Załącznik nr 1 do zapytania

„Dostawa systemu zabezpieczeń klasy UTM”

1. Wymagania dotyczące realizacji przedmiotu Zamówienia

1.1. Wymagania ogólne dotyczące dostawy i instalacji elementów zamówienia

- Dostarczony sprzęt musi być fabrycznie nowy (zapakowany w opakowanie przeznaczone dla przedmiotu zamówienia), wyprodukowany nie wcześniej niż 2021 r. Nie dopuszcza się urządzeń noszących jakiekolwiek widoczne ślady użycia, odnawianych, demonstracyjnych lub powystawowych oraz wykorzystanych przynajmniej raz w innym projekcie.
- Wraz ze sprzętem muszą zostać dostarczone wszystkie niezbędne licencje oprogramowania pozwalające na poprawne funkcjonowanie sprzętu oraz opisanych funkcjonalności .

2. Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest dostawa systemu zabezpieczeń klasy UTM dla lokalizacji Ceglana

Tabela 1. Elementy systemu bezpieczeństwa

Nazwa	Liczba zamawianego sprzętu
System UTM w konfiguracji wysokiej dostępności (HA) wraz z systemem logowania, raportowania i korelacji	1 komplet tj. 2 sztuki urządzeń – system UTM HA 1 komplet tj. 1 urządzenie/system wirtualny – system logowania, raportowania, korelacji

Tabela 2. Wymagania wspólne dla systemu bezpieczeństwa

Wymagania wspólne		
1.	Ogólne	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 systemu UTM dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym (nie dotyczy systemu centralnego logowania, raportowania i korelacji).
2.	Licencje	- w ramach postępowania Wykonawca dostarczy minimum następujące licencje: • licencje umożliwiające korzystanie z aktualizacji baz funkcji ochronnych producenta i serwisów przez cały okres gwarancji. Muszą one obejmować co najmniej: kontrolę aplikacji, IPS, antywirus’a (z uwzględnieniem sygnatur do

		ochrony urządzeń mobilnych – co najmniej dla systemu operacyjnego Android), • licencje umożliwiające analizę typu antyspam, web filtering, bazy reputacyjne adresów IP/domen **Wszystkie licencje na okres zgodny z zaoferowanym okresem wsparcia gwarancyjnego**

Tabela 3. Szczegółowe parametry techniczne systemu bezpieczeństwa

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
System UTM w konfiguracji wysokiej dostępności (HA) Zamawiający wymaga dostarczenia jednego klastra wysokiej dostępności (HA) dla lokalizacji Ceglana. Na klaster składać się będą dwa urządzenia fizyczne lub dwa pre-instalowane systemy wirtualne tzw. Virtual Appliance wraz ze sprzętem i systemem operacyjnym na którym będą mogły być uruchomione, z którym będą kompatybilne i na którym ich wydajność nie będzie mniejsza od równorzędnego systemu na urządzeniach fizycznych. Zamawiający oświadcza, iż posiada wdrożony i działający system bezpieczeństwa w oparciu o urządzenia FortiGate 600C pracujące w klastrze HA oraz personel przeszkolony z jego obsługi. Używany obecnie klaster urządzeń FortiGate 600C nie będzie nadal wykorzystywany w strukturze sieciowej Zamawiającego, jednocześnie Zamawiający zgadza się na program wymiany posiadanych urządzeń FortiGate 600C na nowe zgodne z poniższymi wymaganiami (zwrot starych urządzeń zostanie potwierdzony stosownym protokołem)		
1.	Redundancja, monitoring i wykrywanie awarii	- system musi pełnić funkcje: Firewall'a, IPSec, Kontroli Aplikacji oraz IPS - system musi posiadać możliwość łączenia w klaster Active-Active lub Active-Passive, a w obu tych trybach musi istnieć funkcja synchronizacji sesji firewall - system musi posiadać funkcje monitoringu i wykrywania uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych - system musi posiadać monitoring stanu realizowanych połączeń VPN - system musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP, jednocześnie musi istnieć możliwość tworzenia interfejsów redundantnych
2.	Interfejsy, zasilanie	- każde z urządzeń w klastrze HA składające się na system realizujący funkcję Firewall musi dysponować: minimum 10 portami Gigabit Ethernet RJ-45 minimum 8 gniazdami SFP 1 Gbps minimum 2 gniazdami SFP+ 10 Gbps - każde z urządzeń w klastrze HA składające się na system musi zostać wyposażone w dwa moduły SFP+ 10Gbps LRM i kablami światłowodowymi MM OM3/125 o

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
		długości 2m~5m do połączenia z przełącznikiem szkieletowym Zamawiającego - każde z urządzeń w klastrze HA składające się na system Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB - w ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych – definiowanych jako VLAN'y w oparciu o standard 802.1Q - system musi być wyposażony w zasilanie AC 220/230V - każde z urządzeń w klastrze HA składające się na system bezpieczeństwa musi być wyposażony w dodatkowy redundantny zasilacz, zasilacz ten musi być kompatybilny z oferowanym rozwiązaniem. - w przypadku zaoferowania rozwiązania opartego o tzw. Virtual Appliance Zamawiający wymaga aby sprzęt na którym będzie to rozwiązanie pracować zapewniało redundantne zasilanie w oparciu o minimum dwa zasilacze
3.	Wydajność systemu bezpieczeństwa	- w zakresie Firewall'a obsługa nie mniej niż 8 milionów jednoczesnych połączeń oraz nie mniej niż 390 tysięcy nowych połączeń na sekundę - przepustowość Stateful Firewall nie mniej niż 36 Gbps - przepustowość Firewall'a z włączoną funkcją Kontroli Aplikacji nie mniej niż 15 Bps - wydajność szyfrowania IPSec VPN nie mniej niż 20 Gbps - 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 10 Gbps - wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami IPS, Application Control, Antywirus minimum 7 Gbps - wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http minimum 8 Gbps
4.	Funkcje systemu UTM	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci komercyjnych platform sprzętowych lub programowych: - kontrola dostępu – zapora ogniowa klasy Statefull Inspection - kontrola aplikacji - poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN - ochrona przed Malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS - ochrona przed atakami - Intrusion Prevention System

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
		- kontrola stron WWW - kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP - zarządzanie pasmem (QoS, Traffic Shaping) - mechanizmy ochrony przed wyciekiem poufnej informacji (DLP) - dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych - w ramach postępowania muszą zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu Client-to-Site - analiza ruchu szyfrowanego protokołem SSL - analiza ruchu szyfrowanego protokołem SSH
4a.	Polityki Firewall	- polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń - system musi zapewniać translację adresów NAT źródłowego i docelowego, translację PAT oraz translację jeden do jeden, translację jeden do wielu, dedykowany ALG (Application Level Gateway) dla protokołu SIP - w ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN
4b.	Połączenia VPN	- system musi umożliwiać konfigurację połączeń typu IPSec VPN i zapewniać wsparcie dla IKE v1 oraz v2, obsługę szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM), obsługę protokołu Diffie-Hellman grup 19 i 20, wsparcie dla pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE, tworzenie połączeń typu Site-to-Site oraz Client-to-Site, monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności, możliwość wyboru tunelu przez protokoły dynamicznego routingu (np. OSPF) oraz routingu statycznego, obsługę mechanizmów IPSec NAT Traversal, DPD, Xauth, mechanizm „Split tunneling” dla połączeń Client-to-Site - system musi umożliwiać konfigurację połączeń typu SSL VPN i zapewniać 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), pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
4c.	Routing i obsługa łączy WAN	- w zakresie routingu rozwiązanie powinno zapewniać obsługę routingu statycznego, polityk ruchu bazujących na routingu, protokołów dynamicznego routingu w oparciu o protokoły RIPv2, OSPF, BGP oraz PIM - system musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN
4d.	Zarządzanie pasmem	- system Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu - musi istnieć możliwość określania pasma dla poszczególnych aplikacji - system musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL
4e.	Kontrola antywirusowa	- silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) - system musi umożliwiać skanowanie archiwów, w tym co najmniej: ZIP, RAR - system musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android) - system musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze.
4f.	Ochrona przed atakami (IPS)	- ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych - system powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach - baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora - administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur - system musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DdoS - 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 - wykrywanie i blokowanie komunikacji C&C do sieci Botnet

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
4g.	Kontrola aplikacji	- funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP - baza Kontroli Aplikacji powinna zawierać minimum 2250 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora - aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików - baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P - administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur
4h.	Kontrola stron internetowych (WWW)	- moduł kontroli WWW musi korzystać z bazy adresów URL pogrupowanych w kategorie tematyczne - filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard - administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL - administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania
4i.	Uwierzytelnianie użytkowników w ramach sesji	- system Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu, haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych - musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego - rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów np. RADIUS lub API
4j.	Zarządzanie systemem	- 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 - komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów - powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
		administracyjnego - system musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow - system musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację - element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall
4k.	Logowanie zdarzeń	- 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 - w ramach logowania system pełniący funkcję Firewall 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 - logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu - musi istnieć możliwość logowania do serwera SYSLOG
5.	Certyfikaty	System musi posiadać deklarację zgodności Poszczególne elementy oferowanego systemu bezpieczeństwa muszą posiadać następujące certyfikacje: - certyfikacja ICSA lub EAL4 dla oferowanego urządzenia, - certyfikat ICSA lub rekomendacja respektowana przez NATO i Unię Europejską NATO Restricted i UE Restricted dla funkcji IPS, IPSec VPN, SSL VPN
6.	Pozostałe	- system UTM realizujący funkcje Firewall musi dawać możliwość pracy w jednym z trzech trybów tj.: routera z funkcja NAT, transparentnym oraz w trybie monitorowania na porcie SPAN, - musi być zapewniona możliwość budowy minimum dwóch oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: routingu, firewall'a, IPSec VPN, antywirusa, IPS, kontroli aplikacji, - musi istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu UTM,

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
		- musi wspierać Ipv4 oraz Ipv6 w zakresie: firewall'a, ochrony w warstwie aplikacji, protokołów routingu dynamicznego.
System logowania, raportowania i korelacji Zamawiający wymaga dostarczenia jednego systemu, który: - zastąpi pracę posiadanego systemu analizy logów i raportowania FortiAnalyzer 200D, - będzie umożliwiał centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej DOSTARCZANEJ w ramach niniejszego postepowania infrastruktury zabezpieczeń Klasy UTM jak również posiadanego już przez Zamawiającego systemu zabezpieczeń klasy UTM zbudowanego na urządzeniach fizycznych FortiGate 600E (klaster HA) oraz, oraz systemu ochrony aplikacji webowych FortiWeb 400C, poprzez ich integrację w zakresie opisanym poniżej.		
7.	Kompatybilność	Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy lub komercyjnych platform działających w środowisku wirtualnym lub w postaci komercyjnej platformy działających na bazie systemu linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: Vmware ESX/ESXi 5.5,6.0,6.5,6.7, Microsoft Hyper-V 2008 R2,2012, R2,2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).
8.	Interfejsy, dyski	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności minimum 6 TB.
9.	Wydajność	Rozwiązanie musi umożliwiać kolekcjonowanie logów z wszystkich wskazanych systemów posiadanych przez Zamawiającego, tj. FortiGate 600E, FortiWeb400C, oraz dostarczanych w ramach niniejszego postępowania. Rozwiązanie musi umożliwiać kolekcjonowanie logów z minimum 1000 systemów. System musi być w stanie przyjmować minimum 11 GB logów na dzień.
10.	Funkcje systemu	W ramach centralnego systemu zarządzenia muszą być realizowane co najmniej poniższe funkcje dla wszystkich podłączonych do systemu urządzeń: W zakresie logowania:

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
		- podgląd logowanych zdarzeń w czasie rzeczywistym, - możliwość przeglądania logów historycznych z funkcją filtrowania, - dostępne predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa obejmujące co najmniej: • listę najczęściej wykrywanych ataków, • listę najbardziej aktywnych użytkowników, • listę najczęściej wykorzystywanych aplikacji, • listę najczęściej odwiedzanych stron www, • listę krajów, do których nawiązywane są połączenia • listę najczęściej wykorzystywanych polityk firewall • informacje o realizowanych połączeniach IPSec W zakresie raportowania: - możliwość generowania raportów co najmniej w formatach: PDF, CSV, - dostępne predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników, - możliwość definiowania własnych raportów, - możliwość spolszczenia raportów, - możliwość generowania raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesyłania wyników na określony adres lub adresy email. W zakresie korelacji logów: - umożliwiać określenie urządzeń, dla których proces korelacji ma być realizowany, - umożliwiać konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa,

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
		- umożliwiać wybór kategorii zdarzeń dla których tworzone będą reguły korelacyjne, - umożliwiać korelację zdarzeń co najmniej z następujących kategorii zdarzeń: malware, aplikacje sieciowe, email, IPS, traffic, systemowe (utracone połączenia vpn, utracone połączenia sieciowe).
11.	Komunikacja/eksport danych	Rozwiązanie musi posiadać możliwość przesyłanie kopii logów do innych systemów logowania i przetwarzania danych. W tym zakresie musi zapewniać mechanizmy filtrowania dla wysyłanych logów. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
12.	Zarządzenie	System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów HTTPS oraz SSH lub producent rozwiązania musi dostarczyć dedykowana konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. Proces uwierzytelniania administratorów musi być realizowany w oparciu o lokalna bazę, Radius, LDAP, PKI. System musi umożliwiać zdefiniowanie co najmniej 3 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
13.	Licencje	System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu, a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.