Zakup urządzenia klasy UTM

1. Komplet składający się z urządzenia klasy UTM wraz z subskrypcją zabezpieczeń, zgodną z opisem poniżej.
2. Zaoferowane rozwiązanie klasy UTM ma być dostarczone, zainstalowane i skonfigurowane według zaleceń Zamawiającego w jego siedzibie
3. Wykonawca zobowiązuje się do przeprowadzenia na własny koszt szkolenia dla 3 administratorów w zakresie wdrożenia i zarządzania dostarczonymi urządzeniami w terminie ustalonym z Zamawiającym.

ARCHITEKTURA SYSTEMU OCHRONY
1. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym w aktualnej wersji sprzętowej i programowej. 2. Rozwiązanie musi wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część jako router, część jako bridge).
1. Metalowa obudowa o wysokości max 1U przeznaczona do montażu w szafie RACK 19” 2. Minimalna liczba i typ interfejsów fizycznych: 6x GE (IEEE 1000Base-T), 2x GE (IEEE 1000Base-X), 3. Zainstalowane wkładki wielomodowe: IEEE 1000Base-X 2 szt. 4. Minimalna liczba nowych połączeń na sekundę: 135 000 5. Minimalna liczba jednoczesnych połączeń: 8 200 000 6. Minimalna przepustowość Firewall: 14 000 Mbps 7. Minimalna przepustowość IPS: 2 700 Mbps 8. Minimalna przepustowość NGFW: 2 900 Mbps 9. Zintegrowany wielofunkcyjny wyświetlacz LCD.
POZOSTAŁE
1. Oferta musi zawierać subskrypcje dla wszystkich wymaganych modułów na okres nie krótszy niż **36 miesięcy.** 2. Możliwość automatycznego pobierania subskrypcji dla wszystkich wymaganych modułów w okresie trwania subskrypcji. 3. Wsparcie techniczne w trybie 8x5 na okres nie krótszy niż **36 miesięcy**. 4. Gwarancja na sprzęt na okres nie krótszy niż **36 miesięcy**. 5. Możliwość automatycznego pobierania nowego oprogramowania systemowego, aktualizacji i poprawek w okresie trwania gwarancji.

PODSTAWOWE FUNKCJE SYSTEMU OCHRONY	
Zarządzanie i utrzymanie	1. Rozwiązanie musi być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI). 2. Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup. 3. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP. 4. Rozwiązanie musi oferować wiersz poleceń za pomocą protokołu SSH z autoryzacją za pośrednictwem kluczy RSA, DSA lub ECDSA o długości min. 4096 bitów. 5. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych

	urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 6. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). 7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. 8. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SNMP. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3 9. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP lub via email. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu. 10. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). 11. System ochrony musi umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive.
Zapora sieciowa, konfiguracja sieciowa oraz routing	1. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection. 2. Rozwiązanie musi umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, użytkownik, grupa lub czas. 3. System musi umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. 4. Rozwiązanie musi zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. 5. Rozwiązanie musi pozwolić na definiowanie własnych polis NAT wraz z IP masquerading. 6. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection). 7. System musi zapewniać ochrona przed skanowaniem portów (portscan blocking). 8. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). 9. Rozwiązanie musi zapewniać obsługę routingu statycznego. 10. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). 11. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. 12. System musi oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. 13. System musi oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP. 14. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. 15. Wymagane jest by rozwiązanie zapewniało obsługę dowolnych modemów USB 3G/LTE/UMTS pochodzących od dowolnego producenta.

	16. Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). 17. System musi zapewniać pełną obsługę usług DNS, DHCP oraz NTP. 18. Rozwiązanie musi zapewniać wsparcie dla IPv6 wraz z tunelowaniem 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).
Podstawowe kształtowanie pasma oraz limity ilości danych	1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników. 2. Rozwiązanie musi pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.
Bezpieczna sieć bezprzewodowa	1. Ze względu na planowaną rozbudowę systemu o obsługę sieci WiFi, oferowany system musi zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania. 2. Zarządzanie punktami dostępowymi sieci bezprzewodowej musi odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej. 3. Rozwiązanie musi umożliwiać obsługę wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej. 4. Rozwiązanie musi oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise. 5. Rozwiązanie musi zapewniać wsparcie dla IEEE 802.1X (RADIUS Authentication).
Autoryzacja użytkowników	1. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników 2. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS, LDAP 3. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory 4. System musi oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. 5. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP. 6. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal.
Samoobsługowy portal dla użytkowników	1. Rozwiązanie musi udostępniać plik instalacyjny agenta do autentykacji w sieci. 2. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). 3. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows, Mac OS X, Linux, iOS, Android. 4. Rozwiązanie musi umożliwiać zmianę nazwy użytkownika oraz hasła. 5. Rozwiązanie musi pozwalać na podglądu statystyk ruchu generowanego przez użytkownika. 6. Rozwiązanie musi oferować samoobsługowe zarządzanie kwarantanną dla wiadomości email.
Podstawowe opcje VPN	System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń: 1. Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA

	2. Client-to-site VPN: IPSec, PPTP, L2TP, SSL
Klient IPSec VPN (dostępny osobno)	1. Autoryzacja poprzez współdzielony klucz Pre-Shared Key (PSK), PKI (X.509), Smartcard, Token + XAUTH. 2. Szyfrowanie z użyciem AES, DES, 3DES, Blowfish, RSA (2048 bit), DH grupy 1/2/5/14, MD5 oraz SHA-256/384/512. 3. Monitorowanie stanu połączenia.
OCHRONA SIECI	
IPS	1. Moduł ochrony klasy IPS z bazą minimum 7000 sygnatur. 2. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS. 3. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń. 4. System musi generować alerty w przypadku wykrycia ataku.
OCHRONA I KONTROLA WEB ORAZ APLIKACJI	
Ochrona i kontrola Web	1. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS. 2. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP. 3. Rozwiązanie musi oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. walidacją certyfikatów. 4. Rozwiązanie musi zawierać przynajmniej 90 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www. 5. Rozwiązanie musi umożliwiać definiowanie polityk dostępu do internetu w oparciu o harmonogramy dzienne/tygodniowe/miesięczne/roczne dla użytkowników i grup użytkowników.
Ochrona i kontrola aplikacji	1. Rozwiązanie musi oferować bazę danych opisująca co najmniej 2500 aplikacji. 2. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji. 3. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikro-aplikacji. 4. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
Kształtowanie pasma dla Web i Aplikacji	1. Rozwiązanie musi oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron lub per aplikacja celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download/łącznie. 2. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym (shared).
OCHRONA I KONTROLA EMAIL	
Ochrona i kontrola Email	1. Rozwiązanie musi oferować możliwość wyboru trybu pracy: Transparent Email Proxy lub Explicit Email Proxy (jako MTA). 2. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S, IMAP, IMAPS. 3. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP. 4. System musi umożliwiać uruchomienie drugiego niezależnego silnika antywirusowego. 5. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń. 6. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników. 7. Rozwiązanie musi umożliwiać akceptowanie lub odrzucanie wiadomości przekraczających określony przez administratora rozmiar.

	8. System musi wykrywać próby phishingu przez analizę adresów URL zamieszczanych w treści wiadomości. 9. Rozwiązanie musi oferować ochronę przed wyciekiem danych (DLP) na podstawie predefiniowanych wzorców lub kryteriów zdefiniowanych przez administratora. 10. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL. 11. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów IP i email. 12. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka. 13. Dopuszcza się zastosowanie modułu wbudowanego w urządzenie lub poprzez dostarczenie dedykowanego urządzenia tego samego producenta.
Kwarantanna Email	1. System musi zapewniać wbudowany system kwarantanny dla wiadomości sklasyfikowanych jako spam z opcją powiadamiania użytkownika. 2. System musi zapewniać wbudowany system kwarantanny dla wiadomości sklasyfikowanych jako zainfekowane przez malware.
OCHRONA SERWERÓW APLIKACYJNYCH WEB	
WAF	1. Dodatkowy moduł ochrony klasy Web Application Firewall. 2. Rozwiązanie musi oferować mechanizm Form hardening. 3. Rozwiązanie musi oferować ochronę przed SQL injection. 4. Rozwiązanie musi oferować ochronę przed Cross-site scripting. 5. System musi zapewniać inspekcję ruchu HTTP oraz HTTPS (SSL). 6. System musi pozwalać na podpisywanie plików cookies. 7. Rozwiązanie musi oferować wsparcie dla Path-based routing. 8. Rozwiązanie umożliwiające publikowanie aplikacji web w Internecie na zasadzie wirtualnych serwerów aplikacyjnych. 9. Rozwiązanie musi oferować mechanizm rozkładający ruch odwiedzających między rzeczywiste serwery aplikacyjne (Load Balancing). 10. Dopuszcza się zastosowanie modułu wbudowanego w urządzenie lub poprzez dostarczenie dedykowanego urządzenia tego samego producenta.
LOGOWANIE I RAPORTOWANIE	
Logowanie i raportowanie	1. System musi umożliwiać składowanie oraz archiwizację logów. 2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. 3. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych). 4. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog. 5. System musi zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza 6. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację
OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY	
On-cloud Sandboxing	1. Dodatkowy moduł ochrony klasy on-cloud Sanbox. 2. Rozwiązanie umożliwiające dodatkową inspekcję plików wykonywalnych w tym .exe, .com, .dll.

	3. Rozwiązanie umożliwiające dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf. 4. Rozwiązanie umożliwiające dodatkową inspekcję plików .pdf. 5. Rozwiązanie umożliwiające dodatkową inspekcję plików archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .7z, .cab. 6. System zapewniający dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows i MacOS. 7. System ochrony ze średnim realnym czasem analizy kodu poniżej 120 sekund. 8. System powinien oferować szczegółowe raporty wyników analizy. 9. System musi posiadać moduł Sandbox, który pozwala na weryfikację plików w chmurze producenta. 10. Dopuszcza się zastosowanie modułu wbudowanego w urządzenie lub poprzez dostarczenie dedykowanego urządzenia tego samego producenta.
POZOSTAŁE	
Certyfikaty	CE, FCC
Rozbudowa	Ze względu na planowaną rozbudowę systemu ochrony sieci wymagane jest, by producent rozwiązania posiadał w swojej ofercie system ochrony poczty oraz stron www (oprogramowanie bezpieczeństwa instalowane na komputerach i telefonach).

INSTALACJA I KONFIGURACJA
Zamawiający wymaga dostarczenia i montażu urządzeń we wskazanej lokalizacji Zamawiającego. Wykonawca będzie zobowiązany: 1. przeprowadzić testy funkcjonalne i wydajnościowe na środowisku testowym, 2. aktywować wszystkie zakupione licencje, 3. zaktualizować urządzenia i oprogramowanie do najnowszej wersji, 4. zainstalować i skonfigurować oprogramowanie zarządzające, 5. przeprowadzić testy funkcjonalne i wydajnościowe na środowisku produkcyjnym, 6. przeprowadzić symulację awarii i przełączenia klastra z urządzenia na urządzenie, 7. przeprowadzić co najmniej 8-godzinne szkolenie stanowiskowe dla 3 administratorów z podstawowej obsługi urządzeń i oprogramowania.

Gwarancja i serwis
Wymagania ogólne dla dostarczanych rozwiązań :
1. Dostarczone urządzenia musza być fabrycznie nowe, nieużywane w innych projektach, nie wycofane z produkcji i pochodzić z legalnego, polskiego kanału dystrybucji. 2. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na teren Polski – ze względów gwarancyjnych niedopuszczalne jest dostarczanie sprzętu z tzw. brokerki, 3. Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie zapisanym w specyfikacjach sprzętu, 4. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień dostawy, 5. Całość dostarczonego sprzętu i oprogramowanie musi być ze sobą kompatybilna, 6. Wykonawca winien w momencie dostawy przedłożyć dokumenty potwierdzające, że posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.
Warunki gwarancji i serwisu :
1. Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta dostarczonych rozwiązań, 2. Serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu,

3. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (od poniedziałku do piątku, w godzinach 8-17), fax, e-mail lub WWW (przez całą dobę),
4. Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań,