Załącznik - Nr 1

UTM – 2 szt.

Wymagania:	
Sekcja 1 — Interfejs	
1	Urządzenie musi posiadać interfejs WWW z poziomu, którego administrator może wykonać wszystkie czynności administracyjne
2	Rozwiązanie musi posiadać możliwość podpięcia rozwiązania do systemu centralnego zarządzania i zarządzania urządzeniem poprzez dedykowaną aplikacje.
3	Rozwiązanie musi posiadać możliwość zarządzania nim z poziomu chmurowego portalu centralnego zarządzania. Dostęp do portalu chmurowego musi być dostarczony w ramach podstawowej licencji.
4	Z poziomu interfejsu WWW administrator musi mieć możliwość szybkiego przeglądu stanu urządzenia widząc na pierwszej stronie minimum następujące informacje: - wersja oprogramowania układowego, - nazwa urządzenia, - adres sprzętowy urządzenia, - czas pracy urządzenia od ostatniego restartu, - status sieci internet, - status sieci wifi, - ostatnio wykryte urządzenia w sieci wraz z alertami, - aktywność sieci zawierającą wykres ilości pakietów i ilości danych przepływających w czasie rzeczywistym przez urządzenie.
5	Urządzenie musi możliwość wyświetlenie wszystkich aktywnych urządzeń pracujących w sieci, w postaci listy dostępnej bezpośrednio z interfejsu WWW.
6	Jeśli urządzenie posiada moduł sieci bezprzewodowej to musi umożliwiać wyświetlenie aktywnych urządzeń podłączonych do sieci bezprzewodowej, wraz z informacjami o jakości sygnału dla pojedynczych urządzeń.
7	Urządzenie musi umożliwiać generowanie raportów ogólnych zawierających status urządzenia minimum w odstępach: - ostatnia godzina, - ostatni dzień,
8	Urządzenie musi umożliwiać generowanie raportów z aktywności użytkowników i komputerów minimum w odstępach: - ostatnia godzina, - ostatni dzień, - ostatni tydzień, - ostatni miesiąc,
9	Urządzenie musi umożliwiać na wydruk raportów z aktywnością użytkowników bezpośrednio z poziomu interfejsu WWW rozwiązania.
10	Urządzenie musi umożliwiać przegląd i wyszukiwanie logów sieciowych bezpośrednio z interfejsu WWW.
11	Urządzenie musi umożliwiać przegląd i wyszukiwanie logów systemowych bezpośrednio z interfejsu WWW.
12	Jeśli urządzenie posiada moduł sieci bezprzewodowej to musi umożliwiać monitorowanie okolicznych sieci bezprzewodowych znajdujących się w zasięgu urządzenia, oraz pozwalać na ich przegląd bezpośrednio z interfejsu WWW.
13	Urządzenie musi mieć możliwość na wyświetlenia: - stanu zasobów sprzętowych, - tablicy routingu, - stanu połączenia z usługami chmurowymi, bezpośrednio z poziomu interfejsu WWW
14	Urządzenie musi posiadać funkcje pozwalające na wykonanie testów działania sieci dostępne bezpośrednio z interfejsu WWW. Wymagane są minom narzędzia takie jak: - ping, - traceroute, - dns lookup, - tcpdump,
15	Urządzenie musi umożliwiać wygenerowanie plików diagnostycznych z działania systemu urządzenia, bezpośrednio z interfejsu WWW.
16	Interfejs WWW musi umożliwiać zalogowanie się wielu administratorom jednocześnie.
Sekcja 2 — Funkcjonalności	
Numer	Wymaganie
1.	Urządzenie musi mieć możliwość pracy zarówno w trybie monitorowania, jak i w trybie inline.
2.	Urządzenie musi być minimalnie wyposażone w następujące moduły funkcjonalne: - Firewall, - Kontrola aplikacji i URL Filtering, - Rozpoznawanie użytkowników, - QoS, - IPS, - Anti-Virus, - Anti-Bot, - Emulacja zagrożeń (dodatkowo punktowane 20 pkt) - Antyspam, - VPN Site-to-Site, - VPN Client-to-Site,
3.	Urządzenie musi mieć możliwość monitorowania dostępu do internetu poprzez weryfikacje podanych przez administratora hostów.

Załącznik - Nr 1

	Urządzenie musi monitorować minimum następujące parametry sieciowe: - Utrata pakietów, - Średnie opóźnienie, - Minimalne opóźnienie, - Maksymalne opóźnienie, - Jitter,
4.	Urządzenie musi umożliwiać pełną rekonfigurację interfejsów wewnętrznych, wspierając m.in.: - Stworzenie wirtualnego switch z interfejsów, - Stworzenie interfejsów typu bridge, - Agregacji interfejsów m.in. za pomocą LACP.
5.	Urządzenie musi mieć możliwość filtrowania urządzeń poprzez filtrowanie adresów MAC.
6.	Urządzenie musi posiadać mechanizm DNS Proxy.
7.	Urządzenie musi posiadać możliwość ograniczenia dostępu administracyjnego tylko z konkretnych podsieci, oraz tylko z konkretnych stref.
8.	Urządzenie musi mieć możliwość synchronizacji czasu poprzez protokół NTP.
9.	Urządzenie musi mieć możliwość uruchomienia serwera NTP bezpośrednio na urządzeniu.
10.	Urządzenie musi wspierać serwisy DDNS, minimum: - DynDNS - no-ip.org
11.	Urządzenie musi posiadać funkcję pozwalającą na zarządzenie urządzeniem z sieci internet, nawet jeśli znajduje się za NATem. Funkcja ta nie może wymagać od administratora uruchomienia tunelu VPN do sieci wewnętrznej.
12.	Urządzenie musi mieć możliwość pracownia w klastrze wysokiej dostępności.
13.	Urządzenie musi posiadać predefiniowane profile pracy Firewalla, Kontroli aplikacji, URL Filteringu i modułu IPS.
14.	Urządzenie musi umożliwiać ręczne definiowanie reguł działających na: - firewallu, - module kontroli aplikacji i URL Filteringu, - module IPS,
15.	Urządzenie musi umożliwiać logowanie każdej sesji zezwolonej lub zablokowanej.
16.	Urządzenie musi posiadać dwa osobne zestawy reguł. Jeden dla połączeń wychodzących do internetu, drugi dla obsługi połączeń wewnętrznych.
17.	Urządzenie musi posiadać predefiniowaną politykę translacji adresów, pozwalającą na jej zastosowanie przy połączeniach wychodzących do internetu.
18.	Urządzenie musi wspierać filtrowanie protokołów VoIP, oraz pozwalać na konfiguracje filtrowania tych urządzeń za pomocą prostego kreatora konfiguracji.
19.	Urządzenie musi mieć możliwość integrowania się z usługami katalogowymi, minimum Microsoft Active Directory.
20.	Urządzenie musi mieć możliwość inspekcji ruchu SSL.
21.	Urządzenie musi mieć możliwość kategoryzowania stron HTTPS bez inspekcji ruchu SSL.
22.	Urządzenie musi posiadać interfejs, w którym administrator może znaleźć wszystkie zainfekowane urządzenia w sieci.
23.	Urządzenie musi mieć możliwość całkowitego wyłączenia modułu IPS i uruchomienia go tylko w trybie IDS.
24.	Urządzenie musi umożliwiać na stworzenie tuneli VPN typu client-2-site minimum w formie: - dedykowane klienta VPN dostarczanego przez producenta rozwiązania, - mobilnego klient VPN dostarczanego przez producenta rozwiązania, - portalu SSL VPN, - klienta wbudowanego w system Windows,
25.	Urządzenie musi posiadać moduł kontroli aplikacji zawierający ponad 9300 różnych aplikacji.
26.	Urządzenie musi umożliwiać inspekcje ponad 70 protokołów przemysłowych w tym minimum: - BACNet, - CIP, - DNP3, - IEC-60870-5-104, - IEC 60870-6 (ICCP), - IEC 61850, - MMS, - ModBus, - OPC DA & UA, - Profinet, - Step7 (Siemens)
27.	Urządzenie musi posiadać funkcjonalność tzw. Virtual Patchingu. Funkcja ta pozwala na zablokowanie ataków kierowanych na podatne urządzenie, które z różnych przyczyn nie mogą zostać zaktualizowane przez administratora.
28.	Lista wspieranych przez moduł kontroli aplikacji, aplikacji musi być publicznie dostępna i pozwalać na przeszukiwanie jej z wykorzystaniem różnych filtrów.
Sekcja 3 — Wydajność	
Numer	Wymaganie
1	Urządzenie musi być przystosowane do pracy w temperaturach od 0 stopni do 40 stopni Celsiusa.
2	Urządzenie musi posiadać następujące certyfikacje: CB 62368-1, CE, FCC IC Class B, VCCI, AS/NZS RCM EMC.

Załącznik - Nr 1

3	Urządzenie musi posiadać następujące porty: - LAN: 17 x 1GbE, - WAN: 1x1GbE - USB typ C do połączenia konsolowego, - 2 x Port USB 3.0, - wielkość pamięci nieulotnej 32 GB
4	Wymagane przepustowość urządzenia dla: - Ruchu NGTP: 1450 Mbps, - Ruchu NGFW: 3150 Mbps, - Ruchu IPS: 3450 Mbps, - Ruchu Firewall: min. 4800 Mbps, - Firewalla i pakietów UDP o wielkości 1518 bajtów: min. 8000 Mbps - VPN AES-128: min. 1300 Mbps, - Połączeń na sekundę: min. 54000 - Jednoczesnych połączeń: min. 245000
Sekcja 4 — Certyfikaty	
Numer	Wymaganie
1.	Oświadczenie producenta, iż oferent jest autoryzowanym przedstawicielem producenta rozwiązania UTM
Szkolenie: Zakres szkolenia po wdrożeniowego." Tryby pracy urządzeń w sieci Użycie GUI i CLI do zadań konfiguracyjnych Omówienie zasad dostępu sieciowego do zabezpieczanych sieci za pomocą reguł zapory sieciowej. Omówienie funkcji przekierowywania portów, source NAT i destination NAT Uwierzytelnianie użytkowników za pomocą reguł zapory sieciowe Omówienie zagadnień związanych z szyfrowaniem i operacji opartych na certyfikatach Omówienie jak role i uprawnienia administracyjne wspomagają politykę zarządzania Omówienie wdrożeń i środowisk dla VPN typu Site-to-Site i zdalnego dostępu VPN Omówienie jak analizować i interpretować ruch VPN Omówienie praktyk wykonania okresowych zadań administratora Szkolenie dla wyznaczonych pracowników Zamawiającego min. 2 Użytkowników.	

Usługa wdrożenia UTM – 1 szt.

Lp.	Usługa wdrożenia UTM
1.	Zamawiający planuje zainstalowanie dwóch urządzeń bezpieczeństwa - Firewall. Zostaną one uruchomione i skonfigurowane jako klaster Active-Standby, dzięki temu w momencie awarii urządzenia głównego, urządzenie zapasowe, będzie w stanie przejąć pracę urządzenia głównego, bez dodatkowej inicjatywy administratora. Klaster zostanie zaktualizowany do najnowszej, rekomendowanej przez producenta wersji w celu zapewnienia najwyższej możliwej na dany moment funkcjonalności i bezpieczeństwa. Konfiguracja sieciowa, w tym interfejsów lokalnych, WAN, routingu oraz protokołów komunikacyjnych zostanie odtworzona z obecnej konfiguracji Zamawiającego lub zaostanie wykonana wg nowych wytycznych dostarczonych przez Zamawiającego. Zakończenie tego etapu poprzedzą testy komunikacyjne weryfikujące wszystkie uruchomione funkcjonalności oraz prawidłowe działanie samego klastra. Kolejnym krokiem będzie zapewnienie dostępu do urządzenia. Utworzone zostaną konta użytkowników lokalnych z zachowaniem polityk bezpieczeństwa i ograniczonego dostępu do pewnych funkcjonalności. Zostaną skonfigurowane połączenia VPN umożliwiające zdalny dostęp do klastra. Klasyfikacja użytkowników opierać się będzie o miejsca gdzie użytkownicy mogą się dostać oraz o poziom uprawnień dzielony na: • odczyt/zapis, • tylko odczyt, • dostęp zabroniony. Aby zapewnić bezpieczeństwo i kontrolę sieci utworzone zostaną polityki bezpieczeństwa. Powstaną na podstawie już istniejących polityk lub informacji dostarczonych bezpośrednio przez Zamawiącego. Zostanie utworzona baza obiektów wykorzystywanych w sieci Zamawiającego, które później posłużą jako obiekty źródłowe/docelowe przy kreowaniu polityk. Po odtworzeniu pełnej listy polityk wykonane zostaną testy komunikacyjne potwierdzające prawidłowe dostępy w sieci lub ich celowy brak. Ostatnim etapem będzie konfiguracja cyklicznego backupu konfiguracji i polityk w celu zabezpieczenia się przed utratą części lub całości danych. Zostanie sporządzona dokumentacja powykonawcza opisująca wdrożenie oraz wykorzystane funcjonalności
2.	Zakres działań: 1. Analiza przedwdrożeniowa obejmująca weryfikację logicznej konfiguracji sieci Zamawiającego niezbędna do przygotowania projektu technicznego; analiza będzie obejmować spotkania robocze na których Zamawiający przedstawi infrastrukturę sieciową, systemową oraz aplikacyjną w zakresie niezbędnym do realizacji przedmiotu zamówienia. 2. Opracowanie projektu technicznego opisującego konfigurację urządzeń i oprogramowania niezbędnego do realizacji wdrożenia. 3. Instalacja sprzętu wraz z okablowaniem w serwerowni określonej w zaakceptowanym przez Zamawiającego projekcie technicznym, Wykonawca będzie zobowiązany do posprzątania miejsc instalacji urządzeń w siedzibie Zamawiającego, oraz pozostawienia tych miejsc w stanie nie gorszym od zastanego przed przystąpieniem do prac. 4. Opracowanie scenariuszy testowych potwierdzających zgodność dostarczonych rozwiązań z SIWZ, zatwierdzeniu scenariuszy przez

	Zamawiającego i przeprowadzenie testów zgodnie ze scenariuszami. 5. Przeprowadzenie testów. 6. Wykonanie dokumentacji powykonawczej opisującej szczegółową konfigurację wdrożonego rozwiązania.