Wykonawca:

…………………………………………………………………

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

reprezentowany przez:

…………………………………………………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji*

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

Zamawiający odrzuci ofertę, której minimalne parametry techniczne nie będą spełniały wymagań opisu przedmiotu zamówienia.

**UWAGA!** Wykonawca jest zobowiązany podać dokładny opis oferowanego urządzenia w prawej kolumnie tabeli „szczegółowy zakres przedmiotu zamówienia oferowany przez Wykonawcę”.

|  |  |  |
| --- | --- | --- |
| **LP.** | **MINIMALNY ZAKRES PRZEDMIOTU ZAMÓWIENIA WYMAGANY** **PRZEZ ZAMAWIAJĄCEGO** | **PARAMETRY OFEROWANE PRZEZ WYKONAWCĘ** **(Wykonawca wypełnia wpisując konkretne parametry oferowanego urządzenia zgodne z wymaganiami Zamawiającego** |
| **Nazwa producenta:** **…………………………………………………………****Typ produktu, model:** **…………………………………………………………** |
|  | Oprogramowanie musi charakteryzować się następującymi cechami: |  |
| 1. | Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor) |  |
| 2. | System musi odsługiwać minimum 10 000 urządzeń klienckich (w tym gości). Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniana po rozłączeniu urządzenia. |  |
| 3. | Praca w klastrze niezawodnościowym jako maszyny wirtualne w trybie hub and spoke. Wymagane jest dostarczenie licencji na jedno urządzenie typu hub i dwa urządzenia typu spoke. |  |
| 4. | Musi posiadać wbudowany serwer Radius oraz TACACS +  |  |
| 5. | Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym:* Cisco Systems
* Fortinet
* Microsoft
* Alcatel-lucent Enterprise
* Huawei Networks
* Extreme Networks
* PaloAlto Networks
* Producenta posiadanych przez Zamawiającego urządzeń firmy [Hewlett Packard Enterprise](https://www.hpe.com/pl/en/home.html)
 |  |
| 6. | Oprogramowanie musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera.  |  |
| 7. | Rozwiązanie musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego. |  |
| 8. | Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych. |  |
| 9. | Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych * Microsoft Active Directory
* Radius
* Kerberos
* LDAP
* ODBC
* Współpraca z serwerami tokenów
 |  |
| 10. | Musi obsługiwać metody profilowania * DHCP
* TCP
* MAC OUI
* SNMP

Cisco device sensor |  |
| 11. | Wspierać protokoły * Radius, Radius CoA, TACACS +, web authentication, SAML v2.0
* EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
* PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)
* TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)
* EAP-TLS
* PAP, CHAP, MSCHAPv1 i v2, EAP-MD5
* NAC, Microsoft NAP
* Windows machine authentication
* MAC Auth
* Audit (role oparte na porcie oraz skanowanie podatności)
* OCSP (Online Certificate Status Protocol)
* SNMP generic MIB, SNMP private MIB
* CEF (Common Event Format), LEEF (Log Event Extended Format)
* TLS 1.2
 |  |
| 12. | Oprogramowanie musi posiadać funkcję integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami  |  |
| 13. | Oprogramowanie w postaci maszyny wirtualnej musi mieć możliwość uruchomienia na platformach witalizacyjnych: * Co najmniej ESX 4.0, ESXi 4.1 do 6.0

Co najmniej Hyper-V 2012 R2 oraz Windows 2012 R2 enterprise  |  |
| 14. | Oprogramowanie musi posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich 10 000. Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte. |  |
| 15. | System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności* Samodzielna rejestracja klientów gościnnych w oparciu o:
* Adres e-mail
* Numer telefonu (wiadomość SMS)
* Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link)
* Logowanie w oparciu o portale społecznościowe
* Funkcja integracji z systemami trzecimi poprzez API
* Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową
* Wbudowany system reklamowy umożliwiający integrację z zewnętrznymi serwisami umożliwiającymi w prosty sposób promowanie ofert promocyjnych, materiałów multimedialnych oraz aplikacji mobilnych.
* Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.
* Funkcja personalizacji strony gościnnej
 |  |
| 16. | Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji. |  |
| 17. | Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działu IT  |  |
| 18. | Oprogramowanie musi wspierać obsługę następujących systemów operacyjnych * MS Windows
* Mac OS X
* iOS
* Android
* Chromebook
* Ubuntu
 |  |
| 19. | Oprogramowanie musi umożliwiać klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci  |  |
| 20. | Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej  |  |
| 21. | Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu. |  |
| 22. | Funkcja tworzenia unikalnych certyfikatów dla urządzeń.  |  |
| 23. | Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń  |  |
| 24. | Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID  |  |
| 25. | Posiadać moduł odpowiedzialny za kontrolę końcówek klienckich. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji. |  |
| 26. | System kontroli końcówek klienckich musi mieć następujące funkcjonalności * System musi wspierać następujące systemy operacyjne
* Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis)
* Apple Mac OS X 10.7 i nowsze
* Red HAT Enterprise Linux 4 i nowsze
* CentOS 4 (Community Enterprise Operating System) i nowsze
* Fedora Core 5 i nowsze
* SUSE linux 10.x i nowsze
* Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall
* Wyświetlanie informacji on-line o statusie monitorowanych końcówek
* System powinien obsługiwać agenta w formie:
* Stałej (Presistent Agent)
* Tymczasowej (Dissolvabe Agent)
* Agenta NAP
 |  |
| 27. | Minimum 3 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. |  |
| 28. | Zaoferowane rozwiązanie musi być uznane przez firmę analityczną Gartner Research. To znaczy musi być wymienione w bieżącym na moment składania oferty raporcie Market Guide for Network Access Control lub musi być wymienione w Gartner Peer Insights w kategorii Network Access Control, gdzie musi posiadać przynajmniej 100 opinii i status „Customer’s Choice”. |  |
| 29. | Do rozwiązania musi być dostępna publicznie, na stronie producenta, dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań. |  |
| 30. | Oferta musi zawierać kompletne zestawianie numerów katalogowych produktów i wszystkich jego dodatkowych składników umożliwiających ich jednoznaczną identyfikację u producenta sprzętu  |  |
| 31. | - Wszystkie elementy tworzące spójny ekosystem opisane w tym dokumencie (to jest: przełączniki, punkty dostępowe, kontrolery i system kontroli dostępu) muszą posiadać jeden, wspólny punkt kontaktu serwisowego w celu wspólnej diagnozy i pomocy technicznej dla całego środowiska a nie dla pojedynczych jego elementów.  |  |
| 32. | - Zamawiający może zażądać przed dostawą przeprowadzenia testów wybranych funkcji sprzętu i oprogramowania wymaganych w niemniejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłużysz niż 2 tygodnie od chwili zażądania przez Zamawiającego ich przeprowadzenia. Nieprzystąpienie do testów lub nieskuteczne ich przeprowadzenie (brak potwierdzenia przez Zamawiającego, że testy zostały zakończone pomyślnie) skutkować będzie odrzuceniem oferty. |  |

............................, dnia .................................