ACCESS CONTROL LISTS (ACL)

CISCO ”Best Practice regler.”:

- Extended ACLs – Placeres **tættest muligt på Source** IP adresserne.
- Standard ACLs – Placeres **tættest muligt på Destination** IP adresserne.

Det vigtigste for os er normalt at placere filtreringen (ACL) således vores netværk (og vort udstyr) påvirkes mindst muligt. F.eks. hvis vi vil filtrere Ping signaler kommende udefra således de ikke bliver routet på vores netværksudstyr (og derved tager båndbredde og processor kraft) er det bedst at placere sådan en ACL ”INBOUND” på det interface som leder ud på internettet. Denne type ACL vil være en EXTENDED ACL fordi vi filtrerer på bestemte typer data (PING PAKKER / ICMP og ICMP_ECHO.)

Husk at der i alle ACL er en implicit (usynlig) linje til sidst som betyder ”Deny Any Any) Derfor vær sikker på at de linjer du har skrevet i din ACL ikke kun indeholder Deny statements.

STANDARD ACL PÅ ROUTER (IPv4)	EXTENDED ACL PÅ ROUTER (IPv4)
1-99 og **1300-1999** (kan navngives) Kan filtrere på: **Source IP** adresser	**100-199** og **2000-2699** (kan navngives) Kan filtrere på: **Source** og **Destination IP** adresser **Protokoller** og **Port** numre
SYNTAKS: Router(config)# **access-list** *access-list-number* **deny permit remark** *source* [*source-wildcard*] [**log**] **“Access-list 1 permit 192.168.0.0 0.0.0.127”**	**SYNTAKS:** Router(config)# **access-list** *access-list-number* **deny permit remark** source [*source-wildcard*] **operator** *operand* **port** *port-number or name* destination [*destination-wildcard*] **operator** *operand* **port** *port-number or name* **established** **“access-list 101 permit tcp 192.168.0.0 0.0.0.127 any eq 80”**
LINKNING TIL ROUTNINGS INTERFACE: Router(config-if)# **ip access-group** { *access-list-number* | *access-list-name* } { **in** | **out** }	**LINKNING TIL ROUTNINGS INTERFACE:** Som STANDARD ACL
LINKNING TIL LINE INTERFACE: Router(config-line)# **access-class** *access-list-number* { **in** [**vrf-also**] | **out** }	**LINKNING TIL LINE INTERFACE:** Som STANDARD ACL

IPv6 ACL
Named only (ingen nummerering – skal navngives) Filtrerer på Source, Destination IP, Protokoller og Port numre (**Som EXTENDED ACL IPv4**.)