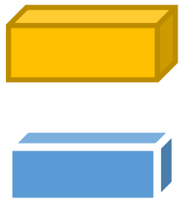

DIGINTO
Nätverkssäkerhet

Access Control List – ACL

STANDARD

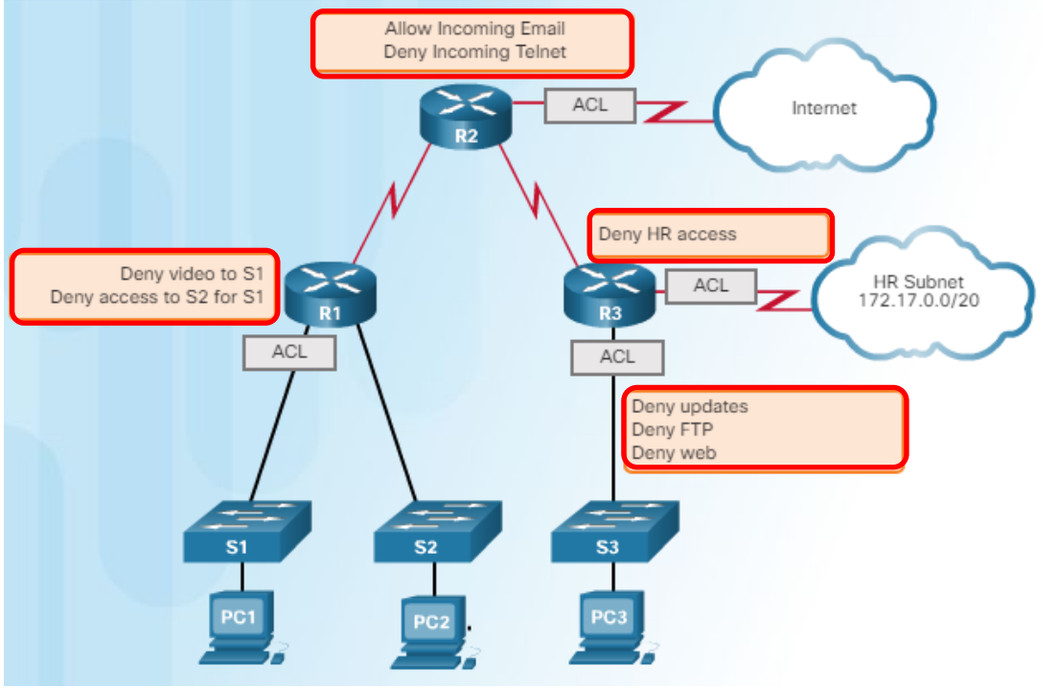
Vad är en Access Control List?

- 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



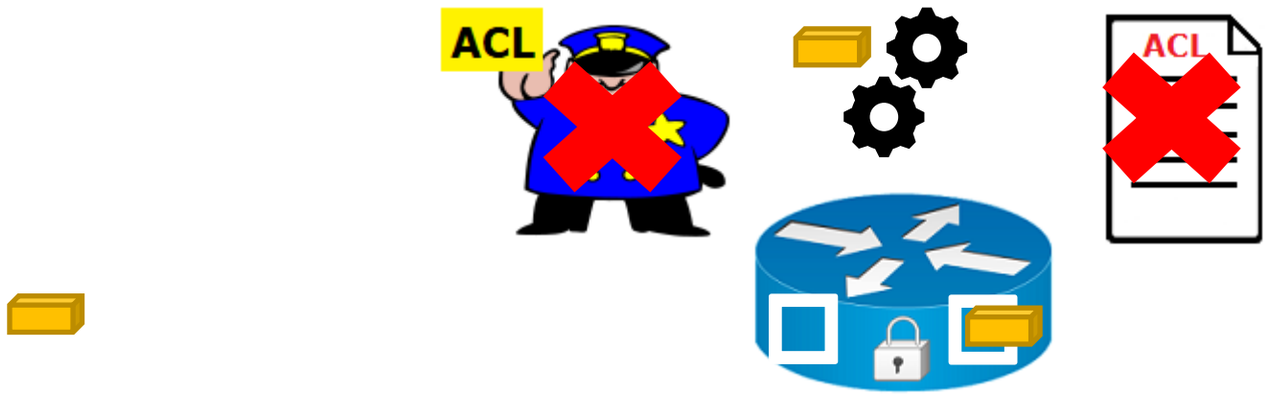
Vad kan man åstadkomma med ACL?

- 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 ---------- 192.168.1.1
- 192.168.1.1 –- 255.255.255.255 ---------- 0.0.0.0
- 192.168.1.1 –- 0.0.0.255 ---------- 192.168.1.0
- 192.168.16.0 – 0.0.15.255 ---------- 192.168.16.0 till 192.168.31.255
- 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

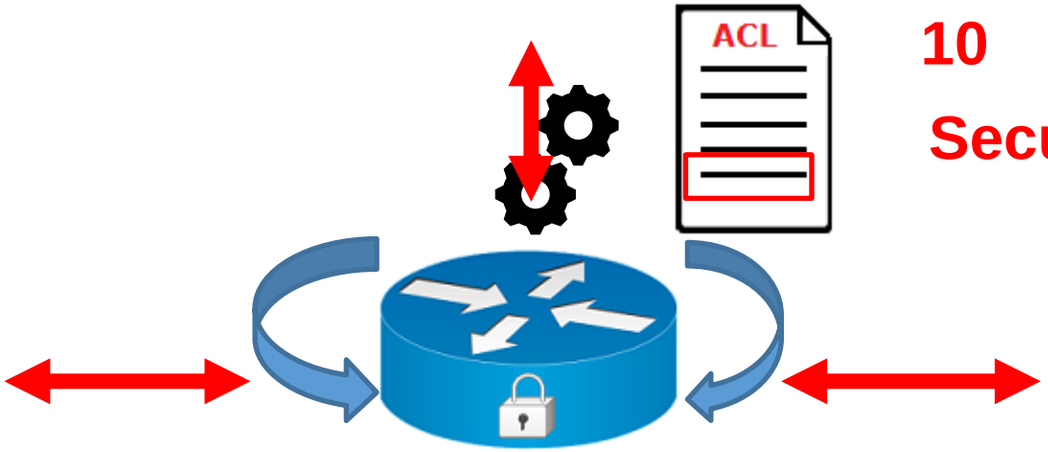
Vad ska man tänka på när man konfigurerar ACL?

- 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?

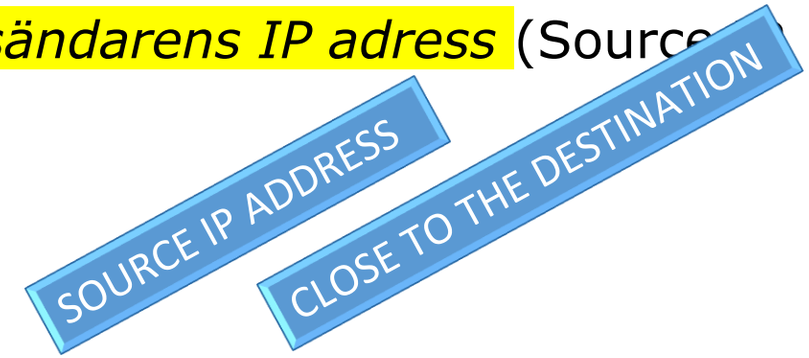
- Några ordnycklar som host och any
- *Host* ersätter 0.0.0.0 och *Any* ersätter 255.255.255.255
- host 192.168.10.10 istället 192.168.10.10 0.0.0.0
- Any istället 0.0.0.0 255.255.255.255
- Sist i ACL-lista finns en blockering till allt nätverkstrafik.
- Det kallas *implicit deny any*
- ACL kan bara 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.



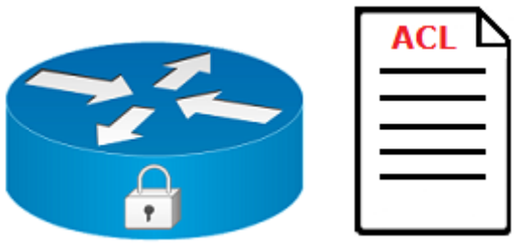
Typer av ACL

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

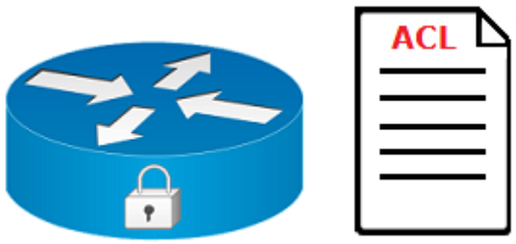


Standard eller Extended ACL?
Har jag kontroll över nätet?
Hur påverkas nätverkstrafiken?



Typer av ACL

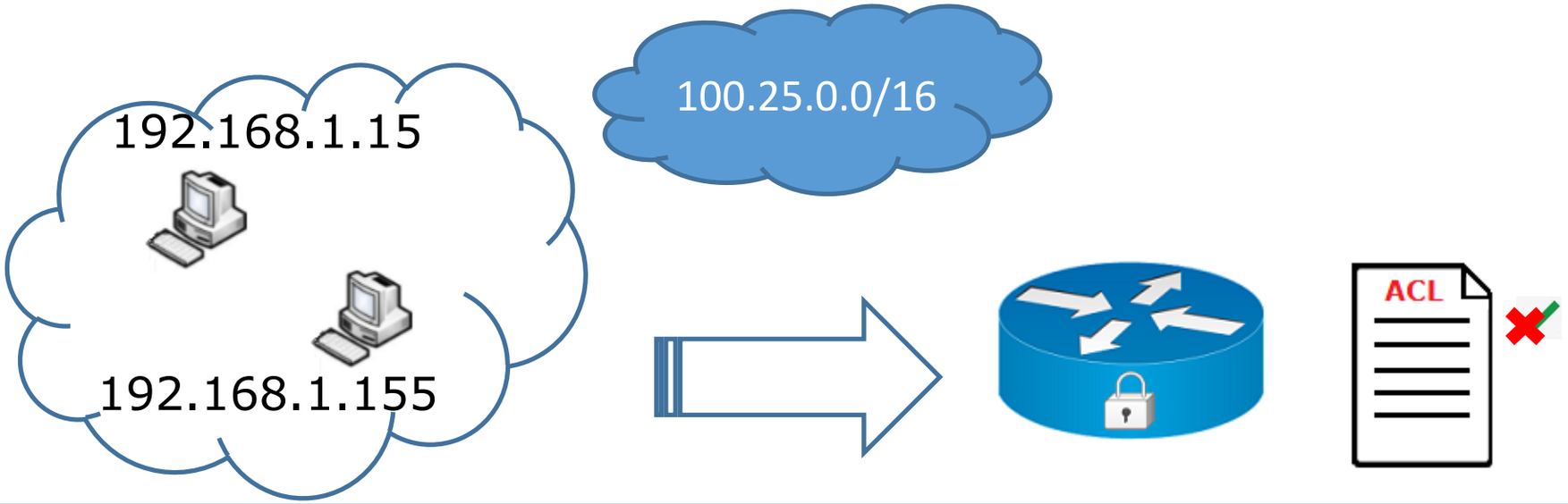
- Standard ACL identifieras normalt med ett nummer från intervallet 1 till 99 eller 1300 – 1999
- Router(config)# access-list 10
- Standard ACL kan också identifieras med ett namn
- Router(config)# ip access-list standard Block_Telnet
- Extended ACL identifieras med ett nummer från intervallet 100 till 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

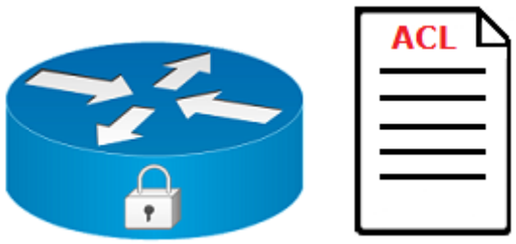
Standard ACL - syntax

- 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

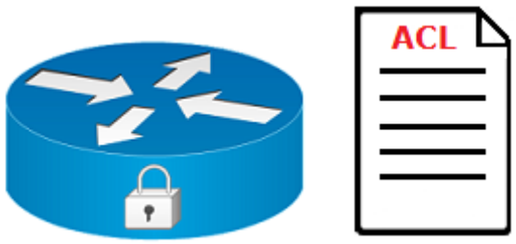
- Standard ACL identifieras med ett nummer men också med ett namn.
- Konfigurationen skiljer sig en aning
- Router(config-if)# ip access-list ACL_ namn in | out
- Exempel:
- Router(config)# ip access-list Standard Secure_Telnet
- Router(config-std-nacl)# permit 20.0.0.10 0.0.0.0
- Router(config-std-nacl)#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



Standard ACL - syntax

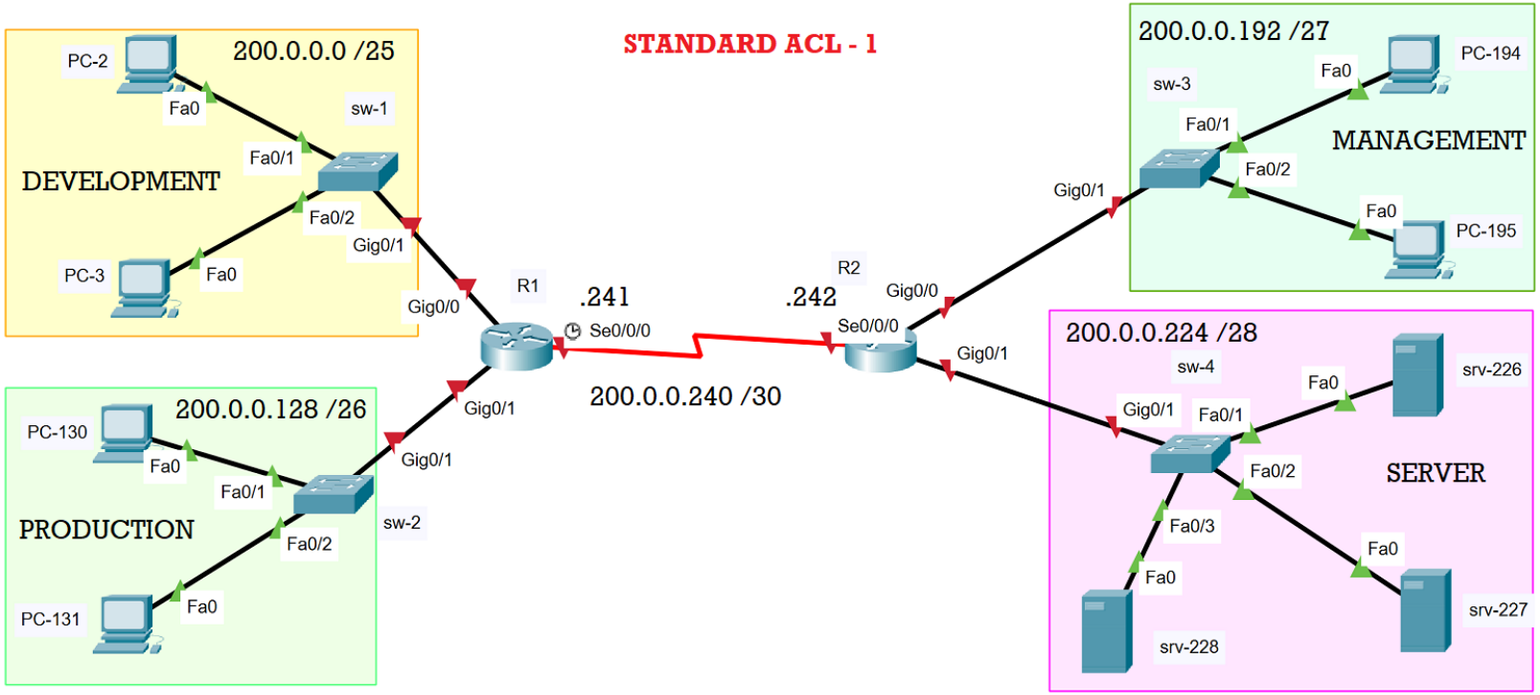
1. Permit 20.0.0.10
2. Deny any (alla andra)

- Router(config)# access-list 10 permit 20.0.0.10 0.0.0.0
- Router(config)# access-list 10 deny any
- 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



Standard ACL - 1

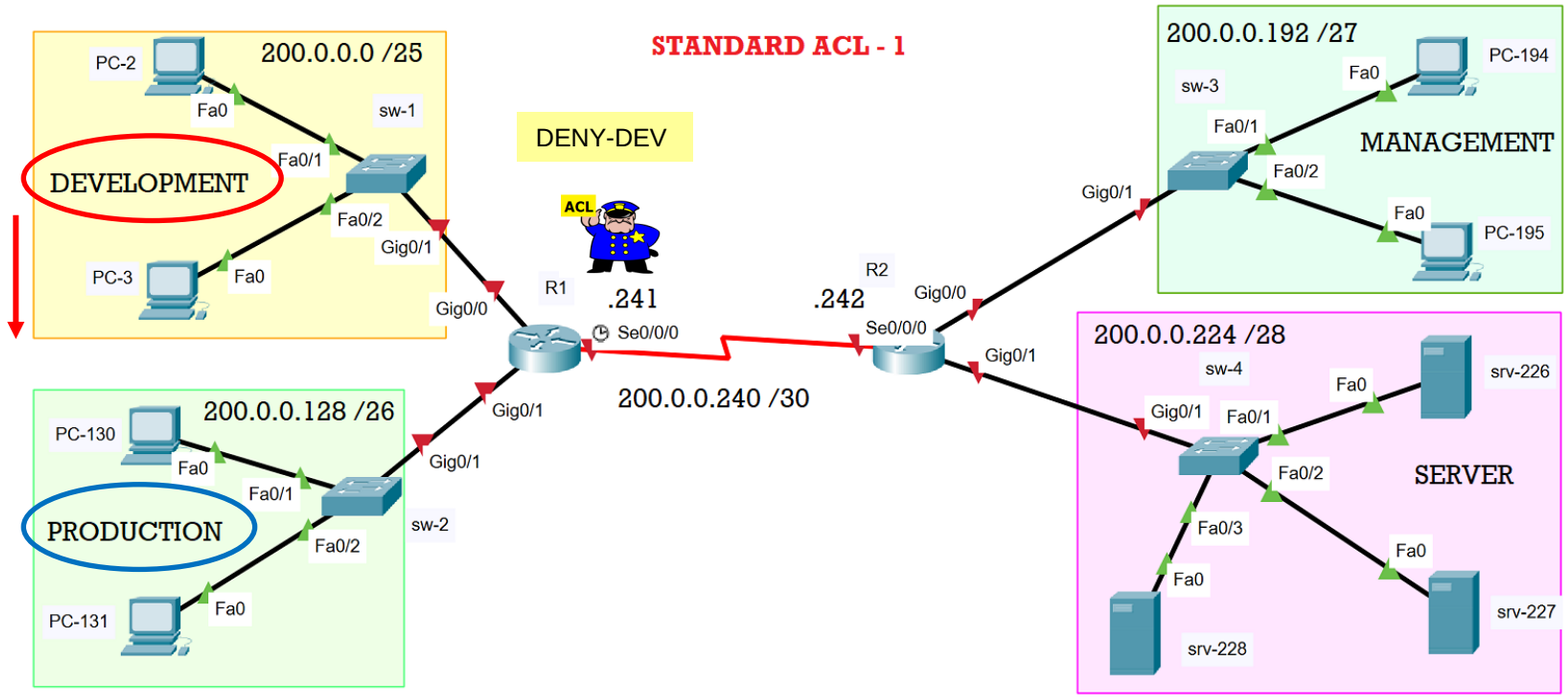
1. Development och Production blockeras till externa nätverk, men nej till varandra.
2. Host 200.0.0.2 från Development har ingen åtkomst till andra nät förutom sitt nät
3. Endast 200.0.0.130 från Production har åtkomst till Management, inte till Server.
4. Endast 200.0.0.131 från Production har åtkomst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



Standard ACL - 1

Development ska ha åtkomst endast till Production, inte till Management och inte heller till server

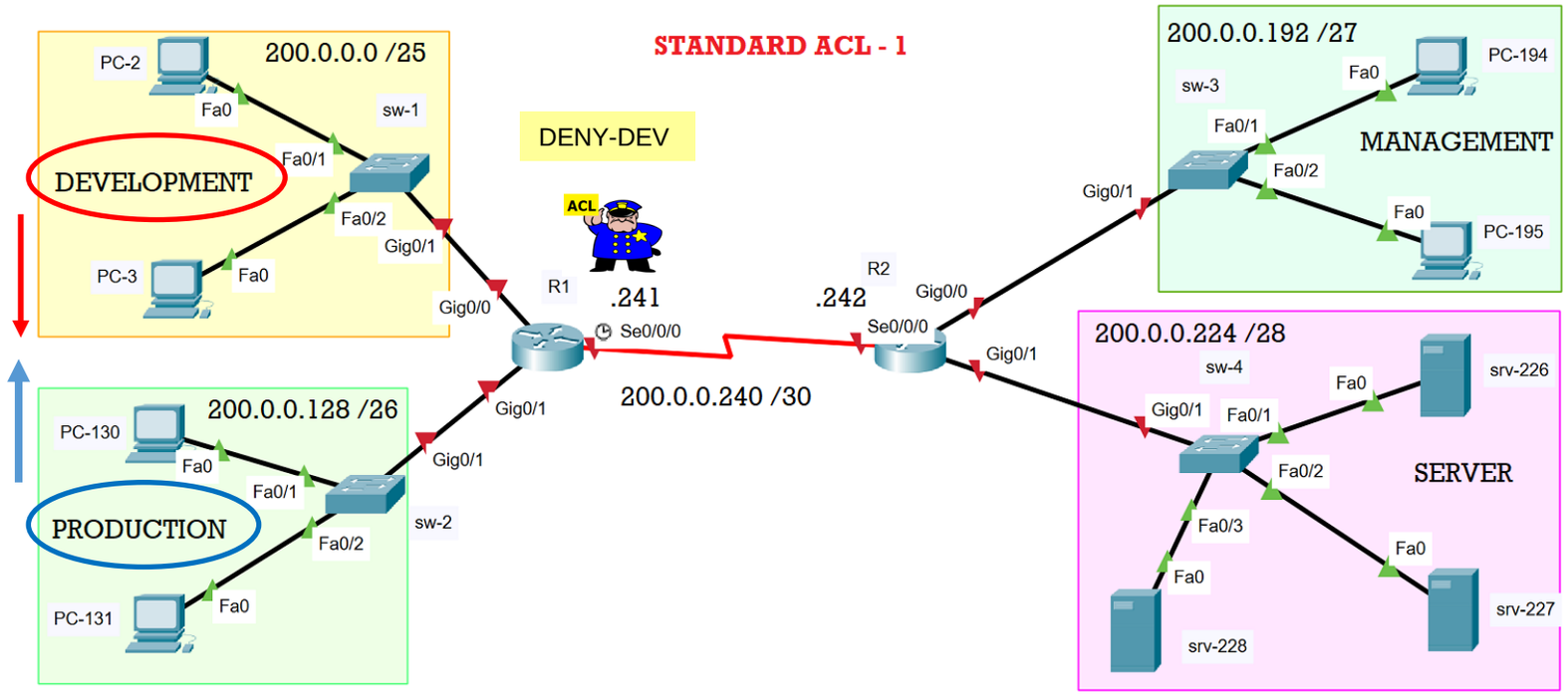
- R1(config)# ip access-list standard DENY-DEV
- R1(config-std-nacl)# 10 deny 200.0.0.0 0.0.0.127
- R1(config-std-nacl)# exit
- R1(config)# interface s0/0/0
- R1(config-if)# ip access-group DENY-DEV out
- R1(config-if)# end



Standard ACL - 1

Production ska ha åtkomst endast till Development, inte till Management och inte heller till server

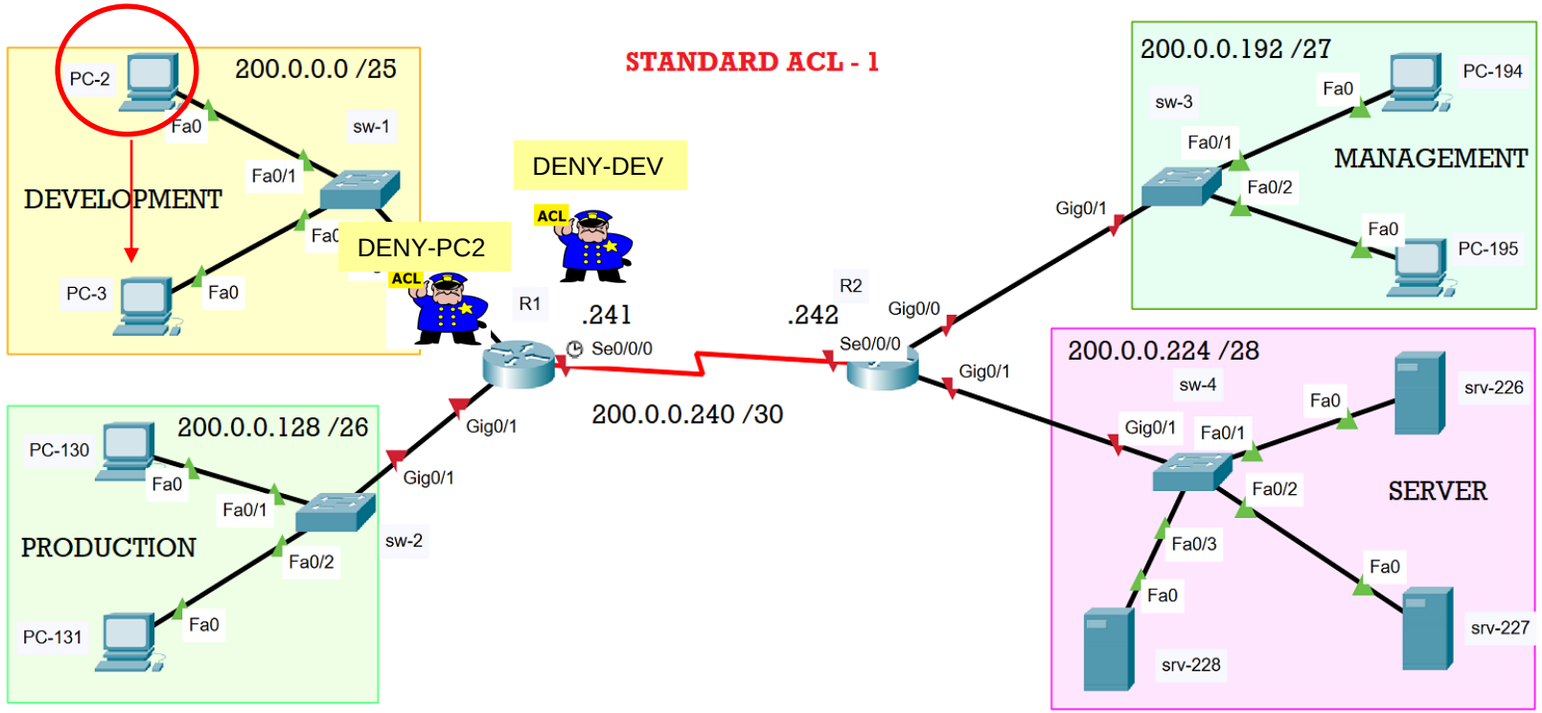
- R1(config)# ip access-list standard DENY-DEV
- R1(config-std-nacl)# 20 deny 200.0.0.128 0.0.0.63
- R1(config-std-nacl)# exit
- R1(config)#



Standard ACL - 1

Endast PC-2 med IP-adress 200.0.0.2 från Development har ingen åtkomst till andra delnät förutom sitt eget.

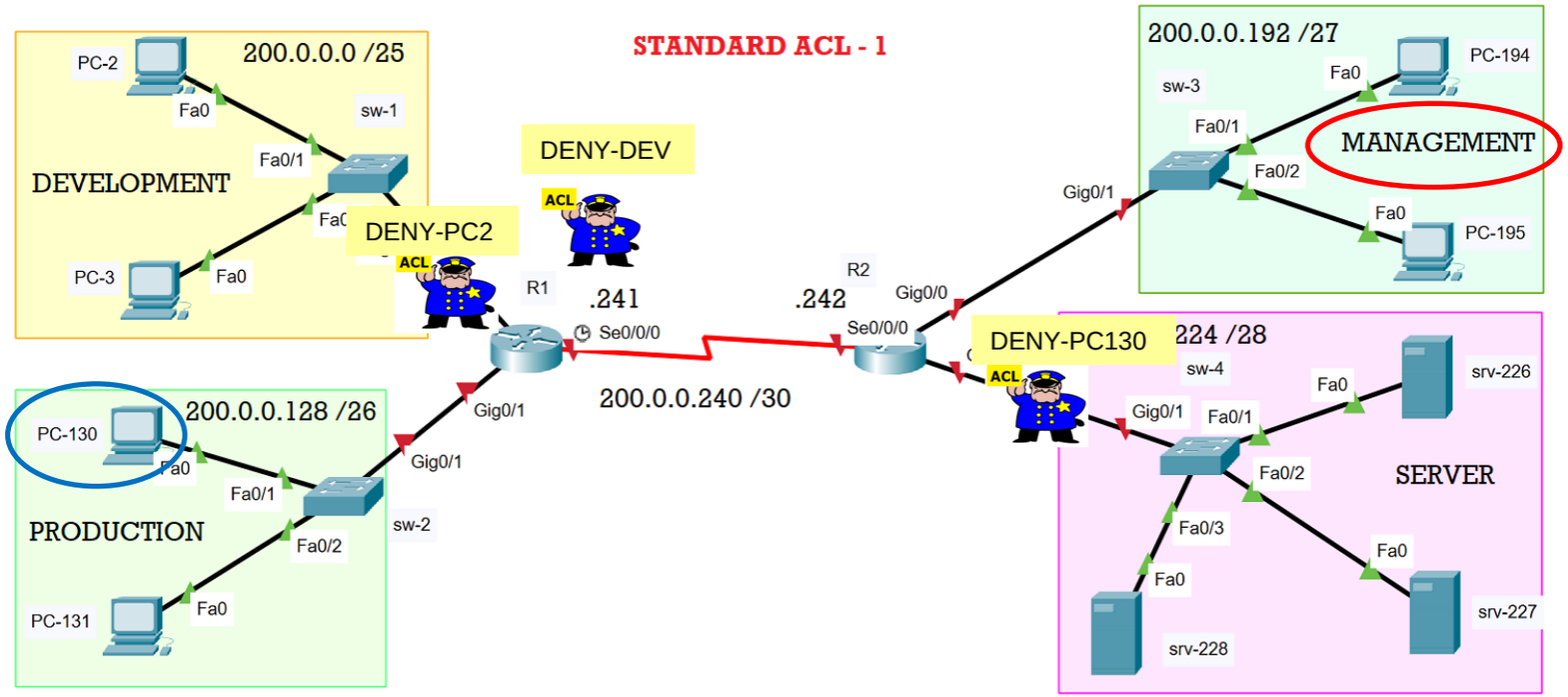
- R1(config)# ip access-list standard DENY-PC2
- R1(config-std-nacl)# 10 deny host 200.0.0.2
- R1(config-std-nacl)# 20 permit any
- R1(config-std-nacl)# exit
- R1(config)# interface G0/0
- R1(config-if)# ip access-group DENY-PC2 in
- R1(config-if)# end
- R1# show access-lists



Standard ACL - 1

Endast PC-130 med IP-adress 200.0.0.130 från Production har åtkomst till Management, men inte till Server.

- Här behöver vi ett undantag för PC-130 som inkluderas i DENY-DEV ACL tillämpad på R1.
- Vi behöver en ny ACL på router R2 som ska blockera PC-130 att komma åt till SERVER nätverk.



Standard ACL - 1

Endast PC-130 med IP-adress 200.0.0.130 från Production har åtkomst till Management, men inte till server.

- Här behöver vi ett undantag för PC-130 som inkluderas i DENY-DEV ACL tillämpad på R1.
- Vi behöver en ny ACL på router R2 som ska blockera PC-130 att komma åt till SERVER nätverk.
- R1(config)#ip access-list standard DENY-DEV
- R1(config-std-nacl)#11 permit host 200.0.0.130
- R1(config-std-nacl)#exit
- R2(config)#ip access-list standard DENY-PC130
- R2(config-std-nacl)#10 deny host 200.0.0.130
- R2(config-std-nacl)#20 permit any
- R2(config-std-nacl)#exit
- R2(config)#
- R2(config)#interface G0/1
- R2(config-if)#ip access-group DENY-PC130 out
- R2(config-if)#exit
- R2(config)#
- Verifiera konfigurationerna.

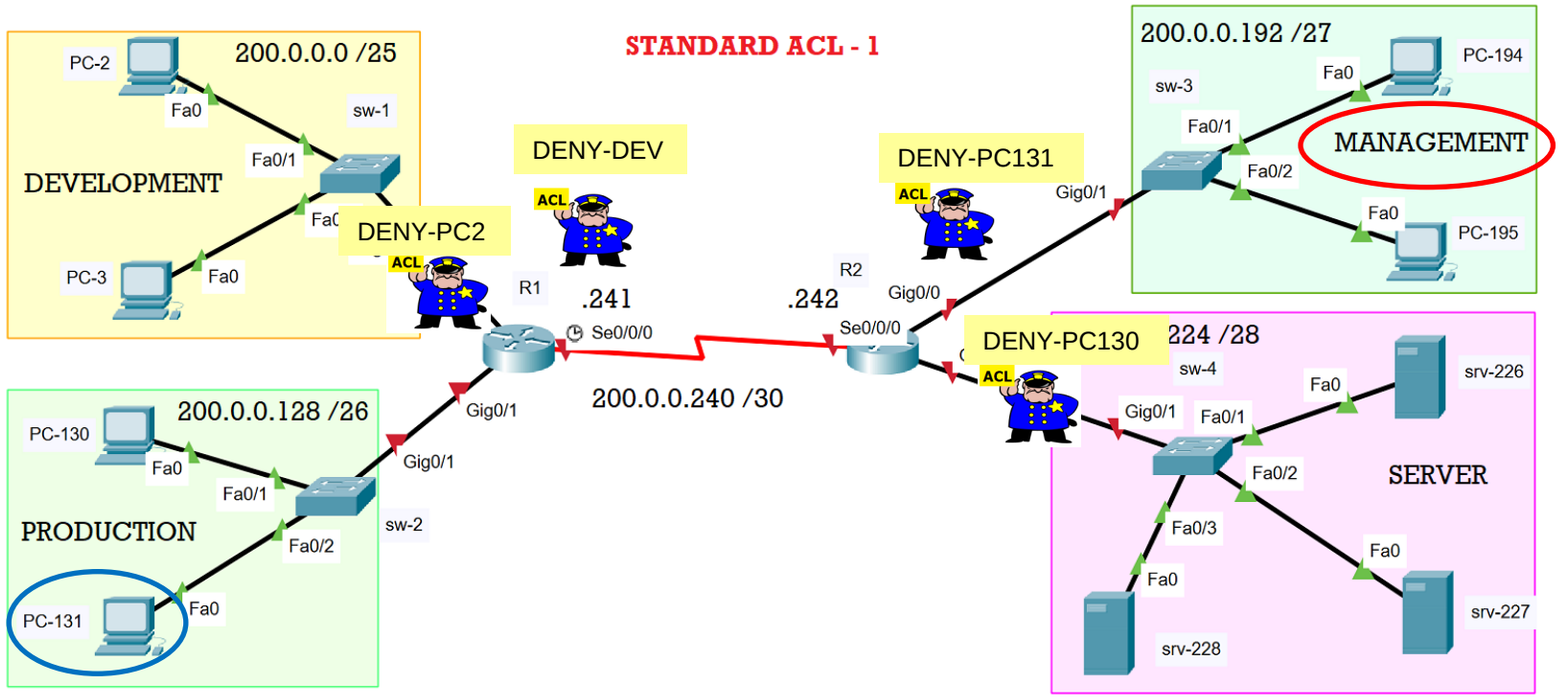
```
R1#show access-lists
Standard IP access list DENY-DEV
    10 deny 200.0.0.0 0.0.0.127 (24 match(es))

    20 deny 200.0.0.128 0.0.0.63 (8 match(es))
```

Standard ACL - 1

Endast PC-131 med IP-adress 200.0.0.131 från Production har åtkomst till Server, men inte till Management.

- Här behöver vi ett undantag för PC-131 som inkluderas i DENY-DEV ACL tillämpad på R1.
- Vi behöver en ny ACL på router R2 som ska blockera PC-131 att komma åt till Management nät.



Standard ACL - 1

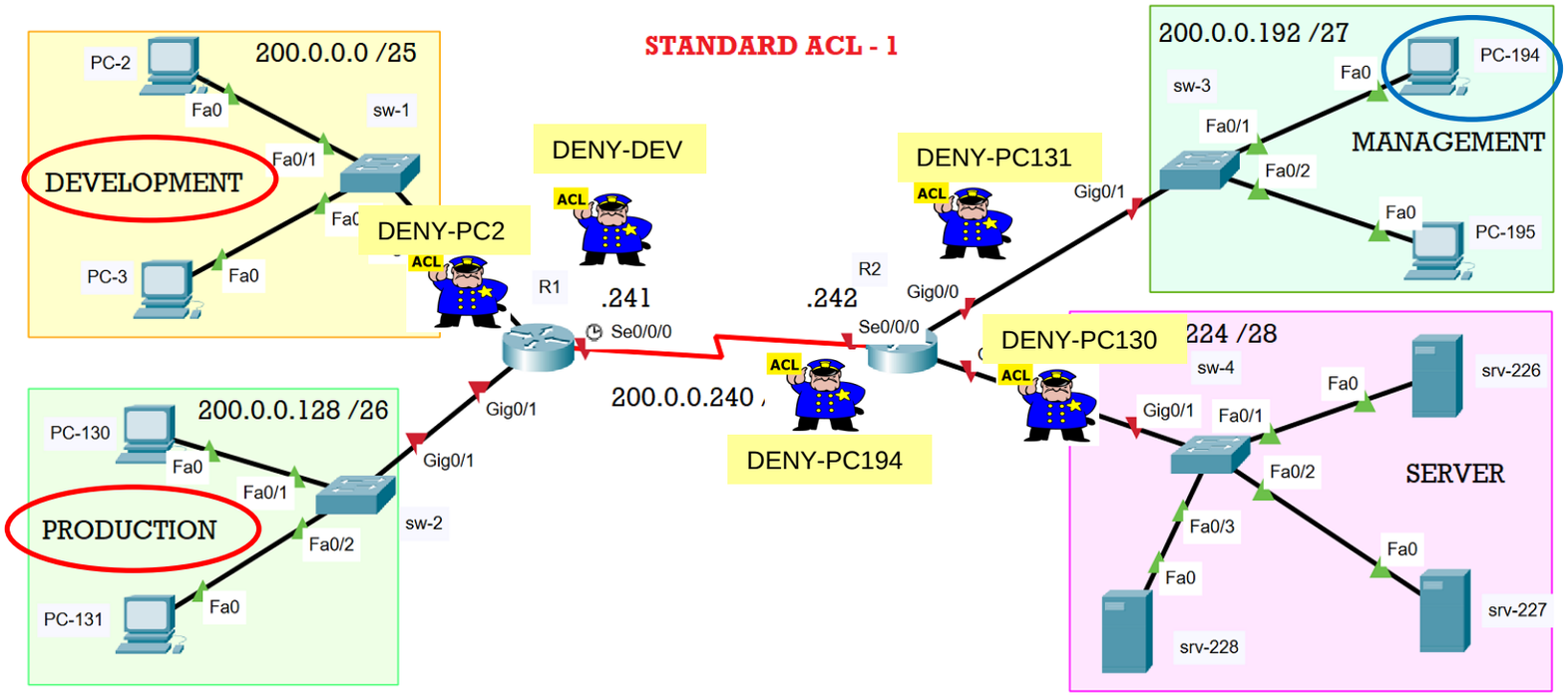
Endast PC-131 med IP-adress 200.0.0.131 från Production har åtkomst till Server, men inte till Management.

- Här behöver vi ett undantag för PC-131 som inkluderas i DENY-DEV ACL tillämpad på R1.
- Vi behöver en ny ACL på router R2 som ska blockera PC-131 att komma åt till Management nät.
- R1(config)#ip access-list standard DENY-DEV
- R1(config-std-nacl)#12 permit host 200.0.0.131
- R1(config-std-nacl)#exit
- R2(config)#ip access-list standard DENY-PC131
- R2(config-std-nacl)#deny host 200.0.0.131
- R2(config-std-nacl)#permit any
- R2(config-std-nacl)#exit
- R2(config)#
- R2(config)#int G0/0
- R2(config-if)#ip access-group DENY-PC131 out
- R2(config-if)#exit
- R2(config)#
- Verifiera att endast PC-131 kan komma åt SERVER nätverk, men inte till MANAGMENT nätverk

Standard ACL - 1

Endast PC-194 med IP-adress 200.0.0.194 från Management har åtkomst till SERVER, men inte till Development och inte heller till Production.

- Vi behöver skapa en access list på R2 som blockerar PC-194 åtkomst till DEVELOPMENT och PRODUCTION



Standard ACL - 1

Endast PC-194 med IP-adress 200.0.0.194 från Management har åtkomst till SERVER, men inte till Development och inte heller till Production.

- Vi behöver skapa en access list på R2 som blockerar PC-194 åtkomst till DEVELOPMENT och PRODUCTION
- R2(config)#ip access-list standard DENY-PC194
- R2(config-std-nacl)#10 deny host 200.0.0.194
- R2(config-std-nacl)#20 permit any
- R2(config-std-nacl)#exit
- R2(config)#interface s0/0/0
- R2(config-if)#ip access-group DENY-PC194 out
- R2(config-if)#exit
- Verifiera


DIGINTO
Nätverkssäkerhet