# **Zaproszenie do szacowania ceny urządzeń sieciowych.**

1. Informacje ogólne

Fundacja Platforma Przemysłu Przyszłości (FPPP) z siedzibą w Radomiu, ul. Tarnobrzeska 9, zwraca się z uprzejmą prośbą o wstępne oszacowanie cen.

Niniejsze ogłoszenie nie stanowi oferty w rozumieniu przepisów ustawy z dnia 23 kwietnia 1964 r. Kodeks Cywilny (Dz. U. z 2014 r. poz. 121, z późn. zm.), jak również nie jest zaproszeniem do składania ofert w rozumieniu ustawy - Prawo zamówień publicznych.

1. Cel i przedmiot zapytania:

Celem zapytania jest rozpoznanie dostępności aktywnych urządzeń sieciowych do budowy sieci LAN i WAN oraz szacowanie ich ceny wraz z wykonaniem usług, o których poniżej. Uzyskane odpowiedzi są niezbędne do ustalenia właściwego trybu postępowania o zamówienie publiczne.

W ramach realizacji zamówienie, konieczne będzie:

* Sprzedaż i dostawa urządzeń do biura w Radomiu.
* Instalacja, konfiguracja i uruchomienie.
* Udzielenie gwarancji na 24 miesiące od daty uruchomienia.
* Zapewnienie dostępu do najnowszych wersji oprogramowania wbudowanego drukarki do nowych wersji w trakcie gwarancji
* Naprawa w rygorze czasowym NBD.
* Wykonanie jednorazowego szkolenia pracowników FPPP w zakresie administracji urządzeniem, po jego dostawie i instalacji.
1. Specyfikacja techniczna

Poniższa tabela przedstawia wymagania techniczne.

**Wymagania dotyczące urządzeń dostępowych do sieci WIFi.**

|  |  |
| --- | --- |
| Ilość urządzeń | 1 |
| Widoczność | Wszystkie urządzenia dostępowe WiFi pod wspólnym SSID (routing) i hasłem |
| Goście | Konfiguracja wydzielonej sieci dla gości |
| Generowanie i dystrybucja czasowo ograniczonych (do maksymalnie 12 godzin) indywidualnych haseł dostępowych do sieci dla gości |
| Generowanie i dystrybucja czasowo ograniczonego (do maksymalnie 12 godzin) jednego hasła dostępowego dla wielu gości (konferencje, szkolenia itd.) |
| Transfer danych | przez Ethernet do co najmniej 1000 Mbit/s |
| Transfer danych | przez WiFi do co najmniej 1200 Mbit/s |
| Obsługa pasma | Co najmniej na częstotliwościach 2.4GHz oraz 5GHz |
| Protokoły komunikacji | Co najmniej 802.11ax oraz 802.11a/b/g/n/ac. |
| Priorytety | Urządzenia muszą pozwalać na określanie priorytetu transmitowanych danych i odpowiednie ich kolejkowanie. W tym celu punkty dostępowe muszą również wspierać standard Wi-Fi Multimedia (WMM) i aktywnie go wykorzystywać |
| Obsługa szyfrowania | 802.1x RADIUS, AES, HTTPS, SSH, WPA-PSK, WPA-TKIP, WPA2 |
| Interfejsy | Na potrzeby komunikacji z przełącznikami punkt dostępowy powinien posiadać dwa interfejsy 1Gbps, oba aktywnie wykorzystywane do transmisji danych |
| Zasilanie | Poprzez sieć Ethernet (PoE) oraz 230 V |
| Utrzymanie | Oprogramowanie wbudowane (firmware) musi być uaktualniane do najnowszych wersji przez cały czas trwania Umowy. |

**Wymagania dotyczące urządzeń sieci LAN.**

|  |  |
| --- | --- |
| Ilość urządzeń | 2 |
| Urządzenie/funkcje | Przełącznik zarządzany sieci LAN |
| Liczba obsługiwanych Użytkowników | Do 40 w tym 3 urządzenia dostępowe WiFi |
| Redundancja | Wszystkie przełączniki w stosie muszą równolegle przetwarzać ruch a awaria jednego z nich nie może spowodować braku komunikacji na drugim, poprawnie pracującym przełączniku. |
| Sieci wirtualne | Przełączniki muszą pozwalać na separację ruchu Użytkowników, gości, usług oraz urządzeń typu kamery i telefony za pomocą VLANów. Dodatkowo przełączniki muszą pozwalać na konfigurację reguł QoS. Przełączniki powinny obsługiwać przynajmniej 8 kolejek, do których przypisywany będzie ruch różnych aplikacji |
| Funkcja stosu | Przełączniki muszą być wyposażone w porty pozwalające na zestawienie tzw. stosu (jednego logicznego przełącznika, składającego się z wielu przełączników fizycznych). Łączna przepustowość interfejsów wykorzystywanych do zestawienia stosu musi być nie mniejsza niż 40Gbps |
| Porty | Wszystkie porty pracujące w standardach 1Gbps (standard 10/100/1000BaseT) |
| Montaż | W szafie 19” |
| Bezpieczeństwo | W celu zabezpieczenia się przed dołączaniem do sieci nieuprawnionych urządzeń przełączniki muszą pozwalać na uwierzytelnienie Użytkowników. Jako minimum wymagana jest możliwość uwierzytelniania się przy wykorzystaniu standardu 802.1x oraz przy pomocy sprzętowego adresu MAC urządzenia |
| Technologia PoE | Tak |
| Naprawa/wymiana | Następny Dzień Roboczy |

**Wymagania dotyczące urządzeń sieci WAN.**

|  |  |
| --- | --- |
| Ilość urządzeń | 2 |
| Urządzenie/funkcje  | Firewall, router, VPN, UTM |
| Redundancja | Wymagana praca równoległa obu urządzeń dla obu łączy. W przypadku awarii jednego z urządzeń, drugie urządzenie przejmuje obsługę ruchu z obu łączy. |
| Ochrona antywirusowa | Wymagana funkcjonalność kontroli antywirusowej poczty elektronicznej (SMTP, POP3, IMAP), FTP oraz HTTP. Kontrola antywirusowa musi być realizowana sprzętowo. |
| Ochrona antyspamowa | Wymagana funkcjonalność kontroli antyspamowej działającego w oparciu o mechanizm blacklist. |
| Filtrowanie stron WWW | Wymagana funkcjonalność kontroli filtrowania stron WWW w zależności od kategorii treści stron |
| Montaż | W szafie 19” |
| Filtrowanie ruchu | Wymagane posiadanie funkcji filtrowania zawartości ruchu HTTP, FTP i protokołów poczty elektronicznej (SMTP, POP3, IMAP) w celu blokowania potencjalnie szkodliwych obiektów. Urządzenie musi filtrować ruch na podstawie kryteriów obejmujących co najmniej: typy MIME, rozszerzenia plików, elementy ActiveX, Java i cookies |
| Dynamiczny routing | Wymagana obsługa protokołów dynamicznego routingu: RIP, OSPF oraz BGP. |
| Zarządzanie ruchem | Wymagane posiadanie mechanizmów priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. |
| Ciągłość działania | Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie. Urządzenia muszą funkcjonować w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze musi się odbywać przezroczyście dla Użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. |
| Obsługa VLAN | Urządzenie musi obsługiwać sieci VLAN. Urządzenie musi obsługiwać protokół LACP w celu agregowania fizycznych połączeń Ethernet |
| Zabezpieczenie przed atakami intruzów | Firewall musi posiadać funkcję wykrywania i blokowania ataków intruzów (IPS, intrusion prevention) realizowaną sprzętowo. System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące (D)DoS oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych ataków (intruzów, robaków) musi odbywać się w regułach polityki bezpieczeństwa. Zapory firewall muszą posiadać proste mechanizmy umożliwiające ochronę przez wyciekiem danych (Data Loss Prevention) |
| Obsługa VPN | Wymagane zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. |
| Polityki bezpieczeństwa | Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, Użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. |
| Montaż | W szafie 19” |
| Licencje | Wymagane jest zapewnienie licencji lub subskrypcji na 24 miesięcy na funkcjonalność IPS, Antywirus, URL Filtering Antispam |
| Utrzymanie | Baza sygnatur IPS musi być udostępniana przez producenta urządzenia firewall przez cały okres gwarancji. Baza sygnatur ataków musi być aktualizowana przez producenta codziennie. Oprogramowanie wbudowane (firmware) musi być uaktualniane do najnowszych wersji przez cały czas trwania umowy. |
| Naprawa/wymiana | Następny Dzień Roboczy |

1. Termin realizacji.

Przewidywany czas zakupu – 30 dni od daty zamówienia, nie później niż 20.09.2021.

1. Terminy dotyczące niniejszego zapytania

Odpowiedzi na niniejsze zapytanie należy złożyć w terminie do 30.06.2021 r. do godz. 18:00 w formie elektronicznej na adres zamowienia@fppp.gov.pl. W tytule email należy umieścić „Odpowiedź na zapytanie – urządzenia sieciowe”.

1. Zakres składanych dokumentów

W ramach odpowiedzi konieczne jest złożenie wypełnionego Załącznika 1 - formularz szacowania ceny. Dodatkowo, jeżeli istnieje taka konieczność z punktu widzenia składającego, prosimy o przesłanie opisów, materiałów informacyjnych i uzupełnienia do złożonej odpowiedzi.

1. Kontakt:

Osobą uprawnioną do kontaktów w ramach niniejszego zapytania jest Paweł Jachyra,
tel. +48 607 145 886, e-mail: pawel.jachyra@fppp.gov.pl

1. Załączniki:

Załącznik 1 – formularz szacowania ceny