Załącznik nr 8

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

dotyczy:

„Budowa kompleksu budynków w miejscowości Zielonki Parcele w Gminie Stare Babice składającego się z budynku szkolno-dydaktycznego, ośrodka kultury i hali sportowej z zapleczem – Zadanie 18: zakup i dostawa sprzętu i osprzętu sieciowego IT".

Nr referencyjny: **DIMiR / PD / 11 / 12 / 2017**

1. Przedmiotem zamówienia jest zakup i dostawa sprzętu i osprzętu sieciowego IT, na które składać się będzie:
   1.1. Zakup i dostawa przełączników sieci typu LAN warstwy 3 z PoE+ i możliwością pracy w stosie – ilość: 12 (dwanaście) sztuk,
   1.2. Zakup i dostawa wkładki typu SFP+ 10Gbps LR SMF 2km kompatybilnej z oferowanym przełącznikiem - ilość 20 (dwadzieścia) sztuk
   1.3. Zakup i dostawa patchcordu światłowodowego singlemode typu LC-LC, 9/125um, o długości 1 m – ilość: 10 (dziesięć) szt.
   1.4. Zakup i dostawa patchcordu światłowodowego singlemode typu LC-LC, 9/125um, o długości 3 m – ilość: 20 (dwadzieścia) szt.
   1.5. Zakup i dostawa kabla typu DAC SFP+ kompatybilnego z oferowanym przełącznikiem, o długości 1 m – ilość: 8 (osiem) szt.
   1.6. Zakup i dostawa patchcordu RJ45 UTP kat. 6 o długości 1 m – ilość: 100 (sto) szt.
   1.7. Zakup i dostawa patchcordu RJ45 UTP kat. 6 o długości 2 m – ilość: 200 (dwieście) szt.
   1.8. Zakup i dostawa patchcordu RJ45 UTP kat. 6 o długości 3 m – ilość: 300 (trzysta) szt.
   1.9. Zakup i dostawa patchcordu RJ45 UTP kat. 6 o długości 5 m – ilość: 100 (sto) szt.
   1.10. Zakup i dostawa patchcordu RJ45 UTP kat. 6 o długości 10 m – ilość: 20 (dwadzieścia) szt.
2. Wsparcie przy wdrożeniu urządzeń w siedzibie zamawiającego w wymiarze 30h przez inżyniera sieciowego posiadającego doświadczenie w konfiguracji przełączników sieciowych.
3. Dostawa i wdrożenie systemu pracującego w trybie wirtualnej maszyny do monitorowania pracy dostarczonych przełączników sieciowych oraz wysyłania alertów o zaistniałych systuacjach krytycznych.
4. Zakup i dostarczenie - wielozadaniowego systemu zabezpieczeń sieciowych wraz ze wsparciem przy wdrożeniu w wymiarze 20 h wykonanym przez inżyniera certyfikowanego przez producenta systemu.
5. Zakup i dostawa sprzętu sieciowego sieci bezprzewodowej, na który składać się będzie:
   5.1. Zakup i dostawa kontrolera sieci bezprzewodowej wraz z 33 licencjami.
   5.2. Zakup i dostawa punktów dostępowych wewnętrznych – 25 sztuk.
   5.3. Zakup i dostawa punktów dostępowych zewnętrznych – 8 sztuk.
6. Zakup i dostawa serwera rack 1U.
7. zakup i dostawa macierzy dyskowej – 1 sztuka

Ad.1 Wymagania szczegółowe dotyczące przełączników sieci LAN warstwy 3:

1. Wykonawca musi być autoryzowanym partnerem handlowym producenta przedmiotu zamówienia lub sam jest producentem przedmiotu zamówienia.
2. Dostarczony przedmiot zamówienia musi być:
   2.1.1. fabrycznie nowy, oraz pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, oraz jest objęty gwarancją producenta,
   2.1.2. Typ i liczba portów liniowych w ramach urządzenia:
      2.1.2.1. Minimum 48 portów RJ45 - 10/100/1000 Ethernet
      2.1.2.2. Minimum 4 porty na wkładki SFP+ (10Gbps Ethernet).
      2.1.2.3. Wszystkie porty liniowe muszą być z przodu obudowy.
   2.1.3. Wymagane jest, aby minimum 48 portów dostępowych 10/100/1000 obsługiwały standard zasilania poprzez sieć LAN (Power over Ethernet) zgodnie ze standardami IEEE 802.3af oraz IEEE 802.3at. Budżet mocy PoE/PoE+ dla wszystkich portów nie może być mniejszy niż 370W.
   2.1.4. Urządzenie musi obsługiwać minimum 4000 VLAN 802.1q

2.1.5. Urządzenie musi obsługiwać minimum 16200 adresów MAC
2.1.6. Urządzenie musi posiadać min. 1GB pamięci DRAM i 2GB pamięci flash
2.1.7. Parametry fizyczne – możliwość montażu w szafie 19", wielkość urządzenia nie może przekroczyć 1U
2.1.8. Urządzenie musi być pozbawione wentylatorów lub umożliwiać ich programowe wyłączenie przy ograniczeniu budżetu mocy PoE.
2.1.9. Minimalna wydajność przełączania ruchu 134Mpps oraz wymagana minimalna przepustowość matrycy 180Gb/s.
2.1.10. Urządzenie musi posiadać funkcjonalność łączenia w stosy z zachowaniem następującej parametrów:
    2.1.10.1. Do min. 8 jednostek w stosie
    2.1.10.2. Magistrala stackująca o przepustowości co najmniej 40Gbps
    2.1.10.3. Możliwość tworzenia połączeń EtherChannel LACP zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (Cross-stack EtherChannel) – minimum z 6 różnych przełączników w stosie jednocześnie
    2.1.10.4. Jeżeli realizacja funkcji stackowania wymaga dodatkowych modułów/kabli itp. ich dostarczenie w ramach tego postępowania nie jest wymagane. Dopuszczalne jest stackowanie po portach liniowych opisanych w punkcie 1b (SFP+) lub portach dedykowanych.
2.1.11. Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9216 bajtów (Jumbo Frames)
2.1.12. Urządzenie musi wspierać mechanizm QinQ
2.1.13. Obsługa protokołu NTP lub SNTP
2.1.14. Musi zapewniać obsługę min. 1000 tras w bazie Forwarding Information Base (FIB) IPv4 lub IPv6.
2.1.15. Musi zapewniać routing statyczny, dynamiczny i wsparcie dla protokołów multicast: OSPFv2, OSPFv3, RIP, RIP-NG, PIM-SM, PIM-DM, PIM-SSM, PIM-Passive. Jeśli funkcjonalność wymaga dodatkowej licencji – jest ona wymagana na tym etapie postępowania.
2.1.16. Musi zapewniać obsługę protokołów First-Hop Redundancy – np. VRRP zarówno dla IPv4 jaki i IPv6. Jeśli funkcjonalność wymaga dodatkowej licencji – jest ona wymagana na tym etapie postępowania.
2.1.17. Obsługa ruchu multicast – IGMPv2, IGMPv3, MLDv1/2 Snooping.
2.1.18. Wsparcie dla protokołów Per-VLAN Spanning-Tree, IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 252 instancji protokołu STP
2.1.19. Wsparcie dla funkcji BPDU Guard oraz funkcji wykrywania i zabezpieczenia przed pętlami Layer 2.
2.1.20. Wsparcie dla funkcji Auto-MDI/MDI-X na portach 10/100/1000
2.1.21. Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP Server oraz wspierać funkcję DHCP Helper
2.1.22. Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad.
2.1.23. Przełącznik musi obsługiwać następujące mechanizmy bezpieczeństwa:
    2.1.23.1. Minimum 3 poziomów dostępu administracyjnego
    2.1.23.2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL. Wsparcie dla Critical-VLAN, Restricted-VLAN oraz Guest-VLAN.
    2.1.23.3. Obsługa Private VLAN
    2.1.23.4. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    2.1.23.5. Możliwość uwierzytelniania użytkowników w oparciu o portal www (WebAuth)
    2.1.23.6. Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC
    2.1.23.7. Wymagana jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie
    2.1.23.8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176.

2.1.23.9. Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6
2.1.23.10. Obsługa list kontroli dostępu (ACL)
2.1.23.11. Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection
2.1.23.12. Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
2.1.23.13. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne)

2.1.24. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
2.1.24.1. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS)
2.1.24.2. Implementacja co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu WRR lub SRR lub innego podobnego dla obsługi tych kolejek
2.1.24.3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
2.1.24.4. Możliwość mapowania ruchu do określonych kolejek QoS z wykorzystaniem ACL
2.1.24.5. Możliwość ograniczania pasma dostępnego na każdym porcie jednocześnie dla ruchu wychodzącego oraz przychodzącego za pomocą Shapingu lub Policingu.

2.1.25. Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP)
2.1.26. Obsługa protokołu UDLD.
2.1.27. Obsługa protokołu wspierającego topologię pierścienia zbudowaną z przełączników (tzw. Ethernet Ring) – Np. G.8032 lub REP lub MRP lub inny równoważny.
2.1.28. Obsługa protokołu GVRP lub MVRP lub innego równoważnego (np. VTP).
2.1.29. Obsługa protokołu OpenFlow 1.3 lub nowszego dla współpracy z kontrolerem OpenFlow.
2.1.30. Wsparcie dla AAA z wykorzystaniem serwerów TACACS oraz Radius.
2.1.31. Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli
2.1.32. Urządzenie musi posiadać port konsoli szeregowej (RJ45 lub DB9), port konsoli USB (dla laptopów bez portu szeregowego) oraz port Ethernet typu out-of-band (niezależny od portów liniowych opisanych w pkt.1) – do zarządzania.
2.1.33. Urządzenie musi być wyposażone w port USB umożliwiający podłączenie pamięci flash.
2.1.34. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją.
2.1.35. MTBF (Mean Time Between Failure) nie może być mniejszy niż 600000 godzin.

Ad.4 Wielozadaniowy system zabezpieczeń sieciowych musi spełniać następujące właściwości / umożliwiać realizację następujących funkcjonalności:

1. System zabezpieczeń firewall musi być dostarczony w formie dwóch maszyn wirtualnych pracujących w klastrze. W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość oprogramowania musi być dostarczana i wspierana przez jednego producenta.
2. System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 4 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 2 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 800 000 jednoczesnych połączeń.
3. System zabezpieczeń firewall musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA.
4. Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach

inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).

5. System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.
6. System zabezpieczeń firewall musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.
7. System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
8. Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).
9. System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
10. System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
11. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 4 Gbit/s.
12. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).
13. Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
14. Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
15. System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.
16. System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
17. System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
18. System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
19. System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
20. System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.
21. System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji

użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.

22. System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
23. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
24. System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
25. System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
26. Wymagania podstawowe identyfikacja użytkowników
27. System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
28. System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.
29. System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.
30. Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.
31. Wymagania ochrony IPS, AV, anty-spyware, URL, zero-day
32. System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL.
33. System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
34. System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
35. System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
36. System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

37. System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
38. System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
39. System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
40. System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
41. System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
42. System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
43. System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
44. System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
45. System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
46. System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
47. System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
48. System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany.
49. System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
50. System zabezpieczeń firewall musi posiadać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 2 Gbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.
51. Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".
52. Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”.

53. System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.
54. Wymagania dodatkowe NAT, DoS, IPSEC VPN, SSL VPN, QoS
55. System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
56. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
57. System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
58. System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.
59. System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.
60. System zabezpieczeń firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną). Musi istnieć możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci.
61. System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0.
62. System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
63. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
64. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
65. Wymagania dodatkowe środowisko wirtualne vmware
66. System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.
67. Wymagania zarządzanie i raportowanie
68. Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
69. System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji

urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.

70. System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian, których są autorami.
71. System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
72. System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
73. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
74. System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.
75. System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
76. System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 60 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
77. System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
78. System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
79. System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.
80. System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
81. System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
82. System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.
83. System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
84. System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
85. System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
86. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym.
87. Wraz z systemem zabezpieczeń wymagane jest dostarczenie opieki technicznej ważnej przez okres 3 lat. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz jego autoryzowanego polskiego przedstawiciela, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, aktualizację bazy ataków IPS, definicji wirusów, bazy kategorii stron WWW, dostęp do systemu „Sand-Box" a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.
88. Dostawca powinien być autoryzowanym partnerem producenta rozwiązania, tj. powinien przedstawić zaświadczenie potwierdzające taką certyfikację, a także 2 imienne certyfikaty autoryzowanych inżynierów wystawione dla jego pracowników.

Ad. 5.1 Wymagania szczegółowe dotyczące kontrolera sieci bezprzewodowej:

Element	Charakterystyka
Architektura	– Pełna kompatybilność i współpraca z oferowanymi AP. Zamawiający wymaga aby urządzenia pochodziły od tego samego producenta, niemniej jednak dopuszcza się zastosowanie urządzeń różnych producentów pod warunkiem uzyskania pełnej kompatybilności i wymaganej funkcjonalności. – Kontoler musi oferować możliwość uruchomienia na środowisku wirtualnym Vmware oraz Microsoft Hyper-V. Architektura musi być zgodna ze standardem European Telecommunications Standards Institute (ETSI) NFV – Możliwość pracy w klastrze active-active z balansowaniem rozłożenia podłączonych punktów dostępowych. Awaria pojedynczego urządzenia w klastrze nie może mieć wpływu na ruch z urządzeń klienckich WIFI, ani powodować degradacji usługi WIFI np. konieczność ponownej autentykacji i asocjacji – Kontroler dostarczony z licencjami na obsługę min. 33 AP (rozwiązanie musi zapewniać gotowość rozbudowy systemu czyli możliwość licencyjnego rozszerzenia do obsługi min. 1000 AP dla pojedynczego kontrolera oraz do 3000 AP w przypadku klastra kontrolerów) – Kontroler musi wspierać obsługę min. 25000 aktywnych użytkowników sieci bezprzewodowej (w przypadku klastra kontrolerów rozwiązanie musi wspierać obsługę do 60000 aktywnych użytkowników) – Możliwość skonfigurowania minimum 2000 niezależnych sieci WLAN (SSID) dla zapewnienia separacji usług w sieci bezprzewodowej. – Obsługa adresacji IPv4 oraz trybu dual-stack IPv4/IPv6 – Kontroler musi oferować przesyłanie ruchu bezpośrednio z AP zgodnie z regułami sieci przewodowej L2/L3, bez konieczności tunelowania całości ruchu przez kontroler – Kontroler musi zapewniać wysoką odporność na awarie usług dla klientów, czyli w przypadku awarii kontrolera (nawet pracującego w trybie pojedynczym) nie zostanie przerwana usługa pracy sieci WIFI dla podłączonych użytkowników ani możliwość podłączania się nowych użytkowników. Musi to być zapewnione minimalnie dla następujących sieci WIFI: o bez autentykacji o z autentykacją WPA2/PSK o dla sieci z portalem gościnnym (o ile baza danych użytkowników gościnnych jest trzymana na zewnętrznym serwerze) o dla sieci z autentykacją i uwierzytelnianiem z WPA2/AES (tzw Enterprise WPA2). W przypadku gdy zewnętrzna baza danych RADIUS jest trzymana na zewnętrznym serwerze o dla sieci z autentykacją przez portal WWW do serwerów AD lub LDAP – Wsparcie dla trybu multitenant, czyli możliwość kreowania osobnych podmiotów biznesowych z dedykowanymi usługami kontrolera: o możliwość definiowania osobnych uprawnień administracyjnych dla danego podmiotu o możliwość uruchamiania poszczególnych usług typu Dostęp Gościnny lub HotSpot dla określonego podmiotu o możliwość tworzenia osobnych grup/stref AP dla danego podmiotu z granulacją wersji oprogramowania (grupy AP pracują z innymi wersjami oprogramowania w celu obsługi AP, które nie są już obsługiwane w nowszej wersji) oraz możliwość zdefiniowania osobnego kody kraju per grupa/strefa tak aby AP mogły pracować w krajach gdzie występują inne regulacje radiowe o wybór dostępnych kanałów dla grupy AP o wybór szerokości kanału dla danej grupy o osobne raportowanie dla danego podmiotu – Funkcjonalność pozwalająca na blokowanie użytkowników, którzy nie otrzymali bądź zmienili adres IP otrzymany z serwera DHCP. – Obsługa protokołu 802.11e (WMM), w celu zapewnienia odpowiedniej jakości usług (QoS) poszczególnym usługom przenoszonym w sieci (głos, video, dane). – Funkcjonalność tworzenia list kontroli dostępu warstw L2/3/4 z funkcjonalnościami zaawansowanego filtrowania ruchu. Właściwe filtrowanie ruchu odbywać musi się na AP, tak by odfiltrować niepożądany ruch już na wejściu do sieci.

	– Funkcjonalność stosowania różnych list kontroli dostępu dla poszczególnych WLAN. – Funkcjonalność rozpoznawania i raportowania wykorzystywanych aplikacji per user, per AP, per SSID – Funkcjonalność zablokowania określonych aplikacji per SSID – Funkcjonalność wykrywania i raportowania obcych AP. Raportowanie w postaci alarmów oraz powiadomienia mail. Raportowanie musi oferować możliwość granulacji zależnego od typu zdarzenia: o Raportuj wszystkie obce punkty dostępowe o Raportuj tylko obce punkty dostępowe generujące następujące zdarzenia tzw. Malicious AP: SSID Spoofing, obcy AP podłączony do sieci kablowej L2, MAC Spoofing o Możliwość ochrony użytkowników sieci bezprzewodowej przed podłączaniem się do tzw. Malicious AP – Kontroler musi oferować ustrukturyzowany interfejs programistyczny Restful/JSON API umożliwiający budowanie własnych aplikacji do zarządzania i monitorowania kontrolera i zarządzanych przez niego punktów dostępowych. Wymagane jest aby dla API był dostępny publiczny dokument opisujący sposób komunikacji z API tzw. programming API reference guide. – Kontroler musi oferować możliwość zbierania informacji na temat uruchomionych sieci bezprzewodowych, obsługiwanych punktów dostępowych oraz podłączonych urządzeniach oraz budowania raportów ze wsteczną datą minimum do 30 dni. Restart kontrolera nie powinien powodować utraty zebranych danych i przedstawianych raportów – W przypadku wykorzystania kontrolera jako klienta NAS dla RADIUSa możliwość określenia sposobu przedstawienia się kontrolera do serwera RADIUS z wykorzystaniem: WLAN BSSID, AP MAC lub innego zdefiniowanego przez administratora – W przypadku pracy kontrolera jako RADIUS proxy możliwość podglądu statystyk komunikacji z serwerem RADIUS takich jak: liczba sesji autentykacyjnych, liczba sesji accountingowych, liczba requestów CoA (Change of Authorization, RFC5176) w tym odpowiedzi DM (Disconnect Message) – Możliwość podglądu komend wydanych przez administratora systemu – Możliwość podglądu informacji statystycznych do 3 dni w zakresie podłączonych urządzeń. Co najmniej musi być możliwość określenia dokładnego czasu podłączenia się do danego SSID, BSSID dla danego podłączenia, adres IP przydzielonego dla danego podłączenia, liczba bajtów wysłana i odebrana dla danego podłączenia – Możliwość eksportu do serwera Syslog informacji na temat sesji podłączonych urządzeń, co najmniej następujących danych: klient mac adres, klient IP adres, adres IP przeznaczenia, rodzaj protokołu, adres mac punktu dostępowego, z którego sesja była inicjowana
Funkcjonalności Wifi	– Obsługa 802.1Q VLAN z możliwością zarówno ustawienia osobnego VLANu dla każdej sieci WLAN oraz nadrzędnie przydzielanie użytkownika do odpowiedniego VLAN-u zgodnie z odpowiedzią serwera RADIUS, pozwalając na pełną separację ruchu. – Funkcjonalność ukrywania poszczególnych sieci WLAN (SSID). – Funkcjonalność uruchamiania/wyłączania poszczególnych sieci WLAN (SSID) w określonych godzinach bądź dniach tygodnia (harmonogram tygodniowy z ziarnistością co najmniej godzinną) – Funkcjonalność automatycznego wyłączenia rozgłaszania danego BSSID w przypadku niedostępności bramy wyjścia (ang. Default Gateway). – Funkcjonalność ograniczania prędkości przesyłu danych klientów per każda sieć WLAN (SSID), konfigurowalne osobno dla kierunku uplink i downlink. – Funkcjonalność ograniczania maksymalnej ilości użytkowników w poszczególnych sieciach WLAN (na każdy moduł radiowy AP), w trosce o zapewnienie odpowiedniej jakości połączeń. – Wsparcie dla funkcjonalności przenoszenia klientów pomiędzy pasmami radiowymi danego AP. Wymagana możliwość procentowego zdefiniowania obciążenia pasma w zależności od ilości klientów. – Funkcjonalność izolacji klientów sieci radiowej (uruchamiane osobno na każde SSID) uniemożliwiającą im bezpośrednią komunikację ze sobą w ramach tej samej sieci WLAN – Funkcjonalność zachowania ciągłości działania sieci WLAN z autentykacją 802.1X oraz autentykacją o wewnętrzny captive portal (np. dostęp gościnny) nawet w przypadku awarii połączenia pomiędzy punktem dostępowym, a kontrolerem sieci. – obsługa standardu 802.11r oraz 802.11k – obsługa standardu 802.11w MFP – Możliwość mapowania ustawień QoS User Priority/Class of Service protokołu 802.1p na wartości DSCP – Obsługa VLAN pooling

	– Obsługa Proxy ARP
Zarządzanie AP	– Funkcjonalność automatycznego wykrywania kontrolera przez AP w warstwie L2 i L3. W przypadku L3 musi być możliwość wykorzystania przynajmniej 3 trybów wykrywania kontrolera: o opcja 43 serwera DHCP o przez zapytanie DNS o ręczne zdefiniowanie na poziomie AP – Automatyczny upgrade oprogramowania systemowego na AP z wykorzystaniem bezpiecznego protokołu SSL. – Dynamiczne zarządzanie częstotliwościami radiowymi oraz mocą wszystkich AP w celu optymalnego pokrycia terenu i unikania interferencji. – Optymalizacja doboru kanału przez AP w czasie rzeczywistym. – Funkcjonalność automatycznego równoważenia obciążenia AP przez klientów sieci radiowej, pozwalająca zapobiec sytuacji nadmiernego obciążenia pojedynczego AP przez wielu klientów, podczas gdy sąsiednie AP byłyby nie obciążone. – Wsparcie dla funkcjonalności client admission control, czyli zdefiniowania progu pojemności, po którego punkt dostępowy nie będzie przyjmował nowych połączeń. W ramach funkcjonalności musi istnieć możliwość wyznaczenia progu na podstawie minimum następujących parametrów: liczba podłączonych urządzeń, maksymalna utylizacja radia, średnia przepustowość dla urządzenia. – Kontroler musi oferować funkcjonalność mesh (sieć kratowa) pozwalającą na radiowe podłączenie AP bez przyłącza kablowego do innego AP w sieci (uplink radiowy). System powinien automatycznie optymalizować topologię mesh tak, aby zapewnić najlepszą przepustowość i automatycznie przywracać poprawną pracę systemu w przypadku awarii. W przypadku awarii danego uplinku, sieć automatycznie powinna przełączyć AP do alternatywnego uplinku w tym samym lub sąsiadującym drzewie mesh. Działanie sieci mesh może być uzależnione od wybory typu AP. – Kontroler musi zapewniać możliwość monitorowania parametrów pracy punktów dostępowych wraz z porównaniem tych parametrów do innych punktów dostępowych zdefiniowanych w grupie. Monitorowanie parametrów radiowych musi umożliwiać definiowanie warunków krytycznych punktu dostępowego powyżej którego przekroczeniu punkt dostępowy jest oznaczany odpowiednim statusem. Dla punktów dostępowych musi być konieczność zdefiniowania następujących parametrów pracy punktu dostępowego: opóźnienie na interfejsie radiowym, utylizacje kanału radiowego, liczba prób podłączeń niezakończona sukcesem. Wbudowany analityczny system musi automatycznie prowadzić ranking punktów dostępowych wraz z historycznymi wartościami przez co znacząco usprawniony jest proces izolowania problemu i określenia zakresu problemu, który może degradować jakość pracy sieci WIFI. Analityczny system musi umożliwiać śledzenie trendów pracy parametrów punktu dostępowego do 30 dni wstecz.
Autentykacja	– Wsparcie dla następujących algorytmów i mechanizmów bezpieczeństwa sieci radiowej: WEP, WPA-TKIP, WPA2-AES, 802.11i, PSK. – Wsparcie trybu prywatny PSK, w którym to każdy użytkownik sieci w pojedynczym SSID otrzymuje swój własny klucz PSK służący do autentykacji do sieci bezprzewodowej – Autentykacja użytkowników sieci radiowej za pośrednictwem zewnętrznych serwerów AAA (nie mniej niż Active Directory, LDAP, Radius) oraz za pomocą lokalnej bazy danych na Kontrolerze. – Funkcjonalność Captive Portal – Uwierzytelnianie Hotspot za pomocą protokołu WISPr. – Wsparcie dla standardu HotSpot 2.0 (Wi-Fi Certified Passpoint). – Obsługa gościnnych sieci WLAN (Guest WLAN) z autoryzacją na podstawie generowanych guestpass'ów. Wymagana jest obsługa dostarczania Guest Pass przez usługę SMS. Wbudowana lokalna baza danych kont gościnnych musi umożliwiać wsparcie dla 10000 kont gościnnych. – Kontroler musi umożliwiać identyfikację typu urządzenia/systemu operacyjnego użytkownika sieci bezprzewodowej wraz z funkcjonalnością przypisania odpowiedniej polityki dostępu (VLAN, limity prędkości itp.) dla urządzenia na podstawie typu/systemu operacyjnego. – Możliwość włączenia protokołu LDAP przez SSL

Zarządzanie	– Dostęp do interfejsu zarządzającego kontrolera tylko przez bezpieczne szyfrowane protokoły takie jak SSH i HTTPS. Jeżeli urządzenie obsługuje protokoły telnet lub http, musi istnieć możliwość ich wyłączenia. – Szyfrowanie ruchu zarządzającego pomiędzy Kontrolerem, a AP. – Obsługa protokołu SNMPv3. – Monitorowanie parametrów Kontrolera i generowanie na ich podstawie statystyk. Kontroler musi oferować 30 dniowe statystyki dla następujących parametrów: użycie procesora, użycie pamięci, ilość ruchu typu management – Kontroler musi posiadać wbudowany generator ruchu pozwalający na rzeczywisty pomiar przepływności pakietowej pomiędzy Kontrolerem a dowolnym AP. – Możliwość prezentacji graficznej rozmieszczenia punktów dostępowych na wbudowanych mapach Google wraz z wyświetleniem minimum informacji o: ▪ Nazwie punktu dostępowego ▪ Modelu punktu dostępowego ▪ Adresu IP ▪ MAC adresu ▪ Czasie ostatniego pojawienia się w systemie ▪ Ilości podłączonych urządzeń klienckich – Możliwość prezentacji rozmieszczanie punktów dostępowych na zdefiniowanych własnych mapach wraz z wyświetleniem minimum informacji o: ▪ Nazwa punktu dostępowego ▪ Adres IP ▪ Kanały pracy AP ▪ Liczba podłączonych klientów ▪ Opóźnienie dla każdego interfesju radiowego ▪ Utylizacje każdego interfejsu radiowego ▪ Liczba prób podłączeń klientów które nie zakończyły się podłączeniem do sieci tzw. connection failures – Wbudowana funkcjonalność diagnostyki klientów sieci WIFI z wizualnym przedstawieniem fazy podłączenia lub braku podłączenia klienta do sieci WIFI. Wizualizacja musi nie tylko przedstawiać fazy podłączenia do interfejsu radiowego, ale również fazy autentykacji do serwera AAA czy serwera DHCP wraz z informacjami na temat zwracanych parametrów np. lista atrybutów RADIUS czy adres IP otrzymany z serwera DHCP jak również informacje na temat ewentualnych błędów. Wszystko ma być dostępne z jednego wbudowanego narzędzia dostępnego w kontroler bezprzewodowy bez konieczności składania raportów z kilku różnych narzędzi. Funkcjonalność wizualnego diagnozowania połączeń ma być dostępna dla sieci typu Open, PSK oraz 802.1X – Wsparcie dla Role-Based Policy umożlwiające granulacje polityk dostępowych do sieci w zależności od roli użytkownika. Dla danego użytkownika być możliwość określenia polityk ruchu czyli VLANu dostępowego, ograniczenia przepustowości, list kontroli dostępu L3/L4 oraz dostępnych aplikacji – Wsparcie dla rozpoznawania, kontroli i monitorowania aplikacji musi być realizowane w oparciu o silnik deep-packet inspection. System musi oferować listę dostępnych aplikacji, które chcemy kontrolować w zależności od kategorii lub umożliwiać zdefiniowanie aplikacji opisanych manualnie na podstawie portu, rodzaju protokołu. Dla skategoryzowanych aplikacji musi być możliwość upgradu sygnatur aplikacji. Upgrade sygnatur nie może być osobno płatny lecz wchodzić w zakres wykupionego wsparcie technicznego

Ad. 5.2 Wymagania szczegółowe dotyczące punktów dostępowych wewnętrznych:

1. Punkt dostępowy musi wspierać następujące tryby pracy
   1.1. standalone (zarządzanie punktem odbywa się poprzez interfejs przeglądarki internetowej, telnet i SSH)
   1.2. zarządzany przez zewnętrzny kontroler sieci bezprzewodowej
   1.3. jako samodzielny kontroler sieci bezprzewodowej umożliwiający zarządzanie grupą do 20 punktów dostępowych. Punkt dostępowy w roli kontrolera musi zapewniać także obsługę klientów 802.11a/b/g/n/ac
2. Równoczesna praca w paśmie 2,4 GHz oraz 5 GHz
3. Obsługa standardów 802.11a/b/g/n/ac
4. Obsługa standardu bezprzewodowego 802.11d, 802.11h

5. Praca w trybie MIMO 2x2:2
6. Wsparcie dla:
   6.1. Tx DL MU-MIMO
   6.2. Rx MCS 8-9 (256-QAM),
   6.3. Rx A-MPDU of A-MSDU,
   6.4. Tx SU beamformer,
   6.5. Low Density Parity Check coding
7. Anteny wbudowane i zintegrowane z punktem dostępowym z wzmocnieniem minimum 3 dBi dla 2.4 GHz oraz 5 GHz
8. Wsparcie dla technologii beamforming 802.11ac TxBF oraz technologii formowania wiązki dla klientów typu „legacy" (802.11a/b/g/n) umożliwiające osiągnięcie dodatkowego wzmocnienia na poziomie minimum 4 dB
9. Certyfikowany przez Wi-Fi Alliance w zakresie Passpoint Online Signup (OSU) and Policy Provisioning
10. Minimalna czułość odbiornika dla 2.4 GHz: -101 dBm
11. Obsługa minimum 400 podłączonych stacji klienckich
12. Wbudowane wsparcie dla analizy spektrum widma
13. Obsługa sieci typu mesh
14. Obsługa 802.3at PoE oraz 802.3af PoE
15. Obsługa Multicast IP video streaming
16. Nie mniej niż 16 BSSID z własną polityką dostępu i regułami QoS
17. Nie mniej niż 4 kolejki QoS per stacja kliencka i wsparcie standardu 802.11e/WMM
18. Obsługiwane protokoły / standardy zabezpieczeń: WEP/WPA-PSK/WPA-TKIP/WPA2-AES/802.11i
19. Obsługa trybu pracy Router z funkcjonalnością NAT i serwera DHCP
20. Obsługa autentykacji 802.1x dla portu Ethernet: tryb suplikanta i autentykatora
21. Kanały pracy:
    21.1. IEEE 802.11n: 2.4 – 2.484 GHz oraz 5.15 – 5.25 GHz, 5.25 – 5.35 GHz, 5.47 – 5.725 GHz, 5.725 – 5.85 GHz
22. Obsługiwana szybkość transmisji:
    22.1. 802.11ac: 6.5 - 867Mbps
    22.2. 802.11n: 6.5Mbps – 300Mbps
    22.3. 802.11a: 54, 48, 36, 24, 18, 12, 9, 6Mbps
    22.4. 802.11b: 11, 5.5, 2, 1 Mbps
    22.5. 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps
23. Charakterystyka punktów dostępowych:
    23.1. Zasilanie poprzez PoE lub zasilacz 12V DC
    23.2. Wyposażony w dwa port RJ-45, auto MDX, jeden z możliwością zasilania PoE, auto-sensing 10/100/1000mbps
    23.3. Praca w temperaturze 0-50C, wilgotność do 95% (bez kondensacji)
    23.4. Wyposażone w gniazdo bezpieczeństwa umożliwiające zamontowanie linki bezpieczeństwa zabezpieczającej urządzenia przed kradzieżą
24. Optymalizacja pracy systemu poprzez funkcje:
    24.1. Automatycznego wyboru najlepszego kanału pracy w oparciu o realną przepustowość/pojemność kanałów dla 2.4 lub 5 GHz wraz z możliwością przeniesienia klienta na optymalny kanał z wykorzystaniem standardu 802.11h
    24.2. Airtime fairness
25. Zgodność ze standardem VLAN 802.1q
26. Wbudowany port USB 2.0 umożliwiający obsługę sensorów standardu BLE lub wbudowana funkcjonalność BLE

Ad. 5.3 Wymagania szczegółowe dotyczące punktów dostępowych zewnętrznych:

1. Punkt dostępowy musi wspierać następujące tryby pracy
   1.1. standalone (zarządzanie punktem odbywa się poprzez interfejs przeglądarki internetowej, telnet i SSH)
   1.2. zarządzany przez zewnętrzny kontroler sieci bezprzewodowej

1.3. jako samodzielny kontroler sieci bezprzewodowej umożliwiający zarządzanie grupą do 20 punktów dostępowych. Punkt dostępowy w roli kontrolera musi zapewniać także obsługę klientów 802.11a/b/g/n/ac
2. Równoczesna praca w paśmie 2,4 GHz oraz 5 GHz
3. Obsługa standardów 802.11a/b/g/n/ac
4. Praca w trybie MIMO 2x2:2
5. Szerokość kanału 20/40 dla 2,4GHz oraz 20/40/80 (dla 802.11ac)
6. Wsparcie dla 32 BSSID
7. Obsługa 802.3at PoE oraz 802.3af PoE, nie dopuszczana jest degradacja parametrów usług punktu dostępowego przy zasilaniu 802.3af
8. Obsługa minimum 500 podłączonych stacji klienckich
9. Anteny wbudowane i zintegrowane z punktem dostępowym z wzmocnieniem minimum 3 dBi dla 2.4 GHz oraz 5 GHz
10. Kanały pracy:
    10.1. IEEE 802.11n: 2.4 – 2.472 GHz oraz 5.15 – 5.25 GHz, 5.25 – 5.35 GHz, 5.47 – 5.725 GHz, 5.725 – 5.825 GHz
11. Obsługiwana szybkość transmisji:
    11.1. 802.11ac: 6.5 - 867Mbps
    11.2. 802.11n: 6.5Mbps – 300Mbps
    11.3. 802.11a: 54, 48, 36, 24, 18, 12, 9, 6Mbps
    11.4. 802.11b: 11, 5.5, 2, 1 Mbps
    11.5. 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps
12. Obsługiwane protokoły / standardy zabezpieczeń: WEP/WPA-PSK/WPA-TKIP/WPA2-AES/802.11i
13. Wyposażony w minimum jeden port Ethernet 10/100/1000 Base-T
14. Praca w temperaturze od -20^{o}C do +65 ^{o}C
15. Punkt dostępowy zgodny ze standardem odporności na warunki atmosferyczne IP67
16. Zamawiający nie dopuszcza użycia nieintegralnej, zewnętrznej obudowy w celu spełnienia wymagań
17. Waga nieprzekraczająca 1kg (nie wliczając zestawu montażowego)
18. Wymiary nieprzekraczające 20 x 16 x 10 cm (nie wliczając zestawu montażowego)

Ad. 6 Wymagania szczegółowe dotyczące serwera rack:

1. Obudowa typu Rack 19” wraz z elementami niezbędnymi do montażu w szafie (zestaw do zamontowania serwerów na wysuwanych szynach w szynach w szafie 19”) o wysokości nie przekraczającej 1U
2. Płyta główna zaprojektowana i trwale oznakowana przez producenta serwera z możliwością zainstalowania minimum 2 procesorów
3. Chipset płyty głównej rekomendowany przez producenta procesora
4. Procesor minimum ośmiordzeniowy w architekturze x86 64-bitowy, dedykowany do pracy w serwerach wieloprocesorowych.
5. Ilość zainstalowanych procesorów: 2 szt.
6. Ilość pamięci obsługiwanej przez serwer: 768GB.
7. Ilość slotów pamięci: min. 24
8. Zainstalowana pamięć: min. 32GB na każdy procesor.
9. Dedykowany kontroler dyskowy RAID zapewniający funkcjonalność RAID na poziomach 0, 1, 10, 5, 50
10. Typ i ilość zainstalowanych dysków: min. 4 dyski 1TB typu „hot-swap” SATA 2,5” min 7200rpm, z możliwością zainstalowania co najmniej 10 dysków 2,5” w technologii „hot-swap”
11. Interfejsy sieciowe: min. 4 porty Ethernet 10/100/1000 RJ-45 oraz min. 4 porty SFP+ 10Gb wspierające mechanizm DPDK
12. Karta do zdalnego zarządzania: tak
13. Min. 2 redundantne zasilacze o mocy 650-870 W „hot-swap”
14. Obsługiwane systemy operacyjne: Microsoft Windows Server, Linux (Red Hat, SUSE), VMware
15. Gwarancja: min. 12 miesięcy z czasem reakcji serwisu w następnym dniu roboczym.

Ad.7 Wymagania szczegółowe dotyczące macierzy dyskowej:

1. Procesor 4 rdzeniowy o taktowaniu min. 2.1 GHz
2. Pamięć RAM 8GB
3. Maksymalna możliwa ilość pamięci RAM: 64GB
4. Obudowa do montażu w szafie rack wraz z szynami, wysokość 2U
5. Ilość kieszeni hot-swap (wymiana dysków podczas pracy bez wyłączania macierzy) na dyski
6. 3,5”: 8
7. Ilość kieszeni M.2: 2
8. Ilość zainstalowanych dysków: 4 sztuki, każdy o pojemności 6TB, przeznaczone do urządzeń NAS, zgodne z oferowanym urządzeniem (znajdujące się na liście dysków zgodnych publikowanej przez producenta)
9. 4 interfejsy sieciowe Gigabit RJ-45 Ethernet
10. 2 interfejsy sieciowe 10GbE SFP+
11. Dwa wbudowane redundantne zasilacze
12. Dwa wbudowane porty USB 3.0 i cztery wbudowane porty USB 2.0
13. Wsparcie dla RAID 0,1,5,6,10, RAID hot spare, migracja poziomów Online RAID
14. Wbudowana obsługa iSCSI z obsługą min. 256 LUN
15. Obsługa protokołów współdzielenia plików CIFS/SMB, AFP, NFS, FTP/FTPS, HTTP/HTTPS,
16. Obsługa Windows ACL
17. Obsługiwane protokoły sieciowe: TCP/IP, DHCP, CIFS/SMB, NFS, HTTP, HTTPS, FTP, Telnet,
18. SSH, iSCSI, SNMP
19. Obsługiwane systemy plików dla dysków zewnętrzynych: EXT3, EXT4, NTFS, FAT32, HFS+
20. Certyfikat zgodności z systemami wirtualizacyjnymi: VMWARE, HYPER-V, CITRIX
21. Współpraca z Microsoft Active Directory w zakresie autoryzacji dostępu
22. Powiadamianie o zdarzeniach za pomocą e-mail
23. Połączenia szyfrowane: HTTPS, FTP z SSL/TLS
24. Wsparcie dla funkcji Wake On LAN
25. Możliwość rozbudowy funkcjonalności oprogramowania za pomocą dodatkowych pakietów instalowanych z poziomu menu administracyjnego