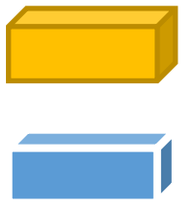

DIGINTO
Nätverkssäkerhet


DIGINTO
Access Control List - ACL

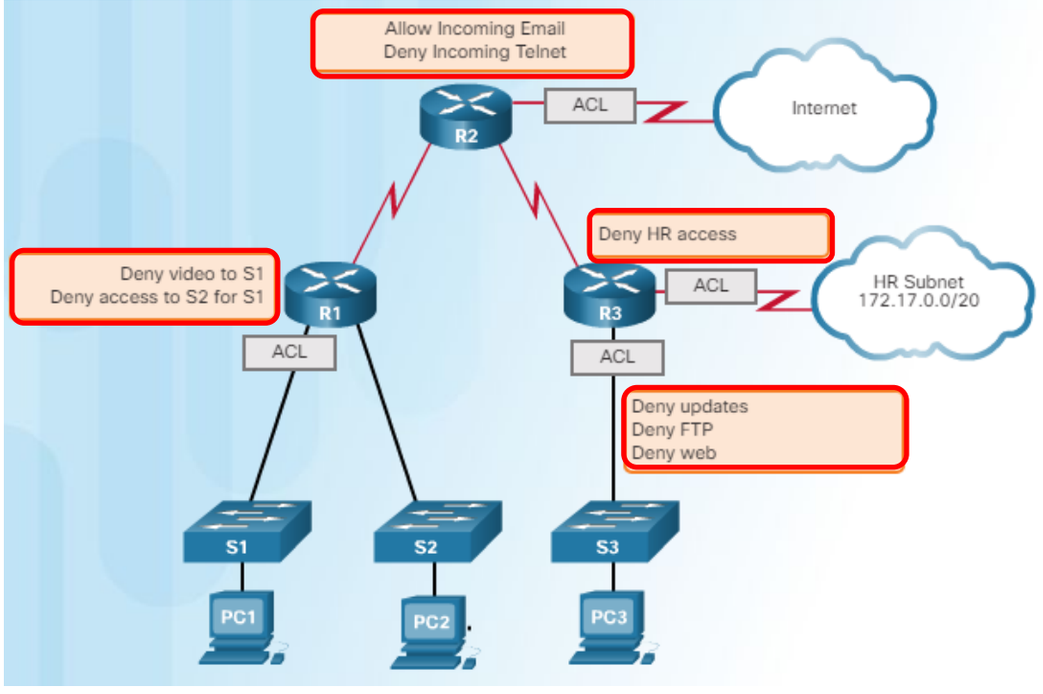
Vad är en Access Control List?

- En ACL är en sekventiell lista av tillåtande och nekande satser kända som *Access Control Entries*.
- Vi kan tolka ACL som en samling av villkor som ska uppfyllas innan en router tar emot ett paket och innan paketet släpps vidare.
- Vi kan ställa in så många villkor som vi vill ha i en och samma ACL.
- ACL är den viktigaste kunskap för nätverksadministratörer.
- Säkerhets specialister föredrar använda dedikerade brandvägg.
- Brandvägg grundar sitt arbete i ACL.
- ACL kan konfigureras på vanliga Cisco routrar



Vad kan man åstadkomma med ACL?

- Begränsa nätverkstrafik för att öka nätverksprestanda.
- ACL kan blockera videotrafik om företagspolicyn inte tillåter det.
- ACL kan tillåta/neka åtkomst till en host i ett nät eller till hela nätverket.
- ACL kan säkerställa att uppdateringarna kommer från tillförlitliga källor.
- ACL kan filtrera nätverkstrafik baserat på trafiktyp.
- Till exempel kan en ACL tillåta e-posttrafik, men blockera all Telnet-trafik.



När kan routrar filtrera paket?

- Paketfiltrering sker i skikten 3 och 4, Transport och nätverk.
- Ett paket interagerar med tre komponenter i sin resa genom en router
- Packet kommer i kontakt med ett interface (Entrance)
- Routern gör sitt vägval och tar ett vidarebefordringsbeslut
- Paket lämnar routern via ett interface (Exit)
- Vi kan inte filtrera paketet mitt i routerns pakethantering.
- Vidarebefordringsbeslutsprocessen har sin egen logik och bör inte interfereras för filtreringsändamål.

När kan routrar filtrera paket?

- ACL-villkor som tillämpas vid ingång-interface definieras som inkommande filter, "*Inbound filter*".
- ACL-villkor som tillämpas vid utgång-interface definieras som utgående filter, "*Outbound filter*".
- Inkommande filter filtrerar trafiken innan router startar vidarebefordringsbeslutet.
- Utgående filter filtrerar trafiken efter att routern har tagit vidarebefordringsbeslutet.

Wildcard – inverterat nätmask

- Wildcard användas för att identifiera bitar i en destinationsadress.
- Wildcard är en inverterad nätmask där 1 blir 0 och 0 blir 1
- 255.255.255.0
- 1111 1111.1111 1111.1111 1111.0000 0000
- 0000 0000.0000 0000.0000.0000.1111 1111
- 0.0.0.255
- Vad blir wilcard för 255.255.248.0?
- 1111 1111.1111 1111.1111 1000.0000 0000
- 0000 0000.0000 0000.0000 0111.1111 1111
- 0.0.7.255
- 255.255.255.255 - 255.255.248.0 = 0.0.255-248.255 = 0.0.7.255
- Vilka delar i IP-adressen 192.168.10.0 matchar med 0.0.255.255
- I en wildcard ignoreras alla ettor, det vill säga alla 255 nollställs i adressen

	Decimal Address	Binary Address
IP Address to be Processed	192.168.10.0	11000000.10101000.00001010.00000000
Wildcard Mask	0.0.255.255	00000000.00000000.11111111.11111111
Resulting IP Address		11000000.10101000.00000000.00000000

Wildcard – inverterat nätmask

- Vilka bitar i adresser nedan matchar med respektive wildcard?
- 192.168.1.1 –- 0.0.0.0 ---------- 192.16
- 192.168.1.1 –- 255.255.255.255 ---------- 0.0.0.0
- 192.168.1.1 –- 0.0.0.255 ---------- 192.168
- 192.168.16.0 – 0.0.15.255 ---------- 192.168
- Vad? 0.0.15.
- I adressen ska matcha de två första oktett och fyra bitar i tredje oktett.
- 192.168.16.0 = 1100 0000.1010 1000.0001 0000.0000 0000
- 0.0.15.255 = 1111 1111.1111 1111.1111 0000.0000 0000
- 192.168.31.0 = 1100 0000.1010 1000.0001 1111.0000 0000

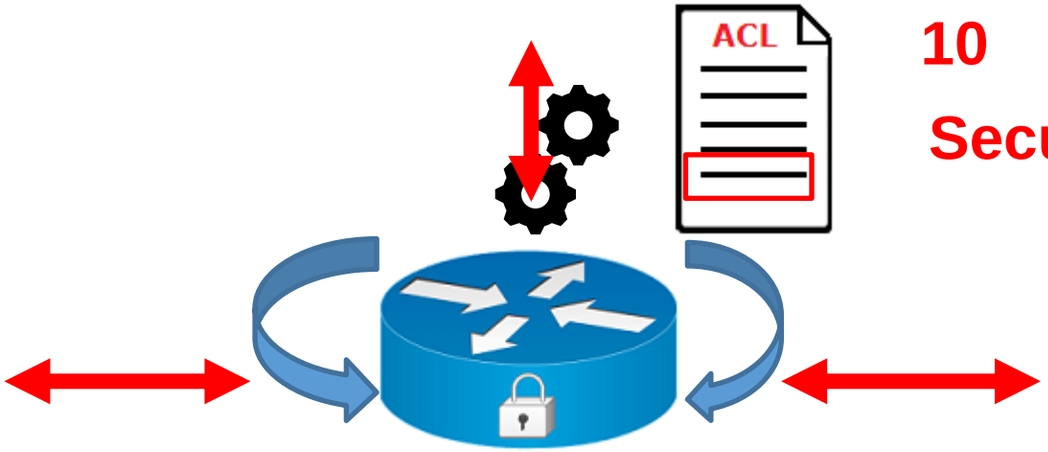
Vad ska man tänka på när man konfigurerar ACL?

- Varje paket kontrolleras med uppsatta villkor i en ACL-lista.
- ACL bearbetas alltid uppifrån och ner i sekventiellt ordning.
- Det finns två möjliga åtgärder. Permit och Deny
- När i en kontroll hittas en match för ett paket kommer ingen ytterligare kontroller att göras för det paketet.
- Interfacen kommer att vidta åtgärder baserade på matchning med ett villkor i ACL-lista.

- Access-list 10 deny 10.0.0.0 0.0.0.255
- Access-list 10 deny 20.0.0.0 0.0.0.255
- Access-list 10 deny 30.0.0.0 0.0.0.255
- Access-list 10 permit 40.0.0.200 0.0.0.255

Vad ska man tänka på när man konfigurerar ACL?

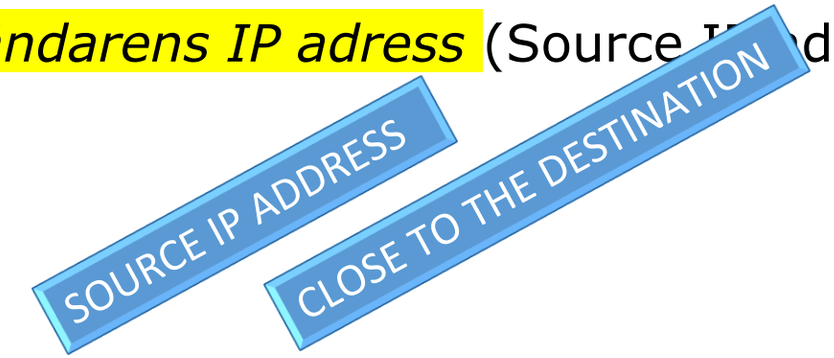
- Några ordnycklar som host och any
- *Host* ersätter 0.0.0.0 och *Any* ersätter 255.255.255.255
- host 192.168.10.10 istället 192.168.10.10 0.0.0.0
- Any istället 0.0.0.0 255.255.255.255
- Sist i ACL-lista finns en blockering till allt nätverkstrafik.
- Det kallas *implicit deny any*
- ACL kan bara filtrera paket från nätverket till nätverket.
- inte den trafik som kommer från routern själv.
- Varje ACL skapas med ett unikt nummer eller namn som identifikation.
- En routers ACL är bara en lista och har ingen påverkan i nätverkstrafiken så länge den inte är applicerad på ett specifikt interface.



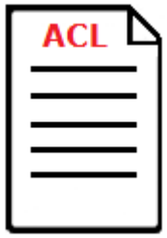
Typer av ACL

- Standard ACL (1 - 99 och 1300 - 1999).
  - Standard ACL filtrerar paket grundad endast på *avsändarens IP adress* (Source IP 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

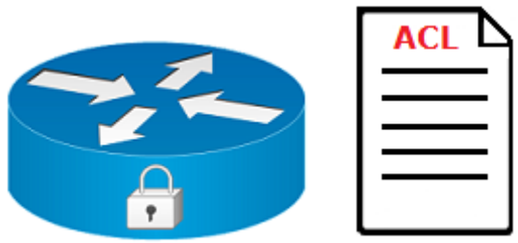


Standard eller Extended ACL?
Har jag kontroll över nätet?
Hur påverkas nätverkstrafiken?



Typer av ACL

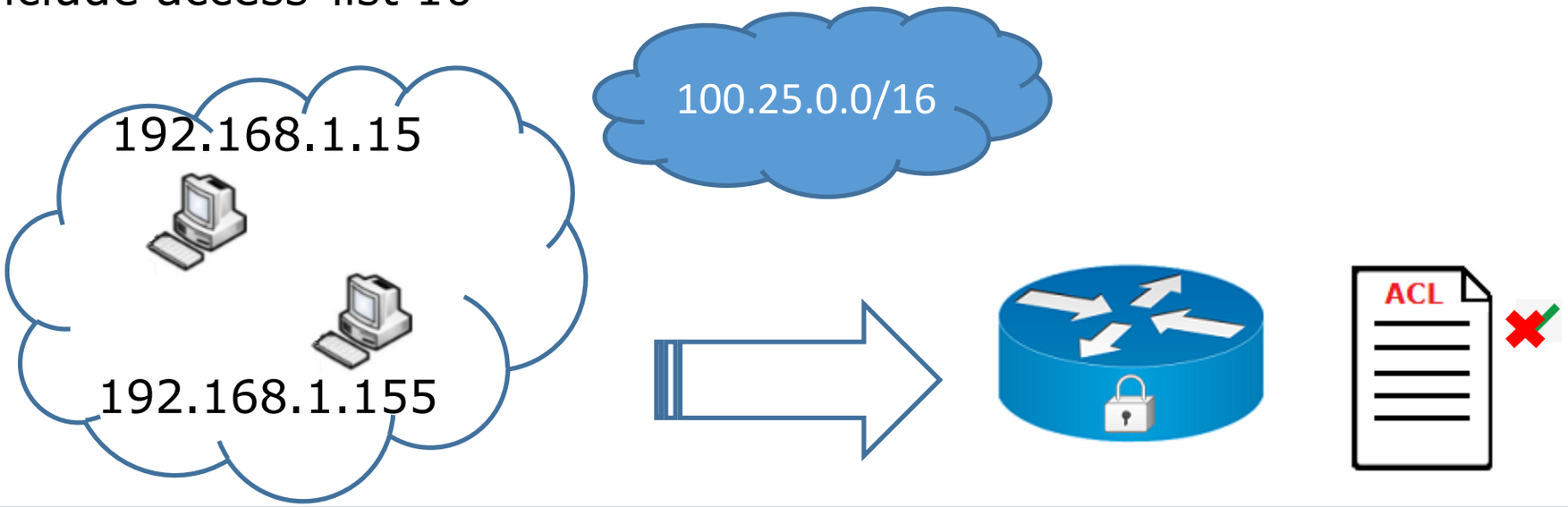
- Standard ACL identifieras normalt med ett nummer från intervallet 1 till 99 eller 1300 – 1999
- Router(config)# access-list 10
- Standard ACL kan också identifieras med ett namn
- Router(config)# ip access-list standard Block_Telnet
- Extended ACL identifieras med ett nummer från intervallet 100 till 199 eller 2000 till 2699
- Router(config)# access-list 102
- Extended ACL kan också identifieras med ett namn
- Router(config)# ip access-list extended Block_Telnet
- Sammanfattningsvis:
- Numerisk ACL
  - Numerisk standard ACL
  - Numerisk extended ACL
- Namngiven ACL (named)
  - Namngiven standard ACL
  - Namngiven extended ACL



Numerisk och namngiven Standard ACL

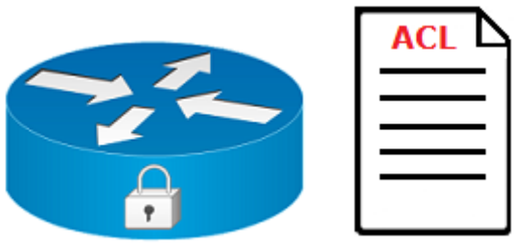
Standard ACL - syntax

- I global konfigurationsläge:
- R1(config)# access-list [1-99] [permit | deny] [source IP] [wildcard]
- Till exempel:
- Tillåt nätverkstrafik från 192.168.1.0 /24
- R1(config)# access-list 5 permit 192.168.1.0 0.0.0.255
- Neka nätverkstrafik från 100.25.0.0 /16
- R1(config)# access-list 10 deny 100.25.0.0 0.0.255.255
- R1# show access-lists
- R1# show run | include access-list 10



Standard ACL - syntax

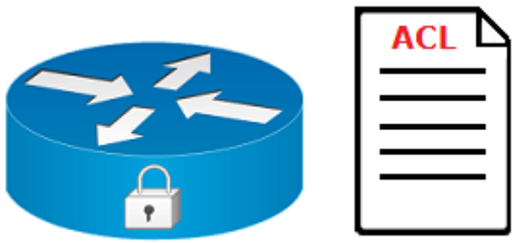
- Standard ACL identifieras med ett nummer men också med ett namn.
- Konfigurationen skiljer sig en aning
- Router(config-if)# ip access-list ACL_ namn in | out
- Exempel:
- Router(config)# ip access-list Standard Secure_Telnet
- Router(config-std-nacl)# permit 20.0.0.10 0.0.0.0
- Router(config-std-nacl)# exit
- Router(config)#
- Router(config)# interface seriell 0/0/0
- Router(config-if)# ip access-group Secure_Telnet in



Standard ACL - syntax

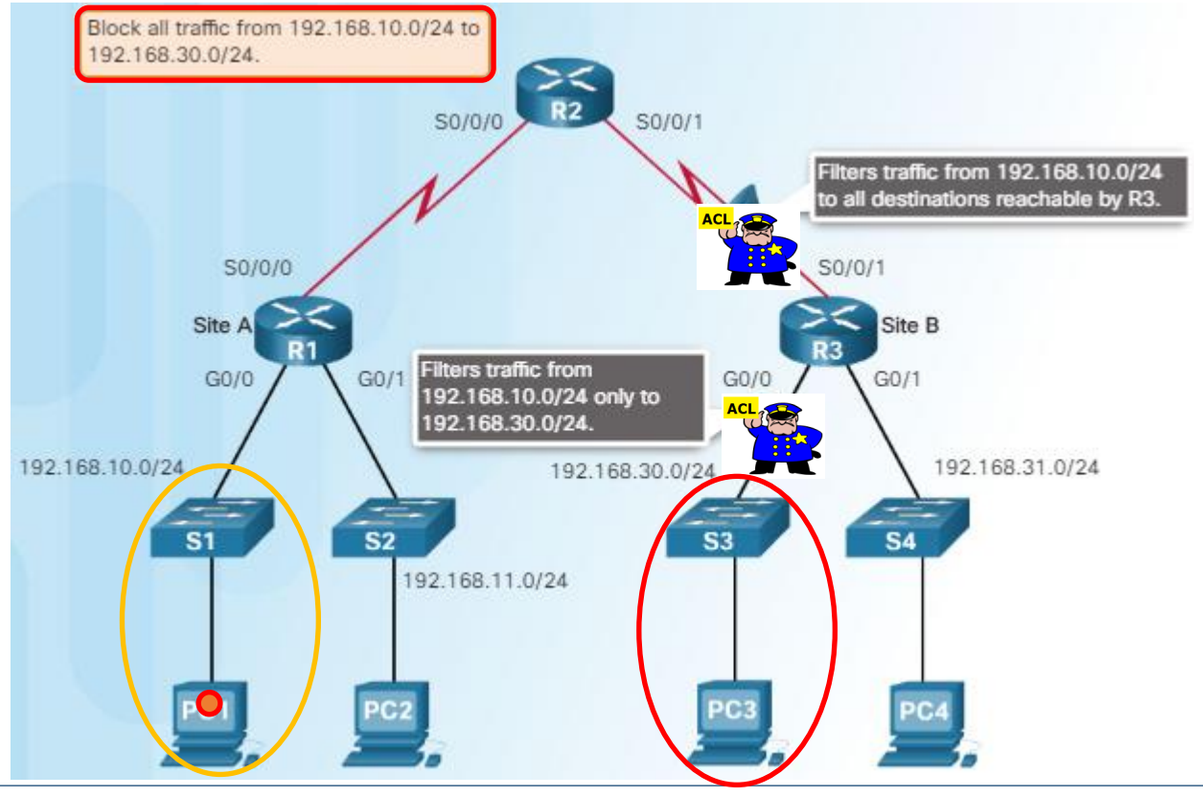
1. Permit 20.0.0.10
2. Deny any (alla andra)

- Router(config)# access-list 10 permit 20.0.0.10 0.0.0.0
- Router(
- Ordningen av villkoren spelar stor roll vid filtrering.
- Om vi skapar först villkoret deny blockerar vi trafiken från alla host, inklusive 20.0.0.10:
- Router(config)# access-list 10 deny any
- Router(config)# access-list 10 permit 20.0.0.10 0.0.0.0
- Implicit deny statement (deny any) finns sist i varje ACL
- Det vi behöver konfigurera är endast ett villkor:
- Router(config)# access-list 10 permit 20.0.0.10 0.0.0.0
- Router(config)# access-list 10 permit host 20.0.0.10
- Router(config)# int fa0/0
- Router(config)# ip access-group 10 out



Typer av ACL – placering och riktning

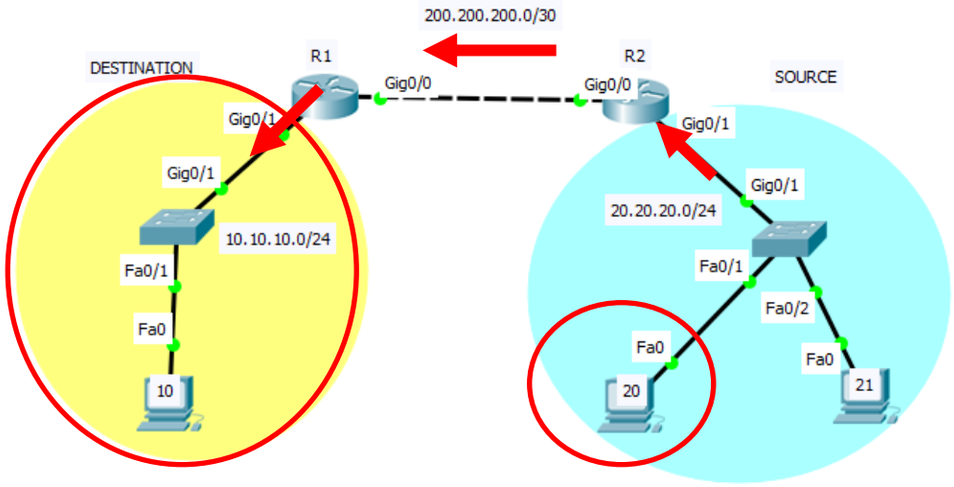
- Administratören vill förhindra åtkomst till 192.168.30.0/24-nätverk från 192.168.10.0/24-nätverk med en standard ACL.
- En av två möjliga interface på R3 skulle kunna användas:
- *S0/0/1* - förhindrar trafik till 192.168.30.0/24 men också till 192.168.31.0/24 och alla andra nät anslutna till R3.
- *G0/0* - förhindrar trafik endast till 192.168.30.0/24



Standard ACL – placering och riktning

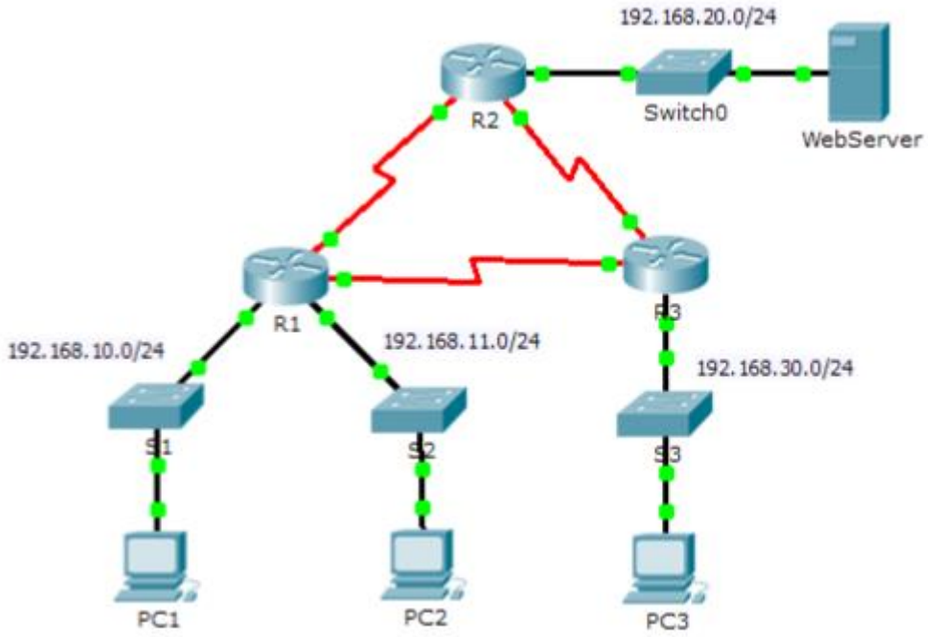
- Skapa en standard ACL som blockerar trafik från host 20.20.20.20 till nätverk 10.10.10.0
  - R1(config)# access-list 10 deny 20.20.20.20 0.0.0.0
  - Eller
  - R1(config)# access-list 10 deny host 20.20.20.20
  - R1(config)# access-list 10 permit any
- Applicera på ett interface
  - R1(config)# interface g0/1
  - R1(config-if)# ip access-group 10 **out**
- Verifiera att endast host 20.20.20.21 kan pinga till 10.10.10.10
  - R1# show access-list
  - R1# show ip interface g0/1

Från routers perspektiv!



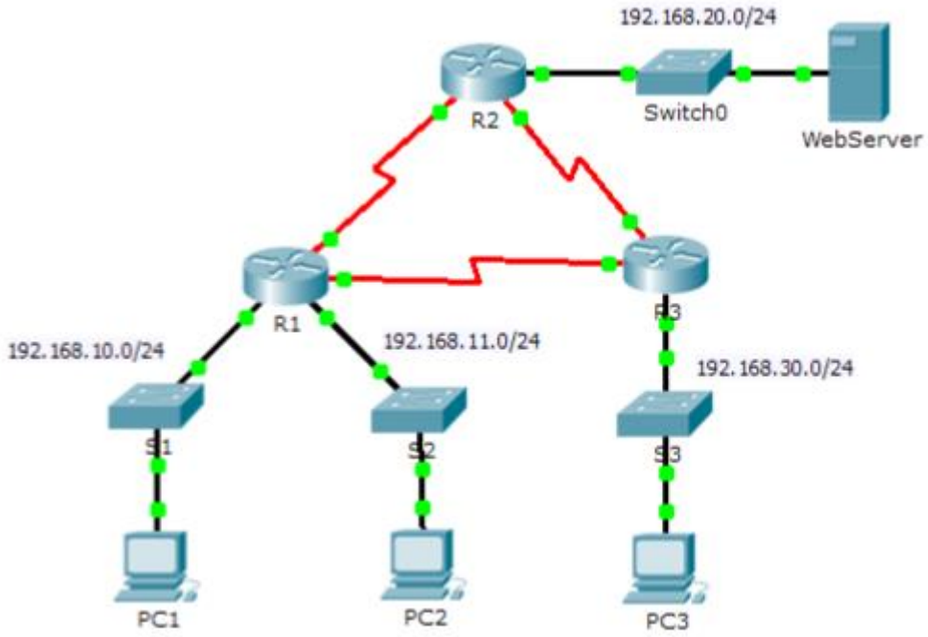
Standar ACL – exempel 1

- Nätverk 192.168.11.0/24 är inte tillåtet åtkomst till webb-server i nätverk 192.168.20.0/24. Alla andra ät tillåtna.
- ACL på R3: nät 192.168.10.0/24 nekas åtkomst till 192.168.30.0 nätet. Alla andra nät är tillåtna
- R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
- R2(config)# access-list 1 permit any
- R2(config)# interface g0/0
- R2(config-if)# ip access-group 1 out
- R2(config-if)# end
- R2#



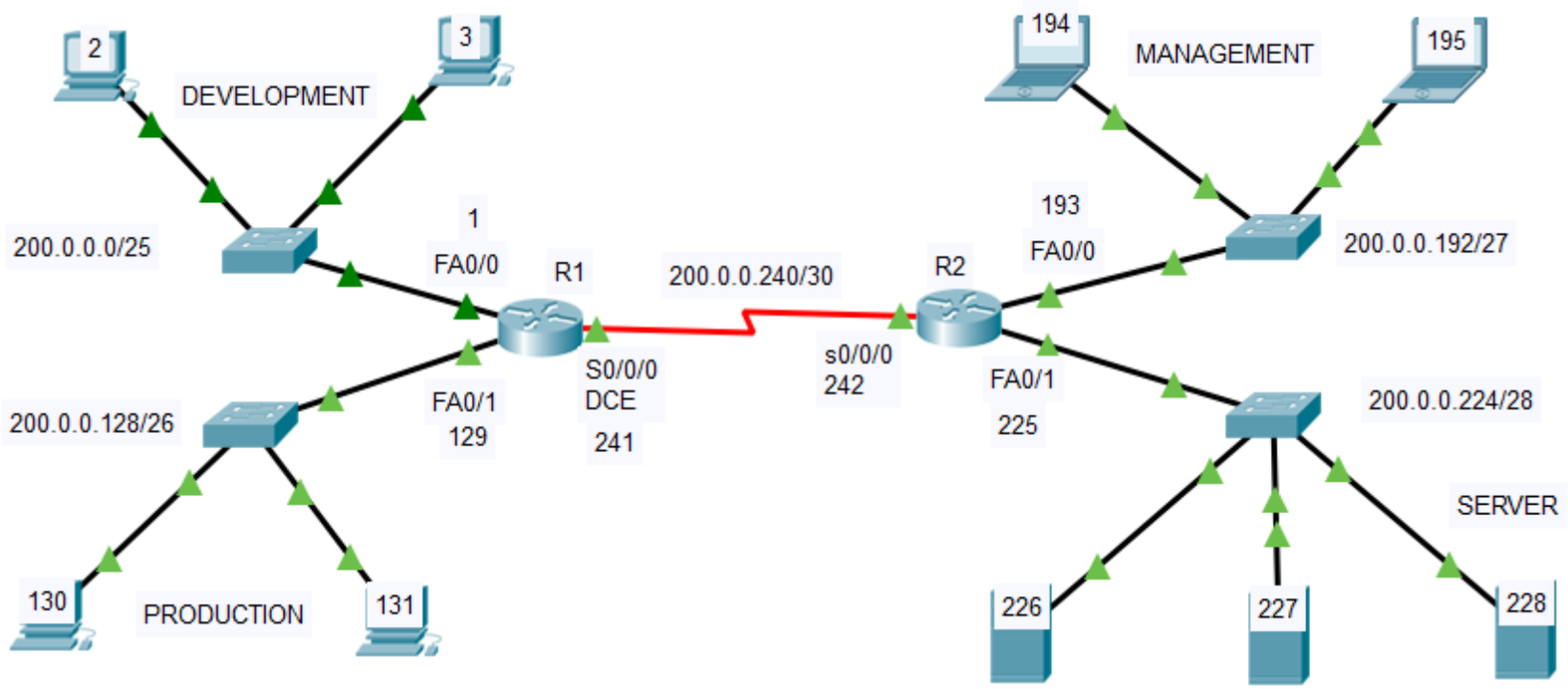
Standar ACL – exempel 1

- Nätverk 192.168.11.0/24 är inte tillåtet åtkomst till webb-server i nätverk 192.168.20.0/24. Alla andra ät tillåtna.
- ACL på R3: nät 192.168.10.0/24 nekas åtkomst till 192.168.30.0 nätet. Alla andra nät är tillåtna
- R3(config)# access-list 1 deny 192.168.11.0 0.0.0.255
- R3(config)# access-list 1 permit any
- R3(config)# interface g0/0
- R3(config-if)# ip access-group 1 out
- R3(config-if)# end
- R3#
- Testa konfigurationerna



Avancerad Standard ACL konfigurationer

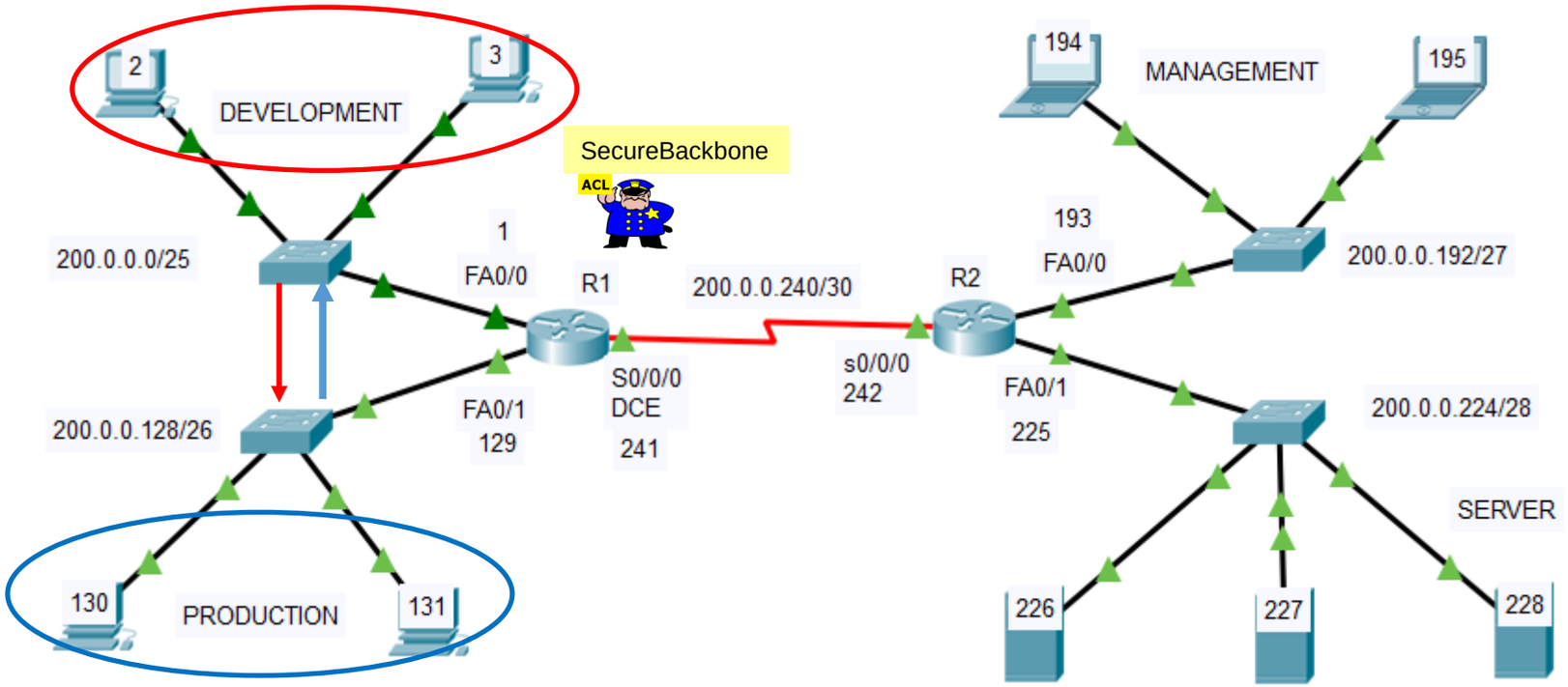
1. Development och Production blockeras till externa nätverk, men nej till varandra.
2. Host 200.0.0.2 från Development har ingen åtkomst till andra nät förutom sitt nät
3. Endast 200.0.0.130 från Production har åtkomst till Management, inte till Server.
4. Endast 200.0.0.131 från Production har åtkomst till Server, inte till Management.
5. Endast 200.0.0.194 från Management har åtkomst till Server, inte till Development och Production.



Avancerad Standard ACL konfigurationer

1. Development och Production blockeras till externa nät.

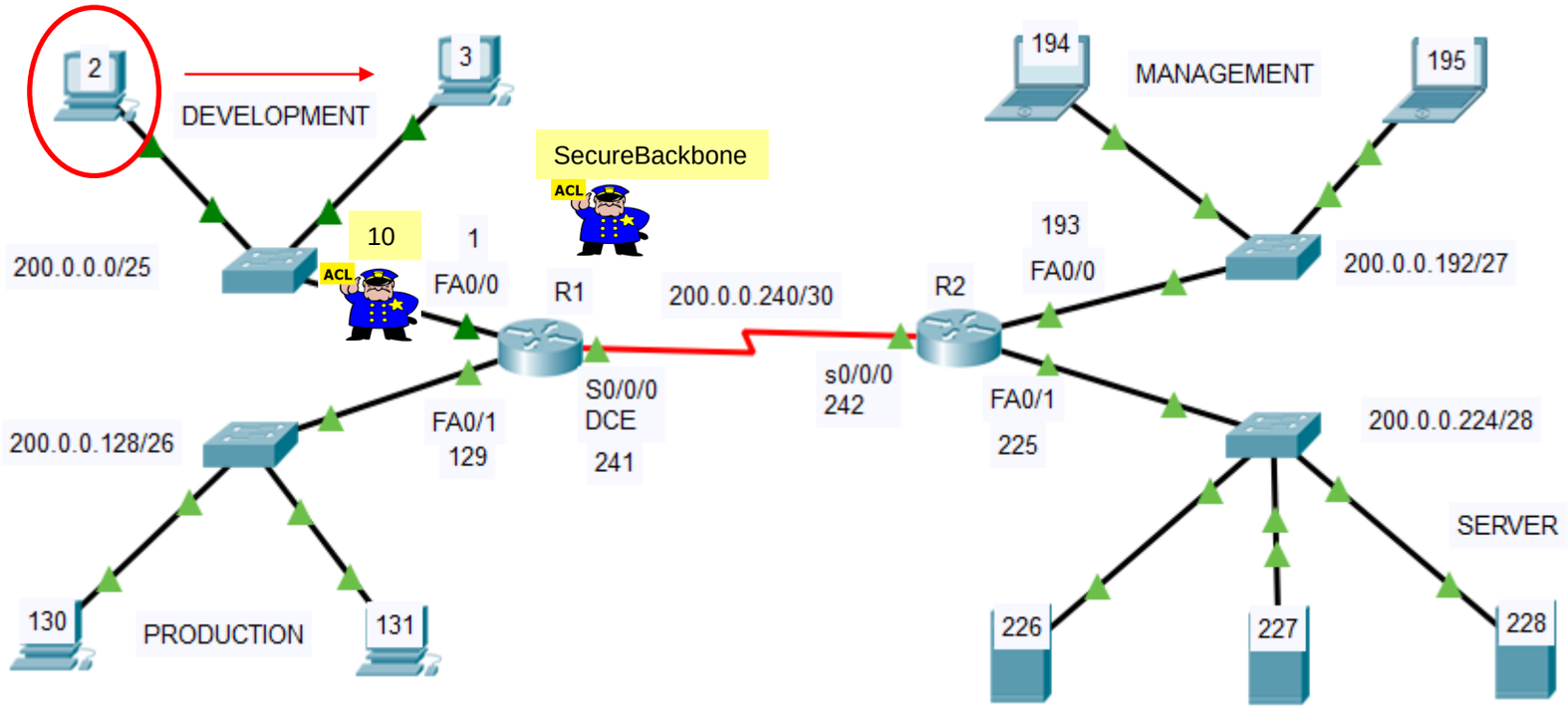
- R1(config)# ip access-list standard SecureBackbone
- R1(config-std-nacl)# deny 200.0.0.0 0.0.0.127
- R1(config-std-nacl)# deny 200.0.0.128 0.0.0.63
- R1(config-std-nacl)# exit
- R1(config)# interface s0/0/0
- R1(config-if)# ip access-group SecureBackbone out
- R1(config-if)# end



Avancerad Standard ACL konfigurationer

2. Host 200.0.0.2 från Development har ingen åtkomst till andra nät förutom sitt eget nät

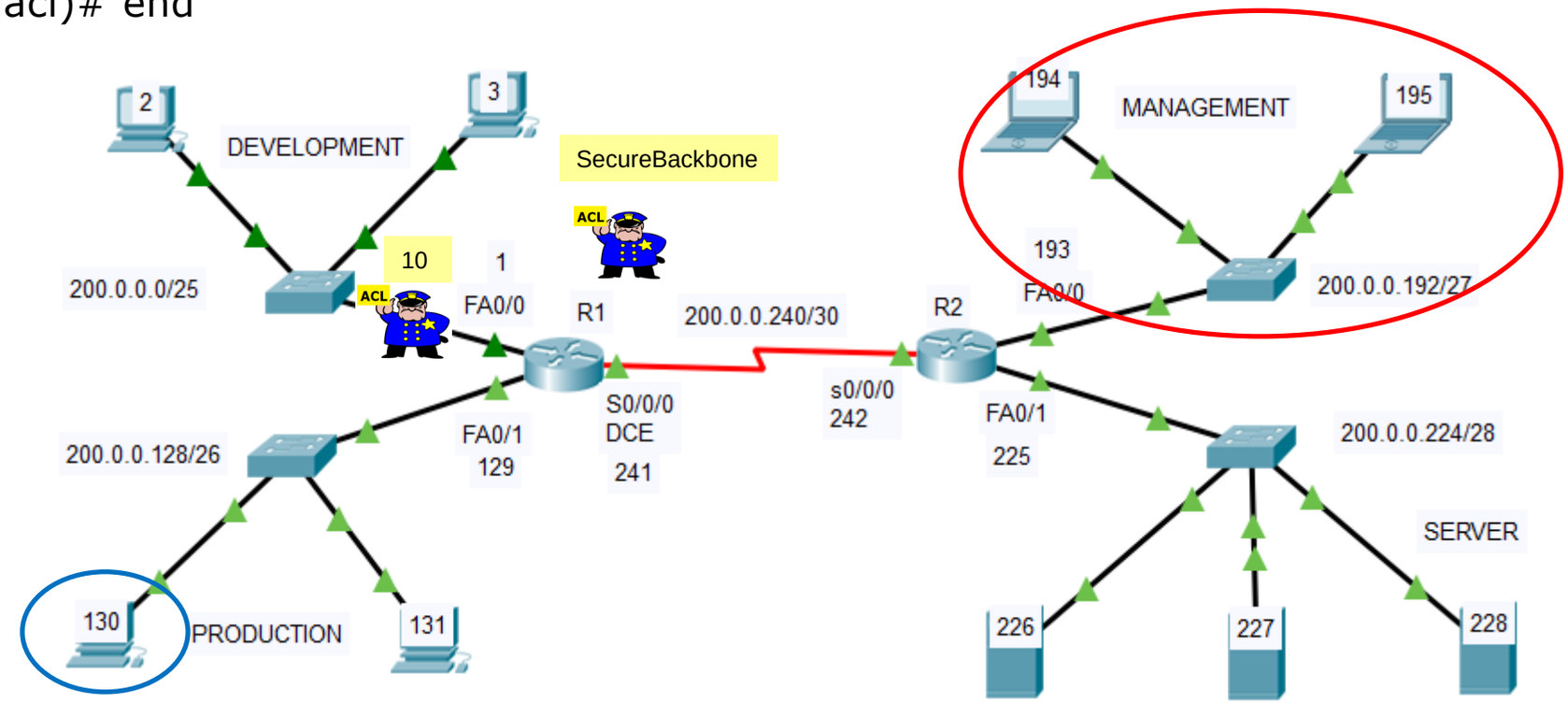
- R1(config)# access-list 10 deny host 200.0.0.2
- R1(config)# access-list 10 permit any
- R1(config)# interface fa0/0
- R1(config-if)# ip access-group 10 in
- R1(config-if)# end
- R1# show access-lists



Avancerad Standard ACL konfigurationer

3. Endast 200.0.0.130 från Production ska ha åtkomst till Management, inte till Server.

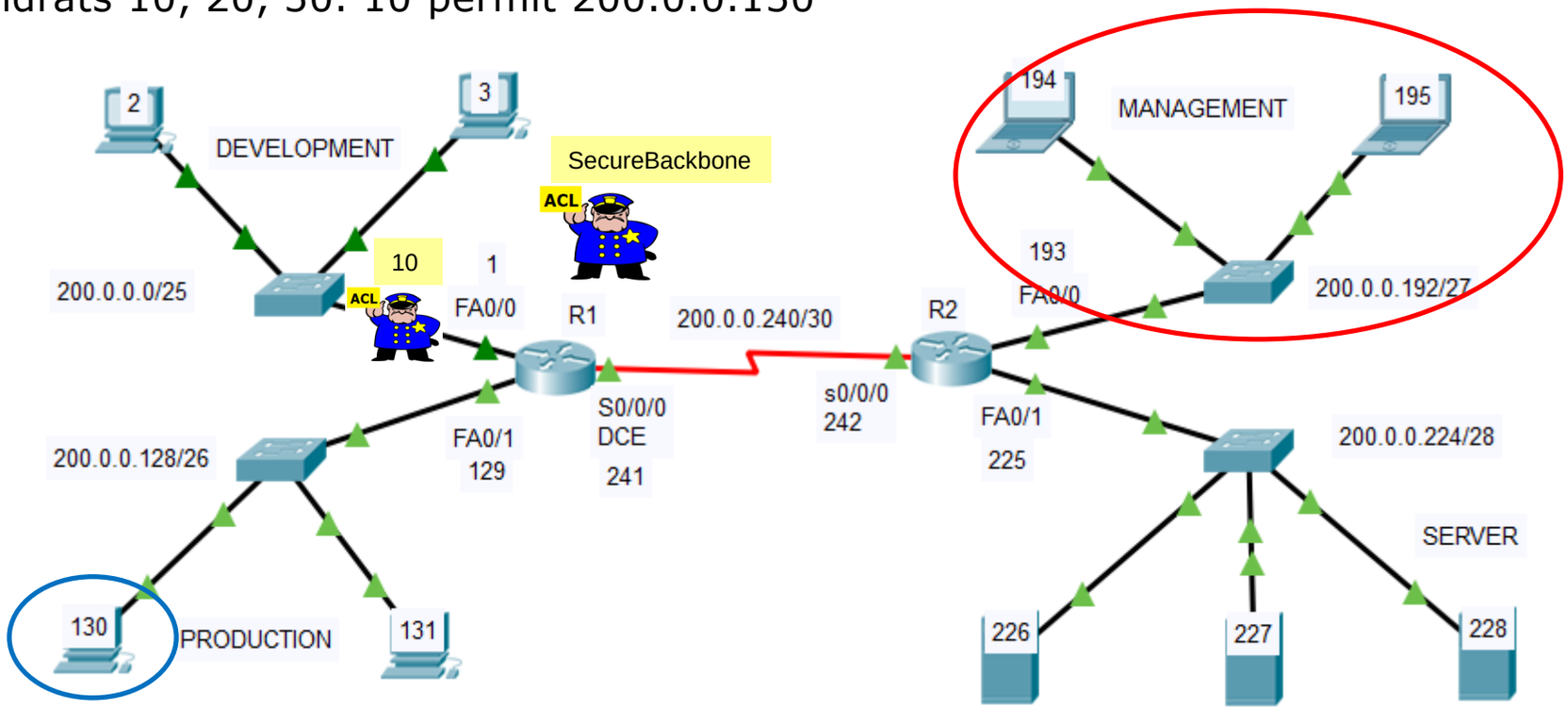
- Först redigerar vi ACL SecureBackbone eftersom Production blockeras där.
- R1# show access-list SecureBackbone
  - 10 deny 200.0.0.0 0.0.0.127
  - 20 deny 200.0.0.128 0.0.0.63
- R1(config)# ip access-list standard SecureBackbone
- R1(config-std-nacl)# 11 permit host 200.0.0.130
- R1(config-std-nacl)# end



Avancerad Standard ACL konfigurationer

3. Endast 200.0.0.130 från Production har åtkomst till Management, inte till Server.

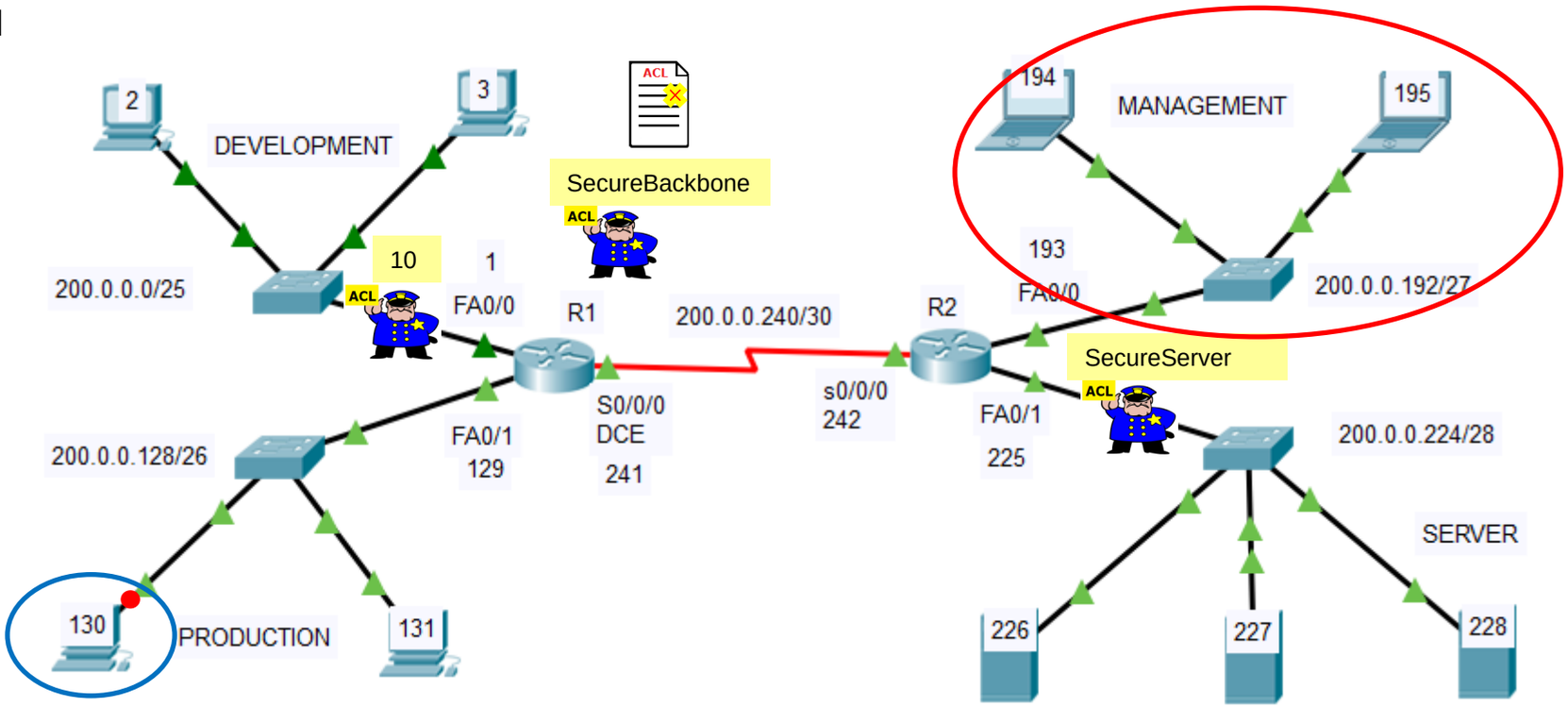
- R1# show access-list secureBackbone
  - 11 permit host 200.0.0.130
  - 10 deny 200.0.0.0 0.0.0.127
  - 20 deny 200.0.0.128 0.0.0.63
- Vad har det hänt? konstig beteende, kör copy run start och därefter kör reload.
- R1# show access-list secureBackbone
- Nu har allting ändrats 10, 20, 30. 10 permit 200.0.0.130



Avancerad Standard ACL konfigurationer

3. Endast 200.0.0.130 från Production har åtkomst till Management, inte till Server.

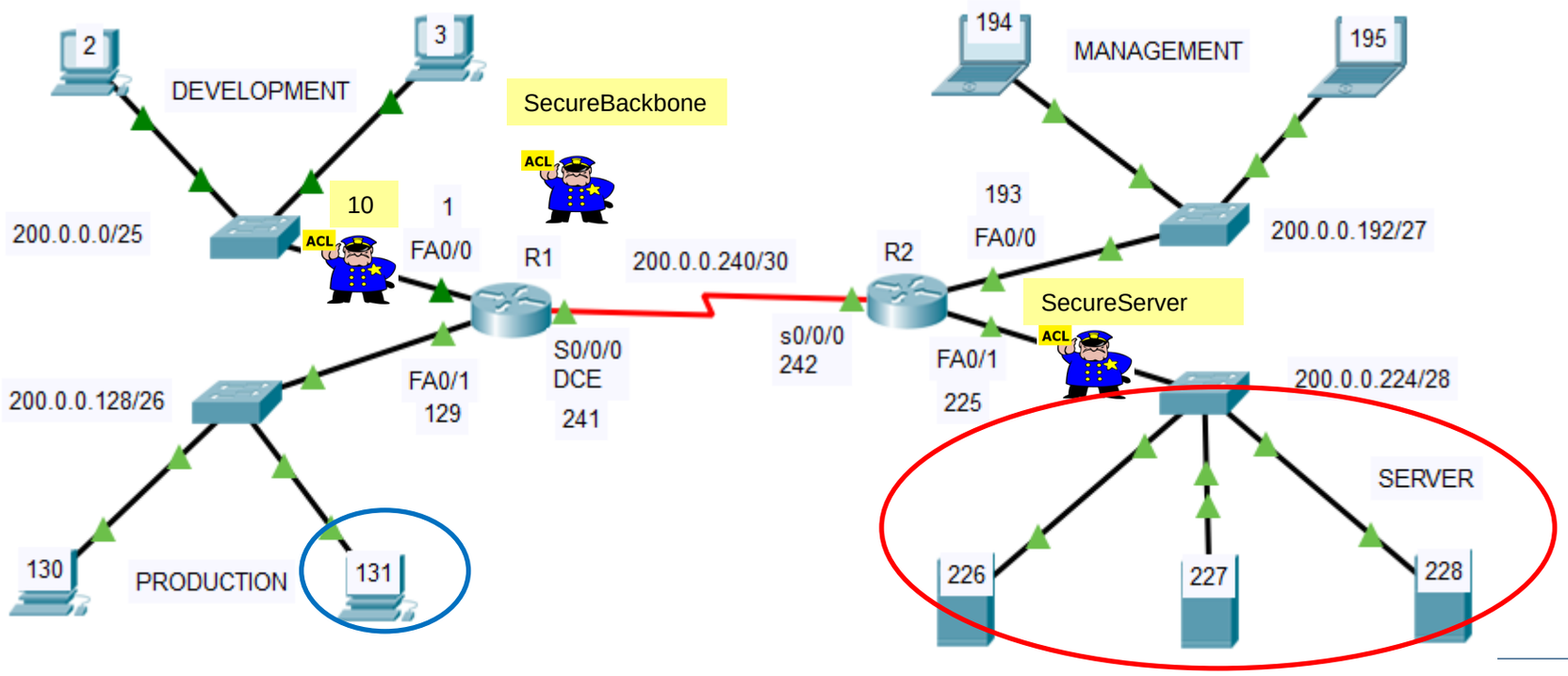
- Nu kan host 130 ta sig ur till Management men också till Server så vi måste blockera åtkomst till Server:
- R2(config)# ip access-list standard SecureServer
- R2(config-std-nacl)# deny host 200.0.0.130
- R2(config-std-nacl)# permit any
- R2(config-std-nacl)# exit
- R2(config)# interface fa0/1
- R2(config-if)# ip access-group SecureServer out
- R2(config-if)# end



Avancerad Standard ACL konfigurationer

4. Endast 200.0.0.131 från Production har åtkomst till Server, inte till Management.

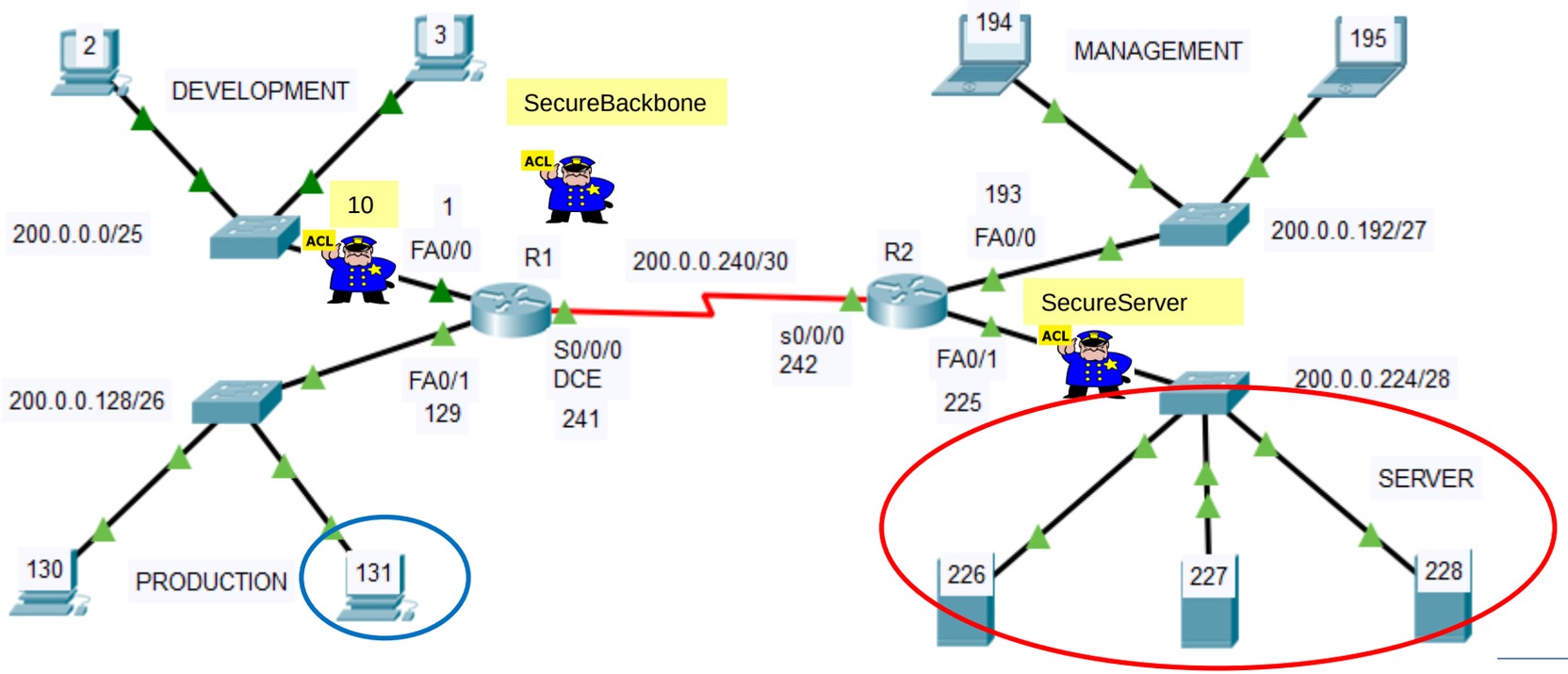
- Återigen behöver vi redigera ACL SecureBackbone eftersom Production blockeras.
- R1# show access-list SecureBackbone
  - 10 deny 200.0.0.0 0.0.0.127
  - 20 permit host 200.0.0.130
  - 30 deny 200.0.0.128 0.0.0.63
- Fel ordning?
- Inte riktigt eftersom det fungerade i villkor 3.



Avancerad Standard ACL konfigurationer

4. Endast 200.0.0.131 från Production har åtkomst till Server, inte till Management.

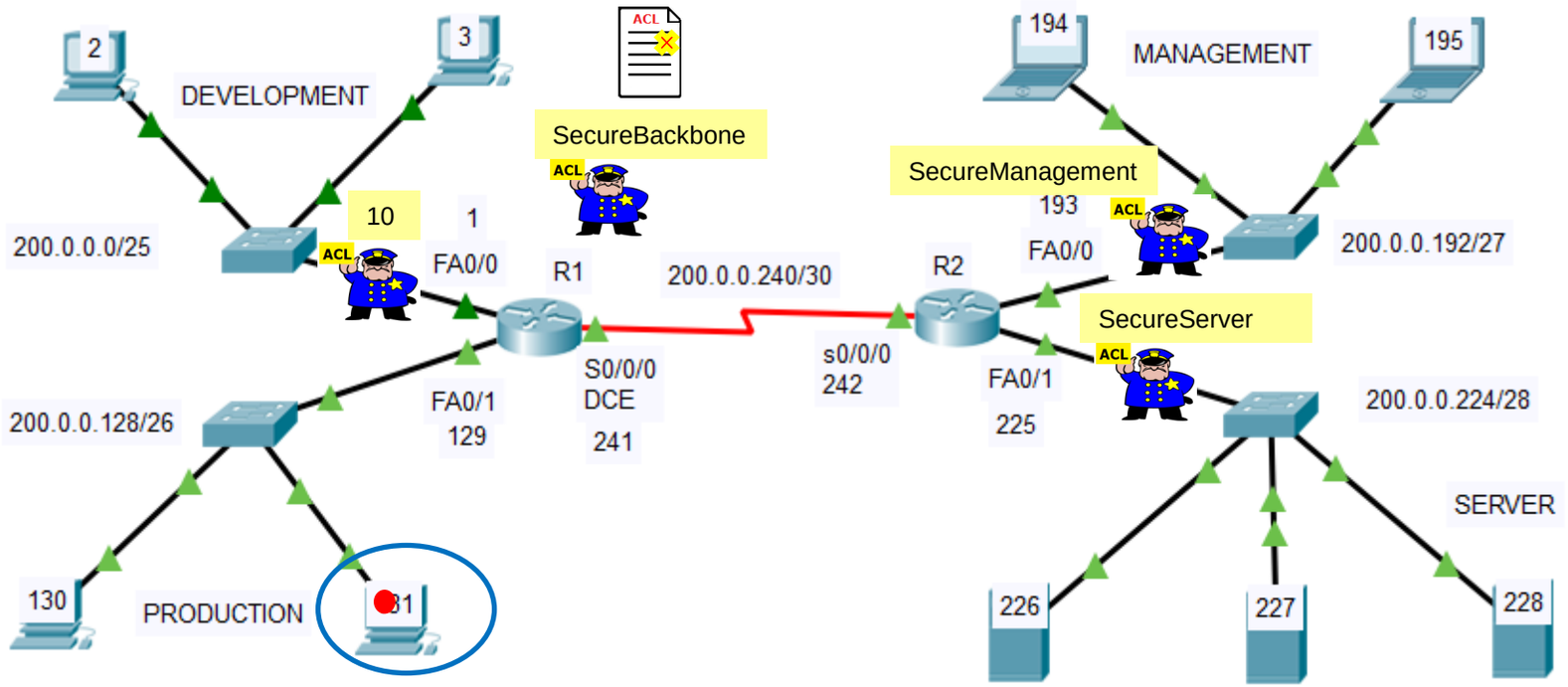
- R1(config)# ip access-list standard SecureBackbone
- R1(config-std-nacl)# 12 permit host 200.0.0.131
- R1(config-std-nacl)# end
- R1# show access-list SecureBackbone
  - 10 permit host 200.0.0.130
  - 12 permit host 200.0.0.131
  - 10 deny 200.0.0.0 0.0.0.127
  - 20 deny 200.0.0.128 0.0.0.63



Avancerad Standard ACL konfigurationer

4. Endast 200.0.0.131 från Production har åtkomst till Server, inte till Management.

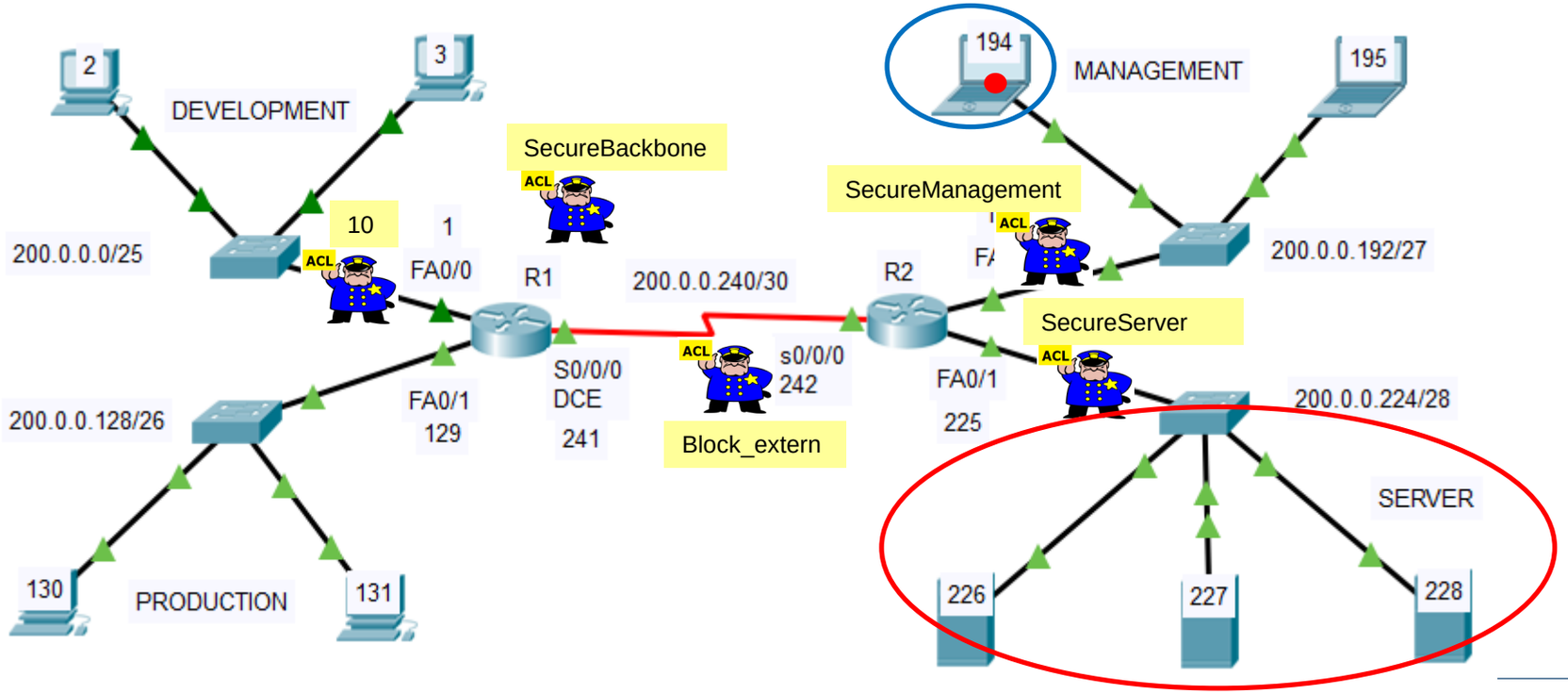
- Nu kan host 131 komma åt till Server men också till Management så vi måste blockera det.
- R2(config)# ip access-list standard SecureManagement
- R2(config-std-nacl)# deny host 200.0.0.131
- R2(config-std-nacl)# permit any
- R2(config-std-nacl)# exit
- R2(config)# interface fa0/0
- R2(config-if)# ip access-group SecureManagement out
- R2(config-if)# end



Avancerad Standard ACL konfigurationer

5. Endast 200.0.0.194 från Management har åtkomst till Server, inte till Development och Production.

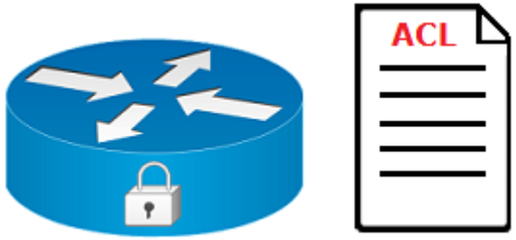
- R2(config)# ip access-list standard Block_extern
- R2(config-dst-nacl)# deny host 200.0.0.194
- R2(config-dst-nacl)# permit any
- R2(config-dst-nacl)# exit
- R2(config)# interface s0/0/0
- R2(config-if)# ip access-group Block_extern out
- R2(config-if)# end



Numerisk och namngiven Extended ACL

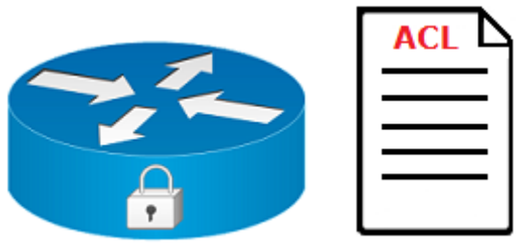
Extended ACL

- *Vad är en Extended ACL?*
- En ordnad lista över villkor som måste uppfyllas för tillåta paket 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.



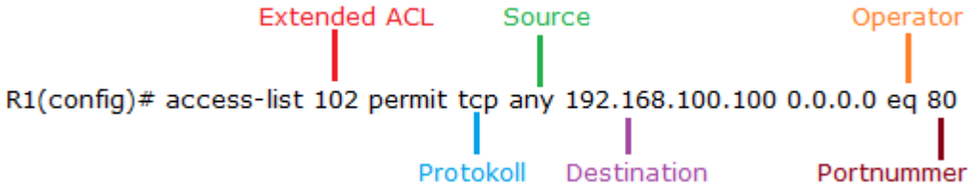
Extended ACL

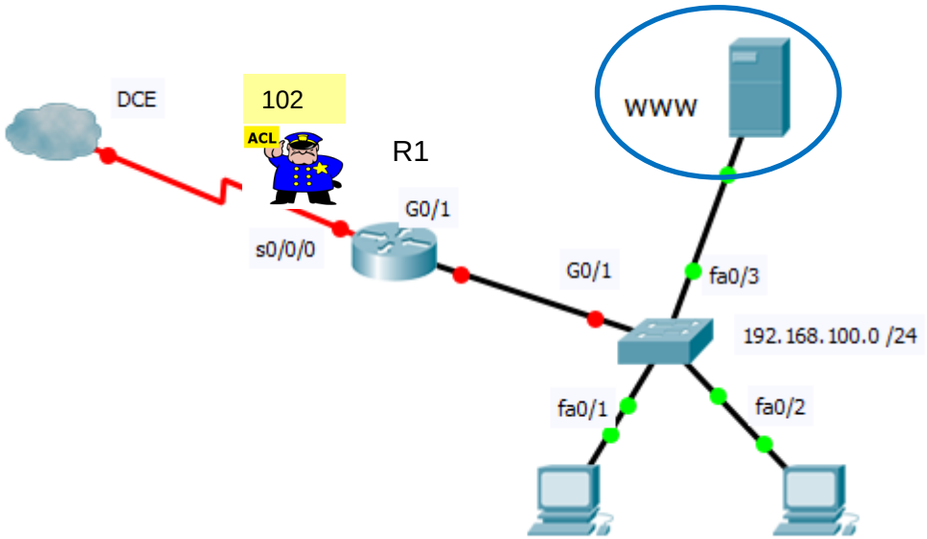
- *Syntax*
- access-list <nummer 100-199> <permit | deny> <protokoll> <source IP> <wildcard mask> <operator> <source port> <destination IP> <wildcard mask> <operator> <destination port> <options> <log>
- R1(config)# access-list 102 permit tcp any 192.168.100.100 0.0.0.0 eq 80
- Förklaringar:
  - *access-list* 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

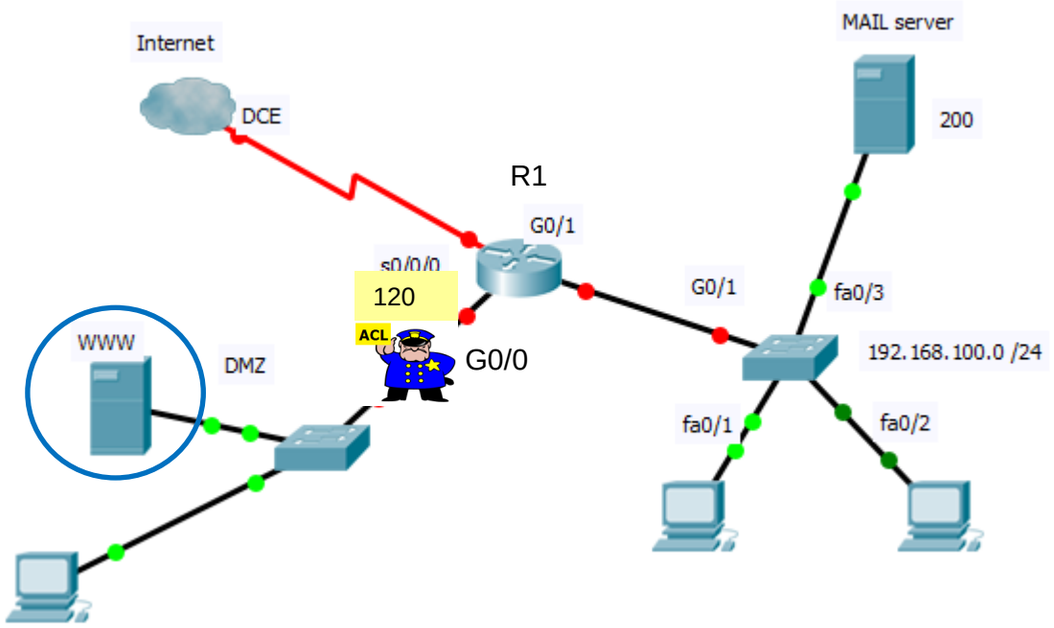
- *Var ska du applicera dina ACL?*
- Scenario 1
- I denna scenario är ditt mål att filtrera inkommande trafik så att användare utanför ditt nätverk kan komma åt webbservern (192.168.100.100) via port 80.
- All annan inkommande nätverkstrafik ska nekas.
- R1(config)# access-list 102 permit tcp any 192.168.100.100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





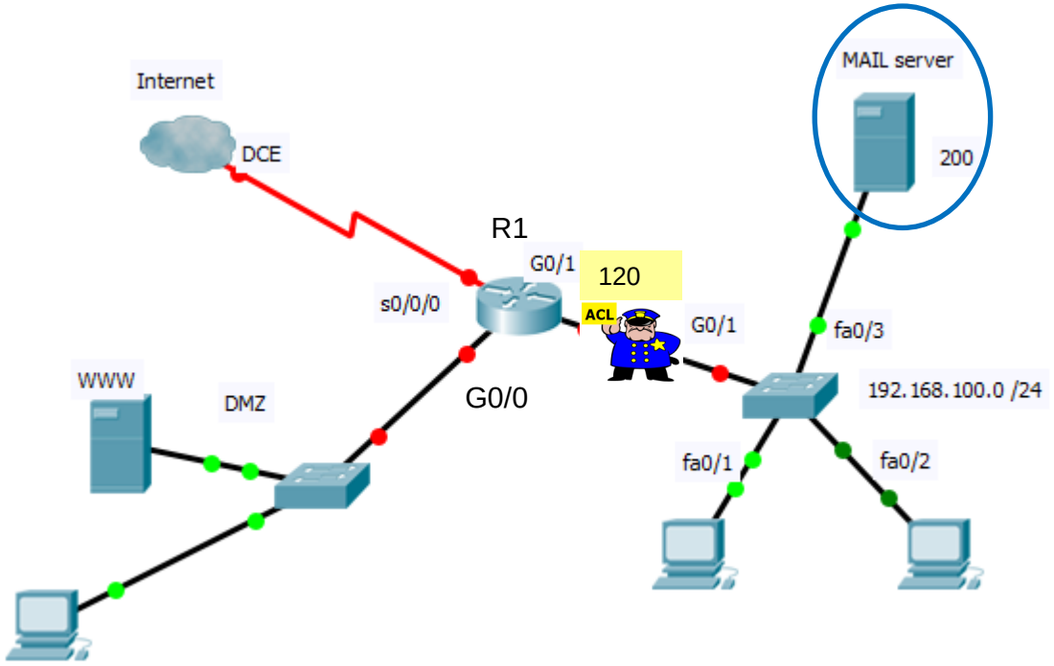
Extended ACL

- *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



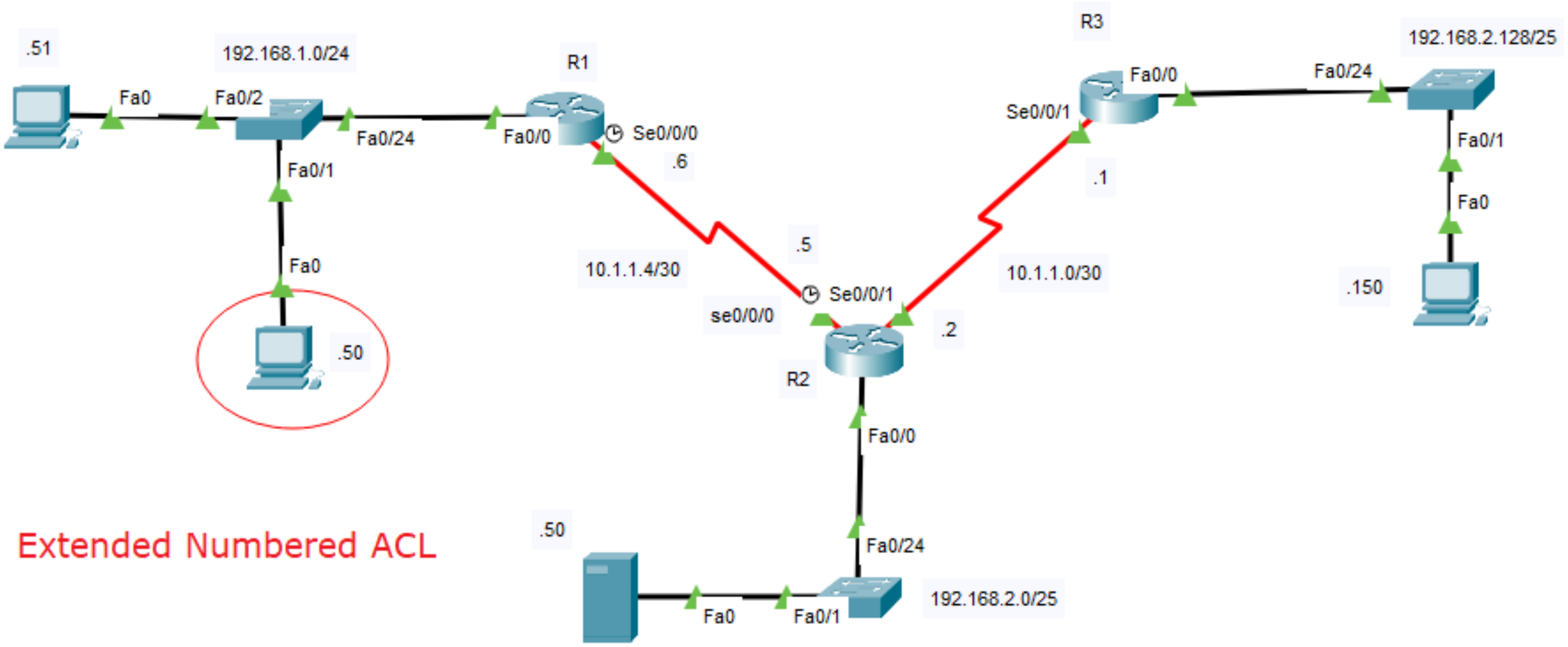
Extended ACL

- *Var ska du applicera dina ACL?*
- Scenario 2 – 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 102 out



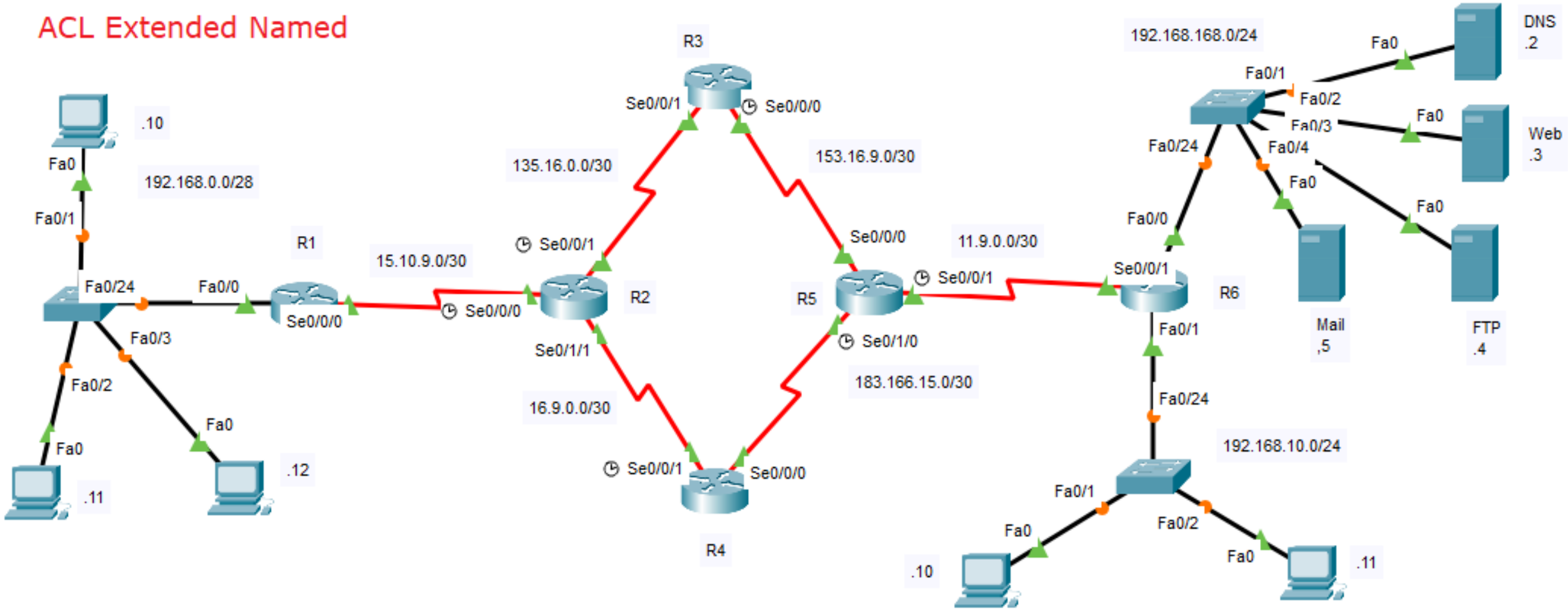
Avancerad Extended ACL – Exempel 1

1. Host 192.168.1.50 nekas åtkomst till 192.168.2.50 med protokoll HTTP och HTTPS.
2. Alla andra tillåts



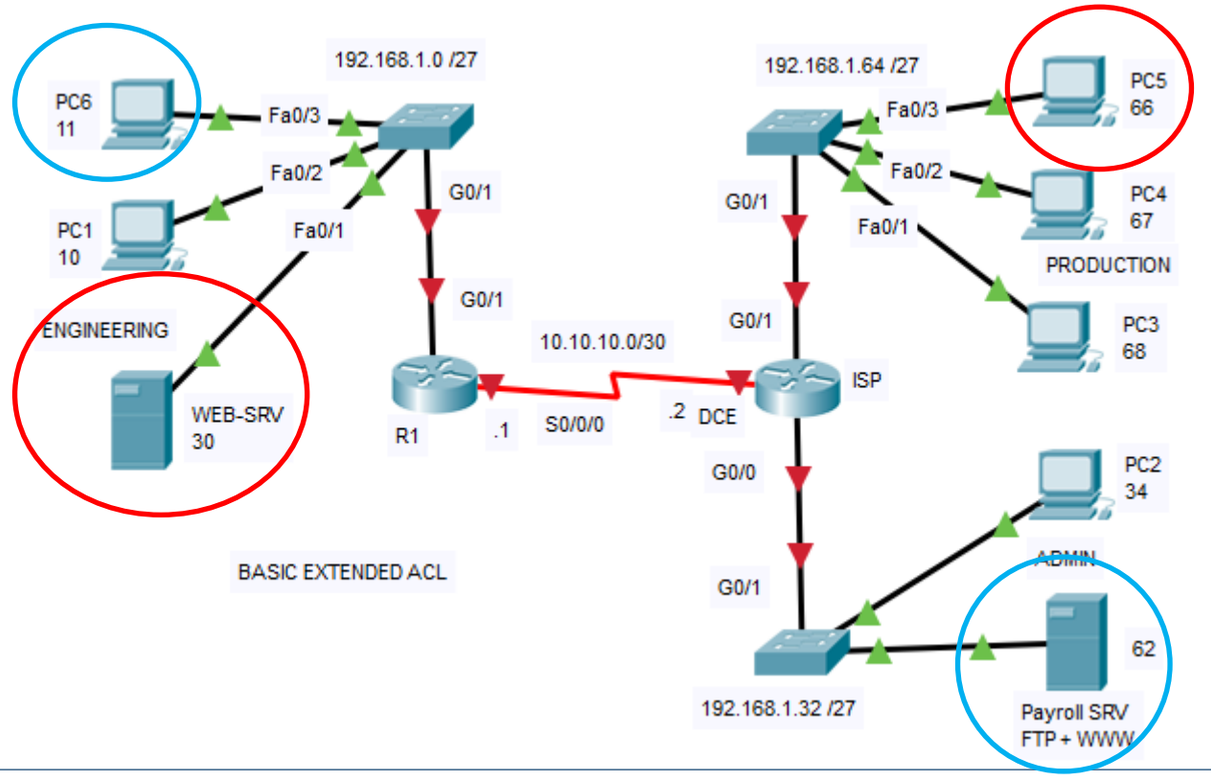
Avancerad Extended ACL – Exempel 2

1. Neka host 192.168.0.10 åtkomst till host 192.168.168.3 via ping
2. Neka host 192.168.0.11 åtkomst till host 192.168.168.3 via http
3. Neka nätet 192.168.10.0 åtkomst till FTP server



Avancerad Extended ACL – Exempel 3

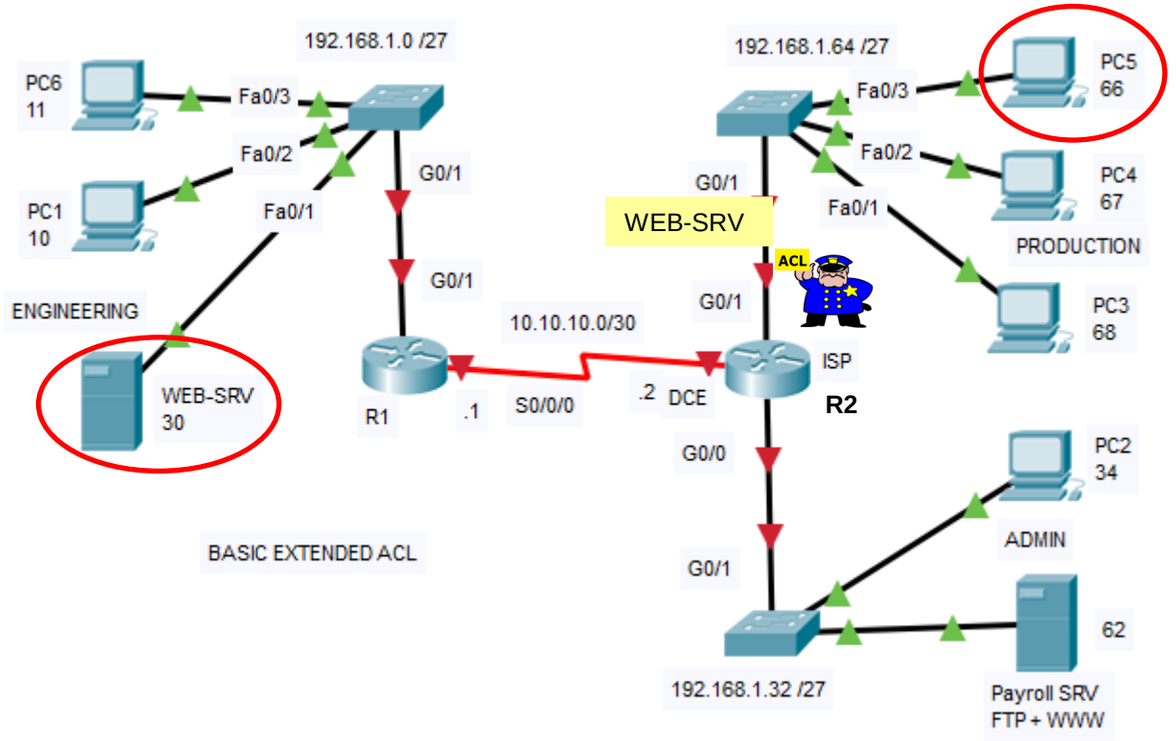
1. Endast host PC5 från "Production" nätverk får komma åt server WEB-SRV på Engineering nätverk.
2. Alla andra host i "Production" nätverk blockeras åtkomst till samma server.
3. Endast host PC6 från "Engineering" nätverk får komma åt servern Payroll-SRV på "Admin" nätverk. Åtkomsten är endast via www och ftp,
4. alla andra host från samma nät nekas åtkomst till servern.
5. Resterande trafik tillåts.



Avancerad Extended ACL – Exempel 3

1. Endast host PC5 från "Production" nätverk får komma åt server WEB-SRV på Engineering nätverk. Alla andra host i "Production" nätverk blockeras åtkomst till samma server.

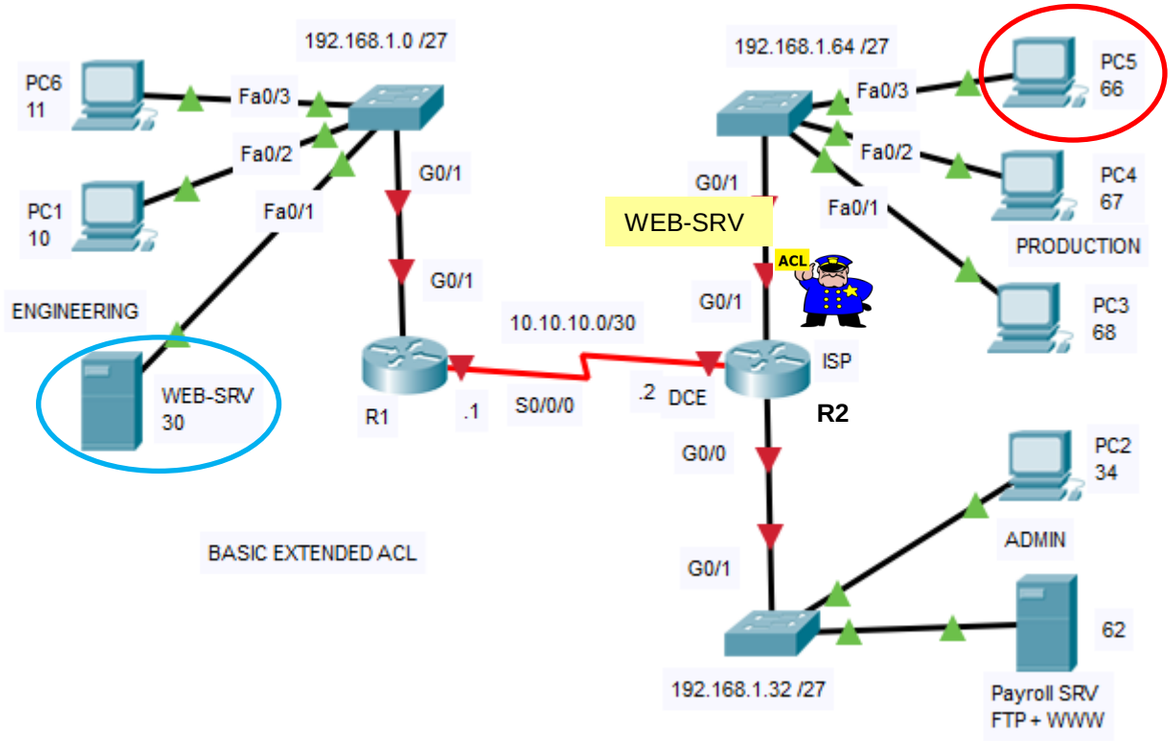
- R2(config)# ip access-list extended WEB-SRV
- R2(config-ext-nacl)# remark Allow Only PC5 from Production to WEB-SRV
- R2(config-ext-nacl)# 10 permit tcp host 192.168.1.66 host 192.168.1.30 eq www
- R2(config-ext-nacl)# 20 deny ip 192.168.1.64 0.0.0.31 host 192.168.1.30
- R2(config-ext-nacl)# 30 permit ip any any
- R2(config-ext-nacl)#exit



Avancerad Extended ACL – Exempel 3

1. Endast host PC5 från "Production" nätverk får komma åt server WEB-SRV på Engineering nätverk. Alla andra host i "Production" nätverk blockeras åtkomst till samma server.

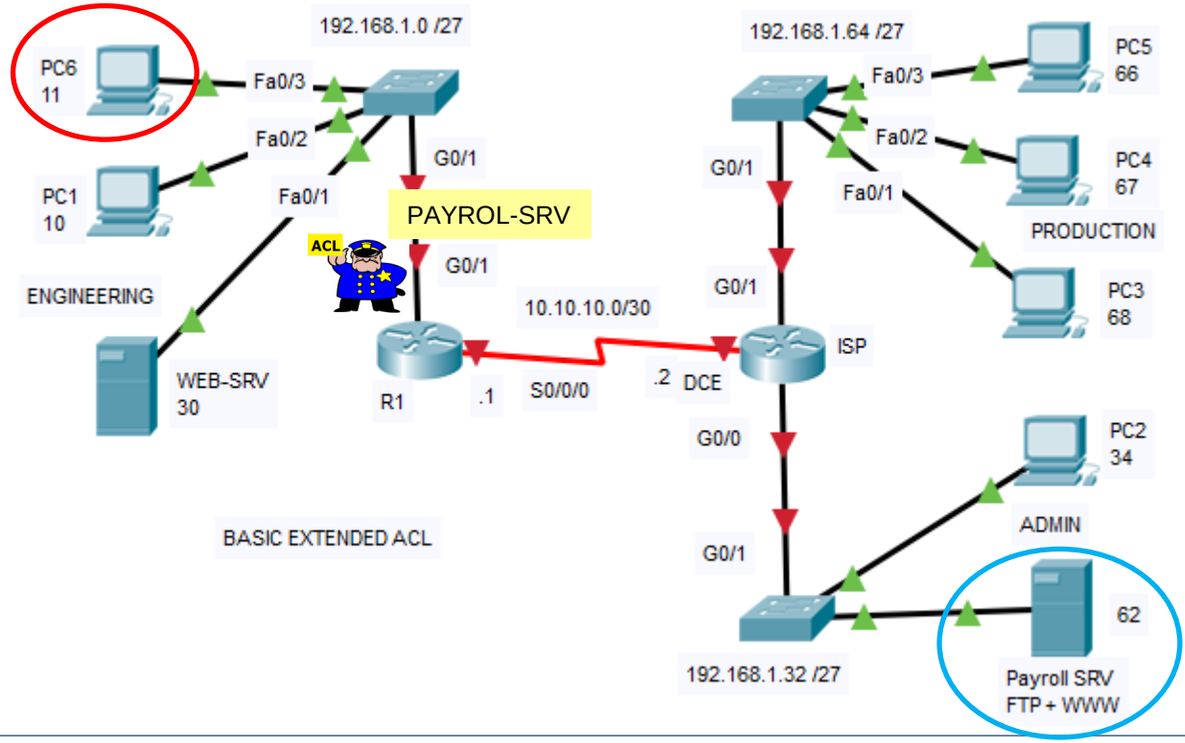
- *ACL applicering*
- R2(config)#inter g0/1
- R2(config-if)#ip access-group WEB-SRV in
- *Verifiering*
- R2#sh access-lists
- Från PC5 starta en webbläsare och ange WEB-SRV IP-adress: 192.168.1.30
- Testa från PC4 och PC3 samma åtkomst



Avancerad Extended ACL – Exempel 3

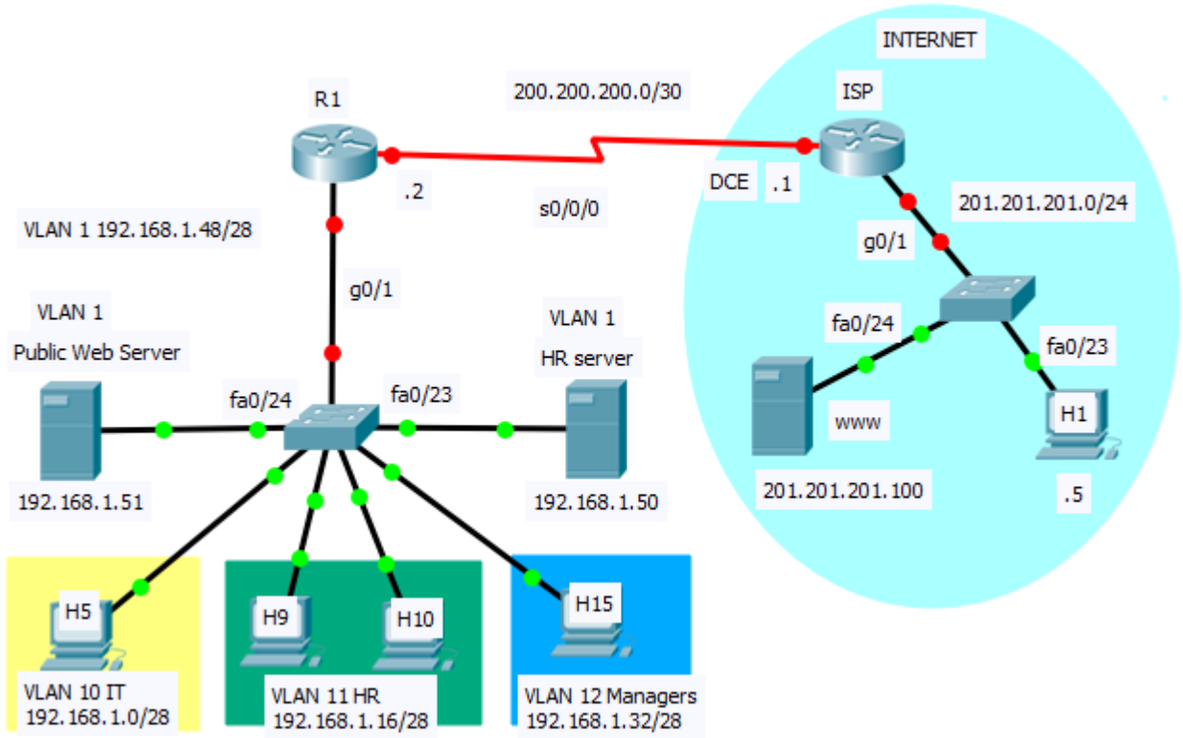
2. Endast host PC6 från "Engineering" får komma åt servern Payroll-SRV på "Admin". Åtkomsten är endast via www och ftp, alla andra host från samma nät nekas åtkomst till servern. Resterande trafik tillåts.

- R1(config)# ip access-list extended PAYROL-SRV
- R1(config-ext-nacl)# remark Allow Only PC6 to access Payrol Server
- R1(config-ext-nacl)# 10 permit tcp host 192.168.1.11 host 192.168.1.62 eq www
- R1(config-ext-nacl)# 20 permit tcp host 192.168.1.11 host 192.168.1.62 eq ftp
- R1(config-ext-nacl)# 30 deny ip 192.168.1.0 0.0.0.31 host 192.168.1.62
- R1(config-ext-nacl)# 40 permit ip any any
- *ACL applicering*
- R2(config)#inter g0/1
- R2(config-if)#ip access-group WEB-SRV in



Avancerad Extended ACL – Exempel 4

- Krav 1: Endast host i VLAN 10 får kontakta router R1 och switch sw1 via TELNET
- Krav 2: Endast VLAN 12 Managers och servers i VLAN 1 får åtkomst till Internet
- Krav 3: Den publika webb-server tillämpar port forwarding via port 80 endast
- Krav 4: Endast host i VLAN 11 HR får kontakta HR-server med IP-adress 192.168.1.50
- Alla konfigurationer finns på DIGINTO




DIGINTO
Nätverkssäkerhet