Szczegółowy opis przedmiotu zamówienia

Przedmiotem zamówienia jest:

- dostawa dwóch urządzeń PulseSecure PSA3000 lub równoważnych wraz z licencjami, zwanych łącznie „systemem”,
- migracja posiadanego przez Zamawiającego systemu zdalnego dostępu użytkowników do sieci opartego o klaster urządzeń Juniper MAG-2600 do nowej wersji systemu opartego dostarczone urządzenia PulseSecure PSA3000 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 8.3.R7.

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

1. jednoczesna minimalna ilość równoczesnych użytkowników mogących się podłączyć do systemu poprzez tunel VPN: 50,
2. jednoczesna minimalna ilość równoczesnych użytkowników korzystających z funkcjonalności spotkań wirtualnych (Pulse Colaboration meetings): 50.
3. W przypadku awarii jednego z urządzeń w klastrze, drugie urządzenie musi utrzymywać wymaganą liczbę licencji przez przynajmniej 5 dni.

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

a. autoryzacja z wykorzystaniem certyfikatu stacji komputerowej użytkownika łączącego się poprzez VPN,
b. Klient VPN zainstalowany na komputerach posiada funkcję „Host Checker” – kontrola parametrów komputera/rejestru/uruchamianych aplikacji i w przypadku wykrycia odstępstwa od zdefiniowanych reguł uniemożliwienie zdalnego logowania,
c. Automatyczne połączenie klienta VPN do systemu VPN zależnie od wykrytej lokalizacji, zgodnie z wcześniej zdefiniowanymi regułami.

**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. Wszystkie prace związane z wdrożeniem i konfiguracją dostarczonego systemu muszą zostać zakończone w jednym oknie serwisowym tj. jeśli okno serwisowe zostanie zaplanowanie w terminie od piątku do niedzieli, to w poniedziałek wszyscy użytkownicy wykorzystujący system do połączenia do sieci muszą poprawnie autoryzować się z wykorzystaniem nowego systemu (ewentualnie jeśli migracja się nie uda to musi być możliwość autoryzowania użytkowników za pomocą starego systemu).

W ramach wdrożenia należy dokonać przeglądu konfiguracji w posiadanym przez Zamawiającego systemie SIEM Splunk, dotyczącej części SSLVPN i jeśli będzie to niezbędne zmodyfikować ją lub stworzyć na nowo aby było możliwe przeglądanie zdarzeń z nowego systemu. Należy przyjąć iż Zamawiający wykorzystuje nie więcej niż 5 raportów i 2 dashbordy prezentujące informacje z obecnego systemu VPN

**III Gwarancja:**

1. gwarancja producenta oferowanego systemu VPN dostępu użytkowników do sieci min. 36 miesięcy od daty podpisania protokołu odbioru w miejscu instalacji urządzeń,
2. możliwość zgłaszania usterki/awarii systemu VPN dostępu użytkowników do sieci 24h 7 dni w tygodniu,
3. usunięcie usterki/awarii systemu VPN dostępu użytkowników do sieci 24h od chwili zgłoszenia awarii,
4. wykonanie aktualizacji oprogramowania układowego, suplikanta lub innego oprogramowania wchodzącego w skład systemu VPN dostępu 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**

PSA3000 – licencja POLSEC i COLABORATION

1. Urządzenie musi być oparte o dedykowaną platformę sprzętową oraz zapewniać obsługę co najmniej 50 jednoczesnych użytkowników zarówno dla funkcjonalności VPN jak i dla funkcjonalności spotkań wirtualnych z możliwością rozbudowy do minimum 200 użytkowników.
2. Urządzenie musi posiadać min 3 porty 1 GbE.
3. Urządzenie musi posiadać dedykowany port zarządzający 1 GbE.
4. Urządzenie musi posiadać przepustowość minimum 200 Mbps.
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. System musi umożliwiać tworzenie i wymuszanie szczegółowych polityk dostępu użytkowników VPN 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. System 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.
   f. hasła jednorazowe generowane w oparciu o algorytm TOTP (Time-based One-time Password Algorithm)

9. Urządzenie musi umożliwiać uwierzytelnienie dwuskładnikowe (hasło statyczne plus certyfikat, hasło dynamiczne plus certyfikat). Musi istnieć możliwość rozdzielenia serwera autentykacji użytkowników od serwera autoryzacji dostępu do zasobów.
10. 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.
11. Urządzenie musi umożliwiać budowanie konfiguracji odpornych na awarię w trybie Aktywny/Aktywny oraz Aktywny/Pasywny.
12. System zarządzający urządzeniami musi umożliwiać spójne zarządzanie z jednej konsoli administracyjnej wieloma urządzeniami w przypadku budowania konfiguracji nadmiarowych.
13. System musi być zarządzane poprzez przeglądarkę Web.
14. System musi umożliwiać wykonywanie kopii zapasowych konfiguracji lokalnie lub na zewnętrznym serwerze FTP oraz SCP.
15. Urządzenie musi umożliwiać integrację z zewnętrznymi serwerami SNMP v.2 oraz SYSLOG.
16. Urządzenie musi przechowywać dwie wersje oprogramowania oraz umożliwiać reset do wersji fabrycznej.

Na wykonawcy ciąży obowiązek wykazania równoważności oferowanego rozwiązania równoważnego.