

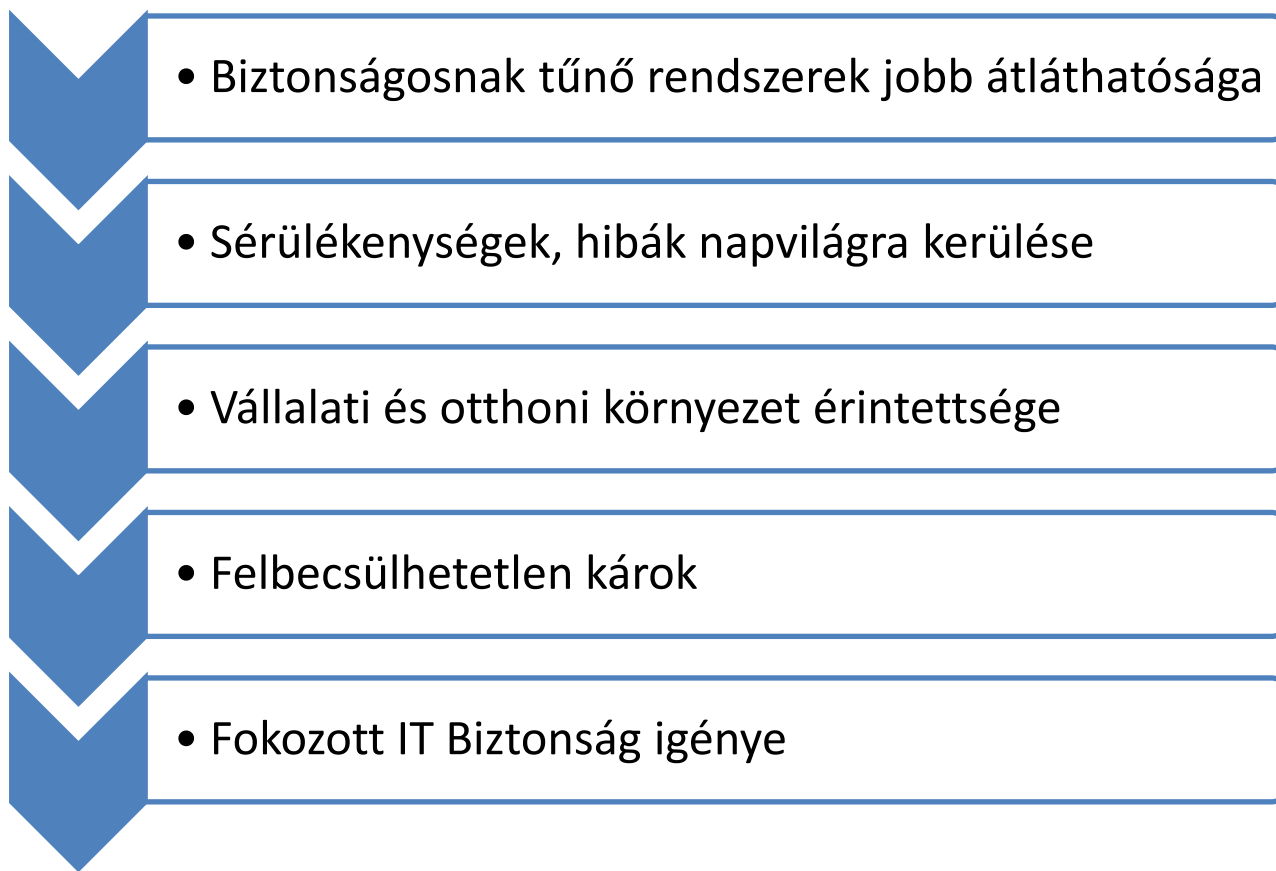
Cisco Identity Services Engine

Izsó Krisztián
Péti Zoltán



Bevezetés

Szakképzett informatikusok számának növekedése



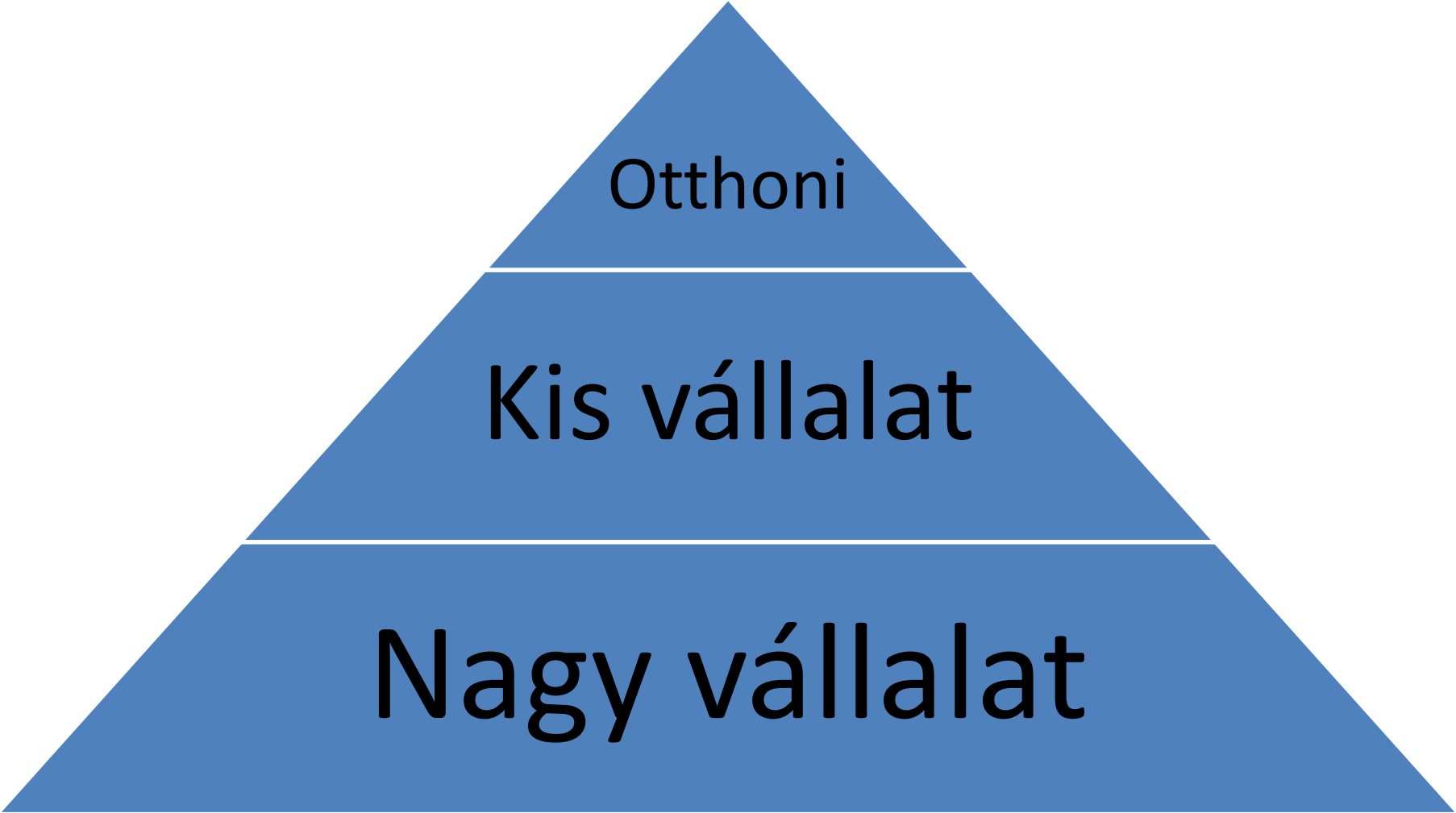
Kezdetleges védekezési formák



Víruskereső

Tűzfal - Szoftver / Hardver

Kár érték



Otthoni

Kis vállalat

Nagy vállalat

Biztonsági rés

A
céges
privát
hálózat

- Felépítése
- Hozzáférhetősége

Mobil eszközök a vállalatban

Notebook

Okostelefon

iPad

Egy lehetséges megoldás

Kinek ?

- Közép- és Nagyvállalatok számára

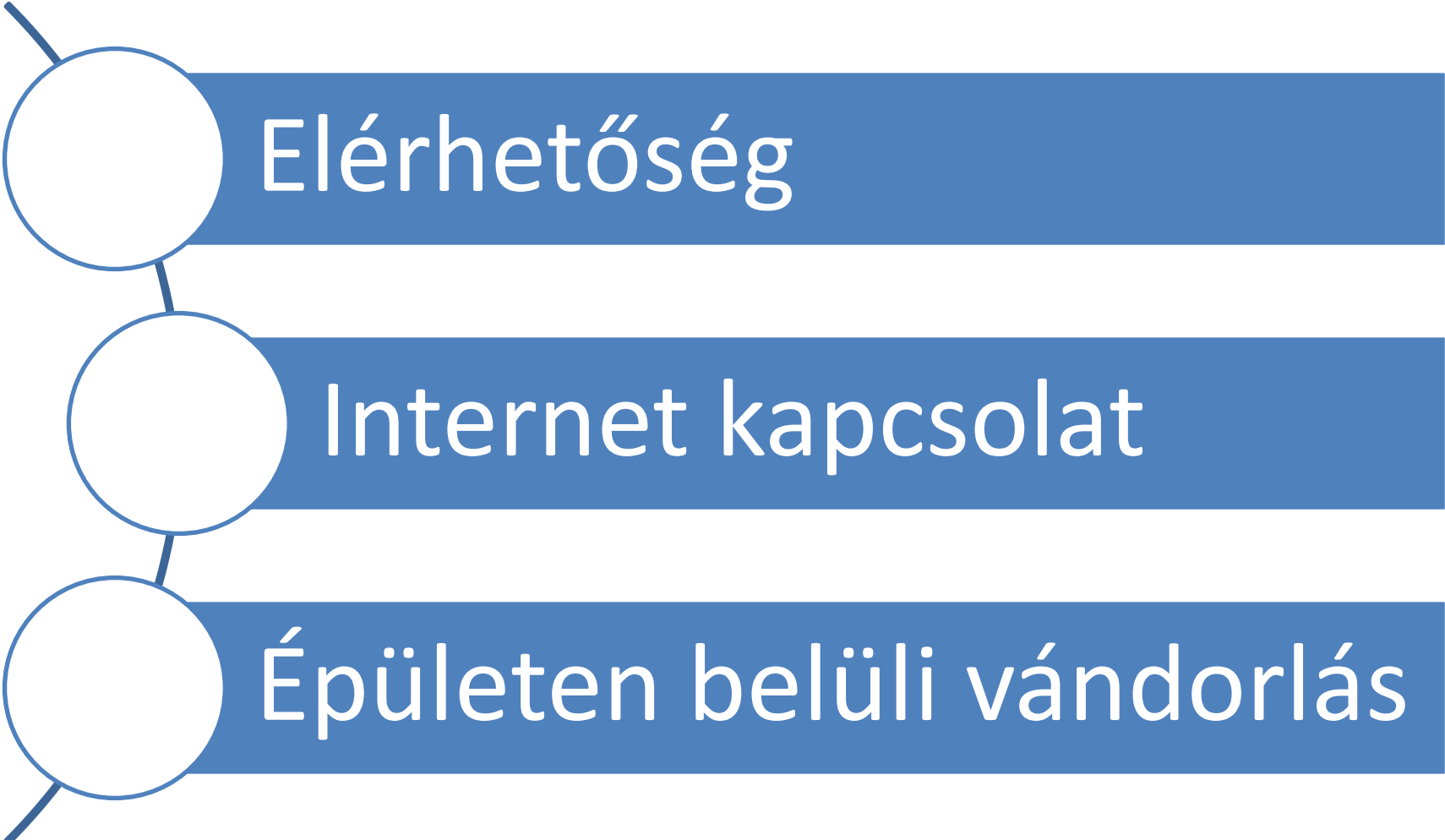
Mit ad ?

- OSI modell alsó rétegeitől induló védelmet
- Mobilitás támogatását

Mi ez ?

- Cisco ISE

Mobilitás építőkövei

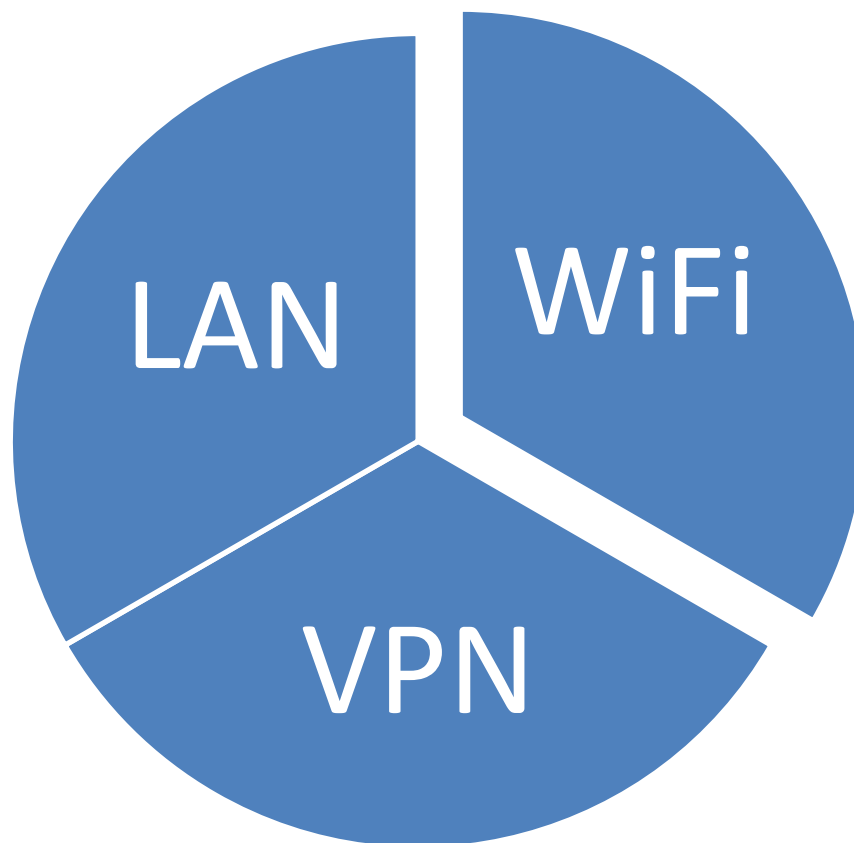


Elérhetőség

Internet kapcsolat

Épületen belüli vándorlás

Csatlakozás a hálózathoz



Engedély nélküli hozzáférés



Vezetékes
hálózaton



Vezeték nélküli
hálózaton

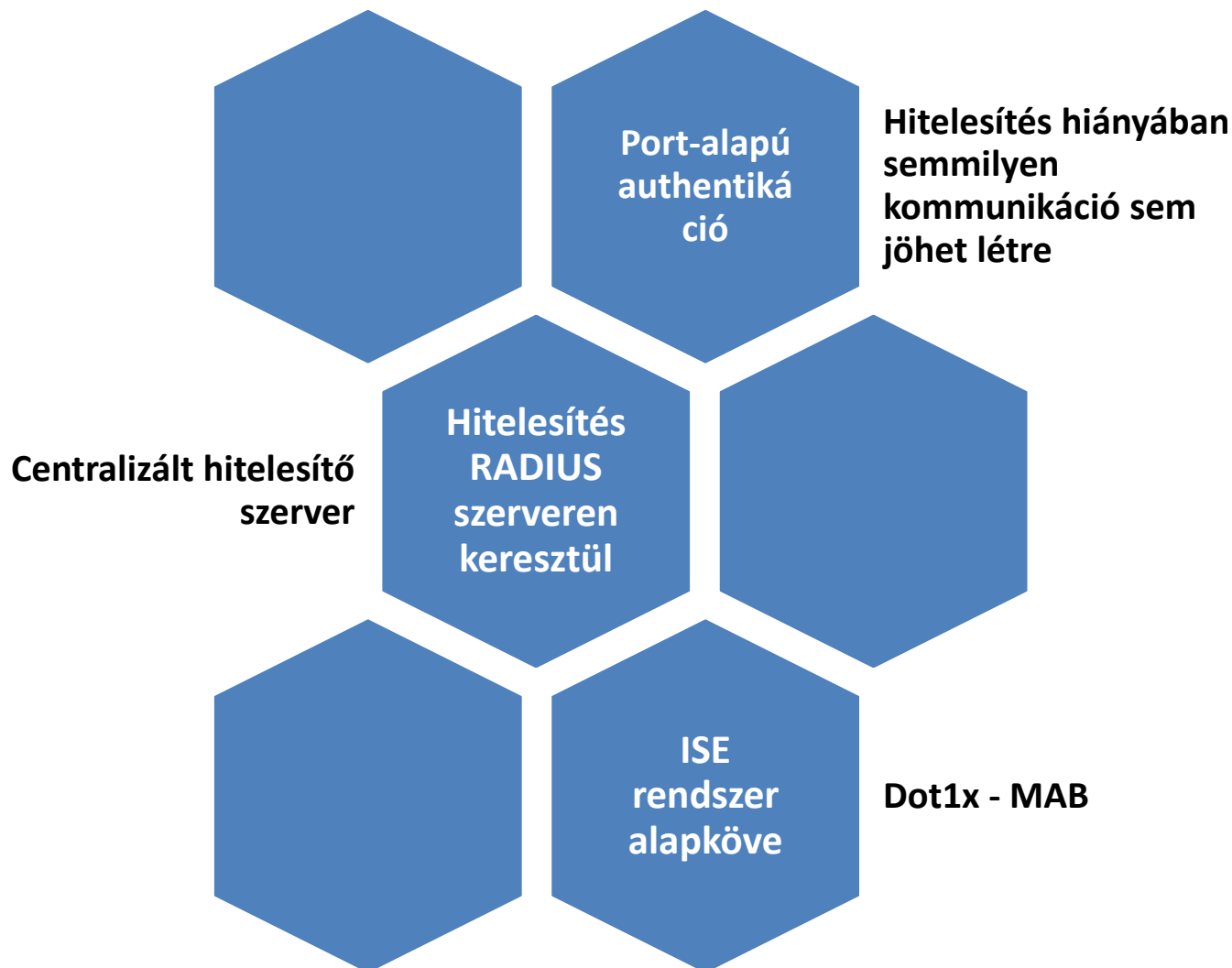
Vezetések hálózat védelme 1

Port letiltása (admin shutdown)

Cisco Port-security feature

- Fix munkaállomásoknál kiszámítható, jó megoldás
- MAC cím klónozás problémája
- Mobil eszközöknél használhatatlan

Vezetések hálózat védelme 2



Vezeték nélküli hálózat védelme



Alapértelmezetten védtelen

- A megfelelő biztonsághoz minimális szaktudás szükséges



Kezdetleges védekezési lehetőségek

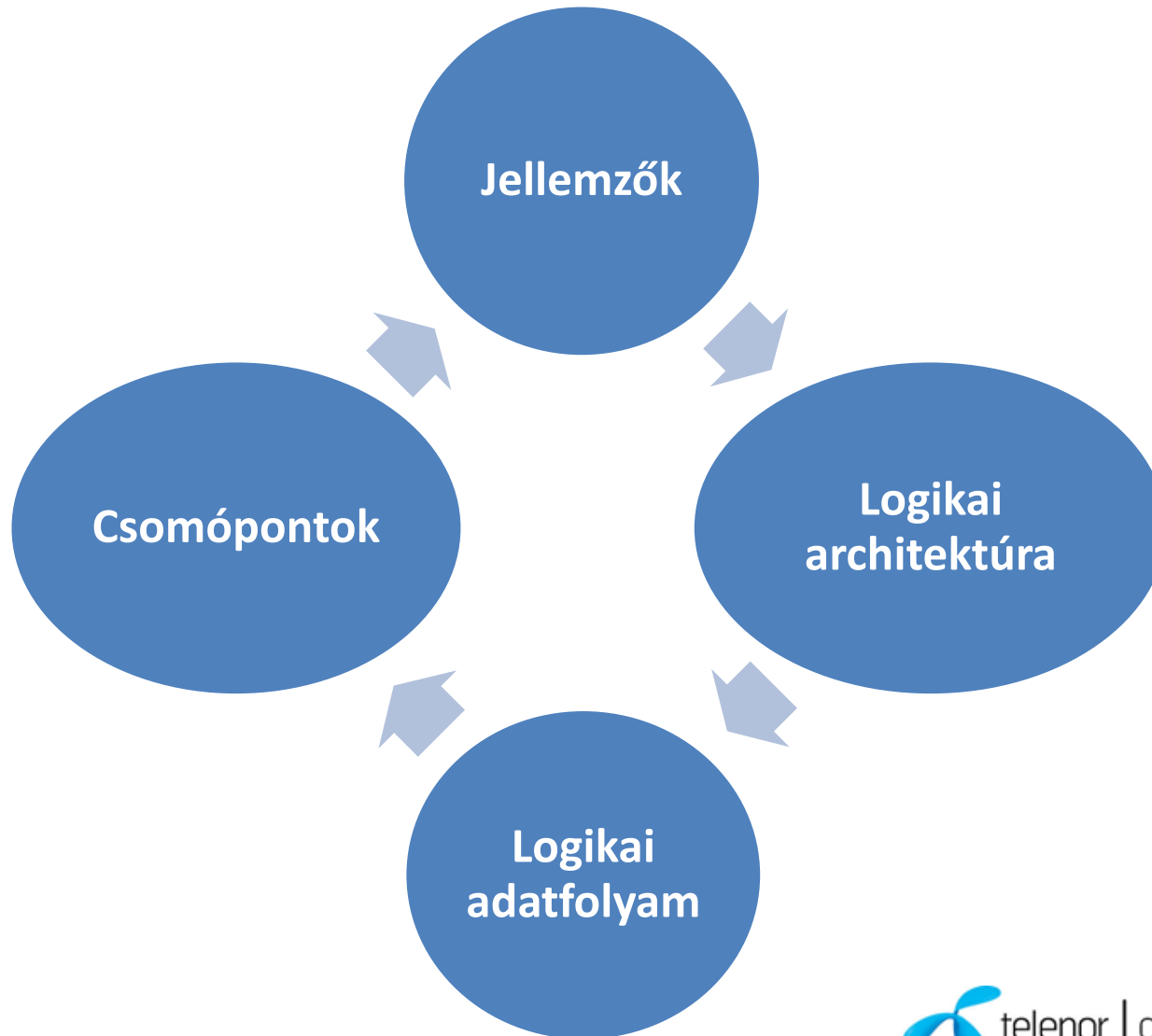
- SSID broadcast kikapcsolása
- Jelszavas hitelesítés, titkosítási algoritmusok



Infrastrukturális tervezés

- Egységes Wifi infrastruktúra
- Vendég Wifi hálózat

CISCO ISE



Jellemzők

Identitás alapú hozzáférés szabályzó rendszer

- Hitelesítendő eszköz / Felhasználó = Identitás

5 alapvető aspektus

- Authentikáció
- Rendszerelemzés
- Autorizáció
- Szolgáltatási szint
- Naplózás

Logikai architektúra

Szolgáltatási csomópontokból áll

Redundánsan telepíthető

Központi admin felületen kezelhető minden

ISE logikai folyamat



ISE Logical Architecture forrás: ([1]anonymous, 2013)

ISE csomópontok

Admin node

- ISE rendszer konfigurálása, web GUI

Monitoring node

- Log gyűjtés, elemzések, hibakeresés, riportok

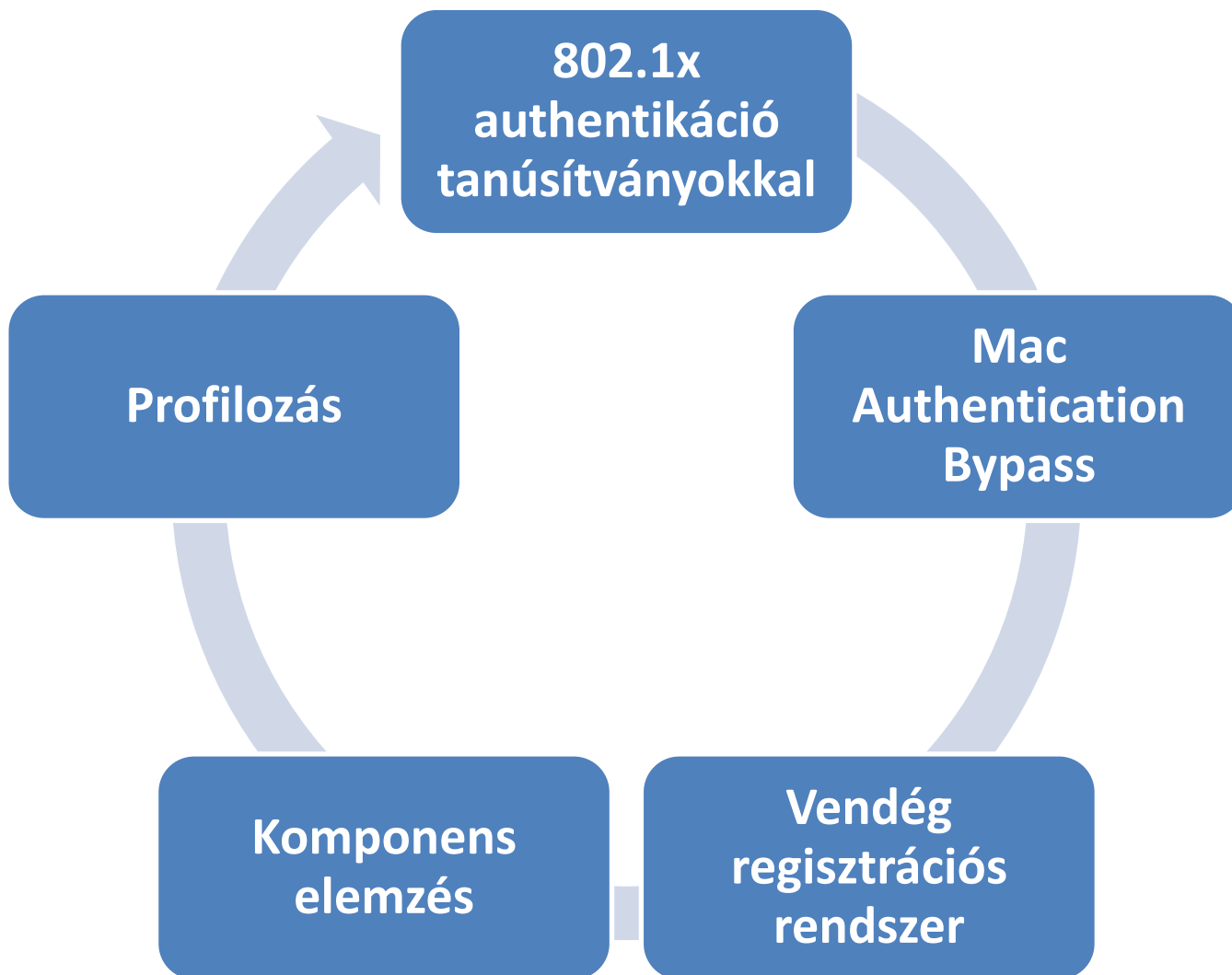
Policy service node

- Felhasználók kiértékelése, vendég hozzáférés biztosítása, NAC agenttel kommunikál

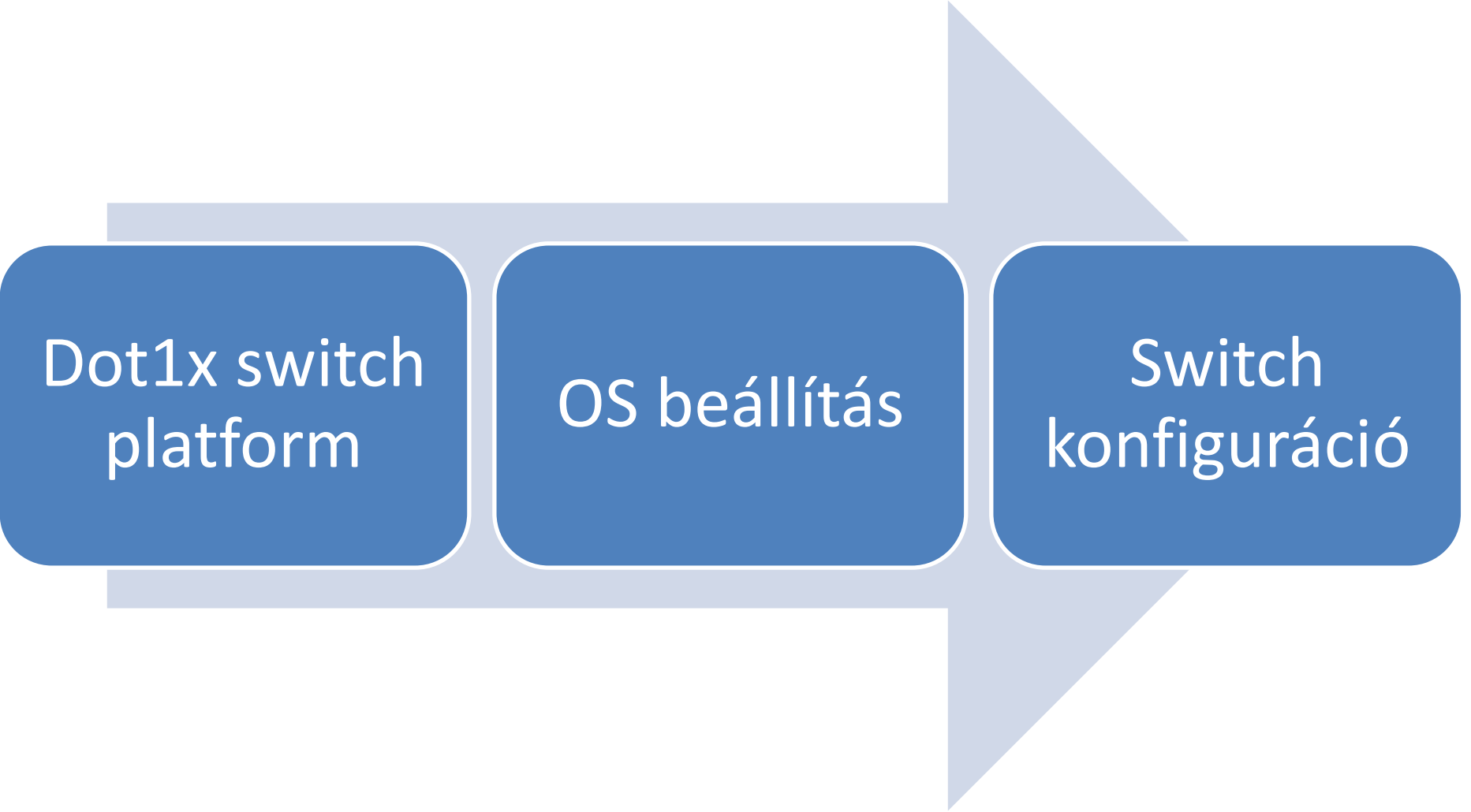
In-line posture node

- Wifi kontroller, VPN koncentrátor mögött
- Adatforgalom áthalad rajta
- Folyamatosan változó szabályok

ISE funkciók



802.1x autentikáció tanúsítványokkal



Dot1x switch
platform

OS beállítás

Switch
konfiguráció

Dot1x switchport konfig

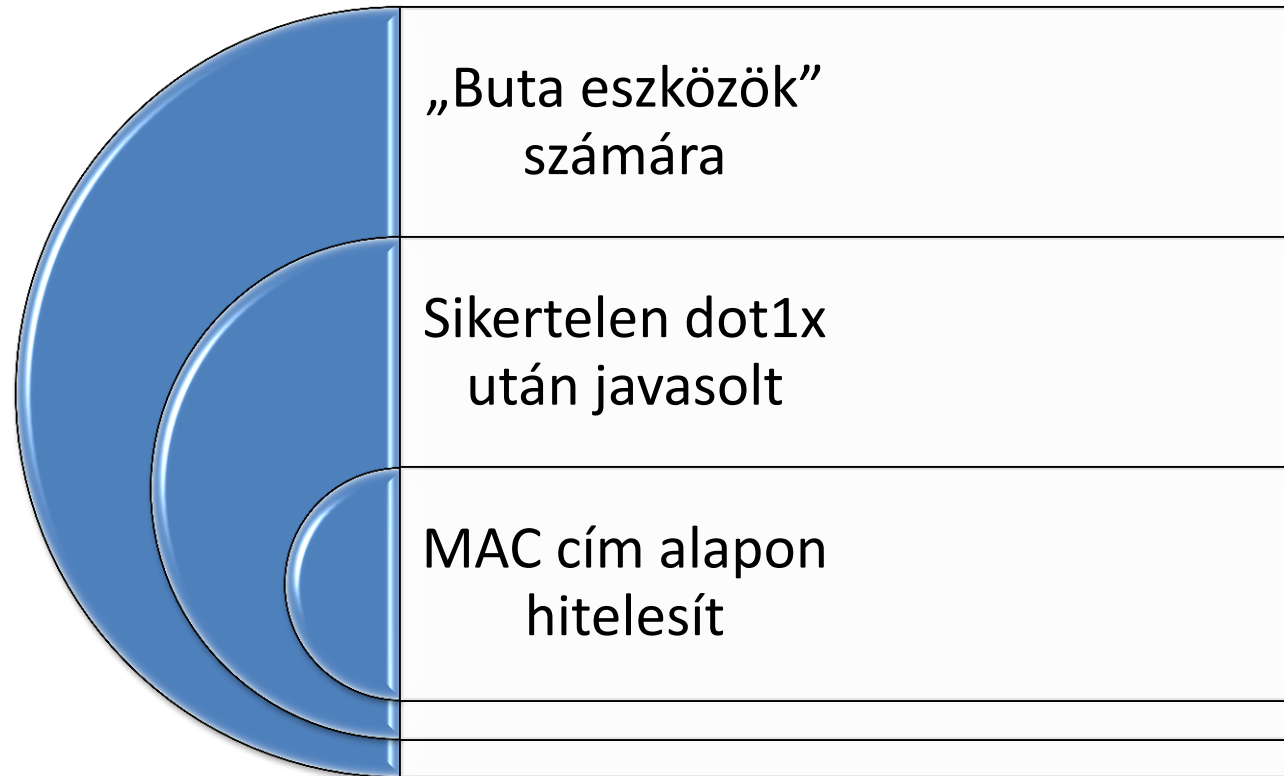
```
interface GigabitEthernet1/15
description == 802.1X port ==
switchport
switchport access vlan 460
switchport mode access
ip arp inspection limit rate 25 burst interval 2
ip access-group ACL-DEFAULT in
logging event link-status
authentication event fail action next-method
authentication event server alive action reinitialize
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer restart 120
authentication timer reauthenticate server
authentication timer inactivity server
authentication violation replace
mab
dot1x pae authenticator
dot1x timeout quiet-period 10
dot1x timeout tx-period 10
power inline never
spanning-tree portfast edge
spanning-tree bpduguard enable
end
```

Sikeres Dot1x auth

```
sw- #sho authentication sessions interface gigabitEthernet 1/15
      Interface: GigabitEthernet1/15
      MAC Address: 0023.ae5b.c2f3
      IP Address: 10.64.58.25
      User-Name:
      Status: Authz Success
      Domain: DATA
      Oper host mode: single-host
      Oper control dir: both
      Authorized By: Authentication Server
      Vlan Policy: 458
      ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC-544f05ed
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: 0A40FA060000031E687786E1C
      Acct Session ID: 0x0000D2F7
      Handle: 0x000000A1

Runnable methods list:
      Method   State
      dot1x    Authc Success
      mab       Not run
```

Mac Authentication Bypass



MAC cloning probléma ?

MAB switch konfig

```
interface GigabitEthernet1/0/47
description == MFP_802.1X port - BF-DT-2 ==
switchport access vlan 408
switchport mode access
ip access-group ACL-DEFAULT in
power inline never
authentication event fail action next-method
authentication event server alive action reinitialize
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer restart 120
authentication timer reauthenticate server
authentication timer inactivity server
authentication violation replace
mab
dot1x pae authenticator
dot1x timeout quiet-period 10
dot1x timeout tx-period 10
end
```


Sikeres MAB

```
sw- #sh authentication sessions interface Gi1/0/47
```

Interface	MAC Address	Method	Domain	Status	Fg	Session ID
Gi1/0/47	0011.85d8.c99b	mab	DATA	Auth		AC1C2619000000FAF0003B66E

Key to Session Events Status Flags:

- A - Applying Policy (multi-line status for details)
- D - Awaiting Deletion
- F - Final Removal in progress
- I - Awaiting IIF ID allocation
- P - Pushed Session (non-transient state)
- R - Removing User Profile (multi-line status for details)
- U - Applying User Profile (multi-line status for details)
- X - Unknown Blocker

Runnable methods list:

Handle	Priority	Name
10	5	dot1x
12	10	mab
6	15	webauth

Vendég regisztrációs rendszer

Problémák

- Statikus jelszavak
- Sávszélesség pazarlás

Megoldás

- Kettős portál rendszer : Szponzor - Vendég

Szponzor portál

[Create Accounts](#) [Manage Accounts \(1\)](#) [Pending Accounts \(2\)](#) [Notices \(0\)](#)

Guest type:

Employee-Internet

Maximum devices that can be connected: 20
Maximum access duration: 90 days

Provide Guest Information:

Last name:*

Email address:

Phone number:*

Comment

Language:

English - English

Access Information

Duration:*

36

 Days (Maximum: 90)

From Date (yyyy-mm-dd) *

2015-10-27

From Time *

18:27

To Date (yyyy-mm-dd) *

2015-12-01

To Time *

23:59

Create

11. ábra ISE szponzor portál

Komponens elemzés

- A hitelesítendő eszköz biztonságos ?
- Szándékos vagy nem szándékos károkozás



- Eszköz

- Kiértékelés (NAC Agent)

- **Go / No Go !**

Profilozás



BYOD támogatása

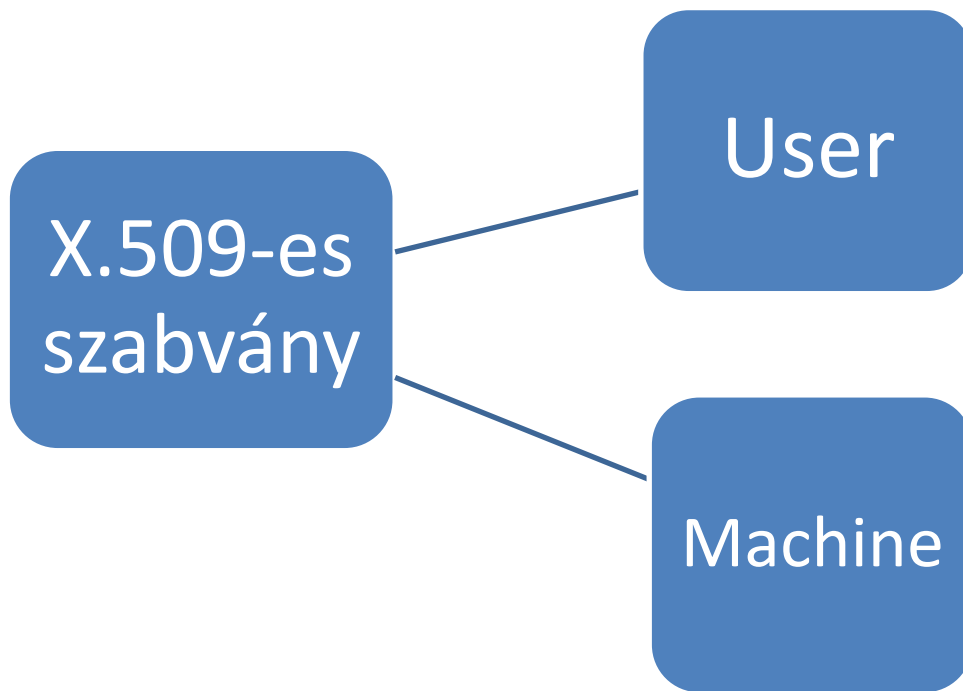
- Dinamikus felismerés
- Eltérő szabályozás / eszköz



Logikai csoportokba helyezés

- Hardver alapon : Apple, Blackberry
- OS alapon : Windows 7 , MAC OS X, Win XP

Tanúsítványkezelés ISE alatt



X.509-es tanúsítvány

„Publikus kulcsú infrastruktúrában a tanúsítványok feladata elsősorban egy adott publikus kulcs és az ahhoz tartozó titkos kulcs összekapcsolása. Ugyanakkor a tanúsítványoktól elvárjuk, hogy rendelkezzen mindazokkal a tulajdonságokkal, amikkel mondjuk egy személyi igazolvány vagy egy bankkártya. Elvárjuk, hogy az egyes személyek, szervezetek azonosítását, kezelését épp olyan, de inkább nagyobb biztonsággal el tudjuk végezni, mint ahogy azt az offline megfelelőikkel természetesen és magától értetődően tesszük. Elvárjuk tőlük mindazt a biztonságot és kényelmet és természetesen azt, hogy ezt a modern hálózati környezetben hajtsa végre.”

(Folláth János, 2011)

Tanúsítványok kezelése



Több szintű hitelesítésre alkalmas



Hitelesítő szerver feladata a
tanúsítvány kiértékelése



Tanúsítvány (hitelesítés) + Active
Directory (autorizáció)

Machine Tanúsítvány példa

Field	Value
Issuer	
Valid from	2015. március 11. 15:22:49
Valid to	2018. március 10. 15:22:49
Subject	
Public key	RSA (2048 Bits)
Certificate Template Inform...	Template=1.3.6.1.4.1.311.21...
Enhanced Key Usage	Client Authentication (1.3.6.1....

User tanúsítvány példa

	Issuer	
	Valid from	2015. augusztus 31. 7:21:08
	Valid to	2016. augusztus 30. 7:21:08
	Subject	
	Public key	RSA (2048 Bits)
	Certificate Template Inform...	Template=1.3.6.1.4.1.311.21...
	Enhanced Key Usage	Client Authentication (1.3.6.1....

Folyamat összegzése

- Helytől független munkavégzés
- Machine cert. (Hitelesítés)
- User cert. (Autorizáció)
- Kettős kiértékelés
- Biztonságos hozzáférés

Tesztet 1

Normál működés



Teszt alany : Nagy Ottó



Modell: HP Elitbook 840



MAC cím: 64:51:06:A0:72:20



Tartományi felhasználónév:
Otto.Nagy@xyz.com

Switch konfig

```
interface GigabitEthernet1/0/46
description == 802.1X port ==
switchport access vlan 460
switchport mode access
ip access-group ACL-DEFAULT in
authentication event fail action next-method
authentication event server alive action reinitialize
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer restart 120
authentication timer reauthenticate server
authentication timer inactivity server
authentication violation replace
mab
dot1x pae authenticator
dot1x timeout quiet-period 10
dot1x timeout tx-period 10
```

Sikeres Hitelesítés

```
#sh authentication sessions interface gigabitEthernet 1/0/46
```

Interface	MAC Address	Method	Domain	Status Fg	Session ID
Gi1/0/46	6451.06a0.7220	dot1x	DATA	Auth	0A40FA3F0000020C894324046

Key to Session Events Status Flags:

- A - Applying Policy (multi-line status for details)
- D - Awaiting Deletion
- F - Final Removal in progress
- I - Awaiting IIF ID allocation
- P - Pushed Session (non-transient state)
- R - Removing User Profile (multi-line status for details)
- U - Applying User Profile (multi-line status for details)
- X - Unknown Blocker

Runnable methods list:

Handle	Priority	Name
10	5	dot1x
12	10	mab
6	15	webauth

Machine auth logok

Overview

Event	5200 Authentication succeeded
Username	Otto.Nagy-NB.xyz.com
Endpoint Id	64:51:06:A0:72:20 ⊕
Endpoint Profile	HP-Device
Authentication Policy	LAN_HUN >> LAN-HUN_auth >> Default
Authorization Policy	LAN_HUN >> LAN_HU_-_machine
Authorization Result	HU_machine_auth_limited

User Auth logok

Overview

Event	5200 Authentication succeeded
Username	Otto.Nagy@xyz.com
Endpoint Id	64:51:06:A0:72:20 ⓘ
Endpoint Profile	HP-Device
Authentication Policy	LAN_HUN >> LAN-HUN_auth >> User_auth
Authorization Policy	LAN_HUN >> No_posture_LAN_HU
Authorization Result	HU_FINANCE_VLAN

Teszt eset 2

Lopott notebook



Hackelt admin jelszó



Kísérlet a céges hálózatra való
csatlakoztatásra

Machine auth

```
#sh authentication sessions int gi1/0/46 details
  Interface: GigabitEthernet1/0/46
    IIF-ID: 0x103EFC000000103B
  MAC Address: 6451.06a0.7220
  IPv6 Address: Unknown
  IPv4 Address: 10.64.63.53
  User-Name: Otto.Nagy-NB.xyz.com
  Status: Authorized
  Domain: DATA
  Oper host mode: single-host
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: 0A40FA3F000020D6850C191A
  Acct Session ID: 0x00002D7E
    Handle: 0x11000F47
  Current Policy: POLICY_Gi1/0/46
```

Server Policies:

```
  Vlan Group: Vlan: 460
  ACS ACL: xACSACLx-IP-Update_and_DCs-55b09c9a
```

Method status list:

Method	State
dot1x	Authc Success
mab	Stopped

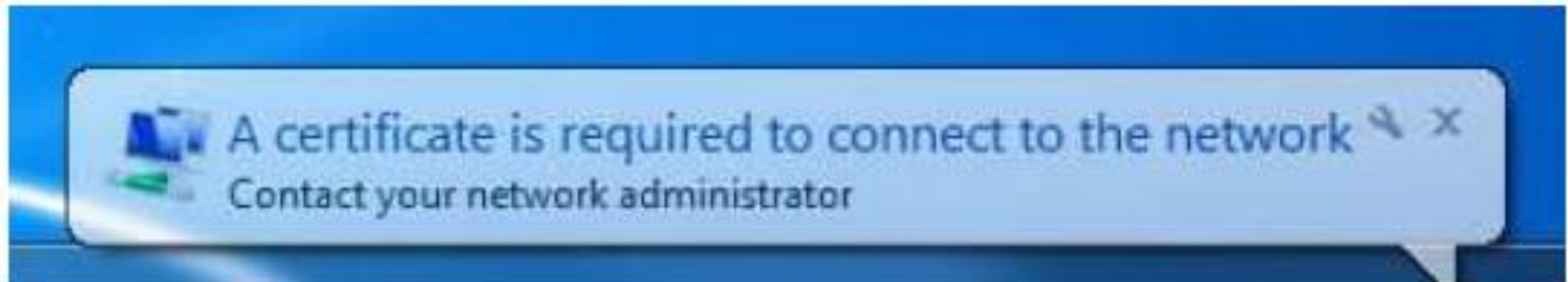
Tört Admin jelszó után

```
#sh authentication sessions int gi1/0/46 details
  Interface: GigabitEthernet1/0/46
    IIF-ID: 0x103EFC00000103B
  MAC Address: 6451.06a0.7220
  IPv6 Address: Unknown
  IPv4 Address: 10.64.63.53
  User-Name: 645106a07220
    Status: Unauthorized
    Domain: DATA
  Oper host mode: single-host
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: 0A40FA3F000020D6850C191A
  Acct Session ID: Unknown
    Handle: 0x11000F47
  Current Policy: POLICY_Gi1/0/46
```

Method status list:

Method	State
dot1x	Stopped
mab	Stopped

Sikertelen hitelesítés



Overview

Event	5400 Authentication failed
Username	64:51:06:A0:72:20 ⊕
Endpoint Id	64:51:06:A0:72:20 ⊕
Endpoint Profile	HP-Device
Authentication Policy	LAN_HUN >> MAB >> Default
Authorization Policy	LAN_HUN >> Default
Authorization Result	DenyAccess

Tesztet 3

Idegen notebook



Tetszőleges felhasználónév



Modell: Fujitsu-Siemens S7210



MAC cím: 00:17:42:79:87:51



Tartományi felhasználónév:

Aladar.Kocsis@kertemkft.com

Switchport - MAC

```
#sh mac address-table dynamic interface gigabitEthernet 2/25
```

Legend: * - primary entry
age - seconds since last seen
n/a - not available
S - secure entry
R - router's gateway mac address entry
D - Duplicate mac address entry

Displaying entries from active supervisor:

	vlan	mac address	type	learn	age	ports
*	460	0017.4279.8751	dynamic	Yes	0	Gi2/25

Nem létező machine tanúsítvány

```
#show authentication sessions interface gigabitEthernet 2/25
```

```
Interface: GigabitEthernet2/25
```

```
MAC Address: 0017.4279.8751
```

```
IP Address: 10.64.60.99
```

```
User-Name: 001742798751
```

```
Status: Authz Failed
```

```
Domain: DATA
```

```
Oper host mode: single-host
```

```
Oper control dir: both
```

```
Session timeout: N/A
```

```
Idle timeout: N/A
```

```
Common Session ID: 0A40FA0600003F6C2636EA50
```

```
Acct Session ID: 0x0001254D
```

```
Handle: 0xA4000F48
```

```
Runnable methods list:
```

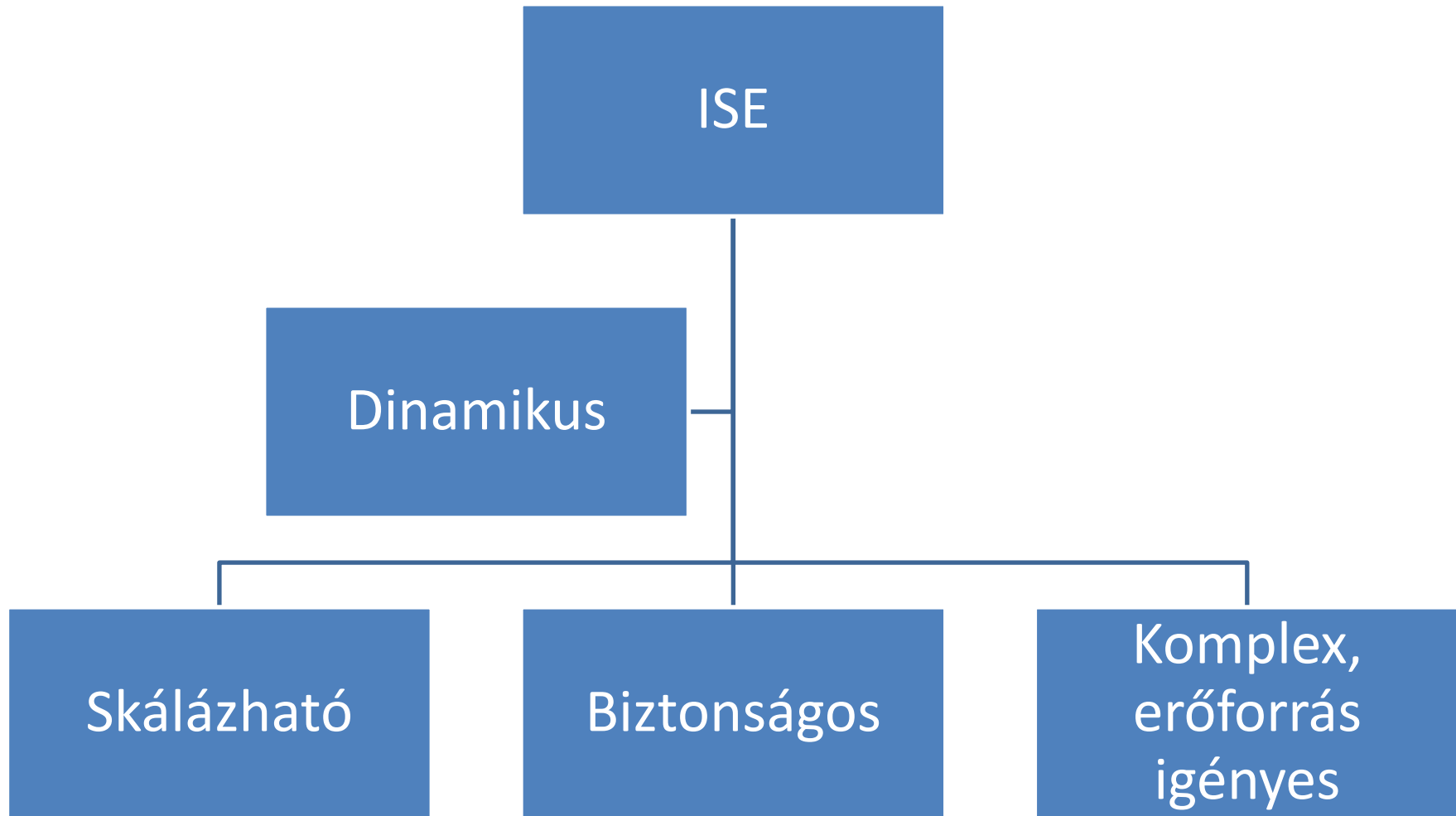
Method	State
dot1x	Failed over
mab	Failed over

ISE logok

Overview

Event	5400 Authentication failed
Username	00:17:42:79:87:51 ⓘ
Endpoint Id	00:17:42:79:87:51 ⓘ
Endpoint Profile	Unknown
Authentication Policy	LAN_HUN >> MAB >> Default
Authorization Policy	LAN_HUN >> Default
Authorization Result	DenyAccess

ISE rendszer összefoglalás



Kérdések



Köszönjük a figyelmet

