

## Szczegółowy opis przedmiotu zamówienia

Przedmiotem zamówienia jest:

- sprzedaż i dostawa dwóch urządzeń PulseSecure PSA5000 lub równoważnych, zwane łącznie „systemem”
- migracja posiadanego przez Zamawiającego systemu kontroli dostępu komputerów, urządzeń i użytkowników do sieci opartego o klaster urządzeń Juniper IC-4500 do nowej wersji systemu opartego o dostarczone urządzenia PulseSecure PSA5000 lub równoważne,

### **I Opis przedmiotu zamówienia:**

Dostarczony system (urządzenia i funkcjonalność) musi mieć co najmniej pełną funkcjonalność posiadanego systemu (urządzeń i funkcjonalności), pracującego obecnie pod kontrolą systemu PulseSecure w wersji 5.1.R6.

Minimalne parametry licencyjne, które muszą być spełnione przez dostarczony system:

1. jednoczesna minimalna ilość użytkowników autoryzujących się suplikantem 802.1x: 1000,
2. jednoczesna minimalna ilość urządzeń i komputerów autoryzujących się adresem mac: 2000.

Funkcjonalności jakie są obecnie wykorzystywane i nowy system też je musi posiadać:

- a. w przypadku blokady/unieważnienia konta użytkownika zainstalowany na komputerze suplikant natychmiastowo odłącza komputer od sieci (przełącza port przełącznika do zdefiniowanego vlanu gości),
- b. suplikant zainstalowany na komputerach posiada funkcję „Host Checker” – czyli kontroli parametrów komputera/rejestru/systemu plików/uruchamianych aplikacji i w przypadku wykrycia odstępstwa od zdefiniowanych reguł natychmiastowej blokady dostępu do sieci,
- c. suplikant zainstalowany na komputerach posiada obsługę automatycznego połączenia ze zdefiniowaną siecią wifi zgodnie z wcześniej zdefiniowanymi ustawieniami.

Dodatkowo dostarczony wraz z nowym systemem suplikant zainstalowany na komputerach/laptopach musi obsługiwać posiadany przez Zamawiającego system zdalnego dostępu SSL VPN oparty o produkt PulseSecure MAG 2600 w wersji 8.1R9.1.

### **II Wdrożenie:**

W ramach migracji starego systemu do nowego (dostarczonego w ramach tego zamówienia) należy wykonać wszelkie niezbędne prace wdrożeniowe, przeniesienie konfiguracji urządzeń ze starego systemu do nowego oraz konfigurację automatycznej dystrybucji suplikantów na komputery użytkowników (np. z wykorzystaniem Microsoft AD). Wszystkie prace związane z wdrożeniem i konfiguracją dostarczonego systemu muszą zostać zakończone w jednym oknie serwisowym tj. jeśli okno serwisowe zostanie zaplanowane w terminie od piątku do niedzieli, to w poniedziałek wszystkie urządzenia jakie autoryzowane były w sieci z wykorzystaniem starego systemu kontroli dostępu komputerów urządzeń i użytkowników muszą poprawnie autoryzować się z wykorzystaniem nowego systemu (ewentualnie jeśli migracja się nie uda to musi być możliwość autoryzowania użytkowników za pomocą starego systemu).

### **III Gwarancja:**

## Szczegółowy opis przedmiotu zamówienia

1. gwarancja producenta oferowanego systemu kontroli dostępu komputerów, urządzeń i użytkowników do sieci min. 24 miesiące od daty podpisania protokołu odbioru w miejscu instalacji urządzeń,
2. możliwość zgłaszania usterki/awarii systemu kontroli dostępu komputerów, urządzeń i użytkowników do sieci 24h 7 dni w tygodniu,
3. usunięcie usterki/awarii systemu kontroli dostępu komputerów, urządzeń i użytkowników do sieci 24h od chwili zgłoszenia awarii,
4. wykonanie aktualizacji oprogramowania układowego, suplikanta lub innego oprogramowania wchodzącego w skład systemu kontroli dostępu komputerów, urządzeń i użytkowników do sieci w przypadku zaleceń producenta oferowanego systemu,
5. cała obsługa serwisu gwarancyjnego musi odbywać się w języku polskim,
6. wsparcie techniczne w okresie gwarancyjnym świadczone telefonicznie oraz pocztą elektroniczną przez producenta lub polskiego partnera serwisowego producenta, obejmujące wymianę uszkodzonego urządzenia, bieżącą pomoc w konfiguracji systemu, dostęp do nowych wersji oprogramowania systemu, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

**IV Miejsce instalacji:**

1. Kraków, ul. Józefa 21.
2. Kraków, ul. Racławicka 56a.

**V Opis systemu równoważnego**

## PSA5000 – licencja POLSEC i PROFIER-RADIUS-SERVER

1. Urządzenie musi być oparte o dedykowaną platformę sprzętową oraz zapewniać obsługę co najmniej 1 000 jednoczesnych użytkowników z możliwością rozbudowy do 10 000 użytkowników.
2. Urządzenie musi posiadać min 2 porty 1 GbE.
3. Urządzenie musi posiadać dedykowany port zarządzający 1 GbE.
4. Urządzenie musi posiadać przepustowości 1 Gb/s.
5. Urządzenie musi być wyposażone w dysk twardy o pojemności min 500 GB.
6. Urządzenie musi mieć możliwość montażu w szafie 19”, a jego wysokość nie może być większa niż 1U.
7. Rozwiązanie musi umożliwiać tworzenie i wymuszanie szczegółowych polityk kontroli dostępu użytkowników do zasobów sieciowych. Polityki mogą być tworzone minimum w oparciu o tożsamość użytkownika, stan bezpieczeństwa jego urządzenia dostępowego, lokalizację sieciową lub dowolną kombinację powyższych kryteriów.
8. Wymuszanie polityk dostępu do sieci musi być możliwe w warstwie 2 modelu ISO/OSI z wykorzystaniem standardu 802.1X w celu zapewnienia funkcji NAC (ang. Network Access Control) w sieci oraz w warstwie 3 modelu ISO/OSI w celu zapewnienia kontroli dostępu na poziomie zasobu.
9. Urządzenie musi umożliwiać budowanie infrastruktury NAC we współpracy z rozwiązaniami sieciowymi dowolnego dostawcy spełniającymi standard 802.1x/EAP,
10. Urządzenie musi umożliwiać uwierzytelnienie przy pomocy adresu MAC dla 2000 jednocześnie podłączonych urządzeń.

## Szczegółowy opis przedmiotu zamówienia

11. Urządzenie musi zawierać wbudowany serwer RADIUS umożliwiający uwierzytelnienie w warstwie 2 modelu ISO/OSI w oparciu o standard 802.1x bez konieczności stosowania rozwiązań trzecich dla 10 000 jednocześnie podłączonych urządzeń.
12. Urządzenie musi posiadać możliwość wykrywania typu urządzenia użytkownika i wykorzystania tej informacji przy przypisaniu polityki dostępu.
13. Urządzenie musi umożliwiać autentykację użytkowników w oparciu o:
  - a. serwery RADIUS,
  - b. usługi katalogowe LDAP, Microsoft Active Directory, Novell NDS/eDirectory,
  - c. lokalną bazę użytkowników – zdefiniowanych w urządzeniu,
  - d. system RSA SecurID,
  - e. certyfikaty X.509.
14. Urządzenie musi umożliwiać uwierzytelnienie dwuskładnikowe (hasło statyczne plus certyfikat, hasło dynamiczne plus certyfikat). Musi istnieć możliwość rozdzielania serwera autentykacji użytkowników od serwera autoryzacji dostępu do zasobów.
15. System musi umożliwiać szczegółową weryfikację stanu bezpieczeństwa urządzeń z których użytkownik uzyskuje dostęp do zasobów. Musi istnieć możliwość:
  - a. sprawdzenia obecności konkretnego procesu, pliku, wpisu w rejestrze Windows,
  - b. sprawdzenia czy włączono odpowiednie usługi zabezpieczeń zarówno w momencie logowania jak w trakcie trwania sesji,
  - c. integracji z systemami weryfikacji stanu bezpieczeństwa firm trzecich.
16. Urządzenie musi umożliwiać budowanie konfiguracji odpornych na awarię w trybie Aktywny/Aktywny oraz Aktywny/Pasywny.
17. System zarządzający urządzeniami musi umożliwiać spójne zarządzanie z jednej konsoli administracyjnej wieloma urządzeniami w przypadku budowania konfiguracji nadmiarowych.
18. Urządzenie musi być zarządzane poprzez przeglądarkę Web.
19. Urządzenie musi umożliwiać wykonywanie kopii zapasowych konfiguracji lokalnie lub na zewnętrznym serwerze FTP oraz SCP.
20. Urządzenie musi umożliwiać integrację z zewnętrznymi serwerami SNMP v.2 oraz SYSLOG.
21. Urządzenie musi przechowywać dwie wersje oprogramowania oraz umożliwiać reset do wersji fabrycznej.

Na wykonawcy ciąży obowiązek wykazania równoważności oferowanego rozwiązania równoważnego.