Vállalati WIFI használata az OTP Banknál

Ujvári Dániel – OTP BANK – IKO – rendszermérnök

2013. május. 23.

IT Üzemeltetési Igazgatóság

otpbank
Megbízunk egymásban

OTP BANK ITÜIG – IKO kompetenciák

- Alap hálózati infrastruktúra tervezés és üzemeltetés
- Cisco IP telefónia és hagyományos TDM rendszerek
- Bankcsoport szintű Videokonferencia hálózat
- **Központi és fióki WIFI infrastruktúra tervezés**

A WIFI hálózat iránti igény kialakulása

Az OTP Bankban egymással szinte párhuzamosan 3 területen merült fel igény WIFI hálózat kiépítésére

- Felsővezetői mobilitás, személyenként olykor több mobil eszköz
- Irattárban használt vonalkód olvasó PDA eszközök mobil használata
- Fióki ügyfél WIFI, a várakozási idő élménydúsabb eltöltésére

A megfogalmazott elvárások (központi)

- Tervezés és kivitelezés a biztonsági szabályzatokkal való összhangban történhet
- Teljes RF lefedettség a bank központi épületeiben a mobilitás miatt (Voice over WIFI)
- A cél nem csak internet hozzáférés

  Egységes vezeték nélküli infrastruktúra, többféle céllal

  Korábbi sziget wifik kiváltása (nincs managment)

  Kalóz wifik feltérképezése
- Lényeges jellemzői:
  - Részben a bank meglévő infrastruktúráját használja
  - Egyelőre a központi épületekben érhető el
  - Jelenleg 4db állandó és néhány ideiglenes SSID (VIP, Belső, Normál net, Vendég net)
  - Különböző azonosítási metódusok az egyes SSID-ken
  - Cisco Bring Your Own Device (BYOD) megoldás az alapja.

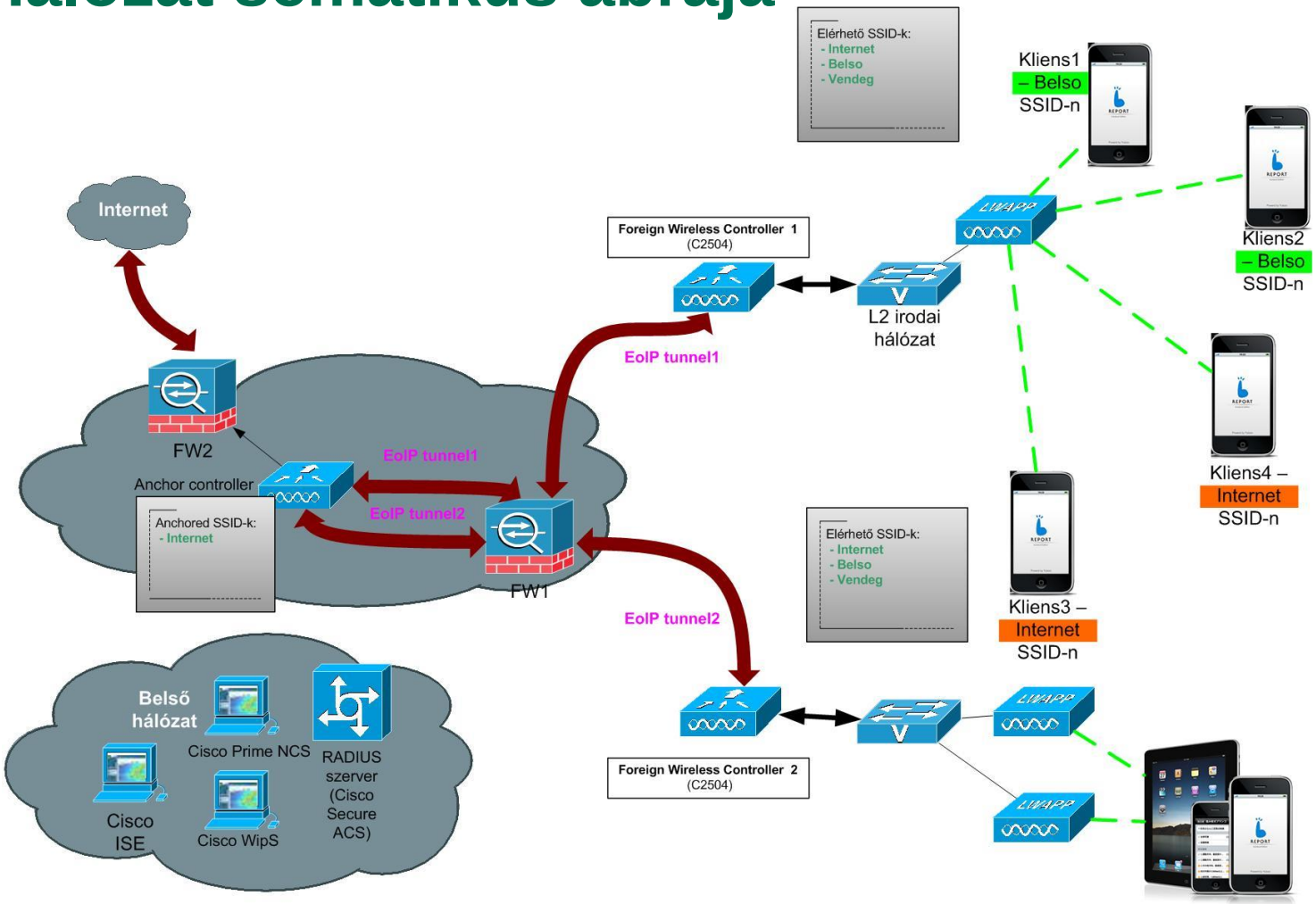
A megfogalmazott elvárások (fióki)

- Teljesen független a központi WIFI-től és a banki hálózattól
- Csak internet elérés

- Teljesen nyitott, Hot Spot jellegű, de a forgalom szűrve van (CISCO ScanSafe – felhő alapú)
- Fiókok ügyfélterében

- Helyi ADSL-vonalakon megy ki a tényleges forgalom

Hálózat sematikus ábrája



A választott technikai megoldás

- **Cisco CleanAir Technology**
- Chip szintű spektrum analízis
- Öngyógyító” és „Önoptimalizáló”
- Air quality index (AQI)
- Problémás helyek megjelenítése
- Interferensek megjelenítése
- Együttműködés a Mobility Services Enginnel

- **Dual Band működés (egy időben 2,4GHz-en és 5GHz-en is működik)**
- **Gigabites uplink**

WIFI biztonság, kliens beállítások

Kliens beállítás:

SSID neve kis / nagybetű érzékeny
Azonosítás: WPA2-Enterprise

Csak felhasználó azonosítás
Plusz biztonsági faktor az AD csoportagság)

Vezetéknélküli behatolás védelem (WIPS)

- Idegen Access Point-ok detektálás és besorolása:
  - Csatlakozik-e a vezetékes hálózathoz?
  - Kliensek csatlakoznak-e hozzá?
  - Ellenséges vagy baráti AP?
  - Honeypot AP (vállalati SSID-t sugárzó idegen AP)?
- Különböző típusú rádiós támadások detektálása, menedzsment rendszerben megfelelő szintű riasztás megjelenése
- Idegen AP-k illetve rádiós támadók lokalizálása térképen
- Veszélyes AP-k manuális illetve automatikus elszigetelése
- Rádiós támadók feketelistázása

Vendég WIFI hozzáférés

Vendégek számára ideiglenes account-ot lehet felvenni
A szponzorok tudják létrehozni a vendég felhasználókat
Sponsor webes felület elérése
Kik a szponzorok?

Elsősorban titkársági dolgozók
Webes felületen rögzíthetők a felhasználók ideiglenes felhasználó nevei, egyelőre csak angol nyelvű GUI felület

Üzemeltetési, bevezetési tapasztalatok

- RF problémák és megoldásaik
- Sokszínű kliensek beállítási nehézségei
- 2,4GHz-en interferáló eszközök
- Mikrohullámú mozgásérzékelők
- Mikrohullámú sütők
- Bluetooth
- Egyéb wifi berendezések acess pointok
- Wifi kamerák
- Vezeték nélküli telefonok
- Javasolt, lehetőleg 5GHz-es kliens berendezések használata
- Kisebb egy adott AP hatósugara, de
- Kevesebb interferens
- Jobb sávszélesség kihasználtság
- Több lehetséges működési csatorna

További tervek

- Minden épület lefedése
- Mobile Device Management
  - Kliens eszköz biztonsági policy beállítások
  - Egységesített policy, kliens típusonként egyéni hozzáférési jogosultságokkal
  - Kliensek állapotának vizsgálata

Köszönöm a figyelmet!