

OPIS PRZEDMIOTU ZAMÓWIENIA

I. Przedmiot zamówienia

1. Przedmiotem zamówienia jest:
 - 1.1. Rozbudowa posiadanego przez Zamawiającego systemu dostępu do zasobów sieciowych Cisco Identity Services Engine (Cisco ISE) lub dostarczenie systemu równoważnego. („System”)
 - 1.2. Wdrożenie i świadczenie usług wsparcia dla Systemu przez okres 3 lat od dnia jego uruchomienia.
 - 1.3. Sukcesywne dostawy licencji dla stacji końcowych w ramach prawa opcji, dla jednostek organizacyjnych PGL LP.
2. Zamówienie będzie realizowane w dwóch etapach. W ramach Etapu nr 1 Wykonawca wykona rozbudowę systemu lub dostawę systemu równoważnego. Natomiast Etap nr 2 będzie obejmował zamówienia opcjonalne na dostawę licencji stacji końcowych dla jednostek organizacyjnych PGL LP.
3. Zamawiający informuje, że w jednostkach PGL LP zatrudnionych jest około 29000 pracowników.

II. Etap nr 1: Rozbudowa posiadanego przez Zamawiającego systemu dostępu do zasobów sieciowych Cisco Identity Services Engine (Cisco ISE) lub dostarczenie systemu równoważnego.

1. Opis posiadanego rozwiązania
Obecnie posiadany przez Zamawiającego, system dostępu do zasobów sieciowych, został wdrożony w układzie klastra niezawodnościowego rozdystrybuowanego w ośrodkach przetwarzania danych Zamawiającego. Zbudowany jest z klastra dwóch serwerów Cisco ISE 2.1 VM Medium. Zamawiający posiada 600 licencji ISE BASE. Zamawiający informuje, iż posiada zasoby sprzętowe oraz licencje wirtualizacyjne dla systemu działającego w środowisku VMware. Zamawiający informuje również, iż posiadane licencje ISE objęte są kontraktem serwisowym do dnia 28.02.2022 r.
2. Zakres rozbudowy systemu:
 - 2.1. Aktualizacji posiadanej wersji systemu ISE do najnowszej zalecanej.
 - 2.2. Dostarczeniu dwóch nowych serwerów Cisco ISE VM z przeznaczeniem dla ról Administration (PAN) i Monitoring (MnT).
 - 2.3. Dostarczeniu dwóch nowych serwerów Cisco ISE VM z przeznaczeniem dla roli Policy Service (PSN).
 - 2.4. Zmiany roli obecnie posiadanych przez Zamawiającego serwerów z Cisco ISE VM Medium PAN/MnT/PSN na PSN.53,

- 2.5. Dostarczeniu i uruchomieniu nowych licencji ISE-A-LIC zwiększających pojemność systemu.
- 2.6. Dostarczeniu i uruchomieniu licencji Cisco ISE Device Admin Node.

3. Wymagania dotyczące topologii systemu

3.1. Docelowa topologia ma zapewniać redundancję systemu z zapewnieniem wysokiej dostępności. System ma być złożony z sześciu serwerów działających w środowisku wirtualnym VMware posiadanym przez Zamawiającego. Dwóch maszyn ISE VM Large (PAN/MnT) oraz czterech maszyn ISE VM Medium (PSN). Serwery muszą zostać rozlokowane równomiernie pomiędzy ośrodki przetwarzania danych Zamawiającego.

3.2. Uzyskany system dostępu do zasobów sieciowych musi:

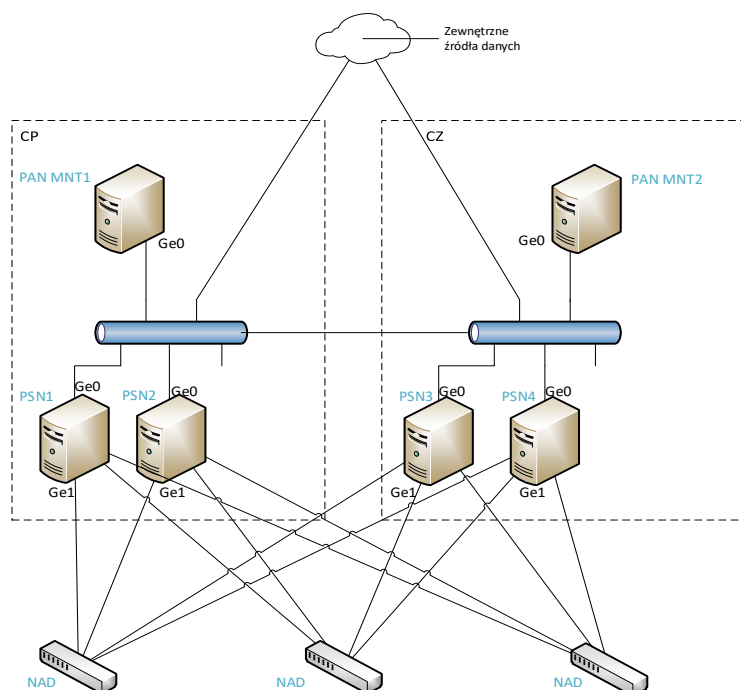
3.2.1. Pozwalać na jednoczesną obsługę:

- 1) Minimum 35 000 urządzeń końcowych takich jak np. komputery stacjonarne, laptopy, urządzenia mobilne, telefony IP, drukarki itp.
- 2) Minimum 3 000 urządzeń sieciowych takich jak np. routery, przełączniki sieciowe, punkty dostępowe sieci bezprzewodowej.

3.3. System musi działać, jako jedna całość i być uruchomiony symetrycznie w dwóch ośrodkach przetwarzania danych Zamawiającego.

3.4. System musi być odporny na awarię pojedynczego ośrodka przetwarzania danych bez utraty wydajności lub równoczesną awarię dwóch PSN w przypadku dostępności obu centrów przetwarzania.

4. Poniższy diagram przedstawia założoną architekturę Systemu:



5. Specyfikacja wymaganych licencji podstawowych oraz subskrypcji:

LP	Nr. Katalogowy	Opis	Ilość
----	----------------	------	-------

1	R-ISE-VMC-K9	Cisco ISE Virtual Machine Large	4
2	CON-ECMU-RISE9KVM SWSS UPGRADES	Cisco ISE Virtual Machine Common PID 3 lata	4
3	L-ISE-TACACS-ND=	Cisco ISE Device Admin Node License	2
4	ISE-A-LIC	Cisco Identity Service Engine Advantage Subscription	5000

6. Wymagania dla systemu równoważnego

6.1 Rozwiązanie musi znajdować się w przewodniku Gartnera po rynku systemów kontroli dostępu do sieci, dostępnym na stronie <https://www.gartner.com/en/documents/4002144/market-guide-for-network-access-control>, oraz posiadać średnią ocenę, co najmniej 4.0 z minimum 120 recenzji dostępnych na stronie <https://www.gartner.com/reviews/market/network-access-control>.

6.2 Docelowa topologia ma zapewniać redundancję systemu z zapewnieniem wysokiej dostępności. Serwery muszą zostać rozlokowane równomiernie pomiędzy ośrodki przetwarzania danych Zamawiającego.

6.3 Uzyskany System dostępu do zasobów sieciowych musi:

6.3.1. Pozwalać na jednoczesną obsługę:

1) Minimum 35 000 urządzeń końcowych takich jak np. komputery stacjonarne, laptopy, urządzenia mobilne, telefony IP, drukarki itp.

2) Minimum 3 000 urządzeń sieciowych takich jak np. routery, przełączniki sieciowe, punkty dostępowe sieci bezprzewodowej.

6.3.2. System musi działać, jako jedna całość i być uruchomiony symetrycznie w dwóch ośrodkach przetwarzania danych Zamawiającego.

6.3.3. System musi być odporny na awarię pojedynczego ośrodka przetwarzania danych bez utraty wydajności.

6.3.4. Zamawiający informuje, iż posiada zasoby sprzętowe oraz licencje wirtualizacyjne dla systemu działającego w środowisku Vmware, jednak nie mogą być one większe niż w przypadku dostarczenia klastra ISE(zasoby rekomendowane w dokumentacji producenta), będącego przedmiotem postępowania.

6.4 System zapewnia pełne zarządzanie cyklem życiowym dostępu do zasobów sieciowych, niezależnie od miejsca uzyskiwanego dostępu. System realizuje wsparcie dla dostępu gościnnego w sieci, identyfikację stacji, rejestrację urządzeń. System może 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.

- 6.4.1 System umożliwia instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych.
- 6.4.2 System umożliwia elastyczną rozbudowę poprzez dodawanie licencji dla podstawowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych.
- 6.4.3 System umożliwia instalację na maszynie wirtualnej (VM) i maszynie fizycznej, w tym:
 - 6.4.3.1 Na VMware wersji 8 dla ESXi 5.1 U2 .
 - 6.4.3.2 Na VMware wersji 11 dla ESXi 6.x i nowszych.
 - 6.4.3.3 Na hypervisorze KVM na Red Hat Enterprise Linux (RHEL) 7.0
 - 6.4.3.4 Microsoft Hyper-V.
 - 6.4.3.5 Na serwerach fizycznych wspieranych przez producenta.
- 6.4.4 System umożliwia realizację wysokiej dostępności elementów funkcjonalnych.
- 6.4.5 System umożliwia zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).
- 6.4.6 System umożliwia tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled).
- 6.4.7 System umożliwia uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
- 6.4.8 System umożliwia kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:
 - 6.4.8.1 dostęp do interfejsu konfiguracji usług tożsamości 802.1X.
 - 6.4.8.2 dostęp do interfejsu konfiguracji urządzeń sieciowych.
 - 6.4.8.3 dostęp do interfejsu konfiguracji polityk.
 - 6.4.8.4 dostęp do interfejsu konfiguracji kontroli dostępu gościnnego.
 - 6.4.8.5 dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania.
 - 6.4.8.6 System posiada możliwość podłączenia i identyfikacji urządzenia końcowego z wykorzystaniem OUI adresów MAC.
- 6.5 Mechanizmy uwierzytelniania 802.1x .
 - 6.5.1 System wspiera następujące protokoły uwierzytelniania i standardy:
 - 6.5.1.1 RADIUS, zgodnie z dokumentami:
 - 6.5.1.1.1 RFC 2865 — Remote Authentication Dial In User Service (RADIUS).
 - 6.5.1.1.2 RFC 2866 — RADIUS Accounting.
 - 6.5.1.1.3 RFC 2869 — RADIUS Extensions.
 - 6.5.1.2 RADIUS Proxy dla zewnętrznego serwera RADIUS
 - 6.5.2 System wspiera protokół Windows Active Directory, w tym co najmniej następujące repozytoria AD:
 - 6.5.2.1 Microsoft Windows Active Directory 2012.
 - 6.5.2.2 Microsoft Windows Active Directory 2012 R2.
 - 6.5.2.3 Microsoft Windows Active Directory 2016.
 - 6.5.3 System wspiera protokół Lightweight Directory Access Protocol (LDAP).
 - 6.5.4 System wspiera serwery Radius Token OTP, w tym, co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865.
 - 6.5.5 System wspiera następujące protokoły uwierzytelniania:

- 6.5.5.1 PAP/ASCII
- 6.5.5.2 CHAP
- 6.5.5.3 MS-CHAPv1
- 6.5.5.4 MS-CHAPv2
- 6.5.5.5 EAP-MD5
- 6.5.5.6 EAP-TLS
- 6.5.5.7 Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:
 - 6.5.5.7.1 EAP-MS-CHAPv2
 - 6.5.5.7.2 EAP-GTC
 - 6.5.5.7.3 EAP-TLS
- 6.5.5.8 System umożliwia konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect.
- 6.5.6 System wspiera implementację 802.1X z przynajmniej następującymi suplikantami:
 - 6.5.6.1 wbudowanym klientem 802.1X dla Windows 10.
 - 6.5.6.2 wbudowanym klientem 802.1X dla Windows 8 i 8.1.
 - 6.5.6.3 Apple Mac OS X Supplicant.
 - 6.5.6.4 Apple iOS Supplicant.
 - 6.5.6.5 Google Android Supplicant.
- 6.5.7 System umożliwia tworzenie polityk uwierzytelniania 802.1X opartych złożone o reguły (rule-based).
- 6.5.8 System umożliwia uwierzytelnianie 802.1X maszyn i użytkowników.
- 6.5.9 System umożliwia tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o reguły.
- 6.5.10 System posiada lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym).
- 6.5.11 System posiada lokalną bazę stacji końcowych. Lokalna baza stacji końcowych jest tworzona per stacja końcowa na podstawie unikalnego adresu MAC.
- 6.5.12 System wspiera uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
- 6.5.13 System wspiera uwierzytelnienie stacji końcowych na podstawie adresów MAC zawartych w katalogu LDAP oraz autoryzację urządzenia na podstawie innych atrybutów przypisanych do obiektu(który zawiera adres MAC uwierzytelnianego urządzenia).
- 6.5.14 System wspiera zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices), w tym:
 - 6.5.14.1 tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host per port.
 - 6.5.14.2 tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia.
 - 6.5.14.3 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.

- 6.5.14.4 tryb uwierzytelniania 802.1X pozwalający wiele hostów na jednym porcie fizycznym.
- 6.5.14.5 mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny.
- 6.5.14.6 mechanizm umożliwiający poprawną obsługę sytuacji, w której nowy host podłącza się do portu na którym uprzednio było uwierzytelnione urządzenie, w tym w VLANie głosowym.
- 6.5.14.7 mechanizm przypisania VLANu w procesie uwierzytelnienia i kontroli dostępu 802.1X.
- 6.5.14.8 mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1X kompatybilny z przełącznikami Cisco (dACL).
- 6.5.14.9 obsługa przypisania listy kontroli dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki.
- 6.5.14.10 mechanizm 802.1x umożliwiający realizację dostępu gościnnego w dedykowanym VLANie (Guest VLAN) dla użytkowników gościnnych.
- 6.5.14.11 mechanizm 802.1x umożliwiający przypisanie urządzenia telefonii IP do dedykowanego VLANu w sytuacji, gdy serwer AAA jest niedostępny.
- 6.5.14.12 uwierzytelnienie 802.1X urządzenia telefonii IP znajdującego się w VLANie głosowym.
- 6.5.14.13 współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN.
- 6.5.14.14 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.
- 6.5.14.15 możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego, jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznika.
- 6.5.15 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) gdzie dostawcą tożsamości jest katalog Active Directory lub zamiennie wewnętrzna baza systemu.
- 6.5.16 System wspiera m.in. następujące urządzenia sieciowe, jako klientów RADIUS (NAD - Network Access Device):
 - 6.5.16.1 Przełączniki Ethernet. Lista wspieranych przełączników Cisco oraz producentów trzecich dostępna jest na stronach Cisco (wraz z wersjami oprogramowania).
 - 6.5.16.2 Kontrolery sieci bezprzewodowej. Lista wspieranych kontrolerów sieci bezprzewodowej Cisco oraz producentów trzecich dostępna jest na stronach Cisco (wraz z wersjami oprogramowania).
 - 6.5.16.3 Koncentratory VPN. Lista wspieranych koncentratorów VPN Cisco oraz producentów trzecich dostępna jest na stronach Cisco (wraz z wersjami oprogramowania).

6.5.17 funkcjonalność serwera TACACS+ do administrowania urządzeniami sieciowymi w zakresie usług terminalowych, bez konieczności rozbudowy sprzętowej, w pełnym zakresie AAA.

6.6 Realizacja dostępu gościnnego

6.6.1 System umożliwia realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, między innymi dla:

6.6.1.1 Microsoft Windows 10, Windows 8.1, Windows 8.

6.6.1.2 Apple Mac OS X 10.x.

6.6.1.3 Apple iOS5.0.1 i nowszych.

6.6.1.4 Google Android dla 2.2 i nowszych.

6.6.1.5 Linux.

6.6.2 System umożliwia dodawanie kont gościnnych przez wybrane osoby (sponsor).

6.6.3 System zapewnia uwierzytelnienie sponsora, które musi odbywać sekwencyjnie się w oparciu o:

6.6.3.1 wewnętrzną bazę użytkowników.

6.6.3.2 zewnętrzne repozytorium użytkowników.

6.6.4 System umożliwia konfigurację uprawnień sponsora, w tym uprawnienia do:

6.6.4.1 logowania się do systemu.

6.6.4.2 tworzenia pojedynczego konta gościnnego.

6.6.4.3 tworzenia wielu kont gościnnych.

6.6.4.4 importowania kont gościnnych z pliku CSV.

6.6.4.5 wysyłania wiadomości email po utworzeniu konta gościnnego.

6.6.4.6 wysyłania wiadomości SMS po utworzeniu konta gościnnego.

6.6.4.7 wyświetlenia hasła konta gościnnego.

6.6.4.8 wydrukowania danych konta gościnnego.

6.6.4.9 wyświetlenia danych stworzonych kont gościnnych.

6.6.4.10 zawieszenia (suspend) i reinicjacji kont gościnnych.

6.6.5 System umożliwia personalizację wyglądu portalu sponsora i gościa, w tym:

6.6.5.1 zmianę logo strony logowania.

6.6.5.2 zmianę obrazu tła strony logowania.

6.6.5.3 zmianę logo banneru.

6.6.5.4 zmianę obrazu tła banneru.

6.6.5.5 zmianę koloru tła strony z treścią.

6.6.6 System umożliwia zmianę adresu URL i FQDN strony sponsora.

6.6.7 System posiada wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim, angielskim, francuskim, niemieckim i hiszpańskim.

6.6.8 System umożliwia stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim.

6.6.9 System umożliwia wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora:

6.6.9.1 Imienia

6.6.9.2 Nazwiska

6.6.9.3 Firmy

6.6.9.4 adresu e-mail

6.6.9.5 numeru telefonu

6.6.9.6 danych opcjonalnych (nie mniej niż 5 dodatkowych pól)

6.6.10 System umożliwia konfigurację dla użytkowników gościnnych:

6.6.10.1 wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP).

6.6.10.2 zezwolenia gościom na zmianę hasła.

6.6.10.3 samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora.

6.6.11 System umożliwia honorowanie ustawień locale przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego.

6.6.12 System umożliwia konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego.

6.6.13 System umożliwia konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługuje, co najmniej 20 urządzeń per konto gościnne.

6.6.14 System umożliwia konfigurację czasu ważności hasła w dniach w przedziale zadany w dniach.

6.6.15 System umożliwia określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny.

6.6.16 System umożliwia konfigurację polityki złożoności haseł użytkowników gościnnych.

6.6.17 System umożliwia konfigurację polityki nazwy (login) użytkownika gościnnego w tym, co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika.

6.6.18 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.

6.6.19 System umożliwia udostępnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP i poprzez SMS,

6.6.20 System wspiera API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych.

6.7 Profilowanie urządzeń

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

6.7.2 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.

6.7.3 System umożliwia dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł:

6.7.3.1 DHCP

6.7.3.2 DHCP SPAN

6.7.3.3 HTTP

6.7.3.4 RADIUS

6.7.3.5 SNMP

6.7.3.6 Network Scan (NMAP lub inne narzędzie profilowania aktywnego)

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

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

6.7.6 System posiada dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla:

6.7.6.1 Stacji roboczych pracujących z systemami FreeBSD, Linux, Macintosh, Microsoft Windows, Sun,

6.7.6.2 Urządzeń mobilnych: Android, Apple, Blackberry

6.7.6.3 Telefonów IP.

6.7.6.4 Drukarek sieciowych.

6.7.6.5 Systemów videokonferencyjnych w tym terminali i urządzeń z nimi powiązanych.

6.7.6.6 Routerów.

6.7.6.7 Punktów dostępu bezprzewodowego.

6.7.7 System umożliwia subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, w tym następujących informacji:

6.7.7.1 reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci.

6.7.7.2 reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie <http://standards.ieee.org/develop/regauth/oui/oui.txt>.

6.7.8 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.

6.7.9 System jest kompatybilny z technologią Cisco Device-Sensor (tworzenie profili urządzeń na podstawie pakietów account'ingowych wysyłanych z przełącznika, zawierające dane z próbek DHCP, LLDP, CDP itd.)

6.7.10 Możliwość używania wyrażeń regularnych przy tworzeniu warunków profilu.

6.8 Możliwość rozbudowy o licencje umożliwiające Analizę stacji końcowej (Posture Assessment) w zakresie:

6.8.1 Pobrania bazy wiedzy reguł analizy stacji końcowej (Posture) dla wspieranych systemów Antywirusowych (AV) i Antispyware (AS) ze strony producenta.

6.8.2 Kontroli zachowania dla stacji końcowych, które nie posiadają zainstalowanego agenta głębokiej analizy stacji końcowej (Posture).

6.8.3 Głębokiej analizy stacji końcowej Windows pod kątem plików (File Condition), w tym:

6.8.3.1 istnienia pliku na stacji końcowej.

6.8.4 Głębokiej analizy stacji końcowej pod kątem wpisów w rejestrze (Registry Condition) z systemem:

6.8.4.1 Windows 8 i 8.1

6.8.4.2 Windows 10

6.8.5 Głębokiej analizy stacji końcowej, pod kątem uruchomionych aplikacji (Application Condition), z systemem:

6.8.5.1 Windows 8 i 8.1

6.8.5.2 Windows 10

6.8.6 Głębokiej analizy stacji końcowej, pod kątem uruchomionych usług (Service Condition), z systemem:

6.8.6.1 Windows 8 i 8.1

6.8.6.2 Windows 10

6.8.7 Tworzenia 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:

6.8.7.1 parametrów dostępu do sieci

6.8.7.2 lokalizacji stacji końcowej

6.8.7.3 nazwy użytkownika

6.8.7.4 adresu IP stacji

6.8.7.5 metody uwierzytelnienia

6.8.7.6 statusu uwierzytelnienia

6.8.7.7 repozytorium użytkowników użytych dla uwierzytelnienia atrybutów RADIUS, w tym:

6.8.7.7.1 Calling-Station-ID

6.8.7.7.2 Framed-IP-Address

6.8.7.7.3 NAS-Identifier

6.8.7.7.4 NAS-Port-Type

6.8.7.7.5 Service-Type

6.8.7.7.6 User-Name

6.8.7.8 parametrów sesji w tym:

6.8.7.8.1 typu żądania agenta na stacji końcowej (początkowe/initial lub reassessment)

6.8.7.8.2 architektury systemu operacyjnego na stacji końcowej (32-bit lub 64-bit)

6.8.7.8.3 adresu URL, z którego nastąpiło przekierowanie

6.8.8 Głębokiej analizy stacji końcowej pod względem systemów antywirusowych (obecności w systemie, aktualności definicji z systemem):

6.8.8.1 Windows 8 i 8.1

6.8.8.2 Windows 10

6.9 Obsługa serwerów certyfikatów CA.

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

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

6.9.3 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.

6.9.4 Funkcja CA zapewnia przynajmniej następujące funkcjonalności:

6.9.4.1 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

6.9.4.2 Key Management: generacja i bezpieczne przechowywanie kluczy i certyfikatów w modelu rozproszonym

6.9.4.3 Certificate Storage: bezpieczne przechowywanie certyfikatów użytkowników i stacji

6.9.4.4 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

6.10 Raportowanie

System musi umożliwiać generowanie m.in. następujących raportów:

6.10.1 raportów dla protokołów AAA:

6.10.2 raportów dozwolonych protokołów

6.10.3 raportów dla poszczególnych instancji serwerów systemu,

6.10.4 raportów dla stacji końcowych

6.10.5 raportów błędów

6.11 Alarmy

6.11.1 System umożliwia generowanie alarmów systemowych w sytuacjach krytycznych za pomocą

6.11.1.1 wiadomości e-mail

6.11.1.2 syslog

6.11.2 Alarmy mogą być generowane w następujących sytuacjach:

6.11.2.1 ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu

6.11.2.2 status krytycznych procesów będzie niepożądany

6.11.2.3 stan obciążenia Systemu wzrośnie powyżej zadanego poziomu

6.11.3 System posiada zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:

6.11.3.1 wyszukiwanie zdarzeń RADIUS z uwzględnieniem:

6.11.3.1.1 nazwy użytkownika

6.11.3.1.2 adresu MAC

6.11.3.1.3 statusu uwierzytelnienia (udana lub nieudana)

6.11.3.1.4 powodu, jeżeli uwierzytelnienie nieudane

6.11.3.1.5 zakresu czasowego, co do dnia, godziny i minuty

6.11.3.2 wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do Systemu

6.12 Wsparcie dla protokołu IPv6

6.12.1 System pozwala na zarządzanie administracyjne za pomocą interfejsu graficznego udostępnionego administratorowi z wykorzystaniem adresacji IPv6

6.12.2 System pozwala na konfigurację NTP IPv6

6.12.3 System umożliwia stworzenie reguł ograniczających dostęp administracyjny do linii poleceń lub interfejsu graficznego w oparciu o adres IPv6

- 6.12.4 System umożliwia konfigurację serwerów SNMP w oparciu o adresację IPv6
- 6.12.5 System umożliwia wysyłanie SNMP Trap do serwera SNMP IPv6
- 6.12.6 System umożliwia integrację z Active Directory w oparciu o IPv6
- 6.12.7 System umożliwia połączenie z serwerem Radius z wykorzystaniem adresu IPv6

III. Etap nr 1: Wdrożenie

Zamawiający przewiduje następujący proces wdrożenia:

1. Konsultacje, analiza środowiska Zamawiającego, opracowanie koncepcji docelowego Systemu w układzie HA.
2. Testy przeprowadzane wspólnie przez Zamawiającego i Wykonawcę

2.1. Testy funkcjonalne

Testy funkcjonalne będą wykonane na przełącznikach CISCO 2960 i 9200L z aktualnie wspieranym oprogramowaniem, będą zawierać następujący zakres:

- 2.1.1. AAA z metodą uwierzytelnienia EAP-TLS, gdzie dostawcą tożsamości będą usługi katalogowe Active-Directory,
- 2.1.2. AAA z metodą uwierzytelnienia EAP-TLS, z CA CUCM
- 2.1.3. AAA z metodą uwierzytelnienia PEAP, gdzie dostawcą tożsamości będą usługi katalogowe Active-Directory,
- 2.1.4. AAA z metodą uwierzytelnienia MAB, gdzie dostawcą tożsamości będzie wewnętrzna baza systemu,
- 2.1.5. AAA poprzez portal webowy, gdzie dostawcą tożsamości będą usługi katalogowe Active-Directory,
- 2.1.6. usługi profilowania z wykorzystaniem próbek dhcp, active directory i nmap, http.
- 2.1.7. usługi TACACS+(AAA), gdzie magazynem poświadczeń będą lokalna baza użytkowników i usługi katalogowe Active-Directory
- 2.1.8. AAA z metodą uwierzytelnienia PEAP, gdzie stacja robocza była wcześniej uwierzytelniona na podstawie profilu usługi profilowania(CoA)
- 2.1.9. funkcjonowania CoA w pełnym zakresie.
- 2.1.10. AAA poprzez portal web'wy, gdzie dostawcą tożsamości jest wewnętrzna baza systemu, wraz z konfiguracją portalu sponsora.

2.2. Testy niezawodnościowe

- 2.1.1. Wyłączanie pojedynczo węzłów w każdym centrum przetwarzania danych, sprawdzanie ciągłości działania systemu, włączenie węzłów, sprawdzenie integralności systemu
- 2.1.2. Wyłączenie centrum przetwarzania CP, sprawdzenie ciągłości działania systemu, włączenie centrum przetwarzania CP, sprawdzenie integralności systemu

2.1.3. Wyłączenie centrum przetwarzania CZ, sprawdzenie ciągłości działania systemu, włączenie centrum przetwarzania CZ, sprawdzenie integralności systemu

2.1.4. Przeprowadzenie operacji backup&restore przy użyciu wewnętrznych mechanizmów dostarczanego systemu, dla wszystkich węzłów.

3. Przeniesienie konfiguracji z obecnie posiadanego środowiska, która zawiera:

3.1. AAA z metodą uwierzytelnienia EAP-TLS, gdzie dostawcą tożsamości będą usługi katalogowe Active-Directory

3.2. AAA poprzez portal webowy, gdzie dostawcą tożsamości jest wewnętrzna baza systemu, wraz z konfiguracją portalu sponsora(grupy AD).

3.3. Zamawiający informuje, że kontrolery sieci bezprzewodowej to aktualnie wspierane kontrolery firmy CISCO.

4. Przygotowanie dokumentacji i projektu powdrożeniowego w porozumieniu z Zamawiającym, zawierającej:

4.1. Szczegółową strukturę systemu

4.2. Konfigurację systemu(Zamawiający nie będzie wymagał konfiguracji systemu, poza zakresem określonym w punkcie 2

4.3. Opracowanie wzorców konfiguracji dla przełączników sieciowych(wykorzystanych w testach)

4.4. Opracowanie procedury disaster recovery

5. Wymagania dodatkowe w przypadku dostarczenia systemu równoważnego

5.1. **Szkolenie** - W przypadku dostarczenia systemu równoważnego, Zamawiający będzie wymagał organizacji przez Wykonawcę autoryzowanego szkolenia producenta z zakresu konfiguracji i obsługi dostarczonego systemu, dla 5 pracowników Zamawiającego, w wymiarze nie mniejszym niż 32 godziny robocze.

5.1.1. Wykonawca zapewni materiały szkoleniowe w języku polskim lub angielskim oraz przekaże je Zamawiającemu wraz z autorskimi prawami majątkowymi. Szkolenie odbędzie się w języku polskim.

5.1.2. Szkolenie odbędzie się stacjonarne w ośrodku szkoleniowym na terenie Polski, w terminie uzgodnionym z Zamawiającym, jednak nie później niż 20 dni roboczych od daty odbioru wdrożenia.

5.1.3. Zamawiający wymaga, by Trener posiadał certyfikat upoważniający do przeprowadzania szkoleń.

5.1.4. Zamawiający sfinansuje dojazd własnych pracowników na szkolenie. Pozostałe koszty wykonania szkolenia, w tym materiały szkoleniowe, koszty sali, wykładowców, ewentualnego cateringu pokrywa Wykonawca w ramach wynagrodzenia.

5.1.5. Szkolenie podlega ocenie warunkującej odbiór. Ocena zostanie dokonana na podstawie ankiety wypełnianej przez słuchaczy, obejmującej ocenę prowadzenia zajęć przez wykładowcę, ocenę materiałów szkoleniowych oraz zakresu przekazanej wiedzy. Kryteria oceny są następujące:

–Najwyższa ocena 5, najniższa ocena 2

- Średnia ocen 3,0 i powyżej oznacza należyście przeprowadzone szkolenie
- Średnia ocen 2,9 i poniżej oznacza nienależyście przeprowadzone szkolenie.

5.1.6. Szkolenie przeprowadzone nienależyście Wykonawca powtórzy na własny koszt, w terminie wyznaczonym przez Zamawiającego, jednak nie później niż w terminie 10 dni roboczych od dnia zakończenia szkolenia podlegających powtórzeniu.

5.2. W przypadku dostarczenia systemu równoważnego Wykonawca dostarczy i wdroży kompletny system, spełniający wszystkie wymagania wskazane w OPZ, który zastąpi posiadaną obecnie infrastruktury ISE.

IV. Etap nr 2. Systematyczne dostarczanie licencji

Zakup dodatkowych licencji dla stacji końcowych z 3 letnim okresem wsparcia, liczonym od daty dostarczenia licencji, w ramach prawa opcji. Ilość licencji zakupiona w ramach prawa opcji będzie ograniczona do 30 000 sztuk.

V. Zakres wsparcia – subskrypcje (dotyczy oprogramowania dostarczanego zarówno w ramach Etapu nr 1 jak i Etapu nr 2)

Dostarczony System musi pochodzić od jednego producenta i posiadać 36 miesięczne subskrypcje serwisowe producenta niezależne od statusu partnerskiego Wykonawcy. Zamawiający wymaga, aby dostawca był autoryzowanym przedstawicielem producenta oprogramowania.

Oferowane wsparcie musi zapewnić Zamawiającemu przez cały okres trwania:

1. Bezpośredni i wolny od dodatkowych opłat dostęp do pomocy technicznej producenta przez telefon, e-mail oraz WWW, w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją Systemu
2. Wsparcie musi być realizowane w trybie 24/7. Wykonawca zobowiązuje się do potwierdzenia przyjęcia zgłoszenia awarii od uprawnionego przedstawiciela Zamawiającego maksymalnie do 4 godzin od chwili otrzymania zgłoszenia za pośrednictwem poczty elektronicznej (e-mail), telefonicznie lub w inny zatwierdzony przez Zamawiającego sposób.
3. Wykonawca zapewni Zamawiającemu realizację zgłoszenia poprzez usunięcie awarii w terminie do 48 h od momentu przekazania zgłoszenia. Jeśli usunięcie awarii w opinii Wykonawcy wymaga czasu dłuższego niż 48 h, na wydłużenie czasu naprawy wymagana jest zgoda Koordynatora merytorycznego Umowy ze strony Zamawiającego. Uzgodnienie terminu zakończenia prac między koordynatorami Stron musi mieć miejsce w ciągu 24 h od momentu przyjęcia zgłoszenia przez Wykonawcę. Wymagana forma pisemna.

4. W okresie wsparcia wymagany jest dostęp do wszystkich najnowszych wersji oprogramowania, poprawek, patchy, itp.