Załącznik nr 5A do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

„Zakup i dostarczenie infrastruktury IT na potrzeby realizacji projektów.
Pakiet A – Zakup, dostarczenie i przekazanie do użytkowania licencji, zapór sieciowych typu UTM.”

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

Spis treści

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

1 Definicje i skróty:

Użyte w niniejszym OPZ i załącznikach wszelkie nazwy własne, normy, aprobaty, specyfikacje techniczne, systemy referencji technicznych, procesy charakteryzujące produkt lub usługę, należy rozumieć każdorazowo, jak opatrzone dopiskiem „lub równoważne".

Definicja/skrót	Opis
Administrator	Osoba, zespół osób lub jednostka zajmująca się zarządzaniem systemem i odpowiadająca za jego sprawne działanie posiadająca uprawnienia do części administracyjnych systemu.
RPO WK-P	Regionalny Program Operacyjny Województwa Kujawsko-Pomorskiego.
UTM	(Unified Threat Management) Zapora sieciowa.
VM	Maszyna wirtualna.
VPN	(Virtual Point Network) Określenie na bezpieczne, szyfrowane połączenie pomiędzy dwoma sieciami lub między użytkownikiem a siecią.
TRADEUP	Odświeżenie, uaktualnienie urządzenia do jego najnowszej wersji.
Zamawiający	Urząd Marszałkowski Województwa Kujawsko-Pomorskiego w Toruniu (Lider Projektów) działający na rzecz Partnerów Projektów „Infostrada Kujaw i Pomorza - Usługi w Zakresie E-Administracji i Informacji Przestrzennej", „Infostrada Kujaw i Pomorza 2.0" oraz „Budowa Kujawsko-Pomorskiego systemu udostępniania elektronicznej dokumentacji medycznej – Etap I" wymienionych w Załączniku nr 2 do OPZ – Wykaz Partnerów Projektów i Sprzętu.

2 Obowiązujące przepisy prawne:

1) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. z 4.04.2019 r. Dz. U. z 2019 poz. 700).
2) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z dnia 27.04.2016 r. (Dz. Urz. UE. L Nr 119) RODO. Ustawa z dnia 10.05.2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).
3) Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tj. z 13.12.2018 r. Dz. U. z 2019 r. poz. 123).

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

4) Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (tj. z 7.12.2018 r. Dz. U. z 2019 r. poz. 162).
5) Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (tj. z 3.10.2018 r. Dz. U. z 2018 r. poz. 2096).
6) Ustawa z dnia 29 września 1994 r. o rachunkowości (tj. z 17.01.2019 r. Dz. U. z 2019 r. poz. 351).
7) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz. U. Nr. 206 poz. 1518).
8) Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. Nr. 14, poz. 67).
9) Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr. 159, poz. 948).
10) Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. Nr. 128, poz. 1402, z późn. zm.).
11) Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (tj. z 29.06.2018 r. Dz. U. z 2018 r. poz. 1330).
12) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz. U. 2006 Nr. 206 poz. 1518).
13) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L Nr.119).

3 Informacja o projektach:

1) Projekt „Infostrada Kujaw i Pomorza - Usługi w Zakresie E-Administracji i Informacji Przestrzennej" współfinansowany w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2007 – 2013, „Infostrada Kujaw i Pomorza 2.0" oraz „Budowa Kujawsko-Pomorskiego systemu udostępniania elektronicznej dokumentacji medycznej – Etap I" współfinansowane są ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego (RPO WK-P) na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektu.
2) Celem głównym projektów jest wdrażanie działań związanych z cyfryzacją Województwa Kujawsko-Pomorskiego.
3) Realizacja celów projektów zapewni wsparcie gospodarcze i społeczne rozwoju Województwa Kujawsko-Pomorskiego poprzez podniesienie poziomu bezpieczeństwa przetwarzania i gromadzenia danych cyfrowych, w tym danych osobowych.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

4 Przedmiot zamówienia:

1) Modernizacja istniejących systemów zabezpieczeń sieciowych Zamawiającego poprzez dostarczenie nowych zestawów urządzeń ochrony sieci typu UTM oraz modernizację istniejących urządzeń ochrony sieci typu UTM poprzez:
    a) przedłużenie licencji na użytkowanie oraz odświeżenie zapór sieciowych typu UTM będących w posiadaniu Zamawiającego (stosowanym rozwiązaniem są Fortigate'y 60D) nabytych w ramach projektu „Infostrada Kujaw i Pomorza – Usługi w Zakresie E-Administracji i Informacji Przestrzennej", używanych przez Zamawiającego oraz udzielenie nieodpłatnej gwarancji na dostarczony sprzęt dla Partnerów Projektu,
    b) dostarczenie nowych licencji na użytkowanie wraz z zaporami sieciowymi typu UTM w ramach projektu „Infostrada Kujaw i Pomorza 2.0" oraz udzielenie nieodpłatnej gwarancji na dostarczony sprzęt dla Partnerów Projektu,
    c) dostarczenie nowych licencji na użytkowanie wraz z zaporami sieciowymi typu UTM w ramach projektu „Budowa Kujawsko-Pomorskiego systemu udostępniania elektronicznej dokumentacji medycznej – Etap I" oraz udzielenie nieodpłatnej gwarancji na dostarczony sprzęt dla Partnerów Projektu.
2) Wykonawca w szczególności zobowiązany jest do:
    a) kompleksowej realizacji przedmiotu zamówienia co obejmuje niezbędne oprogramowanie, licencje i inne niezbędne elementy składające się na ich prawidłowe funkcjonowanie wraz z pełną obsługą i wsparciem technicznym w ramach okresu gwarancyjnego,
    b) dostarczenia do lokalizacji wskazanych przez Partnerów Projektów „Infostrada Kujaw i Pomorza - Usługi w Zakresie E-Administracji i Informacji Przestrzennej", „Infostrada Kujaw i Pomorza 2.0" oraz „Budowa Kujawsko-Pomorskiego systemu udostępniania elektronicznej dokumentacji medycznej – Etap I" zestawów zapór sieciowych typu UTM.

5 Zakres prac:

5.1 Dostarczenie licencji w opcji Trade Up

Zgodnie z Załącznikiem nr 1 „Specyfikacja Techniczna", punkt 1 oraz z Załącznikiem nr 2A do OPZ - Wykaz Partnerów Projektów i Sprzętu, Wykonawca zapewni niezbędne licencje i oprogramowanie związane z realizacją zamówienia, a także przeprowadzi odnowienie licencji FORTINET oraz TRADEUP dotychczas stosowanego rozwiązania Fortigate'y 60D do najnowszej wersji. Liczba i rodzaj licencji do dostarczenia określone zostały w Załączniku nr 2A do OPZ - Wykaz Partnerów Projektów i Sprzętu w części dotyczącej Projektu „Infostrada Kujaw i Pomorza - Usługi w Zakresie E-Administracji i Informacji Przestrzennej".

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

5.2 Dostarczenie licencji i urządzeń:

Zgodnie z Załącznikiem nr 1 „Specyfikacja Techniczna", punkty 2-4 oraz z Załącznikiem nr 2A do OPZ - Wykaz Partnerów Projektów i Sprzętu, Wykonawca dostarczy fizyczne elementy infrastrukturalne, zapory sieciowe typu UTM do wskazanych jednostek. Poprzez wdrożenie rozumiane jest wprowadzenie konfiguracji, przeniesienia konfiguracji zgodnie z potrzebami Partnerów Projektów oraz utworzenie połączeń VPN z infrastrukturą Lidera Projektów. Wszystkie dostarczone urządzenia muszą być nowe, pochodzić z oficjalnego kanału dystrybucji dla Polski oraz posiadać wsparcie i gwarancję producenta według wymogów opisanych w OPZ. Dostarczenie musi odbyć się w uzgodnieniu z administratorami Partnerów po uprzednim uzgodnieniu terminu i miejsca dostaw. Liczba i rodzaj urządzeń do dostarczenia określone zostały w Załączniku nr 2 do OPZ - Wykaz Partnerów Projektów i Sprzętu w części dotyczącej projektów „Infostrada Kujaw i Pomorza 2.0" oraz „Budowa Kujawsko-Pomorskiego systemu udostępniania elektronicznej dokumentacji medycznej – Etap I".

6 Wymogi w zakresie nieodpłatnej gwarancji i licencji:

6.1 Wymogi w zakresie świadczenia nieodpłatnej gwarancji:

1) Urządzenia muszą zostać objęte wsparciem gwarancyjnym i wsparciem producenta polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie 24x7. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne.
2) Przyjmowanie zgłoszeń serwisowych musi być realizowane całodobowo w systemie online Wykonawcy, który umożliwia podgląd wszystkich dokonanych zgłoszeń, czas ich realizacji oraz bieżący ich status.
3) Czas realizacji zgłoszenia musi wynosić do 12 godzin od przyjęcia zgłoszenia.
4) Czas usunięcia błędu nie może być dłuższy niż 24 godziny.
5) Wymiana uszkodzonego sprzętu musi zostać dokonana w czasie nie dłuższym niż 48 godzin.
6) Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia serwisu.
7) Oferent winien przedłożyć do oferty :
    a) oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego usługi serwisowe o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej),
    b) certyfikat ISO 9001 podmiotu serwisującego.
8) Okres objęcia oferowanych rozwiązań w zakresie nieodpłatnej gwarancji oraz wsparcia producenta w okresie nie krótszym niż 24 miesiące.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

9) Świadczenie bezpośredniego wsparcia technicznego w ramach okresu gwarancyjnego obejmować ma wszystkich Partnerów Projektów biorących udział w postępowaniu, którzy otrzymają licencje i zapory sieciowe typu UTM.
10) Wykonawca zobowiązany jest do świadczenia wsparcia technicznego w ramach okresu gwarancyjnego dla wszystkich dostarczonych elementów w ramach zamówienia.
11) Przez wsparcie techniczne w ramach okresu gwarancyjnego Zamawiający rozumie wszelkie prace, opłaty, koszty, operacje niezbędne do utrzymania w pełni funkcjonującego przedmiotu zamówienia.
12) Do zadań realizowanych przez Wykonawcę w ramach świadczenia wsparcia technicznego należy:
    a) integracja UTM'ów z systemami Partnerów Projektów,
    b) kreowanie, przenoszenie, zabezpieczanie, testowanie, przywracanie, aktualizacja, bieżące utrzymanie urządzeń w środowisku infrastrukturalnym,
    c) wsparcie systemów funkcjonujących w środowisku infrastrukturalnym oraz w innych obszarach funkcjonowania zapór sieciowych typu UTM,
    d) zdalne sprawdzanie systemu, wprowadzenie aktualizacji,
    e) aktualizacja oprogramowania ze względu na błędy bezpieczeństwa,
    f) realizacja bieżących czynności administracyjnych,
    g) analiza incydentów oraz problemów wraz z pełnym przywracaniem funkcjonalności,
    h) inne niezbędne działania związane z utrzymaniem systemów bezpieczeństwa sieci, związane z przedmiotem zamówienia.
13) W przypadku zmian prawnych w okresie utrzymania systemu Wykonawca zobowiązany jest do wprowadzenia wszelkich zmian, poprawek, zabezpieczeń, wynikających ze zmienionych przepisów prawnych.
14) Do dyspozycji w ramach nieodpłatnej gwarancji Wykonawca przeznaczy w ramach wsparcia technicznego 400 roboczogodzin na prace określone w punkcie 6 zlecone przez Zamawiającego przez cały czas trwania gwarancji wynikający z przedmiotowego Zamówienia.
15) Zgłoszenia w ramach wsparcia technicznego będą przyjmowane w języku polskim, w trybie 8x5, przez dedykowany moduł internetowy oraz infolinię Wykonawcy, który umożliwia podgląd wszystkich dokonanych zgłoszeń, czas ich realizacji oraz bieżący ich status.
16) Wsparcie techniczne w ramach okresu gwarancji świadczone będzie od dnia podpisania bez uwag protokołu odbioru końcowego przedmiotu zamówienia przez cały okres gwarancji.

6.2 Wymogi w zakresie licencji:

1) W przypadku trade up'u urządzeń dostarczonych Partnerom Projektu „Infostrada Kujaw i Pomorza - Usługi w Zakresie E-Administracji i Informacji Przestrzennej" okres objęcia oferowanych rozwiązań w zakresie licencji w okresie nie krótszym niż 12 miesięcy.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

2) W przypadku zakupu nowych licencji i urządzeń dostarczonych Partnerom Projektów „Infostrada Kujaw i Pomorza 2.0" oraz „Budowa Kujawsko-Pomorskiego systemu udostępniania elektronicznej dokumentacji medycznej – Etap I" okres objęcia oferowanych rozwiązań w zakresie licencji w okresie nie krótszym niż 24 miesiące.
3) W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: kontrolę aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), analizę typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

7 Wdrożenie i odbiór:

7.1 Harmonogram realizacji wdrożenia:

1) Rozpoczęcie prac nastąpi z chwilą podpisania Umowy.
2) Realizacja przedmiotu zamówienia powinna nastąpić nie później niż w terminie zaoferowanym przez Wykonawcę – w ciągu 30 dni, 45 dni lub 60 dni kalendarzowych od daty zawarcia Umowy.
3) Realizacja i odbiór przedmiotu zamówienia będzie obejmowała:
    a) dostarczenie zestawów infrastruktury IT do odpowiednich lokalizacji,
    b) przeprowadzenie wdrożenia zgodnie ze specyfikacją do każdego rodzaju systemu ochrony sieci,
    c) zgłoszenie gotowości do odbioru przedmiotu zamówienia przez Wykonawcę,
    d) odbiór przedmiotu zamówienia przez Zamawiającego,
    e) rozpoczęcie okresu nieodpłatnej gwarancji.
4) Wykonawca zgłasza gotowość do odbioru przedmiotu zamówienia najpóźniej na 5 dni kalendarzowych przed terminem, o którym mowa w pkt. 7.1.2
5) Wykonawca musi dostarczyć protokoły częściowe podpisane w sposób czytelny przez osoby upoważnione do składania oświadczeń woli w imieniu jednostki z imienną pieczątką, w przypadku jej braku pieczątką jednostki, przez Partnerów Projektów „Infostrada Kujaw i Pomorza - Usługi w Zakresie E-Administracji i Informacji Przestrzennej", „Infostrada Kujaw i Pomorza 2.0" oraz „Budowa Kujawsko-Pomorskiego systemu udostępniania elektronicznej dokumentacji medycznej – Etap I". Odbiór lub zgłoszenie uwag przez Partnerów nastąpi w ciągu 7 dni kalendarzowych.
6) Potwierdzeniem realizacji umowy jest protokół odbioru końcowy podpisany przez Lidera Projektów „Infostrada Kujaw i Pomorza - Usługi w Zakresie E-Administracji i Informacji Przestrzennej", „Infostrada Kujaw i Pomorza 2.0" oraz „Budowa Kujawsko-Pomorskiego systemu udostępniania elektronicznej dokumentacji medycznej – Etap I" na podstawie dostarczonych przez Wykonawcę Umowy wszystkich podpisanych przez Partnerów Projektów, bez uwag, protokołów częściowych. Odbiór lub zgłoszenie uwag przez Lidera nastąpi w ciągu 7 dni kalendarzowych od dostarczenia ostatniego protokołu częściowego.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

7) W ramach Projektu "Infostrada Kujaw i Pomorza - Usługi w Zakresie E-Administracji i Informacji Przestrzennej" faktury należy wystawić oddzielnie i wyodrębnić je z pozostałych zakupów. Wynika to z faktu, że sprzęt rozliczany w ramach tego zadania jest finansowany w całości ze środków Jednostek Samorządu Terytorialnego i nie jest dotowany.
8) Podstawą do wystawienia faktury za zrealizowanie przedmiotu zamówienia będzie protokół częściowy sporządzony przez Zamawiającego.

7.2 Zobowiązania Wykonawcy:

1) Wykonawca udzieli Zamawiającemu pełnej informacji na temat stanu realizacji przedmiotu zamówienia, na każde wezwanie Zamawiającego.
2) Zapewnienie, że dostarczone przez Wykonawcę informacje będą prawdziwe i kompletne.
3) Wykonawca zobowiązany będzie współdziałać z osobami wskazanymi przez Zamawiającego.

7.3 Zobowiązania Zamawiającego:

1) Udostępnienie dokumentów, materiałów, danych, dokumentacji i informacji będących w posiadaniu Zamawiającego, niezbędnych do realizacji przedmiotu zamówienia.
2) Udzielanie Wykonawcy na bieżąco niezbędnych do realizacji przedmiotu zamówienia wyjaśnień oraz przekazywania niezbędnych informacji.
3) Zapewnienie, że dostarczone przez Zamawiającego informacje będą prawdziwe i kompletne.
4) Informowanie Wykonawcy o wszelkich czynnościach podejmowanych w związku z realizacją projektu, jeśli będą one miały związek z realizacją przedmiotu zamówienia przez Wykonawcę.
5) Konsultowanie i uzgadnianie wdrażanego systemu zgodnie z wymaganiami OPZ.

Załączniki:

1. Załącznik nr 1 – Specyfikacja Techniczna,
2. Załącznik nr 2A – Wykaz Partnerów Projektu i sprzętu.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

Załącznik nr 1
Specyfikacja Techniczna

1 System ochrony sieci typ I Trade Up dla Partnerów projektu pn. „Infostrada Kujaw i Pomorza - Usługi w Zakresie E-Administracji i Informacji Przestrzennej" – 76 szt.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Komponent	Minimalne wymagania
Ogólne	System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: 1. Firewall. 2. Ochrony w warstwie aplikacji. 3. Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall musi dysponować minimum: a) 10 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.
Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. Analiza ruchu szyfrowanego protokołem SSH.
Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: a) Translację jeden do jeden oraz jeden do wielu. b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: a) Wsparcie dla IKE v1 oraz v2. b) Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). c) Obsługa protokołu Diffie-Hellman grup 19 i 20. d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. h) Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. i) Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: a) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: a) Routingu statycznego. b) Policy Based Routingu. c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Kontrola Antywirusowa	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Zaproponowane rozwiązanie musi posiadać możliwość zarządzania poprzez posiadany przez Zamawiającego system centralnego zarządzania firmy Fortinet - FortiManager.
Logowanie	1. Zaproponowane rozwiązanie musi posiadać możliwość logowania zdarzeń i archiwizowania danych do posiadanego przez Zamawiającego systemu centralnego gromadzenia logów firmy Fortinet - FortiAnalyzer. 2. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	4. Musi istnieć możliwość logowania do serwera SYSLOG.
Zarządzanie urządzeniami AccessPoint	Powinna istnieć możliwość zarządzania posiadanymi przez Zamawiającego cienkimi punktami dostępowymi FortiAP, w celu zapewnienia spójności zarządzania i uzyskania wymaganego poziomu bezpieczeństwa. Kontroler sieci wireless ma być uruchomiony w obrębie urządzenia bezpieczeństwa gwarantującego ochronę dla obsługiwanych sieci wireless i przewodowych.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: a) ICSA lub EAL4 dla funkcji Firewall.
Serwis	Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię. Oferent winien przedłożyć dokumenty: a) Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). b) Certyfikat ISO 9001 podmiotu serwisującego.
Inne	1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2004, Nr 229, poz. 2315 z późn zm.) 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. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
Wdrożenie	1. Dostarczenie urządzenia do wskazanej lokalizacji. 2. Instalacja fizyczna urządzenia oraz aktualizacja do najnowszej dostępnej wersji oprogramowania układowego. 3. Połączenie z obecną infrastrukturą zamawiającego, pozwalającą na zdalny dostęp do dostarczonych urządzeń. 4. Podłączenie urządzeń w miejsce obecnie posiadanych przez Zamawiającego urządzeń. 5. Konfiguracja przełącznika sieciowego w zakresie konfiguracji portu. 6. Przeniesienie konfiguracji z obecnego urządzenia na nowe. 7. Analiza aktualnych polityk i konfiguracji zaimplementowanych na urządzeniu.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	8. Optymalizacja polityk i konfiguracji celem zwiększenia bezpieczeństwa stosowanych zabezpieczeń. 9. Analiza skonfigurowanych połączeń SSL VPN w zakresie wprowadzenia zmian w topologii istniejących połączeń, w szczególności przy uwzględnieniu połączeń typu ADVPN. Przedstawienie do akceptacji przez Zamawiającego projektu uruchomienia/zmiany ustawień. Wprowadzenie zmian po uzyskaniu akceptacji Zamawiającego. 10. Przegląd profili zabezpieczeń ujętych w sekcji „Security Profiles" w zakresie dostępnych funkcjonalności. Przedstawienie do akceptacji przez Zamawiającego projektu uruchomienia/zmiany ustawień. Zamawiający zastrzega możliwość zlecenia w ramach wdrożenia dokonania zmian konfiguracyjnych we wszystkich funkcjonalnościach dostępnych w sekcji „Security Profiles" w szczególności: Webfilter, Antivirus, Application Control, VoIP, Proxy Options, SSL/SSH Inspection. 11. Włączenie i skonfigurowanie w środowisku Zamawiającego SSL Deep Inspection. 12. Przygotowanie serwera Radius w oparciu o posiadane serwery i licencje Zamawiajacego (Windows Server 2012R2) 13. Konfiguracja dodatkowego połączenia WAN realizowanego przez zapasowe przyłącze do sieci Internet w zakresie obsługi ruchu HTTP, HTTPS oraz protokołów obsługi poczty elektronicznej (awaryjne przełączenie w przypadku utraty dostępu do sieci świadczonej przez głównego operatora). 14. Włączenie Fortifabric i ujęcie wszystkich urządzeń dostarczanych w ramach umowy oraz obecnie posiadanych rozwiązań przez Zamawiającego (4 sztuki Fortigate seria E, Fortimail). 15. Aktualizacja klienta FSSO na kontrolerze domeny. 16. Wykonanie dokumentacji powdrożeniowej w szczególności obejmującej procedurę zgłaszania awarii.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

2 System ochrony sieci typ I dla Partnerów projektu pn. „Infostrada Kujaw i Pomorza 2.0" oraz „Budowa Kujawsko-Pomorskiego systemu udostępniania elektronicznej dokumentacji medycznej – Etap I" – 97 szt.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Komponent	Minimalne wymagania
Ogólne	System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: 1. Firewall. 2. Ochrony w warstwie aplikacji. 3. Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall musi dysponować minimum: a. 10 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.
Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. Analiza ruchu szyfrowanego protokołem SSH.
Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: a) Translację jeden do jeden oraz jeden do wielu. b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: a) Wsparcie dla IKE v1 oraz v2. b) Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	c) Obsługa protokołu Diffie-Hellman grup 19 i 20. d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. h) Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. i) Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: a) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: a) Routingu statycznego. b) Policy Based Routingu. c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Kontrola Antywirusowa	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Zaproponowane rozwiązanie musi posiadać możliwość zarządzania poprzez posiadany przez Zamawiającego system centralnego zarządzania firmy Fortinet - FortiManager.
Logowanie	1. Zaproponowane rozwiązanie musi posiadać możliwość logowania zdarzeń i archiwizowania danych do posiadanego przez Zamawiającego systemu centralnego gromadzenia logów firmy Fortinet - FortiAnalyzer. 2. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
Zarządzanie urządzeniami AccessPoint	Powinna istnieć możliwość zarządzania posiadanymi przez Zamawiającego cienkimi punktami dostępowymi FortiAP, w celu zapewnienia spójności zarządzania i uzyskania wymaganego poziomu bezpieczeństwa. Kontroler sieci wireless ma być uruchomiony w obrębie urządzenia bezpieczeństwa gwarantującego ochronę dla obsługiwanych sieci wireless i przewodowych.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	a) ICSA lub EAL4 dla funkcji Firewall.
Serwis	Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię. Oferent winien przedłożyć dokumenty: a) Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). b) Certyfikat ISO 9001 podmiotu serwisującego.
Inne	1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2004, Nr 229, poz. 2315 z późn zm.) 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. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
Wdrożenie	1. Dostarczenie urządzenia do wskazanej lokalizacji. 2. Instalacja fizyczna urządzenia oraz aktualizacja do najnowszej dostępnej wersji oprogramowania układowego. 3. Połączenie z obecną infrastrukturą zamawiającego, pozwalającą na zdalny dostęp do dostarczonych urządzeń. 4. Podłączenie urządzeń w miejsce obecnie posiadanych przez Zamawiającego urządzeń. 5. Konfiguracja przełącznika sieciowego w zakresie konfiguracji portu. 6. Przeniesienie konfiguracji z obecnego urządzenia na nowe. 7. Analiza aktualnych polityk i konfiguracji zaimplementowanych na urządzeniu. 8. Optymalizacja polityk i konfiguracji celem zwiększenia bezpieczeństwa stosowanych zabezpieczeń. 9. Analiza skonfigurowanych połączeń SSL VPN w zakresie wprowadzenia zmian w topologii istniejących połączeń, w szczególności przy uwzględnieniu połączeń typu ADVPN. Przedstawienie do akceptacji przez Zamawiającego projektu uruchomienia/zmiany ustawień. Wprowadzenie zmian po uzyskaniu akceptacji Zamawiającego.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	10. Przegląd profili zabezpieczeń ujętych w sekcji „Security Profiles" w zakresie dostępnych funkcjonalności. Przedstawienie do akceptacji przez Zamawiającego projektu uruchomienia/zmiany ustawień. Zamawiający zastrzega możliwość zlecenia w ramach wdrożenia dokonania zmian konfiguracyjnych we wszystkich funkcjonalnościach dostępnych w sekcji „Security Profiles" w szczególności: Webfilter, Antivirus, Application Control, VoIP, Proxy Options, SSL/SSH Inspection. 11. Włączenie i skonfigurowanie w środowisku Zamawiającego SSL Deep Inspection. 12. Przygotowanie serwera Radius w oparciu o posiadane serwery i licencje Zamawiajacego (Windows Server 2012R2) 13. Konfiguracja dodatkowego połączenia WAN realizowanego przez zapasowe przyłącze do sieci Internet w zakresie obsługi ruchu HTTP, HTTPS oraz protokołów obsługi poczty elektronicznej (awaryjne przełączenie w przypadku utraty dostępu do sieci świadczonej przez głównego operatora). 14. Włączenie Fortifabric i ujęcie wszystkich urządzeń dostarczanych w ramach umowy oraz obecnie posiadanych rozwiązań przez Zamawiającego (4 sztuki Fortigate seria E, Fortimail). 15. Aktualizacja klienta FSSO na kontrolerze domeny. 16. Wykonanie dokumentacji powdrożeniowej w szczególności obejmującej procedurę zgłaszania awarii.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

3 System ochrony sieci typ II dla Partnerów projektu pn. „Infostrada Kujaw i Pomorza 2.0" – 34 szt.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Komponent	Minimalne wymagania
Ogólne	System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: 1. Firewall. 2. Ochrony w warstwie aplikacji. 3. Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall musi dysponować minimum: a) 10 portami Gigabit Ethernet RJ-45. b) 2 gniazdami SFP 1 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.
Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. Analiza ruchu szyfrowanego protokołem SSH.
Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: a) Translację jeden do jeden oraz jeden do wielu. b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: a) Wsparcie dla IKE v1 oraz v2. b) Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). c) Obsługa protokołu Diffie-Hellman grup 19 i 20.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. h) Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. i) Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: a) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: a) Routingu statycznego. b) Policy Based Routingu. c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Kontrola Antywirusowa	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Zaproponowane rozwiązanie musi posiadać możliwość zarządzania poprzez posiadany przez Zamawiającego system centralnego zarządzania firmy Fortinet - FortiManager.
Logowanie	1. Zaproponowane rozwiązanie musi posiadać możliwość logowania zdarzeń i archiwizowania danych do posiadanego przez Zamawiającego systemu centralnego gromadzenia logów firmy Fortinet - FortiAnalyzer. 2. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: a) ICSA lub EAL4 dla funkcji Firewall.
Serwis	Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię. Oferent winien przedłożyć dokumenty: a) Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). b) Certyfikat ISO 9001 podmiotu serwisującego.
Inne	1. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. 2. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2004, Nr 229, poz. 2315 z późn zm.) 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.
Wdrożenie	1. Dostarczenie urządzenia zamówionych przez zamawiającego do wskazanej lokalizacji. 2. Instalacja fizyczna urządzeń oraz aktualizacja do najnowszej dostępnej wersji oprogramowania układowego. 3. Połączenie z obecną infrastrukturą zamawiającego, pozwalającą na zdalny dostęp do dostarczonych urządzeń. 4. Konfiguracja przełącznika sieciowego w zakresie konfiguracji portu. 5. Analiza aktualnych polityk zaimplementowanych na urządzeniach brzegowych. 6. Optymalizacja i przeniesienie aktualnych polityk na nowo dostarczone urządzenia. 7. Przygotowanie harmonogramu przełączeń oraz listy systemów do zweryfikowania po przełączeniu z aktywnego na nowe urządzenie. 8. Wykonanie przełączenia oraz testy poprawności działania po przełączeniu. 9. Wykonanie dokumentacji powdrożeniowej w szczególności obejmującej procedurę zgłaszania awarii.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

4 System ochrony sieci typ III dla Partnerów projektu pn. „Infostrada Kujaw i Pomorza 2.0" oraz „Budowa Kujawsko-Pomorskiego systemu udostępniania elektronicznej dokumentacji medycznej – Etap I" – 11 szt.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Komponent	Minimalne wymagania
Ogólne	System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: 1. Firewall. 2. Ochrony w warstwie aplikacji. 3. Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall musi dysponować minimum: a) 16 portami Gigabit Ethernet RJ-45. b) 8 gniazdami SFP 1 Gbps. c) 2 gniazdami SFP+ 10 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.
Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL.
Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: a) Translację jeden do jeden oraz jeden do wielu. b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: a) Wsparcie dla IKE v1 oraz v2.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	b) Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). c) Obsługa protokołu Diffie-Hellman grup 19 i 20. d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. h) Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. i) Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: a) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: a) Routingu statycznego. b) Policy Based Routingu. c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Kontrola Antywirusowa	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Zaproponowane rozwiązanie musi posiadać możliwość zarządzania poprzez posiadany przez Zamawiającego system centralnego zarządzania firmy Fortinet - FortiManager.
Logowanie	1. Zaproponowane rozwiązanie musi posiadać możliwość logowania zdarzeń i archiwizowania danych do posiadanego przez Zamawiającego systemu centralnego gromadzenia logów firmy Fortinet - FortiAnalyzer. 2. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: a) ICSA lub EAL4 dla funkcji Firewall.
Serwis	Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię. Oferent winien przedłożyć dokumenty: a) Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). b) Certyfikat ISO 9001 podmiotu serwisującego.
Inne	1. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. 2. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2004, Nr 229, poz. 2315 z późn. zm.) 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.
Wdrożenie	1. Dostarczenie urządzeń zamówionych przez zamawiającego do odpowiednich lokalizacji. 2. Instalacja fizyczna urządzeń oraz aktualizacja do najnowszej dostępnej wersji oprogramowania układowego. 3. Połączenie z obecną infrastrukturą zamawiającego, pozwalającą na zdalny dostęp do dostarczonych urządzeń. 4. Analiza aktualnych polityk zaimplementowanych na urządzeniach brzegowych. 5. Optymalizacja i przeniesienie aktualnych polityk na nowo dostarczone urządzenia. 6. Przygotowanie harmonogramu przełączeń oraz listy systemów do zweryfikowania po przełączeniu z aktywnego na nowe urządzenie. 7. Wykonanie przełączenia oraz testy poprawności działania po przełączeniu. 8. Wykonanie dokumentacji powdrożeniowej w szczególności obejmującej procedurę zgłaszania awarii.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

5 System ochrony sieci typ IV dla Partnerów projektu pn. „Infostrada Kujaw i Pomorza 2.0" – 2 szt.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym, chyba że wymaganie to zostało wprost określone inaczej.

Komponent	Minimalne wymagania
Ogólne	System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: 1. Firewall. 2. Ochrony w warstwie aplikacji. 3. Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall musi dysponować minimum: a) 18 portami Gigabit Ethernet RJ-45. b) 8 gniazdami SFP 1 Gbps. c) 2 gniazdami SFP+ 10 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w dwa redundantne zasilacze AC 230 V, 50 H.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	5. Sumaryczne zapotrzebowanie energetyczne wszystkich oferowanych urządzeń w trybie pracy z maksymalnym poborem prądu nie może przekraczać 1000 W. 6. Obudowy wszystkich oferowanych urządzeń muszą być przystosowane i dostarczone wraz z odpowiednimi uchwytami pozwalającymi na montaż w szafie RACK o szerokości 19". Wysokość obudowy pojedynczego urządzenia nie może przekraczać 1U, a sumaryczna wysokość wszystkich oferowanych urządzeń nie może przekraczać 4U. Głębokość obudowy pojedynczego urządzenia nie może przekraczać 500 mm.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz 250 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 25 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 12 Gbps. 4. Wydajność szyfrowania IPSec VPN dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 13 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.
Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL.
Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: a) Translację jeden do jeden oraz jeden do wielu. b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: a) Wsparcie dla IKE v1 oraz v2. b) Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). c) Obsługa protokołu Diffie-Hellman grup 19 i 20. d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. h) Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. i) Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: a) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: a) Routingu statycznego. b) Policy Based Routingu. c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

Kontrola Antywirusowa	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: d) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. e) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. f) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Zaproponowane rozwiązanie musi posiadać możliwość zarządzania poprzez posiadany przez Zamawiającego system centralnego zarządzania firmy Fortinet - FortiManager.
Logowanie	1. Zaproponowane rozwiązanie musi posiadać możliwość logowania zdarzeń i archiwizowania danych do systemu centralnego gromadzenia logów. 2. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: a) ICSA lub EAL4 dla funkcji Firewall.
Serwis	Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię. Oferent winien przedłożyć dokumenty: a) Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). b) Certyfikat ISO 9001 podmiotu serwisującego.
Inne	1. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. 2. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2004, Nr 229, poz. 2315 z późn. zm.) 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.
Wdrożenie	1. Dostarczenie urządzeń i licencji zamówionych przez zamawiającego do odpowiedniej lokalizacji. 2. Wykonanie dokumentacji powdrożeniowej w szczególności obejmującej procedurę zgłaszania awarii.
System centralnego gromadzenia logów	1. Zaproponowane rozwiązanie musi zostać dostarczone z systemem centralnego gromadzenia i archiwizowania oraz analizy logów przesyłanych z oferowanego Systemu ochrony sieci. 2. System musi zapewniać odbiór, zapis, przechowywanie i analizę danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego odbierania logów z wielu urządzeń raportujących.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.

	3. Gromadzenie i analiza logów musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa Systemu ochrony sieci typ IV. 4. System centralnego gromadzenia logów powinien być dostarczony w postaci maszyny wirtualnej przystosowanej do uruchomienia z wykorzystaniem hypervisora VMware vSphere, Xen lub Hyper-V z licencjami pozwalającymi na: a. gromadzenie danych logów z co najmniej 5 urządzeń b. używanie co najmniej 1000 GB przestrzeni dyskowej na składowanie logów oraz uruchomienie co najmniej następujących funkcjonalności: a. wykrywanie i raportowanie zagrożeń bezpieczeństwa i ataków przy zastosowaniu wskaźników naruszeń tworzonych i dostarczanych przez producenta systemu w oparciu o analizę danych z czujników rozlokowanych na całym świecie; aktualizacje informacji o wskaźnikach naruszeń muszą być udostępniane przez producenta codziennie i automatycznie pobierane przez system gromadzenia logów b. udostępnianie ostrzeżeń w postaci alertów o wykrytych zagrożeniach typu outbreak oraz dostarczanie ich opisu oraz zaleceń co do sposobu reagowania; raporty o zagrożeniach i zalecenia co do sposobu reagowania muszą być tworzone przez producenta systemu w czasie rzeczywistym i automatycznie pobierane przez system gromadzenia logów. 5. Wszystkie niezbędne licencje systemu centralnego gromadzenia logów muszą być ważne przez okres co najmniej 36 miesięcy, muszą zapewnić wsparcie producenta dla systemu w trybie 24x7 oraz muszą być dostosowane dla systemu gromadzącego minimum 2 GB logów dziennie. 6. Zamawiający oczekuje dostawy jednej instancji systemu centralnego gromadzenia logów dla zamawianych 2 sztuk Systemu ochrony sieci typ IV. 7. Dostarczenie komponentów sprzętowych oraz licencji platformy wirtualizacyjnej dla systemu centralnego gromadzenia logów nie wchodzi w zakres dostawy objętej niniejszym postępowaniem.

Projekty współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektów.