



## **DOTACJE NA INNOWACJE**

Baranowo, dnia 24 listopada 2011 r.

**KAEM Spółka z ograniczoną odpowiedzialnością**  
**Spółka komandytowo - akcyjna**  
Baranowo, ul. Rzemieślnicza 14  
62-081 Przeźmierowo

Tel.: (61) 816 30 00  
Fax.: (61) 816 30 50  
mail: biuro@kaem.pl

### **ZAPYTANIE OFERTOWE**

Zwracam się z prośbą o przedstawienie oferty na dostawę i instalację następujących urządzeń:

**1. Dwa redundantne firewalle sprzętowe.**

**Szczegóły specyfikacji znajdują się w Załączniku nr 1 do Zapytania**

Każde z urządzeń powinno mieć 3-letnią gwarancję. Po dostarczeniu należy zainstalować w miejscu wskazanym przez zamawiającego.

Złożona oferta powinna zawierać, co najmniej:

- nazwę i adres oferenta,
- opis nawiązujący do parametrów wyszczególnionych w zapytaniu ofertowym,
- wartość oferty (netto oraz brutto),
- termin ważności oferty,
- termin realizacji zamówienia

Wskazane jest, by oferta zawierała również inne, dodatkowe informacje, np. dodatkowe funkcje dostawy, warunki płatności i dostawy, możliwe do uzyskania upusty, maksymalny czas realizacji, itd.

Oferta powinna być sporządzona na papierze firmowym oferenta lub opatrzona pieczętką firmową, posiadać datę sporządzenia oraz powinna być podpisana przez oferenta.

Oferta powinna być przesłana za pośrednictwem poczty polskiej, kuriera bądź odebrana osobiście przez kupującego.

Termin składania ofert upływa w dniu **6 grudnia 2011 r.**

Z poważaniem

## DOTACJE NA INNOWACJE

### ZAŁĄCZNIK NR 1

#### SPECYFIKACJA TECHNICZNA

##### 1. Redundantny Firewall Sprzętowy

Parametr	Charakterystyka (wymagania)
System zabezpieczeń sprzętowo-programowych	System musi obsługiwać Nielimitowaną ilość użytkowników w ramach realizowanych systemów zabezpieczeń i umożliwiać realizację następujących funkcji: <ul style="list-style-type: none"> <li>• Firewall klasy Stateful Inaspection</li> <li>• Antywirus</li> <li>• System detekcji i prewencji włamań (IPS)</li> <li>• VPN zgodny z IPSec, PPTP, L2TP i SSL-VPN</li> <li>• Antyspam</li> <li>• Filtracja stron WWW</li> <li>• Kontrola aplikacji na bazie sygnatur</li> <li>• Kontrola pasma (Traffic Management)</li> <li>• Zintegrowane zarządzanie sieciami WiFi w oparciu o dedykowane accesspointy</li> <li>• Ochrona aplikacji webowych za pomocą Web Application Firewall U</li> </ul>
Typ urządzenia	Urządzenie typu UTM, zapewniające funkcjonalności: Firewall, Gateway VPN, ochrona przed wirusami, spyware, system IPS, filtrowanie treści, działające w klastrze wysokiej dostępności Active-Passive
Specyfikacja fizyczna urządzenia	Dedykowane rozwiązanie sprzętowe Obudowa 1U przeznaczona do montażu w szafie RACK Pamięć RAM: minimum 1 GB Storage: rozwiązanie wyposażone w dysk twardy, przestrzeń dyskowa minimum 70 GB Ilość interfejsów: <ul style="list-style-type: none"> <li>• nie mniej niż 8 konfigurowalnych interfejsów Gigabit Ethernet</li> <li>• nie mniej niż 2 interfejsy USB</li> </ul>
Wydajność urządzeń pracujących w klastrze HA Active-Passive	Obsługa Nielimitowanej ilości hostów w sieci chronionej Przepustowość zapory sieciowej nie mniejsza niż 2,8 Gbps. Przepustowość modułu VPN (AES) nie mniejsza

## DOTACJE NA INNOWACJE

	<p>niż 450 Mbps. Przepustowość modułu IPS nie mniejsza niż 700 Mbps Ilość jednocześnie obsługiwanych sesji: nie mniej niż 280 000</p>
<p><b>Funkcjonalności urządzeń w zakresie konfiguracji połączeń zdalnych VPN</b></p>	<ul style="list-style-type: none"> <li>• Minimalna ilość jednocześnie obsługiwanych połączeń SSL VPN: 80.</li> <li>• Minimalna ilość klientów VPN SSL w cenie urządzenia: 200.</li> <li>• Wspierane mechanizmy uwierzytelniania i szyfrowania: 3DES, AES (128, 192, 256-bit), MD5, SHA-1.</li> <li>• Wspierane mechanizmy wymiany kluczy: Manual Key, PKI (X.509).</li> <li>• Obsługa funkcjonalności: L2TP IPSec oraz DHCP over VPN.</li> </ul>
<p><b>Sieciowe funkcjonalności urządzeń</b></p>	<p>Możliwość pracy jako Router lub Bridge</p> <ul style="list-style-type: none"> <li>• Obsługa nie mniej niż 512 sieci VLAN działających zgodnie ze standardem 802.1Q.</li> <li>• Wbudowany serwer DHCP umożliwiający przydzielanie adresów statycznie, dynamicznie, przekierowanie zgłoszeń do zewnętrznego serwera DHCP.</li> <li>• Wsparcie mechanizmów NAT: 1:1, 1:many, many:1, many:many.</li> <li>• Możliwość kreowania reguł routingu statycznego</li> <li>• Wsparcie dynamicznych protokołów routingu: OSPF i wsparcie dla routowania transmisji multicast.</li> <li>• Wsparcie funkcjonalności QoS: DSCP-bits, możliwość ustawienia przynajmniej 100 reguł określających maksymalne i gwarantowane pasmo.</li> <li>• Możliwość skonfigurowania przynajmniej 3 łączy WAN, działających w trybie redundantnym lub umożliwiających</li> </ul>

## DOTACJE NA INNOWACJE

	<p>równoważenie obciążeń dla ruchu wychodzącego.</p> <ul style="list-style-type: none"> <li>• Możliwość konfiguracji reguł równoważenia obciążeń dla ruchu przychodzącego do hostów znajdujących się w sieci chronionej.</li> <li>• Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), pełna kompatybilność z większością urządzeń i serwerów VoIP.</li> </ul>
<b>Funkcjonalności urządzeń w zakresie uwierzytelniania użytkowników</b>	<p>Lokalna baza użytkowników umożliwiająca wykreowanie nie mniej niż 200 kont.</p> <p>Uwierzytelnianie użytkowników w oparciu o: Active Directory, LDAP, lokalna baza użytkowników – system powinien oferować mechanizm Single Sign-On.</p> <p>Wymagane jest, aby uwierzytelnianie użytkowników odbywało się z lokalnej bazy, skonfigurowanej na urządzeniu lub z zewnętrznego serwera Active Directory.</p>
<b>Funkcjonalności urządzeń w zakresie zarządzania i wysokiej dostępności</b>	<ul style="list-style-type: none"> <li>• Możliwość zarządzania urządzeniem poprzez wbudowany interfejs webowy dostępny przez: HTTPS</li> <li>• Praca w klastrze wysokiej dostępności w trybie Active – Passive</li> </ul>
<b>Funkcjonalności urządzeń w zakresie mechanizmów filtrowania Deep Packet Inspection i Statefull Packet Inspection</b>	<p>Możliwość kreowania reguł Firewall dla ruchu przychodzącego/wychodzącego z/do poszczególnych podsieci, w określonych przedziałach czasu, z uwzględnieniem użytkowników, dla których reguła ma być aktywna</p> <ul style="list-style-type: none"> <li>• Możliwość włączania i wyłączania reguł Firewall i NAT bez konieczności ich usuwania</li> </ul> <p><b>Wymagane jest, aby na urządzeniach uruchomione były następujące usługi w subskrypcji na 3 lata:</b></p> <ul style="list-style-type: none"> <li>• zintegrowana ochrona antywirusowa, składająca się z 2 niezależnych skanerów, zapewniająca skanowanie ruchu na protokołach HTTP, HTTPS i FTP. Filtr antywirusowy powinien zapewniać skanowanie plików</li> </ul>



## DOTACJE NA INNOWACJE

	<p>skompresowanych.</p> <ul style="list-style-type: none"><li>• Wymagane jest, aby możliwe było włączenie lub wyłączenie usługi antywirus dla poszczególnych zdefiniowanych maszyn/podsieci</li><li>• sonda IPS (detekcja i blokowanie wtargnięć do sieci) zapewniająca skanowanie ruchu w oparciu o sygnatury dostarczone przez producenta. System musi rozpoznawać i blokować ataki dla dedykowanych usług takich jak: serwery pocztowe, serwery webowe, ataki na aplikacje np. MS Office i inne.</li><li>• Rozwiązanie powinny umożliwiać wykrywanie i blokowanie zdarzeń takich jak: korzystanie z programów do wymiany plików P2P (np. BitTorrent, eMule, etc.), korzystanie z komunikatorów internetowych (np. Yahoo Messenger, Google Talk, Skype, etc).</li><li>• Wymagana jest możliwość włączenia lub wyłączenia usługi IPS dla poszczególnych maszyn/podsieci</li><li>• sieciowa ochrona antyspyware, zapewniająca skanowanie ruchu HTTP, HTTPS i FTP.</li><li>• usługa filtrowania treści stron WWW, zapewniająca blokowanie apletów Java, aplikacji Active-X, definiowanie białych i czarnych list stron www, a także blokowanie stron na podstawie ich reputacji</li><li>• Dodatkowo wymagane jest tworzenie reguł filtrowania treści dla poszczególnych grup użytkowników umożliwiających filtrowanie treści w oparciu o bazę stron zestawionych, w co najmniej 60 kategoriach. Wymagane jest, aby mechanizm filtrowania treści uwzględniał także filtrowanie stron HTTPS oraz możliwość włączenia lub wyłączenia mechanizmu filtrowania treści dla poszczególnych maszyn bądź podsieci.</li><li>• Wymagana jest możliwość skonfigurowania połączeń VPN (SSL lub IPSec) client-site, aby cały ruch z połączonych do urządzeń klientów przesyłany był poprzez urządzenia i możliwe było jego skanowanie przez mechanizmy</li></ul>
--	--

## DOTACJE NA INNOWACJE

	<p>bezpieczeństwa.</p> <ul style="list-style-type: none"> <li>• Wymaga się, aby mechanizmy antywirus, antyspyware nie posiadały ograniczeń co do wielkości skanowanych plików</li> <li>• System ochrony ruchu pocztowego musi oferować wielowarstwowe mechanizmy antyspamowe zawierające zróżnicowane pod względem złożoności filtry w tym: sprawdzanie SMTP HELLO, revDNS, SPF, Greylisting, filtr reputacji nadawcy, BATV</li> <li>• Rozwiązanie musi umożliwiać budowanie centralnie zarządzanych sieci bezprzewodowych w standardach b/g/n w oparciu o dedykowane access pointy tego samego producenta, co oferowane rozwiązanie</li> <li>• System musi być wyposażony w mechanizmy ochrony aplikacji webowych przed atakami typu XSS oraz SQL Injection z możliwością podpisywania cyfrowego plików cookie.</li> </ul>
<p><b>Rozwiązanie do raportowania</b></p>	<p>Wymagane jest, aby dostarczone rozwiązanie zapewniało monitorowanie, rejestrację i graficzną prezentację danych dotyczących zdarzeń obsługiwanych przez mechanizmy bezpieczeństwa. Wymagane jest, aby rozwiązanie oferowało zestaw zdefiniowanych typów raportów. Niezbędne dane to średnia zajętość łącza w podziale na dni i godziny, wykorzystanie pasma przez każdego z użytkowników z podziałem na protokoły, informacje dotyczące przeglądanych witryn przez każdego z użytkowników sieci informatycznej, informacje dotyczące użytkowników łamiących zasady przeglądania witryn, informacje dotyczącą ataków, detekcji intruzów, zagrożeń antywirusowych. Wymagane jest aby rozwiązanie raportujące było tego samego producenta co oferowany system bezpieczeństwa. Dopuszcza się rozwiązania zintegrowane jak i narzędzia zewnętrzne.</p>
<p><b>Gwarancja, wsparcie techniczne i aktualizacja systemu</b></p>	<p>Wymagane jest, aby dostarczane urządzenia objęte były okresem gwarancji przez okres 3 lat, z możliwością przedłużenia na dłuższy okres czasu. Wymagane jest, aby w ramach gwarancji uszkodzone urządzenie zostało wymienione w</p>



## DOTACJE NA INNOWACJE

	<p>48 godzin. Wymagane jest, aby urządzenia objęte było wsparciem technicznym 24x7 (wraz z możliwością dokonywania aktualizacji oprogramowania up-to-date w ramach posiadanego wsparcia technicznego), realizowanym przez producenta przez okres 3 lat z możliwością przedłużenia na dłuższy okres czasu.</p>
--	---