



Informačné systémy
Bezpečnosť
Infraštruktúra



Identity Based Access Control

Marek Kl'oc

CCIE#21288

Agenda

- Čo je IBAC
- Prečo sa zaujímať o IBAC
- “Access Control” - Riadený prístup
- “Identity” - Identita
- Kde je možné uplatniť IBAC
- IBAC – použitie #1 (Identity Firewall)
- IBAC – použitie #2 (Identity PacketFilter)

Čo je IBAC - popis

- Ďalší evolučný stupeň oproti „traffic based“
- Riadený prístup na základe identity – funkcionality infraštruktúry vykonávajúca autentizáciu, autorizáciu a „enforcement“, pričom rozhodovacia logika je spojená s rolou identity koncového zariadenia/užívateľa
- Komponenty architektúry IBAC:
 - Policy definition and decision point
 - AA server
 - Identity store
 - Policy enforcement point
 - Firewaling
 - » Aplikačná inšpekcia (MPF)
 - » Filtrovanie IP komunikácie
 - Web a Email ochrana
 - Bezpečnostný monitoring

Prečo sa zaujímať o IBAC -> Výhody

- Presnejšie definovanie bezpečnostných politík
 - napr. jeden z užívateľov skupiny, potrebuje prístup mimo služieb danej role prislúchajúcej skupine
- Topologická nezávislosť
 - užívateľ má rovnaký prístup bez ohľadu kde práve nachádza (z pohľadu logickej topológie)
- Zjednodušenie sieťovej infraštruktúry
 - Eliminuje sa statické priradenie Rola -> VLAN
- Zjednodušenie administratívnej správy pre definovanie politík
 - Postačuje definovanie identity a priradenie role
 - Zmena v organizačnej štruktúre nevyžaduje zásah do infraštruktúry
- Presnejšie identifikovanie útočníka resp. obete útoku

Access Control „riadený prístup“

-> „zhmotnenie“ firemnej bezpečnostnej politiky (BP)

- Proces (decision), pri ktorom sieťová infraštruktúra (security services) kontrolujú a uplatňujú firemnú bezpečnostnú politiku.
- Firemná bezpečnostná politika definuje, kto čo môže.

Access Control „riadený prístup“ - BP

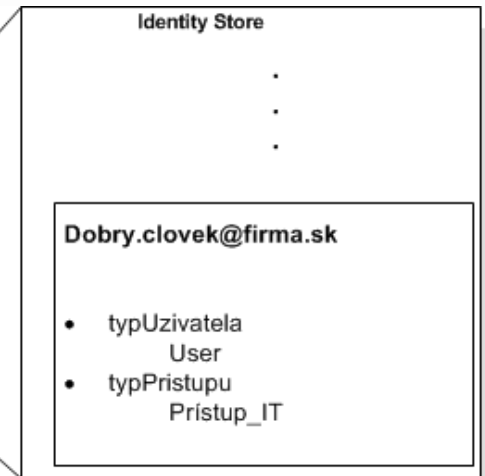
| Kategória | Typ | Popis |
|-----------------|---------------------|--|
| Typ používateľa | User | Interný zamestnanec, pracovná stanica musí spĺňať podmienky firemnej bezpečnostnej politiky. |
| | Contractor | Zamestnanec externej firmy s platnou zmluvou, pracovná stanica musí spĺňať podmienky firemnej bezpečnostnej politiky. |
| | Guest | Akýkoľvek používateľ, na ľubovoľnej pracovnej stanici, poskytuje sa mu len Internetový prístup s možnosťou vytvoriť vzdialený prístup. |
| Typ prístupu | Neobmedzený prístup | Nie sú aplikované žiadne obmedzenia. |
| | Prístup_HR | Obmedzený prístup na skupinu serverov do úrovne L4. |
| | Prístup_IT | Obmedzený prístup na skupinu serverov do úrovne L4. |
| | Blokovaný prístup | Prístup úplne zablokovaný. |
| | Vzdialený_prístup | Umožnený vzdialený prístup z Internetu s pomocou VPN klienta (použitie len v kombinácií s obmedzeným prístupom). Prístup len do manažmentovej siete. |
| | Prístup_Guest | Prístupu do Internetu s možnosťou vytvorenia vzdialeného pripojenia do domovskej siete. Webová autentizácia. Registrácia na recepcii spoločnosti. |

Access Control „riadený prístup“ - BP

| Typ používateľa | Typ prístupu | Požiadavky na konfiguráciu | Typ identity | Požadovaný rozsah prístupu |
|-----------------|---------------|-----------------------------|--------------------------------|---|
| User | Prístup_IT | Aplikovaná GP | Certifikát resp. Meno/Heslo | Prístup na servery: A1.firma.sk; A2.firma.sk Neobmedzený prístup na web |
| User | Prístup_HR | Aplikovaná GP | Certifikát resp. Meno/Heslo | Prístup na servery: B2.firma.sk Web prístup na www.cisco.com |
| Contractor | Prístup_IT | Aktívny dot1x klient | Meno/Heslo | Web prístup na servery C1.firma.sk v čase 8,00 – 16,00 hod. |
| Guest | Prístup_Guest | Neznáma pracovná stanica | Meno/heslo | Prístup na Internet |

Identita

„Je množina atribútov, trvalých a dočasných spojených s identifikátorom užívateľa“



- Typy identifikátorov
 - Meno – napr. user@company.org
 - Certifikát (Subject resp. SAN)
 - IP adresa (pozn. nutné chrániť IP komunikáciu s použitím IPSG a DAI)
 - MAC Adresa – použitie len v nutnom prípade, zásadne pre obmedzený rozsah prístupu
 - Security Group Tag (SGT)
- Úložisko atribútov (Identity store)
 - Identity management – IDM (LDAP + kontrola)
 - Active Directory
 - Generický LDAP (custom)

Kde je možné uplatniť IBAC

- Identity Firewall
 - Filtrovanie paketov (ACL)
 - Aplikačná inšpekcia (MPF)
- Identity PacketFilter- základné filtrovanie paketov do úrovne L4
 - Firewall - Igress ACL
 - Prístupové prepínače - Igress ACL
 - Vzdialený prístup (RAVPN) - Igress ACL
 - Prepínače dátového centra - Egress ACL na (TrustSec)
 - Bezdrôtové siete - Igress ACL
- Web & Email appliance
 - definovanie výnimiek pre uplatnenie politík
 - Manažment prístup na zariadenia

Identity Based Firewall - scenár

Užívateľ **Dobry.Clovek** s rolou **Pristup_IT** požaduje prístup na www.facebook.com, vzhľadom k jeho pracovnej náplni (fb avatar).

Poznámka: základná firemná politika „zakazuje“ prístup na www.facebook.com počas pracovnej doby zamestnancom okrem výnimiek

Definícia problému:

- ~~➤ Definovanie iACL~~
- ~~➤ Vytvorenie segmentu pre jedného užívateľa (IT + prístup na FB)~~
- ~~➤ Umiestnenie užívateľa do segmentu s HR~~
- Použitie Identity Firewallu
- Definovanie výnimky/politiky na Web app. (proxy s URL filtrom)

Identity Based Firewall - Komponenty

- Prístupová politika – určuje pravidlá kto môže pristupovať kam
- MS Active Directory
 - Autentizácia užívateľov
 - Vytváranie log záznamov
- Externý identity store (IDM)
 - Definovanie atribútov Identifikátorov a.k.a identít
- AD User Agent – získavanie informácií z AD
 - Spracovávanie log záznamov z AD
 - Reportovanie IP na Užívateľ mapovania pre FW
- Firewall
 - Komunikácia s externým Identity storom pre zistenie typu prístupu
 - Dotazovanie sa AD User Agentu pre mapovanie IP na užívateľa
 - Definovanie/Aplikovanie prístupovej politiky
- Pracovná stanica + Užívateľ

Identity Based Firewall - Komponenty

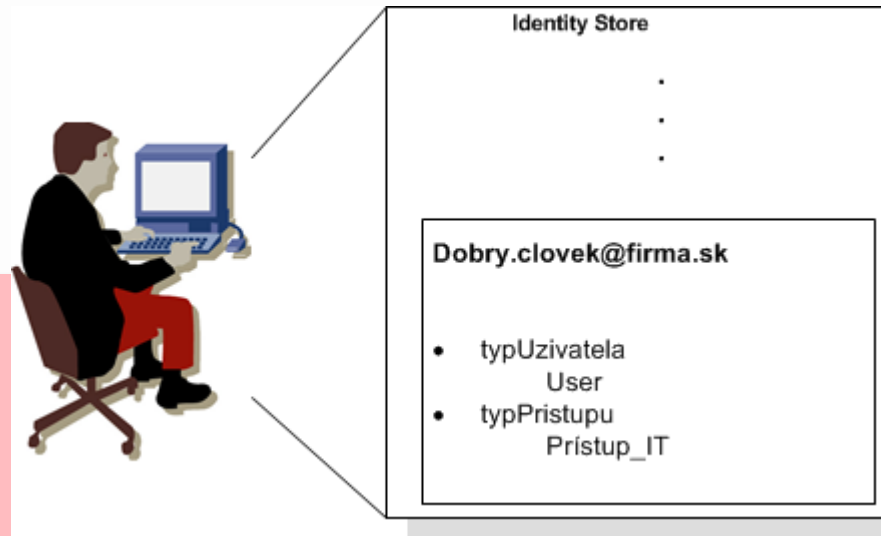
```
object-group user USERS_HR
  user-group FIRMA\\HR
```

!

```
object network FB
  fqdn www.facebook.com
```

!

```
access-list GLOBAL_P permit ip user FIRMA\dobry.clovek object FB eq 80
access-list GLOBAL_P permit ip object-group-user USERS_HR any object FB eq 80
access-list GLOBAL_P deny ip any object facebook
access-group GLOBAL_P global
```

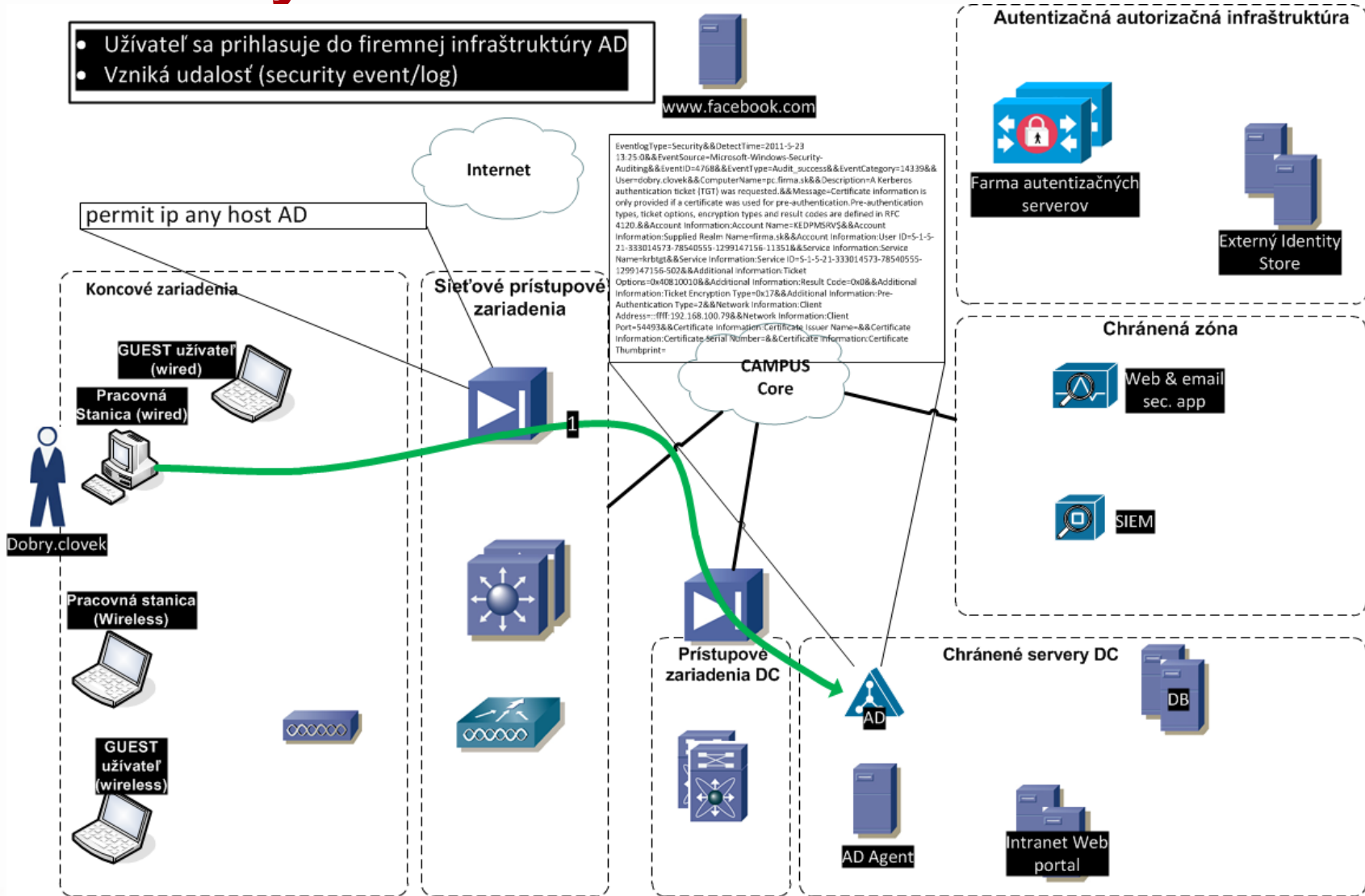


Identity Based Firewall #1

- Užívateľ sa prihlasuje do firemnej infraštruktúry AD
- Vzniká udalosť (security event/log)



www.facebook.com



```
EventLogType=Security&&DetectTime=2011-5-23
13.75.0&&EventSource=Microsoft-Windows-Security-Auditing&&EventID=4768&&EventType=Audit_success&&EventCategory=14339&&
User=Dobry.clovek&&ComputerName=pc.firma.sk&&Description=A Kerberos authentication ticket (TGT) was requested.&&Message=Certificate information is only provided if a certificate was used for pre-authentication.Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.&&Account Information:Account Name=KEDPM$RV$&&Account Information:Supplied Realm Name=firma.sk&&Account Information:User ID=5-1-5-21-333014573-78540555-1299147156-11351&&Service Information:Service Name=krbtgt&&Service Information:Service ID=5-1-5-21-333014573-78540555-1299147156-502&&Additional Information:Ticket Options=0&&Additional Information:Result Code=0&&Additional Information:Ticket Encryption Type=0x17&&Additional Information:Pre-Authentication Type=2&&Network Information:Client Address=ffff:192.168.100.798&&Network Information:Client Port=54493&&Certificate Information:Certificate Issuer Name=&&Certificate Information:Certificate Serial Number=&&Certificate Information:Certificate Thumbprint=
```

Autentizačná autorizačná infraštruktúra

Farma autentizačných serverov

Externý Identity Store

Chránená zóna

Web & email sec. app

SIEM

Chránené servery DC

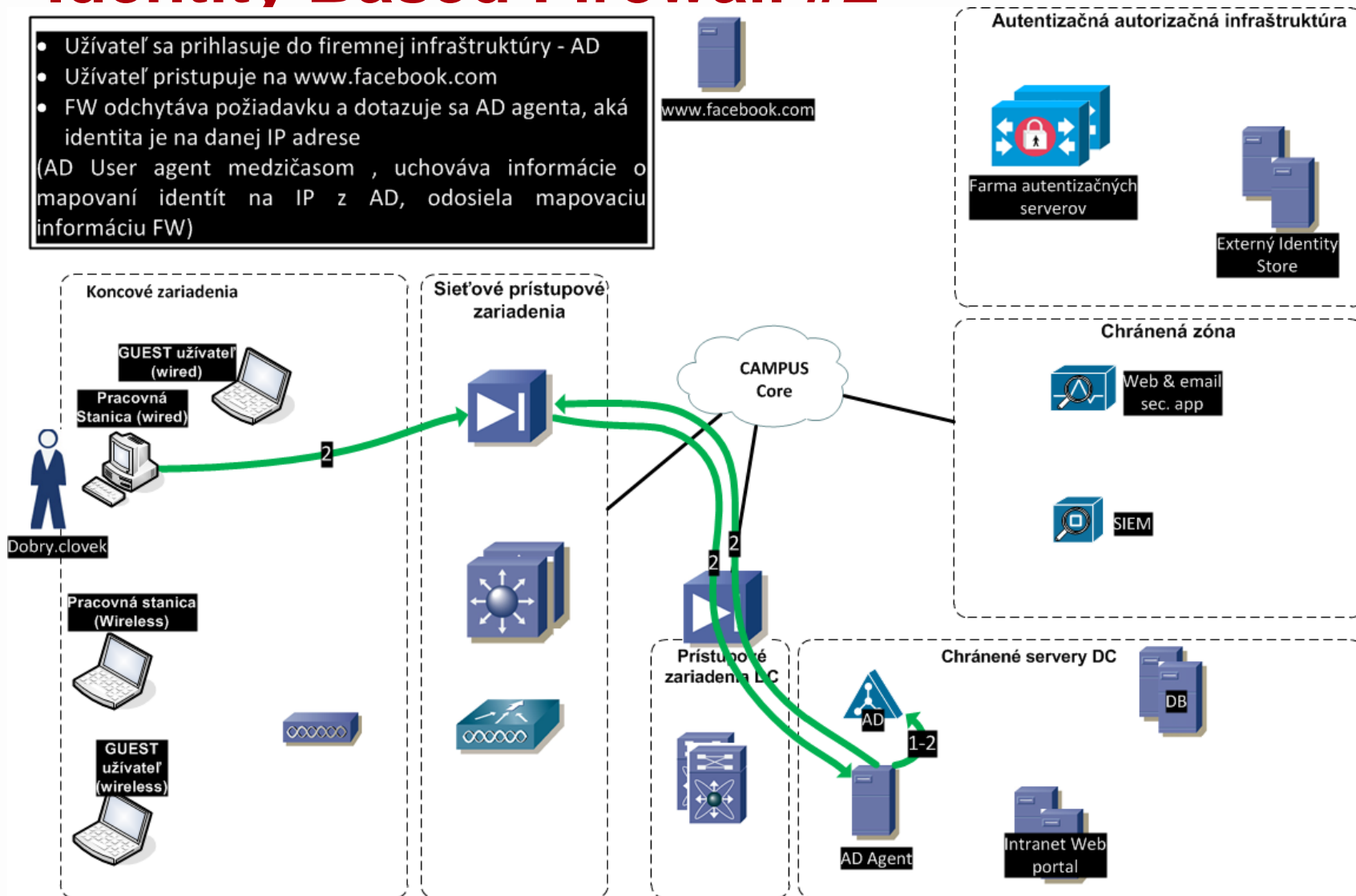
AD Agent

DB

Intranet Web portal

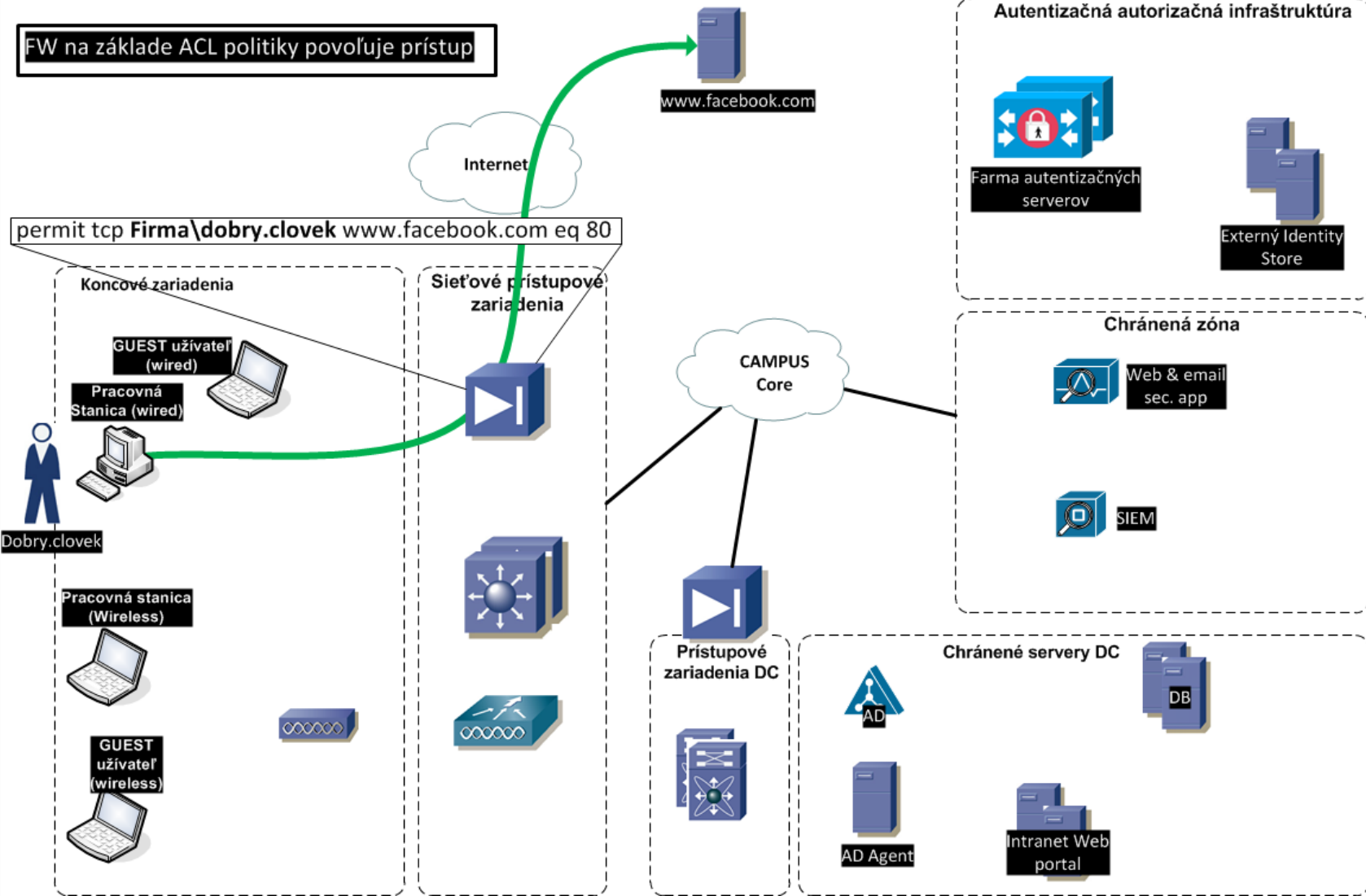
Identity Based Firewall #2

- Užívateľ sa prihlasuje do firemnej infraštruktúry - AD
- Užívateľ pristupuje na www.facebook.com
- FW odchyťáva požiadavku a dotazuje sa AD agenta, aká identita je na danej IP adrese
(AD User agent medzičasom , uchováva informácie o mapovaní identít na IP z AD, odosiela mapovaciu informáciu FW)



Identity Based Firewall #3

FW na základe ACL politiky povoľuje prístup



Identity packetFilter – scenár

- Filtrovanie IP prevádzky virtuálnych pracovných staníc podľa BP

Definícia problému: na jednej virtuálnej pracovnej stanici sa menia užívatelia s rozdielnym typom prístupu.

Možnosti:

- Pre každý typ prístupu definovať infraštruktúru (iACL)
 - Nevýhoda: pracovná stanica je pevne priradená do infraštruktúry, napr. pracovná stanica pre HR, pracovná stanice pre IT
- Aplikovať ACL pre danú IP komunikáciu podľa aktuálne prihlásenej identity

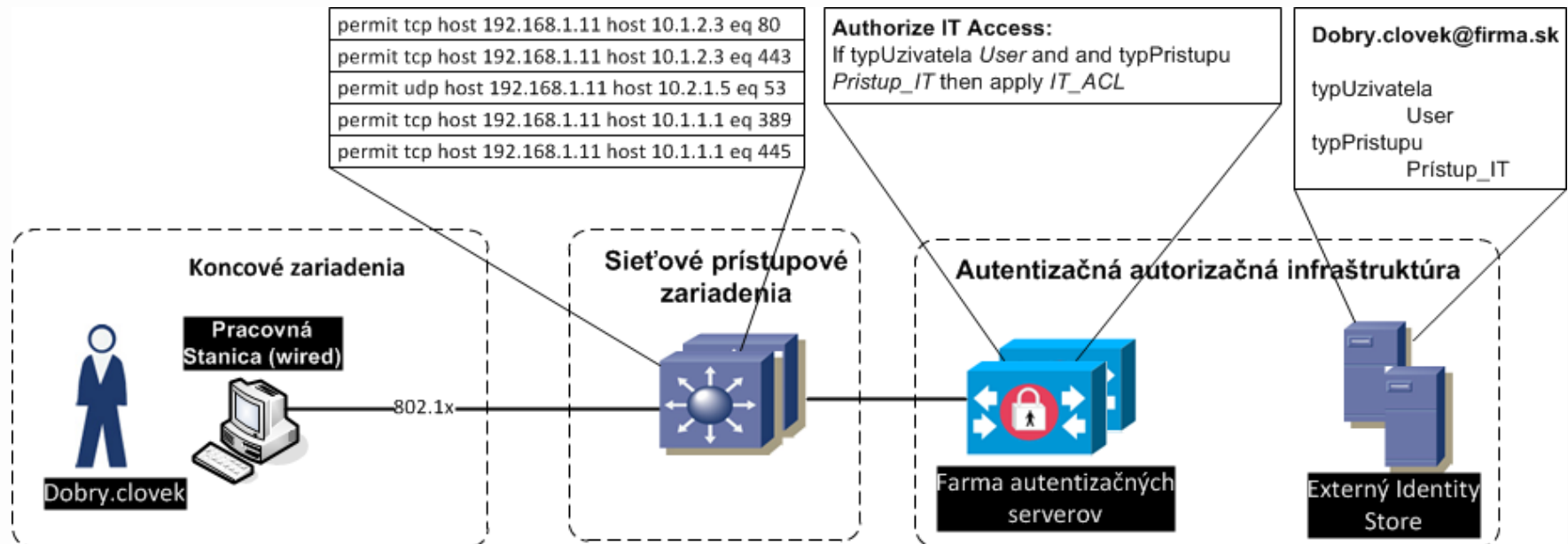
Identity packetFilter – Zákl. princíp IBNS

Komponenty:

- **Sieťové prístupové zariadenia** – zariadenia poskytujúce sieťový prístup (Network access devices – NAD, napr. prepínače, smerovače, bezdrôtové prístupové body, Cisco ASA). Sieťové prístupové zariadenia na základe autorizácie autentizačným a autorizačným serverom presadzujú prístupovú politiku vo vzťahu k pripájaným zariadeniam (povoľujú resp. obmedzujú prístup k sieťovým službám pre pripájané koncové zariadenia)
- **Autentizačný server** - vyhodnocuje rozsah prístupu oproti definovanej prístupovej politike a v súlade s touto prístupovou politikou vynúti presadenie prístupovej politiky na sieťovom prístupovom zariadení (napr. prepínač, bezdrôtový prístupový bod, ...).
- **Externý Identity Store (IS)** – centrálné úložisko atribútov pre určenie rozsahu prístupu pre autentizovanú infraštruktúru. Ako IS môže byť použitý generická adresárová služba prístupná protokolom LDAP alebo Microsoft *Active Directory*
- **Pracovná stanica** – zariadenie požadujúce pripojenie na sieť
 - *Suplikant* – komponent pracovnej stanice komunikujúci s autentikátorom. Pracovná stanica môže obsahovať suplikanta pre wired (drôtovú) a wireless (bezdrôtovú) sieť. Ako suplikant pre pracovné stanice s OS Windows je možné použiť špecializovaného klienta Cisco Secure Services Client alebo natívneho suplikanta v OS Windows XP

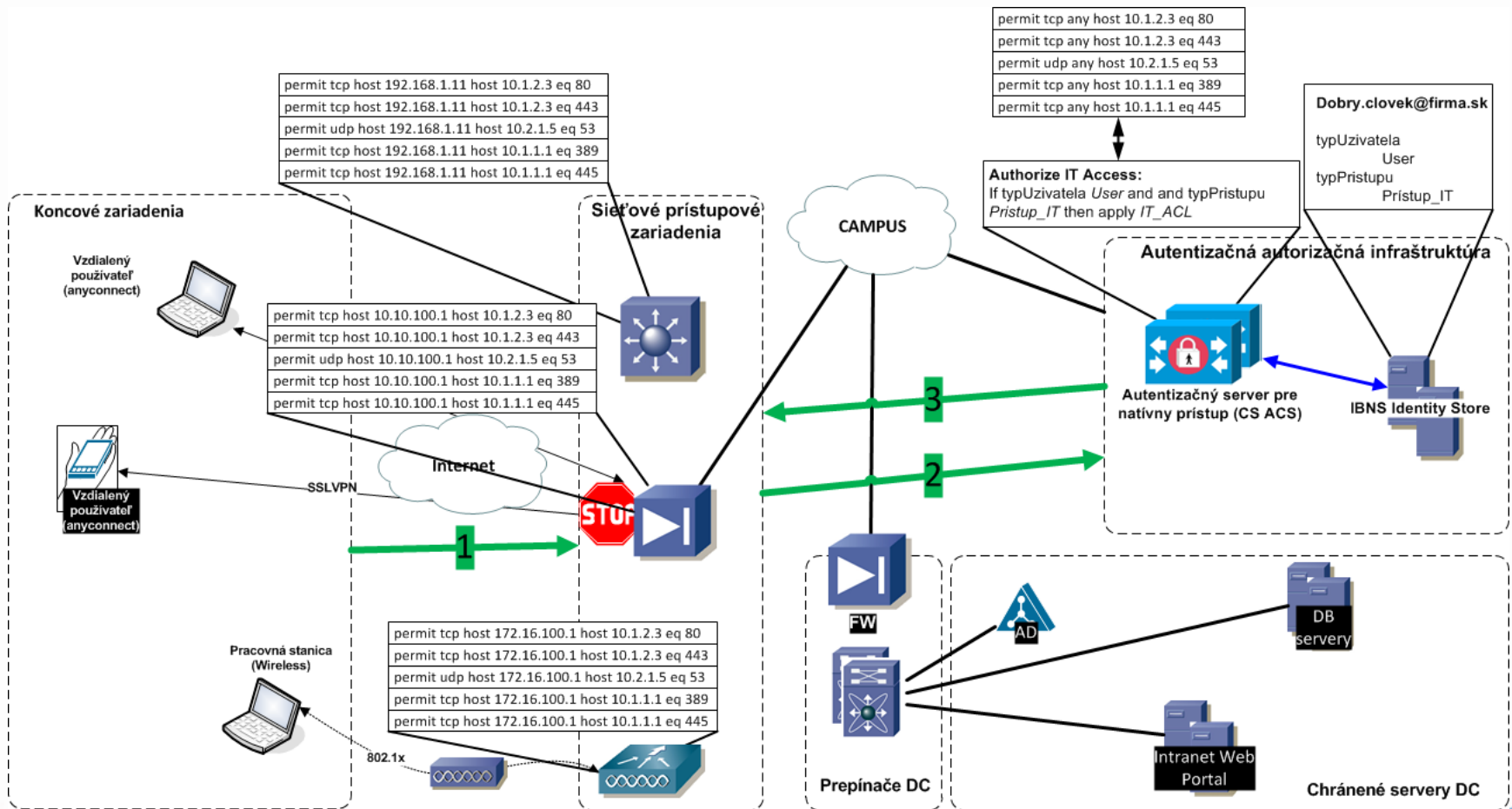
Identity packetFilter – Zákl. princíp IBNS

1. Koncové zariadenie sa pripája do infraštruktúry
2. Sieťové prístupové zariadenie vykonáva AA
3. Autentizačný server zisťuje príslušnosť identity a typu prístupu
4. Autentizačný server autorizuje prístupové zariadenie
5. Prístupové zariadenie aplikuje nastavenia

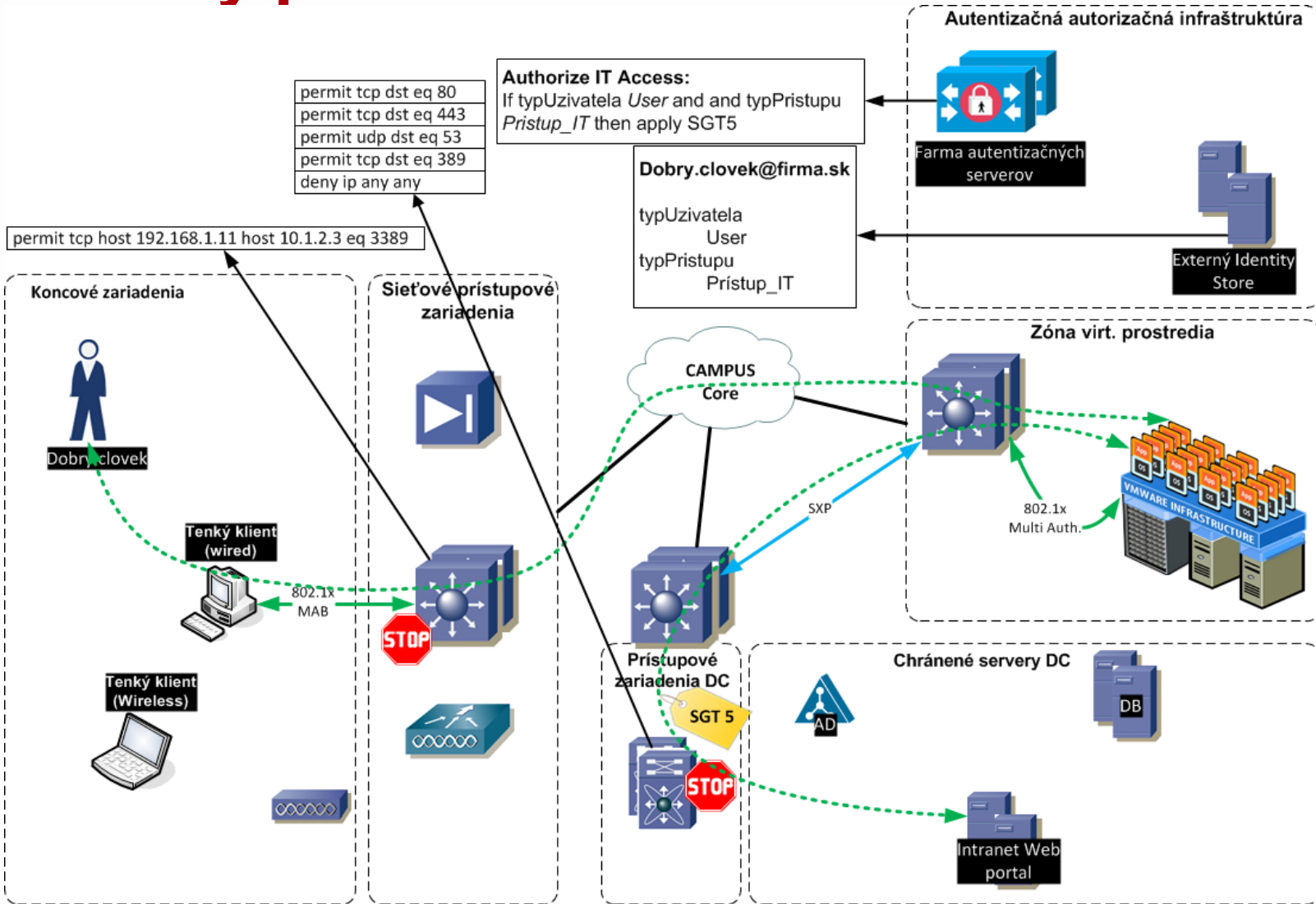


Identity packetFilter

1. Koncové zariadenie sa pripája do infraštruktúry
2. Sieťové prístupové zariadenie vykonáva AA
3. Autentizačný server notifikuje prístupové zariadenie



Identity packetFilter a TrustSec



Zhodnotenie pre IBAC - todo

1. Dynamické prístupové zoznamy (dACL) na všetkých zariadenia napr. Wifi
2. Change of Authorization (CoA) na na všetkých zariadeniach napr. ASA
3. Identity firewall (IDF) – definovanie politík s pomocou ACS
4. SGT enforcement na ASA zariadeniach



Ďakujem za pozornosť

marek.kloc@lynx.sk