Ostatnia aktualizacja: 03/ 2012

CC Otwarte Systemy Komputerowe Sp. z o.o.

Sieci WiFi dla przedsiębiorstw

Sieci WiFi – rozwój i oczekiwania

Bezprzewodowe sieci lokalne zyskują coraz większą popularność w zastosowaniach biznesowych. Wydajność dostępnych rozwiązań rośnie - obecnie oferowane są już punkty dostępowe generacji „n" o przepustowościach dochodzących do 600Mbps. Rośnie też liczba urządzeń wykorzystujących WiFi - takich jak np. smartfony, tablety, telefony VoIP, itd. Użytkownicy urządzeń mobilnych coraz częściej oczekują dostępu WiFi w lokalizacjach takich jak: hotele, kampusy akademickie, obiekty sportowe, czy placówki służby zdrowia.

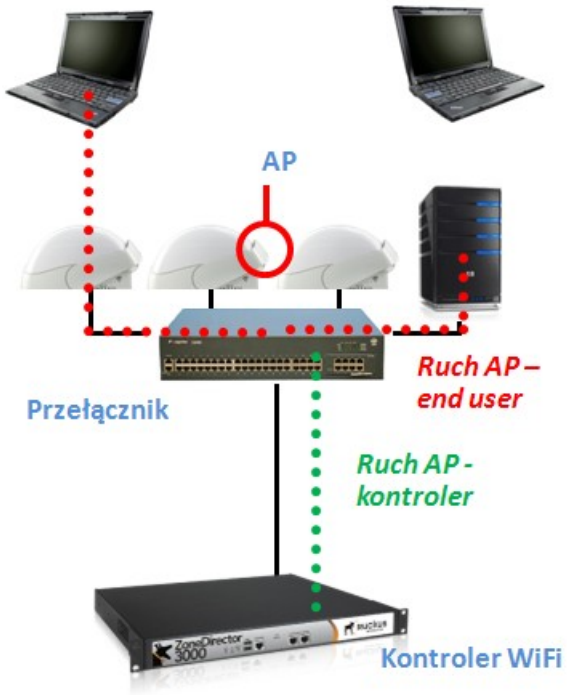
Wymagania stawiane wdrożeniom WiFi w większej skali są zupełnie odmienne od tych stawianych rozwiązaniom „domowym", czy też rozwiązaniom małej skali wykorzystującym kilka punktów dostępowych (AP). Technologia nadawcza w obydwu przypadkach jest taka sama, jednak rozwiązania średniej i dużej skali wymagają zaadresowania następujących dodatkowych kwestii:

- zapewnienie wydajnej obsługi bardzo wielu klientów jednocześnie,
- obsługa roamingu dla urządzeń mobilnych – możliwie transparentnie dla użytkowników,
- zapewnienie bezpieczeństwa użytkowników oraz własnej infrastruktury IT – np. wykrywanie obcych i/lub wrogich punktów dostępowych,
- zapewnienie autoryzacji i rozliczania użytkowników – wymagana może być integracja z domeną Windows, captive portal, itp.,
- zapewnienie kontroli dostępu w wydzielonych wirtualnych strefach: np. dostęp dla gości powinien być ograniczony do dostępu internetowego, pracownicy tymczasowi powinni dodatkowo posiadać dostęp do poczty elektronicznej i wybranych serwisów intranetowych, a uprawnienia pracowników etatowych powinny pokrywać się z uprawnieniami, jakie posiadają w tradycyjnej sieci
- wydajna obsługa ruchu VoIP,
- optymalizacja liczby punktów dostępowych – mniej AP – niższe koszty,
- centralizacja zarządzania i diagnostyki punktów dostępowych,
- zapewnienie realizacji usług w nietypowych warunkach otoczenia: np. gdy niemożliwe jest bezpośrednie połączenie AP do sieci – praca w trybie mesh i praca dwu-zakresowa,
- praca w trudnych warunkach fizycznych: zastosowania zewnętrzne, zastosowania przemysłowe,
- obsługa specyficznych potrzeb branżowych: np. dystrybucja sygnału IPTV w hotelach.

ul. Rakowiecka 36
02-532 Warszawa
tel. +48 22 646-68-73
fax +48 22 606-37-80
e-mail:office@cc.com.pl
Web: http://www.cc.com.pl/

Sieci WiFi – technologia i możliwości

Architektura średnich i dużych sieci WiFi bazuje na dwu elementach: punktach dostępowych (AP) oraz kontrolerach. Pojedyńczy punkt dostępowy zapewnia łączność WiFi w swoim otoczeniu, może też realizować wybrane funkcje administracyjne, kontroler służy do zarządzania AP-kami i realizacji funkcji bezpieczeństwa, autoryzacji użytkowników, realizacji roamingu, itp. Podział ról między AP a kontroler (lub kontrolery) różni się w zależności od dostawcy sprzętu: w niektórych rozwiązaniach AP realizują praktycznie wyłącznie funkcje radiowe, całość „logiki" związanej z obsługą ruchu sieciowego przypada na kontroler. W innych rozwiązaniach AP może pracować w zakresie podstawowych funkcji autonomicznie – posiada własny interfejs zarządzający dostępny przez WWW, jednak funkcje takie jak np. captive portal czy autoryzacja realizowane są na kontrolerze. W jeszcze innych rozwiązaniach oferowany jest „rozproszony kontroler" realizowany na wybranym AP.



W zależności od rozwiązania różnie kształtuje się ruch sieciowy między AP, urządzeniami użytkowników a kontrolerem – patrz rysunek obok.

W większych instalacjach używa się więcej niż jednego kontrolera: w układzie redundantnym (klaster HA) lub hierarchicznym – np. lokalne sieci WiFi nadzorowane są przez lokalne kontrolery, te z kolei nadzorowane są przez główny kontroler z centrali.

Sieci WiFi – zaawansowane funkcje i rozwiązania

WIDS – ochrona sieci

Otwartość medium komunikacji jakim jest WiFi sprawia, że z założenia sieć bezprzewodowa jest bardziej narażona na „podsłuch", gdyż nie wymaga on fizycznego dostępu do infrastruktury (ruch można np. podsłuchać z parkingu przed biurem lub z innego piętra). Z tego powodu sieci bezprzewodowe stwarzają nowe możliwości szpiegostwa przemysłowego i wycieków danych, nawet w przypadku, gdy sieć firmowa jest poprawnie zabezpieczona – np. zestawione ad-hoc połączenie pomiędzy siecia LAN, a osobą znajdującą się fizycznie poza firmą, pozwala na przesłanie znacznej ilości danych w krótkim czasie. Odrębne zagrożenie stanowi ryzyko utraty prawnie chronionych danych osobowych.

Dlatego też współczesne rozwiązania WiFi oferują ochronę na poziomie kontolera – posiada on wbudowane funkcje typowe dla systemu firewall, a także funkcje specyficzne dla sieci WiFi - takie jak: wykrywanie obcych AP czy wykrywanie spoofingu (podszywania się).

ul. Rakowiecka 36
02-532 Warszawa
tel. +48 22 646-68-73
fax +48 22 606-37-80
e-mail:office@cc.com.pl
Web: http://www.cc.com.pl/

Funkcje te połączone są też z mechanizmem powiadamiania administratora o wykrytych zagrożeniach.

Kontrola dostępu, izolacja klientów

Kontrola dostępu ma szczególne znaczenie w środowisku biurowym, gdzie np. istotne jest oddzielenie uprawnień pracowników, konsultantów oraz gości. Autoryzacja użytkowników może następować przy pomocy bazy danych wprowadzonej przez administratora do kontrolera lub też poprzez protokół LDAP, RADIUS – dzięki czemu możliwa jest integracja np. z Microsoft ActivDirectory lub usługami 802.1X. Uwierzytelnienie gości może następować poprzez tzw. „captive portal" - użytkownik łączący się z siecią jest przekierowywany do strony WWW, na której musi się zautoryzować. Autoryzacja następuje typowo przy pomocy nazwy użytkownika i hasła, ale można też np. posłużyć się wydanym przez operatora kodem jednorazowym o limitowanym czasie ważności. Na podstawie przeprowadzonej autoryzacji użytkownik może być przypisany do określonego VLAN-u oraz uzyskać określone uprawienia w sieci. Kontroler WiFi może też wykrywać próby wielokrotnie nieudanych autoryzacji i blokować prowadzące je urządzenia (tzw. „blacklisting").

Kontrola pasma

Zaawansowane systemy WiFi realizują podział i kontrolę dostępnego pasma radiowego poprzez osobne kolejkowanie ruchu w zależności od SSID, grupy użytkowników i indywidualnego użytkownika. Dzięki temu można np. wydajniej obsłużyć dostęp dla pracowników limitując pasmo przeznaczone dla gości – już na poziomie AP.

Mechanizm „client load ballancing" pozwala z kolei na optymalizację przydziału klientów do AP w tych lokalizacjach, w których zasięg poszczególnych AP się pokrywa, dzięki czemu następuje optymalizacja wykorzystania punktów dostępowych i ruch sieciowy może zostać obsłużony efektywniej, co jest szczególnie ważne w obszarach o dużym zagęszczeniu użytkowników (np. sale audytoryjne i konferencyjne, itp.)

Obsługa VoIP

Obsługa bezprzewodowych telefonów Voice over IP narzuca dodatkowe wymagania na sieć WiFi, są to przede wszystkim: zapewnienie dobrego pokrycia sygnałem WiFi, rezerwacja i stablilność minimalnego pasma oraz zapewnienie roamingu użytkowników przemieszających się w zasięgu różnych AP. Istotna jest też autoryzacja urządzeń VoIP pochodzących od różnych producentow i pracujących z różnymi systemami: iOS, Symbian, BlackBerry, Android.

ul. Rakowiecka 36 tel. +48 22 646-68-73 e-mail:office@cc.com.pl
02-532 Warszawa fax +48 22 606-37-80 Web: http://www.cc.com.pl/

Topologia mesh

W określonych warunkach podłączenie AP do sieci Ethernet może być trudne lub nawet niemożliwe, tak jest np. w przypadku AP montowanych w otwartym terenie – w realizacji sieci osiedlowych oraz w środowiskach przemysłowych (np. duże hale, lub parki maszynowe gdzie prowadzenie okablowania jest kosztowne). W takich sytuacjach należy rozważyć realizację sieci WiFi o topologii „mesh" (siatka) w której sygnał prowadzony jest od AP do AP drogą radiową. Możliwe są też rozwiązania, w których sygnał dystrybowany jest pasmem 5Ghz do AP pracujących w paśmie 2,4GHz.

***Rysunek** – przykład osiedlowej sieci WiFi, w której połączenie AP zrealizowano jako „mesh".*

Wymagania branżowe

Zastosowanie: / Wymagania:	Biuro / średnia firma	Biuro, korporacja, wiele oddziałów	Sale konferen-cyjne	Obiekty sportowe	Hotele	Przemysł	Kampus / osiedle
Autoryzacja użytkowników	X	X			X	X	
Bezpieczeństwo	X	X			X	X	
Integracja z LDAP, RADIUS, MS AD	X	X				X	
Zróżnicowane uprawnienia użytkowników	X	X				X	
Obsługa VoIP	X	X				X	
Roaming			X	X		X	X
Mesh				X		X	X
Duża gęstość użytkowników	X	X	X	X			
AP zewnętrzne / trudne warunki fizyczne						X	X
IPTV i obsługa transmisji mediów strumieniowych					X		X

ul. Rakowiecka 36
02-532 Warszawa
tel. +48 22 646-68-73
fax +48 22 606-37-80
e-mail:office@cc.com.pl
Web: http://www.cc.com.pl/

Słownik

- **AP – Access Point** – punkt dostępowy sieci WiFi zgodny ze standardem 802.11a/b/g/n
- Captive Portal -
- **WIDS** – Wireless Intrusion Detection – oprogramowanie wykrywające i blokujące zagrożenie dla bezpieczeństwa sieci WiFi oraz na styku WiFi i sieci przewodowej.
- **Rogue Access Point** - nawet w przypadku dobrze zabezpieczonej sieci lub w przypadku gdy firma nie stosuje technologii WiFi punkt dostępowy podłączony do sieci LAN przez nieautoryzowaną osobę (np. w miejsce komputera stacjonarnego) może być wykorzystany do przechwycenia części ruchu sieciowego lub do uzyskania dostępu do komputerów pracowników (zwłaszcza notebooków).
- **Wirless uplink** – połączenie typu ad hoc zestawione między komputerem podłączonym do sieci lokalnej, a komputerem poza firmą może być wykorzystane do transmisji poufnych danych na zewnątrz firmy. Ten scenariusz może być zrealizowany zarówno poprzez klasycznego szpiega przemysłowego, jak i przez nieświadomego pracownika, którego komputer został przejęty przez hackera.
- **Instant Access Point** – technologia firmy Aruba polegająca na wirtualizacji funkcji kontrolera i ich realizacji w AP.
- **BeamFlex** – technologia firmy Ruckus polegająca na formowaniu pola sygnału WiFi przy pomocy zestawu wielu anten o różnej polaryzacji. Dzięki zmiejszeniu zakłóceń, oraz zwiększeniu mocy sygnału AP jest w stanie wydajniej obsłużyć większą liczbę klientów

Od czego zacząć?

Wybór rozwiązania bezprzewodowego należy rozpocząć od sformułowania kilku podstawowych pytań technicznych oraz biznesowych:

- Ilu użytkowników bezprzewodowych liczy moja sieć i ilu będzie liczyć za rok?
- Czy mam odziały lub biura regionalne i czy chcę wdrożyć sieć bezprzewodową także w nich? Jak duże i na ile autonomiczne są oddziały?
- Jakie jest fizyczne rozmieszczenie pomieszczeń i gdzie powinna być dostępna sieć WiFi? Czy możliwe jest wyróżnienie obszarów o zwiększonym zapotrzebowaniu na dostęp do sieci?
- Czy sieć bezprzewodowa będzie dostępna w pomieszczeniach nie biurowych – tj. np. w halach produkcyjnych lub na otwartym powietrzu, albo też w obszarach cechujących się szczególnie trudnymi warunkami środowiskowymi (wysoka lub niska temperatura, itp)? Czy konieczne będzie zastosowanie punktów dostępowych o podwyższonej odporności na wpływy środowiska?
- Czy poziom uprawnień użytkowników będzie zróżnicowany? Czy chcemy rozgraniczyć uprawnienia pracowników, gości, pracowników sezonowych, itp. ?
- Czy rozważamy wykorzystanie bezprzewodowego VoIP (VoWLAN)?

ul. Rakowiecka 36 tel. +48 22 646-68-73 e-mail:office@cc.com.pl
02-532 Warszawa fax +48 22 606-37-80 Web: http://www.cc.com.pl/

- Jak będą autoryzowani użytkownicy? Czy wymagana będzie integracja z domeną Windows, systemem VPN, itp.?

- Na ile istotne są dla nas zagrożenia związane z utratą poufnych danych / szpiegostwem przemysłowym? Czy chcemy wykrywać tego typu zagrożenia i automatycznie reagować na nie?

Przed rozpoczęciem wyboru producenta systemu wireless powinniśmy przygotować następującą (lub podobną) tabelkę:

• Całkowita liczba użytkowników w centrali i ew. oddziałach • Liczba oddziałów w których ma być wdrożony WLAN	_____ _____
Powierzchnia przestrzeni biurowej i innej, na której ma być wdrożona sieć WiFi	_____
Czy jest wymagana autoryzacja domeny lub podobna?	[TAK] [NIE]
Czy mają być zastosowane zróżnicowane uprawnienia ?	[TAK] [NIE]
Czy będzie wdrożony VoWLAN (VoIP na WiFi)?	[TAK] [NIE]
Czy wymagane będzie raportowanie z wykorzystania sieci WLAN?	[TAK] [NIE]
Czy chcemy wykrywać i automatycznie reagować na zagrożenia takie jak „Rogue AP”	[TAK] [NIE]

Wybrane referencje CC w zakresie rozwiązań firewall i ochrony danych:

- BRE Corporate Finance S.A.,
- Biuro Trybunał Konstytucyjnego
- CA IB S.A.
- Sodexo Pass Polska Sp z o.o.
- FM Polska Sp z o.o. (FM Logistic)
- Krajowe Biuro Wyborcze
- Ministerstwo Sprawiedliwości
- Narodowe Centrum Badań Jądrowych
- Nestle Polska S.A.
- Opera TFI
- PGE S.A.
- Bank Millennium S.A.
- PBP Bank Polska S.A.
- Provident Polska S.A.,
- RockWool Polska S.A.,
- Uniwersytet Warszawski, Wydział Chemii
- Urząd M.st. Warszawa – Ursynów,
- Zelmer

Więcej informacji o firmie znajdziecie Państwo w Internecie, na stronach: **http://www.cc.com.pl/**

Kontakt:
Dział Techniczny: tech@cc.com.pl

Dział Handlowy: sales@cc.com.pl

ul. Rakowiecka 36 tel. +48 22 646-68-73 e-mail:office@cc.com.pl
02-532 Warszawa fax +48 22 606-37-80 Web: http://www.cc.com.pl/