# Access control list

Least privilege concept

ACL – Súbor pravidiel, dáme ich na interface (na 1 int – 2 smery, vieme dat 2 ACL [1 na kazdy smer])

Standard ACL :

- Nie je tu protokol, iba dáme line vty

- Čisto iba zdrojova IP, skôr na management veci

- ACL – Permit/Deny/Remark – Source Addr

Extended ACL :

- Je tam aj protokol

- ACL – Permit/Deny/Remark – Protokol Source Addr– Destination Addr

Applying an ACL

Syntax – apply an ACL to an interface   
 ip access-group in\out

Syntax – apply an ACL to the VTY lines  
 access-class in\out

Show access-list  
 ukaze co je povolene

ACL guidelines

* create an ACL globally and then apply it
* ensure the last statement is an implicit “deny any” | “deny any any”
* remember that statement order is important bcs ACLs are processed top-down. As soon its matched the ACL is exited.
* …

Mitigate attacks

Antispoofing with ACLs   
 block weird ip, private ips, ip as broadcast or 0.0.0.0

Permitting necessary traffic through a firewall  
 permit specific type of msg and ip and port  
 access-list 180 permit udp any host 192.168.20.2 eq domain

Mitigating ICMP abuse  
 permit icmp any ani echo-reply  
 …

Firewall technologies

Jednoduche pravidla v firewall v beznom routry je ze vsetko von z siete je povolene a aj odpovede, ale vsetko co chce ist dnu je blokovane

1st gen Firewall - je na 3 a 4tej vrstve  
 ….  
 next gen firewall - dnesne firewalls, vieme specifikovat kt aplikacia na   
 (napr facebooku) bude povolena

Vieme tur obit aj security layer-i  
 a maju centralizovany management

Spoofing – tvárenie sa ako niekto iný

SNMP – protokol na dačo s monitoring systemom, kontroluje stav zariadeni

DMZ – Demilitarized zone, niečo medzi trust a untrust, mame tma servre ktore komunikuju s ovnkajškom a keby niekto napadne DMZtku tak nenapadne naše všekto