**MCPS.ZP/KBCH/351-3-1/2020 Załącznik nr 1 do Zapytania ofertowego**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Dostawa urządzeń sieciowych na potrzeby Mazowieckiego Centrum Polityki Społecznej**

Zamówienie obejmuje dostawę wraz konfiguracją sprzętu sieciowego na potrzeby Mazowieckiego Centrum Polityki Społecznej. Wykonawca zobowiązany jest dostarczyć urządzenia zgodne ze specyfikacją opisaną poniżej do wskazanych lokalizacji Zamawiającego:

# Urządzenie UTM (unified threat management) o przepustowości min. 6Gbps – 1 szt.

## Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.

## Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

## Interfejsy, Dysk, Zasilanie

1. System realizujący funkcję Firewall musi dysponować minimum **10 portami Gigabit Ethernet RJ-45**.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

## Parametry wydajnościowe

1. W zakresie Firewall’a obsługa nie mniej niż **700 tys.** jednoczesnych połączeń oraz **35 tys.** nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż **6 Gbps**.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż **1.7 Gbps**.
4. Wydajność szyfrowania IPSec VPN nie mniej niż **6.2 Gbps**.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum **1.4 Gbps**.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum **700 Mbps**.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum **720 Mbps**.

## Funkcje Systemu Bezpieczeństwa

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.

## Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
	1. Translację jeden do jeden oraz jeden do wielu.
	2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

## Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
2. Wsparcie dla IKE v1 oraz v2.
3. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
4. Obsługa protokołu Diffie-Hellman grup 19 i 20.
5. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
6. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
7. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
8. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
9. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
10. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
11. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
12. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
13. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
14. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

## Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
	1. Routingu statycznego.
	2. Policy Based Routingu.
	3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

## Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

## Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, rar.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

## Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

## Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

## Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

## Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
	1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
	2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
	3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign-On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

## Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

## Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

## Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać certyfikacje ICSA lub EAL4 dla funkcji Firewall.

## Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Aplikacji,
2. IPS,
3. Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android),
4. Analiza typu Sandbox,
5. Antyspam,
6. Web Filtering,
7. bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

## Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# Urządzenie UTM (unified threat management) o przepustowości min. 10Gbps – 1 szt.

## Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.

## Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

## Interfejsy, Dysk, Zasilanie

1. System realizujący funkcję Firewall musi dysponować minimum:
	1. **16 portami Gigabit Ethernet RJ-45.**
	2. **8 gniazdami SFP 1 Gbps.**
	3. **2 gniazdami SFP+ 10 Gbps.**
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

## Parametry wydajnościowe

1. W zakresie Firewall’a obsługa nie mniej niż **1.4 mln** jednoczesnych połączeń oraz **50 tys.** nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż **10 Gbps**.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż **2.1 Gbps**.
4. Wydajność szyfrowania IPSec VPN nie mniej niż **10 Gbps**.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum **2.5 Gbps**.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum **900 Mbps**.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum **900 Mbps**.

## Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

## Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
	1. Translację jeden do jeden oraz jeden do wielu.
	2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

## Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
	1. Wsparcie dla IKE v1 oraz v2.
	2. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
	3. Obsługa protokołu Diffie-Hellman grup 19 i 20.
	4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
	5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
	6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
	7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
	8. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
	9. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
	1. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
	2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
	3. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

## Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
	1. Routingu statycznego.
	2. Policy Based Routingu.
	3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

## Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

## Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, rar.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

## Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

## Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

## Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

## Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
	1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
	2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
	3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign-On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

## Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

## Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

## Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

1. ICSA lub EAL4 dla funkcji Firewall.
2. ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
3. ICSA dla funkcji SSL VPN.

## Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Aplikacji,
2. IPS,
3. Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android),
4. Analiza typu Sandbox,
5. Antyspam,
6. Web Filtering,
7. bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

## Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# Przełącznik sieciowy 48-portowy – 2 szt.

Dostarczone przełączniki sieciowe powinny posiadać następujące parametry:

1. Co najmniej 48 portów gigabitowych w standardzie 100/1000BaseT
2. Co najmniej 4 porty 1000BaseX ze stykiem definiowanym przez SFP (dopuszcza się porty typu Combo, współdzielone z portami 10/100/1000BaseT)
3. Możliwość rozbudowy o dodatkowe 4 porty SFP+ lub 4 porty 10GBaseT lub 1 port QSFP+ (wszystkie opcje muszą być dostępne. Dodatkowe porty muszą być w pełni niezależne od portów podstawowych i muszą być dostępne z przodu urządzenia. Nie dopuszcza się uzyskania portów SFP+ poprzez zastosowanie kabli rozszywających.
4. Minimum 2 dedykowane porty stackujące (niezależne od portów SFP+), pozwalające na połączenie w stos minimum 10 przełączników. Agregowana prędkość magistrali stackującej nie może być mniejsza niż 100Gb/s. Stos musi być widoczny jako jedno urządzenie (wspólne zarządzanie z jednej linii komend, analogiczne do przełącznika modularnego). Dopuszcza się rozwiązanie, w którym porty stackujące dostępne są w postaci opcjonalnego modułu (niezależnego od modułów 10Gb i 40Gb opisanych w punktach powyższych).
5. Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika), nie licząc magistrali stackującej
6. Wydajność: minimum 112 Mp/s
7. Tablica adresów MAC o wielkości minimum 32000 pozycji
8. Obsługa ramek Jumbo
9. Minimum 4GB pamięci stałej typu Flash, minimum 1GB pamięci RAM
10. Minimum 12MB bufora pakietów
11. Automatyczne wykrywanie punktów bezprzewodowych podłączonych do przełącznika (**co najmniej 2 punktów opisanych w punkcie 4**), automatyczne konfigurowanie portów, do których są one podłączone (minimum sieć VLAN, CoS)
12. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych
13. Port USB
14. Dwa, modularne, wewnętrzne zasilacze prądu zmiennego. Przy wykorzystaniu obydwu źródeł zasilania – zasilacze powinny pracować w trybie redundantnym oraz być wymieniane na gorąco.
15. Routing IPv4 – minimum: statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
16. Routing IPv6 – minimum: statyczny, RIPng, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
17. Obsługa protokołu VRRP
18. Wielkość tablicy rutingu: minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6
19. IGMPv1/v2/v3 Snooping; MLDv1/v2 Snooping, PIM Dense Mode, PIM Sparse Mode
20. Obsługa VXLAN
21. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
22. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN
23. Funkcja Root Guard oraz BPDU protection
24. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie
25. Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping
26. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
27. Obsługa standardu 802.1p – min. 8 kolejek na porcie
28. Funkcja mirroringu portów
29. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
30. Funkcja autoryzacji użytkowników zgodna z 802.1x
31. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
32. RADIUS Accounting
33. Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3
34. OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic.
35. Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP)
36. Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow.
37. Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow.
38. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
39. Zarządzanie poprzez port konsoli (pełne) (RS-232 i USB), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
40. Obsługa Syslog
41. Obsługa SNTPv4 lub NTP
42. Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku
43. Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej
44. Wsparcie dla funkcji Private VLAN lub równoważnego
45. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link Detection Protocol (DLDP) lub równoważnego
46. Minimalny zakres pracy od 0°C do 45°C
47. Wysokość w szafie 19” – 1U, głębokość nie większa niż 50 cm
48. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
49. 10 letnia gwarancja (serwis) producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie technicznego (niezależnego od zgłaszania usterek) wsparcia telefonicznego w trybie 8x5 przez okres co najmniej 10 lat. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

# Bezprzewodowe punkty dostępowe – 4 szt.

Dostarczone bezprzewodowe punktu dostępowe powinny spełniać następujące wymagania:

1. Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz a/n/ac wave 2/ax, oraz 2.4GHz b/g/n/ax.
2. Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej
3. Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera:
	1. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https
	2. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki
	3. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania.
4. Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2:
	1. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego
	2. W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny
	3. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe
	4. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję
	5. Tworzenie klastra do 130 urządzeń
5. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP
6. Punkt dostępowy musi mieć możliwość pracy jako analizator widma
7. W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa
8. W system musi być wbudowany serwer DHCP
9. W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów
10. Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:
	1. EAP-TLS
	2. PEAP-MSCHAPv2
	3. PEAP-GTC
	4. TTLS-MSCHAPv2
11. Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP
12. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID
13. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN
14. Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez:
	1. Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania
	2. Zewnętrzny portal WWW
15. Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT
16. Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne
17. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:
	1. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe
	2. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu
	3. Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma
	4. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału
	5. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz
	6. Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac wave 2 oraz starszych (802.11b/g)
	7. Wsparcie dla 802.11d oraz 802.11h
	8. Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane
18. Minimalizacja interferencji związanych z sieciami 3G/4G LTE
19. Punkt dostępowy musi mieć wbudowany moduł Bluetooth Low Energy (BLE5.0) (co najmniej 7dBm) wykorzystywany w systemie nawigacji wewnątrzbudynkowej
20. Punkt dostępowy musi mieć wbudowany moduł Zigbee (802.15.4) (co najmniej 6dBm)
21. Obsługa roamingu klientów w warstwie 2
22. Obsługa monitoringu przez SNMP
23. Obsługa logowania na zewnętrznym serwerze SYSLOG
24. W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci
25. W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci
26. Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:
	1. Widok diagnostyczny prezentujący problemy z sygnałem/prędkością
	2. Wykorzystanie pasma
	3. Ilość klientów korzystających z systemu/interferujących
	4. Ilość ramek wejściowych/wyjściowych dla każdego radia
	5. Ilość odrzuconych/błędnych ramek/s dla każdego radia
	6. Szum tła dla każdego radia
	7. Wyświetlanie logów systemowych
27. Punkt dostępowy musi posiadać co najmniej 2 wbudowane anteny pracujące w trybie 2x2 MIMO, z parametrami co najmniej: 4.3 dBi dla 2,4GHz, 5.5 dBi dla 5 GHz
28. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac 1 Wave, 802.11ac 2 Wave, 802.11ax
29. Praca w trybie SU MIMO 2X2:2 dla 5GHz
30. Specyfikacja radia 802.11a/n/ac/ax:
	1. Obsługiwana technologia OFDM oraz OFDMA
	2. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
	3. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm
	4. Prędkości transmisji:
		* 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a,
		* MCS0-MCS23 (6,5Mbps do 450Mbps) dla 802.11n
		* MCS0-MCS9, NSS = 1-4 (6.5 Mbps do 1733 Mbps) dla 802.11ac
		* MCS0 do MCS11, NSS = 1-2 (3.6 Mbps do 574 Mbps) dla 802.11ax (2,4GHz)
		* MCS0 do MCS11, NSS = 1-4 (3.6 Mbps do 4803 Mbps) dla 802.11ax (5GHz)
	5. Obsługa HT – kanały 20/40MHz dla 802.11n
	6. Obsługa VHT – kanały 20/40/80/160MHz dla 802.11ac
	7. Obsługa HE – kanały 20/40/80/160MHz dla 802.11ax
	8. Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz
	9. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac
	10. Wsparcie dla:
		* MRC (Maximal ratio combining)
		* CDD/CSD (Cyclic delay/shift diversity)
		* STBC (Space-time block coding)
		* LDPC (Low-density parity check)
		* Technologia TxBF
31. Specyfikacja radia 802.11b/g/n/ax:
	1. Technologia direct sequence spread spectrum (DSSS), OFDM, OFDMA
	2. Typy modulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM, 256-QAM, 1024-QAM
	3. Moc transmisji konfigurowalna przez administratora
32. Punkt dostępowy musi posiadać co najmniej:
	1. 1 interfejs 100/1000BaseT
		* z funkcją auto-sensing link oraz MDI/MDX
		* z funkcją PoE/PoE+
		* ze wsparciem dla standardu 802.3az Energy Efficient Ethernet (EEE)
	2. interfejs konsoli RS-232 (RJ-45) lub USB
	3. interfejs USB 2.0 (Typ-A, niezależny od portu konsoli)
	4. przycisk przywracający konfigurację fabryczną
	5. slot zabezpieczający Keningston
33. Parametry pracy urządzenia:
	1. Temperatura otoczenia (zakres minimalny): 0-50 º C
	2. Wilgotność (zakres minimalny): 5% - 92%
	3. Obsługiwane standardy:
* Ethernet IEEE 802.3 / IEEE 802.3u
* Power-over-Ethernet IEEE 802.3af
* Wireless IEEE 802.11a/b/g/n/ac/ax
	1. Znak CE
	2. EN 60601-1-1, EN60601-1-2
1. Punkt dostępowy zasilony przy użyciu zgodnym ze standardem 802.3at PoE lub przy pomocy lokalnego zasilacza DC (zasilacz nie musi być dołączony)
2. Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac
3. Wszystkie dostępne na urządzeniu funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
4. Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni
5. Punkt dostępowy musi być objęty co najmniej ograniczoną dożywotnią gwarancja producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła zamiennik. Gwarancja musi być realizowana bezpośrednio przez producenta sprzętu.

**Do dostarczonych urządzeń należy dostarczyć, zainstalować i skonfigurować
system monitoringu i zarządzania spełniający następujące wymagania:**

1. Monitoring stanu sieci i analiza problemów
2. Możliwość podglądu stanu pracy urządzeń
3. Możliwość podglądu podłączonych klientów
4. Możliwość sprawdzania alertów po nazwie puntu dostępowego lub przełącznika , adresu
mac oraz numerze seryjnym
5. Informację o wersji oprogramowania FW zainstalowanego na urządzeniach
6. Możliwość prześledzenia indywidualnych danych klienta radiowego takich jak ilość
przesłanych danych, poziom sygnału, prędkość połączenia, historię asocjacji oraz rodzaj
urządzenia.
7. Intensyfikacja obcych urządzeń w sieci wykorzystując system WIDS
8. Możliwość uruchomienia linii poleceń bezpośredni na punkcie dostępowym lub przełączniku.
9. Dostęp gościnny
10. Umożliwienie samo rejestracji użytkownika w naszej sieci gościnne
11. Umożliwienie dostępu sponsorowanego dla pracowników nie należących do IT takich jak
recepcjonistka itp. dla tworzenia tymczasowych kont gościnnych
12. Umożliwienie logowania się do sieci gościnnej z wykorzystaniem portali społecznościowych
takich jak Facebook, Google+, Twitter and LinkedIn
13. Analityka obecności
14. Funkcjonalność umożliwiająca zbieranie informacji na temat osób odwiedzających lokalizację na podstawie danych wysyłanych przez urządzenia mobilne w zasięgu pracy sieci WiFI. Uzyskanie danych w czasie rzeczywistym oraz danych historycznych na temat ilości osób przewijających się przez lokalizacje, ile osób postanowiło wejść do obiektu jak długo w nim spędzili. Funkcjonalność może być uruchamiana poprzez wykupienie dodatkowych licencji.
15. Monitoring i zarządzenia aplikacjami.
16. System ma mieć możliwość wyświetlania informacji na temat aplikacji wykorzystywanych przez klientów radiowych. Umożliwić wyświetlanie rodzaju aplikacji, jej nazwy, kategorii wyświetlanych stron www oraz ich reputacji. System musi umożliwić tworzenie reguł określających dostęp do wybranych aplikacji oraz stron www.
17. Możliwość automatycznej konfiguracji nowych urządzeń.
18. System musi mieć możliwość raportowania minimum dla poszczególnych funkcji:
	1. Zdefiniowanej grupy użytkowników
	2. Raport sieciowy zawierający minimum:
		* Ilość AP
		* Model AP
		* Całkowitą ilość użytkowników per SSID
		* Klientów bezprzewodowych
		* Ilość przesłanych danych bezprzewodowo wartość szczytowa tzw. Peak Usage
		* Top 10 kategorii stron web odwiedzanych przez użytkowników
		* Przełączniki
		* Modele przełączników
		* Top 10 portów przełączników wg obciążenia (Tx/Rx)
		* Statystyki szczytowe Uplinku przewodowego
	3. Raporty bezpieczeństwa
		* Całkowita ilość wykrytych obcych (Rogue) punktów bezprzewodowych
		* Całkowita ilość Wireless Intrusions
		* Zgodność z PCI
		* Wyświetla wynik weryfikacji PCI Compliance jako Pass lub Fail
		* Inwentaryzacja klientów
		* Top 10 klientów wg obciążenia
		* Top 10 AP wg wykorzystania sieci
		* Całkowite obciążenie wg SSID klientów bezprzewodowych
	4. Raport pojemności
		* Top 25 AP pod względem ilości użytkowników wartości szczytowe ( peak client)
		* Top 25 przełączników pod względem ilości przesłanych danych
		* Ilość wykorzystanych licencji
	5. Raport Aplikacyjny
		* Top 10 aplikacji używanych przez klientów
		* Top 10 kategorii stron web odwiedzanych przez klientów
		* Top 10 aplikacji używanych przez klientów wg SSID
	6. Raport sesji klientów
		* Rodzaj systemu operacyjnego używanego przez klienta
		* Rodzaju połączenia SSID
		* Adresu mac przynależnego do producenta urządzeń
	7. Raport stanu środowiska radiowego
		* Zmian kanałów pracy (AP)
		* Zmian mocy nadawania (AP)
		* Średniego poziomu szumów (w dBm)
		* Średniej zajętości kanału
		* Całkowitej ilości błędów