Załącznik nr 3 do SWZ

Numer referencyjny postępowania:
SZP/DIT/32/2023

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA
NA ZADANIE: „DOSTAWA SYSTEMU UWIERZYTELNIENIA DOSTĘPU DO SIECI LAN/WLAN/VPN”

Przedmiotem zamówienia jest „**Dostawa systemu uwierzytelnienia dostępu do sieci LAN/WLAN/VPN”**

System powinien zostać dostarczony w formie 2 maszyn wirtualnych wraz z odpowiednimi licencjami umożliwiającymi wykorzystanie wszystkich funkcjonalności opisanych w niniejszym dokumencie dla 500 sesji.

System powinien zapewniać pełne zarządzanie cyklem życiowym dostępu do zasobów sieciowych, niezależnie od miejsca uzyskiwanego dostępu. System powinien realizować wsparcie dla dostępu gościnnego w sieci, identyfikację stacji, rejestrację urządzeń. System powinien obejmować kontrolą dostęp wszystkich urządzeń podłączonych do sieci IP w tym terminali, komputerów PC, smartfonów i tabletów, telefonii IP, terminali video i innych podłączonych urządzeń.

I. PODSTAWOWE CECHY SYSTEMU

1. System powinien umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych.
2. System powinien umożliwiać elastyczną rozbudowę poprzez dodawanie licencji dla podstawowych
   i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych.
3. System powinien umożliwiać wysoką skalowalność i rozbudowę w miarę wzrostu liczby urządzeń.
4. System powinien umożliwiać instalację na maszynie wirtualnej (VM) i maszynie fizycznej, w tym na:
   4.1. VMware wersji 8 dla ESXi 5.1 U2
   4.2. VMware wersji 11 dla ESXi 6.x
   4.3. WMware Cloud w AWS
   4.4. Azure VMware Solution
   4.5. hypervisorze KVM na Red Hat Enterprise Linux (RHEL)
   4.6. Microsoft Hyper-V
   4.7. AWS EC2
      4.7.1. serwerach fizycznych wspieranych przez producenta
5. System powinien umożliwiać wydzielenie określonych elementów funkcjonalnych, instalowanych jako oddzielne maszyny fizyczne lub wirtualne, w tym:
   5.1. Wydzielenie podsystemu zarządzania (Administration), umożliwiającego administratorowi dostęp do interfejsu graficznego (GUI) za pomocą przeglądarki web i zmianę konfiguracji systemu oraz jego monitorowanie

tel. (61) 8310-142; 8310-242
email: zamowienia.publiczne@orsk.pl

5.2. Wydzielenie podsystemu monitoringu, logowania i rozwiązywania problemów, umożliwiającego gromadzenie wiadomości logowania z:
  5.2.1. Przełączników dostępowych
    5.2.1.1. sesji uwierzytelniania 802.1X
    5.2.1.2. zdarzeń kontroli dostępu (autoryzacji)
    5.2.1.3. zdarzeń związanych z błędami
    5.2.1.4. zdarzeń związanych z alarmami systemowymi
  5.2.2. Wydzielenie serwerów usługowych realizujących funkcje:
    5.2.2.1. serwera RADIUS dla infrastruktury sieciowej
    5.2.2.2. serwera polityk uwierzytelniania i kontroli dostępu 802.1X
    5.2.2.3. serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego
    5.2.2.4. serwera profilowania stacji końcowych
5.3. System powinien umożliwiać realizację wysokiej dostępności elementów funkcjonalnych,
  w tym:
  5.3.1. zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu
  5.3.2. zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych
5.4. System powinien umożliwiać 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.
5.5. System powinien umożliwiać zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).
5.6. System powinien umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled).
5.7. System powinien umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
5.8. System powinien umożliwiać uwierzytelnianie administratorów za pomocą zewnętrznych repozytoriów - m.in. Active Directory, Radius i SAML 2.0.
5.9. System powinien umożliwiać wymuszenie reguł złożoności haseł dla administratorów, w tym co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. System wymusza hasło różne od trzech poprzednich haseł i jego zmianę co określoną ilość dni
5.10. System powinien umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:
  5.10.1. dostęp do interfejsu konfiguracji usług tożsamości 802.1X
  5.10.2. dostęp do interfejsu konfiguracji urządzeń sieciowych
  5.10.3. dostęp do interfejsu konfiguracji polityk
  5.10.4. dostęp do interfejsu konfiguracji kontroli dostępu gościnnego
  5.10.5. dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania
5.11. System powinien umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.
5.12. System powinien posiadać możliwość podłączenia i identyfikacji urządzenia końcowego z wykorzystaniem MUD (Manufacturer Usage Description) zgodnie ze standardem IETF i RFC8520.
5.13. System powinien wspierać REST API do masowych operacji CRUD (Create, Read, Update, Delete) m.in. na użytkownikach, stacjach końcowych oraz urządzeniach sieciowych.

tel. (61) 8310-142; 8310-242
email: zamowienia.publiczne@orsk.pl

5.14. System powinien wspierać REST API do monitorowania w czasie rzeczywistym sesji oraz stacji końcowych.
5.15. System powinien wspierać REST API do konfiguracji i zarządzania m.in. politykami Radius, kopiami zapasowymi oraz repozytoriami plików.
5.16. System powinien umożliwiać rozbudowanie funkcjonalności o m.in. profilowanie urządzeń oraz weryfikację stanu stacji końcowej– z ang. posture assessment, bez konieczności rozbudowy sprzętowej.
5.17. System powinien umożliwiać rozbudowanie funkcjonalności o serwer TACACS+ do administrowania urządzeniami sieciowymi bez konieczności rozbudowy sprzętowej.

II. MECHANIZM UWIERZYTELNIENIA 802.1x

1. System powinien wspierać następujące protokoły uwierzytelniania i standardy:
   1.1. RADIUS, zgodnie z dokumentami:
      1.1.1. RFC 2138 — Remote Authentication Dial In User Service (RADIUS)
      1.1.2. RFC 2139 — RADIUS Accounting
      1.1.3. RFC 2865 — Remote Authentication Dial In User Service (RADIUS)
      1.1.4. RFC 2866 — RADIUS Accounting
      1.1.5. RFC 2867 — RADIUS Accounting for Tunnel Protocol Support
      1.1.6. RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
      1.1.7. RFC 2869 — RADIUS Extensions
2. RADIUS Proxy dla zewnętrznego serwera RADIUS
3. System powinien wspierać protokół Windows Active Directory, w tym następujące repozytoria AD:
   3.1. Microsoft Windows Active Directory 2003 32bit
   3.2. Microsoft Windows Active Directory 2003 R2 32bit i 64bit
   3.3. Microsoft Windows Active Directory 2008 32bit i 64bit
   3.4. Microsoft Windows Active Directory 2008 R2 64bit
   3.5. Microsoft Windows Active Directory 2012
   3.6. Microsoft Windows Active Directory 2012 R2
   3.7. Microsoft Windows Active Directory 2016
   3.8. Microsoft Windows Active Directory 2019
   3.9. System wspiera protokół Lightweight Directory Access Protocol (LDAP)
4. System powinien wspierać protokół Security Assertion Markup Language (SAML) 2.0 oraz funkcjonalność Single Sign-On (SSO).
5. System powinien wspierać integrację z Azure Active Directory z użyciem technologii Oauth ROPC w celu uwierzytelnienia klientów 802.1x.
6. System powinien wspierać serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865
7. System powinien wspierać następujące protokoły uwierzytelniania:
   7.1. PAP/ASCII
   7.2. CHAP
   7.3. MS-CHAPv1
   7.4. MS-CHAPv2
   7.5. EAP-MD5
   7.6. LEAP
   7.7. EAP-TLS
   7.8. EAP-TTLS
   7.9. Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:
      7.9.1. EAP-MS-CHAPv2
      7.9.2. EAP-GTC

tel. (61) 8310-142; 8310-242
email: zamowienia.publiczne@orsk.pl

7.9.3. EAP-TLS
7.10. Tunnel Extensible Authentication Protocol (TEAP) z metodami wewnętrznymi:
7.10.1. EAP-MS-CHAPv2
7.10.2. EAP-TLS
8. System powinien umożliwiać konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect
9. System powinien wspierać implementację 802.1X z przynajmniej następującymi suplikantami:
9.1. wbudowanym klientem 802.1X dla Windows 10
9.2. wbudowanym klientem 802.1X dla Windows 7
9.3. wbudowanym klientem 802.1X dla Windows 8 i 8.1
9.4. Apple Mac OS X Supplicant
9.5. Apple iOS Supplicant
9.6. Google Android Supplicant
10. System powinien umożliwiać tworzenie polityk uwierzytelniania 802.1X opartych złożone o reguły (rule-based).
11. System powinien umożliwiać uwierzytelnianie 802.1X maszyn i użytkowników.
12. System powinien umożliwiać tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o reguły.
13. System powinien posiadać lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym)
14. System powinien posiadać lokalną bazę stacji końcowych. Lokalna baza stacji końcowych jest tworzona per stacja końcowa na podstawie unikalnego adresu MAC.
15. System powinien wspierać uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC
16. System powinien wspierać zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices), w tym:
16.1. tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host per port
16.2. tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia
16.3. Tryb uwierzytelniania 802.1X, w którym dozwolone jest jedno urządzenie telefonii IP w domenie głosowej (Voice VLAN) i jeden w host w domenie danych (Data VLAN) na jednym porcie fizycznym
16.4. tryb uwierzytelniania 802.1X dozwalający wiele hostów na jednym porcie fizycznym
16.5. mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny
16.6. mechanizm umożliwiający poprawną obsługę sytuacji, w której nowy host podłącza się do portu, na którym uprzednio było uwierzytelnione urządzenie w tym w VLANie głosowym.
16.7. mechanizm umożliwiający wysłanie informacji o reloadzie urządzenia (przełącznika) dostępowego do serwera AAA. Dzięki temu uwierzytelnione aktywne sesje związane z tym konkretnym urządzeniem zostaną usunięte z listy na serwerze AAA.
16.8. mechanizm przypisania VLANu w procesie uwierzytelnienia i kontroli dostępu 802.1X
16.9. mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1X
16.10. obsługa przypisania listy kontroli dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki

tel. (61) 8310-142; 8310-242
email: zamowienia.publiczne@orsk.pl

16.11. mechanizm 802.1x umożliwiający realizację dostępu gościnnego w dedykowanym VLANie (Guest VLAN) dla użytkowników gościnnych
16.12. mechanizm 802.1x umożliwiający przypisanie urządzenia telefonii IP do dedykowanego VLANu w sytuacji, gdy serwer AAA jest niedostępny
16.13. przypisanie przez serwer AAA dla użytkownika nie jednego, lecz grupy VLANów dla użytkownika, z których przełącznik wybiera jeden, w którym jest najmniej użytkowników
16.14. uwierzytelnienie 802.1X urządzenia telefonii IP znajdującego sie w VLANie głosowym
16.15. współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN
16.16. 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
16.17. możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznika

17. System powinien wspierać uwierzytelnianie nazwą użytkownika i hasłem przez portal web, jako jedną z metod uwierzytelniania do sieci, (dotyczy m.in. w sytuacji, gdy stacja ma niepoprawnie skonfigurowane lub niedziałające oprogramowanie suplikanta 802.1X)
18. System powinien wspierać m.in. następujące urządzenia sieciowe jako klientów RADIUS (NAD - Network Access Device):
    18.1. Przełączniki Ethernet. Lista wspieranych przełączników Cisco oraz producentów trzecich dostępna jest na stronach Cisco (wraz z wersjami oprogramowania).
    18.2. Kontrolery sieci bezprzewodowej. Lista wspieranych kontrolerów sieci bezprzewodowej Cisco oraz producentów trzecich dostępna jest na stronach Cisco (wraz z wersjami oprogramowania).
    18.3. Koncentratory VPN. Lista wspieranych koncentratorów VPN Cisco oraz producentów trzecich dostępna jest na stronach Cisco (wraz z wersjami oprogramowania).

III. REALIZACJA DOSTĘPU GOŚCINNEGO

1. System powinien umożliwiać realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, między innymi dla:
   1.1. Microsoft Windows 10, Windows 8.1, Windows 8, Windows 7
   1.2. Apple Mac OS X 10.x oraz 11.x
   1.3. Apple iOS 11.x, 12.x, 13.x i nowszych
   1.4. Google Android dla wersji 7.x i nowszych
   1.5. Linux
2. System powinien umożliwiać dodawanie kont gościnnych przez wybrane osoby (sponsor).
3. System powinien zapewniać uwierzytelnienie sponsora które musi odbywać sekwencyjnie się w oparciu o:
   3.1. wewnętrzną bazę użytkowników
   3.2. zewnętrzne repozytorium użytkowników
4. System powinien umożliwiać konfigurację uprawnień sponsora, w tym uprawnienia do:
   4.1. logowania się do systemu
   4.2. tworzenia pojedynczego konta gościnnego
   4.3. tworzenia wielu kont gościnnych
   4.4. importowania kont gościnnych z pliku CSV
   4.5. wysyłania wiadomości email po utworzeniu konta gościnnego
   4.6. wysyłania wiadomości SMS po utworzeniu konta gościnnego

4.7. wyświetlenia hasła konta gościnnego
4.8. wydrukowania danych konta gościnnego
4.9. wyświetlenia danych stworzonych kont gościnnych
4.10. zawieszenia (suspend) i reinicjacji kont gościnnych

5. System powinien umożliwiać personalizację wyglądu portalu sponsora i gościa, w tym:
   5.1. zmianę logo strony logowania
   5.2. zmianę obrazu tła strony logowania
   5.3. zmianę logo bannera
   5.4. zmianę obrazu tła bannera
   5.5. zmianę koloru tła strony z treścią
6. System powinien umożliwiać zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP i portu HTTPS
7. System powinien umożliwiać zmianę adresu URL i FQDN strony sponsora.
8. System powinien umożliwiać 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
9. System powinien posiadać wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim, angielskim, francuskim, niemieckim i hiszpańskim
10. System powinien umożliwiać stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim.
11. System powinien umożliwiać wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora:
    11.1. Imienia
    11.2. Nazwiska
    11.3. Firmy
    11.4. adresu e-mail
    11.5. numeru telefonu
    11.6. danych opcjonalnych (nie mniej niż 5 dodatkowych pól)
12. System powinien umożliwiać konfigurację dla użytkowników gościnnych:
    12.1. wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP)
    12.2. zezwolenia gościom na zmianę hasła oraz odzyskiwanie zapomnianego hasła,
    12.3. samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora
13. System powinien umożliwiać honorowanie ustawień locale przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego.
14. System powinien umożliwiać konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego.
15. System powinien umożliwiać konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługuje co najmniej 20 urządzeń per konto gościnne.
16. System powinien umożliwiać konfigurację czasu ważności hasła w dniach w przedziale zadanym w dniach.
17. System powinien umożliwiać określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny
18. System powinien umożliwiać konfigurację polityki złożoności haseł użytkowników gościnnych:
19. System powinien umożliwiać konfigurację polityki nazwy (login) użytkownika gościnnego w tym co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika

tel. (61) 8310-142; 8310-242
email: zamowienia.publiczne@orsk.pl

20. System powinien umożliwiać 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.
21. System powinien umożliwiać przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsu IP, portu HTTPS i certyfikatu SSL dla FQDN.
22. System powinien umożliwiać udostępnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP, secure SMTP i poprzez SMS,
23. System powinien umożliwiać wykorzystanie protokołu SAML 2.0 oraz funkcjonalności SSO dla portali gościnnych oraz sponsora.
24. System powinien wspierać API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych.

IV. RAPORTOWANIE

1. System powinien umożliwiać generowanie m.in. następujących raportów:
   - 1.1 Raportów dla protokołów AAA:
   - 1.2 Diagnostyki protokołów AAA
   - 1.3 Trendów uwierzytelnienia 802.1X
   - 1.4 Accountingu RADIUS
   - 1.5 Uwierzytelniania RADIUS
   - 1.6 Raportów dozwolonych protokołów
   - 1.7 Sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym:
     - 1.7.1 uwierzytelnień pomyślnych
     - 1.7.2 uwierzytelnień nieudanych
     - 1.7.3 „N" największych ilości uwierzytelnień RADIUS per protokół EAP (Top5), w tym:
       - 1.7.3.1 uwierzytelnień pomyślnych
       - 1.7.3.2 uwierzytelnień nieudanych
   - 1.8 Raportów dla poszczególnych instancji serwerów systemu, w tym:
     - 1.8.1 uwierzytelnień RADIUS per serwer
     - 1.8.2 Top „N" uwierzytelnień per serwer
     - 1.8.3 monitorowania Online Certificate Status Protocol (OCSP)
     - 1.8.4 administratorów systemu i ich uprawnień
     - 1.8.5 logowania administratorów do systemu
     - 1.8.6 zmian konfiguracji serwera dokonanych przez administratorów
     - 1.8.7 stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS)
     - 1.8.8 zmian operacyjnych serwera dokonanych przez administratorów
     - 1.8.9 zmian haseł przez użytkowników
   - 1.9 Raportów dla stacji końcowych, w tym:
     - 1.9.1 uwierzytelnień typu MAC Authentication
     - 1.9.2 Top „N" uwierzytelnień per adres MAC stacji
     - 1.9.3 Top „N" uwierzytelnień per maszyna
     - 1.9.4 Top „N" uwierzytelnień per RADIUS Calling Station ID
     - 1.9.5 działań podsystemu profilera per adres MAC
     - 1.9.6 czasu wymaganego na sprofilowanie stacji per adres MAC
   - 1.10 Raportów dla błędów, w tym:
     - 1.10.1 błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił
     - 1.10.2 sumarycznych przyczyn nieudanych uwierzytelnień
     - 1.10.3 Top „N" uwierzytelnień per rodzaj błędu
   - 1.11 Raportów dla urządzeń sieciowych:
     - 1.11.1 sumarycznych uwierzytelnień dla urządzeń sieciowych

tel. (61) 8310-142; 8310-242
email: zamowienia.publiczne@orsk.pl

1.11.2 Top „N” uwierzytelnień per urządzenie sieciowe
1.11.3 niedostępności serwera AAA dla urządzenia sieciowego
1.11.4 wiadomości logowanych przez urządzenia sieciowe
1.11.5 stanu portów i sesji urządzenia sieciowego widocznych przez SNMP

1.12 Raportów użytkowników:
1.12.1 sumarycznych uwierzytelnień użytkowników
1.12.2 Top „N”uwierzytelnień per użytkownik
1.12.3 sesji użytkowników gościnnych
1.12.4 aktywności użytkowników gościnnych
1.12.5 sumarycznych uwierzytelnień sponsorów dostępu gościnnego
1.12.6 uwierzytelnień per unikalny użytkownik

1.13 Raportów katalogu sesji
1.13.1 aktywnych sesji RADIUS
1.13.2 historii sesji RADIUS
1.13.3 zaterminowanych sesji RADIUS

V. ALARMY I DIAGNOSTYKA

1. System powinien umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą
   1.1. wiadomości e-mail
   1.2. syslog
2. Alarmy powinny być generowane w następujących sytuacjach:
   2.1. ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu
   2.2. opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego
   2.3. status krytycznych procesów będzie niepożądany, w tym status:
      2.3.1. procesu wewnętrznej bazy danych systemu
      2.3.2. serwera aplikacyjnego systemu
      2.3.3. bazy danych sesji
      2.3.4. kolektora i procesora wiadomości log
      2.3.5. błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej)
      2.3.6. stan obciążenia systemu wzrośnie powyżej zadanego poziomu, w tym:
         2.3.6.1. obciążenie systemu (load)
         2.3.6.2. zajętość pamięci
3. System powinien posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
   3.1. badanie łączności IP za pomocą ping, nslookup, traceroute
   3.2. wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
      3.2.1. nazwy użytkownika
      3.2.2. adresu MAC
      3.2.3. statusu uwierzytelnienia (udana lub nieudana)
      3.2.4. powodu, jeżeli uwierzytelnienie nieudane
      3.2.5. zakresu czasowego, co do dnia, godziny i minuty
   3.3. wykonanie zdalnego polecenia na urządzeniu sieciowym
   3.4. ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem:
      3.4.1. definicji serwerów AAA
      3.4.2. protokołu RADIUS
      3.4.3. odkrywania urządzeń
      3.4.4. logowania
      3.4.5. uwierzytelniania Web

tel. (61) 8310-142; 8310-242
email: zamowienia.publiczne@orsk.pl

3.4.6. konfiguracji trybu 802.1X

3.5. wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu

VI. WSPARCIE DLA PROTOKOŁU IPv6

1. System powinien posiadać wsparcie dla SSH IPv6
2. System powinien pozwalać na zarządzanie administracyjne za pomocą interfejsu graficznego udostępnionego administratorowi z wykorzystaniem adresacji IPv6
3. System powinien pozwalać na konfigurację NTP IPv6
4. System umożliwia stworzenie reguł ograniczających dostęp administracyjny do linii poleceń lub interfejsu graficznego w oparciu o adres IPv6
5. System powinien umożliwiać konfigurację serwerów SNMP w oparciu o adresację IPv6
6. System powinien umożliwiać wysyłanie SNMP Trap do serwera SNMP IPv6
7. System powinien umożliwiać integrację z Active Directory w oparciu o IPv6
8. System powinien umożliwiać połączenie z serwerem Radius z wykorzystaniem adresu IPv6

VII. DOBRE PRAKTYKI REALIZACJI ROZWIĄZANIA

1. System powinien spełniać następujące warunki dobrych praktyk realizacji systemu uwierzytelnienia dostępu do sieci
2. System powinien występować w formie pojedynczego rozwiązania jak też systemu złożonego z kilku komponentów.
3. W przypadku zastosowania rozwiązania złożonego z kilku komponentów system powinien zapewniać pojedynczy interfejs konfiguracyjny, zarządzający i monitorujący zapewniający możliwość wymuszenia spójnej polityki bezpieczeństwa dla dostępu LAN/WLAN/VPN.
4. Niezależnie od tego czy system występuje w formie pojedynczego rozwiązania lub jest złożony z kilku komponentów, powinien on być serwisowany jako jeden system w ramach pojedynczej usługi wsparcia.

VIII. GWARANCJA ORAZ WSPARCIE

Gwarancja: System powinien być objęty serwisem gwarancyjnym producenta przez oferowany okres miesięcy (min. 36 miesięcy), polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

tel. (61) 8310-142; 8310-242
email: zamowienia.publiczne@orsk.pl