Zapytanie ofertowe

Agencja Oceny Technologii Medycznych i Taryfikacji z siedzibą w Warszawie przy ul. Przeskok 2, zaprasza potencjalnych Wykonawców do złożenia oferty w zakresie dostawy rozwiązania kontroli dostępu do sieci tzw. NAC (Network Access Control) oraz 2 szt. przełączników sieciowych wraz z wsparciem technicznym, niezbędnymi usługami informatycznymi w zakresie wdrożenia.

Opis Przedmiotu Zamówienia:

Rozwiązanie kontroli dostępu do sieci (NAC):

1. Przedmiotem niniejszego zamówienia jest dostawa rozwiązania kontroli dostępu do sieci NAC (Network Access Control) wraz z wdrożeniem i gwarancją.
2. Ze względu na uzyskanie jednorodności technicznej, technologicznej i zarządzającej, Zamawiający wymaga, aby dostarczone rozwiązanie miało możliwość zarządzania oraz w pełni współpracowało z przełącznikami już posiadanymi przez Zamawiającego tj. Cisco Catalyst 2960-X, Cisco Catalyst 2960-S, Cisco C3850 48, Cisco Nexus 93180YC-FX3, Cisco Catalyst 9200L 48, Cisco Nexus 3064-X
3. Zamawiający wymaga, aby zaoferowane rozwiązanie było dostępne oraz nie było przez niego przewidziane do wycofania ze sprzedaży i wsparcia (brak na listach End-of-Sale lub End-of-Life lub równoważne) – na dzień składania oferty.
4. Dostarczony system musi być legalny, pochodzący z legalnego kanału dystrybucyjnego, dopuszczony do obrotu na terenie Unii Europejskiej,
5. Dostarczane oprogramowanie musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw.
6. System musi posiadać gwarancję Producenta udzieloną na okres minimum 36 miesięcy. Gwarancja musi zawierać w sobie możliwość automatycznej i ręcznej aktualizacji oprogramowania oraz sygnatur.
7. Zamawiający wymaga, aby zaoferowany system był uznanym rozwiązaniem na Świecie. Producent zaoferowanego systemu musi występować w rankingu Gartnera dla systemów kontroli dostępu do sieci na stronie internetowej: https://www.gartner.com/reviews/market/network-access-controli posiadać tam minimum 200 recenzji ze średnią oceną co najmniej 4.2 Jako równoważny dla rankingu Gartnera Zamawiający dopuści również inny raport udostępniany publicznie, powszechnie akceptowany, mający charakter zewnętrznego i obiektywnego raportu rynkowego dotyczącego rozwiązań Network Access Control (NAC), który zapewnia analizę, wgląd w kierunek oraz dojrzałość uczestników i jest udostępniany przez podmiot publikujący badania i raporty dla rynku IT przez co najmniej ostatnich 10 lat.
8. System musi składać się z co najmniej dwóch maszyn wirtualnych.
9. System musi zostać dostarczony w formie w formie wirtualnej umożliwiającej instalacje na środowisku vSphere min w wersji 6.7.
10. System umożliwia realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, między innymi dla systemów:
    a. Microsoft Windows 10, Windows 8.1, Windows 8, Windows 7,
    b. Apple Mac OS X 10.x oraz 11.x,
    c. Apple iOS 11.x, 12.x, 13.x i nowszych,
    d. Google Android dla wersji 7.x i nowszych,
    e. Linux.
11. System umożliwia dodawanie kont gościnnych przez wybrane osoby (sponsor).
12. System zapewnia uwierzytelnienie sponsora które musi odbywać sekwencyjnie się w oparciu o wewnętrzną bazę użytkowników oraz zewnętrzne repozytorium użytkowników.

13. System umożliwia konfigurację uprawnień sponsora, w tym uprawnienia do:
    a. logowania się do systemu
    b. tworzenia pojedynczego konta gościnnego
    c. tworzenia wielu kont gościnnych
    d. importowania kont gościnnych z pliku CSV
    e. wysyłania wiadomości email po utworzeniu konta gościnnego
    f. wysyłania wiadomości SMS po utworzeniu konta gościnnego
    g. wyświetlenia hasła konta gościnnego
    h. wydrukowania danych konta gościnnego
    i. wyświetlenia danych stworzonych kont gościnnych
    j. zawieszenia (suspend) i reinicjacji kont gościnnych
14. System umożliwiać personalizację wyglądu portalu sponsora i gościa, w tym:
    a. zmianę logo strony logowania,
    b. zmianę obrazu tła strony logowania,
    c. zmianę logo bannera,
    d. zmianę obrazu tła bannera,
    e. zmianę koloru tła strony z treścią.
15. System umożliwia zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP i portu HTTPS
16. System umożliwia zmianę adresu URL i FQDN strony sponsora.
17. System 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
18. System posiada wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim, angielskim, francuskim, niemieckim i hiszpańskim
19. System umożliwia stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim.
20. System umożliwia wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora:
    a. imienia,
    b. nazwiska,
    c. firmy,
    d. adresu e-mail,
    e. numeru telefonu,
    f. danych opcjonalnych.
21. System umożliwia konfigurację dla użytkowników gościnnych:
    a. wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP)
    b. zezwolenia gościom na zmianę hasła oraz odzyskiwanie zapomnianego hasła,
    c. samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora.
22. System umożliwia honorowanie ustawień językowych przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego.
23. System umożliwia konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego.
24. System umożliwia konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługuje co najmniej 20 urządzeń per konto gościnne.
25. System umożliwia konfigurację czasu ważności hasła w dniach w przedziale zadanym w dniach.
26. System umożliwia określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny.

27. System umożliwia konfigurację polityki złożoności haseł użytkowników gościnnych.
28. System umożliwia konfigurację polityki nazwy (login) użytkownika gościnnego w tym co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika.
29. System 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.
30. System umożliwia przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsu IP, portu HTTPS i certyfikatu SSL dla FQDN.
31. System umożliwia udostępnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP, secure SMTP i poprzez SMS.
32. System umożliwia wykorzystanie protokołu SAML 2.0 oraz funkcjonalności SSO dla portali gościnnych oraz sponsora.
33. System wspiera API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych.
34. System musi posiadać wbudowany serwer RADIUS
35. System musi posiadać wbudowany serwer TACACS+ (nie jest wymagane dostarczenie licencji na uruchomienie tej funkcjonalności).
36. System musi umożliwiać bezpośrednią integrację z LDAP oraz Active Directory.
37. System umożliwia uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
38. System umożliwia uwierzytelnianie administratorów za pomocą zewnętrznych repozytoriów - m.in. Active Directory, Radius i SAML 2.0.
39. System musi umożliwiać automatyczną autoryzację urządzeń i użytkowników domenowych.
40. System musi wspierać obsługę protokołu 802.1x
41. Zamawiający przewiduje, że rozwiązanie będzie zarządzać 400 urządzeniami w infrastrukturze.
42. Okres ważności rozwiązania w tym niezbędnych licencji to min. 36 miesięcy.
43. Gwarancja, przez okres min. 36 miesięcy (w zależności od oferty) od daty odbioru bez zastrzeżeń, potwierdzonego protokołem.
44. W ramach gwarancji musi być zapewniona możliwość zgłaszania i komunikacji przez: stronę internetową, email oraz telefonicznie w języku polskim lub angielskim - wsparcie przy rozwiązywaniu problemów związanych z działaniem systemu NAC oraz systemów wspomagających w trybie 8x5, tj. co najmniej 8 godzin, przez 5 dni w tygodniu.
45. Czas reakcji na zgłoszony drogą mailową lub telefoniczną problem – maks. 60 minut, liczony w godzinach przyjmowania zgłoszeń.
46. Przy wystąpieniu awarii systemu, któregokolwiek z jego komponentów – naprawa w terminie do 8 godzin roboczych od daty diagnozy. Naprawa świadczona zdalnie lub w miejscu instalacji systemu.
47. Dostęp (tj. uprawnienie do pobierania i instalowania) do wszystkich aktualizacji dotyczących oferowanego systemu NAC oraz wszystkich systemów wspomagających w ramach wymaganych funkcjonalności, wydawanych przez Producenta.
48. Dostęp do bazy wiedzy oraz dokumentacji producenta dotyczących instalacji, konfiguracji i utrzymania - w języku polskim lub angielskim.
49. W ramach gwarancji muszą być także zapewnione wszystkie dostępne aktualizacje oprogramowania.

Przełączniki sieciowe. Specyfikacja dotyczy 1 urządzenia. Są to wymagania minimalne:

1. Przełącznik musi być wyposażony w min. 48 portów 10/100/1000 oraz min. 4 porty SFP/SFP+.
2. Porty SFP/SFP+ muszą umożliwiać ich obsadzenie modułami 10GBase-SR, 10GBase-LR.

3. Urządzenie musi obsługiwać minimum 4000 sieci VLAN i 16000 adresów MAC.
4. Przełącznik musi dysponować mocą PoE/PoE+ na poziomie 370W (przy zainstalowanym jednym zasilaczu)
5. Urządzenie musi mieć możliwość montażu w szafie 19", a jego wysokość nie może być większa niż 1 U.
6. Wydajność przełączania (switching capacity) musi wynosić minimum 150 Gbps.
7. Urządzenie musi posiadać możliwość łączenia w stosy z zachowaniem następującej funkcjonalności:
    a. obsługa min. 4 jednostek w stosie;
    b. magistrala stakująca o wydajności co najmniej 80 Gb/s;
    c. możliwość tworzenia połączeń cross-stack link aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad;
    d. zarządzanie poprzez jeden adres IP;
    e. stos widoczny jako jeden node dla procesu spanning-tree.

W celu uzyskania tej funkcjonalności dopuszcza się konieczność doposażenia urządzenia w dodatkowy, opcjonalny moduł.

8. Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości 9198 bajtów.
9. Obsługa protokołu NTP.
10. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.ls Multi-Instance Spanning Tree.
11. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
12. Urządzenie musi zapewniać możliwość routingu statycznego i dynamicznego dla IPv4 (OSPF) oraz funkcjonalności Policy-based routingu. Urządzenie musi mieć możliwość zapewnienia wsparcie dla zaawansowanych protokołów routingu IPv4 (OSPF, ISIS) i IPv6 (OPSFv3), routingu multicast (PIM-SM, PIM-SSM) poprzez wgranie odpowiedniej licencji.
13. Przełącznik musi obsługiwać następujące mechanizmy bezpieczeństwa:
    a. wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level);
    b. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL;
    c. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC;
    d. możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X (bez konieczności stosowania zewnętrznego serwera www).
14. Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC oraz uwierzytelniania w oparciu o www.
15. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie.
16. Wsparcie dla standardu IEEE 802.1ae (MACsec).
17. Wsparcie dla mechanizmów zabezpieczenia CoPP.
18. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176.
19. Możliwość uzyskania dostępu do urządzenia przez SNMPv2 oraz SNMPv3, SSHv2 z obsługą certyfikatów typu self-signed.
20. Obsługa list kontroli dostępu (ACL), mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard. Wymagane jest, aby listy ACL posiadały domyślny wpis „blokuj" dla ostatniego, niewidocznego wpisu w ACL.
21. Funkcjonalność Protected Port.

22. Przełącznik musi wspierać mechanizmy QoS związane z zapewnieniem jakości usług w sieci.
23. Wsparcie dla automatyzacji zadań, np. Embedded Event Manager (EEM), Python.
24. Obsługa protokołu CDP lub LLDP.
25. Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli.
26. Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN).
27. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 4 plików konfiguracyjnych.
28. Oferowany przełącznik musi być wyposażony w zasilacz podstawowy i redundantny o mocy minimum 600W.
29. Wraz z urządzeniem muszą być dostarczone licencje umożliwiające uruchomienie Flexible NetFlow (lub równoważnej).
30. Zaoferowane przełączniki muszą być dostarczone z serwisem 36 miesięcznym liczonym od dnia podpisania bez uwag protokołu odbioru Urządzeń, działającym w trybie 8x5 oraz z możliwością bezpośredniego pobrania z serwisu producenta wszystkich aktualizacji oprogramowania.

Wykonawca w ramach realizacji zamówienia:

1. Dostarczy system oraz urządzenia sieciowe na własny koszt oraz zamontuje, skonfiguruje i uruchomi w lokalizacji Zamawiającego (Warszawa).
2. Skonfiguruje system do pracy produkcyjnej wykonując m.in. konfigurację wstępną.
3. W przypadku, gdy zaoferowany przez Wykonawcę system nie będzie współdziałać ze środowiskiem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy tego środowiska, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem środowiska Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie tego środowiska.
4. Konfigurację autentykacji z wykorzystaniem protokołu 802.1x wraz z integracją Active Directory
5. Konfigurację systemu w celu umożliwienia integracji z systemem monitorowania Zamawiającego – Zabbix ver. 6.0 LTS.
6. Wykonawca sporządzi dokumentację powykonawczą, którą przekaże Zamawiającemu, zawierającą minimum:
    a. Schemat i opis podłączenia systemu w infrastrukturze Zamawiającego.
    b. Opis konfiguracji wszystkich parametrów systemu.
    c. Instrukcję wykonywania i przywracania kopii zapasowej konfiguracji systemu.
    d. Instrukcję wgrywania nowszych wersji oprogramowania przy zachowaniu ciągłości działania.
7. Dokona instruktażu stanowiskowego dla minimum 2 osób co najmniej w zakresie:
    a. Administrowania konfiguracją systemu (konfiguracja, update, logowanie)
    b. Szczegółowego administrowania systemem kontroli dostępu obejmującego wszystkie parametry systemu.
8. Wymaga się aby technik realizujący wdrożenie posiadał autoryzację producenta z zakresu administrowania wdrażanym rozwiązaniem na poziomie wymaganym do realizacji elementów wdrożenia.

Kryteria oceny ofert:
- 100% cena

Sposób złożenia oferty:

Ofertę należy przesłać w wersji elektronicznej wraz z wypełnionym formularzem ofertowym podając cenę netto i brutto (do formularza ofertowego należy dołączyć załącznik z wyszczególnionymi cenami poszczególnych komponentów) na adres mailowy: zp@aotm.gov.pl, w terminie do **05 lipca 2024 roku** do końca dnia.

W przypadku pytań, prosimy o kontakt:
a) Łukasz Bieńkowski – w zakresie merytorycznych zagadnień dotyczących przedmiotu zamówienia l.bienkowski@aotm.gov.pl, tel. 887 83 06 83;

b) Paweł Kosowski – w zakresie merytorycznych zagadnień dotyczących przedmiotu zamówienia p.kosowski@aotm.gov.pl;

c) Dawid Załęcki – w zakresie procedury udzielenia zamówienia publicznego oraz warunków realizacji umowy;
d.zalecki@aotm.gov.pl : tel. 727 787 388.

1.Niniejsze postępowanie o udzielenie zamówienia publicznego jest prowadzone w trybie zapytania ofertowego na podstawie regulaminu udzielania zamówień Agencji oraz przepisów Kodeksu Cywilnego, dalej: KC z wyłączeniem stosowania przepisów ustawy Prawo Zamówień Publicznych, dalej: Pzp.
2.W zakresie nieuregulowanym w niniejszym zapytaniu, mają zastosowanie przepisy ustawy KC.
3.Zamawiający ma prawo unieważnić niniejsze zapytanie ofertowe w każdym czasie bez podawania przyczyny. W takim przypadku Wykonawcy zostaną poinformowani o zamknięciu postępowania bez dokonania wyboru oferty najkorzystniejszej.
4.Postępowanie prowadzone jest w języku polskim. Wszelka korespondencja z Wykonawcami winna być prowadzona w języku polskim.
5.Zamawiającym jest: Agencja Oceny Technologii Medycznych i Taryfikacji, ul. Przeskok 2, 00-032 Warszawa.