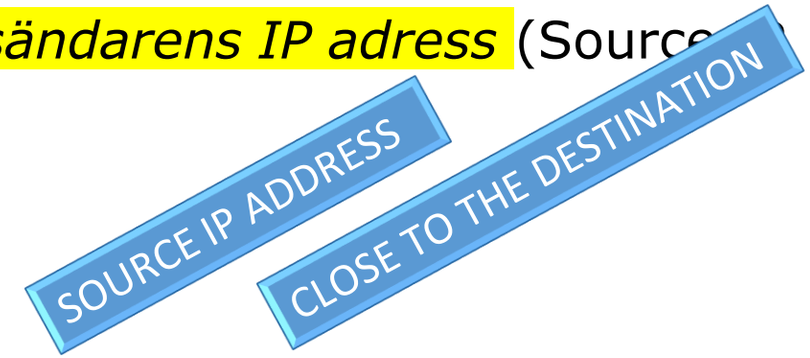
Nätverkssäkerhet

Numerisk och namngiven Extended ACL

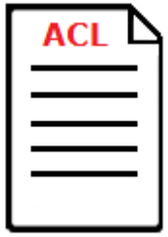
Typer av ACL

- Standard ACL (1 - 99 och 1300 - 1999).
  - Standard ACL filtrerar paket grundad endast på *avsändarens IP adress* (Source address) och tillämpas *nära destinationen*
- Extended ACL (100 - 199 och 2000 - 2699).
- Extended ACL filtrerar paket grundad i
  - Avsändarens IP adress (Source IP address)
  - Mottagarens IP adress (Destination IP addres)
  - Protokolltyp
  - Port nummer
- Vart ska ACL tillämpas?
- Regler för ACL
  - En lista per typ, per riktning, per interface
  - Ett ACL nummer identifierar typen
  - Inga betydelse inom varje intervall

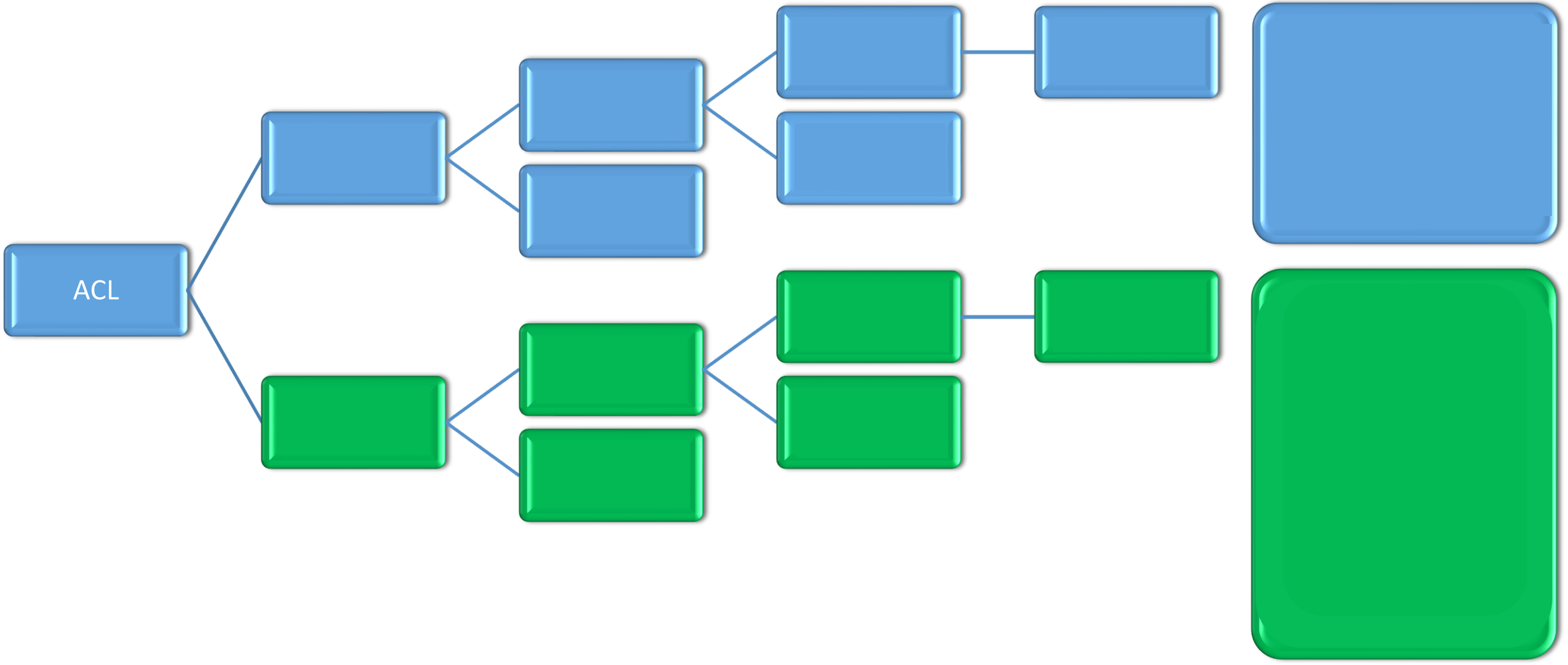
CLOSE TO THE SOURCE



Standard eller Extended ACL?
Har jag kontroll över nätet?
Hur påverkas nätverkstrafiken?

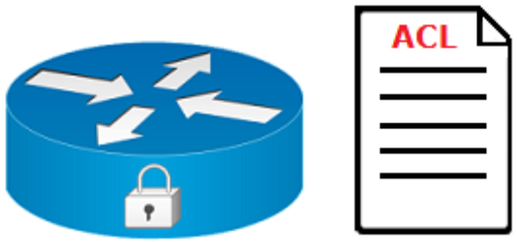


ACL typer



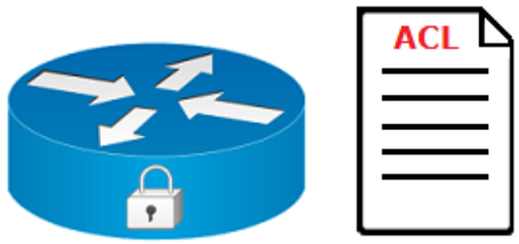
Extended ACL

- *Vad är en Extended ACL?*
- En ordnad lista över villkor som måste uppfyllas så att paket tillåtas eller nekas passera genom routern.
- Extended ACL baseras på source och destinations IP-adresser, portnummer och protokolltyp.
- *Vad bör man tänka på?*
  - Fullständig kontroll över nätverksdesignen
  - Fullständig kontroll över protokoll och deras portnummer
  - Definiera vilka tjänster ska tillåtas eller nekas i enlighet med en säkerhetspolicy
  - Planera skapande av ACL och välj rätt interface för ACL-tillämpning.
  - Analysera ordningen av alla villkor i alla ACL
  - Man ska inte glömma att i slutet av listan finns ett osynligt villkor som nekar allt.



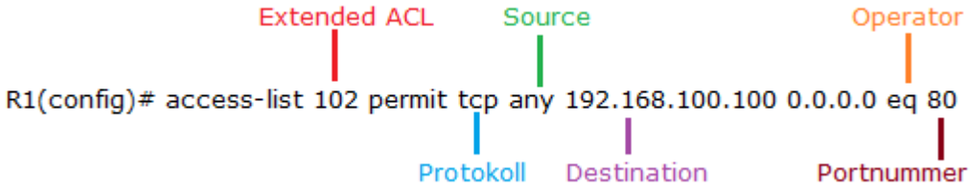
Extended ACL

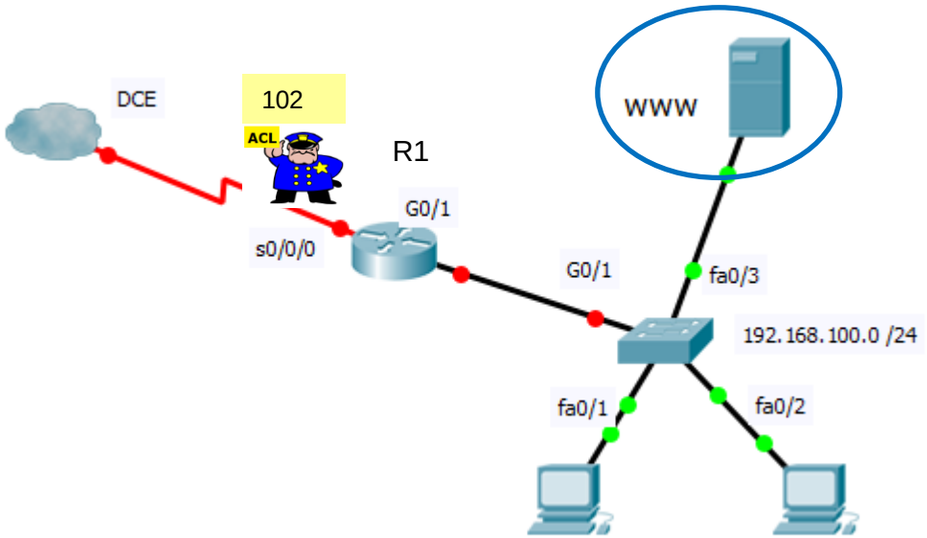
- *Syntax*
- access-list <nummer 100-199> <permit | deny> <protokoll> <source IP> <wildcard mask> <operator> <source port> <destination IP> <wildcard mask> <operator> <destination port> <options> <log>
- R1(config)# access-list 102 permit tcp any 192.168.100.100 0.0.0.0 eq 80
- Förklaringar:
  - *access-list* är kommandot som skapar en ACL
  - Extended ACL identifieras med ett nummer från intervallet *100-199 eller 2000-2699*
  - antingen *permit* eller *deny,* inte båda
  - protokoll såsom IP, TCP, UDP, ICMP, GRE och IGRP. TCP, UDP och ICMP använder IP i nätverksskiktet.
  - source IP-adress och dess wildcard mask
  - flera *operator* kan användas *lt*, *gt*, *eq*, *neq* och *portnummer*
  - destination IP-adress och dess wildcard mask



Extended ACL

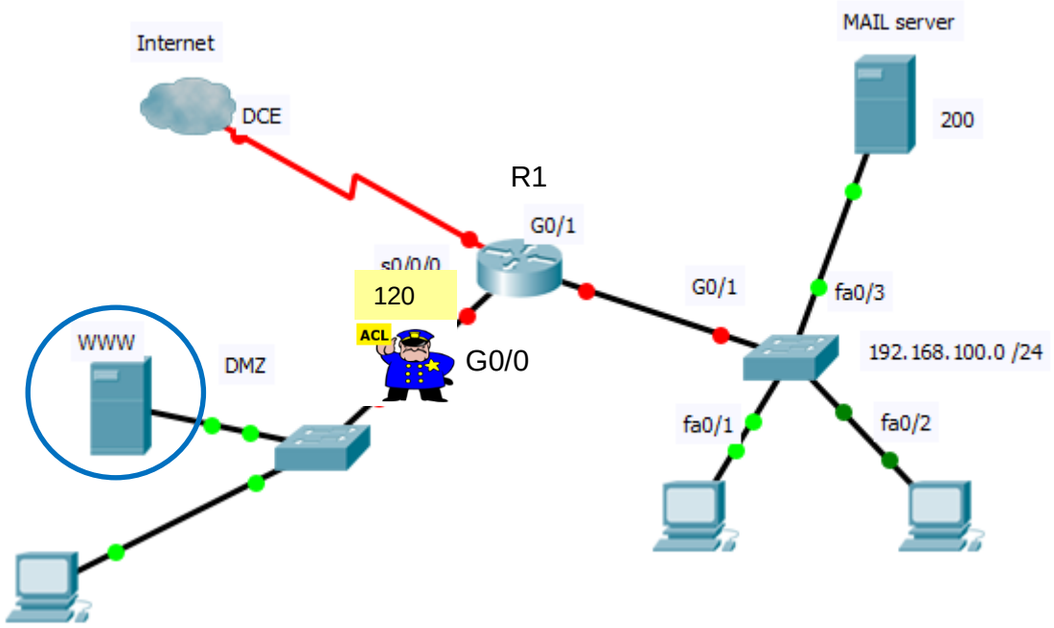
- *Var ska du applicera dina ACL?*
- Scenario 1
- I denna scenario är ditt mål att filtrera inkommande trafik så att användare utanför ditt nätverk kan komma åt webbservern (192.168.100.100) via port 80.
- All annan inkommande nätverkstrafik ska nekas.
- R1(config)# access-list 102 permit tcp any 192.168.100.100 0.0.0.0 eq 80
- R1(config)# int s0/0/0
- R1(config-if)# ip access-group 102 in





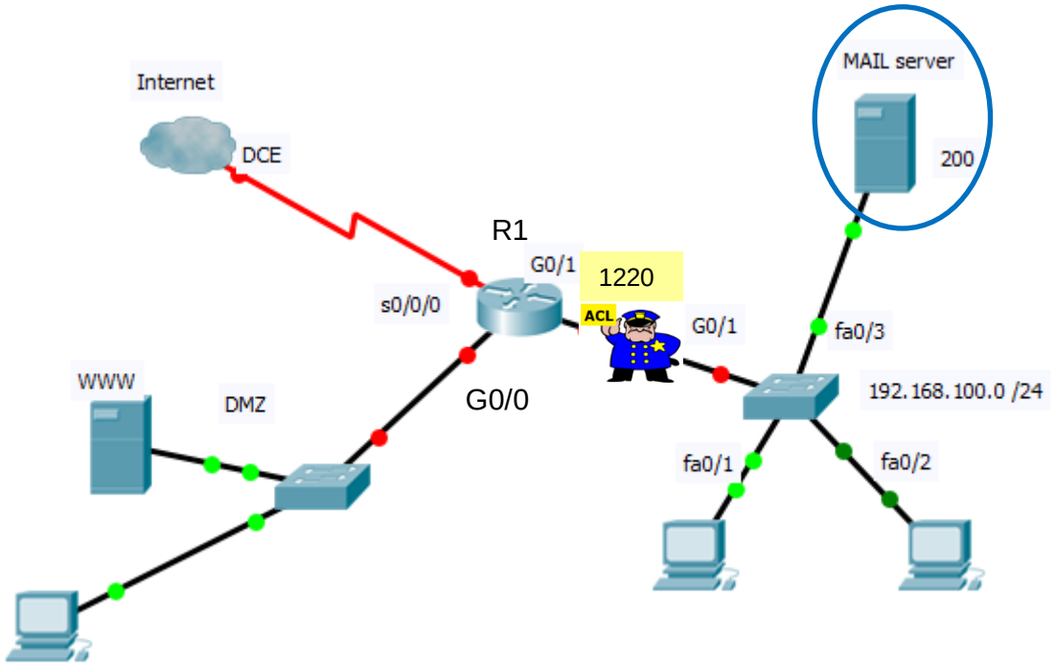
Extended ACL

- *Var ska du applicera dina ACL?*
- Scenario 2 – www IP 192.168.200.200
  - Tillåta all trafik till den offentliga webbservern i DMZ nätverk.
- R1(config)# access-list 120 permit tcp any 192.168.200.200 0.0.0.0 eq 80
- R1(config)# int G0/0
- R1(config-if)# ip access-group 120 out



Extended ACL

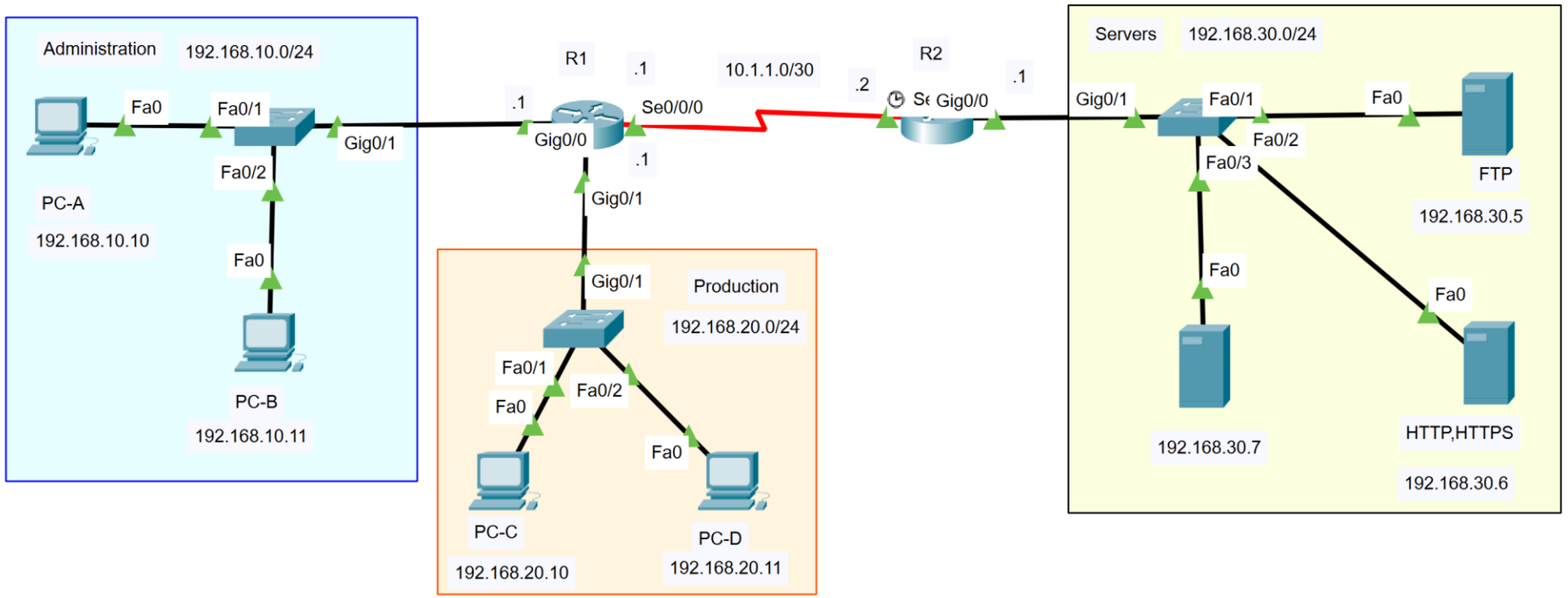
- *Var ska du applicera dina ACL?*
- Scenario 3 – MAIL server IP 192.168.100.200
  - Tillåta endast e-posttrafik till MAIL-server
- R1(config)# access-list 122 permit tcp any 192.168.100.200 0.0.0.0 eq 25
- R1(config)# int G0/1
- R1(config-if)# ip access-group 122 out
- R1(config-if)#exit
- R1(config)#




DIGINTO
Extended ACL 1

Extended ACL - 1

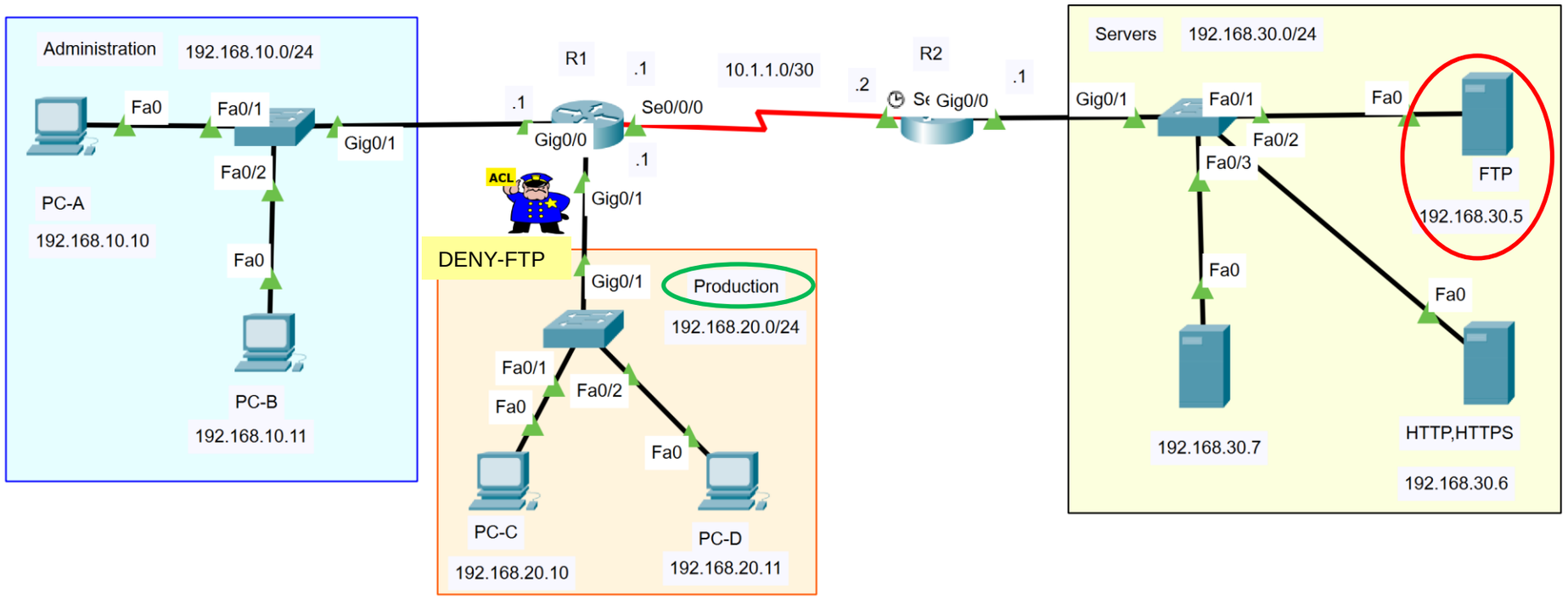
- *Task 1: Endast host i Production nätverk nekas åtkomst till FTP server.*
- *Task 2: Host PC-A behöver komma åt HTTP-server med IP-adress 192.168.30.6. Åtkomsten ska tillåtas endast via HTTPS och inte med HTTP.*
- *Task 3: Host PC-D nekas IP-kommunikation via PING med server adresserad med 192.168.30.7 medan alla andra host får kontakta servern via PING.*



Extended ACL 1 – Task 1

Endast hosts i Production nät nekas åtkomst till FTP server.

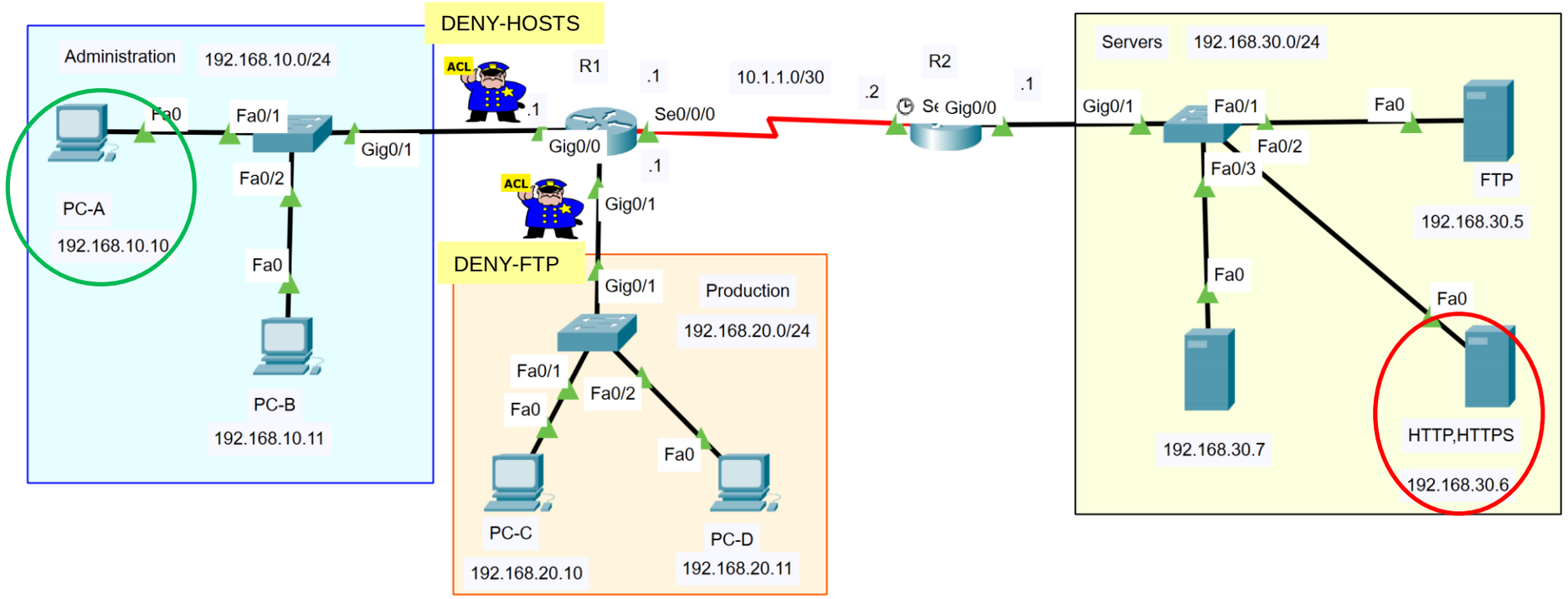
- R1(config)#ip access-list extended DENY-FTP
- R1(config-ext-nacl)#10 deny tcp 192.168.20.0 0.0.0.255 host 192.168.30.5 eq ftp
- R1(config-ext-nacl)#20 permit ip any any
- R1(config-ext-nacl)#exit
- R1(config)#interface g0/1
- R1(config-if)#ip access-group DENY-FTP in
- R1(config-if)#exit



Extended ACL 1 – Task 2

Host PC-A får komma åt HTTP-server endast via HTTPS.

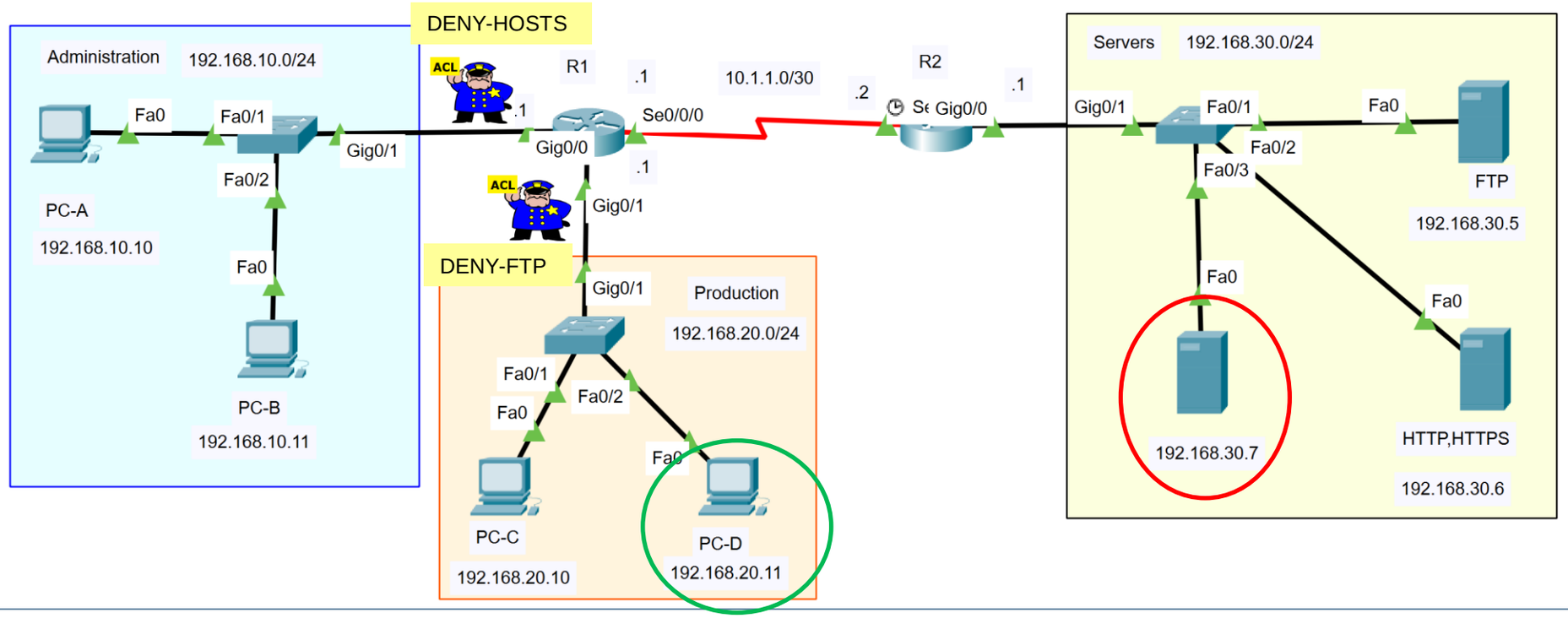
- R1(config)#ip access-list extended DENY-HOSTS
- R1(config-ext-nacl)#10 deny tcp host 192.168.10.10 host 192.168.30.6 eq www
- R1(config-ext-nacl)#20 permit ip any any
- R1(config-ext-nacl)#exit
- R1(config)#interface g0/0
- R1(config-if)#ip access-group DENY-HOSTS in
- R1(config-if)#end



Extended ACL 1 – Task 3

Endast host PC-D nekas IP-kommunikation via PING med server adresserad med 192.168.30.7

- R1(config)#ip access-list extended DENY-FTP
- R1(config-ext-nacl)#15 deny icmp host 192.168.20.11 host 192.168.30.7 echo
- R1(config-ext-nacl)#end
- R1#
- Verifiera konfigurationerna



Nätverkssäkerhet