System uwierzytelnienia dostępu do sieci LAN/WLAN/VPN
Liczba kompletów – 1 szt

1. System musi zostać dostarczona w formie maszyny wirtualnej pracującej w środowisku VMware ESXi.
2. System musi umożliwiać współpracę z urządzeniami wielu producentów, w tym co najmniej: Cisco, Juniper, HP, Brocade.
3. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji dla podstawowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych.
4. System musi umożliwiać obsługę co najmniej 1500 jednoczesnych sesji
5. System musi umożliwiać obsługę co najmniej 7000 jednoczesnych sesji w przypadku wzrostu liczby obsługiwanych urządzeń.
6. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych.
7. System musi umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego.
8. System musi umożliwiać zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).
9. System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych.
10. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
11. System musi umożliwiać wymuszenie reguł złożoności haseł dla administratorów.
12. System musi umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:
    a) dostęp do interfejsu konfiguracji usług tożsamości 802.1X
    b) dostęp do interfejsu konfiguracji urządzeń sieciowych
    c) dostęp do interfejsu konfiguracji polityk
    d) dostęp do interfejsu konfiguracji kontroli dostępu gościnnego
    e) dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania
13. System musi posiadać panel informacyjny, który można dostosować do potrzeb administratora poprzez wyświetlania widget-ów prezentujących co najmniej poniższe informacje:
    a) Utylizacja CPU
    b) Wykorzystanie pamięci systemu
    c) Typy oraz profile podłączonych urządzeń końcowych
    d) Typy urządzeń sieciowych
    e) Podsumowania profilowania urządzeń końcowych
    f) Systemy operacyjne urządzeń końcowych
    g) Status zalogowanych gości
14. System musi wspierać mechanizmy uwierzytelniania 802.1x i spełniać niżej wymienione wymagania:
    a. System wspiera następujące protokoły uwierzytelniania i standardy:
        i. RADIUS, zgodnie z dokumentami:
            1. RFC 2138 — Remote Authentication Dial In User Service (RADIUS)
            2. RFC 2139 — RADIUS Accounting
            3. RFC 2865 — Remote Authentication Dial In User Service (RADIUS)
            4. RFC 2866 — RADIUS Accounting
            5. RFC 2867 — RADIUS Accounting for Tunnel Protocol Support
            6. RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
            7. RFC 2869 — RADIUS Extensions
        ii. RADIUS Proxy dla zewnętrznego serwera RADIUS
    b. System wspiera protokół Windows Active Directory.
    c. System wspiera protokół Lightweight Directory Access Protocol (LDAP)
    d. System wspiera serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865
    e. System umożliwia integrację z bazą danych ODBC.
    f. System wspiera protokół SAMLv2, co umożliwia integrację z przynajmniej następującymi rozwiązaniami IdP:
        i. Oracle Access Manager (OAM)
        ii. Oracle Identity Federation (OIF)

iii. SecureAuth
iv. PingOne
v. PingFederate
vi. Azure Active Director

g. System wspiera następujące protokoły uwierzytelniania:
   i. PAP/ASCII
   ii. CHAP
   iii. MS-CHAPv1
   iv. MS-CHAPv2
   v. EAP-MD5
   vi. LEAP
   vii. EAP-TLS
   viii. Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:
      1. EAP-MS-CHAPv2
      2. EAP-GTC
      3. EAP-TLS

h. System umożliwia konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect
i. System wspiera implementację 802.1X z przynajmniej następującymi suplikantami:
   i. wbudowanym klientem 802.1X dla Windows 10
   ii. Apple Mac OS X Supplicant
j. System umożliwia tworzenie polityk uwierzytelniania 802.1X opartych złożone o reguły (rule-based).
k. System umożliwia uwierzytelnianie 802.1X maszyn i użytkowników.
l. System umożliwia tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o reguły.
m. System posiada lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym)
n. System posiada lokalną bazę stacji końcowych. Lokalna baza stacji końcowych jest tworzona per stacja końcowa na podstawie unikalnego adresu MAC.
o. System wspiera uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC
p. System wspiera zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices).
q. System wspiera 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).
r. System wspiera m.in. następujące urządzenia sieciowe, jako klientów RADIUS (NAD - Network Access Device):
   i. Przełączniki Ethernet. Lista wspieranych przełączników jest dostępna na stronie producenta (wraz z wersjami oprogramowania).
   ii. Kontrolery sieci bezprzewodowej. Lista wspieranych kontrolerów sieci bezprzewodowej dostępna jest na stronach producenta (wraz z wersjami oprogramowania).
   iii. Koncentratory VPN. Lista wspieranych koncentratorów dostępna jest na stronach producenta (wraz z wersjami oprogramowania).

15. System musi wspierać funkcjonalność serwera TACACS+ do administrowania urządzeniami sieciowymi. Jeśli funkcjonalność ta wymaga dodatkowej licencji, to Zamawiający nie wymaga jej dostarczenia w ramach postępowania.
16. System musi wspierać interfejs API.
17. System musi posiadać moduł umożliwiający realizację dostępu gościnnego, który spełnia niżej wymienione wymagania:
    a. system umożliwia realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową
    b. system umożliwia dodawanie kont gościnnych przez wybrane osoby (sponsor)
    c. system umożliwia samodzielną rejestrację klientów gościnnych
    d. system umożliwia realizację dostępu gościnnego poprzez logowanie w oparciu o portal społecznościowy

e. system umożliwia konfigurację uprawnień sponsora, w tym uprawnienia do:
   i. logowania się do systemu
   ii. tworzenia pojedynczego konta gościnnego
   iii. tworzenia wielu kont gościnnych
   iv. importowania kont gościnnych z pliku CSV
   v. wysyłania wiadomości email po utworzeniu konta gościnnego
   vi. wysyłania wiadomości SMS po utworzeniu konta gościnnego
   vii. wyświetlenia hasła konta gościnnego
   viii. wydrukowania danych konta gościnnego
   ix. wyświetlenia danych stworzonych kont gościnnych
   x. zawieszenia (suspend) i reinicjacji kont gościnnych
f. System umożliwia zaawansowaną personalizację wyglądu portalu sponsora i gościa, w tym m.in.:
   i. zmianę logo strony logowania
   ii. zmianę obrazu tła strony logowania
   iii. zmianę logo bannera
   iv. zmianę obrazu tła bannera
   v. zmianę koloru tła strony z treścią
g. System umożliwia zmianę adresu URL i FQDN strony sponsora.
h. 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
i. System posiada wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim, angielskim, francuskim, niemieckim i hiszpańskim
j. System umożliwia stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim.
k. System umożliwia wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora:
   i. Imienia
   ii. Nazwiska
   iii. Firmy
   iv. adresu e-mail
   v. numeru telefonu
   vi. danych opcjonalnych
l. System umożliwia konfigurację dla użytkowników gościnnych:
   i. wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP)
   ii. zezwolenia gościom na zmianę hasła
   iii. samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora
m. System umożliwia honorowanie ustawień locale przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego.
n. System umożliwia konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego.
o. System umożliwia konfigurację maksymalnej liczby urządzeń per konto gościnne.
p. System umożliwia określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego.
q. 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.
r. System umożliwia konfigurację dostępu dla gości po samodzielnej rejestracji bez akceptacji przez sponsora od 5 do 30 minut.

18. System musi umożliwiać generowanie m.in. następujących raportów:
    a. raportów dla protokołów AAA:
       i. diagnostyki protokołów AAA
       ii. trendów uwierzytelnienia 802.1X
       iii. accountingu RADIUS
       iv. uwierzytelniania RADIUS
    b. raportów dozwolonych protokołów
       i. sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym:

1. uwierzytelnień pomyślnych
2. uwierzytelnień nieudanych

ii. „N" największych ilości uwierzytelnień RADIUS per protokół EAP (Top5), w tym:
1. uwierzytelnień pomyślnych
2. uwierzytelnień nieudanych

c. raportów dla poszczególnych instancji serwerów systemu, w tym:
i. uwierzytelnień RADIUS per serwer
ii. Top „N" uwierzytelnień per serwer
iii. monitorowania Online Certificate Status Protocol (OCSP)
iv. administratorów systemu i ich uprawnień
v. logowania administratorów do systemu
vi. zmian konfiguracji serwera dokonanych przez administratorów
vii. stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS)
viii. zmian operacyjnych serwera dokonanych przez administratorów

d. raportów dla stacji końcowych, w tym:
i. uwierzytelnień typu MAC Authentication
ii. Top „N" uwierzytelnień per adres MAC stacji
iii. Top „N" uwierzytelnień per maszyna
iv. Top „N" uwierzytelnień per RADIUS Calling Station ID
v. działań podsystemu profilera per adres MAC
vi. czasu wymaganego na sprofilowanie stacji per adres MAC

e. raportów dla błędów, w tym:
i. błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił
ii. sumarycznych przyczyn nieudanych uwierzytelnień
iii. Top „N" uwierzytelnień per rodzaj błędu

f. raportów dla urządzeń sieciowych:
i. sumarycznych uwierzytelnień dla urządzeń sieciowych
ii. Top „N" uwierzytelnień per urządzenie sieciowe
iii. niedostępności serwera AAA dla urządzenia sieciowego
iv. wiadomości logowanych przez urządzenia sieciowe
v. stanu portów i sesji urządzenia sieciowego widocznych przez SNMP

g. raportów użytkowników:
i. sumarycznych uwierzytelnień użytkowników
ii. Top „N" uwierzytelnień per użytkownik
iii. sesji użytkowników gościnnych
iv. aktywności użytkowników gościnnych
v. sumarycznych uwierzytelnień sponsorów dostępu gościnnego
vi. uwierzytelnień per unikalny użytkownik

h. raportów katalogu sesji:
i. aktywnych sesji RADIUS
ii. historii sesji RADIUS
iii. zaterminowanych sesji RADIUS

19. System umożliwia generowanie alarmów systemowych w sytuacjach krytycznych za pomocą
a. wiadomości e-mail
b. syslog
20. System musi posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów.
21. System musi posiadać wsparcie dla protokołu IPv6.
22. System musi umożliwiać rozbudowę systemu poprzez dodanie dodatkowych licencji o następujące funkcjonalności:

A. Profilowanie urządzeń:

I. System umożliwia dokonanie profilowania (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu.

II. System 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.

III. System 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)

IV. System umożliwia wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji.

V. System umożliwia dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy.

VI. System 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

VII. System 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

VIII. System 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.

IX. System wspiera raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta.

B. Analiza stacji końcowej

I. System umożliwia pobranie bazy wiedzy reguł analizy stacji końcowej (Posture) dla wspieranych systemów Antywirusowych (AV) i Antispyware (AS) ze strony producenta.

II. System umożliwia kontrolę zachowania dla stacji końcowych, które nie posiadają zainstalowanego agenta głębokiej analizy stacji końcowej (Posture).

III. System umożliwia regularne ponawianie głębokiej analizy stacji końcowej (periodic reassessment) w przedziale od 1 do 24 godzin.

IV. System umożliwia przedstawienie użytkownikowi dokumentu Polityki Akceptowalnego Użycia (AUP). Polityka AUP jest prezentowana w postaci strony web po procesie głębokiej analizy stacji. Zawartość dokumentu AUP jest konfigurowalna.

V. System umożliwia głęboką analizę stacji końcowej Windows pod kątem plików (File Condition), w tym:
a. istnienia pliku na stacji końcowej
b. wersji pliku na stacji końcowej (równa, wcześniejsza niż, późniejsza niż)
c. daty utworzenia i modyfikacji pliku na stacji końcowej (równa, wcześniej niż, później niż)

VI. System umożliwia głęboką analizę stacji końcowej z systemem:
a. Windows 7
b. Windows 8 i 8.1

c. Windows 10

pod kątem wpisów w rejestrze (Registry Condition), w tym:

- kluczy rejestru z kluczem root: HKLM, HKCC, HKCU, HKU, HKCR ze

zadanym podkluczem pod kątem:

- istnienia lub nieistnienia klucza
- wartości klucza rejestru
- istnienia i domyślnej wartości klucza rejestru typu Number, String, Version

VII. System umożliwia głęboką analizę stacji końcowej z systemem:

a. Windows 7
b. Windows 8 i 8.1
c. Windows 10

pod kątem uruchomionych aplikacji (Application Condition) w tym:

- nazwy uruchomionego lub nieuruchomionego procesu

VIII. System umożliwia głęboką analizę stacji końcowej z systemem:

a. Windows 7
b. Windows 8 i 8.1
c. Windows 10

pod kątem uruchomionych usług systemowych (Service Condition), w tym:

- nazwy uruchomionej lub nieuruchomionej usługi

IX. System umożliwia tworzenie słownika prostych i złożonych warunków (Simple i Compound Condition) dla głębokiej analizy stacji końcowej za pomocą wyrażeń logicznych AND, OR, NOT, w tym z uwzględnieniem:

- parametrów dostępu do sieci, w tym:
- lokalizacji stacji końcowej
- nazwy użytkownika
- adresu IP stacji
- metody uwierzytelnienia
- statusu uwierzytelnienia
- repozytorium użytkowników użytych dla uwierzytelnienia
- atrybutów RADIUS, w tym:
  - Calling-Station-ID
  - Framed-IP-Address
  - NAS-Identifier
  - NAS-IP-Address
  - NAS-Port-Type
  - Service-Type
  - User-Name
- parametrów sesji w tym:
  - typu żądania agenta na stacji końcowej (początkowe/initial lub reassessment)
  - architektury systemu operacyjnego na stacji końcowej (32-bit lub 64-bit)
  - adresu URL, z którego nastąpiło przekierowanie

X. System umożliwia głęboką analizę stacji końcowej z systemem:

a. Windows 7
b. Windows 8 i 8.1
c. Windows 10
d. Mac OS-X

pod kątem zainstalowanych aplikacji Antywirusowych (AV Compound Condition), w tym:

- stwierdzenia czy system AV jest obecny na stacji
- stwierdzenia czy definicje sygnatur AV są nie starsze niż zadana ilość dni od:
  - daty ostatniego pliku definicji
  - aktualnego czasu systemowego

C. Obsługa serwerów certyfikatów CA

I. System posiada funkcję zintegrowanego centrum certyfikacji, Certificate Authority (CA) lub zapewniać współpracę z zewnętrznym centrum CA.

II. Funkcja CA umożliwia wystawianie certyfikatów dla urządzeń, które uzyskują dostęp do sieci w procesie BYOD, dla realizacji bezpiecznego uwierzytelniania przy pomocy EAP-TLS.

III. System 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.

IV. Funkcja CA zapewnia przynajmniej następujące funkcjonalności:
1. 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
2. Key Management: generacja i bezpieczne przechowywanie kluczy i certyfikatów w modelu rozproszonym
3. Certificate Storage: bezpieczne przechowywanie certyfikatów użytkowników i stacji
4. 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

Jeżeli funkcjonalności opisane w punkcie 22 wymagają wykupienia dodatkowych licencji, to Zamawiający nie wymaga ich dostarczenia w chwili zakupu systemu.

Rozwiązanie musi być objęte 3-letnim serwisem świadczonym bezpośrednio przez producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego oraz do aktualizacji oprogramowania urządzenia.

Wdrożenie systemu:

W ramach wdrożenia przedmiotowego systemu Zamawiający wymaga:

I. Konfiguracji urządzeń sieciowych (ok. 50 szt.) do współpracy z zamawianym systemem
II. Integracji systemu z usługą Active Directory
III. Integracji systemu z siecią Wireless
IV. Konfigurację mechanizmów uwierzytelnienia 802.1x dla maszyn i użytkowników
V. Przeszkolenie administratorów z obsługi systemu