Ełckie Centrum Kultury
19-300 Ełk, ul. Wojska Polskiego 47
tel./fax 87 621 80 00, tel. 87 621 52 50
REGON 000687400 NIP 848-11-35-538

.....
(pieczęć Zamawiającego)

Znak sprawy: DAK.713.1.2019

Ełk, 16 listopada 2021 r.
(miejscowość i data)

ZAPYTANIE CENOWE

Ełckie Centrum Kultury, ul. Wojska Polskiego 47, 19-300 Ełk, zaprasza do złożenia oferty na **dostawę serwera NAS wraz z systemem bezpieczeństwa w ramach projektu pt. „Razem – współpraca kulturalna na polsko-rosyjskim pograniczu"**, dofinansowanego ze środków Programu Współpracy Transgranicznej Polska-Rosja 2014-2020.

I. Opis przedmiotu zamówienia:

Serwer NAS wraz z systemem bezpieczeństwa

Minimalne wymagania:
Dostarczony serwer wraz z systemem bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. 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 dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Serwer sieciowy NAS z 5 kieszeniami. Wyposażony jest w czterordzeniowy procesor 2.0GH, 8 GB pamięci RAM DDR4. Przepustowość odczytu i zapisu 450 MB/s. Obsługa Windows AD, LDAP oraz Domain Trust.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu,

Firewalla, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie: Firewall, Ochrony w warstwie aplikacji, Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii:

1. 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.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum 5 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewalla obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.

Funkcje bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.

6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

Polityki, Firewall:

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

   Translację jeden do jeden oraz jeden do wielu.

   Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. 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.
5. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

W zakresie routingu rozwiązanie powinno zapewniać obsługę:

Routingu statycznego.

Policy Based Routingu.

Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

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.

Ochrona przed malware:

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. 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.

4. Filtr WWW musi dostarczać kategorii stron zabronionych prawem.
5. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
6. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak Google, oraz Yahoo.
7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Zarządzanie:

1. 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.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Serwer NAS musi mieć obsadzone wszystkie 5 szt. dyskami twardymi o pojemności 4 TB każdy przeznaczonymi do zastosowań serwerowych NAS.

Termin realizacji zamówienia: 15 grudnia 2021 r.
Okres gwarancji: 24 miesiące od dnia odbioru.
Miejsce dostawy: Ełckie Centrum Kultury – Szkoła Artystyczna, ul. Armii Krajowej 21, 19-300 Ełk.

II. Warunki, jakie musi spełniać Wykonawca: ---

III. Warunki płatności:

Płatność dokonana będzie po potwierdzeniu protokołem zdawczo-odbiorczym właściwej realizacji

zamówienia, w terminie 30 dni od dnia dostarczenia prawidłowo wystawionej faktury Zamawiającemu, przelewem na rachunek bankowy wskazany w fakturze.

IV. Kryteria oceny ofert: najniższa cena brutto - 100%

Cena zaproponowana i ustalona w ofercie jest ryczałtową ceną brutto (zawierającą obowiązujący podatek VAT) i musi zawierać wszelkie koszty niezbędne do zrealizowania zamówienia. Cena ofertowa podana przez Wykonawcę obowiązuje przez okres ważności umowy i nie podlega waloryzacji. Rozliczenia pomiędzy Zamawiającym a Wykonawcą prowadzone będą wyłącznie w złotych polskich.

V. Sposób przygotowania oferty:

1. Ofertę należy sporządzić w formie pisemnej, w języku polskim, zgodnie ze wzorem oferty (załącznik nr 1).
2. Wypełniona i podpisana odręcznie przez osobę upoważnioną oferta powinna zostać zeskanowana i przesłana drogą elektroniczną na adres e-mail: monika.muzylo@eck.elk.pl.
3. **Termin składania ofert** – 24 listopada 2021 r. Zamawiający nie będzie rozpatrywał ofert, które nie wpłyną w terminie.

VI. Informacje dodatkowe

1. Osoba upoważniona do kontaktu z Wykonawcami: Artur Dobkowski, e-mail: artur.dobkowski@eck.elk.pl, tel. 601 693 826.
2. Zamawiający zastrzega sobie prawo do unieważnienia zapytania ofertowego na każdym jego etapie bez podania przyczyny, a także do pozostawienia zapytania ofertowego bez wyboru oferty, zwłaszcza w sytuacji, kiedy cena najkorzystniejszej oferty przewyższać będzie kwotę, którą Zamawiający może przeznaczyć na sfinansowanie zamówienia.

Załączniki:

Załącznik nr 1 – Wzór oferty
Załącznik nr 2 – Klauzula informacyjna z art. 13 RODO

DYREKTOR
EŁCKIEGO CENTRUM KULTURY
16.11.2021 Aneta Wenta

Data i podpis Zamawiającego

Sporządziła Monika Mużyło, Specjalista ds. pozyskiwania funduszy unijnych, monika.muzylo@eck.elk.pl, 87 621 80 05.