



ACL



Hoofdstuk 8



Inleiding



ACL werking



IPv4 ACL aanmaken



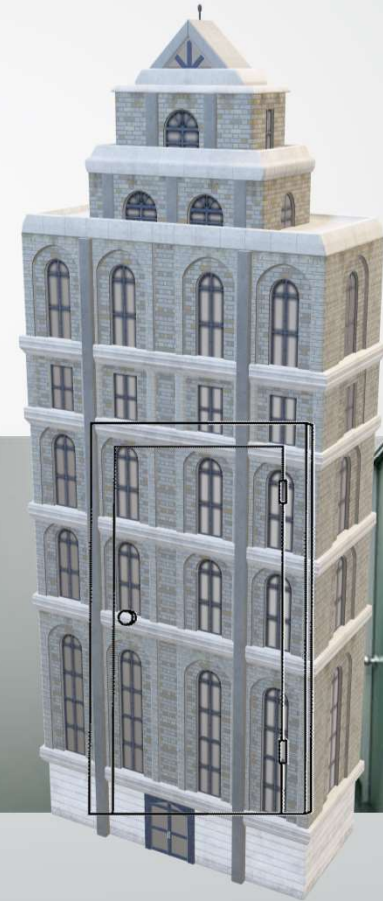
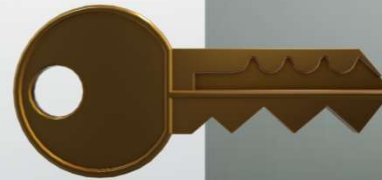
Troubleshooting

Inleiding

- ➔ ACL = Access Control List
 - ✓ Security feature
 - ✓ Netwerk trafiek filteren
 - ✓ Gelijkaardig met een firewall

Inleiding

- ➔ Je kan dit vergelijken met een gebouw
- ➔ Je hebt een bepaalde sleutel nodig
- ➔ Je kan hier specifieke deuren mee openen



ACL werking

- ➔ ACL = series van commands
- ➔ Controle of een router een packet forward of dropped



ACL werking

➔ ACL taken:

- ✓ Limiteert network trafiek
- ✓ Traffic flow control
- ✓ Basis security
- ✓ Filtering op type
- ✓ Hosts screenen op permission



ACL werking

→ ACL standaard niet actief

→ 1 entry in de lijst = ACE (access Control Entry)

ACL werking

➔ Packet filtering op layer 3 & 4

- ✓ Source IP bekijken van een packet
- ✓ Lijst afgaan in de ACL (sequentiëel)
- ✓ Tot juiste ACE tegenkomt



ACL werking

→ Eerste entry in de ACL = prioriteit

⇒ Onderste = laagste priority.

→ Laatste ACE = altijd een deny



Als de source IP met geen enkele ACE matched word die laatste deny regel toegepast



ACL werking

➔ ACL richtingen

Inbound ACL

Outbound ACL

ACL werking

Inbound ACL

- ➔ Filteren pakketten die toekomen op interface
- ➔ Gerouteerd naar outbound interface

ACL werking

FUTURE-PROOF

PEOPLE-CENTRIC

Inbound ACL

Outbound ACL

ACL werking

Outbound ACL

- Filteren pakketten na routing
- Ongeacht inbound interface

ACL werking

➔ ACL gebruikt een wildcard

- ✓ Wildcard bevat 32 bits
- ✓ Zoals een subnetmask gebruikt het de enen en nullen
- ✓ Volgen andere regels dan een subnetmask

ACL werking

➞ Wildcard:

✓ binaire enen en nullen om individuele IPv4 adressen of groepen te filteren

⇒ 0 = match de overeenkomende bit vanuit het adres

⇒ 1 = negeer de overeenkomende bit vanuit het adres

ACL werking

➔ Wildcard vinden:

- ✓ Neem het subnetmask van je range
- ✓ Zet die onder 255.255.255.255
- ✓ Trek het subnetmask af van dit en je krijgt je wildcard

$$\begin{array}{r} 255.255.255.255 \\ - 255.255.255.000 \\ \hline \end{array}$$

255

$$\begin{array}{r} 255.255.255.255 \\ - 255.255.255.240 \\ \hline \end{array}$$

15

$$\begin{array}{r} 255.255.255.255 \\ - 255.255.254.000 \\ \hline \end{array}$$

1.255



ACL werking

➞ Speciale adressen:

⇒ 0.0.0.0

✓ 1 specifiek adres

✓ Vervangen door parameter *“host”*

```
R1# config t  
R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0
```



```
R1# config t  
R1(config)# access-list 1 permit host 192.168.10.10
```

ACL werking

➞ Speciale adressen:

⇒ 255.255.255.255

✓ Alle adressen

✓ Vervangen door parameter "any"

```
R1# config t  
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
```



```
R1# config t  
R1(config)# access-list 1 permit any
```

ACL werking

➔ Algemene regels voor ACLs:

✓ Één ACL per protocol



✓ Één ACL per richting



✓ Één ACL per interface



IPv4 ACL aanmaken

➔ Voor je start eerst:

✓ Nadenken en ontwerpen

⇒ Stel eerst gerichte vragen



IPv4 ACL aanmaken

➔ Ontwerpen ACLs:

- ✓ Gebruik van ACL?
- ✓ Permit of deny?
- ✓ Welke prioriteit in de lijst?
- ✓ Welke adressen?



IPv4 ACL aanmaken

➔ Het command bestaat uit verschillende delen.

✓ **Router(config)#** access-list "*access-list-number*" {deny|permit |remark} "*source*" [source-wildcard][log]

```
R1# config t
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
```

IPv4 ACL aanmaken

➔ Het command bestaat uit verschillende delen.

✓ **Router(config)#** access-list 'access-list-number' {deny|permit |remark} "source" [source-wildcard][log]

```
R1# config t
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
```



IPv4 ACL aanmaken

➔ Het command bestaat uit verschillende delen.

✓ **Router(config)#** access-list **"access-list-number"** [deny|permit |remark} "source" [source-wildcard][log]

```
R1# config t
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
```


IPv4 ACL aanmaken

➔ Het command bestaat uit verschillende delen.

✓ **Router(config)#** access-list "*access-list-number*" {deny|permit |remark} "*source*" [source-wildcard][log]

```
R1# config t
R1(config)# access-list 1 permit 192.168.10 0.0.0.0.255
```

IPv4 ACL aanmaken

➔ Het command bestaat uit verschillende delen.

✓ **Router(config)#** access-list "*access-list-number*" {deny|permit |remark} "*source*" [source-wildcard][log]

```
R1# config t
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
```

IPv4 ACL aanmaken

➔ Het command bestaat uit verschillende delen.

✓ **Router(config)#** access-list "*access-list-number*" {deny|permit |remark} "*source*" [source-wildcard] [log]

```
R1# config t
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
```

IPv4 ACL aanmaken

➔ Naam geven aan access list:

⇒ Makkelijker herkennen en functie weergeven

```
R1# config t
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

IPv4 ACL aanmaken

➔ Wijs de access list toe aan een interface:

✓ **Router(config-if)# ip access-group { access-list-number | access-list-name } { in | out }**


```
R1# config t
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface serial 0/0/0
R1(config-if)# ip access-group 1 out
```

IPv4 ACL aanmaken

➔ Wijs de access list toe aan een interface:

✓ Router(config-if)# **ip access-group** { access-list-number | access-list-name } { in | out }

```
R1# config t
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface serial 0/0/0
R1(config-if)# ip access-group 1 out
```




IPv4 ACL aanmaken

➔ Wijs de access list toe aan een interface:

✓ **Router(config-if)# ip access-group** { access-list-number | access-list-name } { in | out }

```
R1# config t
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface serial 0/0/0
R1(config-if)# ip access-group 1 out
```



IPv4 ACL aanmaken

➔ Wijs de access list toe aan een interface:

✓ **Router(config-if)# ip access-group { access-list-number | access-list-name } { in | out }**

```
R1# config t
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface serial 0/0/0
R1(config-if)# ip access-group 1 out
```

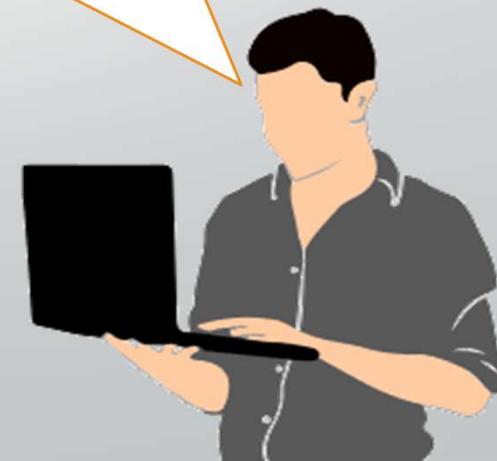

IPv4 ACL aanmaken

- ➔ Range toelaten – 192.168.10.0/24
- ➔ Specifiek adres blokkeren – 192.168.10.10

```
R1# config t
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# INTERFACE S0/0/0
R1(config-if)# ip access-group 1 out
```

Als je deze acties in je ACL wil, wat is dan de juiste volgorde van ingeven?

Dat doe ik zo



IPv4 ACL aanmaken

➔ Entries sequence numbers geven:

⇒ Custom volgorde dat gegevens worden uitgelezen

```
R1# config t
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.11
R1(config-std-nacl)# end
```

TIP

- Gebruik dit bij het bijplaatsen van entries tussen de bestaande entries

IPv4 ACL aanmaken



Beveilig VTY lijnen met een ACL

TIP

➔ Meer controle:

⇒ Wie heeft toegang?

⇒ Bovenop paswoord = extra veilig

```
R1# config t
R1(config)# line vty 0 15
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# access-class 21 in
R1(config-line)# exit
R1(config)# access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 21 deny any
```

Troubleshooting



➔ Als ACL activeren problemen geeft:

- ✓ PC's die geen toegang meer hebben
- ✓ Netwerken communiceren niet meer goed
- ✓ Je kan aan resources niet meer aan

Troubleshooting



➔ Kijk na:

- ✓ Staat de ACL wel op de juiste interface?
- ✓ Staat het in de juiste richting? (inbound/outbound)
- ✓ Is je adres info voor de ACL juist?
- ✓ Heb je de juiste wildcard gebruikt?

Troubleshooting

➞ gebruik:

⇒ *"show access-list"*

- ✓ Toont inhoud lijst
- ✓ Iets geblokeerd zonder de rest toe te staan?



Troubleshooting

➔ show access-list

```
R1# show access-list
Standard IP access list 10
 10 deny 192.168.11.10
R1#
```

Als ik het “show access-list” command ingeef krijg ik dit als resultaat. Wat is mijn probleem?

Op het einde staat er altijd een “deny all”, dus nu is er niets toegelaten!



Troubleshooting

➔ show access-list

Ja, als het doel is om enkel dit IP te blokkeren. Dan zorgen we dat de rest word toegelaten.

Kunnen we dit oplossen?

```
R1(config)# access-list 10 permit any
R1(config)# end
R1# show access-list
Standard IP access list 10
 10 deny 192.168.11.10
 20 permit any (4 match(es))
R1#
```





PT_ACL

Practice
Makes Perfect

