**ZAŁĄCZNIK NR 2 DO SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**ZAKUP SYSTEMU NAC NA POTRZEBY INFRASTRUKTURY INFORMATYCZNEJ SWD PRM**

# Spis treści

[Spis treści 2](#_Toc118971094)

[I. Słowniki i skróty 3](#_Toc118971095)

[II. Przedmiot zamówienia 4](#_Toc118971096)

[III. Wymagania Ogólne 4](#_Toc118971097)

[IV. Wymagania dodatkowe 17](#_Toc118971098)

[V. Świadczenie serwisu gwarancyjnego i gwarancji 17](#_Toc118971099)

[VI. Zasady odbioru przedmiotu umowy 19](#_Toc118971100)

# Słowniki i skróty

Dla potrzeb niniejszego opracowania przyjmuję się następujące definicje skrótów i pojęć:

| **Skrót/pojęcie** | **Definicja** |
| --- | --- |
| **Awaria**  | Oznacza utrudnienie działania oprogramowania systemu NAC w środowisku produkcyjnym w zakresie podstawowych funkcjonalności, w tym w szczególności brak możliwości włączenie, wyłączenia.  |
| **Dni Robocze** | Oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy, w godz. od 8:00 do 15:35. |
| **Oprogramowanie Standardowe** | Oznacza oprogramowanie powszechnie dostępne i eksploatowane na dzień złożenia oferty, będące w użytkowaniu lub zamówieniu Zamawiającego. |
| **Rozwiązanie NAC** | System teleinformatyczny, którego celem jest uwierzytelnianie urządzeń i użytkowników na brzegu sieci IT oraz uwierzytelnianie administratorów w dostępie do urządzeń – przydzielając właściwe uprawnienia. |
| **SWD PRM** | Systemy Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego wraz z zainstalowanym oprogramowaniem standardowym, aplikacyjnym oraz infrastrukturą sprzętową. |
| **Umowa** | Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia. |
| **Urządzenia** | Urządzenia fizyczne lub w postaci maszyn wirtualnych. Mogą to być urządzenia fizyczne: switch, kontroler WLAN, urządzenia wirtualne – softphone, urządzenia końcowe klienckie Zamawiającego (laptop, telefon IP, drukarka). |
| **Usługa Serwisu** | Usługa świadczona w ramach gwarancji udzielonej przez Wykonawcę, polegająca na zapewnieniu przez Wykonawcę poprawności i ciągłości prawidłowego działania Oprogramowania Standardowego oraz jego poszczególnych komponentów. |
| **Użytkownik** | Zamawiający oraz jego pracownicy. |
| **Wykonawca** | Podmiot realizujący zamówienie. |
| **Zamawiający** | Lotnicze Pogotowie Ratunkowe. |

# Przedmiot zamówienia

Przedmiotem zamówienia jest zakup rozwiązania typu Network Access Control umożliwiającego uwierzytelnienie oraz autoryzację urządzeń w sieci LAN, a także uwierzytelnienie i autoryzację administratorów Urządzeń Zamawiającego. Rozwiązanie w trybie wysokiej dostępności składa się
z 2 wirtualnych systemów obsługujących 2200 sesji uwierzytelniających urządzenia końcowe Zamawiającego oraz 2 systemów dla uwierzytelniania administratorów.

Rozwiązanie będzie objęte gwarancją i wsparciem technicznym producenta lub autoryzowanego serwisu producenta na przez okres 3 lat od dnia podpisania protokołu odbioru. Wszelkie zapisy zawierające parametry techniczne należy odczytywać jako parametry minimalne.

# Wymagania Ogólne

Wymagania dotyczące rozwiązania NAC

Wykonawca w ramach realizacja przedmiotu zamówienia zapewni:

1. pełne zarządzanie cyklem życiowym dostępu do zasobów sieciowych, niezależnie od miejsca uzyskiwanego dostępu,
2. wsparcie dla dostępu gościnnego w sieci, identyfikację stacji, rejestrację urządzeń,
3. kontrolę dostępu wszystkich urządzeń podłączonych do sieci IP w tym terminali, komputerów PC, smartfonów i tabletów, telefonii IP, terminali video i innych podłączonych urządzeń,
4. uwierzytelnienie oraz autoryzację oraz rozliczalność działań administratorów w infrastrukturze sieciowej.

Tabela 1 Specyfikacja pojedynczego kompletu

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Numer produktu** | **Opis** | **Ilość** |
| 1 | ISE-A-LIC | Cisco Identity Service Engine Advantage Subscription | 2200 |
| 2 | **L-ISE-TACACS-ND=** | Cisco ISE Device Admin Node License | 2 |
| 2 | **R-ISE-VMC-K9=** | Cisco ISE Virtual Machine Common PID | 2 |

Zamawiający dopuszcza rozwiązanie równoważne, pod warunkiem spełnienia przez nie następujących minimalnych wymagań:

Tabela 2 Wymagania dla rozwiązań równoważny

| **Kod wymagania** | **Opis wymagań** |
| --- | --- |
| **Podstawowe cechy systemu** |
|  | Rozwiązanie umożliwia instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych. |
|  | Rozwiązanie umożliwia elastyczną rozbudowę poprzez dodawanie licencji dla podstawowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych. |
|  | Rozwiązanie umożliwia wysoką skalowalność i rozbudowę w miarę wzrostu liczby Urządzeń. |
|  | W scenariuszu, w którym wszystkie komponenty rozwiązania znajdują się na pojedynczym serwerze jest on w stanie obsłużyć następującą liczbę jednoczesnych sesji: 2200 sesji. |
|  | Rozwiązanie umożliwia instalację na maszynie wirtualnej (VM) i maszynie fizycznej, w tym na systemach:* VMware wersji 11 dla ESXi 6.x,
* WMware Cloud w AWS,
* Azure VMware Solution,
* hypervisorze KVM na Red Hat Enterprise Linux (RHEL),
* Microsoft Hyper-V,
* AWS EC2,
* serwerach fizycznych wspieranych przez producenta.
 |
|  | Rozwiązanie umożliwia wydzielenie określonych elementów funkcjonalnych, instalowanych jako oddzielne maszyny fizyczne lub wirtualne, w tym:* wydzielenie podsystemu zarządzania (Administration), umożliwiającego administratorowi dostęp do interfejsu graficznego (GUI) za pomocą przeglądarki web i zmianę konfiguracji rozwiązania oraz jego monitorowanie;
* wydzielenie podsystemu monitoringu, logowania i rozwiązywania problemów, umożliwiającego gromadzenie wiadomości logowania z:
* przełączników dostępowych,
* sesji uwierzytelniania 802.1X,
* zdarzeń kontroli dostępu (autoryzacji),
* zdarzeń związanych z błędami,
* zdarzeń związanych z alarmami systemowymi;
* wydzielenie serwerów usługowych realizujących funkcje:
* serwera RADIUS dla infrastruktury sieciowej,
* serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
* serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego,
* serwera profilowania stacji końcowych .
 |
|  | Rozwiązanie umożliwia realizację wysokiej dostępności elementów funkcjonalnych, w tym:* zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu;
* zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych.
 |
|  | Rozwiązanie umożliwia aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych – co najmniej przez serwer TFTP, serwer FTP/SFTP, serwer HTTP/HTTPS, udział NFS. |
|  | Rozwiązanie umożliwia zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback). |
|  | Rozwiązanie umożliwia tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled). |
|  | Rozwiązanie umożliwia uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników. |
|  | Rozwiązanie umożliwia uwierzytelnianie administratorów za pomocą zewnętrznych repozytoriów - m.in. Active Directory, Radius i SAML 2.0. |
|  | Rozwiązanie umożliwia wymuszenie reguł złożoności haseł dla administratorów, w tym co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. Rozwiązanie wymusza hasło różne od trzech poprzednich haseł i jego zmianę co określoną ilość dni |
|  | Rozwiązanie umożliwia kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:* dostęp do interfejsu konfiguracji usług tożsamości 802.1X,
* dostęp do interfejsu konfiguracji urządzeń sieciowych,
* dostęp do interfejsu konfiguracji polityk,
* dostęp do interfejsu konfiguracji kontroli dostępu gościnnego,
* dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania.
 |
|  | Rozwiązanie umożliwia kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP. |
|  | Rozwiązanie posiada możliwość podłączenia i identyfikacji urządzenia końcowego z wykorzystaniem MUD (Manufacturer Usage Description) zgodnie ze standardem IETF i RFC8520. |
|  | Rozwiązanie wspiera REST API do masowych operacji CRUD (Create, Read, Update, Delete) m.in. na użytkownikach, stacjach końcowych oraz urządzeniach sieciowych.  |
|  | Rozwiązanie wspiera REST API do monitorowania w czasie rzeczywistym sesji oraz stacji końcowych. |
|  | Rozwiązanie wspiera REST API do konfiguracji i zarządzania m.in. politykami Radius, kopiami zapasowymi oraz repozytoriami plików. |
| **Mechanizmy uwierzytelniania 802.1x** |
|  | Rozwiązanie wspiera następujące protokoły uwierzytelniania i standardy:RADIUS, zgodnie z dokumentami:* RFC 2138 — Remote Authentication Dial In User Service (RADIUS)
* RFC 2139 — RADIUS Accounting
* RFC 2865 — Remote Authentication Dial In User Service (RADIUS)
* RFC 2866 — RADIUS Accounting
* RFC 2867 — RADIUS Accounting for Tunnel Protocol Support
* RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
* RFC 2869 — RADIUS Extensions
 |
|  | RADIUS Proxy dla zewnętrznego serwera RADIUS. |
|  | Rozwiązanie wspiera protokół Windows Active Directory, w tym następujące repozytoria AD:* Microsoft Windows Active Directory 2003 32bit
* Microsoft Windows Active Directory 2003 R2 32bit i 64bit
* Microsoft Windows Active Directory 2008 32bit i 64bit
* Microsoft Windows Active Directory 2008 R2 64bit
* Microsoft Windows Active Directory 2012
* Microsoft Windows Active Directory 2012 R2
* Microsoft Windows Active Directory 2016
* Microsoft Windows Active Directory 2019
 |
|  | Rozwiązanie wspiera protokół Lightweight Directory Access Protocol (LDAP). |
|  | Rozwiązanie wspiera protokół Security Assertion Markup Language (SAML) 2.0 oraz funkcjonalność Single Sign-On (SSO). |
|  | Rozwiązanie wspiera integrację z Azure Active Directory z użyciem technologii Oauth ROPC w celu uwierzytelnienia klientów 802.1x. |
|  | Rozwiązanie wspiera serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865. |
|  | Rozwiązanie wspiera następujące protokoły uwierzytelniania:* PAP/ASCII,
* CHAP,
* MS-CHAPv1,
* MS-CHAPv2,
* EAP-MD5,
* LEAP,
* EAP-TLS,
* EAP-TTLS,
* Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:
* EAP-MS-CHAPv2,
* EAP-GTC,
* EAP-TLS,
* Tunnel Extensible Authentication Protocol (TEAP) z metodami wewnętrznymi:
* EAP-MS-CHAPv2,
* EAP-TLS.
 |
|  | Rozwiązanie umożliwia konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect. |
|  | Rozwiązanie wspiera implementację 802.1X z przynajmniej następującymi suplikantami:* wbudowanym klientem 802.1X dla Windows 10,
* wbudowanym klientem 802.1X dla Windows 7,
* wbudowanym klientem 802.1X dla Windows 8 i 8.1,
* Apple Mac OS X Supplicant,
* Apple iOS Supplicant,
* Google Android Supplicant.
 |
|  | Rozwiązanie umożliwia tworzenie polityk uwierzytelniania 802.1X opartych o złożone reguły (rule-based). |
|  | Rozwiązanie umożliwia uwierzytelnianie 802.1X maszyn i użytkowników. |
|  | Rozwiązanie umożliwia tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o reguły. |
|  | Rozwiązanie posiada lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym.) |
|  | Rozwiązanie posiada lokalną bazę stacji końcowych. Lokalna baza stacji końcowych jest tworzona per stacja końcowa na podstawie unikalnego adresu MAC.  |
|  | Rozwiązanie wspiera uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC. |
|  | Rozwiązanie wspiera zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD – Network Access Devices), w tym:* tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host per port,
* tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia,
* tryb uwierzytelniania 802.1X, w którym dozwolone jest jedno urządzenie telefonii IP w domenie głosowej (Voice VLAN) i jeden host w domenie danych (Data VLAN) na jednym porcie fizycznym,
* tryb uwierzytelniania 802.1X dozwalający wiele hostów na jednym porcie fizycznym,
* mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny,
* mechanizm umożliwiający poprawną obsługę sytuacji, w której nowy host podłącza się do portu, na którym uprzednio było uwierzytelnione urządzenie w tym w VLANie głosowym,
* mechanizm umożliwiający wysłanie informacji o restarcie urządzenia (przełącznika) dostępowego do serwera AAA. Dzięki temu uwierzytelnione aktywne sesje związane z tym konkretnym urządzeniem zostaną usunięte z listy na serwerze AAA,
* mechanizm przypisania VLANu w procesie uwierzytelnienia i kontroli dostępu 802.1X,
* mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1X,
* obsługa przypisania listy kontroli dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki,
* mechanizm 802.1x umożliwiający realizację dostępu gościnnego w dedykowanym VLAN’ie (Guest VLAN) dla użytkowników gościnnych,
* mechanizm 802.1x umożliwiający przypisanie urządzenia telefonii IP do dedykowanego VLANu w sytuacji, gdy serwer AAA jest niedostępny,
* przypisanie przez serwer AAA dla użytkownika nie jednego, lecz grupy VLAN’ów dla użytkownika, z których przełącznik wybiera jeden, w którym jest najmniej użytkowników
* uwierzytelnienie 802.1X urządzenia telefonii IP znajdującego się w VLAN’ie głosowym,
* współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN,
* możliwość elastycznej konfiguracji kolejności metod 802.1X użytych do uwierzytelnienia stacji, w tym uwierzytelnienia względem centralnej bazy MAC, metod EAP dla 802.1X i uwierzytelnienia web,
* możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznik.
 |
|  | Rozwiązanie wspiera uwierzytelnianie nazwą użytkownika i hasłem przez portal web, jako jedną z metod uwierzytelniania do sieci, (dotyczy m.in. sytuacji, gdy stacja ma niepoprawnie skonfigurowane lub niedziałające oprogramowanie suplikanta 802.1X). |
| **Realizacja dostępu gościnnego** |
|  | Rozwiązanie umożliwia realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, między innymi dla:* Microsoft Windows 10, Windows 8.1, Windows 8, Windows 7,
* Apple Mac OS X 10.x oraz 11.x,
* Apple iOS 11.x, 12.x, 13.x i nowszych,
* Google Android dla wersji 7.x i nowszych,
* Linux.
 |
|  | Rozwiązanie umożliwia dodawanie kont gościnnych przez wybrane osoby (sponsor). |
|  | Rozwiązanie zapewnia uwierzytelnienie sponsora, które musi odbywać sekwencyjnie w oparciu o:* wewnętrzną bazę użytkowników,
* zewnętrzne repozytorium użytkowników.
 |
|  | Rozwiązanie umożliwia konfigurację uprawnień sponsora, w tym uprawnienia do:* logowania się do systemu,
* tworzenia pojedynczego konta gościnnego,
* tworzenia wielu kont gościnnych,
* importowania kont gościnnych z pliku CSV,
* wysyłania wiadomości email po utworzeniu konta gościnnego,
* wysyłania wiadomości SMS po utworzeniu konta gościnnego,
* wyświetlenia hasła konta gościnnego,
* wydrukowania danych konta gościnnego,
* wyświetlenia danych stworzonych kont gościnnych,
* zawieszenia (suspend) i reinicjacji kont gościnnych.
 |
|  | Rozwiązanie umożliwiać personalizację wyglądu portalu sponsora i gościa, w tym:* zmianę logo strony logowania,
* zmianę obrazu tła strony logowania,
* zmianę logo bannera,
* zmianę obrazu tła bannera,
* zmianę koloru tła strony z treścią.
 |
|  | Rozwiązanie umożliwia zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP i portu HTTPS. |
|  | Rozwiązanie umożliwia zmianę adresu URL i FQDN strony sponsora. |
|  | Rozwiązanie umożliwia automatyczne kasowanie wygasłych kont gościnnych: na żądanie i okresowo co zadaną liczbę dni i o określonej godzinie. System umożliwia wyświetlenie czasu ostatniego kasowania wygasłych kont gościnnych i następnego kasowania wygasłych kont gościnnych. |
|  | Rozwiązanie posiada wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim, angielskim, francuskim, niemieckim i hiszpańskim. |
|  | Rozwiązanie umożliwia stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim. |
|  | Rozwiązanie umożliwia wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora:* Imienia,
* Nazwiska,
* Firmy,
* adresu e-mail,
* numeru telefonu,
* danych opcjonalnych (nie mniej niż 5 dodatkowych pól).
 |
|  | Rozwiązanie umożliwia konfigurację dla użytkowników gościnnych:* wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP),
* zezwolenia gościom na zmianę hasła oraz odzyskiwanie zapomnianego hasła,
* samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora.
 |
|  | Rozwiązanie umożliwia honorowanie ustawień local przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego. |
|  | Rozwiązanie umożliwia konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego. |
|  | Rozwiązanie umożliwia konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługuje co najmniej 20 urządzeń per konto gościnne. |
|  | Rozwiązanie umożliwia konfigurację czasu ważności hasła w dniach w przedziale zadanym w dniach. |
|  | Rozwiązanie umożliwia określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny. |
|  | Rozwiązanie umożliwia konfigurację polityki złożoności haseł użytkowników gościnnych. |
|  | Rozwiązanie umożliwia konfigurację polityki nazwy (login) użytkownika gościnnego w tym co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika. |
|  | Rozwiązanie umożliwia tworzenie portalu typu Hotspot bez konieczności uwierzytelniania się gościa nazwą użytkownika i hasłem z opcjonalną akceptacją AUP (Acceptable Use Policy) i z koniecznością podania kodu dostępu. |
|  | Rozwiązanie umożliwia przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsu IP, portu HTTPS i certyfikatu SSL dla FQDN. |
|  | Rozwiązanie umożliwia udostępnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP, secure SMTP i poprzez SMS.  |
|  | Rozwiązanie umożliwia wykorzystanie protokołu SAML 2.0 oraz funkcjonalności SSO dla portali gościnnych oraz sponsora. |
|  | Rozwiązanie wspiera API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych. |
| **Profilowanie urządzeń** |
|  | Rozwiązanie umożliwia dokonanie profilowania (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu. |
|  | Rozwiązanie umożliwia wykorzystanie danych z procesu profilowania do zdefiniowania polityk bezpieczeństwa. W szczególności zapewnia możliwość stworzenia polityk np. dla wszystkich drukarek, dla wszystkich urządzeń mobilnych, dla wszystkich stacji z Windows, etc. |
|  | Rozwiązanie umożliwia dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł:* DHCP,
* DHCP SPAN,
* http,
* RADIUS,
* DNS,
* SNMP,
* Network Scan (NMAP lub inne narzędzie profilowania aktywnego).
 |
|  | Rozwiązanie umożliwia wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji. |
|  | Rozwiązanie umożliwia dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy. |
|  | Rozwiązanie posiada dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla:* Stacji roboczych pracujących z systemami FreeBSD, Linux, Macintosh, Microsoft Windows, Sun,
* Urządzeń mobilnych: Android, Apple, Blackberry,
* Telefonów IP,
* Drukarek sieciowych,
* Systemów wideokonferencyjnych w tym terminali i urządzeń z nimi powiązanych,
* Routerów,
* Punktów dostępu bezprzewodowego.
 |
|  | Rozwiązanie umożliwia subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, w tym następujących informacji:* reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci,
* reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie <http://standards.ieee.org/develop/regauth/oui/oui.txt>.
 |
|  | Rozwiązanie umożliwia włączenie funkcjonalności regularnej (z częstotliwością dobową) i automatycznej subskrypcji nowych profili urządzeń ze strony producenta o zadanej godzinie lub jej całkowite wyłączenie w dowolnym momencie. |
|  | Rozwiązanie wspiera raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta. |
| **Wymiana informacji kontekstowych oraz automatyzacji odpowiedzi** |
|  | Rozwiązanie umożliwia wymianę informacji kontekstowych dotyczących sesji użytkowników oraz urządzeń. Wymiana ta może występować w obu kierunkach – system NAC może zarówno udostępniać informacje jak i przyjmować je z zewnętrznych systemów producenta oraz firm trzecich.  |
|  | Wymiana informacji realizowana jest z użyciem dedykowanej szyny wymiany informacji w architekturze Consumer-Provider, opartej o technologie REST oraz Websocket. System NAC pełni rolę serwera wymiany informacji.  |
|  | Wymiana informacji może zostać skonfigurowana z kilkudziesięcioma rodzajami systemów klasy enterprise, m.in.: next-generation firewall, network detection and response (NDR)/flow monitoring, Security Information Event Management (SIEM), IoT Security, DNS, DHCP and IP (DDI) management, skanowania/zarządzania podatnościami.  |
|  | Rozwiązanie umożliwia zmianę autoryzacji stacji w oparciu o dyspozycje otrzymane poprzez szynę wymiany informacji. Zmiana autoryzacji może spowodować m.in. przeniesienie stacji do VLAN’u kwarantanny o ograniczonym dostępie do sieci lub dezaktywację portu, do którego podłączona jest stacja w celu odcięcia jej dostępu do sieci.  |
| **Obsługa serwerów certyfikatów CA** |
|  | Rozwiązanie posiada funkcję zintegrowanego centrum certyfikacji, Certificate Authority (CA) lub zapewniać współpracę z zewnętrznym centrum CA.  |
|  | Funkcja CA umożliwia wystawianie certyfikatów dla urządzeń, które uzyskują dostęp do sieci w procesie BYOD, dla realizacji bezpiecznego uwierzytelniania przy pomocy protokołu EAP-TLS. |
|  | Rozwiązanie wspiera hierarchiczność CA dla rozproszonego wdrożenia w dużej skali. W sytuacji rozproszenia systemu na wiele serwerów, serwery nadrzędne oferują funkcję Root CA, zaś serwery przetwarzające wspierają funkcję Subordinate CA (SCEP RA) dla wystawiania certyfikatów. |
|  | Funkcja CA zapewnia przynajmniej następujące funkcjonalności:* Certificate Issuance: sprawdzenie i podpisywanie Certificate Signing Request (CSR) dla stacji końcowych, które chcą uzyskać dostęp do sieci za pomocą bezpiecznej metody uwierzytelniania EAP-TLS,
* Key Management: generacja i bezpieczne przechowywanie kluczy, i certyfikatów w modelu rozproszonym,
* Certificate Storage: bezpieczne przechowywanie certyfikatów użytkownikówi stacji,
* Online Certificate Status Protocol (OCSP): wsparcie dla sprawdzenia ważności certyfikatów za pomocą protokołu OCSP wraz ze wsparciem dla wysokiej dostępności, przynajmniej dwóch serwerów OCSP per CA.
 |
| **Raportowanie** |
|  | Rozwiązanie umożliwia generowanie m.in. następujących raportów:* raportów dla protokołów AAA:
* diagnostyki protokołów AAA
* trendów uwierzytelnienia 802.1X
* accountingu RADIUS
* uwierzytelniania RADIUS
* raportów dozwolonych protokołów
* sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym:
* uwierzytelnień pomyślnych
* uwierzytelnień nieudanych
* „N” największych ilości uwierzytelnień RADIUS per protokół EAP (Top5), w tym:
* uwierzytelnień pomyślnych
* uwierzytelnień nieudanych
* raportów dla poszczególnych instancji serwerów systemu, w tym:
* uwierzytelnień RADIUS per serwer
* Top „N” uwierzytelnień per serwer
* monitorowania Online Certificate Status Protocol (OCSP)
* administratorów systemu i ich uprawnień
* logowania administratorów do systemu
* zmian konfiguracji serwera dokonanych przez administratorów
* stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS)
* zmian operacyjnych serwera dokonanych przez administratorów
* zmian haseł przez użytkowników
* raportów dla stacji końcowych, w tym:
* uwierzytelnień typu MAC Authentication
* Top „N” uwierzytelnień per adres MAC stacji
* Top „N” uwierzytelnień per maszyna
* Top „N” uwierzytelnień per RADIUS Calling Station ID
* działań podsystemu profilera per adres MAC
* czasu wymaganego na sprofilowanie stacji per adres MAC
* raportów dla błędów, w tym:
* błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił
* sumarycznych przyczyn nieudanych uwierzytelnień
* Top „N” uwierzytelnień per rodzaj błędu
* raportów dla urządzeń sieciowych:
* sumarycznych uwierzytelnień dla urządzeń sieciowych
* Top „N” uwierzytelnień per urządzenie sieciowe
* niedostępności serwera AAA dla urządzenia sieciowego
* wiadomości logowanych przez urządzenia sieciowe
* stanu portów i sesji urządzenia sieciowego widocznych przez SNMP
* raportów użytkowników:
* sumarycznych uwierzytelnień użytkowników
* Top „N” uwierzytelnień per użytkownik
* sesji użytkowników gościnnych
* aktywności użytkowników gościnnych
* sumarycznych uwierzytelnień sponsorów dostępu gościnnego
* uwierzytelnień per unikalny użytkownik
* raportów katalogu sesji
* aktywnych sesji RADIUS
* historii sesji RADIUS
* za terminowanych sesji RADIUS
 |
| **Alarmy i diagnostyka** |
|  | Rozwiązanie umożliwia generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:* wiadomości e-mail,
* syslog.
 |
|  | Alarmy mogą być generowane w następujących sytuacjach:* ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu,
* opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego,
* status krytycznych procesów będzie niepożądany, w tym status:
* procesu wewnętrznej bazy danych systemu,
* serwera aplikacyjnego systemu,
* bazy danych sesji,
* kolektora i procesora wiadomości log,
* błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej),
* stan obciążenia systemu wzrośnie powyżej zadanego poziomu, w tym:
* obciążenie systemu (load),
* zajętość pamięci.
 |
|  | Rozwiązanie posiada zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:* badanie łączności IP za pomocą ping, nslookup, traceroute,
* wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
* nazwy użytkownika,
* adresu MAC,
* statusu uwierzytelnienia (udana lub nieudana),
* powodu, jeżeli uwierzytelnienie nieudane,
* zakresu czasowego, co do dnia, godziny i minuty,
* wykonanie zdalnego polecenia na urządzeniu sieciowym,
* ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem:
* definicji serwerów AAA,
* protokołu RADIUS,
* odkrywania urządzeń,
* logowania,
* uwierzytelniania Web,
* konfiguracji trybu 802.1X,
* wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu.
 |
| **Wsparcie dla protokołu IPv6** |
|  | Rozwiązanie posiada wsparcie dla SSH IPv6. |
|  | Rozwiązanie pozwala na zarządzanie administracyjne za pomocą interfejsu graficznego udostępnionego administratorowi z wykorzystaniem adresacji IPv6. |
|  | Rozwiązanie pozwala na konfigurację NTP IPv6. |
|  | Rozwiązanie umożliwia stworzenie reguł ograniczających dostęp administracyjny do linii poleceń lub interfejsu graficznego w oparciu o adres IPv6. |
|  | Rozwiązanie umożliwia konfigurację serwerów SNMP w oparciu o adresację IPv6. |
|  | Rozwiązanie umożliwia wysyłanie SNMP Trap do serwera SNMP IPv6. |
|  | Rozwiązanie umożliwia integrację z Active Directory w oparciu o IPv6. |
|  | Rozwiązanie umożliwia połączenie z serwerem Radius z wykorzystaniem adresu IPv6. |
| **Administrowanie urządzeniami sieciowymi** |
|  | Rozwiązanie umożliwia aktywację serwera TACACS+ na wszystkich lub wybranych maszynach (wirtualnych bądź fizyczych) będących jego częścią. |
|  | Serwer TACACS+ umożliwia uwierzytelnienie administratorów urządzeń sieciowych (np. przełączników oraz ruterów) oraz autoryzację zgodną ze skonfigurowaną na Rozwiązanie NAC polityką. |
|  | Polityki TACACS+ umożliwiają m.in. określenie czy określony w polityce administrator bądź grupa administratorów, dla określonych urządzeń, otrzyma pełne przywileje operacyjne i konfiguracyjne czy też ich ograniczony zakres (np. możliwość wykonywania tylko określonych komend). |
| **Dobre praktyki realizacji rozwiązań** (Rozwiązanie spełnia następujące warunki dobrych praktyk realizacji systemu uwierzytelnienia dostępu do sieci) |
|  | Rozwiązanie może występować w formie pojedynczego rozwiązania jak też systemu złożonego z kilku komponentów.  |
|  | W przypadku zastosowania rozwiązania złożonego z kilku komponentów rozwiązanie zapewnia pojedynczy interfejs konfiguracyjny, zarządzający i monitorujący zapewniający możliwość wymuszenia spójnej polityki bezpieczeństwa dla dostępu LAN/WLAN/VPN.  |
|  | Niezależnie od tego czy NAC występuje w formie pojedynczego rozwiązania lub jest złożony z kilku komponentów, może on być serwisowany jako jedno rozwiązanie w ramach pojedynczej usługi wsparcia. |

# Wymagania dodatkowe

Wykonawca musi zapewnić Zamawiającemu możliwość odnowienia, po wygaśnięciu zawartej umowy serwisowej, usługi wsparcia producenta bez konieczności uiszczania dodatkowych opłat wznowieniowych, z wyjątkiem sytuacji, kiedy producent w okresie trwania usługi zakończy świadczenie usług wsparcia technicznego dla licencji będących przedmiotem zamówienia.

# Świadczenie serwisu gwarancyjnego i gwarancji

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis funkcjonalności** |
| **WUS.01** | Na dostarczone rozwiązanie Wykonawca zapewni wsparcie producenta wraz z gwarancją liczoną od daty podpisania protokołu odbioru przedmiotu zamówienia na okres 36 miesięcy opartego na świadczeniach serwisowych producenta. |
| **WUS.02** | Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu: * prawo do pobierania nowych wersji i aktualizacji przez okres minimum 36 miesięcy od podpisania protokołu odbioru produktu;
* możliwość aktualizacji oprogramowania poprzez dostęp do zasobów producenta rozwiązania;
* dostęp do pomocy technicznej producenta;
* nieograniczoną liczbę zgłoszeń serwisowych;
* dostęp do materiałów producenta takich jak: techniczna dokumentacja, internetowa baza wiedzy, forum internetowe producenta oprogramowania/urządzeń;
* dostęp do poprawek i uaktualnień oprogramowania objętego usługą wsparcia oraz nowych wersji;
* dostęp do portalu www producenta Oprogramowania Standardowego umożliwiającego zarządzanie posiadanymi licencjami, podniesienie lub obniżenie (jeśli producent oficjalnie wspiera poprzednie wersje) wersji oprogramowania;
* dostęp do rejestru licencji (dostępnego przez portal www producenta oprogramowania/urządzeń).
 |
| **WUS.03** | Wykonawca wraz z dostawą licencji na Oprogramowanie Standardowe w tym procedury zgłaszania awarii, dostępne kanały komunikacyjne z serwisem producenta. Do zamówienia muszą zostać dostarczone procedury zgłaszania awarii w formie elektronicznej edytowalnej. |
| **WUS.04** | Przyjęcie do realizacji zgłoszenia powinno zostać niezwłocznie potwierdzone przez Wykonawcę, zwrotnie na adres e-mail zgłaszającego. |
| **WUS.05** | Za moment zgłoszenia przyjmuje się datę i godzinę zarejestrowania przez system elektroniczny Wykonawcy, w szczególności odebrania przesyłki e-mail przez system pocztowy lub zarejestrowanie zdarzenia przez Zamawiającego w udostępnionym przez Wykonawcę systemie zgłoszeniowym. W przypadku zgłoszenia telefonicznego moment zgłoszenia zostanie ustalony z Zamawiającym w trakcie tego zgłoszenia i potwierdzony w e-mailu. |
| **WUS.06** | Czas reakcji Wykonawcy na zgłoszenie awarii wynosi do 4 godzin od momentu zgłoszenia awarii, przez wszystkie dni w roku |
| **WUS.07** | Wykonawca dokona usunięcia Awarii w terminie nie dłuższym niż 72 godziny od momentu zgłoszenia. |
| **WUS.08** | Przez usunięcie Awarii należy rozumieć przywrócenie pierwotnej funkcjonalności sprzed wystąpienia Awarii albo zaproponowanie procedury obejścia zaistniałych Awarii bez rozwiązania problemu, pod warunkiem, że na przedstawioną przez Wykonawcę propozycję Zamawiający wyrazi zgodę. |
| **WUS.09** | Wykonawca najpóźniej w 1 Dzień Roboczy, po rozwiązaniu każdego incydentu serwisowego przedstawi raport z tego Incydentu serwisowego (prezentujący, co najmniej czasy przyjęcia zgłoszenia o Incydencie serwisowym oraz rozwiązania incydentu serwisowego, a także przyczyny, sposoby rozwiązania i działania zapobiegające występowaniu Incydentu serwisowego). |
| **WUS.10** | Zamawiający uprawniony jest do opóźnienia terminu rozpoczęcia usuwania awarii przez Wykonawcę, w takim przypadku gwarantowany czas naprawy ulegnie odpowiedniemu wydłużeniu i będzie liczony względem wskazanego przez Zamawiającego terminu.  |
| **WUS.11** | W przypadku zdiagnozowania błędów w używanej przez Zamawiającego wersji Oprogramowania, Wykonawca zapewni Zamawiającemu dostęp do najnowszych wersji oprogramowania urządzeń posiadających wsparcie producenta, pozwalających na usuniecie tych błędów. W przypadku wykrycia błędu, dla którego brak jest w danym momencie odpowiedniej aktualizacji, Wykonawca dokona eskalacji zgłoszenia do producenta. Wykonawca zapewnia i zobowiązuje się, że zgodnie z niniejszą specyfikacją korzystanie przez Zamawiającego z oprogramowania w ramach wsparcia technicznego nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.  |
| **WUS.12** | Z tytułu świadczenia przez Wykonawcę usługi serwisu gwarancyjnego Zamawiający nie ponosi dodatkowych kosztów. |
| **WUS.13** | Zamawiający wymaga elastyczności w rozbudowie, aby była możliwość bez konieczności uzyskania zgody Wykonawcy czy Producenta, rozbudowy posiadanych urządzeń o kolejne moduły rozszerzeń. Rozbudowa nie może powodować utraty praw gwarancyjnych do istniejącej i rozszerzonej konfiguracji danego urządzenia.  |
| **WUS.14** | Dla oprogramowania obowiązują prawa gwarancyjne producenta. |
| **WUS.15** | Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady. |

# Zasady odbioru przedmiotu umowy

**Zasady Ogólne**

1. Przedmiot Umowy należy dostarczyć zgodnie z zasadami i terminami wskazanymi w Umowie.
2. Przedmiot Umowy podlegać będzie odbiorowi ilościowo – jakościowemu.
3. Odbiór zostanie przeprowadzony w biurze Zamawiającego przy ul. Maszewskiej 20 lok. U1, w Warszawie, w obecności przedstawicieli Wykonawcy i Zamawiającego w godz. 8:00 – 15:35 lub elektronicznie na adres mailowy wskazany przez Zamawiającego.
4. Odbiór zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego i Wykonawcy protokołu odbioru ilościowo – jakościowego, którego wzór stanowi załącznik nr 3 do Umowy.

 **Odbiór ilościowo – jakościowy**

1. Celem czynności kontrolnych prowadzonych w ramach odbioru ilościowo – jakościowego jest sprawdzenie kompletności dostarczonego przedmiotu Umowy i potwierdzenie zgodności
z zakresem określonym w Umowie oraz sprawdzenie wszystkich wymagań funkcjonalnych
i potwierdzenie zgodności ze szczegółowym opisem przedmiotu Umowy.
2. Wykonawca będzie odpowiedzialny za dostarczenie i zaprezentowanie dostarczonego przedmiotu Umowy.
3. Podstawą dokonania odbioru ilościowo – jakościowego jest przeprowadzenie z pozytywnym skutkiem sprawdzeń kompletności oraz poprawności działania Oprogramowania dostarczonego w ramach Umowy wraz z wymaganymi licencjami – weryfikacja polega na sprawdzeniu obecności licencji w portalu producenta przypisanych do konta Zamawiającego.
4. Pozytywny wynik odbioru ilościowo – jakościowego zostanie potwierdzony podpisaniem protokołu odbioru ilościowo – jakościowego.