

- I. Wymagania minimalne dla punktu dostępowego bezprzewodowej sieci WiFi kampusu PG zwanego dalej AP – szt. 150 w zamówieniu podstawowych plus 150 szt. w opcji**
- I.1. AP musi zapewniać obsługę poniższych standardów, protokołów, technologii i funkcjonalności przewidzianych dla sieci bezprzewodowych WiFi:
- I.1.1. obsługa 802.11a/b/g/n/ac/ax
 - I.1.2. obsługa OFDMA (uplink/downlink), TWT, BSS Coloring
 - I.1.3. obsługa MU-MIMO – min. 4x4:4
 - I.1.4. obsługa kanałów 20, 40 MHz dla 802.11n
 - I.1.5. obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax
 - I.1.6. obsługa prędkości PHY do 3,47 Gbps (ac)
 - I.1.7. obsługa prędkości PHY do 5,38 Gbps (ax)
 - I.1.8. obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
 - I.1.9. obsługa beamforming dla klientów 802.11a/g/n/ac/ax
 - I.1.10. obsługa MRC (Maximal Ratio Combining)
- I.2. AP musi zapewniać obsługę szerokiego zakresu kanałów radiowych co najmniej w poniższych zakresach:
- I.2.1. dla zakresu 2.4 GHz: min. 13 kanałów
 - I.2.2. dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów
 - I.2.3. dla zakresu 5GHz (extended UNII-2): min. 8 kanałów
- I.3. AP musi zapewniać konfigurowanie mocy nadajnika co najmniej w poniższych zakresach:
- I.3.1. dla zakresu 2.4 GHz: do 100 mW
 - I.3.2. dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW
 - I.3.3. dla zakresu 5GHz (extended UNII-2): do 200 mW
- I.4. AP musi zapewniać zmiany trybu pracy modułów radiowych (elastyczna praca drugiego modułu) co najmniej w poniższych trybach:
- I.4.1. jeden moduł pracujący w paśmie 2,4GHz, drugi moduł pracujący w paśmie 5GHz
 - I.4.2. oba moduły pracujące w paśmie 5GHz na różnych kanałach w celu wytworzenia mikro i makro komórki radiowej
- I.5. AP musi zapewniać zgodność z protokołem CAPWAP (RFC 5415), oraz zapewniać zarządzanie przez kontroler WLAN z poniższymi minimalnymi funkcjonalnościami:
- I.5.1. automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN
 - I.5.2. optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)
 - I.5.3. obsługa min. 16 BSSID
 - I.5.4. definiowanie polityk bezpieczeństwa (dla każdego SSID z osobna) z możliwością rozgłaszania lub ukrycia poszczególnych SSID
 - I.5.5. uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w
 - I.5.6. obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN)
 - I.5.7. możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączeniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników
 - I.5.8. obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6
 - I.5.9. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN, wireless IDS)
 - I.5.10. obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h
 - I.5.11. obsługa IPv6
 - I.5.12. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r
 - I.5.13. obsługa mechanizmów QoS:
 - I.5.13.1. ograniczanie ruchu do użytkownika, z możliwością konfiguracji dla każdego użytkownika z osobna
 - I.5.13.2. obsługa WMM, TSPEC, U-APSD
 - I.5.14. współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne
 - I.5.15. wsparcie dla poniższych metod EAP:
 - I.5.15.1. EAP-TLS,
 - I.5.15.2. EAP-TTLS,
 - I.5.15.3. EAP-PEAP,

I.5.15.4. EAP-GTC,

I.5.15.5. EAP-SIM

I.5.16. wsparcie IEEE 802.11i, WPA3, WPA2, WPA

I.5.17. wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej ze wsparciem dla:

I.5.17.1. EAP-FAST,

I.5.17.2. EAP-TLS,

I.5.17.3. EAP-PEAP)

I.6. AP musi zapewniać tryb pracy jako kontroler sieci bezprzewodowej o następujących minimalnych funkcjonalnościach:

I.6.1. zmiana trybu pracy AP np. poprzez wgranie odpowiedniej wersji oprogramowania nie może generować żadnych kosztów po stronie zamawiającego w okresie trwania kontraktu serwisowego

I.6.2. AP musi zapewniać obsługę min 100 innych punktów dostępowych AP – pełnić dla nich funkcję kontrolera

I.6.3. AP musi zapewniać obsługę min. 2000 klientów bezprzewodowych

I.6.4. AP musi zapewniać konfigurację min 16 sieci bezprzewodowych

I.6.5. AP musi zapewniać centralną optymalizację wykorzystania pasma radiowego:

I.6.5.1. ograniczanie wpływu zakłóceń,

I.6.5.2. kontrola mocy,

I.6.5.3. dobór kanałów,

I.6.5.4. reakcja na zmiany

I.6.6. AP musi zapewniać obsługę szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r

I.6.7. AP musi zapewniać obsługę mechanizmów wsparcia roamingu – IEEE 802.11k, IEEE 802.11v

I.6.8. AP musi zapewniać jednoczesną obsługę transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN)

I.6.9. AP musi zapewniać wykrywanie do 1000 obcych klientów bezprzewodowych oraz do 100 obcych AP

I.6.10. AP musi zapewniać konfigurację polityk bezpieczeństwa dla każdego SSID z osobna

I.6.11. AP musi zapewniać obsługę WPA2 i WPA3 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników-lokalny RADIUS)

I.6.12. AP musi zapewniać współpracę z serwerami autoryzacyjnymi RADIUS (konfigurowane dla każdego SSID z osobna)

I.6.13. AP musi zapewniać tworzenie list kontroli dostępu w oparciu o adresy IPv4 oraz o nazwy domenowe

I.6.14. AP musi zapewniać filtrowanie MAC adresów (Whitelist)

I.6.15. AP musi zapewniać analizę ruchu pozwalającą na:

I.6.15.1. identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie min. 1000 aplikacji)

I.6.15.2. kontrolę aplikacji (limitowanie, markowanie, dropowanie)

I.6.16. AP musi zapewniać dwukierunkowe limitowanie transmisji dla:

I.6.16.1. każdego klienta bezprzewodowego z osobna,

I.6.16.2. każdego WLAN z osobna,

I.6.16.3. każdego BSSID z osobna

I.6.17. AP musi zapewniać profilowanie (rozpoznawanie typów) urządzeń podłączających się do sieci bezprzewodowej

I.6.18. AP musi zapewniać obsługę mechanizmów QoS (WMM, priorytetyzacja, Voice CAC)

I.6.19. AP musi zapewniać obsługę dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym

I.6.20. AP musi zapewniać obsługę kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na wbudowanym kontrolerze) z określeniem czasu ważności konta;

I.6.21. AP musi zapewniać zarządzanie przez HTTPS

I.6.22. AP musi zapewniać wsparcie SSH, SNMP, NTP, SYSLOG

I.6.23. AP musi zapewniać obsługę aktualizacji oprogramowania przez SFTP

I.6.24. AP musi posiadać wbudowany serwer DHCP

I.6.25. AP musi posiadać wbudowany mechanizm redundancji automatycznie wybierający kontroler zapasowy wśród grupy obsługiwanych punktów dostępowych mogących pełnić funkcję kontrolera

I.6.26. AP musi posiadać zintegrowany moduł analizatora widma częstotliwościowego (dotyczy zakresów 2.4GHz i 5GHz) i zapewniać poniższe min. parametry i funkcjonalności:

I.6.26.1. dokładność analizy (kwant próbkowania) nie gorsza niż 315 kHz

I.6.26.2. zakres częstotliwościowy zgodny z zakresem pracy modułów radiowych

I.6.26.3. automatyczne wykrywanie i klasyfikację źródeł interferencji (Bluetooth, DECT, urządzenia mikrofalowe, urządzenia transmisji audio wideo, urządzenia zakłócające itp.)

I.6.26.4. współpraca z mechanizmami optymalizacji wykorzystania pasma radiowego

- I.6.27. AP musi posiadać min. jeden interfejs MultiGigabit Ethernet (100/1000/2500) zgodny z IEEE 802.3bz
- I.6.28. AP musi posiadać min. jeden interfejs konsoli zarządzającej – dostawca musi zapewnić okablowanie niezbędne do podłączenia stacji zarządzającej(PC) do portu konsolowego AP
- I.6.29. AP musi posiadać min. jeden port USB
- I.6.30. AP musi zapewniać pełną funkcjonalność przy zasilaniu przez PoE+ (IEEE 802.3at),
- I.6.31. AP musi zapewniać uruchomienie AP z wykorzystaniem PoE (802.3af)
- I.6.32. AP musi posiadać anteny zintegrowane (wewnętrzne) o zysku min:
 - I.6.32.1. dla modułu umożliwiającego pracę w obu pasmach:
 - I.6.32.1.1. min. 4 dBi dla pasma 2,4 GHz
 - I.6.32.1.2. min. 5 dBi dla pasma 5 GHz
 - I.6.32.2. dla dedykowanego modułu 5 GHz: min. 4dBi
- I.6.33. AP musi posiadać obudowę przystosowaną do pracy w min. zakresie temperatur 0 – 50°C
- I.6.34. AP musi posiadać diodową sygnalizację stanu urządzenia z możliwością deaktywacji
- I.6.35. AP musi posiadać certyfikację dla WiFi Alliance w zakresach:
 - I.6.35.1. 802.11 a/b/g/n/ac,
 - I.6.35.2. WMM,
 - I.6.35.3. Passpoint
- I.6.36. AP musi posiadać wbudowane radio Bluetooth Low Energy (BLE) 5.0
- I.6.37. Punkt dostępowy musi być przygotowany do obsługi standardu 802.15.4 (Zigbee, Thread, BLE)
- I.6.38. Punkt dostępowy musi być przygotowany na uruchamianie aplikacji użytkownika dostępnych bezpośrednio na AP – dostawca musi zapewnić API oraz niezbędne licencje i niezbędne środowisko hardware/software/SDK
- I.6.39. AP musi być dostarczony ze wszystkimi niezbędnymi elementami montażowymi niezbędnymi do prawidłowego montażu AP na ścianie lub suficie.
- I.6.40. Wraz z AP musi być dostarczona licencja dla kontrolera z pkt. II specyfikacji na obsługę przez kontroler dostarczonego AP
- I.6.41. AP musi być objęty 3 letnim wsparciem technicznym producenta
- I.6.42. AP musi być objęty 3 letnią gwarancją producenta

II. Wymagania minimalne dla kontrolera sieci bezprzewodowej WiFi kampusu PG zwanego dalej kontrolerem - 2 szt.

II.1. Kontroler musi zapewniać centralną kontrolę punktów dostępu bezprzewodowego z pkt. I z obsługą poniższych standardów, protokołów, technologii i funkcjonalności:

- II.1.1. Kontroler musi być zrealizowany w postaci specjalizowanego/dedykowanego urządzenia tzw. Hardware Appliance producenta dostosowanego do wymagań wyszczególnionych w pkt. II niniejszej specyfikacji
- II.1.2. W przypadku zaproponowania rozwiązania w oparciu o serwer z platformą wirtualizacyjną Zamawiający wymaga dostarczenia serwera zgodnego z posiadaną infrastrukturą Cisco UCS i posiadaną platformą wirtualizacyjną VMware vSphere Enterprise Plus oraz wszystkimi związanymi z tym licencjami i kontraktami serwisowymi na okres 3 lat wraz z raportem z badań na potwierdzenie wymaganej wydajności z niezależnego od producenta centrum badawczego.
- II.1.3. Kontroler musi zapewniać zarządzanie politykami bezpieczeństwa
- II.1.4. Kontroler musi zapewniać wykrywanie zagrożeń w sieci bezprzewodowej
- II.1.5. Kontroler musi zapewniać zarządzanie pasmem radiowym
- II.1.6. Kontroler musi zapewniać zarządzanie mobilnością
- II.1.7. Kontroler musi zapewniać zarządzanie jakością transmisji zgodnie z protokołem CAPWAP (RFC 5415)
- II.1.8. Kontroler musi zapewniać obsługę min. 30000 klientów bezprzewodowych jednocześnie. W chwili dostawy musi być wyposażony w licencje na obsługę 2000 klientów bezprzewodowych. Przyszłościowa rozbudowa o obsługę dodatkowych klientów bezprzewodowych musi być realizowana na drodze zakupu dodatkowych licencji.
- II.1.9. Kontroler musi posiadać min. 4 interfejsy TX/RX 10Gbps SM LC WDM każdy
- II.1.10. Kontroler musi zapewniać łączenie interfejsów w grupę logiczną by zabezpieczyć przed awarią pojedynczego interfejsu
- II.1.11. Kontroler musi zapewniać wydajność urządzenia dla ruchu tunelowanego o przepustowości min. 40 Gbps
- II.1.12. Kontroler musi zapewniać zarządzanie pasmem radiowym punktów dostępowych min. w zakresie:
 - II.1.12.1. automatyczna adaptacja do zmian w czasie rzeczywistym
 - II.1.12.2. optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
 - II.1.12.3. dynamiczne przydzielanie kanałów radiowych
 - II.1.12.4. wykrywanie, eliminacja i unikanie interferencji
 - II.1.12.5. równoważenie obciążenia punktów dostępowych
 - II.1.12.6. tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych
 - II.1.12.7. automatyczna dystrybucja klientów pomiędzy punkty dostępowe
 - II.1.12.8. mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych
 - II.1.12.9. dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe
- II.1.13. Kontroler musi zapewniać mapowanie SSID do segmentów VLAN w sieci przewodowej w trybach:
 - II.1.13.1. 1:1
 - II.1.13.2. 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty)
 - II.1.13.3. tunelowanie ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID)
- II.1.14. Kontroler musi zapewniać obsługę sieci kratowych z poniższymi funkcjonalnościami:
 - II.1.14.1. komunikacja między punktami dostępowymi bez medium kablowego
 - II.1.14.2. separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi)
 - II.1.14.3. automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo)
 - II.1.14.4. automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)
 - II.1.14.5. autoryzacja punktów dostępowych w oparciu o:
 - II.1.14.5.1. certyfikaty
 - II.1.14.5.2. adresy MAC
- II.1.15. Kontroler musi zapewniać obsługę poniższych mechanizmów bezpieczeństwa:
 - II.1.15.1. 802.11i, WPA3, WPA2, WPA, WEP
 - II.1.15.2. 802.1x z EAP min.:
 - II.1.15.2.1. PEAP,
 - II.1.15.2.2. EAP-TLS,
 - II.1.15.2.3. EAP-FAST

- II.1.15.3. obsługa serwerów autoryzacyjnych min:
 - II.1.15.3.1. RADIUS,
 - II.1.15.3.2. TACACS+,
 - II.1.15.3.3. wbudowana lokalna baza użytkowników
- II.1.15.4. kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID
- II.1.15.5. obsługa profilowania użytkowników min.:
 - II.1.15.5.1. przydział sieci VLAN
 - II.1.15.5.2. przydział list kontroli dostępu (ACL)
- II.1.15.6. uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 – wsparcie dla IEEE 802.11w
- II.1.15.7. uwierzytelnianie punktów dostępowych w oparciu o certyfikaty
- II.1.15.8. obsługa list kontroli dostępu (ACL)
- II.1.15.9. obsługa indywidualnych kluczy PSK per klient dla sieci SSID, która nie wykorzystuje mechanizmów 802.1X
- II.1.15.10. wykrywanie i dezaktywacja obcych punktów dostępowych
- II.1.15.11. ochrona kryptograficzna (DTLS) ruchu kontrolnego i ruchu użytkowników CAPWAP
- II.1.15.12. DHCP proxy
- II.1.15.13. zabezpieczenia zapewniające autentyczność sprzętową oraz software'ową min.:
 - II.1.15.13.1. kryptograficzne podpisywanie obrazów oprogramowania
 - II.1.15.13.2. bezpieczny proces sekwencji startowej (bootowanie) elementów systemowych
 - II.1.15.13.3. wbudowany moduł sprzętowy unikalnie identyfikujący urządzenie i jego pochodzenie
- II.1.16. Kontroler musi zapewniać obsługę ruchu unicast IPv4 i IPv6
- II.1.17. Kontroler musi zapewniać obsługę ruchu multicast IPv4 i IPv6 w tym:
 - II.1.17.1. IGMP / MLD snooping
 - II.1.17.2. optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym)
 - II.1.17.3. obsługa konwersji ruchu multicast do unicast
- II.1.18. Kontroler musi zapewniać obsługę mobilności (roaming-u) użytkowników (IPv4 i IPv6, w ramach i pomiędzy kontrolerami)
- II.1.19. Kontroler musi zapewniać obsługę mechanizmów wspomagania roamingu:
 - II.1.19.1. IEEE 802.11r
 - II.1.19.2. 802.11k
- II.1.20. Kontroler musi zapewniać wsparcie dla IEEE 802.11u
- II.1.21. Kontroler musi zapewniać obsługę mechanizmów QoS w tym:
 - II.1.21.1. 802.1p
 - II.1.21.2. WMM, TSpec, U-APSD
 - II.1.21.3. Ograniczanie pasma dla każdego użytkownika z osobna
 - II.1.21.4. Call Admission Control, SIP CAC, Call Snooping
 - II.1.21.5. równomierna obsługa klientów sieci bezprzewodowej w oparciu o użycie czasu antenowego (również w trybie mesh)
 - II.1.21.6. kontrola przydziału czasu antenowego (od AP do klienta mobilnego) dla danego SSID
- II.1.22. Kontroler musi zapewniać obsługę dostępu gościnnego (IPv4 i IPv6) w tym:
 - II.1.22.1. przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony)
 - II.1.22.2. przekierowanie użytkowników do strony logowania na zewnętrznym serwerze
- II.1.23. Kontroler musi zapewniać współpracę z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne,
- II.1.24. Kontroler musi zapewniać obsługę tagów telemetrycznych
- II.1.25. Kontroler musi zapewniać obsługę NTP wersji 4 (IPv4 oraz IPv6)
- II.1.26. Kontroler musi zapewniać definiowanie polityk dostępu do sieci bezprzewodowej na podstawie czasu logowania
- II.1.27. Kontroler musi zapewniać obsługę Hotspot 2.0
- II.1.28. Kontroler musi zapewniać obsługę redundancji rozwiązania (N+1)
- II.1.29. Kontroler musi zapewniać obsługę redundancji 1:1 (active/standby) zapewniającej:
 - II.1.29.1. utrzymanie sesji punktów dostępowych oraz urządzeń mobilnych na wypadek awarii aktywnego kontrolera
 - II.1.29.2. synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej

- II.1.30. Kontroler musi posiadać dedykowane interfejsy SFP służące do połączenia dwóch kontrolerów w redundanтную parę 1:1
- II.1.31. Kontroler musi zapewniać analizę ruchu przechodzącego przez kontroler pozwalającą na identyfikację oraz klasyfikację na poziomie aplikacji (warstwa 7); obsługa markowania, limitowania lub odrzucania ruchu; rozpoznawanie ponad 1000 aplikacji
- II.1.32. Kontroler musi zapewniać zbieranie i eksport statystyk ruchu sieciowego za pomocą protokołu NetFlow lub sFlow
- II.1.33. Kontroler musi zapewniać profilowanie urządzeń podłączających się do sieci bezprzewodowej w oparciu o informacje z:
 - II.1.33.1. HTTP,
 - II.1.33.2. DHCPoraz przydzielanie na tej podstawie odpowiednich uprawnień i parametrów dostępowych, takich jak:
 - II.1.33.3. VLAN,
 - II.1.33.4. polityka QoS,
 - II.1.33.5. lista kontroli dostępu,
 - II.1.33.6. czas trwania sesji
- II.1.34. Kontroler musi zapewniać obsługę protokołu Bonjour poprzez wbudowany mDNS Gateway, zbierający ogłoszenia o dostępności danych usług i odpowiadający na zapytania klientów
- II.1.35. Kontroler musi zapewniać zarządzanie przez min.:
 - II.1.35.1. HTTPS,
 - II.1.35.2. SNMP,
 - II.1.35.3. SSH,
 - II.1.35.4. NETCONF,
 - II.1.35.5. port konsoli szeregowej
- II.1.36. Kontroler musi zapewniać wsparcie API min. dla:
 - II.1.36.1. NETCONF - RFC4741
 - II.1.36.2. NETCONF - RFC4742
 - II.1.36.3. YANG - RFC6020
- II.1.37. Kontroler musi posiadać wbudowaną bazę najlepszych praktyk (best practice) konfiguracji z możliwością łatwej ich implementacji (lub cofnięcia zmian) jednym przyciskiem
- II.1.38. Kontroler musi posiadać redundancję zasilacza i wentylatory
- II.1.39. Wraz z kontrolerem muszą być dostarczone licencje pozwalające na wieczyste wykorzystywanie wszystkich wymaganych funkcjonalności niezależnie od wykupionego wsparcia technicznego/subskrypcji/supportu u producenta
- II.1.40. Kontroler musi być objęty 3 letnim wsparciem technicznym producenta, w tym dostęp do bazy wiedzy producenta i aktualizacji oprogramowania
- II.1.41. Kontroler musi być objęty 3 letnią gwarancją producenta w trybie:
 - II.1.41.1. „następny dzień roboczy” - NBD
 - II.1.41.2. jeżeli kontroler posiada wymienne nośniki informacji (HDD/SSD/SD itp.) – tryb „zachowaj nośnik informacji/dysk twardy”

III. Wymagania minimalne na system zarządzania siecią przewodową i bezprzewodową kampusu PG zwany dalej systemem - 1 szt.

III.1. System musi stanowić jednolite rozwiązanie zarządzania siecią przewodową i bezprzewodową w szczególności dla AP z pkt. I oraz kontrolerów z pkt. II niniejszej specyfikacji

III.2. System zarządzania musi posiadać następujące minimalne funkcjonalności ogólne:

III.2.1. Musi zapewniać pracę w trybie WebGUI pozwalając administratorowi na dostęp z dowolnego (po uzyskaniu odpowiednich uprawnień) miejsca w sieci

III.2.2. Musi posiadać interfejs bazujący na HTML5

III.2.3. Musi zapewniać dostęp do konfiguracji wszystkich wymienionych funkcjonalności z pkt. III.1 III.2 III.3 niniejszej specyfikacji z poziomu WebGUI

III.2.4. Musi zapewniać budowanie widoków przez użytkownika

III.2.5. Musi posiadać funkcje szybkiej nawigacji wraz z szybkim wyświetlaniem informacji przy zbliżeniu kursora myszy do interesującego obiektu

III.2.6. Musi zapewniać hierarchizację zarządzania w tym min.:

III.2.6.1. określenia domen administracyjnych dla administratorów

III.2.6.2. wykorzystania wbudowanej bazy administratorów

III.2.6.3. wykorzystania zewnętrznego serwera uwierzytelniającego

III.2.7. Musi posiadać narzędzia pozwalające na podział urządzeń w logiczne grupy reprezentujące np.:

III.2.7.1. oddziały,

III.2.7.2. lokalizacje,

III.2.7.3. budynki

III.2.7.4. inne definiowalne podgrupy

III.2.8. Musi zapewniać widok pozwalający na rozmieszczenie urządzeń/grup urządzeń na mapie geograficznej wraz z dynamiczną zmianą stanu ikony reprezentującej daną lokalizację w zależności od alarmów i ogólnej kondycji sieci w danej lokalizacji

III.2.9. Musi zapewniać współpracę z serwerami czasu (NTP)

III.2.10. Musi posiadać wbudowane formularze do konfiguracji usług na nowych urządzeniach

III.2.11. Musi posiadać wbudowane formularze do weryfikacji możliwości urządzeń pod kątem uruchomienia nowych usług (np. IEEE 802.1X)

III.2.12. Musi posiadać narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku

III.2.13. Musi zapewniać tworzenie raportów dotyczących:

III.2.13.1. urządzeń sieciowych,

III.2.13.2. urządzeń klienckich

III.2.13.3. wydajności sieci

III.2.13.4. luk bezpieczeństwa na urządzeniach sieciowych

III.2.14. Musi zapewniać zbieranie Netflow/sFlow z urządzeń sieciowych

III.2.15. Musi posiadać narzędzie pozwalające na monitoring wydajności sieci wraz z:

III.2.15.1. zbieraniem informacji o aplikacjach w sieci i parametrach ich działania,

III.2.15.2. analizą, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacje oraz jakie jest ich wykorzystanie, itp.

III.2.16. Musi posiadać narzędzie pozwalające na diagnostykę działania urządzenia przez wykonanie min.:

III.2.16.1. ping

III.2.16.2. traceroute

III.2.16.3. połączenie się z urządzeniem przez min.:

III.2.16.3.1. telnet,

III.2.16.3.2. ssh,

III.2.16.3.3. http,

III.2.16.3.4. https

III.2.17. Musi zapewniać wyświetlanie wykresów korelujących zmiany w konfiguracji ze zdarzeniami na urządzeniu w celu lepszej i szybszej diagnostyki problemów

III.2.18. Musi posiadać narzędzie pozwalające na analizę połączenia urządzeń klienckich i użytkowników podłączonych w sposób przewodowy oraz bezprzewodowy do infrastruktury; narzędzie powinno pozwalać na m.in.: zbieranie informacji o parametrach połączenia i umożliwiać administratorowi szybką analizę problemów związanych z podłączeniem urządzenia do infrastruktury

- III.2.19. Musi zapewniać współpracę z systemem do uwierzytelniania i autoryzacji urządzeń klienckich i użytkowników w celach:
- III.2.19.1. zbierania informacji o polityce dostępowej nałożonej na urządzenie
 - III.2.19.2. generowania raportów dotyczących statystyk AAA
- III.2.20. Musi zapewniać API REST do integracji z innymi narzędziami/systemami
- III.2.21. Musi posiadać odpowiednią liczbę licencji jeśli są odrębnie wymagane do zarządzania bezprzewodowymi punktami dostępowymi z pkt. I
- III.2.22. System musi zostać dostarczony w formie maszyny wirtualnej dedykowanej dla posiadanej przez Zamawiającego platformy wirtualizacji VMware vSphere ESX wraz ze wszystkimi wymaganymi licencjami i wsparciem technicznym na okres 3 lat
- III.3. System zarządzania musi posiadać min. szczególne funkcjonalności w zakresie zarządzania siecią przewodową:
- III.3.1. Musi zarządzać i zbierać statystyki z wykorzystaniem co najmniej SNMP
- III.3.2. Musi posiadać narzędzia automatycznej identyfikacji i wyszukiwania urządzeń instalowanych w sieci, w tym możliwość manualnego oraz automatycznego dodawania urządzeń za pośrednictwem protokołów takich jak:
- III.3.2.1. LLDP,
 - III.3.2.2. ARP,
 - III.3.2.3. OSPF,
- III.3.3. Musi posiadać narzędzia wyświetlania urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu
- III.3.4. Musi udostępniać mapę topologii urządzeń z połączeniami oraz wizualizacją alarmów na urządzeniach
- III.3.5. Musi posiadać narzędzia do konfiguracji urządzeń w zakresie przynajmniej interfejsów, list kontroli dostępu, wybranych protokołów routingu na routerach
- III.3.6. Musi posiadać wbudowane przykładowe wzorce konfiguracji urządzeń, takie jak: konfiguracja usług bezpieczeństwa, agregacji linków, konfiguracji: NTP, SNMP, NAT, itp.
- III.3.7. Musi posiadać narzędzie do tworzenia wzorców konfiguracji na urządzeniach
- III.3.8. Musi posiadać funkcje archiwizacji konfiguracji, przeglądania zmian konfiguracji, automatyzacji zbierania konfiguracji urządzeń
- III.3.9. Musi posiadać narzędzie do weryfikacji poprawności zgodności konfiguracji wraz z zadanym wzorcem konfiguracji (statycznym lub opartym o wzorce regularne) z możliwością korekty konfiguracji na prawidłową
- III.3.10. Musi posiadać narzędzie do przeprowadzania inwentaryzacji komponentów używanych w sieci w tym sprzętu i oprogramowania systemowego urządzeń sieciowych
- III.3.11. Musi posiadać narzędzie do zarządzania obrazami oprogramowania urządzeń
- III.3.12. Musi posiadać narzędzie umożliwiające zbieranie informacji o parametrach urządzeń, min. takich jak:
- III.3.12.1. obciążenie CPU,
 - III.3.12.2. zajętość pamięci,
 - III.3.12.3. dostępność,
 - III.3.12.4. ilość portów,
 - III.3.12.5. użycie portów
- III.3.13. Musi posiadać mechanizmy wspomagające wyszukiwanie, izolację problemów i ich rozwiązywanie
- III.3.14. Musi zapewniać zbieranie statystyki za pomocą protokołu Netflow/sFlow
- III.3.15. Musi zapewniać monitoring wydajności sieci wraz z możliwością zbierania informacji o aplikacjach w sieci i parametrach ich działania pozwalające na analizę min.:
- III.3.15.1. ilości ruchu,
 - III.3.15.2. czasu odpowiedzi,
 - III.3.15.3. czasu transakcji
 - III.3.15.4. czasu opóźnienia
- III.3.16. Musi zapewniać monitoring ruchu użytkowników z możliwością analizy min.:
- III.3.16.1. którzy użytkownicy generują najwięcej ruchu,
 - III.3.16.2. z jakich korzystają aplikacje
 - III.3.16.3. jakie jest ich wykorzystanie
- III.3.17. Musi posiadać narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku
- III.3.18. Musi posiadać narzędzie do zbierania alarmów pochodzących z urządzeń i kategoryzacji alarmów
- III.3.19. Musi informować o alarmach/incydentach przez powiadomienie e-mail
- III.3.20. Musi posiadać narzędzie do konfiguracji, monitoringu i optymalizacji usług WAN (technologia VPN, polityka routingu oraz polityka QoS z podziałem na aplikacje)

- III.4. System zarządzania musi posiadać min. szczególne funkcjonalności w zakresie zarządzania siecią bezprzewodową:
- III.4.1. Musi zapewniać graficzne planowanie i zarządzanie siecią bezprzewodową z wykorzystaniem własnych planów budynków w tym min.:
- III.4.1.1. hierarchiczne mapy lokalizacji
III.4.1.2. mapy zasięgu
- III.4.2. Musi zapewniać zarządzanie punktami dostępowymi i kontrolerami
- III.4.3. Musi zapewniać monitorowanie autonomicznych punktów dostępowych
- III.4.4. Musi zapewniać monitorowanie informacji pochodzących z punktów dostępowych takich jak:
- III.4.4.1. poziom szumu,
III.4.4.2. poziom sygnału,
III.4.4.3. interferencje sygnału,
- III.4.5. Musi zapewniać monitorowanie parametrów pracy kontrolerów bezprzewodowych, w tym również parametrów pracy (zasilacze, wentylatory) zapasowych kontrolerów w parze HA
- III.4.6. Musi zapewniać raportowanie i statystykę min.:
- III.4.6.1. wydajności urządzeń,
III.4.6.2. obciążenia sieci,
III.4.6.3. alarmów pochodzących z urządzeń
- III.4.7. Musi posiadać wbudowane formularze do tworzenia min.:
- III.4.7.1. polityki bezpieczeństwa dla wielu punktów dostępu radiowego,
III.4.7.2. polityki QoS dla wielu punktów dostępu radiowego,
- III.4.8. Musi zapewniać automatyczne wykrywanie nowych punktów dostępowych w sieci radiowej
- III.4.9. Musi zapewniać obsługę sieci kratowych
- III.4.10. Musi posiadać narzędzie do zbierania ruchu z określonego punktu dostępowego oraz klienta bezprzewodowego do pliku pcap z możliwością określenia filtrów i czasu zbierania ruchu
- III.4.11. Musi zapewniać wykrywanie nieautoryzowanych punktów dostępowych z określeniem ich lokalizacji na żądanie
- III.4.12. Musi posiadać narzędzie do wykrywania czy nieautoryzowany punkt dostępowy podłączony jest do naszej infrastruktury przewodowej
- III.4.13. Musi zapewniać zarządzanie wersjami oprogramowania urządzeń
- III.4.14. Musi posiadać mechanizmy tworzenia kopii zapasowych
- III.4.15. Musi zapewniać obsługę dostępu bezprzewodowego dla gości
- III.4.16. Musi posiadać narzędzie do planowania radiowego w oparciu o zadane plany budynku i potencjalne usługi sieci bezprzewodowej pozwalające min. na:
- III.4.16.1. automatyczne rozmieszczenie punktów dostępowych
III.4.16.2. manualne rozmieszczenie punktów dostępowych
- III.4.17. Musi posiadać narzędzie do inspekcji poprawności rozmieszczenia punktów dostępowych pod kątem usług głosowych oraz usług lokalizacji
- III.4.18. Musi posiadać narzędzie do stopniowej aktualizacji oprogramowania na punktach dostępowych w celu minimalizacji przerw w pracy sieci
- III.4.19. Musi zapewniać współpracę z analizatorami widma częstotliwościowego
- III.4.20. Musi zapewniać współpracę z systemami lokalizacji urządzeń radiowych z prezentacją graficzną na mapie (punktów dostępowych, klientów, itp. np. Google Maps lub OpenMap itp.)
- III.4.21. System musi być objęty 3 letnim wsparciem technicznym producenta
- III.4.22. System musi być objęty 3 letnią gwarancją producenta

IV. Wymagania minimalne dla serwera uwierzytelniania i autoryzacji sieci przewodowej i bezprzewodowej kampusu PG zwany dalej serwerem UA - 2 szt.

IV.1. Serwer UA musi być zrealizowany w postaci specjalizowanego/dedykowanego urządzenia tzw. Hardware Appliance producenta dostosowanego do wymagań wyszczególnionych w pkt. IV niniejszej specyfikacji

IV.2. W przypadku zaproponowania rozwiązania w oparciu o serwer z platformą wirtualizacyjną Zamawiający wymaga dostarczenia serwera zgodnego z posiadaną infrastrukturą Cisco UCS i posiadaną platformą wirtualizacyjną VMware vSphere Enterprise Plus oraz wszystkimi związanymi z tym licencjami i kontraktami serwisowymi na okres 3 lat - wraz z raportem z badań na potwierdzenie wymaganej wydajności z niezależnego od producenta centrum badawczego.

IV.3. Serwer UA musi zapewniać pełne zarządzanie cyklem życiowym dostępu do zasobów sieciowych, niezależnie od miejsca uzyskiwanego dostępu.

IV.4. Serwer UA musi realizować wsparcie dla dostępu gościnnego w sieci, identyfikację stacji, rejestrację urządzeń.

IV.5. Serwer UA musi pozwalać na objęcie kontrolą dostępu wszystkich podłączanych do sieci IP urządzeń w tym:

- IV.5.1. terminali,
- IV.5.2. komputerów PC,
- IV.5.3. smartfonów i tabletów,
- IV.5.4. telefonii IP,
- IV.5.5. terminali video
- IV.5.6. i innych

IV.6. Serwer UA musi integrować wszystkie funkcjonalności z pkt. IV niniejszej specyfikacji w powiązaniu z AP z pkt. I i kontrolerami z pkt. II

IV.7. System musi być objęty 3 letnim wsparciem technicznym producenta

IV.8. System musi być objęty 3 letnią gwarancją producenta typu:

- IV.8.1. „następny dzień roboczy” NBD
- IV.8.2. jeżeli serwer UA posiada wymienne nośniki informacji (HDD/SSD/SD itp.) – tryb „zachowaj nośnik informacji/dysk twardy”

IV.9. Podstawowe min. cechy serwera UA

IV.9.1. Serwer UA musi umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych.

IV.9.2. Serwer UA musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji dla podstawowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych.

IV.9.3. Serwer UA musi zapewniać uwierzytelnianie 802.1x oraz profilowanie dla:

- IV.9.3.1. min. 2000 urządzeń końcowych dołączonych do sieci
- IV.9.3.2. zapewniać skalowalność do min. 5000

IV.9.4. Serwer UA musi być zrealizowany w oparciu o dedykowaną platformę sprzętową producenta

IV.9.5. Serwer UA musi zapewniać wydzielenie określonych elementów funkcjonalnych, w tym:

IV.9.5.1. Wydzielenie podsystemu zarządzania (Administration), umożliwiającego administratorowi dostęp do interfejsu graficznego (GUI) za pomocą przeglądarki web i zmianę konfiguracji systemu oraz jego monitorowanie

IV.9.5.2. Wydzielenie podsystemu monitoringu, logowania i rozwiązywania problemów, umożliwiającego gromadzenie wiadomości logowania z:

- IV.9.5.2.1. przełączników dostępowych
- IV.9.5.2.2. sesji uwierzytelniania 802.1X
- IV.9.5.2.3. zdarzeń kontroli dostępu (autoryzacji)
- IV.9.5.2.4. zdarzeń związanych z błędami
- IV.9.5.2.5. zdarzeń związanych z alarmami systemowymi

IV.9.5.3. Wydzielenie serwerów usługowych realizujących funkcje:

- IV.9.5.3.1. serwera RADIUS dla infrastruktury sieciowej
- IV.9.5.3.2. serwera polityk uwierzytelniania i kontroli dostępu 802.1X

- IV.9.5.3.3. serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego
 - IV.9.5.3.4. serwera profilowania stacji końcowych
- IV.9.6. Serwer UA musi zapewniać realizację wysokiej dostępności elementów funkcjonalnych, w tym:
- IV.9.6.1. zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu
 - IV.9.6.2. zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych
- IV.9.7. Serwer UA musi zapewniać aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych w tym min. przez:
- IV.9.7.1. serwer TFTP,
 - IV.9.7.2. serwer FTP/SFTP,
 - IV.9.7.3. serwer HTTP/HTTPS,
 - IV.9.7.4. udział NFS
- IV.9.8. Serwer UA musi zapewniać zarządzanie łątkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).
- IV.9.9. Serwer UA musi zapewniać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled).
- IV.9.10. Serwer UA musi zapewniać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
- IV.9.11. Serwer UA musi zapewniać wymuszenie reguł złożoności haseł dla administratorów, w tym:
- IV.9.11.1. minimalną długość hasła
 - IV.9.11.2. wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny.
 - IV.9.11.3. wymuszenie hasła różnego od trzech poprzednich haseł
 - IV.9.11.4. wymuszenie zmiany hasła co określoną ilość dni
- IV.9.12. Serwer UA musi zapewniać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora w tym min.:
- IV.9.12.1. dostęp do interfejsu konfiguracji usług tożsamości 802.1X
 - IV.9.12.2. dostęp do interfejsu konfiguracji urządzeń sieciowych
 - IV.9.12.3. dostęp do interfejsu konfiguracji polityk
 - IV.9.12.4. dostęp do interfejsu konfiguracji kontroli dostępu gościnnego
 - IV.9.12.5. dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania
- IV.9.13. Serwer UA musi zapewniać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.
- IV.9.14. Serwer UA musi zapewniać podłączenie i identyfikację urządzenia końcowego z wykorzystaniem MUD (Manufacturer Usage Description) zgodnie ze standardem IETF i RFC8520.
- IV.9.15. Zamawiający wymaga dostarczenia systemu w postaci dwóch dedykowanych, redundantnych urządzeń pochodzących od producenta urządzeń i systemów z pkt. I, pkt. II, pkt. III wraz ze wszystkimi niezbędnymi licencjami dla urządzeń i systemów oraz wsparciem technicznym na 3 lata

IV.10. Mechanizmy uwierzytelniania 802.1x

IV.10.1. Serwer UA musi zapewniać wsparcie dla następujących protokołów uwierzytelniania i standardów:

IV.10.1.1. RADIUS, zgodnie z dokumentami:

- IV.10.1.1.1. RFC 2138 — Remote Authentication Dial In User Service (RADIUS)
- IV.10.1.1.2. RFC 2139 — RADIUS Accounting
- IV.10.1.1.3. RFC 2865 — Remote Authentication Dial In User Service (RADIUS)
- IV.10.1.1.4. RFC 2866 — RADIUS Accounting
- IV.10.1.1.5. RFC 2867 — RADIUS Accounting for Tunnel Protocol Support
- IV.10.1.1.6. RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
- IV.10.1.1.7. RFC 2869 — RADIUS Extensions

IV.10.1.2. RADIUS Proxy dla zewnętrznego serwera RADIUS

IV.10.2. Serwer UA musi zapewniać wsparcie dla protokołu Windows Active Directory, w tym następujące repozytoria AD:

- IV.10.2.1. Microsoft Windows Active Directory 2003 32bit
- IV.10.2.2. Microsoft Windows Active Directory 2003 R2 32bit i 64bit
- IV.10.2.3. Microsoft Windows Active Directory 2008 32bit i 64bit
- IV.10.2.4. Microsoft Windows Active Directory 2008 R2 64bit
- IV.10.2.5. Microsoft Windows Active Directory 2012
- IV.10.2.6. Microsoft Windows Active Directory 2012 R2
- IV.10.2.7. Microsoft Windows Active Directory 2016

IV.10.3. Serwer UA musi zapewniać wsparcie dla protokołu Lightweight Directory Access Protocol (LDAP)

IV.10.4. Serwer UA musi zapewniać wsparcie dla serwera Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865

IV.10.5. Serwer UA musi zapewniać wsparcie dla następujących protokołów uwierzytelniania:

- IV.10.5.1. PAP/ASCII
- IV.10.5.2. CHAP
- IV.10.5.3. MS-CHAPv1
- IV.10.5.4. MS-CHAPv2
- IV.10.5.5. EAP-MD5
- IV.10.5.6. EAP-TLS
- IV.10.5.7. Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:

IV.10.5.7.1. EAP-MS-CHAPv2

IV.10.5.7.2. EAP-GTC

IV.10.5.7.3. EAP-TLS

IV.10.5.7.4. Serwer UA musi zapewniać konfigurację mechanizmów:

IV.10.5.7.4.1. PEAP Session Resume,

IV.10.5.7.4.2. PEAP Session Timeout

IV.10.5.7.4.3. Fast Reconnect

IV.10.6. Serwer UA musi zapewniać implementację 802.1X z przynajmniej następującymi suplikantami:

- IV.10.6.1. wbudowanym klientem 802.1X dla Windows 10
- IV.10.6.2. wbudowanym klientem 802.1X dla Windows Vista
- IV.10.6.3. wbudowanym klientem 802.1X dla Windows 7
- IV.10.6.4. wbudowanym klientem 802.1X dla Windows 8 i 8.1
- IV.10.6.5. Apple Mac OS X Supplicant
- IV.10.6.6. Apple iOS Supplicant
- IV.10.6.7. Google Android Supplicant

IV.10.7. Serwer UA musi zapewniać tworzenie polityk uwierzytelniania 802.1X opartych złożone o reguły (rule-based).

IV.10.8. Serwer UA musi zapewniać uwierzytelnianie 802.1X maszyn i użytkowników.

IV.10.9. Serwer UA musi zapewniać tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o reguły.

IV.10.10. Serwer UA musi posiadać lokalną bazę użytkowników:

- IV.10.10.1. dla każdego użytkownika z osobna
 - IV.10.10.2. w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym)
- IV.10.11. Serwer UA musi posiadać lokalną bazę stacji końcowych tworzoną dla każdej stacji końcowej z osobna na podstawie unikalnego adresu MAC.
- IV.10.12. Serwer UA musi zapewniać uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC
- IV.10.13. Serwer UA musi zapewniać zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices), w tym:
- IV.10.13.1. tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host per port
 - IV.10.13.2. tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia
 - IV.10.13.3. 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
 - IV.10.13.4. tryb uwierzytelniania 802.1X pozwalający wiele hostów na jednym porcie fizycznym
 - IV.10.13.5. mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny
 - IV.10.13.6. mechanizm umożliwiający poprawną obsługę sytuacji w której nowy host podłącza się do portu na którym uprzednio było uwierzytelnione urządzenie, w tym w VLANie głosowym
 - IV.10.13.7. 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.
 - IV.10.13.8. mechanizm przypisania VLAN'u w procesie uwierzytelnienia i kontroli dostępu 802.1X
 - IV.10.13.9. mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1X
 - IV.10.13.10. obsługa przypisania listy kontroli dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki
 - IV.10.13.11. mechanizm 802.1x umożliwiający realizację dostępu gościnnego w dedykowanym VLANie (Guest VLAN) dla użytkowników gościnnych
 - IV.10.13.12. mechanizm 802.1x umożliwiający przypisanie urządzenia telefonii IP do dedykowanego VLANu w sytuacji, gdy serwer AAA jest niedostępny
 - IV.10.13.13. przypisanie przez serwer AAA dla użytkownika nie jednego, lecz grupy VLANów dla użytkownika, z których przełącznik wybiera jeden, w którym jest najmniej użytkowników
 - IV.10.13.14. uwierzytelnienie 802.1X urządzenia telefonii IP znajdującego się w VLANie głosowym
 - IV.10.13.15. współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN
 - IV.10.13.16. 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
 - IV.10.13.17. możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego, jako stacji końcowej w celu zapobiegnięcia połączenia do sieci nieuprawnionego przełącznika
- IV.10.14. Serwer UA musi zapewniać 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)
- IV.10.15. Serwer UA musi zapewniać wsparcie dla min. następujących urządzeń sieciowych, jako klientów RADIUS (NAD - Network Access Device):
- IV.10.15.1. Przełączniki Ethernet – co najmniej w zakresie AAA, Profiling, BYOD, Guest, Posture dla poniższych producentów:
 - IV.10.15.1.1. przełączniki sieciowe firmy Cisco Systems:
 - IV.10.15.1.1.1. IE 2000, IE3000, IE4000, IE5000,,
 - IV.10.15.1.1.2. Catalyst 2960
 - IV.10.15.1.1.3. Catalyst 3560
 - IV.10.15.1.1.4. Catalyst 3650
 - IV.10.15.1.1.5. Catalyst 3750
 - IV.10.15.1.1.6. Catalyst 3850
 - IV.10.15.1.1.7. Catalyst 4500-X
 - IV.10.15.1.2. przełączniki sieciowe firmy Juniper Networks:
 - IV.10.15.1.2.1. EX3300
 - IV.10.15.1.3. przełączniki HP Development Company:
 - IV.10.15.1.3.1. ProCurve 2900,

- IV.10.15.1.3.2. H3C,
- IV.10.15.1.3.3. ProCurve

IV.10.15.2. Kontrolery sieci bezprzewodowej dedykowane do współpracy z Access Point'ami z pkt I - co najmniej w zakresie:

- IV.10.15.2.1. AAA,
- IV.10.15.2.2. Profiling,
- IV.10.15.2.3. BYOD,
- IV.10.15.2.4. Guest,
- IV.10.15.2.5. Guest Originating URL,
- IV.10.15.2.6. Posture,
- IV.10.15.2.7. MDM

IV.10.16. Serwer UA musi zapewniać rozbudowę funkcjonalności o serwer TACACS+ do administrowania urządzeniami sieciowymi bez konieczności rozbudowy sprzętowej

IV.11. Realizacja dostępu gościnnego

IV.11.1. Serwer UA musi zapewniać realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, między innymi dla:

- IV.11.1.1. Microsoft Windows 10, Windows 8.1, Windows 8, Windows 7, Microsoft Windows Vista,
- IV.11.1.2. Apple Mac OS X 10.x
- IV.11.1.3. Apple iOS 8.0, 7.x, 6.1, 6, 5.1, 5.0.1
- IV.11.1.4. Google Android dla 2.2 i nowszych
- IV.11.1.5. Linux

IV.11.2. Serwer UA musi zapewniać dodawanie kont gościnnych przez wybrane osoby (sponsor).

IV.11.3. Serwer UA musi zapewniać uwierzytelnienie sponsora które musi odbywać się sekwencyjnie w oparciu o:

- IV.11.3.1. wewnętrzną bazę użytkowników
- IV.11.3.2. zewnętrzne repozytorium użytkowników

IV.11.4. Serwer UA musi zapewniać konfigurację uprawnień sponsora, w tym uprawnienia do:

- IV.11.4.1. logowania się do systemu
- IV.11.4.2. tworzenia pojedynczego konta gościnnego
- IV.11.4.3. tworzenia wielu kont gościnnych
- IV.11.4.4. importowania kont gościnnych z pliku CSV
- IV.11.4.5. wysyłania wiadomości e-mail po utworzeniu konta gościnnego
- IV.11.4.6. wysyłania wiadomości SMS po utworzeniu konta gościnnego
- IV.11.4.7. wyświetlenia hasła konta gościnnego
- IV.11.4.8. wydrukowania danych konta gościnnego
- IV.11.4.9. wyświetlenia danych stworzonych kont gościnnych
- IV.11.4.10. zawieszenia (suspend) i re-inicjacji kont gościnnych

IV.11.5. Serwer UA musi zapewniać personalizację wyglądu portalu sponsora i gościa, w tym:

- IV.11.5.1. zmianę logo strony logowania
- IV.11.5.2. zmianę obrazu tła strony logowania
- IV.11.5.3. zmianę logo banneru
- IV.11.5.4. zmianę obrazu tła banneru
- IV.11.5.5. zmianę koloru tła strony z treścią

IV.11.6. Serwer UA musi zapewniać zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP i portu HTTPS

IV.11.7. Serwer UA musi zapewniać zmianę adresu URL i FQDN strony sponsora.

IV.11.8. Serwer UA musi zapewniać automatyczne kasowanie wygasłych kont gościnnych w tym:

- IV.11.8.1. na żądanie
- IV.11.8.2. okresowo co zadaną liczbę dni
- IV.11.8.3. określonej godzinie.

IV.11.9. Serwer UA musi zapewniać wyświetlenie czasu ostatniego kasowania wygasłych kont gościnnych i następnego kasowania wygasłych kont gościnnych

IV.11.10. Serwer UA musi posiadać wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach:

- IV.11.10.1. polskim,
- IV.11.10.2. angielskim,
- IV.11.10.3. francuskim,
- IV.11.10.4. niemieckim,
- IV.11.10.5. hiszpańskim

IV.11.11. Serwer UA musi zapewniać stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim.

IV.11.12. Serwer UA musi zapewniać wymuszenie wpisania w formularzu rejestracyjnym min. następujących danych gościa w trakcie tworzenia konta przez sponsora:

- IV.11.12.1. Imienia
- IV.11.12.2. Nazwiska

- IV.11.12.3. Firmy
 - IV.11.12.4. adresu e-mail
 - IV.11.12.5. numeru telefonu
 - IV.11.12.6. danych opcjonalnych (nie mniej niż 5 dodatkowych pól)
- IV.11.13. Serwer UA musi zapewniać konfigurację dla użytkowników gościnnych:
- IV.11.13.1. wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP)
 - IV.11.13.2. zezwolenia gościom na zmianę hasła
 - IV.11.13.3. samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora
- IV.11.14. Serwer UA musi zapewniać honorowanie ustawień locale przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego.
- IV.11.15. Serwer UA musi zapewniać konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego.
- IV.11.16. Serwer UA musi zapewniać konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługę min 20 urządzeń per konto gościnne.
- IV.11.17. Serwer UA musi zapewniać konfigurację czasu ważności hasła w dniach w przedziale zadany w dniach.
- IV.11.18. Serwer UA musi zapewniać określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny
- IV.11.19. Serwer UA musi zapewniać konfigurację polityki złożoności haseł użytkowników gościnnych.
- IV.11.20. Serwer UA musi zapewniać konfigurację polityki nazwy (login) użytkownika gościnnego w tym min.:
- IV.11.20.1. tworzenie nazwy użytkownika z adresu e-mail
 - IV.11.20.2. ustalenie minimalnej długości nazwy użytkownika
- IV.11.21. Serwer UA musi zapewniać 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.
- IV.11.22. Serwer UA musi zapewniać przypisanie do każdego portalu gościnnego niezależnego:
- IV.11.22.1. wzorca językowego,
 - IV.11.22.2. interfejsu IP,
 - IV.11.22.3. portu HTTPS
 - IV.11.22.4. certyfikatu SSL dla FQDN
- IV.11.23. Serwer UA musi zapewniać udostępnienie danych logowania gościnnego za pomocą e-mail przez konfigurację bramy SMTP.
- IV.11.24. Serwer UA musi zapewniać udostępnienie danych logowania gościnnego za pomocą SMS przez konfigurację bramy SMS.
- IV.11.25. Serwer UA musi zapewniać wsparcie API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontaktach gościnnych.

IV.12. Profilowanie urządzeń

- IV.12.1. Serwer UA musi zapewniać profilowanie (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu.
- IV.12.2. Serwer UA musi zapewniać wykorzystanie danych z procesu profilowania do zdefiniowania polityk bezpieczeństwa. W szczególności zapewnić możliwość stworzenia polityk np. dla:
- IV.12.2.1. wszystkich drukarek,
 - IV.12.2.2. wszystkich urządzeń mobilnych,
 - IV.12.2.3. wszystkich stacji z Windows, etc.
- IV.12.3. Serwer UA musi zapewniać profilowanie stacji końcowych poprzez analizę informacji pochodzących z min. następujących źródeł:
- IV.12.3.1. DHCP
 - IV.12.3.2. DHCP SPAN
 - IV.12.3.3. HTTP
 - IV.12.3.4. RADIUS
 - IV.12.3.5. DNS
 - IV.12.3.6. SNMP
 - IV.12.3.7. Network Scan (NMAP lub inne narzędzie profilowania aktywnego)
- IV.12.4. Serwer UA musi zapewniać wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji.
- IV.12.5. Serwer UA musi zapewniać dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy.
- IV.12.6. Serwer UA musi posiadać dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla:
- IV.12.6.1. Stacji roboczych pracujących z systemami:
 - IV.12.6.1.1. FreeBSD,
 - IV.12.6.1.2. Linux,
 - IV.12.6.1.3. Macintosh,
 - IV.12.6.1.4. Microsoft Windows,
 - IV.12.6.2. Urządzeń mobilnych:
 - IV.12.6.2.1. Android,
 - IV.12.6.2.2. Apple,
 - IV.12.6.3. Telefonów IP
 - IV.12.6.4. Drukarek sieciowych
 - IV.12.6.5. Systemów wideokonferencyjnych w tym terminali i urządzeń z nimi powiązanych
 - IV.12.6.6. Routerów
 - IV.12.6.7. Punktów dostępu bezprzewodowego
- IV.12.7. Serwer UA musi zapewniać subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, w tym następujących informacji:
- IV.12.7.1. reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci
 - IV.12.7.2. reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie <http://standards.ieee.org/develop/regauth/oui/oui.txt>
- IV.12.8. Serwer UA musi zapewniać 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.
- IV.12.9. Serwer UA musi zapewniać raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta.

IV.13. Analiza stacji końcowej (Posture Assessment)

- IV.13.1. Serwer UA musi zapewniać pobranie bazy wiedzy reguł analizy stacji końcowej (Posture) dla wspieranych systemów Antywirusowych (AV) i Antispyware (AS) ze strony producenta.
- IV.13.2. Serwer UA musi zapewniać kontrolę zachowania dla stacji końcowych, które nie posiadają zainstalowanego agenta głębokiej analizy stacji końcowej (Posture).
- IV.13.3. Serwer UA musi zapewniać regularne ponawianie głębokiej analizy stacji końcowej (periodic reassessment) w przedziale od 1 do 24 godzin.
- IV.13.4. Serwer UA musi zapewniać przedstawienie użytkownikowi dokumentu Polityki Akceptowalnego Użycia (AUP) w tym:
- IV.13.4.1. Polityka AUP jest prezentowana w postaci strony web po procesie głębokiej analizy stacji.
 - IV.13.4.2. Zawartość dokumentu AUP jest konfigurowalna.
- IV.13.5. Serwer UA musi zapewniać głęboką analizę stacji końcowej Windows pod kątem plików (File Condition), w tym:
- IV.13.5.1. istnienia pliku na stacji końcowej
 - IV.13.5.2. wersji pliku na stacji końcowej (równa, wcześniejsza niż, późniejsza niż)
 - IV.13.5.3. daty utworzenia i modyfikacji pliku na stacji końcowej (równa, wcześniej niż, później niż)
- IV.13.6. Serwer UA musi zapewniać głęboką analizę stacji końcowej pod kątem wpisów w rejestrze (Registry Condition), w tym:
- IV.13.6.1. kluczy rejestru z kluczem root:
 - IV.13.6.1.1. HKLM,
 - IV.13.6.1.2. HKCC,
 - IV.13.6.1.3. HKCU,
 - IV.13.6.1.4. HKU,
 - IV.13.6.1.5. HKCR,
 - IV.13.6.1.6. z zadany podkluczempod kątem:
 - IV.13.6.1.7. istnienia lub braku klucza,
 - IV.13.6.1.8. wartości klucza rejestru,
 - IV.13.6.1.9. istnienia i wartości domyślnej klucza rejestru typu min.:
 - IV.13.6.1.9.1. Number,
 - IV.13.6.1.9.2. String,
 - IV.13.6.1.9.3. Version
- dla min. wersji systemów operacyjnych zainstalowanych na stacjach klienckich:
- IV.13.6.1.10. Windows 7 i nowsze
- IV.13.7. Serwer UA musi zapewniać głęboką analizę stacji końcowej z systemem:
- IV.13.7.1. Windows 7 i nowsze
- pod kątem uruchomionych aplikacji (Application Condition), w tym:
- IV.13.7.2. nazwy uruchomionego lub nieuruchomionego procesu
- IV.13.8. Serwer UA musi zapewniać głęboką analizę stacji końcowej z systemem:
- IV.13.8.1. Windows 7 i nowsze
- pod kątem uruchomionych usług systemowych (Service Condition), w tym:
- IV.13.8.2. nazwy uruchomionej lub nieuruchomionej procesu
- IV.13.9. Serwer UA musi zapewniać 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:
- IV.13.9.1. parametrów dostępu do sieci, w tym:
 - IV.13.9.1.1. lokalizacji stacji końcowej

- IV.13.9.1.2. nazwy użytkownika
- IV.13.9.1.3. adresu IP stacji
- IV.13.9.1.4. metody uwierzytelnienia
- IV.13.9.1.5. statusu uwierzytelnienia
- IV.13.9.1.6. repozytorium użytkowników użytych dla uwierzytelnienia
- IV.13.9.1.7. atrybutów RADIUS, w tym:

- IV.13.9.1.7.1. Calling-Station-ID
- IV.13.9.1.7.2. Framed-IP-Address
- IV.13.9.1.7.3. NAS-Identifier
- IV.13.9.1.7.4. NAS-IP-Address
- IV.13.9.1.7.5. NAS-Port-Type
- IV.13.9.1.7.6. Service-Type
- IV.13.9.1.7.7. User-Name

- IV.13.9.1.8. parametrów sesji w tym:

- IV.13.9.1.8.1. typu żądania agenta na stacji końcowej (początkowe/initial lub reassessment)
- IV.13.9.1.8.2. architektury systemu operacyjnego na stacji końcowej (32-bit lub 64-bit)
- IV.13.9.1.8.3. adresu URL, z którego nastąpiło przekierowanie

IV.13.10. Serwer UA musi zapewniać głęboką analizę stacji końcowej z systemem:

- IV.13.10.1. Windows 7 i nowsze
- IV.13.10.2. Mac OS-X

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

- IV.13.10.2.1. stwierdzenia czy system AV jest obecny na stacji
- IV.13.10.2.2. stwierdzenia czy definicje sygnatur AV są nie starsze niż zadana ilość dni od:
 - IV.13.10.2.2.1. daty ostatniego pliku definicji
 - IV.13.10.2.2.2. aktualnego czasu systemowego

IV.13.11. Serwer UA musi zapewniać głęboką analizę stacji końcowej z systemem:

- IV.13.11.1. Windows 7 i nowsze
- IV.13.11.2. Mac OS-X

pod kątem zainstalowanych aplikacji AntiSpyware (AS Compound Condition), w tym:

- IV.13.11.2.1. stwierdzenia czy system AS jest obecny na stacji
- IV.13.11.2.2. stwierdzenia czy definicje sygnatur AS są nie starsze niż zadana ilość dni od:
 - IV.13.11.2.2.1. daty ostatniego pliku definicji
 - IV.13.11.2.2.2. aktualnego czasu systemowego

IV.14. Obsługa serwerów certyfikatów CA

- IV.14.1. Serwer UA musi posiadać funkcję zintegrowanego centrum certyfikacji, Certificate Authority (CA) lub zapewniać współpracę z zewnętrznym centrum CA.
- IV.14.2. Funkcja CA serwera UA musi zapewniać wystawianie certyfikatów dla urządzeń, które uzyskują dostęp do sieci w procesie BYOD, dla realizacji bezpiecznego uwierzytelniania przy pomocy EAP-TLS.
- IV.14.3. Serwer UA musi zapewniać hierarchiczność CA dla rozproszonego wdrożenia w dużej skali w tym w sytuacji rozproszenia systemu na wiele serwerów:
 - IV.14.3.1.1. serwery nadrzędne muszą zapewniać funkcję Root CA,
 - IV.14.3.1.2. serwery przetwarzające muszą zapewniać funkcję Subordinate CA (SCEP RA) dla wystawiania certyfikatów.
- IV.14.4. Funkcja CA w systemie UA musi zapewniać min. następujące funkcjonalności:
 - IV.14.4.1. 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
 - IV.14.4.2. Key Management: generacja i bezpieczne przechowywanie kluczy i certyfikatów w modelu rozproszonym
 - IV.14.4.3. Certificate Storage: bezpieczne przechowywanie certyfikatów użytkowników i stacji
 - IV.14.4.4. 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

IV.15. Raportowanie

IV.15.1. Serwer UA musi zapewniać generowanie m.in. następujących raportów:

IV.15.1.1. raportów dla protokołów AAA:

- IV.15.1.1.1. diagnostyki protokołów AAA
- IV.15.1.1.2. trendów uwierzytelnienia 802.1X
- IV.15.1.1.3. accountingu RADIUS
- IV.15.1.1.4. uwierzytelniania RADIUS

IV.15.1.2. raportów dozwolonych protokołów:

IV.15.1.2.1. sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym:

- IV.15.1.2.1.1. uwierzytelnień pomyślnych
- IV.15.1.2.1.2. uwierzytelnień nieudanych

IV.15.1.2.2. „N” największych ilości uwierzytelnień RADIUS per protokół EAP (Top5), w tym:

- IV.15.1.2.2.1. uwierzytelnień pomyślnych
- IV.15.1.2.2.2. uwierzytelnień nieudanych

IV.15.1.3. raportów dla poszczególnych instancji serwerów systemu, w tym:

- IV.15.1.3.1. uwierzytelnień RADIUS per serwer
- IV.15.1.3.2. Top „N” uwierzytelnień per serwer
- IV.15.1.3.3. monitorowania Online Certificate Status Protocol (OCSP)
- IV.15.1.3.4. administratorów systemu i ich uprawnień
- IV.15.1.3.5. logowania administratorów do systemu
- IV.15.1.3.6. zmian konfiguracji serwera dokonanych przez administratorów
- IV.15.1.3.7. stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS)
- IV.15.1.3.8. zmian operacyjnych serwera dokonanych przez administratorów
- IV.15.1.3.9. zmian haseł przez użytkowników

IV.15.1.4. raportów dla stacji końcowych, w tym:

- IV.15.1.4.1. uwierzytelnień typu MAC Authentication
- IV.15.1.4.2. Top „N” uwierzytelnień per adres MAC stacji
- IV.15.1.4.3. Top „N” uwierzytelnień per maszyna
- IV.15.1.4.4. Top „N” uwierzytelnień per RADIUS Calling Station ID
- IV.15.1.4.5. działań podsystemu profilera per adres MAC
- IV.15.1.4.6. czasu wymaganego na sprofilowanie stacji per adres MAC

IV.15.1.5. raportów dla błędów, w tym:

- IV.15.1.5.1. błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił
- IV.15.1.5.2. sumarycznych przyczyn nieudanych uwierzytelnień
- IV.15.1.5.3. Top „N” uwierzytelnień per rodzaj błędu

IV.15.1.6. raportów dla urządzeń sieciowych:

- IV.15.1.6.1. sumarycznych uwierzytelnień dla urządzeń sieciowych
- IV.15.1.6.2. Top „N” uwierzytelnień per urządzenie sieciowe
- IV.15.1.6.3. niedostępności serwera AAA dla urządzenia sieciowego
- IV.15.1.6.4. wiadomości logowanych przez urządzenia sieciowe
- IV.15.1.6.5. stanu portów i sesji urządzenia sieciowego widocznych przez SNMP

IV.15.1.7. raportów użytkowników:

- IV.15.1.7.1. sumarycznych uwierzytelnień użytkowników
- IV.15.1.7.2. Top „N” uwierzytelnień per użytkownik
- IV.15.1.7.3. sesji użytkowników gościnnych
- IV.15.1.7.4. aktywności użytkowników gościnnych
- IV.15.1.7.5. sumarycznych uwierzytelnień sponsorów dostępu gościnnego
- IV.15.1.7.6. uwierzytelnień per unikalny użytkownik

IV.15.1.8. raportów katalogu sesji w tym:

IV.15.1.8.1. aktywnych sesji RADIUS

IV.15.1.8.2. historii sesji RADIUS

IV.15.1.8.3. zaterminowanych sesji RADIUS

IV.16. Alarmy

IV.16.1. Serwer UA musi zapewniać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą min.:

- IV.16.1.1. wiadomości e-mail
- IV.16.1.2. syslog

IV.16.2. Alarmy muszą być generowane w następujących sytuacjach:

- IV.16.2.1. ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu
- IV.16.2.2. opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego
- IV.16.2.3. status krytycznych procesów będzie niepożądany, w tym status:
 - IV.16.2.3.1. procesu wewnętrznej bazy danych systemu
 - IV.16.2.3.2. serwera aplikacyjnego systemu
 - IV.16.2.3.3. bazy danych sesji
 - IV.16.2.3.4. kolektora i procesora wiadomości log
 - IV.16.2.3.5. błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej)
 - IV.16.2.3.6. stan obciążenia systemu wzrośnie powyżej zadanego poziomu, w tym:
 - IV.16.2.3.6.1. obciążenie systemu (load)
 - IV.16.2.3.6.2. zajętość pamięci

IV.16.3. Serwer UA musi posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:

- IV.16.3.1. badanie łączności IP za pomocą ping, nslookup, traceroute
- IV.16.3.2. wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
 - IV.16.3.2.1. nazwy użytkownika
 - IV.16.3.2.2. adresu MAC
 - IV.16.3.2.3. statusu uwierzytelnienia (udana lub nieudana)
 - IV.16.3.2.4. powodu, jeżeli uwierzytelnienie nieudane
 - IV.16.3.2.5. zakresu czasowego, co do dnia, godziny i minuty
- IV.16.3.3. wykonanie zdalnego polecenia na urządzeniu sieciowym
- IV.16.3.4. ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem:
 - IV.16.3.4.1. definicji serwerów AAA
 - IV.16.3.4.2. protokołu RADIUS
 - IV.16.3.4.3. odkrywania urządzeń
 - IV.16.3.4.4. logowania
 - IV.16.3.4.5. uwierzytelniania Web
 - IV.16.3.4.6. konfiguracji trybu 802.1X
- IV.16.3.5. wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu

IV.17. Dobre praktyki realizacji rozwiązania

IV.17.1. Serwer UA musi spełniać następujące warunki dobrych praktyk realizacji systemu uwierzytelnienia dostępu do sieci:

- IV.17.1.1. System może występować w formie pojedynczego rozwiązania jak też systemu złożonego z kilku komponentów.
- IV.17.1.2. W przypadku zastosowania rozwiązania złożonego z kilku komponentów system zapewnia pojedynczy interfejs konfiguracyjny, zarządzający i monitorujący zapewniający możliwość wymuszenia spójnej polityki bezpieczeństwa dla dostępu LAN/WLAN/VPN.
- IV.17.1.3. Niezależnie od tego czy system występuje w formie pojedynczego rozwiązania lub jest złożony z kilku komponentów, może on być serwisowany jako jeden system w ramach pojedynczej usługi wsparcia.

V. Uruchomienie i wdrożenie systemu.**V.1. W ramach prac wdrożeniowych i uruchomieniowych Zamawiający oczekuje od potencjalnego dostawcy systemu zrealizowania co najmniej poniższych scenariuszy dostępu do sieci:**

- V.1.1. dostęp do dedykowanej sieci WiFi z zabezpieczeniami Enterprise min. WPA2/CCMP-AES z dedykowanym dla niej VLAN'em w wersji tunelowanej i bridge'owanej lokalnie na switch'u do którego jest podpięty AP – switche HP ProCurve2920 i Juniper EX3300, serwer OpenLDAP Zamawiającego, serwer FreeRadius Zamawiającego
- V.1.2. dostęp do dedykowanej sieci WiFi z zabezpieczeniami Personal min. WPA2/PSK/CCMP-AES z dedykowanym dla niej VLAN'em w wersji tunelowanej i bridge'owanej lokalnie na switch'u do którego jest podpięty AP – switche HP ProCurve2920 i Juniper EX3300
- V.1.3. dostęp gościnny do sieci WiFi z zabezpieczeniem w oparciu o dedykowany captive portal z dedykowanym VLAN'em i weryfikacją dostępu przez SMS/e-mail
- V.1.4. dostęp do dedykowanej sieci WiFi do bezpiecznego roaming'u dla użytkowników jednostek naukowych oraz szkolnictwa wyższego zgodnie z wytycznymi Europejskiej konfederacji Eduroam, serwer LDAP Zamawiającego
- V.1.5. dostęp do sieci przewodowej w oparciu o 802.1x dla dedykowanych, wskazanych przez Zamawiającego przełączników sieciowych HP ProCurve 2920 oraz Juniper EX3300, serwer LDAP Zamawiającego, serwer FreeRadius Zamawiającego
- V.1.6. dostęp gościnny do sieci przewodowej w oparciu o captive portal z dedykowanym VLAN'em i weryfikacją dostępu przez SMS/e-mail
- V.1.7. Konfiguracja list ACL dynamicznie przypisywanych użytkownikom w procesie uzyskiwania dostępu do sieci za pomocą atrybutów pobieranych z serwerów Radius/FreeRadius, LDAP/OpenLDAP

VI. Ogólne warunki gwarancji i wsparcia na systemu.

- VI.1. Wszystkie serwery i kontrolery oferowane w ramach zestawu do transmisji bezprzewodowej wifi mają posiadać gwarancję producenta na okres 36 miesięcy realizowaną w reżimie 8x5xNBD.
- VI.2. System zarządzania siecią przewodową i bezprzewodową oraz licencje dostępowe dla AP mają być objęte gwarancją producenta na okres 36 miesięcy realizowaną w reżimie 8x5xNBD.
- VI.3. Punkty dostępowe mają posiadać gwarancję producenta na okres 36 miesięcy oraz posiadać wsparcie producenta, w tym dostęp do bazy wiedzy oraz aktualizacji oprogramowania.
- VI.4. Cały zestaw do transmisji bezprzewodowej wifi ma być objęty wsparciem technicznym Wykonawcy przez okres 36 miesięcy w reżimie 8x5xNBD.