

Załącznik nr 1.2 do SWZ**Opis przedmiotu zamówienia****Znak Sprawy: IP.271.1.2026****CZĘŚĆ II ZAMÓWIENIA – Wzmocnienie obszaru technicznego - Dostawa urządzenia UTM wraz ze wsparciem do Urzędu Gminy Urszulin**

Przedmiotem zamówienia jest dostawa i konfiguracja urządzenia klasy UTM (Unified Threat Management) wraz z oprogramowaniem i licencjami obejmującymi funkcje ochrony sieci takie jak: firewall, IPS, ochrona antywirusowa, filtrowanie treści internetowych, kontrola aplikacji oraz VPN w środowisku Zamawiającego. Urządzenie ma umożliwiać bezpieczną ochronę sieci lokalnej przed zagrożeniami zewnętrznymi i wewnętrznymi.

Minimalne parametry techniczne i funkcjonalne:

Element konfiguracji	Wymagania minimalne
Elementy systemu bezpieczeństwa	<ul style="list-style-type: none">• Urządzenie musi mieć możliwość jednoczesnej pracy w trybie Layer 3 (routing), transparentnym (most) i Layer 2 (port mirroring) bez konieczności wirtualizacji sprzętu• Możliwość stworzenia minimum 64 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q.• W zakresie Firewall, obsługa nie mniej niż 1 500 000 jednoczesnych połączeń i 48000 nowych połączeń na sekundę• System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o minimalnej pojemności 8 GB do celów logowania i raportowania• Możliwość rozszerzenia pamięci do co najmniej 1.9TB poprzez dodatkowy dysk SSD bez otwierania obudowy urządzenia• Musi posiadać 2x USB 3.0 z przodu urządzenia• Musi posiadać 1x port konsoli• System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu• System musi mieć możliwość włączenia min 1 systemu wirtualnego bez

	<p>dodatkowej licencji i możliwości rozszerzenia do minimum 5 poprzez dodatkową licencję w przyszłości</p> <ul style="list-style-type: none"> • Systemy wirtualne muszą obsługiwać QOS • System pełniący funkcję zapory musi posiadać nie mniej niż: 8x GE interfejsów • System musi posiadać co najmniej jedną parę interfejsów typu bypass. • Urządzenie musi posiadać dedykowany port przeznaczony do zarządzania • System musi posiadać możliwość wykorzystania portu USB jako Modemu WAN 4G • System musi posiadać zewnątrz przycisk, pozwalając na reset urządzenia do ustawień fabrycznych, bez konieczności logowania się do urządzenia
Funkcjonalności	<ul style="list-style-type: none"> • Kontrola dostępu — zaporą sieciową Stateful Inspection • Ochrona przed wirusami - komercyjny antywirus [AV] • Poufność danych - IPSec VPN i SSL VPN • Kontrola witryn sieci Web — filtr URL • Kontrola zawartości poczty - antyspam (dla protokołów SMTP, POP3) • Kontrola przepustowości i ruchu [QoS i kształtowanie ruchu] z alokacją Tunnel w oparciu o strefę bezpieczeństwa, interfejs, adres, użytkownika/grupę użytkowników, serwera/ grupę serwerów, aplikację/grupę aplikacji, TOS, VLAN • Kontrola aplikacji i rozpoznawanie ruchu P2P (wideo, gry itp.) oraz ograniczanie nowych połączeń i jednoczesnych sesji • Reputacja IP • Cloud Sandbox • API – możliwość wgrywania i wyciągania informacji z systemu dedykowanym interfejsem Rest API
Wydajność	<ul style="list-style-type: none"> • Analiza ruchu szyfrowanego protokołem SSL • Wydajność Firewall co najmniej 5 Gb/s • Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym IPS i kontrolą aplikacji co najmniej 1.7 Gb/s • Wydajność ochrony przed atakami (IPS) minimum 2.8 Gb/s • Wydajność AV nie mniej niż 1.7 Gb/s • Wydajność skanowania z włączoną kontrolą aplikacji, AV, IPS, filtrem URL nie mniejsza niż 0.8 Gb/s
Funkcjonalności VPN	<ul style="list-style-type: none"> • Wydajność IPSec VPN, nie mniej niż 2.7 Gb/s • Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja • Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem • Monitorowanie stanu tuneli VPN i utrzymywanie ich aktywności

	<ul style="list-style-type: none"> • Praca w topologiach Hub and Spoke i Mesh • Wspierane mechanizmy : IPSec NAT Traversal, DPD, Replay Detection, Xauth, DHCP over IPsec, • Wsparcie grup DH dla IKEv1: 1,2,5,19,20,21,24 • Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,19,20,21,24 • Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance) co najmniej w zakresie: <ul style="list-style-type: none"> - Wersji systemu operacyjnego - Zaaplikowanych patchy - Ustawień internetowych - Zainstalowanego oprogramowania antywirusowego - Włączonego Firewalla - Walidacji kluczy rejestru - Walidacji istnienia plików - Walidacji uruchomionych procesów - Walidacji uruchomionych lub zainstalowanych serwisów • Możliwość rozszerzania ilości użytkowników VPN odpowiednią licencją • Obsługa PnPVPN (Plug and Play VPN)
Routing	<ul style="list-style-type: none"> • Rozwiązanie musi zapewniać: obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP, IS-IS • Obsługa Policy Based Routing • Funkcjonalność Virtual Wire
Translacja adresów NAT	<ul style="list-style-type: none"> • Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego • Obsługa NAT46, NAT64, DNS64 • Wsparcie dla STUN
Polityka bezpieczeństwa systemu	<ul style="list-style-type: none"> • Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje bezpieczeństwa, rejestrowanie zdarzeń i zarządzanie pasmem sieci (w tym gwarantowaną i maksymalną przepustowość, priorytety) • Możliwość budowania min. 8000 polityk • Musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego • Musi być w stanie skonfigurować agregowane polityki • Musi być w stanie ograniczyć sesje na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu aplikacji (mysql, ms-

	sql, sqlnet, pobieranie P2P)
Wydzielenie stref bezpieczeństwa	<ul style="list-style-type: none"> • Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN • Musi mieć możliwość konfiguracji oddzielnych wirtualnych routerów • Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników
Ochrona antywirusowa	<ul style="list-style-type: none"> • Silnik antywirusowy musi być oparty na przepływie tzw. flow-based • Musi umożliwiać skanowanie protokołów HTTP, SMTP, POP3, IMAP, FTP / SFTP, SMB • Możliwość ręcznego dodawania lub usuwania sygnatury MD5 do bazy danych AV • Musi obsługiwać wykrywanie wirusów w plikach skompresowanych, takich jak RAR, ZIP, GZIP, BZIP2, TAR, a także wykrywać wielowarstwowe pliki skompresowane dla nie mniej niż 5 warstw dekompresji
Równoważenie obciążenia	<ul style="list-style-type: none"> • Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łączy dla określonej nazwy domeny oraz monitorowanie stanu łączy poprzez aktywną metodę wykrywania • Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted leastconnection i weighted round-robin • Kontrola stanu serwera, monitorowanie sesji i ochrona sesji
Ochrona IPS	<ul style="list-style-type: none"> • Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury. • Baza danych wykrytych ataków musi zawierać co najmniej 16000 sygnatur. Dodatkowo musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i Ddos. • Funkcjonalność zapobiegania atakom SQL injection, XSS injection • Możliwość budowania własnych niestandardowych reguł IPS
Obrona przed atakiem	<ul style="list-style-type: none"> • Ochrona przed nieprawidłowym działaniem protokołu • Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment itp. • Wsparcie IPv4 jak i IPv6 dla ochrony przed DNS query flood i DNS reply

	<p>flood</p> <ul style="list-style-type: none"> • Biała lista docelowych adresów IP
Ochrona antyspam	<ul style="list-style-type: none"> • Rozwiązanie musi zapewniać ochronę przed spamem w czasie rzeczywistym • Wspieranymi protokołami są minimum SMTP, SMTPS, POP3, POP3S • Skanowanie antyspamowe musi odbywać się w ruchu w obu kierunkach • Musi istnieć możliwość dodawania wyjątków w zakresie skanowania antyspamowego, minimum białych list domen
Kontrola aplikacji	<ul style="list-style-type: none"> • Kontrola aplikacji musi być w stanie kontrolować ruch w oparciu o głęboką analizę pakietów, a nie tylko w oparciu o wartości portów TCP/UDP • Baza danych aplikacji zawierająca ponad 6000 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka
Filtr adresów URL	<ul style="list-style-type: none"> • Baza filtrów URL pogrupowana w co najmniej 64 kategorie tematyczne. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków. • Możliwość zdefiniowania własnej bazy kategorii www. • Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL. • Kategorie takie jak hazard, malware, spam, botnety • Obsługa Safe Search • Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne • Dostosowanie strony ostrzeżenia
Ochrona danych	<ul style="list-style-type: none"> • Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy • Identyfikacja protokołu pliku, w tym HTTP, FTP, SMTP, POP3, IMAP • Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS • Filtrowanie plików przesyłanych przez SMB

Reputacja IP	<ul style="list-style-type: none"> • Identyfikacja i filtrowanie ruchu z ryzykownych adresów IP, takich jak hosty botnet, spamerzy, węzły Tor, podejrzane hosty i adresy IP atakujące metodą brute force • Logowanie, odrzucanie pakietów lub blokowanie dla różnych rodzajów ryzykownego ruchu IP
Zapobieganie botnetom	<ul style="list-style-type: none"> • Wykrywanie intranetowych hostów botnetu, monitorując połączenia C&C i blokowanie dalszych zaawansowanych zagrożeń takich jak botnet i oprogramowanie ransomware • Wsparcie DNS sinkhole • Wsparcie wykrywania tunelowania DNS • Wyrwanie i blokowanie DGA
Cloud Sandbox	<ul style="list-style-type: none"> • Złośliwe oprogramowanie emulowane w wirtualnym środowisku oparte na architekturze chmury w celu wykrywania nieznanych zagrożeń • Obsługa protokołów, takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB • Obsługa typów plików : PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów • Obsługa blokowania wyników wykrywania w celu szybkiego blokowania nieznanych zagrożeń
Uwierzytelnianie użytkownika	<ul style="list-style-type: none"> • System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika z nie mniej niż: <ul style="list-style-type: none"> - Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu - Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP - Hasła dynamiczne (RADIUS) oparte o zewnętrzne bazy danych - Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA • Musi umożliwiać budowę architektury uwierzytelniania pojedynczego logowania w środowisku Active Directory • Wsparcie usług terminalowych • Uwierzytelnianie użytkownika przez Web przed dostępem do internetu • Obsługa dwuskładnikowego uwierzytelniania, SMSy, certyfikaty i tokeny

	<ul style="list-style-type: none"> System musi posiadać moduł ZTNA, w celu uwierzytelniania użytkowników bazując na regułach i zasadach zdefiniowanych przed administratora
Raportowanie i przeglądanie logów	<ul style="list-style-type: none"> Wbudowany w system bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż: <ul style="list-style-type: none"> - Posiadanie predefiniowanych raportów dla ruchu internetowego, modułu IPS, skanera antywirusowego i antyspamowego - Generowanie co najmniej 10 rodzajów raportów
Certyfikaty	<p>Rozwiązanie musi posiadać</p> <ul style="list-style-type: none"> certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSA Labs dla funkcji Firewall być pozycjonowanym w raporcie Gartnera przez ostatnie 8 lat
Zarządzanie	<ul style="list-style-type: none"> Elementy systemu muszą mieć możliwość zarządzania lokalnie (HTTPS, SSH) oraz współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja między systemami bezpieczeństwa a platformami zarządzania musi odbywać się za pomocą protokołów szyfrowanych. Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI lub po pomocą linii komend (COM Port, SSH, Telnet) bez instalowania oddzielnego oprogramowania, takiego jak dedykowana aplikacja
Gwarancja i dostawa	<ul style="list-style-type: none"> 36-miesięczną gwarancję producenta na dostarczone elementy systemu Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 36 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C) Wsparcie techniczne dystrybutora rozwiązań w języku polskim Oferta musi być złożona przez autoryzowanego partnera

INFORMACJA KONCOWA

Wszystkie ewentualne nazwy własne i marki handlowe urządzeń i elementów zawarte w opisie przedmiotu zamówienia, zostały użyte w celu sprecyzowania oczekiwań jakościowych i technologicznych Zamawiającego.

Zamieszczone w specyfikacji nazwy technologicznych lub producentów kluczowych komponentów użyto jedynie w celu przykładowym.

Zamawiający informuje, że dopuszcza składanie ofert, w których poszczególne urządzenia bądź materiały wymienione w opisie przedmiotu zamówienia mogą być zastąpione urządzeniami bądź materiałami/elementami równoważnymi. Poprzez pojęcie materiałów/elementów i urządzeń równoważnych należy rozumieć materiały zapewniające uzyskanie parametrów technicznych nie gorszych od założonych w opisie przedmiotu zamówienia. Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia w stosunku do przewidzianych w niniejszym zaproszeniu, ani do zmiany ceny.

INFORMACJA KONCOWA

Wszystkie ewentualne nazwy własne i marki handlowe urządzeń i elementów zawarte w opisie przedmiotu zamówienia, zostały użyte w celu sprecyzowania oczekiwań jakościowych i technologicznych Zamawiającego.

Zamieszczone w specyfikacji nazwy technologicznych lub producentów kluczowych komponentów użyto jedynie w celu przykładowym.

Zamawiający informuje, że dopuszcza składanie ofert, w których poszczególne urządzenia bądź materiały wymienione w opisie przedmiotu zamówienia mogą być zastąpione urządzeniami bądź materiałami/elementami równoważnymi. Poprzez pojęcie materiałów/elementów i urządzeń równoważnych należy rozumieć materiały zapewniające uzyskanie parametrów technicznych nie gorszych od założonych w opisie przedmiotu zamówienia. Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia w stosunku do przewidzianych w niniejszym zaproszeniu, ani do zmiany ceny.