DAI 0104-16/20
Załącznik nr 2

.....
pieczęć Wykonawcy

.....
Miejscowość, data

Nazwa Wykonawcy.....

.....

Adres Wykonawcy.....

.....

Tel/fax .....

Adres e-mail.....

NIP.....

REGON.....

OFERTA
NA DOSTAWĘ DO SIEDZIBY WOJEWÓDZKIEGO FUNDUSZU OCHRONY ŚRODOWISKA I GOSPODARKI WODNEJ W KIELCACH

UTM – urządzenie zabezpieczające sieć

CZĘŚĆ III

Nawiązując do zaproszenia WFOŚiGW w Kielcach znak **DAI 0104-16/20** do złożenia oferty na dostawę do siedziby Wojewódzkiego Funduszu Ochrony Środowiska i Gospodarki Wodnej w Kielcach: **UTM -urządzenie zabezpieczające sieć.**

Składamy oraz oferujemy wykonanie powyższego zamówienia, zgodnie z wymogami określonymi w opisie przedmiotu zamówienia (zał. nr 1 do zaproszenia):

1. Łączna cena oferty:

netto - .....zł
(słownie.....
..... złotych.)

brutto - .....zł
(słownie.....
..... złotych)

W tym:

1) **UTM- urządzenie zabezpieczające sieć**

Producent:.....

Nazwa urządzenia i nr produktu (product number):

.....

Cena urządzenia netto (szt):.....

Cena urządzenia brutto (szt): .....

2) **Licencje/ support/ gwarancja/ inne**
Należy podać product number, cena – (jeżeli jest taka możliwość)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. Określamy spełnienie wszystkich określonych w **opisie przedmiotu zamówienia** minimalnych wymagań.

Lp.	Opis Elementów	Wymagania minimalne	Potwierdzenie oferowanych min. parametrów: **(TAK/NIE)**
1	System musi wspierać IPv4 oraz IPv6 w zakresie:	• Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego	
2	Redundancja, monitoring i wykrywanie awarii	• 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.	

		• Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. • Monitoring stanu realizowanych połączeń VPN. • System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych	
3	Interfejsy, Dysk, Zasilanie:	• System realizujący funkcję Firewall musi dysponować minimum: o 10 portami Gigabit Ethernet RJ-45. • 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. • **Wbudowany dysk twardy m.in. do przechowywania logów**	
4	Parametry wydajnościowe:	• W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. • Przepustowość Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. • Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. • Wydajność szyfrowania IPSec VPN nie mniej niż 6.2 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 1.4 Gbps. • Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. • **Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu https minimum 620 Mbps.**	
5	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: • Kontrola dostępu - zapora ogniowa klasy Stateful 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. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. • Zarządzanie pasmem (QoS, Traffic shaping). • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). • Analiza ruchu szyfrowanego protokołem SSL.	

6	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: o Translację jeden do jeden oraz jeden do wielu. o Dedykowany ALG (Application Level Gateway) dla protokołu SIP. • W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.	
7	Połączenia VPN	• System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: o Wsparcie dla IKE v1 oraz v2. o Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). o Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. o Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. o Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. o Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. o Mechanizm „Split tunneling" dla połączeń Client-to-Site. • System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: o 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. o Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. o **Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.**	
8	Routing i obsługa łączy WAN	• W zakresie routingu rozwiązanie powinno zapewniać obsługę: o Routingu statycznego. o Policy Based Routingu. o Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.	
9	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.	
10	Ochrona przed malware	• 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. • System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	
11	Ochrona przed atakami	• 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 5000 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.	
12	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 2000 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.	
13	Kontrola WWW	• Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. • 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. • Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.	

		• Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. • Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google czy Yahoo. • Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. • W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.	
14	Uwierzytelnianie użytkowników w ramach sesji	• System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: o Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. o Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. o Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. • Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. • Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.	
15	Zarządzanie	• 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 dwu-składnikowego dla dostępu 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. • Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	
16	Logowanie	• 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.	
17	Zabezpieczenie końcówek PC (Endpoint Protection)	• Dedykowane oprogramowanie producenta sprzętu, instalowane na urządzeniach końcowych np. komputerach stacjonarnych/laptopach z systemem operacyjnym Win 10 lub 8.1. tzn. „agent", który posiada min.: o Ochrona przed AntiMalware o Web Filtering o Kontrola urządzeń USB o Inwentaryzacja oprogramowania o Połączenia zdalne ▪ IPSec VPN ▪ SSL VPN o Centralne zarządzanie o Centralne miejsce na logi i raporty Licencja dla min. 60 końcówek (komputerów, laptopów) Na okres **12 miesięcy**	
18	Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.	
19	Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: • Firewall, • Kontrola Aplikacji, • IPS, • Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), • Analiza typu Sandbox, • Antyspam, • Web Filtering, bazy reputacyjne adresów IP/domen • Urządzenie w ramach dostarczonych licencji musi mieć możliwość bezpiecznego udostępnienia aplikacji webowych (stron internetowych) w sieci WAN – zabezpieczenie typu WAF. • Centralne zarządzanie oraz analiza logami bezpośrednio na urządzeniu i w chmurze o czas przechowywania logów co najmniej 12 miesięcy licencje na okres **36 miesięcy**.	
20	Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres **36 miesięcy**, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp	

		do aktualizacji oprogramowania oraz wsparcie techniczne w trybie **24x7.** W przypadku uszkodzenia sprzętu wymiana na nowe – maksymalny czas dostawy nowego urządzenia do siedziby ZAMAWIJACEGO nie może być dłuższy niż **4 godz.** Ponadto WYKONAWCA zapewni: • Wsparcie techniczne certyfikowanych inżynierów, • Pomoc przy rejestracji urządzenia, • Doradztwo w zakresie konfiguracji, • Zakładanie zgłoszeń serwisowych u Producenta rozwiązania, • Pomoc w procesie realizacji naprawy i wymiany urządzeń w ramach gwarancji urządzenia, • **Wdrożenie urządzenia zgodnie z instrukcjami i pod potrzeby ZAMAWIAJĄCEGO (pełna konfiguracja)** • w przypadku konieczności zmiany konfiguracji urządzenia – pomoc w dostosowaniu do aktualnych potrzeb (min. 15 zgłoszeń na rok).	
21	Szkolenie	**WYKONAWCA zobowiązany jest przeszkolić Pracowników działu IT ZAMAWIAJĄCEGO z rozwiązania, które dostarczy.** Szkolenie ma zostać przygotowane i przeprowadzone w pełni profesjonalnie, WYKONAWCA, w ramach składanej oferty dostarczy agendę szkolenia wraz z potrzebnym czasem jaki będzie potrzebny na przepracowanie danych zagadnień. Przed szkoleniem ZAMAWIAJĄCY zobowiązany jest dostarczyć materiały szkoleniowe, zgodne z agendą szkolenia. Na szkoleniu powinna być przedstawiona praktyczna wiedza połączona z przykładami oraz ćwiczeniami dla kursantów w postaci laboratoriów. Szkolenie ma objąć zagadnienia **podstawowe jak również średnio zaawansowane dostarczonego rozwiązania** m.in. takie jak (*ZAMAWIAJĄCY nie określa tutaj wszystkich zagadnień, które WYKONAWCA przeprowadzi w ramach swojego autorskiego szkolenia, a jedynie te, które muszą być*) kursant po szkoleniu będzie miał wiedzę z zakresu: • podstawowych zagadnień związanych z szyfrowaniem oraz operacje oparte na certyfikatach. • potrafił identyfikować ruch zabezpieczony protokołem SSL/TLS, i przeciwdziałać ewentualnemu obchodzeniu reguł bezpieczeństwa poprzez szyfrowanie komunikacji. • stosować techniki kontroli aplikacji do monitorowania i kontrolowania komunikacji sieciowej, które mogą wykorzystywać standardowe lub niestandardowe protokoły i porty. • chronić się przed wyciekami danych, identyfikując pliki z danymi wrażliwymi i blokując możliwość ich przesłania poza chronione sieci. • zbierać i prawidłowo interpretować logi. • umiejętnie walcz z podstawowymi technikami hackerskimi i zabezpieczyć się przed atakami • Analizować ruch sieciowy na urządzeniu, wykrywać i podejmować decyzję nt. utworzenia odpowiednich ról na firewall w celu zablokowania lub przepuszczenia danego ruchu.	

		Szkolenie nie może być krótsze jak **20 godzin**, (**max. Ilość godzin jaką ZAMAWIAJĄCY** jest w stanie **dziennie poświęcić na szkolenie to 4 h.** Szkolenie zorganizowane w formie **online**, w szkoleniu będzie brało udział dwóch Pracowników działu IT ZAMAWIAJĄCEGO. Termin szkolenia będzie ustalony po dostarczeniu rozwiązania i jego wdrożeniu. Szkolenie musi zostać przeprowadzone przez **certyfikowanego inżyniera, który posiada najwyższy stopień certyfikacji danego rozwiązania oraz ma doświadczenie w prowadzeniu tego typu szkoleń.**	
22	Wdrożenie	WYKONAWCA po dostarczeniu rozwiązania, w ramach oferty wdroży ww. system. Wdrożenie obejmuje min.: • konfiguracja metod logowania, • konfiguracja Interface, • konfiguracja podsieci, • Konfiguracja DMZ, • konfiguracja WAN, SD-WAN, routing • konfiguracja polityk bezpieczeństwa (zgodnych z zapotrzebowaniem) • konfiguracja profili bezpieczeństwa (zgodnych z zapotrzebowaniem) • stworzenie obiektów zgodnych z topologią sieci • konfiguracja przekierowań • konfiguracja VPN Client-2-Site • konfiguracja VPN Site-2-Site • konfiguracja ustawień systemowych urządzenia • testowanie wdrożonej konfiguracji • utworzenie kopi zapasowej po zakończonej pracy • inne konfiguracje, które podczas wdrożenia zleci ZAMAWIAJĄCY	

3. **Na potwierdzenie, iż oferowany przedmiot zamówienia jest zgodny z wymogami Zamawiającego, dołączamy do oferty specyfikację techniczną (karty produktowe) oferowanego sprzętu, a także dokumenty określone w dodatkowych wymaganiach opisu przedmiotu zamówienia (załącznik nr 1 do zaproszenia).**

3. **Oświadczamy że udzielamy Zamawiającemu gwarancji na sprzęt zgodnie z minimalnymi wymaganiami określonymi w opisie przedmiotu zamówienia**

4. **Akceptujemy określone w załączniku nr 3 do zaproszenia** zamieszczonego na stronie internetowej WFOŚiGW w Kielcach w ramach zamówienia znak **DAI 0104-16/20 warunki umowy** i zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na określonych w ofercie warunkach w miejscu i terminie wyznaczonym przez Zamawiającego.

5. Oferta składa się z.....kolejno ponumerowanych stron, od.....str. do..... str.

6. **Określamy termin związania ofertą ..... dni kalendarzowych.**

7. Zobowiązujemy się do realizacji zamówienia, **tj. dostawy do siedziby Zamawiającego w ciągu ..... dni kalendarzowych** od daty podpisania umowy do siedziby Zamawiającego na własny koszt i własnym transportem.

8. Do kontaktu z Zamawiającym upoważnione są następujące osoby:
   a) .....tel.....,e-mail .....
   b) .....tel.....,e-mail.....
   c) .....tel.....,e-mail.....
   d) .....tel.....,e-mail.....

10. Do podpisania protokołu odbioru upoważnione są następujące osoby:
    a) .....tel.....,e-mail .....
    b) .....tel.....,e-mail.....
    c) .....tel.....,e-mail.....

11. Do podpisania umowy upoważnione są następujące osoby:
    a) .....tel.....,e-mail .....
    b) .....tel.....,e-mail.....
    c) .....tel.....,e-mail.....

12. Zobowiązujemy się dostarczyć dokument potwierdzający reprezentację najpóźniej w dniu podpisania umowy.

.....

podpis osób uprawnionych
do składania oświadczeń woli
w imieniu Wykonawcy