

A biztonsági és hálózatüzemeltet szakemberek nem ok nélkül tartanak a hagyományos wireless technológiától. Míg a felhasználói oldalról –a notebook-ok, PDA-k, VoIP telefonok terjedésével- egyre nagyobb az igény a hálózat mobilitásának növelésére, a hagyományos vagy nem kell en fejlett technológiák számtalan problémát okoznak:

„Plug and pray”: a hatalmas költséggel kiépített, gondosan beállított határvédelmi megoldások nem tudják megvédeni a hálózatot az új dimenzióból érkező támadásokkal szemben.

„Number est omen”: az egyedi Wi-Fi eszközök növelik a hálózat menedzselhetetlenségét. Négy-öt wireless hozzáférési pont már kezelhetetlenné tehet egy hálózatot.

„Lassú az Internet” effektus: a Wi-Fi kapcsolat sebessége jóval elmarad a kábeles hálózatétól.

„Nem m ködik az Internet” effektus: a wireless eszközök egymással interferálva leronthatják az átviteli teljesítményt és az alkalmazások m kódése bizonytalanná válhat.

„Nightmare in the air”: a hibakeresés rémálommá válik. Nem csak a saját, de a szomszédos wireless eszközök is megzavarják hálózatunkat.

Az Aruba biztonságos vállalati Wi-Fi hálózat

Megfelelve a **legmagasabb biztonsági követelmények** elvárásainak (FIPS-140-2, CC-EAL2, ICISA) az Aruba Wi-Fi hálózat képes akár magasabb szintű biztonságot nyújtani, mint a megszokott kábeles hálózatok, úgy a betörésbiztonság, mint az üzembiztonság tekintetében. Teljesítményét tekintve ma a Wi-Fi hálózat már **költséghatékony alternatívája lehet az Ethernet hálózatnak** is, hiszen akár **több mint 180 Mbps valós átviteli kapacitása** a legtöbb igényt b-ven kielégíti.

Akár sok ezer eszköz is egyszer en, központosítottan menedzselhet . A Microsoft világméret Aruba Wi-Fi hálózatában például **több mint 13.000 Wi-Fi eszköz szolgál ki 80.000 felhasználót**.

Szakítva a hagyományos port centrikus hálózati modellel, az Aruba számára a biztonság mellett legfontosabb a mobilitás. Az Aruba **user centric network** elve azt jelenti, hogy a felhasználó hálózati elérését nem az határozza meg, hogy honnan csatlakozik, hanem hogy milyen jogosultságokkal rendelkezik a hálózatban. Csatlakozzon egy másik irodából, épületb- l, vagy akár otthonról, **a felhasználó mindig ugyanazt látja a hálózaton: amit a jogosultságai megengednek**.

Nem véletlen, hogy a világ vezet vállalatai és intézményei Aruba Wi-Fi hálózatra támaszkodnak. **7.000 ügyfele a terület 2. legnagyobb gyártójává teszi**, közéjük tartozik a Microsoft, Google, eBay, SAP, Samsung, Sony, Flextronics, Bridgestone, Black&Decker, Yahoo, Red Bull, American Express, Henkel, Intel, Ohio State University, Washington University, Yale, Stanford és a British Telecom.

Az Aruba biztonságos vállalati wireless hálózat legfőbb elnyei:

■ Menedzsment és üzembehelyezés

- Vállalati szintű menedzsment, akár több ezer Access Point központi kezelése.
- Vékony AP eszközök, nincs szükség elzetes konfigurációra a beillesztéshez.
- A hálózati infrastruktúra nem igényel változtatást, nincs szükség VLAN konfigurációkra vagy a wireless hálózat leválasztására.
- Tipikusan egyszer bb, gyorsabb és biztonságosabb illeszkedés bármely homogén vagy inhomogén hálózatba ezen eszközök Wi-Fi megoldásainál is
- Virtuális SSID rendszer, tetsz leges számú SSID létrehozása, önálló IP tartományokkal, t zfalszabályokkal és autentikációval. Egyszer en szétbontható (akár külön VLAN-okba) a vállalati és a vendég adatforgalom (vállalati SSID, vendég SSID). Sávzélesség menedzsment lehet ségek a virtuális SSID-khez.

■ Rádiófrekvencia-menedzsment

- Access Pointok automatikus csatornaválasztása akár századmásodpercenként utánhangolva
- Access Pointok adáser ssége akár századmásodpercenként utánhangolva
- Kliensek adáser sségének beállítása kliensszoftver nélkül
- Airtime Fairness, band steering, air performance protection

■ Biztonság

- Egyedülálló integrált, min sített t zfal (CC EAL 2, FIPS 140-2, ICASA), wireless-wired és wireless-wireless irányban is.
- Integrált VPN-koncentrátor
- Titkosítás a klienst l a kontrollerig, megszakítás nélkül
- Az Access Pointokban nincs a titkosításra, a felhasználókra vagy a hálózatra vonatkozó információ (a kontroller IP-címét kivéve)
- Integrált Wireless IDS/IPS, a rosszindulatú AP-k és wireless bridgek lebénítása. A támadók pontos lokalizációja és kizárása. Támadások felismerése akár szignatúra alapon is.
- Integrált Network Access Control, vagy saját NAC eszköz esetén egyszer integráció.
- Roaming szolgáltatás az AP eszközök között. Ha a használt AP eszköz elérhetetlenné válik, felhasználó kapcsolatai nem szakadnak meg, 30ms-on belül átvált a következ elérhet Access Pointra, melyhez kliensszoftver nem szükséges.
- *Remote Network* funkciók. A *Remote AP*k segítségével a kisebb irodák hálózata a központból konfigurálható és menedzselhet .