KFKI T-Systems

Jogában áll belépni?!

Détári Gábor, rendszermérnök

KFKI T-Systems

Tartalom:

- Aggasztó kérdések, tapasztalatok, hiányosságok
- Mit, és hogyan szabályozzunk?
- A NAC lehetőségei
- A Cisco NAC alkalmazása a hálózat védelmére

KFKI T-Systems

Aggasztó kérdések

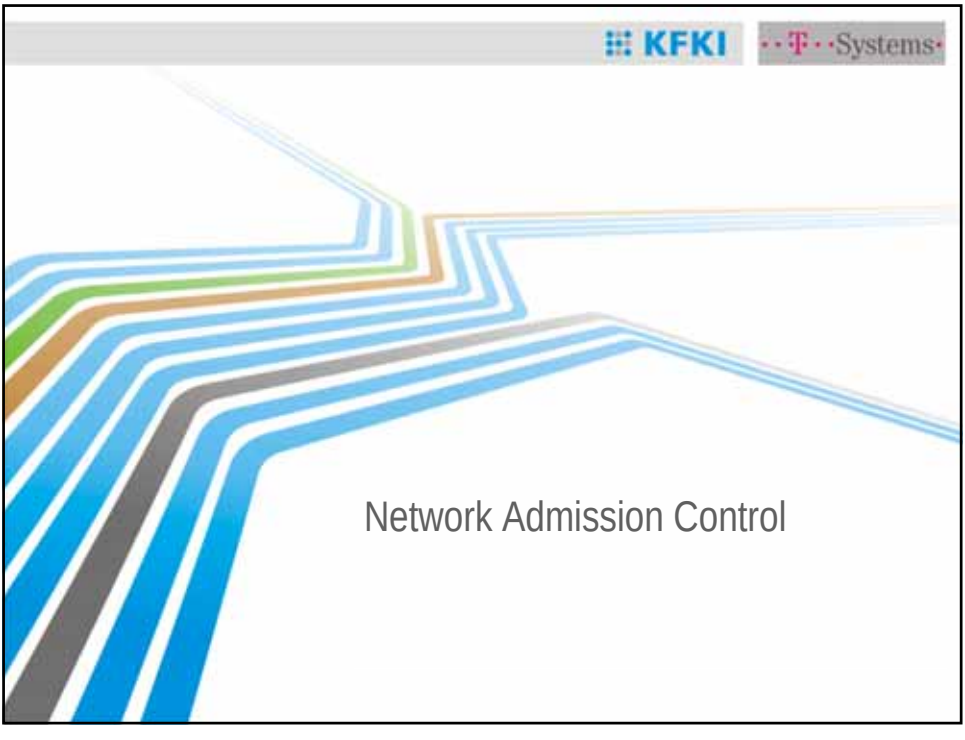
KFKI T-Systems

Alapvető kérdések a házirendről

- Létezik-e biztonsági házirend?
- Ellenőrzött-e a házirend betartása?
  - pl. szankciók meghatározása, kivételek visszaszorítás
- Követi-e a házirend a infrastruktúra változásait?
  - pl. vidéki telephelyek nyitása, távmunka bevezetése

Alapvető kérdések a házirendről

- Minden belépési pontot megfelelően ellenőrzünk?
  - helyi vezetékes, wireless, távoli belépési pontok, partnerek
- Milyen technikai ellenőrzések történnek egy belépésnél?
  - szabad, részben szabad, felhasználó/eszköz azonosítás,
  - felhasználó és házirend megfelelés



Network Admission Control

- Egy **Policy Firewall** az architektúrában
- Túllép a hagyományos felhasználó vagy eszköz authentikáción

- Feladata:
  - biztonsági **házirend betartatása**
  - felhasználó **hitelesítés**
  - **karantén** kezelése
  - lehetőség a **javítások** elvégzésére
  - **proaktív** védelem biztosítása
  - egyszerű, gazdaságos, központi **menedzsment** biztosítása

Hol alkalmazzuk a NAC-ot?

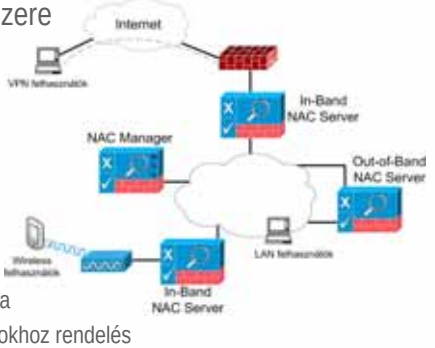
- Mindenhol, ahol technika oldalról támogatni kell a biztonsági házirendet

- Jellemzően:
  - mobil munkások
  - vendégek
  - partnerek
  - külső alvállalkozók hálózati hozzáférése esetén

A Cisco NAC koncepciója

Cisco NAC = Cisco Clean Access

- Cisco hozzáférés szabályozó rendszere



- Feladata:
  - policy teljesítésének vizsgálata az összes belépési ponton
  - csatlakozni kívánó felhasználók azonosítása
  - a felhasználó és az eszköz alapján csoportokhoz rendelés
  - szükség esetén karantén
  - segítség a házirendnek való megfelelősben frissítések elérhetősége

Cisco Clean Access Manager

- A házirend implementálása
- Központi menedzsment felület az összes NAC Serverhez
- Felhasználók authentikálása
- A döntéshozó elem
- Automatikus frissítések
- Switchek kezelése (SNMP fogadása és vezérlés)
- Log kezelés
- Redundancia lehetőség

Cisco Clean Access Server

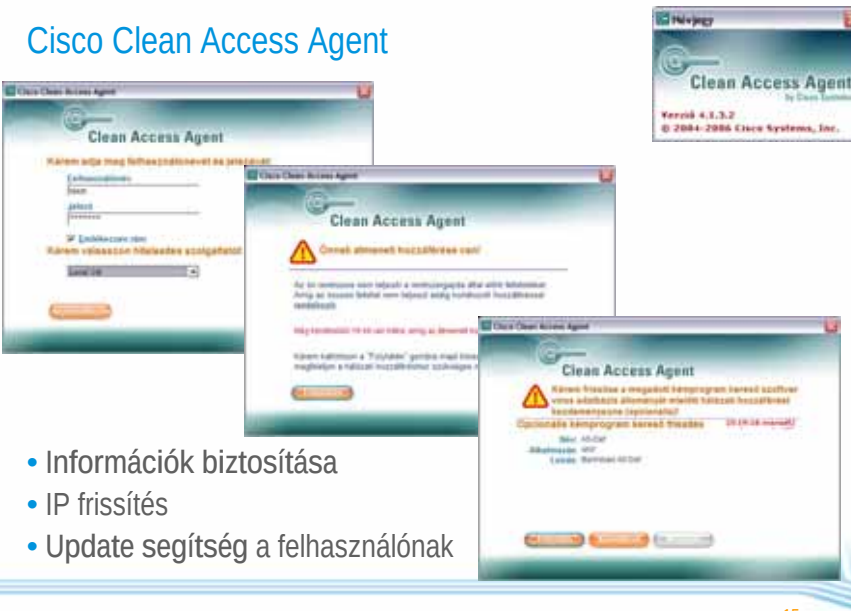
- Felhasználók szeparálása
- Route vagy bridge funkció
- Információk begyűjtése a NAC Manager számára
- A kapott értékelés alapján a szabályok betartatás
- Webes authentikáció biztosítása
- Redundancia lehetőség

Telepítési módok

- A Clean Access Server elhelyezése a hálózati forgalomba

Software-only (customer provides hardware)	or	Appliance (Cisco provides hardware)
Virtual Gateway (bridged)	or	Real-IP Gateway (routed)
L2 Client Access	or	L3 Client Access
In-band Server	or	Out-of-band Server

Cisco Clean Access Agent

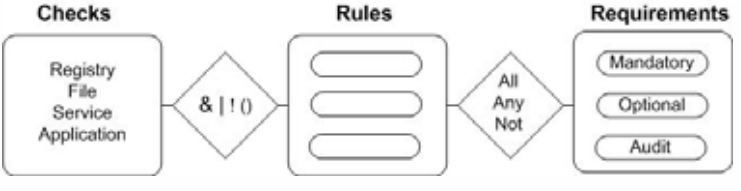


- Információk biztosítása
- IP frissítés
- Update segítség a felhasználónak

Cisco NAC Web Agent

- Vendégek, partnerek esetén
- ActiveX vagy Java segítségével
- Ellenőrzés Nessus scanner komponensekkel

Ellenőrzések



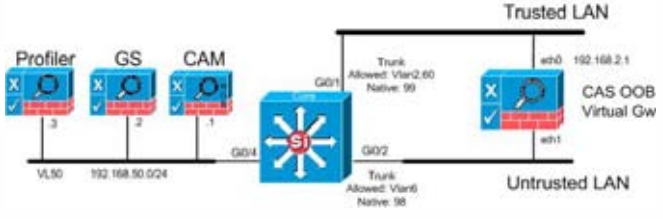
- Registry check: key, value
- File check: existance, date, version
- Service, Applicalion check: status
- User role-okhoz Requirenment-et rendelünk

Cisco NAC kiegészítő komponensek

- NAC Profiler & Collector
  - Külön appliance
  - Eszköz profil menedzsment és viselkedés követés
  - Collector:
    - A Clean Access Server része
    - A Profiler-nek gyűjt információkat
    - NetMap, NetTrap, NetWatch, NetInquiry, NetRelay
- NAC Guest Server
  - Külön appliance
  - Vendégmenedzsment támogatás
  - API-n és RADIUS-on keresztül

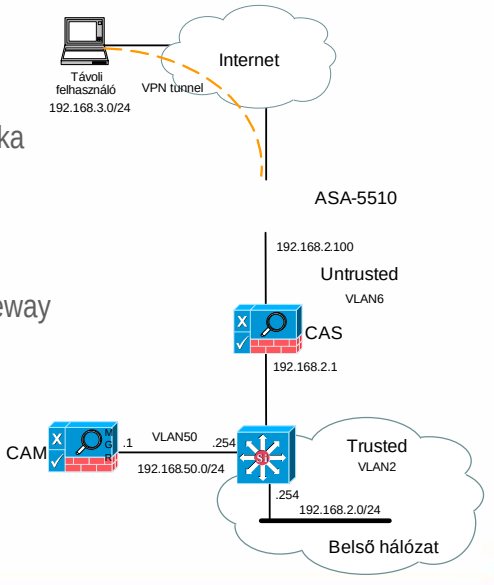
Védett LAN

- A switchek SNMP trap-et küldenek az új MAC címekről a CAM-nak
- A CAM értékel és vezérli a switchet
- A felhasználó a CAS-on keresztül authentikál
- A CAM értékel és vezérli a switchet



Védett távmunka

- A hagyományos távmunka megoldás kiterjesztése
- In-Band, L3, Virtual vagy Real IP gateway megoldás
- A végponton Clean Access Agent



Összefoglalás

- Házirend
  - Átfogó, aktuális, betartható és **betartatott** biztonsági házirend kell
- Cisco Clean Access
  - appliance alapú hozzáférés szabályozó rendszer
  - hálózat peremén képes észlelni a csatlakozást
  - automatizált karantén és fertőzés mentesítés
- Komponensek:
  - Clean Access Server (Virtual vagy Real IP gateway, Out-of-band vagy In-band)
  - Clean Access Manager (Központi menedzsment felület: kiértékelés, hozzáférési engedélyezés)