bezpłatnego przejęcia usług przez innego partnera lub producenta w przypadku niewywiązywania się Wykonawcy z przyjętych zobowiązań.
5. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
6. Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowanie uprawnień Zamawiającego wynikających z rękojmi za wady.

7. Wykonawca zobowiązuje się do świadczenia usług gwarancji w tym wsparcia technicznego z należytą starannością, z uwzględnieniem ogólnie przyjętych i stosowanych standardów i procedur przy tego rodzaju usługach, a także zaleceń lub procedur określonych przez Producenta sprzętu.
8. Wykonawca zobowiązuje się świadczyć usługi gwarancyjne w miejscu użytkowania sprzętu, z możliwością naprawy w serwisie Wykonawcy, jeżeli naprawa sprzętu w miejscu użytkowania okaże się niemożliwa.
9. W przypadku braku możliwości dokonania naprawy w miejscu użytkowania sprzętu i konieczności jego dostarczenia do punktu serwisowego wskazanego przez Wykonawcę, koszty dostarczenia uszkodzonego sprzętu do punktu serwisowego oraz z punktu serwisowego do miejsca użytkowania pokrywa Wykonawca.
10. Wykonawca zobowiązuje się do ponoszenia wszelkich kosztów naprawy sprzętu, w tym kosztów części zamiennych i podzespołów transportu, instalacji, konfiguracji i uruchomienia sprzętu.
11. Do dostarczonego sprzętu będą dołączone karty gwarancyjne zawierające numery seryjne urządzeń i podzespołów/modułów, termin i warunki ważności gwarancji, adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne.
12. Wykonawca zobowiązuje się przyjmować zgłoszenia gwarancyjne poprzez stronę www Wykonawcy dostępną przez całą dobę, 365 dni w roku.
13. Wykonawca dostarczy dane niezbędne do autoryzacji na stronie www Wykonawcy w celu dokonywania zgłoszeń serwisowych przez Zamawiającego.
14. Zamawiający wymaga również zapewnienia możliwości dokonywania zgłoszeń serwisowych poprzez e-mail w przypadku braku możliwości dokonania zgłoszenia serwisowego przez stronę www (np. w przypadku braku dostępności dedykowanej strony www).
15. Wykonawca potwierdzi otrzymanie zgłoszenia serwisowego poprzez wysłanie wiadomości e-mail na adres Zamawiającego.
16. Wszelkie wykonane przez Wykonawcę lub jego przedstawicieli czynności serwisowe wymagają dokumentowania w formie pisemnej.
17. Zgłoszenia o awariach będą przyjmowane przez 24 godz. na dobę, przez 7 dni w tygodniu, 365 dni w roku.
18. Wymagany czas na wykonanie naprawy wynosi 24 godziny od momentu potwierdzenia zgłoszenia telefonicznego lub pisemnie do siedziby serwisu, natomiast działania serwisowe należy podjąć w ciągu 4 godzin od momentu zgłoszenia telefonicznego lub pisemnie do siedziby serwisu.
19. Zamawiający dopuszcza możliwość usunięcia awarii lub usterki poprzez dostarczenie i uruchomienie sprzętu zastępczego z zachowaniem terminów określonych w pkt. 18. Wykonawca zobowiązany jest do dostarczenia w tym terminie Zamawiającemu kompatybilnego sprzętu zastępczego, wolnego od wad, o parametrach wydajnościowych i funkcjonalnych nie gorszych niż sprzęt podlegający naprawie, zobowiązując się jednocześnie do usunięcia awarii lub usterki w terminie nie dłuższym niż 30 dni od przesłania zgłoszenia serwisowego.
20. Dostarczenie przez Wykonawcę w wymaganym przez Zamawiającego terminie sprzętu zastępczego będzie traktowane jako wykonanie naprawy.
21. Przez usunięcie awarii należy rozumieć przywrócenie funkcjonalności sprzętu z przed awarii we wszystkich modułach i zaprzestaniu stosowania przez obsługę w bieżącej pracy rezerwowego sprzętu i/lub zastępczych procedur.

22. W przypadku usunięcia awarii przez Wykonawcę poprzez wymianę elementów, zostaną zainstalowane fabrycznie nowe elementy o parametrach wydajnościowych i funkcjonalnych nie gorszych niż elementy wymieniane.
23. Po usunięciu każdej awarii, Wykonawca zobowiązuje się do doprowadzenia całego sprzętu do stanu integralnej całości w rozumieniu poprawnego działania wszystkich zainstalowanych modułów.
24. Czas naprawy liczony będzie w godzinach, od momentu wysłania przez Zamawiającego do Wykonawcy formularza „Zgłoszenie o świadczenie usługi gwarancyjnej/asysty technicznej”.
25. Fakt awarii, naprawy i ewentualnie wymiany sprzętu na nowy będzie każdorazowo odnotowywany w karcie gwarancyjnej.
26. Wykonawca zobowiązany jest w dniu wykonania naprawy do potwierdzenia wykonania naprawy na protokole zgłoszenia serwisowego. Ww. dokument musi zostać podpisany (data, godzina i podpis) przez przedstawiciela Zamawiającego. Data i godzina podpisania ww. dokumentu bez zastrzeżeń przez przedstawiciela Zamawiającego jest datą i godziną wykonania usługi naprawy.
27. W przypadku wystąpienia awarii tego samego elementu po wykonaniu 3 napraw w okresie obowiązywania umowy, Wykonawca zobowiązuje się na pisemne wezwanie Zamawiającego do wymiany tego elementu na fabrycznie nowy, nieużywany i wolny od wad, tego samego producenta i tego samego typu, o parametrach wydajnościowych i funkcjonalnych nie gorszych niż element wymieniany w terminie 30 dni od dnia otrzymania od Zamawiającego wezwania do wymiany. Nowe elementy muszą być wyprodukowane nie wcześniej niż 6 miesięcy przed terminem składania ofert.
28. W przypadku dokonania naprawy przez Wykonawcę poprzez wymianę elementów, zostaną zainstalowane fabrycznie nowe elementy o parametrach wydajnościowych i funkcjonalnych nie gorszych niż elementy wymieniane.
29. W okresie udzielonej gwarancji Wykonawca zobowiązuje się do stałego monitorowania podatności i luk bezpieczeństwa dostarczonego systemu oraz informowania Zamawiającego o metodach usuwania przedmiotowych podatności w systemie.
30. W okresie udzielonej gwarancji Wykonawca zobowiązuje się do współpracy z Zamawiającym w zakresie wykrytych przez Zamawiającego, bądź podmiot trzeci podatności i luk w systemie oraz zobowiązuje się do niezwłocznego zgłoszenia do Producenta zmian i poprawek w systemie.
31. W okresie udzielonej gwarancji w ramach asysty technicznej Wykonawca zobowiązuje się do współpracy z Zamawiającym w zakresie kontroli i audytów systemu, wykonanych w ramach wewnętrznych struktur Zamawiającego lub wykonywanych przez niezależne podmioty zewnętrzne.

V. Asysta techniczna Wykonawcy

1. Wykonawca zapewni świadczenie usługi asysty technicznej w ramach której zapewni:
 - a) stabilną pracę wdrożonego systemu,
 - b) dodawanie nowych, określonych przez Zamawiającego funkcjonalności,
 - c) dostosowanie systemu do nowych rozwiązań technologicznych,
 - d) porady eksperckie,
 - e) dodatkowe integracje z systemami wewnętrznymi,
 - f) nie rzadziej niż raz na 180 dni, analizę w zakresie uaktualnień poziomu oprogramowania sprzętu, poziomu firmware'u (mikrokodów);

2. Usługi asysty technicznej będą świadczone i rozliczane w wymiarze 48 roboczogodzin na okres 12 miesięcy (w roboczogodzinę wsparcia nie wlicza się czasu dojazdu oraz ilości osób świadczących usługę, tzn. nie ma znaczenia ile osób jednocześnie będzie świadczyło usługę w ramach jednej roboczogodziny). Usługa będzie świadczona dla infrastruktury Zamawiającego (sprzętu i oprogramowania).
3. Asysta techniczna będzie świadczona w języku polskim i realizowana zdalnie lub lokalnie w zależności od metodyki właściwej dla zdefiniowanego problemu według decyzji Wykonawcy. Na wyraźne wezwanie Zamawiającego inżynier wsparcia technicznego ma obowiązek przybyć do siedziby Zamawiającego i tam realizować zgłoszenie.
4. W ramach asysty technicznej Wykonawca zapewni, zgodnie z potrzebami Zamawiającego, co najmniej dwóch inżynierów, którzy posiadają certyfikat na poziomie minimum certyfikowany administrator bezpieczeństwa oraz certyfikowany ekspert ds. bezpieczeństwa w zakresie wdrożonego sprzętu. Osoby skierowane do realizacji zamówienia muszą posiadać aktualne certyfikaty w okresie obowiązywania umowy.
5. Zakres czynności wykonywanych w ramach asysty technicznej nie może być tożsamy z zakresem objętym serwisem gwarancyjnym. W przypadku, gdy Zamawiający zleci Wykonawcy prace, które powinny być zrealizowane w ramach serwisu gwarancyjnego, Wykonawca ma obowiązek poinformowania o tym fakcie Zamawiającego.
6. Zamawiający będzie przekazywać Wykonawcy zlecenia w ramach asysty technicznej, w których określi przedmiot zlecenia oraz określi maksymalny, oczekiwany termin realizacji zlecenia.
7. Wykonawca w terminie wyznaczonym przez Zamawiającego, nie krótszym niż jeden dzień roboczy od otrzymania zlecenia, przekaże Zamawiającemu propozycję wykonania zlecenia zawierającą w szczególności zakres prac zawartych w zleceniu oraz proponowaną liczbę roboczogodzin niezbędnych do wykonania zlecenia.
8. Zamawiający może zaakceptować propozycję wykonania zlecenia albo zażądać od Wykonawcy, w wyznaczonym terminie, dodatkowych wyjaśnień, informacji do przedstawionej propozycji wykonania zlecenia.
9. W przypadku akceptacji propozycji wykonania zlecenia Zamawiający przedłoży Wykonawcy zaakceptowane zlecenie zawierające w szczególności zakres prac, liczbę roboczogodzin niezbędną do wykonania prac, termin wykonania prac.
10. Rozliczenie godzin w ramach asysty technicznej odbywać się będą na podstawie podpisanych bez zastrzeżeń, przez Wykonawcę i Zamawiającego „**Protokół odbioru usługi gwarancyjnej/ asysty technicznej**”

VI: Realizacja przedmiotu umowy

Zadanie 1.

Wykonanie projektu technicznego obejmującego całość wdrożenia oraz przygotowanie procedur eksploatacyjnych i scenariuszy testowych.

W ramach realizacji tego zadania Wykonawca zrealizuje następujące prace:

1. Przeprowadzi szczegółową analizę potrzeb Zamawiającego w zakresie stawianych wymagań w celu dostosowania projektu technicznego z uwzględnieniem możliwości skalowalności rozwiązania.

2. Analiza będzie obejmować spotkania robocze, w trakcie, których Zamawiający przedstawi szczegółową budowę sieci wraz z konfiguracją poszczególnych urządzeń, w zakresie niezbędnym do realizacji przedmiotu zamówienia.
3. Obecna infrastruktura sieciowa jest kompletna i poprawnie realizuje założone funkcjonalności. Jednakże ze względu na złożony charakter zamówienia Zamawiający wymaga, aby Wykonawca w przypadku potrzeby dodatkowej instalacji technicznej poinformował Zamawiającego o takiej sytuacji oraz uzgodnił z Zamawiającym sposób rozwiązania zagadnienia technicznego.
4. Projekt Techniczny musi być wykonany przez Wykonawcę w oparciu o propozycję rozwiązań technicznych bazujących na opisie przedmiotu zamówienia, wymaganiach przedstawionych przez administratorów Zamawiającego oraz zaleceniach producenta urządzeń i dobrych praktykach w tym zakresie.
5. Projekt techniczny powinien uwzględniać wszystkie prace prowadzone w Data Center Zamawiającego przy urządzeniach dostarczanych w ramach postępowania.
6. Projekt techniczny przygotowany przez Wykonawcę powinien:
 - a) dokumentować wszystkie prace wykonane przy urządzeniach Zamawiającego zgodnie z zebranymi wymogami i obejmować wszystkie prace obejmujące dostarczone i posiadane urządzenia w lokalizacji Zamawiającego,
 - b) przewidywać rozbudowę i modernizację systemu służącego do zabezpieczenia sieci komputerowej i serwerowej o elementy, które zapewnią zwiększenie funkcjonalności zapory brzegowej.
7. Wykonawca przygotowuje koncepcję konfiguracji wdrażanych zapór brzegowych, zapewniającą integrację budowanego rozwiązania z istniejącą siecią Zamawiającego wprowadzając wysoki poziom bezpieczeństwa, kontroli ruchu oraz wysoką dostępność, niezawodność, minimalizację opóźnień oraz szybką konwergencję sieci w razie awarii.
8. Wykonawca opracuje koncepcję konfiguracji w zakresie zabezpieczenia budowanego rozwiązania oraz przygotowuje i określi (w porozumieniu z Zamawiającym) wymagania co do stref bezpieczeństwa, translacji ruchu – wraz z określeniem niskopoziomowych polityk bezpieczeństwa.
9. Wykonawca w ramach projektu uwzględni protokoły używane obecnie w sieci Zamawiającego - planowane wdrożenie powinno uwzględniać dostarczenie podobnej - nie gorszej od obecnej - funkcjonalności do wykorzystywanych protokołów.
10. W ramach realizacji zadania Wykonawca dostarczy następujące dokumenty:
 - a) Szczegółowy Projekt Techniczny
 - b) Specyfikacja Wymagań dla Lokalizacji – dokument zawierać będzie szczegółową specyfikację wymagań elektrycznych, fizycznych i środowiskowych, które muszą być spełnione przez Zamawiającego dla umożliwienia instalacji urządzeń.
 - c) Plan Testów – dokument zdefiniuje i opisz zakres procedur i/lub testów, które są niezbędne dla przetestowania i ustalenia „gotowości do pracy” poszczególnych urządzeń.
11. Projekt techniczny będzie podlegał procedurze odbioru, na następujących warunkach:
 - a) Wykonawca przekaże Zamawiającemu drogą elektroniczną do akceptacji projekt techniczny w terminie nie dłuższym niż 21 dni kalendarzowych od dnia zawarcia umowy,
 - b) Zamawiający w terminie nie dłuższym niż 3 dni kalendarzowe od dnia dostarczenia projektu technicznego, poinformuje Wykonawcę o jego akceptacji lub konieczności wprowadzenia zmian,

- c) Wszystkie uwagi do projektu technicznego zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 3 dni kalendarzowe od dnia ich otrzymania,
 - d) Zamawiający w terminie 3 dni kalendarzowe od dnia powtórnego dostarczenia przez Wykonawcę poprawionego projektu technicznego, poinformuje wykonawcę o jego akceptacji lub konieczności wprowadzenia zmian,
 - e) Zamawiający zastrzega sobie prawo do dwukrotnego zgłoszenia zmian w projekcie technicznym,
 - f) W przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia Projektu technicznego nie później niż po 5 dniach kalendarzowych.
 - g) Komunikacja pomiędzy Zamawiającym a Wykonawcą w zakresie akceptacji projektu technicznego, następować będzie drogą mailową na adresy Wykonawcy i Zamawiającego wskazane w umowie;
12. Zatwierdzony Projekt techniczny zostanie przekazany Zamawiającemu najpóźniej w dniu podpisania **protokołu odbioru projektu technicznego**.
13. Potwierdzeniem odbioru Projektu technicznego będzie „Protokół odbioru projektu technicznego” podpisany z wynikiem pozytywnym.

Zadanie 2.

Dostawa systemu/oprogramowania i urządzeń do wskazanej przez Zamawiającego lokalizacji wraz ze wszystkimi niezbędnymi komponentami oraz instalacja i wdrożenie systemu zapory brzegowej.

A. Zakup i dostawa urządzeń zapory brzegowej (HA) w konfiguracji minimum.

Wykonawca dostarczy do wskazanej lokalizacji Zamawiającego wymagane urządzenia wraz z oprogramowaniem, zgodne z poniższym opisem:

Produkt	SKU	Ilość
Quantum Force 29100 Plus Appliance with SandBlast subscription package for 1 year	CPAP-SG29100-PLUS-SNBT	2
Next Generation Threat Prevention for additional 2 years for 29100 PLUS Appliance	CPSB-NGTP-29100-PLUS-2Y	2
2 Port 40GBase QSFP+ / 100GBase QSFP28 interface card for 19000/29000 appliances	CPAC-2-40/100F-D	2
SFP+ transceiver for 10G fiber Ports- short range (10GBase-SR)- for 19000/29000 appliances	CPAC-TR-10SR-D	16
Bi-directional QSFP28 transceiver for 100G fiber Ports - short range (100GBase-SR-BD)	CPAC-TR-100SR-BiDi	4
SFP28 transceiver module for 25G fiber ports- short range (25GBase-SR)- for 19000/29000 appliances	CPAC-TR-25SR-D	8
Smart-1 600-M Base Gen-6 Security Management appliance for 25 gateways	CPAP-NGSM600M-BASE-EVNT	1
Smart-1 6000-L Base SmartEvent appliance for 75 gateways (perpetual)	CPAP-NGSM6000L-BASE-EVNT	1

Zamawiający dopuszcza składanie ofert równoważnych w rozumieniu art. 99 ust. 5 ustawy Pzp. W przypadku zaoferowania rozwiązania równoważnego na Wykonawcy spoczywa obowiązek wykazania jego równoważności.

Zastosowanie rozwiązania równoważnego nie będzie wymagało żadnych nakładów po stronie Zamawiającego celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury.

Zamawiający dopuszcza dostarczenie przez Wykonawcę urządzeń równoważnych spełniających poniższe wymagania:

I. 2 szt. urządzeń typu NG Firewall – system HA

1. Wszystkie wymagane funkcjonalności muszą być dostępne w dniu składania oferty.
2. System zabezpieczeń musi być dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance) przystosowane do instalacji w szafach rack 19 cali.
3. W komplecie muszą znajdować się szyny umożliwiające montaż urządzenia w szafie rack oraz kable zasilające, zaślepki na miejsca dla nieużywanych modułów itp.
4. W ramach postępowania muszą zostać dostarczone dwa kompletne, gotowe do pracy urządzenia skonfigurowane w trybie HA (ang. High Availability).
5. Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta.
6. System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
7. System musi umożliwiać działanie w następujących trybach pracy:
 - a) rutera (tzn. w warstwie 3 modelu OSI),
 - b) przełącznika (tzn. w warstwie 2 modelu OSI),
 - c) w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA),
 - d) w trybie pasywnego nasłuchu (sniffer/tap).
8. System musi obsługiwać adresy IPv4 oraz IPv6. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF dla IPv4 i IPv6.
9. System musi obsługiwać nie mniej niż 5 wirtualnych instancje systemu zabezpieczeń (w zakresie VPN, Firewall, IPS, Routing). Protokoły routingu dynamicznego nie mniej niż RIP, OSPF, BGP muszą być dostępne w każdym z wirtualnych systemów.
10. Każde z urządzeń w klastrze HA musi być wyposażone w co najmniej następujące interfejsy sieciowe:
 - a) 8 portów 1/10GBASE-F obsadzone wkładkami SFP+,
 - b) 4 porty 10/25GBASE-F obsadzone wkładkami min. 10 Gbps,
 - c) 2 porty 40/100GBASE-F obsadzone wkładkami min. 40 Gbps.
11. Każde z urządzeń w klastrze HA musi być wyposażone w co najmniej jeden port konsoli oraz w co najmniej jeden dedykowany port zarządzający.
12. System musi być wyposażony w co najmniej 1 parę dedykowanych portów na potrzeby HA.
13. Każde z urządzeń w klastrze HA musi posiadać przepustowość ruchu co najmniej 30 Gbit/s dla kontroli zawartości tj.: firewall, kontrola aplikacji na wszystkich portach, IPS, antywirus, antymalware i antyspyware. Wydajność IPsec VPN urządzenie musi wynosić co najmniej 75 Gbit/s.

14. Każde z urządzeń w klastrze HA musi obsługiwać nie mniej niż 20 000 000 jednoczesnych połączeń i umożliwiać zestawianie nie mniej niż 900 000 połączeń na sekundę.
15. Każde z urządzeń w klastrze HA musi posiadać co najmniej 2 redundantne zasilacze umożliwiające podłączenie urządzenia do sieci energetycznej 230V.
16. System zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
17. Polityki zabezpieczeń firewall muszą uwzględniać:
 - a) adresy IP klientów i serwerów,
 - b) protokoły i usługi sieciowe,
 - c) aplikacje,
 - d) kategorie URL,
 - e) użytkowników aplikacji i grupy,
 - f) reakcje zabezpieczeń,
 - g) rejestrowanie zdarzeń i alarmowanie
18. System musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. musi blokować wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
19. System musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania.
20. System musi pozwalać na blokowanie ruchu na podstawie dynamicznych, zewnętrznych źródeł danych (przynajmniej plików TXT).
21. System zabezpieczeń musi umożliwiać blokowanie transmisji plików na podstawie nagłówka MIME, na podstawie rozszerzenia.
22. System musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników - integracja z Active Directory. Polityka kontroli dostępu (firewall) powinna precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci.
23. Każde z urządzeń w klastrze HA musi pozwalać na lokalne (na dysk urządzenia) zbieranie i analizowanie logów. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu URL, deszyfracji SSL.
24. System musi wykonywać statyczną i dynamiczną translację adresów NAT (musi wspierać zarówno SNAT jak i DNAT).
25. System musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN).
26. System musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja/polityka przynajmniej dla ruchu http, smtp, imap, pop3, ftp, smb - bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirusowych musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
27. System musi posiadać moduł wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywana na urządzeniu, regularnie

aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

28. System musi posiadać moduł antymalware lub antyspyware. Baza sygnatur musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
 29. Zarządzanie systemem musi odbywać się ze stacji administratora poprzez linię poleceń (CLI) oraz graficzną konsolę Web GUI lub dedykowaną aplikację.
 30. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
 31. System bezpieczeństwa musi umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż baza lokalna oraz serwer Radius.
 32. Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji.
 33. Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania SSH.
 34. System musi zapewniać możliwość rozbudowy o funkcjonalności:
 - a) DNS sinkholing. Funkcjonalność zabezpieczania DNS dostępna na urządzeniu musi umożliwiać procesowanie zapytań DNS w celu wykrywania i blokowania: zagrożeń, wycieku danych (exfiltracja), tunelowania DNS.
 - b) Przechwytywanie i przesyłanie do zewnętrznych systemów typu „SandBox” plików różnych typów przechodzących przez firewall w celu ochrony przed zagrożeniami typu zero-day.
 - c) Możliwość filtrowania URL, musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. Wymagane jest posiadanie oddzielnych kategorii dla zagrożeń typu malware, phishing, command-and-control oraz ostatnio zarejestrowane domeny (NRD). Równolegle z oceną URL musi być dokonywany i określany poziom ryzyka związany z danym URL na poziomie małe ryzyko, średnie ryzyko, wysokie ryzyko.
- Zamawiający nie wymaga powyższych funkcjonalności w momencie dostarczenia systemu przez Wykonawcę.
35. Zamawiający dopuszcza by funkcja ręcznego tworzenia sygnatur (IPS) była realizowana bezpośrednio na urządzeniu lub na konsoli zarządzającej.
 36. Urządzenie musi posiadać możliwość wykonania kopii migawkowych oraz jej odtworzenie, zawierających konfigurację wraz z systemem operacyjnym w formie pliku binarnego.
 37. Zamawiający wymaga następujących funkcjonalności wraz z niezbędnymi subskrypcjami/licencjami, jeśli są one konieczne: IPS, Antywirus, Kontrola aplikacji, Antymalware, Antyspyware.
 38. Zamawiający wymaga zapewnienia odpowiednich subskrypcji, gwarancji i licencji dla systemu w okresie trwania gwarancji.

II. 1 szt. Centralny System Zarządzania i Raportowania (CSZiR)

1. Zamawiający posiada centralny system zarządzania firmy Check Point (Smart-1 6000L APPLIANCE, Smart-1 600M MANAGEMENT APPLIANCES) który udostępni Wykonawcy do wykorzystania w celu zbudowania systemu zarządzania i raportowania.

W przypadku wykorzystania tych urządzeń Wykonawca zobowiązuje się do objęcia ich wsparciem producenta na okres trwania gwarancji.

2. W przypadku jeżeli Wykonawca nie wykorzysta udostępnionych w pkt. 1 urządzeń jest zobowiązany dostarczyć wraz z urządzeniami NGFW:
 - a) oprogramowanie zarządzania i raportowania przystosowane do współpracy z dostarczonymi urządzeniami,
 - b) odpowiednią, komercyjną platformę sprzętową (appliance) z systemem operacyjnym wraz z licencjami (o ile będzie wymagana) i gwarancją na okres trwania umowy,
 - c) przeszkolić 6 pracowników Zamawiającego w zakresie administracji i użytkowania dostarczonego systemu zarządzania zgodnie z zapisami ogólnymi zawartymi w Zadaniu 4.
3. Centralny System Zarządzania i Raportowania musi być spójny i kompatybilny z urządzeniami dostarczonymi w ramach postępowania i stanowić produkt tego samego producenta co oferowane urządzenia.
4. CSZiR musi umożliwiać zarządzanie urządzeniami typu NG Firewall HA. Poprzez zarządzanie należy rozumieć konfigurację polityki bezpieczeństwa (polityka firewall, VPN, polityka ochrony antywirusowej, antyspamowej, ochrony przed atakami sieciowymi, atakami typu botnet, kontrola aplikacji), zarządzanie kontami administratorów i użytkowników, obsługę zdarzeń generowanych przez moduły zapór sieciowych.
5. System musi umożliwiać zarządzanie urządzeniami NGFW w zakresie określonym w Zadaniu 2 pkt. I.
6. CSZiR musi umożliwiać obsługę logów co najmniej w zakresie:
 - a) logów ruchu sieciowego (w tym traffic, threat, IPS, AV, itp.):
 - i. 3000 zdarzeń na sekundę,
 - ii. retencja danych nie mniej niż 100 dni;
 - b) logów administracyjne (w tym logi systemowe, uwierzytelnienia administratorów, aktualizacje, zmiany konfiguracyjne, itp.):
 - i. 100 logów na sekundę,
 - ii. retencja danych nie mniej niż 730 dni.
7. CSZiR powinien być obsługiwany za pomocą konsoli użytkownika, która ma być dostarczona w postaci graficznej konsoli administratora (GUI) działającej pod systemem operacyjnym Windows. Konsola zarządzania powinna posiadać możliwości automatycznej weryfikacji spójności i niesprzeczności wprowadzonej polityki bezpieczeństwa.
8. Komunikacja pomiędzy modułem zapory sieciowej (funkcjonujących na zewnętrznych urządzeniach) i modułem zarządzania i raportowania (CSZiR) powinna być szyfrowana i uwierzytelniona z użyciem certyfikatów cyfrowych generowanych przez moduł zarządzania i raportowania(CSZiR).
9. Komunikacja pomiędzy interfejsem GUI i modułem zarządzania i raportowania (CSZiR) musi być szyfrowana.
10. Uwierzytelnianie administratorów powinno umożliwiać wykorzystanie następujących metod:
 - a) kont lokalnych,
 - b) zewnętrznym serwerem RADIUS,

- c) uwierzytelnienie wieloskładnikowe przynajmniej na podstawie loginu i hasła oraz przynajmniej certyfikatu dla przeglądarki/urządzenia lub kodu OTP lub tokenu sprzętowego
11. Musi istnieć możliwość definiowania szczegółowych uprawnień administratorów, minimalnie:
 - a) do odczytu logów,
 - b) do przeglądania konfiguracji zapory brzegowej,
 - c) do administracji urządzeniami systemu zapory brzegowej,
 - d) do administracji kontami użytkowników poszczególnych elementów systemu.
 12. System zarządzania i raportowania (CSZiR) musi być w stanie wyświetlić z graficznej konsoli listę aktywnych połączeń obsługiwanych przez moduły zapór sieciowych. Informacja o połączeniu powinna zawierać minimum adres źródła, adres przeznaczenia, port źródła, port przeznaczenia oraz identyfikator usługi sieciowej.
 13. System zarządzania i raportowania (CSZiR) musi umożliwiać wyszukiwanie i filtrację zdarzeń wygenerowanych przez moduły zabezpieczeń. Administrator powinien móc zdefiniować własne szablony wyszukiwania i wyświetlania zdarzeń.
 14. CSZiR musi umożliwiać monitorowanie i prezentowanie za pomocą graficznej konsoli takich parametrów zarządzanych zapór sieciowych takich jak: średnie obciążenie procesora, zajętość pamięci operacyjnej, zajętość przestrzeni dyskowej, wersję oprogramowania zapory sieciowej, nazwę i wersję zainstalowanej polityki bezpieczeństwa.
 15. CSZiR musi umożliwiać graficzne wyświetlanie statystyk ruchu sieciowego, przetwarzanego przez zapory sieciowe.
 16. CSZiR musi pobierać dzienniki zdarzeń (logi) z urządzeń przez niego zarządzanych i na tej podstawie przedstawiać administratorom informacje na temat stanu bezpieczeństwa i wykrytych incydentów.
 17. CSZiR musi posiadać możliwość prezentacji zdarzeń zgodnie z określonymi przez administratora parametrami dla zadanego przedziału czasu i wyświetlane zbiorczo w postaci graficznej.
 18. CSZiR musi umożliwiać graficzną prezentację zdarzeń pogrupowanych w zależności od kraju pochodzenia źródła transmisji.
 19. System raportowania musi posiadać możliwość powiadamiania administratorów co najmniej za pomocą email, SNMP trap w przypadku zaistnienia określonego zdarzenia.
 20. Dostarczone rozwiązanie musi umożliwiać wykonywanie kopii zapasowych konfiguracji urządzeń i polityk bezpieczeństwa oraz ich odtwarzanie z poziomu systemu zarządzania.
 21. Kopia zapasowa wykonana za pomocą systemu zarządzania musi umożliwiać odtworzenie konfiguracji i polityk bezpieczeństwa na tym samym lub innym urządzeniu tego samego typu i o takiej samej konfiguracji sprzętowej w przypadku wymiany lub awarii.
 22. Zamawiający wymaga dostarczenie odpowiednich subskrypcji, gwarancji i licencji dla w/w rozwiązania na okres nie mniej niż czas trwania gwarancji.
 23. Potwierdzeniem odbioru zadania będzie „Protokół odbioru dostawy urządzeń zapory brzegowej” podpisany z wynikiem pozytywnym.

B. Instalacja i wdrożenie urządzeń zapory brzegowej (HA)

1. Dostarczony system służący do zabezpieczenia dostępu do sieci komputerowej i serwerowej powinien realizować wszystkie obecne funkcje sieciowe i bezpieczeństwa Zamawiającego wraz z subskrypcją zabezpieczeń.
2. Realizowane prace nie mogą w żaden sposób zakłócić lub uniemożliwić prawidłowego funkcjonowania systemów informatycznych Zamawiającego. Prace „wrażliwe” - wymagające okna serwisowego muszą być wykonywane w obustronnie ustalonym terminie uzgodnionym pomiędzy Wykonawcą i Zamawiającym.
3. Wykonawca zamontuje we wskazanej przez Zamawiającego lokalizacji dostarczone urządzenia w szafach rack 19 cali.
4. Wykonawca wykona połączenie dostarczonych urządzeń z siecią energetyczną Zamawiającego o parametrach 230V \pm 10%, 50Hz. W szafach rack są dostępne listwy zasilające z gniazdami C13.
5. Wykonawca wykona połączenie dostarczonych urządzeń z siecią logiczną Zamawiającego.
6. Wykonawca zobowiązany jest do przeniesienia istniejących polityk (ok. 1000 polityk), reguł dostępu VPN (IPSec VPN, SSLVPN) i całej konfiguracji sieciowej z obecnego Firewalla Zamawiającego do nowego systemu.
7. Wykonawca zintegruje dostarczone produkty zarówno pomiędzy sobą, jak i z elementami systemu teleinformatycznego Zamawiającego:
 - a) system autoryzacji oparty o serwer Radius,
 - b) Active Directory (synchronizacja użytkowników i grup użytkowników),
 - c) Zabbix (snmpv3, snmp trap),
 - d) SIEM (syslog, definicja wszystkich pól),
 - e) TruView (netflow, tap),w sposób wynikający z uzgodnień z Zamawiającym (określonych w Projekcie Technicznym) oraz przewidzianych przez dokumentację dla produktów, zgodnie z najlepszymi praktykami i doświadczeniem Wykonawcy.
8. Po wykonaniu prac związanych z instalacją sprzętu, Wykonawca będzie zobowiązany do pozostawienia miejsc, w których prowadzone były prace w siedzibie Zamawiającego, w stanie nie gorszym od zastanego przed przystąpieniem do prac.
9. Wykonawca jest zobowiązany do posprzątania i wywiezienia we własnym zakresie wszelkich opakowań, palet, folii itp. materiałów pozostałych po dostarczonych elementach infrastruktury i oprogramowania.
10. Wykonawca przeprowadzi testy akceptacyjne potwierdzające zgodność instalacji z wymaganiami opisanymi w Projekcie Technicznym – Plan Testów.
11. Potwierdzeniem odbioru zadania będzie „Protokół odbioru Instalacja i wdrożenie urządzeń zapory brzegowej” podpisany z wynikiem pozytywnym.

Zadanie 3.

Wykonanie Dokumentacji powykonawczej

1. Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji przedmiotu zamówienia charakteryzowały się takimi elementami jak:
 - a) struktura dokumentu, rozumiana jako podział danego dokumentu na rozdziały, podrozdziały i sekcje, w czytelny i zrozumiały sposób,

- b) zachowaniem standardów, rozumianych jako zachowaniem spójnej struktury, formy i sposobu pisanie dla poszczególnych dokumentów oraz fragmentów tego samego dokumentu,
 - c) kompletnością dokumentu, rozumiana jako pełne przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia.
2. Zamawiający wymaga, aby cała dokumentacja, o której mowa poniżej podlegała jego akceptacji, a także, aby została dostarczona w języku polskim, w wersji elektronicznej w niezabezpieczonym/edytowalnym formacie Word i PDF (na zewnętrznym nośniku danych USB) i drukowanej w 2 egzemplarzach.
 3. Wytworzona dokumentacja nie będzie opatrzona logo Wykonawcy.
 4. Dokumentacja powykonawcza będzie stanowiła zaktualizowany projekt techniczny rozszerzony o schematy połączeń, konfigurację urządzeń, specyfikację i opis zastosowanych interfejsów, sposób konfiguracji sprzętu i oprogramowania, a także będzie zawierała procedury:
 - a) administracji i eksploatacji systemu,
 - b) testowe,
 - c) konserwacji systemu,
 - d) awaryjne,
 - e) zabezpieczeń konfiguracji (backup),
 - f) identyfikacji nieprawidłowości w działaniu systemu i kwalifikacji awarii,
 - g) zgłoszeń serwisowych.
 5. Dokumentacja powykonawcza podlegała będzie procedurze odbioru, na następujących warunkach:
 - a) Wykonawca przekaże Zamawiającemu drogą elektroniczną do akceptacji dokumentację powykonawczą nie później niż w ciągu 7 dni kalendarzowych od daty odbioru wdrożenia.
 - b) Zamawiający w terminie nie dłuższym niż 2 dni kalendarzowe od dnia dostarczenia przez Wykonawcę dokumentacji powykonawczej, poinformuje Wykonawcę o jej akceptacji lub konieczności wprowadzenia zmian;
 - c) Wszystkie uwagi do dokumentacji powykonawczej zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 2 dni kalendarzowe od dnia ich otrzymania;
 - d) Zamawiający w terminie 2 dni kalendarzowych od dnia powtórnego dostarczenia przez Wykonawcę poprawionej dokumentacji powykonawczej, poinformuje Wykonawcę o jej akceptacji lub konieczności wprowadzenia zmian;
 - e) Zamawiający zastrzega sobie prawo do dwukrotnego zgłoszenia zmian w dokumentacji powykonawczej;
 6. W przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo wskazania ostatecznego terminu dostarczenia dokumentacji nie dłużej niż 5 dni kalendarzowych.
 7. Komunikacja pomiędzy Zamawiającym a Wykonawcą w zakresie akceptacji dokumentacji powykonawczej, następować będzie drogą mailową na adresy Wykonawcy i Zamawiającego wskazane w umowie.
 8. Zatwierdzona dokumentacja powykonawcza zostanie przekazana Zamawiającemu najpóźniej w dniu podpisania protokołu odbioru Dokumentacji powykonawczej.

9. Potwierdzeniem odbioru zaakceptowanej przez Zamawiającego Dokumentacji powykonawczej będzie Protokół odbioru Dokumentacji powykonawczej podpisany z wynikiem pozytywnym.

Zadanie 4.

Przeprowadzenie warsztatów szkoleniowych dla administratorów.

Wykonawca przeprowadzi szkolenie z zakresu obsługi, konfiguracji i oprogramowania dostarczonych urządzeń. Szkolenie powinno trwać od 3 do 5 dni i być zrealizowane w formie warsztatów.

1. Program warsztatów powinien zawierać informacje dotyczące tematyki prowadzonych warsztatów z podziałem na zajęcia teoretyczne i praktyczne. Program powinien zawierać również informacje dotyczące wiedzy i umiejętności jakie zdobędą uczestnicy po zakończeniu warsztatów. Zamawiający zastrzega sobie prawo do korekty programu warsztatów w zakresie nieograniczonym regulacjami prawnymi.
2. Wykonawca, w uzgodnieniu z Zamawiającym, przygotuje szczegółowe harmonogramy – z rozpisaniem na dni i godziny - oraz programy warsztatów i dostarczy je do 7 dni roboczych przed realizacją zamówienia do akceptacji przez Zamawiającego. Zamawiający zastrzega sobie możliwość korekty przedstawionych dokumentów.
3. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu. Harmonogram powinien zostać wydrukowany i rozdany uczestnikom szkolenia na pierwszym spotkaniu.
4. Wykonawca, zgodnie z planem szkoleń i w terminach przewidzianych w zatwierdzonym harmonogramie przeprowadzi szkolenia w ośrodku szkoleniowym na terenie Warszawy dla 6 osób, w dwóch nie nakładających się turach - w każdej turze zostanie przeszkolonych 3 pracowników Zamawiającego.
5. W przypadku szkoleń przeprowadzanych poza terenem Warszawy, Wykonawca poniesie całkowite koszty zakwaterowania i wyżywienia uczestników szkolenia.
6. Wykonawca musi dysponować lub zapewnić na cele realizacji przedmiotu zamówienia odpowiednio wykwalifikowaną kadrę, której powierzy realizację przedmiotu zamówienia w zakresie szkoleń. Wymagane jest, aby kadra trenerska posiadała udokumentowane co najmniej 2 letnie doświadczenie w przedmiocie szkolenia.
7. Wykonawca powinien dysponować lub zapewnić na cele realizacji przedmiotu zamówienia bazę szkoleniową z odpowiednimi pomieszczeniami wraz z zapleczem do przeprowadzenia szkolenia 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.
8. W pobliżu sali wykładowej (w tym samym budynku) powinna znajdować się toaleta z węzłem sanitarnym.
9. Zajęcia powinny odbywać się w dni powszednie od poniedziałku do piątku, w godzinach od 8:00 do 17.00, nie więcej niż 8 godzin dziennie.
10. Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika do danego rodzaju szkolenia, pozwalające na samodzielną edukację z zakresu tematyki szkoleń (opracowania, wydruki materiałów szkoleniowych).
11. Komplet materiałów szkoleniowych dla każdego uczestnika szkolenia obejmuje:

- a) papierową wersję materiałów szkoleniowych. Zamawiający dopuszcza dostarczenie materiałów w formie elektronicznej, np. dokumenty w standardzie PDF, w miejsce materiałów papierowych;
 - b) materiały papiernicze (notatnik, długopis) i inne środki dydaktyczne niezbędne do realizacji szkolenia.
12. Komplet materiałów powinien zostać rozdany uczestnikom szkolenia w pierwszym dniu zajęć. Koszty opracowania, transportu i powielenia materiałów ponosi Wykonawca.
 13. Wykonawca zapewni na potrzeby wyżywienia uczestników szkoleń odpowiednie pomieszczenie oraz niezbędną liczbę stołów i krzeseł. Zamawiający nie dopuszcza serwowania posiłków w tej samej sali, w której odbywają się szkolenia.
 14. Miejsce posiłku nie powinno być oddalone dalej niż 10 minut drogi pieszo od miejsca szkolenia.
 15. Wykonawca zapewni min. 2 przerwy kawowe podczas jednego dnia szkoleniowego
 16. Czas na przerwy kawowe i obiadowe należy doliczyć do założonej liczby godzin szkolenia.
 17. Koszty posiłków, dowozu, sprzętu i obsługi ponosi Wykonawca.
 18. Szkolenia muszą być prowadzone w języku polskim.
 19. Każdy uczestnik szkolenia otrzyma certyfikat/imienne zaświadczenia jego ukończenia potwierdzające, że nabyli wiedzę zgodną z celem szkolenia.
 20. Potwierdzeniem prawidłowej realizacji warsztatów będzie podpisany bez zastrzeżeń przez Zamawiającego „**Protokół odbioru warsztatów szkoleniowych**” wraz z dołączonymi załącznikami:
 - a) oryginalną listą obecności,
 - b) harmonogramem i programem warsztatu (nazwę, tematykę i czas trwania warsztatów, datą i miejscem warsztatów oraz imię i nazwisko oraz specjalizację osób prowadzących warsztaty),
 - c) ankiety oceny warsztatu przeprowadzonej wśród uczestników warsztatu.
 21. W przypadku negatywnej oceny warsztatu (średnia z oceny trenera / trenerów poniżej 3), Wykonawca przeprowadzi dodatkowe warsztat na koszt własny, dochowując terminu realizacji zadania. Organizacja dodatkowego warsztatu będzie wymagała uzgodnienia z Zamawiającym terminu oraz osoby prowadzącej zajęcia. Ponowne przeprowadzenie warsztatu musi się odbyć nie później niż 5 dni roboczych przed terminem zakończenia Zadania. Koszt ponownego zorganizowania i przeprowadzenia warsztatu ponosi Wykonawca.

Wykaz warsztatów szkoleniowych

A. Warsztaty z podstawowych funkcjonalności zapory brzegowej (firewall)

1. Podczas warsztatów uczestnik powinien nauczyć się korzystania z podstawowych funkcjonalności systemu służącego do zabezpieczenia sieci komputerowej i serwerowej, w tym np. profili bezpieczeństwa.
2. W trakcie zajęć praktycznych tzw. laboratoriów uczestnik zapozna się z zasadami tworzenia polityk zapory sieciowej, uwierzytelnianiem użytkowników, SSL VPN, dial-up IPsec VPN oraz nauczy się jak chronić swoją sieć LAN za pomocą profili bezpieczeństwa, takich jak IPS, antywirus, filtrowanie ruchu www, kontrola aplikacji i wielu innych.
3. Istotne elementy, które powinno zawierać szkolenie:
 - a) polityki zapory sieciowej,
 - b) translacja adresów sieciowych (NAT),

- c) uwierzytelnianie użytkowników,
 - d) logowanie i monitoring,
 - e) filtr stron www,
 - f) kontrola aplikacji,
 - g) antywirus, SSL VPN.
4. Po ukończeniu warsztatów Uczestnik powinien posiadać niezbędną wiedzę i umiejętności pozwalające na samodzielną konfigurację na poziomie podstawowym szeregu elementów kompletnego systemu bezpieczeństwa sieci w tym min.:
- a) wybrać odpowiedni tryb pracy urządzenia dla swojej sieci,
 - b) używać GUI jak i CLI do zadań administracyjnych,
 - c) zidentyfikować charakterystyczne cechy systemu bezpieczeństwa,
 - d) kontrolować dostęp sieciowy do zabezpieczanych sieci za pomocą reguł zapory sieciowej,
 - e) stosować funkcję przekierowywania portów, source NAT i destination NAT,
 - f) uwierzytelniać użytkowników za pomocą reguł zapory sieciowej,
 - g) potrafić identyfikować ruch zabezpieczony protokołem SSL/TLS, i przeciwdziałać ewentualnemu omijaniu reguł bezpieczeństwa poprzez szyfrowanie komunikacji,
 - h) konfigurować profile bezpieczeństwa, aplikacje do monitorowania i kontrolowania komunikacji sieciowej aplikacji, które mogą wykorzystywać standardowe lub niestandardowe protokoły i porty,
 - i) skutecznie wdrożyć SSL VPN jako bezpieczną metodę dostępu do zasobów znajdujących się w chronionych sieciach, zbierać i prawidłowo interpretować logi na urządzeniach.

B. Warsztaty w zakresie kompleksowej ochrony sieci

1. Warsztaty powinny być rozwinięciem zagadnień z warsztatów z podstawowych funkcjonalności urządzeń zapory brzegowej.
2. W ramach warsztatów zostaną przeprowadzone zajęcia praktyczne tzw. laboratoria, które obejmą swoim zakresem:
 - a) routing i load balancing – omówienie metod rozkładania ruchu, potencjalne problemy z NAT,
 - b) inspekcję ruchu SSL – zarządzanie certyfikatami, praktyczna analiza ruchu zabezpieczonego protokołem SSL, wpływ SSL na pracę modułów bezpieczeństwa, potencjalne problemy,
 - c) High Availability – zasada działania HA, konfiguracja tryby Active-Passive vs Active-Active,
 - d) IPSec VPN – konfiguracja topologii, rozwiązanie problemu identycznej adresacji sieci lokalnych.

C. Warsztaty wprowadzające do zagadnień związanych z systemem centralnego zarządzania, logowania i analizy systemu zapory brzegowej

1. Warsztaty powinny dostarczyć uczestnikom wiedzę i praktyczne umiejętności potrzebne do administracji systemem zabezpieczeń oraz do administracji urządzeniem centralnego logowania i analizy.
2. Tematyka warsztatów powinna koncentrować się na omówieniu i zapoznaniu się z:

- a) zaawansowanymi funkcjonalnościami systemu związanymi z konfiguracją, zarządzaniem i monitoringiem wielu urządzeń,
 - b) zaawansowanymi możliwościami i konfiguracją oraz sposobami diagnozowanie pracy urządzenia oraz generowanie raportów,
3. Istotne elementy, które powinno zawierać warsztatów:
- a) podstawowa konfiguracja – ustawienia systemowe, zapisywanie i odtwarzanie konfiguracji, zabezpieczanie konfiguracji, równoczesna praca kilku administratorów,
 - b) centralne zarządzanie urządzeniami – dodawanie urządzeń, zarządzanie wieloma urządzeniami, skrypty,
 - c) polityki i obiekty – tworzenie i instalacja polityk, konfiguracja dynamicznych obiektów, konfiguracja dostępu VPN,
 - d) dodatkowe ustawienia – diagnostyka komunikacji z zarządzanymi urządzeniami, tryb wysokiej dostępności (HA),
 - e) podstawowa konfiguracja i zarządzanie logami – ustawienia systemowe, zapisywanie, odtwarzanie i zabezpieczanie konfiguracji, domeny administracyjne,
 - f) rejestracja urządzeń – lista urządzeń, dodawanie nowych urządzeń, blokowanie urządzeń, dodawanie innych urządzeń wspierających protokół syslog, zabezpieczanie komunikacji,
 - g) logi i archiwa – przetwarzanie i przeglądanie logów, przeszukiwanie logów, agregacja logów, przekazywanie logów, przywracanie logów, archiwizacja logów, alerty, archiwizacja,
 - h) raporty – tworzenie i generowanie raportów, wykresy, przeglądanie raportów.

VI. Wzory protokołów

Protokół odbioru usługi gwarancyjnej/asysty technicznej

w ramach umowy nr

za okres

1. Formularz podsumowujący wykonanie prac w ramach realizacji usług opieki gwarancyjnej/asysty technicznej

Nr Zgłoszenia/ Data i godzina	Czas realizacji wniosku <i>[godziny]</i>	Uwagi Zrealizowany zgodnie*/niezgodnie z Umową

2. Uwagi Zamawiającego:

.....

3. Wynik odbioru:

- a) Pozytywny*) – Zamawiający dokonuje odbioru przekazanego Protokołu bez zastrzeżeń i stwierdza, że usługa gwarancyjna/asysty techniczna w nim przedstawione zostały wykonane zgodnie z wymogami określonymi w Umowie. Opóźnienia wskazane zostały w pkt 2.
- b) Negatywny*) – Zamawiający odmawia odbioru przekazanego Protokołu w związku z rozbieżnościami:

.....

.....

.....

.....

*) – niepotrzebne skreślić,

**) – jeżeli dotyczy.

WYKONAWCA

ZAMAWIAJĄCY

Imię i nazwisko

Imię i nazwisko

/pieczętka firmowa, data podpis/

/pieczętka firmowa, data podpis)

.....
(pieczęć firmowa Zamawiającego)

Warszawa, dnia

.....
Nazwa Wykonawcy

Zgłoszenie o świadczenie usługi gwarancyjnej /asysty technicznej

nr z dnia

do umowy nr

Zakres usług w ramach usługi gwarancyjnej/ asysty technicznej:

.....
.....
.....

Uwagi:

.....
.....

.....
Imię i nazwisko pracownika Zamawiającego

Spis treści

Rozdział I: Definicje	1
Rozdział II: Opis infrastruktury Zamawiającego²	3
Rozdział III: Wymagania ogólne.....	3
Rozdział IV: Gwarancja – poziom usług serwisowych.....	5
Rozdział VI: Realizacja przedmiotu umowy	8
Zadanie 1.....	8
Zadanie 2.....	10
1. Zakup i dostawa urządzeń zapory brzegowej (HA) w konfiguracji minimum.	10
1. Instalacja i wdrożenie urządzeń zapory brzegowej (HA)	16
Zadanie 3.....	16
Zadanie 4.....	18
Rozdział VI: Wzory protokołów	22